(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第4739404号
(P4739404)

(45)発行日　平成23年8月3日(2011.8.3)　(24)登録日　平成23年5月13日(2011.5.13)

(51)Int.Cl.		F I		
H04L 9/32	(2006.01)	H04L	9/00	675B
G09C 1/00	(2006.01)	H04L	9/00	675Z
G06F 21/24	(2006.01)	G09C	1/00	640D
		G06F	12/14	560C

請求項の数 10　(全 18 頁)

(21)出願番号　特願2008-500360 (P2008-500360)
(86)(22)出願日　平成18年2月14日 (2006.2.14)
(86)国際出願番号　PCT/JP2006/302522
(87)国際公開番号　WO2007/094043
(87)国際公開日　平成19年8月23日 (2007.8.23)
審査請求日　平成20年6月25日 (2008.6.25)

(73)特許権者　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号
(74)代理人　100101856
弁理士　赤澤　日出夫
(72)発明者　吉岡　孝司
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

審査官　石田　信行

最終頁に続く

(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

(57)【特許請求の範囲】

【請求項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第３版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。

【請求項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。

【請求項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、該部分識別情報と前記第２ｂ版部分識別情報とを比較することを特徴とする電子入札／開札プログラム。

【請求項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。

【請求項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。

【請求項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。

【請求項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。

【請求項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

識別可能に表す第３版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。
【請求項９】
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第３版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。
【請求項１０】
請求項９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。
【発明の詳細な説明】
【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言われている。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）入札受付担当者と入札者の結託、（２）開札担当者と入札者の結託、（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）入札受付担当者と入札者の結託では、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社の入札した\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）開札担当者と入札者の結託では、例えば以下のような場合があげられる。
【００１３】
例えば、開札担当者と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社の入札金額に対し、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開札システム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が入った場合は入開札システム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、入札受付前の入開札システム

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のと同時に以下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、各入札者がいくらの金額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を入開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の開札前の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】

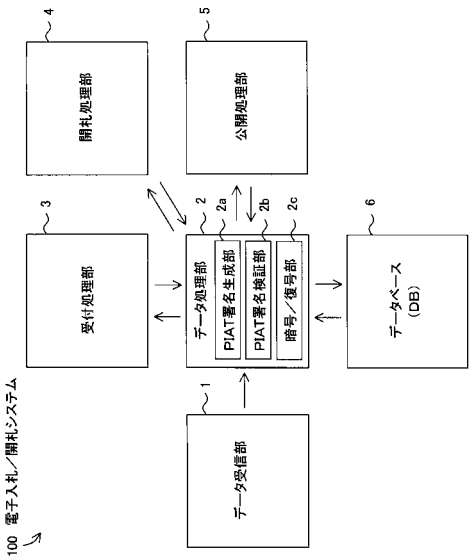
なお、図示したフローチャートやステップに示された各動作をコンピュータにより実行させるプログラムを提供することにより、本発明の電子入札／開札プログラムを提供することができる。これらプログラムはコンピュータにより読取可能な媒体に記録されてコンピュータにより実行させることができる。ここで、コンピュータにより読取可能な媒体としては、ＣＤ－ＲＯＭやフレキシブルディスク、ＤＶＤディスク、光磁気ディスク、ＩＣカード等の可搬型記憶媒体や、コンピュータプログラムを保持するデータベース、或いは、他のコンピュータ並びにそのデータベースや、更に回線上の伝送媒体をも含むものである。

【産業上の利用可能性】

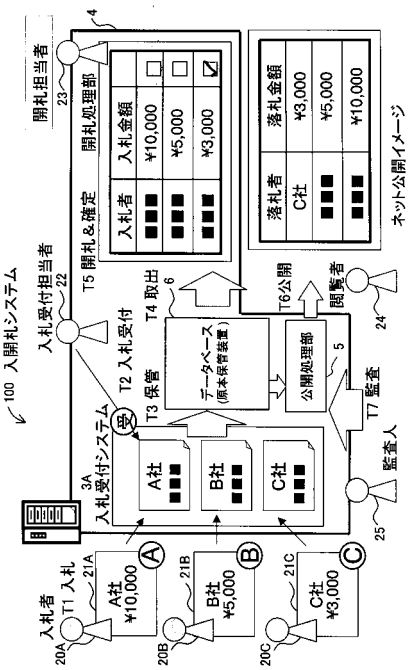
【００７２】

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。

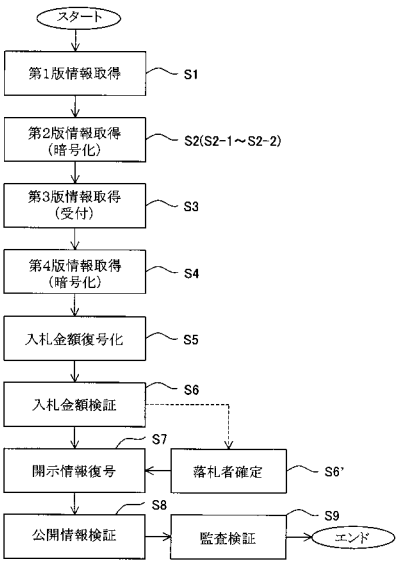
【図１】



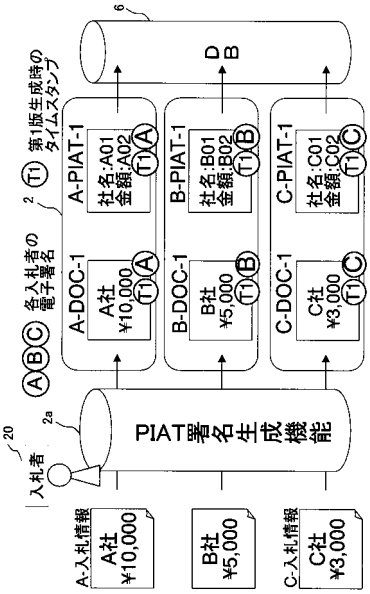
【図２】



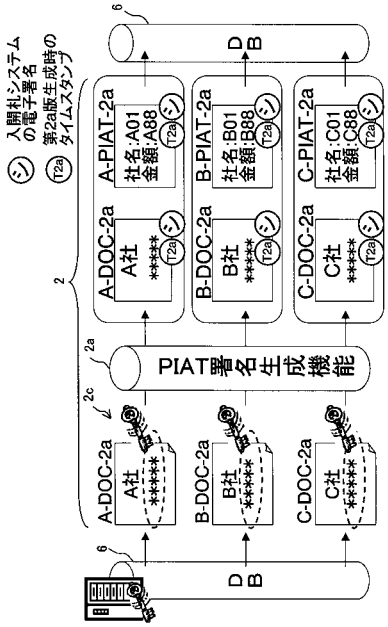
【図３】


スタート
第1版情報取得
S1
第2版情報取得（暗号化）
S2(S2-1～S2-2)
第3版情報取得（受付）
S3
第4版情報取得（暗号化）
S4
入札金額復号化
S5
入札金額検証
S6
開示情報復号
S7
落札者確定
S6'
公開情報検証
S8
監査検証
S9
エンド

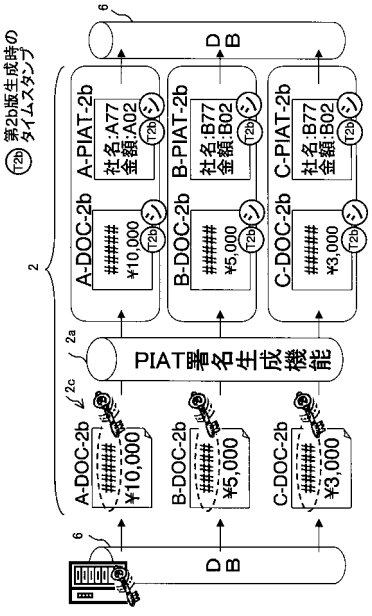
【図４】


PIAT署名生成機能
入札者
A-入札情報
B-入札情報
C-入札情報
A-DOC-1
B-DOC-1
C-DOC-1
A-PIAT-1
B-PIAT-1
C-PIAT-1
第1版生成時のタイムスタンプ
各入札者の電子署名
DB

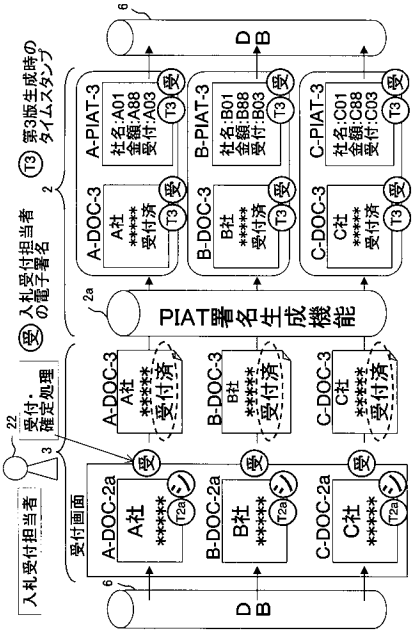
【図５】


入開札システムの電子署名
第2a版生成時のタイムスタンプ
PIAT署名生成機能
A-DOC-2a
B-DOC-2a
C-DOC-2a
A-PIAT-2a
B-PIAT-2a
C-PIAT-2a
DB

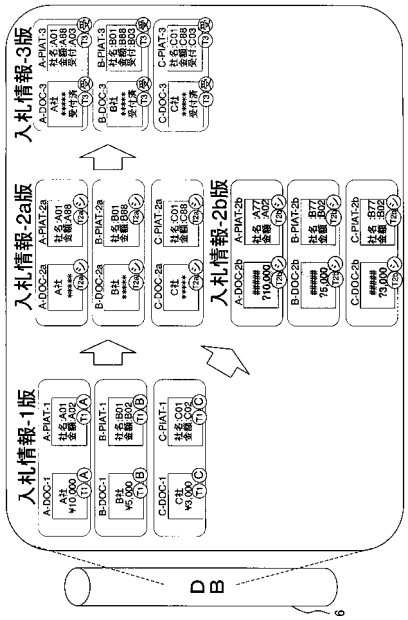
【図６】


第2b版生成時のタイムスタンプ
PIAT署名生成機能
A-DOC-2b
B-DOC-2b
C-DOC-2b
A-PIAT-2b
B-PIAT-2b
C-PIAT-2b
DB

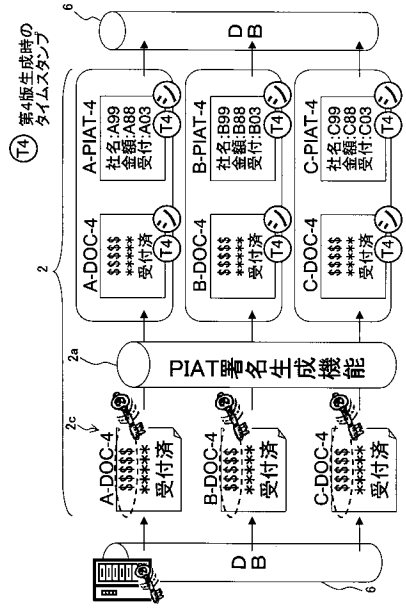
【図７】


入札受付担当者
受付・確定処理
受付画面
入札受付担当者の電子署名
第3版生成時のタイムスタンプ
PIAT署名生成機能
A-DOC-2a
B-DOC-2a
C-DOC-2a
A-DOC-3
B-DOC-3
C-DOC-3
A-PIAT-3
B-PIAT-3
C-PIAT-3
DB

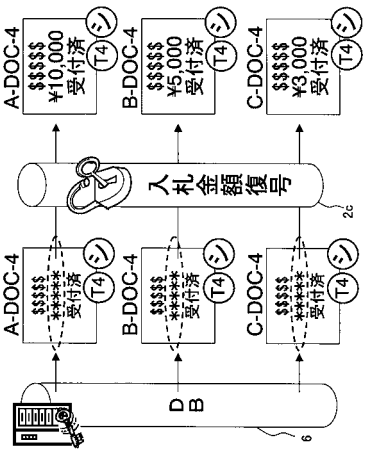
【図８】


入札情報-1版
入札情報-2a版
入札情報-2b版
入札情報-3版
DB

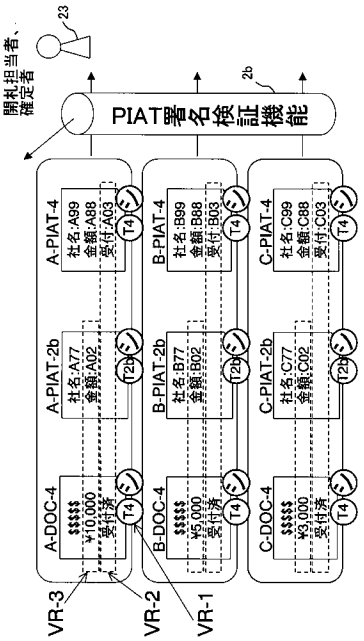
【図９】


第4版生成時のタイムスタンプ
PIAT署名生成機能
A-DOC-4
B-DOC-4
C-DOC-4
A-PIAT-4
B-PIAT-4
C-PIAT-4
DB

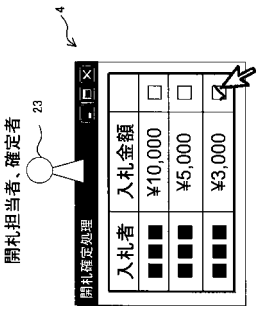
【図１０】


入札金額復号
A-DOC-4
B-DOC-4
C-DOC-4
DB

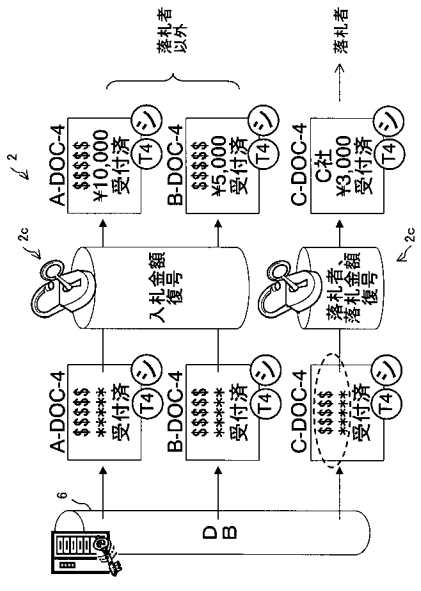
【図１１】



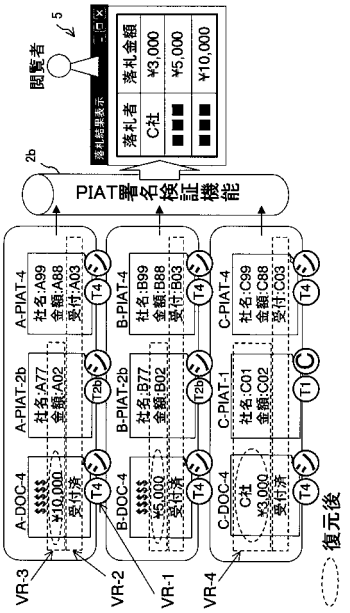
【図１２】



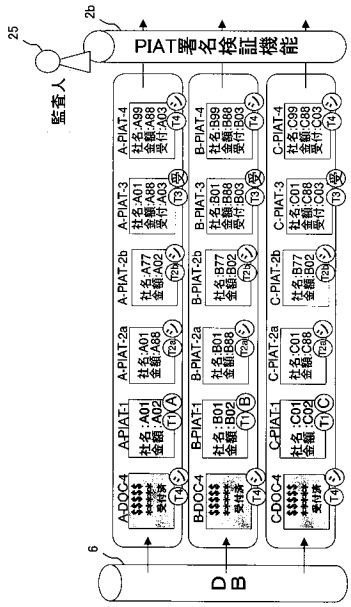
【図１３】



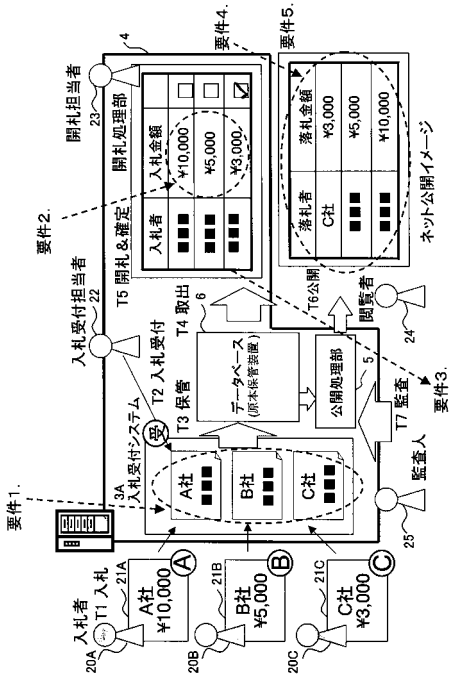
【図１４】



【図１５】


PIAT署名検証機能
監査人
A-DOC4
B-DOC4
C-DOC4
A-PIAT-1
B-PIAT-1
C-PIAT-1
A-PIAT-2a
B-PIAT-2a
C-PIAT-2a
A-PIAT-2b
B-PIAT-2b
C-PIAT-2b
A-PIAT-3
B-PIAT-3
C-PIAT-3
A-PIAT-4
B-PIAT-4
C-PIAT-4
DB

【図１６】


要件1.
要件2.
要件3.
要件4.
要件5.
入札者
入札受付担当者
開札担当者
開札処理部
入札金額
落札者
落札金額
A社
B社
C社
¥10,000
¥5,000
¥3,000
T1 入札
T2 入札受付
T3 保管
T4 取出
T5 開札&確定
T6公開
T7 監査
入札受付システム
データベース
公開処理部
監査人
閲覧者
ネット公開イメージ

フロントページの続き

(56)参考文献 特開２００２－１３３０１９（ＪＰ，Ａ）
特開２００１－３１９０９７（ＪＰ，Ａ）
特開２００１－１４７９８４（ＪＰ，Ａ）
特開２００１－３４６８２（ＪＰ，Ａ）
特開２０００－２００３１１（ＪＰ，Ａ）
特開平２－１１８８７６（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
H04L 9/32
G09C 1/00
G06F 21/24