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

特許第4768979号
(P4768979)

(45)発行日　平成23年9月7日(2011.9.7)　(24)登録日　平成23年6月24日(2011.6.24)

| (51)Int.Cl. | | F I | | |
|---|---|---|---|---|
| G06Q 30/00 | (2006.01) | G06F | 17/60 | 318G |
| G06Q 10/00 | (2006.01) | G06F | 17/60 | 170Z |
| G06Q 50/00 | (2006.01) | G06F | 17/60 | 334 |
| H04L 9/32 | (2006.01) | G06F | 17/60 | 512 |
| | | G06F | 17/60 | ZEC |

請求項の数 19　(全 30 頁)　最終頁に続く

(21)出願番号　特願2004-304948 (P2004-304948)
(22)出願日　平成16年10月19日 (2004.10.19)
(65)公開番号　特開2006-119771 (P2006-119771A)
(43)公開日　平成18年5月11日 (2006.5.11)
審査請求日　平成19年7月4日 (2007.7.4)

(73)特許権者　000003078
株式会社東芝
東京都港区芝浦一丁目１番１号
(73)特許権者　301063496
東芝ソリューション株式会社
東京都港区芝浦一丁目１番１号
(74)代理人　100091351
弁理士　河野　哲
(74)代理人　100088683
弁理士　中村　誠
(74)代理人　100108855
弁理士　蔵田　昌俊
(74)代理人　100075672
弁理士　峰　隆司

最終頁に続く

(54)【発明の名称】匿名注文システム、装置及びプログラム

(57)【特許請求の範囲】
【請求項１】
追跡機能を有するグループ署名方式により、商品又はサービスからなる販売対象の匿名注文と、前記匿名注文に応じた販売対象の販売とを実行する匿名注文システムであって、
前記匿名注文をする購入者の個人情報及びグループ署名関連情報を記憶装置に記憶し、販売店から受けた注文ＩＤ及びグループ署名を含む匿名注文情報に基づいて、前記追跡機能により、当該グループ署名を復号して得られたグループ署名関連情報から前記記憶装置内の対応する個人情報を特定し、この個人情報を外部の配送手段による配送のために出力する管理者装置と、
前記購入者の購入者装置から販売対象特定情報及び注文要求を受けると、前記購入者装置に注文ＩＤを発行し、当該販売対象特定情報から当該注文ＩＤを含み販売対象特定情報を含まない注文基本情報と販売対象特定情報を含む注文詳細情報とを生成し、前記購入者装置に前記注文基本情報及び前記注文詳細情報を送り返し、前記購入者装置から前記注文基本情報、前記注文詳細情報を秘匿した秘匿注文詳細情報及びグループ署名を含む匿名注文情報を受けると、当該秘匿注文詳細情報及び当該グループ署名を検証して検証結果が正当のとき、当該匿名注文情報を前記管理者装置に送出する販売店装置と、
前記購入者の操作により、前記販売対象特定情報及び注文要求を前記販売店装置に送信し、前記販売店装置から注文ＩＤを含む前記注文基本情報及び前記注文詳細情報を受けると、前記注文基本情報及び前記注文詳細情報を画面表示し、前記購入者の操作により、注文内容が正しいことが確認された場合には、前記注文基本情報及び前記注文詳細情報に基

づいて、この注文ＩＤ及びグループ署名を含む匿名注文情報を生成し、得られた匿名注文情報を前記販売店装置に送信する購入者装置と
を備えており、
前記購入者装置は、
前記購入者の操作により、前記販売店装置に販売対象特定情報及び注文要求を送信する対象情報送信手段と、
この送信に応じて前記販売店装置から注文ＩＤを含む前記注文基本情報及び前記注文詳細情報を受けると、前記注文基本情報及び前記注文詳細情報を画面表示して前記購入者に注文内容の確認を促し、前記購入者の操作により、注文内容が正しいことが確認された場合には、前記注文詳細情報を秘匿した前記秘匿注文詳細情報として、当該注文詳細情報のハッシュ値を生成する詳細情報生成手段と、
前記グループ署名方式により前記グループ署名を生成するグループ署名生成手段と、
前記注文基本情報及び前記秘匿注文詳細情報を少なくとも含むメッセージ部分と、このメッセージ部分に対して生成した前記グループ署名とを前記匿名注文情報として編集する編集手段と、
前記編集手段により得られた匿名注文情報を前記販売店装置に送信する匿名情報送信手段と
を備えたことを特徴とする匿名注文システム。
【請求項２】
請求項１に記載の匿名注文システムに用いられる前記販売店装置であって、
前記購入者装置から受けた販売対象特定情報及び注文要求に基づいて、注文ＩＤを含む前記注文基本情報及び前記注文詳細情報からなる注文情報を生成し、この注文情報を前記購入者装置に送信する注文情報生成手段と、
前記購入者装置から前記注文基本情報及び前記秘匿注文詳細情報を少なくとも含むメッセージ部分と前記グループ署名とを含む匿名注文情報を受けると、当該秘匿注文詳細情報及び当該グループ署名を検証する署名検証手段と、
この検証の結果が正当のとき、当該匿名注文情報を前記管理者装置に送出する送信手段と
を備えたことを特徴とする販売店装置。
【請求項３】
請求項１に記載の匿名注文システムに用いられる前記販売店装置のプログラムであって、
前記販売店装置のコンピュータを、
前記購入者装置から受けた販売対象特定情報及び注文要求に基づいて、注文ＩＤを含む前記注文基本情報及び前記注文詳細情報からなる注文情報を生成し、この注文情報を前記購入者装置に送信する注文情報生成手段、
前記購入者装置から前記注文基本情報及び前記秘匿注文詳細情報を少なくとも含むメッセージ部分と前記グループ署名とを含む匿名注文情報を受けると、前記販売対象特定情報から計算したハッシュ値によって当該秘匿注文詳細情報を検証し、メモリ内のグループ公開鍵に基づいて、当該グループ署名を検証する署名検証手段、
この署名検証手段による検証の結果がそれぞれ正当のとき、当該匿名注文情報を前記管理者装置に送出する送信手段、
として機能させるためのプログラム。
【請求項４】
追跡機能を有するグループ署名方式により、商品又はサービスからなる販売対象の匿名注文と、前記匿名注文に応じた販売対象の販売とを実行する匿名注文システムに用いられ、
前記匿名注文をする購入者の個人情報及びグループ署名関連情報を記憶装置に記憶し、販売店から受けた注文ＩＤ及びグループ署名を含む匿名注文情報に基づいて、前記追跡機能により、当該グループ署名を復号して得られたグループ署名関連情報から前記記憶装置

内の対応する個人情報を特定し、この個人情報を外部の配送手段による配送のために出力する管理者装置と、

前記購入者の購入者装置から販売対象特定情報及び注文要求を受けると、前記購入者装置に注文ＩＤを発行し、当該販売対象特定情報から当該注文ＩＤを含み販売対象特定情報を含まない注文基本情報と販売対象特定情報を含む注文詳細情報とを生成し、前記購入者装置に前記注文基本情報及び前記注文詳細情報を送り返し、前記購入者装置から前記注文基本情報、前記注文詳細情報を秘匿した秘匿注文詳細情報及びグループ署名を含む匿名注文情報を受けると、当該秘匿注文詳細情報及び当該グループ署名を検証して検証結果が正当のとき、当該匿名注文情報を前記管理者装置に送出する販売店装置と、の両装置と通信可能な、前記購入者の購入者装置であって、

前記購入者の操作により、前記販売店装置に販売対象特定情報及び注文要求を送信する対象情報送信手段と、

この送信に応じて前記販売店装置から注文ＩＤを含む前記注文基本情報及び前記注文詳細情報を受けると、前記注文基本情報及び前記注文詳細情報を画面表示し、前記購入者の操作により、注文内容が正しいことが確認された場合には、前記注文基本情報及び前記注文詳細情報に基づいて、この注文ＩＤ及びグループ署名を含む匿名注文情報を生成する匿名情報生成手段と、

得られた匿名注文情報を前記販売店装置に送信する匿名情報送信手段と

を備えており、

前記匿名情報生成手段は、

前記注文ＩＤを含む前記注文基本情報及び前記注文詳細情報を画面表示して前記購入者に注文内容の確認を促し、前記購入者の操作により、注文内容が正しいことが確認された場合には、前記注文詳細情報を秘匿した前記秘匿注文詳細情報として、当該注文詳細情報のハッシュ値を生成する詳細情報生成手段と、

前記グループ署名方式により前記グループ署名を生成するグループ署名生成手段と、

前記注文基本情報及び前記秘匿注文詳細情報を少なくとも含むメッセージ部分と、このメッセージ部分に対して生成した前記グループ署名とを前記匿名注文情報として編集する編集手段と

を備えたことを特徴とする購入者装置。

【請求項５】

請求項４に記載の購入者装置において、

前記管理者装置へのメッセージを前記管理者装置の公開鍵により暗号化して秘匿し、管理者秘匿メッセージを生成する第１秘匿メッセージ生成手段を備え、

前記編集手段は、前記管理者秘匿メッセージを前記メッセージ部分に含めることを特徴とする購入者装置。

【請求項６】

請求項５に記載の購入者装置において、

前記管理者装置へのメッセージは、購入者とは異なる送り先情報を含むことを特徴とする購入者装置。

【請求項７】

請求項４乃至請求項６のいずれか１項に記載の購入者装置において、

前記販売店へのメッセージを前記販売店装置の公開鍵により暗号化して秘匿し、販売店秘匿メッセージを生成する第２秘匿メッセージ生成手段を備え、

前記編集手段は、前記販売店秘匿メッセージを前記メッセージ部分に含めることを特徴とする購入者装置。

【請求項８】

追跡機能を有するグループ署名方式により、商品又はサービスからなる販売対象の匿名注文と、前記匿名注文に応じた販売対象の販売及び提供とを実行するための匿名注文システムに用いられ、

前記匿名注文をする購入者の個人情報及びグループ署名関連情報を記憶装置に記憶し、

注文ＩＤ及びグループ署名を含む匿名注文情報を受けると、前記追跡機能により、当該グループ署名を復号して得られたグループ署名関連情報から前記記憶装置内の対応する個人情報を特定するための管理者装置と、

前記購入者の購入者装置から販売対象特定情報及び注文要求を受けると、前記購入者装置に注文ＩＤを発行し、当該販売対象特定情報から当該注文ＩＤを含み販売対象特定情報を含まない注文基本情報と販売対象特定情報を含む注文詳細情報とを生成し、前記購入者装置に前記注文基本情報及び前記注文詳細情報を送り返し、前記購入者装置から前記注文基本情報、前記注文詳細情報を秘匿した秘匿注文詳細情報及びグループ署名を含む匿名注文情報を受けると、当該秘匿注文詳細情報及び当該グループ署名を検証して検証結果が正当のとき、当該注文ＩＤに対応する販売対象を前記購入者に販売するための販売店装置と、の両装置と通信可能な、前記購入者の購入者装置であって、

前記購入者の操作により、前記販売店装置に販売対象特定情報及び注文要求を送信する対象情報送信手段と、

この送信に応じて前記販売店装置から注文ＩＤを含む前記注文基本情報及び前記注文詳細情報を受けると、前記注文基本情報及び前記注文詳細情報を画面表示して前記購入者に注文内容の確認を促し、前記購入者の操作により、注文内容が正しいことが確認された場合には、前記注文基本情報及び前記注文詳細情報に基づいて、前記注文詳細情報を秘匿した前記秘匿注文詳細情報として、当該注文詳細情報のハッシュ値を生成する詳細情報生成手段と、

前記グループ署名方式により前記グループ署名を生成するグループ署名生成手段と、

前記注文基本情報及び前記秘匿注文詳細情報を少なくとも含むメッセージ部分と、このメッセージ部分に対して生成した前記グループ署名とを前記匿名注文情報として編集する編集手段と、

前記編集手段により得られた匿名注文情報を前記販売店装置に送信する匿名情報送信手段と

を備えたことを特徴とする購入者装置。

【請求項９】

追跡機能を有するグループ署名方式により、商品又はサービスからなる販売対象の匿名注文と、前記匿名注文に応じた販売対象の販売及び提供とを実行するための匿名注文システムに用いられ、

前記匿名注文をする購入者の個人情報及びグループ署名関連情報を記憶装置に記憶し、注文ＩＤ及びグループ署名を含む匿名注文情報を受けると、前記追跡機能により、当該グループ署名を復号して得られたグループ署名関連情報から前記記憶装置内の対応する個人情報を特定するための管理者装置と、

前記購入者の購入者装置から販売対象特定情報及び注文要求を受けると、前記購入者装置に注文ＩＤを発行し、当該販売対象特定情報から当該注文ＩＤを含み販売対象特定情報を含まない注文基本情報と販売対象特定情報を含む注文詳細情報とを生成し、前記購入者装置に前記注文基本情報及び前記注文詳細情報を送り返し、前記購入者装置から前記注文基本情報、前記注文詳細情報を秘匿した秘匿注文詳細情報及びグループ署名を含む匿名注文情報を受けると、当該秘匿注文詳細情報及び当該グループ署名を検証して検証結果が正当のとき、当該注文ＩＤに対応する販売対象を前記購入者に販売するための販売店装置と、の両装置と通信可能な、前記購入者の購入者装置であって、

前記購入者の操作により、前記販売店装置に販売対象特定情報及び注文要求を送信する対象情報送信手段と、

この送信に応じて前記販売店装置から注文ＩＤを含む前記注文基本情報及び前記注文詳細情報を受けると、前記注文基本情報及び前記注文詳細情報を画面表示して前記購入者に注文内容の確認を促し、前記購入者の操作により、注文内容が正しいことが確認された場合には、前記注文詳細情報を秘匿した前記秘匿注文詳細情報として、当該注文詳細情報のハッシュ値を生成する詳細情報生成手段と、

前記管理者装置へのメッセージを前記管理者装置の公開鍵により暗号化して秘匿し、管

理者秘匿メッセージを生成する管理者秘匿メッセージ生成手段と、
前記グループ署名方式により前記グループ署名を生成するグループ署名生成手段と、
前記注文基本情報、前記秘匿注文詳細情報及び前記管理者秘匿メッセージを少なくとも含むメッセージ部分と、このメッセージ部分に対して生成した前記グループ署名とを前記匿名注文情報として編集する編集手段と、
前記編集手段により得られた匿名注文情報を前記販売店装置に送信する匿名情報送信手段と
を備えたことを特徴とする購入者装置。
【請求項１０】
追跡機能を有するグループ署名方式により、商品又はサービスからなる販売対象の匿名注文と、前記匿名注文に応じた販売対象の販売及び提供とを実行するための匿名注文システムに用いられ、
前記匿名注文をする購入者の個人情報及びグループ署名関連情報を記憶装置に記憶し、注文ＩＤ及びグループ署名を含む匿名注文情報を受けると、前記追跡機能により、当該グループ署名を復号して得られたグループ署名関連情報から前記記憶装置内の対応する個人情報を特定するための管理者装置と、
前記購入者の購入者装置から販売対象特定情報及び注文要求を受けると、前記購入者装置に注文ＩＤを発行し、当該販売対象特定情報から当該注文ＩＤを含み販売対象特定情報を含まない注文基本情報と販売対象特定情報を含む注文詳細情報とを生成し、前記購入者装置に前記注文基本情報及び前記注文詳細情報を送り返し、前記購入者装置から前記注文基本情報、前記注文詳細情報を秘匿した秘匿注文詳細情報及びグループ署名を含む匿名注文情報を受けると、当該秘匿注文詳細情報及び当該グループ署名を検証して検証結果が正当のとき、当該注文ＩＤに対応する販売対象を前記購入者に販売するための販売店装置と、の両装置と通信可能な、前記購入者の購入者装置であって、
前記購入者の操作により、前記販売店装置に販売対象特定情報及び注文要求を送信する対象情報送信手段と、
この送信に応じて前記販売店装置から注文ＩＤを含む前記注文基本情報及び前記注文詳細情報を受けると、前記注文基本情報及び前記注文詳細情報を画面表示して前記購入者に注文内容の確認を促し、前記購入者の操作により、注文内容が正しいことが確認された場合には、前記注文詳細情報を秘匿した前記秘匿注文詳細情報として、当該注文詳細情報のハッシュ値を生成する詳細情報生成手段と、
前記管理者装置へのメッセージとして、購入者とは異なる送り先情報を含むメッセージを前記管理者装置の公開鍵により暗号化して秘匿し、管理者秘匿メッセージを生成する管理者秘匿メッセージ生成手段と、
前記グループ署名方式により前記グループ署名を生成するグループ署名生成手段と、
前記注文基本情報、前記秘匿注文詳細情報及び前記管理者秘匿メッセージを少なくとも含むメッセージ部分と、このメッセージ部分に対して生成した前記グループ署名とを前記匿名注文情報として編集する編集手段と、
前記編集手段により得られた匿名注文情報を前記販売店装置に送信する匿名情報送信手段と
を備えたことを特徴とする購入者装置。
【請求項１１】
追跡機能を有するグループ署名方式により、商品又はサービスからなる販売対象の匿名注文と、前記匿名注文に応じた販売対象の販売及び提供とを実行するための匿名注文システムに用いられ、
前記匿名注文をする購入者の個人情報及びグループ署名関連情報を記憶装置に記憶し、注文ＩＤ及びグループ署名を含む匿名注文情報を受けると、前記追跡機能により、当該グループ署名を復号して得られたグループ署名関連情報から前記記憶装置内の対応する個人情報を特定するための管理者装置と、
前記購入者の購入者装置から販売対象特定情報及び注文要求を受けると、前記購入者装

置に注文ＩＤを発行し、当該販売対象特定情報から当該注文ＩＤを含み販売対象特定情報を含まない注文基本情報と販売対象特定情報を含む注文詳細情報とを生成し、前記購入者装置に前記注文基本情報及び前記注文詳細情報を送り返し、前記購入者装置から前記注文基本情報、前記注文詳細情報を秘匿した秘匿注文詳細情報及びグループ署名を含む匿名注文情報を受けると、当該秘匿注文詳細情報及び当該グループ署名を検証して検証結果が正当のとき、当該注文ＩＤに対応する販売対象を前記購入者に販売するための販売店装置と、の両装置と通信可能な、前記購入者の購入者装置であって、

前記購入者の操作により、前記販売店装置に販売対象特定情報及び注文要求を送信する対象情報送信手段と、

この送信に応じて前記販売店装置から注文ＩＤを含む前記注文基本情報及び前記注文詳細情報を受けると、前記注文基本情報及び前記注文詳細情報を画面表示して前記購入者に注文内容の確認を促し、前記購入者の操作により、注文内容が正しいことが確認された場合には、前記注文詳細情報を秘匿した前記秘匿注文詳細情報として、当該注文詳細情報のハッシュ値を生成する詳細情報生成手段と、

前記販売店へのメッセージを前記販売店装置の公開鍵により暗号化して秘匿し、販売店秘匿メッセージを生成する販売店秘匿メッセージ生成手段と、

前記グループ署名方式により前記グループ署名を生成するグループ署名生成手段と、

前記注文基本情報、前記秘匿注文詳細情報及び前記販売店秘匿メッセージを少なくとも含むメッセージ部分と、このメッセージ部分に対して生成した前記グループ署名とを前記匿名注文情報として編集する編集手段と、

前記編集手段により得られた匿名注文情報を前記販売店装置に送信する匿名情報送信手段と

を備えたことを特徴とする購入者装置。

【請求項１２】

追跡機能を有するグループ署名方式により、商品又はサービスからなる販売対象の匿名注文と、前記匿名注文に応じた販売対象の販売とを実行する匿名注文システムに用いられ、

前記匿名注文をする購入者の個人情報及びグループ署名関連情報を記憶装置に記憶し、販売店から受けた注文ＩＤ及びグループ署名を含む匿名注文情報に基づいて、前記追跡機能により、当該グループ署名を復号して得られたグループ署名関連情報から前記記憶装置内の対応する個人情報を特定し、この個人情報を外部の配送手段による配送のために出力する管理者装置と、

前記購入者の購入者装置から販売対象特定情報及び注文要求を受けると、前記購入者装置に注文ＩＤを発行し、当該販売対象特定情報から当該注文ＩＤを含み販売対象特定情報を含まない注文基本情報と販売対象特定情報を含む注文詳細情報とを生成し、前記購入者装置に前記注文基本情報及び前記注文詳細情報を送り返し、前記購入者装置から前記注文基本情報、前記注文詳細情報を秘匿した秘匿注文詳細情報及びグループ署名を含む匿名注文情報を受けると、当該秘匿注文詳細情報及び当該グループ署名を検証して検証結果が正当のとき、当該匿名注文情報を前記管理者装置に送出する販売店装置と、の両装置と通信可能な、前記購入者の購入者装置のプログラムであって、

前記購入者装置のコンピュータを、

前記購入者の操作により、前記販売店装置に販売対象特定情報及び注文要求を送信する対象情報送信手段、

この送信に応じて前記販売店装置から注文ＩＤを含む前記注文基本情報及び前記注文詳細情報を受けると、前記注文基本情報及び前記注文詳細情報を画面表示し、前記購入者の操作により、注文内容が正しいことが確認された場合には、前記注文基本情報及び前記注文詳細情報とメモリ内のメンバ秘密鍵及びメンバ証明書に基づいて、この注文ＩＤ及びグループ署名を含む匿名注文情報を生成する匿名情報生成手段、

得られた匿名注文情報を前記販売店装置に送信する匿名情報送信手段、

として機能させ、

前記匿名情報生成手段は、
前記注文ＩＤを含む前記注文基本情報及び前記注文詳細情報を画面表示して前記購入者に注文内容の確認を促し、前記購入者の操作により、注文内容が正しいことが確認された場合には、前記注文詳細情報を秘匿した前記秘匿注文詳細情報として、当該注文詳細情報のハッシュ値を生成する詳細情報生成手段と、
前記グループ署名方式により前記グループ署名を生成するグループ署名生成手段と、
前記注文基本情報及び前記秘匿注文詳細情報を少なくとも含むメッセージ部分と、このメッセージ部分に対して生成した前記グループ署名とを前記匿名注文情報として編集する編集手段と
を含むことを特徴とするプログラム。
【請求項１３】
請求項１２に記載のプログラムにおいて、
前記購入者装置のコンピュータを、
前記管理者装置へのメッセージを前記管理者装置の公開鍵により暗号化して秘匿し、管理者秘匿メッセージを生成する第１秘匿メッセージ生成手段として機能させ、
前記編集手段は、前記管理者秘匿メッセージを前記メッセージ部分に含めることを特徴とするプログラム。
【請求項１４】
請求項１３に記載のプログラムにおいて、
前記管理者装置へのメッセージは、購入者とは異なる送り先情報を含むことを特徴とするプログラム。
【請求項１５】
請求項１２乃至請求項１４のいずれか１項に記載のプログラムにおいて、
前記購入者装置のコンピュータを、
前記販売店へのメッセージを前記販売店装置の公開鍵により暗号化して秘匿し、販売店秘匿メッセージを生成する第２秘匿メッセージ生成手段として機能させ、
前記編集手段は、前記販売店秘匿メッセージを前記メッセージ部分に含めることを特徴とするプログラム。
【請求項１６】
追跡機能を有するグループ署名方式により、商品又はサービスからなる販売対象の匿名注文と、前記匿名注文に応じた販売対象の販売及び提供とを実行するための匿名注文システムに用いられ、
前記匿名注文をする購入者の個人情報及びグループ署名関連情報を記憶装置に記憶し、注文ＩＤ及びグループ署名を含む匿名注文情報を受けると、前記追跡機能により、当該グループ署名を復号して得られたグループ署名関連情報から前記記憶装置内の対応する個人情報を特定するための管理者装置と、
前記購入者の購入者装置から販売対象特定情報及び注文要求を受けると、前記購入者装置に注文ＩＤを発行し、当該販売対象特定情報から当該注文ＩＤを含み販売対象特定情報を含まない注文基本情報と販売対象特定情報を含む注文詳細情報とを生成し、前記購入者装置に前記注文基本情報及び前記注文詳細情報を送り返し、前記購入者装置から前記注文基本情報、前記注文詳細情報を秘匿した秘匿注文詳細情報及びグループ署名を含む匿名注文情報を受けると、当該秘匿注文詳細情報及び当該グループ署名を検証して検証結果が正当のとき、当該注文ＩＤに対応する販売対象を前記購入者に販売するための販売店装置と、の両装置と通信可能な前記購入者の購入者装置に用いられるプログラムであって、
前記購入者装置のコンピュータを、
前記購入者の操作により、前記販売店装置に販売対象特定情報及び注文要求を送信する対象情報送信手段、
この送信に応じて前記販売店装置から注文ＩＤを含む前記注文基本情報及び前記注文詳細情報を受けると、前記注文基本情報及び前記注文詳細情報を画面表示して前記購入者に注文内容の確認を促し、前記購入者の操作により、注文内容が正しいことが確認された場

合には、前記注文詳細情報を秘匿した前記秘匿注文詳細情報として、当該注文詳細情報のハッシュ値を生成する詳細情報生成手段、
前記グループ署名方式により前記グループ署名を生成するグループ署名生成手段、
前記注文基本情報及び前記秘匿注文詳細情報を少なくとも含むメッセージ部分と、このメッセージ部分に対して生成した前記グループ署名とを前記匿名注文情報として編集する編集手段、
前記編集手段により得られた匿名注文情報を前記販売店装置に送信する匿名情報送信手段、
として機能させるためのプログラム。
【請求項１７】
追跡機能を有するグループ署名方式により、商品又はサービスからなる販売対象の匿名注文と、前記匿名注文に応じた販売対象の販売及び提供とを実行するための匿名注文システムに用いられ、
前記匿名注文をする購入者の個人情報及びグループ署名関連情報を記憶装置に記憶し、注文ＩＤ及びグループ署名を含む匿名注文情報を受けると、前記追跡機能により、当該グループ署名を復号して得られたグループ署名関連情報から前記記憶装置内の対応する個人情報を特定するための管理者装置と、
前記購入者の購入者装置から販売対象特定情報及び注文要求を受けると、前記購入者装置に注文ＩＤを発行し、当該販売対象特定情報から当該注文ＩＤを含み販売対象特定情報を含まない注文基本情報と販売対象特定情報を含む注文詳細情報とを生成し、前記購入者装置に前記注文基本情報及び前記注文詳細情報を送り返し、前記購入者装置から前記注文基本情報、前記注文詳細情報を秘匿した秘匿注文詳細情報及びグループ署名を含む匿名注文情報を受けると、当該秘匿注文詳細情報及び当該グループ署名を検証して検証結果が正当のとき、当該注文ＩＤに対応する販売対象を前記購入者に販売するための販売店装置と、の両装置と通信可能な、前記購入者の購入者装置に用いられるプログラムであって、
前記購入者装置のコンピュータを、
前記購入者の操作により、前記販売店装置に販売対象特定情報及び注文要求を送信する対象情報送信手段、
この送信に応じて前記販売店装置から注文ＩＤを含む前記注文基本情報及び前記注文詳細情報を受けると、前記注文基本情報及び前記注文詳細情報を画面表示して前記購入者に注文内容の確認を促し、前記購入者の操作により、注文内容が正しいことが確認された場合には、前記注文詳細情報を秘匿した前記秘匿注文詳細情報として、当該注文詳細情報のハッシュ値を生成する詳細情報生成手段、
前記管理者装置へのメッセージを前記管理者装置の公開鍵により暗号化して秘匿し、管理者秘匿メッセージを生成する管理者秘匿メッセージ生成手段、
前記グループ署名方式により前記グループ署名を生成するグループ署名生成手段、
前記注文基本情報、前記秘匿注文詳細情報及び前記管理者秘匿メッセージを少なくとも含むメッセージ部分と、このメッセージ部分に対して生成した前記グループ署名とを前記匿名注文情報として編集する編集手段、
前記編集手段により得られた匿名注文情報を前記販売店装置に送信する匿名情報送信手段、
として機能させるためのプログラム。
【請求項１８】
追跡機能を有するグループ署名方式により、商品又はサービスからなる販売対象の匿名注文と、前記匿名注文に応じた販売対象の販売及び提供とを実行するための匿名注文システムに用いられ、
前記匿名注文をする購入者の個人情報及びグループ署名関連情報を記憶装置に記憶し、注文ＩＤ及びグループ署名を含む匿名注文情報を受けると、前記追跡機能により、当該グループ署名を復号して得られたグループ署名関連情報から前記記憶装置内の対応する個人情報を特定するための管理者装置と、

前記購入者の購入者装置から販売対象特定情報及び注文要求を受けると、前記購入者装置に注文ＩＤを発行し、当該販売対象特定情報から当該注文ＩＤを含み販売対象特定情報を含まない注文基本情報と販売対象特定情報を含む注文詳細情報とを生成し、前記購入者装置に前記注文基本情報及び前記注文詳細情報を送り返し、前記購入者装置から前記注文基本情報、前記注文詳細情報を秘匿した秘匿注文詳細情報及びグループ署名を含む匿名注文情報を受けると、当該秘匿注文詳細情報及び当該グループ署名を検証して検証結果が正当のとき、当該注文ＩＤに対応する販売対象を前記購入者に販売するための販売店装置と、の両装置と通信可能な、前記購入者の購入者装置に用いられるプログラムであって、

前記購入者装置のコンピュータを、

前記購入者の操作により、前記販売店装置に販売対象特定情報及び注文要求を送信する対象情報送信手段、

この送信に応じて前記販売店装置から注文ＩＤを含む前記注文基本情報及び前記注文詳細情報を受けると、前記注文基本情報及び前記注文詳細情報を画面表示して前記購入者に注文内容の確認を促し、前記購入者の操作により、注文内容が正しいことが確認された場合には、前記注文詳細情報を秘匿した前記秘匿注文詳細情報として、当該注文詳細情報のハッシュ値を生成する詳細情報生成手段、

前記管理者装置へのメッセージとして、購入者とは異なる送り先情報を含むメッセージを前記管理者装置の公開鍵により暗号化して秘匿し、管理者秘匿メッセージを生成する管理者秘匿メッセージ生成手段、

前記グループ署名方式により前記グループ署名を生成するグループ署名生成手段、

前記注文基本情報、前記秘匿注文詳細情報及び前記管理者秘匿メッセージを少なくとも含むメッセージ部分と、このメッセージ部分に対して生成した前記グループ署名とを前記匿名注文情報として編集する編集手段、

前記編集手段により得られた匿名注文情報を前記販売店装置に送信する匿名情報送信手段、

として機能させるためのプログラム。

【請求項１９】

追跡機能を有するグループ署名方式により、商品又はサービスからなる販売対象の匿名注文と、前記匿名注文に応じた販売対象の販売及び提供とを実行するための匿名注文システムに用いられ、

前記匿名注文をする購入者の個人情報及びグループ署名関連情報を記憶装置に記憶し、注文ＩＤ及びグループ署名を含む匿名注文情報を受けると、前記追跡機能により、当該グループ署名を復号して得られたグループ署名関連情報から前記記憶装置内の対応する個人情報を特定するための管理者装置と、

前記購入者の購入者装置から販売対象特定情報及び注文要求を受けると、前記購入者装置に注文ＩＤを発行し、当該販売対象特定情報から当該注文ＩＤを含み販売対象特定情報を含まない注文基本情報と販売対象特定情報を含む注文詳細情報とを生成し、前記購入者装置に前記注文基本情報及び前記注文詳細情報を送り返し、前記購入者装置から前記注文基本情報、前記注文詳細情報を秘匿した秘匿注文詳細情報及びグループ署名を含む匿名注文情報を受けると、当該秘匿注文詳細情報及び当該グループ署名を検証して検証結果が正当のとき、当該注文ＩＤに対応する販売対象を前記購入者に販売するための販売店装置と、の両装置と通信可能な、前記購入者の購入者装置に用いられるプログラムであって、

前記購入者装置のコンピュータを、

前記購入者の操作により、前記販売店装置に販売対象特定情報及び注文要求を送信する対象情報送信手段、

この送信に応じて前記販売店装置から注文ＩＤを含む前記注文基本情報及び前記注文詳細情報を受けると、前記注文基本情報及び前記注文詳細情報を画面表示して前記購入者に注文内容の確認を促し、前記購入者の操作により、注文内容が正しいことが確認された場合には、前記注文詳細情報を秘匿した前記秘匿注文詳細情報として、当該注文詳細情報のハッシュ値を生成する詳細情報生成手段、

前記販売店へのメッセージを前記販売店装置の公開鍵により暗号化して秘匿し、販売店秘匿メッセージを生成する販売店秘匿メッセージ生成手段、
前記グループ署名方式により前記グループ署名を生成するグループ署名生成手段、
前記注文基本情報、前記秘匿注文詳細情報及び前記販売店秘匿メッセージを少なくとも含むメッセージ部分と、このメッセージ部分に対して生成した前記グループ署名とを前記匿名注文情報として編集する編集手段、
前記編集手段により得られた匿名注文情報を前記販売店装置に送信する匿名情報送信手段、
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、グループ署名方式を用いた匿名注文システム、装置及びプログラムに係り、特に、サービス提供者が個人情報を管理する必要が無く、利用者が匿名性を有して注文内容に関するプライバシを保護し得る匿名注文システム、装置及びプログラムに関する。

【背景技術】

【０００２】

グループ署名は、１９９１年チャウム（Chaum）ら（非特許文献１参照）により提案された以下の性質（１）～（４）を満たす電子署名方式であり、匿名性を持った電子署名と言える。

【０００３】

（１）グループに所属するメンバのみが、メンバ署名鍵を用いてグループを代表する署名（グループ署名）を生成できる。

【０００４】

（２）グループ公開鍵により、グループ署名の正当性（グループメンバが生成した署名であること）を検証できる。

【０００５】

（３）グループ署名から署名を生成したグループメンバを特定することはできない（Anonymity；匿名性）。

【０００６】

（４）グループ秘密鍵により、グループ署名から署名を生成したグループメンバを特定（トレース）できる（Traceability；追跡能力）。

【０００７】

しかしながら、チャウムらにより提案されたグループ署名方式は、署名サイズ・鍵サイズがグループメンバ数に依存する等により、効率が非実用的である。また、安全性が不十分である。その後、グループ署名方式が満たすべき安全性としては、以下の要件が提案されている。

【０００８】

２つのグループ署名が、同一のグループメンバが署名したものかどうか判別できない（Unlinkability；非結合性）。

【０００９】

グループメンバが結託しても、メンバをトレース不可能なグループ署名を生成することができない（Coalition-Resistance；耐結託性）。

【００１０】

グループ秘密鍵を知っていても、グループメンバになりすましてグループ署名を生成することができない（Exculpability；弁解能力）。

【００１１】

以降、多くのグループ署名方式が提案されてきたが、その中でも２０００年アテニース（Ateniese）ら（非特許文献２参照）により提案されたグループ署名方式は、署名サイズ・鍵サイズがグループメンバ数に依存せず、さらに強ＲＳＡ仮定および決定性ディフィー

ヘルマン（Decisional Diffie-Hellman）問題の困難性仮定の下で上記の安全性要件を全て満たすことが証明された方式であり、効率・安全性の両面で実用に耐えうる唯一の方式であると考えられる。なお、強ＲＳＡ仮定とは、ｎ＝ｐｑ、ｐ＝２ｐ’＋１、ｑ＝２ｑ’＋１、（ｐ，ｑ，ｐ’，ｑ’：素数）を満たすｎ、平方剰余群ＱＲ（ｎ）（位数ｐ’ｑ’）の任意の元ｕ∈ＱＲ（ｎ）が与えられたとき、$z \equiv u^e \pmod{n}$を満たすｅ＞１を見つけることが困難という仮定である。決定性ディフィーヘルマン問題とは、巡回群Ｇ＝〈ｇ〉（ここでは上記ｎの平方剰余群ＱＲ（ｎ））について、ｇ，$g^x$，$g^y$，$g^z$∈Ｇが与えられたとき，$g^{xy}$と、$g^z$とが等しいかどうかを決める問題である。

【００１２】

ここで、非特許文献１，２等に記載されたグループ署名方式に類似するグループ署名方式を標準的な例として述べる（非特許文献３参照）。ここで、次の表１は、この標準的なグループ署名方式の記号とその説明を示している。

【表１】

| 表記記号 | 説明 |
|---|---|
| ＳＰＫ | 知識の署名 |
| $\alpha$，$\beta$ | 述語を満たすパラメータ |
| ｍ | メッセージ |
| $\varepsilon$ | 偽造を許す確率を定める定数 |
| Ｈ（ ） | ハッシュ関数 |
| ｋ | ハッシュ関数の演算後のビット長 |
| ｇ | 乗法群の生成元 |
| Ｇ | 乗法群：Ｇ＝＜ｇ＞ |
| Ｌ | 生成元ｇの位数 |
| ｙ | 署名者の公開鍵、乗法群Ｇの元：ｙ∈Ｇ |
| ｘ | 署名者の秘密鍵：$y = g^x$ |
| ｒ | 乱数 |
| ｕ | 署名者の計算結果：$u = g^r$など |
| ｅ | ハッシュ関数の計算結果：ｅ＝Ｈ（ｇ‖ｙ‖ｕ‖ｍ） |
| ｖ | 署名者の計算結果：ｖ＝ｒ－ｅｘなど |
| ＧＭ | グループ管理者 |
| ＥＭ | 追跡機関 |
| Ａ | メンバ |
| $P_G$ | グループ管理者ＧＭの公開鍵 |
| $S_G$ | グループ管理者ＧＭの秘密鍵 |
| $P_E$ | 追跡機関ＥＭの公開鍵 |
| $S_E$ | 追跡機関ＥＭの秘密鍵 |
| $P_A$ | メンバＡの公開鍵：$P_A$＝ｙ（メンバＡが署名者の時） |
| $S_A$ | メンバＡの秘密鍵：$S_A$＝ｘ（メンバＡが署名者の時） |
| $\sigma_A$ | メンバ証明書：$sig_{S_G}(P_A)$ |
| $sig_{SG}$（ ） | 秘密鍵Ｓｇによるデジタル署名 |
| $ID_A$ | メンバＩＤ |
| ｃ | 公開鍵$P_E$で暗号化した値：$c = E_{P_E}(P_A) = P_A^{P_E}$ |
| ^ | べき乗を表す符号 |

【００１３】

（初期設定）

グループ管理者ＧＭ及び追跡機関ＥＭは、それぞれ公開鍵、秘密鍵のペア（ＰＧ，ＳＧ），（ＰＥ，ＳＥ）を作成する。また、グループ公開鍵（ＰＧ，ＰＥ）及び生成元ｇ等が公開される。

【００１４】

メンバＡとなるユーザは、例えば生成元ｇに基づき、以下の関係をもつ公開鍵と秘密鍵のペア（ＰＡ，ＳＡ）を生成する。

【００１５】

$PA = g^{SA}$

次に、ユーザは秘密鍵ＳＡにより公開鍵ＰＡに署名処理を施し、デジタル署名$Sig_{SA}$（ＰＡ）を得る。ユーザは、鍵ペア（ＰＡ，ＳＡ）が正しく生成された旨（述語）の次のような知識署名ＳＰＫ(Signature based on a Proof of Knowledge)を生成する。但し、初期設定なので、ここではメッセージｍは存在しない。

【００１６】

$$SPK\{(\alpha) \mid PA = g^{\alpha}\}(m) = SPK\{(SA) \mid PA = g^{SA}\}(m)$$

この知識署名ＳＰＫは、$e = H(g \| PA \| g^{v} PA^{e} \| m)$を満たす$(e, v) \in \{0,1\}^{k} \times [-2^{|L|+k}, 2^{\varepsilon(|L|+k)}]$で与えられる。ユーザは、乱数$r \in \{0,1\}^{\varepsilon(|L|+k)}$に基づいて、$u = g^{r}$を計算し、$e = H(g \| PA \| u \| m)$とし、$v = r - eSA$を整数上で求める。

【００１７】

しかる後、ユーザは、公開鍵ＰＡ、デジタル署名$Sig_{SA}$（ＰＡ）及び知識署名ＳＰＫ＝（ｅ，ｖ）をグループ管理者ＧＭに送信する。

【００１８】

グループ管理者ＧＭは、これらを受けると、公開鍵ＰＡによりデジタル署名$Sig_{SA}$（ＰＡ）を検証し、公開鍵ＰＡ及び生成元ｇにより知識署名（ｅ，ｖ）を検証する。なお、知識署名の検証は、$e = H(g \| PA \| g^{v} PA^{e} \| m)$に基づいて行う。

【００１９】

両者の検証により正当性を確認すると、グループ管理者ＧＭは、自己の秘密鍵ＳＧにより、次のようにユーザの公開鍵ＰＡに署名処理を施し、得られたメンバ証明書σＡをユーザに返信する。これにより、ユーザはメンバＡとなる。

【００２０】

$\sigma A = Sig_{SG}(PA)$

また、グループ管理者ＧＭは、メンバＡのメンバＩＤ、公開鍵及び証明書の組（ＩＤＡ，ＰＡ，σＡ）を秘密裏に保管するとともに、メンバＡの公開鍵とデジタル署名のペア（ＰＡ，$Sig_{SA}$（ＰＡ））をメンバリストに追加する。

【００２１】

（グループ署名生成）

署名者としてのメンバＡは、次のように、メッセージｍに対し、秘密鍵及びメンバ証明書のペア（ｘ，σＡ）を有する旨を証明する知識署名$SPK_{\sigma, x}$を生成する。なお、ｘ＝ＳＡである。

【００２２】

$$\begin{aligned} SPK_{\sigma, x} &= SPK\{(\alpha, \beta) \mid Verify_{PG}(f(\alpha), \beta) = 1\}(m) \\ &= SPK\{(x, \sigma A) \mid Verify_{PG}(f(x), \sigma A) = 1\}(m) \\ &= (e1, v1) \end{aligned}$$

但し、$e1 = H(g \| PA \| g^{r \wedge PG} \| m)$、$v1 = r - e1(x + \sigma A)$

また、署名者としてのメンバＡは、次のように、メッセージｍに対し、秘密鍵ＰＡを追跡機関ＥＭの公開鍵ＰＥで暗号化した値$c = E_{PE}$（ＰＡ）（追跡可能性）と、この値ｃの平文（ＰＡ）に対応する秘密鍵ｘを有する旨を証明する知識署名$SPK_{c}$を生成する。

【００２３】

$$\begin{aligned} SPK_{c} &= SPK\{(\alpha, \beta) \mid Verify_{PE}(f(\alpha), \beta) = 1\}(m) \\ &= SPK\{(x, c) \mid Verify_{PE}(f(x), c) = 1\}(m) \\ &= (e2, v2) \end{aligned}$$

但し、$e2 = H(g \| PA \| g^{r \wedge PE} \| m)$、$v2 = r - e2(x + c)$

しかる後、メンバＡは、メッセージｍと共に、各データ（$SPK_{\sigma, x}$、ｃ、$SPK_{c}$）を署名として検証者に送信する。なお、ｃは、証明書σＡを暗号化した値$c = E_{PE}$（σ

A）としてもよい。
【００２４】
（グループ署名検証）
検証者は、メッセージｍと共に、各データ（$SPK_{\sigma,x}$、ｃ、$SPK_c$）を署名として受けると、グループ公開鍵ＰＧ，ＰＥに基づいて、知識署名$SPK_{\sigma,x}$＝（ｅ１，ｖ１）及び$SPK_c$＝（ｅ２，ｖ２）を検証する。
【００２５】
$e1=H(g \| PA \| g^{v1} \cdot {}^{PG}PA^{e1} \cdot {}^{PG} \| m)$
$e2=H(g \| PA \| g^{v2} \cdot {}^{PE}PA^{e2} \cdot {}^{PE} \| m)$
検証者は、メンバＡの生成した署名が正当なとき、メッセージｍに基づく処理を実行する。一方、検証者は、メンバＡの生成した署名に不正があったとき、暗号化された値ｃを追跡機関ＥＭに送信する。
【００２６】
（追跡）
追跡機関ＥＭは、検証者ｓから受けた値ｃ（＝$E_{PE}$（ＰＡ））を自己の秘密鍵ＳＥにより復号し、得られたメンバＡの公開鍵ＰＡをグループ管理者ＧＭに送信する。グループ管理者ＧＭは、公開鍵ＰＡからメンバＡを特定する。
【００２７】
以上が標準的なグループ署名方式であるが、他のグループ署名方式も同様な性質をもっている。
【非特許文献１】D. Chaum, E. van Heyst, “Group Signatures”, EUROCRYPT’91, LNCS 547, Springer-Verlag, pp.257-265, 1991.
【非特許文献２】G. Ateniese , J. Camenisch, M. Joye and G. Tsudik. A practical and provably secure coalition-resistant group signature scheme. CRYPTO 2000, LNCS 1880, Springer-Verlag, pp.255-270, 2000.
【非特許文献３】宮地充子、菊池浩明　編著、「情報セキュリティ」、オーム社、ＩＳＢＮ４－２７４－１３２８４－６、ｐｐ．１１２－１１４．
【特許文献１】特開２００４－５４９０５号公報
【発明の開示】
【発明が解決しようとする課題】
【００２８】
本発明者の検討によれば、オンラインで商品又はサービスを注文する際には、匿名性と注文内容に関するプライバシについて以下のような課題があると考えられる。
【００２９】
匿名性に関しては、個人情報を管理するコストとリスクが高まる一方であり、サービス提供者にとっては個人情報を管理しなければサービスを提供できないことは望ましくない。また、サービス利用者にとっても複数のサービス提供者がそれぞれ個人情報を管理している状態は望ましくない。
【００３０】
しかしながら、一般的な注文では、サービス提供者に個人情報を渡す必要がある。なお、個人情報を渡さず、個人ＩＤを渡す方法も考えられるが、個人ＩＤでは完全な匿名性は実現できない。理由は、複数の異なる注文が同一のサービス利用者によるものか否かが判断可能なことから、その利用者の注文履歴を把握して趣味・趣向などを知ることが可能なためである。更に、個人ＩＤを渡す場合、注文の際にサービス提供者との送受信だけでは済まず、個人情報の管理サーバなどにアクセスする必要がある方式では、注文の処理効率が悪いものとなってしまう。特許文献１ではグループ署名を利用し、完全な匿名で効率よくオンラインサービスを受けることができるが、物流を伴う商品の購入などは考慮されていない。
【００３１】
注文内容のプライバシに関しては、上記いずれの方法であっても「誰が」「何を」注文

したかがサービス提供者に知られるので、プライバシ保護の観点から望ましくない。
【００３２】
さらに、匿名性と注文内容のプライバシを考慮する場合であっても、サービス提供者がマーケット情報を取得できる仕組みは必要である。
【００３３】
本発明は上記実情を考慮してなされたもので、オンライン以外のサービスを行うサービス提供者が個人情報を管理する必要が無く、利用者の匿名性を実現し得る匿名注文システム、装置及びプログラムを提供することを目的とする。
【００３４】
また、本発明の他の目的は、注文内容のプライバシを保護し得る匿名注文システム、装置及びプログラムを提供することにある。
【００３５】
さらに、本発明の他の目的は、匿名性と注文内容のプライバシ保護を実現しつつサービス提供者がマーケット情報を取得し得る匿名注文システム、装置及びプログラムを提供することにある。
【課題を解決するための手段】
【００３６】
第１の発明は、追跡機能を有するグループ署名方式により、商品又はサービスからなる販売対象の匿名注文と、前記匿名注文に応じた販売対象の販売とを実行する匿名注文システムであって、前記匿名注文をする購入者の個人情報及びグループ署名関連情報を記憶装置に記憶し、販売店から受けた注文ＩＤ及びグループ署名を含む匿名注文情報に基づいて、前記追跡機能により、当該グループ署名を復号して得られたグループ署名関連情報から前記記憶装置内の対応する個人情報を特定し、この個人情報を外部の配送手段による配送のために出力する管理者装置と、前記購入者の購入者装置に注文ＩＤを発行し、前記購入者装置からこの注文ＩＤ及びグループ署名を含む匿名注文情報を受けると、当該グループ署名を検証して検証結果が正当のとき、当該匿名注文情報を前記管理者装置に送出する販売店装置と、前記購入者の操作により、前記販売店装置から注文ＩＤを受けると、この注文ＩＤ及びグループ署名を含む匿名注文情報を生成し、得られた匿名注文情報を前記販売店装置に送信する購入者装置とを備えた匿名注文システムである。
【００３７】
第２の発明は、追跡機能を有するグループ署名方式により、商品又はサービスからなる販売対象の匿名注文を実行するための匿名注文システムに用いられ、前記匿名注文をする購入者をグループ署名方式のメンバとして管理し、注文ＩＤ及びグループ署名を含む匿名注文情報を受けると、このグループ署名から前記追跡機能により購入者を特定するための管理者装置と、前記購入者の購入者装置に注文ＩＤを発行し、前記購入者装置からこの注文ＩＤ及びグループ署名を含む匿名注文情報を受けると、当該グループ署名を検証して検証結果が正当のとき、当該注文ＩＤに対応する販売対象を前記購入者に販売するための販売店装置と、の両装置と通信可能な、前記購入者の購入者装置であって、前記購入者の操作により、前記販売店装置に販売対象特定情報を送信する対象情報送信手段と、この送信に応じて前記販売店装置から注文ＩＤを受けると、この注文ＩＤを含み前記販売対象特定情報を含まない注文基本情報を生成する基本情報生成手段と、前記販売対象特定情報を秘匿した注文詳細情報を生成する詳細情報生成手段と、前記グループ署名方式により前記グループ署名を生成するグループ署名生成手段と、前記注文基本情報、前記注文詳細情報及び前記販売店秘匿メッセージを少なくとも含むメッセージ部分と前記グループ署名とを前記匿名注文情報として編集する編集手段と、前記編集手段により得られた匿名注文情報を前記販売店装置に送信する匿名情報送信手段とを備えた購入者装置である。
【００３８】
第３の発明は、追跡機能を有するグループ署名方式により、商品又はサービスからなる販売対象の匿名注文と、前記匿名注文に応じた販売対象の販売及び提供とを実行するための匿名注文システムに用いられ、前記匿名注文をする購入者の購入者装置と前記販売をす

る販売店の販売店装置との両装置と通信可能で、前記購入者の個人情報及びグループ署名関連情報を記憶装置に記憶して管理する管理者装置であって、前記販売店又は販売店装置から注文ＩＤ及びグループ署名を含む匿名注文情報を受けると、前記追跡機能により、当該グループ署名を復号して得られたグループ署名関連情報から前記記憶装置内の対応する購入者の個人情報を特定する購入者特定手段と、前記特定した個人情報から個人を特定可能な情報を削除してマーケット情報を生成するマーケット情報生成手段と、得られたマーケット情報を前記販売店装置に送信するマーケット情報送信手段とを備えた管理者装置である。

【００３９】

（作用）

第１の発明によれば、販売店装置は、購入者装置から注文ＩＤ及びグループ署名を含む匿名注文情報を受けると、当該グループ署名を検証して検証結果が正当のとき、当該匿名注文情報を管理者装置に送出する。管理者装置は、この匿名注文情報に基づいて、追跡機能により、当該グループ署名を復号して得られたグループ署名関連情報から記憶装置内の対応する個人情報を特定し、この個人情報を外部の配送手段による配送のために出力する。外部の配送手段は、この個人情報に基づいて販売対象を購入者に配送する。

【００４０】

従って、サービス提供者としての販売店装置が個人情報を管理する必要が無く、利用者の匿名性を実現することができる。また、管理者装置が匿名注文情報を扱うので、注文内容に関するプライバシを管理者装置から保護することができる。

【００４１】

また、第２の発明は、前述した作用に加え、購入者装置としては、秘匿メッセージ生成手段により、販売店へのメッセージを販売店装置の公開鍵により暗号化して販売店秘匿メッセージを生成し、編集手段により、この販売店秘匿メッセージを含むように匿名注文情報を編集するので、第三者から秘匿した状態で販売店にメッセージを伝えることができる。

【００４２】

一方、第３の発明は、前述した作用に加え、管理者装置としては、マーケット情報生成手段により、特定した個人情報から個人を特定可能な情報を削除してマーケット情報を生成し、マーケット情報送信手段により、このマーケット情報を販売店装置に送信するので、購入者を秘匿した状態で注文に関するマーケット情報を販売店に提供することができる。

【発明の効果】

【００４３】

以上説明したように本発明によれば、サービス提供者が個人情報を管理する必要が無く、利用者の匿名性を実現できる。また、注文内容のプライバシを保護できる。さらに、匿名性と注文内容のプライバシ保護を実現しつつサービス提供者がマーケット情報を取得できる。

【発明を実施するための最良の形態】

【００４４】

以下、本発明の各実施形態について図面を参照しながら説明する。なお、各実施形態では、匿名注文システムの一例として、物流会社（グループ管理者、追跡機関）、購入者（メンバ、署名者）及び販売店（署名検証者）からなり、物流を伴うオンラインでの商品購入に適用した場合を代表例に挙げて述べる。なお、商品に代えて、サービスを用いても良いことは言うまでもない。また、以下の各実施形態は、非特許文献３のグループ署名を代表例に挙げて述べているが、これに限らず、任意のグループ署名方式についても、メッセージｍをｍ＝（ｍ１‖Ｈ（ｍ２））又はｍ＝（ｍ１‖Ｈ（ｍ２）‖ＥPSP（ｍ３）‖EGM（ｍ４））とすることにより、同様に適用できることも言うまでもない。

【００４５】

（第１の実施形態）

図１は本発明の第１の実施形態に係る匿名注文システムの構成を示す模式図である。この匿名注文システムは、物流会社装置１０、販売店装置２０及び購入者装置３０が互いにネットワーク４１～４４を介して接続されている。

【００４６】

ここで、物流会社装置１０は、物流会社用記憶装置１１、初期設定部１２、販売店登録部１３、購入者登録部１４、決済処理部１５、注文検証部１６、購入者特定部１７及びマーケット情報生成部１８を備えている。

【００４７】

物流会社用記憶装置１１は、各部１２～１８から読出／書込可能なメモリであり、図２に示すように、グループ管理情報、秘密管理情報、メンバリスト、販売店登録情報及び注文履歴リストが記憶されるものである。

【００４８】

ここで、グループ管理情報は、グループ公開鍵（ＰＧ，ＰＥ）、グループ秘密鍵（ＳＧ，ＳＥ）、物流会社公開鍵ＰＧＭ、物流会社秘密鍵ＳＧＭからなる。

【００４９】

秘密管理情報（購入者のグループ署名関連情報）は、メンバ毎のメンバＩＤ、メンバ公開鍵ＰＡ及びメンバ証明書σＡからなる。

【００５０】

メンバリストは、メンバＩＤ毎のメンバの個人情報、メンバ公開鍵ＰＡ及びデジタル署名$Sig_{SA}$（ＰＡ）からなるリストである。メンバの個人情報は、例えば氏名、住所、年齢層、性別、決済情報（銀行口座情報又はクレジットカード番号など）からなり、所望により、Ｅメールアドレス、ＩＰアドレス等のネットワークアドレス情報、電話番号など任意の情報を付加してもよい。なお、メンバリスト内のメンバ公開鍵も購入者のグループ署名関連情報に該当する。

【００５１】

販売店登録情報は、販売店情報及び販売店公開鍵ＰＳＰからなる。販売店情報は、例えば販売店名、住所、電話番号、Ｅメールアドレス、決済情報（銀行口座情報又はクレジットカード番号など）からなる。

注文履歴リストは、過去の注文における匿名注文情報ｍのリストである。

【００５２】

初期設定部１２は、システム立ち上げ時に１回だけ使用され、グループ公開鍵・秘密鍵のペア（ＰＧ，ＳＧ），（ＰＥ，ＳＥ）を生成する機能と、物流会社公開鍵・秘密鍵のペア（ＰＧＭ，ＳＧＭ）を生成する機能と、生成した鍵ペアからなるグループ管理情報を物流会社用記憶装置１１に書込む機能とを有するものである。

【００５３】

販売店登録部１３は、販売店を登録する際に、販売店装置２０から受けた販売店情報及び販売店公開鍵ＰＳＰを含む販売店登録情報を物流会社用記憶装置１１に書込む機能と、書込の後、物流会社用記憶装置１１内のグループ公開鍵（ＰＧ，ＰＥ）を販売店装置２０に返信する機能とをもっている。

【００５４】

購入者登録部１４は、購入者装置３０から受けた個人情報に基づいて、購入者が匿名注文サービスを受けられるか否かを審査する機能と、審査の結果を購入者装置３０に通知する機能と、審査を通過したとき、購入者装置３０との間でチャレンジ・レスポンス認証をする機能と、購入者装置３０から受けたデジタル署名$Sig_{SA}$（ＰＡ）及び知識署名ＳＰＫを検証する機能と、両者の検証により正当性を確認すると、グループ秘密鍵ＳＧによりメンバ公開鍵ＰＡに署名処理を施してメンバ証明書σＡ（＝$Sig_{SG}$（ＰＡ））を作成する機能と、メンバＡのメンバＩＤ、公開鍵及び証明書の組（ＩＤＡ，ＰＡ，σＡ）からなる秘密管理情報を物流会社記憶装置１１の耐タンパー領域に保管するとともに、メンバ公開鍵ＰＡとデジタル署名のペア（ＰＡ，$Sig_{SA}$（ＰＡ））をメンバリストに追加する機能と、メンバ証明書σＡを購入者装置３０に送信する機能とをもっている。

【００５５】
決済処理部１５は、物流会社用記憶装置１１内のメンバリストに記載のメンバ個人情報に基づいて、代理決済を行う機能をもっている。
【００５６】
注文検証部１６は、販売店から匿名注文情報を受け取ると、物流会社用記憶装置１１内の注文履歴リストに同一情報があるか否かを調べ、同一情報がある場合には不正な要求として商品配送・決済を拒否し、否の場合には匿名注文情報に含まれるグループ署名の正当性を検証する機能と、署名が不正な場合に商品配送・決済を拒否する機能と、署名の正当性が確認できた場合のみ受理し、匿名注文情報を注文履歴リストに追加して物流会社用記憶装置１１に保存する機能とをもっている。
【００５７】
購入者特定部１７は、匿名注文情報内のグループ署名ｃ（＝$E_{PE}$（PA））をグループ秘密鍵SEにより復号し、得られたメンバ公開鍵PAからメンバリストを参照して署名者（＝購入者）を特定する追跡機能をもっている。
【００５８】
マーケット情報生成部１８は、特定した署名者の情報から個人を特定できる情報（例、住所、氏名等）を削除してマーケット情報を生成するものであり、得られたマーケット情報を販売店装置２０に送信する機能とをもっている。マーケット情報とは、注文に関する情報のうち、個人を特定できない情報であり、商品の購買層を示すのに有効な情報である。
【００５９】
販売店装置２０は、販売店用記憶装置２１、登録要求部２２、注文受付部２３、注文情報生成部２４、注文検証部２５及び決済要求部２６を備えている。
【００６０】
販売店用記憶装置２１は、各部２２～２６から読出／書込可能なメモリであり、図３に示すように、注文情報生成情報（＝匿名注文情報検証情報）、商品情報及び注文受付リストが記憶されるものである。
【００６１】
注文情報生成情報は、グループ公開鍵（PG, PE）、販売店公開鍵PSP、販売店秘密鍵SSPからなる。
【００６２】
商品情報は、購入者装置３０から受ける商品特定情報（販売対象特定情報）から注文情報を作成するための関連情報であり、例えば商品分類ｍ１３、商品ＩＤｍ２１、商品名ｍ２１及び単価ｍ２３を含むものである。なお、商品特定情報とは、販売店が提供する商品を特定するための情報であり、管理者に知られたくない情報であって、図４に示すように、商品ＩＤ（例、商品番号）ｍ２１及び個数ｍ２４などが使用可能となっている。
【００６３】
注文受付リストは、購入者装置３０から受けた注文情報ｍ１，ｍ２及び匿名注文情報ｍ、（$SPK_{\sigma, x}$、ｃ、$SPK_{c}$）のリストである。
【００６４】
注文情報とは、注文基本情報ｍ１と注文詳細情報ｍ２を含むものである。
【００６５】
注文基本情報ｍ１とは、商品代金の決済のために必要最低限の情報であり、例えば、注文ＩＤｍ１１、販売店名ｍ１２、商品分類ｍ１３、合計金額ｍ１４及び支払方法ｍ１５からなる。
【００６６】
注文詳細情報ｍ２とは、商品に関する情報のうち、プライバシの観点から販売店以外（＝管理者など）には秘匿されることが望ましい情報であり、少なくとも商品特定情報を含み、他に任意の情報を付加したものであって、例えば商品ＩＤｍ２１、商品名ｍ２２、単価ｍ２３、個数ｍ２４及び注文日時ｍ２５からなる。

匿名注文情報については後述する。

【００６７】

登録要求部２２は、販売店員の操作により、登録要求部２２が販売店情報及び販売店公開鍵PSPを物流会社装置１０に送信する機能と、物流会社装置１０から受けたグループ公開鍵（PG, PE）を販売店用記憶装置２２に書き込む機能とをもっている。

【００６８】

注文受付部２３は、購入者装置３０と、販売店装置２０内の各部２４，２５との間に位置するインターフェイス機能をもっている。

【００６９】

注文情報生成部２４は、購入者装置３０から受ける商品特定情報から注文情報生成情報に基づいて、注文基本情報ｍ１と注文詳細情報ｍ２からなる注文情報ｍを生成する機能と、得られた注文情報ｍと、販売店公開鍵PSPとを購入者装置３０に送信する機能をもっている。

【００７０】

注文検証部２５は、購入者装置３０から匿名注文情報を受けると、販売店用記憶装置２１内の匿名注文検証情報に基づいて匿名注文情報の正当性を検証する機能と、正当性を検証できた場合に注文を受け付け、注文情報と匿名注文情報を販売店用記憶装置２１に保存する機能と、匿名注文情報とともに、発送先の代わりに注文ＩＤが記載された伝票を発行する機能とをもっている。

【００７１】

決済要求部２６は、匿名注文情報を物流会社装置１０に送信して決済を要求する機能と、決済終了後、物流会社装置１０から受けたマーケット情報を物流会社用記憶装置１１に保存する機能をもっている。なお、決済要求部２６の決済要求機能は、本実施形態では伝票の匿名注文情報により決済を要求するために使用しないが、商品がデジタルコンテンツの場合などに好適に使用可能となっている。

【００７２】

購入者装置３０は、購入者用記憶装置３１、登録要求部３２、商品選択部３３、匿名注文部３４、匿名情報生成部３５及び注文確認部３６を備えている。

【００７３】

購入者用記憶装置３１は、各部３２～３５から読出／書込可能なメモリであり、図５に示すように、匿名注文情報生成情報及び注文済情報が記憶されるものである。

【００７４】

匿名注文情報生成情報は、グループ公開鍵（PG, PE）、メンバ公開鍵PA、メンバ秘密鍵SA、メンバ証明書σA、物流会社公開鍵PGMからなる。

【００７５】

注文済情報は、注文情報ｍ１，ｍ２及び匿名注文情報ｍ、（$SPK_{\sigma, x}$、ｃ、$SPK_{c}$）からなる。

【００７６】

匿名注文情報とは、図６に示すように、注文基本情報ｍ１、秘匿注文詳細情報H（ｍ２）、販売店への秘匿メッセージ$E_{PSP}$（ｍ３）、物流会社への秘匿メッセージ$E_{PGM}$（ｍ４）、匿名注文正当性検証情報（$SPK_{\sigma, x}$、ｃ、$SPK_{c}$）を含む。

【００７７】

秘匿注文詳細情報H（ｍ２）とは、注文詳細情報ｍ２を知らないと作れない情報であり、注文を受けた販売店が匿名注文情報の正当性を検証するために利用する。但し、秘匿注文詳細情報H（ｍ２）から注文詳細情報ｍ２を復元できなくてもよい。よって、ここではハッシュ値H（ｍ２）を用いるが、これに限らず、販売店の公開鍵PGMで暗号化された注文詳細情報ｍ２としてもよい。

【００７８】

販売店への秘匿メッセージ$E_{PSP}$（ｍ３）とは、購入者が販売店だけに伝えたいメッセージであり、例えば、クーポン券の番号や、割引用のキーワード等があって、販売店だけ

が復号可能な形態で暗号化されている。

【００７９】

物流会社への秘匿メッセージ$E_{PGM}$（ｍ４）とは、購入者が物流会社だけに伝えたいメッセージであり、例えば、商品の送り先などがあり、物流会社だけが復号可能な形態で暗号化されている。

【００８０】

匿名注文正当性検証情報（$SPK_{\sigma,x}$、ｃ、$SPK_{c}$）とは、匿名注文情報の正当性を検証するためのグループ署名であり、匿名注文検証情報に基づき、注文検証部２５により正当性を検証可能となっている。これにより販売店は注文を受けてよいことを確認できるが、個人情報を一切取得できない。また、グループ管理情報とともに購入者特定部１４により、正当性が検証可能であり、正当な場合には生成した購入者を特定可能となっている。

【００８１】

登録要求部３２は、購入者の操作により、個人情報を物流会社装置１０に送信する機能と、物流会社装置１４から受けた審査を通過した旨の通知に基づいて、匿名注文システムのメンバとしてのメンバ公開鍵・秘密鍵のペア（PA，SA）を生成して購入者用記憶装置３１に書き込む機能と、物流会社装置１０との間でチャレンジ・レスポンス認証を実行する機能と、デジタル署名$Sig_{SA}$（PA）及び知識署名ＳＰＫ＝（ｅ，ｖ）を生成し、これらデジタル署名$Sig_{SA}$（PA）及び知識署名ＳＰＫを物流会社装置１０に送信する機能と、物流会社装置１０から受けたメンバ証明書σAを購入者用記憶装置３１に保存する機能とをもっている。

【００８２】

商品選択部３３は、購入者の操作により、商品特定情報及び注文要求を販売店装置に送信するものである。

【００８３】

匿名注文部３４は、販売店装置２０と、購入者装置３０内の各部３３，３５，３６との間に位置するインターフェイス機能をもっている。

【００８４】

匿名情報生成部３５は、購入者の操作により、購入者用記憶装置３１内の匿名注文生成情報に基づいて、注文基本情報ｍ１及び注文詳細情報ｍ２から匿名注文情報を生成するものであり、得られた匿名注文情報を匿名注文部３４を介して販売店装置２０に送信する機能をもっている。

【００８５】

注文確認部３６は、販売店装置２０から受けた注文基本情報ｍ１と注文詳細情報ｍ２とを画面表示し、購入者に注文内容の確認を促す機能をもっている。

【００８６】

次に、以上のように構成された匿名注文システムの動作を図７乃至図１６を用いて説明する。

（初期設定；図８乃至図１０）

物流会社装置１０は、匿名注文サービスを立ち上げる際に（ＳＴ１）、物流会社員の操作により、初期設定部１２が匿名注文用グループをセットアップし、グループ公開鍵・秘密鍵のペア（PG，SG），（PE，SE）を生成すると共に、自己の物流会社公開鍵・秘密鍵のペア（PGM，SGM）を生成し、これらの鍵ペアからなるグループ管理情報を物流会社用記憶装置１１に書き込む。物流会社装置１０は、以上の処理をサービス立ち上げ時の最初の１回だけ行えばよい。これにより、物流会社装置１０は、匿名注文サービスの提供が可能となる。

【００８７】

販売店装置２０においては、匿名注文サービスの提供を開始する際に、販売店員の操作により、登録要求部２２が販売店情報及び販売店公開鍵PSPを物流会社装置１０に送信する（ＳＴ２）。

【００８８】
物流会社装置１０では、販売店登録部１３が、これら販売店情報及び販売店公開鍵ＰSPを含む販売店登録情報を物流会社用記憶装置１１に書込み、販売店登録処理を実行する（ＳＴ３）。販売店登録部１３は、物流会社用記憶装置１１内のグループ公開鍵（PG, PE）を販売店装置２０に返信する（ＳＴ４）。
【００８９】
販売店装置２０では、登録要求部２２がグループ公開鍵（PG, PE）を注文情報生成情報及び匿名注文情報検証情報の一部として販売店用記憶装置２２に書き込む。注文情報生成情報及び匿名注文情報検証情報としては、他に、販売店の公開鍵・秘密鍵のペア（PSP, SSP）がある。販売店装置２０では、以上の処理を物流会社に登録する際の最初の１回だけ行えばよい。
【００９０】
購入者装置３０では、購入者の操作により、登録要求部３２が個人情報を物流会社装置１０に送信する（ＳＴ４）。物流会社装置１４では、購入者登録部１４がこの個人情報に基づいて、購入者が匿名注文サービスを受けられるか否かを審査し（ＳＴ６）、例えば審査を通過した旨を購入者装置３０に通知する（ＳＴ７）。
【００９１】
購入者装置３０では、登録要求部３２がこの通知に基づいて、匿名注文システムのメンバとしてのメンバ公開鍵・秘密鍵のペア（PA, SA）を生成して購入者用記憶装置３１に書き込む（ＳＴ８）。しかる後、購入者装置３０では、登録要求部３２が物流会社装置１０との間でチャレンジ・レスポンス認証を実行する（ＳＴ９）。なお、チャレンジ・レスポンス認証の過程で、メンバ公開鍵PA及び物流会社公開鍵PGMは、購入者装置３０と物流会社装置１０との間で共有される。
【００９２】
ステップＳＴ９のチャレンジ・レスポンスにより、相互に認証が完了すると、購入者装置３０は、登録要求部３２がデジタル署名$Sig_{SA}$（PA）及び知識署名ＳＰＫ＝（ｅ，ｖ）を生成し、これらデジタル署名$Sig_{SA}$（PA）及び知識署名ＳＰＫを物流会社装置１０に送信する（ＳＴ１０）。
【００９３】
物流会社装置１０では、購入者登録部１４が、これらデジタル署名$Sig_{SA}$（PA）及び知識署名ＳＰＫを検証し（ＳＴ１１）、両者の検証により正当性を確認すると、グループ秘密鍵SGによりメンバ公開鍵PAに署名処理を施してメンバ証明書σA（＝$Sig_{SG}$（PA））を作成する（ＳＴ１２）。
【００９４】
しかる後、購入者登録部１４は、メンバＡのメンバＩＤ、公開鍵及び証明書の組（ＩＤA, PA, σA）からなる秘密管理情報を物流会社記憶装置１１の耐タンパー領域に保管するとともに、メンバ公開鍵PAとデジタル署名のペア（PA, $Sig_{SA}$（PA））をメンバリストに追加する。
【００９５】
また、物流会社装置１０は、購入者登録部１４がメンバ証明書σAを購入者装置３０に送信する（ＳＴ１４）。購入者装置３０では、登録要求部３２がメンバ証明書σAを購入者用記憶装置３１に保存する（ＳＴ１５）。購入者装置３０は、以上の処理をメンバ登録時の最初の１回だけ行えばよい。購入者はここで生成されたメンバ秘密鍵SA・メンバ証明書σAを利用して何度でも匿名注文を行うことができる
（匿名注文・配送・決済；図１１乃至図１６）
購入者装置３０は、購入者の操作により、商品選択部３３が商品特定情報及び注文要求を販売店装置に送信する（ＳＴ２１）。
【００９６】
販売店装置２０は、注文情報生成部２４がこの商品特定情報から注文情報生成情報に基づいて、注文基本情報ｍ１と注文詳細情報ｍ２からなる注文情報ｍを生成し、得られた注

文情報と販売店公開鍵PSPとを購入者装置３０に送信する（ＳＴ２２）。

【００９７】

ここで、注文情報mは、注文基本情報ｍ１と注文詳細情報ｍ２とが互いに連接して形成されている（m＝｛ｍ１‖ｍ２｝）。

注文基本情報は物流会社が商品配送・決済を行うのに必要な最低限の情報であり、注文を一意に識別するための情報である注文ＩＤを含む。注文詳細情報はそれ以外の詳細な情報であり、購入者のプライバシ保護の観点から物流会社に対しては秘匿されることが望ましい。

【００９８】

以下に注文基本情報ｍ１、注文詳細情報ｍ２の具体例をあげる（図４参照）。

注文基本情報ｍ１＝（注文ＩＤ‖販売店名‖商品分類‖合計金額‖支払方法）
＝（ｍ１１‖ｍ１２‖ｍ１３‖ｍ１４‖ｍ１５）
注文詳細情報ｍ２＝（商品番号‖商品名‖単価‖個数‖注文日時）
＝（ｍ２１‖ｍ２２‖ｍ２３‖ｍ２４‖ｍ２５）

商品分類ｍ１３は本、ＣＤ、ＤＶＤ等を指す。商品名ｍ２２はそのタイトル等を指す。

【００９９】

購入者装置３０は、これら注文基本情報ｍ１と注文詳細情報ｍ２とを注文確認部３６が画面表示する。購入者は、この画面表示により、注文内容が自分の意図したものであるかを確認し、購入者装置３０を操作する。購入者装置３０は、購入者の操作により、匿名情報生成部３５が購入者用記憶装置３１内の匿名注文生成情報に基づいて、注文基本情報ｍ１及び注文詳細情報ｍ２から匿名注文情報を生成し（ＳＴ２３）、この匿名注文情報を匿名注文部３４を介して販売店装置２０に送信する（ＳＴ２４）。

【０１００】

匿名注文情報は、少なくとも注文基本情報ｍ１、注文詳細情報のハッシュ値Ｈ（ｍ２）、販売店への秘匿メッセージＥＰSP（ｍ３）、物流会社への秘匿メッセージＥＰGM（ｍ４）、これらを連接したメッセージｍ（＝ｍ１‖Ｈ（ｍ２）‖ＥPSP（ｍ３）‖ＥPGM（ｍ４））に対するグループ署名（$SPK_{\sigma,x}$、ｃ、$SPK_{c}$）からなる（図６参照）。但し、各秘匿メッセージＥPSP（ｍ３），ＥPGM（ｍ４）は、それぞれ省略可能である。ここでは省略した場合を述べる。

【０１０１】

グループ署名（$SPK_{\sigma,x}$、ｃ、$SPK_{c}$）は、グループ公開鍵（PG, PE）、購入者のメンバ秘密鍵SA・証明書σAから計算される。ここで、グループ署名生成関数をGrSigで表すと、匿名注文情報は次式で表される。

【０１０２】

匿名注文情報＝（ｍ‖GrSig（ｍ））
＝（ｍ１‖Ｈ（ｍ２）‖GrSig（ｍ１‖Ｈ（ｍ２））

秘匿メッセージを省略しない場合、上式のｍにｍ１‖Ｈ（ｍ２）‖ＥPSP（ｍ３）‖ＥPGM（ｍ４））を代入すればよい。なお、秘匿メッセージを省略する／しないのいずれにしても、グループ署名の生成方法自体は前述した通りであるが、メッセージｍの構成が従来とは異なるものとなっている。

【０１０３】

販売店装置２０は、匿名注文情報を受けると、注文検証部２５が販売店用記憶装置２１内の匿名注文検証情報に基づいて匿名注文情報の正当性を検証し（ＳＴ２５）、注文詳細情報のハッシュ値Ｈ（ｍ２）が正しく計算されていることと、グループ署名（$SPK_{\sigma,x}$、$SPK_{c}$）が正当であることを確認できた場合にのみ注文を受け付け（ＳＴ２６；正当）、それ以外の場合は注文を拒否する（ＳＴ２６；不当）。

【０１０４】

販売店装置２０は、注文検証部２５が注文を受け付けると注文情報と匿名注文情報を販売店用記憶装置２１に保存する（ＳＴ２７）。さらに、販売店装置２０は、匿名注文情報とともに、発送先の代わりに注文ＩＤが記載された伝票を発行する。この伝票は、販売店

員により、梱包された商品に貼り付けられて発送される（ＳＴ２８）。この伝票は代理決済要求としても作用する。

【０１０５】

以上のような匿名注文においては、注文詳細情報ｍ２がハッシュ値Ｈ（ｍ２）で秘匿された匿名注文情報により、購入者が「何を」買ったかを秘匿し、注文内容に関する購入者のプライバシを守ることができる。

【０１０６】

注文手続き開始のリクエストから注文確定までの間、購入者の個人情報は仮名、ＩＤも含めて一切送られておらず、また物流会社へのアクセスも一切行われていないことが匿名注文の大きな特長の１つである。

【０１０７】

次に、商品配送及び決済について説明する。

物流会社は、販売店が受注した商品の配送および決済を行う。物流会社装置１０は、販売店による不正を防ぐため、過去に受け取った匿名注文情報を注文履歴リストとして物流会社用記憶装置１１に保存している。

【０１０８】

物流会社装置１０は、販売店から匿名注文情報を受け取ると、注文検証部１６が注文履歴リストに同じ情報がないかを調べ、同じ情報が見つかった場合には不正な要求として商品配送・決済を拒否する。そうでない場合には匿名注文情報に含まれるグループ署名の正当性を検証する（ＳＴ２９）。

【０１０９】

注文検証部１６は、署名が不正な場合にも商品配送・決済を拒否し（ＳＴ３０；拒否）、署名の正当性が確認できた場合のみ受理し（ＳＴ３０；受理）、匿名注文情報を注文履歴リストに追加して物流会社用記憶装置１１に保存する。これにより、物流会社は、販売店の不正な要求を防止する。

【０１１０】

続いて、物流会社装置１０は、購入者特定部１７が匿名注文情報内のグループ署名ｃ（＝$E_{PE}$（PA））をグループ秘密鍵SEにより復号し、得られたメンバ公開鍵PAからメンバリストを参照して署名者を特定し（ＳＴ３１）、住所・氏名等の特定内容を画面表示するか又は貼付シールとして発行する（住所情報出力手段）。

【０１１１】

物流会社員は、対応する商品の伝票に特定した署名者の情報を記入して商品を配送する（ＳＴ３２；外部の配送手段）。なお、署名者の特定処理は、グループ管理情報とメンバの個人情報を持つ唯一の装置である物流会社装置１０のみが実行できる。また、物流会社装置１０では、決済処理部１５が物流会社用記憶装置１１内のメンバリストに記載のメンバ個人情報に基づいて、購入者の金融機関等から代理決済を行い（ＳＴ３３）、商品代金を販売店（の金融機関等）へ支払う（ＳＴ３４）。さらに、物流会社装置１０では、マーケット情報生成部１８が、特定した署名者の情報から個人を特定できる情報（例、住所、氏名等）を削除し、例えば都道府県、年齢層及び性別からなるマーケット情報を生成し、このマーケット情報を販売店装置２０に送信する（ＳＴ３５）。販売店装置２０では、このマーケット情報を保存し、各種の分析などに使用可能とする。

【０１１２】

上述したように本実施形態によれば、販売店装置２０は、購入者装置３０から注文ＩＤ及びグループ署名を含む匿名注文情報を受けると、当該グループ署名を検証して検証結果が正当のとき、当該匿名注文情報と当該注文ＩＤに対応する商品とを商品名を秘匿した状態で物流会社装置１０に送る。管理者装置１０は、この匿名注文情報に基づいて、追跡機能により、当該グループ署名を復号して得られたメンバ公開鍵PAから記憶装置１０内の対応する個人情報を特定し、この個人情報を外部の配送手段（物流会社員）による配送のために画面表示又はシール発行等の形態で出力する。物流会社員は、この個人情報に基づいて販売対象を購入者に配送する。

【０１１３】
従って、サービス提供者としての販売店装置２０が個人情報を管理する必要が無く、利用者の匿名性を実現することができる。また、物流会社装置１０が匿名注文情報を扱うので、注文内容に関するプライバシを物流会社装置１０から保護することができる。
【０１１４】
すなわち、従来のグループ署名方式を単にオンラインショッピングに適用すると、注文内容が管理者装置１０に知られてプライバシを保護できないと考えられるが、本実施形態によれば、注文内容を秘匿した注文詳細情報Ｈ（ｍ２）を用いるので、プライバシを保護することができる。
【０１１５】
補足すると、「誰が」「何を」注文したかを知るのは購入者本人だけである。注文は購入者と販売店の間のやりとりだけで完結する。販売店は「何を」注文したかは分かるが、「誰が」注文したかが分からない。物流会社は「誰が」注文したかは分かるが、「何を」注文したかが（商品分類以上には）分からない。更に補足すると、販売店は「誰が」注文したかが分からない匿名注文でありながら、各種の分析に必要な、注文に関するマーケット情報を得ることができる。
【０１１６】
続いて、このような本実施形態の効果を詳細に説明する。具体的には、従来のオンラインサービス注文（一般注文）と匿名注文システムを利用したオンラインサービス注文（匿名注文）を比較し、登場人物である購入者（サービス利用者）、販売店（サービス提供者）、物流会社（個人情報管理機関）ごとに利点を述べる。
【０１１７】
（購入者Ａの利点）
（Ａ１：匿名注文が可能）
従来の一般注文では、購入者は販売店ごとに個人情報を渡し、販売店それぞれが個人情報を管理する必要がある。また、購入代金決済のためにクレジットカード会社などの決済事業者にも個人情報を登録してあることが一般的である。すなわち、購入者の個人情報は多くの場所に拡散して管理されている状態であり、ずさんな管理が行われているところが１個所でもあれば個人情報の漏洩につながってしまう。購入者にとって、利用する全ての販売店のセキュリティポリシーを把握し個人情報が適正に管理されているかを知ることは困難であり、個人情報漏洩のリスクが高い。実際、販売店に個人情報を渡すことに抵抗を感じるサービス利用者は多く、米国でのＲＳＡセキュリティ社の調査によれば、４４％ものユーザがサービスを受ける際に個人情報を提供することに抵抗を感じている。
【０１１８】
これに対し、匿名注文では、販売店には一切の個人情報を渡す必要がなく、個人情報を物流会社のみに預けておけばよい。購入者は、セキュリティポリシーや個人情報管理に関して物流会社さえ信頼できれば、どの販売店でも安心して注文することができる。
【０１１９】
（Ａ２：注文のプライバシを保護）
従来の一般注文では、販売店が「誰が」「何を」注文したかを把握できる。
【０１２０】
これに対し、本実施形態の匿名注文では、販売店は「何を」注文したかしか分からず、物流会社は「誰が」注文したかしか分からない。これにより、注文に関する購入者のプライバシを保護できる。
【０１２１】
（Ａ３：注文手続きの簡素化）
従来の一般注文では、Cookieなどを利用して個人情報の入力を省略することで注文を簡易化する方法が知られている。しかしこれは同じサービス提供者での２度目以降の注文に限られ、初回利用時には個人情報の入力が必要である。
【０１２２】

これに対し、本実施形態の匿名注文では、初回、2回目以降に関わらず個人情報の入力が不要であり、簡単に注文を行うことができる。

【０１２３】

（販売店ＳＰの利点）

（ＳＰ１：個人情報管理のコスト・リスクを排除）

従来の一般注文では、注文を受けるためには個人情報の管理が必要となる。しかし相次ぐ個人情報漏洩問題や個人情報保護法の施行により、厳重な個人情報管理が求められるようになっているため管理コストは増加する一方である。また、個人情報が漏洩した際の社会的信用の失墜など、リスクの大きさは計り知れない。

【０１２４】

これに対し、本実施形態の匿名注文では、個人情報を扱わずに受注することで、これらのコストやリスクを排除することができる。

【０１２５】

（ＳＰ２：潜在的な需要の取り込み）

購入者の利点で述べた通り、個人情報を渡すことに抵抗を感じている購入者は数多く、特に初めて利用する販売店には抵抗が大きいと考えられる。中断されるオンライントランザクションの推定額は２００４年には６３０万ドルにも上るとの調査結果もあり、この潜在的需要を一部でも取り込めることは販売店にとって大きなメリットとなる。

【０１２６】

（ＳＰ３：個人情報を管理せずにマーケット情報を入手）

従来の一般注文では、販売店ごとに個人情報を管理しているため詳細なマーケット情報を取得できる。

【０１２７】

これに対し、本実施形態の匿名注文では、一般注文と同様のマーケット情報を直接入手することはできないが、物流会社を通じてマーケット情報を取得することが可能である。

【０１２８】

（物流会社ＧＭの利点）

（１：既存の個人情報の活用）

前述した通り、個人情報の管理には多大なコストとリスクが伴うため、管理している個人情報を有効に活用することが望まれる。

【０１２９】

物流会社は匿名注文システムを利用して新たなサービスを行うことができる。匿名注文に対する需要は購入者の利点、販売店の利点で述べた通りであり、個人情報の有効活用を期待できる。

【０１３０】

（第２の実施形態）

次に、本発明の第２の実施形態に係る匿名注文システムについて説明する。

本実施形態は、第１の実施形態の変形例であり、プレゼントのように購入者が商品の発送先として自分の住所以外を指定する構成である。

【０１３１】

具体的には、本実施形態は第１の実施形態とほぼ同様であるが、図６に示したように、プレゼントの送り先を示すメッセージｍ４を物流会社公開鍵ＰGMで暗号化し、得られた物流会社への秘匿メッセージ$E_{PGM}$（ｍ４）を匿名注文情報に含めている。匿名注文情報にプレゼントかどうかを表すフラグを追加してもよい。

【０１３２】

以上のような構成では、図１７に示すように、ステップＳＴ２３ａにおいて秘匿メッセージ$E_{PGM}$（ｍ４）を含む匿名注文情報が生成され、ステップＳＴ３２ａにおいて商品が送り先に配送される。その他の動作は前述した通りである。

【０１３３】

従って、本実施形態によれば、第１の実施形態の効果に加え、購入者が商品の発送先と

して自分の住所以外を指定することができる。

【０１３４】

（第３の実施形態）

次に、本発明の第３の実施形態に係る匿名注文システムについて説明する。

本実施形態は、第１の実施形態の変形例であり、商品をデジタルコンテンツとした構成である。これに伴い、物流会社装置１０に代えて、物流会社装置１０と同様の構成をもつクレジット会社装置１０’を備えている。

【０１３５】

以上のような構成では、図１８に示すように、ステップＳＴ２８ｂにおいて暗号化デジタルコンテンツが販売店装置２０からクレジット会社装置１０’に送信され、ステップＳＴ３２ｂ－１（住所出力手段、提供手段）において、ＳＴ３１で特定された購入者の個人情報として記憶装置１１から読み出された購入者のネットワークアドレス情報に向けて暗号化デジタルコンテンツが購入者装置１０に送信される。暗号化デジタルコンテンツは、購入者のメンバ公開鍵PAで暗号化されたものである。また、ステップＳＴ３２ｂ－２において暗号化デジタルコンテンツがメンバ秘密鍵SAにより復号されて購入者用記憶装置１１に保存される。その他の動作は前述した通りである。

【０１３６】

従って、本実施形態によれば、商品をデジタルコンテンツとしても、第１の実施形態と同様の作用効果を得ることができる。また、本実施形態は、第２の実施形態に適用し、暗号化デジタルコンテンツを購入者装置１０以外の送り先アドレスに送信することもできる。また、本実施形態は、図１８のステップＳＴ２８ｂにおける暗号化デジタルコンテンツとステップＳＴ３２ｂ－１とを省略し、ステップＳＴ２６の正当メッセージに代えて暗号化デジタルコンテンツを販売店装置２０が購入者装置３０に送信する構成に変形してもよい。この変形例によれば、暗号化デジタルコンテンツをクレジットカード会社装置１０’を介さずに送信できるので、デジタルコンテンツを迅速に購入者に提供できる。

【０１３７】

なお、上記各実施形態に記載した手法は、コンピュータに実行させることのできるプログラムとして、磁気ディスク（フロッピー（登録商標）ディスク、ハードディスクなど）、光ディスク（ＣＤ－ＲＯＭ、ＤＶＤなど）、光磁気ディスク（ＭＯ）、半導体メモリなどの記憶媒体に格納して頒布することもできる。

【０１３８】

また、この記憶媒体としては、プログラムを記憶でき、かつコンピュータが読み取り可能な記憶媒体であれば、その記憶形式は何れの形態であっても良い。

【０１３９】

また、記憶媒体からコンピュータにインストールされたプログラムの指示に基づきコンピュータ上で稼働しているＯＳ（オペレーティングシステム）や、データベース管理ソフト、ネットワークソフト等のＭＷ（ミドルウェア）等が本実施形態を実現するための各処理の一部を実行しても良い。

【０１４０】

さらに、本発明における記憶媒体は、コンピュータと独立した媒体に限らず、ＬＡＮやインターネット等により伝送されたプログラムをダウンロードして記憶または一時記憶した記憶媒体も含まれる。

【０１４１】

また、記憶媒体は１つに限らず、複数の媒体から本実施形態における処理が実行される場合も本発明における記憶媒体に含まれ、媒体構成は何れの構成であっても良い。

【０１４２】

尚、本発明におけるコンピュータは、記憶媒体に記憶されたプログラムに基づき、本実施形態における各処理を実行するものであって、パソコン等の１つからなる装置、複数の装置がネットワーク接続されたシステム等の何れの構成であっても良い。

【０１４３】

また、本発明におけるコンピュータとは、パソコンに限らず、情報処理機器に含まれる演算処理装置、マイコン等も含み、プログラムによって本発明の機能を実現することが可能な機器、装置を総称している。

【０１４４】

なお、本願発明は、上記実施形態そのままに限定されるものではなく、実施段階ではその要旨を逸脱しない範囲で構成要素を変形して具体化できる。また、上記実施形態に開示されている複数の構成要素の適宜な組合せにより種々の発明を形成できる。例えば、実施形態に示される全構成要素から幾つかの構成要素を削除してもよい。更に、異なる実施形態に亘る構成要素を適宜組合せてもよい。

【図面の簡単な説明】

【０１４５】

【図１】本発明の第１の実施形態に係る匿名注文システムの構成を示す模式図である。

【図２】同実施形態における物流会社用記憶装置を説明するための模式図である。

【図３】同実施形態における販売店用記憶装置を説明するための模式図である。

【図４】同実施形態における注文情報等を説明するための模式図である。

【図５】同実施形態における購入者用記憶装置を説明するための模式図である。

【図６】同実施形態における匿名注文情報等を説明するための模式図である。

【図７】同実施形態における初期設定の動作を説明するためのシーケンス図である。

【図８】同実施形態における立ち上げの動作を説明するための模式図である。

【図９】同実施形態における販売店登録の動作を説明するための模式図である。

【図１０】同実施形態における購入者登録の動作を説明するための模式図である。

【図１１】同実施形態における匿名注文・配送・決済の動作を説明するためのシーケンス図である。

【図１２】同実施形態における匿名注文の動作を説明するための模式図である。

【図１３】同実施形態における匿名注文の動作を詳細に説明するための模式図である。

【図１４】同実施形態における匿名注文の検証処理を説明するための模式図である。

【図１５】同実施形態における商品配送・決済の動作を説明するための模式図である。

【図１６】同実施形態における署名者特定・マーケット情報生成の動作を説明するための模式図である。

【図１７】本発明の第２の実施形態に係る匿名注文システムの動作を説明するためのシーケンス図である。

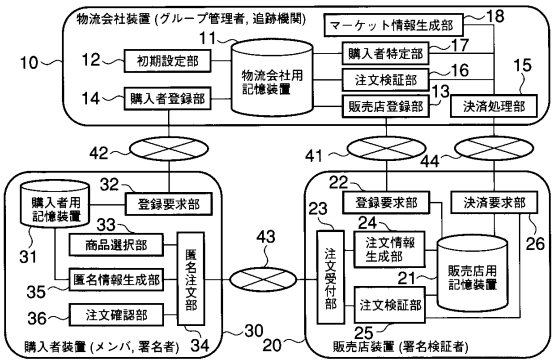
【図１８】本発明の第３の実施形態に係る匿名注文システムの動作を説明するためのシーケンス図である。

【符号の説明】

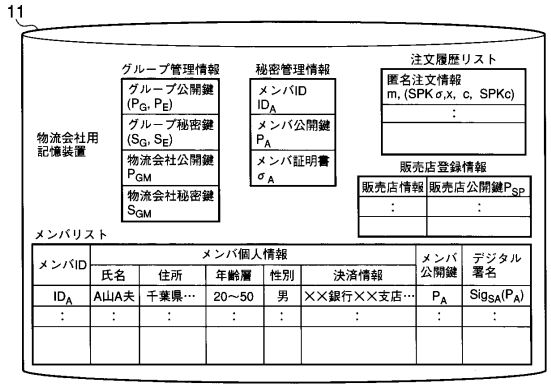
【０１４６】

１０…物流会社装置、１１…物流会社用記憶装置、１２…初期設定部、１３…販売店登録部、１４…購入者登録部、１５…決済処理部、１６…注文検証部、１７…購入者特定部、１８…マーケット情報生成部、２０…販売店装置、２１…販売店用記憶装置、２２，３２…登録要求部、２３…注文受付部、２４…注文情報生成部、２５…注文検証部、２６…決済要求部、３０…購入者装置、３１…購入者用記憶装置、３３…商品選択部、３４…匿名注文部、３５…匿名情報生成部、３６…注文確認部、４１～４４…ネットワーク。

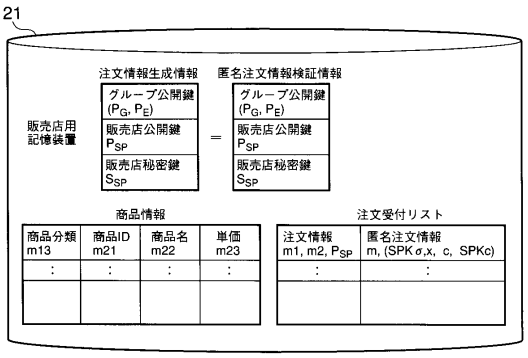
【図１】



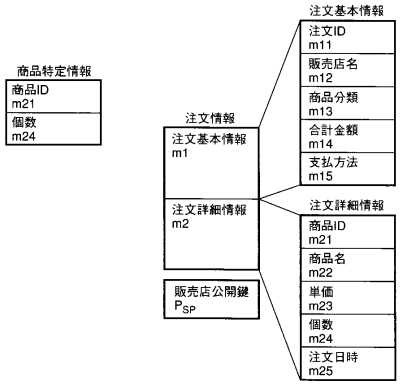

【図２】



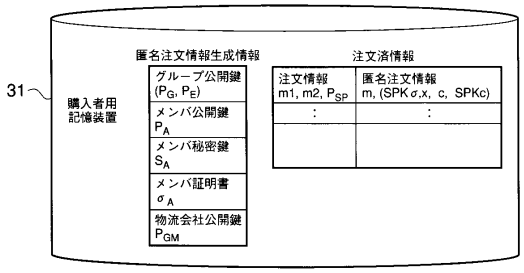

【図３】



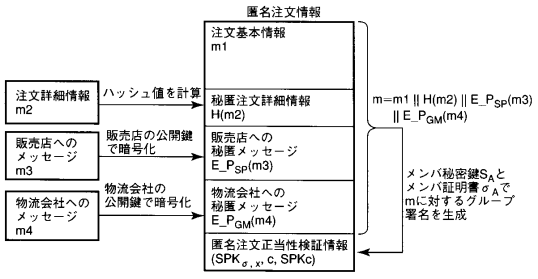

【図４】



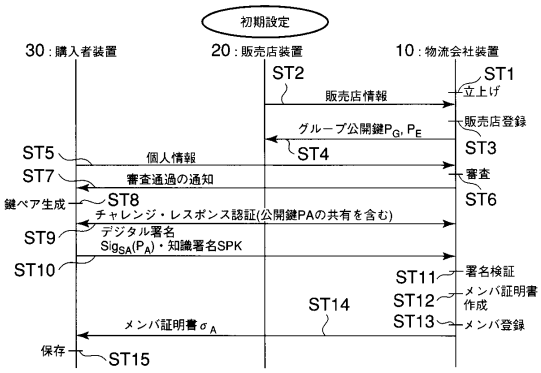

【図５】



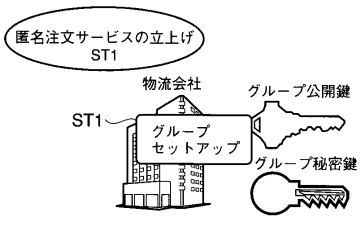

【図６】



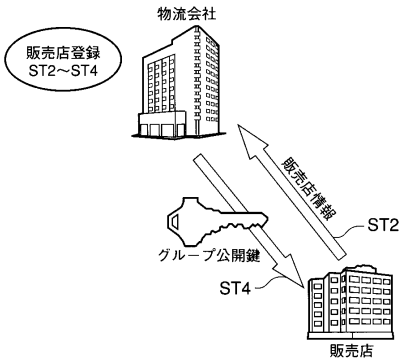

【図７】



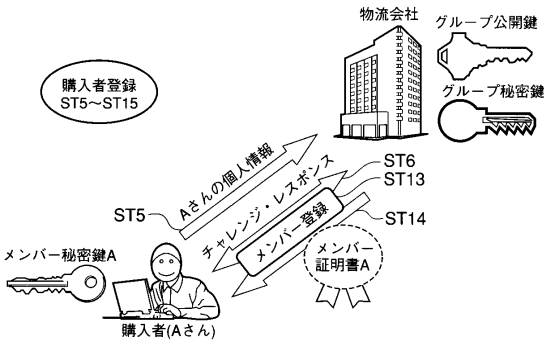

【図８】



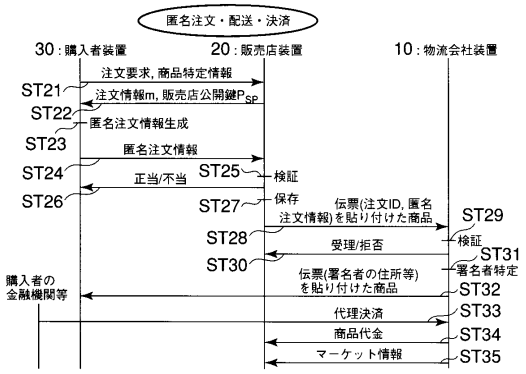
【図９】



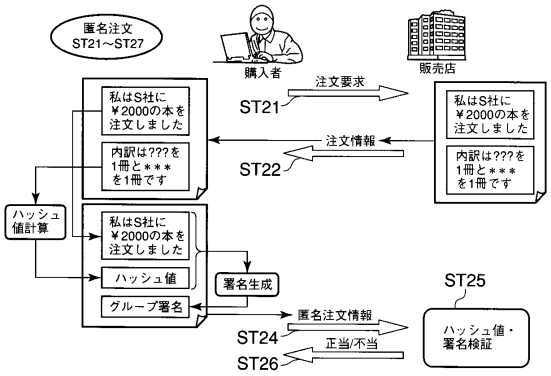

【図１０】



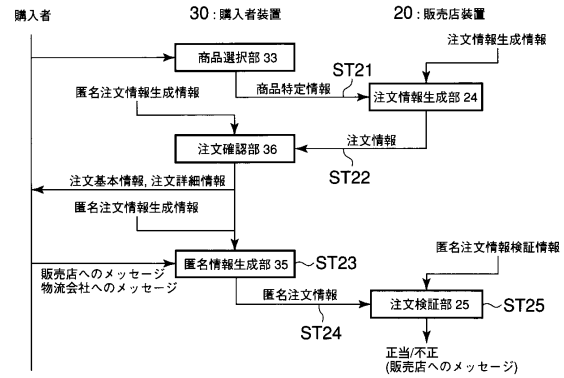

【図１１】



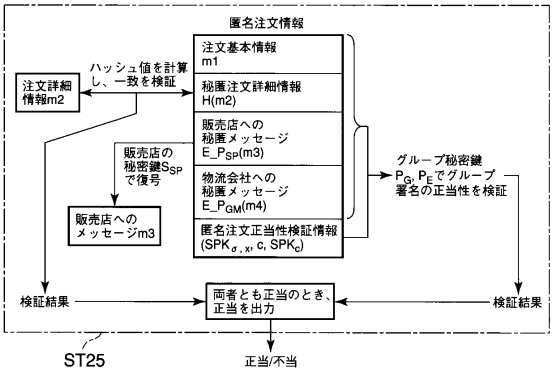

【図１２】



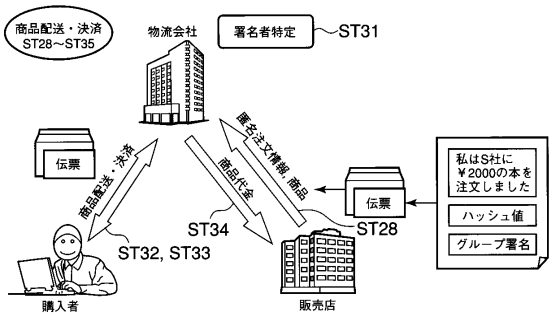

【図１３】



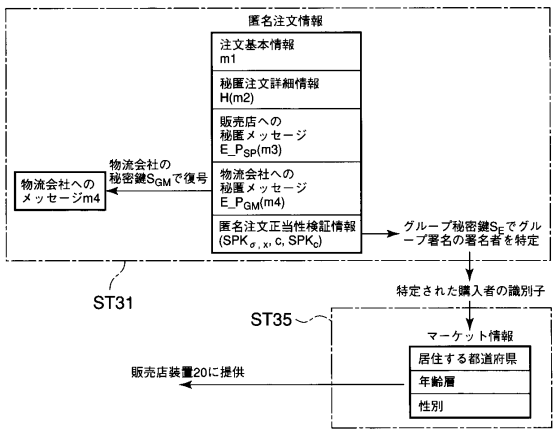

【図１４】



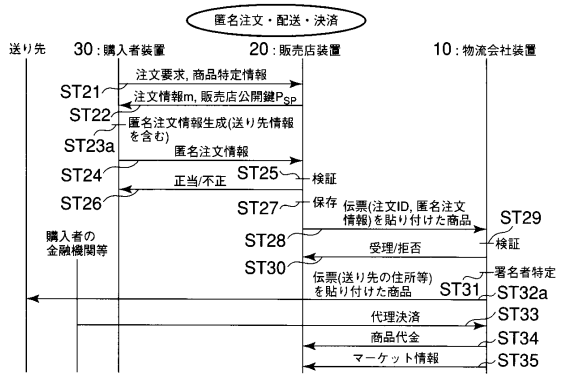

【図１５】



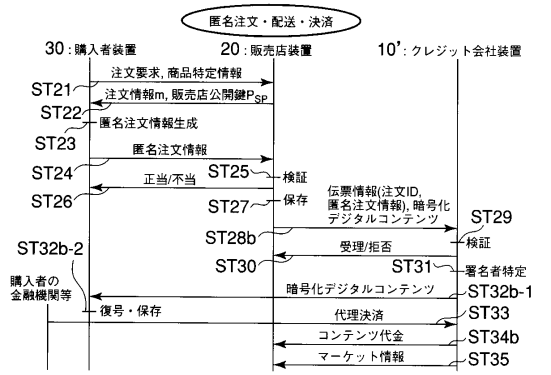

【図１６】



【図１７】


匿名注文・配送・決済
送り先
30：購入者装置
20：販売店装置
10：物流会社装置
注文要求, 商品特定情報
ST21
注文情報m, 販売店公開鍵$P_{SP}$
ST22
匿名注文情報生成(送り先情報を含む)
ST23a
匿名注文情報
ST24
正当/不正
ST25
検証
ST26
ST27
保存
伝票(注文ID, 匿名注文情報)を貼り付けた商品
ST29
検証
購入者の金融機関等
ST28
受理/拒否
ST30
伝票(送り先の住所等)を貼り付けた商品
署名者特定
ST31
ST32a
代理決済
ST33
商品代金
ST34
マーケット情報
ST35

【図１８】


匿名注文・配送・決済
30：購入者装置
20：販売店装置
10'：クレジット会社装置
注文要求, 商品特定情報
ST21
注文情報m, 販売店公開鍵$P_{SP}$
ST22
匿名注文情報生成
ST23
匿名注文情報
ST24
正当/不当
ST25
検証
ST26
ST27
保存
伝票情報(注文ID, 匿名注文情報), 暗号化デジタルコンテンツ
ST29
ST28b
検証
受理/拒否
ST32b-2
ST30
ST31
署名者特定
購入者の金融機関等
暗号化デジタルコンテンツ
ST32b-1
復号・保存
代理決済
ST33
コンテンツ代金
ST34b
マーケット情報
ST35

フロントページの続き

(51)Int.Cl. FI
H04L 9/00 675B

(74)代理人 100109830
弁理士 福原 淑弘
(74)代理人 100084618
弁理士 村松 貞男
(74)代理人 100092196
弁理士 橋本 良郎
(72)発明者 吉田 琢也
東京都港区芝浦一丁目１番１号 東芝ソリューション株式会社内
(72)発明者 岡田 光司
東京都港区芝浦一丁目１番１号 東芝ソリューション株式会社内
(72)発明者 加藤 岳久
東京都港区芝浦一丁目１番１号 東芝ソリューション株式会社内

審査官 宮久保 博幸

(56)参考文献 特開２００２－００７９０４（ＪＰ，Ａ）
特開２０００－２１５２５２（ＪＰ，Ａ）
米国特許出願公開第２００２／０１１６３３７（ＵＳ，Ａ１）
特開２００４－０５４９０５（ＪＰ，Ａ）
特開２００４－２５８８９７（ＪＰ，Ａ）
特開２００４－１０２７６６（ＪＰ，Ａ）
特開２００４－１３９４１３（ＪＰ，Ａ）
加藤岳久，Ｒ＆Ｄ最前線 プライバシーを保護する匿名認証技術，東芝レビュー，日本，株式会社東芝，２００３年１２月 １日，第５８巻，第１２号，ｐ．７２－７３

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｑ １０／００－５０／００
Ｈ０４Ｌ ９／３２