(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2008-242585
(P2008-242585A)
(43)公開日　平成20年10月9日(2008.10.9)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/20	(2006.01)	G06F	15/00	330A	5B285
H04L 9/32	(2006.01)	H04L	9/00	673A	5J104

審査請求 未請求　請求項の数 8　ＯＬ　（全 15 頁）

(21)出願番号　特願2007-79016(P2007-79016)
(22)出願日　平成19年3月26日(2007.3.26)

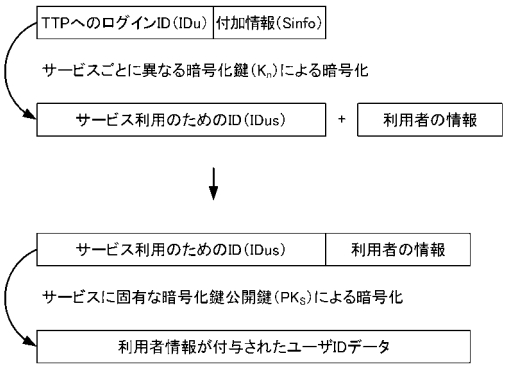
（出願人による申告）平成１８年度、総務省、「認証機能を具備するサービスプラットフォーム技術」委託研究、産業活力再生特別措置法第３０条の適用を受ける特許出願

(71)出願人　599108264
株式会社ＫＤＤＩ研究所
埼玉県ふじみ野市大原二丁目１番１５号
(74)代理人　100106002
弁理士　正林　真之
(74)代理人　100114775
弁理士　高岡　亮一
(74)代理人　100120891
弁理士　林　一好
(74)代理人　100122426
弁理士　加藤　清志
(72)発明者　渡辺　龍
埼玉県ふじみ野市大原二丁目１番１５号
株式会社ＫＤＤＩ研究所内

最終頁に続く

(54)【発明の名称】サービス利用識別情報生成装置、サービス利用識別情報生成システム、サービス利用識別情報生成方法およびプログラム

(57)【要約】
【課題】ＴＴＰおよびサービス提供サーバの通信負担を抑えつつ、第三者に秘匿した状態で必要な利用者情報を入手できる。
【解決手段】受信したユーザのログイン情報に付加情報を付与し、ユーザのログイン情報に付加情報を付与した情報をユーザが提供を受けるサービスごとに異なる暗号化鍵で暗号化する。そして、暗号化された情報に利用者に関する情報を付与し、暗号化された情報に利用者に関する情報を付与した情報をサービス利用識別情報生成装置固有の暗号化鍵で暗号化する。
【選択図】図４



【特許請求の範囲】
【請求項１】
ユーザ端末と、サービス提供者が管理するサービス提供サーバとにネットワークを介して接続され、ユーザによるサービス利用の際に、前記サービス提供サーバがユーザを識別するためのサービス利用識別情報を生成するサービス利用識別情報生成装置であって、
ユーザのログイン情報を受信する受信手段と、
該受信したユーザのログイン情報に付加情報を付与して、前記ユーザが提供を受けるサービスごとに異なる暗号化鍵で暗号化する暗号化処理手段と、
該暗号化処理手段において暗号化された情報に利用者に関する情報を付与し、装置固有の暗号化鍵で暗号化してサービス利用識別情報を生成するサービス利用識別情報生成手段と、
該生成したサービス利用識別情報を前記サービス提供サーバに送信する送信手段と、
を備えたことを特徴とするサービス利用識別情報生成装置。
【請求項２】
ユーザ端末と、サービス提供者が管理するサービス提供サーバと、信頼できる第三者機関が管理しユーザ認証を行うとともにユーザがサービスを利用するためのサービス利用識別情報を生成する管理サーバとからなるサービス利用識別情報生成システムであって、
前記管理サーバが、ユーザのログイン情報を受信する受信手段と、
該受信したユーザのログイン情報に付加情報を付与して、前記ユーザが提供を受けるサービスごとに異なる暗号化鍵で暗号化する暗号化処理手段と、
該暗号化処理手段において暗号化された情報に利用者に関する情報を付与し、信頼できる第三者機関固有の暗号化鍵で暗号化してサービス利用識別情報を生成するサービス利用識別情報生成手段と、
該生成されたサービス利用識別情報を前記サービス提供サーバに送信する送信手段と、
を備えたことを特徴とするサービス利用識別情報生成システム。
【請求項３】
ユーザ端末と、サービス提供者が管理するサービス提供サーバとにネットワークを介して接続され、ユーザによるサービス利用の際に、前記サービス提供サーバがユーザを識別するためのサービス利用識別情報を生成するサービス利用識別情報生成装置であって、
ユーザのログイン情報を受信する受信手段と、
該受信したユーザのログイン情報に付加情報を付与して、前記ユーザが提供を受けるサービスごとに異なる暗号化鍵で暗号化する暗号化処理手段と、
該暗号化処理手段において暗号化された情報に利用者に関する情報を付与し、前記サービス提供サーバとの間で共有された暗号化鍵で暗号化してサービス利用識別情報を生成するサービス利用識別情報生成手段と、
該生成したサービス利用識別情報を前記サービス提供サーバに送信する送信手段と、
を備えたことを特徴とするサービス利用識別情報生成装置。
【請求項４】
ユーザ端末と、サービス提供者が管理するサービス提供サーバと、信頼できる第三者機関が管理しユーザ認証を行うとともにユーザがサービスを利用するためのサービス利用識別情報を生成する管理サーバとからなるサービス利用識別情報生成システムであって、
前記管理サーバが、ユーザのログイン情報を受信する受信手段と、
該受信したユーザのログイン情報に付加情報を付与して、前記ユーザが提供を受けるサービスごとに異なる暗号化鍵で暗号化する暗号化処理手段と、
該暗号化処理手段において暗号化された情報に利用者に関する情報を付与し、前記サービス提供サーバと前記信頼できる第三者機関との間で共有された暗号化鍵で暗号化してサービス利用識別情報を生成するサービス利用識別情報生成手段と、
該生成されたサービス利用識別情報を前記サービス提供サーバに送信する送信手段と、
を備えたことを特徴とするサービス利用識別情報生成システム。
【請求項５】

ユーザ端末と、サービス提供者が管理するサービス提供サーバとにネットワークを介して接続され、ユーザによるサービス利用の際に、前記サービス提供サーバがユーザを識別するためのサービス利用識別情報を生成するサービス利用識別情報生成装置におけるサービス利用識別情報生成方法であって、
受信したユーザのログイン情報に付加情報を付与する第１のステップと、
該ユーザのログイン情報に付加情報を付与した情報を前記ユーザが提供を受けるサービスごとに異なる暗号化鍵で暗号化する第２のステップと、
該暗号化された情報に利用者に関する情報を付与する第３のステップと、
該暗号化された情報に利用者に関する情報を付与した情報をサービス利用識別情報生成装置固有の暗号化鍵で暗号化する第４のステップと、
を有することを特徴とするサービス利用識別情報生成方法。
【請求項６】
ユーザ端末と、サービス提供者が管理するサービス提供サーバとにネットワークを介して接続され、ユーザによるサービス利用の際に、前記サービス提供サーバがユーザを識別するためのサービス利用識別情報を生成するサービス利用識別情報生成装置におけるサービス利用識別情報生成方法であって、
受信したユーザのログイン情報に付加情報を付与する第１のステップと、
該ユーザのログイン情報に付加情報を付与した情報を前記ユーザが提供を受けるサービスごとに異なる暗号化鍵で暗号化する第２のステップと、
該暗号化された情報に利用者に関する情報を付与する第３のステップと、
該暗号化された情報に利用者に関する情報を付与した情報を前記サービス提供サーバとサービス利用識別情報生成装置との間で共有された暗号化鍵で暗号化する第４のステップと、
を有することを特徴とするサービス利用識別情報生成方法。
【請求項７】
ユーザ端末と、サービス提供者が管理するサービス提供サーバとにネットワークを介して接続され、ユーザによるサービス利用の際に、前記サービス提供サーバがユーザを識別するためのサービス利用識別情報を生成するサービス利用識別情報生成装置におけるサービス利用識別情報生成方法をコンピュータに実行させるためのプログラムであって、
受信したユーザのログイン情報に付加情報を付与する第１のステップと、
該ユーザのログイン情報に付加情報を付与した情報を前記ユーザが提供を受けるサービスごとに異なる暗号化鍵で暗号化する第２のステップと、
該暗号化された情報に利用者に関する情報を付与する第３のステップと、
該暗号化された情報に利用者に関する情報を付与した情報をサービス利用識別情報生成装置固有の暗号化鍵で暗号化する第４のステップと、
をコンピュータに実行させるためのプログラム。
【請求項８】
ユーザ端末と、サービス提供者が管理するサービス提供サーバとにネットワークを介して接続され、ユーザによるサービス利用の際に、前記サービス提供サーバがユーザを識別するためのサービス利用識別情報を生成するサービス利用識別情報生成装置におけるサービス利用識別情報生成方法をコンピュータに実行させるためのプログラムであって、
受信したユーザのログイン情報に付加情報を付与する第１のステップと、
該ユーザのログイン情報に付加情報を付与した情報を前記ユーザが提供を受けるサービスごとに異なる暗号化鍵で暗号化する第２のステップと、
該暗号化された情報に利用者に関する情報を付与する第３のステップと、
該暗号化された情報に利用者に関する情報を付与した情報を前記サービス提供サーバとサービス利用識別情報生成装置との間で共有された暗号化鍵で暗号化する第４のステップと、
をコンピュータに実行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、ユーザＩＤに対して付加的な情報および利用者に関する情報を付与するとともに、この情報を第三者に対して秘匿化するサービス利用識別情報生成装置、サービス利用識別情報生成システム、サービス利用識別情報生成方法およびプログラムに関する。
【背景技術】
【０００２】
従来、図７に示すように、インターネット上でサービス利用の利便性を向上させる技術として、ユーザ端末１００と、信頼のおける第三者機関（ＴＴＰ：Ｔｒｕｓｔｅｄ　Ｔｈｉｒｄ　Ｐａｒｔｙ）２００と、サービス提供サーバ３００とからなるシステムにおいて、このＴＴＰ２００を利用したシングルサインオン（ＳＳＯ：Ｓｉｎｇｌｅ　Ｓｉｇｎ　Ｏｎ）と呼ばれる技術がある。
【０００３】
このＴＴＰ２００を利用するＳＳＯ技術では、その利用にあたり、ユーザのプライバシーを保護するために、ユーザが利用するサービス（サービス提供者）に対して、サービスごとにＩＤ（Ｉｄｅｎｔｉｆｉｅｒ）を変更することが必要とされる。これは、異なるサービスに対して同じＩＤを利用させてしまうと、サービス提供側が結託した場合に、それぞれのサービスにおけるユーザの行動を付き合わせることができてしまうためである。
【０００４】
また、サービスごとにＩＤを変更することに加えて、接続ごとにもＩＤを変更することが必要とされている。すなわち、同じサービスであっても、常に同じＩＤで利用し続けた場合には、そのユーザの行動をトレースできてしまうためである。この場合、特定のユーザの行動をトレースできることを利用して、ショッピングサイトのように、お勧め商品の紹介（リコメンデーションサービスあるいは、パーソナライゼーションサービスと呼ぶ）を提供することも可能となるが、その一方で、ユーザによっては、このようにユーザ自身の行動が把握されることを嫌がる可能性もある。
【０００５】
さらに、このような、ＴＴＰ２００を利用したＳＳＯ技術の利用にあたり、ＴＴＰ２００が本人の特定を実施できるよう、ＩＤのユーザと本人（この場合は、ＴＴＰ２００へのログインＩＤ）との対応関係をＴＴＰ２００が把握できることも併せて必要とされている。このため、ＴＴＰ２００でのサービス利用時のＩＤの管理にあたり、ＴＴＰ２００での管理コストを低減することを目的として、暗号化の技法を利用する手法が提案されている（例えば、特許文献１参照。）。
【０００６】
この従来のＩＤ管理手法では、ＴＴＰ２００へのログインＩＤに生成日時といった動的な情報や、固定のビット列などの静的な情報を付加した後に暗号化を施したものをサービス利用のためのＩＤとして生成している。このため、ユーザとＩＤとの関係を把握するには、新たに生成したサービス利用のためのＩＤを、生成の際に利用した暗号化鍵を用いて復号してやればよい。そのため、ＴＴＰ２００自身では、ユーザ（ユーザのＴＴＰ２００へのログインＩＤ）と新たに生成したサービス利用のためのＩＤとの対応関係を保持する必要はなく、ＴＴＰ２００が管理すべき情報は、ＩＤの生成に利用した鍵のみとなる。したがって、ＴＴＰ２００における管理コストを低減することができる。
【０００７】
また、上記従来のＩＤ管理手法においては、ＩＤ生成に利用した鍵が漏洩した際のリスクを低減するために、サービスごとに利用する暗号化鍵を変更する手法が提案されている。そのため、鍵が漏洩した場合でも、その被害はそのサービスに限定でき、被害が他のサービスに波及することが防げるようになっている。
【特許文献１】特開２００６－２４４４２０号公報
【発明の開示】
【発明が解決しようとする課題】

【０００８】
しかしながら、上記従来のＩＤ管理手法は、サービス提供者が、自身のサービスの利用者を識別するための手法であり、識別子に利用者に関する情報は付与されてはいない。このため、サービス提供者がユーザの情報を取得するためには、別途、サービス提供者とＴＴＰ（あるいは、ユーザの情報の管理元）とが通信を行なう必要があるという問題がある。また、別途、利用者の情報を証明するための属性証明書などを利用する方式も提案されているが、この場合も、識別子の取得とは別に、通信が発生するという問題がある。
【０００９】
そこで、本発明は、上記の課題に鑑みてなされたものであり、ＴＴＰおよびサービス提供サーバの通信負担を抑えつつ、第三者に秘匿した状態で必要な利用者情報を入手できるサービス利用識別情報生成装置、サービス利用識別情報生成システム、サービス利用識別情報生成方法およびプログラムを提供することを目的とする。
【課題を解決するための手段】
【００１０】
本発明は、上述の課題を解決するために以下の事項を提案している。
（１）本発明は、ユーザ端末（例えば、図１のユーザ端末１００に相当）と、サービス提供者が管理するサービス提供サーバ（例えば、図１のサービス提供サーバ３００に相当）とにネットワークを介して接続され、ユーザによるサービス利用の際に、前記サービス提供サーバがユーザを識別するためのサービス利用識別情報を生成するサービス利用識別情報生成装置であって、ユーザのログイン情報を受信する受信手段（例えば、図２の受信部２１に相当）と、該受信したユーザのログイン情報に付加情報を付与して、前記ユーザが提供を受けるサービスごとに異なる暗号化鍵で暗号化する暗号化処理手段（例えば、図２の暗号化部２２に相当）と、該暗号化処理手段において暗号化された情報に利用者に関する情報を付与し、装置固有の暗号化鍵で暗号化してサービス利用識別情報を生成するサービス利用識別情報生成手段（例えば、図２のサービス利用識別情報生成部２４に相当）と、該生成したサービス利用識別情報を前記サービス提供サーバに送信する送信手段（例えば、図２の送信部２５に相当）と、を備えたことを特徴とするサービス利用識別情報生成装置を提案している。
【００１１】
この発明によれば、受信手段がユーザのログイン情報を受信し、暗号化処理手段が、受信したユーザのログイン情報に付加情報を付与して、ユーザが提供を受けるサービスごとに異なる暗号化鍵で暗号化を行う。そして、サービス利用識別情報生成手段が、暗号化処理手段において暗号化された情報に利用者に関する情報を付与し、装置固有の暗号化鍵で暗号化してサービス利用識別情報を生成し、送信手段が生成したサービス利用識別情報をサービス提供サーバに送信する。したがって、サービス利用識別情報生成装置が、サービスごとに異なる暗号化鍵を用いてＩＤを生成するにあたり、利用者に関する情報を、生成したＩＤ自身に付与し、さらに、全体を、装置固有の暗号化鍵で暗号化するため、利用者に関する情報をＩＤの生成を行ったＴＴＰおよび情報の提供を受けるサービス提供者サーバ以外の者に対して、秘匿化することができる。
【００１２】
（２）本発明は、ユーザ端末（例えば、図１のユーザ端末１００に相当）と、サービス提供者が管理するサービス提供サーバ（例えば、図１のサービス提供サーバ３００に相当）と、信頼できる第三者機関が管理しユーザ認証を行うとともにユーザがサービスを利用するためのサービス利用識別情報を生成する管理サーバとからなるサービス利用識別情報生成システムであって、前記管理サーバが、ユーザのログイン情報を受信する受信手段（例えば、図２の受信部２１に相当）と、該受信したユーザのログイン情報に付加情報を付与して、前記ユーザが提供を受けるサービスごとに異なる暗号化鍵で暗号化する暗号化処理手段（例えば、図２の暗号化部２２に相当）と、該暗号化処理手段において暗号化された情報に利用者に関する情報を付与し、信頼できる第三者機関固有の暗号化鍵で暗号化してサービス利用識別情報を生成するサービス利用識別情報生成手段（例えば、図２のサー

ビス利用識別情報生成部２４に相当）と、該生成されたサービス利用識別情報を前記サービス提供サーバに送信する送信手段（例えば、図２の送信部２５に相当）と、を備えたことを特徴とするサービス利用識別情報生成システムを提案している。

【００１３】

この発明によれば、管理サーバ内の受信手段がユーザのログイン情報を受信し、暗号化処理手段が、受信したユーザのログイン情報に付加情報を付与して、ユーザが提供を受けるサービスごとに異なる暗号化鍵で暗号化を行う。そして、サービス利用識別情報生成手段が、暗号化処理手段において暗号化された情報に利用者に関する情報を付与し、装置固有の暗号化鍵で暗号化してサービス利用識別情報を生成し、送信手段が生成したサービス利用識別情報をサービス提供サーバに送信する。したがって、管理サーバが、サービスごとに異なる暗号化鍵を用いてＩＤを生成するにあたり、利用者に関する情報を、生成したＩＤ自身に付与し、さらに、全体を、装置固有の暗号化鍵で暗号化するため、利用者に関する情報をＩＤの生成を行ったＴＴＰおよび情報の提供を受けるサービス提供者サーバ以外の者に対して、秘匿化することができる。また、サービス提供サーバは、自身が持つ秘密鍵により復号化を行い、サービス利用のためのＩＤと、利用者情報とを個別の通信を行うことなく取得することができる。

【００１４】

（３）本発明は、ユーザ端末（例えば、図１のユーザ端末１００に相当）と、サービス提供者が管理するサービス提供サーバ（例えば、図１のサービス提供サーバ３００に相当）とにネットワークを介して接続され、ユーザによるサービス利用の際に、前記サービス提供サーバがユーザを識別するためのサービス利用識別情報を生成するサービス利用識別情報生成装置であって、ユーザのログイン情報を受信する受信手段（例えば、図２の受信部２１に相当）と、該受信したユーザのログイン情報に付加情報を付与して、前記ユーザが提供を受けるサービスごとに異なる暗号化鍵で暗号化する暗号化処理手段（例えば、図２の暗号化部２２に相当）と、該暗号化処理手段において暗号化された情報に利用者に関する情報を付与し、前記サービス提供サーバとの間で共有された暗号化鍵で暗号化してサービス利用識別情報を生成するサービス利用識別情報生成手段（例えば、図２のサービス利用識別情報生成部２４に相当）と、該生成したサービス利用識別情報を前記サービス提供サーバに送信する送信手段（例えば、図２の送信部２５に相当）と、を備えたことを特徴とするサービス利用識別情報生成装置を提案している。

【００１５】

この発明によれば、受信手段がユーザのログイン情報を受信し、暗号化処理手段が、受信したユーザのログイン情報に付加情報を付与して、ユーザが提供を受けるサービスごとに異なる暗号化鍵で暗号化を行う。そして、サービス利用識別情報生成手段が、暗号化処理手段において暗号化された情報に利用者に関する情報を付与し、サービス提供サーバとの間で共有された暗号化鍵で暗号化してサービス利用識別情報を生成し、送信手段が生成したサービス利用識別情報をサービス提供サーバに送信する。したがって、サービス利用識別情報生成装置が、サービスごとに異なる暗号化鍵を用いてＩＤを生成するにあたり、利用者に関する情報を、生成したＩＤ自身に付与し、さらに、全体を、サービス提供サーバとの間で共有された暗号化鍵で暗号化するため、利用者に関する情報をＩＤの生成を行ったＴＴＰおよび情報の提供を受けるサービス提供者サーバ以外の者に対して、秘匿化することができる。

【００１６】

（４）本発明は、ユーザ端末（例えば、図１のユーザ端末１００に相当）と、サービス提供者が管理するサービス提供サーバ（例えば、図１のサービス提供サーバ３００に相当）と、信頼できる第三者機関が管理しユーザ認証を行うとともにユーザがサービスを利用するためのサービス利用識別情報を生成する管理サーバとからなるサービス利用識別情報生成システムであって、前記管理サーバが、ユーザのログイン情報を受信する受信手段（例えば、図２の受信部２１に相当）と、該受信したユーザのログイン情報に付加情報を付与して、前記ユーザが提供を受けるサービスごとに異なる暗号化鍵で暗号化する暗号化処

理手段（例えば、図２の暗号化部２２に相当）と、該暗号化処理手段において暗号化された情報に利用者に関する情報を付与し、前記サービス提供サーバと前記信頼できる第三者機関との間で共有された暗号化鍵で暗号化してサービス利用識別情報を生成するサービス利用識別情報生成手段（例えば、図２のサービス利用識別情報生成部２４に相当）と、該生成されたサービス利用識別情報を前記サービス提供サーバに送信する送信手段（例えば、図２の送信部２５に相当）と、を備えたことを特徴とするサービス利用識別情報生成システムを提案している。

【００１７】

この発明によれば、管理サーバ内の受信手段がユーザのログイン情報を受信し、暗号化処理手段が、受信したユーザのログイン情報に付加情報を付与して、ユーザが提供を受けるサービスごとに異なる暗号化鍵で暗号化を行う。そして、サービス利用識別情報生成手段が、暗号化処理手段において暗号化された情報に利用者に関する情報を付与し、サービス提供サーバと信頼できる第三者機関との間で共有された暗号化鍵で暗号化してサービス利用識別情報を生成し、送信手段が生成したサービス利用識別情報をサービス提供サーバに送信する。したがって、管理サーバが、サービスごとに異なる暗号化鍵を用いてＩＤを生成するにあたり、利用者に関する情報を、生成したＩＤ自身に付与し、さらに、全体を、サービス提供サーバと信頼できる第三者機関との間で共有された暗号化鍵で暗号化するため、利用者に関する情報を、ＩＤの生成を行ったＴＴＰおよび情報の提供を受けるサービス提供者サーバ以外の者に対して、秘匿化することができる。また、サービス提供サーバは、サービス提供サーバと信頼できる第三者機関との間で共有された暗号化鍵により復号化を行い、サービス利用のためのＩＤと、利用者情報とを個別の通信を行うことなく取得することができる。

【００１８】

（５）本発明は、ユーザ端末と、サービス提供者が管理するサービス提供サーバとにネットワークを介して接続され、ユーザによるサービス利用の際に、前記サービス提供サーバがユーザを識別するためのサービス利用識別情報を生成するサービス利用識別情報生成装置におけるサービス利用識別情報生成方法であって、受信したユーザのログイン情報に付加情報を付与する第１のステップ（例えば、図３のステップＳ１０１、Ｓ１０２に相当）と、該ユーザのログイン情報に付加情報を付与した情報を前記ユーザが提供を受けるサービスごとに異なる暗号化鍵で暗号化する第２のステップ（例えば、図３のステップＳ１０３に相当）と、該暗号化された情報に利用者に関する情報を付与する第３のステップ（例えば、図３のステップＳ１０４に相当）と、該暗号化された情報に利用者に関する情報を付与した情報をサービス利用識別情報生成装置固有の暗号化鍵で暗号化する第４のステップ（例えば、図３のステップＳ１０５に相当）と、を有することを特徴とするサービス利用識別情報生成方法を提案している。

【００１９】

この発明によれば、受信したユーザのログイン情報に付加情報を付与し、ユーザのログイン情報に付加情報を付与した情報をユーザが提供を受けるサービスごとに異なる暗号化鍵で暗号化する。そして、暗号化された情報に利用者に関する情報を付与し、この暗号化された情報に利用者に関する情報を付与した情報をサービス利用識別情報生成装置固有の暗号化鍵で暗号化する。したがって、サービスごとに異なる暗号化鍵を用いてＩＤを生成するにあたり、利用者に関する情報を、生成したＩＤ自身に付与し、さらに、全体を、サービス利用識別情報生成装置固有の暗号化鍵で暗号化するため、利用者に関する情報をＩＤの生成を行ったＴＴＰおよび情報の提供を受けるサービス提供者サーバ以外の者に対して、秘匿化することができる。

【００２０】

（６）本発明は、ユーザ端末と、サービス提供者が管理するサービス提供サーバとにネットワークを介して接続され、ユーザによるサービス利用の際に、前記サービス提供サーバがユーザを識別するためのサービス利用識別情報を生成するサービス利用識別情報生成装置におけるサービス利用識別情報生成方法であって、受信したユーザのログイン情報に

付加情報を付与する第１のステップ（例えば、図３のステップＳ１０１、Ｓ１０２に相当）と、該ユーザのログイン情報に付加情報を付与した情報を前記ユーザが提供を受けるサービスごとに異なる暗号化鍵で暗号化する第２のステップ（例えば、図３のステップＳ１０３に相当）と、該暗号化された情報に利用者に関する情報を付与する第３のステップ（例えば、図３のステップＳ１０４に相当）と、該暗号化された情報に利用者に関する情報を付与した情報を前記サービス提供サーバとサービス利用識別情報生成装置との間で共有された暗号化鍵で暗号化する第４のステップ（例えば、図３のステップＳ１０５に相当）と、を有することを特徴とするサービス利用識別情報生成方法を提案している。

【００２１】

この発明によれば、受信したユーザのログイン情報に付加情報を付与し、ユーザのログイン情報に付加情報を付与した情報をユーザが提供を受けるサービスごとに異なる暗号化鍵で暗号化する。そして、暗号化された情報に利用者に関する情報を付与し、暗号化された情報に利用者に関する情報を付与した情報をサービス提供サーバとの間で共有された暗号化鍵で暗号化する。したがって、サービスごとに異なる暗号化鍵を用いてＩＤを生成するにあたり、利用者に関する情報を、生成したＩＤ自身に付与し、さらに、全体を、サービス提供サーバとの間で共有された暗号化鍵で暗号化するため、利用者に関する情報をＩＤの生成を行ったＴＴＰおよび情報の提供を受けるサービス提供者サーバ以外の者に対して、秘匿化することができる。

【００２２】

（７）本発明は、ユーザ端末と、サービス提供者が管理するサービス提供サーバとにネットワークを介して接続され、ユーザによるサービス利用の際に、前記サービス提供サーバがユーザを識別するためのサービス利用識別情報を生成するサービス利用識別情報生成装置におけるサービス利用識別情報生成方法をコンピュータに実行させるためのプログラムであって、受信したユーザのログイン情報に付加情報を付与する第１のステップ（例えば、図３のステップＳ１０１、Ｓ１０２に相当）と、該ユーザのログイン情報に付加情報を付与した情報を前記ユーザが提供を受けるサービスごとに異なる暗号化鍵で暗号化する第２のステップ（例えば、図３のステップＳ１０３に相当）と、該暗号化された情報に利用者に関する情報を付与する第３のステップ（例えば、図３のステップＳ１０４に相当）と、該暗号化された情報に利用者に関する情報を付与した情報をサービス利用識別情報生成装置固有の暗号化鍵で暗号化する第４のステップ（例えば、図３のステップＳ１０５に相当）と、をコンピュータに実行させるためのプログラムを提案している。

【００２３】

この発明によれば、受信したユーザのログイン情報に付加情報を付与し、ユーザのログイン情報に付加情報を付与した情報をユーザが提供を受けるサービスごとに異なる暗号化鍵で暗号化する。そして、暗号化された情報に利用者に関する情報を付与し、暗号化された情報に利用者に関する情報を付与した情報をサービス利用識別情報生成装置固有の暗号化鍵で暗号化する。したがって、サービスごとに異なる暗号化鍵を用いてＩＤを生成するにあたり、利用者に関する情報を、生成したＩＤ自身に付与し、さらに、全体を、サービス利用識別情報生成装置固有の暗号化鍵で暗号化するため、利用者に関する情報をＩＤの生成を行ったＴＴＰおよび情報の提供を受けるサービス提供者サーバ以外の者に対して、秘匿化することができる。

【００２４】

（８）本発明は、ユーザ端末と、サービス提供者が管理するサービス提供サーバとにネットワークを介して接続され、ユーザによるサービス利用の際に、前記サービス提供サーバがユーザを識別するためのサービス利用識別情報を生成するサービス利用識別情報生成装置におけるサービス利用識別情報生成方法をコンピュータに実行させるためのプログラムであって、受信したユーザのログイン情報に付加情報を付与する第１のステップ（例えば、図３のステップＳ１０１、Ｓ１０２に相当）と、該ユーザのログイン情報に付加情報を付与した情報を前記ユーザが提供を受けるサービスごとに異なる暗号化鍵で暗号化する第２のステップ（例えば、図３のステップＳ１０３に相当）と、該暗号化された情報に利

用者に関する情報を付与する第３のステップ（例えば、図３のステップＳ１０４に相当）と、該暗号化された情報に利用者に関する情報を付与した情報を前記サービス提供サーバとサービス利用識別情報生成装置との間で共有された暗号化鍵で暗号化する第４のステップ（例えば、図３のステップＳ１０５に相当）と、をコンピュータに実行させるためのプログラムを提案している。

【００２５】

この発明によれば、受信したユーザのログイン情報に付加情報を付与し、ユーザのログイン情報に付加情報を付与した情報をユーザが提供を受けるサービスごとに異なる暗号化鍵で暗号化する。そして、暗号化された情報に利用者に関する情報を付与し、暗号化された情報に利用者に関する情報を付与した情報をサービス提供サーバとの間で共有された暗号化鍵で暗号化する。したがって、サービスごとに異なる暗号化鍵を用いてＩＤを生成するにあたり、利用者に関する情報を、生成したＩＤ自身に付与し、さらに、全体を、サービス提供サーバとの間で共有された暗号化鍵で暗号化するため、利用者に関する情報をＩＤの生成を行ったＴＴＰおよび情報の提供を受けるサービス提供者サーバ以外の者に対して、秘匿化することができる。

【発明の効果】

【００２６】

本発明によれば、ＩＤ自身に情報を付与することができ、しかも、第三者にはその情報が理解できないという効果がある。また、ＩＤ自身に利用者の情報が付与されているので、サービス提供者とＴＴＰの間で、利用者の情報取得に本来必要な通信を行なう必要がないという効果がある。

【００２７】

また、本発明によれば、付与した情報を隠蔽するための暗号化処理にあたり、サービス提供者の認証に利用する公開鍵証明書を添付した公開鍵を利用できるため、付加的情報を必要としないという効果がある。さらに、上記の公開鍵の利用の他に、ＴＴＰとサービス提供者間で事前に共有された共有鍵を利用することもできるが、この場合、必要な情報の増加量としては、サービスひとつに対して、暗号化のための鍵ひとつであるため、サービス提供者、ＴＴＰ双方にとって大きな負担とはならないという効果がある。

【発明を実施するための最良の形態】

【００２８】

以下、本発明の実施形態について、図面を用いて、詳細に説明する。

なお、本実施形態における構成要素は適宜、既存の構成要素等との置き換えが可能であり、また、他の既存の構成要素との組合せを含む様々なバリエーションが可能である。したがって、本実施形態の記載をもって、特許請求の範囲に記載された発明の内容を限定するものではない。

【００２９】

＜サービス利用識別情報生成システムの構成＞

本実施形態に係るサービス利用識別情報生成システムは、図１に示すように、ユーザ端末１００と、サービス利用識別情報生成装置または管理サーバとしてのＴＴＰ２００と、サービス提供サーバ３００とから構成され、これらユーザ端末１００、管理サーバとしてのＴＴＰ２００、サービス提供サーバ３００は、それぞれネットワークを介して接続されている。

【００３０】

ユーザ端末１００は、サービス提供サーバ３００に対する接続要求をサービス利用識別情報生成装置または管理サーバとしてのＴＴＰ２００に送信する。また、サービスの提供をはじめて受ける場合には、サービス利用識別情報生成装置または管理サーバとしてのＴＴＰ２００に対して、ＩＤの生成要求を発行し、管理サーバとしてのＴＴＰ２００から取得したサービス利用ＩＤに基づき、サービス提供サーバ３００によるサービスの提供を受ける。

【００３１】

サービス利用識別情報生成装置または管理サーバとしてのＴＴＰ２００は、信頼のおける第三者機関が管理するサーバであって、その詳細な構成については後述する。本実施形態においては、図２における受信部２１が、ユーザ端末１００からログイン情報を受信し、暗号化部２２が、受信したユーザのログイン情報に付加情報を付与して、ユーザが提供を受けるサービスごとに異なる暗号化鍵で暗号化を行う。そして、サービス利用識別情報生成部２４が、暗号化部２２において暗号化された情報に利用者に関する情報を付与し、装置固有の暗号化鍵で暗号化してサービス利用識別情報を生成し、送信部２５が生成したサービス利用識別情報をサービス提供サーバ３００に送信する。

【００３２】

サービス提供サーバ３００は、サービス利用識別情報生成装置または管理サーバとしてのＴＴＰ２００から通知されたＩＤにより、ユーザを識別し、ユーザの管理を実行するとともに、利用者情報を取得する。

【００３３】

＜生成されるＩＤの構成＞

次に、図４から図６を用いて、本実施形態において、生成されるＩＤの構成について説明する。

まず、図４に示すように、ユーザ端末１００のそれぞれが有するサービス利用識別情報生成装置または管理サーバとしてのＴＴＰ２００へのログインＩＤ（ＩＤｕ）に所定の付加情報（Ｓｉｎｆｏ）を結合する。そして、この結合された情報をサービスごとに異なる暗号化鍵（Ｋｎ）で暗号化する。さらに、この情報に、利用者の情報を結合し、この結合された情報をサービス利用識別情報生成装置または管理サーバとしてのＴＴＰ２００固有の暗号化鍵（PK_S）で暗号化して、これを利用者情報が付与されたユーザＩＤデータとする。なお、サービス提供サーバ３００では、図６に示すように、ＴＴＰ２００から送信された利用者情報が付与されたユーザＩＤデータをサービス提供サーバ３００が有する秘密鍵（SK_S）で復号して、それぞれＩＤとして、あるいは、ユーザの情報として利用する。

【００３４】

次に、図５の場合には、ユーザ端末１００のそれぞれが有するサービス利用識別情報生成装置または管理サーバとしてのＴＴＰ２００へのログインＩＤ（ＩＤｕ）に所定の付加情報（Ｓｉｎｆｏ）を結合する。そして、この結合された情報をサービスごとに異なる暗号化鍵（Ｋｎ）で暗号化する。さらに、この情報に、利用者の情報を結合し、この結合された情報をサービス利用識別情報生成装置または管理サーバとしてのＴＴＰ２００とサービス提供サーバ３００とが共有する暗号化鍵（K_{S-TTP}）で暗号化して、これを利用者情報が付与されたユーザＩＤデータとする。なお、サービス提供サーバ３００では、ＴＴＰ２００から送信された利用者情報が付与されたユーザＩＤデータをサービス提供サーバ３００が有する共有鍵（K_{S-TTP}）で復号して、それぞれＩＤとして、あるいは、ユーザの情報として利用する。

【００３５】

したがって、サービス利用識別情報生成装置または管理サーバとしてのＴＴＰ２００が、サービスごとに異なる暗号化鍵（Ｋｎ）を用いてＩＤを生成するにあたり、利用者に関する情報を、生成したＩＤ自身に付与し、さらに、全体を、サービス利用識別情報生成装置または管理サーバとしてのＴＴＰ２００固有の暗号化鍵（PK_S）あるいはＴＴＰ２００とサービス提供サーバ３００とが共有する暗号化鍵（K_{S-TTP}）で暗号化するため、利用者に関する情報を第三者に対して秘匿化することができ、さらに、全体をひとつのＩＤとすることができる。

【００３６】

＜サービス利用識別情報生成装置の構成＞

本実施形態に係るサービス利用識別情報生成装置は、図２に示すように、受信部２１と、暗号化部２２と、鍵データベース２３と、サービス利用識別情報生成部２４と、送信部２５とから構成されている。

【００３７】
受信部２１は、ユーザ端末１００からサービス提供サーバ３００に対する接続要求を受信する。なお、この際、サービス利用識別情報生成装置または管理サーバとしてのＴＴＰ２００に対するログインＩＤも併せて受信する。
【００３８】
暗号化部２２は、受信部２１が受信したユーザのログインＩＤ（ＩＤｕ）に所定の付加情報（Ｓｉｎｆｏ）を結合するとともに、鍵データベース２３内に格納されたサービスごとに異なる暗号化鍵（Ｋｎ）を用いて、上記結合した情報を暗号化する。なお、所定の付加情報（Ｓｉｎｆｏ）は、ＩＤの生成時刻のように動的に変動するものでもよいし、固定のビット列でもよい。
【００３９】
鍵データベース３０は、サービスごとに異なる暗号化鍵（Ｋｎ）およびサービス利用識別情報生成装置または管理サーバとしてのＴＴＰ２００固有の暗号化鍵（PK_S）あるいはＴＴＰ２００とサービス提供サーバ３００とが共有する暗号化鍵（K_{S-TTP}）を格納する。なお、データベースは、ハードディスク、ＲＡＭ（Ｒａｎｄｏｍ Ａｃｃｅｓｓ Ｍｅｍｏｒｙ）であってもよく、また、単一のハードウェアで構成されている必要はなく、個別の記録部や専用装置であってもよい。
【００４０】
サービス利用識別情報生成部２４は、上記暗号化部２２において暗号化された情報に利用者に関する情報を結合し、この結合した情報を鍵データベース２３内に格納されたサービス利用識別情報生成装置または管理サーバとしてのＴＴＰ２００固有の暗号化鍵（PK_S）あるいはＴＴＰ２００とサービス提供サーバ３００とが共有する暗号化鍵（K_{S-TTP}）でさらに暗号化して利用者情報が付与されたユーザＩＤデータを生成する。
【００４１】
送信部２５は、サービス利用識別情報生成部２４において生成されたサービス利用識別情報をサービス提供サーバ３００に送信する。
【００４２】
＜サービス利用識別情報生成システムの処理＞
次に、図３を用いて、本実施形態に係るサービス利用識別情報生成システムの処理について説明する。
【００４３】
まず、サービス利用識別情報生成装置の受信部２１がユーザ端末１００からサービス提供サーバ３００への接続仲介要求を受信する（ステップＳ１０１）。なお、このとき、同時に、サービス利用識別情報生成装置または管理サーバとしてのＴＴＰ２００に対するログインＩＤも併せて受信する。
【００４４】
暗号化部２２は、受信部２１からユーザのログインＩＤ（ＩＤｕ）を入力すると、これに、所定の付加情報（Ｓｉｎｆｏ）を結合するとともに（ステップＳ１０２）、鍵データベース２３内に格納されたサービスごとに異なる暗号化鍵（Ｋｎ）を用いて、上記結合した情報を暗号化する（ステップＳ１０３）。
【００４５】
サービス利用識別情報生成部２４は、暗号化部２２から暗号化された情報を入力すると、この情報に利用者に関する情報を結合し（ステップＳ１０４）、この結合した情報を鍵データベース２３内に格納されたサービス利用識別情報生成装置または管理サーバとしてのＴＴＰ２００固有の暗号化鍵（PK_S）あるいはＴＴＰ２００とサービス提供サーバ３００とが共有する暗号化鍵（K_{S-TTP}）でさらに暗号化して利用者情報が付与されたユーザＩＤデータを生成する（ステップＳ１０５）。
【００４６】
したがって、本実施形態によれば、サービス利用識別情報生成装置または管理サーバとしてのＴＴＰ２００が、サービスごとに異なる暗号化鍵（Ｋｎ）を用いてＩＤを生成する

にあたり、利用者に関する情報を、生成したＩＤ自身に付与し、さらに、全体を、サービス利用識別情報生成装置または管理サーバとしてのＴＴＰ２００固有の暗号化鍵（PK_S）あるいはＴＴＰ２００とサービス提供サーバ３００とが共有する暗号化鍵（K_{S-TTP}）で暗号化するため、利用者に関する情報を第三者に対して秘匿化することができ、さらに、全体をひとつのＩＤとすることができる。

【００４７】

なお、サービス利用識別情報生成装置およびサービス利用識別情報生成システムのそれぞれの処理をコンピュータ読み取り可能な記録媒体に記録し、この記録媒体に記録されたプログラムをサービス利用識別情報生成装置およびサービス利用識別情報生成システムに読み込ませ、実行することによって本発明のサービス利用識別情報生成装置およびサービス利用識別情報生成システムを実現することができる。ここでいうコンピュータシステムとは、ＯＳや周辺装置等のハードウェアを含む。

【００４８】

また、「コンピュータシステム」は、ＷＷＷ（Ｗｏｒｌｄ　Ｗｉｄｅ　Ｗｅｂ）システムを利用している場合であれば、ホームページ提供環境（あるいは表示環境）も含むものとする。また、上記プログラムは、このプログラムを記憶装置等に格納したコンピュータシステムから、伝送媒体を介して、あるいは、伝送媒体中の伝送波により他のコンピュータシステムに伝送されても良い。ここで、プログラムを伝送する「伝送媒体」は、インターネット等のネットワーク（通信網）や電話回線等の通信回線（通信線）のように情報を伝送する機能を有する媒体のことをいう。

【００４９】

また、上記プログラムは、前述した機能の一部を実現するためのものであっても良い。さらに、前述した機能をコンピュータシステムにすでに記録されているプログラムとの組合せで実現できるもの、いわゆる差分ファイル（差分プログラム）であっても良い。

【００５０】

以上、この発明の実施形態につき、図面を参照して詳述してきたが、具体的な構成はこの実施形態に限られるものではなく、この発明の要旨を逸脱しない範囲の設計等も含まれる。

【図面の簡単な説明】

【００５１】

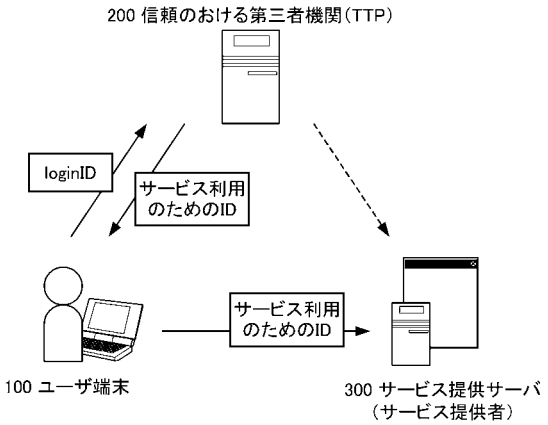
【図１】本実施形態に係るサービス利用識別情報生成システムの構成図である。
【図２】本実施形態に係るサービス利用識別情報生成装置の構成図である。
【図３】本実施形態に係るサービス利用識別情報生成システムの処理フローである。
【図４】本実施形態に係るサービス利用識別情報の構成を示す図である。
【図５】本実施形態に係るサービス利用識別情報の構成を示す図である。
【図６】本実施形態に係るサービス利用識別情報の複号化処理を示す図である。
【図７】従来のシステム構成を示す図である。

【符号の説明】

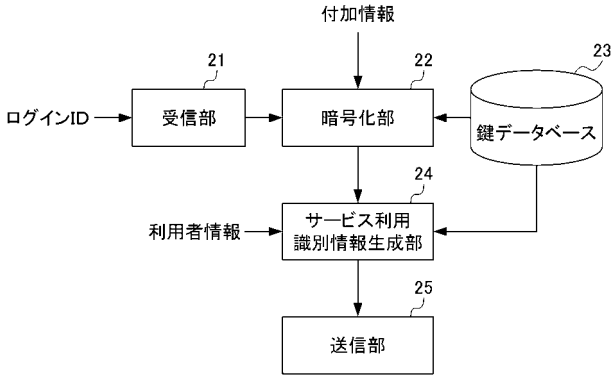
【００５２】

２１・・・受信部
２２・・・暗号化部
２３・・・鍵データベース
２４・・・サービス利用識別情報生成部
２５・・・送信部
１００・・・ユーザ端末
２００・・・ＴＴＰ
３００・・・サービス提供サーバ

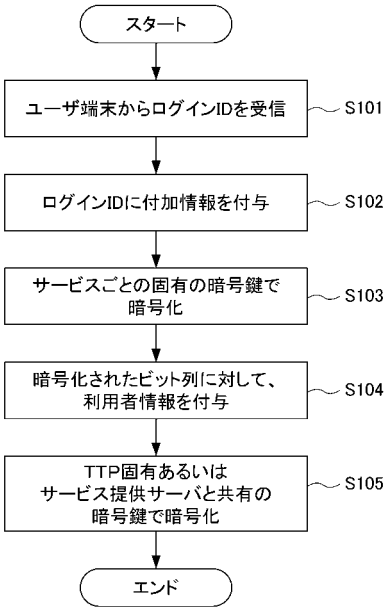
【図１】


200 信頼のおける第三者機関（TTP）
loginID
サービス利用のためのID
サービス利用のためのID
100 ユーザ端末
300 サービス提供サーバ（サービス提供者）

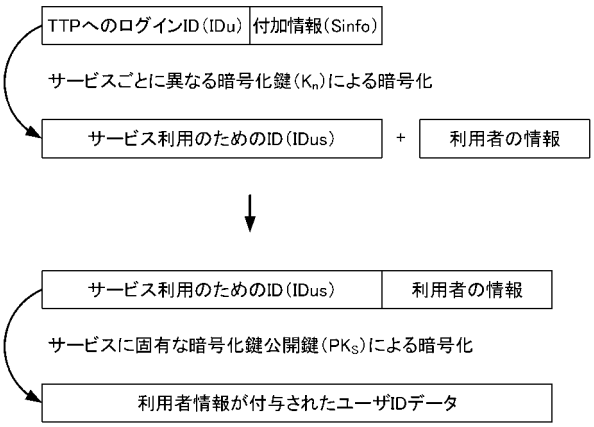
【図２】


付加情報
21
22
23
ログインID
受信部
暗号化部
鍵データベース
24
利用者情報
サービス利用識別情報生成部
25
送信部

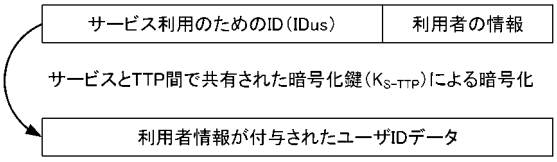
【図３】


スタート
ユーザ端末からログインIDを受信
S101
ログインIDに付加情報を付与
S102
サービスごとの固有の暗号鍵で暗号化
S103
暗号化されたビット列に対して、利用者情報を付与
S104
TTP固有あるいはサービス提供サーバと共有の暗号鍵で暗号化
S105
エンド

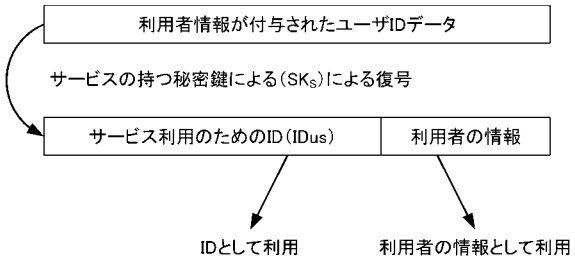
【図４】


TTPへのログインID（IDu）
付加情報（Sinfo）
サービスごとに異なる暗号化鍵（K_n）による暗号化
サービス利用のためのID（IDus）
+
利用者の情報
サービス利用のためのID（IDus）
利用者の情報
サービスに固有な暗号化鍵公開鍵（PK_S）による暗号化
利用者情報が付与されたユーザIDデータ

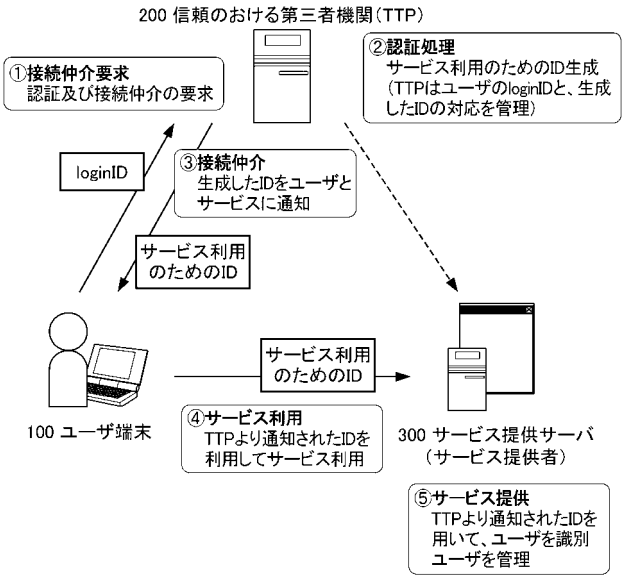
【図５】


サービス利用のためのID（IDus）
利用者の情報
サービスとTTP間で共有された暗号化鍵（K_{S-TTP}）による暗号化
利用者情報が付与されたユーザIDデータ

【図６】


利用者情報が付与されたユーザIDデータ
サービスの持つ秘密鍵による（SK_S）による復号
サービス利用のためのID（IDus）
利用者の情報
IDとして利用
利用者の情報として利用

【図７】


200 信頼のおける第三者機関（TTP）
①接続仲介要求
認証及び接続仲介の要求
②認証処理
サービス利用のためのID生成
（TTPはユーザのloginIDと、生成したIDの対応を管理）
loginID
③接続仲介
生成したIDをユーザとサービスに通知
サービス利用のためのID
サービス利用のためのID
100 ユーザ端末
④サービス利用
TTPより通知されたIDを利用してサービス利用
300 サービス提供サーバ
（サービス提供者）
⑤サービス提供
TTPより通知されたIDを用いて、ユーザを識別
ユーザを管理

フロントページの続き

(72)発明者　窪田　歩
埼玉県ふじみ野市大原二丁目１番１５号　株式会社ＫＤＤＩ研究所内
(72)発明者　田中　俊昭
埼玉県ふじみ野市大原二丁目１番１５号　株式会社ＫＤＤＩ研究所内

Ｆターム(参考) 5B285 AA04 BA10 CA02 CA23 CA41 CB73 CB85
5J104 AA07 AA16 AA32 AA34 EA03 EA15 EA16 EA17 JA03 KA02
KA04 NA02 NA05 NA27 NA37 NA38 PA07