

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第4820997号
(P4820997)

(45) 発行日 平成23年11月24日(2011.11.24)

(24) 登録日 平成23年9月16日(2011.9.16)

(51) Int.Cl.		F I			
H04L	9/32	(2006.01)	H04L	9/00	675B
G06Q	30/00	(2006.01)	H04L	9/00	673C
			G06F	17/60	332

請求項の数 12 (全 42 頁)

(21) 出願番号	特願2006-96692(P2006-96692)	(73) 特許権者	504145320
(22) 出願日	平成18年3月31日(2006.3.31)		国立大学法人福井大学
(65) 公開番号	特開2007-274289(P2007-274289A)		福井県福井市文京3丁目9番1号
(43) 公開日	平成19年10月18日(2007.10.18)	(74) 代理人	100111855
審査請求日	平成21年1月8日(2009.1.8)		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
		審査官	新田 亮

最終頁に続く

(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) 【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进行处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进行处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

10

【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进行处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、

20

次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进行处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、

30

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。

40

【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进行处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 $V_s(k + 1)$ ($s = 1, 2, \dots, M$) 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

50

確認情報 $W_t(k)$ ($t=1, 2, \dots, M$) 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 $S_j(k)$ ($j=1, 2, \dots, P$) 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 $S_j(k)$ 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 $r_{k+1}W_t(k)$ ($t=1, 2, \dots, M$) を復号化処理して集計値 $X_u(k)$ ($u=1, 2, \dots, M$) 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} ($i=1, 2, \dots, P; j=1, 2, \dots, P$) 及び乱数 r_k ($k=1, 2, \dots$) 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 $V_s(k)$ (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 ($j=1, 2, \dots, P$) を以下の式 (B)

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

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 $S_j(k)$ 及び係数データ a_{ij} に基づいて取引識別情報 $T(1) \sim T(N)$ に関するデータ $E(k)$ の集計値 $E(k)$ 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 $S_j(k)$ 及び係数データ a_{ij} に基づいて取引識別情報 $T(1) \sim T(N)$ 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 $r_k V_s(k)$ 並びに取引識別情報 $T(1) \sim T(N+1)$ 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 $r_{k+1} W_t(k)$ を算出するとともに集計値 $r_{k+1} W_t(k)$ を送信する要素集計値算出手段と、集計値 $r_k V_s(k)$ とサービス利用装置から送信された集計値 $X_u(k)$ 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 $V_s(k)$ ($s=1, 2, \dots, M$) 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 $W_t(k)$ ($t=1, 2, \dots, M$) 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 $V_s(k)$ (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} ($i=1,2,\dots,P; j=1,2,\dots,P$) 及び乱数 r_k ($k=1,2,\dots$) を用いた互いに独立な一次結合データ $S_j(k)$ ($j=1,2,\dots,P$) を以下の式 (B)

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

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 $S_j(k)$ を算出するとともに結合集計データ $S_j(k)$ 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 $S_j(k)$ 及び係数データ a_{ij} に基づいて取引識別情報 $T(1) \sim T(N)$ に関するデータ $E(k)$ の集計値 $E(k)$ 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 $S_j(k)$ 及び係数データ a_{ij} に基づいて取引識別情報 $T(1) \sim T(N)$ 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 $r_k V_s(k)$ 並びに取引識別情報 $T(1) \sim T(N+1)$ 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 $r_{k+1} W_t(k)$ を算出するとともに集計値 $r_{k+1} W_t(k)$ 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 $r_{k+1} W_t(k)$ を復号化処理して集計値 $X_u(k)$ ($u=1,2,\dots,M$) 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 X_u と集計値 $r_k V_s(k)$ 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 $V_s(k+1)$ ($s=1,2,\dots,M$) 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 $W_t(k)$ ($t=1,2,\dots,M$) 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 $S_j(k)$ ($j=1,2,\dots,P$) 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 $S_j(k)$ 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 $r_{k+1} W_t(k)$ ($t=1,2,\dots,M$) を復号化処理して集計値 $X_u(k)$ ($u=1,2,\dots,M$) 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を判定する手段

10

20

30

40

50

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} ($i=1,2,\dots,P; j=1,2,\dots,P$) 及び乱数 r_k ($k=1,2,\dots$) 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 $S_j(k)$ ($j=1,2,\dots,P$) を以下の式 (B)

$$S_j(k) = a_{1j}E(k) + \{a_{(1+1)j}V_1(k) + a_{(2+1)j}V_2(k) + \dots + a_{(M+1)j}V_M(k)\}r_k + \{a_{(M+1+1)j}W_1(k) + a_{(M+2+1)j}W_2(k) + \dots + a_{(2M+1)j}W_M(k)\}r_{k+1} + a_{(2M+2)j}R(k) \dots (B) \quad 10$$

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 $S_j(k)$ 及び係数データ a_{ij} に基づいて取引識別情報 $T(1) \sim T(N)$ に関するデータ $E(k)$ の集計値 $E(k)$ 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 $S_j(k)$ 及び係数データ a_{ij} に基づいて取引識別情報 $T(1) \sim T(N)$ 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 $r_k V_s(k)$ 並びに取引識別情報 $T(1) \sim T(N+1)$ 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 $r_{k+1} W_t(k)$ を算出するとともに集計値 $r_{k+1} W_t(k)$ を送信する手段、 20

集計値 $r_k V_s(k)$ とサービス利用装置から送信された集計値 $X_u(k)$ 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 $V_s(k+1)$ ($s=1,2,\dots,M$) 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 $W_t(k)$ ($t=1,2,\dots,M$) 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 $S_j(k)$ ($j=1,2,\dots,P$) 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 $S_j(k)$ を算出するとともに結合集計データ $S_j(k)$ 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 $r_{k+1} W_t(k)$ ($t=1,2,\dots,M$) を復号化処理して集計値 $X_u(k)$ ($u=1,2,\dots,M$) を生成する要素集計値処理手段とを備え、 30

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 40

の知らない P^2 個の係数データ a_{ij} ($i=1,2,\dots,P; j=1,2,\dots,P$) 及び乱数 r_k ($k=1,2,\dots$) 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 ($j=1,2,\dots,P$) を以下の式 (D)

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

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 $S_j(k)$ 及び係数データ a_{ij} に基づいて取引識別情報 $T(1) \sim T(N)$ に関するデータ $E(k)$ の集計値 $E(k)$ 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 $S_j(k)$ 及び係数データ a_{ij} に基づいて取引識別情報 $T(1) \sim T(N)$ に関する回数データ $Q(k)$ の集計値 $Q(k)$ を算出して集計値 $Q(k)$ 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 $S_j(k)$ 及び係数データ a_{ij} に基づいて取引識別情報 $T(1) \sim T(N)$ 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 $r_k V_s(k)$ 並びに取引識別情報 $T(1) \sim T(N+1)$ 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 $r_{k+1} W_t(k)$ を算出するとともに集計値 $r_{k+1} W_t(k)$ を送信する要素集計値算出手段と、集計値 $r_k V_s(k)$ とサービス利用装置から送信された集計値 $X_u(k)$ 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进行处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 $V_s(k+1)$ ($s=1,2,\dots,M$) 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 $W_t(k)$ ($t=1,2,\dots,M$) 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} ($i=1,2,\dots,P; j=1,2,\dots,P$) 及び乱数 r_k ($k=1,2,\dots$) を用いた互いに独立な一次結合データ $S_j(k)$ ($j=1,2,\dots,P$) を以下の式 (D)

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

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 $S_j(k)$ を算出するとともに結合集計データ $S_j(k)$ 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 $S_j(k)$ 及び係数データ a_{ij} に基づいて取引識別情報 $T(1) \sim T(N)$ に関するデータ $E(k)$ の集計値 $E(k)$ 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 $S_j(k)$ 及び係数データ a_{ij} に基づいて取引識別情報 $T(1) \sim T(N)$ に関する回数データ $Q(k)$ の集計値 $Q(k)$ を算出して集計値 $Q(k)$ 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 $S_j(k)$ 及び係数データ a_{ij} に基づいて取引識別情報 $T(1) \sim T(N)$ 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 $r_k V_s(k)$ 並びに取引識別情報 $T(1) \sim T(N+1)$ 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 $r_{k+1} W_t(k)$ を算出するとともに集計値 $r_{k+1} W_t(k)$ 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 $r_{k+1} W_t(k)$ を復号化処理して集計値 $X_u(k)$ ($u=1,2,\dots,M$) 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 $X_u(k)$ と集計値 $r_k V_s(k)$ 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サービス取引方法。

10

【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进行处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、

20

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 $V_s(k+1)$ ($s=1,2,\dots,M$) 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 $W_t(k)$ ($t=1,2,\dots,M$) を生成する手段、

30

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 $S_j(k)$ ($j=1,2,\dots,P$) 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 $S_j(k)$ を算出するとともに結合集計データ $S_j(k)$ 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、

40

サービス提供装置から送信された集計値 $r_{k+1} W_t(k)$ ($t=1,2,\dots,M$) を復号化処理して集計値 $X_u(k)$ ($u=1,2,\dots,M$) 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进行处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

50

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} ($i=1, 2, \dots, P; j=1, 2, \dots, P$) 及び乱数 r_k ($k=1, 2, \dots$) を用いた互いに独立な一次結合データ S_j ($j=1, 2, \dots, P$) を以下の式 (D)

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

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 $S_j(k)$ 及び係数データ a_{ij} に基づいて取引識別情報 $T(1) \sim T(N)$ に関するデータ $E(k)$ の集計値 $E(k)$ 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 $S_j(k)$ 及び係数データ a_{ij} に基づいて取引識別情報 $T(1) \sim T(N)$ に関する回数データ $Q(k)$ の集計値 $Q(k)$ を算出して集計値 $Q(k)$ 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 $S_j(k)$ 及び係数データ a_{ij} に基づいて取引識別情報 $T(1) \sim T(N)$ 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 $r_k V_s(k)$ 並びに取引識別情報 $T(1) \sim T(N+1)$ 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 $r_{k+1} W_t(k)$ を算出するとともに集計値 $r_{k+1} W_t(k)$ を送信する手段、

集計値 $r_k V_s(k)$ とサービス利用装置から送信された集計値 $X_u(k)$ 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、

10

20

30

40

50

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。

10

【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に基づきサービス提供を行う点が記載されている。

【0007】

20

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。

30

【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】

40

【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

50

とはできないのが現状である。

【 0 0 1 2 】

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】

【 0 0 1 3 】

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。

【 0 0 1 4 】

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。

【 0 0 1 5 】

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

10

20

30

40

50

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。

10

【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 $V_s(k+1)$ ($s=1,2,\dots,M$)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 $W_t(k)$ ($t=1,2,\dots,M$)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 $S_j(k)$ ($j=1,2,\dots,P$)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 $S_j(k)$ 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 $r_{k+1}W_t(k)$ ($t=1,2,\dots,M$)を復号化処理して集計値 $X_u(k)$ ($u=1,2,\dots,M$)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} ($i=1,2,\dots,P; j=1,2,\dots,P$)及び乱数 r_k ($k=1,2,\dots$)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 ($j=1,2,\dots,P$)を以下の式(B)

20

30

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

40

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 $S_j(k)$ 及び係数データ a_{ij} に基づいて取引識別情報 $T(1) \sim T(N)$ に関するデータ $E(k)$ の集計値 $E(k)$ 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 $S_j(k)$ 及び係数データ a_{ij} に基づいて取引識別情報 $T(1) \sim T(N)$ 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 $r_kV_s(k)$ 並びに取引識別情報 $T(1) \sim T(N+1)$ 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 $r_{k+1}W_t(k)$ を算出するとともに集計値 $r_{k+1}W_t(k)$ を送信す

50

る要素集計値算出手段と、集計値 $r_k V_s(k)$ とサービス利用装置から送信された集計値 $X_u(k)$ 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进行处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 $V_s(k)$ ($s=1,2,\dots,M$) 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 $W_t(k)$ ($t=1,2,\dots,M$) 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} ($i=1,2,\dots,P; j=1,2,\dots,P$) 及び乱数 r_k ($k=1,2,\dots$) を用いた互いに独立な一次結合データ $S_j(k)$ ($j=1,2,\dots,P$) を以下の式 (B)

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

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 $S_j(k)$ を算出するとともに結合集計データ $S_j(k)$ 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 $S_j(k)$ 及び係数データ a_{ij} に基づいて取引識別情報 $T(1) \sim T(N)$ に関するデータ $E(k)$ の集計値 $E(k)$ 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 $S_j(k)$ 及び係数データ a_{ij} に基づいて取引識別情報 $T(1) \sim T(N)$ 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 $r_k V_s(k)$ 並びに取引識別情報 $T(1) \sim T(N+1)$ 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 $r_{k+1} W_t(k)$ を算出するとともに集計値 $r_{k+1} W_t(k)$ 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 $r_{k+1} W_t(k)$ を復号化処理して集計値 $X_u(k)$ ($u=1,2,\dots,M$) 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 X_u と集計値 $r_k V_s(k)$ 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进行处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 $V_s(k+1)$ ($s=1,2,\dots,M$) 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 $W_t(k)$ ($t=1,2,\dots,M$) 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 $S_j(k)$ ($j=1,2,\dots,P$) 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 $S_j(k)$ 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 $r_{k+1}W_t(k)$ ($t=1,2,\dots,M$) を復号化処理して集計値 $X_u(k)$ ($u=1,2,\dots,M$) 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 10
 サービスを提供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} ($i=1,2,\dots,P; j=1,2,\dots,P$) 及び乱数 r_k ($k=1,2,\dots$) 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 ($j=1,2,\dots,P$) を以下の式 (B) 20

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

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 $S_j(k)$ 及び係数データ a_{ij} に基づいて取引識別情報 $T(1) \sim T(N)$ に関するデータ $E(k)$ の集計値 $E(k)$ 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 $S_j(k)$ 及び係数データ a_{ij} に基づいて取引識別情報 $T(1) \sim T(N)$ 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 $r_kV_s(k)$ 並びに取引識別情報 $T(1) \sim T(N+1)$ 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 $r_{k+1}W_t(k)$ を算出するとともに集計値 $r_{k+1}W_t(k)$ を送信する手段、集計値 $r_kV_s(k)$ とサービス利用装置から送信された集計値 $X_u(k)$ 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。 30

【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提供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 $V_s(k+1)$ ($s=1,2,\dots,M$) 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 $W_t(k)$ ($t=1,2,\dots,M$) 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 $S_j(k)$ ($j=1,2,\dots,P$) 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 (40

10

20

30

40

50

k)を各j毎にkについて集計した結合集計データ $S_j(k)$ を算出するとともに結合集計データ $S_j(k)$ 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 $r_{k+1}W_t(k)$ ($t=1,2,\dots,M$)を復号化処理して集計値 $X_u(k)$ ($u=1,2,\dots,M$)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が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} ($i=1,2,\dots,P; j=1,2,\dots,P$)及び乱数 r_k ($k=1,2,\dots$)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

10

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 $S_j(j=1,2,\dots,P)$ を以下の式(D)

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

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 $S_j(k)$ 及び係数データ a_{ij} に基づいて取引識別情報 $T(1) \sim T(N)$ に関するデータ $E(k)$ の集計値 $E(k)$ 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 $S_j(k)$ 及び係数データ a_{ij} に基づいて取引識別情報 $T(1) \sim T(N)$ に関する回数データ $Q(k)$ の集計値 $Q(k)$ を算出して集計値 $Q(k)$ 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 $S_j(k)$ 及び係数データ a_{ij} に基づいて取引識別情報 $T(1) \sim T(N)$ 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 $r_k V_s(k)$ 並びに取引識別情報 $T(1) \sim T(N+1)$ 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 $r_{k+1} W_t(k)$ を算出するとともに集計値 $r_{k+1} W_t(k)$ を送信する要素集計値算出手段と、集計値 $r_k V_s(k)$ とサービス利用装置から送信された集計値 $X_u(k)$ が矛盾する

20

30

【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が判定するとともに、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 $V_s(k+1)$ ($s=1,2,\dots,M$)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 $W_t(k)$ ($t=1,2,\dots,M$)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

40

50

む $P (P - 2 M + 3)$ 個の値の、サービス利用装置が知らない係数データ $a_{ij} (i=1,2, \dots, P; j=1,2, \dots, P)$ 及び乱数 $r_k (k=1,2, \dots)$ を用いた互いに独立な一次結合データ $S_j (k) (j=1,2, \dots, P)$ を以下の式 (D)

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

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 $S_j (k)$ を算出するとともに結合集計データ $S_j (k)$ 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 $S_j (k)$ 及び係数データ a_{ij} に基づいて取引識別情報 $T (1) \sim T (N)$ に関するデータ $E (k)$ の集計値 $E (k)$ 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 $S_j (k)$ 及び係数データ a_{ij} に基づいて取引識別情報 $T (1) \sim T (N)$ に関する回数データ $Q (k)$ の集計値 $Q (k)$ を算出して集計値 $Q (k)$ 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 $S_j (k)$ 及び係数データ a_{ij} に基づいて取引識別情報 $T (1) \sim T (N)$ 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 $r_k V_s (k)$ 並びに取引識別情報 $T (1) \sim T (N + 1)$ 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 $r_{k+1} W_t$ を算出するとともに集計値 $r_{k+1} W_t (k)$ 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 $r_{k+1} W_t (k)$ を復号化処理して集計値 $X_u (k) (u=1,2, \dots, M)$ 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 X_u と集計値 $r_k V_s (k)$ 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。

【 0 0 2 3 】

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 $V_s (k + 1) (s=1,2, \dots, M)$ 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 $W_t (k) (t=1,2, \dots, M)$ 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 $S_j (k) (j=1,2, \dots, P)$ 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 $S_j (k)$ を算出するとともに結合集計データ $S_j (k)$ 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 $r_{k+1} W_t (k) (t=1,2, \dots, M)$ を復号化処理して集計値 $X_u (k) (u=1,2, \dots, M)$ を生成する手段、として機能させる。

【 0 0 2 4 】

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

10

20

30

40

50

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} ($i=1, 2, \dots, P; j=1, 2, \dots, P$) 及び乱数 r_k ($k=1, 2, \dots$) を用いた互いに独立な一次結合データ S_j ($j=1, 2, \dots, P$) を以下の式 (D)

$$S_j(k) = a_{1j}E(k) + a_{2j}Q(k) + \{a_{(1+2)j}V_1(k) + a_{(2+2)j}V_2(k) + \dots + a_{(M+2)j}V_M(k)\}r_k + \{a_{(M+1+2)j}W_1(k) + a_{(M+2+2)j}W_2(k) + \dots + a_{(2M+2)j}W_M(k)\}r_{k+1} + a_{(2M+3)j}R(k) \cdot \dots \quad (D) \quad 10$$

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 $S_j(k)$ 及び係数データ a_{ij} に基づいて取引識別情報 $T(1) \sim T(N)$ に関するデータ $E(k)$ の集計値 $E(k)$ 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 $S_j(k)$ 及び係数データ a_{ij} に基づいて取引識別情報 $T(1) \sim T(N)$ に関する回数データ $Q(k)$ の集計値 $Q(k)$ を算出して集計値 $Q(k)$ 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 $S_j(k)$ 及び係数データ a_{ij} に基づいて取引識別情報 $T(1) \sim T(N)$ 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 $r_k V_s(k)$ 並びに取引識別情報 $T(1) \sim T(N+1)$ 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 $r_{k+1} W_t(k)$ を算出するとともに集計値 $r_{k+1} W_t(k)$ を送信する手段、集計値 $r_k V_s(k)$ とサービス利用装置から送信された集計値 $X_u(k)$ 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が否かを、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

10

20

30

40

50

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 $V_s(k)$ ($s=1,2,\dots,M$)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 $W_t(k)$ ($t=1,2,\dots,M$)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} ($i=1,2,\dots,P; j=1,2,\dots,P$)及び乱数 r_k ($k=1,2,\dots$)を用いた互いに独立な一次結合データ $S_j(k)$ ($j=1,2,\dots,P$)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 $S_j(k)$ を算出するとともに結合集計データ $S_j(k)$ 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 $S_j(k)$ 及び係数データ a_{ij} に基づいて取引識別情報 $T(1) \sim T(N)$ に関するデータ $E(k)$ の集計値 $E(k)$ を算出しているため、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 $S_j(k)$ をサービス利用装置から得ることができれば、集計値 $E(k)$ 、集計値 $r_k V_s(k)$ 、集計値 $r_{k+1} W_t(k)$ 及び集計値 $R(k)$ 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 $E(k)$ 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 $S_j(k)$ 及び係数データ a_{ij} に基づいて取引識別情報 $T(1) \sim T(N)$ 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 $r_k V_s(k)$ 並びに取引識別情報 $T(1) \sim T(N+1)$ 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 $r_{k+1} W_t(k)$ を算出して、集計値 $r_{k+1} W_t(k)$ をサービス利用装置で復号

10

20

30

40

50

化処理して集計値 $X_U(k)$ 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もなく取引識別情報 $T(1) \sim T(N+1)$ 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 $T(1) \sim T(N)$ に関する要素データと乱数の積の集計値 $r_k V_s(k)$ 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 $V_s(k+1)$ ($s=1, 2, \dots, M$) 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 $W_t(k)$ ($t=1, 2, \dots, M$) 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} ($i=1, 2, \dots, P; j=1, 2, \dots, P$) 及び乱数 r_k ($k=1, 2, \dots$) を用いた互いに独立な一次結合データ $S_j(k)$ ($j=1, 2, \dots, P$) 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 $S_j(k)$ を算出するとともに結合集計データ $S_j(k)$ 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 $S_j(k)$ 及び係数データ a_{ij} に基づいて取引識別情報 $T(1) \sim T(N)$ に関するデータ $E(k)$ の集計値 $E(k)$ を算出しているため、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。また、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 $S_j(k)$ をサービス利用装置から得ることができれば、集計値 $E(k)$ 、集計値 $Q(k)$ 、集計値 $r_k V_s(k)$ 、集計値 $r_{k+1} W_t(k)$ 及び集計値 $R(k)$ 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 $E(k)$ 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 S_j 及び係数データ a_{ij} に基づいて取引識別情報 $T(1) \sim T(N)$ に関する回数データ $Q(k)$ の集計値

10

20

30

40

50

$Q(k)$ を算出して集計値 $Q(k)$ 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、 $Q(1) \sim Q(N)$ までを加算した集計値 $Q(k)$ からサービス取引した最後の回数順が特定されて、次の回数順である $Q(N+1)$ 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のが可能となる。

【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 $V_s(k)$ (k)及び次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 $S_j(k)$ 及び係数データ a_{ij} に基づいて取引識別情報 $T(1) \sim T(N)$ 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 $r_k V_s(k)$ 及び取引識別情報 $T(1) \sim T(N+1)$ 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 $r_{k+1} W_t(k)$ を算出して、集計値 $r_{k+1} W_t(k)$ をサービス利用装置で復号化処理して集計値 $X_u(k)$ 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 $T(1) \sim T(N+1)$ 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 $T(1) \sim T(N)$ に関する要素データと乱数の積の集計値 $r_k V_s(k)$ 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

10

20

30

40

50

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 DB 111 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 DB 111 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。

10

【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

$$x = p \text{ XOR } r$$

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。

20

【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。

30

【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。

40

【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

$$y = x \text{ XOR } q$$

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

50

ド x は、

$$x = p \text{ XOR } r$$

であるので、 $q = p$ ならば、

$$y = x \text{ XOR } q = p \text{ XOR } r \text{ XOR } p = r \cdots (E)$$

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、

$$x \text{ XOR } p = 011000 = r$$

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】

10

20

30

40

50

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る、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。

10

20

30

40

50

【 0 0 5 5 】

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。

【 0 0 5 6 】

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} ($i=1,2, \dots, 2M+2; j=1,2, \dots, 2M+2$)及び乱数発生部127で生成される十分長い乱数の列 r_k ($k=1,2, \dots$)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。

【 0 0 5 7 】

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。

【 0 0 5 8 】

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。

【 0 0 5 9 】

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 $W_t(0)$ ($t=1,2, \dots, M$)、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 ($j=1,2, \dots, 2M+2$)を以下の式(A)

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

により算出する。

【 0 0 6 0 】

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 $E(k)$ ($k=1,2, \dots, N$)、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 $T(k)$ ($k=1,2, \dots, N$)に基づくM個の要素データ $V_s(k)$ ($s=1,2, \dots, M$)及び次回のサービス取引の取引識別情報 $T(k+1)$ ($k=1,2, \dots, N$)に基づいて暗号化処理されたM個の確認情報 $W_t(k)$ ($t=1,2, \dots, M$)、乱数発生部127で発生させた乱数 $R(k)$ ($k=1,2, \dots, N$)、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 $S_j(k)$ ($j=1,2, \dots, 2M+2$)を以下の式(B)

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

10

20

30

40

50

により算出する。

【 0 0 6 1 】

なお、算出する一次結合データ $S_j(k)$ ($j=1,2,\dots,2M+2$) 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 $(P \times 2M+2)$ となるように設定すればよい。そして、それに合わせて係数データ a_{ij} についても、 P^2 個の係数データ a_{ij} ($i=1,2,\dots,P; j=1,2,\dots,P$) に設定すればよい。

【 0 0 6 2 】

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 S_j 及び係数データ a_{ij} に基づいて、取引識別情報 $T(1) \sim T(N)$ に関するデータ $E(k)$ の集計値 $E(k)$ 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 $S_j(k)$ 及び係数データ a_{ij} に基づいて、取引識別情報 $T(1) \sim T(N)$ 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 $V_s(k)$ 並びに取引識別情報 $T(1) \sim T(N+1)$ 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 $r_{k+1} W_t$ を算出して集計値 $r_{k+1} W_t$ をサービス利用装置 2 に送信する。

【 0 0 6 3 】

不正判定部 126 は、集計値 $r_k V_s$ 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 $X_u(k)$ が一致しているか否か判定する。

【 0 0 6 4 】

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} ($s=1,2,\dots,M; t=1,2,\dots,M$) を記憶する係数データ記憶部 230 を記憶している。

【 0 0 6 5 】

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。

【 0 0 6 6 】

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 $T(k+1)$ ($k=1,2,\dots,N$) 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。

【 0 0 6 7 】

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っ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。

10

20

30

40

50

【 0 0 6 8 】

暗号化処理部 2 2 2 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。

$$X = r^p X$$

処理された暗号化取引識別情報を署名処理部 1 2 3 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。

$$r^p X = (r^p X)^q$$

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 2 2 3 では、暗号化処理部 2 2 2 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。

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

ここで、 $p q = 1$ であるから、

$$(r^{pq} X^q) / r = (r X^q) / r = X^q$$

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

$$X^q = X^{qp} = X$$

となって確認することができる。

【 0 0 6 9 】

確認情報処理部 2 2 4 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 $V_s (1)$ ($s=1, 2, \dots, M$) 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 $W_t (0)$ ($t=1, 2, \dots, M$) 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) ($k=1, 2, \dots, N$) に基づいて計算される M 個の要素データ $V_s (k + 1)$ ($s=1, 2, \dots, M$) 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 $W_t (k)$ ($t=1, 2, \dots, M$) を生成する。

【 0 0 7 0 】

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 2 3 0 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)

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

により算出される。

【 0 0 7 1 】

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。

【 0 0 7 2 】

結合集計部 2 2 5 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 $S_j (k)$ 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

10

20

30

40

50

タ $S_j(k)$ 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 $S_j(k)$ は、図10の最下段の式で表される。この式は、集計値 $E(k)$ 、集計値 $r_k V_s(k)$ 、集計値 $r_{k+1} W_t(k)$ 及び集計値 $R(k)$ 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。

10

【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 $S_j(k)$ 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 $E(k)$ 、集計値 $r_k V_s(k)$ 、集計値 $r_{k+1} W_t(k)$ 及び集計値 $R(k)$ 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 $E(k)$ を算出することが可能となる。

【0075】

また、結合集計データ $S_j(k)$ 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。

20

【0076】

ここで集計値 $r_{k+1} W_t(k)$ は取引識別情報 $T(1) \sim T(N)$ 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 $r_k V_s(k)$ 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 $r_k V_s(k)$ を算出する。

【0077】

さらに、集計値算出部125は、集計値 $r_{k+1} W_t(k)$ 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 $r_{k+1} W_t(k)$ を復号化処理して集計値 $X_u(k)$ ($u=1,2,\dots,M$) 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 $r_{k+1} W_t(k)$ が要素データ $V_s(k)$ の各 s 毎の k についての集計値 $r_k V_s(k)$ 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 $r_{k+1} W_t(k)$ 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 $X_u(k)$ を得ることができる。

30

【0078】

要素集計処理部226が算出処理した集計値 $X_u(k)$ は、取引識別情報 $T(1) \sim T(N+1)$ 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 $r_k V_s(k)$ 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 $S_j(k)$ 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 $r_k V_s(k)$ 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 $X_u(k)$ 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。

40

50

【 0 0 7 9 】

要素集計処理部 2 2 6 では、集計値 $V_s(k)$ 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。

【 0 0 8 0 】

図 1 1 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 1 2 8 が記憶されている (S 2 0 0)。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 (S 2 0 1、S 2 0 2) 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 (S 2 0 3)。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 (S 2 0 4)。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 2 2 8 に記憶される (S 2 0 5)。

10

【 0 0 8 1 】

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 2 2 2 で行い (S 2 0 6)、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 2 2 4 で確認情報 $W_t(0)$ を生成する (S 2 0 7)。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 (S 2 0 8)。サービス提供装置 1 では、署名処理部 1 2 3 で暗号化取引識別情報 $T(1)$ に署名処理を行い (S 2 0 9)、結合計算部 1 2 4 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 (S 2 1 0)。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 (S 2 1 1)、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 2 2 3 で処理されて署名入りの取引識別情報 $T(1)$ となり (S 2 1 2)、登録部 2 2 8 に登録され、一次結合データ S_j は登録部 2 2 9 に登録される (S 2 1 2)。

20

【 0 0 8 2 】

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。

30

【 0 0 8 3 】

図 1 2 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 (S 3 0 0、S 3 0 1) 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、署名入りの取引識別情報 $T(k)$ を読み出して (S 3 0 2) 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 (S 3 0 3)。

【 0 0 8 4 】

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 (S 3 0 4) 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 (S 3 0 5)。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 (S 3 0 6)。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 (S 3 0 7)。

40

【 0 0 8 5 】

ステップ S 3 0 5 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 (S 3 0 8) サービス処理は行われぬ。

【 0 0 8 6 】

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、

50

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なっているので、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実際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 $S_j(k)$ 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 S_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 $S_j(k)$ 、係数データ a_{ij} 及び r_k に基づいて、集計値 $E(k)$ 、集計値 $r_k V_s(k)$ 及び集計値 $r_{k+1} W_t(k)$ を算出する (S407)。そして、集計値 $r_k V_s(k)$ 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 $r_{k+1} W_t(k)$ 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 $r_{k+1} W_t(k)$ に基づいて集計値 $X_u(k)$ を算出処理し (S410)、算出された集計値 $X_u(k)$ 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 $X_u(k)$ 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

10

20

30

40

50

）、一致する場合には正しく集計されたものとして集計値 $E(k)$ 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 (S 4 1 3)。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 (S 4 1 4)。

【0095】

ステップ S 4 1 2 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 (S 4 1 5)。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 $b_{s,t}$ 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。

10

【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 2 2 4 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。

20

【0098】

図 1 4 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)

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

30

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)

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

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。

40

【0099】

図 1 5 から図 1 7 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 1 1 から図 1 3 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 1 5 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 (S 5 0 6) その要素データ $V_s(0)$ を生成して (S 5 0 7) 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 (

50

S 5 0 8)。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 (S 5 0 9) 登録部 2 2 9 に登録される (S 5 1 0)。

【0 1 0 1】

サービス取引を行う場合の処理に関するフローでは、図 1 6 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 (S 6 1 0)。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 (S 6 1 5)。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 (S 6 1 6) 登録部 2 2 9 に登録される (S 6 1 8)。

【0 1 0 2】

利用料金等の集計処理に関するフローでは、図 1 7 に示すように、結合集計データ $S_j(k)$ の算出処理後最後のサービス取引で利用した取引識別情報 $T(N)$ を読み出して (S 7 0 4) その要素データ $V_s(N)$ を生成し (S 7 0 5) 結合集計データ $S_j(k)$ 及び $V_s(N)$ をサービス提供装置 1 に送信する (S 7 0 6)。サービス提供装置 1 では、結合集計データ $S_j(k)$ を用いて、集計値 $E(k)$ 、集計値 $r_k V_s(k)$ 及び集計値 $r_k W_t(k-1)$ を算出して (S 7 0 7)、集計値 $r_k V_s(k)$ から $r_N V_s(N)$ を減算処理し (S 7 0 8)、集計値 $r_k W_t(k-1)$ をサービス利用装置 2 に送信する (S 7 0 9)。サービス利用装置 2 では、集計値 $r_k W_t(k-1)$ から集計値 $X_u(k-1)$ を算出して (S 7 1 0) サービス提供装置 1 に送信し (S 7 1 1)、サービス提供装置 1 では、ステップ S 7 0 8 で算出した集計値と集計値 $X_u(k-1)$ とが一致しているか判定して (S 7 1 2) 不正判定を行う。

【0 1 0 3】

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。

【0 1 0 4】

図 1 8 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。

【0 1 0 5】

サービス提供装置 1 の情報処理部 1 0 は、取引識別情報生成部 1 2 0、取引識別情報判定部 1 2 1、サービス処理部 1 2 2、署名処理部 1 2 3、結合計算部 1 2 4、集計値算出部 1 2 5、不正判定部 1 2 6 及び乱数発生部 1 2 7 を備えており、こうした機能は、記憶部 1 1 に記憶されたサービス提供プログラム 1 1 0 により実現される。

【0 1 0 6】

記憶部 1 1 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 1 2 8、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} ($i=1, 2, \dots, 2M+3; j=1, 2, \dots, 2M+3$) 及び十分多い乱数の列 r_k ($k=1, 2, \dots$) を記憶する係数データ記憶部 1 2 9 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 1 2 7 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。

【0 1 0 7】

取引識別情報生成部 1 2 0 及びサービス処理部 1 2 2 は、上述の実施形態と同様の機能を備えている。

【0 1 0 8】

結合計算部 1 2 4 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 $W_t(0)$ ($t=1, 2, \dots, M$)、乱数発生部 1 2 7 で発生させた乱数 $R(0)$ 、係数データ記憶部 1 2 9 に記憶された

10

20

30

40

50

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 $S_j(0)$ ($j=1,2, \dots, 2M+3$) を以下の式 (I)

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

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 $E(k)$ ($k=1,2, \dots, N$)、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 $Q(k)$ ($k=1,2, \dots, N$)、今回のサービス取引の取引識別情報 $T(k)$ ($k=1,2, \dots, N$) に基づく M 個の要素データ $V_s(k)$ ($s=1,2, \dots, M$)、次回のサービス取引の取引識別情報 $T(k+1)$ ($k=1,2, \dots, N$) に基づいて暗号化処理された M 個の確認情報 $W_t(k)$ ($t=1,2, \dots, M$)、乱数発生部 127 で発生させた乱数 $R(k)$ ($k=1,2, \dots, N$) 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 $S_j(k)$ ($j=1,2, \dots, 2M+3$) を以下の式 (J)

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

により算出する。

【0110】

なお、算出する一次結合データ $S_j(k)$ ($j=1,2, \dots, 2M+2$) 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 $(2M+3)$ 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} ($i=1,2, \dots, P; j=1,2, \dots, P$) 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 $S_j(k)$ 及び係数データ a_{ij} に基づいて、取引識別情報 $T(1) \sim T(N)$ に関するデータ $E(k)$ の集計値 $E(k)$ 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 $S_j(k)$ 及び係数データ a_{ij} に基づいて取引識別情報 $T(1) \sim T(N)$ に関する回数データ $Q(k)$ の集計値 $Q(k)$ 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 $S_j(k)$ 及び係数データ a_{ij} に基づいて取引識別情報 $T(1) \sim T(N)$ 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 $r_k V_s$ 並びに取引識別情報 $T(1) \sim T(N+1)$ に関する初期確認情報と乱数の積 $r_1 W_t(0)$ 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 $r_{k+1} W_t(k)$ を算出して集計値 $r_{k+1} W_t(k)$ 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 $Q(k)$ 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 $r_k V_s(k)$ 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 $X_u(k)$ 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

10

20

30

40

50

別情報のリスト 2 2 7、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 2 2 8、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 (2 M + 3) 個の一次結合データ $S_j(k)$ を記憶する登録部 2 2 9、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 2 3 0 を記憶している。

【 0 1 1 4 】

取引識別情報取得部 2 2 0 は、上述の実施形態と同様の機能を備えている。

【 0 1 1 5 】

識別データ生成部 2 3 1 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。

10

【 0 1 1 6 】

暗号化処理部 2 2 2 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 2 2 3 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 2 2 8 に記憶する。

20

【 0 1 1 7 】

暗号化処理部 2 2 2 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 1 2 3 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 2 2 3 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。

【 0 1 1 8 】

確認情報処理部 2 2 4 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。

30

【 0 1 1 9 】

結合集計部 2 2 5 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 $S_j(k)$ 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 $S_j(k)$ 、要素データ $V_s(N+1)$ 及び回数データ Q (N + 1) を送信する。

40

【 0 1 2 0 】

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 1 9 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 $S_j(k)$ は、図 1 9 の最下段の式で求められる。この式は、集計値 $E(k)$ 、集計値 $Q(k)$ 、集計値 $r_k V_s(k)$ 、集計値 $r_{k+1} W_t(k)$ 及び集計値 $R(k)$ の (2 M + 3) 個のデータを変数として係数データ a_{ij} を用いた (2 M + 3) 個の連立一次方程式となっている。

50

【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 $S_j(k)$ 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 $E(k)$ 、集計値 $Q(k)$ 、集計値 $r_k V_s(k)$ 、集計値 $r_{k+1} W_t(k)$ 及び集計値 $R(k)$ 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 $E(k)$ を算出することが可能となる。

【0122】

また、一次結合データ $S_j(k)$ 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。

10

【0123】

不正判定部126は、集計値 $Q(k)$ を用いて不正判定を行う場合には、集計値 $Q(k)$ が取引識別情報 $T(1) \sim T(N)$ 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 $(N+1)$ となっており、集計値は1から N までの整数を連続して加算した値 $N \cdot (N+1) / 2$ となるが、集計値算出部125から得られた集計値 $Q(k)$ 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。

20

【0124】

不正判定部126で集計値 $r_k V_s(k)$ 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 $T(1) \sim T(N)$ 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 $r_k V_s(k)$ に対して、集計値 $r_{k+1} W_t(k)$ は、取引識別情報 $T(1) \sim T(N)$ 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 $r_k V_s(k)$ 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 $T(1) \sim T(N+1)$ に関する集計値を算出する。

30

【0125】

そして、集計値算出部125は、集計値 $r_{k+1} W_t(k)$ 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 $X_u(k)$ を算出し、算出処理した集計値 $X_u(k)$ が、取引識別情報 $T(1) \sim T(N+1)$ 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 $r_k V_s(k)$ 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が判定することで、不正操作が行われたか否かを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 $S_j(k)$ 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 $r_k V_s(k)$ 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 $X_u(k)$ 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。

40

【0126】

要素集計処理部226では、集計値 $r_k V_s(k)$ 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

50

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、サービス利用装置 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】

10

20

30

40

50

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 $S_j(k)$ 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)。

10

【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なっているので、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】

20

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)。

30

【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 $S_j(k)$ 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 $S_j(k)$ 、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 S_j 及び係数データ a_{ij} に基づいて、集計値 $E(k)$ 、集計値 $Q(k)$ 、集計値 $r_k V_s(k)$ 及び集計値 $r_{k+1} W_t(k)$ を算出する (S1008)。そして、算出された集計値 $Q(k)$ 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 $r_k V_s(k)$ 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 $r_{k+1} W_t(k)$ は、サービス利用装置 2 に送信する (S1011)。

40

【0141】

サービス利用装置 2 は、集計値 $r_{k+1} W_t(k)$ に基づいて集計値 $X_u(k)$ を算出処理し (S1012)、算出された集計値 $X_u(k)$ をサービス提供装置 1 に送信する (S1013)。

【0142】

50

サービス提供装置 1 は、送信された集計値 $X_u(k)$ とステップ S 1 0 1 0 で算出した集計値が一致するか判定し (S 1 0 1 4)、一致する場合には正しく集計されたものとして集計値 $E(k)$ 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 (S 1 0 1 5)。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 (S 1 0 1 6)。

【0143】

ステップ S 1 0 0 9 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 1 0 1 4 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 (S 1 0 1 7)。

【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、よりの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言い、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、今後ユキキュピタス・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。

10

20

30

40

50

【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。

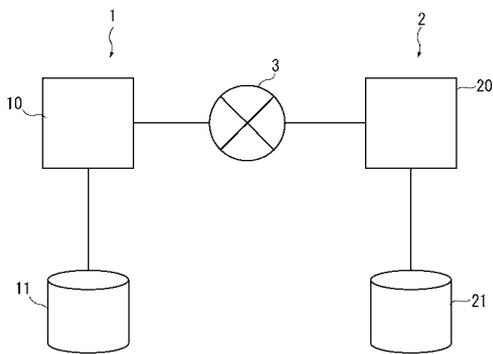
【符号の説明】

【0149】

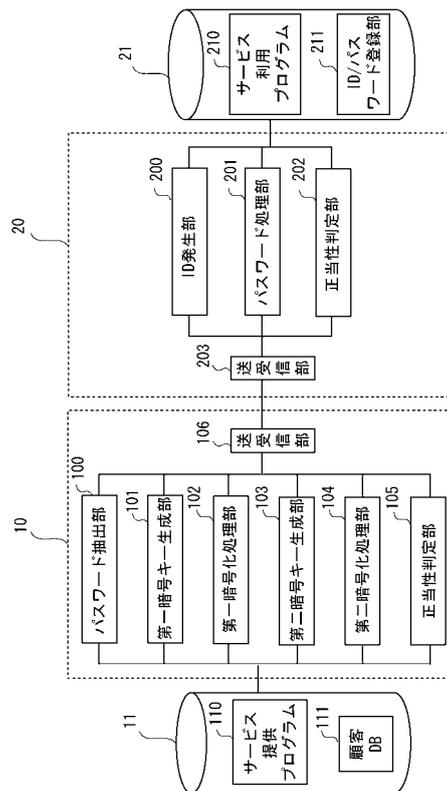
- 1 サービス提供装置
- 2 サービス利用装置
- 3 ネットワーク
- 10 情報処理部
- 11 記憶部
- 20 情報処理部
- 21 記憶部

10

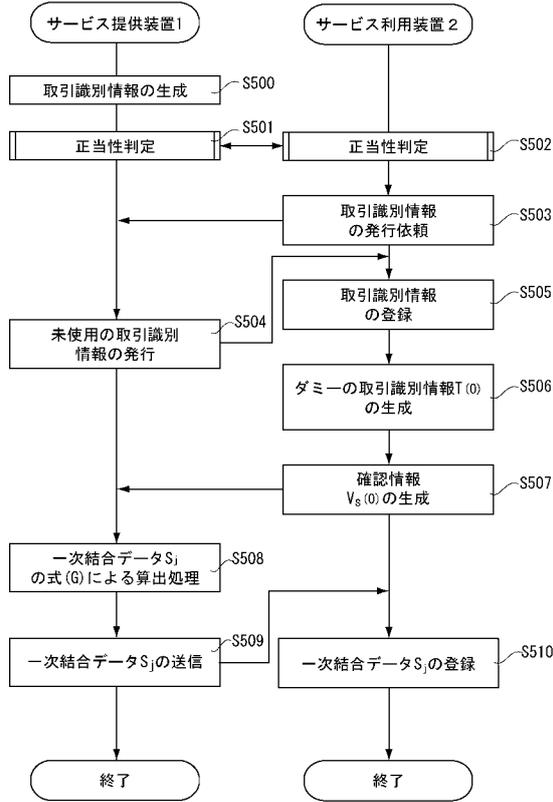
【図1】



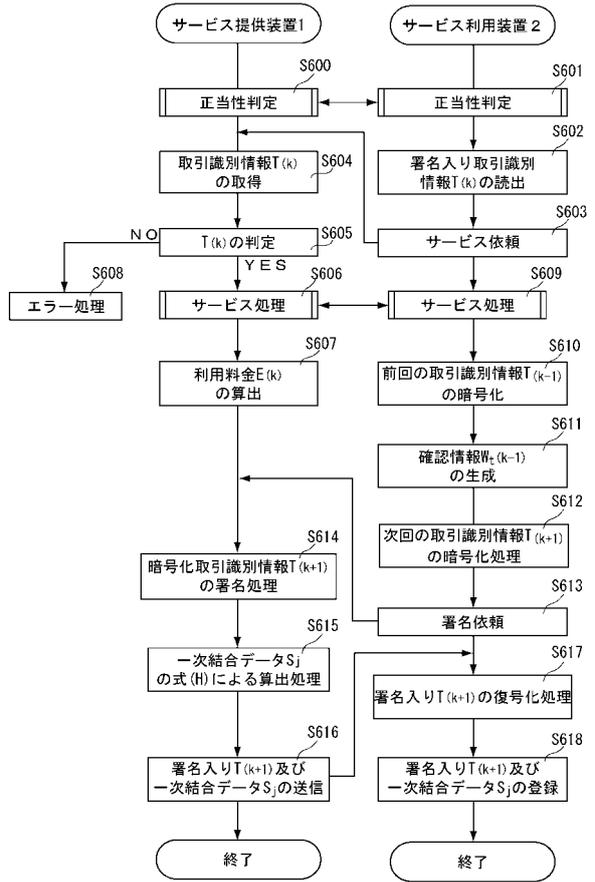
【図2】



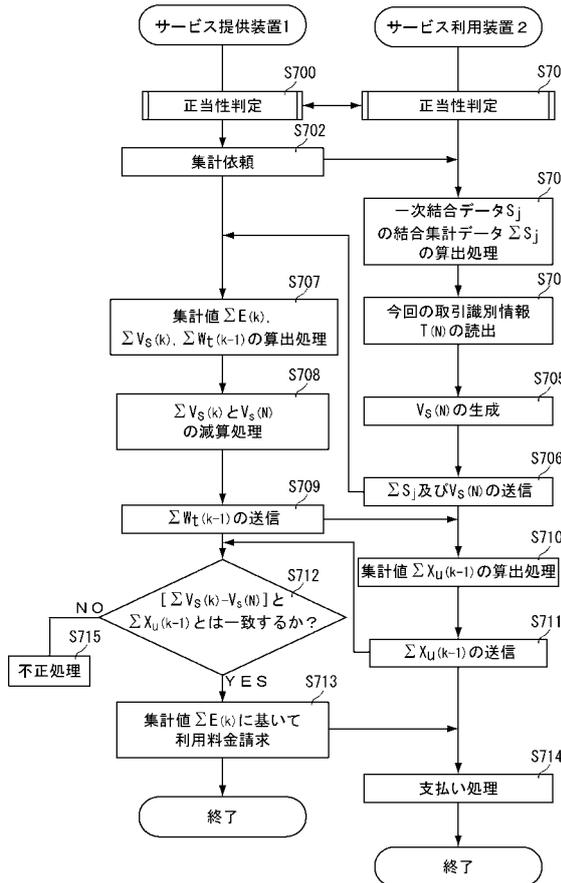
【図15】



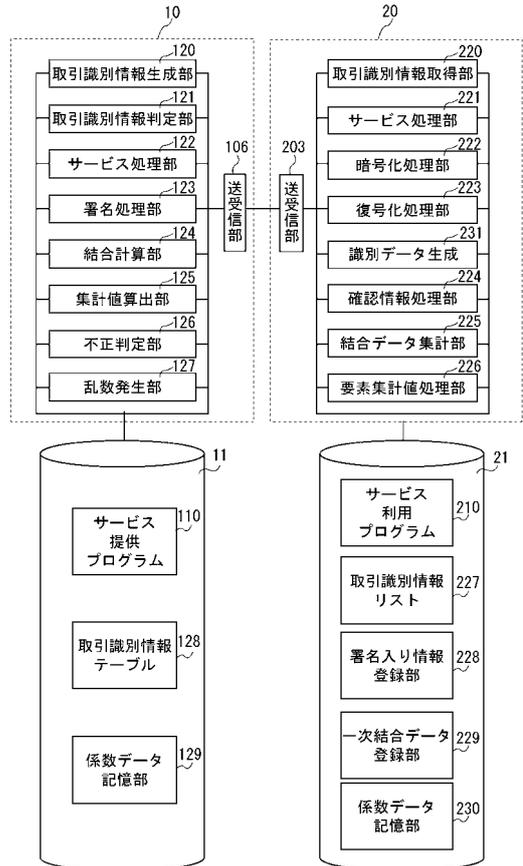
【図16】



【図17】



【図18】



フロントページの続き

- (56)参考文献 特開2006-279595(JP,A)
米国特許出願公開第2004/0122767(US,A1)
Shinsuke Tamura, Tatsuro Yanase, Information Sharing among Untrustworthy Entities” ,
電気学会論文誌C 電子・情報・システム部門誌, 2005年11月 1日, vol. 125, no. 11
, pp. 1767-1772

- (58)調査した分野(Int.Cl., DB名)
H04L 9/32
G06Q 30/00