(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4664107号
(P4664107)
(45)発行日　平成23年4月6日(2011.4.6)　(24)登録日　平成23年1月14日(2011.1.14)

(51)Int.Cl.　　F I
G06F 21/24 (2006.01)　　G06F 12/14 560C
G06F 21/20 (2006.01)　　G06F 15/00 330A
G06Q 50/00 (2006.01)　　G06F 17/60 132

請求項の数 20　(全 32 頁)

(21)出願番号　特願2005-102712 (P2005-102712)
(22)出願日　平成17年3月31日 (2005.3.31)
(65)公開番号　特開2006-285490 (P2006-285490A)
(43)公開日　平成18年10月19日 (2006.10.19)
審査請求日　平成20年3月26日 (2008.3.26)

（出願人による申告）国等の委託研究の成果に係る特許出願（平成１６年度、総務省、情報通信研究機構委託研究「通信ネットワーク利用放送技術に関する研究開発（平成１５年度拡充課題）」、産業活力再生特別措置法第３０条の適用を受けるもの）

(73)特許権者　000005108
株式会社日立製作所
東京都千代田区丸の内一丁目６番６号
(73)特許権者　000004352
日本放送協会
東京都渋谷区神南２丁目２番１号
(73)特許権者　591053926
財団法人エヌエイチケイエンジニアリングサービス
東京都世田谷区砧一丁目１０番１１号
(74)代理人　100080001
弁理士　筒井　大和

最終頁に続く

(54)【発明の名称】事業者側装置、利用者側装置、個人情報閲覧更新システムおよび個人情報閲覧更新方法

(57)【特許請求の範囲】
【請求項１】
事業者側で利用者の提供する個人情報を収集し、前記利用者に対して、収集した前記個人情報の内容を送信し、前記利用者側で前記事業者側より送信された前記個人情報の内容の閲覧および更新をするシステムの事業者側装置であって、
前記利用者から収集した個人情報を登録する利用者情報データベースと、
個人情報を持ちその個人情報を提供する前記利用者側より個人情報を受信し、受信した個人情報を前記利用者情報データベースに登録する個人情報受信手段と、
閲覧用のハッシュ値と前記個人情報を提供する際に付与した自身の作成した電子著名との整合性を検証し、閲覧用の個人情報の各項目について、自身の持つデータベースより各項目の値を取得して閲覧し、更新のある項目について送信することが可能な前記利用者側からの要求に応じて、前記利用者に対して、前記利用者情報データベースに登録した閲覧用の個人情報を送信する際に、前記閲覧用の個人情報の各項目をハッシュ値として送信して、前記利用者に対して収集した個人情報を閲覧させる利用者情報開示手段とを備え、
前記個人情報受信手段は、前記利用者側で前記ハッシュ値に基づいて閲覧された項目のうち、更新のある項目があった場合、前記利用者側から送信されたその更新した値を受信し、前記利用者情報データベースに登録することを特徴とする事業者側装置。
【請求項２】
請求項１記載の事業者側装置において、
前記個人情報受信手段は、

前記利用者側から受け取った送信用個人情報に含まれる各項目の乱数と各項目の個人情報の値とを合わせて項目毎にハッシュ値を生成するハッシュ値計算手段と、
生成した各項目のハッシュ値を全て合わせたものと、前記送信用個人情報に含まれる利用者側の電子署名との整合性が取れるかどうかを検証する署名検証手段と、
署名検証した前記送信用個人情報を前記利用者情報データベースに登録するデータベース登録手段とを有することを特徴とする事業者側装置。
【請求項３】
請求項１記載の事業者側装置において、
前記利用者情報開示手段は、
閲覧対象となる前記利用者の情報について、前記利用者情報データベースに登録された個人情報より、前記各項目の個人情報の値と前記各項目の乱数と前記利用者の電子署名を取得するデータ取得手段と、
前記各項目の乱数と各項目の個人情報の値とを合わせて項目毎にハッシュ値を生成するハッシュ値計算手段と、
生成した前記各項目のハッシュ値を全て合わせたものに対して事業者側の電子署名を生成する署名作成手段と、
前記各項目の乱数と前記各項目のハッシュ値と前記利用者の電子署名と前記事業者の電子署名とからなる閲覧用個人情報を作成し、利用者側に送信する閲覧用個人情報送信手段とを有することを特徴とする事業者側装置。
【請求項４】
請求項１記載の事業者側装置において、
前記利用者情報開示手段は、
前記利用者、あるいは、前記利用者の個人情報を必要とする他の事業者より、個人情報閲覧要求を受信する要求受信手段と、
閲覧対象となる前記利用者の情報について、前記利用者情報データベースに登録された個人情報より、前記各項目の個人情報の値と前記各項目の乱数と前記利用者の電子署名を取得するデータ取得手段と、
前記各項目の乱数と各項目の個人情報の値とを合わせて項目毎にハッシュ値を生成するハッシュ値計算手段と、
誰に対してどの項目の個人情報を秘匿するかを示す開示制御情報を記載した事業者開示ポリシーファイルに基づき、開示する項目については、前記各項目の個人情報の値と前記各項目の乱数と、開示しない項目については、前記生成したハッシュ値と、前記利用者側の電子署名とからなる開示用利用者情報を作成する開示用利用者情報作成手段と、
前記生成した開示用利用者情報に対して前記事業者側の電子署名を生成し、前記開示用利用者情報に付与して送信する送信手段とを有することを特徴とする事業者側装置。
【請求項５】
請求項１記載の事業者側装置において、
前記利用者情報開示手段は、
前記利用者、あるいは、前記利用者の個人情報を必要とする他の事業者より、個人情報閲覧要求を受信する要求受信手段と、
閲覧対象となる前記利用者の情報について、前記利用者情報データベースに登録された個人情報より、前記各項目の個人情報の値と前記各項目の乱数と前記利用者の電子署名とを取得するデータ取得手段と、
前記各項目の乱数と各項目の個人情報の値とを合わせて項目毎にハッシュ値を生成するハッシュ値計算手段と、
誰に対してどの項目の個人情報を秘匿するかを示す開示制御情報を記載した事業者開示ポリシーファイルおよび前記閲覧対象となる前記利用者から送信された個人開示ポリシーファイルに基づき、開示する項目については、前記各項目の個人情報の値と前記各項目の乱数と、開示しない項目については、前記生成したハッシュ値と、前記利用者側の電子署名とからなる開示用利用者情報を作成する開示用利用者情報作成手段と、

前記作成した開示用利用者情報に対して前記事業者側の電子署名を生成し、前記開示用利用者情報に付与して送信する送信手段とを有することを特徴とする事業者側装置。

【請求項６】

事業者側で利用者の提供する個人情報を収集し、前記利用者に対して、収集した前記個人情報の内容を送信し、前記利用者側で前記事業者側より送信された前記個人情報の内容の閲覧および更新をするシステムの利用者側装置であって、

前記個人情報を格納しておく個人情報データベースと、

前記利用者の提供する個人情報を自身のデータベースに登録する前記事業者側に対して前記個人情報を送信する個人情報送信手段と、

前記利用者に対して閲覧用の個人情報の各項目をハッシュ値として送信する前記事業者に対して登録された前記個人情報の閲覧を要求し、前記事業者側から閲覧用の個人情報の各項目をハッシュ値として受信し、受信した閲覧用の個人情報の各項目のハッシュ値と前記閲覧用の個人情報に含まれる前記利用者側装置が作成した利用者署名との整合性を検証した後、前記閲覧用の個人情報の各項目について、前記個人情報データベースより各項目の値を取得して閲覧し、更新のある項目については、前記事業者側に更新した値を送信する利用者情報閲覧手段とを備えたことを特徴とする利用者側装置。

【請求項７】

請求項６載の利用者側装置において、

前記個人情報送信手段は、

項目毎に乱数を生成する乱数生成手段と、

前記生成した乱数と各項目の個人情報の値とを合わせて項目毎にハッシュ値を生成するハッシュ値計算手段と、

生成した前記各項目のハッシュ値を全て合わせたものに対して利用者側の電子署名を生成する署名作成手段と、

前記各項目の個人情報の値と前記各項目の乱数と前記利用者側の電子署名からなる送信用個人情報を作成し、事業者側に送信する送信用個人情報送信手段と、

前記送信用個人情報を前記個人情報データベースに登録するデータベース登録手段とを有することを特徴とする利用者側装置。

【請求項８】

請求項６記載の利用者側装置において、

前記利用者情報閲覧手段は、

前記事業者側より受け取った前記閲覧用個人情報に含まれる各項目のハッシュ値を全て合わせたものと、前記閲覧用個人情報に含まれる前記事業者側の電子署名との整合性が取れるかどうかを検証する事業者署名検証手段と、

前記事業者側より受け取った前記閲覧用個人情報に含まれる各項目のハッシュ値を全て合わせたものと、前記閲覧用個人情報に含まれる前記利用者側の電子署名との整合性が取れるかどうかを検証する利用者署名検証手段と、

前記閲覧用個人情報の各項目について、前記個人情報データベースに登録された自身の個人情報の各項目の値を取得して、前記個人情報データベースより取得した項目の値を表示し閲覧するデータ表示手段と、

前記利用者署名検証手段によって、整合性がとれず改ざんされていることが検証された場合においては、前記データ表示手段により前記閲覧用個人情報の各項目の値を表示する際に、前記閲覧用個人情報に含まれる各項目のハッシュ値と前記個人情報データベースに記録された各項目のハッシュ値から改ざんされている項目を特定し、そのデータを表示する改ざん検知手段とを有することを特徴とする利用者側装置。

【請求項９】

請求項６記載の利用者側装置において、

前記利用者情報閲覧手段は、

前記事業者側より受け取った前記閲覧用個人情報について、変更がある項目が存在する場合に、各項目について乱数を生成する乱数生成手段と、

前記生成した乱数と、変更がある項目を含む各項目の個人情報の値とを合わせて項目毎にハッシュ値を生成するハッシュ値計算手段と、
生成した前記各項目のハッシュ値を全て合わせたものに対して利用者側の電子署名を生成する署名作成手段と、
前記各項目の個人情報について、変更がある項目についてはその項目の値と前記生成した乱数と、変更が無い項目については前記生成した乱数と、前記利用者側の電子署名とからなる更新用個人情報を作成し、前記事業者側に送信する更新用個人情報送信手段と、
前記生成した各項目の乱数と、前記変更がある項目の値と、前記利用者側の電子署名とを前記個人情報データベースに登録するデータベース登録手段とを有することを特徴とする利用者側装置。

【請求項１０】
請求項６記載の利用者側装置において、
前記個人情報送信手段は、
項目毎に乱数を生成する乱数生成手段と、
前記生成した乱数と各項目の個人情報の値とを合わせて項目毎にハッシュ値を生成するハッシュ値計算手段と、
生成した前記各項目のハッシュ値を全て合わせたものに対して利用者側の電子署名を生成する署名作成手段と、
前記各項目の個人情報の値と前記各項目の乱数と、前記利用者側の電子署名と、誰に対してどの項目の個人情報を秘匿するかを示す開示制御情報を記載した個人開示ポリシーファイルとからなる送信用個人情報を作成し、前記事業者側に送信する送信用個人情報送信手段と、
前記送信用個人情報を前記個人情報データベースに登録し、前記個人開示ポリシーファイルを前記利用者側装置に格納するデータベース登録手段とを有することを特徴とする利用者側装置。

【請求項１１】
利用者から収集した個人情報を登録する利用者情報データベースを有し、利用者から個人情報を収集し、前記利用者に対して、収集した前記個人情報の内容の閲覧および更新をさせる事業者側装置と、
自身の個人情報を格納しておく個人情報データベースを有し、前記個人情報を前記事業者側装置に送信し、前記事業者側装置に前記個人情報の閲覧を要求し、要求に応じて前記事業者側装置より送られた個人情報を、閲覧および更新する利用者側装置とを備え、
前記事業者側装置は、
前記利用者側装置より個人情報を受信し、受信した個人情報を前記利用者情報データベースに登録する個人情報受信手段と、
前記利用者側装置からの要求に応じて、前記利用者に対して、前記利用者情報データベースに登録した閲覧用の個人情報を送信する際に、前記閲覧用の個人情報の各項目をハッシュ値として送信して、前記利用者に対して収集した個人情報を閲覧させる利用者情報開示手段とを有し、
前記利用者側装置は、
前記事業者側装置に対して個人情報を送信する個人情報送信手段と、
前記事業者側装置に対して登録された前記個人情報の閲覧を要求し、前記事業者側装置より受信した前記閲覧用の個人情報の各項目のハッシュ値と前記閲覧用の個人情報に含まれる前記利用者側装置が作成した利用者署名との整合性を検証した後、前記閲覧用の個人情報の各項目について、前記個人情報データベースより各項目の値を取得して前記閲覧用の個人情報を閲覧し、更新のある項目については、前記事業者側装置に更新した値を送信する利用者情報閲覧手段とを有することを特徴とする個人情報閲覧更新システム。

【請求項１２】
利用者から収集した個人情報を登録する利用者情報データベースを有し、利用者から個人情報を収集し、前記利用者に対して、収集した前記個人情報の内容の閲覧および更新を

させる事業者側装置と、
自身の個人情報を格納しておく個人情報データベースを有し、前記個人情報を前記事業者側装置に送信し、前記事業者側装置に前記個人情報の閲覧を要求し、要求に応じて前記事業者側装置より送られた個人情報を、閲覧および更新する利用者側装置とを備えた個人情報閲覧更新システムにおける個人情報閲覧更新方法であって、
前記事業者側装置の個人情報受信手段により、前記利用者側装置より個人情報を受信し、
前記事業者側装置の利用者情報開示手段により、前記利用者側装置からの要求に応じて、前記利用者に対して閲覧用の個人情報を送信する際に、前記閲覧用の個人情報の各項目をハッシュ値として送信して、前記利用者に対して収集した個人情報を閲覧させ、
前記利用者側装置の個人情報送信手段により、前記事業者側装置に対して個人情報を送信し、
前記利用者側装置の利用者情報閲覧手段により、前記事業者側装置に対して登録された自らの個人情報の閲覧を要求し、前記事業者側装置より受信した閲覧用の個人情報の各項目のハッシュ値と前記閲覧用の個人情報に含まれる前記利用者側装置が作成した利用者署名との整合性を検証した後、前記閲覧用の個人情報の各項目について、前記個人情報データベースより各項目の値を取得して前記閲覧用の個人情報を閲覧し、更新のある項目については、前記事業者側装置に更新した値を送信することを特徴とする個人情報閲覧更新方法。
【請求項１３】
請求項１２記載の個人情報閲覧更新方法において、
前記個人情報送信手段は、
項目毎に乱数を生成する乱数生成ステップと、
前記生成した乱数と各項目の個人情報の値とを合わせて項目毎にハッシュ値を生成するハッシュ値計算ステップと、
生成した前記各項目のハッシュ値を全て合わせたものに対して利用者側装置の電子署名を生成する署名作成ステップと、
前記各項目の個人情報の値と前記各項目の乱数と前記利用者側装置の電子署名からなる送信用個人情報を作成し、事業者側装置に送信する送信用個人情報送信ステップと、
前記送信用個人情報を前記個人情報データベースに登録するデータベース登録ステップとを実行することを特徴とする個人情報閲覧更新方法。
【請求項１４】
請求項１２記載の個人情報閲覧更新方法において、
前記個人情報受信手段は、
前記利用者側装置から受け取った前記送信用個人情報に含まれる各項目の乱数と各項目の個人情報の値とを合わせて項目毎にハッシュ値を生成するハッシュ値計算ステップと、
生成した各項目のハッシュ値を全て合わせたものと、前記送信用個人情報に含まれる利用者側装置の電子署名との整合性が取れるかどうかを検証する署名検証ステップと、
署名検証した前記送信用個人情報を前記利用者情報データベースに登録するデータベース登録ステップとを実行することを特徴とする個人情報閲覧更新方法。
【請求項１５】
請求項１２記載の個人情報閲覧更新方法において、
前記利用者情報開示手段は、
閲覧対象となる利用者の情報について、前記利用者情報データベースに登録された個人情報より、前記各項目の個人情報の値と前記各項目の乱数と前記利用者の電子署名を取得するデータ取得ステップと、
前記各項目の乱数と各項目の個人情報の値とを合わせて項目毎にハッシュ値を生成するハッシュ値計算ステップと、
生成した前記各項目のハッシュ値を全て合わせたものに対して事業者側装置の電子署名を生成する署名作成ステップと、

前記各項目の乱数と前記各項目のハッシュ値と前記利用者の電子署名と前記事業者の電子署名とからなる閲覧用個人情報を作成し、利用者側装置に送信する閲覧用個人情報送信ステップとを実行することを特徴とする個人情報閲覧更新方法。

【請求項１６】

請求項１２記載の個人情報閲覧更新方法において、

前記利用者情報閲覧手段は、

前記事業者側装置より受け取った前記閲覧用個人情報に含まれる各項目のハッシュ値を全て合わせたものと、前記閲覧用個人情報に含まれる事業者側装置の電子署名との整合性が取れるかどうかを検証する事業者署名検証ステップと、

前記事業者側装置より受け取った前記閲覧用個人情報に含まれる各項目のハッシュ値を全て合わせたものと、前記閲覧用個人情報に含まれる前記利用者側装置の電子署名との整合性が取れるかどうかを検証する利用者署名検証ステップと、

前記閲覧用個人情報の各項目について、前記個人情報データベースに登録された自身の個人情報の各項目の値を取得して、前記個人情報データベースより取得した項目の値を表示し閲覧するデータ表示ステップと、

前記利用者署名検証ステップによって、整合性が取れず改ざんされていることが検証された場合においては、前記データ表示ステップにより前記閲覧用個人情報の各項目の値を表示する際に、前記閲覧用個人情報に含まれる各項目のハッシュ値と前記個人情報データベースに記録された各項目のハッシュ値から改ざんされている項目を特定し、そのデータを表示する改ざん検知ステップとを実行することを特徴とする個人情報閲覧更新方法。

【請求項１７】

請求項１２記載の個人情報閲覧更新方法において、

前記利用者情報閲覧手段は、

前記事業者側装置より受け取った前記閲覧用個人情報について、変更がある項目が存在する場合に、各項目について乱数を生成する乱数生成ステップと、

前記生成した乱数と、変更がある項目を含む各項目の個人情報の値とを合わせて項目毎にハッシュ値を生成するハッシュ値計算ステップと、

生成した前記各項目のハッシュ値を全て合わせたものに対して利用者側装置の電子署名を生成する署名作成ステップと、

前記各項目の個人情報について、変更がある項目についてはその項目の値と前記生成した乱数と、変更が無い項目については前記生成した乱数と、前記利用者側装置の電子署名とからなる更新用個人情報を作成し、事業者側装置に送信する更新用個人情報送信ステップと、

前記生成した各項目の乱数と、前記変更がある項目の値と、前記利用者側装置の電子署名とを前記個人情報データベースに登録するデータベース登録ステップとを実行することを特徴とする個人情報閲覧更新方法。

【請求項１８】

請求項１２記載の個人情報閲覧更新方法において、

前記個人情報送信手段は、

項目毎に乱数を生成する乱数生成ステップと、

前記生成した乱数と各項目の個人情報の値とを合わせて項目毎にハッシュ値を生成するハッシュ値計算ステップと、

生成した前記各項目のハッシュ値を全て合わせたものに対して利用者側装置の電子署名を生成する署名作成ステップと、

前記各項目の個人情報の値と前記各項目の乱数と、前記利用者側装置の電子署名と、誰に対してどの項目の個人情報を秘匿するかを示す開示制御情報とを記載した個人開示ポリシーファイルと、からなる送信用個人情報を作成し、事業者側装置に送信する送信用個人情報送信ステップと、

前記送信用個人情報を前記個人情報データベースに登録し、前記個人開示ポリシーファイルを前記利用者側装置に格納するデータベース登録ステップとを実行することを特徴と

する個人情報閲覧更新方法。
【請求項１９】
請求項１２記載の個人情報閲覧更新方法において、
前記利用者情報開示手段は、
前記利用者、あるいは、前記利用者の個人情報を必要とする他の事業者端末より、個人情報閲覧要求を受信する要求受信ステップと、
閲覧対象となる前記利用者の情報について、前記利用者情報データベースに登録された個人情報より、前記各項目の個人情報の値と前記各項目の乱数と前記利用者の電子署名を取得するデータ取得ステップと、
前記各項目の乱数と各項目の個人情報の値とを合わせて項目毎にハッシュ値を生成するハッシュ値計算ステップと、
誰に対してどの項目の個人情報を秘匿するかを示す開示制御情報を記載した事業者開示ポリシーファイルに基づき、開示する項目については、前記各項目の個人情報の値と前記各項目の乱数と、開示しない項目については、前記生成したハッシュ値と、前記利用者側装置の電子署名からなる開示用利用者情報を作成する開示用利用者情報作成ステップと、
前記作成した開示用利用者情報に対して事業者側装置の電子署名を生成し、前記開示用利用者情報に付与して送信する送信ステップとを実行することを特徴とする個人情報閲覧更新方法。
【請求項２０】
請求項１２記載の個人情報閲覧更新方法において、
前記利用者情報開示手段は、
前記利用者、あるいは、前記利用者の個人情報を必要とする他の事業者より、個人情報閲覧要求を受信する要求受信ステップと、
閲覧対象となる前記利用者の情報について、前記利用者情報データベースに登録された個人情報より、前記各項目の個人情報の値と前記各項目の乱数と前記利用者の電子署名とを取得するデータ取得ステップと、
前記各項目の乱数と各項目の個人情報の値とを合わせて項目毎にハッシュ値を生成するハッシュ値計算ステップと、
誰に対してどの項目の個人情報を秘匿するかを示す開示制御情報を記載した事業者開示ポリシーファイルおよび前記閲覧対象となる前記利用者から送信された個人開示ポリシーファイルに基づき、開示する項目については、前記各項目の個人情報の値と前記各項目の乱数と、開示しない項目については、前記生成したハッシュ値と、前記利用者側の電子署名とからなる開示用利用者情報を作成する開示用利用者情報作成ステップと、
前記作成した開示用利用者情報に対して前記事業者側の電子署名を生成し、前記開示用利用者情報に付与して送信する送信ステップとを実行することを特徴とする個人情報閲覧更新方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、事業者側装置、利用者側装置、個人情報閲覧更新システムおよび個人情報閲覧更新方法に関し、特に、その個人情報保護管理技術に関する。
【背景技術】
【０００２】
インターネットや家庭内のネットワークが普及し、いわゆるＰＣだけでなく、それ以外の一般家電製品にもネットワーク対応型が普及し始めている。こうした中で、個人のプロフィールや家電の使用状況など生活に密着した個人情報が、通信ネットワークを介して容易に送信可能となり、オンラインで個人情報を収集しサービス提供に利用する事業が急増している。
【０００３】
このようなサービスにおいては、個人情報が頻繁にネットワーク上を流れることになる

。第三者による個人情報の悪用や改ざんを防ぐためには、このネットワーク上を流れる個人情報の保護が重要である。

【０００４】

個人情報の漏洩を保護する技術としては、ネットワーク上を流れる個人情報の開示を制御する技術（例えば、特許文献１参照）がある。また、第三者による改ざんを防止する技術としては、電子署名の技術がある（例えば、特許文献２参照）。

【特許文献１】特開２００４－２５８８７２号公報

【特許文献２】特開２００１－１６７０８６号公報

【発明の開示】

【発明が解決しようとする課題】

【０００５】

前述のような個人情報を利用したサービスを行う場合、サービス利用者からサービス事業者に個人情報の送信が発生するだけではなく、サービス事業者からサービス利用者にも個人情報が送られる場合がある。例えば、サービス利用者が、どの事業体で自らのどのような個人情報が管理されていて、さらに自らが開示した情報と相違がないか確認したり、一度送信した個人情報を更新したい場合がある。その時には、サービス利用者は、サービス事業者より自らの送信した個人情報を閲覧させてもらう必要がある。

【０００６】

従来技術では、暗号化、および電子署名の添付により、送受信される個人情報を保護しているものの、第三者による成りすましがあった場合、個人情報が盗まれてしまう恐れがあった。特に、上記のように相互で頻繁に個人情報のやり取りが発生する場合、その危険性はますます増大する。

【０００７】

サービス事業者は、収集した個人情報をサービス利用者に示して、個人情報の管理状況や改ざんされていないことを確認させ、サービス利用者の不安を取り除いて信頼を得ることが望ましい。しかし、一方で、サービス事業者は、個人情報の漏洩・改ざんの危険を防止するため、できる限りサービス利用者の閲覧要求に応えて個人情報を送信することは避けたい。

【０００８】

特許文献１に記載された技術では、サービス利用者の開示ポリシーに応じて、サービス事業者が開示する情報を制御する方法については記載されているが、個人情報の内容を秘匿したまま全個人情報が改ざんされていないことをサービス利用者が確認する方法については、記載されていない。

【０００９】

特許文献２に記載された技術では、個人情報の各項目に対して改ざん検知のための電子署名を作成する方法については記載されているが、開示制御された後の個人情報について、元の電子署名を変更することなく、元の個人情報の原本性を確認することについては、記載されていない。

【００１０】

そこで、本発明の目的は、個人情報を秘匿したまま個人情報の管理状況や完全性の確認、あるいは更新のために個人情報提供者が自らの提供した個人情報を安全に閲覧更新する事業者側装置、利用者側装置、個人情報閲覧更新システムおよび個人情報閲覧更新方法を提供することにある。

【課題を解決するための手段】

【００１１】

本発明による事業者側装置は、事業者側で利用者から個人情報を収集し、利用者に対して、収集した個人情報の内容の閲覧および更新をさせるシステムの事業者側装置であって、利用者に対して閲覧用の個人情報を送信する際に、閲覧用の個人情報の各項目をハッシュ値として送信し、利用者側でハッシュ値に基づいて閲覧された項目について、更新のある場合、その更新した値を利用者側から受信するものである。

【００１２】
また、本発明による事業者側装置は、事業者側で利用者から個人情報を収集し、利用者に対して、収集した個人情報の内容の閲覧および更新をさせるシステムの事業者側装置であって、利用者から収集した個人情報を登録する利用者情報データベースと、利用者側より個人情報を受信し、受信した個人情報を利用者情報データベースに登録する個人情報受信手段と、利用者側からの要求に応じて、利用者に対して、利用者情報データベースに登録した閲覧用の個人情報を送信する際に、閲覧用の個人情報の各項目をハッシュ値として送信して、利用者に対して収集した個人情報を閲覧させる利用者情報開示手段とを備え、個人情報受信手段は、利用者側でハッシュ値に基づいて閲覧された項目について、更新のある場合、その更新した値を利用者側から受信するものである。

【００１３】
また、本発明による利用者側装置は、事業者側で利用者から個人情報を収集し、利用者に対して、収集した個人情報の内容の閲覧および更新をさせるシステムの利用者側装置であって、利用者に対して閲覧用の個人情報の各項目をハッシュ値として送信する事業者に対して登録された個人情報の閲覧を要求し、事業者側から閲覧用の個人情報の各項目をハッシュ値として受信し、受信した閲覧用の個人情報の各項目のハッシュ値と閲覧用の個人情報に含まれる利用者側装置が作成した利用者署名との整合性を検証した後、閲覧用の個人情報の各項目について、個人情報データベースより各項目の値を取得して閲覧し、更新のある項目については、事業者側に更新した値を送信する利用者情報閲覧手段とを備えたものである。

【００１４】
また、本発明による個人情報閲覧更新システムは、利用者から収集した個人情報を登録する利用者情報データベースを有し、利用者から個人情報を収集し、利用者に対して、収集した個人情報の内容の閲覧および更新をさせる事業者側装置と、自身の個人情報を格納しておく個人情報データベースを有し、個人情報を事業者側装置に送信し、事業者側装置に個人情報の閲覧を要求し、要求に応じて事業者側装置より送られた個人情報を、閲覧および更新する利用者側装置とを備え、事業者側装置は、利用者側装置より個人情報を受信し、受信した個人情報を利用者情報データベースに登録する個人情報受信手段と、利用者側装置からの要求に応じて、利用者に対して、利用者情報データベースに登録した閲覧用の個人情報を送信する際に、閲覧用の個人情報の各項目をハッシュ値として送信して、利用者に対して収集した個人情報を閲覧させる利用者情報開示手段とを有し、利用者側装置は、事業者側装置に対して個人情報を送信する個人情報送信手段と、事業者側装置に対して登録された個人情報の閲覧を要求し、事業者側装置より受信した閲覧用の個人情報の各項目のハッシュ値と閲覧用の個人情報に含まれる利用者側装置が作成した利用者署名との整合性を検証した後、閲覧用の個人情報の各項目について、個人情報データベースより各項目の値を取得して閲覧用の個人情報を閲覧し、更新のある項目については、事業者側装置に更新した値を送信する利用者情報閲覧手段とを有するものである。

【００１５】
具体的には、利用者と個人情報を収集してサービス提供に利用する事業者において、以下を行う。

個人情報送受信時には、以下の処理が行われる。

【００１６】
利用者は、開示する個人情報の生成・編集を行い、開示する個人情報の各項目毎に乱数を生成して、乱数付き個人情報のハッシュ値を算出する。ハッシュ値を作成する際に、生成した乱数を反映させることにより、推測攻撃による個人情報漏洩を防止することができる。次に、利用者は、全ての項目のハッシュ値を統合したものに対してディジタル署名を作成し、各項目の個人情報、各項目の乱数、署名からなる送信用個人情報を作成する。また、利用者は、送信用個人情報をログとして自装置に記録するとともに、送信用個人情報を事業者へ送信する。

【００１７】

事業者は、受け取った送信用個人情報の中の利用者の署名を検証した後、送信用個人情報を自装置に記録する。

【００１８】

個人情報閲覧更新時には、以下の処理が行われる。

【００１９】

事業者は、利用者より自らの個人情報の閲覧請求を受け取ると、利用者の認証を行い本人確認する。次に、事業者は、その利用者より以前に受け取った送信用個人情報から、全項目について、各項目の乱数、利用者の署名を取得し、各項目の乱数付き個人情報のハッシュ値を算出する。次に、事業者は、各項目の乱数付き個人情報のハッシュ値を統合したものから事業者のディジタル署名を作成して、各項目の乱数、各項目の乱数付き個人情報のハッシュ値、利用者の署名、事業者の署名からなる閲覧用個人情報を作成し、利用者に送信する。

【００２０】

利用者は、受け取った閲覧用個人情報の中の利用者の署名と事業者の署名の検証を行い、さらに、自装置に記録されている送信用個人情報との整合性を検証する。また、利用者は、上記検証後、自装置に記録されている個人情報から各項目の個人情報を取得し、表示する。また、閲覧した個人情報の項目に変更がある場合、利用者は、変更項目の個人情報について乱数を生成して、乱数付き個人情報のハッシュ値を算出する。次に、利用者は、変更の無い項目を含む全ての項目のハッシュ値を統合したものに対してディジタル署名を作成し、変更項目の個人情報、変更項目の乱数、署名からなる更新用個人情報を作成し、事業者に送信する。

【発明の効果】

【００２１】

本発明によれば、個人情報を提供した利用者が、事業者側が改ざんすることなく自らが送信した通りの個人情報を管理していることを閲覧・確認できる。

【００２２】

また、本発明によれば、第三者に通信の内容が漏洩したとしても何の情報も与えず、個人情報を安全に保護するとともに、個人情報を提供した利用者は、提供される閲覧用個人情報から、本人の個人情報の内容の閲覧およびその原本性の確認を行うことができる。

【発明を実施するための最良の形態】

【００２３】

以下、本発明の実施の形態を図面に基づいて詳細に説明する。なお、実施の形態を説明するための全図において、同一の部材には原則として同一の符号を付し、その繰り返しの説明は省略する。

【００２４】

（実施の形態１）

＜個人情報閲覧更新システムの構成＞

図１により、本発明の実施の形態１に係る個人情報閲覧更新システムの構成について説明する。図１は本発明に実施の形態１に係る個人情報閲覧更新システムの概略を示す概略図、図２は本発明に実施の形態１に係る個人情報閲覧更新システムの事業者側装置の内部構成を示す構成図、図３は本発明に実施の形態１に係る個人情報閲覧更新システムの利用者側装置の内部構成を示す構成図である。

【００２５】

図１において、個人情報閲覧更新システムは、個人情報を収集してサービス提供に利用する事業者側装置１０１と、サービス利用のために自らの個人情報を提供する利用者側装置１０２～１０４から構成される。利用者側装置は、サービスを利用する利用者数分が存在する。事業者側装置１０１と利用者側装置１０２～１０４は、ネットワーク１０５を介して繋がっている。

【００２６】

事業者側装置１０１の内部構成は、図２に示すように、記憶装置２０２と、ネットワー

クを介して他の装置と通信を行うための通信装置２０４と、キーボードやマウスなどの入力装置２０５と、ディスプレイなどの表示装置２０６と、ＣＰＵ２０１と、これらを接続するインタフェース２０３とから構成される。

【００２７】

記憶装置２０２には、利用者に個人情報送付を要求し、利用者からの個人情報を受け取って格納する個人情報受信プログラム２０７と、利用者からの閲覧要求に応じて、格納している利用者情報を開示する利用者情報開示手段である利用者情報開示プログラム２０８と、個人情報の各項目に対して識別のために付与された識別ＩＤ（以下、項目ＩＤと呼ぶ）と個人情報の各項目との対応関係を記録した項目ＩＤファイル２０９と、個人情報の各項目について、誰にどのような場合に開示するかといった開示ポリシーを記録した事業者開示ポリシーファイル２１０と、各利用者から受け取った個人情報が登録されている利用者情報データベース２１１が格納されている。

【００２８】

以下の説明における各プログラム２０７、２０８の処理は、インタフェース２０３を介して呼び出された各プログラムをＣＰＵ２０１が実行することにより、事業者側装置１０１上で実現されるものである。各プログラム２０７、２０８は、予め記憶装置２０２に格納されていてもよいし、事業者側装置１０１が利用可能な媒体を介して導入されてもよい。媒体とは、例えば、事業者側装置１０１に着脱可能な記憶媒体や、通信装置２０４に接続するネットワークまたはネットワークを伝搬する搬送波といった通信媒体を含む。

【００２９】

利用者側装置１０２～１０４の内部構成は、図３に示すように、記憶装置３０２と、ネットワークを介して他の装置と通信を行うための通信装置３０４と、キーボードやマウスなどの入力装置３０５と、ディスプレイなどの表示装置３０６と、ＣＰＵ３０１と、これらを接続するインタフェース３０３とから構成される。

【００３０】

記憶装置３０２には、事業者からの個人情報送付要求を受け、自身の持つ個人情報を、署名を付与した後に要求元の事業者に送信する個人情報送信手段である個人情報送信プログラム３０７と、事業者に対して、事業者が格納している自身の利用者情報の閲覧更新を要求する利用者情報閲覧手段である利用者情報閲覧プログラム３０８と、個人情報の各項目に対して識別のために付与された項目ＩＤと個人情報の各項目との対応関係を記録した項目ＩＤファイル２０９と、個人情報の各項目について、誰にどのような場合に開示するかといった開示ポリシーを記録した個人開示ポリシーファイル３０９と、自身の個人情報が登録されている個人情報データベース３１０が格納されている。

【００３１】

以下の説明における各プログラム３０７、３０８の処理は、利用者側装置１０２～１０４上で実現されるものである。各プログラム３０７、３０８の実行および格納方法については、前述の事業者側装置１０１と同様である。

【００３２】

＜個人情報閲覧更新システムのデータフローの概要＞

次に、図４により、本発明の実施の形態１に係る個人情報閲覧更新システムのデータフローの概要について説明する。図４は本発明の実施の形態１に係る個人情報閲覧更新システムのデータフローの概要を説明するための説明図である。

【００３３】

図４に示すように、個人情報を利用したサービスを提供する事業者側装置１０１と、そのサービスを利用する利用者側装置１０２～１０４との間でやり取りされるデータフローの概要としては、まず、事業者側装置１０１は、利用者側装置１０２～１０４に対して、個人情報送信要求４０１を送信して、個人情報を要求する（個人情報要求処理）（Ｓ１０１）。

【００３４】

個人情報送信要求４０１を受け取った利用者側装置１０２～１０４は、開示する個人情

報の生成・編集を行い、送信用個人情報４０２を送信する（個人情報送信処理）（Ｓ１０２）。送信用個人情報４０２には、送信する個人情報に対して、開示制御用処理を施して作成された利用者の電子署名４０３が含まれる。

【００３５】

事業者側装置１０１は、利用者側装置１０２～１０４より、送信用個人情報４０２を受け取り、送信用個人情報４０２に含まれる個人情報および利用者署名４０３を、利用者情報データベース２１１に格納する（個人情報受信処理）。

【００３６】

利用者側装置１０２～１０４は、事業者側装置１０１に対して、個人情報閲覧要求４０４を送信して、登録されている自身の個人情報の閲覧を要求する（個人情報閲覧要求処理）（Ｓ１０３）。

【００３７】

個人情報閲覧要求４０４を受け取った事業者側装置１０１は、個人情報の各項目が秘匿された閲覧用個人情報４０５を送信する（閲覧用個人情報送信処理）（Ｓ１０４）。閲覧用個人情報４０５には、個人情報受信時に利用者情報データベース２１１に格納された利用者署名４０３と、利用者に送信する閲覧用個人情報に対して作成された事業者の電子署名４０６が含まれる。

【００３８】

利用者側装置１０２～１０４は、事業者側装置１０１より、閲覧用個人情報４０５を受け取り、閲覧用個人情報４０５に含まれる利用者署名４０３と事業者署名４０６を検証した後、閲覧用個人情報に対応する個人情報を自身の個人情報データベース３１０より呼び出し、表示する（個人情報閲覧処理）。

【００３９】

閲覧用個人情報４０５を受け取った利用者側装置１０２～１０４は、その閲覧用個人情報４０５の内容を更新する場合には、更新する個人情報の生成を行い、更新用個人情報４０７を送信する（個人情報更新処理）（Ｓ１０５）。

【００４０】

＜個人情報送信処理＞

次に、図５～図７により、本発明の実施の形態１に係る個人情報閲覧更新システムの個人情報送信処理について説明する。図５は本発明の実施の形態１に係る個人情報閲覧更新システムの個人情報送信処理の処理フローであり、ここでは、利用者側装置１０２が、利用者ＩＤ「１」を持つ場合の利用者側装置１０２での処理を示している。図６は本発明の実施の形態１に係る個人情報閲覧更新システムの項目ＩＤファイルを示す図、図７は本発明の実施の形態１に係る個人情報閲覧更新システムの送信用個人情報を示す図である。

【００４１】

利用者ＩＤは、利用者の識別のために、事業者により利用者毎に付与される識別ＩＤであり、郵送、あるいは、ネットワークなどの通信手段を用いて、利用者に渡される。利用者側装置１０２は、事業者側装置１０１から個人情報送信要求を受け取ると、個人情報送信プログラム３０７により、以下のＳ５０１～Ｓ５０５の個人情報送信処理を行う。

【００４２】

Ｓ５０１では、入力された項目ＩＤファイル２０９の各項目について、各項目毎に乱数（ｒ１～ｒ８）を生成する。項目ＩＤファイル２０９は、図６に示すように、個人情報の各項目に対して識別のために付与された項目ＩＤと個人情報の各項目との対応関係（レコード６０１～６０８）を記録したファイルである。例えば、レコード６０１は、項目名「郵便番号」は、項目ＩＤ「１」であることを表している。ただし、項目ＩＤファイル２０９に記載されている項目ＩＤと個人情報の各項目との対応関係は、事業者側装置１０１と利用者側装置１０２～１０４とで一致させておく必要がある。そのために、個人情報送信要求時、あるいは定期的に項目ＩＤファイル２０９を事業者側装置１０１から利用者側装置１０２～１０４に受け渡しても良いし、利用者側装置１０２～１０４から事業者側装置１０１に取得しに行っても良い。

【００４３】
Ｓ５０２では、入力された個人情報５０６の各項目について、各項目の値とＳ５０１で作成した各項目毎の乱数を足し合わせたものに対し、ハッシュ値を計算する。例えば、項目ＩＤ「１」の項目「郵便番号」については、値「１２３－４５６７」と乱数「ｒ１」を足し合わせたデータに対してハッシュ関数を適用して、ハッシュ値「３Ａ１Ｂ２８５３９Ｃ２１０ＤＤＥ・・・」を生成する。ハッシュ値「３Ａ１Ｂ２８５３９Ｃ２１０ＤＤＥ・・・」の作成に、乱数「ｒ１」を利用することによって、推測攻撃により、ハッシュ値「３Ａ１Ｂ２８５３９Ｃ２１０ＤＤＥ・・・」から元の値「１２３－４５６７」が漏洩するのを防止することができる。乱数を利用しない場合、例えば、「０００－００００」「０００－０００１」「０００－０００２」…と順に数字を当てはめてハッシュ値を生成することにより、ハッシュ値「３Ａ１Ｂ２８５３９Ｃ２１０ＤＤＥ・・・」にぴったり合う郵便番号を見つけることができてしまう。

【００４４】
上記、個人情報５０６は、登録フォームを表示して利用者に値を入力させて取得しても良いし、利用者により予め個人情報が登録されたデータベースや記憶媒体から取得しても良い。

【００４５】
Ｓ５０３では、Ｓ５０２で作成した各項目のハッシュ値を全て足し合わせたものに対して、利用者の秘密鍵を用いて、公開鍵暗号方式により、利用者の署名６１８（以後、利用者ＩＤ「１」の利用者署名を、利用者１署名と呼ぶ）を作成する。

【００４６】
Ｓ５０４では、利用者ＩＤ、Ｓ５０１で入力された項目ＩＤ、Ｓ５０１で作成した各項目の乱数、Ｓ５０２で入力された個人情報の各項目名とその値、Ｓ５０３で作成した利用者１署名からなる送信用個人情報４０２（図７の６０９～６１８）を作成し、送信用個人情報４０２を事業者側装置１０１に送信する。送信の際は、共通鍵暗号方式などによって、送信用個人情報４０２を暗号化して送信することが望ましい。

【００４７】
Ｓ５０５では、Ｓ５０４で作成した送信用個人情報４０２を、個人情報データベース３１０に登録する。

【００４８】
＜個人情報受信処理＞
次に、図８および図９により、本発明の実施の形態１に係る個人情報閲覧更新システムの個人情報受信処理について説明する。図８は本発明の実施の形態１に係る個人情報閲覧更新システムの個人情報受信処理の処理フロー、図９は本発明の実施の形態１に係る個人情報閲覧更新システムの利用者情報データベースの構成を示す図である。

【００４９】
事業者装置１０１は、利用者側装置１０２から送信用個人情報４０２を受け取ると、個人情報受信プログラム２０７により、以下のＳ７０１～Ｓ７０３の個人情報受信処理を行う。

【００５０】
Ｓ７０１では、利用者側装置１０２から受け取った送信用個人情報４０２（送信用個人情報が送信時に共通鍵暗号方式等によって暗号化されている場合は、復号して送信用個人情報４０２を得る）に含まれる個人情報の各項目（レコード６１０～６１７）について、「値」と「乱数」を足し合わせたものに対し、ハッシュ値を計算する。例えば、項目ＩＤ「１」の項目「郵便番号」については、値「１２３－４５６７」と乱数「ｒ１」を足し合わせたデータに対してハッシュ関数を適用して、ハッシュ値「３Ａ１Ｂ２８５３９Ｃ２１０ＤＤＥ・・・」を生成する。

【００５１】
Ｓ７０２では、利用者の公開鍵を用いて、公開鍵暗号方式により、送信用個人情報４０２に含まれる利用者１署名６１８と、Ｓ７０１で作成した各項目のハッシュ値を全て足し

合わせたものとの整合性を調べることによって、利用者１署名６１８を検証する。ここで使用する利用者の公開鍵は、個人情報送信時に、送信用個人情報４０２とともに、利用者側装置１０２から事業者側装置１０１に送られても良いし、予め事業者側装置１０１の利用者情報データベース２１１に利用者毎に登録しておいても良い。

【００５２】

Ｓ７０３では、Ｓ７０２で検証した送信用個人情報４０２について、各項目の項目ＩＤとその項目の値、その項目に対する乱数（８０２、８０３）、および利用者１署名６１８を利用者情報データベース２１１に登録する。

【００５３】

図９に示すように、利用者情報データベース２１１の構成としては、利用者毎に利用者情報が登録されている（レコード８０５、８０６）。各レコードには、項目ＩＤとその項目の値、その項目に対する乱数が項目毎に登録され（８０２、８０３）、その登録情報に対する利用者署名が登録されている（８０４）。ここで、レコード８０５の利用者署名８０４は、送信用個人情報４０２に含まれる利用者の署名６１８である。

【００５４】

なお、Ｓ７０２での利用者１署名６１８の検証の結果、利用者１の署名として検証できなかった場合は、利用者側装置１０２に対して、送信用個人情報４０２の再度問い合わせを行い、再度、Ｓ７０２での利用者１署名６１８の検証を行う。

【００５５】

＜閲覧用個人情報送信処理＞

次に、図１０および図１１により、本発明の実施の形態１に係る個人情報閲覧更新システムの閲覧用個人情報送信処理について説明する。図１０は本発明の実施の形態１に係る個人情報閲覧更新システムの閲覧用個人情報送信処理の処理フローであり、ここでは、利用者ＩＤ「１」を持つ利用者側装置１０２が、事業者側装置１０１に対して、個人情報閲覧要求を送信した場合の処理を示している。図１１は本発明の実施の形態１に係る個人情報閲覧更新システムの閲覧用個人情報を示す図である。

【００５６】

事業者側装置１０１は、利用者側装置１０２から個人情報閲覧要求４０４を受け取ると、利用者情報開示プログラム２０８により、以下のＳ９０１～Ｓ９０４の閲覧用個人情報送信処理を行う。

【００５７】

Ｓ９０１では、利用者ＩＤ「１」を入力として利用者情報データベース２１１を検索し、利用者ＩＤ「１」に該当するレコード８０５より、利用者ＩＤ「１」の個人情報を取得する。また、入力された項目ＩＤファイル２０９から、各項目ＩＤと項目名との関係を取得する（例えば、項目ＩＤ「１」＝項目名「郵便番号」）。

【００５８】

Ｓ９０２では、Ｓ９０１で取得したレコード８０５に含まれる個人情報の各項目（８０２、８０３など）について、「値」と「乱数」を足し合わせたものに対し、ハッシュ値を計算する。例えば、項目ＩＤ「１」の項目については、値「１２３－４５６７」と乱数「ｒ１」を足し合わせたデータに対してハッシュ関数を適用して、ハッシュ値「３Ａ１Ｂ２８５３９Ｃ２１０ＤＤＥ・・・」を生成する。

【００５９】

Ｓ９０３では、Ｓ９０２で作成した各項目のハッシュ値を全て足し合わせたものに対して、事業者の秘密鍵を用いて、公開鍵暗号方式により、事業者の署名１０１０（以後、利用者ＩＤ「１」向けの閲覧用個人情報に対する事業者署名を、事業者署名１と呼ぶ）を作成する。

【００６０】

Ｓ９０４では、Ｓ９０１で入力された利用者ＩＤ「１」と、各項目毎にＳ９０１で取得した項目ＩＤと項目名とＳ９０２で生成したハッシュ値（レコード１００２～１００９）と、Ｓ９０１で取得したレコード８０５に含まれる利用者１署名６１８と、Ｓ９０３で作

成した事業者署名１（１０１０）からなる図１１に示すような、閲覧用個人情報４０５を作成して、利用者側装置１０２に送信する。送信の際は、共通鍵暗号方式などによって、閲覧用個人情報４０５を暗号化して送信することが望ましい。

【００６１】

上記、閲覧用個人情報４０５には、各項目の値は記載されず、各項目のハッシュ値のみが記載されている。このため、利用者側装置１０２以外の端末によって閲覧用個人情報４０５が盗聴された場合であっても、各項目の値、すなわち利用者側装置１０２の個人情報の漏洩を防止できる。

【００６２】

＜個人情報閲覧処理＞

次に、図１２および図１３により、本発明の実施の形態１に係る個人情報閲覧更新システムの個人情報閲覧処理について説明する。図１２は本発明の実施の形態１に係る個人情報閲覧更新システムの個人情報閲覧処理の処理フローであり、ここでは、利用者ＩＤ「１」を持つ利用者側装置１０２が、事業者側装置１０１から、閲覧用個人情報４０５を受信した場合の処理を示している。図１３は本発明の実施の形態１に係る個人情報閲覧更新システム個人情報閲覧画面を示す図である。

【００６３】

利用者側装置１０２は、事業者側装置１０１から閲覧用個人情報４０５を受け取ると、利用者情報閲覧プログラム３０８により、以下のＳ１１０１～Ｓ１１０３の個人情報閲覧処理を行う。

【００６４】

Ｓ１１０１では、事業者の公開鍵を用いて、公開鍵暗号方式により、事業者側装置１０１より受け取った閲覧用個人情報４０５に含まれる事業者署名１（１０１０）と、閲覧用個人情報４０５に含まれる各項目のハッシュ値を全て足し合わせたものとの整合性を調べることによって、事業者署名１（１０１０）を検証する。ここで使用する事業者の公開鍵は、閲覧用個人情報送信時に、閲覧用個人情報４０５とともに、事業者側装置１０１から利用者側装置１０２に送られても良いし、予め利用者側装置１０２中に格納しておいても良い。この事業者署名１（１０１０）により、利用者は、受け取った閲覧用個人情報４０５が、正当な事業者から送られてきたものであることを検証することができる。

【００６５】

Ｓ１１０２では、利用者の公開鍵を用いて、公開鍵暗号方式により、閲覧用個人情報４０５に含まれる利用者１署名６１８と、閲覧用個人情報４０５に含まれる各項目のハッシュ値を全て足し合わせたものとの整合性を調べることによって、利用者１署名６１８を検証する。これにより、利用者は、以前に自分が送信した個人情報が改ざんされていないことを検証することができる。

【００６６】

Ｓ１１０３では、閲覧用個人情報４０５の各項目について、個人情報データベース３１０に記録された送信用個人情報４０２より各項目の値を取得し、例えば、図１３に示すような個人情報閲覧画面１１０４に、利用者ＩＤ、項目ＩＤ、項目名、項目の値を表示する。閲覧用個人情報４０５には、各項目のハッシュ値しか記載されていないが、個人情報データベース３１０に記録された情報を利用することによって、利用者に対しては、各項目の値を表示することができる。

【００６７】

なお、Ｓ１１０１での事業者署名１（１０１０）の検証の結果、事業者署名１として検証できなかった場合は、事業者側装置１０１に対して、閲覧用個人情報４０５の再度問い合わせを行い、再度、Ｓ１１０１での事業者署名１（１０１０）の検証を行う。また、Ｓ１１０２での利用者１署名６１８の検証の結果、利用者１の署名として検証できなかった場合は、事業者側装置１０１に対して、閲覧用個人情報４０５の再度問い合わせを行い、再度、Ｓ１１０２での利用者１署名６１８の検証を行う。

【００６８】

また、Ｓ１１０２での利用者１署名６１８の検証の結果、以前に自分が送信した個人情報が改ざんされていることが検証された場合は、Ｓ１１０３でのデータ表示の際に、閲覧用個人情報４０５の各項目のハッシュ値と個人情報データベース３１０に記録された情報によるハッシュ値から、改ざんされている項目を特定し、そのデータを個人情報閲覧画面１１０４に表示することが可能である。

【００６９】

＜個人情報更新処理＞

次に、図１４～図１６により、本発明の実施の形態１に係る個人情報閲覧更新システムの個人情報更新処理について説明する。図１４は本発明の実施の形態１に係る個人情報閲覧更新システムの個人情報更新処理の処理フローであり、ここでは、利用者ＩＤ「１」を持つ利用者側装置１０２が、事業者側装置１０１から、閲覧用個人情報４０５を受信した時に、その内容を更新する場合の処理を示している。図１５は本発明の実施の形態１に係る個人情報閲覧更新システムの更新用個人情報を示す図、図１６は本発明の実施の形態１に係る個人情報閲覧更新システムの更新済個人情報を示す図である。

【００７０】

利用者側装置１０２は、事業者側装置１０１から閲覧用個人情報４０５を受け取り、前述のＳ１１０１～Ｓ１１０３により個人情報を閲覧し、その内容に対して更新がある時は、利用者情報閲覧プログラム３０８により、以下のＳ１２０１～Ｓ１２０５の個人情報更新処理を行う。

【００７１】

Ｓ１２０１では、利用者は、個人情報閲覧画面１１０４において、変更がある項目に対して、更新情報の入力を行い、その項目の値を変更する。ここでは、個人情報閲覧画面１１０４のレコード１１１１の項目の値「Ａ@ＸＸＸ．ｃｏ．ｊｐ」が「Ａ更新@ＸＸＸ．ｃｏ．ｊｐ」に更新された場合について説明する。

【００７２】

次に、レコード１１０６～１１１３の各項目について、各項目毎に乱数（ｒ１１～ｒ１８）を生成する。なお、この乱数については、必ずしも生成する必要は無く、個人情報データベース３１０に登録された送信用個人情報４０２の乱数（ｒ１～ｒ８）を再度利用しても良いし、更新する項目のみ乱数を新たに生成し、更新しない項目については、個人情報データベース３１０に登録された送信用個人情報４０２の乱数を再利用しても良い。実施の形態では、同じ乱数を長期間利用することによる安全性の低下を防ぐため、個人情報更新のたびに全項目の乱数を再生成することとしている。

【００７３】

Ｓ１２０２では、更新済みの個人情報閲覧画面１１０４の各項目について、各項目の値とＳ１２０１で作成した各項目毎の乱数を足し合わせたものに対し、ハッシュ値を計算する。例えば、項目ＩＤ「１」の項目「郵便番号」については、値「１２３－４５６７」と乱数「ｒ１１」を足し合わせたデータに対してハッシュ関数を適用して、ハッシュ値「３Ａ１Ｂ２８５３９Ｃ２１０ＤＤＥ・・・」を生成する。変更済みの項目ＩＤ「６」の項目「Ｅメール」については、値「Ａ更新@ＸＸＸ．ｃｏ．ｊｐ」と乱数「ｒ１６」を足し合わせたデータに対してハッシュ関数を適用して、ハッシュ値「３９０３ＡＣＣ７８３０Ｄ２２９１・・・」を生成する。

【００７４】

Ｓ１２０３では、Ｓ１２０２で作成した各項目のハッシュ値を全て足し合わせたものに対して、利用者の秘密鍵を用いて、公開鍵暗号方式により、利用者１署名２（１３１０）を作成する。

【００７５】

Ｓ１２０４では、利用者ＩＤ、更新済みの個人情報閲覧画面１１０４の各項目の項目ＩＤと項目名、Ｓ１２０１で作成した各項目の乱数、Ｓ１２０１で更新された項目についてのみその項目の値（図１５のレコード１３０７参照）、Ｓ１２０３で作成した利用者１署名２（１３１０）からなる更新用個人情報４０７（内容については、図１５のレコード１

３０１～１３１０を参照）を作成し、更新用個人情報４０７を事業者側装置１０１に送信する。送信の際は、共通鍵暗号方式などによって、更新用個人情報４０７を暗号化して送信することが望ましい。

【００７６】

Ｓ１２０５では、各項目の乱数および、項目ＩＤ「６」の項目「Ｅメール」が値「Ａ更新@ＸＸＸ．ｃｏ．ｊｐ」に更新された更新済個人情報１２０６（図１６のレコード１３０７、１３１０～１３１８参照）を個人情報データベース３１０に登録する。

【００７７】

上記、更新用個人情報送信について、事業者側装置１０１に対して送信するのは、更新した項目の値と各項目の乱数のみであり、変更の無い個人情報については、送信しない。更新用個人情報４０７を受け取った事業所側装置１０１は、既に利用者情報データベース２１１に登録してある個人情報と、更新用個人情報４０７に含まれる更新された項目の値と再生成された各項目の乱数から、各項目のハッシュ値を計算し、利用者の公開鍵を用いて、利用者１署名２（１３１０）を検証することができる。検証した後、事業者側装置１０１は、利用者情報データベース２１１の利用者ＩＤ「１」のレコード８０５に対して、更新用個人情報４０７に含まれる更新された項目の値と再生成された各項目の乱数、および利用者１署名２を上書きして登録する。

【００７８】

（実施の形態２）

実施の形態２は、実施の形態１において、事業者側装置１０１を所有する例えば放送事業者などの事業者が、事業者が所有する他の装置などとの間で、利用者情報の閲覧処理を行うものである。

【００７９】

＜個人情報閲覧更新システムの構成＞

図１７により、本発明の実施の形態２に係る個人情報閲覧更新システムの構成について説明する。図１７は本発明に実施の形態２に係る個人情報閲覧更新システムの概略を示す概略図である。

【００８０】

図１７において、個人情報閲覧更新システムは、個人情報を収集して放送サービスの提供に利用する放送事業者１４０４と、サービス利用のために自らの個人情報を提供する利用者側装置１０２～１０４から構成される。放送事業者１４０４は、視聴率を集計し、より良い番組作りのための指標を生成する視聴率集計部門装置１４０１と、利用者を登録・管理する利用者管理部門装置１４０２と、視聴料の徴収等を行う課金部門装置１４０３を持つ。利用者側装置は、サービスを利用する利用者数分が存在する。視聴率集計部門装置１４０１と利用者管理部門装置１４０２と課金部門装置１４０３と利用者側装置１０２～１０４は、ネットワーク１０５を介して繋がっている。

【００８１】

利用者管理部門装置１４０２の内部構成は、前述の実施の形態１における事業者側装置１０１の内部構成と同じである。また、利用者側装置１０２～１０４の内部構成は、前述の実施の形態１における利用者側装置１０２～１０４の内部構成と同じである。

【００８２】

＜個人情報閲覧更新システムのデータフローの概要＞

次に、図１８により、本発明の実施の形態２に係る個人情報閲覧更新システムのデータフローの概要について説明する。図１８は本発明の実施の形態２に係る個人情報閲覧更新システムのデータフローの概要を説明するための説明図である。

【００８３】

図１８に示すように、個人情報を利用した放送サービスを提供する放送事業者１４０４と、そのサービスを利用する利用者側装置１０２～１０４との間でやり取りされるデータフローの概要としては、まず、利用者管理部門装置１４０２は、利用者側装置１０２～１０４に対して、個人情報送信要求１５０１を送信して、個人情報を要求する（個人情報要

求処理）（Ｓ２０１）。

【００８４】

個人情報送信要求１５０１を受け取った利用者側装置１０２～１０４は、開示する個人情報の生成・編集を行い、送信用個人情報１５０２を送信する（個人情報送信処理）（Ｓ２０２）。送信用個人情報１５０２には、送信する個人情報に対して、開示制御用処理を施して作成された利用者の電子署名が含まれる。利用者管理部門装置１４０２は、利用者側装置１０２～１０４より、送信用個人情報１５０２を受け取り、送信用個人情報１５０２に含まれる個人情報および利用者署名を、利用者情報データベース２１１に格納する（個人情報受信処理）。

【００８５】

利用者側装置１０２～１０４は、利用者管理部門装置１４０２に対して、個人情報閲覧要求１５０３を送信して、登録されている自身の個人情報の閲覧を要求する（個人情報閲覧要求処理）（Ｓ２０３）。個人情報閲覧要求１５０３を受け取った利用者管理部門装置１４０２は、個人情報の各項目が秘匿された閲覧用個人情報１５０４を送信する（閲覧用個人情報送信処理）（Ｓ２０４）。閲覧用個人情報１５０４には、個人情報受信時に利用者情報データベース２１１に格納された利用者署名と、利用者に送信する閲覧用個人情報に対して作成された利用者管理部門の電子署名が含まれる。

【００８６】

利用者側装置１０２～１０４は、利用者管理部門装置１４０２より、閲覧用個人情報１５０４を受け取り、閲覧用個人情報１５０４に含まれる利用者署名と利用者管理部門署名を検証した後、閲覧用個人情報に対応する個人情報を自身の個人情報データベース３１０より呼び出し、表示する（個人情報閲覧処理）。

【００８７】

視聴率集計部門装置１４０１は、利用者管理部門装置１４０２に対して、集計情報閲覧要求１５０６を送信して、利用者管理部門装置１４０２の利用者情報データベース２１１に登録されている個人情報の閲覧を要求する（集計情報閲覧要求処理）（Ｓ２０５）。集計情報閲覧要求１５０６を受け取った利用者管理部門装置１４０２は、個人情報の項目のうち、視聴率集計部門に必要な項目のみ開示し、その他の項目は秘匿した集計用個人情報１５０７を送信する（集計用個人情報送信処理）（Ｓ２０６）。

【００８８】

集計用個人情報１５０７には、利用者からの個人情報受信時に利用者情報データベース２１１に格納された利用者署名と、視聴率集計部門に送信する集計用個人情報に対して作成された利用者管理部門の電子署名が含まれる。視聴率集計部門装置１４０１は、利用者管理部門装置１４０２より、集計用個人情報１５０７を受け取り、集計用個人情報１５０７に含まれる利用者署名と利用者管理部門署名を検証した後、集計用個人情報を表示する（集計情報閲覧処理）。

【００８９】

課金部門装置１４０３は、利用者管理部門装置１４０２に対して、課金情報閲覧要求１５０８を送信して、利用者管理部門装置１４０２の利用者情報データベース２１１に登録されている個人情報の閲覧を要求する（課金情報閲覧要求処理）（Ｓ２０７）。課金情報閲覧要求１５０８を受け取った利用者管理部門装置１４０２は、個人情報の項目のうち、課金部門に必要な項目のみ開示し、その他の項目は秘匿した課金用個人情報１５０９を送信する（課金用個人情報送信処理）（Ｓ２０８）。

【００９０】

課金用個人情報１５０９には、利用者からの個人情報受信時に利用者情報データベース２１１に格納された利用者署名と、課金部門に送信する課金用個人情報に対して作成された利用者管理部門の電子署名が含まれる。課金部門装置１４０３は、利用者管理部門装置１４０２より、課金用個人情報１５０９受け取り、課金用個人情報１５０９に含まれる利用者署名と利用者管理部門署名を検証した後、課金用個人情報を表示する（課金情報閲覧処理）。

【００９１】
＜個人情報登録処理＞
次に、図１９～図２１により、本発明の実施の形態２に係る個人情報閲覧更新システムの個人情報登録処理について説明する。図１９は本発明の実施の形態２に係る個人情報閲覧更新システムの個人情報登録処理の処理フローであり、ここでは、利用者側装置１０２が、利用者ＩＤ「１」を持つ場合の利用者側装置１０２での処理を示している。図２０は本発明の実施の形態２に係る個人情報閲覧更新システムの項目ＩＤファイルを示す図、図２１は本発明の実施の形態２に係る個人情報閲覧更新システムの個人情報データを示す図である。
【００９２】
本実施の形態において、利用者ＩＤは、利用者の識別のために、事業者により利用者毎に付与される識別ＩＤであり、郵送、あるいは、ネットワークなどの通信手段を用いて、利用者に渡される。利用者側装置１０２は、まず個人情報送信プログラム３０７により、以下のＳ１６０１～Ｓ１６０３の個人情報登録処理を行う。
【００９３】
Ｓ１６０１では、項目ＩＤファイル１６０４を入力として、個人情報登録フォームを表示する。項目ＩＤファイル１６０４は、図２０に示すように、個人情報の各項目に対して識別のために付与された項目ＩＤと個人情報の各項目との対応関係（レコード１７０１～１７１０）を記録したファイルである。例えば、レコード１７０１は、項目名「郵便番号」が、項目ＩＤ「１」であることを表している。ただし、項目ＩＤファイル１６０４に記載されている項目ＩＤと個人情報の各項目との対応関係は、放送事業者１４０４と利用者側装置１０２～１０４とで一致させておく必要がある。
【００９４】
そのために、個人情報送信要求時、あるいは定期的に項目ＩＤファイル２０９を放送事業者１４０４から利用者側装置１０２～１０４に受け渡しても良いし、利用者側装置１０２～１０４から放送事業者１４０４に取得しに行っても良い。個人情報登録フォームは、利用者が自身の個人情報を入力するためのフォームであり、利用者は、氏名、住所といった個人情報を入力する。
【００９５】
また、登録した個人情報を放送事業者に開示するか否か（以後、個人開示ポリシーと呼ぶ）についても各項目毎に入力する。個人情報は、個人情報登録フォームにより入力しても良いし、予め個人情報が登録してある記憶媒体から入力しても良い。
【００９６】
Ｓ１６０２では、Ｓ１６０１で入力された個人開示ポリシーより、個人開示ポリシーファイル３０９を作成して、利用者側装置１０２に格納する。個人開示ポリシーファイル３０９には、例えば、「非開示　７：職業」といった「項目ＩＤ：７の職業は開示しない」という内容が記載されている。「項目ＩＤ：７の職業は、課金部門には開示しない」といったように、開示先別に個人開示ポリシーを設定しても良い。
【００９７】
Ｓ１６０３では、Ｓ１６０１で入力された個人情報（例えば図２１に示す個人情報データ１６０５）を個人情報データベース３１０に登録する。図２１に示すように、個人情報データ１６０５は、Ｓ１６０１で入力された個人情報が項目毎に登録されている（レコード１７１２～レコード１７２１）。ここで、レコード１７２１の視聴履歴は、利用者が入力しても良いし、放送視聴の際に視聴装置により自動で格納された視聴履歴を利用しても良い。
【００９８】
＜個人情報送信処理＞
次に、図２２および図２３により、本発明の実施の形態２に係る個人情報閲覧更新システムの個人情報送信処理について説明する。図２２は本発明の実施の形態２に係る個人情報閲覧更新システムの個人情報送信処理の処理フロー、図２３は本発明の実施の形態２に

係る個人情報閲覧更新システムの送信用個人情報を示す図である。

【００９９】

利用者側装置１０２は、利用者管理部門装置１４０２から個人情報送信要求を受け取ると、個人情報送信プログラム３０７により、以下のＳ１８０１～Ｓ１８０５の個人情報送信処理を行う。

【０１００】

Ｓ１８０１では、入力された項目ＩＤファイル１６０４の各項目について、各項目毎に乱数（ｒ１～ｒ１０）を生成する。

【０１０１】

Ｓ１８０２では、個人情報データベース３１０に登録された個人情報データ１６０５の各項目について、各項目の値とＳ１８０１で作成した各項目毎の乱数を足し合わせたものに対し、ハッシュ値を計算する。例えば、項目ＩＤ「１」の項目「郵便番号」については、値「１２３－４５６７」と乱数「ｒ１」を足し合わせたデータに対してハッシュ関数を適用して、ハッシュ値「３Ａ１Ｂ２８５３９Ｃ２１０ＤＤＥ・・・」を生成する。

【０１０２】

Ｓ１８０３では、Ｓ１８０２で作成した各項目のハッシュ値を全て足し合わせたものに対して、利用者の秘密鍵を用いて、公開鍵暗号方式により、利用者１署名１９１１（利用者ＩＤ「１」の利用者署名）を作成する。

【０１０３】

Ｓ１８０４では、利用者ＩＤ、Ｓ１８０１で入力された項目ＩＤ、Ｓ１８０１で作成した各項目の乱数、Ｓ１８０２で入力された個人情報の各項目名とその値、Ｓ１８０３で作成した利用者１署名１９１１からなる送信用個人情報１５０２（内部構成は、図２３の１９０１～１９１２を参照）を作成し、送信用個人情報１５０２を利用者管理部門装置１４０２に送信する。送信の際は、共通鍵暗号方式などによって、送信用個人情報１５０２を暗号化して送信することが望ましい。

【０１０４】

ここで、送信用個人情報に、個人開示ポリシーファイル３０９のコピーを添付して、利用者管理部門装置１４０２に送っても良い。個人開示ポリシーファイル３０９に、例えば「項目ＩＤ：７の職業は、課金部門には開示しない」という内容が記載されている場合、この個人開示ポリシーファイルを受け取った利用者管理部門装置１４０２は、この個人開示ポリシーファイルに基づき、課金部門に対して項目ＩＤ「７」の情報を秘匿して（ハッシュ値のみ開示して）個人情報を開示することができる。すなわち、放送事業者内においても、利用者の意思に基づいた開示制御を行うことができる。

【０１０５】

Ｓ１８０５では、Ｓ１８０４で作成した送信用個人情報１５０２に含まれる利用者ＩＤ、Ｓ１８０１で入力された項目ＩＤ、Ｓ１８０１で作成した各項目の乱数、Ｓ１８０２で入力された個人情報の各項目名とその値、Ｓ１８０３で作成した利用者１署名１９１１を、個人情報データ１６０５に上書きし、個人情報データベース３１０に登録する。

【０１０６】

＜個人情報受信処理＞

次に、図２４および図２５により、本発明の実施の形態２に係る個人情報閲覧更新システムの個人情報受信処理について説明する。図２４は本発明の実施の形態２に係る個人情報閲覧更新システムの個人情報受信処理の処理フロー、図２５は本発明の実施の形態２に係る個人情報閲覧更新システムの利用者情報データベースの構成を示す図である。

【０１０７】

利用者管理部門装置１４０２は、利用者側装置１０２から送信用個人情報１５０２を受け取ると、個人情報受信プログラム２０７により、以下のＳ２００１～Ｓ２００３の個人情報受信処理を行う。

【０１０８】

Ｓ２００１では、利用者側装置１０２から受け取った送信用個人情報１５０２（送信用

個人情報が送信時に共通鍵暗号方式等によって暗号化されている場合は、復号して送信用個人情報１５０２を得る）に含まれる個人情報の各項目（図２３のレコード１９０１～１９１０）について、「値」と「乱数」を足し合わせたものに対し、ハッシュ値を計算する。例えば、項目ＩＤ「１」の項目「郵便番号」については、値「１２３－４５６７」と乱数「ｒ１」を足し合わせたデータに対してハッシュ関数を適用して、ハッシュ値「３Ａ１Ｂ２８５３９Ｃ２１０ＤＤＥ・・・」を生成する。

【０１０９】

Ｓ２００２では、利用者の公開鍵を用いて、公開鍵暗号方式により、送信用個人情報１５０２に含まれる利用者１署名１９１１と、Ｓ２００１で作成した各項目のハッシュ値を全て足し合わせたものとの整合性を調べることによって、利用者１署名１９１１を検証する。ここで使用する利用者の公開鍵は、個人情報送信時に、送信用個人情報１５０２とともに、利用者側装置１０２から利用者管理部門装置１４０２に送られても良いし、予め利用者管理部門装置１４０２の利用者情報データベース２１１に利用者毎に登録しておいても良い。

【０１１０】

Ｓ２００３では、Ｓ２００２で検証した送信用個人情報１５０２について、各項目の項目ＩＤとその項目の値、その項目に対する乱数（図２５の１９１４、１９１５）、および利用者１署名１９１１を利用者情報データベース２１１に登録する。

【０１１１】

図２５に示すように、利用者情報データベース２１１の構成としては、利用者毎に利用者情報が登録されている（図２５のレコード１９１８、１９１９）。各レコードには、項目ＩＤとその項目の値、その項目に対する乱数が項目毎に登録され（図２５の１９１４、１９１５）、その登録情報に対する利用者署名が登録されている（図２５の１９１７）。ここで、レコード１９１８の利用者署名１９１７は、送信用個人情報１５０２に含まれる利用者の署名１９１１である。

【０１１２】

＜閲覧用個人情報送信処理＞

次に、図２６および図２７により、本発明の実施の形態２に係る個人情報閲覧更新システムの閲覧用個人情報送信処理について説明する。図２６は本発明の実施の形態２に係る個人情報閲覧更新システムの閲覧用個人情報送信処理の処理フローであり、ここでは、視聴率集計部門装置１４０１が、利用者管理部門装置１４０２に対して、利用者ＩＤ「１」の個人情報について、集計情報閲覧要求１５０６を送信した場合の処理を示している。図２７は本発明の実施の形態２に係る個人情報閲覧更新システムの開示用個人情報を示す図である。

【０１１３】

利用者管理部門装置１４０２は、定期的に、あるいは、他の装置から閲覧要求を受け取ると、利用者情報開示プログラム２０８により、以下のＳ２１０１～Ｓ２１０５の処理を行う。

【０１１４】

Ｓ２１０１では、利用者側装置１０２～１０４より個人情報閲覧要求１５０３（実施の形態１の個人情報閲覧要求４０４に相当）、あるいは、視聴率集計部門装置１４０１より集計情報閲覧要求１５０６、課金部門装置１４０３より課金情報閲覧要求１５０８を受信する。利用者管理部門装置１４０２が、定期的に閲覧用個人情報送信処理を行う場合は、Ｓ２１０１の処理は省略される。

【０１１５】

利用者側装置１０２～１０４より個人情報閲覧要求１５０３（実施の形態１の個人情報閲覧要求４０４に相当）を受信した場合の処理は、前述の実施の形態１の図１０のＳ９０１～Ｓ９０４の処理を行う。

【０１１６】

視聴率集計部門装置１４０１より集計情報閲覧要求１５０６、あるいは、課金部門装置

１４０３より課金情報閲覧要求１５０８を受信した場合は、以下のＳ２１０２～Ｓ２１０５の処理を行う。

【０１１７】

Ｓ２１０２では、利用者ＩＤ「１」を入力として利用者情報データベース２１１を検索し、利用者ＩＤ「１」に該当するレコード８０５より、利用者ＩＤ「１」の個人情報を取得する。個人情報検索のための利用者ＩＤ「１」は、集計情報閲覧要求１５０６に含まれる。

【０１１８】

Ｓ２１０３では、Ｓ２１０２で取得したレコード１９１８に含まれる個人情報の各項目（図２５に示す１９１４、１９１５など）について、「値」と「乱数」を足し合わせたものに対し、ハッシュ値を計算する。例えば、項目ＩＤ「１」の項目については、値「１２３－４５６７」と乱数「ｒ１」を足し合わせたデータに対してハッシュ関数を適用して、ハッシュ値「３Ａ１Ｂ２８５３９Ｃ２１０ＤＤＥ・・・」を生成する。

【０１１９】

Ｓ２１０４では、事業者開示ポリシーファイル２１０を入力として、まず視聴率集計部門装置１４０１にどの項目を開示するのか調べる。ここでは、視聴率集計部門装置１４０１に開示する項目を集計部門開示項目、開示しない項目を集計部門非開示項目と呼ぶこととする。

【０１２０】

図２６に示す事業者開示ポリシーファイル２１０によると、項目名「居住地域」と「視聴履歴」のみが集計部門開示項目であり、その他の項目は、集計部門非開示項目である。そこで、Ｓ２１０３で生成したハッシュ値を基に、図２７に示すような内部構造を持つ開示用個人情報２１０６を作成する。

【０１２１】

閲覧対象個人情報の持ち主の利用者について、Ｓ１８０４において送信用個人情報に個人開示ポリシーファイル３０９が添付されていた場合、事業者開示ポリシーファイル２１０の他に、閲覧対象個人情報の持ち主の利用者の個人開示ポリシーファイル３０９も合わせて考慮して、視聴率集計部門装置１４０１にどの項目を開示するのか決定する。

【０１２２】

集計部門開示項目については、開示値としてその項目の値、およびハッシュ値作成に用いた乱数を記載する（図２７のレコード２２０９、２２１０）。集計部門非開示項目については、Ｓ２１０３で生成したハッシュ値を記載する（図２７のレコード２２０１～２２０８）。

【０１２３】

利用者１署名１９１１は、個人情報送信時に利用者によって作成された署名であり、利用者情報データベース２１１の１９１７から取得される。利用者１署名１９１１は、利用者情報データベース２１１に登録された個人情報（図２５のレコード１９１８）が、利用者によって登録されたものであることを証明する。以上作成した全項目（図２７のレコード２２０１～２２１０を全て足し合わせたもの）に対して、利用者管理部門の秘密鍵を用いて、公開鍵暗号方式により、利用者管理部門の署名２２１１（以後、利用者ＩＤ「１」の集計用個人情報に対する利用者管理部門署名を、管理部門署名１と呼ぶ）を作成する。

【０１２４】

作成した管理部門署名１は、正当に開示したことを証明するために、利用者情報データベース２１１の項目１９１６にログとして記録しても良い。

【０１２５】

Ｓ２１０５では、Ｓ２１０４で作成した開示用個人情報２１０６を、視聴率集計部門装置１４０１に送信する。送信の際は、共通鍵暗号方式などによって、開示用個人情報２１０６を暗号化して送信することが望ましい。

【０１２６】

上記、開示用個人情報２１０６には、集計部門非開示項目については、その値は記載さ

れず、ハッシュ値のみが記載されている。このため、視聴率集計部門には、視聴率の集計などその部門が必要とする個人情報以外の情報は渡されず、視聴率集計部門による情報漏洩など放送事業者内部による個人情報の漏洩の被害を抑えることができる。

【０１２７】

視聴率集計部門装置１４０１では、図２７に示す開示用個人情報２１０６に含まれるレコード２２０９、２２１０の項目の値から視聴率集計に必要な情報のみ取得する。レコード２２０９、２２１０については、ハッシュ値作成に利用した乱数が記載されているので、その乱数を用いて、ハッシュ関数により、レコード２２０９、２２１０の項目のハッシュ値を生成することができる。

【０１２８】

その他の項目（図２７のレコード２２０１～２２０８）については、ハッシュ値が記載されているので、全項目のハッシュ値を取得することができ、利用者１署名１９１１を検証することによって、集計部門非開示項目は秘匿されたまま開示用個人情報２１０６が利用者の登録した正当な個人情報であることを確認できる。

【０１２９】

以上、本発明者によってなされた発明を実施の形態に基づき具体的に説明したが、本発明は前記実施の形態に限定されるものではなく、その要旨を逸脱しない範囲で種々変更可能であることはいうまでもない。

【図面の簡単な説明】

【０１３０】

【図１】本発明に実施の形態１に係る個人情報閲覧更新システムの概略を示す概略図である。

【図２】本発明に実施の形態１に係る個人情報閲覧更新システムの事業者側装置の内部構成を示す構成図である。

【図３】本発明に実施の形態１に係る個人情報閲覧更新システムの利用者側装置の内部構成を示す構成図である。

【図４】本発明の実施の形態１に係る個人情報閲覧更新システムのデータフローの概要を説明するための説明図である。

【図５】本発明の実施の形態１に係る個人情報閲覧更新システムの個人情報送信処理の処理フローである。

【図６】本発明の実施の形態１に係る個人情報閲覧更新システムの項目ＩＤファイルを示す図である。

【図７】本発明の実施の形態１に係る個人情報閲覧更新システムの送信用個人情報を示す図である。

【図８】本発明の実施の形態１に係る個人情報閲覧更新システムの個人情報受信処理の処理フローである。

【図９】本発明の実施の形態１に係る個人情報閲覧更新システムの利用者情報データベースの構成を示す図である。

【図１０】本発明の実施の形態１に係る個人情報閲覧更新システムの閲覧用個人情報送信処理の処理フローである。

【図１１】本発明の実施の形態１に係る個人情報閲覧更新システムの閲覧用個人情報を示す図である。

【図１２】本発明の実施の形態１に係る個人情報閲覧更新システムの個人情報閲覧処理の処理フローである。

【図１３】本発明の実施の形態１に係る個人情報閲覧更新システム個人情報閲覧画面を示す図である。

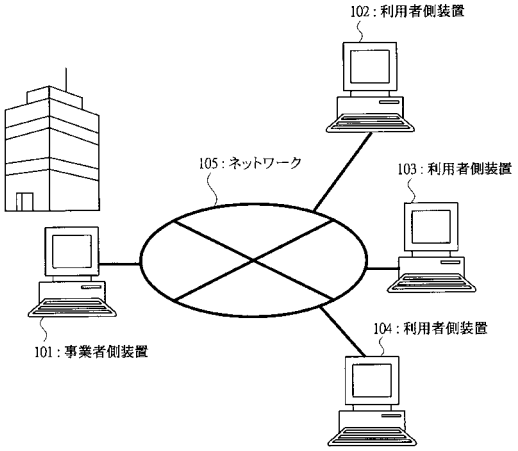
【図１４】本発明の実施の形態１に係る個人情報閲覧更新システムの個人情報更新処理の処理フローである。

【図１５】本発明の実施の形態１に係る個人情報閲覧更新システムの更新用個人情報を示す図である。

【図１６】本発明の実施の形態１に係る個人情報閲覧更新システムの更新済個人情報を示す図である。
【図１７】本発明に実施の形態２に係る個人情報閲覧更新システムの概略を示す概略図である。
【図１８】本発明の実施の形態２に係る個人情報閲覧更新システムのデータフローの概要を説明するための説明図である。
【図１９】本発明の実施の形態２に係る個人情報閲覧更新システムの個人情報登録処理の処理フローである。
【図２０】本発明の実施の形態２に係る個人情報閲覧更新システムの項目ＩＤファイルを示す図である。
【図２１】本発明の実施の形態２に係る個人情報閲覧更新システムの個人情報データを示す図である。
【図２２】本発明の実施の形態２に係る個人情報閲覧更新システムの個人情報送信処理の処理フローである。
【図２３】本発明の実施の形態２に係る個人情報閲覧更新システムの送信用個人情報を示す図である。
【図２４】本発明の実施の形態２に係る個人情報閲覧更新システムの個人情報受信処理の処理フローである。
【図２５】本発明の実施の形態２に係る個人情報閲覧更新システムの利用者情報データベースの構成を示す図である。
【図２６】本発明の実施の形態２に係る個人情報閲覧更新システムの閲覧用個人情報送信処理の処理フローである。
【図２７】本発明の実施の形態２に係る個人情報閲覧更新システムの開示用個人情報を示す図である。
【符号の説明】
【０１３１】
１０１…事業者側装置、１０２～１０４…利用者側装置、１０５…ネットワーク、２０１…ＣＰＵ、２０２…記憶装置、２０３…インタフェース、２０４…通信装置、２０５…入力装置、２０６…表示装置、２０７…個人情報受信プログラム、２０８…利用者情報開示プログラム、２０９…項目ＩＤファイル、２１０…事業者開示ポリシーファイル、２１１…利用者情報データベース、３０１…ＣＰＵ、３０２…記憶装置、３０３…インタフェース、３０４…通信装置、３０５…入力装置、３０６…表示装置、３０７…個人情報送信プログラム、３０８…利用者情報閲覧プログラム、３０９…個人開示ポリシーファイル、３１０…個人情報データベース、４０１…個人情報送信要求、４０２…送信用個人情報、４０３…利用者署名、４０４…個人情報閲覧要求、４０５…閲覧用個人情報、４０６…事業者署名、４０７…更新用個人情報、５０６…個人情報、６１８…利用者１署名、１０１０…事業者署名１、１１０４…個人情報閲覧画面、１２０６…更新済個人情報、１３１０…利用者１署名２、１４０１…視聴率集計部門装置、１４０２…利用者管理部門装置、１４０３…課金部門装置、１４０４…放送事業者、１５０１…個人情報送信要求、１５０２…送信用個人情報、１５０３…個人情報閲覧要求、１５０４…閲覧用個人情報、１５０５…更新用個人情報、１５０６…集計情報閲覧要求、１５０７…集計用個人情報、１５０８…課金情報閲覧要求、１５０９…課金用個人情報、１６０４…項目ＩＤファイル、１６０５…個人情報データ、２１０６…開示用個人情報。

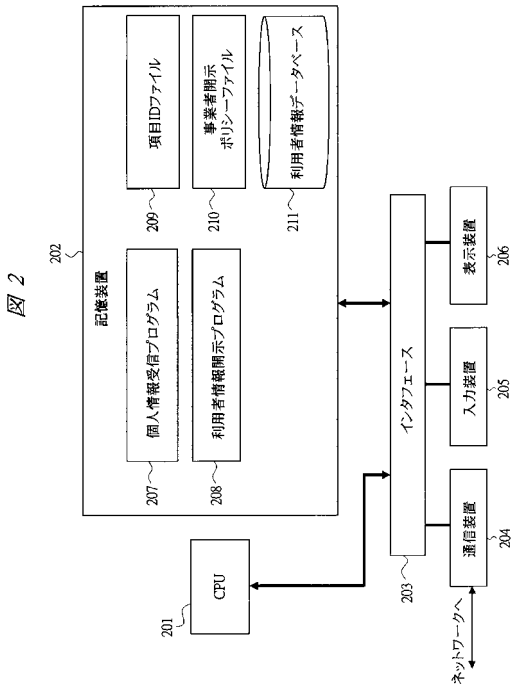
【図１】

図 1



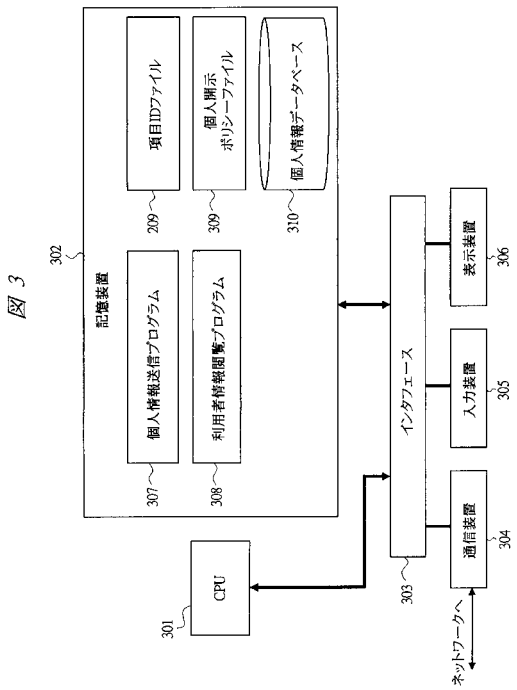
【図２】

図 2



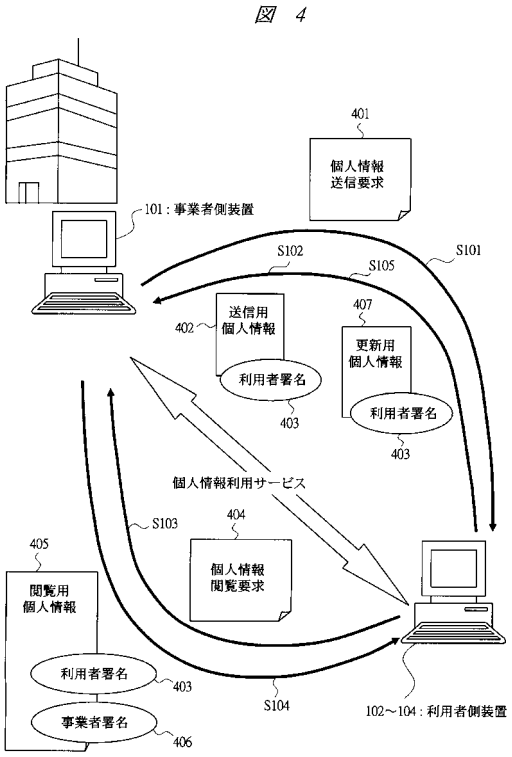
【図３】

図 3



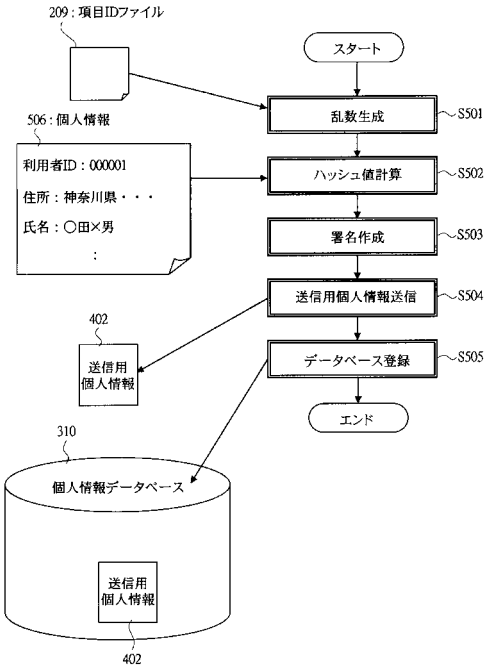
【図４】

図 4



【図５】

図 5



【図６】

図 6

209：項目IDファイル

	項目名	項目ID
601	郵便番号	1
602	住所	2
603	氏名	3
604	クレジット番号	4
605	電話番号	5
606	Eメール	6
607	職業	7
608	趣味	8

【図７】

図 7

402：送信用個人情報

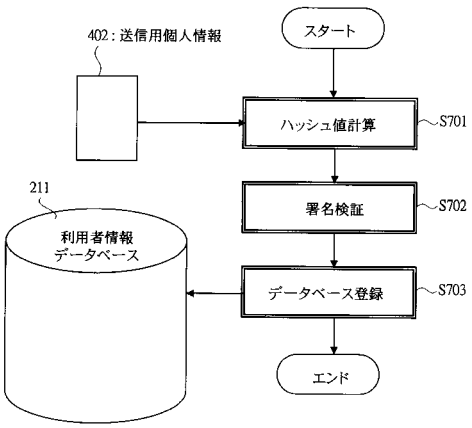
609 利用者ID：000001

	項目ID	項目名	値	乱数
610	1	郵便番号	123-4567	r1
611	2	住所	神奈川県川崎市・・・	r2
612	3	氏名	○田×男	r3
613	4	クレジット番号	0123456789	r4
614	5	電話番号	044-000-0000	r5
615	6	Eメール	A@XXX.co.jp	r6
616	7	職業	会社員	r7
617	8	趣味	音楽鑑賞	r8

618 利用者1署名

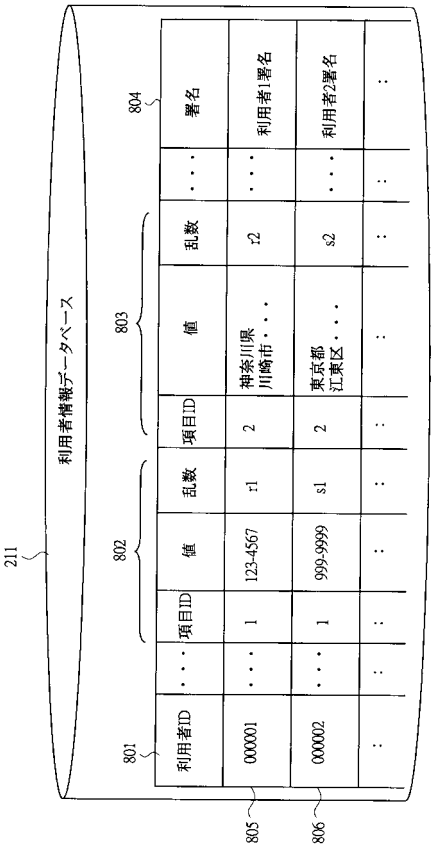
【図８】

図 8



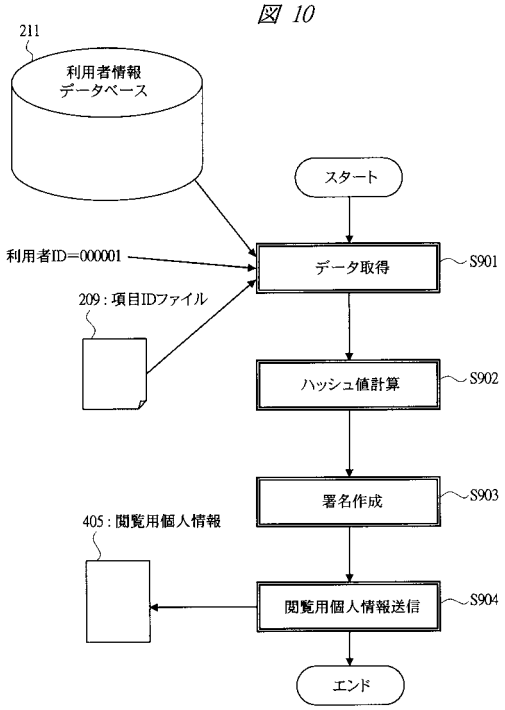
【図９】

図 9



【図１０】

図 10



【図１１】

図 11

405：閲覧用個人情報

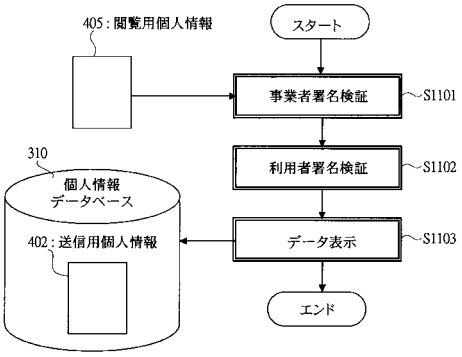
	利用者ID：000001			
	項目ID	項目名	ハッシュ値	乱数
1002	1	郵便番号	3A1B28539C210DDE・・・	
1003	2	住所	8439900A71B28E21・・・	
1004	3	氏名	B25391F210C462A8・・・	
1005	4	クレジット番号	72CA32819402D27E・・・	
1006	5	電話番号	93284733BA1D94A6・・・	
1007	6	Eメール	42DAE1849201A281・・・	
1008	7	職業	8392109474820A3・・・	
1009	8	趣味	940B216E199BB219・・・	

1001

利用者1署名（618）　事業者署名1（1010）

【図１２】

図 12



【図１３】

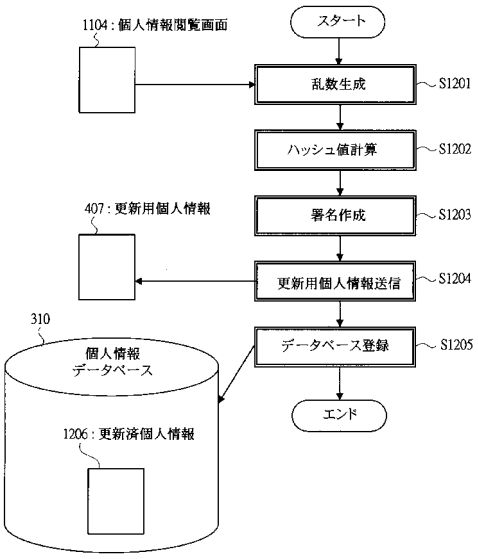
図 13

1104：個人情報閲覧画面

1105	利用者ID：000001		
	項目ID	項目名	値
1106	1	郵便番号	123-4567
1107	2	住所	神奈川県川崎市・・・
1108	3	氏名	○田×男
1109	4	クレジット番号	0123456789
1110	5	電話番号	044-000-0000
1111	6	Eメール	A@XXX.co.jp
1112	7	職業	会社員
1113	8	趣味	音楽鑑賞

【図１４】

図 14



【図１５】

図 15

407：更新用個人情報

1301

利用者ID：000001			
項目ID	項目名	値	乱数
1	郵便番号		r11
2	住所		r12
3	氏名		r13
4	クレジット番号		r14
5	電話番号		r15
6	Eメール	A更新@XXX.co.jp	r16
7	職業		r17
8	趣味		r18
利用者1署名2			

1302 1303 1304 1305 1306 1307 1308 1309 1310

【図１６】

図 16

1206：更新済個人情報

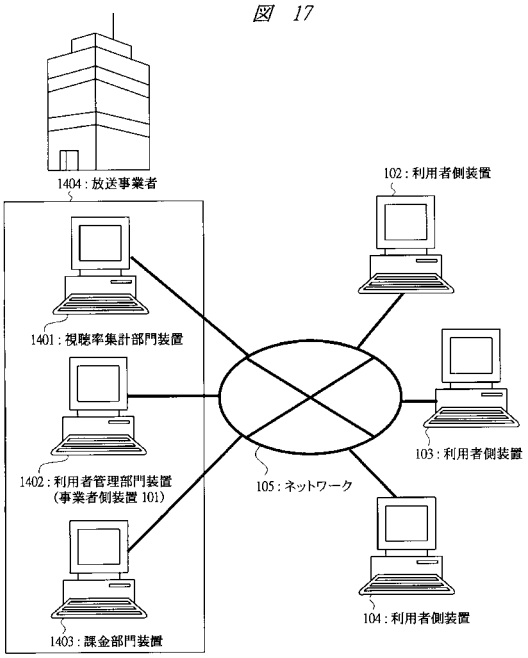
1311

利用者ID：000001			
項目ID	項目名	値	乱数
1	郵便番号	123-4567	r11
2	住所	神奈川県川崎市・・・	r12
3	氏名	○田×男	r13
4	クレジット番号	0123456789	r14
5	電話番号	044-000-0000	r15
6	Eメール	A更新@XXX.co.jp	r16
7	職業	会社員	r17
8	趣味	音楽鑑賞	r18
利用者1署名2			

1312 1313 1314 1315 1316 1307 1317 1318 1310

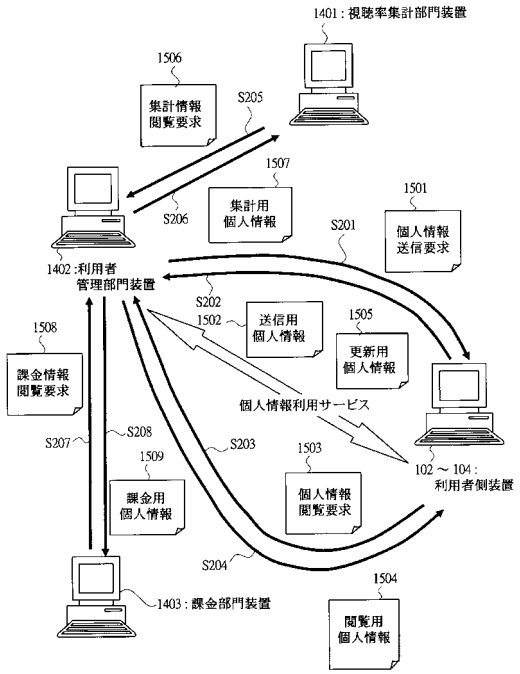
【図１７】

図 17



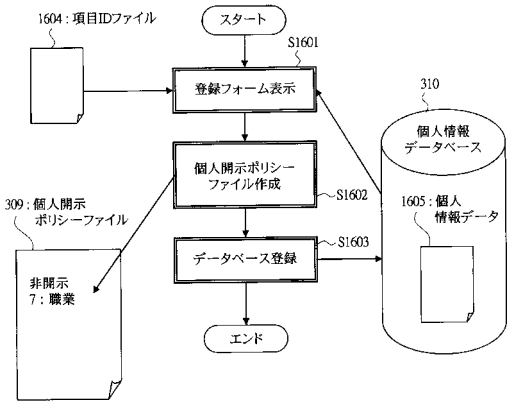
【図１８】

図 18



【図１９】

図 19



【図２０】

図 20

1604：項目IDファイル

	項目名	項目ID
1701	郵便番号	1
1702	住所	2
1703	氏名	3
1704	クレジット番号	4
1705	電話番号	5
1706	Eメール	6
1707	職業	7
1708	趣味	8
1709	居住地域	9
1710	視聴履歴	10

【図２１】

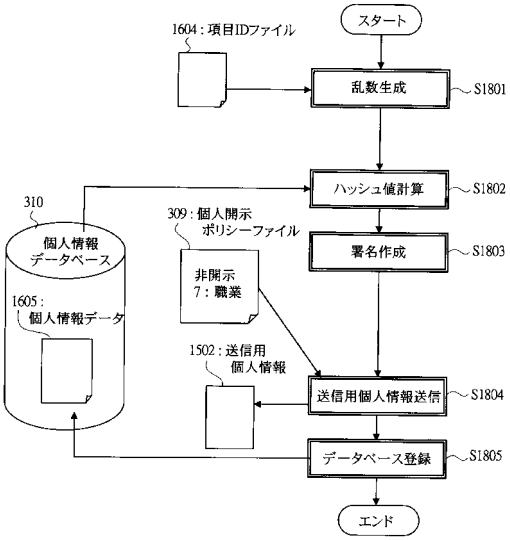
図 21

1605：個人情報データ

	利用者ID：000001			
	項目ID	項目名	値	乱数
1712	1	郵便番号	123-4567	
1713	2	住所	神奈川県川崎市・・・	
1714	3	氏名	○田×男	
1715	4	クレジット番号	0123456789	
1716	5	電話番号	044-000-0000	
1717	6	Eメール	A@XXX.co.jp	
1718	7	職業	会社員	
1719	8	趣味	音楽鑑賞	
1720	9	居住地域	関東	
1721	10	視聴履歴	視聴履歴	

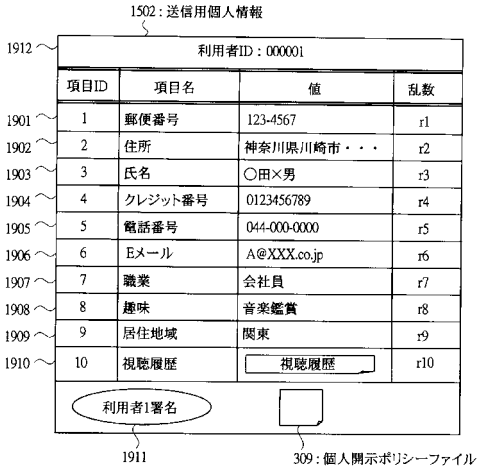
【図２２】

図 22



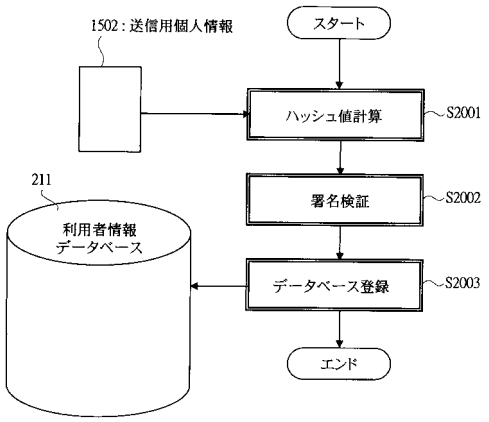
【図２３】

図 23



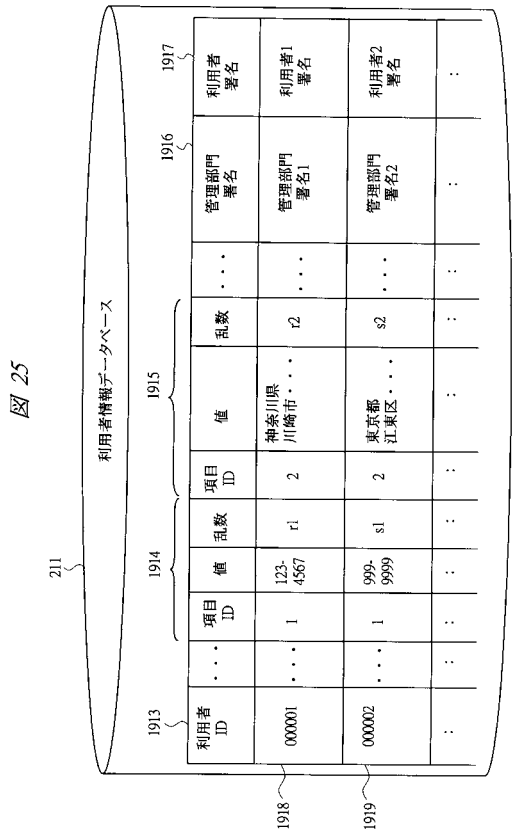
【図２４】

図 24



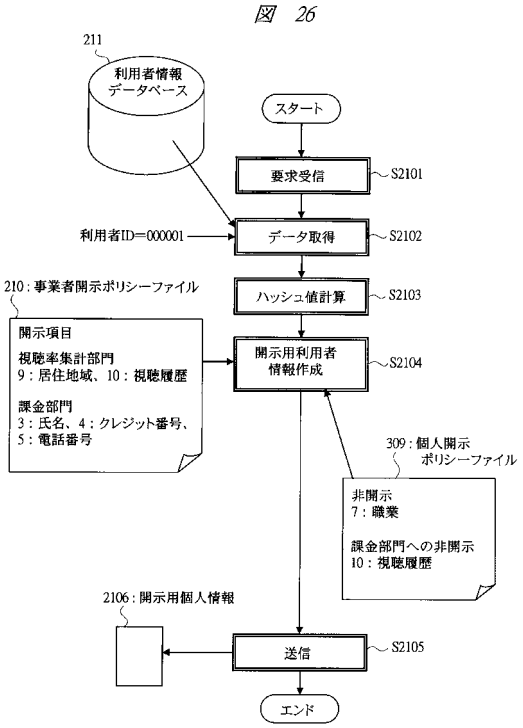
【図２５】

図 25



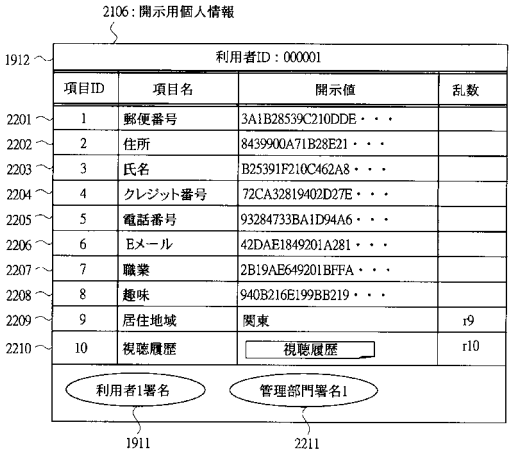
【図２６】

図 26



【図２７】

図 27


2106：開示用個人情報
1912
利用者ID：000001
項目ID
項目名
開示値
乱数
2201
1
郵便番号
3A1B28539C210DDE・・・
2202
2
住所
8439900A71B28E21・・・
2203
3
氏名
B25391F210C462A8・・・
2204
4
クレジット番号
72CA32819402D27E・・・
2205
5
電話番号
93284733BA1D94A6・・・
2206
6
Eメール
42DAE1849201A281・・・
2207
7
職業
2B19AE649201BFFA・・・
2208
8
趣味
940B216E199BB219・・・
2209
9
居住地域
関東
r9
2210
10
視聴履歴
視聴履歴
r10
利用者1署名
管理部門署名1
1911
2211

フロントページの続き

(72)発明者　今泉　浩幸
東京都世田谷区砧一丁目１０番１１号　財団法人エヌエイチケイエンジニアリングサービス内
(72)発明者　河合　輝男
東京都世田谷区砧一丁目１０番１１号　財団法人エヌエイチケイエンジニアリングサービス内
(72)発明者　藤井　亜里砂
東京都世田谷区砧一丁目１０番１１号　日本放送協会　放送技術研究所内
(72)発明者　大竹　剛
東京都世田谷区砧一丁目１０番１１号　日本放送協会　放送技術研究所内
(72)発明者　中村　晴幸
東京都世田谷区砧一丁目１０番１１号　日本放送協会　放送技術研究所内
(72)発明者　真島　恵吾
東京都世田谷区砧一丁目１０番１１号　日本放送協会　放送技術研究所内
(72)発明者　谷本　幸一
神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所　システム開発研究所内
(72)発明者　山田　隆亮
神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所　システム開発研究所内
(72)発明者　小島　弘之
神奈川県川崎市幸区鹿島田８９０番地　株式会社日立製作所　アウトソーシング事業部内

審査官　深沢　正志

(56)参考文献　特開２００４－１９２３５３（ＪＰ，Ａ）
特開２００５－０５１７３４（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／００　－　２１／２４