

(19) 世界知的所有権機関
国際事務局



(43) 国際公開日
2007年8月23日 (23.08.2007)

PCT

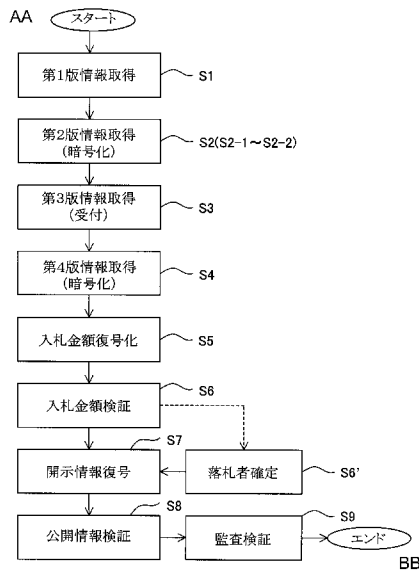
(10) 国際公開番号
WO 2007/094043 A1

- (51) 国際特許分類: *H04L 9/32* (2006.01) *G06Q 30/00* (2006.01)
G06Q 10/00 (2006.01) 原区上小田中4丁目1番1号富士通株式会社内 Kanagawa (JP).
- (21) 国際出願番号: PCT/JP2006/302522
- (22) 国際出願日: 2006年2月14日 (14.02.2006)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (71) 出願人 (米国を除く全ての指定国について): 富士通株式会社 (FUJITSU LIMITED) [JP/JP]; 〒2118588 神奈川県川崎市中原区上小田中4丁目1番1号 Kanagawa (JP).
- (72) 発明者; および
- (75) 発明者/出願人 (米国についてのみ): 吉岡 孝司 (YOSHIOKA, Takashi) [JP/JP]; 〒2118588 神奈川県川崎市
- (74) 代理人: 赤澤 日出夫 (AKAZAWA, Hideo); 〒1640001 東京都中野区中野4-5-1 中野K Iビル4階 Tokyo (JP).
- (81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.
- (84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY,

[続葉有]

(54) Title: ELECTRONIC BIDDING/BIDDING OPENING PROGRAM, ELECTRONIC BIDDING/BIDDING OPENING SYSTEM, AND ELECTRONIC BIDDING/BIDDING OPENING METHOD

(54) 発明の名称: 電子入札/開札プログラム、電子入札/開札システム、及び電子入札/開札方法



- AA START
- S1 ACQUIRE FIRST EDITION INFORMATION
- S2 ACQUIRE SECOND EDITION INFORMATION (ENCRYPTION)
- S3 ACQUIRE THIRD EDITION INFORMATION (RECEPTION)
- S4 ACQUIRE FOURTH EDITION INFORMATION (ENCRYPTION)
- S5 DECRYPT BID AMOUNT OF MONEY
- S6 VERIFY BID AMOUNT OF MONEY
- S7 DECRYPT DISCLOSURE INFORMATION
- S6' DECIDE BIDDING WINNER
- S8 VERIFY PUBLIC INFORMATION
- S9 VERIFY AUDIT
- BB END

(57) Abstract: It is possible to provide an electronic bidding/bidding opening program capable of guaranteeing validity of bidding information and checking whether the bidding information has been tampered. A predetermined validity concerning a bidding winning process is verified by acquiring bidding information, partial identification information expressing each part of the bidding information which can be distinguished from the other part, a plurality of information obtained by encrypting a plurality of appropriate positions of the bidding information, and information obtained by encrypting the partial identification information and an amount of money added by a signature of a staff in charge and using a predetermined combination of some of the aforementioned information.

(57) 要約: 入札情報の正当性を保証し、更には入札情報の改ざんの有無の証明を行うことを可能とする電子入札/開札プログラム等を得る。入札情報と、入札情報の各部分を他の部分から識別可能に表す部分識別情報と、入札情報の複数の適所のそれぞれを暗号化した複数の情報及び、それらの部分識別情報及び金額を暗号化した情報に受付担当者の署名を付した情報とを取得し、これら複数の情報のうちのいずれかの情報の所定の組み合わせにより落札処理に関する所定の正当性を検証する。

WO 2007/094043 A1



KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

2文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

添付公開書類:

— 国際調査報告書

明 細 書

電子入札／開札プログラム、電子入札／開札システム、及び電子入札／開札方法

技術分野

[0001] 本発明は、複数のエンティティを電子文書が流通する際に、入札情報の正当性を保証し、更には入札情報の改ざんの有無の証明を行うことを可能とする電子入札／開札プログラム、電子入札／開札システム、及び電子入札／開札方法に関するものである。

背景技術

[0002] 近年のITの進展に伴い、行政文書や民間企業の帳簿、契約書等の形態は、従来の紙文書での運用、保管から電子(デジタル)文書へと徐々に移行されつつある。具体的には、スキャナ装置の普及に伴い、従来紙で保存されていた文書を容易に電子データ化することが可能となった。更に、高解像度を内蔵するイメージスキャナの実用化に伴い、一定のセキュリティ要件を満足すれば従来認められなかった紙文書の電子保存が容認されるようになった(e-文書法:2005年4月施行に伴う)。

[0003] 一方、このような文書の電子保存要求の増加とともに、電子文書を安全に保管、管理する技術の必要性が高まっている。従来、紙として保存されていた文書を、紙と同等の証拠能力を維持した状態で電子的に保存するためには、“改ざん検出”、“改ざん防止”、“作成者の識別”、“アクセス管理又はその制御”、“履歴管理”等の技術要件を満たす必要があるとされている。このような要件を満たすためには、従来の文書管理システムでは機能不足であり、最近では、このような技術要件を満足する「原本性保証システム」の開発、市場投入が急速に進んでいる。

[0004] この「原本性保証システム」において、最も一般的に用いられているセキュリティ要素技術に電子署名とタイムスタンプがある。電子署名は、文書の作成者(本人性)を特定できるのと同時に、その文書が作成時点から変更がないこと(非改ざん性)を第三者に証明することができると共に、第三者により確認することができる技術である。またタイムスタンプは、電子署名の機能を有すると共に、電子文書の確定時刻を証明

することができるという機能を有する。

[0005] 上記のような技術を利用して実現されている従来の原本性保証の考え方は、確定された最終形態の文書を原本として安全に管理するというように、いわゆる紙文書を鍵付き書庫等に保管するのと同様、原本の所在が明確である文書を対象としている。このような環境下においては、電子署名、タイムスタンプは本人性や非改ざん性を保証するのに非常に有効な技術となる(例えば下記特許文献1, 2、非特許文献1参照)。

[0006] 特許文献1, 2は、電子文書の原本性を確保する技術である。また、非特許文献1は、電子文書の墨塗り問題を解決する技術であり、また、非特許文献2は、開示部分に対する追加的な墨塗りの可否を制御可能とする電子文書墨塗り技術について提案したものである。

特許文献1:特開2000-285034号公報

特許文献2:特開2001-117820号公報

非特許文献1:情報処理学会/コンピュータセキュリティ研究会(CSEC)論文「電子文書墨塗り問題(2003/7/17)(2003-CSEC-22-009)」

非特許文献2:SCIS2004論文「開示条件を制御可能な電子文書墨塗り技術」

発明の開示

発明が解決しようとする課題

[0007] しかしながら、申請書や稟議書のように、文書に直接、追加や訂正、秘匿等の部分操作がなされ、転々流通する文書の原本性保証を考慮した場合、一般的な電子署名、タイムスタンプの方式では、その性質上、一切の加工が許されないため、逆に障害となる。上述の従来技術では、以上のような点が考慮されておらず、電子署名を使って電子データを完全なまま保存するための技術が中心であった。つまり、電子署名付き文書に対して一部変更を行うと署名検証に失敗してしまい、その結果、一部変更文書の完全性が保証することができなかった。

[0008] また、その回避策として、一部変更した文書を新たな版数として更新し、この一部変更文書に対して電子署名を付与すれば署名検証は成功するが、変更箇所以外の改ざん(変更)を検出することができなかった。正当な変更の事例として情報公開法、個

個人情報保護法に基づく非開示部分の墨塗り処理があるが、墨塗り処理と同時に他の開示箇所を不正に変更しても検出できないという課題があった。

[0009] また、電子入札／開札システムの現状の課題としては、(1)入札受付担当者が入札者の結託、(2)開札担当者が入札者の結託、(3)入札情報の公開時のプライバシー不考慮などの問題がある。

[0010] まず、(1)入札受付担当者が入札者の結託では、例えば、以下のような場合があげられる。

[0011] 入札受付担当者とB社が結託したとする。この場合、B社には受付終了時刻間際まで入札行為を保留させ、その最低金額、この例ではC社が入札した¥3,000が最低金額と判断してB社へ通知する。B社はその最低金額を更に下回る¥2,000を入札し、落札させるという不正行為である。これは、入札受付担当者がその他の入札者(A社、C社)が入札した金額を事前に参照することが可能になることから生じる。

[0012] 次に、(2)開札担当者が入札者の結託では、例えば以下のような場合があげられる。

[0013] 例えば、開札担当者でB社の結託を考えた場合、落札者は最低金額の¥3,000を提示したC社にも係らず、B社が入札金額に対し、最低金額の¥3,000を更に下回る¥2,000に書き換え、B社を故意的に落札させるという不正行為である。これも、開札担当者がその他の入札者(A社、C社)が入札した金額を事前に参照することが可能になることから生じる。加えて、入札時点の情報が正しく使われているかどうか必ずしもチェックされていないことも原因のひとつとして考えられる。

[0014] 最後に、(3)入札情報の公開時のプライバシー不考慮については、閲覧者等の第三者に公開される際、落札者以外の情報まですべて開示され、プライバシー情報の保護が考慮されていないのが現状である。2005年4月に施行された個人情報保護法の観点からこれらの入札情報は非開示とすべき項目であるのは自明である。また、この対策としてプライバシー情報の一部を墨塗りして第三者に公開することが考えられるが、先に示したように従来技術では、墨塗り処理と同時に他の開示箇所を不正に変更しても検出することができず、入札時点の情報を正しく使って開札処理がなされたかどうか判断することができないという課題が残る。

[0015] 本発明は、上述した従来の問題点を解決するためになされたものであり、入札者と入札受付担当者、および入札者と開札担当者の結託や不正を防止（検出）できる電子入札／開札プログラム、電子入札／開札システム、及び電子入札／開札方法を提供する。また、入札時点の情報を使って正しく開札処理していることの証明ができる電子入札／開札プログラム、電子入札／開札システム、及び電子入札／開札方法を提供する。さらに一部秘匿を行っても開札結果の正当性が証明できる電子入札／開札プログラム、電子入札／開札システム、及び電子入札／開札方法を提供する。更には、「いつ」、「誰が」、「何を」、「どのように」に変更等を行ったか、また「どの箇所に対してそれらを行ったか」を証明可能とする電子入札／開札プログラム、電子入札／開札システム、及び電子入札／開札方法を提供することを目的とする。

課題を解決するための手段

[0016] 上述した課題を解決するため、本発明は、電子データで作成される入札情報に基づいて入札及び開札処理をコンピュータにより実行させる電子入札／開札プログラムであって、

前記入札情報と、該入札情報の各部分を他の部分から識別可能に表す部分識別情報とを取得し、それぞれ第1版入札情報及び第1版部分識別情報として登録する第1版情報取得ステップと、前記第1版情報取得ステップにより取得された前記第1版入札情報における入札金額部分を暗号化してなる第2a版入札情報と、該第2a版入札情報の各部分を他の部分から識別可能に表す第2a版部分識別情報とを取得すると共に、前記第1版入札情報における入札者部分を暗号化してなる第2b版入札情報と、該第2b版入札情報の各部分を他の部分から識別可能に表す第2b版部分識別情報とを取得し、それぞれ登録する第2版情報取得ステップと、前記第2版情報取得ステップにより取得された前記第2a版入札情報に対し入札受付担当者による電子署名を施してなる第3版入札情報と、該第3版入札情報の各部分を他の部分から識別可能に表す部分識別情報とを取得し、それぞれ登録する第3版情報取得ステップと、前記3版情報取得ステップにより取得された前記第3版入札情報における入札者部分を暗号化してなる第4版入札情報と、該第4版入札情報の各部分を他の部分から識別可能に表す第4版部分識別情報とを取得し、それぞれ登録する第4版情報

取得ステップと、前記第1版乃至第4版情報取得ステップにより取得された複数の版情報のうちのいずれかの版情報の所定の組み合わせにより落札処理に関する所定の正当性を検証する検証ステップとをコンピュータに実行させる。

- [0017] また、本発明の電子入札／開札プログラムにおいて、前記検証ステップは、前記第4版情報取得ステップにより取得された第4版入札情報および前記第2版情報取得ステップにより取得された第2b版部分識別情報とに基づいて開札時の入札金額の検証を行うことを特徴とする。
- [0018] また、本発明の電子入札／開札プログラムにおいて、前記検証ステップは、前記第4版情報取得ステップにより取得された第4版入札情報において入札金額部分を復号化すると共に、該入札金額部分の部分識別情報を取得し、該部分識別情報を前記第2b版部分識別情報とを比較して行うことを特徴とする。
- [0019] また、本発明の電子入札／開札プログラムにおいて、前記各情報取得ステップで取得される取得情報には、電子署名又はタイムスタンプが付されており、前記検証ステップは、これら電子署名又はタイムスタンプを用いて改ざんの有無を検出することを特徴とする。
- [0020] また、本発明の電子入札／開札プログラムにおいて、前記検証ステップは、落札結果について、落札者とそれ以外の者に応じて部分開示・非開示を行いつつ、それらの情報の正当性を確認させる支援を行うことを特徴とする。
- [0021] また、本発明の電子入札／開札プログラムにおいて、前記各情報取得ステップで取得される全ての取得情報には、電子署名又はタイムスタンプが付されており、前記検証ステップは、これら電子署名又はタイムスタンプが付された前記第1版部分識別情報、前記第2a版部分識別情報、前記第2b版部分識別情報、前記第3版部分識別情報、前記第4版入札情報、及び前記第4版部分識別情報を用いて監査のための検証を行うことを特徴とする。
- [0022] また、本発明の電子入札／開札プログラムにおいて、前記部分識別情報は、入札情報を複数の部分に区切り、各部分の情報を一方向性ハッシュ関数を用いて生成されるハッシュ情報として取得されることを特徴とする。
- [0023] また、本発明は、電子データで作成される入札情報に基づいて入札及び開札処理

を行う電子入札／開札システムであって、前記入札情報と、該入札情報の各部分を他の部分から識別可能に表す部分識別情報とを取得し、それぞれ第1版入札情報及び第1版部分識別情報として登録する第1版情報取得部と、前記第1版情報取得部により取得された前記第1版入札情報における入札金額部分を暗号化してなる第2a版入札情報と、該第2a版入札情報の各部分を他の部分から識別可能に表す第2a版部分識別情報とを取得すると共に、前記第1版入札情報における入札者部分を暗号化してなる第2b版入札情報と、該第2b版入札情報の各部分を他の部分から識別可能に表す第2b版部分識別情報とを取得し、それぞれ登録する第2版情報取得部と、前記第2版情報取得部により取得された前記第2a版入札情報に対し入札受付担当者による電子署名を施してなる第3版入札情報と、該第3版入札情報の各部分を他の部分から識別可能に表す部分識別情報とを取得し、それぞれ登録する第3版情報取得部と、前記3版情報取得部により取得された前記第3版入札情報における入札者部分を暗号化してなる第4版入札情報と、該第4版入札情報の各部分を他の部分から識別可能に表す第4版部分識別情報とを取得し、それぞれ登録する第4版情報取得部と、前記第1版乃至第4版情報取得部により取得された複数の版情報のうちのいずれかの版情報の所定の組み合わせにより落札処理に関する所定の正当性を検証する検証部とを備えてなる。

[0024] また、本発明は、電子データで作成される入札情報に基づいて入札及び開札処理をコンピュータが行う電子入札／開札方法であって、前記入札情報と、該入札情報の各部分を他の部分から識別可能に表す部分識別情報とを取得し、それぞれ第1版入札情報及び第1版部分識別情報として登録する第1版情報取得ステップと、前記第1版情報取得ステップにより取得された前記第1版入札情報における入札金額部分を暗号化してなる第2a版入札情報と、該第2a版入札情報の各部分を他の部分から識別可能に表す第2a版部分識別情報とを取得すると共に、前記第1版入札情報における入札者部分を暗号化してなる第2b版入札情報と、該第2b版入札情報の各部分を他の部分から識別可能に表す第2b版部分識別情報とを取得し、それぞれ登録する第2版情報取得ステップと、前記第2版情報取得ステップにより取得された前記第2a版入札情報に対し入札受付担当者による電子署名を施してなる第3版入札

情報と、該第3版入札情報の各部分を他の部分から識別可能に表す部分識別情報とを取得し、それぞれ登録する第3版情報取得ステップと、前記3版情報取得ステップにより取得された前記第3版入札情報における入札者部分を暗号化してなる第4版入札情報と、該第4版入札情報の各部分を他の部分から識別可能に表す第4版部分識別情報とを取得し、それぞれ登録する第4版情報取得ステップと、前記第1版乃至第4版情報取得ステップにより取得された複数の版情報のうちのいずれかの版情報の所定の組み合わせにより落札処理に関する所定の正当性を検証する検証ステップとを備える。

図面の簡単な説明

- [0025] [図1]本発明の実施の形態を示すブロック図である。
[図2]本発明の実施の形態の概要を示す説明図である。
[図3]本発明の実施の形態の動作を示すフローチャートである。
[図4]第1版情報取得ステップを示す図である。
[図5]第2a版情報取得ステップを示す図である。
[図6]第2b版情報取得ステップを示す図である。
[図7]第3版情報取得ステップを示す図である。
[図8]データベース内の取得情報の保存状態を示す図である。
[図9]第4版情報取得ステップを示す図である。
[図10]入札金額復号ステップを示す図である。
[図11]開札時の入札金額検証ステップを示す図である。
[図12]落札者確定処理を示す図である。
[図13]落札結果公開前の開示情報復号ステップを示す図である。
[図14]落札結果公開時の検証ステップを示す図である。
[図15]監査ステップを示す図である。
[図16]本発明の実施の形態の効果を示す図である。

発明を実施するための最良の形態

- [0026] 以下、本発明の実施の形態を図面を用いて説明する。

図1は本発明の実施の形態における入札／開札システム(以下入開札システムとい

う)のブロック図、図2は本発明の実施の形態の運用形態の概要を示す説明図、図3は実施の形態の動作を示すフローチャートである

[0027] 実施の形態における入札システム100は、図1に示すように、入札情報を受信するデータ受信部1、システム内で後述する種々のデータ処理を行うデータ処理部2、入札の受付担当者との協働により入札受付を行う受付処理部3、開札の際に開札担当者23との協働により開札処理を行う開札処理部4、閲覧者24に開札結果の公開を行う公開処理部5、入札情報及び各種取得情報データを格納するデータベース5とを備える。データ処理部2は、後述するPIAT署名を生成するPIAT署名生成部2a、PIAT署名を検証するPIAT署名検証部2b、情報データの暗号化及び復号化を行う暗号／復号部2cを備える。

[0028] 図2においては、入札受付システム3Aがデータ受信部1と受付処理部3を備え、入札者20A～20Cが入札T1のために使用する入札者側クライアント21A～21Cからの入札情報を受信し、入札の受付担当者22との協働により入札受付T2を行うように構成されている。そして開札処理部4は、開札T5の際に開札担当者23との協働により開札処理を行い、公開処理部5が閲覧者24に開札結果の公開T6を行う。また、監査人24による監査T7が入った場合は入札システム100のデータベースから得られる種々の情報に基づいて監査のための検証が行われる。

[0029] 以下、本発明の実施の形態の動作及びその作用を図3～図16を用いて具体的に説明する。

[0030] (入札時(第1版情報取得):S1)

入札時においては、まず、図3、図4に示すように、入札受付システム100は、各入札者20A～20Cからの入札情報(A～C入札情報)を受信し、入札情報から部分識別情報(入札(原本)情報の各部分及びその記載事項を識別可能に示す情報)の生成を行う。部分識別情報は、入札情報の各部分(例えば、一文字単位、もしくは、XMLデータであれば一要素単位でもよい)に対して変更の有無が確認できるよう各部分のハッシュ情報を算出するとともに、そのハッシュ情報が入札情報どの部分に相当するかの位置情報が記載されている。

[0031] そして、各項目のハッシュ情報の集まりを署名情報として記録する。以下、この機能

(入札情報の各項目に対するハッシュ情報を算出し、各項目のハッシュ情報の集まりを署名情報として生成する機能)を「PIAT署名生成機能」2aと称すると共に、生成された署名情報を「PIAT署名」と称する。

[0032] PIAT署名情報によれば、発注書の変更有無を検出し、かつ、変更箇所(変更位置)を特定し、これらに加えて、変更箇所以外の不変を第三者に証明可能とすることができる。PIAT署名情報から入札情報の内容が容易に推測されては困るため、例えば一方向性ハッシュ関数と乱数を組み合わせて生成するようにすることが好ましい。

[0033] これは例えば、乱数“XYZ”に、“社名A”という文字列を連結し、文字列“XYZ社名A”に対するハッシュ情報、例えば“A01”を生成する。以下、他項目についても同様の生成処理が行われる。この例では乱数を使用しているが、当該目的のために乱数以外の手法を用いても構わない。例えば、その時点で入力した事を示すためのタイムスタンプ等の時刻情報を用いてもよい。

[0034] 入札情報(A[~]C-DOC-1)とPIAT署名(A[~]C-PIAT-1)は、入札者の電子署名とその時点のタイムスタンプ(T1)をそれぞれ付与され、DB(原本保管装置)6に第1版として保存される。なお、実施の形態では、PIAT署名生成機能2aは、入開札システム100内の一つの機能として説明しているが、この機能は入札者側のクライアント21A~21C(入札者側コンピュータ内)に持つようにしてもよい。

[0035] (入札受付前(第2版情報取得):S2)

次に図5、図6に示すように、入開札システム100は、入札受付前に入開札システム100自身の処理として、入札者20A~20Cからの入札情報を受信すると同時に以下2つの処理を行う。

[0036] (処理A:S2-1)入札受付時の入札者と入札受付担当者との結託を防ぐための入札金額の暗号化(図5)。

(処理B:S2-2)入札時の情報を使って開札処理していることを事後保証するための入札者の暗号化(図6)。

[0037] ここで、特に(B)で生成された情報は、開札時における入札金額の正当性検証に利用される。

[0038] (処理A:S2-1)

上記(処理A)の詳細を図5を用いて説明する。この段階では、入札受付時の入札者と入札受付担当者との結託を防ぐため、DB6内に保存された第1版の入札情報(A[~]C -DOC-1)、PIAT署名(A[~]C -PIAT-1)のペアを取り出し、入開札システム100自身が入札金額部分を暗号化(墨塗り)処理する。

[0039] ここでの暗号化とは、入開札システム100しか知り得ない暗号化鍵を別途用意し、この暗号化鍵を用いて各入札者の入札金額部分を暗号化処理することを意味している。このように入札金額部分を暗号化処理することにより、入札受付時に入札受付担当者が各入札者の入札金額を参照することができないため、入札者との結託を防止することが可能となる。

[0040] 各入札者の入札金額部分を暗号化処理した入札情報(A[~]C -DOC-2a)を第2a版として、第1版時同様にPIAT署名生成機能2aを用いて入札情報の各項目に対するハッシュ情報を算出し、各項目のハッシュ情報の集まりをPIAT署名(A[~]C -PIAT-2a)として記録する。

[0041] 更に、入札情報(A[~]C -DOC-2a)とPIAT署名(A[~]C -PIAT-2a)は、入開札システム100の電子署名とその時点のタイムスタンプ(T2a)をそれぞれ付与し、DB6に第2a版として保存する。

[0042] (処理B:S2-2)

上記(処理B)の詳細を図6を用いて説明する。この段階では、入札時の情報を使って開札処理していることを事後保証するため、DB6内に保存された第1版の入札情報(A[~]C -DOC-1)、PIAT署名(A[~]C -PIAT-1)のペアを取り出し、入開札システム100自身が入札者部分を暗号化(墨塗り)処理する。

[0043] ここでの暗号化とは、入開札システム100しか知り得ない暗号化鍵を別途用意し、この暗号化鍵を用いて各入札者の入札者部分を暗号化処理することを示している。入札受付前処理として処理Aでも同様の処理を行ったが、この暗号化鍵は入札者用、入札金額用と項目毎に分けてもよいし、同一でもよい。ただし、この暗号化鍵の保管は入開札システム100の中で安全に保護できる仕組みが必要である。このように入札者部分を暗号化処理することにより、開札時における入札金額の正当性証明を行うことが可能となる。

- [0044] 入開札システム100は、各入札者部分を暗号化処理した入札情報(A~C-DOC-2b)を第2b版として、第1版同様にPIAT署名生成機能を用いて入札情報の各項目に対するハッシュ情報を算出し、各項目のハッシュ情報の集まりをPIAT署名(A~C-PIAT-2b)として記録する。そして、入札情報(A~C-DOC-2b)とPIAT署名(A~C-PIAT-2b)に、入開札システム100の電子署名とその時点のタイムスタンプ(T2b)をそれぞれ付与され、DBに第2b版として保存する。
- [0045] この時点で、第2版は、第2a版、第2b版の2つの系列に分かれて管理され、第2a版は、入札受付時の入札者と入札受付担当者との結託を防ぐための情報として、第2b版は開札時における入札金額の正当性証明の情報として利用される。
- [0046] (入札受付時(第3版情報取得):S3)
入札受付時の詳細を図7を用いて説明する。入札受付時には、DB6内に保存された第2a版の入札情報(A~C-DOC-2a)、PIAT署名(A~C-PIAT-2a)のペアを取り出し、入札受付担当者22が受付処理部3の受付画面にてその内容を確認する。
- [0047] この時、入開札システム100の電子署名とその時点のタイムスタンプを検証することにより、入開札システム100が入札者から正しく受信したことを確認できる。この時点で入札金額は秘匿されているため、入札者と入札受付担当者の結託を阻止することが可能となる。
- [0048] つまり、現実社会における封書による入札行為に例えるならば、封書に入札金額を明記した用紙を格納し、封書の外側には入札者の氏名(会社等)が明記されている状態に相当する。入札受付担当者は封書の上から受付印を押印するようなイメージとなるため、各入札者がいくらで入札したかどうかについてはこの時点では確認することができない。
- [0049] 入札受付担当者22が受付処理を行うと、入開札システム100は、第2a版の入札情報(A~C-DOC-2a)に対して、受付済を示す項目を一部追加し、第3版の入札情報(A~C-DOC-3)を生成する。第1版時同様にPIAT署名生成機能2aを用いて入札情報の各項目に対するハッシュ情報を算出し、各項目のハッシュ情報の集まりをPIAT署名(A~C-PIAT-3)として記録する。
- [0050] 更に、入札情報(A~C-DOC-3)とPIAT署名(A~C-PIAT-3)に、入札受付担当者の

電子署名とその時点のタイムスタンプ(T3)をそれぞれ付与し、DB6に第3版として保存する。

[0051] 図8は、入札受付処理完了時点(第3版生成完了時点)のDB6内の保存状態を示している。第2版は、第2a版、第2b版の2つの系列に分かれて管理されている様子がわかる。

[0052] (開札前(第4版情報取得):S4)

図9に開札前処理において入札暗号化処理を行って第4版を取得する動作を示す。この段階では、開札時の入札者と開札担当者との結託を防ぐため、DB6内に保存された第3版の入札情報(A~C-DOC-3)、PIAT署名(A~C-PIAT-3)のペアを取り出し、入開札システム100自身が入札者部分を暗号化(墨塗り)処理する。ここでの暗号化とは、入開札システム100しか知り得ない暗号化鍵を別途用意し、この暗号化鍵を用いて各入札者の入札者部分を暗号化処理することを意味している。

[0053] このように入札者部分を暗号化処理することにより、開札時に開札担当者が各入札者の情報を参照することができないため、入札者との結託を防止することが可能となる。

[0054] 入開札システム100は、各入札者部分を暗号化処理した入札情報(A~C-DOC-4)を第4版として、第1版同様にPIAT署名生成機能2aを用いて入札情報の各項目に対するハッシュ情報を算出し、各項目のハッシュ情報の集まりをPIAT署名(A~C-PIAT-4)として記録する。また、(A~C-DOC-4)とPIAT署名(A~C-PIAT-4)に、入開札システムの電子署名とその時点のタイムスタンプ(T4)をそれぞれ付与し、DB6に第4版として保存する。

[0055] (入札金額復号:S5)

図10は入札金額復号処理を示す図である。この段階では、DB6内に保存された第4版の入札情報(A~C-DOC-4)、PIAT署名(A~C-PIAT-4)のペアを取り出し、暗号化されている入札金額部分の復号処理を行う。入開札システム100は、第4版取得時において暗号化時に使用した鍵を取り出し、入札金額部分を復号する。

[0056] (開札時)

(入札金額検証:S6)

図11は入札金額検証処理を示す図である。この段階では、入札金額(入札情報)が入札時点の情報を使って正しく処理していることを開札担当者が確認を行う。入札金額の正当性を検証するための情報として、第4版の入札情報(A[~]C-DOC-4)、PIAT署名(A[~]C-PIAT-4)、第2b版のPIAT署名(A[~]C-PIAT-2b)を使用する。

[0057] まず、これら3つの情報に付与された電子署名、タイムスタンプの検証を行い、事後改ざんされていないことを確認する(図中VR-1)。

[0058] 次に、第4版の入札情報(A[~]C-DOC-4)中の受付済部分に対するハッシュ情報を算出し、PIAT署名(A[~]C-PIAT-4)中の受付部分のハッシュ情報(A03)を取り出して双方の比較、検証を行う(図中VR-2)。この比較、検証が同一であれば、この入札情報は正しく受付されていることが確認できる。

[0059] 更に、第4版の入札情報(A[~]C-DOC-4)中の入札金額部分に対するハッシュ情報を算出し、PIAT署名(A[~]C-PIAT-4)中の入札金額部分のハッシュ情報(A02)を取り出して双方の比較、検証を行う(図中VR-3)。この比較、検証が同一であれば、入札金額が入札時点の情報を使って正しく処理していることを確認することが可能となる。

[0060] これらVR-1~VR-3は、PIAT署名検証機能2bとして提供される。ここで、A[~]C-PIAT-2bを生成・保持した理由として再確認してみると、A[~]C-PIAT-1の各情報を用いれば、入札金額が入札時点の情報を使って正しく処理していることを確認することが可能である。しかしながら、A[~]C-PIAT-1には各入札者の電子署名が付与されているため、この時点での入札金額検証には用いることができない。なぜなら、電子署名の確認(図中VR-1)により、誰がいくら入札したかを開札担当者が確認できてしまうからである。したがって、A[~]C-PIAT-2bを入札システム自身が事前に生成・保持しておくことにより、この段階での入札金額の検証に入札者の情報を伏せたまま利用することが可能になる。

[0061] (落札者確定:S6[^])

図12は開札処理部4を用いた落札者確定処理を示す図である。この段階では、開札担当者23は入札金額の正当性を確認後、各入札金額を参考に落札確定処理を行う。この例では、¥3,000を入札した入札者が落札したことを示している。実際に入札者の情報は、S2の開札前に入札者暗号化の段階で暗号化処理して秘匿されている

ため、開札担当者が入札者と入札金額の対応をこの時点ではとることができない。したがって、入札者との結託を防ぐことが可能となる。

[0062] (落札結果公開前)

(開示情報復号:S7)

図13は落札結果公開前における開示情報復号処理を示す図である。この段階では、閲覧者等の第三者に落札結果を公開するため、プライバシー情報の保護を行うことを目的として開示に必要な情報のみの復号を行う。DB6内に保存された第4版の入札情報(A~C-DOC-4)を取り出し、暗号化されている部分の復号処理を行う。

[0063] 具体的には入開札システム100は、暗号化時に使用した鍵を取り出し、落札者以外(本例ではC社が落札したことを既に確認しているため、落札者以外はA社とB社と確認できている)の情報については入札金額部分のみを、落札者(本例ではC社が落札したことを既に確認済み)の情報については、落札者の情報、および落札金額ともに復号する。この例では、落札者以外には、入札金額のみを、落札者にはすべての情報を開示するとしているが、このような方式を取り入れれば、落札者以外の情報は入札金額もすべて伏せ、落札者、落札金額のみを開示させる等の柔軟な対応が可能となる。

[0064] (公開情報検証:S8)

図14は公開情報検証処理を示す図である。この段階では、一部秘匿しても開札結果の正当性を閲覧者等の第三者が確認を行うことができる。開札結果の正当性を検証するための情報として、第4版の入札情報(A~C-DOC-4)、PIAT署名(A~C-PIAT-4)、第2b版のPIAT署名(A~C-PIAT-2b)、第1版(図示しない)のPIAT署名(A~C-PIAT-1)を使用する。第1版のPIAT署名(A~C-PIAT-1)については、この時点で落札者がC社と確認済みのため、C社の第1版のPIAT署名(C-PIAT-1)を使用できる。まず、これら3つの情報に付与された電子署名、タイムスタンプの検証を行い、事後改ざんされていないことを確認する(図中VR-1)。

[0065] 次に、第4版の入札情報(A~C-DOC-4)中の受付済部分に対するハッシュ情報を算出し、PIAT署名(A~C-PIAT-4)中の受付部分のハッシュ情報(A03)を取り出して双方の比較、検証を行う(図中VR-2)。この比較、検証が同一であれば、この入札情

報は正しく受付されていることが確認できる。

[0066] 更に、入札金額の検証については、第4版の入札情報(A[~]C-DOC-4)中の入札金額部分に対するハッシュ情報を算出し、PIAT署名(A[~]C-PIAT-4)中の入札金額部分のハッシュ情報(A02)を取り出して双方の比較、検証を行う(図中VR-3)。この比較・検証が同一であれば、入札金額が入札時点の情報を使って正しく処理していることを確認することが可能となる。

[0067] 更に、落札者および落札金額については落札したC社の第1版のPIAT署名(C-PIAT-1)を使用できるため、VR-3の検証に加え、社名と入札金額双方について入札時点の情報を使って正しく処理していることを確認することが可能となる(図中VR-4)。これらVR-1~VR-4は、PIAT署名検証機能2bとして提供される。

[0068] (監査検証:S9)

図15は監査時の処理を示す図である。この段階では、第三者公的機関等により落札結果の正当性に関する監査を行う。具体的には、DB6内に保存されている第4版の入札情報(A[~]C-DOC-4)、全版数のPIAT署名(A[~]C-PIAT-1~3)を取り出し、PIAT署名検証機能を用いて監査を行う。

[0069] これらの情報を用いてPIAT署名検証を行えば、「いつ」、「誰が」、「何を」、「どのように」に加え、「どの箇所を」の正当性を検証することが可能となる。加えて、S6の開札時の入札金額検証、S7の落札結果公開前の開示情報復号、S8の落札結果公開時の検証同様、VR-1~VR-4の検証を行えば、入札時点の情報を使って正しく処理していることを確認することが可能となる。

[0070] 以上に説明したように、本発明の実施の形態によれば、図16に示すように、以下の5要件を実効あらしめることが明らかである。

(要件1)入札受付担当者と入札者の結託、不正を検出することができ、またそれを防止する。

(要件2)入札時点の情報を使って正しく開札処理していることを証明する。

(要件3)開札担当者と入札者の結託、不正を検出することができ、またそれを防止する。

(要件4)一部秘匿を行っても、開札結果の正当性を証明できる。

(要件5)原本等に対して、「いつ」、「誰が」、「何を」、「どのように」加え、「どの箇所」に対して加えたかを証明できる。

[0071] なお、図示したフローチャートやステップに示された各動作をコンピュータにより実行させるプログラムを提供することにより、本発明の電子入札／開札プログラムを提供することができる。これらプログラムはコンピュータにより読取可能な媒体に記録されてコンピュータにより実行させることができる。ここで、コンピュータにより読取可能な媒体としては、CD-ROMやフレキシブルディスク、DVDディスク、光磁気ディスク、ICカード等の可搬型記憶媒体や、コンピュータプログラムを保持するデータベース、或いは、他のコンピュータ並びにそのデータベースや、更に回線上の伝送媒体をも含むものである。

産業上の利用可能性

[0072] 以上説明したように、本発明によれば、入札情報の正当性を保証し、更には入札情報の改ざんの有無の証明を行うことを可能とすることができる。

請求の範囲

[1] 電子データで作成される入札情報に基づいて入札及び開札処理をコンピュータにより実行させる電子入札／開札プログラムであって、

前記入札情報と、該入札情報の各部分を他の部分から識別可能に表す部分識別情報とを取得し、それぞれ第1版入札情報及び第1版部分識別情報として登録する第1版情報取得ステップと、

前記第1版情報取得ステップにより取得された前記第1版入札情報における入札金額部分を暗号化してなる第2a版入札情報と、該第2a版入札情報の各部分を他の部分から識別可能に表す第2a版部分識別情報とを取得すると共に、前記第1版入札情報における入札者部分を暗号化してなる第2b版入札情報と、該第2b版入札情報の各部分を他の部分から識別可能に表す第2b版部分識別情報とを取得し、それぞれ登録する第2版情報取得ステップと、

前記第2版情報取得ステップにより取得された前記第2a版入札情報に対し入札受付担当者による電子署名を施してなる第3版入札情報と、該第3版入札情報の各部分を他の部分から識別可能に表す部分識別情報とを取得し、それぞれ登録する第3版情報取得ステップと、

前記3版情報取得ステップにより取得された前記第3版入札情報における入札者部分を暗号化してなる第4版入札情報と、該第4版入札情報の各部分を他の部分から識別可能に表す第4版部分識別情報とを取得し、それぞれ登録する第4版情報取得ステップと、

前記第1版乃至第4版情報取得ステップにより取得された複数の版情報のうちのいずれかの版情報の所定の組み合わせにより落札処理に関する所定の正当性を検証する検証ステップと

をコンピュータに実行させる電子入札／開札プログラム。

[2] 請求項1に記載の電子入札／開札プログラムにおいて、

前記検証ステップは、前記第4版情報取得ステップにより取得された第4版入札情報および前記第2版情報取得ステップにより取得された第2b版部分識別情報とに基づいて開札時の入札金額の検証を行うことを特徴とする電子入札／開札プログラム。

- [3] 請求項2に記載の電子入札／開札プログラムにおいて、
前記検証ステップは、前記第4版情報取得ステップにより取得された第4版入札情報において入札金額部分を復号化すると共に、該入札金額部分の部分識別情報を取得し、該部分識別情報を前記第2b版部分識別情報とを比較して行うことを特徴とする電子入札／開札プログラム。
- [4] 請求項2に記載の電子入札／開札プログラムにおいて、
前記各情報取得ステップで取得される取得情報には、電子署名又はタイムスタンプが付されており、前記検証ステップは、これら電子署名又はタイムスタンプを用いて改ざんの有無を検出することを特徴とする電子入札／開札プログラム。
- [5] 請求項2に記載の電子入札／開札プログラムにおいて、
前記検証ステップは、落札結果について、落札者とそれ以外の者に応じて部分開示・非開示を行いつつ、それらの情報の正当性を確認させる支援を行うことを特徴とする電子入札／開札プログラム。
- [6] 請求項1に記載の電子入札／開札プログラムにおいて、
前記各情報取得ステップで取得される全ての取得情報には、電子署名又はタイムスタンプが付されており、前記検証ステップは、これら電子署名又はタイムスタンプが付された前記第1版部分識別情報、前記第2a版部分識別情報、前記第2b版部分識別情報、前記第3版部分識別情報、前記第4版入札情報、及び前記第4版部分識別情報を用いて監査のための検証を行うことを特徴とする電子入札／開札プログラム。
- [7] 請求項1乃至請求項6のいずれかに記載の電子入札／開札プログラムにおいて、
前記部分識別情報は、入札情報を複数の部分に区切り、各部分の情報を一方向性ハッシュ関数を用いて生成されるハッシュ情報として取得されることを特徴とする電子入札／開札プログラム。
- [8] 電子データで作成される入札情報に基づいて入札及び開札処理を行う電子入札／開札システムであって、
前記入札情報と、該入札情報の各部分を他の部分から識別可能に表す部分識別情報とを取得し、それぞれ第1版入札情報及び第1版部分識別情報として登録する第1版情報取得部と、

前記第1版情報取得部により取得された前記第1版入札情報における入札金額部分を暗号化してなる第2a版入札情報と、該第2a版入札情報の各部分を他の部分から識別可能に表す第2a版部分識別情報とを取得すると共に、前記第1版入札情報における入札者部分を暗号化してなる第2b版入札情報と、該第2b版入札情報の各部分を他の部分から識別可能に表す第2b版部分識別情報とを取得し、それぞれ登録する第2版情報取得部と、

前記第2版情報取得部により取得された前記第2a版入札情報に対し入札受付担当者による電子署名を施してなる第3版入札情報と、該第3版入札情報の各部分を他の部分から識別可能に表す部分識別情報とを取得し、それぞれ登録する第3版情報取得部と、

前記3版情報取得部により取得された前記第3版入札情報における入札者部分を暗号化してなる第4版入札情報と、該第4版入札情報の各部分を他の部分から識別可能に表す第4版部分識別情報とを取得し、それぞれ登録する第4版情報取得部と

、
前記第1版乃至第4版情報取得部により取得された複数の版情報のうちのいずれかの版情報の所定の組み合わせにより落札処理に関する所定の正当性を検証する検証部と

を備えてなる電子入札／開札システム。

[9] 請求項8に記載の電子入札／開札システムにおいて、

前記検証部は、前記第4版情報取得部により取得された第4版入札情報および前記第2版情報取得部により取得された第2b版部分識別情報とに基づいて開札時の入札金額の検証を行うことを特徴とする電子入札／開札システム。

[10] 請求項9に記載の電子入札／開札システムにおいて、

前記検証部は、前記第4版情報取得部により取得された第4版入札情報において入札金額部分を復号化すると共に、該入札金額部分の部分識別情報とを取得し、該部分識別情報を前記第2b版部分識別情報とを比較して行うことを特徴とする電子入札／開札システム。

[11] 請求項9に記載の電子入札／開札システムにおいて、

前記各情報取得部で取得される取得情報には、電子署名又はタイムスタンプが付されており、前記検証部は、これら電子署名又はタイムスタンプを用いて改ざんの有無を検出することを特徴とする電子入札／開札システム。

[12] 請求項9に記載の電子入札／開札システムにおいて、

前記検証部は、落札結果について、落札者とそれ以外の者に応じて部分開示・非開示を行いつつ、それらの情報の正当性を確認させる支援を行うことを特徴とする電子入札／開札システム。

[13] 請求項8に記載の電子入札／開札システムにおいて、

前記各情報取得部で取得される全ての取得情報には、電子署名又はタイムスタンプが付されており、前記検証部は、これら電子署名又はタイムスタンプが付された前記第1版部分識別情報、前記第2a版部分識別情報、前記第2b版部分識別情報、前記第3版部分識別情報、前記第4版入札情報、及び前記第4版部分識別情報を用いて監査のための検証を行うことを特徴とする電子入札／開札システム。

[14] 請求項8乃至請求項13のいずれかに記載の電子入札／開札システムにおいて、

前記部分識別情報は、入札情報を複数の部分に区切り、各部分の情報を一方向性ハッシュ関数を用いて生成されるハッシュ情報として取得されることを特徴とする電子入札／開札システム。

[15] 電子データで作成される入札情報に基づいて入札及び開札処理をコンピュータが行う電子入札／開札方法であって、

前記入札情報と、該入札情報の各部分を他の部分から識別可能に表す部分識別情報とを取得し、それぞれ第1版入札情報及び第1版部分識別情報として登録する第1版情報取得ステップと、

前記第1版情報取得ステップにより取得された前記第1版入札情報における入札金額部分を暗号化してなる第2a版入札情報と、該第2a版入札情報の各部分を他の部分から識別可能に表す第2a版部分識別情報とを取得すると共に、前記第1版入札情報における入札者部分を暗号化してなる第2b版入札情報と、該第2b版入札情報の各部分を他の部分から識別可能に表す第2b版部分識別情報とを取得し、それぞれ登録する第2版情報取得ステップと、

前記第2版情報取得ステップにより取得された前記第2a版入札情報に対し入札受付担当者による電子署名を施してなる第3版入札情報と、該第3版入札情報の各部分を他の部分から識別可能に表す部分識別情報とを取得し、それぞれ登録する第3版情報取得ステップと、

前記3版情報取得ステップにより取得された前記第3版入札情報における入札者部分を暗号化してなる第4版入札情報と、該第4版入札情報の各部分を他の部分から識別可能に表す第4版部分識別情報とを取得し、それぞれ登録する第4版情報取得ステップと、

前記第1版乃至第4版情報取得ステップにより取得された複数の版情報のうちのいずれかの版情報の所定の組み合わせにより落札処理に関する所定の正当性を検証する検証ステップと

を備える電子入札／開札方法。

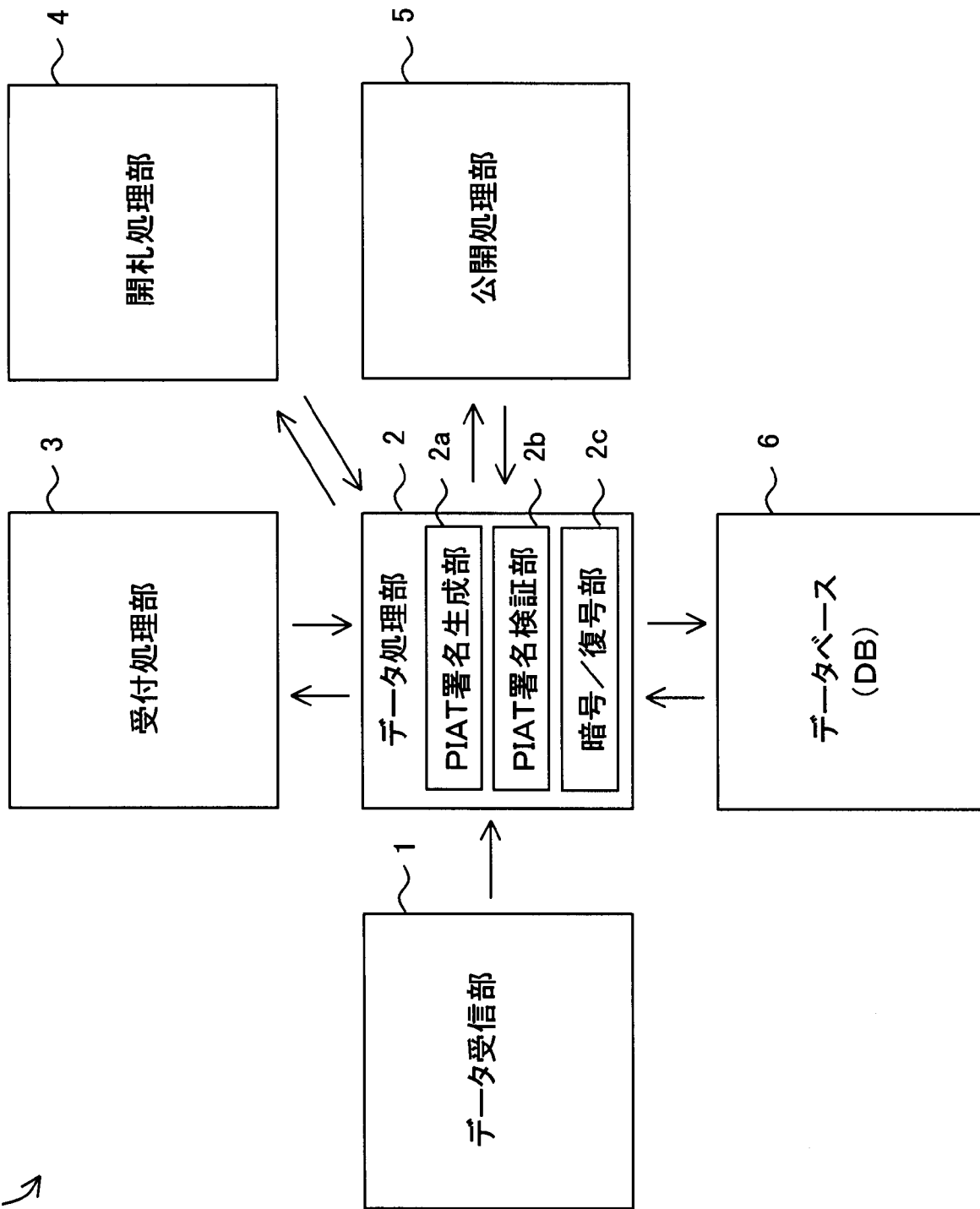
- [16] 請求項15に記載の電子入札／開札方法において、
前記検証ステップは、前記第4版情報取得ステップにより取得された第4版入札情報および前記第2版情報取得ステップにより取得された第2b版部分識別情報とに基づいて開札時の入札金額の検証を行うことを特徴とする電子入札／開札方法。
- [17] 請求項16に記載の電子入札／開札方法において、
前記検証ステップは、前記第4版情報取得ステップにより取得された第4版入札情報において入札金額部分を復号化すると共に、該入札金額部分の部分識別情報を取得し、該部分識別情報を前記第2b版部分識別情報とを比較して行うことを特徴とする電子入札／開札方法。
- [18] 請求項15に記載の電子入札／開札方法において、
前記各情報取得ステップで取得される取得情報には、電子署名又はタイムスタンプが付されており、前記検証ステップは、これら電子署名又はタイムスタンプを用いて改ざんの有無を検出することを特徴とする電子入札／開札方法。
- [19] 請求項16に記載の電子入札／開札方法において、
前記検証ステップは、落札結果について、落札者とそれ以外の者に応じて部分開示・非開示を行いつつ、それらの情報の正当性を確認させる支援を行うことを特徴と

する電子入札／開札方法。

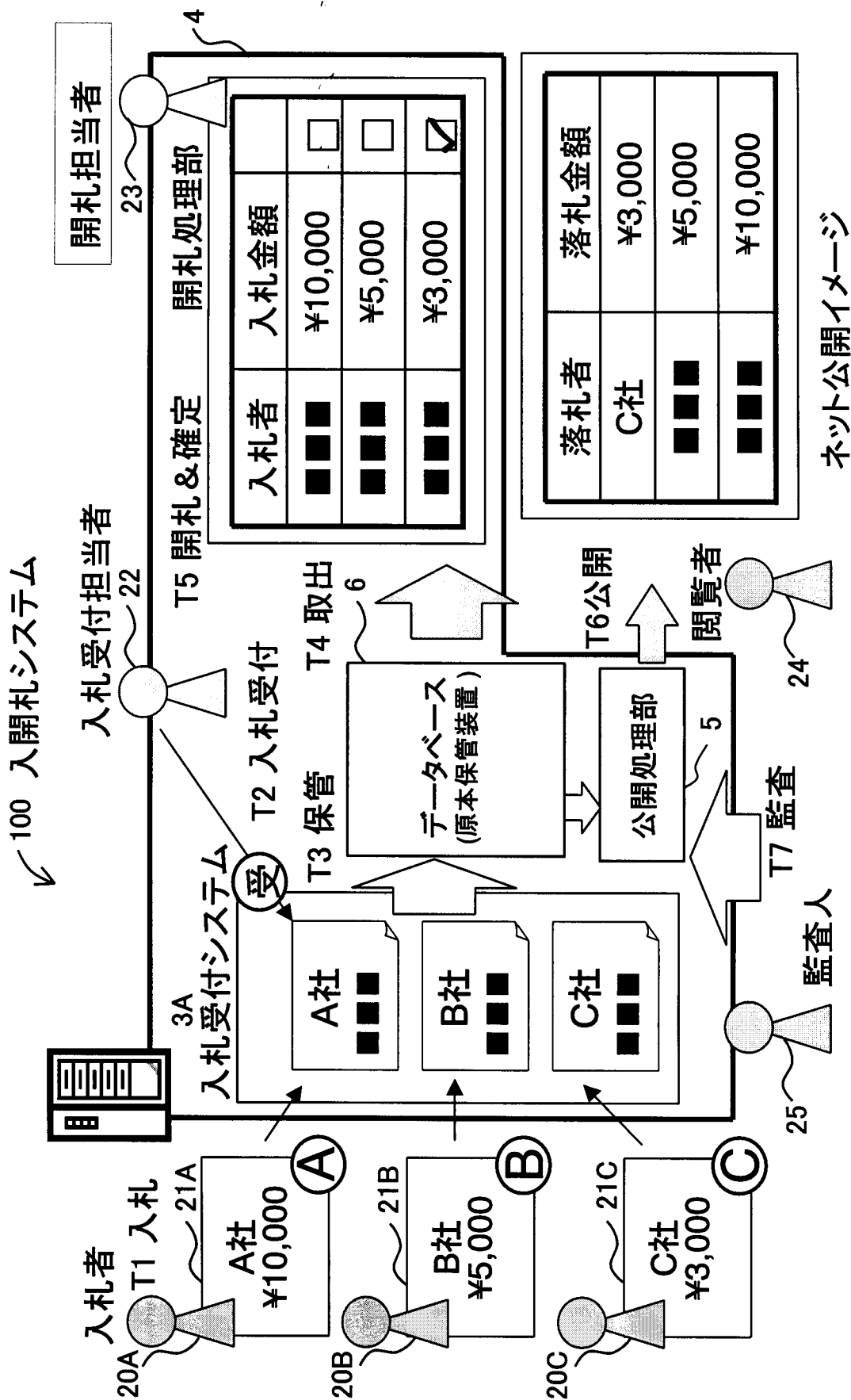
- [20] 請求項15に記載の電子入札／開札方法において、
前記各情報取得ステップで取得される全ての取得情報には、電子署名又はタイムスタンプが付されており、前記検証ステップは、これら電子署名又はタイムスタンプが付された前記第1版部分識別情報、前記第2a版部分識別情報、前記第2b版部分識別情報、前記第3版部分識別情報、前記第4版入札情報、及び前記第4版部分識別情報を用いて監査のための検証を行うことを特徴とする電子入札／開札プログラム。

[図1]

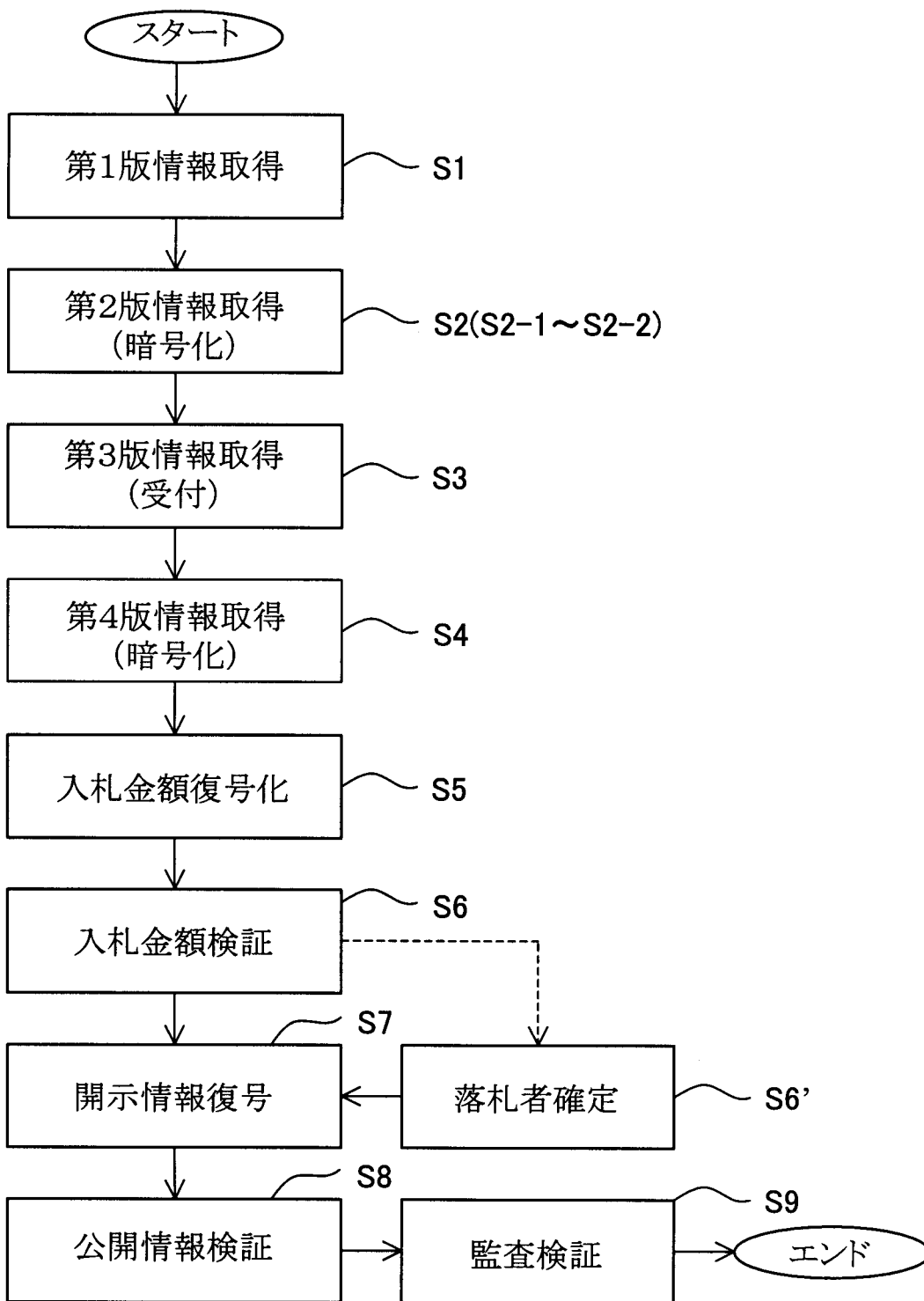
100 電子入札／開札システム



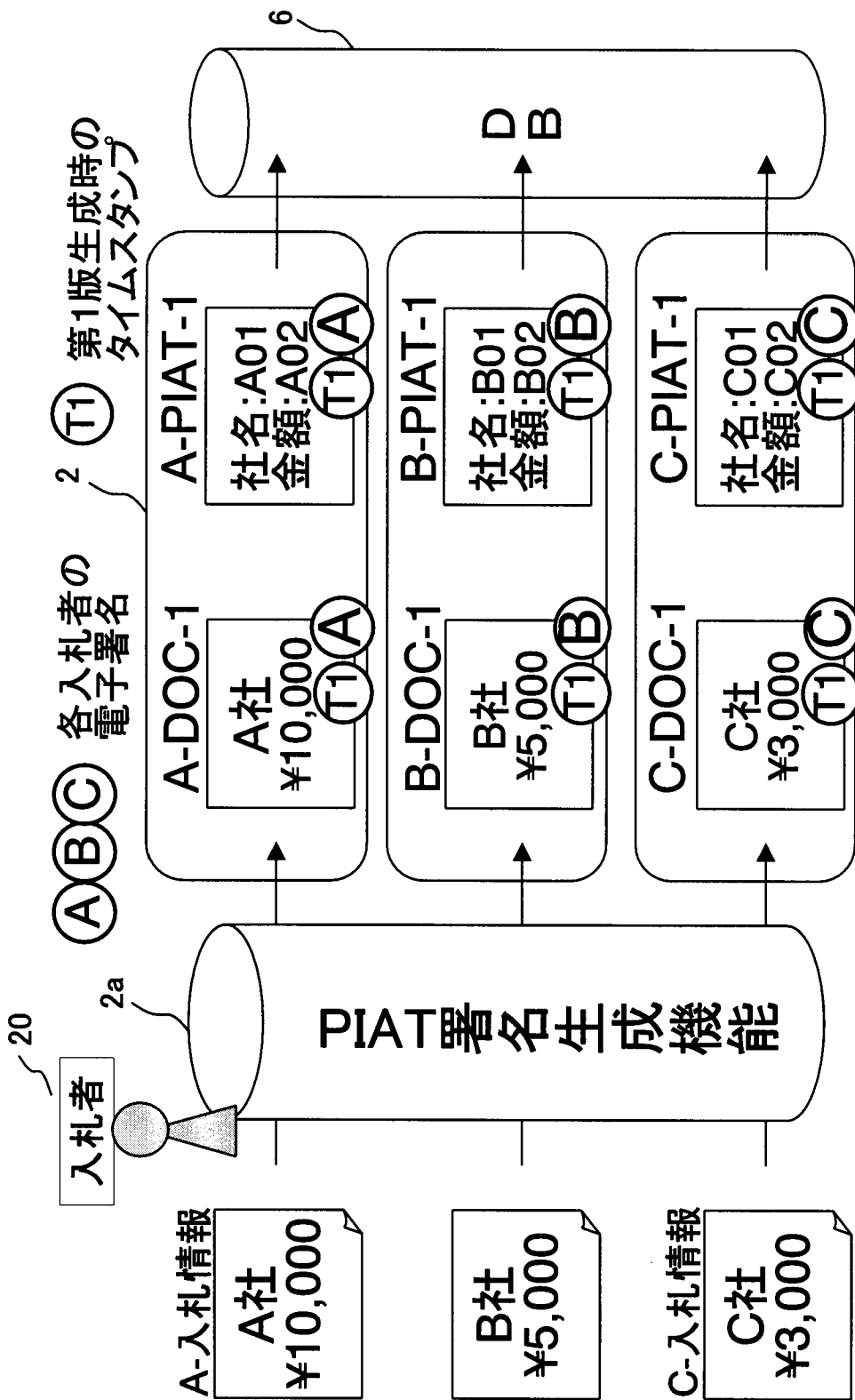
[図2]



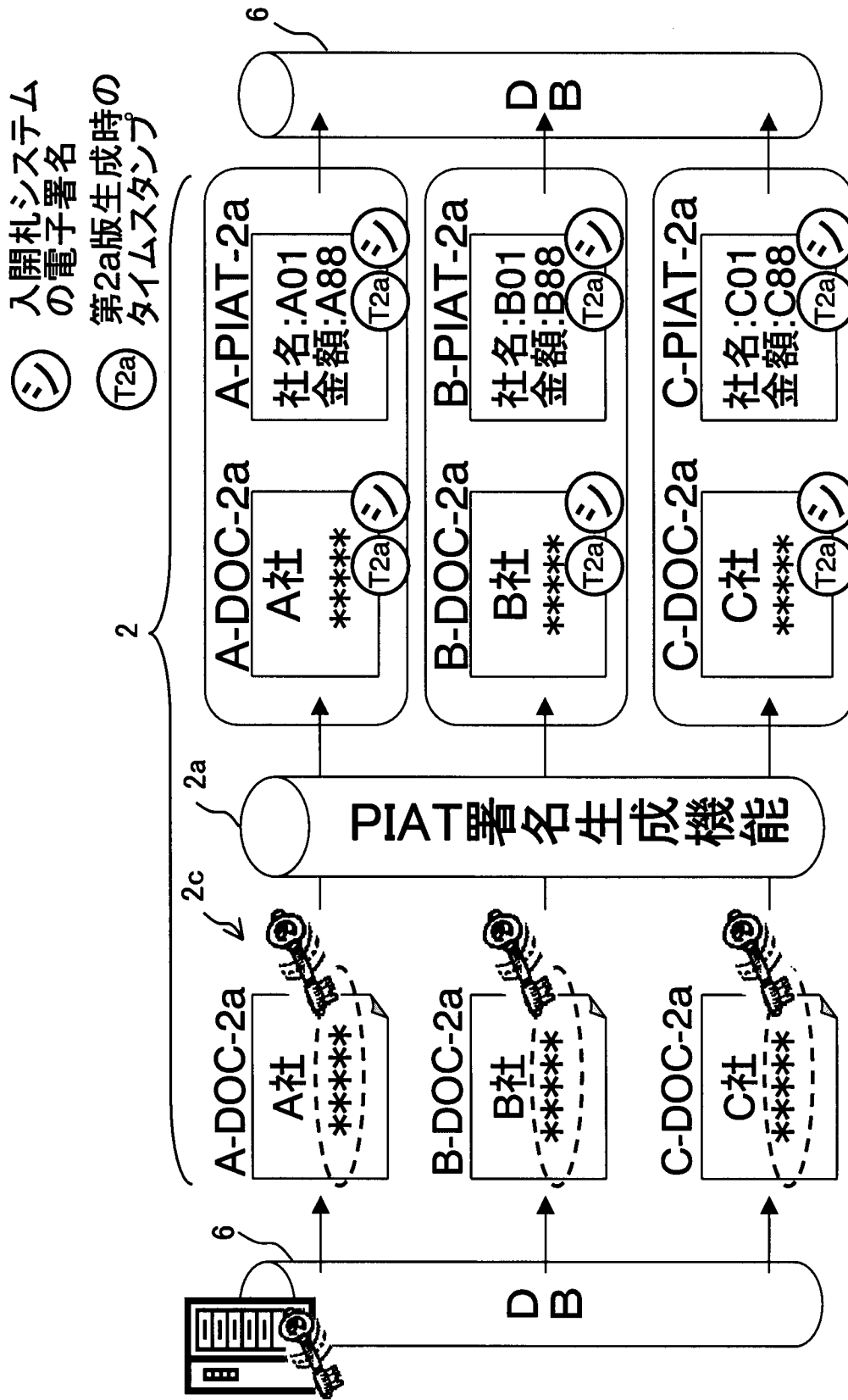
[図3]



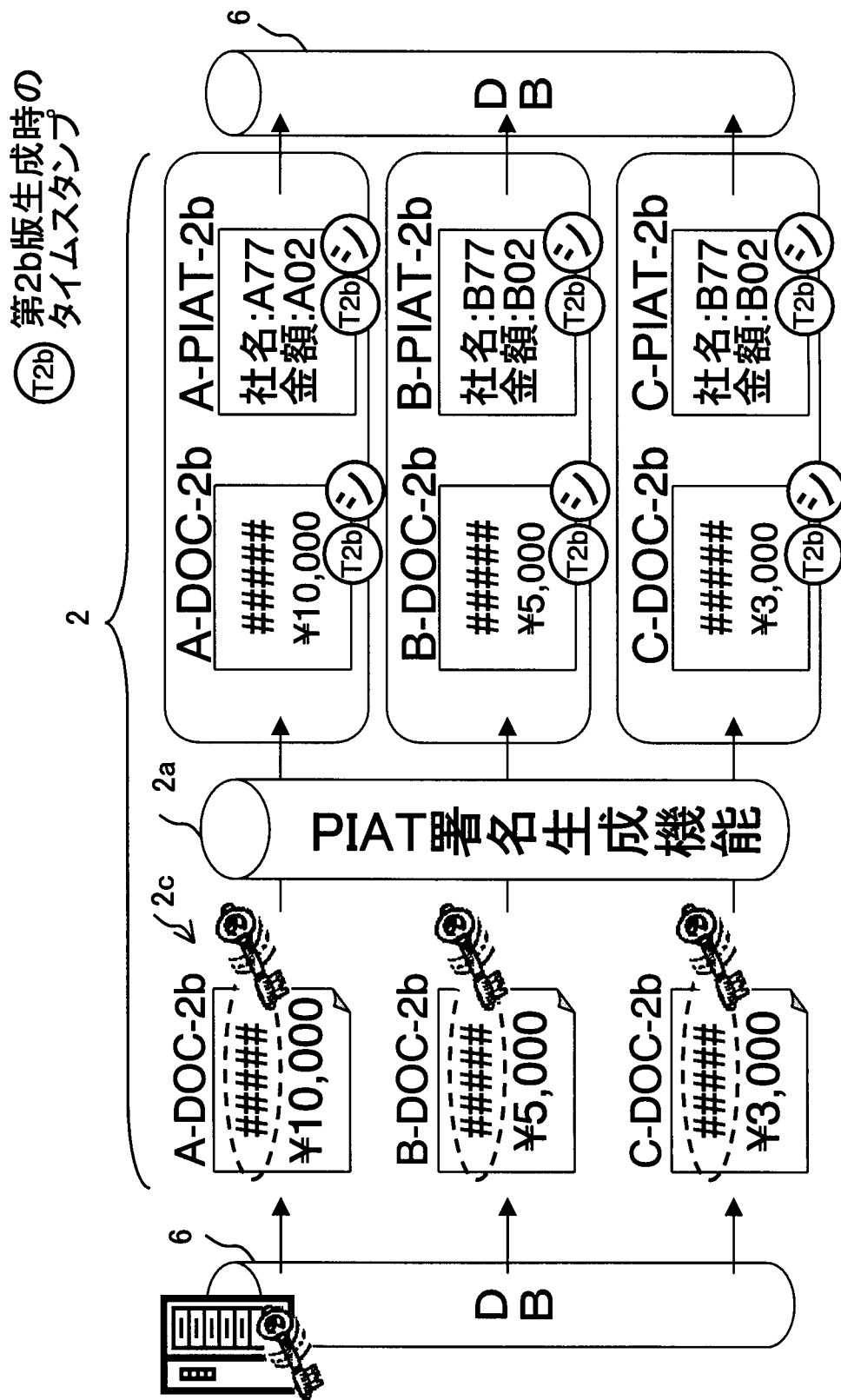
[図4]



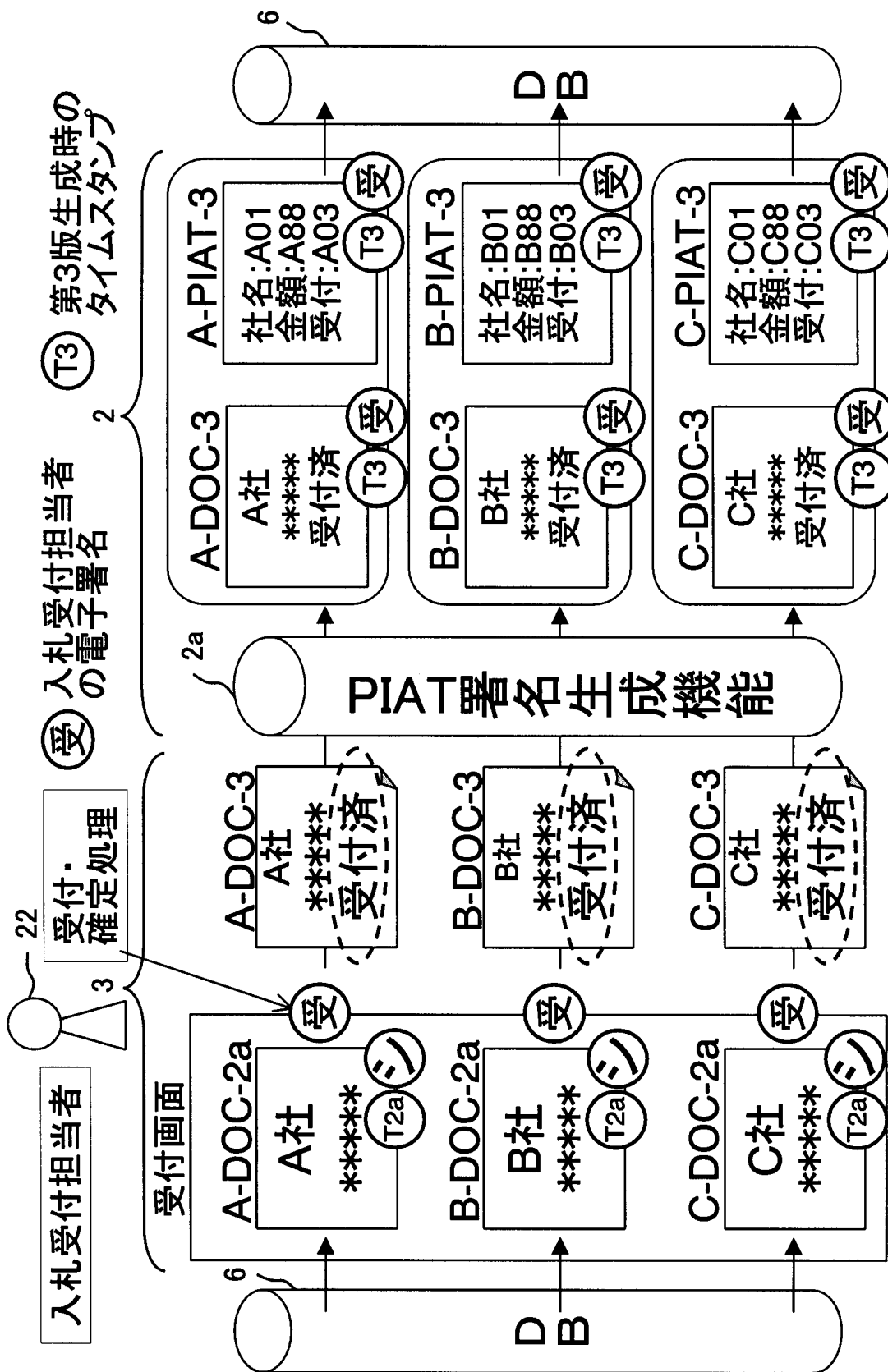
[図5]



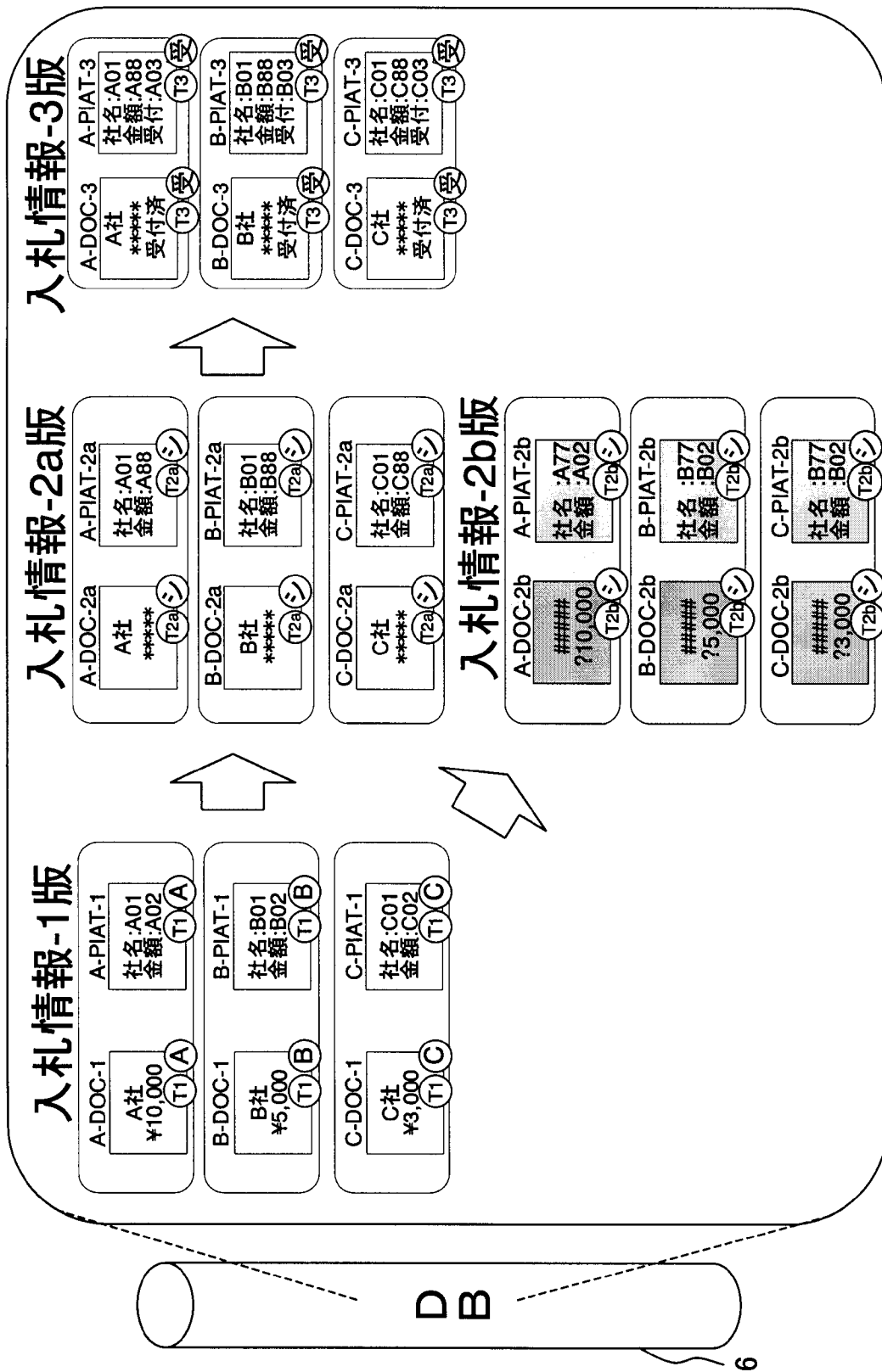
[図6]



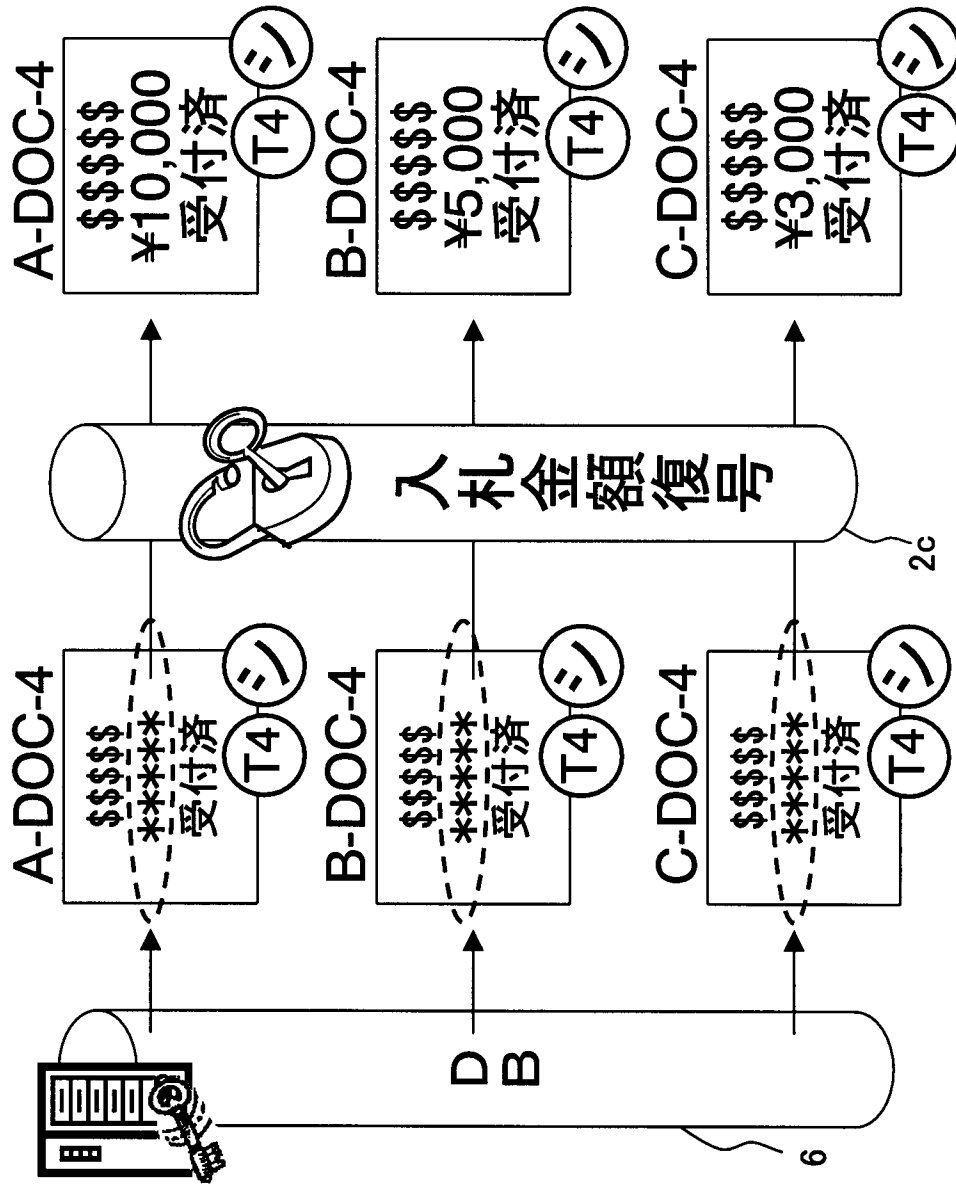
[図7]



[図8]



[図10]



[図12]

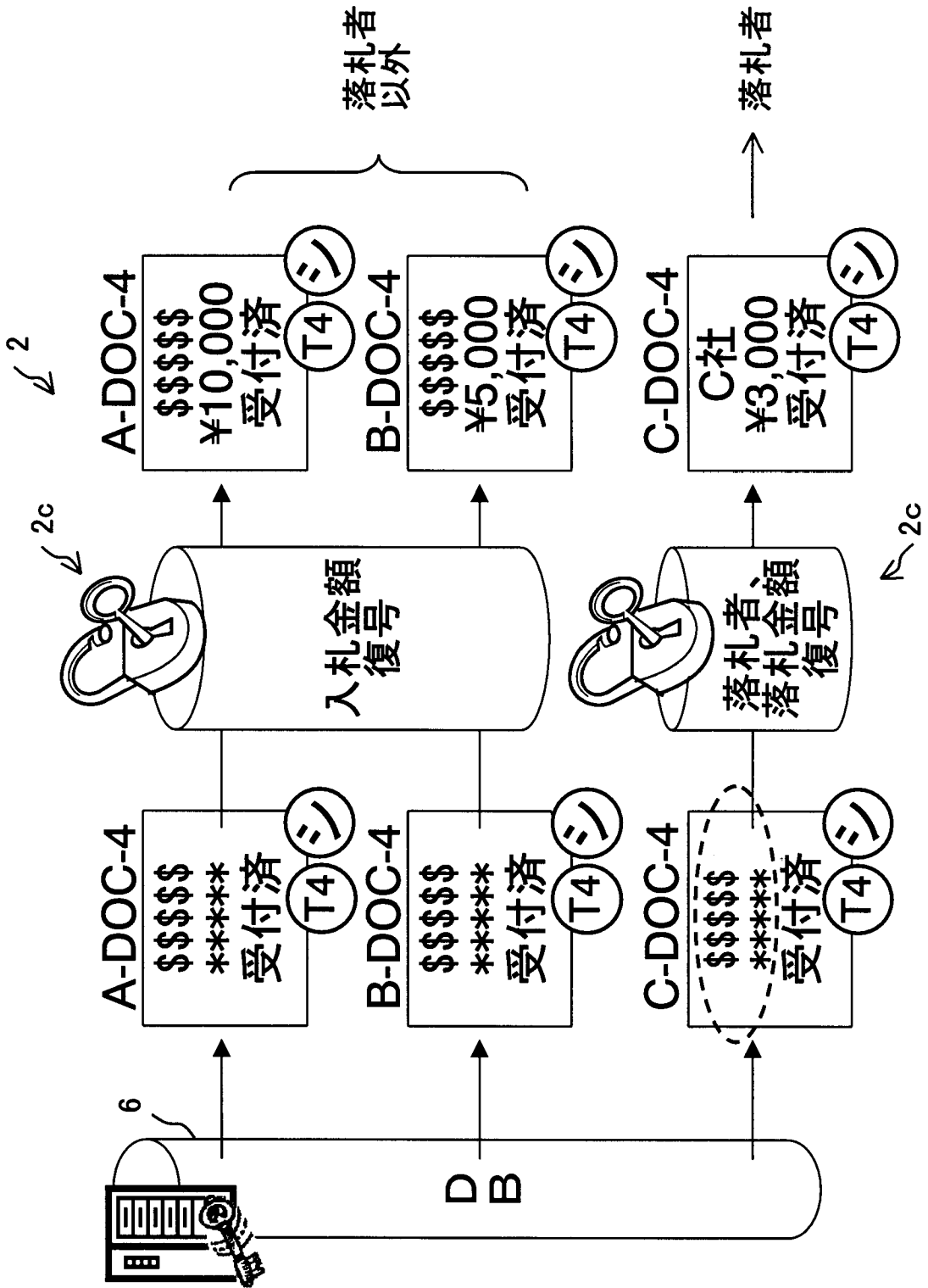
開札担当者、確定者

23

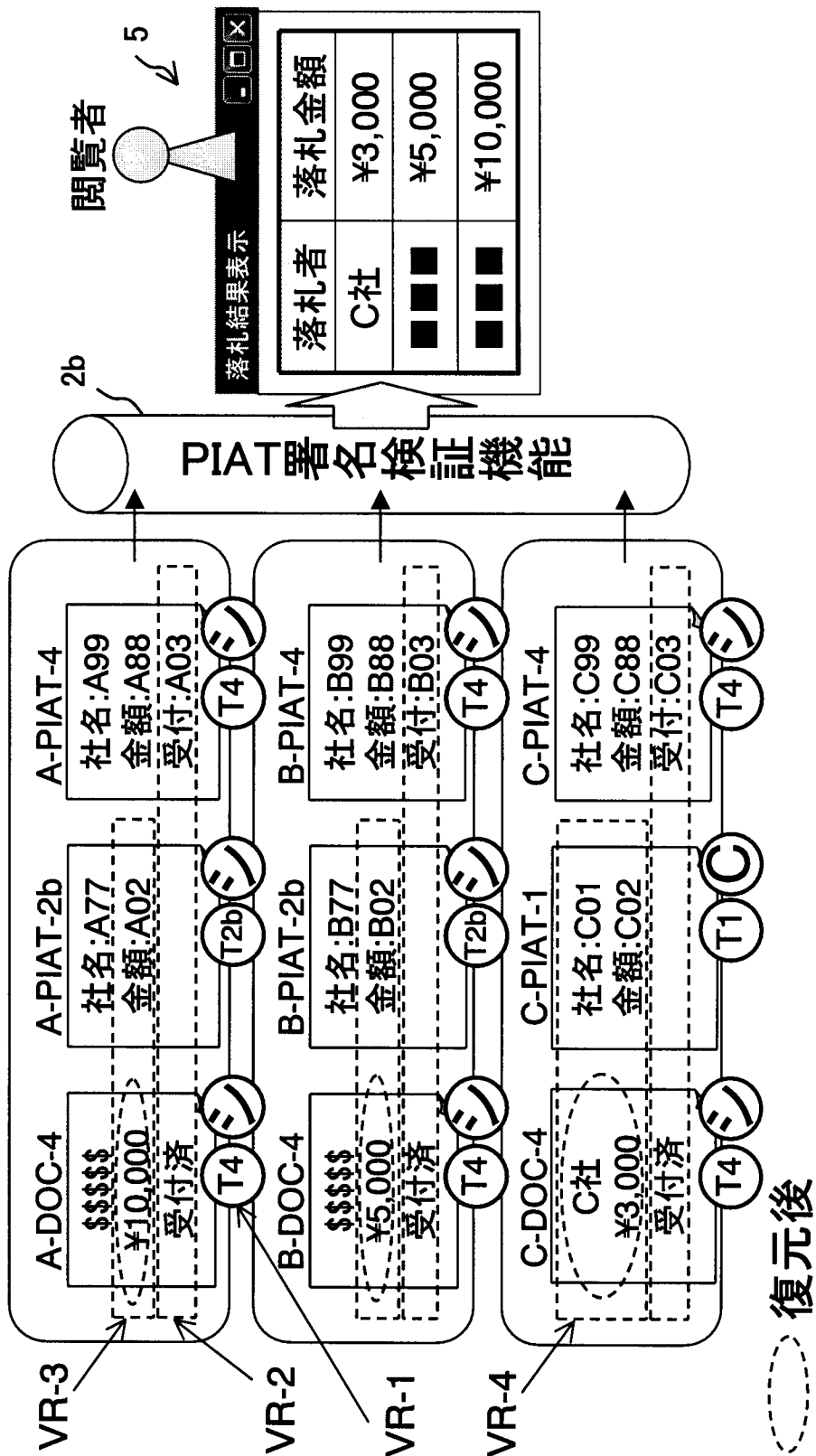
4

入札者	入札金額	
■ ■ ■	¥10,000	<input type="checkbox"/>
■ ■ ■	¥5,000	<input type="checkbox"/>
■ ■ ■	¥3,000	<input checked="" type="checkbox"/>

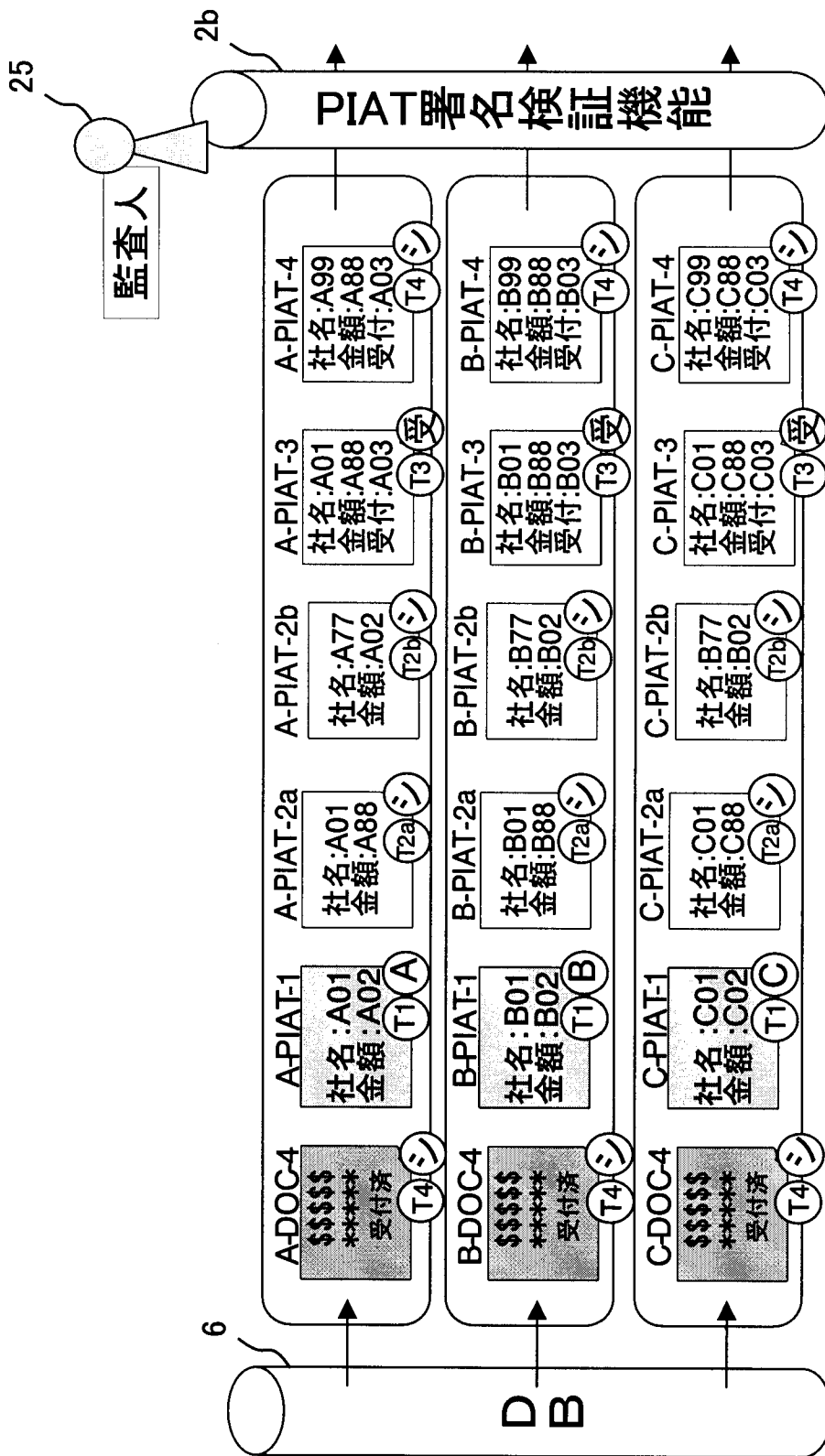
[図13]



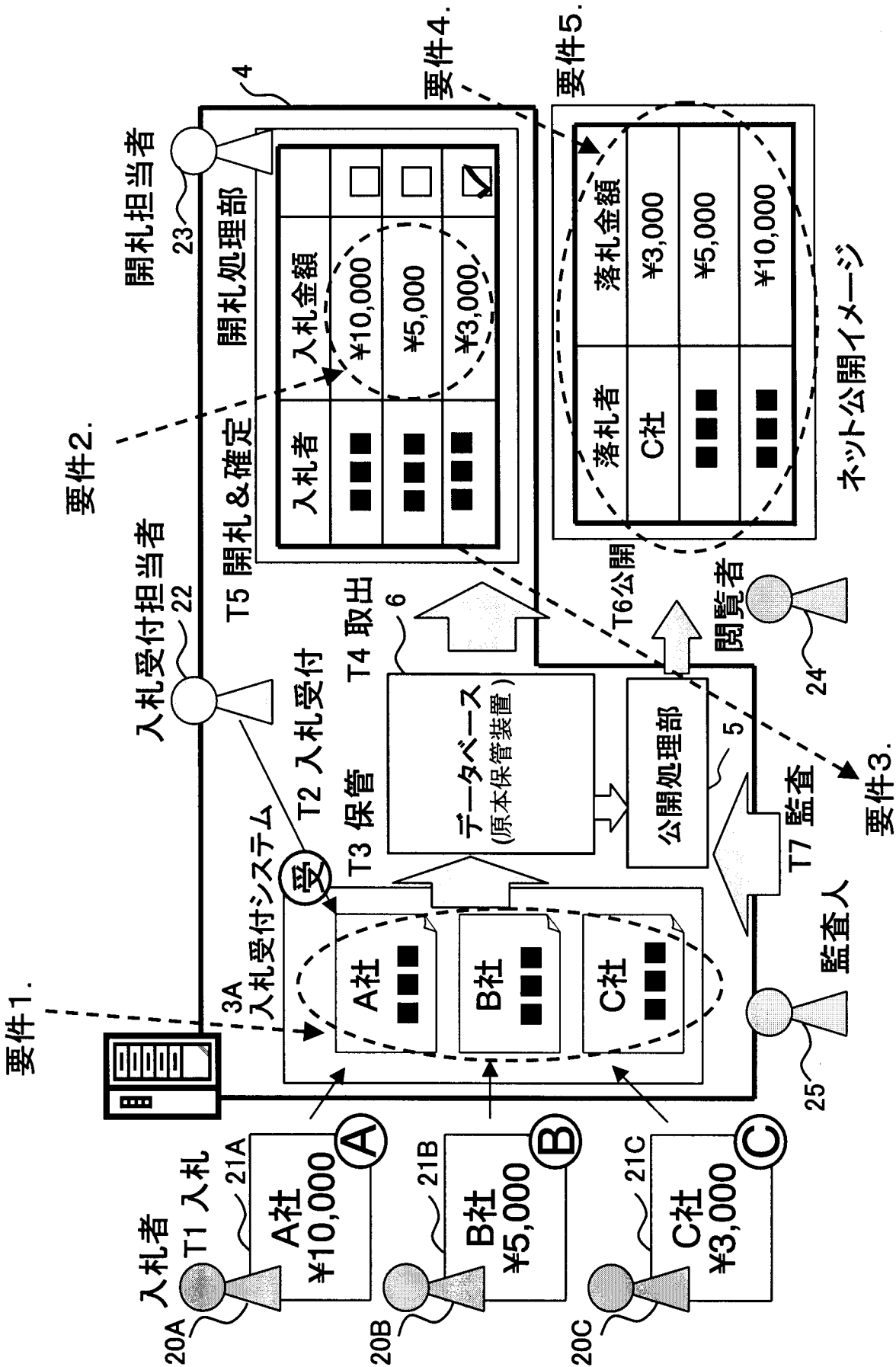
[図14]



[図15]



[図16]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2006/302522

A. CLASSIFICATION OF SUBJECT MATTER

H04L9/32(2006.01), **G06Q10/00**(2006.01), **G06Q30/00**(2006.01)

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06Q10/00, G06Q30/00, G09C1/00, H04L9/32

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2006
Kokai Jitsuyo Shinan Koho	1971-2006	Toroku Jitsuyo Shinan Koho	1994-2006

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2005-51734 A (Hitachi, Ltd.), 24 February, 2005 (24.02.05), Full text & EP 1498799 A2	1-20
A	JP 2001-147984 A (NTT Data Corp.), 29 May, 2001 (29.05.01), Full text (Family: none)	1-20
A	JP 2001-34682 A (Nippon Telegraph And Telephone Corp.), 09 February, 2001 (09.02.01), Full text & EP 1071025 A2	1-20

Further documents are listed in the continuation of Box C. See patent family annex.

* Special categories of cited documents:	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A" document defining the general state of the art which is not considered to be of particular relevance	"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E" earlier application or patent but published on or after the international filing date	"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&" document member of the same patent family
"O" document referring to an oral disclosure, use, exhibition or other means	
"P" document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search 25 April, 2006 (25.04.06)	Date of mailing of the international search report 02 May, 2006 (02.05.06)
Name and mailing address of the ISA/ Japanese Patent Office	Authorized officer
Facsimile No.	Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2006/302522

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2000-200311 A (NEC Corp.), 18 July, 2000 (18.07.00), Full text & EP 1020809 A2	1-20
A	JP 2-118876 A (Nippon Telegraph And Telephone Corp.), 07 May, 1990 (07.05.90), Full text (Family: none)	1-20

A. 発明の属する分野の分類 (国際特許分類 (IPC))
 Int.Cl. H04L9/32(2006.01), G06Q10/00(2006.01), G06Q30/00(2006.01)

B. 調査を行った分野
 調査を行った最小限資料 (国際特許分類 (IPC))
 Int.Cl. G06Q 10/00, G06Q 30/00, G09C 1/00, H04L 9/32

最小限資料以外の資料で調査を行った分野に含まれるもの
 日本国実用新案公報 1922-1996年
 日本国公開実用新案公報 1971-2006年
 日本国実用新案登録公報 1996-2006年
 日本国登録実用新案公報 1994-2006年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
A	J P 2 0 0 5 - 5 1 7 3 4 A (株式会社日立製作所) 2005.02.24, 全文 & EP 1498799 A2	1-20
A	J P 2 0 0 1 - 1 4 7 9 8 4 A (株式会社エヌ・ティ・ティ・データ) 2001.05.29, 全文 (ファミリーなし)	1-20
A	J P 2 0 0 1 - 3 4 6 8 2 A (日本電信電話株式会社) 2001.02.09, 全文 & EP 1071025 A2	1-20

C欄の続きにも文献が列挙されている。 パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー	の日の後に公表された文献
「A」特に関連のある文献ではなく、一般的技術水準を示すもの	「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの	「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)	「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「O」口頭による開示、使用、展示等に言及する文献	「&」同一パテントファミリー文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願	

国際調査を完了した日 25.04.2006	国際調査報告の発送日 02.05.2006
--------------------------	--------------------------

国際調査機関の名称及びあて先 日本国特許庁 (ISA/J P) 郵便番号100-8915 東京都千代田区霞が関三丁目4番3号	特許庁審査官 (権限のある職員) 石田 信行 電話番号 03-3581-1101 内線 3546	5 S	9 4 6 9
---	--	-----	---------

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
A	JP 2000-200311 A (日本電気株式会社) 2000.07.18, 全文 & EP 1020809 A2	1-20
A	JP 2-118876 A (日本電信電話株式会社) 1990.05.07, 全文 (ファミリーなし)	1-20