

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号
特開2003-46500
(P2003-46500A)

(43) 公開日 平成15年2月14日 (2003.2.14)

(51) Int.Cl. ⁷	識別記号	F I	テマコード* (参考)
H 0 4 L 9/32		G 0 6 F 15/00	3 3 0 B 5 B 0 8 5
G 0 6 F 15/00	3 3 0	G 0 9 C 1/00	6 4 0 Z 5 J 1 0 4
G 0 9 C 1/00	6 4 0	H 0 4 L 9/00	6 7 5 D
			6 7 5 B
			6 7 3 C
審査請求 有 請求項の数50 O L (全 25 頁)			

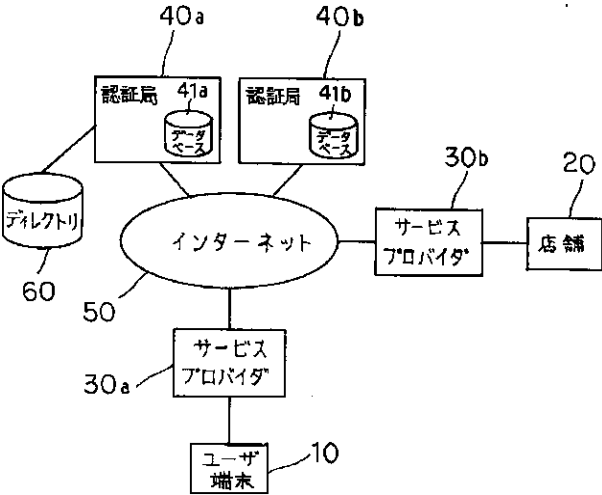
(21) 出願番号	特願2001-236726 (P2001-236726)	(71) 出願人	000004237 日本電気株式会社 東京都港区芝五丁目7番1号
(22) 出願日	平成13年8月3日 (2001.8.3)	(72) 発明者	田嶋 優一 東京都港区芝五丁目7番1号 日本電気株式会社内
		(72) 発明者	千葉 胤明 東京都港区芝五丁目7番1号 日本電気株式会社内
		(74) 代理人	100088328 弁理士 金田 暢之 (外2名)
		最終頁に続く	

(54) 【発明の名称】 個人情報管理システム及び個人情報管理方法、並びに情報処理サーバ

(57) 【要約】

【課題】 インターネットに接続可能な領域に登録された個人情報のセキュリティ性を向上させる。

【解決手段】 ユーザ端末10のユーザが個人情報を認証局40aに提出すると、認証局40aにおいて、提出された個人情報を2つのデータ片に分割し、一方のデータ片を、認証局40aが具備するデータベース41aに登録し、他方のデータ片を、認証局40bに送信し、認証局40bが具備するデータベース41bに登録する。その後、個人情報の取得が要求された場合、認証局40aにおいて、認証局40bからデータベース41bに登録されたデータ片を取得し、データベース41aに登録されたデータ片と認証局40bから取得したデータ片とを結合し、個人情報を復元する。



【特許請求の範囲】

【請求項1】 インターネットに接続可能な少なくとも1つの端末と、前記インターネットに接続可能な領域に登録される個人情報を公開鍵方式によって証明するとともに前記個人情報を前記領域に登録し、前記公開鍵方式によって証明される要求に対して前記個人情報を前記要求を送信した端末に送信する認証手段とを少なくとも有してなる個人情報管理システムにおいて、

前記認証手段は、前記個人情報を複数のデータに分割し、該複数のデータのうち少なくとも1つのデータを当該認証手段が具備するデータベースに登録し、他のデータを当該認証手段とは異なる管理下の前記インターネットに接続可能な他の領域に登録し、前記公開鍵方式によって証明される、前記個人情報を取得する要求が前記端末から送信されてきた場合、前記分割された複数のデータを結合して前記個人情報を復元し、該個人情報を、前記要求を送信した端末に送信することを特徴とする個人情報管理システム。

【請求項2】 請求項1に記載の個人情報管理システムにおいて、
前記認証手段は、前記他のデータの登録先を示すリンク情報を保持し、前記要求が送信されてきた場合、前記リンク情報に基づいて前記他のデータの登録先を認識することを特徴とする個人情報管理システム。

【請求項3】 請求項1に記載の個人情報管理システムにおいて、
前記認証手段は、当該認証手段が具備するデータベースに登録されるデータに前記他のデータの登録先を示すリンク情報を付与することを特徴とする個人情報管理システム。

【請求項4】 請求項1に記載の個人情報管理システムにおいて、
前記認証手段は、前記個人情報を予め決められた固定長毎に複数のデータに分割し、分割された複数のデータを決められた配列方法によって少なくとも2つのデータ片とし、該データ片毎に、当該認証手段が具備するデータベースあるいは前記他の領域に登録することを特徴とする個人情報管理システム。

【請求項5】 請求項1に記載の個人情報管理システムにおいて、
前記認証手段は、前記個人情報を互いに等しい任意長毎に複数のデータに分割し、分割された複数のデータを決められた配列方法によって少なくとも2つのデータ片とし、該データ片毎に、当該認証手段が具備するデータベースあるいは前記他の領域に登録することを特徴とする個人情報管理システム。

【請求項6】 請求項1に記載の個人情報管理システムにおいて、
前記認証手段は、前記個人情報を互いに異なる任意長毎に複数のデータに分割し、分割された複数のデータを決

められた配列方法によって少なくとも2つのデータ片とし、該データ片毎に、当該認証手段が具備するデータベースあるいは前記他の領域に登録することを特徴とする個人情報管理システム。

【請求項7】 請求項4乃至6のいずれか1項に記載の個人情報管理システムにおいて、
前記認証手段は、前記データ片毎に、前記個人情報の分割方法及び配列方法に関する情報を付与することを特徴とする個人情報管理システム。

10 【請求項8】 請求項4乃至7のいずれか1項に記載の個人情報管理システムにおいて、
前記認証手段は、前記個人情報を暗号化し、該暗号化した個人情報及び暗号化に用いた暗号鍵を複数のデータに分割することを特徴とする個人情報管理システム。

【請求項9】 請求項4乃至8のいずれか1項に記載の個人情報管理システムにおいて、
前記認証手段は、前記データ片をそれぞれ暗号化することを特徴とする個人情報管理システム。

20 【請求項10】 インターネットに接続可能な少なくとも1つの端末と、前記インターネットに接続可能な領域に登録される個人情報を公開鍵方式によって証明するとともに前記個人情報を前記領域に登録し、前記公開鍵方式によって証明される要求に対して前記個人情報を前記要求を送信した端末に送信する認証手段とを少なくとも有してなる個人情報管理システムにおいて、
前記認証手段は、前記個人情報を複数のデータに分割し、該複数のデータを互いに異なる管理下の前記インターネットに接続可能な領域に登録するとともに、前記複数のデータの登録先を示すリンク情報を保持し、前記公開鍵方式によって証明される、前記個人情報を取得する要求が前記端末から送信されてきた場合、前記分割された複数のデータを前記リンク情報に基づいて取得し、取得した複数のデータを結合して前記個人情報を復元し、該個人情報を、前記要求を送信した端末に送信することを特徴とする個人情報管理システム。

30 【請求項11】 請求項1乃至10のいずれか1項に記載の個人情報管理システムにおいて、
前記他の領域のうち少なくとも1つは、前記インターネットに接続可能な領域に登録される個人情報を公開鍵方式によって証明する他の認証手段であることを特徴とする個人情報管理システム。

40 【請求項12】 インターネットに接続可能な少なくとも1つの端末と、該端末の前記インターネットへの接続を執り行うサービスプロバイダと、前記インターネットに接続可能な領域に登録される個人情報を公開鍵方式によって証明する認証手段とを少なくとも有してなる個人情報管理システムにおいて、
前記サービスプロバイダは、前記個人情報を複数のデータに分割し、該複数のデータのうち少なくとも1つのデータを当該サービスプロバイダが具備するデータベース

に登録し、他のデータを前記認証手段が具備するデータベースを含む、当該サービスプロバイダとは異なる管理下の前記インターネットに接続可能な他の領域に登録し、前記公開鍵方式によって証明される、前記個人情報を取得する要求が前記端末から送信されてきた場合、前記分割された複数のデータを結合して前記個人情報を復元し、該個人情報を、前記要求を送信した端末に送信することを特徴とする個人情報管理システム。

【請求項13】 請求項12に記載の個人情報管理システムにおいて、前記サービスプロバイダは、前記他のデータの登録先を示すリンク情報を保持し、前記要求が送信されてきた場合、前記リンク情報に基づいて前記他のデータの登録先を認識することを特徴とする個人情報管理システム。

【請求項14】 請求項12に記載の個人情報管理システムにおいて、前記サービスプロバイダは、当該サービスプロバイダが具備するデータベースに登録されるデータに前記他のデータの登録先を示すリンク情報を付与することを特徴とする個人情報管理システム。

【請求項15】 請求項12に記載の個人情報管理システムにおいて、前記サービスプロバイダは、前記個人情報を予め決められた固定長毎に複数のデータに分割し、分割された複数のデータを決められた配列方法によって少なくとも2つのデータ片とし、該データ片毎に、当該サービスプロバイダが具備するデータベースあるいは前記他の領域に登録することを特徴とする個人情報管理システム。

【請求項16】 請求項12に記載の個人情報管理システムにおいて、前記サービスプロバイダは、前記個人情報を互いに等しい任意長毎に複数のデータに分割し、分割された複数のデータを決められた配列方法によって少なくとも2つのデータ片とし、該データ片毎に、当該サービスプロバイダが具備するデータベースあるいは前記他の領域に登録することを特徴とする個人情報管理システム。

【請求項17】 請求項12に記載の個人情報管理システムにおいて、前記サービスプロバイダは、前記個人情報を互いに異なる任意長毎に複数のデータに分割し、分割された複数のデータを決められた配列方法によって少なくとも2つのデータ片とし、該データ片毎に、当該サービスプロバイダが具備するデータベースあるいは前記他の領域に登録することを特徴とする個人情報管理システム。

【請求項18】 請求項15乃至17のいずれか1項に記載の個人情報管理システムにおいて、前記サービスプロバイダは、前記データ片毎に、前記個人情報の分割方法及び配列方法に関する情報を付与することを特徴とする個人情報管理システム。

【請求項19】 請求項15乃至18のいずれか1項に

記載の個人情報管理システムにおいて、前記サービスプロバイダは、前記個人情報を暗号化し、該暗号化した個人情報及び暗号化に用いた暗号鍵を複数のデータに分割することを特徴とする個人情報管理システム。

【請求項20】 請求項15乃至19のいずれか1項に記載の個人情報管理システムにおいて、前記サービスプロバイダは、前記データ片をそれぞれ暗号化することを特徴とする個人情報管理システム。

10 【請求項21】 インターネットに接続可能な少なくとも1つの端末と、該端末の前記インターネットへの接続を執り行うサービスプロバイダと、前記インターネットに接続可能な領域に登録される個人情報を公開鍵方式によって証明する認証手段とを少なくとも有してなる個人情報管理システムにおいて、前記サービスプロバイダは、前記個人情報を複数のデータに分割し、該複数のデータを互いに異なる管理下の前記インターネットに接続可能な領域に登録するとともに、前記複数のデータの登録先を示すリンク情報を保持し、前記公開鍵方式によって証明される、前記個人情報を取得する要求が前記端末から送信されてきた場合、前記分割された複数のデータを前記リンク情報に基づいて取得し、取得した複数のデータを結合して前記個人情報を復元し、該個人情報を、前記要求を送信した端末に送信することを特徴とする個人情報管理システム。

20 【請求項22】 インターネットに接続可能な領域に個人情報を登録し、公開鍵方式によって証明される、前記個人情報を取得する要求が出された場合に、前記個人情報を前記要求元に送信する個人情報管理方法であって、30 前記個人情報を複数のデータに分割し、分割された複数のデータを少なくとも2つのデータ片とし、該データ片毎に互いに異なる管理下の領域に登録し、前記要求が出された場合、前記分割された複数のデータを結合して前記個人情報を復元し、該個人情報を前記要求元に送信することを特徴とする個人情報管理方法。

【請求項23】 請求項22に記載の個人情報管理方法において、前記データ片が登録される領域のうち1つの領域において、他のデータ片の登録先を示すリンク情報を保持しておき、前記要求が出された場合、前記リンク情報に基づいて前記他のデータ片の登録先を認識することを特徴とする個人情報管理方法。

40 【請求項24】 請求項22に記載の個人情報管理方法において、前記データ片に、他のデータ片の登録先を示すリンク情報を付与しておき、前記要求が出された場合、前記リンク情報に基づいて前記他のデータ片の登録先を認識することを特徴とする個人情報管理方法。

50 【請求項25】 請求項22に記載の個人情報管理方法において、

前記個人情報を予め決められた固定長毎に複数のデータに分割することを特徴とする個人情報管理方法。

【請求項26】 請求項22に記載の個人情報管理方法において、

前記個人情報を互いに等しい任意長毎に複数のデータに分割することを特徴とする個人情報管理方法。

【請求項27】 請求項22に記載の個人情報管理方法において、

前記個人情報を互いに異なる任意長毎に複数のデータに分割することを特徴とする個人情報管理方法。

【請求項28】 請求項25乃至27のいずれか1項に記載の個人情報管理方法において、

前記データ片毎に、前記個人情報の分割方法に関する情報を付与することを特徴とする個人情報管理方法。

【請求項29】 請求項25乃至28のいずれか1項に記載の個人情報管理方法において、

前記個人情報を暗号化し、該暗号化した個人情報及び暗号化に用いた暗号鍵を複数のデータに分割することを特徴とする個人情報管理方法。

【請求項30】 請求項25乃至29のいずれか1項に記載の個人情報管理方法において、

前記データ片をそれぞれ暗号化することを特徴とする個人情報管理方法。

【請求項31】 インターネットに接続可能な領域に登録される個人情報を公開鍵方式によって証明するとともに前記個人情報を前記領域に登録し、前記公開鍵方式によって証明される要求に対して前記個人情報を前記要求元に送信する認証手段内に設けられた情報処理サーバであって、

前記個人情報を複数のデータに分割し、該複数のデータのうち少なくとも1つのデータを前記認証手段が具備するデータベースに登録し、他のデータを前記認証手段とは異なる管理下の前記インターネットに接続可能な他の領域に登録し、前記公開鍵方式によって証明される、前記個人情報を取得する要求が送信されてきた場合、前記分割された複数のデータを結合して前記個人情報を復元し、該個人情報を前記要求元に送信することを特徴とする情報処理サーバ。

【請求項32】 請求項31に記載の情報処理サーバにおいて、

前記他のデータの登録先を示すリンク情報を保持し、前記要求が送信されてきた場合、前記リンク情報に基づいて前記他のデータの登録先を認識することを特徴とする情報処理サーバ。

【請求項33】 請求項31に記載の情報処理サーバにおいて、

前記認証手段が具備するデータベースに登録されるデータに前記他のデータの登録先を示すリンク情報を付与することを特徴とする情報処理サーバ。

【請求項34】 請求項31に記載の情報処理サーバに

おいて、

前記個人情報を予め決められた固定長毎に複数のデータに分割し、分割された複数のデータを決められた配列方法によって少なくとも2つのデータ片とし、該データ片毎に、前記認証手段が具備するデータベースあるいは前記他の領域に登録することを特徴とする情報処理サーバ。

【請求項35】 請求項31に記載の情報処理サーバにおいて、

10 前記個人情報を互いに等しい任意長毎に複数のデータに分割し、分割された複数のデータを決められた配列方法によって少なくとも2つのデータ片とし、該データ片毎に、前記認証手段が具備するデータベースあるいは前記他の領域に登録することを特徴とする情報処理サーバ。

【請求項36】 請求項31に記載の情報処理サーバにおいて、

前記個人情報を互いに異なる任意長毎に複数のデータに分割し、分割された複数のデータを決められた配列方法によって少なくとも2つのデータ片とし、該データ片毎に、前記認証手段が具備するデータベースあるいは前記他の領域に登録することを特徴とする情報処理サーバ。

【請求項37】 請求項34乃至36のいずれか1項に記載の情報処理サーバにおいて、

前記データ片毎に、前記個人情報の分割方法及び配列方法に関する情報を付与することを特徴とする情報処理サーバ。

【請求項38】 請求項34乃至37のいずれか1項に記載の情報処理サーバにおいて、

30 前記個人情報を暗号化し、該暗号化した個人情報及び暗号化に用いた暗号鍵を複数のデータに分割することを特徴とする情報処理サーバ。

【請求項39】 請求項34乃至38のいずれか1項に記載の情報処理サーバにおいて、

前記データ片をそれぞれ暗号化することを特徴とする情報処理サーバ。

【請求項40】 インターネットに接続可能な領域に登録される個人情報を公開鍵方式によって証明するとともに前記個人情報を前記領域に登録し、前記公開鍵方式によって証明される要求に対して前記個人情報を前記要求元に送信する認証手段内に設けられた情報処理サーバであって、

40 前記個人情報を複数のデータに分割し、該複数のデータを互いに異なる管理下の前記インターネットに接続可能な領域に登録するとともに、前記複数のデータの登録先を示すリンク情報を保持し、前記公開鍵方式によって証明される、前記個人情報を取得する要求が前記端末から送信されてきた場合、前記分割された複数のデータを前記リンク情報に基づいて取得し、取得した複数のデータを結合して前記個人情報を復元し、該個人情報を、前記要求を送信した端末に送信することを特徴とする情報処

理サーバ。

【請求項41】 インターネットに接続可能な端末の前記インターネットへの接続を執り行うサービスプロバイダ内に設けられた情報処理サーバであって、前記個人情報を複数のデータに分割し、該複数のデータのうち少なくとも1つのデータを前記サービスプロバイダが具備するデータベースに登録し、他のデータを、前記インターネット上に登録される個人情報を公開鍵方式によって証明する認証手段が具備するデータベースを含む、前記サービスプロバイダとは異なる管理下の前記インターネットに接続可能な領域に登録し、前記公開鍵方式によって証明される、前記個人情報を取得する要求が前記端末から送信されてきた場合、前記分割された複数のデータを結合して前記個人情報を復元し、該個人情報を、前記要求を送信した端末に送信することを特徴とする情報処理サーバ。

【請求項42】 請求項41に記載の情報処理サーバにおいて、前記他のデータの登録先を示すリンク情報を保持し、前記要求が送信されてきた場合、前記リンク情報に基づいて前記他のデータの登録先を認識することを特徴とする情報処理サーバ。

【請求項43】 請求項41に記載の情報処理サーバにおいて、前記サービスプロバイダが具備するデータベースに登録されるデータに前記他のデータの登録先を示す情報を付与することを特徴とする情報処理サーバ。

【請求項44】 請求項41に記載の情報処理サーバにおいて、前記個人情報を予め決められた固定長毎に複数のデータに分割し、分割された複数のデータを決められた配列方法によって少なくとも2つのデータ片とし、該データ片毎に、前記サービスプロバイダが具備するデータベースあるいは前記他の領域に登録することを特徴とする情報処理サーバ。

【請求項45】 請求項41に記載の情報処理サーバにおいて、前記個人情報を互いに等しい任意長毎に複数のデータに分割し、分割された複数のデータを決められた配列方法によって少なくとも2つのデータ片とし、該データ片毎に、前記サービスプロバイダが具備するデータベースあるいは前記他の領域に登録することを特徴とする情報処理サーバ。

【請求項46】 請求項41に記載の情報処理サーバにおいて、前記個人情報を互いに異なる任意長毎に複数のデータに分割し、分割された複数のデータを決められた配列方法によって少なくとも2つのデータ片とし、該データ片毎に、前記サービスプロバイダが具備するデータベースあるいは前記他の領域に登録することを特徴とする情報処

理サーバ。

【請求項47】 請求項44乃至46のいずれか1項に記載の情報処理サーバにおいて、前記データ片毎に、前記個人情報の分割方法及び配列方法に関する情報を付与することを特徴とする情報処理サーバ。

【請求項48】 請求項44乃至47のいずれか1項に記載の情報処理サーバにおいて、前記個人情報を暗号化し、該暗号化した個人情報及び暗号化に用いた暗号鍵を複数のデータに分割することを特徴とする情報処理サーバ。

【請求項49】 請求項44乃至48のいずれか1項に記載の情報処理サーバにおいて、前記データ片をそれぞれ暗号化することを特徴とする情報処理サーバ。

【請求項50】 インターネットに接続可能な端末の前記インターネットへの接続を執り行うサービスプロバイダ内に設けられた情報処理サーバであって、前記個人情報を複数のデータに分割し、該複数のデータを互いに異なる管理下の前記インターネットに接続可能な領域に登録するとともに、前記複数のデータの登録先を示すリンク情報を保持し、前記公開鍵方式によって証明される、前記個人情報を取得する要求が前記端末から送信されてきた場合、前記分割された複数のデータを前記リンク情報に基づいて取得し、取得した複数のデータを結合して前記個人情報を復元し、該個人情報を、前記要求を送信した端末に送信することを特徴とする情報処理サーバ。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、インターネットに接続可能な領域に個人情報を管理する個人情報管理システム及び個人情報管理方法に関する。

【0002】

【従来の技術】昨今、インターネットやパソコンが急速に普及し、個人が時間や場所を問わずにインターネットに接続することが容易に行われるようになってきている。また、それに伴い、インターネット上にホームページを開設し、このホームページを用いて情報を提供したり、商品等を販売したりする企業団体等が急速に増加している。

【0003】例えば、ホームページを用いての商品等の販売、いわゆるオンラインショッピングにおいては、商品やサービス等を家庭等にて容易に購入することができるため、その利用者は増加傾向にある。

【0004】一般的なオンラインショッピングにおいては、ユーザが商品等を購入する場合、まず、パソコン等の端末に表示される商品やサービス等の中からユーザが所望の商品あるいはサービスを選択して購入を決定し、その後、ユーザの氏名や住所、電話番号、E-mail

アドレス等からなる顧客情報を入力するとともに、代金の支払い方法を選択する。

【0005】上記の方法にて決定された購入商品や支払い方法、並びに顧客情報の内容をユーザが確認した後、商品等の発注がかけられる。

【0006】図13は、一般的なオンラインショッピングシステムの一例を示す図である。

【0007】本従来例は図13に示すように、インターネット550に接続可能なユーザ端末510と、ユーザ端末510が加入し、ユーザ端末510のインターネット550への接続を執り行うサービスプロバイダ530aと、インターネット550に接続可能に構成される端末（不図示）とユーザ端末510のユーザに関する個人情報登録されたデータベース521とを具備し、商品等を販売する店舗520と、店舗520が加入し、店舗520の端末のインターネット550への接続を執り行うサービスプロバイダ530bとから構成されている。

【0008】以下に、上記のように構成されたオンラインショッピングシステムにおいてオンラインショッピングを利用する際の処理について、ユーザ端末510のユーザが店舗520にて取り扱う商品を購入する場合の処理を例に挙げて説明する。

【0009】図14は、図13に示したオンラインショッピングシステムにおいてオンラインショッピングを利用する際の処理を説明するためのフローチャートである。

【0010】ユーザ端末510のユーザが店舗520にて取り扱う商品を購入する場合は、まず、店舗520が運営するショッピングサイトにユーザ端末510を用いてアクセスする（ステップS101）。

【0011】すると、店舗520が運営するショッピングサイトがインターネット550を介してユーザ端末510に送信され（ステップS102）、表示される（ステップS103）。

【0012】ユーザ端末510のユーザは、ユーザ端末510に表示されたショッピングサイトを閲覧して所望の商品を選択する（ステップS104）。

【0013】また、ユーザ端末510のユーザは、ユーザ端末510に表示されるショッピングサイト内の所定の領域に、ユーザの氏名や住所、電話番号、電子メールアドレス等の個人情報を入力するか、あるいは店舗520にて発行されたID及びパスワードを入力し（ステップS105）、これらの情報の入力とステップS104における商品の選択とにより注文書を作成し、該注文書を店舗520に送信する（ステップS106）。ここで、ステップS105における情報の入力は、ユーザ端末510のユーザが店舗520に個人情報を登録していない場合は個人情報を入力し、ユーザ端末510のユーザが店舗520に個人情報を既に登録している場合は、店舗520からユーザ端末510のユーザを識別するた

めのID及びパスワードが発行されているためこれらID及びパスワードを入力する。

【0014】店舗520は、ユーザ端末510から送信されてきた注文書をインターネット550を介して受け取ると（ステップS107）、注文書にID及びパスワードが入力されているのか、あるいは個人情報が入力されているかを判断し（ステップS108）、個人情報が入力されている場合は、該個人情報をデータベース521に登録するとともに、ユーザ端末510のユーザに該ユーザを識別可能なID及びパスワードを発行する（ステップS110）。なお、個人情報は、発行されたID及びパスワードと対応づけられてデータベース521に登録される。

【0015】ユーザ端末510のユーザは、店舗520にて発行されたID及びパスワードをユーザ端末510にて受信することにより受け取り（ステップS111）、その後、店舗520が運営するショッピングサイトにてオンラインショッピングを利用する場合に、ショッピングサイトに個人情報を入力せず、ステップS111にて受け取ったID及びパスワードを入力することにより注文書を作成することになる。

【0016】その後、店舗520は、ステップS107にて受け取った注文書に基づいて、商品の発送、代金の請求を行う（ステップS112）。

【0017】ユーザ端末510のユーザは、店舗520から発送された商品を受け取るとともにその商品の代金を支払う（ステップS113）。

【0018】一方、ステップS107にて店舗520がユーザ端末510から受け取った注文書にID及びパスワードが入力されている場合は、店舗520は、入力されたID及びパスワードが正しいかどうかを判断し（ステップS114）、入力されたID及びパスワードが正しい場合、該ID及びパスワードに対応する個人情報をデータベース521から取り出し（ステップS115）、ステップS112における処理に移行し、データベース521から取り出した個人情報とステップS107にて受け取った注文書とに基づいて、商品の発送、代金の請求を行う。

【0019】また、入力されたID及びパスワードが正しくなかった場合は、その旨をユーザ端末510のユーザに通知する（ステップS116、S117）。

【0020】上述したようなオンラインショッピングシステムにおいては、ユーザが一度オンラインショッピングを利用した場合に、次回からの利用の際に個人情報を再度入力しなくても済むように、個人情報が店舗520が具備するデータベース521に登録されるが、このような個人情報の登録は、ユーザが利用するオンラインショッピングのサイト毎に必要であり、その店舗毎のデータベースにそれぞれ個人情報が登録されることとなるため、登録の手間がかかるとともに、個人情報が盗まれる

可能性が高くなってしまふ。

【0021】また、オンラインショッピングにおける個人情報管理においては、セキュリティ対策が十分なされているとはいえず、外部からの不正アクセスや内部の人間による不正アクセスによって個人情報が漏洩する可能性が高い。

【0022】一方、近年、インターネットを介しての情報のやりとりのセキュリティ性を向上させるために、公開鍵方式を用いて情報をやりとりする技術が利用されている。

【0023】図15は、公開鍵方式を利用した情報処理システムの一構成例を示す図である。

【0024】本従来例は図15に示すように、インターネット550に接続可能なユーザ端末510と、ユーザ端末510が加入し、ユーザ端末510のインターネット550への接続を執り行うサービスプロバイダ530と、ユーザ端末510のユーザに関する個人情報及び予め登録された公開鍵を証明する認証局540と、ユーザ端末510のユーザが認証局540に予め登録した公開鍵が登録されたディレクトリ560とから構成されている。

【0025】以下に、上記のように構成された情報処理システムにおいて情報がやりとりされる際の処理について説明する。

【0026】まず、ユーザ端末510のユーザの認証局540に対する登録処理について説明する。

【0027】図16は、図15に示した情報処理システムにおけるユーザ端末510のユーザの認証局540に対する登録処理を説明するためのフローチャートである。

【0028】まず、ユーザ端末510のユーザは、ユーザ端末510を用いて、公開鍵方式において1セットとなる公開鍵と秘密鍵を作成し（ステップS121）、この公開鍵と電子メールアドレスや住所等からなる個人情報とを認証局540に提出する（ステップS122）。なお、公開鍵と個人情報の認証局540への提出は、ユーザ端末510を用いてインターネット550を介して行うことや、ユーザ端末510のユーザが郵送で行うこと等が考えられる。

【0029】認証局540は、公開鍵と個人情報とを受け取ると（ステップS123）、受け取った個人情報が正しいものであるかどうかの確認を行う（ステップS124）。この個人情報の確認においては、個人情報に含まれる電子メールアドレスに電子メールでパスワードを送信したり、個人情報に含まれる住所にパスワードを郵送したりして、そのパスワードが正しくユーザに届くかどうかを確認する等の方法によって行う。

【0030】ステップS124において、ユーザから受け取った個人情報が正しいものであることが確認された場合、認証局540は、ステップS123にて受け取っ

た個人情報のうちユーザを識別可能な必要最低限の情報と公開鍵がユーザ端末510のユーザのものであることを証明する証明書を発行し（ステップS125）、この証明書を公開鍵とともにユーザ端末510のユーザに送付する。

【0031】ユーザ端末510のユーザは、認証局540から送付された証明書を受け取る（ステップS126）。

【0032】また、認証局540は、ステップS123にて受け取った公開鍵とステップS125にて発行した証明書をディレクトリ560に登録し、公開する（ステップS127）。

【0033】一方、ステップS124において、ユーザから受け取った個人情報が正しいものではないことが確認された場合は、個人情報が正しくない旨がユーザ端末510のユーザに通知される（ステップS128、S129）。

【0034】なお、認証局540が有するデータベース541に登録される個人情報は、サーバやファイアウォールのアクセス制御機能により、外部に対して非公開の領域に登録されており、外部からは閲覧不可能になっている。

【0035】次に、認証局540の利用方法について説明する。

【0036】図16に示した一連の処理によって認証局540に登録を行ったユーザが、インターネット550を介して所望の情報を送信する場合、送信する情報を秘密鍵を用いて暗号化し、暗号化した情報を送信先にインターネット550を介して送信する。

【0037】情報の送信先においては、ディレクトリ560からユーザの公開鍵を取得し、取得した公開鍵を用いて、暗号化された情報を復号化し、それにより、受け取った情報がユーザ端末510のユーザによって作成されたものであることを確認する。

【0038】このような公開鍵方式を利用した情報のやりとりは、重要な取り引き等、送信元の人物を確認する必要がある場合や、事後否認を防ぎたい時に利用される。

【0039】そこで、図15に示したような認証局540に、ユーザ端末510の個人情報を登録しておき、該個人情報を、図13に示したようなオンラインショッピングに利用すれば、上述したような、ユーザが利用するオンラインショッピングのサイト毎に個人情報を入力する手間を省くことができるとともに、個人情報が盗まれる可能性を低減することができるようになる。

【0040】

【発明が解決しようとする課題】しかしながら、上述したように、ユーザに関する個人情報を、インターネットに接続可能な1つの領域に登録した場合であっても、サーバやファイアウォールのアクセス制御機能により、外

部に対して非公開の領域に登録されているものの、一塊のデータファイルとして1つの領域に登録されているため、セキュリティホール等を利用した外部からの不正アクセスや内部の人間による不正アクセスにより閲覧されてしまう虞れがある。

【0041】また、ユーザに関する個人情報を暗号化した状態で登録しておく方法も用いられているが、その場合、登録された個人情報が盗まれたとしてもその内容が暗号化されているため閲覧不可能であるものの、高速な計算機を用いて時間をかければ暗号化された個人情報が解読されてしまう虞れがある。

【0042】本発明は、上述したような従来の技術が有する問題点に鑑みてなされたものであって、インターネットに接続可能な領域に登録された個人情報のセキュリティ性を向上させることができる個人情報管理システム及び個人情報管理方法、並びにサーバを提供することを目的とする。

【0043】

【課題を解決するための手段】上記目的を達成するために本発明は、インターネットに接続可能な少なくとも1つの端末と、前記インターネットに接続可能な領域に登録される個人情報を公開鍵方式によって証明するとともに前記個人情報を前記領域に登録し、前記公開鍵方式によって証明される要求に対して前記個人情報を前記要求を送信した端末に送信する認証手段とを少なくとも有してなる個人情報管理システムにおいて、前記認証手段は、前記個人情報を複数のデータに分割し、該複数のデータのうち少なくとも1つのデータを当該認証手段が具備するデータベースに登録し、他のデータを当該認証手段とは異なる管理下の前記インターネットに接続可能な他の領域に登録し、前記公開鍵方式によって証明される、前記個人情報を取得する要求が前記端末から送信されてきた場合、前記分割された複数のデータを結合して前記個人情報を復元し、該個人情報を、前記要求を送信した端末に送信することを特徴とする。

【0044】また、前記認証手段は、前記他のデータの登録先を示すリンク情報を保持し、前記要求が送信されてきた場合、前記リンク情報に基づいて前記他のデータの登録先を認識することを特徴とする。

【0045】また、前記認証手段は、当該認証手段が具備するデータベースに登録されるデータに前記他のデータの登録先を示すリンク情報を付与することを特徴とする。

【0046】また、前記認証手段は、前記個人情報を予め決められた固定長毎に複数のデータに分割し、分割された複数のデータを決められた配列方法によって少なくとも2つのデータ片とし、該データ片毎に、当該認証手段が具備するデータベースあるいは前記他の領域に登録することを特徴とする。

【0047】また、前記認証手段は、前記個人情報を互

いに等しい任意長毎に複数のデータに分割し、分割された複数のデータを決められた配列方法によって少なくとも2つのデータ片とし、該データ片毎に、当該認証手段が具備するデータベースあるいは前記他の領域に登録することを特徴とする。

【0048】また、前記認証手段は、前記個人情報を互いに異なる任意長毎に複数のデータに分割し、分割された複数のデータを決められた配列方法によって少なくとも2つのデータ片とし、該データ片毎に、当該認証手段が具備するデータベースあるいは前記他の領域に登録することを特徴とする。

【0049】また、前記認証手段は、前記データ片毎に、前記個人情報の分割方法及び配列方法に関する情報を付与することを特徴とする。

【0050】また、前記認証手段は、前記個人情報を暗号化し、該暗号化した個人情報及び暗号化に用いた暗号鍵を複数のデータに分割することを特徴とする。

【0051】また、前記認証手段は、前記データ片をそれぞれ暗号化することを特徴とする。

【0052】また、インターネットに接続可能な少なくとも1つの端末と、前記インターネットに接続可能な領域に登録される個人情報を公開鍵方式によって証明するとともに前記個人情報を前記領域に登録し、前記公開鍵方式によって証明される要求に対して前記個人情報を前記要求を送信した端末に送信する認証手段とを少なくとも有してなる個人情報管理システムにおいて、前記認証手段は、前記個人情報を複数のデータに分割し、該複数のデータを互いに異なる管理下の前記インターネットに接続可能な領域に登録するとともに、前記複数のデータの登録先を示すリンク情報を保持し、前記公開鍵方式によって証明される、前記個人情報を取得する要求が前記端末から送信されてきた場合、前記分割された複数のデータを前記リンク情報に基づいて取得し、取得した複数のデータを結合して前記個人情報を復元し、該個人情報を、前記要求を送信した端末に送信することを特徴とする。

【0053】また、前記他の領域のうち少なくとも1つは、前記インターネットに接続可能な領域に登録される個人情報を公開鍵方式によって証明する他の認証手段であることを特徴とする。

【0054】また、インターネットに接続可能な少なくとも1つの端末と、該端末の前記インターネットへの接続を執り行うサービスプロバイダと、前記インターネットに接続可能な領域に登録される個人情報を公開鍵方式によって証明する認証手段とを少なくとも有してなる個人情報管理システムにおいて、前記サービスプロバイダは、前記個人情報を複数のデータに分割し、該複数のデータのうち少なくとも1つのデータを当該サービスプロバイダが具備するデータベースに登録し、他のデータを前記認証手段が具備するデータベースを含む、当該サー

ビスプロバイダとは異なる管理下の前記インターネットに接続可能な他の領域に登録し、前記公開鍵方式によって証明される、前記個人情報を取得する要求が前記端末から送信されてきた場合、前記分割された複数のデータを結合して前記個人情報を復元し、該個人情報を、前記要求を送信した端末に送信することを特徴とする。

【0055】また、前記サービスプロバイダは、前記他のデータの登録先を示すリンク情報を保持し、前記要求が送信されてきた場合、前記リンク情報に基づいて前記他のデータの登録先を認識することを特徴とする。

【0056】また、前記サービスプロバイダは、当該サービスプロバイダが具備するデータベースに登録されるデータに前記他のデータの登録先を示すリンク情報を付与することを特徴とする。

【0057】また、前記サービスプロバイダは、前記個人情報を予め決められた固定長毎に複数のデータに分割し、分割された複数のデータを決められた配列方法によって少なくとも2つのデータ片とし、該データ片毎に、当該サービスプロバイダが具備するデータベースあるいは前記他の領域に登録することを特徴とする。

【0058】また、前記サービスプロバイダは、前記個人情報を互いに等しい任意長毎に複数のデータに分割し、分割された複数のデータを決められた配列方法によって少なくとも2つのデータ片とし、該データ片毎に、当該サービスプロバイダが具備するデータベースあるいは前記他の領域に登録することを特徴とする。

【0059】また、前記サービスプロバイダは、前記個人情報を互いに異なる任意長毎に複数のデータに分割し、分割された複数のデータを決められた配列方法によって少なくとも2つのデータ片とし、該データ片毎に、当該サービスプロバイダが具備するデータベースあるいは前記他の領域に登録することを特徴とする。

【0060】また、前記サービスプロバイダは、前記データ片毎に、前記個人情報の分割方法及び配列方法に関する情報を付与することを特徴とする。

【0061】また、前記サービスプロバイダは、前記個人情報を暗号化し、該暗号化した個人情報及び暗号化に用いた暗号鍵を複数のデータに分割することを特徴とする。

【0062】また、前記サービスプロバイダは、前記データ片をそれぞれ暗号化することを特徴とする。

【0063】また、インターネットに接続可能な少なくとも1つの端末と、該端末の前記インターネットへの接続を執り行うサービスプロバイダと、前記インターネットに接続可能な領域に登録される個人情報を公開鍵方式によって証明する認証手段とを少なくとも有してなる個人情報管理システムにおいて、前記サービスプロバイダは、前記個人情報を複数のデータに分割し、該複数のデータを互いに異なる管理下の前記インターネットに接続可能な領域に登録するとともに、前記複数のデータの登

録先を示すリンク情報を保持し、前記公開鍵方式によって証明される、前記個人情報を取得する要求が前記端末から送信されてきた場合、前記分割された複数のデータを前記リンク情報に基づいて取得し、取得した複数のデータを結合して前記個人情報を復元し、該個人情報を、前記要求を送信した端末に送信することを特徴とする。

【0064】また、インターネットに接続可能な領域に個人情報を登録し、公開鍵方式によって証明される、前記個人情報を取得する要求が出された場合に、前記個人情報を前記要求元に送信する個人情報管理方法であって、前記個人情報を複数のデータに分割し、分割された複数のデータを少なくとも2つのデータ片とし、該データ片毎に互いに異なる管理下の領域に登録し、前記要求が出された場合、前記分割された複数のデータを結合して前記個人情報を復元し、該個人情報を前記要求元に送信することを特徴とする。

【0065】また、前記データ片が登録される領域のうち1つの領域において、他のデータ片の登録先を示すリンク情報を保持しておき、前記要求が出された場合、前記リンク情報に基づいて前記他のデータ片の登録先を認識することを特徴とする。

【0066】また、前記データ片に、他のデータ片の登録先を示すリンク情報を付与しておき、前記要求が出された場合、前記リンク情報に基づいて前記他のデータ片の登録先を認識することを特徴とする。

【0067】また、前記個人情報を予め決められた固定長毎に複数のデータに分割することを特徴とする。

【0068】また、前記個人情報を互いに等しい任意長毎に複数のデータに分割することを特徴とする。

【0069】また、前記個人情報を互いに異なる任意長毎に複数のデータに分割することを特徴とする。

【0070】また、前記データ片毎に、前記個人情報の分割方法に関する情報を付与することを特徴とする。

【0071】また、前記個人情報を暗号化し、該暗号化した個人情報及び暗号化に用いた暗号鍵を複数のデータに分割することを特徴とする。

【0072】また、前記データ片をそれぞれ暗号化することを特徴とする。

【0073】また、インターネットに接続可能な領域に登録される個人情報を公開鍵方式によって証明するとともに前記個人情報を前記領域に登録し、前記公開鍵方式によって証明される要求に対して前記個人情報を前記要求元に送信する認証手段内に設けられた情報処理サーバであって、前記個人情報を複数のデータに分割し、該複数のデータのうち少なくとも1つのデータを前記認証手段が具備するデータベースに登録し、他のデータを前記認証手段とは異なる管理下の前記インターネットに接続可能な他の領域に登録し、前記公開鍵方式によって証明される、前記個人情報を取得する要求が送信されてきた場合、前記分割された複数のデータを結合して前記個人

情報を復元し、該個人情報に前記要求元へ送信することを特徴とする。

【0074】また、前記他のデータの登録先を示すリンク情報を保持し、前記要求が送信されてきた場合、前記リンク情報に基づいて前記他のデータの登録先を認識することを特徴とする。

【0075】また、前記認証手段が具備するデータベースに登録されるデータに前記他のデータの登録先を示すリンク情報を付与することを特徴とする。

【0076】また、前記個人情報を予め決められた固定長毎に複数のデータに分割し、分割された複数のデータを決められた配列方法によって少なくとも2つのデータ片とし、該データ片毎に、前記認証手段が具備するデータベースあるいは前記他の領域に登録することを特徴とする。

【0077】また、前記個人情報を互いに等しい任意長毎に複数のデータに分割し、分割された複数のデータを決められた配列方法によって少なくとも2つのデータ片とし、該データ片毎に、前記認証手段が具備するデータベースあるいは前記他の領域に登録することを特徴とする。

【0078】また、前記個人情報を互いに異なる任意長毎に複数のデータに分割し、分割された複数のデータを決められた配列方法によって少なくとも2つのデータ片とし、該データ片毎に、前記認証手段が具備するデータベースあるいは前記他の領域に登録することを特徴とする。

【0079】また、前記データ片毎に、前記個人情報の分割方法及び配列方法に関する情報を付与することを特徴とする。

【0080】また、前記個人情報を暗号化し、該暗号化した個人情報及び暗号化に用いた暗号鍵を複数のデータに分割することを特徴とする。

【0081】また、前記データ片をそれぞれ暗号化することを特徴とする。

【0082】また、インターネットに接続可能な領域に登録される個人情報を公開鍵方式によって証明するとともに前記個人情報を前記領域に登録し、前記公開鍵方式によって証明される要求に対して前記個人情報を前記要求元へ送信する認証手段内に設けられた情報処理サーバであって、前記個人情報を複数のデータに分割し、該複数のデータを互いに異なる管理下の前記インターネットに接続可能な領域に登録するとともに、前記複数のデータの登録先を示すリンク情報を保持し、前記公開鍵方式によって証明される、前記個人情報を取得する要求が前記端末から送信されてきた場合、前記分割された複数のデータを前記リンク情報に基づいて取得し、取得した複数のデータを結合して前記個人情報を復元し、該個人情報を、前記要求を送信した端末へ送信することを特徴とする。

【0083】また、インターネットに接続可能な端末の前記インターネットへの接続を執り行うサービスプロバイダ内に設けられた情報処理サーバであって、前記個人情報を複数のデータに分割し、該複数のデータのうち少なくとも1つのデータを前記サービスプロバイダが具備するデータベースに登録し、他のデータを、前記インターネット上に登録される個人情報を公開鍵方式によって証明する認証手段が具備するデータベースを含む、前記サービスプロバイダとは異なる管理下の前記インターネットに接続可能な領域に登録し、前記公開鍵方式によって証明される、前記個人情報を取得する要求が前記端末から送信されてきた場合、前記分割された複数のデータを結合して前記個人情報を復元し、該個人情報を、前記要求を送信した端末へ送信することを特徴とする。

【0084】また、前記他のデータの登録先を示すリンク情報を保持し、前記要求が送信されてきた場合、前記リンク情報に基づいて前記他のデータの登録先を認識することを特徴とする。

【0085】また、前記サービスプロバイダが具備するデータベースに登録されるデータに前記他のデータの登録先を示す情報を付与することを特徴とする。

【0086】また、前記個人情報を予め決められた固定長毎に複数のデータに分割し、分割された複数のデータを決められた配列方法によって少なくとも2つのデータ片とし、該データ片毎に、前記サービスプロバイダが具備するデータベースあるいは前記他の領域に登録することを特徴とする。

【0087】また、前記個人情報を互いに等しい任意長毎に複数のデータに分割し、分割された複数のデータを決められた配列方法によって少なくとも2つのデータ片とし、該データ片毎に、前記サービスプロバイダが具備するデータベースあるいは前記他の領域に登録することを特徴とする。

【0088】また、前記個人情報を互いに異なる任意長毎に複数のデータに分割し、分割された複数のデータを決められた配列方法によって少なくとも2つのデータ片とし、該データ片毎に、前記サービスプロバイダが具備するデータベースあるいは前記他の領域に登録することを特徴とする。

【0089】また、前記データ片毎に、前記個人情報の分割方法及び配列方法に関する情報を付与することを特徴とする。

【0090】また、前記個人情報を暗号化し、該暗号化した個人情報及び暗号化に用いた暗号鍵を複数のデータに分割することを特徴とする。

【0091】また、前記データ片をそれぞれ暗号化することを特徴とする。

【0092】また、インターネットに接続可能な端末の前記インターネットへの接続を執り行うサービスプロバイダ内に設けられた情報処理サーバであって、前記個人

情報を複数のデータに分割し、該複数のデータを互いに異なる管理下の前記インターネットに接続可能な領域に登録するとともに、前記複数のデータの登録先を示すリンク情報を保持し、前記公開鍵方式によって証明される、前記個人情報を取得する要求が前記端末から送信されてきた場合、前記分割された複数のデータを前記リンク情報に基づいて取得し、取得した複数のデータを結合して前記個人情報を復元し、該個人情報を、前記要求を送信した端末に送信することを特徴とする。

【0093】（作用）上記のように構成された本発明においては、ユーザが個人情報をインターネットに接続可能な領域に登録する場合、まず、登録すべき個人情報と公開鍵方式における公開鍵とを認証手段あるいはサービスプロバイダに提出する。認証手段は、提出された個人情報が正しいかどうかを確認し、個人情報が正しいことが確認された場合、個人情報及び公開鍵がユーザのものであることを証明する。また、認証手段あるいはサービスプロバイダは、提出された個人情報を複数のデータに分割し、複数のデータのうち少なくとも1つのデータを認証手段あるいはサービスプロバイダが具備するデータベースに登録し、他のデータを認証手段あるいはサービスプロバイダとは異なる管理下のインターネットに接続可能な他の領域に登録する。この際、認証手段あるいはサービスプロバイダは、他のデータの登録先を示すリンク情報を保持しておくか、認証手段あるいはサービスプロバイダが具備するデータベースに登録されるデータに付与しておく。その後、公開鍵方式によって証明される、個人情報を取得する要求がインターネットに接続可能な端末から送信されてきた場合、認証手段あるいはサービスプロバイダは、認証手段あるいはサービスプロバイダのデータベースに登録されたデータを検索するとともに、保持しているリンク情報に基づいて他のデータの登録先を認識し、他のデータの登録先から他のデータを取得し、これらのデータを結合して個人情報を復元して復元した個人情報を端末に送信する。

【0094】このように、インターネットに接続可能な領域に登録される個人情報が複数のデータに分割され、それぞれが異なる管理下の領域に登録されるので、全ての領域に登録されたデータが盗まれない限り個人情報が閲覧されないことになり、インターネットに接続可能な領域に登録された個人情報のセキュリティ性が向上する。

【0095】

【発明の実施の形態】以下に、本発明の実施の形態について図面を参照して説明する。

【0096】（第1の実施の形態）図1は、本発明の個人情報管理システムの第1の実施の形態を示す図である。

【0097】本形態は図1に示すように、インターネット50に接続可能なユーザ端末10と、ユーザ端末10

が加入し、ユーザ端末10のインターネット50への接続を執り行うサービスプロバイダ30aと、インターネット50に接続可能に構成される端末（不図示）を具備し、商品等を販売する店舗20と、店舗20が加入し、店舗20の端末のインターネット50への接続を執り行うサービスプロバイダ30bと、ユーザ端末10のユーザに関する個人情報を証明するとともに、該個人情報を分割し、その一部をデータベース41aに登録し、分割した個人情報のうちデータベース41aに登録しない部分をインターネット50を介して接続可能な認証局40bに送信し、また、店舗20から送られてきた情報によってユーザを認証し、データベース41aに登録された個人情報の一部と認証局40bに送信して認証局40bが有するデータベース41bに登録された個人情報の一部とを結合して結合した個人情報をインターネット50を介して店舗20に送信する認証局40aと、ユーザ端末10のユーザが認証局40aに予め登録した公開鍵が登録されたディレクトリ60とから構成されている。なお、認証局40bは、認証機能を有しないものであってもよい。

【0098】以下に、上記のように構成された個人情報管理システムにおける個人情報管理方法について、ユーザ端末10のユーザが店舗20にて取り扱う商品を購入する場合の処理を例に挙げて説明する。なお、以下に記載する認証局40a、40bにおける処理は、認証局40a、40b内に設けられた情報処理サーバ（不図示）においてそれぞれ行われることが考えられる。

【0099】まず、ユーザ端末10のユーザが個人情報を認証局40aに登録する際の処理について説明する。なお、以下に示すインターネット50を介しての情報のやりとりは、やりとりされる情報が全てSSL（Secure Sockets Layer）等の手段によって暗号化された状態で行われる。

【0100】図2は、図1に示した個人情報管理システムにおいて、ユーザ端末10のユーザが個人情報を認証局40aに登録する際の処理を説明するためのフローチャートである。

【0101】まず、ユーザ端末10のユーザは、ユーザ端末10を用いて、公開鍵方式において1セットとなる公開鍵と秘密鍵を作成し（ステップS1）、この公開鍵と電子メールアドレスや住所等からなる個人情報とを認証局40aに提出する（ステップS2）。なお、公開鍵と個人情報の認証局40aへの提出は、ユーザ端末10を用いてインターネット50を介して行うことや、ユーザ端末10のユーザが郵送で行うこと等が考えられる。

【0102】認証局40aは、公開鍵と個人情報とを受け取ると（ステップS3）、受け取った個人情報が正しいものであるかどうかの確認を行う（ステップS4）。この個人情報の確認においては、個人情報に含まれる電子メールアドレスに電子メールでパスワードを送信した

り、個人情報に含まれる住所にパスワードを郵送したりして、そのパスワードが正しくユーザに届くかどうかを確認する等の方法によって行う。

【0103】ステップS4において、ユーザから受け取った個人情報が正しいものであることが確認された場合、認証局40aは、ユーザから受け取った個人情報を所定の分割方法によって2つのデータ片に分割する(ステップS5)。なお、個人情報の分割は、それぞれが独立では全く意味を持たない情報になるように行うが、その詳細については後述する。

【0104】認証局40aは、分割した個人情報のうち一方のデータ片(以下、データ片Xと称する)をデータベース41aに登録するとともに(ステップS6)、他方のデータ片(以下、データ片Yと称する)をインターネット50を介して認証局40bに送信する(ステップS7)。この際、認証局40aにおいては、データ片Yの登録先となる認証局40bのアドレスや認証局40bを識別可能な識別情報をリンク情報として保持しておく。

【0105】認証局40bは、認証局40aから送信されてきたデータ片Yを受信すると(ステップS8)、受信したデータ片Yを認証局40b内のデータベース41bに登録する(ステップS9)。

【0106】また、認証局40aは、ステップS3にて受け取った個人情報のうちユーザを識別可能な最低限の情報と公開鍵がユーザ端末10のユーザのものであることを証明する証明書を発行し(ステップS10)、この証明書を公開鍵とともにユーザ端末10のユーザに送付する。

【0107】ユーザ端末10のユーザは、認証局40aから送付された証明書を受け取る(ステップS11)。

【0108】また、認証局40aは、ステップS3にて受け取った公開鍵とステップS10にて発行した証明書をディレクトリ60に登録し、公開する(ステップS12)。

【0109】一方、ステップS4において、ユーザから受け取った個人情報が正しいものではないことが確認された場合は、個人情報が正しくない旨がユーザ端末10のユーザに通知される(ステップS13、S14)。

【0110】なお、認証局40a、40bが有するデータベース41a、41bに登録されるデータ片は、サーバやファイアウォールのアクセス制御機能により、外部に対して非公開の領域に登録されており、外部からは閲覧不可能になっている。

【0111】次に、ユーザ端末10のユーザが認証局40a、40bに登録された個人情報を用いて店舗20にて取り扱う商品を購入する際の処理について説明する。

【0112】図3は、図1に示した個人情報管理システムにおいて、ユーザ端末10のユーザが認証局40a、40bに登録された個人情報を用いて店舗20にて取り

扱う商品を購入する際の処理を説明するためのフローチャートである。

【0113】ユーザ端末10のユーザが店舗20にて取り扱う商品を購入する場合は、まず、店舗20が運営するショッピングサイトにユーザ端末10を用いてアクセスする(ステップS21)。

【0114】すると、店舗20が運営するショッピングサイトがインターネット50を介してユーザ端末10に送信され(ステップS22)、表示される(ステップS23)。

【0115】ユーザ端末10のユーザは、ユーザ端末10に表示されたショッピングサイトを閲覧して所望の商品を選択する(ステップS24)。

【0116】店舗20は、ステップS24にてユーザが選択した商品を受注するにあたって必要となる個人情報の項目をリストアップし、それらの項目についてユーザ端末10のユーザに関する個人情報を認証局40aから取得する許可をユーザ端末10のユーザに要求する(ステップS25)。

【0117】ユーザ端末10のユーザは、店舗20から送信されてきた項目を確認し、その項目についてユーザ端末10のユーザに関する個人情報を店舗20が取得することを許可する場合、その旨を示す許可書を作成し、作成した許可書を圧縮し、さらに、圧縮した許可書をステップS1(図2参照)にて作成した秘密鍵を用いて暗号化し、この暗号化した許可書を、作成した許可書とともに店舗20に送信する(ステップS26)。

【0118】店舗20は、ユーザ端末10から送信された許可書をインターネット50を介して受け取ると(ステップS27)、ディレクトリ60の中からユーザ端末10のユーザが登録した公開鍵を取得し(ステップS28)、取得した公開鍵を用いて、受け取った許可書がユーザ端末10のユーザによって作成されたものかどうかを確認する(ステップS29)。なお、ユーザ端末10において作成した許可書と暗号化した許可書とともにユーザの公開鍵を店舗20に送信し、店舗20において、ユーザ端末10から送信されてきた公開鍵を用いて許可書の確認を行うことも考えられる。その場合、店舗20においてディレクトリ60の中から公開鍵を取得する必要がなくなる。

【0119】ここで、ステップS29における許可書の確認について詳細に説明する。

【0120】まず、店舗20は、ステップS27にて受け取った許可書のうち、暗号化された許可書をステップS28にて取得した公開鍵を用いて復号化してみる。その後、暗号化された許可書とともにユーザ端末10から送信されてきた許可書を圧縮し、この圧縮した許可書を復号化された許可書と照合する。この照合の結果、両者が一致した場合、ステップS27にて受け取った許可書がユーザ端末10のユーザによって作成された許可書で

あることが確認される。ここで、店舗20がディレクトリ60から取得した公開鍵は、認証局40aが発行した証明書によって、ユーザ端末10のユーザのものであることが証明されている。

【0121】ステップS29において、受け取った許可書がユーザ端末10のユーザによって作成されたものであることが確認された場合、店舗20は、ユーザ端末10から受け取った許可書と暗号化された許可書を認証局40aに送信する(ステップS30)。

【0122】認証局40aは、店舗20から送信されてきた許可書をインターネット50を介して受け取ると(ステップS31)、ディレクトリ60に登録されたユーザ端末10のユーザの公開鍵を用いて、受け取った許可書がユーザ端末10のユーザによって作成されたものかどうかを確認する(ステップS32)。なお、ここでの許可書の確認においても、店舗20における許可書の確認と同様に行われる。また、認証局40aにおける許可書の確認においても、店舗20における許可書の確認と同様に、店舗20からユーザの公開鍵を送信し、認証局40aにおいて店舗20から送信されてきた公開鍵を用いて行うことも考えられる。

【0123】ステップS32において、受け取った許可書がユーザ端末10のユーザによって作成されたものであることが確認された場合、認証局40aは、ユーザ端末10のユーザに関する個人情報のうちデータ片Xをデータベース41aから検索する(ステップS33)。

【0124】認証局40aは、データベース41aから検索されたデータ片Xと結合することによりユーザ端末10のユーザに関する個人情報となるデータ片Yの登録先となる認証局40bのアドレスや認証局40bを識別可能な識別情報をリンク情報として保持しているため、認証局40aは、このリンク情報に基づいて、データ片Yの登録先となる認証局40bに対してデータ片Yの送信を要求する(ステップS34)。なお、認証局40aが保持しているリンク情報が、認証局40bを識別可能な識別情報である場合は、この識別情報と認証局40bのアドレスとを対応づけたデータベースがさらに必要となる。また、このリンク情報を暗号化して保持しておくことも考えられる。

【0125】認証局40bは、認証局40aからの要求を受信すると、データベース41bの中からデータ片Yを検索し、認証局40aに送信する(ステップS35)。

【0126】認証局40aは、認証局40bから送信されたデータ片Yを受信すると(ステップS36)、データベース41aから検索したデータ片Xと認証局40bから送信されてきたデータ片Yとを結合し、それにより、ユーザ端末10のユーザに関する個人情報を復元する(ステップS37)。なお、データ片X、Yにはそれぞれ、ステップS5(図2参照)にて個人情報が分割さ

れた際に、その分割方法や分割されたデータの配列方法に関する情報が付与されており、認証局40aは、データ片X、Yに付与された分割方法及び配列方法に関する情報に基づいてデータ片Xとデータ片Yとを結合する。

【0127】認証局40aは、復元された個人情報のうち、店舗20にてリストアップされた項目についての個人情報のみを店舗20に送信する(ステップS38)。

【0128】店舗20は、認証局40aから送信されてきたユーザ端末10のユーザに関する個人情報を受け取ると(ステップS39)、受け取った個人情報とステップS24にて選択された商品情報に基づいて、商品の発送、代金の請求を行う(ステップS40)。

【0129】その後、ユーザ端末10のユーザは、店舗20から発送された商品を受け取るとともにその商品の代金を支払う(ステップS41)。

【0130】なお、店舗20においては、商品の販売が完了すると、認証局40aから取得した個人情報を消去する。

【0131】以下に、個人情報の分割方法について複数の例を挙げて詳細に説明する。

【0132】図4は、図1に示した個人情報管理システムにおける個人情報の分割方法の一例を説明するための図である。

【0133】図4に示すように、ユーザ端末10のユーザが認証局40aに提出した個人情報を予め決められた固定長毎に複数のデータに分割し、その複数のデータを決められた配列方法によってデータ片X、Yの2つのデータ片にまとめ、データ片Xを認証局40aのデータベース41aに登録するとともに、データ片Yを認証局40bのデータベース41bに登録する。

【0134】この場合、個人情報の分割方法及び配列方法に関する情報をデータ片X、Yに付与しておくが、本例においては、個人情報が予め決められた固定長のデータに分割されるため、これらの情報を付与しない場合も考えられる。

【0135】図5は、図1に示した個人情報管理システムにおける個人情報の分割方法の他の例を説明するための図である。

【0136】図5に示すように、ユーザ端末10のユーザが認証局40aに提出した個人情報を、乱数、時間、ファイルの容量等の関数によって互いに等しい任意長毎に複数のデータに分割し、その複数のデータを決められた配列方法によってデータ片X、Yの2つのデータ片にまとめ、データ片Xを認証局40aのデータベース41aに登録するとともに、データ片Yを認証局40bのデータベース41bに登録する。

【0137】この場合、個人情報が任意長のデータに分割されるため、その分割方法及び配列方法に関する情報となる任意長をデータ片X、Yに付与しておく必要がある。

【0138】このように分割されたデータ片Xとデータ片Yとを結合する場合は、データ片X、Yにそれぞれ付与された分割方法及び配列方法に関する情報に基づいてデータ片Xとデータ片Yとを結合することになる。

【0139】図6は、図1に示した個人情報管理システムにおける個人情報の分割方法の他の例を説明するための図である。

【0140】図6に示すように、ユーザ端末10のユーザが認証局40aに提出した個人情報を、乱数、時間、ファイルの容量等の関数によって互いに異なる任意長毎に複数のデータに分割し、その複数のデータを決められた配列方法によってデータ片X、Yの2つのデータ片にまとめ、データ片Xを認証局40aのデータベース41aに登録するとともに、データ片Yを認証局40bのデータベース41bに登録する。

【0141】この場合、個人情報が互いに異なる任意長のデータに分割されるため、その分割方法及び配列方法に関する情報となる任意長をデータ片X、Yに付与しておく必要がある。

【0142】このように分割されたデータ片Xとデータ片Yとを結合する場合は、データ片X、Yにそれぞれ付与された分割方法及び配列方法に関する情報に基づいてデータ片Xとデータ片Yとを結合することになる。

【0143】上述した3つの方法において、個人情報を暗号化して登録することも考えられる。

【0144】図7は、図1に示した個人情報管理システムにおける個人情報の分割方法の他の例を説明するための図である。

【0145】図7に示すように、ユーザ端末10のユーザが認証局40aに提出した個人情報をまず暗号化し、暗号化した個人情報及びその暗号化に用いた鍵情報を、図4に示したような固定長あるいは図5または図6に示したような任意長毎に複数のデータに分割し、その複数のデータを決められた配列方法によってデータ片X、Yの2つのデータ片にまとめ、データ片Xを認証局40aのデータベース41aに登録するとともに、データ片Yを認証局40bのデータベース41bに登録する。

【0146】このように分割されたデータ片Xとデータ片Yとを結合する場合は、データ片X、Yに分割方法及び配列方法に関する情報が付与されていればその分割方法及び配列方法に関する情報に基づいてデータ片Xとデータ片Yとを結合し、その後、暗号化された個人情報に付与された鍵情報を用いて、暗号化された個人情報を復号化することになる。

【0147】図8は、図1に示した個人情報管理システムにおける個人情報の分割方法の他の例を説明するための図である。

【0148】図8に示すように、ユーザ端末10のユーザが認証局40aに提出した個人情報を、図4に示したような固定長あるいは図5または図6に示したような任

意長毎に複数のデータに分割し、その複数のデータを決められた配列方法によってデータ片X、Yの2つのデータ片にまとめ、その後、データ片X、Yをそれぞれ暗号化し、暗号化されたデータ片Xを認証局40aのデータベース41aに登録するとともに、暗号化されたデータ片Yを認証局40bのデータベース41bに登録する。なお、暗号化されたデータ片Xには、データ片Yの暗号化に用いた鍵情報を付与し、また、暗号化されたデータ片Yには、データ片Xの暗号化に用いた鍵情報を付与しておく。

【0149】このように分割されたデータ片Xとデータ片Yとを結合する場合は、まず、暗号化されたデータ片Xに付与された鍵情報を用いてデータ片Yを復号化するとともに、暗号化されたデータ片Yに付与された鍵情報を用いてデータ片Xを復号化し、その後、データ片X、Yに分割方法及び配列方法に関する情報が付与されていればその分割方法及び配列方法に関する情報に基づいてデータ片Xとデータ片Yとを結合することになる。

【0150】図9は、図1に示した個人情報管理システムにおける個人情報の分割方法の他の例を説明するための図である。

【0151】図9に示すように、ユーザ端末10のユーザが認証局40aに提出した個人情報をまず暗号化し、暗号化した個人情報及びその暗号化に用いた鍵情報を、図4に示したような固定長あるいは図5または図6に示したような任意長毎に複数のデータに分割し、その複数のデータを決められた配列方法によってデータ片X、Yの2つのデータ片にまとめ、さらに、データ片X、Yをそれぞれ暗号化し、暗号化されたデータ片Xを認証局40aのデータベース41aに登録するとともに、暗号化されたデータ片Yを認証局40bのデータベース41bに登録する。なお、暗号化されたデータ片Xには、データ片Yの暗号化に用いた鍵情報を付与し、また、暗号化されたデータ片Yには、データ片Xの暗号化に用いた鍵情報を付与しておく。

【0152】このように分割されたデータ片Xとデータ片Yとを結合する場合は、まず、暗号化されたデータ片Xに付与された鍵情報を用いてデータ片Yを復号化するとともに、暗号化されたデータ片Yに付与された鍵情報を用いてデータ片Xを復号化し、その後、データ片X、Yに分割方法及び配列方法に関する情報が付与されていればその分割方法及び配列方法に関する情報に基づいてデータ片Xとデータ片Yとを結合し、さらに、結合された個人情報に付与された鍵情報を用いて、暗号化された個人情報を復号化することになる。

【0153】なお、本形態においては、個人情報が分割されたデータ片Xが認証局40aに登録され、データ片Yが認証局40aとは異なる認証局40bに登録されているが、データ片Yの登録先を、サービスプロバイダや認証局40aにて構築された別のネットワークとするこ

とも考えられる。

【0154】また、認証局40aにおいて、分割されたデータ片を登録せず、分割されたデータ片の登録先を示すリンク情報のみを保持しておき、分割されたデータ片を認証局40bを含むインターネット50に接続可能な他の複数の領域にそれぞれ登録することも考えられる。

【0155】(第2の実施の形態)図10は、本発明の個人情報管理システムの第2の実施の形態を示す図である。

【0156】本形態は図2に示すように、インターネット50に接続可能なユーザ端末10と、ユーザ端末10が加入し、ユーザ端末10のインターネット50への接続を執り行うサービスプロバイダ30aと、インターネット50に接続可能に構成される端末(不図示)を具備し、商品等を販売する店舗20と、店舗20が加入し、店舗20の端末のインターネット50への接続を執り行うとともに、ユーザ端末10のユーザに関する個人情報を分割し、その一部をデータベース131bに登録し、分割した個人情報のうちデータベース131bに登録しない部分をインターネット50を介して接続可能な認証局140aに送信し、また、店舗20から送られてきた情報によってユーザを認証し、データベース131bに登録された個人情報の一部と認証局140aに送信して認証局140aが有するデータベース141aに登録された個人情報の一部とを結合して結合した個人情報を店舗20に送信するサービスプロバイダ130bと、ユーザ端末10のユーザが予め登録した公開鍵が登録されたディレクトリ60とから構成されている。

【0157】以下に、上記のように構成された個人情報管理システムにおける個人情報管理方法について、ユーザ端末10のユーザが店舗20にて取り扱う商品を購入する場合の処理を例に挙げて説明する。なお、以下に記載するサービスプロバイダ130b及び認証局140aにおける処理は、サービスプロバイダ130b及び認証局140a内に設けられた情報処理サーバ(不図示)においてそれぞれ行われる。

【0158】まず、ユーザ端末10のユーザが個人情報を登録する際の処理について説明する。なお、以下に示すインターネット50を介しての情報のやりとりは、やりとりされる情報が全てSSL(Secure Sockets Layer)等の手段によって暗号化された状態で行われることが考えられる。

【0159】図11は、図10に示した個人情報管理システムにおいて、ユーザ端末10のユーザが個人情報を登録する際の処理を説明するためのフローチャートである。

【0160】まず、ユーザ端末10のユーザは、ユーザ端末10を用いて、公開鍵方式において1セットとなる公開鍵と秘密鍵を作成し(ステップS51)、この公開鍵と電子メールアドレスや住所等からなる個人情報とを

サービスプロバイダ130bに提出する(ステップS52)。なお、公開鍵と個人情報のサービスプロバイダ130bへの提出は、ユーザ端末10を用いてインターネット50を介して行うことや、ユーザ端末10のユーザが郵送で行うこと等が考えられる。

【0161】サービスプロバイダ130bは、公開鍵と個人情報を受け取ると(ステップS53)、ユーザから受け取った個人情報を所定の分割方法によって2つのデータ片に分割する(ステップS54)。なお、個人情報の分割は、それぞれが独立では全く意味を持たない情報になるように、図4～図9に示したいずれかの方法によって行う。

【0162】サービスプロバイダ130bは、分割した個人情報のうち一方のデータ片(以下、データ片Xと称する)をデータベース131bに登録するとともに(ステップS55)、他方のデータ片(以下、データ片Yと称する)とステップS53にてユーザから受け取った公開鍵及び個人情報をインターネット50を介して認証局140aに送信する(ステップS56)。この際、サービスプロバイダ130bにおいては、データ片Yの登録先となる認証局140aのアドレスや認証局140aを識別可能な識別情報をリンク情報として保持しておく。

【0163】認証局140aは、サービスプロバイダ130bから送信されてきたデータ片Yと個人情報と公開鍵を受信すると(ステップS57)、受信した個人情報が正しいものであるかどうかの確認を行う(ステップS58)。この個人情報の確認においては、個人情報に含まれる電子メールアドレスに電子メールでパスワードを送信したり、個人情報に含まれる住所にパスワードを郵送したりして、そのパスワードが正しくユーザに届くかどうかを確認する等の方法によって行う。

【0164】ステップS58において、サービスプロバイダ130bから送信されてきた個人情報が正しいものであることが確認された場合、受信したデータ片Yを認証局140a内のデータベース141aに登録する(ステップS59)。

【0165】また、認証局140aは、ステップS57にて受け取った個人情報のうちユーザを識別可能な最低限の情報と公開鍵がユーザ端末10のユーザのものであることを証明する証明書を発行し(ステップS60)、この証明書を公開鍵とともにユーザ端末10のユーザに送付する。

【0166】ユーザ端末10のユーザは、認証局140aから送付された証明書を受け取る(ステップS61)。

【0167】また、認証局140aは、ステップS57にて受け取った公開鍵とステップS60にて発行した証明書をディレクトリ60に登録し、公開する(ステップS62)。

【0177】店舗20は、ユーザ端末10から送信された許可書をインターネット50を介して受け取ると（ステップS77）、ディレクトリ60の中からユーザ端末10のユーザが登録した公開鍵を取得し（ステップS78）、取得した公開鍵を用いて、受け取った許可書がユ

【0183】サービスプロバイダ130bは、データベース131bから検索されたデータ片Xと結合することによりユーザ端末10のユーザに関する個人情報となるデータ片Yの登録先となる認証局140aのアドレスや50 認証局140aを識別可能な識別情報をリンク情報とし

て保持しているため、サービスプロバイダ130bは、このリンク情報に基づいて、データ片Yの登録先となる認証局140aに対してデータ片Yの送信を要求する（ステップS84）。なお、サービスプロバイダ130bが保持しているリンク情報が、認証局140aを識別可能な識別情報である場合は、この識別情報と認証局140aのアドレスとを対応づけたデータベースがさらに必要となる。また、このリンク情報を暗号化して保持しておくことも考えられる。

【0184】認証局140aは、サービスプロバイダ130bからの要求を受信すると、データベース141aの中からデータ片Yを検索し、サービスプロバイダ130bに送信する（ステップS85）。

【0185】サービスプロバイダ130bは、認証局140aから送信されたデータ片Yを受信すると（ステップS86）、データベース131bから検索したデータ片Xと認証局140aから送信されてきたデータ片Yとを結合し、それにより、ユーザ端末10のユーザに関する個人情報を復元する（ステップS87）。なお、データ片X、Yにはそれぞれ、ステップS54（図11参照）にて個人情報が分割された際に、その分割方法や分割されたデータの配列方法に関する情報が付与されており、サービスプロバイダ130bは、データ片X、Yに付与された分割方法及び配列方法に関する情報に基づいてデータ片Xとデータ片Yとを結合する。

【0186】サービスプロバイダ130bは、復元された個人情報のうち、店舗20にてリストアップされた項目についての個人情報のみを店舗20に送信する（ステップS88）。

【0187】店舗20は、サービスプロバイダ130bから送信されてきたユーザ端末10のユーザに関する個人情報を受け取ると（ステップS89）、受け取った個人情報とステップS74にて選択された商品情報に基づいて、商品の発送、代金の請求を行う（ステップS90）。

【0188】その後、ユーザ端末10のユーザは、店舗20から発送された商品を受け取るとともにその商品の代金を支払う（ステップS91）。

【0189】なお、店舗20においては、商品の販売が完了すると、サービスプロバイダ130bから取得した個人情報を消去する。

【0190】なお、本形態においては、店舗20の端末のインターネット50への接続を執り行うサービスプロバイダ130bが、ユーザ端末10のユーザに関する個人情報を分割し、その一部をデータベース131bに登録するとともに、分割した個人情報のうちデータベース131bに登録しない部分をインターネット50を介して認証局140aに送信し、また、分割された個人情報の一部の登録先を示すリンク情報を保持し、また、店舗20から送られてきたデータによってユーザを認証し、

データベース131bに登録された個人情報の一部と認証局140aに送信して認証局140aが有するデータベース141aに登録された個人情報の一部とを結合して結合した個人情報を店舗20に送信する場合を例に挙げて説明したが、ユーザ端末10のインターネット50への接続を執り行うサービスプロバイダ30aにおいてこのような処理を行ってもよい。

【0191】また、インターネット上にてサイトを提供するサービスサイトにおいて、ユーザ端末10のユーザに関する個人情報を分割し、その一部をサービスサイトが有するデータベースに登録するとともに、分割した個人情報のうちサービスサイトが有するデータベースに登録しない部分をインターネット50を介して認証局140aに送信し、また、分割された個人情報の一部の登録先を示すリンク情報を保持し、また、店舗20から送られてきたデータによってユーザを認証し、サービスサイトのデータベースに登録された個人情報の一部と認証局140aに送信して認証局140aが有するデータベース141aに登録された個人情報の一部とを結合して結合した個人情報を店舗20に送信するように構成してもよい。

【0192】また、サービスプロバイダ130bにおいて、分割されたデータ片を登録せず、分割されたデータ片の登録先を示すリンク情報のみを保持しておき、分割されたデータ片を認証局140aを含むインターネット50に接続可能な他の複数の領域にそれぞれ登録することも考えられる。

【0193】また、上述した2つの実施の形態においては、認証局40aあるいはサービスプロバイダ130bが、データ片Yの登録先を示すリンク情報を保持しているが、データ片Xにデータ片Yの登録先を示すリンク情報を付与しておくことも考えられる。その場合、認証局40aあるいはサービスプロバイダ130bがリンク情報を保持していなくても、データ片Xを参照すればデータ片Yの登録先を認識することができる。

【0194】また、データ片Yの登録先を示すリンク情報を作成せず、認証局40aあるいはサービスプロバイダ130bが、インターネット50に接続された全ての認証局に対してデータ片Yの送信要求を出すことも考えられる。

【0195】また、個人情報を2つのデータ片X、Yに分割し、データ片Xを認証局40aあるいはサービスプロバイダ130bに登録し、データ片Yを認証局40bあるいは認証局140aに登録しているが、個人情報を3つ以上のデータ片に分割し、それぞれ互いに異なる認証局やサービスプロバイダに登録し、その後、それらを結合することも考えられる。

【0196】また、上述した実施の形態においては、インターネット上にて商品等を購入するオンラインショッピングを例に挙げて説明したが、本発明はオンラインシ

ショッピングに限らず、インターネットに接続可能な領域に個人情報が登録され、この個人情報を用いてインターネット上にて所定の処理を行うものであれば適用することができる。

【0197】

【発明の効果】以上説明したように本発明においては、インターネットに接続可能な領域に登録される個人情報が複数のデータに分割され、それぞれが異なる管理下の領域に登録され、その後、この個人情報を取得する要求が出された場合、異なる管理下の領域に登録されたデータが結合されることにより個人情報が復元される構成としたため、全ての領域に登録されたデータが盗まれない限り個人情報が閲覧されないことになり、インターネット上に登録された個人情報のセキュリティ性を向上させることができる。

【図面の簡単な説明】

【図1】本発明の個人情報管理システムの第1の実施の形態を示す図である。

【図2】図1に示した個人情報管理システムにおいてユーザ端末のユーザが個人情報を認証局に登録する際の処理を説明するためのフローチャートである。

【図3】図1に示した個人情報管理システムにおいてユーザ端末のユーザが認証局に登録された個人情報を用いて店舗にて取り扱う商品を購入する際の処理を説明するためのフローチャートである。

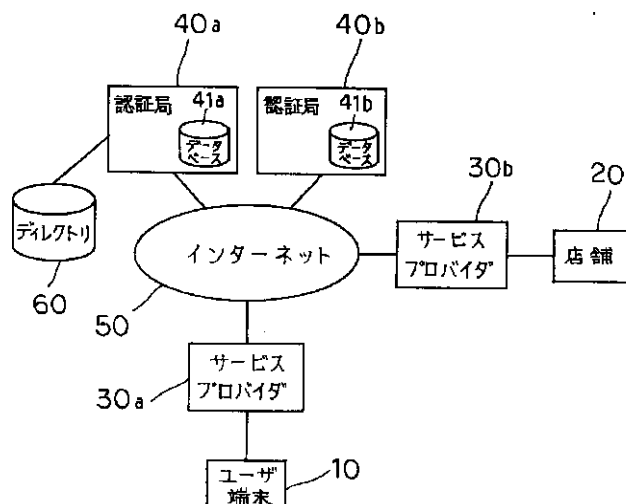
【図4】図1に示した個人情報管理システムにおける個人情報の分割方法の一例を説明するための図である。

【図5】図1に示した個人情報管理システムにおける個人情報の分割方法の他の例を説明するための図である。

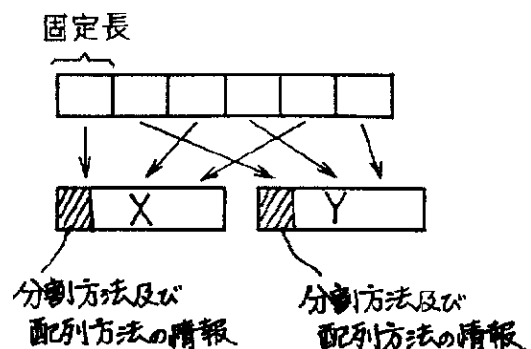
【図6】図1に示した個人情報管理システムにおける個人情報の分割方法の他の例を説明するための図である。

【図7】図1に示した個人情報管理システムにおける個人情報の分割方法の他の例を説明するための図である。*

【図1】



【図4】



*【図8】図1に示した個人情報管理システムにおける個人情報の分割方法の他の例を説明するための図である。

【図9】図1に示した個人情報管理システムにおける個人情報の分割方法の他の例を説明するための図である。

【図10】本発明の個人情報管理システムの第2の実施の形態を示す図である。

【図11】図10に示した個人情報管理システムにおいてユーザ端末のユーザが個人情報を登録する際の処理を説明するためのフローチャートである。

10 【図12】図10に示した個人情報管理システムにおいてユーザ端末のユーザがサービスプロバイダ及び認証局に登録された個人情報を用いて店舗にて取り扱う商品を購入する際の処理を説明するためのフローチャートである。

【図13】一般的なオンラインショッピングシステムの一例を示す図である。

【図14】図13に示したオンラインショッピングシステムにおいてオンラインショッピングを利用する際の処理を説明するためのフローチャートである。

20 【図15】公開鍵方式を利用した情報処理システムの一構成例を示す図である。

【図16】図15に示した情報処理システムにおけるユーザ端末のユーザの認証局に対する登録処理を説明するためのフローチャートである。

【符号の説明】

10 ユーザ端末

20 店舗

30 a, 30 b, 130 b サービスプロバイダ

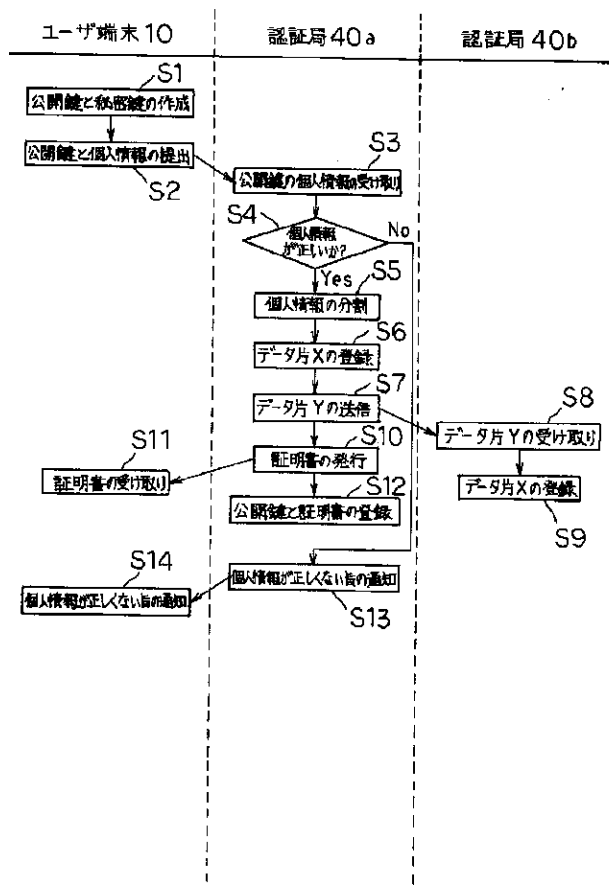
40 a, 40 b, 140 a 認証局

41 a, 41 b, 141 a データベース

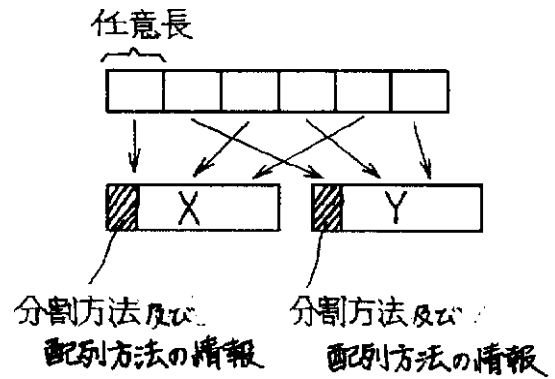
50 インターネット

60 ディレクトリ

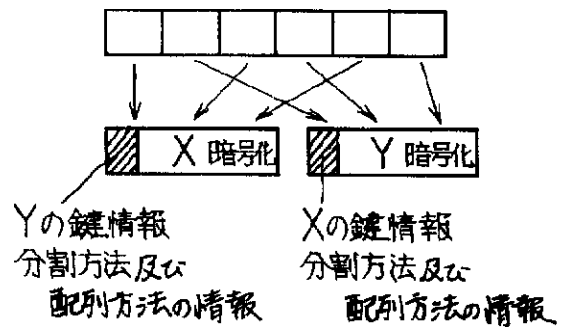
【図2】



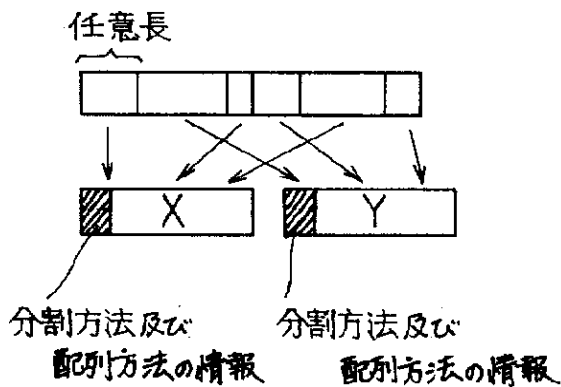
【図5】



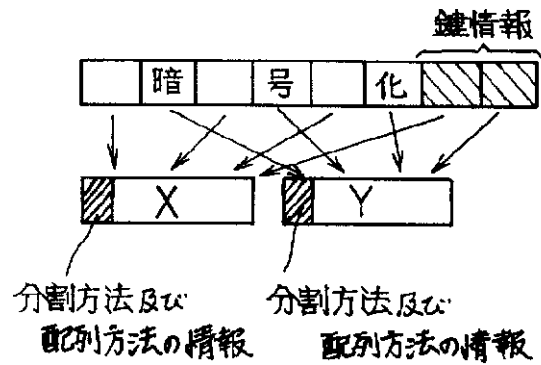
【図8】



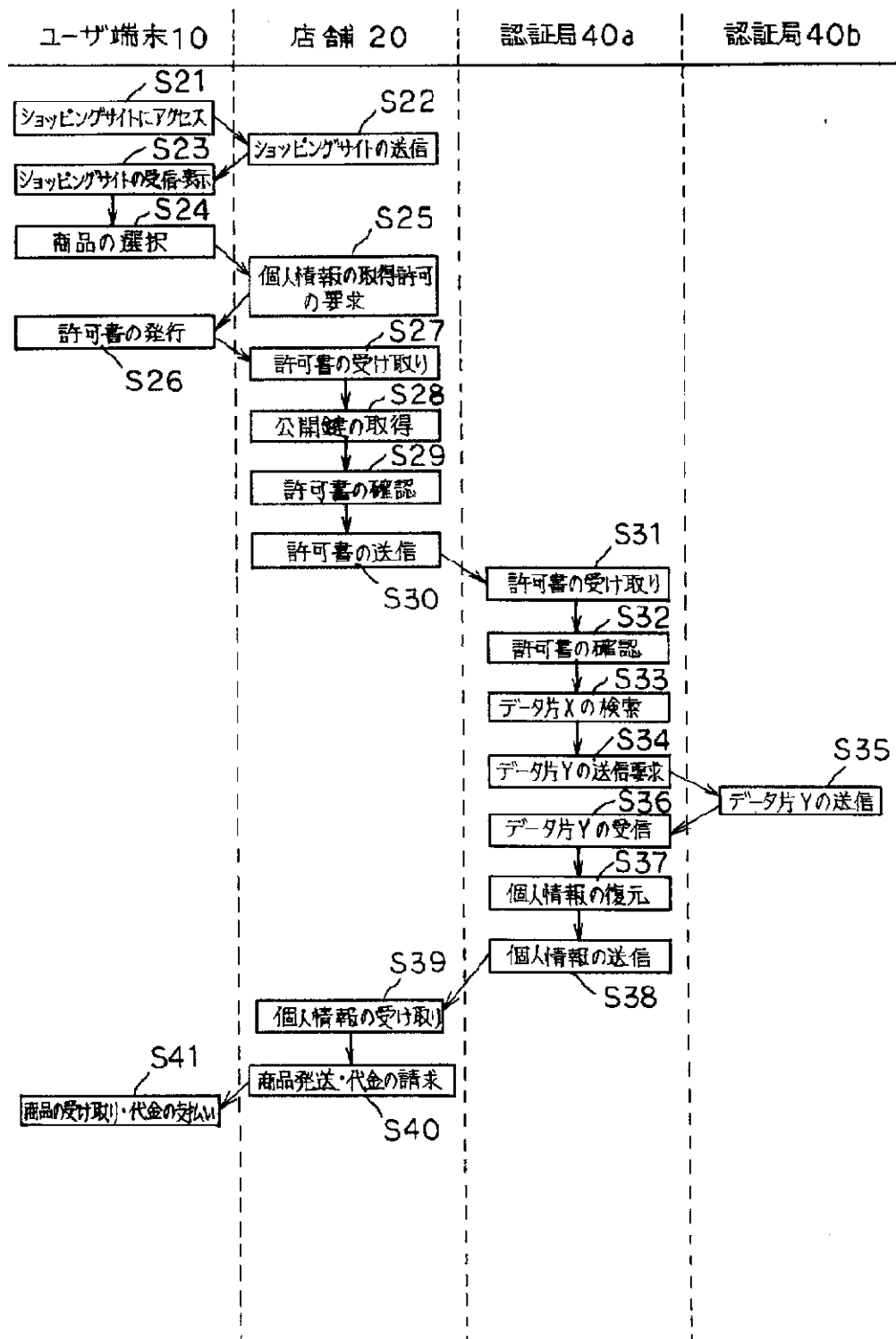
【図6】



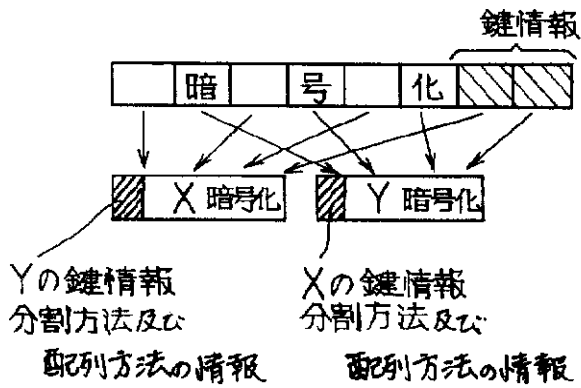
【図7】



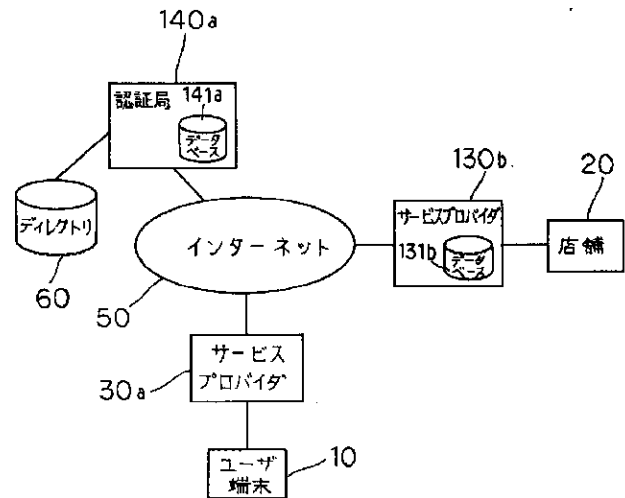
【図3】



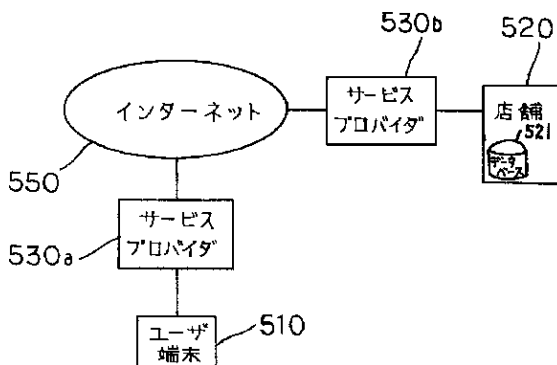
【図9】



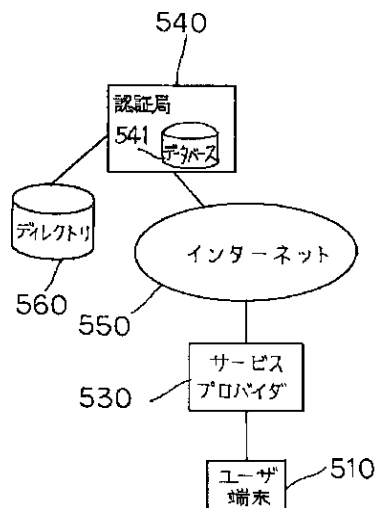
【図10】



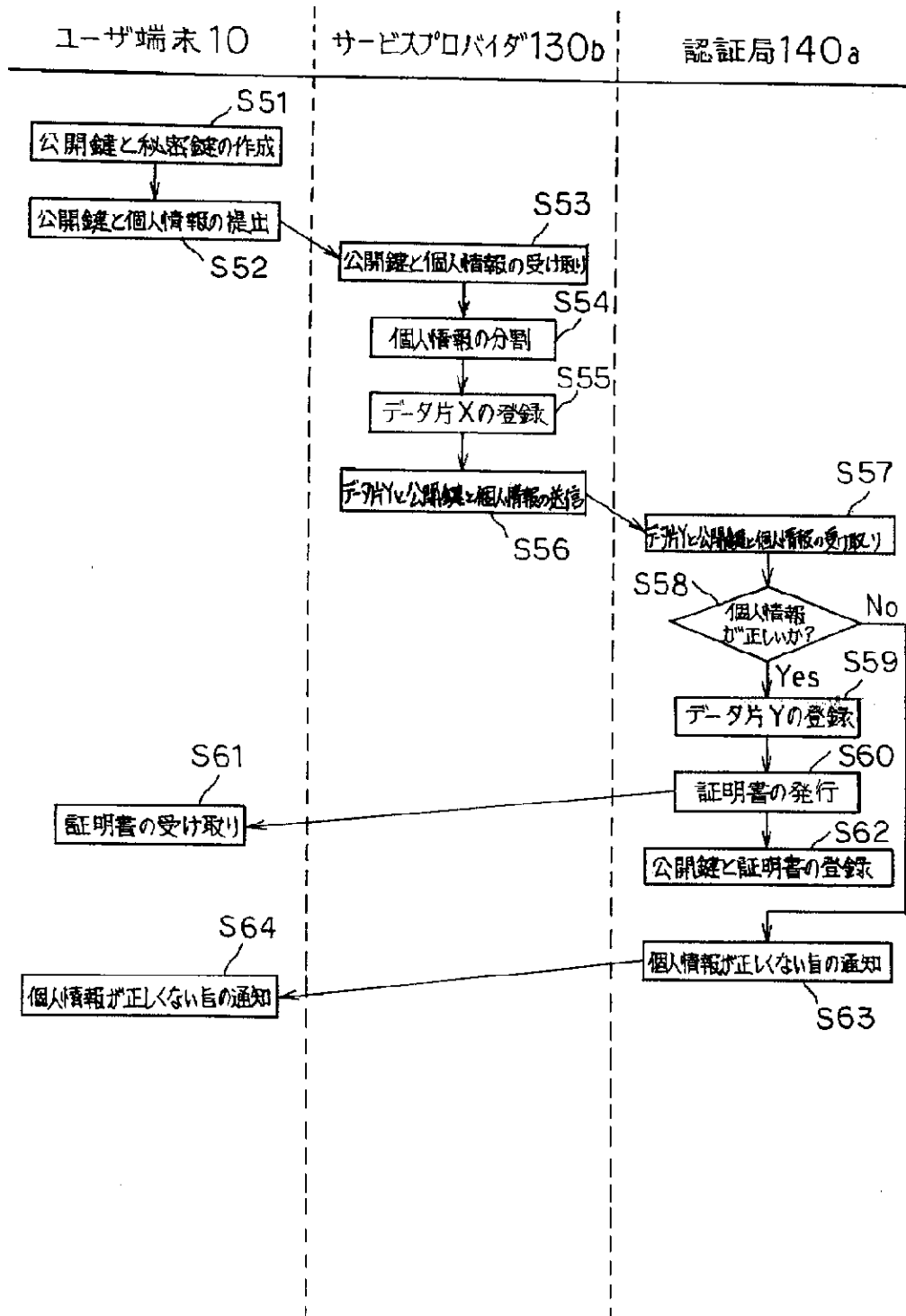
【図13】



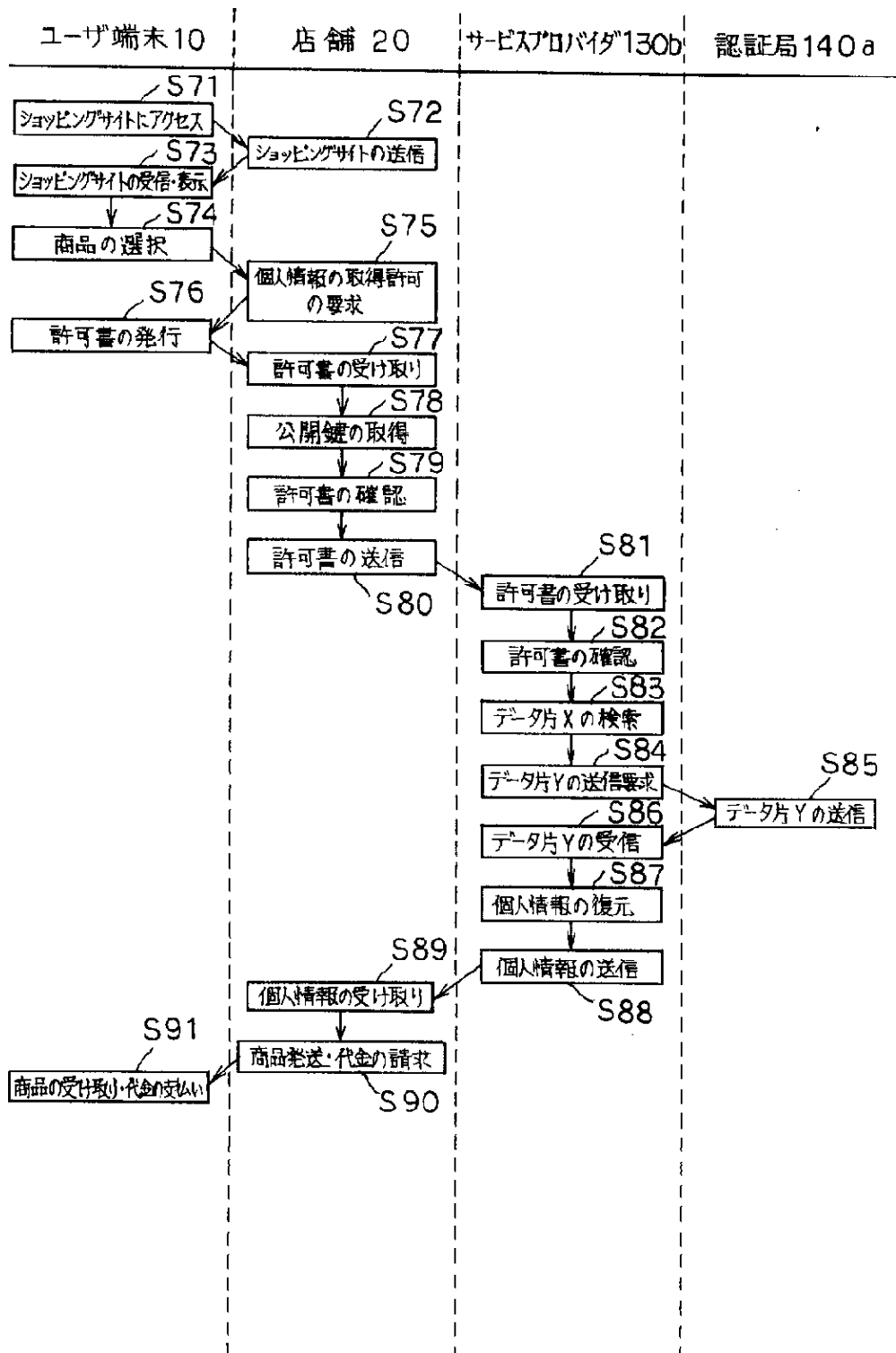
【図15】



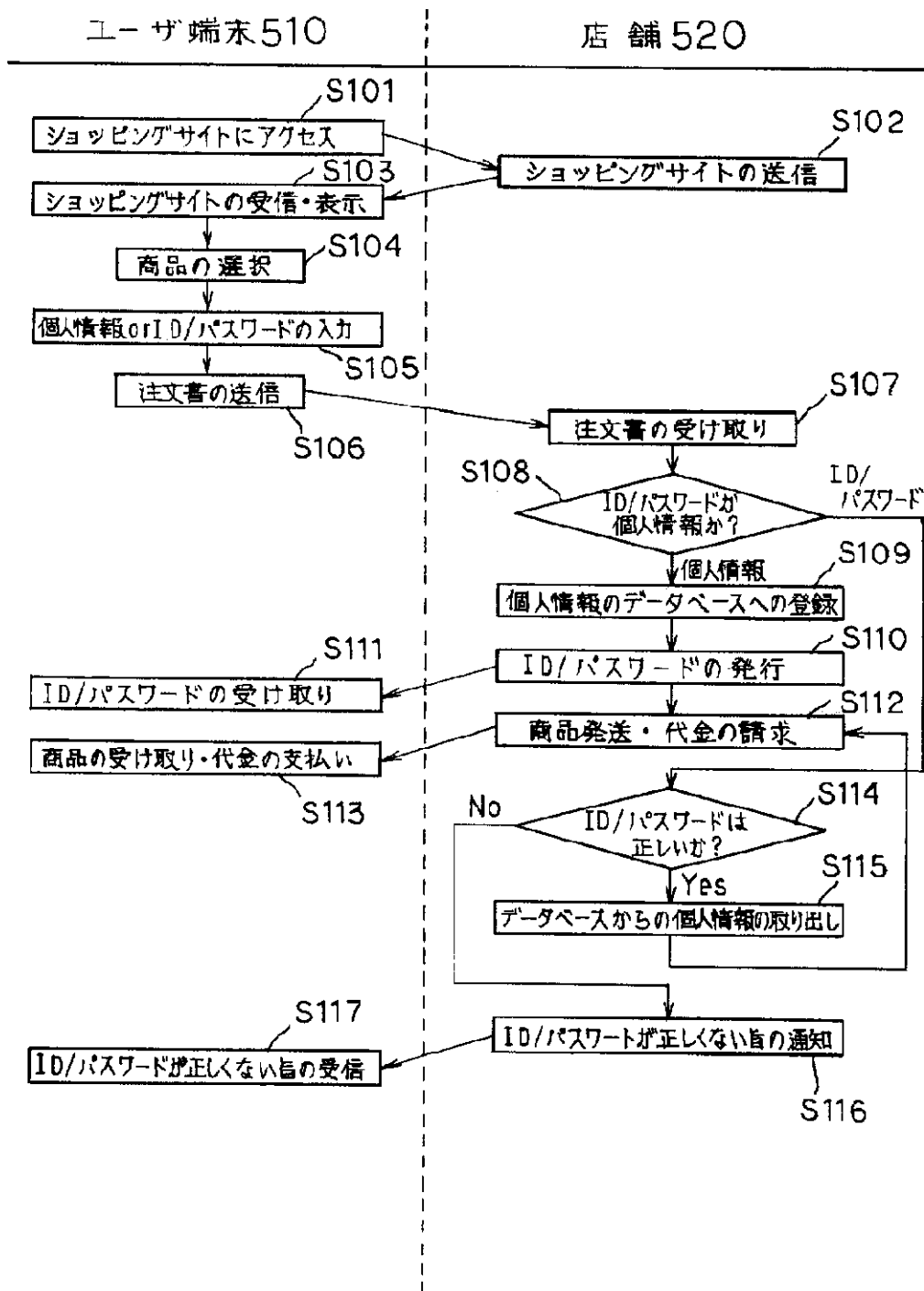
【図11】



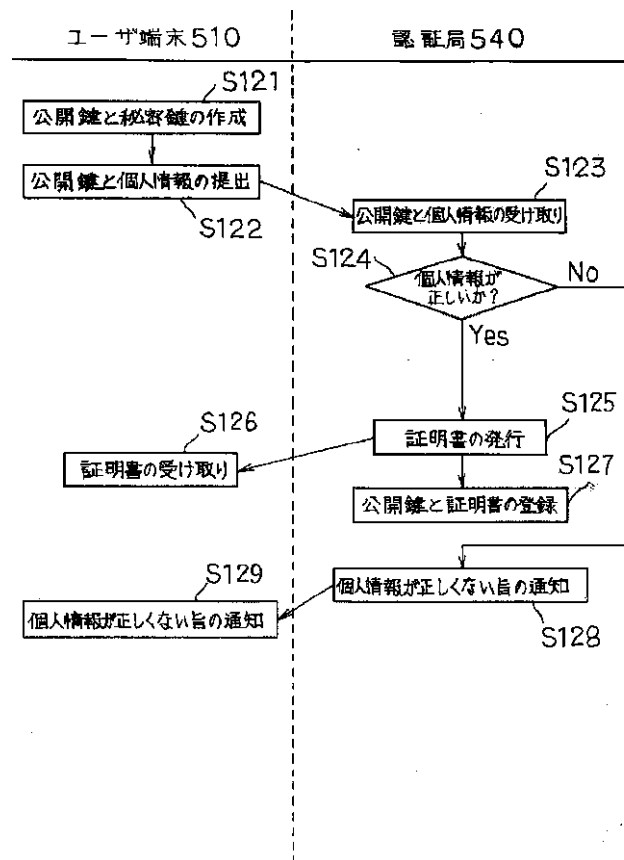
【図12】



【図14】



【図16】



フロントページの続き

(72)発明者 川▲辺▼ 滋
東京都港区芝五丁目7番1号 日本電気株
式会社内

(72)発明者 三露 範久
東京都港区芝五丁目7番1号 日本電気株
式会社内

Fターム(参考) 5B085 AE02 AE29

5J104 AA07 AA16 EA05 EA13 KA01

KA05 MA04 NA01 NA02 PA07