(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2007-274289
(P2007-274289A)
(43)公開日　平成19年10月18日(2007.10.18)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 9/32	(2006.01)	H04L	9/00	675B	5J104
G06Q 30/00	(2006.01)	H04L	9/00	673C	
		G06F	17/60	332	

審査請求 未請求　請求項の数 12　ＯＬ　（全 42 頁）

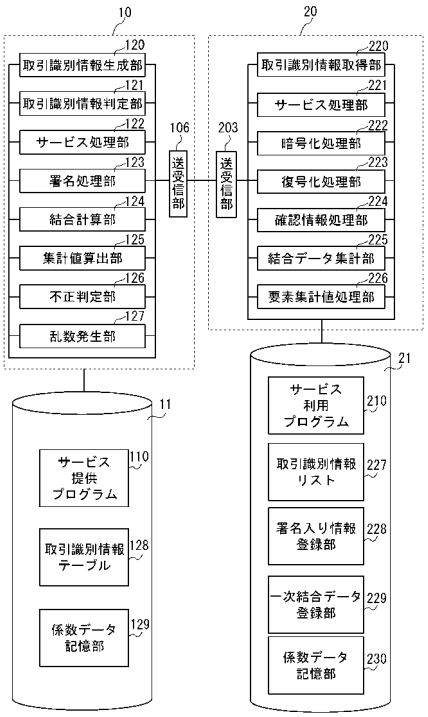
(21)出願番号　特願2006-96692(P2006-96692)
(22)出願日　平成18年3月31日(2006.3.31)

(71)出願人　504145320
国立大学法人福井大学
福井県福井市文京３丁目９番１号
(74)代理人　100111855
弁理士　川崎　好昭
(72)発明者　田村　信介
福井県福井市文京３－９－１　国立大学法人福井大学工学部内

Ｆターム(参考)　5J104 LA06　PA07　PA10

(54)【発明の名称】サービス取引システム及びそのプログラム

(57)【要約】
【課題】本発明は、サービス利用者が個々の取引を自分自身と関連付けられることなくサービス依頼することができるとともにサービス提供者がサービス利用者の利用料金の適正な総額を確実に算定することができるサービス取引システムを提供することを目的とするものである。
【解決手段】サービス提供装置１において生成した取引識別情報をサービス利用装置２で取得し、サービス取引ごとにサービス提供装置１に送信して署名処理したものを次回のサービス取引に使用することで、サービス利用装置２の取引権限をチェックする。また、サービス利用装置２で今回及び次回の取引識別情報に基づいて生成した確認情報を送信してサービス提供装置１で一次結合データを生成し、一次結合データをサービス利用装置２に登録する。サービス取引ごとの一次結合データを集計して利用料金の合計額を算出すると共に確認情報に基づいて集計の際の不正操作を判定する。
【選択図】図７



【特許請求の範囲】
【請求項１】
サービス利用装置と、サービス利用装置に通信手段を介して接続されるとともにサービス利用装置からのサービス依頼を受けて当該サービスを処理するサービス提供装置とを備えているサービス取引システムであって、
前記サービス提供装置は、サービス利用装置から送信された取引識別情報が有効なものであるか否か判定する識別情報判定手段と、取引識別情報が有効と判定された場合にサービス利用装置からの依頼に応じてサービス処理を行うサービス提供手段と、サービス利用装置から送信された暗号化取引識別情報に署名処理する署名処理手段と、サービス利用装置から送信された今回の取引識別情報及び確認情報の組を含む情報をサービス利用装置の取引記録として生成する取引記録生成手段とを備え、
前記サービス利用装置は、メモリに記憶されたサービス提供装置による署名処理済みの取引識別情報をサービス提供装置に送信してサービス依頼を行うサービス依頼手段と、次回のサービス取引の取引識別情報を選択する識別情報選択手段と、取引識別情報を暗号化処理し暗号化取引識別情報を生成する暗号化処理手段と、サービス提供装置から送信された署名処理済みの暗号化取引識別情報を復号化処理して署名処理済みの取引識別情報をメモリに記憶する復号化処理手段と、次回取引のための取引識別情報からサービス提供装置が知らないパラメータを用いて計算される確認情報を生成する確認情報処理手段とを備えていることを特徴とするサービス取引システム。
【請求項２】
サービス利用装置からのサービス依頼を受けてサービス提供装置が当該サービスを処理するサービス取引方法であって、サービス利用装置が予めサービス提供装置から取得した署名処理済みの取引識別情報を送信してサービス提供装置にサービス依頼し、サービス提供装置が、サービス利用装置から送信された取引識別情報が有効なものであるか否かを判定し、取引識別情報が有効と判定された場合にサービス利用装置からの依頼に応じてサービス処理するとともに、サービス利用装置が、次回のサービス取引の取引識別情報を暗号化処理することによって暗号化取引識別情報を生成し、また次回の取引識別情報からサービス提供装置の知らないパラメータを用いて計算される確認情報を生成してそれぞれサービス提供装置に送信し、サービス提供装置が、サービス利用装置から送信された暗号化取引識別情報に対して署名処理するとともに、今回の取引識別情報及び確認情報を含む情報をサービス利用装置の取引記録として生成し、サービス利用装置が、サービス提供装置から送信された署名処理済みの暗号化取引識別情報を復号化処理して署名処理済みの取引識別情報を取得することを特徴とするサービス取引方法。
【請求項３】
サービス利用装置と、サービス利用装置に通信手段を介して接続されるとともにサービス利用装置からのサービス依頼を受けて当該サービスを処理するサービス提供装置とを備えているサービス取引システムにおいて、該サービス利用装置を機能させるためのプログラムであって、
前記サービス利用装置を、
メモリに記憶されたサービス提供装置による署名処理済みの取引識別情報をサービス提供装置に送信してサービス依頼を行う手段、
次回のサービス取引の取引識別情報を選択する手段、
取引識別情報を暗号化処理し暗号化取引識別情報を生成する手段、
次回のサービス取引の取引識別情報からサービス提供装置の知らないパラメータを用いて計算される確認情報を生成する手段、
サービス提供装置から送信された署名処理済みの暗号化取引識別情報を復号化処理して署名処理済みの取引識別情報をメモリに記憶する手段、
として機能させるためのプログラム。
【請求項４】
サービス利用装置と、サービス利用装置に通信手段を介して接続されるとともにサービ

ス利用装置からのサービス依頼を受けて当該サービスを処理するサービス提供装置とを備えているサービス取引システムにおいて、該サービス提供装置を機能させるためのプログラムであって、
前記サービス提供装置を、
サービス利用装置から送信された取引識別情報が有効なものであるか否か判定する手段、
取引識別情報が有効と判定された場合にサービス利用装置からの依頼に応じてサービス処理を行う手段、
サービス利用装置から送信された暗号化取引識別情報に署名処理する手段、
サービス利用装置から送信された今回の取引識別情報と確認情報の組を含む情報をサービス利用装置の取引記録として生成する手段、
として機能させるためのプログラム。
【請求項５】
サービス利用装置と、サービス利用装置に通信手段を介して接続されるとともにサービス利用装置からのサービス依頼を受けて当該サービスを処理するサービス提供装置とを備えているサービス取引システムであって、
前記サービス利用装置は、ｋ回目のサービス取引において（ｋ＋１）回目のサービス取引の取引識別情報Ｔ（ｋ＋１）を暗号化処理し暗号化取引識別情報を生成する暗号化処理手段と、取引識別情報Ｔ（ｋ＋１）から計算されるＭ個の要素データV_s（ｋ＋１）（s=1,2,…,M）のサービス提供装置の知らない係数による互いに独立なＭ個の一次結合である確認情報W_t（ｋ）（t=1,2,…,M）を生成する確認情報処理手段と、サービス提供装置から送信された署名処理済みの暗号化取引識別情報を復号化処理して署名処理済みの取引識別情報をメモリに記憶する復号化処理手段と、メモリに記憶されたｋ回目のサービス取引のための署名処理済みの取引識別情報Ｔ（ｋ）をサービス提供装置に送信してサービス依頼を行うサービス依頼手段と、ｋ回目のサービス取引記録としてサービス提供装置から送信される、後記の式（Ｂ）に基づいて計算される互いに独立なＰ個の一次結合データS_j（ｋ）（j=1,2,…,P）を登録する登録手段と、サービス提供装置からの集計依頼に応じて登録された一次結合データS_j（ｋ）を各ｊ毎にｋについて集計した結合集計データΣS_j（ｋ）を算出するとともに、サービス提供装置から送信された集計値$\Sigma r_{k+1}W_t$（ｋ）（t=1,2,…,M）を復号化処理して集計値ΣX_u（ｋ）（u=1,2,…,M）を生成する要素集計値処理手段とを備え、
前記サービス提供装置は、サービス利用装置から送信された取引識別情報が有効なものであるか否か判定する識別情報判定手段と、取引識別情報が有効と判定された場合にサービス利用装置からの依頼に応じてサービス処理を行うサービス提供手段と、サービス利用装置から送信された暗号化取引識別情報に署名処理する署名処理手段と、サービス利用装置の知らないP^2個の係数データa_{ij}（i=1,2,…,P;j=1,2,…,P）及び乱数r_k（k=1,2,…）の列を記憶する記憶手段と、記憶手段に記憶された係数データa_{ij}及び乱数r_kを用いて、当該サービス取引の利用料金に基づくデータＥ（ｋ）、乱数Ｒ（ｋ）並びにサービス利用装置から送信された取引識別情報Ｔ（ｋ）によって計算されるＭ個の要素データV_s（ｋ）及び確認情報W_t（ｋ）を含むＰ（Ｐ≧２Ｍ＋２）個の値の互いに独立な一次結合データS_j（j=1,2,…,P）を以下の式（Ｂ）

$$S_j(k)=a_{1j}E(k)+\{a_{(1+1)j}V_1(k)+a_{(2+1)j}V_2(k)+\cdots+a_{(M+1)}V_M(k)\}r_k+\{a_{(M+1+1)j}W_1(k)+a_{(M+2+1)j}W_2(k)+\cdots+a_{(2M+1)}W_M(k)\}r_{k+1}+a_{(2M+2)j}R(k)\cdots(B)$$

により算出する結合計算手段と、サービス利用装置のサービス取引回数をＮ回として、サービス利用装置から送信されたＰ個の結合集計データΣS_j（ｋ）及び係数データa_{ij}に基づいて取引識別情報Ｔ（１）～Ｔ（Ｎ）に関するデータＥ（ｋ）の集計値ΣE（ｋ）を算出する合計額算出手段と、サービス利用装置から送信されたＰ個の結合集計データΣS_j（ｋ）及び係数データa_{ij}に基づいて取引識別情報Ｔ（１）～Ｔ（Ｎ）に関する要素データと乱数の積r_kV_s（ｋ）の各ｓ毎のｋについての集計値Σr_kV_s（ｋ）並びに取引識

別情報Ｔ（１）～Ｔ（Ｎ＋１）に関する確認情報と乱数の積$r_{k+1}W_t$（ｋ）の各ｔ毎のｋについての集計値Σ$r_{k+1}W_t$（ｋ）を算出するとともに集計値Σ$r_{k+1}W_t$（ｋ）を送信する要素集計値算出手段と、集計値Σr_kV_s（ｋ）とサービス利用装置から送信された集計値ΣX_u（ｋ）が矛盾するか否か判定する不正判定手段とを備えていることを特徴とするサービス取引システム。

【請求項６】

サービス利用装置からのサービス依頼を受けてサービス提供装置が当該サービスを処理するサービス取引方法であって、

サービス利用装置が、そのｋ回目のサービス取引において予めサービス提供装置から取得した署名処理済みの取引識別情報Ｔ（ｋ）を送信してサービス提供装置にサービス依頼し、サービス提供装置が、サービス利用装置から送信された取引識別情報が有効なものであるか否か判定するとともに、取引識別情報が有効と判定された場合にサービス利用装置からの依頼に応じてサービス処理し、サービス利用装置が、次回のサービス取引の取引識別情報Ｔ（ｋ＋１）を暗号化した暗号化取引識別情報と、取引識別情報Ｔ（ｋ＋１）に基づいて計算されるＭ個の要素データV_s（ｋ）（s=1,2,…,M）のサービス提供装置の知らない係数による互いに独立なＭ個の一次結合である確認情報W_t（ｋ）（t=1,2,…,M）を生成し、サービス提供装置が、次回サービス取引のための暗号化識別情報に署名するとともに、当該サービス取引の利用料金に基づくデータＥ（ｋ）、乱数Ｒ（ｋ）、サービス利用装置から送信された取引識別情報Ｔ（ｋ）に基づいて計算されるＭ個の要素データV_s（ｋ）及び確認情報W_t（ｋ）を含むＰ（Ｐ≧２Ｍ＋２）個の値の、サービス利用装置が知らない係数データa_{ij}（i=1,2,…,P;j=1,2,…,P）及び乱数r_k（k=1,2,…）を用いた互いに独立な一次結合データS_j（ｋ）（j=1,2,…,P）を以下の式（Ｂ）

$S_j(k)=a_{1j}E(k)+\{a_{(1+1)j}V_1(k)+a_{(2+1)j}V_2(k)+\cdots+a_{(M+1)}V_M(k)\}r_k+\{a_{(M+1+1)j}W_1(k)+a_{(M+2+1)j}W_2(k)+\cdots+a_{(2M+1)}W_M(k)\}r_{k+1}+a_{(2M+2)j}R(k)$・・・（Ｂ）

により算出し、算出されたＰ個の一次結合データS_j（ｋ）をサービス利用装置において登録し、サービス提供装置からの集計依頼に応じて、登録されたＮ回分の一次結合データS_j（ｋ）を各ｊ毎にｋについて集計した結合集計データΣS_j（ｋ）を算出するとともに結合集計データΣS_j（ｋ）をサービス提供装置に送信し、サービス提供装置が、サービス利用装置から送信されたＰ個の結合集計データΣS_j（ｋ）及び係数データa_{ij}に基づいて取引識別情報Ｔ（１）～Ｔ（Ｎ）に関するデータＥ（ｋ）の集計値Σ Ｅ（ｋ）を算出し、サービス利用装置から送信されたＰ個の結合集計データΣS_j（ｋ）及び係数データa_{ij}に基づいて取引識別情報Ｔ（１）～Ｔ（Ｎ）に関する要素データと乱数の積r_kV_s（ｋ）の各ｓ毎のｋについての集計値Σr_kV_s（ｋ）並びに取引識別情報Ｔ（１）～Ｔ（Ｎ＋１）に関する確認情報と乱数の積$r_{k+1}W_t$（ｋ）の各ｔ毎のｋについての集計値Σ$r_{k+1}W_t$を算出するとともに集計値Σ$r_{k+1}W_t$（ｋ）をサービス利用装置に送信し、サービス利用装置が、サービス提供装置から送信された集計値Σ$r_{k+1}W_t$（ｋ）を復号化処理して集計値ΣX_u（ｋ）（u=1,2,…,M）を生成し、サービス提供装置が、サービス利用装置から送信された集計値ΣX_uと集計値Σr_kV_s（ｋ）との間に矛盾があるか否かを判定することを特徴とするサービス取引方法。

【請求項７】

サービス利用装置と、サービス利用装置に通信手段を介して接続されるとともにサービス利用装置からのサービス依頼を受けて当該サービスを処理するサービス提供装置とを備えているサービス取引システムにおいて、該サービス利用装置を機能させるためのプログラムであって、

前記サービス利用装置を、

ｋ回目のサービス取引において（ｋ＋１）回目のサービス取引の取引識別情報Ｔ（ｋ＋１）を暗号化処理し暗号化取引識別情報を生成する手段、

取引識別情報Ｔ（ｋ＋１）から計算されるＭ個の要素データV_s（ｋ＋１）（s=1,2,…,M）のサービス提供装置の知らない係数による互いに独立なＭ個の一次結合である確認情

報W_t（ｋ）（t=1,2,…,M）を生成する手段、
サービス提供装置から送信された署名処理済みの暗号化取引識別情報を復号化処理して署名処理済みの取引識別情報をメモリに記憶する復号化処理手段、
メモリに記憶されたｋ回目のサービス取引のための署名処理済みの取引識別情報Ｔ（ｋ）をサービス提供装置に送信してサービス依頼を行う手段、
ｋ回目のサービス取引記録としてサービス提供装置から送信される、後記の式（Ｂ）に基づいて計算される互いに独立なＰ個の一次結合データS_j（ｋ）（j=1,2,…,P）を登録する手段、
サービス提供装置からの集計依頼に応じて登録された一次結合データS_j（ｋ）を各ｊ毎にｋについて集計した結合集計データΣS_j（ｋ）を算出するとともに、サービス提供装置から送信された集計値Σ$r_{k+1}W_t$（ｋ）（t=1,2,…,M）を復号化処理して集計値ΣX_u（ｋ）（u=1,2,…,M）を生成する手段、
として機能させるためのプログラム。
【請求項８】
サービス利用装置と、サービス利用装置に通信手段を介して接続されるとともにサービス利用装置からのサービス依頼を受けて当該サービスを処理するサービス提供装置とを備えているサービス取引システムにおいて、該サービス提供装置を機能させるためのプログラムであって、
前記サービス提供装置を、
サービス利用装置から送信された取引識別情報が有効なものであるか否か判定する手段、
取引識別情報が有効と判定された場合にサービス利用装置からの依頼に応じてサービス処理を行う手段、
サービス利用装置から送信された暗号化取引識別情報に署名処理する手段、
記憶手段に記憶された係数データa_{ij}（i=1,2,…,P;j=1,2,…,P）及び乱数r_k（k=1,2,…）を用いて、当該サービス取引の利用料金に基づくデータＥ（ｋ）、乱数Ｒ（ｋ）並びにサービス利用装置から送信された取引識別情報Ｔ（ｋ）によって計算されるＭ個の要素データV_s（ｋ）及び確認情報W_t（ｋ）を含むＰ（Ｐ≧２Ｍ＋２）個の値の互いに独立な一次結合データS_j（j=1,2,…,P）を以下の式（Ｂ）
$S_j(k)=a_{1j}E(k)+\{a_{(1+1)j}V_1(k)+a_{(2+1)j}V_2(k)+\cdots+a_{(M+1)}V_M(k)\}r_k+\{a_{(M+1+1)j}W_1(k)+a_{(M+2+1)j}W_2(k)+\cdots+a_{(2M+1)}W_M(k)\}r_{k+1}+a_{(2M+2)j}R(k)$・・・（Ｂ）
により算出する手段、
サービス利用装置のサービス取引回数をＮ回として、サービス利用装置から送信されたＰ個の結合集計データΣS_j（ｋ）及び係数データa_{ij}に基づいて取引識別情報Ｔ（１）～Ｔ（Ｎ）に関するデータＥ（ｋ）の集計値ΣＥ（ｋ）を算出する手段、
サービス利用装置から送信されたＰ個の結合集計データΣS_j（ｋ）及び係数データa_{ij}に基づいて取引識別情報Ｔ（１）～Ｔ（Ｎ）に関する要素データと乱数の積r_kV_s（ｋ）の各ｓ毎のｋについての集計値Σr_kV_s（ｋ）並びに取引識別情報Ｔ（１）～Ｔ（Ｎ＋１）に関する確認情報と乱数の積$r_{k+1}W_t$（ｋ）の各ｔ毎のｋについての集計値Σ$r_{k+1}W_t$（ｋ）を算出するとともに集計値Σ$r_{k+1}W_t$（ｋ）を送信する手段、
集計値Σr_kV_s（ｋ）とサービス利用装置から送信された集計値ΣX_u（ｋ）が矛盾するか否かで不正判定する手段、
として機能させるためのプログラム。
【請求項９】
サービス利用装置と、サービス利用装置に通信手段を介して接続されるとともにサービス利用装置からのサービス依頼を受けて当該サービスを処理するサービス提供装置とを備えているサービス取引システムであって、
前記サービス利用装置は、ｋ回目のサービス取引においてサービス取引に使用するために選択された取引識別情報Ｔ（ｋ）とその取引回数に基づいて設定された回数データＱ（

ｋ）を合体して識別データを生成する識別データ生成手段と、次回のサービス取引の識別データＴ（ｋ＋１）Ｑ（ｋ＋１）を暗号化処理し暗号化識別データを生成する暗号化処理手段と、取引識別情報Ｔ（ｋ＋１）から計算されるＭ個の要素データV_s（ｋ＋１）（s=1,2,…,M）のサービス提供装置の知らない係数による互いに独立なＭ個の一次結合である確認情報W_t（ｋ）（t=1,2,…,M）を生成する確認情報処理手段と、サービス提供装置から送信された署名処理済みの暗号化識別データを復号化処理して署名処理済みの識別データをメモリに記憶する復号化処理手段と、メモリに記憶された署名処理済みの識別データをサービス提供装置に送信してサービス依頼を行うサービス依頼手段と、ｋ回目のサービス取引記録としてサービス提供装置から送信される、後記の式（Ｄ）に基づいて計算される互いに独立なＰ個の一次結合データS_j（ｋ）（j=1,2,…,P）を登録する登録手段と、サービス提供装置からの集計依頼に応じて、登録されたＮ回分の一次結合データS_j（ｋ）を各ｊ毎にｋについて集計した結合集計データΣS_j（ｋ）を算出するとともに結合集計データΣS_j（ｋ）及び回数データＱ（Ｎ）に相当する値をサービス提供装置に送信する集計処理手段と、サービス提供装置から送信された集計値$\Sigma r_{k+1}W_t$（ｋ）（t=1,2,…,M）を復号化処理して集計値ΣX_u（ｋ）（u=1,2,…,M）を生成する要素集計値処理手段とを備え、

前記サービス提供装置は、サービス利用装置から送信された取引識別情報が有効なものであるか否か判定する識別情報判定手段と、取引識別情報が有効と判定された場合にサービス利用装置からの依頼に応じてサービス処理を行うサービス提供手段と、サービス利用装置から送信された暗号化識別データに署名処理する署名処理手段と、サービス利用装置の知らないP^2個の係数データa_{ij}（i=1,2,…,P;j=1,2,…,P）及び乱数r_k（k=1,2,…）の列を記憶する記憶手段と、サービス取引において、当該サービス取引の利用料金に基づくデータＥ（ｋ）、乱数Ｒ（ｋ）並びにサービス利用装置から送信された取引識別情報Ｔ（ｋ）によって計算されるＭ個の要素データV_s（ｋ）及び確認情報W_t（ｋ）を含むＰ（Ｐ≧２Ｍ＋３）個の値の、記憶手段に記憶された係数データa_{ij}及び乱数r_kを用いた互いに独立な一次結合データS_j（j=1,2,…,P）を以下の式（Ｄ）

$$S_j(k)=a_{1j}E(k)+a_{2j}Q(k)+\{a_{(1+2)j}V_1(k)+a_{(2+2)j}V_2(k)+\cdots+a_{(M+2)}V_M(k)\}r_k+\{a_{(M+1+2)j}W_1(k)+a_{(M+2+2)j}W_2(k)+\cdots+a_{(2M+2)}W_M(k)\}r_{k+1}+a_{(2M+3)j}R(k)\cdots(D)$$

により算出する結合計算手段と、サービス利用装置のサービス取引回数をＮ回として、サービス利用装置から送信されたＰ個の結合集計データΣS_j（ｋ）及び係数データa_{ij}に基づいて取引識別情報Ｔ（１）～Ｔ（Ｎ）に関するデータＥ（ｋ）の集計値ΣE（ｋ）を算出する合計額算出手段と、サービス利用装置から送信されたＰ個の結合集計データΣS_j（ｋ）及び係数データa_{ij}に基づいて取引識別情報Ｔ（１）～Ｔ（Ｎ）に関する回数データＱ（ｋ）の集計値ΣQ（ｋ）を算出して集計値ΣQ（ｋ）とサービス利用装置から送信された回数データＱ（Ｎ）に相当する値との間の整合性を判定する第一不正判定手段と、サービス利用装置から送信されたＰ個の結合集計データΣS_j（ｋ）及び係数データa_{ij}に基づいて取引識別情報Ｔ（１）～Ｔ（Ｎ）に関する要素データと乱数の積r_kV_s（ｋ）の各ｓ毎のｋについての集計値Σr_kV_s（ｋ）並びに取引識別情報Ｔ（１）～Ｔ（Ｎ＋１）に関する確認情報と乱数の積$r_{k+1}W_t$（ｋ）の各ｔ毎のｋについての集計値$\Sigma r_{k+1}W_t$（ｋ）を算出するとともに集計値$\Sigma r_{k+1}W_t$（ｋ）を送信する要素集計値算出手段と、集計値Σr_kV_s（ｋ）とサービス利用装置から送信された集計値ΣX_u（ｋ）が矛盾するか否か判定する第二不正判定手段とを備えていることを特徴とするサービス取引システム。

【請求項１０】

サービス利用装置からのサービス依頼を受けてサービス提供装置が当該サービスを処理するサービス取引方法であって、

サービス利用装置が、そのｋ回目のサービス取引において予めサービス提供装置から取得した署名処理済みの取引識別情報Ｔ（ｋ）を送信してサービス提供装置にサービス依頼し、サービス提供装置が、サービス利用装置から送信された取引識別情報が有効なもので

あるか否か判定するとともに、取引識別情報が有効と判定された場合にサービス利用装置からの依頼に応じてサービス処理し、サービス利用装置が、次回のサービス取引の取引識別情報Ｔ（ｋ＋１）とその取引回数に基づいて設定された回数データＱ（ｋ＋１）を合体して識別データＴ（ｋ＋１）Ｑ（ｋ＋１）を生成し暗号化して暗号化識別データとしてサービス提供装置に送信し、サービス提供装置が暗号化識別データに署名処理し、サービス利用装置が、署名処理された暗号化識別データを復号化処理して署名処理済みの識別データを取得するとともに、次回の取引識別情報Ｔ（ｋ＋１）に基づいて計算されるＭ個の要素データV_s（ｋ＋１）（s=1,2,…,Ｍ）のサービス提供装置の知らない係数による互いに独立なＭ個の一次結合である確認情報W_t（ｋ）（t=1,2,…,Ｍ）を生成し、サービス提供装置が、当該サービス取引の利用料金に基づくデータＥ（ｋ）、乱数Ｒ（ｋ）、サービス利用装置から送信された識別データＴ（ｋ）Ｑ（ｋ）から求められるＱ（ｋ）、サービス利用装置から送信された識別データＴ（ｋ）Ｑ（ｋ）から求められるＴ（ｋ）に基づいて計算されるＭ個の要素データV_s（ｋ）及びサービス利用装置から送信された確認情報W_t（ｋ）を含むＰ（Ｐ≧２Ｍ＋３）個の値の、サービス利用装置が知らない係数データa_{ij}（i=1,2,…,P;j=1,2,…,P）及び乱数r_k（k=1,2,…）を用いた互いに独立な一次結合データS_j（ｋ）（j=1,2,…,P）を以下の式（Ｄ）

$$S_j(k)=a_{1j}E(k)+a_{2j}Q(k)+\{a_{(1+2)j}V_1(k)+a_{(2+2)j}V_2(k)+\cdots+a_{(M+2)}V_M(k)\}r_k+\{a_{(M+1+2)j}W_1(k)+a_{(M+2+2)j}W_2(k)+\cdots+a_{(2M+2)}W_M(k)\}r_{k+1}+a_{(2M+3)j}R(k)\quad\cdots(D)$$

により算出し、算出されたＰ個の一次結合データS_j（ｋ）をサービス利用装置において登録し、サービス提供装置からの集計依頼に応じて、登録されたＮ回分の一次結合データS_j（ｋ）を各ｊ毎にｋについて集計した結合集計データΣS_j（ｋ）を算出するとともに結合集計データΣS_j（ｋ）及び回数データＱ（Ｎ）に相当する値をサービス提供装置に送信し、サービス提供装置が、サービス利用装置から送信されたＰ個の結合集計データΣS_j（ｋ）及び係数データa_{ij}に基づいて取引識別情報Ｔ（１）～Ｔ（Ｎ）に関するデータＥ（ｋ）の集計値ΣE（ｋ）を算出し、サービス利用装置から送信されたＰ個の結合集計データΣS_j（ｋ）及び係数データa_{ij}に基づいて取引識別情報Ｔ（１）～Ｔ（Ｎ）に関する回数データＱ（ｋ）の集計値ΣQ（ｋ）を算出して集計値ΣQ（ｋ）とサービス利用装置から送信された回数データＱ（Ｎ）に相当する値との間の整合性を判定し、サービス利用装置から送信されたＰ個の結合集計データΣS_j（ｋ）及び係数データa_{ij}に基づいて取引識別情報Ｔ（１）～Ｔ（Ｎ）に関する要素データと乱数の積r_kV_s（ｋ）の各ｓ毎のｋについての集計値Σr_kV_s（ｋ）並びに取引識別情報Ｔ（１）～Ｔ（Ｎ＋１）に関する確認情報と乱数の積$r_{k+1}W_t$（ｋ）の各ｔ毎のｋについての集計値$\Sigma r_{k+1}W_t$を算出するとともに集計値$\Sigma r_{k+1}W_t$（ｋ）をサービス利用装置に送信し、サービス利用装置が、サービス提供装置から送信された集計値$\Sigma r_{k+1}W_t$（ｋ）を復号化処理して集計値ΣX_u（ｋ）（u=1,2,…,Ｍ）を生成し、サービス提供装置が、サービス利用装置から送信された集計値ΣX_uと集計値Σr_kV_s（ｋ）との間に矛盾があるか否かを判定することを特徴とするサービス取引方法。

【請求項１１】

サービス利用装置と、サービス利用装置に通信手段を介して接続されるとともにサービス利用装置からのサービス依頼を受けて当該サービスを処理するサービス提供装置とを備えているサービス取引システムにおいて、該サービス利用装置を機能させるためのプログラムであって、

前記サービス利用装置を、

ｋ回目のサービス取引においてサービス取引に使用するために選択された取引識別情報Ｔ（ｋ）とその取引回数に基づいて設定された回数データＱ（ｋ）を合体して識別データを生成する手段、

次回のサービス取引の識別データＴ（ｋ＋１）Ｑ（ｋ＋１）を暗号化処理し暗号化識別データを生成する手段、

取引識別情報Ｔ（ｋ＋１）から計算されるＭ個の要素データV_s（ｋ＋１）（s=1,2,…,

M）のサービス提供装置の知らない係数による互いに独立なM個の一次結合である確認情報W_t（k）（t=1,2,…,M）を生成する手段、
サービス提供装置から送信された署名処理済みの暗号化識別データを復号化処理して署名処理済みの識別データをメモリに記憶する手段、
メモリに記憶された署名処理済みの識別データをサービス提供装置に送信してサービス依頼を行う手段、
k回目のサービス取引記録としてサービス提供装置から送信される、後記の式（D）に基づいて計算される互いに独立なP個の一次結合データS_j（k）（j=1,2,…,P）を登録する手段、
サービス提供装置からの集計依頼に応じて、登録されたN回分の一次結合データS_j（k）を各j毎にkについて集計した結合集計データΣS_j（k）を算出するとともに結合集計データΣS_j（k）及び回数データQ（N）に相当する値をサービス提供装置に送信する手段、
サービス提供装置から送信された集計値$\Sigma r_{k+1} W_t$（k）（t=1,2,…,M）を復号化処理して集計値ΣX_u（k）（u=1,2,…,M）を生成する手段、
として機能させるためのプログラム。
【請求項１２】
サービス利用装置と、サービス利用装置に通信手段を介して接続されるとともにサービス利用装置からのサービス依頼を受けて当該サービスを処理するサービス提供装置とを備えているサービス取引システムにおいて、該サービス提供装置を機能させるためのプログラムであって、
前記サービス提供装置を、
サービス利用装置から送信された取引識別情報が有効なものであるか否か判定する手段、
取引識別情報が有効と判定された場合にサービス利用装置からの依頼に応じてサービス処理を行う手段、
サービス利用装置から送信された暗号化識別データに署名処理する手段、
サービス取引において、当該サービス取引の利用料金に基づくデータE（k）、乱数R（k）並びにサービス利用装置から送信された取引識別情報T（k）によって計算されるM個の要素データV_s（k）及び確認情報W_t（k）を含むP（P≧２M＋３）個の値の、記憶手段に記憶された係数データa_{ij}（i=1,2,…,P;j=1,2,…,P）及び乱数r_k（k=1,2,…）を用いた互いに独立な一次結合データS_j（j=1,2,…,P）を以下の式（D）
$$S_j(k)=a_{1j}E(k)+a_{2j}Q(k)+\{a_{(1+2)j}V_1(k)+a_{(2+2)j}V_2(k)+\cdots+a_{(M+2)}V_M(k)\}r_k+\{a_{(M+1+2)j}W_1(k)+a_{(M+2+2)j}W_2(k)+\cdots+a_{(2M+2)}W_M(k)\}r_{k+1}+a_{(2M+3)j}R(k)\cdots(D)$$
により算出する手段、
サービス利用装置のサービス取引回数をN回として、サービス利用装置から送信されたP個の結合集計データΣS_j（k）及び係数データa_{ij}に基づいて取引識別情報T（１）～T（N）に関するデータE（k）の集計値ΣE（k）を算出する手段、
サービス利用装置から送信されたP個の結合集計データΣS_j（k）及び係数データa_{ij}に基づいて取引識別情報T（１）～T（N）に関する回数データQ（k）の集計値ΣQ（k）を算出して集計値ΣQ（k）とサービス利用装置から送信された回数データQ（N）に相当する値との間の整合性を判定する手段、
サービス利用装置から送信されたP個の結合集計データΣS_j（k）及び係数データa_{ij}に基づいて取引識別情報T（１）～T（N）に関する要素データと乱数の積$r_k V_s$（k）の各s毎のkについての集計値$\Sigma r_k V_s$（k）並びに取引識別情報T（１）～T（N＋１）に関する確認情報と乱数の積$r_{k+1} W_t$（k）の各t毎のkについての集計値$\Sigma r_{k+1} W_t$（k）を算出するとともに集計値$\Sigma r_{k+1} W_t$（k）を送信する手段、
集計値$\Sigma r_k V_s$（k）とサービス利用装置から送信された集計値ΣX_u（k）が矛盾するか否か不正判定する手段、

として機能させるためのプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、サービス取引システムにおいて、当該システムに関係する個人や物に密接に関連付けられる個別情報や取引情報が特定されることなくサービス取引を実施するサービス取引システム及びそのプログラムに関する。
【背景技術】
【０００２】
インターネット等のネットワークシステムが急速に普及するにつれて、様々な情報がネットワーク上で送受信されている。しかしながら、ネットワーク上でやりとりされる情報は、常に悪意を持った第三者に不正に取得されたり改変される危険性がある。そのため、安全対策として様々な暗号化処理技術が開発されており、ネットワーク上で送受信される情報を暗号化することで情報の不正利用や改変を防止するようにしている。
【０００３】
こうした通信情報の暗号化処理技術は、通信時の不正取得や改変には有効であるが、暗号化処理された情報が正当に取得されて復号化された後の情報の悪用には対応することができない。
【０００４】
すなわち、特定の個人がサービス提供会社にＩＤ及びパスワードを暗号化して送信し、サービス提供会社からサービスを受けた場合、その個人の受けたサービス内容は、ＩＤとともにサービス提供会社に蓄積され、その個人の関連情報として記憶されていく。このように蓄積された個別情報は、サービス提供会社で厳格な情報管理がなされていたとしても不正流用されるおそれがある。特に、情報処理システムの高度化に伴って大量の情報を簡単に処理することができるようになり、その危険性は大きくなっている。
【０００５】
例えば、銀行預金の預け入れや払い出し、クレジットカードを用いた商品の購入といったサービス取引では、サービス提供者である銀行や信販会社によって大量の取引情報が蓄積されるが、これらの取引情報が個人情報と関連付けられて蓄積されるためにこうした情報の保護が必要となる。そのため、サービス取引の際にサービス利用者の匿名性を高めることで、取引情報と個人情報との関連付けられないようする手法が検討されている。
【０００６】
特許文献１では、サービス提供者の端末が、サービス利用者に対してユーザＩＤを生成・発行するとともに該ユーザＩＤの正当性を証明する証明書を生成し、サービスの提供に必要なサービス利用者の個人情報をユーザＩＤと関連付けて記憶し、一の利用者の端末が他の利用者を指定して前記サービス提供者によるサービスを利用する際にユーザＩＤ及び証明書を取得し、該証明書によりユーザＩＤの正当性を検証してサービス提供者の端末に提示し、サービス提供者が該ユーザＩＤに関連付けられた個人情報基づきサービス提供を行う点が記載されている。
【０００７】
特許文献２では、商品の発注者が使用する発注者端末装置で匿名サービス提供者によって公開された公開鍵によって商品の宛先情報を暗号化した宛先暗号化情報を生成し、受注者端末装置では、受信した宛先暗号化情報を出力して匿名サービス端末装置に取り込み、匿名サービス端末装置では、取り込んだ宛先暗号化情報を秘密鍵によって復号して発注された商品の配送先を特定する点が記載されている。
【０００８】
特許文献３では、購入者が加盟店に匿名ＩＤを用いて商品を発注し、加盟店から匿名サービス提供者への商品の発送には購入者の個人情報が記載されていない伝票を用い、匿名サービス提供者において購入者の住所・氏名等が記載された伝票に変換した後、商品を購入者へ配送するようにした点が記載されている。

【０００９】
なお、本明細書において、「個別情報」とは、個人、会社等の法人及び個別に特定されて取り扱われる物（以下「個人等」という。）に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述等により特定の個人等を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人等を識別することができることとなるものを含む。）を意味する。
【特許文献１】特開２００５－５０３３０号公報
【特許文献２】特開２００４－１３９４１３号公報
【特許文献３】特開２００２－７９０４号公報
【発明の開示】
【発明が解決しようとする課題】
【００１０】
上述した特許文献に示すように、サービス利用者とサービス提供者との間に両方に誠実で中立的な機関を設立して、その機関を介してサービス取引が個人情報と関連付けられないようにすることは、中立的な機関においてサービス取引が個人情報と関連付けられるため中立的な機関からの情報漏洩の可能性がある限り絶対的に信用できるシステムとはなっていない。
【００１１】
このように、互いに信用できないサービス利用者及びサービス提供者がネットワークで接続されてサービス取引を実施するシステムでは、互いに安心してサービス取引を行うことはできないのが現状である。
【００１２】
そこで、本発明は、サービス利用者及びサービス提供者が通信手段で接続されてサービス取引を行うサービス取引システムにおいて、サービス利用者が個々の取引を自分自身と関連付けられることなくサービス依頼することができるとともにサービス提供者がサービス利用者の利用料金の適正な総額を確実に算定することができ、またサービス利用者や提供者が不正な取引を実行した場合にはそれを特定することができるサービス取引システムを提供することを目的とするものである。
【課題を解決するための手段】
【００１３】
本発明に係るサービス取引システムは、サービス利用装置と、サービス利用装置に通信手段を介して接続されるとともにサービス利用装置からのサービス依頼を受けて当該サービスを処理するサービス提供装置とを備えているサービス取引システムであって、前記サービス提供装置は、サービス利用装置から送信された取引識別情報が有効なものであるか否か判定する識別情報判定手段と、取引識別情報が有効と判定された場合にサービス利用装置からの依頼に応じてサービス処理を行うサービス提供手段と、サービス利用装置から送信された暗号化取引識別情報に署名処理する署名処理手段と、サービス利用装置から送信された今回の取引識別情報及び確認情報の組を含む情報をサービス利用装置の取引記録として生成する取引記録生成手段とを備え、前記サービス利用装置は、メモリに記憶されたサービス提供装置による署名処理済みの取引識別情報をサービス提供装置に送信してサービス依頼を行うサービス依頼手段と、次回のサービス取引の取引識別情報を選択する識別情報選択手段と、取引識別情報を暗号化処理し暗号化取引識別情報を生成する暗号化処理手段と、サービス提供装置から送信された署名処理済みの暗号化取引識別情報を復号化処理して署名処理済みの取引識別情報をメモリに記憶する復号化処理手段と、次回取引のための取引識別情報からサービス提供装置が知らないパラメータを用いて計算される確認情報を生成する確認情報処理手段とを備えていることを特徴とする。
【００１４】
本発明に係るサービス取引方法は、サービス利用装置からのサービス依頼を受けてサービス提供装置が当該サービスを処理するサービス取引方法であって、サービス利用装置が予めサービス提供装置から取得した署名処理済みの取引識別情報を送信してサービス提供

装置にサービス依頼し、サービス提供装置が、サービス利用装置から送信された取引識別情報が有効なものであるか否かを判定し、取引識別情報が有効と判定された場合にサービス利用装置からの依頼に応じてサービス処理するとともに、サービス利用装置が、次回のサービス取引の取引識別情報を暗号化処理することによって暗号化取引識別情報を生成し、また次回の取引識別情報からサービス提供装置の知らないパラメータを用いて計算される確認情報を生成してそれぞれサービス提供装置に送信し、サービス提供装置が、サービス利用装置から送信された暗号化取引識別情報に対して署名処理するとともに、今回の取引識別情報及び確認情報を含む情報をサービス利用装置の取引記録として生成し、サービス利用装置が、サービス提供装置から送信された署名処理済みの暗号化取引識別情報を復号化処理して署名処理済みの取引識別情報を取得することを特徴とする。

【００１５】

本発明に係るプログラムは、サービス利用装置と、サービス利用装置に通信手段を介して接続されるとともにサービス利用装置からのサービス依頼を受けて当該サービスを処理するサービス提供装置とを備えているサービス取引システムにおいて、該サービス利用装置を機能させるためのプログラムであって、前記サービス利用装置を、メモリに記憶されたサービス提供装置による署名処理済みの取引識別情報をサービス提供装置に送信してサービス依頼を行う手段、次回のサービス取引の取引識別情報を選択する手段、取引識別情報を暗号化処理し暗号化取引識別情報を生成する手段、次回のサービス取引の取引識別情報からサービス提供装置の知らないパラメータを用いて計算される確認情報を生成する手段、サービス提供装置から送信された署名処理済みの暗号化取引識別情報を復号化処理して署名処理済みの取引識別情報をメモリに記憶する手段、として機能させる。

【００１６】

本発明に係る別のプログラムは、サービス利用装置と、サービス利用装置に通信手段を介して接続されるとともにサービス利用装置からのサービス依頼を受けて当該サービスを処理するサービス提供装置とを備えているサービス取引システムにおいて、該サービス提供装置を機能させるためのプログラムであって、前記サービス提供装置を、サービス利用装置から送信された取引識別情報が有効なものであるか否か判定する手段、取引識別情報が有効と判定された場合にサービス利用装置からの依頼に応じてサービス処理を行う手段、サービス利用装置から送信された暗号化取引識別情報に署名処理する手段、サービス利用装置から送信された今回の取引識別情報と確認情報の組を含む情報をサービス利用装置の取引記録として生成する手段、として機能させる。

【００１７】

本発明に係る別のサービス取引システムは、サービス利用装置と、サービス利用装置に通信手段を介して接続されるとともにサービス利用装置からのサービス依頼を受けて当該サービスを処理するサービス提供装置とを備えているサービス取引システムであって、前記サービス利用装置は、ｋ回目のサービス取引において（ｋ＋１）回目のサービス取引の取引識別情報Ｔ（ｋ＋１）を暗号化処理し暗号化取引識別情報を生成する暗号化処理手段と、取引識別情報Ｔ（ｋ＋１）から計算されるＭ個の要素データV_s（ｋ＋１）（s=1,2,…,M）のサービス提供装置の知らない係数による互いに独立なＭ個の一次結合である確認情報W_t（ｋ）（t=1,2,…,M）を生成する確認情報処理手段と、サービス提供装置から送信された署名処理済みの暗号化取引識別情報を復号化処理して署名処理済みの取引識別情報をメモリに記憶する復号化処理手段と、メモリに記憶されたｋ回目のサービス取引のための署名処理済みの取引識別情報Ｔ（ｋ）をサービス提供装置に送信してサービス依頼を行うサービス依頼手段と、ｋ回目のサービス取引記録としてサービス提供装置から送信される、後記の式（Ｂ）に基づいて計算される互いに独立なＰ個の一次結合データS_j（ｋ）（j=1,2,…,P）を登録する登録手段と、サービス提供装置からの集計依頼に応じて登録された一次結合データS_j（ｋ）を各ｊ毎にｋについて集計した結合集計データΣS_j（ｋ）を算出するとともに、サービス提供装置から送信された集計値Σ$r_{k+1}W_t$（ｋ）（t=1,2,…,M）を復号化処理して集計値ΣX_u（ｋ）（u=1,2,…,M）を生成する要素集計値処理手段とを備え、前記サービス提供装置は、サービス利用装置から送信された取引識別情報

が有効なものであるか否か判定する識別情報判定手段と、取引識別情報が有効と判定された場合にサービス利用装置からの依頼に応じてサービス処理を行うサービス提供手段と、サービス利用装置から送信された暗号化取引識別情報に署名処理する署名処理手段と、サービス利用装置の知らないP^2個の係数データa_{ij}（i=1,2,…,P;j=1,2,…,P）及び乱数r_k（k=1,2,…）の列を記憶する記憶手段と、記憶手段に記憶された係数データa_{ij}及び乱数r_kを用いて、当該サービス取引の利用料金に基づくデータE（k）、乱数R（k）並びにサービス利用装置から送信された取引識別情報T（k）によって計算されるM個の要素データV_s（k）及び確認情報W_t（k）を含むP（P≧2M＋2）個の値の互いに独立な一次結合データS_j（j=1,2,…,P）を以下の式（B）

$$S_j(k)=a_{1j}E(k)+\{a_{(1+1)j}V_1(k)+a_{(2+1)j}V_2(k)+\cdots+a_{(M+1)}V_M(k)\}r_k+\{a_{(M+1+1)j}W_1(k)+a_{(M+2+1)j}W_2(k)+\cdots+a_{(2M+1)}W_M(k)\}r_{k+1}+a_{(2M+2)j}R(k)\cdots(B)$$

により算出する結合計算手段と、サービス利用装置のサービス取引回数をN回として、サービス利用装置から送信されたP個の結合集計データΣS_j（k）及び係数データa_{ij}に基づいて取引識別情報T（1）～T（N）に関するデータE（k）の集計値ΣE（k）を算出する合計額算出手段と、サービス利用装置から送信されたP個の結合集計データΣS_j（k）及び係数データa_{ij}に基づいて取引識別情報T（1）～T（N）に関する要素データと乱数の積r_kV_s（k）の各s毎のkについての集計値Σr_kV_s（k）並びに取引識別情報T（1）～T（N＋1）に関する確認情報と乱数の積$r_{k+1}W_t$（k）の各t毎のkについての集計値$\Sigma r_{k+1}W_t$（k）を算出するとともに集計値$\Sigma r_{k+1}W_t$（k）を送信する要素集計値算出手段と、集計値Σr_kV_s（k）とサービス利用装置から送信された集計値ΣX_u（k）が矛盾するか否か判定する不正判定手段とを備えていることを特徴とする。

【００１８】

本発明に係る別のサービス取引方法は、サービス利用装置からのサービス依頼を受けてサービス提供装置が当該サービスを処理するサービス取引方法であって、サービス利用装置が、そのk回目のサービス取引において予めサービス提供装置から取得した署名処理済みの取引識別情報T（k）を送信してサービス提供装置にサービス依頼し、サービス提供装置が、サービス利用装置から送信された取引識別情報が有効なものであるか否か判定するとともに、取引識別情報が有効と判定された場合にサービス利用装置からの依頼に応じてサービス処理し、サービス利用装置が、次回のサービス取引の取引識別情報T（k＋1）を暗号化した暗号化取引識別情報と、取引識別情報T（k＋1）に基づいて計算されるM個の要素データV_s（k）（s=1,2,…,M）のサービス提供装置の知らない係数による互いに独立なM個の一次結合である確認情報W_t（k）（t=1,2,…,M）を生成し、サービス提供装置が、次回サービス取引のための暗号化識別情報に署名するとともに、当該サービス取引の利用料金に基づくデータE（k）、乱数R（k）、サービス利用装置から送信された取引識別情報T（k）に基づいて計算されるM個の要素データV_s（k）及び確認情報W_t（k）を含むP（P≧2M＋2）個の値の、サービス利用装置が知らない係数データa_{ij}（i=1,2,…,P;j=1,2,…,P）及び乱数r_k（k=1,2,…）を用いた互いに独立な一次結合データS_j（k）（j=1,2,…,P）を以下の式（B）

$$S_j(k)=a_{1j}E(k)+\{a_{(1+1)j}V_1(k)+a_{(2+1)j}V_2(k)+\cdots+a_{(M+1)}V_M(k)\}r_k+\{a_{(M+1+1)j}W_1(k)+a_{(M+2+1)j}W_2(k)+\cdots+a_{(2M+1)}W_M(k)\}r_{k+1}+a_{(2M+2)j}R(k)\cdots(B)$$

により算出し、算出されたP個の一次結合データS_j（k）をサービス利用装置において登録し、サービス提供装置からの集計依頼に応じて、登録されたN回分の一次結合データS_j（k）を各j毎にkについて集計した結合集計データΣS_j（k）を算出するとともに結合集計データΣS_j（k）をサービス提供装置に送信し、サービス提供装置が、サービス利用装置から送信されたP個の結合集計データΣS_j（k）及び係数データa_{ij}に基づいて取引識別情報T（1）～T（N）に関するデータE（k）の集計値ΣE（k）を算出し、サービス利用装置から送信されたP個の結合集計データΣS_j（k）及び係数データ

a_{ij}に基づいて取引識別情報Ｔ（１）～Ｔ（Ｎ）に関する要素データと乱数の積$r_k V_s$（ｋ）の各ｓ毎のｋについての集計値Σ$r_k V_s$（ｋ）並びに取引識別情報Ｔ（１）～Ｔ（Ｎ＋１）に関する確認情報と乱数の積$r_{k+1} W_t$（ｋ）の各ｔ毎のｋについての集計値Σ$r_{k+1} W_t$を算出するとともに集計値Σ$r_{k+1} W_t$（ｋ）をサービス利用装置に送信し、サービス利用装置が、サービス提供装置から送信された集計値Σ$r_{k+1} W_t$（ｋ）を復号化処理して集計値ΣX_u（ｋ）（u=1,2,…,Ｍ）を生成し、サービス提供装置が、サービス利用装置から送信された集計値ΣX_uと集計値Σ$r_k V_s$（ｋ）との間に矛盾があるか否かを判定することを特徴とする。

【００１９】

本発明に係るさらに別のプログラムは、サービス利用装置と、サービス利用装置に通信手段を介して接続されるとともにサービス利用装置からのサービス依頼を受けて当該サービスを処理するサービス提供装置とを備えているサービス取引システムにおいて、該サービス利用装置を機能させるためのプログラムであって、前記サービス利用装置を、ｋ回目のサービス取引において（ｋ＋１）回目のサービス取引の取引識別情報Ｔ（ｋ＋１）を暗号化処理し暗号化取引識別情報を生成する手段、取引識別情報Ｔ（ｋ＋１）から計算されるＭ個の要素データV_s（ｋ＋１）（s=1,2,…,Ｍ）のサービス提供装置の知らない係数による互いに独立なＭ個の一次結合である確認情報W_t（ｋ）（t=1,2,…,Ｍ）を生成する手段、サービス提供装置から送信された署名処理済みの暗号化取引識別情報を復号化処理して署名処理済みの取引識別情報をメモリに記憶する復号化処理手段、メモリに記憶されたｋ回目のサービス取引のための署名処理済みの取引識別情報Ｔ（ｋ）をサービス提供装置に送信してサービス依頼を行う手段、ｋ回目のサービス取引記録としてサービス提供装置から送信される、後記の式（Ｂ）に基づいて計算される互いに独立なＰ個の一次結合データS_j（ｋ）（j=1,2,…,Ｐ）を登録する手段、サービス提供装置からの集計依頼に応じて登録された一次結合データS_j（ｋ）を各ｊ毎にｋについて集計した結合集計データΣS_j（ｋ）を算出するとともに、サービス提供装置から送信された集計値Σ$r_{k+1} W_t$（ｋ）（t=1,2,…,Ｍ）を復号化処理して集計値ΣX_u（ｋ）（u=1,2,…,Ｍ）を生成する手段、として機能させる。

【００２０】

本発明に係るさらに別のプログラムは、サービス利用装置と、サービス利用装置に通信手段を介して接続されるとともにサービス利用装置からのサービス依頼を受けて当該サービスを処理するサービス提供装置とを備えているサービス取引システムにおいて、該サービス提供装置を機能させるためのプログラムであって、前記サービス提供装置を、サービス利用装置から送信された取引識別情報が有効なものであるか否か判定する手段、取引識別情報が有効と判定された場合にサービス利用装置からの依頼に応じてサービス処理を行う手段、サービス利用装置から送信された暗号化取引識別情報に署名処理する手段、記憶手段に記憶された係数データa_{ij}（i=1,2,…,P;j=1,2,…,Ｐ）及び乱数r_k（k=1,2,…）を用いて、当該サービス取引の利用料金に基づくデータＥ（ｋ）、乱数Ｒ（ｋ）並びにサービス利用装置から送信された取引識別情報Ｔ（ｋ）によって計算されるＭ個の要素データV_s（ｋ）及び確認情報W_t（ｋ）を含むＰ（Ｐ≧２Ｍ＋２）個の値の互いに独立な一次結合データS_j（j=1,2,…,Ｐ）を以下の式（Ｂ）

$$S_j(k) = a_{1j}E(k) + \{a_{(1+1)j}V_1(k) + a_{(2+1)j}V_2(k) + \cdots + a_{(M+1)}V_M(k)\}r_k + \{a_{(M+1+1)j}W_1(k) + a_{(M+2+1)j}W_2(k) + \cdots + a_{(2M+1)}W_M(k)\}r_{k+1} + a_{(2M+2)j}R(k) \cdots (B)$$

により算出する手段、サービス利用装置のサービス取引回数をＮ回として、サービス利用装置から送信されたＰ個の結合集計データΣS_j（ｋ）及び係数データa_{ij}に基づいて取引識別情報Ｔ（１）～Ｔ（Ｎ）に関するデータＥ（ｋ）の集計値ΣＥ（ｋ）を算出する手段、サービス利用装置から送信されたＰ個の結合集計データΣS_j（ｋ）及び係数データa_{ij}に基づいて取引識別情報Ｔ（１）～Ｔ（Ｎ）に関する要素データと乱数の積$r_k V_s$（ｋ）の各ｓ毎のｋについての集計値Σ$r_k V_s$（ｋ）並びに取引識別情報Ｔ（１）～Ｔ（Ｎ＋１）に関する確認情報と乱数の積$r_{k+1} W_t$（ｋ）の各ｔ毎のｋについての集計値Σr_{k+}

$_1W_t$（ｋ）を算出するとともに集計値Σ$r_{k+1}W_t$（ｋ）を送信する手段、集計値Σr_kV_s（ｋ）とサービス利用装置から送信された集計値ΣX_u（ｋ）が矛盾するか否かで不正判定する手段、として機能させる。

【００２１】

本発明に係るさらに別のサービス取引システムは、サービス利用装置と、サービス利用装置に通信手段を介して接続されるとともにサービス利用装置からのサービス依頼を受けて当該サービスを処理するサービス提供装置とを備えているサービス取引システムであって、前記サービス利用装置は、ｋ回目のサービス取引においてサービス取引に使用するために選択された取引識別情報Ｔ（ｋ）とその取引回数に基づいて設定された回数データＱ（ｋ）を合体して識別データを生成する識別データ生成手段と、次回のサービス取引の識別データＴ（ｋ＋１）Ｑ（ｋ＋１）を暗号化処理し暗号化識別データを生成する暗号化処理手段と、取引識別情報Ｔ（ｋ＋１）から計算されるＭ個の要素データV_s（ｋ＋１）（s=1,2,…,M）のサービス提供装置の知らない係数による互いに独立なＭ個の一次結合である確認情報W_t（ｋ）（t=1,2,…,M）を生成する確認情報処理手段と、サービス提供装置から送信された署名処理済みの暗号化識別データを復号化処理して署名処理済みの識別データをメモリに記憶する復号化処理手段と、メモリに記憶された署名処理済みの識別データをサービス提供装置に送信してサービス依頼を行うサービス依頼手段と、ｋ回目のサービス取引記録としてサービス提供装置から送信される、後記の式（Ｄ）に基づいて計算される互いに独立なＰ個の一次結合データS_j（ｋ）（j=1,2,…,P）を登録する登録手段と、サービス提供装置からの集計依頼に応じて、登録されたＮ回分の一次結合データS_j（ｋ）を各ｊ毎にｋについて集計した結合集計データΣS_j（ｋ）を算出するとともに結合集計データΣS_j（ｋ）及び回数データＱ（Ｎ）に相当する値をサービス提供装置に送信する集計処理手段と、サービス提供装置から送信された集計値Σ$r_{k+1}W_t$（ｋ）（t=1,2,…,M）を復号化処理して集計値ΣX_u（ｋ）（u=1,2,…,M）を生成する要素集計値処理手段とを備え、前記サービス提供装置は、サービス利用装置から送信された取引識別情報が有効なものであるか否か判定する識別情報判定手段と、取引識別情報が有効と判定された場合にサービス利用装置からの依頼に応じてサービス処理を行うサービス提供手段と、サービス利用装置から送信された暗号化識別データに署名処理する署名処理手段と、サービス利用装置の知らないP^2個の係数データa_{ij}（i=1,2,…,P;j=1,2,…,P）及び乱数r_k（k=1,2,…）の列を記憶する記憶手段と、サービス取引において、当該サービス取引の利用料金に基づくデータＥ（ｋ）、乱数Ｒ（ｋ）並びにサービス利用装置から送信された取引識別情報Ｔ（ｋ）によって計算されるＭ個の要素データV_s（ｋ）及び確認情報W_t（ｋ）を含むＰ（Ｐ≧２Ｍ＋３）個の値の、記憶手段に記憶された係数データa_{ij}及び乱数r_kを用いた互いに独立な一次結合データS_j（j=1,2,…,P）を以下の式（Ｄ）

$$S_j(k)=a_{1j}E(k)+a_{2j}Q(k)+\{a_{(1+2)j}V_1(k)+a_{(2+2)j}V_2(k)+\cdots+a_{(M+2)}V_M(k)\}r_k+\{a_{(M+1+2)j}W_1(k)+a_{(M+2+2)j}W_2(k)+\cdots+a_{(2M+2)}W_M(k)\}r_{k+1}+a_{(2M+3)j}R(k)\cdots(D)$$

により算出する結合計算手段と、サービス利用装置のサービス取引回数をＮ回として、サービス利用装置から送信されたＰ個の結合集計データΣS_j（ｋ）及び係数データa_{ij}に基づいて取引識別情報Ｔ（１）～Ｔ（Ｎ）に関するデータＥ（ｋ）の集計値ΣＥ（ｋ）を算出する合計額算出手段と、サービス利用装置から送信されたＰ個の結合集計データΣS_j（ｋ）及び係数データa_{ij}に基づいて取引識別情報Ｔ（１）～Ｔ（Ｎ）に関する回数データＱ（ｋ）の集計値ΣＱ（ｋ）を算出して集計値ΣＱ（ｋ）とサービス利用装置から送信された回数データＱ（Ｎ）に相当する値との間の整合性を判定する第一不正判定手段と、サービス利用装置から送信されたＰ個の結合集計データΣS_j（ｋ）及び係数データa_{ij}に基づいて取引識別情報Ｔ（１）～Ｔ（Ｎ）に関する要素データと乱数の積r_kV_s（ｋ）の各ｓ毎のｋについての集計値Σr_kV_s（ｋ）並びに取引識別情報Ｔ（１）～Ｔ（Ｎ＋１）に関する確認情報と乱数の積$r_{k+1}W_t$（ｋ）の各ｔ毎のｋについての集計値Σ$r_{k+1}W_t$（ｋ）を算出するとともに集計値Σ$r_{k+1}W_t$（ｋ）を送信する要素集計値算出手段と、集計値Σr_kV_s（ｋ）とサービス利用装置から送信された集計値ΣX_u（ｋ）が矛盾す

るか否か判定する第二不正判定手段とを備えていることを特徴とする。

【００２２】

本発明に係るさらに別のサービス取引方法は、サービス利用装置からのサービス依頼を受けてサービス提供装置が当該サービスを処理するサービス取引方法であって、サービス利用装置が、そのｋ回目のサービス取引において予めサービス提供装置から取得した署名処理済みの取引識別情報Ｔ（ｋ）を送信してサービス提供装置にサービス依頼し、サービス提供装置が、サービス利用装置から送信された取引識別情報が有効なものであるか否か判定するとともに、取引識別情報が有効と判定された場合にサービス利用装置からの依頼に応じてサービス処理し、サービス利用装置が、次回のサービス取引の取引識別情報Ｔ（ｋ＋１）とその取引回数に基づいて設定された回数データＱ（ｋ＋１）を合体して識別データＴ（ｋ＋１）Ｑ（ｋ＋１）を生成し暗号化して暗号化識別データとしてサービス提供装置に送信し、サービス提供装置が暗号化識別データに署名処理し、サービス利用装置が、署名処理された暗号化識別データを復号化処理して署名処理済みの識別データを取得するとともに、次回の取引識別情報Ｔ（ｋ＋１）に基づいて計算されるＭ個の要素データV_s（ｋ＋１）（s=1,2,…,M）のサービス提供装置の知らない係数による互いに独立なＭ個の一次結合である確認情報W_t（ｋ）（t=1,2,…,M）を生成し、サービス提供装置が、当該サービス取引の利用料金に基づくデータＥ（ｋ）、乱数Ｒ（ｋ）、サービス利用装置から送信された識別データＴ（ｋ）Ｑ（ｋ）から求められるＱ（ｋ）、サービス利用装置から送信された識別データＴ（ｋ）Ｑ（ｋ）から求められるＴ（ｋ）に基づいて計算されるＭ個の要素データV_s（ｋ）及びサービス利用装置から送信された確認情報W_t（ｋ）を含むＰ（Ｐ≧２Ｍ＋３）個の値の、サービス利用装置が知らない係数データa_{ij}（i=1,2,…,P;j=1,2,…,P）及び乱数r_k（k=1,2,…）を用いた互いに独立な一次結合データS_j（ｋ）（j=1,2,…,P）を以下の式（Ｄ）

$$S_j(k)=a_{1j}E(k)+a_{2j}Q(k)+\{a_{(1+2)j}V_1(k)+a_{(2+2)j}V_2(k)+\cdots+a_{(M+2)}V_M(k)\}r_k+\{a_{(M+1+2)j}W_1(k)+a_{(M+2+2)j}W_2(k)+\cdots+a_{(2M+2)}W_M(k)\}r_{k+1}+a_{(2M+3)j}R(k)\cdots(D)$$

により算出し、算出されたＰ個の一次結合データS_j（ｋ）をサービス利用装置において登録し、サービス提供装置からの集計依頼に応じて、登録されたＮ回分の一次結合データS_j（ｋ）を各ｊ毎にｋについて集計した結合集計データΣS_j（ｋ）を算出するとともに結合集計データΣS_j（ｋ）及び回数データＱ（Ｎ）に相当する値をサービス提供装置に送信し、サービス提供装置が、サービス利用装置から送信されたＰ個の結合集計データΣS_j（ｋ）及び係数データa_{ij}に基づいて取引識別情報Ｔ（１）～Ｔ（Ｎ）に関するデータＥ（ｋ）の集計値ΣE（ｋ）を算出し、サービス利用装置から送信されたＰ個の結合集計データΣS_j（ｋ）及び係数データa_{ij}に基づいて取引識別情報Ｔ（１）～Ｔ（Ｎ）に関する回数データＱ（ｋ）の集計値ΣQ（ｋ）を算出して集計値ΣQ（ｋ）とサービス利用装置から送信された回数データＱ（Ｎ）に相当する値との間の整合性を判定し、サービス利用装置から送信されたＰ個の結合集計データΣS_j（ｋ）及び係数データa_{ij}に基づいて取引識別情報Ｔ（１）～Ｔ（Ｎ）に関する要素データと乱数の積r_kV_s（ｋ）の各ｓ毎のｋについての集計値Σr_kV_s（ｋ）並びに取引識別情報Ｔ（１）～Ｔ（Ｎ＋１）に関する確認情報と乱数の積$r_{k+1}W_t$（ｋ）の各ｔ毎のｋについての集計値$\Sigma r_{k+1}W_t$を算出するとともに集計値$\Sigma r_{k+1}W_t$（ｋ）をサービス利用装置に送信し、サービス利用装置が、サービス提供装置から送信された集計値$\Sigma r_{k+1}W_t$（ｋ）を復号化処理して集計値ΣX_u（ｋ）（u=1,2,…,M）を生成し、サービス提供装置が、サービス利用装置から送信された集計値ΣX_uと集計値Σr_kV_s（ｋ）との間に矛盾があるか否かを判定することを特徴とする。

【００２３】

本発明に係るさらに別のプログラムは、サービス利用装置と、サービス利用装置に通信手段を介して接続されるとともにサービス利用装置からのサービス依頼を受けて当該サービスを処理するサービス提供装置とを備えているサービス取引システムにおいて、該サービス利用装置を機能させるためのプログラムであって、前記サービス利用装置を、ｋ回目

のサービス取引においてサービス取引に使用するために選択された取引識別情報Ｔ（ｋ）とその取引回数に基づいて設定された回数データＱ（ｋ）を合体して識別データを生成する手段、次回のサービス取引の識別データＴ（ｋ＋１）Ｑ（ｋ＋１）を暗号化処理し暗号化識別データを生成する手段、取引識別情報Ｔ（ｋ＋１）から計算されるＭ個の要素データV_s（ｋ＋１）（s=1,2,…,M）のサービス提供装置の知らない係数による互いに独立なＭ個の一次結合である確認情報W_t（ｋ）（t=1,2,…,M）を生成する手段、サービス提供装置から送信された署名処理済みの暗号化識別データを復号化処理して署名処理済みの識別データをメモリに記憶する手段、メモリに記憶された署名処理済みの識別データをサービス提供装置に送信してサービス依頼を行う手段、ｋ回目のサービス取引記録としてサービス提供装置から送信される、後記の式（Ｄ）に基づいて計算される互いに独立なＰ個の一次結合データS_j（ｋ）（j=1,2,…,P）を登録する手段、サービス提供装置からの集計依頼に応じて、登録されたＮ回分の一次結合データS_j（ｋ）を各ｊ毎にｋについて集計した結合集計データΣS_j（ｋ）を算出するとともに結合集計データΣS_j（ｋ）及び回数データＱ（Ｎ）に相当する値をサービス提供装置に送信する手段、サービス提供装置から送信された集計値$\Sigma r_{k+1}W_t$（ｋ）（t=1,2,…,M）を復号化処理して集計値ΣX_u（ｋ）（u=1,2,…,M）を生成する手段、として機能させる。

【００２４】

本発明に係るさらに別のプログラムは、サービス利用装置と、サービス利用装置に通信手段を介して接続されるとともにサービス利用装置からのサービス依頼を受けて当該サービスを処理するサービス提供装置とを備えているサービス取引システムにおいて、該サービス提供装置を機能させるためのプログラムであって、前記サービス提供装置を、サービス利用装置から送信された取引識別情報が有効なものであるか否か判定する手段、取引識別情報が有効と判定された場合にサービス利用装置からの依頼に応じてサービス処理を行う手段、サービス利用装置から送信された暗号化識別データに署名処理する手段、サービス取引において、当該サービス取引の利用料金に基づくデータＥ（ｋ）、乱数Ｒ（ｋ）並びにサービス利用装置から送信された取引識別情報Ｔ（ｋ）によって計算されるＭ個の要素データV_s（ｋ）及び確認情報W_t（ｋ）を含むＰ（Ｐ≧２Ｍ＋３）個の値の、記憶手段に記憶された係数データa_{ij}（i=1,2,…,P;j=1,2,…,P）及び乱数r_k（k=1,2,…）を用いた互いに独立な一次結合データS_j（j=1,2,…,P）を以下の式（Ｄ）

$$S_j(k)=a_{1j}E(k)+a_{2j}Q(k)+\{a_{(1+2)j}V_1(k)+a_{(2+2)j}V_2(k)+\cdots+a_{(M+2)}V_M(k)\}r_k+\{a_{(M+1+2)j}W_1(k)+a_{(M+2+2)j}W_2(k)+\cdots+a_{(2M+2)}W_M(k)\}r_{k+1}+a_{(2M+3)j}R(k)\cdots(D)$$

により算出する手段、サービス利用装置のサービス取引回数をＮ回として、サービス利用装置から送信されたＰ個の結合集計データΣS_j（ｋ）及び係数データa_{ij}に基づいて取引識別情報Ｔ（１）～Ｔ（Ｎ）に関するデータＥ（ｋ）の集計値ΣE（ｋ）を算出する手段、サービス利用装置から送信されたＰ個の結合集計データΣS_j（ｋ）及び係数データa_{ij}に基づいて取引識別情報Ｔ（１）～Ｔ（Ｎ）に関する回数データＱ（ｋ）の集計値ΣQ（ｋ）を算出して集計値ΣQ（ｋ）とサービス利用装置から送信された回数データＱ（Ｎ）に相当する値との間の整合性を判定する手段、サービス利用装置から送信されたＰ個の結合集計データΣS_j（ｋ）及び係数データa_{ij}に基づいて取引識別情報Ｔ（１）～Ｔ（Ｎ）に関する要素データと乱数の積r_kV_s（ｋ）の各ｓ毎のｋについての集計値Σr_kV_s（ｋ）並びに取引識別情報Ｔ（１）～Ｔ（Ｎ＋１）に関する確認情報と乱数の積$r_{k+1}W_t$（ｋ）の各ｔ毎のｋについての集計値$\Sigma r_{k+1}W_t$（ｋ）を算出するとともに集計値$\Sigma r_{k+1}W_t$（ｋ）を送信する手段、集計値Σr_kV_s（ｋ）とサービス利用装置から送信された集計値ΣX_u（ｋ）が矛盾するか否か不正判定する手段、として機能させる。

【発明の効果】

【００２５】

本発明に係るサービス取引システム及びサービス取引方法は、サービス利用装置が予めサービス提供装置から取得した署名処理済みの取引識別情報を送信しサービス提供装置で当該取引識別情報を用いて個々の取引において正当な利用者か否かを、当該取引識別情報

にサービス提供装置の正しい署名があるか、また当該取引識別情報が既に利用されているものではないかを調べることによって判定してサービス処理を行い、サービス取引が正常に完了した後にサービス利用装置から次回のサービス取引の取引識別情報を暗号化処理した暗号化取引識別情報を送信しサービス提供装置で当該暗号化取引識別情報を署名処理して送信し、署名処理済みの暗号化取引識別情報をサービス利用装置で復号化処理して署名処理済みの次回の取引識別情報を取得するようにしているので、個々の取引においても利用者とは関連付けられていない署名処理済みの取引識別情報を用いて正当な利用者であるかサービス提供装置が判定することができる。さらに、次回に使用する取引識別情報は、サービス取引が正常に完了した後に暗号化処理された状態でサービス提供装置に送信されるので、サービス提供装置は次回の取引識別情報を知らずに署名処理することになり、サービス提供装置はサービス利用装置がサービスに関する処理を正しく終了してから次回のサービスを受けることを確認できるが、サービス利用装置が今回のサービス取引と次回のサービス取引との間の関連付けをサービス提供装置に知られることはない。署名処理済みの暗号化取引識別情報は、サービス利用装置で復号化処理されて解読可能な署名処理済みの取引識別情報となり、次回のサービス取引の際にサービス提供装置に送信されるようになる。

【００２６】

以上のように、サービス利用装置は、個々の取引に関して関連付けられることなく取引を行うことができ、個別情報と関連付けられることなく認証を受けてサービス依頼を行うことができれば、利用者の個人情報に関連付けられて取引関連情報を蓄積されることがなくなる。また、サービス提供装置は、利用者を特定することなく利用者の正当性や取引の際の正当性を判定することができ、サービス取引の際の個別情報の管理を厳重に行う必要がなくなり、従来のような第三者機関を介して行う必要もなくなる。

【００２７】

本発明に係る別のサービス取引システム及びサービス取引方法は、サービス利用装置が、そのｋ回目のサービス取引において予めサービス提供装置から取得した署名処理済みの取引識別情報Ｔ（ｋ）を送信してサービス提供装置にサービス依頼し、サービス提供装置が、サービス利用装置から送信された取引識別情報が有効なものであるか否か判定するとともに、取引識別情報が有効と判定された場合にサービス利用装置からの依頼に応じてサービス処理し、サービス利用装置が、次回のサービス取引の取引識別情報Ｔ（ｋ＋１）を暗号化した暗号化取引識別情報と、取引識別情報Ｔ（ｋ＋１）に基づいて計算されるＭ個の要素データV_s（ｋ）（s=1,2,…,M）のサービス提供装置の知らない係数による互いに独立なＭ個の一次結合である確認情報W_t（ｋ）（t=1,2,…,M）を生成し、サービス提供装置が、次回サービス取引のための暗号化識別情報に署名するとともに、当該サービス取引の利用料金に基づくデータＥ（ｋ）、乱数Ｒ（ｋ）、サービス利用装置から送信された取引識別情報Ｔ（ｋ）に基づいて計算されるＭ個の要素データV_s（ｋ）及び確認情報W_t（ｋ）を含むＰ（Ｐ≧２Ｍ＋２）個の値の、サービス利用装置が知らない係数データa_{ij}（i=1,2,…,P;j=1,2,…,P）及び乱数r_k（k=1,2,…）を用いた互いに独立な一次結合データS_j（ｋ）（j=1,2,…,P）を上記の式（Ｂ）により算出し、算出されたＰ個の一次結合データS_j（ｋ）をサービス利用装置において登録し、サービス提供装置からの集計依頼に応じて、登録されたＮ回分の一次結合データS_j（ｋ）を各ｊ毎にｋについて集計した結合集計データΣS_j（ｋ）を算出するとともに結合集計データΣS_j（ｋ）をサービス提供装置に送信し、サービス提供装置が、サービス利用装置から送信されたＰ個の結合集計データΣS_j（ｋ）及び係数データa_{ij}に基づいて取引識別情報Ｔ（１）～Ｔ（Ｎ）に関するデータＥ（ｋ）の集計値ΣＥ（ｋ）を算出しているので、個々の取引に関して関連付けられることなく利用者はサービス取引を依頼することができるとともに、サービス提供装置では特定の利用者による個々の取引の利用料金を知ることなくその合計額のみを確実に算出することができる。すなわち、Ｐ個の一次結合データS_j（ｋ）の算出に用いられる係数データa_{ij}、乱数r_k及び乱数Ｒ（ｋ）はサービス提供装置しか知らないデータとすることで、その算出方法がサービス利用装置に知られることなく一次結合データS_j（

ｋ）の算出結果のみがサービス利用装置に登録されるため、サービス利用装置側で登録された一次結合データS_j（ｋ）を勝手に操作することができない。そして、結合集計データΣS_j（ｋ）をサービス利用装置から得ることができれば、集計値ΣＥ（ｋ）、集計値Σ$r_k V_s$（ｋ）、集計値Σ$r_{k+1} W_t$（ｋ）及び集計値ΣＲ（ｋ）の（２Ｍ＋２）個のデータを変数として係数データa_{ij}を用いたＰ（Ｐ≧２Ｍ＋２）個の連立一次方程式を解くことで、集計値ΣＥ（ｋ）を正確に求めることができる。したがって、個々の取引の利用料金であるＥ（ｋ）を知らなくても集計値を正しく算出して利用者に合計額を請求することが可能となる。

【００２８】

また、サービス利用装置から送信された今回のサービス取引の取引識別情報Ｔ（ｋ）に基づくＭ個の要素データV_s（ｋ）及び次回のサービス取引の取引識別情報Ｔ（ｋ＋１）に基づいて暗号化処理されたＭ個の確認情報W_t（ｋ）を一次結合データS_j（ｋ）の算出式に含ませることで、一連のサービス取引の一次結合データS_j（ｋ）をサービス提供装置の知らない形で互いに関連付けさせることができ、サービス提供装置が個々のサービス取引を関連付けて蓄積することはできなくなる。また、サービス取引が互いに関連付けられることでサービス利用装置での不正操作を判定することも可能となる。すなわち、結合集計データΣS_j（ｋ）及び係数データa_{ij}に基づいて取引識別情報Ｔ（１）～Ｔ（Ｎ）に関する要素データと乱数の積$r_k V_s$（ｋ）の各ｓ毎の集計値Σ$r_k V_s$（ｋ）並びに取引識別情報Ｔ（１）～Ｔ（Ｎ＋１）に関する確認情報と乱数の積$r_{k+1} W_t$（ｋ）の各ｔ毎の集計値Σ$r_{k+1} W_t$（ｋ）を算出して、集計値Σ$r_{k+1} W_t$（ｋ）をサービス利用装置で復号化処理して集計値ΣX_u（ｋ）を得ることで、サービス提供装置は、個別の取引識別情報を知ることなく取引識別情報Ｔ（１）～Ｔ（Ｎ＋１）に関する確認情報と乱数の積の集計値を得ることができる。この値は、サービス利用装置から得られた次回の取引識別情報Ｔ（Ｎ＋１）に基づく要素データV_s（Ｎ＋１）を取引識別情報Ｔ（１）～Ｔ（Ｎ）に関する要素データと乱数の積の集計値Σ$r_k V_s$（ｋ）に加算した値と一致するので、両者が一致するか否か判定すれば、サービス利用装置側で不正操作があったか否か判定することが可能となる。

【００２９】

本発明に係るさらに別のサービス取引システム及びサービス取引方法は、サービス利用装置が、そのｋ回目のサービス取引において予めサービス提供装置から取得した署名処理済みの取引識別情報Ｔ（ｋ）を送信してサービス提供装置にサービス依頼し、サービス提供装置が、サービス利用装置から送信された取引識別情報が有効なものであるか否か判定するとともに、取引識別情報が有効と判定された場合にサービス利用装置からの依頼に応じてサービス処理し、サービス利用装置が、次回のサービス取引の取引識別情報Ｔ（ｋ＋１）とその取引回数に基づいて設定された回数データＱ（ｋ＋１）を合体して識別データＴ（ｋ＋１）Ｑ（ｋ＋１）を生成し暗号化して暗号化識別データとしてサービス提供装置に送信し、サービス提供装置が暗号化識別データに署名処理し、サービス利用装置が、署名処理された暗号化識別データを復号化処理して署名処理済みの識別データを取得するとともに、次回の取引識別情報Ｔ（ｋ＋１）に基づいて計算されるＭ個の要素データV_s（ｋ＋１）（s=1,2,…,Ｍ）のサービス提供装置の知らない係数による互いに独立なＭ個の一次結合である確認情報W_t（ｋ）（t=1,2,…,Ｍ）を生成し、サービス提供装置が、当該サービス取引の利用料金に基づくデータＥ（ｋ）、乱数Ｒ（ｋ）、サービス利用装置から送信された識別データＴ（ｋ）Ｑ（ｋ）から求められるＱ（ｋ）、サービス利用装置から送信された識別データＴ（ｋ）Ｑ（ｋ）から求められるＴ（ｋ）に基づいて計算されるＭ個の要素データV_s（ｋ）及びサービス利用装置から送信された確認情報W_t（ｋ）を含むＰ（Ｐ≧２Ｍ＋３）個の値の、サービス利用装置が知らない係数データa_{ij}（i=1,2,…,P;j=1,2,…,P）及び乱数r_k（k=1,2,…）を用いた互いに独立な一次結合データS_j（ｋ）（j=1,2,…,P）を上記の式（Ｄ）により算出し、算出されたＰ個の一次結合データS_j（ｋ）をサービス利用装置において登録し、サービス提供装置からの集計依頼に応じて、登録されたＮ回分の一次結合データS_j（ｋ）を各ｊ毎にｋについて集計した結合集計データΣ

S_j（ｋ）を算出するとともに結合集計データΣS_j（ｋ）及び回数データＱ（Ｎ）に相当する値をサービス提供装置に送信し、サービス提供装置が、サービス利用装置から送信されたＰ個の結合集計データΣS_j（ｋ）及び係数データa_{ij}に基づいて取引識別情報Ｔ（１）～Ｔ（Ｎ）に関するデータＥ（ｋ）の集計値ΣＥ（ｋ）を算出しているので、個々の取引に関して関連付けられることなく利用者はサービス取引を依頼することができるとともに、サービス提供装置では特定の利用者による個々の取引の利用料金を知ることなくその合計額のみを確実に算出することができる。すなわち、Ｐ個の一次結合データS_j（ｋ）の算出に用いられる係数データa_{ij}、乱数r_k及び乱数Ｒ（ｋ）はサービス提供装置しか知らないデータとすることで、その算出方法がサービス利用装置に知られることなく一次結合データS_j（ｋ）の算出結果のみがサービス利用装置に登録されるため、サービス利用装置側で登録された一次結合データS_j（ｋ）を勝手に操作することができない。そして、結合集計データΣS_j（ｋ）をサービス利用装置から得ることができれば、集計値ΣＥ（ｋ）、集計値ΣＱ（ｋ）、集計値Σ$r_k V_s$（ｋ）、集計値Σ$r_{k+1} W_t$（ｋ）及び集計値ΣＲ（ｋ）の（２Ｍ＋３）個のデータを変数として係数データa_{ij}を用いたＰ（Ｐ≧２Ｍ＋３）個の連立一次方程式を解くことで、集計値ΣＥ（ｋ）を正確に求めることができる。したがって、個々の取引の利用料金であるＥ（ｋ）を知らなくても集計値を正しく算出して利用者に合計額を請求することが可能となる。

【００３０】

そして、サービス利用装置から送信されたＰ個の結合集計データΣS_j及び係数データa_{ij}に基づいて取引識別情報Ｔ（１）～Ｔ（Ｎ）に関する回数データＱ（ｋ）の集計値ΣＱ（ｋ）を算出して集計値ΣＱ（ｋ）とサービス利用装置から送信された回数データＱ（Ｎ＋１）との間の整合性を判定すれば、サービス取引の取引回数に基づく回数データＱ（ｋ）は回数順に従って付与されているので、Ｑ（１）～Ｑ（Ｎ）までを加算した集計値ΣＱ（ｋ）からサービス取引した最後の回数順が特定されて、次回の回数順であるＱ（Ｎ＋１）との整合性を判定することができ、整合していない場合には不正な操作があったものとすることが可能となる。

【００３１】

回数データＱ（ｋ）に関する整合性があると判定された場合には、サービス利用装置から送信された今回のサービス取引の取引識別情報Ｔ（ｋ）に基づくＭ個の要素データV_s（ｋ）及び次回のサービス取引の取引識別情報Ｔ（ｋ＋１）に基づいて暗号化処理されたＭ個の確認情報W_t（ｋ）を用いてさらに不正操作の判定を行うことで、より確実に不正操作の判定を行うことができる。すなわち、要素データV_s（ｋ）及び確認情報W_t（ｋ）を一次結合データS_j（ｋ）の算出式に含ませることで、一連のサービス取引の一次結合データS_j（ｋ）をサービス提供装置の知らない形で互いに関連付けさせることができ、サービス提供装置が個々のサービス取引を関連付けて蓄積することはできなくなる。また、サービス取引が互いに関連付けられることでサービス利用装置での不正操作を判定することも可能となる。結合集計データΣS_j（ｋ）及び係数データa_{ij}に基づいて取引識別情報Ｔ（１）～Ｔ（Ｎ）に関する要素データと乱数の積$r_k V_s$（ｋ）の各ｓ毎の集計値Σ$r_k V_s$（ｋ）及び取引識別情報Ｔ（１）～Ｔ（Ｎ＋１）に関する確認情報と乱数の積$r_{k+1} W_t$（ｋ）の各ｔ毎の集計値Σ$r_{k+1} W_t$（ｋ）を算出して、集計値Σ$r_{k+1} W_t$（ｋ）をサービス利用装置で復号化処理して集計値ΣX_u（ｋ）を得ることで、サービス提供装置は、個別の取引識別情報を知ることなく取引識別情報Ｔ（１）～Ｔ（Ｎ＋１）に関する確認情報と乱数の積の集計値を得ることができる。この値は、サービス利用装置から得られた次回の取引識別情報Ｔ（Ｎ＋１）に基づく要素データV_s（Ｎ＋１）を取引識別情報Ｔ（１）～Ｔ（Ｎ）に関する要素データと乱数の積の集計値Σ$r_k V_s$（ｋ）に加算した値と一致するので、両者が一致するか否か判定すれば、サービス利用装置側で不正操作があったか否か判定することが可能となる。

【発明を実施するための最良の形態】

【００３２】

以下、本発明に係る実施形態について詳しく説明する。なお、以下に説明する実施形態

は、本発明を実施するにあたって好ましい具体例であるから、技術的に種々の限定がなされているが、本発明は、以下の説明において特に本発明を限定する旨明記されていない限り、これらの形態に限定されるものではない。

【００３３】

図１は、本発明に係るサービス取引システムに関する実施形態の構成を示す概略図である。サービス提供装置１は、インターネット等のネットワーク３を介してサービス利用装置２と接続されている。サービス利用装置２は、一般に多数の装置がネットワーク接続されているが、ここでは、理解を容易にするため、サービス利用装置２は、１台だけ記載している。

【００３４】

サービス提供装置１は、情報処理部１０及び記憶部１１を備えており、情報処理部１０が記憶部１１に記憶されたデータ及びプログラムを読み出してデータ処理を行い、サービス利用装置２とデータの送受信を行うようになっている。サービス利用装置２は、それぞれ情報処理部２０及び記憶部２１を備えており、情報処理部２０が記憶部２１に記憶されたデータ及びプログラムを読み出してデータ処理を行い、サービス提供装置１とデータの送受信を行うようになっている。サービス提供装置１及びサービス利用装置２における個別情報処理に関する機能は、予め記録媒体やネットワークを用いてインストールされるプログラムにより実現される。

【００３５】

図２は、サービス提供装置１とサービス利用装置２との間で互いに正当性を判定するための機能ブロック図を示している。サービス提供装置１の情報処理部１０は、パスワード抽出部１００、第一暗号キー生成部１０１、第一暗号化処理部１０２、第二暗号キー生成部１０３、第二暗号化処理部１０４、正当性判定部１０５及び送受信部１０６を備えており、こうした機能は、記憶部１１に記憶されたサービス提供プログラム１１０により実現される。記憶部１１に記憶された顧客ＤＢ１１１には、サービス利用装置を利用する全利用者のＩＤ、パスワード、氏名、住所といった顧客の属性情報が登録されている。

【００３６】

パスワード抽出部１００は、サービス利用装置から受信した複数のＩＤからなるＩＤリストに対応する複数のパスワードｐを記憶部１１の顧客ＤＢ１１１より抽出し、ＩＤリストの配列順序に対応したパスワードリストを作成する。

【００３７】

第一暗号キー生成部１０１は、第一暗号化処理部１０２で用いる第一暗号キーとしてパスワードｐと同じ長さのランダムビットパターンｒを生成する。第一暗号化処理部１０２は、第一暗号キーｒとパスワード抽出部１００で作成されたパスワードリストのパスワードｐとの排他的論理和ｘ

ｘ＝ｐＸＯＲｒ

をｐの暗号化情報として算出し、パスワードリストに対応した暗号パスワードリストを作成する。

【００３８】

第二暗号キー生成部１０３は、第二暗号キーＫを生成し、第二暗号化処理部１０４は、第二暗号キーＫにより第一暗号キーｒを暗号化した暗号化情報Ｋ（ｒ）を算出し、Ｋ（ｒ）及びＫをサービス提供装置の検証情報とする。暗号パスワードリスト及び暗号化情報Ｋ（ｒ）は、第二暗号キーＫとともに送受信部１０６を介してサービス利用装置２に送信される。第二暗号化処理部１０４では、暗号化キー及び復号化キーが異なる暗号方式を用いればよく、例えば、ＲＳＡ等の公知の暗号方式を用いて暗号化処理するようにすればよい。

【００３９】

正当性判定部１０５は、サービス利用装置２からその検証情報として受信したランダムビットパターンと第一暗号キー生成部１０１で生成した第一暗号キーであるランダムビットパターンｒとを照合してサービス利用装置２の正当性を判定する。送受信部１０６は、

サービス利用装置２とデータの送受信を行う。

【００４０】

サービス利用装置２の情報処理部２０は、ＩＤ発生部２００、パスワード処理部２０１、正当性判定部２０２及び送受信部２０３を備えており、こうした機能は、記憶部２１に記憶されたサービス利用プログラム２１０により実現される。記憶部２１は、サービス利用装置２を利用する利用者のＩＤ及びパスワードｐを記憶するＩＤ／パスワード登録部２１１を備えている。

【００４１】

ＩＤ発生部２００は、記憶部２１のＩＤ／パスワード登録部２１１に登録されたＩＤを含む複数のＩＤを発生させてＩＤリストを作成する。当該利用者のＩＤ以外のＩＤについては、全利用者のＩＤ数に基づいてランダムに発生させるようにする。

【００４２】

パスワード処理部２０１は、サービス提供装置から受信した暗号パスワードリストの中のＩＤ／パスワード登録部２１１に登録されたＩＤの位置に相当する暗号パスワードｘとＩＤ／パスワード登録部２１１に登録されたパスワードｑとの排他的論理和ｙ

ｙ＝ｘＸＯＲｑ

を計算して、さらに、ｙをサービス提供装置１から受信した第二暗号キーＫを用いて第二暗号化処理部１０４と同一の暗号方式で暗号化しＫ（ｙ）とする。

【００４３】

ここで、パスワード処理部２０１では、サービス提供装置１から受信した暗号パスワードｘは、

ｘ＝ｐＸＯＲｒ

であるので、ｑ＝ｐならば、

ｙ＝ｘＸＯＲｑ＝ｐＸＯＲｒＸＯＲｐ＝ｒ・・・（Ｅ）

となり、元の第一暗号キーｒが復号化される。例えば、

ｐ＝００１１００

ｒ＝０１１０００

である場合

ｘ＝０１０１００

となる。したがって、

ｘＸＯＲｐ＝０１１０００＝ｒ

となる。

【００４４】

正当性判定部２０２は、サービス提供装置１から受信した暗号化されたランダムビットパターンＫ（ｒ）及びパスワード処理部２０１で計算したＫ（ｙ）をパターン比較して一致するか否か判定する。一致すると判定された場合には、サービス提供装置１は正当なものとしてパスワード処理部２０１で計算したランダムビットパターンｙ（＝ｒ）を検証情報としてサービス提供装置１に送信し、一致しない場合には、サービス提供装置は不正なものとしてランダムビットパターンは送信しない。

【００４５】

図３は、サービス提供装置１及びサービス利用装置２との間で互いに正当性を判定する処理フローを示している。まず、サービス利用装置２は、認証処理を行う場合、全利用者のＩＤからランダムに（Ｎ－１）個のＩＤを発生させる（Ｓ１００）。複数のＩＤを発生させる場合、例えば、予め記憶部２１に全利用者のＩＤ総数が記憶されており、ＩＤ総数の連続番号の中からランダムに選択するようにすればよい。そして、サービス利用装置２に登録された利用者のＩＤを記憶部２１から読み出して、発生させた複数のＩＤとともにランダムに配列させてＮ個のＩＤからなるＩＤリストを作成する（Ｓ１０１）。図４は、ＩＤリストの一例を示す。この例では、ｔ番目に利用者のＩＤ$_k$が設定されている。

【００４６】

作成されたＩＤリストをサービス提供装置１に送信して、リスト中のＮ個のＩＤに対応

するパスワードを記憶部１１から抽出する（Ｓ１０２）。そして、抽出したパスワードをＩＤリストの配列に従って配列してパスワードリストを作成する（Ｓ１０３）。図５は、図４のＩＤリストに基づいて作成されたパスワードリストを示している。パスワードリストのｔ番目には、利用者のパスワードp_kがリストアップされている。

【００４７】

次に、第一暗号キーであるランダムビットパターンｒを発生させて（Ｓ１０４）、パスワードリストのパスワードとランダムビットパターンｒとの排他的論理和ｘを算出する（Ｓ１０５）。パスワードリストの各パスワードについて排他的論理和ｘを算出したら、パスワードリストの配列に従って配列して暗号パスワードリストを作成する（Ｓ１０６）。図６は、図５のパスワードリストに基づいて作成された暗号パスワードリストを示している。暗号パスワードリストのｔ番目の排他的論理和x_kが利用者のパスワードp_kに対応する。

【００４８】

ここで、利用者がp_k以外のパスワードを直接知るのを防ぐ目的で、パスワードリストの各パスワードをランダムビットパターンｒとの排他的論理和ｘを計算する前又は後で、暗号化しておいてもよい。ただし、この場合には、サービス利用装置２がp_kあるいはp_k及びｒの排他的論理和ｘを暗号化した情報が計算できるように、サービス利用装置２でもサービス提供装置１と同じ暗号キーと暗号化機構を備える必要がある。この場合の暗号化方式は、当然暗号キーと復号キーとが異なるものでなければならない。

【００４９】

次に、第二暗号キー生成部１０３において第二暗号キーＫを生成し（Ｓ１０７）、第二暗号キーＫを用いてランダムビットパターンｒを暗号化処理して（Ｓ１０８）、第二暗号キーＫ、暗号化されたランダムビットパターンＫ（ｒ）及び暗号パスワードリストをサービス利用装置２に送信する（Ｓ１０９）。

【００５０】

サービス利用装置２では、受信した暗号パスワードリストの中からｔ番目の排他的論理和x_kを抽出して（Ｓ１１０）、記憶部２１に登録された利用者のパスワードp_kとの排他的論理和を算出する（Ｓ１１１）。ステップＳ１１１での算出処理により、式（Ｅ）に示すように、ランダムビットパターンｙが算出されるので、算出されたランダムビットパターンを第二暗号キーＫを用いて暗号化処理する（Ｓ１１２）。暗号化されたランダムビットパターンＫ（ｙ）をサービス提供装置１から受信したランダムビットパターンＫ（ｒ）と比較して（Ｓ１１３）サービス提供装置１の正当性を判定する。一致する場合には、サービス提供装置１がサービス利用装置２から受信したＩＤリストのすべてのＩＤとランダムビットパターンｒとの排他的論理和を正しく計算したことになり、正当なサービス提供装置であると判定することができる。そこで、ステップＳ１１１で算出したランダムビットパターンｙをサービス提供装置１に送信する（Ｓ１１４）。ステップＳ１１３において両者が一致しない場合にはサービス提供装置は不正なものであると判定してランダムビットパターンｙを送信せず終了する。

【００５１】

サービス提供装置１は、受信したランダムビットパターンｙをステップＳ１０４で発生させたランダムビットパターンｒと比較して（Ｓ１１５）サービス利用装置２の正当性を判定する。一致する場合には、サービス提供装置１から送信した暗号パスワードリストに含まれるパスワードを用いてサービス利用装置２が処理したと判定できるため、サービス利用装置２に対してサービス提供を開始する。一致しない場合には、サービス利用装置２は、暗号パスワードリストに含まれるパスワードを用いて処理していないことから、不正なものとしてエラーメッセージを送信して（Ｓ１１６）終了する。

【００５２】

以上の処理では、サービス利用装置２からＩＤリストを送信しているので、サービス提供装置１ではどのＩＤの利用者がアクセスしてきているのか特定することはなく、利用者の正当性を判定できる。そして、サービス利用装置２では、サービス提供装置１から送信

されたランダムビットパターンＫ（ｒ）と自身が計算したＫ（ｙ）とが一致することを確認することにより、サービス提供装置１が正しく処理していることを確認することができる。この場合、サービス利用装置２に他の利用者のパスワードが送信されるが、パスワード若しくはパスワードとランダムビットパターンとの排他的論理和も暗号キーと復号キーとが異なる暗号方式によって暗号化することで、復号化には別のキーが必要となるので、サービス利用装置での不正な利用は簡単に防止できる。同様に、サービス提供装置１で用いたランダムビットパターンｒの暗号化も暗号キーと復号キーとが異なる暗号方式によって行われるので、暗号化されたランダムビットパターンＫ（ｒ）を直接復号化してサービス提供装置１に送信するといった不正な処理も防止される。すなわち、真正なパスワードがないとサービス利用装置２ではランダムビットパターンｒを復号化することができない。

【００５３】

そして、暗号パスワードリストでは共通のランダムビットパターンｒを用いてパスワードを処理しているので、暗号パスワードリストの何番目のパスワードが復号化されたかについてもサービス提供装置１では特定されない。また、サービス提供装置１では、サービス利用装置２から受信したランダムビットパターンｙにより正当性を判定するので、利用者を特定することなく認証を行うことができる。

【００５４】

以上のように、サービス提供装置１及びサービス利用装置２は、互いに匿名で認証することができる。

【００５５】

図７は、サービス提供装置１とサービス利用装置２との間でサービス取引を行う場合の概略ブロック図である。サービス提供装置１の情報処理部１０は、取引識別情報生成部１２０、取引識別情報判定部１２１、サービス処理部１２２、署名処理部１２３、結合計算部１２４、集計値算出部１２５、不正判定部１２６及び乱数発生部１２７を備えており、こうした機能は、記憶部１１に記憶されたサービス提供プログラム１１０により実現される。

【００５６】

記憶部１１には、生成された取引識別情報Ｔを管理するための取引識別情報テーブル１２８、結合計算処理や集計値算出処理に用いる（２Ｍ＋２）^{2}個の係数データa_{ij}（i=1,2,…,2M+2;j=1,2,…,2M+2）及び乱数発生部１２７で生成される十分長い乱数の列r_k（k=1,2,…）を記憶する係数データ記憶部１２９が記憶されている。係数データa_{ij}は、適当な数値を用いて適当に設定されるが、係数データa_{ij}で構成される行列の行列式が０とならないように設定する。乱数r_kは、乱数発生部により予め十分多くの乱数を発生させて記憶しておく。そして、後述するように、各サービス利用者のｋ回目のサービス取引に関する一次結合データS_jを算出する際には、共通の乱数r_k及びr_{k+1}を使用する。

【００５７】

取引識別情報生成部１２０は、個々のサービス取引を識別するために用いられる取引識別情報Ｔを生成し、生成された取引識別情報Ｔは、取引識別情報テーブル１２８に登録されて管理される。取引識別情報判定部１２１は、サービス利用装置２から送信された取引識別情報が署名済みであり、かつ、取引識別情報テーブル１２８に基づいて未使用のものであることをチェックして正当なサービス依頼か否か判定する。

【００５８】

サービス処理部１２２は、正当なサービス依頼に対して依頼内容に従ってサービス処理を行う。サービス取引が完了すると、サービスの利用料金を算出するとともに使用された取引識別情報について取引識別情報テーブル１２８に使用済みであることを登録する。署名処理部１２３は、サービス取引が完了した後次回に使用する取引識別情報が暗号化処理されてサービス利用装置２から送信されてくると、暗号化取引識別情報に署名処理してサービス利用装置２に送信する。

【００５９】

結合計算部１２４は、サービス利用装置２から送信された最初の取引に使用する取引識別情報Ｔ（１）に基づいて暗号化処理されたＭ個の初期確認情報W_t（０）（t=1,2,…,M）、乱数発生部１２７で発生させた乱数Ｒ（０）、係数データ記憶部１２９に記憶された係数データa_{ij}及び乱数r_1を用いた（２Ｍ＋２）個の一次結合データS_j（j=1,2,…,2M+2）を以下の式（Ａ）

$$S_j=\{a_{(M+1+1)j}W_1(0)+a_{(M+2+1)j}W_2(0)+\cdots+a_{(2M+1)}W_M(0)\}r_1+a_{(2M+2)j}R(0)\cdots(A)$$

により算出する。

【００６０】

また、結合計算部１２４は、サービス利用装置２のｋ回目のサービス取引完了後に、当該サービス取引の利用料金に基づくデータＥ（ｋ）（k=1,2,…,N）、サービス利用装置２から送信された今回のサービス取引の取引識別情報Ｔ（ｋ）（k=1,2,…,N）に基づくＭ個の要素データV_s（ｋ）（s=1,2,…,M）及び次回のサービス取引の取引識別情報Ｔ（ｋ＋１）（k=1,2,…,N）に基づいて暗号化処理されたＭ個の確認情報W_t（ｋ）（t=1,2,…,M）、乱数発生部１２７で発生させた乱数Ｒ（ｋ）（k=1,2,…,N）、係数データ記憶部１２９に記憶された係数データa_{ij}及び乱数r_kを用いた（２Ｍ＋２）個の一次結合データS_j（ｋ）（j=1,2,…,2M+2）を以下の式（Ｂ）

$$S_j(k)=a_{1j}E(k)+\{a_{(1+1)j}V_1(k)+a_{(2+1)j}V_2(k)+\cdots+a_{(M+1)}V_M(k)\}r_k+\{a_{(M+1+1)j}W_1(k)+a_{(M+2+1)j}W_2(k)+\cdots+a_{(2M+1)}W_M(k)\}r_{k+1}+a_{(2M+2)j}R(k)\cdots(B)$$

により算出する。

【００６１】

なお、算出する一次結合データS_j（ｋ）（j=1,2,…,2M+2）の個数は、（２Ｍ＋２）個以上であれば、後述する各集計値を算出することができることから、その個数Ｐを（Ｐ≧２Ｍ＋２）となるように設定すればよい。そして、それに合せて係数データa_{ij}についても、P^2個の係数データa_{ij}（i=1,2,…,P;j=1,2,…,P）に設定すればよい。

【００６２】

集計値算出部１２５は、サービス利用装置から送信された（２Ｍ＋２）個の結合集計データΣS_j及び係数データa_{ij}に基づいて、取引識別情報Ｔ（１）～Ｔ（Ｎ）に関するデータＥ（ｋ）の集計値ΣＥ（ｋ）を算出して、サービス利用装置２がこれまでにＮ回のサービス取引を実行したとすると、Ｎ回のサービス取引に関する利用料金の合計額を求める。さらに、サービス利用装置２から送信された（２Ｍ＋２）個の結合集計データΣS_j（ｋ）及び係数データa_{ij}に基づいて、取引識別情報Ｔ（１）～Ｔ（Ｎ）に関する要素データと乱数の積r_kV_s（ｋ）の各ｓ毎のｋについての集計値ΣV_s（ｋ）並びに取引識別情報Ｔ（１）～Ｔ（Ｎ＋１）に関する初期確認情報W_t（０）及び確認情報と乱数の積$r_{k+1}W_t$（ｋ）の各ｔ毎のｋについての集計値$\Sigma r_{k+1}W_t$を算出して集計値$\Sigma r_{k+1}W_t$をサービス利用装置２に送信する。

【００６３】

不正判定部１２６は、集計値Σr_kV_sにサービス利用装置２から送信された要素データと乱数の積$r_{k+1}V_s$（Ｎ＋１）を各ｓ毎に加算した集計値とサービス利用装置２から送信された集計値ΣX_u（ｋ）が一致しているか否か判定する。

【００６４】

サービス利用装置２の情報処理部２０は、取引識別情報取得部２２０、サービス処理部２２１、暗号化処理部２２２、復号化処理部２２３、確認情報処理部２２４、結合データ集計部２２５及び要素集計値処理部２２６を備えており、こうした機能は、記憶部２１に記憶されたサービス利用プログラム２１０により実現される。記憶部２１には、サービス提供装置１から取得した取引識別情報Ｔに含まれる取引識別情報のリスト２２７、サービス提供装置１で署名処理された取引識別情報が登録された登録部２２８、サービス提供装置１から送信された（２Ｍ＋２）個の一次結合データS_jを記憶する登録部２２９、次回のサービス取引の取引識別情報Ｔ（ｋ＋１）の暗号化処理して確認情報を計算するのに用

いるM^{2}個の係数データb_{st}（s=1,2,…,M;t=1,2,…,M）を記憶する係数データ記憶部２３０を記憶している。

【００６５】

取引識別情報取得部２２０は、サービス取引を開始する前にサービス提供装置１から必要数の取引識別情報を取引識別情報Ｔから選択して取得する。サービス処理部２２１は、登録部２２８に登録された署名処理済みの取引識別情報をサービス提供装置１に送信してサービス依頼を行う。

【００６６】

暗号化処理部２２２は、最初のサービス取引の取引識別情報Ｔ（１）又はサービス取引完了後に次回のサービス取引の取引識別情報Ｔ（ｋ＋１）（k=1,2,…,N）を暗号化処理し暗号化取引識別情報を生成する。また、復号化処理部２２３は、サービス提供装置から送信された署名処理済みの暗号化取引識別情報を復号化処理して署名処理済みの取引識別情報を登録部２２８に記憶する。

【００６７】

取引識別情報Ｔの暗号化処理は、次回のサービス取引で使用する取引識別情報がサービス提供装置に知られてしまうと今回のサービス取引で使用した取引識別情報との関連付けがサービス提供装置側で可能となるためである。また、サービス提供装置にとっては、今回のサービス取引が完了した後に次回のサービス取引の取引識別情報を署名処理するので、正当にサービスを登録したサービス利用者のみに署名処理した取引識別情報を提供することができ、サービス利用額の総計の確実な計算が可能となる。

【００６８】

暗号化処理部２２２における取引識別情報Xの暗号化処理としては、例えば、乱数ｒ及びサービス提供装置１側の公開鍵ｐを用いて以下のように処理する。

$X \rightarrow r^p X$

処理された暗号化取引識別情報を署名処理部１２３においてサービス提供装置１の秘密鍵ｑを用いて以下のように署名処理する。

$r^p X \rightarrow (r^p X)^q$

この場合、取引識別情報Xには乱数ｒが掛けられているため、サービス提供装置１では取引識別情報Xを知ることはできず、ブラインド署名処理が行われることになる。署名処理された暗号化取引識別情報を復号化処理部２２３では、暗号化処理部２２２の暗号化処理で使用した乱数ｒを用いて以下のように処理する。

$(r^p X)^q \rightarrow (r^{pq} X^q) / r$

ここで、ｐｑ＝１であるから、

$(r^{pq} X^q) / r \rightarrow (r X^q) / r \rightarrow X^q$

となり、サービス提供装置１の秘密鍵ｑで署名処理された取引識別情報Xを得ることができる。サービス利用装置が送信した取引識別情報が署名処理されたか否か確認したい場合には、署名処理された取引識別情報にサービス提供装置１の公開鍵ｐを掛けることで

$X^q \rightarrow X^{qp} \rightarrow X$

となって確認することができる。

【００６９】

確認情報処理部２２４は、最初のサービス取引の取引識別情報Ｔ（１）に基づいて計算されるM個の要素データV_s（１）（s=1,2,…,M）のサービス提供装置１の知らない係数による互いに独立なＭ個の一次結合である初期確認情報W_t（０）（t=1,2,…,M）を生成するとともに、サービス取引完了後に今回のサービス取引の回数をｋとして、次回サービス取引の取引識別情報Ｔ（ｋ＋１）（k=1,2,…,N）に基づいて計算されるＭ個の要素データV_s（ｋ＋１）（s=1,2,…,M）のサービス提供装置１の知らない係数による互いに独立なＭ個の一次結合である確認情報W_t（ｋ）（t=1,2,…,M）を生成する。

【００７０】

Ｍ個の要素データV_s（ｋ）は、例えば、図８に示すように、取引識別情報Ｔ（ｋ）を構成するビット列をＭ個に等分した各ビット列とする。次回の取引識別情報Ｔ（ｋ＋１）

に基づいて暗号化処理されたＭ個の確認情報W_t（ｋ）は、図９に示すように、まず、Ｍ個の要素データV_s（ｋ＋１）を生成し、係数データ記憶部２３０に記憶されたM^2個の係数データb_{st}を用いて以下の式（Ｆ）

$W_t(k)=b_{1t}V_1(k+1)+b_{2t}V_2(k+1)+\cdots+b_{Mt}V_M(k+1)$・・・（Ｆ）

により算出される。

【００７１】

M^2個の係数データb_{st}は、サービス利用装置２のみが登録しているので、サービス提供装置１側で確認情報W_t（ｋ）から次回の取引識別情報Ｔ（ｋ＋１）を知ることはできない。したがって、サービス提供装置１において、今回のサービス取引に関連付けて次回のサービス取引を蓄積していくことが防止される。また、サービス提供装置１は、今回の取引識別情報と次回のサービス取引の取引識別情報に関する確認情報に基づいて一次結合データS_j（ｋ）を算出することで、サービス取引の連続性を確保し、サービス利用装置によるサービス取引記録の削除やすり替えなどの改変を集計処理後に確実に検出できるようになる。

【００７２】

結合集計部２２５は、サービス提供装置１からの集計依頼に応じて登録された一次結合データS_j（ｋ）を各ｊ毎にｋについて集計した結合集計データΣS_j（ｋ）を算出するとともに、サービス利用装置２がこれまで受けたサービス取引の回数をＮとすると、次回の取引識別情報Ｔ（Ｎ＋１）に基づいて要素データV_s（Ｎ＋１）を生成して結合集計データΣS_j（ｋ）及び要素データV_s（Ｎ＋１）を送信する。

【００７３】

例えば、サービス提供装置１との間でＮ回のサービス取引が行われたとすると、サービス提供装置１からはサービス利用装置２に、サービス取引前の最初に使用する取引識別情報Ｔ（１）に関するものをS_j（０）とすると、図１０に示すように、S_j（０）からS_j（Ｎ）までの（Ｎ＋１）回分の一次結合データが送信される。そして、サービス提供装置１からの集計依頼があった場合、一次結合データS_j（ｋ）を各ｊ毎にｋについて集計した結合集計データΣS_j（ｋ）は、図１０の最下段の式で表される。この式は、集計値ΣE（ｋ）、集計値$\Sigma r_k V_s$（ｋ）、集計値$\Sigma r_{k+1} W_t$（ｋ）及び集計値ΣR（ｋ）の（２Ｍ＋２）個のデータを変数として係数データa_{ij}を用いた（２Ｍ＋２）個の連立一次方程式となっている。

【００７４】

そのため、サービス提供装置１の集計値算出部１２５では、結合集計データΣS_j（ｋ）を得ることができれば、係数データa_{ij}に基づいて（２Ｍ＋２）個の連立一次方程式を解くことができ、集計値ΣE（ｋ）、集計値$\Sigma r_k V_s$（ｋ）、集計値$\Sigma r_{k+1} W_t$（ｋ）及び集計値ΣR（ｋ）を得ることができる。したがって、サービス提供装置１の集計値算出部１２５では、サービス利用装置２の個々のサービス取引に関する利用料金Ｅ（ｋ）を知らなくてもその集計値ΣE（ｋ）を算出することが可能となる。

【００７５】

また、結合集計データΣS_j（ｋ）の算出式には、サービス利用装置２側が知らない係数データa_{ij}の他に乱数r_k及びＲ（ｋ）が用いられているので、サービス利用装置２において一次結合データS_j（ｋ）の算出式を知ることはできず、不正操作を行うことはできない。

【００７６】

ここで集計値$\Sigma r_{k+1} W_t$（ｋ）は取引識別情報Ｔ（１）～Ｔ（Ｎ）に次回の取引識別情報Ｔ（Ｎ＋１）を加えたものに対応する値であるので、サービス提供装置１の集計値算出部１２５では、得られた集計値$\Sigma r_k V_s$（ｋ）にサービス提供装置１から送信された次回の取引識別情報Ｔ（Ｎ＋１）に対応する要素データV_s（Ｎ＋１）と乱数の積$r_{N+1} V_s$（Ｎ＋１）を各ｓ毎に加えた集計値$\Sigma r_k V_s$（ｋ）を算出する。

【００７７】

さらに、集計値算出部１２５は、集計値$\Sigma r_{k+1}W_t$（ｋ）をサービス利用装置２に送信し、要素集計処理部２２６が、集計値$\Sigma r_{k+1}W_t$（ｋ）を復号化処理して集計値ΣX_u（ｋ）（u=1,2,…,M）を生成する。確認情報W_t（ｋ）が、上述したようにM^2個の係数データb_{st}を用いて式（Ｆ）で算出されていることから、集計値$\Sigma r_{k+1}W_t$（ｋ）が要素データV_s（ｋ）の各ｓ毎のｋについての集計値$\Sigma r_k V_s$（ｋ）を変数として係数データb_{st}を用いたＭ個の連立一次方程式とみることができる。そのため、要素集計処理部２２６では、集計値$\Sigma r_{k+1}W_t$（ｋ）をサービス提供装置１から得ることができれば、係数データb_{st}を用いたＭ個の連立一次方程式を解いて、集計値ΣX_u（ｋ）を得ることができる。

【００７８】

要素集計処理部２２６が算出処理した集計値ΣX_u（ｋ）は、取引識別情報Ｔ（１）～Ｔ（Ｎ＋１）に関する集計値であるため、不正な処理が行われていなければ、集計値$\Sigma r_k V_s$（ｋ）と一致する。そのため、不正判定部１２６で算出した集計値と一致するか否か判定することで、不正操作が行われたか否かチェックすることが可能となる。すなわち、サービス利用装置２側で結合集計データΣS_j（ｋ）を削除したり差し替えたりするなどの不正操作すると、今回及のサービス取引の取引識別情報Ｔ（ｋ）と次回取引の取引識別情報Ｔ（ｋ＋１）から計算した確認情報の整合性がとれなくなり、サービス提供装置１の不正判定部１２６で算出した今回の取引識別情報Ｔ（ｋ）に関する要素データの集計値$\Sigma r_k V_s$（ｋ）とサービス利用装置２の要素集計処理部２２６で算出した次回の取引識別情報Ｔ（ｋ＋１）に関する要素データの集計値ΣX_u（ｋ）が一致しなくなって不正判定部１２６においてチェックされるようになる。

【００７９】

要素集計処理部２２６では、集計値ΣV_s（ｋ）のみをサービス提供装置１に返すようになっているため、個々のサービス取引の取引識別情報Ｔ（ｋ）に関する要素データV_s（ｋ）を知られることがない。

【００８０】

図１１は、サービス取引の実施前に行われる取引識別情報の発行処理に関するフローである。サービス提供装置１では、予め必要数の取引識別情報が生成されて取引識別情報テーブル１２８が記憶されている（Ｓ２００）。まず、図３に示すように、サービス提供装置１とサービス利用装置２との間で互いに正当性の判定が行われて（Ｓ２０１、Ｓ２０２）匿名での認証が行われる。互いに正当性があると判定された場合に、サービス利用装置２は、サービス提供装置１に対して必要な数の取引識別情報の発行依頼を行う（Ｓ２０３）。サービス提供装置１は、未使用の取引識別情報をリストアップして、必要数をサービス利用装置２に発行する（Ｓ２０４）。この場合、リストアップされたものからサービス利用装置２側で選択するようにしてもよい。発行された取引識別情報は、サービス利用装置２の登録部２２８に記憶される（Ｓ２０５）。

【００８１】

次に、最初のサービス取引に用いる取引識別情報Ｔ（１）を選択して暗号化処理を暗号化処理部２２２で行い（Ｓ２０６）、暗号化取引識別情報Ｔ（１）を生成する。そして、選択された取引識別情報Ｔ（１）に基づいて確認情報処理部２２４で確認情報W_t（０）を生成する（Ｓ２０７）。生成された暗号化取引識別情報Ｔ（１）及び初期確認情報W_t（０）を添付してサービス提供装置１に対して署名処理を依頼する（Ｓ２０８）。サービス提供装置１では、署名処理部１２３で暗号化取引識別情報Ｔ（１）に署名処理を行い（Ｓ２０９）、結合計算部１２４で一次結合データS_j（０）を上記の式（Ａ）により算出処理する（Ｓ２１０）。署名処理された暗号化取引識別情報Ｔ（１）及び算出された一次結合データS_j（０）をサービス利用装置２に送信し（Ｓ２１１）、署名処理された暗号化取引識別情報Ｔ（１）は、サービス利用装置２の復号化処理部２２３で処理されて署名入りの取引識別情報Ｔ（１）となり（Ｓ２１２）、登録部２２８に登録され、一次結合データS_jは登録部２２９に登録される（Ｓ２１２）。

【００８２】

以上の処理により、サービス利用装置２は、サービス取引に必要な取引識別情報を取得

するとともに最初に使用する署名入りの取引識別情報を得ることができる。

【００８３】

図１２は、サービス利用装置２によるｋ回目のサービス取引を行う場合の処理に関するフローである。まず、サービス提供装置１とサービス利用装置２との間で互いに正当性の判定が行われて（Ｓ３００、Ｓ３０１）匿名での認証が行われる。互いに正当性があると判定された場合に、サービス利用措置２は、署名入りの取引識別情報Ｔ（ｋ）を読み出して（Ｓ３０２）署名入りの取引識別情報Ｔ（ｋ）を添付しサービス提供装置１に対してサービス依頼を行う（Ｓ３０３）。

【００８４】

サービス提供装置１は、サービス依頼を受けると、署名入りの取引識別情報Ｔ（ｋ）を取得して（Ｓ３０４）正常に署名されているか否か、未使用のものであるか否かチェックし取引識別情報Ｔ（ｋ）の判定を行う（Ｓ３０５）。取引識別情報Ｔ（ｋ）が正常なものであると判定された場合には、サービス処理を開始してサービス利用装置２との間でサービス取引を行う（Ｓ３０６）。そして、サービス取引完了後その利用料金Ｅ（ｋ）を算出する（Ｓ３０７）。

【００８５】

ステップＳ３０５において、取引識別情報Ｔ（ｋ）が正常なものでないと判定された場合にはエラー処理を行い（Ｓ３０８）サービス処理は行われない。

【００８６】

一方、サービス利用装置２は、サービス提供装置１とのサービス取引が開始されると、必要なサービス処理を行い（Ｓ３０９）、サービス取引完了後に次回のサービス取引で使用する取引識別情報Ｔ（ｋ＋１）を選択して暗号化処理部２２２で暗号化され（Ｓ３１０）、暗号化取引識別情報Ｔ（ｋ＋１）を生成する。そして、選択された取引識別情報Ｔ（ｋ＋１）に基づいて確認情報処理部２２４で確認情報W_t（ｋ）を生成する（Ｓ３１１）。生成された暗号化取引識別情報Ｔ（ｋ＋１）を添付してサービス提供装置１に対して署名処理を依頼する（Ｓ３１２）。

【００８７】

サービス提供装置１では、署名処理部１２３で暗号化取引識別情報Ｔ（ｋ＋１）に署名処理を行い（Ｓ３１３）、結合計算部１２４で一次結合データS_j（ｋ）を上記の式（Ｂ）により算出処理する（Ｓ３１４）。署名処理された暗号化取引識別情報Ｔ（ｋ＋１）及び算出された一次結合データS_j（ｋ）をサービス利用装置２に送信し（Ｓ３１５）、署名処理された暗号化取引識別情報Ｔ（ｋ＋１）は、サービス利用装置２の復号化処理部２２３で処理されて署名入りの取引識別情報Ｔ（ｋ＋１）となり（Ｓ３１６）、登録部２２８に登録され、一次結合データS_j（ｋ）は、登録部２２９に登録される（Ｓ３１７）。

【００８８】

以上の処理では、互いの正当性を判定して匿名認証した後においても取引識別情報を用いて署名入りの場合にサービス提供装置１でサービス取引するようにいるので、個々のサービス取引が匿名で行うことができるだけでなく、サービス利用装置の連続する取引が正しく行われることを保証する。また、次回の取引識別情報については暗号化処理された暗号化取引識別情報及び確認情報W_t（ｋ）で処理されるので、今回の取引識別情報との関連付けがなされなず取引識別情報から一連のサービス取引を特定することができない。

【００８９】

サービス提供装置１では、署名入りの取引識別情報により正当なサービス取引権限のある利用者を確実に判定することができる。

【００９０】

図１３は、サービス利用装置２に関する利用料金等の集計処理に関するフローである。集計処理は、サービス提供装置１において所定期間毎に行われる。まず、サービス提供装置１とサービス利用装置２との間で互いに正当性の判定が行われて（Ｓ４００、Ｓ４０１）匿名での認証が行われる。互いに正当性があると判定された場合に、サービス提供装置１は、サービス利用装置２に対して集計依頼を行う（Ｓ４０２）。

【００９１】
サービス利用装置２は、それまでにＮ回のサービス取引をしているとして、集計依頼に基づいて登録部２２９に蓄積された一次結合データS_j（ｋ）についてデータ別に集計して結合集計データΣS_j（ｋ）を算出する（Ｓ４０３）。そして、選択された次回の取引識別情報Ｔ（Ｎ＋１）を読み出して（Ｓ４０４）その要素データV_s（Ｎ＋１）を生成し（Ｓ４０５）、結合集計データΣS_j及び要素データV_s（Ｎ＋１）をサービス提供装置１に送信する（Ｓ４０６）。

【００９２】
サービス提供装置１は、結合集計データΣS_j（ｋ）、係数データa_{ij}及びr_kに基づいて、集計値ΣＥ（ｋ）、集計値Σ$r_k V_s$（ｋ）及び集計値Σ$r_{k+1} W_t$（ｋ）を算出する（Ｓ４０７）。そして、集計値Σ$r_k V_s$（ｋ）に、要素データと乱数の積$r_{N+1} V_s$（Ｎ＋１）を各ｓ毎に加算処理した集計値を求め（Ｓ４０８）、集計値Σ$r_{k+1} W_t$（ｋ）は、サービス利用装置２に送信する（Ｓ４０９）。

【００９３】
サービス利用装置２は、集計値Σ$r_{k+1} W_t$（ｋ）に基づいて集計値ΣX_u（ｋ）を算出処理し（Ｓ４１０）、算出された集計値ΣX_u（ｋ）をサービス提供装置１に送信する（Ｓ４１１）。

【００９４】
サービス提供装置１は、送信された集計値ΣX_u（ｋ）とステップＳ４０８で算出した集計値$r_k V_s$（ｋ）（$r_{N+1} V_s$（Ｎ＋１）を加算した値）が一致するか判定し（Ｓ４１２）、一致する場合には正しく集計されたものとして集計値ΣＥ（ｋ）に基づいてサービス利用装置２に利用料金の請求を行う（Ｓ４１３）。サービス利用装置２は、利用料金の請求に基づいて支払い処理を行う（Ｓ４１４）。

【００９５】
ステップＳ４１２において一致しない場合には、不正操作があったものとして、サービス提供装置１は、不正処理を行う（Ｓ４１５）。不正処理では、例えば、サービス利用装置２に対して係数データb_{st}の開示を求めて、確認情報W_t（ｋ）から要素データV_s（ｋ）を算出し、サービス利用装置２に関するサービス取引で使用した取引識別情報を特定する。そして、特定された取引識別情報に基づいてサービス利用装置２に登録された一次結合データから利用金額を集計してサービス利用装置２に対して請求するようにする。

【００９６】
以上の処理により、サービス利用装置２は、個々のサービス取引に関して知らせることなく所定期間の集計値のみをサービス提供装置１に提供すればよく、サービス提供装置１においても集計値のみを得ることで、正確に利用料金の合計金額を算出することができ、さらに不正操作があったことについても確実に判定することが可能となる。

【００９７】
以上説明した実施形態では、サービス利用装置２の確認情報処理部２２４において今回のサービス取引の取引識別情報Ｔ（ｋ）に基づくＭ個の要素データV_s（ｋ）及び次回のサービス取引の取引識別情報Ｔ（ｋ＋１）に基づいて暗号化処理されたＭ個の要素データW_t（ｋ）を生成してサービス提供装置１に送信するようにしているが、次回のサービス取引の取引識別情報Ｔ（ｋ＋１）の代わりに前回のサービス取引の取引識別情報Ｔ（ｋ－１）を用いることもできる。

【００９８】
図１４は、前回の取引識別情報Ｔ（ｋ－１）を確認情報に用いた場合の一次結合データS_jのリストである。この場合には、サービス利用装置２は、サービス取引開始前にダミーの取引識別情報Ｔ（０）を用いてその要素データV_s（０）を生成し暗号処理せずにサービス提供装置１に送信する。サービス提供装置１は、一次結合データS_j（０）を以下の式（Ｇ）

$$S_j(0) = \{a_{(1+1)j} V_1(0) + a_{(2+1)j} V_2(0) + \cdots + a_{(M+1)} V_M(0)\} r_1 + a_{(2M+2)j} R(0) \quad \cdots (G)$$

により算出する。そして、サービス利用装置２のｋ回目のサービス取引完了後には、今回のサービス取引の取引識別情報Ｔ（ｋ）に基づくＭ個の要素データV_s（ｋ）及び前回の取引識別情報Ｔ（ｋ－１）に基づいて暗号化処理されたＭ個の確認情報W_t（ｋ－１）を生成してサービス提供装置１に送信する。サービス提供装置１は、一次結合データS_j（ｋ）を以下の式（Ｈ）

$$S_j(k)=a_{1j}E(k)+\{a_{(1+1)j}V_1(k)+a_{(2+1)j}V_2(k)+\cdots+a_{(M+1)}V_M(k)\}r_{k+1}+\{a_{(M+1+1)j}W_1(k-1)+a_{(M+2+1)j}W_2(k-1)+\cdots+a_{(2M+1)}W_M(k-1)\}r_k+a_{(2M+2)j}R(k)\cdots(H)$$

により算出する。以上のように算出された一次結合データS_j（ｋ）をサービス利用装置２に送信して登録すれば、上記の実施形態と同様に利用料金の集計及び不正判定を行うことができる。

【００９９】

図１５から図１７は、前回の取引識別情報Ｔ（ｋ－１）を確認情報に用いた場合の処理フローである。図１１から図１３で説明した処理フローと異なる部分について説明を行い、同じ部分については説明を省略する。

【０１００】

サービス取引の実施前に行われる取引識別情報の発行処理に関するフローでは、図１５に示すように、取引識別情報の発行処理後ダミーの取引識別情報Ｔ（０）を生成し（Ｓ５０６）その要素データV_s（０）を生成して（Ｓ５０７）サービス提供装置１に送信し、サービス提供装置１では上記の式（Ｇ）を用いて一次結合データS_j（０）を算出する（Ｓ５０８）。算出された一次結合データS_j（０）は、サービス利用装置２に送信されて（Ｓ５０９）登録部２２９に登録される（Ｓ５１０）。

【０１０１】

サービス取引を行う場合の処理に関するフローでは、図１６に示すように、サービス取引完了後、前回の取引識別情報Ｔ（ｋ－１）を暗号化して確認情報W_t（ｋ－１）を生成する（Ｓ６１０）。生成された確認情報W_t（ｋ－１）をサービス提供装置１に送信して上記の式（Ｈ）を用いて一次結合データS_j（ｋ）を算出する（Ｓ６１５）。算出された一次結合データS_j（ｋ）は、署名入り情報とともにサービス利用装置２に送信されて（Ｓ６１６）登録部２２９に登録される（Ｓ６１８）。

【０１０２】

利用料金等の集計処理に関するフローでは、図１７に示すように、結合集計データΣS_j（ｋ）の算出処理後最後のサービス取引で使用した取引識別情報Ｔ（Ｎ）を読み出して（Ｓ７０４）その要素データV_s（Ｎ）を生成し（Ｓ７０５）結合集計データΣS_j（ｋ）及びV_s（Ｎ）をサービス提供装置１に送信する（Ｓ７０６）。サービス提供装置１では、結合集計データΣS_j（ｋ）を用いて、集計値ΣＥ（ｋ）、集計値Σr_kV_s（ｋ）及び集計値Σr_kW_t（ｋ－１）を算出して（Ｓ７０７）、集計値Σr_kV_s（ｋ）からr_NV_s（Ｎ）を減算処理し（Ｓ７０８）、集計値Σr_kW_t（ｋ－１）をサービス利用装置２に送信する（Ｓ７０９）。サービス利用装置２では、集計値Σr_kW_t（ｋ－１）から集計値ΣX_u（ｋ－１）を算出して（Ｓ７１０）サービス提供装置１に送信し（Ｓ７１１）、サービス提供装置１では、ステップＳ７０８で算出した集計値と集計値ΣX_u（ｋ－１）とが一致しているか判定して（Ｓ７１２）不正判定を行う。

【０１０３】

以上のような処理により、前回の取引識別情報を用いた確認情報でも上述した実施形態と同様に利用料金の集計及び不正判定を行うことができる。

【０１０４】

図１８は、上述した実施形態とは別の実施形態に関する概略ブロック図である。この例では、不正判定を行うために、上述の実施形態で用いた確認情報以外に取引回数を用いるようにしている。なお、上述の実施形態と同様の構成については、説明が重複するため省略する。

【０１０５】

サービス提供装置１の情報処理部１０は、取引識別情報生成部１２０、取引識別情報判定部１２１、サービス処理部１２２、署名処理部１２３、結合計算部１２４、集計値算出部１２５、不正判定部１２６及び乱数発生部１２７を備えており、こうした機能は、記憶部１１に記憶されたサービス提供プログラム１１０により実現される。

【０１０６】

記憶部１１には、生成された取引識別情報Ｔを管理するための取引識別情報テーブル１２８、結合計算処理や集計値算出処理に用いる（２Ｍ＋３）^{2}個の係数データa_{ij}（i=1,2,…,2M+3;j=1,2,…,2M+3）及び十分多い乱数の列r_k（k=1,2,…）を記憶する係数データ記憶部１２９が記憶されている。係数データa_{ij}は、適当な数値を用いて適当に設定されるが、係数データa_{ij}で構成される行列の行列式が０とならないように設定する。乱数r_kは、乱数発生部１２７により予め発生させて記憶しておく。そして、後述するように、各サービス利用者のｋ回目のサービス取引に関する一次結合データS_j（ｋ）を算出する際には、共通の乱数r_k及びr_{k+1}を使用する。

【０１０７】

取引識別情報生成部１２０及びサービス処理部１２２は、上述の実施形態と同様の機能を備えている。

【０１０８】

結合計算部１２４は、サービス利用装置２から送信された最初の取引に使用する取引識別情報Ｔ（１）に基づいて暗号化処理されたＭ個の初期確認情報W_t（０）（t=1,2,…,M）、乱数発生部１２７で発生させた乱数Ｒ（０）、係数データ記憶部１２９に記憶された係数データa_{ij}及び乱数r_1を用いて（２Ｍ＋３）個の一次結合データS_j（０）（j=1,2,…,2M+3）を以下の式（Ｉ）

$$S_j(0)=\{a_{(M+1+2)j}W_1(0)+a_{(M+2+2)j}W_2(0)+\cdots+a_{(2M+2)}W_M(0)\}r_1+a_{(2M+3)j}R(0)\cdots(I)$$

により算出する。

【０１０９】

また、結合計算部１２４は、サービス利用装置２によるｋ回目のサービス取引完了後に、当該サービス取引の利用料金に基づくデータＥ（ｋ）（k=1,2,…,N）、サービス利用装置２から送信された今回のサービス取引の回数に基づく回数データＱ（ｋ）（k=1,2,…,N）、今回のサービス取引の取引識別情報Ｔ（ｋ）（k=1,2,…,N）に基づくＭ個の要素データV_s（ｋ）（s=1,2,…,M）、次回のサービス取引の取引識別情報Ｔ（ｋ＋１）（k=1,2,…,N）に基づいて暗号化処理されたＭ個の確認情報W_t（ｋ）（t=1,2,…,M）、乱数発生部１２７で発生させた乱数Ｒ（ｋ）（k=1,2,…,N）並びに係数データ記憶部１２９に記憶された係数データa_{ij}及び乱数r_kを用いた（２Ｍ＋３）個の一次結合データS_j（ｋ）（j=1,2,…,2M+3）を以下の式（Ｊ）

$$S_j(k)=a_{1j}E(k)+a_{2j}Q(k)+\{a_{(1+2)j}V_1(k)+a_{(2+2)j}V_2(k)+\cdots+a_{(M+2)}V_M(k)\}r_k+\{a_{(M+1+2)j}W_1(k)+a_{(M+2+2)j}W_2(k)+\cdots+a_{(2M+2)}W_M(k)\}r_{k+1}+a_{(2M+3)j}R(k)\cdots(J)$$

により算出する。

【０１１０】

なお、算出する一次結合データS_j（ｋ）（j=1,2,…,2M+2）の個数は、（２Ｍ＋３）個以上であれば、後述する各集計値を算出することができることから、その個数Ｐを（Ｐ≧２Ｍ＋３）となるように設定すればよい。そして、それに合せて係数データa_{ij}についても、Ｐ^{2}個の係数データa_{ij}（i=1,2,…,P;j=1,2,…,P）に設定すればよい。

【０１１１】

集計値算出部１２５は、サービス利用装置２がそれまでに実行した取引の数をＮとすると、サービス利用装置から送信された（２Ｍ＋３）個の結合集計データΣS_j（ｋ）及び係数データa_{ij}に基づいて、取引識別情報Ｔ（１）～Ｔ（Ｎ）に関するデータＥ（ｋ）の集計値ΣＥ（ｋ）を算出してＮ回のサービス取引に関する利用料金の合計額を求める。また、サービス利用装置２から送信された（２Ｍ＋３）個の結合集計データΣS_j（ｋ）及

び係数データa_{ij}に基づいて取引識別情報Ｔ（１）～Ｔ（Ｎ）に関する回数データＱ（ｋ）の集計値ΣＱ（ｋ）を算出する。さらに、サービス利用装置２から送信された（２Ｍ＋３）個の結合集計データΣS_j（ｋ）及び係数データa_{ij}に基づいて取引識別情報Ｔ（１）～Ｔ（Ｎ）に関する要素データと乱数の積r_kV_s（ｋ）の各ｓ毎のｋについての集計値Σr_kV_s並びに取引識別情報Ｔ（１）～Ｔ（Ｎ＋１）に関する初期確認情報と乱数の積r_1W_t（０）及び確認情報と乱数の積$r_{k+1}W_t$（ｋ）の各ｔ毎のｋについての集計値Σ$r_{k+1}W_t$（ｋ）を算出して集計値Σ$r_{k+1}W_t$（ｋ）をサービス利用装置２に送信する。

【０１１２】

不正判定部１２６は、第一の不正判定として、集計値算出部１２５で算出された集計値ΣＱ（ｋ）とサービス利用装置２から送信された回数データＱ（Ｎ＋１）との間の整合性を判定して不正操作があるか否か判定し、回数データＱ（ｋ）に関して整合性がある場合には、第二の不正判定として、集計値Σr_kV_s（ｋ）にサービス利用装置２から送信された要素データと乱数の積$r_{N+1}V_s$（Ｎ＋１）を各ｓ毎に加算した集計値とサービス利用装置２から送信された集計値ΣX_u（ｋ）が一致しているか否か判定する。

【０１１３】

サービス利用装置２の情報処理部２０は、取引識別情報取得部２２０、サービス処理部２２１、暗号化処理部２２２、復号化処理部２２３、識別データ生成部２３１、確認情報処理部２２４、結合データ集計部２２５及び要素集計値処理部２２６を備えており、こうした機能は、記憶部２１に記憶されたサービス利用プログラム２１０により実現される。記憶部２１には、サービス提供装置１から取得した取引識別情報Ｔから選択された取引識別情報のリスト２２７、サービス提供装置１で署名処理された識別データが登録された登録部２２８、各ｋ回目のサービス取引においてサービス提供装置１から送信された（２Ｍ＋３）個の一次結合データS_j（ｋ）を記憶する登録部２２９、次回のサービス取引の取引識別情報Ｔ（ｋ＋１）の暗号化処理に用いるM^2個の係数データb_{st}（s=1,2,…,M;t=1,2,…,M）を記憶する係数データ記憶部２３０を記憶している。

【０１１４】

取引識別情報取得部２２０は、上述の実施形態と同様の機能を備えている。

【０１１５】

識別データ生成部２３１は、サービス取引を行うごとに自動的に１ずつ増加してサービス取引の回数を示す回数データを設定する機能を備えており、最初のサービス取引の取引識別情報Ｔ（１）を選択してその回数データＱ（１）を設定し、両者を合体した識別データＴ（１）Ｑ（１）を生成し、また、ｋ回目のサービス取引完了後に次回のサービス取引の取引識別情報Ｔ（ｋ＋１）（k=1,2,…,N）を選択してその回数データＱ（ｋ）を設定し、両者を合体した識別データＴ（ｋ＋１）Ｑ（ｋ＋１）を生成する。なお、回数データＱ（ｋ）は、取引回数そのもののデータ以外にも、（取引回数－定数）や（取引回数×定数）というように設定してもよく、サービス取引を行うごとに１ずつ増加するように設定されればよい。

【０１１６】

暗号化処理部２２２は、最初のサービス取引の識別データＴ（１）Ｑ（１）又はサービス取引完了後に次回のサービス取引の識別データＴ（ｋ＋１）Ｑ（ｋ＋１）を暗号化処理し暗号化識別データを生成する。また、復号化処理部２２３は、サービス提供装置から送信された署名処理済みの暗号化識別データを復号化処理して署名処理済みの識別データを登録部２２８に記憶する。

【０１１７】

暗号化処理部２２２で暗号化処理された識別データは、サービス提供装置１の署名処理部１２３で署名処理されてサービス利用装置に送信されて復号化処理部２２３で復号化されるが、これら一連の処理は、上述の実施形態と同様に行われる。

【０１１８】

確認情報処理部２２４は、最初のサービス取引の取引識別情報Ｔ（１）に基づいて暗号化処理されたＭ個の初期確認情報W_t（０）（t=1,2,…,M）を生成するとともに、ｋ回目

のサービス取引完了後に次回のサービス取引の取引識別情報Ｔ（ｋ＋１）（k=1,2,…,N）に基づいて計算されるＶ$_s$（ｋ＋１）を暗号化処理したＭ個の確認情報Ｗ$_t$（ｋ）（t=1,2,…,M）を生成する。Ｍ個の要素データＶ$_s$（ｋ＋１）及びＭ個の確認情報Ｗ$_t$（ｋ）は、上述した実施形態と同様に生成される。

【０１１９】

結合集計部２２５は、サービス提供装置１からの集計依頼に応じて登録された一次結合データＳ$_j$（ｋ）を各ｊ毎にｋについて集計した結合集計データΣＳ$_j$（ｋ）を算出するとともに次回の取引識別情報Ｔ（Ｎ＋１）に基づく要素データＶ$_s$（Ｎ＋１）及び次回のサービス取引の回数順に基づく回数データＱ（Ｎ＋１）を生成して結合集計データΣＳ$_j$（ｋ）、要素データＶ$_s$（Ｎ＋１）及び回数データＱ（Ｎ＋１）を送信する。

【０１２０】

例えば、サービス提供装置１との間でＮ回のサービス取引が行われたとすると、サービス提供装置１からサービス利用装置２に、サービス取引前の最初に使用する取引識別情報Ｔ（１）に関するものをＳ$_j$（０）とすると、図１９に示すように、Ｓ$_j$（０）からＳ$_j$（Ｎ）までの（Ｎ＋１）回分の一次結合データがサービス利用装置２に送信される。そして、サービス提供装置１からの集計依頼があった場合、一次結合データＳ$_j$（ｋ）を各ｊ毎にｋについて集計した結合集計データΣＳ$_j$（ｋ）は、図１９の最下段の式で求められる。この式は、集計値ΣＥ（ｋ）、集計値ΣＱ（ｋ）、集計値Σｒ$_k$Ｖ$_s$（ｋ）、集計値Σｒ$_{k+1}$Ｗ$_t$（ｋ）及び集計値ΣＲ（ｋ）の（２Ｍ＋３）個のデータを変数として係数データａ$_{ij}$を用いた（２Ｍ＋３）個の連立一次方程式となっている。

【０１２１】

そのため、サービス提供装置１の集計値算出部１２５では、結合集計データΣＳ$_j$（ｋ）を得ることができれば、係数データａ$_{ij}$に基づいて（２Ｍ＋３）個の連立一次方程式を解くことができ、集計値ΣＥ（ｋ）、集計値ΣＱ（ｋ）、集計値Σｒ$_k$Ｖ$_s$（ｋ）、集計値Σｒ$_{k+1}$Ｗ$_t$（ｋ）及び集計値ΣＲ（ｋ）を得ることができる。したがって、サービス提供装置１の集計値算出部１２５では、サービス利用装置２の個々のサービス取引に関する利用料金Ｅ（ｋ）を知らなくてもその集計値ΣＥ（ｋ）を算出することが可能となる。

【０１２２】

また、一次結合データΣＳ$_j$（ｋ）の算出式には、サービス利用装置２側が知らない係数データａ$_{ij}$の他に乱数ｒ$_k$及びＲ（ｋ）が用いられているので、サービス利用装置２において一次結合データＳ$_j$の算出式を知ることはできず、不正操作を行うことはできない。

【０１２３】

不正判定部１２６は、集計値ΣＱ（ｋ）を用いて不正判定を行う場合には、集計値ΣＱ（ｋ）が取引識別情報Ｔ（１）～Ｔ（Ｎ）に関する回数データの総和であることから、サービス利用装置２から送信された取引識別情報Ｔ（Ｎ＋１）の回数データＱ（Ｎ＋１）との整合性をチェックすることで、一次結合データＳ$_j$の集計において不正操作があったことを判定できる。例えば、回数データＱ（ｋ）が取引回数自体を示すデータの場合回数データＱ（Ｎ＋１）が（Ｎ＋１）となって、集計値は１からＮまでの整数を連続して加算した値Ｎ・（Ｎ＋１）／２となるが、集計値算出部１２５から得られた集計値ΣＱ（ｋ）がこの値と異なっていれば、一次結合データＳ$_j$を一部欠落させて集計していることが疑われて不正操作をチェックすることができる。

【０１２４】

不正判定部１２６で集計値Σｒ$_k$Ｖ$_s$（ｋ）に基づいて不正判定を行う場合には、図１９に示すように、取引識別情報Ｔ（１）～Ｔ（Ｎ）に関する要素データと乱数の積ｒ$_k$Ｖ$_s$（ｋ）を集計した集計値Σｒ$_k$Ｖ$_s$（ｋ）に対して、集計値Σｒ$_{k+1}$Ｗ$_t$（ｋ）は、取引識別情報Ｔ（１）～Ｔ（Ｎ）に次回の取引識別情報Ｔ（Ｎ＋１）を加えたものを集計していることから、結合データ集計部２２５では、次回の取引識別情報Ｔ（Ｎ＋１）に基づいて要素データと乱数の積ｒ$_{N+1}$Ｖ$_s$（Ｎ＋１）を生成してサービス提供装置１に送信し、集計値算出部１２５で集計された集計値Σｒ$_k$Ｖ$_s$（ｋ）に各ｓ毎に要素データと乱数の積ｒ$_{N+1}$Ｖ$_s$

（Ｎ＋１）を加算して取引識別情報Ｔ（１）～Ｔ（Ｎ＋１）に関する集計値を算出する。

【０１２５】

そして、集計値算出部１２５は、集計値$\Sigma r_{k+1}W_t$（ｋ）をサービス利用装置２に送信し、上述した実施形態と同様に要素集計処理部２２６において集計値ΣX_u（ｋ）を算出し、算出処理した集計値ΣX_u（ｋ）が、取引識別情報Ｔ（１）～Ｔ（Ｎ＋１）に関する集計値であるため、不正な処理が行われていなければ、集計値$\Sigma r_k V_s$（ｋ）と一致することから、不正判定部１２６で算出した集計値と一致するか否か判定することで、不正操作が行われたか否かチェックすることが可能となる。サービス利用装置２側で一次結合データΣS_j（ｋ）を不正操作すると、今回及び次回のサービス取引の取引識別情報Ｔ（ｋ）の確認情報とＴ（ｋ＋１）との整合性がとれなくなり、サービス提供装置１の不正判定部１２６で算出した今回の取引識別情報Ｔ（ｋ）に関する要素データの集計値$\Sigma r_k V_s$（ｋ）とサービス利用装置２の要素集計処理部２２６で算出した次回の取引識別情報Ｔ（ｋ＋１）に関する要素データの集計値ΣX_u（ｋ）が一致しなくなって不正判定部１２６においてチェックされるようになる。

【０１２６】

要素集計処理部２２６では、集計値$\Sigma r_k V_s$（ｋ）のみをサービス提供装置１に返すようになっているため、個々のサービス取引の取引識別情報Ｔ（ｋ）に関する要素データV_s（ｋ）を知られることがない。

【０１２７】

図２０は、サービス取引の実施前に行われる取引識別情報の発行処理に関するフローである。サービス提供装置１では、予め必要数の取引識別情報が生成されて取引識別情報テーブル１２８が記憶されている（Ｓ８００）。まず、サービス提供装置１とサービス利用装置２との間で互いに正当性の判定が行われて（Ｓ８０１、Ｓ８０２）匿名での認証が行われる。互いに正当性があると判定された場合に、サービス利用装置２は、サービス提供装置１に対して必要な数の取引識別情報の発行依頼を行う（Ｓ８０３）。サービス提供装置１は、未使用の取引識別情報をリストアップして、必要数をサービス利用装置２に発行する（Ｓ８０４）。発行された取引識別情報は、サービス利用装置２の登録部２２８に記憶される（Ｓ８０５）。

【０１２８】

次に、最初のサービス取引に用いる取引識別情報Ｔ（１）を選択して（Ｓ８０６）その回数データＱ（１）を設定し（Ｓ８０７）識別データＴ（１）Ｑ（１）を生成する（Ｓ８０８）。生成された識別データは暗号化処理部２２２で暗号化処理を行い（Ｓ８０９）、暗号化識別データを生成する。そして、選択された取引識別情報Ｔ（１）に基づいて確認情報処理部２２４で初期確認情報W_t（０）を生成する（Ｓ８１０）。生成された暗号化識別データＴ（１）Ｑ（１）及び初期確認情報W_t（０）を添付してサービス提供装置１に対して署名処理を依頼する（Ｓ８１１）。サービス提供装置１では、署名処理部１２３で暗号化識別データＴ（１）Ｑ（１）に署名処理を行い（Ｓ８１２）、結合計算部１２４で一次結合データS_j（１）を上記の式（Ｉ）により算出処理する（Ｓ８１３）。署名処理された暗号化識別データＴ（１）Ｑ（１）及び算出された一次結合データS_j（１）をサービス利用装置２に送信し（Ｓ８１４）、署名処理された暗号化識別データＴ（１）Ｑ（１）は、サービス利用装置２の復号化処理部２２３で処理されて署名入りの識別データＴ（１）Ｑ（１）となり（Ｓ８１５）、登録部２２８に登録され、一次結合データS_j（１）は登録部２２９に登録される（Ｓ８１６）。

【０１２９】

以上の処理により、サービス利用装置２は、サービス取引に必要な取引識別情報を取得するとともに最初に使用する署名入りの識別データを得ることができる。

【０１３０】

図２１は、サービス利用装置２のｋ回目のサービス取引を行う場合の処理に関するフローである。まず、サービス提供装置１とサービス利用装置２との間で互いに正当性の判定が行われて（Ｓ９００、Ｓ９０１）匿名での認証が行われる。互いに正当性があると判定

された場合に、サービス利用措置２は、署名入りの識別データＴ（ｋ）Ｑ（ｋ）を読み出して（Ｓ９０２）サービス提供装置１に対してサービス依頼を行う（Ｓ９０３）。

【０１３１】

サービス提供装置１は、サービス依頼を受けると、署名入りの識別データＴ（ｋ）Ｑ（ｋ）を取得して（Ｓ９０４）正常に署名されているか否か、取引識別情報Ｔ（ｋ）が未使用のものであるか否かチェックし識別データＴ（ｋ）Ｑ（ｋ）の判定を行う（Ｓ９０５）。識別データＴ（ｋ）Ｑ（ｋ）が正常なものであると判定された場合には、サービス処理を開始してサービス利用装置２との間でサービス取引を行う（Ｓ９０６）。そして、サービス取引完了後その利用料金Ｅ（ｋ）を算出する（Ｓ９０７）。

【０１３２】

ステップＳ９０５において、識別データＴ（ｋ）Ｑ（ｋ）が正常なものでないと判定された場合にはエラー処理を行い（Ｓ９０８）サービス処理は行われない。

【０１３３】

一方、サービス利用装置２は、サービス提供装置１とのサービス取引が開始されると、必要なサービス処理を行い（Ｓ９０９）、サービス取引完了後に次回のサービス取引に用いる取引識別情報Ｔ（ｋ＋１）を選択して（Ｓ９１０）その回数データＱ（ｋ＋１）を設定し（Ｓ９１１）識別データＴ（ｋ＋１）Ｑ（ｋ＋１）を生成する（Ｓ９１２）。生成された識別データは暗号化処理部２２２で暗号化処理を行い（Ｓ９１３）、暗号化識別データを生成する。

【０１３４】

次に、次回の取引識別情報Ｔ（ｋ＋１）に基づいて確認情報処理部２２４で確認情報W_t（ｋ）を生成する（Ｓ９１４）。そして、生成された暗号化識別データＴ（ｋ＋１）Ｑ（ｋ＋１）を添付してサービス提供装置１に対して署名処理を依頼する（Ｓ９１５）。

【０１３５】

サービス提供装置１では、署名処理部１２３で暗号化識別データＴ（ｋ＋１）Ｑ（ｋ＋１）に署名処理を行い（Ｓ９１６）、結合計算部１２４で一次結合データΣS_j（ｋ）を上記の式（Ｊ）により算出処理する（Ｓ９１７）。署名処理された暗号化識別データＴ（ｋ＋１）Ｑ（ｋ＋１）及び算出された一次結合データS_j（ｋ）をサービス利用装置２に送信し（Ｓ９１８）、署名処理された暗号化識別データＴ（ｋ＋１）Ｑ（ｋ＋１）は、サービス利用装置２の復号化処理部２２３で処理されて署名入りの識別データＴ（ｋ＋１）Ｑ（ｋ＋１）となり（Ｓ９１９）、登録部２２８に登録され、一次結合データS_jは、登録部２２９に登録される（Ｓ９２０）。

【０１３６】

以上の処理では、互いの正当性を判定して匿名認証した後においても取引識別情報を用いて署名入りの場合にサービス提供装置１でサービス取引するようにいるので、個々のサービス取引が匿名で正しく実行できるようになる。また、次回の取引識別情報については暗号化処理された暗号化識別データＴ（ｋ＋１）Ｑ（ｋ＋１）で処理されるので、今回の取引識別情報との関連付けがなされず取引識別情報から一連のサービス取引を特定することができない。

【０１３７】

サービス提供装置１では、署名入りの識別データにより正当なサービス取引権限のある利用者を確実に判定することができるとともに、回数データについても署名処理されることで不正判定の際の根拠データとして用いることができる。

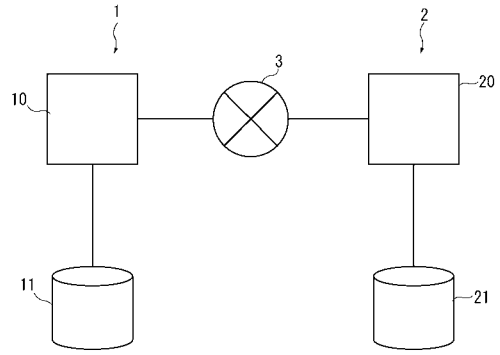
【０１３８】

図２２は、これまでにＮ回のサービス取引を行ったサービス利用装置２に関する利用料金等の集計処理に関するフローである。集計処理は、サービス提供装置１において所定期間毎に行われる。まず、サービス提供装置１とサービス利用装置２との間で互いに正当性の判定が行われて（Ｓ１０００、Ｓ１００１）匿名での認証が行われる。互いに正当性があると判定された場合に、サービス提供装置１は、サービス利用装置２に対して集計依頼を行う（Ｓ１００２）。

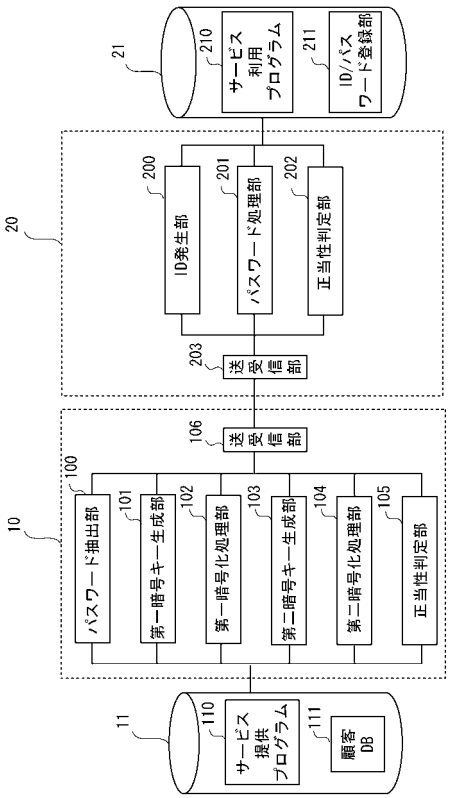
【０１３９】
サービス利用装置２は、集計依頼に基づいて登録部２２９に蓄積された一次結合データS_j（ｋ）を各ｊ毎に集計して結合集計データΣS_j（ｋ）を算出する（Ｓ１００３）。そして、選択された次回の取引識別情報Ｔ（Ｎ＋１）を読み出して（Ｓ１００４）その回数データＱ（Ｎ＋１）を設定する（Ｓ１００５）とともに要素データV_s（Ｎ＋１）を生成し（Ｓ１００６）、結合集計データΣS_j（ｋ）、回数データＱ（Ｎ＋１）及び要素データV_s（Ｎ＋１）をサービス提供装置１に送信する（Ｓ１００７）。
【０１４０】
サービス提供装置１は、結合集計データΣS_j及び係数データa_{ij}に基づいて、集計値ΣＥ（ｋ）、集計値ΣＱ（ｋ）、集計値Σ$r_k V_s$（ｋ）及び集計値Σ$r_{k+1} W_t$（ｋ）を算出する（Ｓ１００８）。そして、算出された集計値ΣＱ（ｋ）とサービス利用装置２から送信された回数データＱ（Ｎ＋１）との間の整合性をチェックし（Ｓ１００９）、両者の間に整合性がある場合には、集計値Σ$r_k V_s$（ｋ）に要素データと乱数の積$r_{N+1} V_s$（Ｎ＋１）を各ｓ毎に加算処理した集計値を求め（Ｓ１０１０）、集計値Σ$r_{k+1} W_t$（ｋ）は、サービス利用装置２に送信する（Ｓ１０１１）。
【０１４１】
サービス利用装置２は、集計値Σ$r_{k+1} W_t$（ｋ）に基づいて集計値ΣX_u（ｋ）を算出処理し（Ｓ１０１２）、算出された集計値ΣX_u（ｋ）をサービス提供装置１に送信する（Ｓ１０１３）。
【０１４２】
サービス提供装置１は、送信された集計値ΣX_u（ｋ）とステップＳ１０１０で算出した集計値が一致するか判定し（Ｓ１０１４）、一致する場合には正しく集計されたものとして集計値ΣＥ（ｋ）に基づいてサービス利用装置２に利用料金の請求を行う（Ｓ１０１５）。サービス利用装置２は、利用料金の請求に基づいて支払い処理を行う（Ｓ１０１６）。
【０１４３】
ステップＳ１００９において回数データＱに関して整合性がない場合及びステップ１０１４において要素データV_s（ｋ）に関して一致しない場合には、不正操作があったものとして、サービス提供装置１は、不正処理を行う（Ｓ１０１７）。
【０１４４】
以上の処理により、サービス提供装置１側では、回数データＱ及び取引識別情報Ｔに関して二重の不正判定を行うことができ、より的確に不正操作を判定することができる。
【０１４５】
なお、以上の例では、取引識別情報をサービス取引装置側で生成してサービス利用装置で取得するようにしているが、第三者機関などが取引識別情報を生成してサービス利用装置に提供するようにしてもよい。また、取引識別情報に基づいて生成される要素データV_s（ｋ）は、サービス提供装置で生成して用いたり、サービス利用装置で生成してサービス提供装置に送信したりすることができ、適宜選択してシステム構成すればよい。
【産業上の利用可能性】
【０１４６】
このように、本発明に係るサービス取引システムでは、サービス利用者側において個々の取引内容を知られることなくサービス取引を行うことができる。また、サービス提供者側においては個別情報を蓄積することなく確実に利用料金の請求を行うことができ、個別情報の管理コストを大幅に低減することができる。そして、利用料金の集計に不正な操作が行われたとしても不正判定を確実に行い、正しい利用料金の請求が行うことが可能となる。
【０１４７】
したがって、今後ユキュビタス・コンピューティングの進展により企業のみならず家庭内にもネットワークが普及した社会において、本発明を用いることでサービス取引を円滑に行うことができる。

【図面の簡単な説明】
【０１４８】
【図１】本発明に係る実施形態の構成を示す概略図である。
【図２】本発明に係る実施形態において正当性を判定するための機能ブロック図である。
【図３】本発明に係る実施形態において正当性を判定するための処理フローである。
【図４】ＩＤリストに関する説明図である。
【図５】パスワードリストに関する説明図である。
【図６】暗号パスワードリストに関する説明図である。
【図７】本発明に係る実施形態におけるサービス取引に関する機能ブロック図である。
【図８】取引識別情報の要素データに関する説明図である。
【図９】取引識別情報の要素データに関する説明図である。
【図１０】一次結合データの集計に関する説明図である。
【図１１】サービス取引の実施前に行われる取引識別情報の発行処理に関するフローである。
【図１２】サービス取引を行う場合の処理に関するフローである。
【図１３】利用料金等の集計処理に関するフローである。
【図１４】変形例における一次結合データの集計に関する説明図である。
【図１５】変形例におけるサービス取引の実施前に行われる取引識別情報の発行処理に関するフローである。
【図１６】変形例におけるサービス取引を行う場合の処理に関するフローである。
【図１７】変形例における利用料金等の集計処理に関するフローである。
【図１８】別の実施形態におけるサービス取引に関する機能ブロック図である。
【図１９】別の実施形態における一次結合データの集計に関する説明図である。
【図２０】別の実施形態におけるサービス取引の実施前に行われる取引識別情報の発行処理に関するフローである。
【図２１】別の実施形態におけるサービス取引を行う場合の処理に関するフローである。
【図２２】別の実施形態における利用料金等の集計処理に関するフローである。
【符号の説明】
【０１４９】
１　　サービス提供装置
２　　サービス利用装置
３　　ネットワーク
10　　情報処理部
11　　記憶部
20　　情報処理部
21　　記憶部

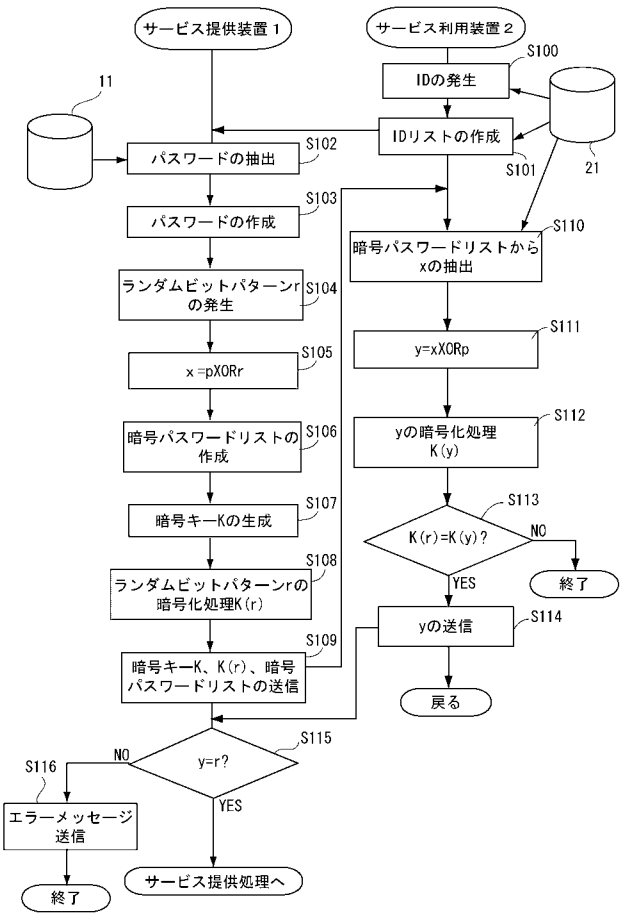
【図１】



【図２】



【図３】



【図４】

1	ID_1
2	ID_5
・	・
・	・
t	ID_k
・	・
・	・
N	ID_m

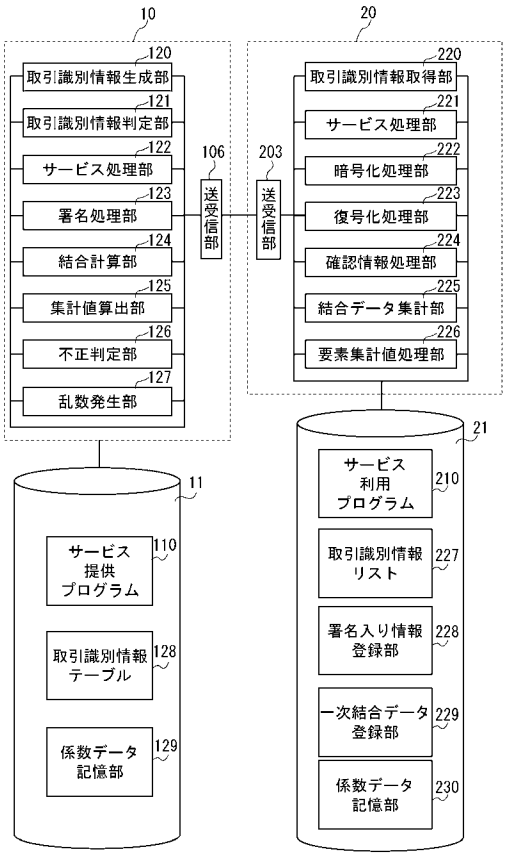
【図５】

1	p_1
2	p_5
・	・
・	・
t	p_k
・	・
・	・
N	p_m

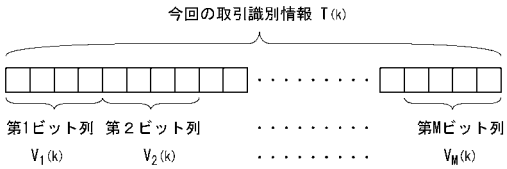
【図６】

1	x_1
2	x_5
・	・
・	・
t	x_k
・	・
・	・
N	x_m

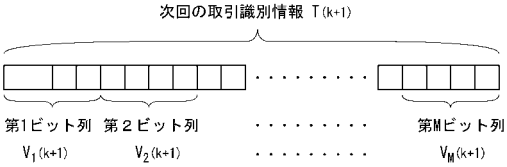
【図７】



【図８】



【図９】



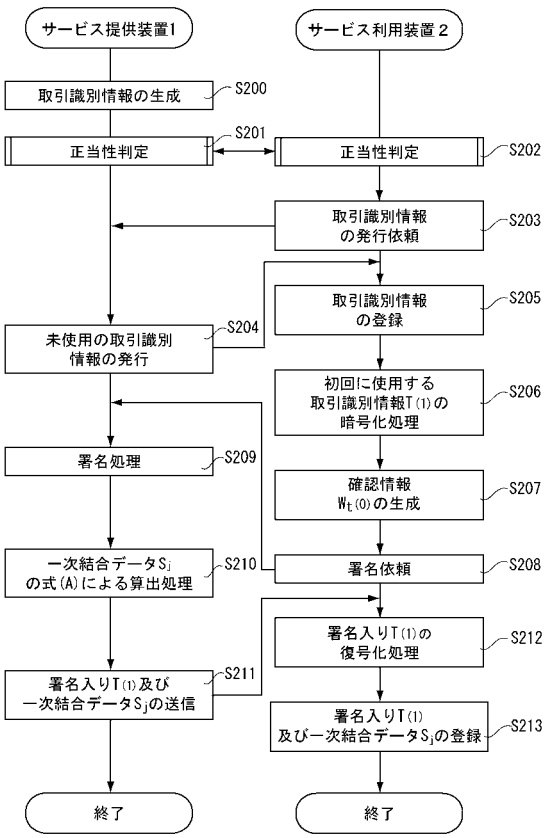
【図１０】

［取引回数］［今回］［次回］［一次結合データ S_j (j=1, 2, …, 2M+2)］

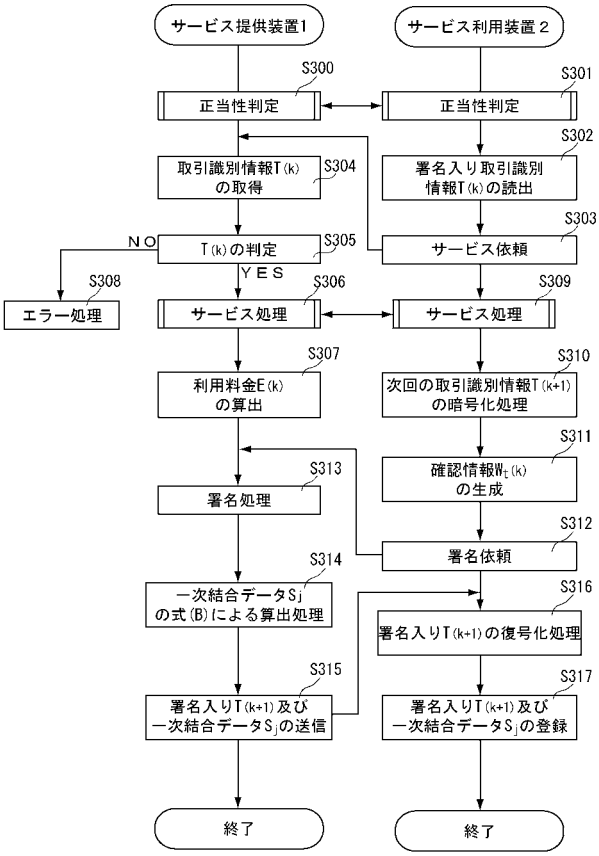
0		T(1)	$S_j = \sum_{t=1}^{M} a_{(M-t-1)j} W_t(0) r_1 + a_{(2M-2)j} R(0)$
1	T(1)	T(2)	$S_j = a_{1j} E(1) + \sum_{s=1}^{M} a_{(s-1)j} V_s(1) r_1 + \sum_{t=1}^{M} a_{(M-t-1)j} W_t(1) r_2 + a_{(2M-2)j} R(1)$
2	T(2)	T(3)	$S_j = a_{1j} E(2) + \sum_{s=1}^{M} a_{(s-1)j} V_s(2) r_2 + \sum_{t=1}^{M} a_{(M-t-1)j} W_t(2) r_3 + a_{(2M-2)j} R(2)$
・	・	・	・
k	T(k)	T(k-1)	$S_j = a_{1j} E(k) + \sum_{s=1}^{M} a_{(s-1)j} V_s(k) r_k + \sum_{t=1}^{M} a_{(M-t-1)j} W_t(k) r_{k-1} + a_{(2M-2)j} R(k)$
・	・	・	・
・	・	・	・
N	T(N)	T(N-1)	$S_j = a_{1j} E(N) + \sum_{s=1}^{M} a_{(s-1)j} V_s(N) r_N + \sum_{t=1}^{M} a_{(M-t-1)j} W_t(N) r_{N-1} + a_{(2M-2)j} R(N)$

$$\sum_{k=0}^{M} S_j = a_{1j} \sum_{k=1}^{M} E(k) + \sum_{s=1}^{M} a_{(s-1)j} \sum_{k=1}^{N} V_s(k) r_k + \sum_{t=1}^{M} a_{(M-t-1)j} \sum_{k=0}^{N} W_t(k) r_{k-1} + \sum_{t=1}^{M} a_{(2M-2)j} R(N)$$

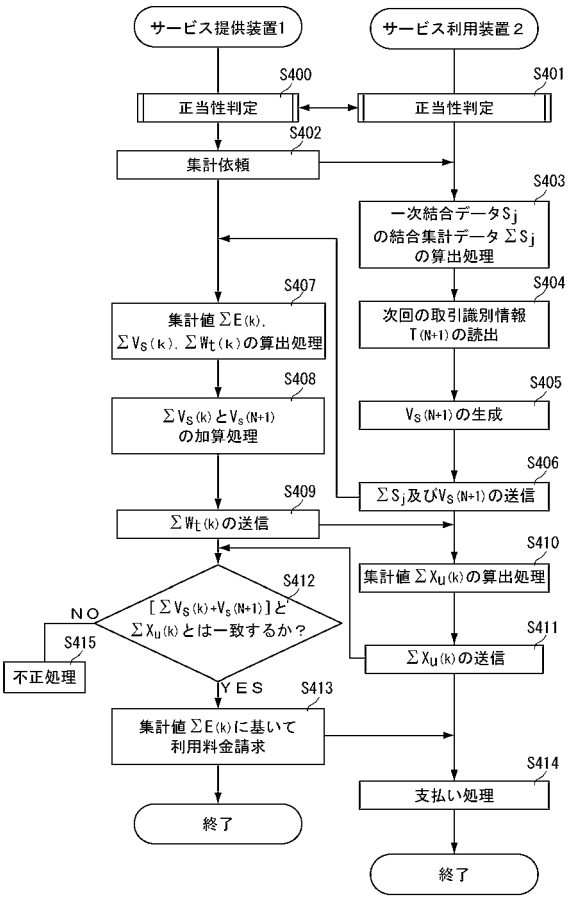
【図１１】



【図１２】



【図１３】



【図１４】

[取引回数] [今回] [前回] [一次結合データ S_j (j=1, 2, …, 2M+2)]

$$0 \quad T(0) \qquad S_j = \sum_{s=1}^{M} a_{(s-1)j} V_s(0)\, r_1 \qquad + a_{(2M-2)j} R(0)$$

$$1 \quad T(1) \quad T(0) \quad S_j = a_{1j} E(1) + \sum_{s=1}^{M} a_{(s-1)j} V_s(1)\, r_2 + \sum_{t=1}^{M} a_{(M+t-1)j} W_t(0)\, r_1 + a_{(2M-2)j} R(1)$$

$$2 \quad T(2) \quad T(1) \quad S_j = a_{1j} E(2) + \sum_{s=1}^{M} a_{(s-1)j} V_s(2)\, r_3 + \sum_{t=1}^{M} a_{(M+t-1)j} W_t(1)\, r_2 + a_{(2M-2)j} R(2)$$

$$\vdots$$

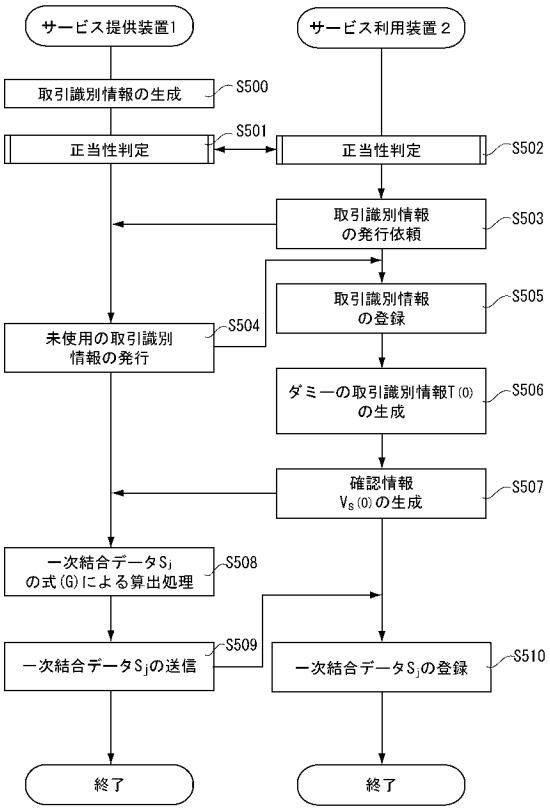
$$k \quad T(k) \quad T(k-1) \quad S_j = a_{1j} E(k) + \sum_{s=1}^{M} a_{(s-1)j} V_s(k)\, r_{k-1} + \sum_{t=1}^{M} a_{(M+t-1)j} W_t(k-1)\, r_k + a_{(2M-2)j} R(k)$$

$$\vdots$$

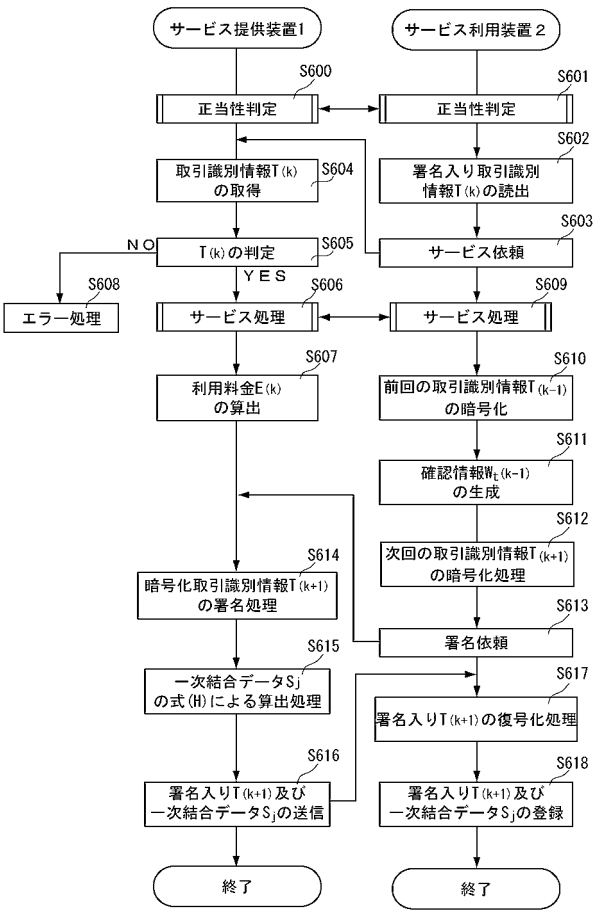
$$N \quad T(N) \quad T(N-1) \quad S_j = a_{1j} E(N) + \sum_{s=1}^{M} a_{(s-1)j} V_s(N)\, r_{N-1} + \sum_{t=1}^{M} a_{(M+t-1)j} W_t(N-1)\, r_N + a_{(2M-2)j} R(N)$$

$$\sum_{k=0}^{M} S_j = a_{1j} \sum_{k=1}^{M} E(k) + \sum_{s=1}^{M} a_{(s-1)j} \sum_{k=0}^{N} V_s(k)\, r_{k-1} + \sum_{t=1}^{M} a_{(M+t-1)j} \sum_{k=0}^{N-1} W_t(k-1)\, r_k + \sum_{t=1}^{M} a_{(2M-2)j} R(N)$$

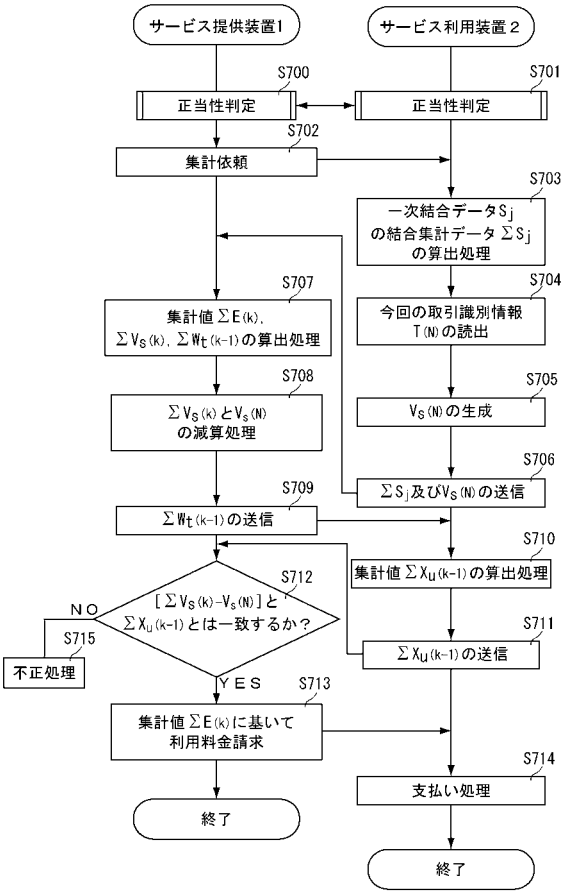
【図１５】



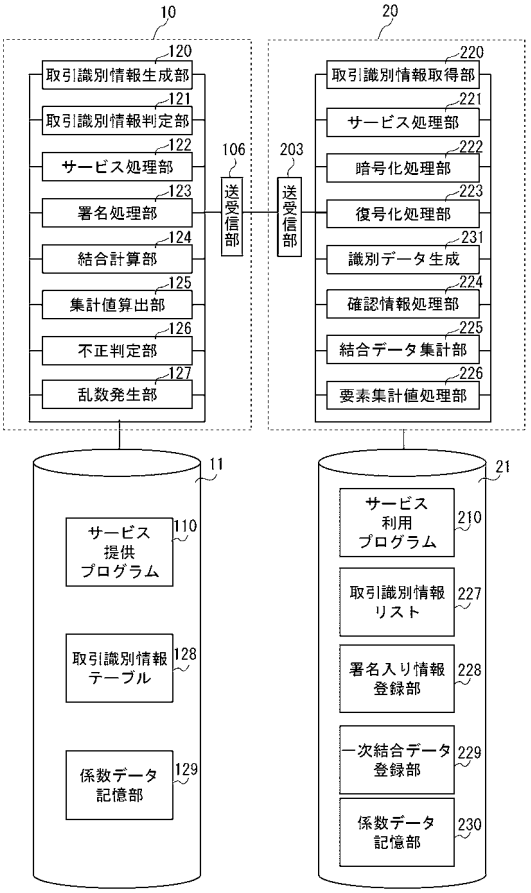
【図１６】



【図１７】



【図１８】



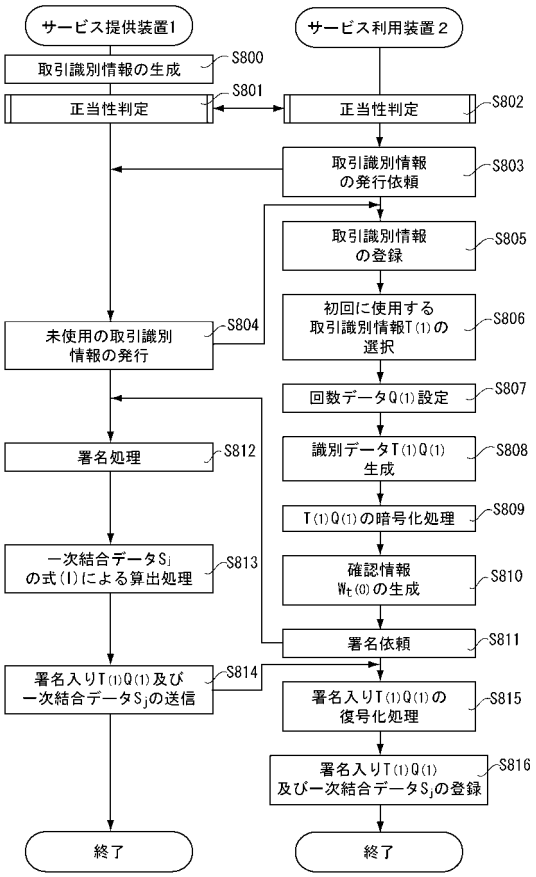
【図１９】

[取引回数][今回][次回][一次結合データ S_j (j=1, 2, …, 2M+2)]

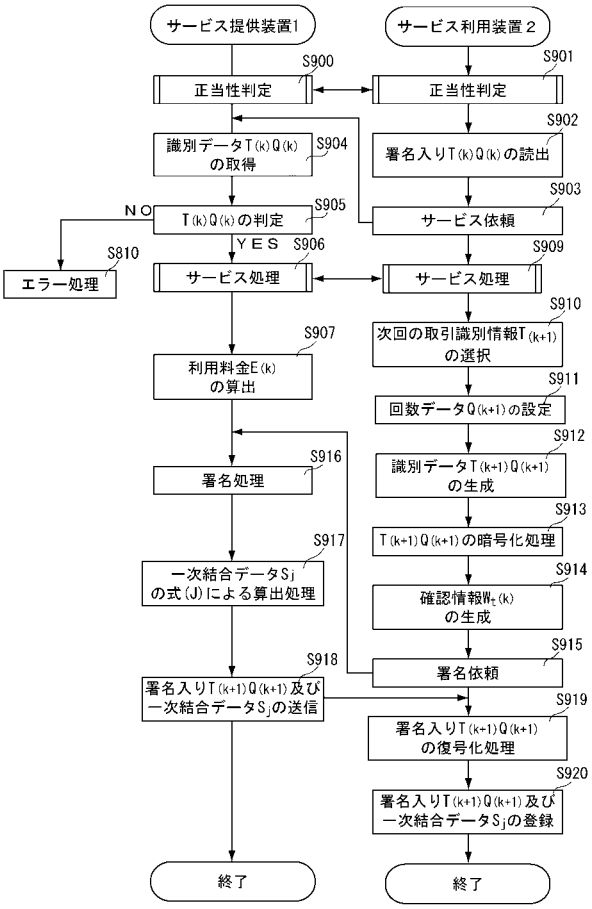
0		T(1)	$S_j = \sum_{t=1}^{M} a_{(M-t-2)j} W_t(0) r_1 + a_{(2M-3)j} R(0)$
1	T(1)	T(2)	$S_j = a_{1j} E(1) + a_{2j} Q(1) + \sum_{s=1}^{M} a_{(s-2)j} V_s(1) r_1 + \sum_{t=1}^{M} a_{(M-t-2)j} W_t(1) r_2 + a_{(2M-3)j} R(1)$
2	T(2)	T(3)	$S_j = a_{1j} E(2) + a_{2j} Q(2) + \sum_{s=1}^{M} a_{(s-2)j} V_s(2) r_2 + \sum_{t=1}^{M} a_{(M-t-2)j} W_t(2) r_3 + a_{(2M-3)j} R(2)$
・	・	・	・
k	T(k)	T(k-1)	$S_j = a_{1j} E(k) + a_{2j} Q(k) + \sum_{s=1}^{M} a_{(s-2)j} V_s(k) r_k + \sum_{t=1}^{M} a_{(M-t-2)j} W_t(k) r_{k-1} + a_{(2M-3)j} R(k)$
・	・	・	・
・	・	・	・
N	T(N)	T(N-1)	$S_j = a_{1j} E(N) + a_{2j} Q(N) + \sum_{s=1}^{M} a_{(s-2)j} V_s(N) r_N + \sum_{t=1}^{M} a_{(M-t-2)j} W_t(N) r_{N-1} + a_{(2M-3)j} R(N)$

$$\sum_{k=0}^{M} S_j = a_{1j} \sum_{k=1}^{M} E(N) + a_{2j} \sum_{k=1}^{M} Q(k) + \sum_{s=1}^{M} a_{(s-2)j} \sum_{k=1}^{N} V_s(k) r_k + \sum_{t=1}^{M} a_{(M-t-2)j} \sum_{k=0}^{N} W_t(k) r_{k-1} + \sum_{t=1}^{M} a_{(2M-3)j} R(N)$$

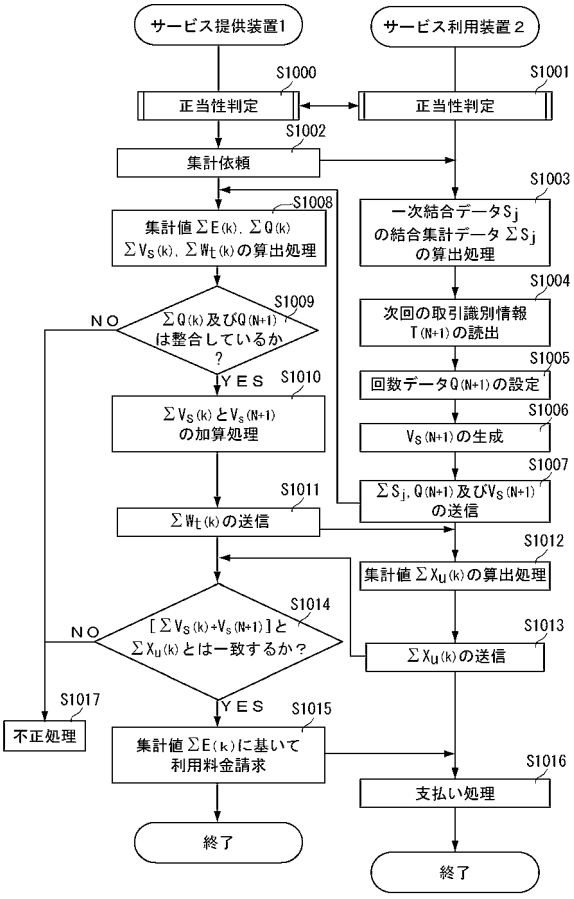
【図２０】



【図２１】


サービス提供装置1
サービス利用装置２
S900
正当性判定
S901
正当性判定
識別データT(k)Q(k)の取得
S904
S902
署名入りT(k)Q(k)の読出
S903
サービス依頼
NO
T(k)Q(k)の判定
S905
YES
S906
サービス処理
S909
サービス処理
S810
エラー処理
S910
次回の取引識別情報T(k+1)の選択
S907
利用料金E(k)の算出
S911
回数データQ(k+1)の設定
S912
識別データT(k+1)Q(k+1)の生成
S916
署名処理
S913
T(k+1)Q(k+1)の暗号化処理
S917
一次結合データSjの式(J)による算出処理
S914
確認情報Wt(k)の生成
S915
署名依頼
S918
署名入りT(k+1)Q(k+1)及び一次結合データSjの送信
S919
署名入りT(k+1)Q(k+1)の復号化処理
S920
署名入りT(k+1)Q(k+1)及び一次結合データSjの登録
終了
終了

【図２２】


サービス提供装置1
サービス利用装置２
S1000
正当性判定
S1001
正当性判定
S1002
集計依頼
S1008
集計値ΣE(k)、ΣQ(k)
ΣVS(k)、ΣWt(k)の算出処理
S1003
一次結合データSjの結合集計データ ΣSjの算出処理
S1009
ΣQ(k)及びQ(N+1)は整合しているか？
NO
YES
S1004
次回の取引識別情報T(N+1)の読出
S1005
回数データQ(N+1)の設定
S1010
ΣVS(k)とVs(N+1)の加算処理
S1006
VS(N+1)の生成
S1007
ΣSj、Q(N+1)及びVS(N+1)の送信
S1011
ΣWt(k)の送信
S1012
集計値ΣXu(k)の算出処理
S1014
[ΣVS(k)+Vs(N+1)]とΣXu(k)とは一致するか？
NO
YES
S1013
ΣXu(k)の送信
S1017
不正処理
S1015
集計値ΣE(k)に基いて利用料金請求
S1016
支払い処理
終了
終了