明　細　書

発明の名称 ： 連携サービス提供システム及びサーバ装置

技術分野

[0001] 本発明の実施形態は、連携サービス提供システム及びサーバ装置に関する。

背景技術

[0002] 複数の装置が情報を相互に送受信して一つのサービスを提供するための連携サービス提供方式としては、各装置を他の装置と直接接続する方式と、ＩＤ変換機能及びログ機能等をもった共通バスを介して各装置を接続する方式とがある。この２つの方式のうち、前者の各装置を他の装置と直接接続する方式は、各装置間で相互に送受信される情報（以下、連携情報と表記する）を集約して管理するポイントがないため、後に送受信内容の検証・監査を行うことが難しい。このため、後者のＩＤ変換機能及びログ機能等をもった共通バスを介して各装置を接続する方式が望ましいとされている。

[0003] 一般に各装置がもつ情報を識別するためのＩＤは、同一の情報を識別するためのＩＤであっても、ＩＤ自体は装置毎に異なっている。ＩＤ変換機能とは、ＩＤ自体は装置毎に異なっていたとしても、同一の情報を識別するためのＩＤであることを証明する機能である。なお、ＩＤ変換機能を実現させるための方式としては、テーブル参照方式と関数方式とがある。

[0004] 例えば、テーブル参照方式を適用した連携サービス提供技術としては、複数の装置を連携させる連携装置に予めテーブルを記憶しておき、各装置を連携させるときにこのテーブルを参照することで、複数の装置間でのＩＤの連携（すなわち、連携情報の送受信）を実現させる連携サービス提供技術がある。

[0005] また、関数方式を適用した連携サービス提供技術としては、例えば、連携させる各装置の一方から送信されたＩＤを含む情報を、ＡＥＳにおける秘密情報を用いて連携装置上で一度復号した後に、他方の装置向けのコードに再

度変換して送信することで、複数の装置間でのＩＤの連携（すなわち、連携情報の送受信）を実現させる連携サービス提供技術がある。

[0006] 更に、関数方式を適用した連携サービス提供技術としては、連携情報に対して公開鍵暗号を用いることで、各装置間での連携情報の送受信を実現させる連携サービス提供技術がある。

[0007] ここで、公開鍵暗号系に関してプロキシ再暗号化（Proxy Re-Encryption）と呼ばれる技術について説明する。

[0008] この技術の基本的なモデルは以下の鍵生成、暗号化、復号、再暗号化鍵生成、再暗号化の５つの関数（以下、アルゴリズムとも表記する）からなる。鍵生成、暗号化、復号の機能は通常の公開鍵暗号と同様である。

[0009] （鍵生成）$KeyGen(1^k)\rightarrow(pk,sk)$

鍵生成アルゴリズムKeyGenは、セキュリティパラメータ1^kが入力されると、公開鍵pkと秘密鍵skの組（pk,sk）を出力する。

[0010] （暗号化）$Enc(pk_A, m)\rightarrow C_A$

暗号化アルゴリズムEncは、ユーザＡの公開鍵pk_Aとメッセージｍが入力されると、ユーザＡ宛の暗号文C_Aを出力する。

[0011] （復号）$Dec(sk_A, C_A)\rightarrow m$

復号アルゴリズムDecは、ユーザＡの秘密鍵sk_Aと、ユーザＡ宛の暗号文C_Aとが入力されると、メッセージｍを出力する。

[0012] （再暗号化鍵生成）$ReKeyGen(pk_A, sk_A, pk_B, sk_B)\rightarrow rk_{A\rightarrow B}$

再暗号化鍵生成アルゴリズムReKeyGenは、ユーザＡの公開鍵pk_A、ユーザＡの秘密鍵sk_A、ユーザＢの公開鍵pk_B、ユーザＢの秘密鍵sk_Bが入力されると、再暗号化鍵$rk_{A\rightarrow B}$を出力する。

[0013] （再暗号化）$ReEnc(rk_{A\rightarrow B}, C_A)\rightarrow C_B$

再暗号化アルゴリズムReEncは、再暗号化鍵$rk_{A\rightarrow B}$と、ユーザＡ宛の暗号文C_Aとが入力されると、ユーザＢ宛の暗号文C_Bを出力する。

[0014] 以上が基本的なモデルである。但し、再暗号化の実現方式に応じて、関数への入力が異なるモデルや、上記以外の関数や鍵を含むモデルも考えられて

いる。

[0015] 例えば、再暗号化鍵生成アルゴリズムの入力において、ユーザＢの秘密鍵ｓｋ$_B$を不要とした非相互作用的（non-interactive）と呼ばれるモデルや、ユーザＡの秘密鍵ｓｋ$_A$に代えて、ユーザＢ宛の再暗号化鍵ｒｋ$_{A\to B}$とユーザＣの秘密鍵ｓｋ$_C$とが入力されるモデルなども考えられている。

[0016] また、再暗号化鍵ｒｋ$_{A\to B}$で暗号文Ｃ$_A$→Ｃ$_B$の再暗号化を行える一方で、その逆の暗号文Ｃ$_B$→Ｃ$_A$の変換を行えない一方向性（unidirectional）と呼ばれるモデル、逆の変換も行える双方向性（bidirectional）と呼ばれるモデルなども知られている。なお、双方向性モデルでは、再暗号化鍵ｒｋ$_{A\to B}$をｒｋ$_{A\Leftrightarrow B}$と表すことがある。

[0017] さらに、公開鍵暗号の中でもＩＤベース暗号に基づく方式も考えられている。その場合、マスター鍵生成のための関数セットアップ（Setup）が増え、鍵生成アルゴリズムKeyGenの入力にマスター鍵とＩＤが追加される。ＩＤベース暗号において、公開鍵ｐｋはＩＤそのものである。

[0018] 具体的な方式の例としては、一方向性モデルでは非特許文献３，４に記載の方式が、双方向性モデルでは非特許文献５に記載の方式が、ＩＤベース暗号では非特許文献６，７などに記載の方式がそれぞれ知られている。なお、実施形態では非特許文献８に記載の方式を参考にしている。

先行技術文献

特許文献

[0019] 特許文献1：特開２００６－１９５７９１号公報

非特許文献

[0020] 非特許文献1：M. Blaze, M. Strauss. Atomic Proxy Cryptography. AT&T Labs Research TR98.5.1, 1997.

非特許文献2：M. Blaze, G. Bleumer, M. Strauss. Divertible Protocols and Atomic Proxy Cryptography. In Eurocrypt’98, LNCS 1403, pp.127-144, 1998.

非特許文献3：G. Ateniese, K. Fu, M. Green, S. Hohenberger. Improved P

roxy Re-Encryption Schemes with Applications to Secure Distributed Storage. In NDSS' 05, 2005.

非特許文献4：B. Libert, D. Vergnaud. Tracing Malicious Proxies in Proxy Re-Encryption. In Pairing 2008, 2008.

非特許文献5：R. Canetti, S. Hohenberger. Chosen-Ciphertext Secure Proxy Re-Encryption. In ACM CCS' 07, 2007.

非特許文献6：M. Green, G. Ateniese. Identity-Based Proxy Re-encryption. In ACN' 07, 2007.

非特許文献7：T. Matsuo. Proxy Re-encryption Systems for Identity-based Encryption. In Pairing 2007, 2007.

非特許文献8：Benoit Libert, Damien Vergnaud, "Unidirectional Chosen-Ciphertext Secure Proxy Re-encryption", Public Key Cryptography 2008, pp. 360-279.

非特許文献9：G. Ateniese, S. Hohenberger, "Proxy re-signature: new definitions, algorithm, and applications", ACM Conference on Computer and Communications Security 2005, pp.310-319

非特許文献10：A. Menezes, P. van Oorschot, S. Vanstone, "Handbook of Applied Cryptography", CRC Press, (1996)

発明の概要

発明が解決しようとする課題

[0021] しかしながら、以上のような連携サービス提供技術では、連携装置上で連携情報（すなわち、ＩＤ）を紐付けることができるといった不都合や、各装置間での連携情報のやり取りの過程を、連携装置上で後に監査・検証することができないといった不都合がある。

[0022] 本発明が解決しようとする課題は、連携装置上での連携情報の紐付を防止し、かつ連携装置上での後の監査・検証を可能にする連携サービス提供システム及びサーバ装置を提供することである。

課題を解決するための手段

[0023] 実施形態の連携サービス提供システムは、再暗号化鍵発行装置と、利用者を識別するために発行されたＩＤを用いて前記利用者に対して各種サービスを提供する複数のサービス装置と、これら複数のサービス装置を連携させる連携装置とが通信可能に接続される。

[0024] 前記連携装置は、第１記憶手段、第２記憶手段、第１生成手段、第１送信手段及び第２送信手段を備えている。

[0025] 前記第１記憶手段は、前記再暗号化鍵発行装置及び前記各サービス装置の公開鍵を記憶する。

[0026] 前記第２記憶手段は、前記各サービス装置から送信される暗号文データを平文データに復号せずに、別のサービス装置の秘密鍵を用いて復号可能にする再暗号化処理を実現させるための再暗号化鍵を記憶する。

[0027] 前記第１生成手段は、前記各サービス装置から送信される暗号文データを受けると、前記記憶された再暗号化鍵を用いて当該暗号文データを再暗号化処理して再暗号文データを生成する。

[0028] 前記第１送信手段は、前記暗号文データを送信したサービス装置とは別のサービス装置に前記生成された再暗号文データを送信する。

[0029] 前記第２送信手段は、前記各サービス装置に前記記憶された公開鍵を送信する。

[0030] 前記各サービス装置は、第３記憶手段、第４記憶手段、第２生成手段、第３送信手段、取得手段、読出手段及び第４送信手段を備えている。

[0031] 前記第３記憶手段は、発行された前記ＩＤを前記各サービス装置特有の利用者の情報を示す利用者情報に対応付けて記憶する。

[0032] 前記第４記憶手段は、前記各サービス装置の秘密鍵を記憶する。

[0033] 前記第２生成手段は、前記利用者の操作に応じて、前記連携装置から送信された再暗号化鍵発行装置の公開鍵を用いて、当該利用者のＩＤを暗号化処理して暗号文データを生成する。

[0034] 前記第３送信手段は、前記生成された暗号文データと共に、別のサービス装置に記憶され、かつ当該暗号文データにより示されるＩＤにより特定され

る利用者の利用者情報を取得したい旨の要求を前記連携装置に送信する。

[0035] 前記取得手段は、前記連携装置から送信された再暗号文データを受けると、前記記憶された秘密鍵を用いて当該再暗号文データを復号し、前記暗号化されたＩＤを取得する。

[0036] 前記読出手段は、前記取得されたＩＤに対応した利用者情報を前記第３記憶手段から読み出す。

[0037] 前記第４送信手段は、前記読み出された利用者情報を前記連携装置を介して別のサービス装置に送信する。

図面の簡単な説明

[0038] [図1]図１は、第１の実施形態に係る連携サービス提供システムの構成例を示す模式図である。

[図2]図２は、同実施形態に係る鍵生成処理の一例を示すシーケンス図である。

[図3]図３は、同実施形態に係るＩＤ発行処理の一例を示すシーケンス図である。

[図4]図４は、同実施形態に係る再暗号化鍵生成処理の一例を示すシーケンス図である。

[図5]図５は、同実施形態に係る連携処理の一例を示すシーケンス図である。

[図6]図６は、第１の実施形態の変形例に係るコード配布処理の一例を示すシーケンス図である。

[図7]図７は、第１の実施形態の変形例に係る連携処理の一例を示すシーケンス図である。

[図8]図８は、第１の実施形態の更なる変形例に係る連携サービス提供システムの構成例を示す模式図である。

[図9]図９は、第１の実施形態の更なる変形例に係る連携処理の一例を示すシーケンス図である。

[図10]図１０は、第２の実施形態に係る連携サービス提供システムの構成例を示す模式図である。

[図11]図１１は、同実施形態に係る連携処理の一例を示すシーケンス図である。

発明を実施するための形態

[0039] ［第１の実施形態］

図１は第１の実施形態に係る連携サービス提供システムの構成例を示す模式図である。連携サービス提供システム１は、図１に示すように、再暗号化鍵発行装置１０、連携装置（サーバ装置と称しても良い）２０、ＩＤ発行装置３０及び複数のサービス装置S_1，S_2を備えている。

[0040] なお、本実施形態では、説明の簡略化のためにサービス装置が２台であると仮定するが、サービス装置の台数はこれに限定されるものでない。また、ＩＤ発行装置３０は、各サービス装置S_1，S_2を利用する利用者を識別するためのＩＤを発行し、このＩＤを前記各サービス装置に配布するものであるが、各サービス装置S_1，S_2を利用する利用者の情報（以下、「利用者情報」と表記）が当該ＩＤと対応付けて記憶されていれば良いため、必ずしも必須の構成ではなく、ＩＤの配布の手段は問わない（本実施形態の構成には無い外部から配布されていても良い）ものとする。

[0041] 以下に、各装置１０～３０，S_1，S_2の構成を具体的に説明する。

[0042] 再暗号化鍵発行装置１０は、セキュリティパラメータ記憶部１１、秘密鍵記憶部１２、一時データ記憶部１３、公開パラメータ生成部１４、暗号化鍵／再暗号化鍵生成部１５、通信部１６及び制御部１７を備えている。

[0043] セキュリティパラメータ記憶部１１は、鍵生成の公開パラメータを生成するために必要となるセキュリティパラメータを記憶する記憶装置である。セキュリティパラメータとは、例えば、公開パラメータを生成するときの条件を規定したしきい値である。

[0044] 秘密鍵記憶部１２は、公開パラメータを用いて暗号化鍵／再暗号化鍵生成部１５により生成された再暗号化鍵発行装置１０自らの鍵ペア（公開鍵／秘密鍵）のうちの秘密鍵を記憶する記憶装置である。

[0045] 一時データ記憶部１３は、暗号化鍵／再暗号化鍵生成部１５により生成さ

れた自装置１０の公開鍵や、公開パラメータ生成部１４及び暗号化鍵／再暗号化鍵生成部１５の処理途中及び処理結果等の一時データを記憶する記憶装置である。

[0046] 公開パラメータ生成部１４は、セキュリティパラメータ記憶部１１から読み出したセキュリティパラメータを用いて鍵生成の公開パラメータを生成する機能と、この公開パラメータを生成する処理の処理途中及び処理結果を一時データ記憶部１３に書込む機能とをもっている。

[0047] 暗号化鍵／再暗号化鍵生成部１５は、公開パラメータ生成部１４により生成された公開パラメータを用いて自装置１０の鍵ペアを生成する機能と、生成した鍵ペアのうちの秘密鍵を秘密鍵記憶部１２に書込み、かつ生成した鍵ペアのうちの公開鍵を一時データ記憶部１３に書込む機能とをもっている。また、暗号化鍵／再暗号化鍵生成部１５は、秘密鍵記憶部１２から読み出した再暗号化鍵発行装置１０の秘密鍵と、後述する連携装置２０から送信された各サービス装置S_1，S_2の公開鍵とを用いて再暗号化鍵を生成する機能と、この再暗号化鍵を生成する処理の処理途中及び処理結果を一時データ記憶部１３に書込む機能とをもっている。

[0048] 通信部１６は、他の装置２０，３０，S_1，S_2と通信可能にするものであり、例えば、公開パラメータ生成部１４により生成された公開パラメータや、暗号化鍵／再暗号化鍵生成部１５により生成された自装置１０の公開鍵や再暗号化鍵を連携装置２０に送信する機能をもっている。また、通信部１６は、再暗号化鍵発行装置１０からの各種要求を連携装置２０に送信する機能をもっている。

[0049] 制御部１７は、各部１１～１６を制御する機能をもっている。

[0050] 連携装置２０は、公開パラメータ記憶部２１、公開鍵記憶部２２、再暗号化鍵記憶部２３、一時データ記憶部２４、再暗号化処理部２５、通信部２６及び制御部２７を備えている。

[0051] 公開パラメータ記憶部２１は、再暗号化鍵発行装置１０から送信された公開パラメータを記憶する記憶装置である。

[0052] 公開鍵記憶部２２は、再暗号化鍵発行装置１０や後述する各サービス装置S_1，S_2から送信された公開鍵を記憶する記憶装置である。

[0053] 再暗号化鍵記憶部２３は、再暗号化鍵発行装置１０から送信された再暗号化鍵を記憶する記憶装置である。

[0054] 一時データ記憶部２４は、再暗号化処理部２５の処理途中及び処理結果等の一時データを記憶する記憶装置である。

[0055] 再暗号化処理部２５は、再暗号化鍵記憶部２３から読み出した再暗号化鍵を用いて、各サービス装置S_1，S_2から送信された暗号文データを再暗号化する機能と、この再暗号化する処理の処理途中及び処理結果を一時データ記憶部２４に書込む機能とをもっている。具体的には、再暗号化処理部２５は、再暗号化鍵記憶部２３から読み出した再暗号化鍵を用いて、一方のサービス装置（例えば、サービス装置S_1）から送信された暗号文データを平文データに復号することなく、他方のサービス装置（例えば、サービス装置S_2）向けの暗号文データに再暗号化する（すなわち、再暗号文データを生成する）機能をもっている。

[0056] 通信部２６は、他の装置１０，３０，S_1，S_2と通信可能にするものであり、例えば、再暗号化鍵発行装置１０から送信された公開パラメータや、再暗号化鍵発行装置１０及び各サービス装置S_1，S_2から送信された公開鍵や、再暗号化鍵発行装置１０から送信された再暗号化鍵を対応した各記憶部２１～２３に書込む機能と、再暗号化処理部２５により再暗号化された再暗号文データを各サービス装置S_1，S_2に送信する機能とをもっている。また、通信部２６は、他の装置１０，３０，S_1，S_2からの要求に応じて、公開パラメータや公開鍵を各装置１０，３０，S_1，S_2に送信する機能をもっている。

[0057] 制御部２７は、各部２１～２６を制御する機能をもっている。

[0058] ＩＤ発行装置３０は、ＩＤ発行情報記憶部３１、ＩＤ発行部３２、通信部３３及び制御部３４を備えている。

[0059] ＩＤ発行情報記憶部３１は、ＩＤ発行部３２により発行されたＩＤを記憶

する記憶装置である。

[0060] ＩＤ発行部３２は、各サービス装置S_1，S_2を利用する利用者を識別するためのユニークなＩＤを発行する機能と、発行したＩＤをＩＤ発行情報記憶部３１に書込む機能とをもっている。

[0061] 通信部３３は、他の装置１０，２０，S_1，S_2と通信可能にするものであり、例えば、ＩＤ発行部３２により発行されたＩＤを各サービス装置S_1，S_2に配布する機能をもっている。

[0062] 制御部３４は、各部３１～３３を制御する機能をもっている。

[0063] 次に、各サービス装置S_1，S_2の具体的な構成について説明するが、以下では、説明の簡略化のために、サービス装置S_1の構成を代表例として説明する。

[0064] サービス装置S_1は、利用者情報記憶部S_11、秘密鍵記憶部S_12、一時データ記憶部S_13、暗号化処理部S_14、復号処理部S_15、サービス処理部S_16、サービス連携要求部S_17、通信部S_18及び制御部S_19を備えている。

[0065] 利用者情報記憶部S_11は、ＩＤ発行装置３０から配布されたＩＤをサービス装置S_1を利用する利用者の情報（利用者情報）に対応付けて記憶する記憶装置である。

[0066] 秘密鍵記憶部S_12は、公開パラメータを用いて暗号化処理部S_14により生成された自装置S_1の鍵ペアのうちの秘密鍵を記憶する記憶装置である。

[0067] 一時データ記憶部S_13は、暗号化処理部S_14により生成された自装置S_1の公開鍵や、暗号化処理部S_14及び復号処理部S_15の処理途中及び処理結果等の一時データを記憶する記憶装置である。

[0068] 暗号化処理部S_14は、連携装置２０から送信された公開パラメータを用いて自装置S_1の鍵ペアを生成する機能と、生成した鍵ペアのうちの秘密鍵を秘密鍵記憶部S_12に書込み、かつ生成した鍵ペアのうちの公開鍵を一時データ記憶部S_13に書込む機能とをもっている。また、暗号化処理部S_14は、連携装置２０から送信された再暗号化鍵発行装置１０の公開鍵を用いて、平文

データ（例えば、利用者情報記憶部Ｓ$_1$１に記憶されたＩＤ等）を暗号化処理することにより暗号文データを生成する機能と、この暗号文データを生成する処理の処理途中及び処理結果を一時データ記憶部Ｓ$_1$３に書込む機能とをもっている。

[0069] 復号処理部Ｓ$_1$５は、秘密鍵記憶部Ｓ$_1$２から読み出した秘密鍵を用いて、連携装置２０から送信された再暗号文データを復号する機能と、この復号する処理の処理途中及び処理結果を一時データ記憶部Ｓ$_1$３に書込む機能とをもっている。

[0070] サービス処理部Ｓ$_1$６は、利用者からの要求に応じて、サービスを提供する機能をもっている。

[0071] サービス連携要求部Ｓ$_1$７は、他のサービス装置が有する情報を取得したい旨を通信部Ｓ$_1$８を介して連携装置２０に要求する機能をもっている。

[0072] 通信部Ｓ$_1$８は、他の装置１０～３０，Ｓ$_2$と通信可能にするものであり、例えば、ＩＤ発行装置３０から配布されたＩＤを利用者情報に対応付けて利用者情報記憶部Ｓ$_1$１に書込む機能と、暗号化処理部Ｓ$_1$４により生成された公開鍵や暗号文データを連携装置２０に送信する機能とをもっている。また、通信部Ｓ$_1$８は、サービス装置Ｓ$_1$からの各種要求を連携装置２０に送信する機能をもっている。

[0073] 制御部Ｓ$_1$９は、各部Ｓ$_1$１～Ｓ$_1$８を制御する機能をもっている。

[0074] なお、各サービス装置Ｓ$_1$，Ｓ$_2$では、利用者に対してそれぞれユニークなサービスを提供するため、他のサービス装置と利用者情報を共有していない。

[0075] 次に、以上のように構成された連携サービス提供システム１の動作の一例を図２乃至図５のシーケンス図を用いて説明する。

[0076] 以下の動作は、（１）事前処理（２）連携処理の手順で実行され、（１）事前処理は、（１－１）鍵生成処理、（１－２）ＩＤ発行処理、（１－３）再暗号化鍵生成処理の手順で実行される。但し、事前処理は必ずしも上記手順で処理を実行しなくてもよい。例えば、ＩＤ発行処理は鍵生成処理の前に

実行されてもよい。

[0077] （１）鍵生成処理は、再暗号化鍵発行装置１０及び各サービス装置S_1，S_2により、図２及び以下の各ステップＳＴ１～ＳＴ２１に示すように実行される。

[0078] 始めに、再暗号化鍵発行装置１０内の公開パラメータ生成部１４は、公開パラメータ（ｐ，λ，Ｇ，G_T，ｇ，ｕ，ｖ，Sig）を生成する（ステップＳＴ１）。具体的には、公開パラメータ生成部１４は、予めセキュリティパラメータ記憶部１１に記憶したセキュリティパラメータλに基づいて、素数位数ｐ＞２λを満たす双線型写像群(bilinear map groups)（Ｇ，G_T）、生成元ｇ，ｕ，ｖ∈Ｇ、強偽造不可能性を満たす使い捨て署名（one-time signature）

[数1]

$\mathrm{Sig}(\hat{G},\hat{S},\hat{V})$を選択する。

ここで、使い捨て署名$\mathrm{Sig}(\hat{G},\hat{S},\hat{V})$（以下、$\mathrm{Sig}(\hat{G},\hat{S},\hat{V})$をSigともいう）における$\hat{G}$は使い捨ての鍵ペア（ｓｓｋ，ｓｖｋ）を生成する機能を意味し、$\hat{S}$はメッセージＩＤに対する署名σを生成する機能を意味し、$\hat{V}$は署名σの正当性を検証する機能を意味する。

[0079] 使い捨て署名については非特許文献１０に詳しい。また、Ｇ，G_Tは楕円曲線で定義される群集合であり、次式に示す如きペアリング関数に用いられる。

[0080] ペアリング関数：ｅ（g_1，g_2）＝g_T

但し、g_1，g_2∈Ｇ、g_T∈G_T

このペアリング関数は、次式に示す如き性質がある。

[0081] ｅ（g^a，ｇ）＝ｅ（ｇ，g^a）＝ｅ（ｇ，ｇ）^{a}

但し、ｇ∈Ｇ、ａ∈Z_p

続いて、通信部１６は、公開パラメータ生成部１４により生成された公開パラメータ（ｐ，λ，Ｇ，G_T，ｇ，ｕ，ｖ，Sig）を連携装置２０に送信する（すなわち、他の装置２０，３０，S_1，S_2に対して公開パラメータを公開

する）（ステップＳＴ２）。

[0082] 次に、連携装置２０内の通信部２６は、再暗号化鍵発行装置１０から送信された公開パラメータ（ｐ，λ，Ｇ，G_T，ｇ，ｕ，ｖ，Sig）を受けると、この公開パラメータを公開パラメータ記憶部２１に書込む（登録する）（ステップＳＴ３）。

[0083] 続いて、再暗号化鍵発行装置１０内の通信部１６は、連携装置２０に対して公開パラメータを配布するよう要求する（ステップＳＴ４）。

[0084] 次に、連携装置２０内の通信部２６は、ステップＳＴ４における再暗号化鍵発行装置１０からの要求を受けると、公開パラメータ記憶部２１に記憶された公開パラメータ（ｐ，λ，Ｇ，G_T，ｇ，ｕ，ｖ，Sig）を再暗号化鍵発行装置１０に送信する（ステップＳＴ５）。

[0085] 続いて、再暗号化鍵発行装置１０内の暗号化鍵／再暗号化鍵生成部１５は、連携装置２０から送信された公開パラメータ（ｐ，λ，Ｇ，G_T，ｇ，ｕ，ｖ，Sig）を通信部１６を介して受けると、この公開パラメータを用いて再暗号化鍵発行装置１０の鍵ペアを生成する（ステップＳＴ６）。具体的には、暗号化鍵／再暗号化鍵生成部１５は、再暗号化鍵発行装置１０の識別情報をｉとしたとき、再暗号化鍵発行装置１０の秘密鍵$x_i \in Z_p^*$を生成し、この秘密鍵x_iを用いて再暗号化鍵発行装置１０の公開鍵

[数2]

$$X_i = g^{x_i}$$

[0086] を生成する。

[0087] 次に、暗号化鍵／再暗号化鍵生成部１５は、ステップＳＴ６において生成した自装置１０の鍵ペアのうちの秘密鍵x_iを秘密鍵記憶部１２に書込み、かつ生成した自装置１０の鍵ペアのうちの公開鍵X_iを一時データ記憶部１３に書込む（ステップＳＴ７）。

[0088] 続いて、通信部１６は、一時データ記憶部１３内の公開鍵X_iを連携装置２０に送信する（すなわち、他の装置２０，３０，S_1，S_2に対して公開鍵X_i

を公開する）（ステップＳＴ８）。

[0089] しかる後、連携装置２０内の通信部２６は、再暗号化鍵発行装置１０から送信された再暗号化鍵発行装置１０の公開鍵Ｘｉを受けると、この公開鍵を公開鍵記憶部２２に書込む（登録する）（ステップＳＴ９）。

[0090] また同様に、サービス装置$Ｓ_1$は、サービス装置$Ｓ_1$の鍵ペアについてもステップＳＴ４～ＳＴ９と同様の処理を実行して、サービス装置$Ｓ_1$内の秘密鍵記憶部$Ｓ_1$２に秘密鍵$ｘ_j$を書込むと共に、連携装置２０に公開鍵$Ｘ_j$を送信することで、連携装置２０内の公開鍵記憶部２２にサービス装置$Ｓ_1$の公開鍵$Ｘ_j$を登録する（ステップＳＴ１０～ＳＴ１５）。

[0091] 更に、サービス装置$Ｓ_2$は、サービス装置$Ｓ_2$の鍵ペアについてもステップＳＴ４～ＳＴ９と同様の処理を実行して、サービス装置$Ｓ_2$内の秘密鍵記憶部$Ｓ_2$２に秘密鍵$ｘ_k$を書込むと共に、連携装置２０に公開鍵$Ｘ_k$を送信することで、連携装置２０内の公開鍵記憶部２２にサービス装置$Ｓ_2$の公開鍵$Ｘ_k$を登録する（ステップＳＴ１６～ＳＴ２１）。

[0092] 以上により、鍵生成処理が完了する。以降、各装置１０～３０，$Ｓ_1$，$Ｓ_2$は、連携装置２０内の公開パラメータ記憶部２１及び公開鍵記憶部２２に公開された公開パラメータ及び公開鍵を適宜取得して、利用することができる。

[0093] （１－２）ＩＤ発行処理は、ＩＤ発行装置３０により、図３及び以下の各ステップＳＴ３１～ＳＴ３５に示すように実行される。

[0094] 始めに、ＩＤ発行装置３０内のＩＤ発行部３２は、各サービス装置$Ｓ_1$，$Ｓ_2$を利用する利用者を識別するためのＩＤを発行し、発行したＩＤをＩＤ発行情報記憶部３１に書込む（ステップＳＴ３１）。

[0095] 続いて、通信部３３は、ＩＤ発行情報記憶部３１に記憶されたＩＤをサービス装置$Ｓ_1$に配布する（ステップＳＴ３２）。

[0096] しかる後、サービス装置$Ｓ_1$内の通信部$Ｓ_1$８は、ＩＤ発行装置３０から配布されたＩＤを受けると、このＩＤを利用者情報に対応付けて利用者情報記憶部$Ｓ_1$１に書込む（ステップＳＴ３３）。

[0097] また同様に、ＩＤ発行装置３０内の通信部３３は、サービス装置S_2に対してステップＳＴ３２と同様の処理を実行し（ステップＳＴ３４）、サービス装置S_2内の通信部$S_2$８は、ステップＳＴ３３と同様の処理を実行して、ＩＤを利用者情報に対応付けて利用者情報記憶部$S_2$１に書込む（ステップＳＴ３５）。

[0098] 以上により、ＩＤ発行処理が完了する。

[0099] （１－３）再暗号化鍵生成処理は、再暗号化鍵発行装置１０により、図４及び以下の各ステップＳＴ４１～ＳＴ４５に示すように実行される。但し、ここでは、再暗号化鍵発行装置１０向けの暗号文データをサービス装置S_2向けの暗号文データに変換する再暗号化鍵を生成する処理について説明する。

[0100] 始めに、再暗号化鍵発行装置１０内の通信部１６は、連携装置２０に対して公開パラメータとサービス装置S_2の公開鍵とを配布するよう要求する（ステップＳＴ４１）。

[0101] 続いて、連携装置２０内の通信部２６は、ステップＳＴ４１における再暗号化鍵発行装置１０からの要求を受けると、公開パラメータ記憶部２１に記憶された公開パラメータ（ｐ，λ，Ｇ，G_T，ｇ，ｕ，ｖ，Sig）と、公開鍵記憶部２２に記憶されたサービス装置S_2の公開鍵X_kとを再暗号化鍵発行装置１０に送信する（ステップＳＴ４２）。

[0102] 次に、再暗号化鍵発行装置１０内の暗号化鍵／再暗号化鍵生成部１５は、公開パラメータ（ｐ，λ，Ｇ，G_T，ｇ，ｕ，ｖ，Sig）とサービス装置S_2の公開鍵X_kとを通信部１６を介して受けると、取得した情報と秘密鍵記憶部１２から読み出した自装置１０の秘密鍵x_iとを用いて、再暗号化鍵発行装置１０向けの暗号文データをサービス装置S_2向けの暗号文データに変換するための再暗号化鍵

[数3]

$$R_{ik} = X_k^{1/X_i} = g^{X_k / X_i}$$

[0103] を生成する（ステップＳＴ４３）。

[0104] 続いて、通信部１６は、生成した再暗号化鍵R_{ik}を連携装置２０に送信する（ステップＳＴ４４）。

[0105] しかる後、連携装置２０内の通信部２６は、再暗号化鍵発行装置１０から送信された再暗号化鍵R_{ik}を受けると、この再暗号化鍵を再暗号化鍵記憶部２３に書込む（登録する）（ステップＳＴ４５）。

[0106] 以上により、再暗号化鍵生成処理が完了する。なお、ここでは、再暗号化鍵発行装置１０向けの暗号文データをサービス装置S_2向けの暗号文データに変換する再暗号化鍵を生成するとしたが、これに限定されず、再暗号化鍵発行装置１０向けの暗号文データをサービス装置S_1向けの暗号文データに変換する再暗号化鍵を生成してもよい。

[0107] （２）連携処理は、連携装置２０及び各サービス装置S_1，S_2により、図５及び以下の各ステップＳＴ５１～ＳＴ６２に示すように実行される。

[0108] 始めに、サービス装置S_1内の通信部$S_1$８は、利用者からの要求に応じて、連携装置２０に対して公開パラメータと再暗号化鍵発行装置１０の公開鍵とを配布するよう要求する（ステップＳＴ５１）。

[0109] 続いて、連携装置２０内の通信部２６は、ステップＳＴ５１におけるサービス装置S_1からの要求に応じて、公開パラメータ記憶部２１に記憶された公開パラメータ（ｐ，λ，Ｇ，G_T，ｇ，ｕ，ｖ，Sig）と、公開鍵記憶部２２に記憶された再暗号化鍵発行装置１０の公開鍵X_iとをサービス装置S_1に送信する（ステップＳＴ５２）。

[0110] 次に、サービス装置S_1内の暗号化処理部$S_1$４は、公開パラメータ（ｐ，λ，Ｇ，G_T，ｇ，ｕ，ｖ，Sig）と公開鍵X_iとを通信部$S_1$８を介して受けると、ステップＳＴ５１における利用者に対応したＩＤを利用者情報記憶部$S_1$１から読み出す（ステップＳＴ５３）。

[0111] 続いて、暗号化処理部$S_1$４は、利用者情報記憶部$S_1$１から読み出したＩＤを再暗号化鍵発行装置１０の公開鍵X_iを用いて暗号化処理して暗号文データを生成する（ステップＳＴ５４）。

[0112] ここで、以下の各ステップＳＴ５４－１～ＳＴ５４－４に示すように、暗

号化処理部$S_1$４による暗号化処理について具体的に説明する。

[0113] 始めに、暗号化処理部$S_1$４は、公開パラメータにおけるセキュリティパラメータλ及び鍵ペア生成機能

[数4]

$\hat{G}$に基づいて、使い捨て署名における署名鍵ｓｓｋと検証鍵ｓｖｋの鍵ペア

$(ssk, svk) \leftarrow \hat{G}(\lambda)$

[0114] を生成し（ステップＳＴ５４－１）、第１暗号化データC_1に検証鍵ｓｖｋをセットする（C_1＝ｓｖｋ）。

[0115] また、暗号化処理部$S_1$４は、第１乱数ｒ$\in Z_p^*$を生成した後に、この第１乱数ｒに基づき、平文データとしてのＩＤ$\in G_T$に対して、以下の第２、第３及び第４暗号化データC_2，C_3, C_4を生成する（ステップＳＴ５４－２）。

[数5]

$$C_2 = X_i^r$$
$$C_3 = e(g,g)^r \cdot ID$$
$$C_4 = \left(u^{svk} \cdot v\right)^r$$

[0116] 具体的には、暗号化処理部$S_1$４は、再暗号化鍵発行装置１０の公開鍵X_iと、第１乱数ｒとに基づいて、第２暗号化データC_2を生成する。また、暗号化処理部$S_1$４は、公開パラメータにおける生成元ｇと、第１乱数ｒと、ＩＤとに基づき、ペアリング関数によって第３暗号化データC_3を生成する。更に、暗号化処理部$S_1$４は、公開パラメータにおける生成元ｕ，ｖと、生成した検証鍵ｓｖｋと、第１乱数ｒとに基づいて、第４暗号化データC_4を生成する。

[0117] ステップＳＴ５４－２の終了後、暗号化処理部$S_1$４は、第３及び第４暗号化データC_3，C_4に対し、公開パラメータにおける署名生成機能

[数6]

$\hat{S}$と生成した署名鍵ｓｓｋによる使い捨て署名σを
次式に示すように生成する（ステップＳＴ５４－３）。
$\sigma=\hat{S}(ssk,(C_3,C_4))$

[0118] しかる後、暗号化処理部$S_1$４は、これら第１乃至第４暗号化データC_1～C_4と使い捨て署名σとを含む暗号文データ$C_i=(C_1, C_2, C_3, C_4, \sigma)$を生成し、得られた暗号文データを一時データ記憶部$S_1$３に書き込む（ステップＳＴ５４－４）。

[0119] 以上のように、ステップＳＴ５４－１～ＳＴ５４－４の処理が完了することで暗号文データが生成される。

[0120] ステップＳＴ５４の後に、サービス連携要求部$S_1$７は、暗号化処理部$S_1$４により生成された暗号文データを用いて、サービス装置S_2が保有する情報の取得を通信部$S_1$８を介して連携装置２０に対して要求する（ステップＳＴ５５）。

[0121] 次に、連携装置２０内の再暗号化処理部２５は、ステップＳＴ５５におけるサービス装置S_1からの要求と暗号文データとを通信部２６を介して受けると、予め再暗号化鍵記憶部２３に記憶した再暗号化鍵R_{ik}を用いて当該暗号文データを再暗号化する（ステップＳＴ５６）。

[0122] ここで、以下の各ステップＳＴ５６－１～ＳＴ５６－３に示すように、再暗号化処理部２５による再暗号化処理について具体的に説明する。

[0123] 始めに、再暗号化処理部２５は、公開パラメータと次の検証式を用い、暗号文データC_{ki}を検証する（ステップＳＴ５６－１）。ここで、２つの検証式が成立すれば検証は成功し、１つでも成立しない検証式があれば検証は失敗する。

[数7]

$$e\left(C_2, u^{C_1} \cdot v\right) \stackrel{?}{=} e\left(X_i, C_4\right)$$

$$\hat{V}\left(C_1, \sigma, \left(C_3, C_4\right)\right) \stackrel{?}{=} 1$$

[0124] 再暗号化処理部２５は、検証に成功すると、第２乱数ｔ∈Z_p*を生成し、次式に示すように、第１、第２及び第３再暗号化データC_2'，C_2''，C_2'''を生成する（ステップＳＴ５６－２）。

[数8]

$$C_2' = X_i^t$$

$$C_2'' = R_{ik}^{1/t} = g^{\left(x_k/x_i\right)^{t^{-1}}}$$

$$C_2''' = C_2^t = X_i^{rt}$$

[0125] 具体的にはステップＳＴ５６－２において、再暗号化処理部２５は、再暗号化鍵発行装置１０の公開鍵X_iと、第２乱数ｔとに基づいて、第１再暗号化データC_2'を生成する。また、再暗号化処理部２５は、再暗号化鍵R_{ik}及び第２乱数ｔに基づいて、第２再暗号化データC_2''を生成する。更に、再暗号化処理部２５は、第２暗号化データC_2及び第２乱数ｔに基づいて、第３再暗号化データC_2'''を生成する。

[0126] ステップＳＴ５６－２の終了後、再暗号化処理部２５は、これら第１乃至第３再暗号化データC_2'～C_2'''を、暗号文データC_i内の第２暗号化データC_2と置換して再暗号文データC_k＝（C_1，C_2'，C_2''，C_2'''，C_3，C_4，σ）を生成し、得られた再暗号文データを一時データ記憶部２４に書込む（ステップＳＴ５６－３）。

[0127] 以上のように、ステップＳＴ５６－１～ＳＴ５６－３の処理が完了することで再暗号文データが生成される。

[0128] ステップＳＴ５６の後に、通信部２６は、生成した再暗号文データC_kをサ

ービス装置S_2に送信し（ステップＳＴ５７）、この再暗号文データを用いてサービス装置S_2が保有する情報の取得を要求する。

[0129] 続いて、サービス装置S_2内の復号処理部$S_2$５は、連携装置２０から送信された再暗号文データC_kを通信部$S_2$８を介して受けると、予め秘密鍵記憶部$S_1$２に記憶した秘密鍵x_kを用いて再暗号文データを復号し、ＩＤを取得する（ステップＳＴ５８）。

[0130] ここで、以下の各ステップＳＴ５８－１～ＳＴ５８－２に示すように、復号処理部$S_2$５による復号処理について具体的に説明する。

[0131] 始めに、復号処理部$S_2$５は、公開パラメータ及び自装置S_2の公開鍵X_kと次の検証式を用い、再暗号文データC_kを検証する（ステップＳＴ５８－１）。ここで、３つの検証式が成立すれば検証は成功し、１つでも成立しない検証式があれば検証は失敗する。

[数9]

$$e(C_2', C_2'') \stackrel{?}{=} e(X_k, g)$$

$$e(C_2''', u^{C_1} \cdot v) \stackrel{?}{=} e(C_2', C_4)$$

$$\hat{V}(C_1, \sigma, (C_3, C_4)) \stackrel{?}{=} 1$$

[0132] 復号処理部$S_2$５は、検証に成功すると、自装置S_2の秘密鍵x_kに基づいて、次式に示すように、再暗号文データC_kからＩＤを復号する（ステップＳＴ５８－２）。

[数10]

$$ID = C_3 \Big/ \left(e(C_2'', C_2''')^{1/x_k} \right)$$

[0133] 以上のように、ステップＳＴ５８－１～ＳＴ５８－２の処理が完了することでＩＤが取得される。

[0134] ステップＳＴ５８の後に、サービス装置$Ｓ_2$内のサービス処理部$Ｓ_2$６は、復号処理部$Ｓ_2$５により復号されたＩＤに対応する利用者情報を利用者情報記憶部$Ｓ_2$１から読み出す（ステップＳＴ５９）。

[0135] 次に、通信部$Ｓ_2$８は、サービス処理部$Ｓ_2$６により読み出された利用者情報を連携情報として連携装置２０に送信する（ステップＳＴ６０）。

[0136] 続いて、連携装置２０内の通信部２６は、サービス装置$Ｓ_2$から送信された連携情報を受けると、この連携情報をサービス装置$Ｓ_1$に送信する（ステップＳＴ６１）。

[0137] しかる後、サービス装置$Ｓ_1$内の通信部$Ｓ_1$８は、連携装置２０から送信された連携情報を受信する。これによりサービス装置$Ｓ_1$は連携情報を取得する（ステップＳＴ６２）。

[0138] 以上説明した第１の実施形態によれば、再暗号化処理部２５を含む連携装置２０と、暗号化処理部$Ｓ_1$４，$Ｓ_2$４、復号処理部$Ｓ_1$５，$Ｓ_2$５及びサービス連携要求部$Ｓ_1$７，$Ｓ_2$７を含む複数のサービス装置$Ｓ_1$，$Ｓ_2$とを備えた構成により、連携装置２０が各サービス装置$Ｓ_1$，$Ｓ_2$間での連携情報のやり取りの過程でＩＤを紐付けることができないため、連携情報に対してのセキュリティ性を向上させることができる。

[0139] また、再暗号化鍵発行装置１０及び連携装置２０が有する情報を用いて（すなわち、各サービス装置$Ｓ_1$，$Ｓ_2$の秘密情報を必要とせずに）、各サービス装置$Ｓ_1$，$Ｓ_2$間での連携情報のやり取りの過程を後に監査・検証することができる。

[0140] なお、本実施形態では、各サービス装置$Ｓ_1$，$Ｓ_2$内の利用者情報記憶部$Ｓ_1$１，$Ｓ_2$１に記憶されたＩＤを再暗号化方式を用いて暗号化したが、これに限定されず、例えばＩＤを共通暗号化方式を用いて暗号化した後に、この共通鍵を再暗号化方式を用いて暗号化するハイブリッド暗号を適用してもよい。

[0141] ［変形例］

以下に、第１の実施形態の変形例について、図６，図７のシーケンス図を用いて説明する。この変形例は、ＩＤ発行装置３０において発行された利用

者のＩＤから生成したコード（配布される前のコードが請求項２における第１のコードにあたる）を各サービス装置S_1，S_2に配布して、このコードを用いて連携処理を実行するものである。なお、（１－１）鍵生成処理と（１－３）再暗号化鍵生成処理とは、前述した第１の実施形態と同一であるため、ここでは詳細な説明を省略する。

[0142] 以下、前述した第１の実施形態とは異なる（１－２´）コード配布処理と（２´）連携処理とについて説明する。

[0143] （１－２´）コード配布処理は、連携装置２０、ＩＤ発行装置３０及び各サービス装置S_1，S_2により、図６及び以下の各ステップＳＴ７１～ＳＴ７９に示すように実行される。

[0144] 始めに、ＩＤ発行装置３０内のＩＤ発行部３２は、各サービス装置S_1，S_2を利用する利用者を識別するためのＩＤを発行し、発行したＩＤをＩＤ発行情報記憶部３１に書込む（ステップＳＴ７１）。

[0145] 続いて、通信部３３は、連携装置２０に対して再暗号化鍵発行装置１０の公開鍵を配布するよう要求する（ステップＳＴ７２）。

[0146] 次に、連携装置２０内の通信部２６は、ステップＳＴ７２におけるＩＤ発行装置３０からの要求を受けると、公開鍵記憶部２２に記憶された再暗号化鍵発行装置１０の公開鍵X_iをＩＤ発行装置３０に送信する（ステップＳＴ７３）。

[0147] 続いて、ＩＤ発行装置３０内のＩＤ発行部３２は、連携装置２０から送信された再暗号化鍵発行装置１０の公開鍵X_iを通信部３３を介して受けると、この公開鍵を用いてＩＤ発行情報記憶部３１に記憶したＩＤを暗号化処理してサービス装置S_1向けの第１コード（請求項２における第１のコード）を生成した後に、生成した第１コードとこの第１コードを生成するときに用いた各種パラメータ（以下、第１パラメータと表記）とをＩＤ発行情報記憶部３１に書込む（ステップＳＴ７４）。なお、ステップＳＴ７４の処理は、ＩＤ発行情報記憶部３１に記憶したＩＤ全てに対して実行される。

[0148] 次に、通信部３３は、ＩＤ発行情報記憶部３１に記憶した複数の第１コー

ドと第１パラメータとをサービス装置S_1に送信する（ステップＳＴ７５）。

[0149] しかる後、サービス装置S_1内の通信部$S_1$８は、ＩＤ発行装置３０から送信された第１コードと第１パラメータとを受けると、これらを利用者情報に対応付けて利用者情報記憶部$S_1$１に書込む（ステップＳＴ７６）。

[0150] また同様に、ＩＤ発行装置３０内のＩＤ発行部３２は、サービス装置S_2向けの第２コード（請求項２における第１のコード）についてもステップＳＴ７４～ＳＴ７６と同様の処理を実行して、第２コードを生成した後に、この第２コードとこの第２コードを生成するときに用いた各種パラメータ（以下、第２パラメータと表記）とをサービス装置S_2に送信する。その後、サービス装置S_2内の通信部$S_2$８は、ＩＤ発行装置３０から送信された第２コードと第２パラメータとを受けると、これらを利用者情報に対応付けて利用者情報記憶部$S_2$１に書込む（ステップＳＴ７７～ＳＴ７９）。

[0151] 以上により、コード配布処理が完了する。

[0152] （２´）連携処理は、連携装置２０及び各サービス装置S_1，S_2により、図７及び以下の各ステップＳＴ８１～ＳＴ９３に示すように実行される。

[0153] 始めに、サービス装置S_1内の暗号化処理部$S_1$４は、利用者からの要求に応じて、この利用者の利用者情報に対応付けられた第１コードを利用者情報記憶部$S_1$１から読み出す（ステップＳＴ８１）。

[0154] 続いて、サービス連携要求部$S_1$７は、暗号化処理部$S_1$４により読み出された第１コードを用いて、サービス装置S_2が保有する情報の取得を通信部$S_1$８を介して連携装置２０に対して要求する（ステップＳＴ８２）。

[0155] 次に、連携装置２０内の再暗号化処理部２５は、ステップＳＴ８２におけるサービス装置S_1からの要求と第１コードとを通信部２６を介して受けると、予め再暗号化鍵記憶部２３に記憶した再暗号化鍵R_{ik}を用いて第１コードを再暗号化する（すなわち、再暗号文データを生成する）（ステップＳＴ８３）。

[0156] 続いて、通信部２６は、生成した再暗号文データをサービス装置S_2に送信し（ステップＳＴ８４）、この再暗号文データを用いてサービス装置S_2が保

有する情報の取得を要求する。

[0157] 次に、サービス装置S_2内の復号処理部S_25は、連携装置２０から送信された再暗号文データを通信部S_28を介して受けると、予め秘密鍵記憶部S_22に記憶した秘密鍵x_kを用いて再暗号文データを復号し、ＩＤを取得する（ステップＳＴ８５）。

[0158] 続いて、通信部S_28は、連携装置２０に対して再暗号化鍵発行装置１０の公開鍵を配布するよう要求する（ステップＳＴ８６）。

[0159] 次に、連携装置２０内の通信部２６は、ステップＳＴ８６におけるサービス装置S_2からの要求を受けると、公開鍵記憶部２２に記憶された再暗号化鍵発行装置１０の公開鍵X_iをサービス装置S_2に送信する（ステップＳＴ８７）。

[0160] 続いて、サービス装置S_2内の暗号化処理部S_24は、連携装置２０から送信された再暗号化鍵発行装置１０の公開鍵X_iを通信部S_28を介して受けると、この公開鍵と予め利用者情報記憶部S_21に記憶した第２パラメータとを用いて、ステップＳＴ８５において復号されたＩＤを暗号化処理して、サービス装置S_2向けの第２´コード（請求項２における第２のコード）を生成する（ステップＳＴ８８）。

[0161] 次に、サービス処理部S_26は、生成した第２´コードと、予め利用者情報記憶部S_21に記憶してあり読み出した第２コードとを比較して、一致するコードから利用者を特定する（ステップＳＴ８９）。

[0162] 続いて、サービス処理部S_26は、特定した利用者の利用者情報と暗号化処理部S_24により生成された第２´コードとを対応付けて利用者情報記憶部S_21に書込む（ステップＳＴ９０）。

[0163] 次に、通信部S_28は、サービス処理部S_26により利用者情報記憶部S_21に記憶した利用者情報を連携情報として連携装置２０に送信する（ステップＳＴ９１）。

[0164] 続いて、連携装置２０内の通信部２６は、サービス装置S_2から送信された連携情報を受けると、この連携情報をサービス装置S_1に送信する（ステップ

ＳＴ９２）。

[0165] しかる後、サービス装置S_1内の通信部$S_1$８は、連携装置２０から送信された連携情報を受信する。これにより、サービス装置S_1は連携情報を取得する（ステップＳＴ９３）。

[0166] 以上説明した第１の実施形態の変形例によれば、前述した第１の実施形態と同様に、再暗号化処理部２５を含む連携装置２０と、暗号化処理部$S_1$４，$S_2$４、復号処理部$S_1$５，$S_2$５及びサービス連携要求部$S_1$７，$S_2$７を含む複数のサービス装置S_1，S_2とを備えた構成により、連携装置２０が各サービス装置S_1，S_2間での連携情報のやり取りの過程でＩＤを紐付けることができないため、連携情報に対してのセキュリティ性を向上させることができる。

[0167] また、再暗号化鍵発行装置１０及び連携装置２０が有する情報を用いて（すなわち、各サービス装置S_1，S_2の秘密情報を必要とせずに）、各サービス装置S_1，S_2間での連携情報のやり取りの過程を後に監査・検証することができる。

[0168] なお、第１の実勢形態の更なる変形例として、図８に示すような構成の連携サービス提供システムを適用することも可能である。この構成は、前述した図１に示す構成をより簡略化したものであり、例えば図９に示すように動作することが可能である。

[0169] このように構成を簡略化することにより、連携装置２０上で監査を行うときには若干の不都合があるものの、連携サービス提供システムを実現するために必要となるシステムコストを低減させることができる。

[0170] ［第２の実施形態］

図１０は第２の実施形態に係る連携サービス提供システムの構成例を示す模式図であり、この連携サービス提供システム１´は前述した第１の実施形態とは異なり、連携サービス提供システム１内からＩＤ発行装置３０を除いた構成となっている。本実施形態は、前述した第１の実施形態の変形例であり、各サービス装置S_1，S_2間において連携する仕組みが既に存在するとし

た上で、連携処理の際に、各サービス装置Ｓ$_1$，Ｓ$_2$間でやり取りするデータを保護するものである。また、各サービス装置Ｓ$_1$，Ｓ$_2$内の連携情報記憶部Ｓ$_1$１′，Ｓ$_2$１′は、前述した第１の実施形態の利用者情報記憶部Ｓ$_1$１，Ｓ$_2$１とは異なり、連携情報（第１の実施形態の利用者情報に相当）を利用者に対応付けて記憶していればよく、利用者を識別するためのＩＤを必ずしも記憶していなくてもよい。

[0171] 以下、前述した第１の実施形態とは異なる（２′′）連携処理について説明する。

[0172] （２′′）連携処理は、連携装置２０及び各サービス装置Ｓ$_1$，Ｓ$_2$により、図１１及び以下の各ステップＳＴ１０１～ＳＴ１１３に示すように実行される。

[0173] 始めに、サービス装置Ｓ$_1$内のサービス連携要求部Ｓ$_1$７は、利用者からの要求に応じて、サービス装置Ｓ$_2$が保有する情報の取得を通信部Ｓ$_1$８を介して連携装置２０に対して要求する（ステップＳＴ１０１）。

[0174] 続いて、連携装置２０内の通信部２６は、ステップＳＴ１０１におけるサービス装置Ｓ$_1$からの要求を受けると、例えば従来の手法を用いて、各サービス装置Ｓ$_1$，Ｓ$_2$間を連携させる連携処理を実行する（ステップＳＴ１０２）。

[0175] 次に、通信部２６は、ステップＳＴ１０２におけるサービス装置Ｓ$_1$からの要求をサービス装置Ｓ$_2$に送信する（ステップＳＴ１０３）。

[0176] 続いて、サービス装置Ｓ$_2$内の通信部Ｓ$_2$８は、連携装置２０から送信されたサービス装置Ｓ$_1$の要求を受けると、ステップＳＴ１０１における利用者に対応した連携情報を連携情報記憶部Ｓ$_2$１′から読み出す（ステップＳＴ１０４）。

[0177] 次に、通信部Ｓ$_2$８は、連携装置２０に対して再暗号化鍵発行装置１０の公開鍵を配布するよう要求する（ステップＳＴ１０５）。

[0178] 続いて、連携装置２０内の通信部２６は、ステップＳＴ１０５におけるサービス装置Ｓ$_2$から送信された要求を受けると、公開鍵記憶部２２に記憶され

た再暗号化鍵発行装置１０の公開鍵X_iをサービス装置S_2に送信する（ステップＳＴ１０６）。

[0179] 次に、サービス装置S_2内の暗号化処理部S_24は、連携装置２０から送信された再暗号化鍵発行装置１０の公開鍵X_iを通信部S_28を介して受けると、この公開鍵を用いてステップＳＴ１０４において読み出した連携情報を暗号化処理して暗号文データを生成する（ステップＳＴ１０７）。

[0180] 続いて、通信部S_28は、生成した暗号文データを連携装置２０に送信する（ステップＳＴ１０８）。

[0181] 次に、連携装置２０内の通信部２６は、サービス装置S_2から送信された暗号文データを受けると、ステップＳＴ１０２の処理と同様に、各サービス装置S_1，S_2間を連携させる連携処理を実行する（ステップＳＴ１０９）。

[0182] 続いて、再暗号化処理部２５は、予め再暗号化鍵記憶部２３に記憶した再暗号化鍵R_{ij}を用いて通信部２６により受信された暗号文データを再暗号化処理して再暗号文データを生成する（ステップＳＴ１１０）。

[0183] 次に、通信部２６は、再暗号化処理部２５により生成された再暗号文データをサービス装置S_1に送信する（ステップＳＴ１１１）。

[0184] 続いて、サービス装置S_1内の復号処理部S_15は、連携装置２０から送信された再暗号文データを通信部S_18を介して受けると、予め秘密鍵記憶部S_12に記憶した秘密鍵x_jを用いて再暗号文データを復号する（ステップＳＴ１１２）。

[0185] しかる後、サービス装置S_1は、連携情報を取得する（ステップＳＴ１１３）。

[0186] 以上説明した第２の実施形態によれば、再暗号化処理部２５を含む連携装置２０と、連携情報記憶部S_11'，S_21'、暗号化処理部S_14，S_24、復号処理部S_15，S_25及びサービス連携要求部S_17，S_27を含む複数のサービス装置S_1，S_2とを備えた構成により、連携装置２０が各サービス装置S_1，S_2間での連携情報のやり取りの過程で連携情報を紐付けることができない上に、各サービス装置S_1，S_2において連携情報を暗号化するため、

連携情報に対してのセキュリティ性をより向上させることができる。

[0187] また、再暗号化鍵発行装置１０及び連携装置２０が有する情報を用いて（すなわち、各サービス装置S_1，S_2の秘密情報を必要とせずに）、各サービス装置S_1，S_2間での連携情報のやり取りの過程を後に監査することができる。

[0188] なお、本実施形態では、各サービス装置S_1，S_2内の連携情報記憶部S_11'，S_21'に記憶された連携情報を再暗号化方式を用いて暗号化したが、これに限定されず、例えば連携情報を共通暗号化方式を用いて暗号化した後に、この共通鍵を再暗号化方式を用いて暗号化するハイブリッド暗号を適用してもよい。

[0189] 以上説明した少なくともひとつの実施形態によれば、再暗号化処理部２５を含む連携装置２０と、暗号化処理部S_14，S_24、復号処理部S_15，S_25及びサービス連携要求部S_17，S_27を含む複数のサービス装置S_1，S_2とを備えた構成により、連携装置上での連携情報の紐付を防止し、かつ連携装置上での後の監査・検証を可能にすることができる。

[0190] なお、上記の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。

[0191] 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。

[0192] 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）等が上記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。

[0193] さらに、各実施形態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。

[0194] また、記憶媒体は１つに限らず、複数の媒体から上記の各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。

[0195] なお、各実施形態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、上記の各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。

[0196] また、各実施形態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。

[0197] なお、本発明のいくつかの実施形態を説明したが、これらの実施形態は、例として提示したものであり、発明の範囲を限定することは意図していない。これら新規な実施形態は、その他の様々な形態で実施されることが可能であり、発明の要旨を逸脱しない範囲で、種々の省略、置き換え、変更を行うことができる。これら実施形態やその変形は、発明の範囲や要旨に含まれるとともに、特許請求の範囲に記載された発明とその均等の範囲に含まれる。

請求の範囲

［請求項1］ 再暗号化鍵発行装置（１０）と、利用者を識別するために発行されたＩＤを用いて前記利用者に対して各種サービスを提供する複数のサービス装置（S_1，S_2）と、これら複数のサービス装置を連携させる連携装置（２０）とが通信可能に接続された連携サービス提供システム（１）であって、

前記連携装置は、

前記再暗号化鍵発行装置及び前記各サービス装置の公開鍵を記憶する第１記憶手段（２２）と、

前記各サービス装置から送信される暗号文データを平文データに復号せずに、別のサービス装置の秘密鍵を用いて復号可能にする再暗号化処理を実現させるための再暗号化鍵を記憶する第２記憶手段（２３）と、

前記各サービス装置から送信される暗号文データを受けると、前記記憶された再暗号化鍵を用いて当該暗号文データを再暗号化処理して再暗号文データを生成する第１生成手段（２５）と、

前記暗号文データを送信したサービス装置とは別のサービス装置に前記生成された再暗号文データを送信する第１送信手段（２６）と、

前記各サービス装置に前記記憶された公開鍵を送信する第２送信手段（２６）と

を備え、

前記各サービス装置は、

発行された前記ＩＤを前記各サービス装置特有の利用者の情報を示す利用者情報に対応付けて記憶する第３記憶手段（$S_1$１，$S_2$１）と、

前記各サービス装置の秘密鍵を記憶する第４記憶手段（$S_1$２，$S_2$２）と、

前記利用者の操作に応じて、前記連携装置内の第１記憶手段に記憶

された再暗号化鍵発行装置の公開鍵を用いて生成された当該利用者のＩＤが暗号化された暗号文データと共に、別のサービス装置に記憶され、かつ当該暗号文データにより示されるＩＤにより特定される利用者の利用者情報を取得したい旨の要求を前記連携装置に送信する第３送信手段（$S_1$７，$S_2$７）と、

前記連携装置から送信された再暗号文データを受けると、前記記憶された秘密鍵を用いて当該再暗号文データを復号し、前記暗号化されたＩＤを取得する取得手段（$S_1$５，$S_2$５）と、

前記取得されたＩＤに対応した利用者情報を前記第３記憶手段から読み出す読出手段（$S_1$４，$S_2$４）と、

前記読み出された利用者情報を前記連携装置を介して別のサービス装置に送信する第４送信手段（$S_1$８，$S_2$８）と

を備えたことを特徴とする連携サービス提供システム。

［請求項2］ 再暗号化鍵発行装置（１０）と、利用者を識別するために発行されたＩＤを用いて前記利用者に対して各種サービスを提供する複数のサービス装置（S_1，S_2）と、これら複数のサービス装置を連携させる連携装置（２０）とが通信可能に接続された連携サービス提供システムで（１）あって、

前記連携装置は、

前記再暗号化鍵発行装置及び前記各サービス装置の公開鍵を記憶する第１記憶手段（２２）と、

前記各サービス装置から送信される暗号文データを平文データに復号せずに、別のサービス装置の秘密鍵を用いて復号可能にする再暗号化処理を実現させるための再暗号化鍵を記憶する第２記憶手段（２３）と、

前記各サービス装置から送信される暗号文データを受けると、前記記憶された再暗号化鍵を用いて当該暗号文データを再暗号化処理して再暗号文データを生成する第１生成手段（２５）と、

前記暗号文データを送信したサービス装置とは別のサービス装置に前記生成された再暗号文データを送信する第１送信手段（２６）と、

前記各サービス装置に前記記憶された公開鍵を送信する第２送信手段（２６）と

を備え、

前記各サービス装置は、

発行された前記ＩＤであって、当該サービス装置に特有な第１のコードと紐付けられているＩＤを前記各サービス装置特有の利用者の情報を示す利用者情報に対応付けて記憶する第３記憶手段（$S_1$１，$S_2$１）と、

前記各サービス装置の秘密鍵を記憶する第４記憶手段（$S_1$２，$S_2$２）と、

前記利用者の操作に応じて、前記連携装置内の第１記憶手段に記憶された再暗号化鍵発行装置の公開鍵を用いて生成された当該利用者のＩＤおよび当該ＩＤに紐付いた前記第１のコードが暗号化された暗号文データと共に、別のサービス装置に記憶され、かつ当該暗号文データにより示されるＩＤにより特定される利用者の利用者情報を取得したい旨の要求を前記連携装置に送信する第３送信手段（$S_1$７，$S_2$７）と、

前記連携装置から送信された再暗号文データを受けると、前記記憶された秘密鍵を用いて当該再暗号文データを復号し、前記暗号化されたＩＤを取得する取得手段（$S_1$５，$S_2$５）と、

前記復号されたＩＤを暗号化して第２のコードを生成する暗号化・生成手段（$S_1$４，$S_2$４）と、

前記第１のコードに対応した利用者情報を前記第３記憶手段から読み出す読出手段（$S_1$６，$S_2$６）と、

前記第１のコードと前記第２のコードとを比較し、前記利用者情報を特定する特定手段（$S_1$６，$S_2$６）と、

前記読み出された利用者情報を前記連携装置を介して別のサービス装置に送信する第４送信手段（$S_1$８，$S_2$８）と

を備えたことを特徴とする連携サービス提供システム。

［請求項3］ 再暗号化鍵発行装置（１０）と、利用者を識別するために発行されたＩＤを用いて前記利用者に対して各種サービスを提供する複数のサービス装置（S_1，S_2）と、これら複数のサービス装置を連携させる連携装置（２０）とが通信可能に接続され、前記各サービス装置が、発行されたＩＤを前記各サービス装置特有の利用者の情報を示す利用者情報に対応付けて記憶する第１記憶手段（$S_1$１，$S_2$１）と、前記各サービス装置の秘密鍵を記憶する第２記憶手段（$S_1$２，$S_2$２）と、前記利用者の操作に応じて、前記連携装置から送信された再暗号化鍵発行装置の公開鍵を用いて、当該利用者のＩＤを暗号化処理して暗号文データを生成する第１生成手段（$S_1$４，$S_2$４）と、前記生成された暗号文データと共に、別のサービス装置に記憶され、かつ当該暗号文データにより示されるＩＤにより特定される利用者の利用者情報を取得したい旨の要求を前記連携装置に送信する第１送信手段（$S_1$７，$S_2$７）と、前記連携装置から送信される再暗号文データを受けると、前記記憶された秘密鍵を用いて当該再暗号文データを復号し、前記暗号化されたＩＤを取得する取得手段（$S_1$５，$S_2$５）と、前記取得されたＩＤに対応した利用者情報を前記第１記憶手段から読み出す読出手段（$S_1$４，$S_2$４）と、前記読み出された利用者情報を前記連携装置を介して別のサービス装置に送信する第２送信手段（$S_1$８，$S_2$８）とを備えた連携サービス提供システム内のサーバ装置であって、

前記サーバ装置は、

前記再暗号化鍵発行装置及び前記各サービス装置の公開鍵を記憶する第３記憶手段（２２）と、

前記各サービス装置から送信される暗号文データを平文データに復

号せずに、別のサービス装置の秘密鍵を用いて復号可能にする再暗号化処理を実現させるための再暗号化鍵を記憶する第４記憶手段（２３）と、

前記各サービス装置から送信される暗号文データを受けると、前記記憶された再暗号化鍵を用いて当該暗号文データを再暗号化処理して再暗号文データを生成する第２生成手段（２５）と、

前記暗号文データを送信したサービス装置とは別のサービス装置に前記生成された再暗号文データを送信する第３送信手段（２６）と、

前記各サービス装置に前記記憶された公開鍵を送信する第４送信手段（２６）と

を備えたことを特徴とするサーバ装置。

［請求項4］ 再暗号化鍵発行装置（１０）と、利用者に対して各種サービスを提供する複数のサービス装置（S_1，S_2）と、これら複数のサービス装置を連携させる連携装置（２０）とが通信可能に接続された連携サービス提供システム（１）であって、

前記連携装置は、

前記再暗号化鍵発行装置及び前記各サービス装置の公開鍵を記憶する第１記憶手段（２２）と、

前記各サービス装置から送信される暗号文データを平文データに復号せずに、別のサービス装置の秘密鍵を用いて復号可能にする再暗号化処理を実現させるための再暗号化鍵を記憶する第２記憶手段（２３）と、

前記各サービス装置から送信される暗号文データを受けると、前記記憶された再暗号化鍵を用いて当該暗号文データを再暗号化処理して再暗号文データを生成する第１生成手段（２５）と、

前記暗号文データを送信したサービス装置とは別のサービス装置に前記生成された再暗号文データを送信する第１送信手段（２６）と、

前記各サービス装置に前記記憶された公開鍵を送信する第２送信手

段（２６）と

を備え、

前記各サービス装置は、

前記各サービス装置間で連携させる連携情報を前記利用者に対応付けて記憶する第３記憶手段（$S_1$１，$S_2$１）と、

前記各サービス装置の秘密鍵を記憶する第４記憶手段（$S_1$２，$S_2$２）と、

前記利用者の操作に応じて、前記連携装置から送信された再暗号化鍵発行装置の公開鍵を用いて、当該利用者に対応付けられた連携情報を暗号化処理して暗号文データを生成する第２生成手段（$S_1$４，$S_2$４）と、

前記生成された暗号文データを前記連携装置に送信する第３送信手段（$S_1$８，$S_2$８）と、

前記連携装置から送信された再暗号文データを受けると、前記記憶された秘密鍵を用いて当該再暗号文データを復号し、前記暗号化された連携情報を取得する取得手段（$S_1$５，$S_2$５）と

を備えたことを特徴とする連携サービス提供システム。

［請求項5］ 再暗号化鍵発行装置（１０）と、利用者に対して各種サービスを提供する複数のサービス装置（S_1，S_2）と、これら複数のサービス装置を連携させる連携装置（２０）とが通信可能に接続され、前記各サービス装置が、前記各サービス装置間で連携させる連携情報を前記利用者に対応付けて記憶する第１記憶手段（$S_1$１，$S_2$１）と、前記各サービス装置の秘密鍵を記憶する第２記憶手段（$S_1$２，$S_2$２）と、前記利用者の操作に応じて、前記連携装置から送信される再暗号化鍵発行装置の公開鍵を用いて、当該利用者に対応付けられた連携情報を暗号化処理して暗号文データを生成する第１生成手段（$S_1$４，$S_2$４）と、前記生成された暗号文データを前記連携装置に送信する第１送信手段（$S_1$８，$S_2$８）と、前記連携装置から送信される

再暗号文データを受けると、前記記憶された秘密鍵を用いて当該再暗号文データを復号し、前記暗号化された連携情報を取得する取得手段（$S_1$５，$S_2$５）とを備えた連携サービス提供システム内のサーバ装置であって、

前記サーバ装置は、

前記再暗号化鍵発行装置及び前記各サービス装置の公開鍵を記憶する第３記憶手段（２２）と、

前記各サービス装置から送信される暗号文データを平文データに復号せずに、別のサービス装置の秘密鍵を用いて復号可能にする再暗号化処理を実現させるための再暗号化鍵を記憶する第４記憶手段（２３）と、

前記各サービス装置から送信される暗号文データを受けると、前記記憶された再暗号化鍵を用いて当該暗号文データを再暗号化処理して再暗号文データを生成する第２生成手段（２５）と、

前記暗号文データを送信したサービス装置とは別のサービス装置に前記生成された再暗号文データを送信する第３送信手段（２６）と、

前記各サービス装置に前記記憶された公開鍵を送信する第４送信手段（２６）と

を備えたことを特徴とするサーバ装置。