

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第4989996号  
(P4989996)

(45) 発行日 平成24年8月1日(2012.8.1)

(24) 登録日 平成24年5月11日(2012.5.11)

(51) Int.Cl.

F I

G 0 6 F 21/20 (2006.01)

G 0 6 F 21/20 1 4 1

H 0 4 L 9/32 (2006.01)

G 0 6 F 21/20 1 3 1 E

H 0 4 L 9/00 6 7 3 A

請求項の数 8 (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)  
 (65) 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)  
 審査請求日 平成21年7月8日 (2009.7.8)

(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

(73) 特許権者 599108264  
 株式会社 K D D I 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 K D D I 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) 【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公開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、

前記送信手段は、前記暗号化処理手段により暗号化した情報を前記ユーザ端末に送信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、

10

20

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公開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、

前記送信手段は、前記暗号化処理手段により暗号化した情報を前記ユーザ端末に送信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公開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、

前記送信手段は、前記暗号化処理手段により暗号化した情報を前記ユーザ端末に送信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公開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、

前記送信手段は、前記暗号化処理手段により暗号化した情報を前記ユーザ端末に送信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公開鍵で暗号化する第 4 のステップと、

前記第 4 のステップで暗号化された情報を前記サービス提供サーバに送信し、前記第 2 のステップで暗号化された情報を前記ユーザ端末に送信する第 5 のステップと、

10

20

30

40

50

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 公開鍵 で暗号化する第 4 のステップと、

前記第 4 のステップで暗号化された情報を前記サービス提供サーバに送信し、前記第 2 のステップで暗号化された情報を前記ユーザ端末に送信する第 5 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 公開鍵 で暗号化する第 4 のステップと、

前記第 4 のステップで暗号化された情報を前記サービス提供サーバに送信し、前記第 2 のステップで暗号化された情報を前記ユーザ端末に送信する第 5 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 公開鍵 で暗号化する第 4 のステップと、

前記第 4 のステップで暗号化された情報を前記サービス提供サーバに送信し、前記第 2 のステップで暗号化された情報を前記ユーザ端末に送信する第 5 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

10

20

30

40

50

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T

10

20

30

40

50

ＴＰ（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】

（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公開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、前記送信手段は、前記暗号化処理手段により暗号化した情報を前記ユーザ端末に送信する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公開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、前記送信手段は、前記暗号化処理手段により暗号化した情報を前記ユーザ端末に送信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。

## 【 0 0 1 3 】

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

10

## 【 0 0 1 4 】

(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公開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、前記送信手段は、前記暗号化処理手段により暗号化した情報を前記ユーザ端末に送信するサービス利用識別情報生成装置を提案している。

20

## 【 0 0 1 5 】

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

30

40

## 【 0 0 1 6 】

(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

50

関との間で共有された暗号化鍵公開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、前記送信手段は、前記暗号化処理手段により暗号化した情報を前記ユーザ端末に送信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公開鍵で暗号化する第4のステップ（例えば、図3のステップS105に相当）と、前記第4のステップで暗号化された情報を前記サービス提供サーバに送信し、前記第2のステップで暗号化された情報を前記ユーザ端末に送信する第5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公開鍵で暗号化する第4のステップ（例えば、図3のステップS105に相当）と、前記第4のステップで暗号化された情報を前記サービス提供サーバに送信し、前記第2のステップで暗号化された情報を前記ユーザ端末に送信する第5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を提案している。

10

#### 【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

20

#### 【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公開鍵で暗号化する第4のステップ（例えば、図3のステップS105に相当）と、前記第4のステップで暗号化された情報を前記サービス提供サーバに送信し、前記第2のステップで暗号化された情報を前記ユーザ端末に送信する第5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を提案している。

30

#### 【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。

40

#### 【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

50

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公開鍵で暗号化する第4のステップ（例えば、図3のステップS105に相当）と、前記第4のステップで暗号化された情報を前記サービス提供サーバに送信し、前記第2のステップで暗号化された情報を前記ユーザ端末に送信する第5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を提案している。

10

#### 【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。

20

#### 【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。

30

#### 【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。

40

#### 【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】

50

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。

10

#### 【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】

20

##### <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 (ID<sub>u</sub>) 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 (K<sub>n</sub>) 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<sub>s</sub>) 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<sub>s</sub>) 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。

30

#### 【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 (ID<sub>u</sub>) 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 (K<sub>n</sub>) 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<sub>s-TTP</sub>) 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<sub>s-TTP</sub>) 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。

40

#### 【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 (K<sub>n</sub>) 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<sub>s</sub>) 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<sub>s-TTP</sub>) で暗号化するため

50

、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(PKs)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(Ks-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(PKs)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(Ks-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

10

20

30

40

50

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 ( $K_n$ ) 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。

10

【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】

20

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。

30

【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。

40

【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

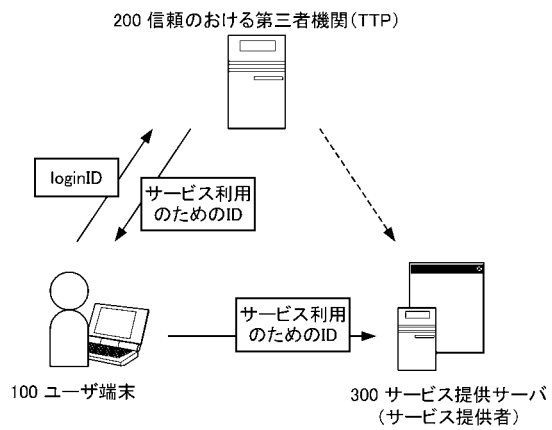
23・・・鍵データベース

24・・・サービス利用識別情報生成部

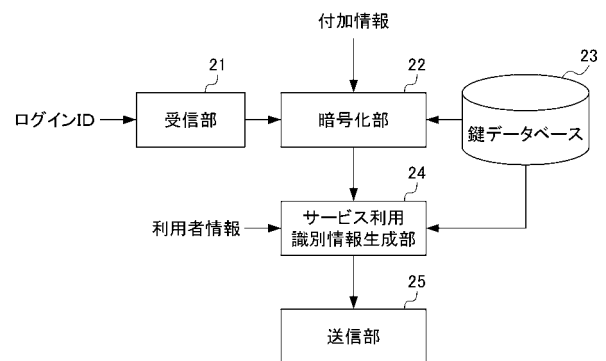
50

2 5 . . . 送信部  
 1 0 0 . . . ユーザ端末  
 2 0 0 . . . T T P  
 3 0 0 . . . サービス提供サーバ

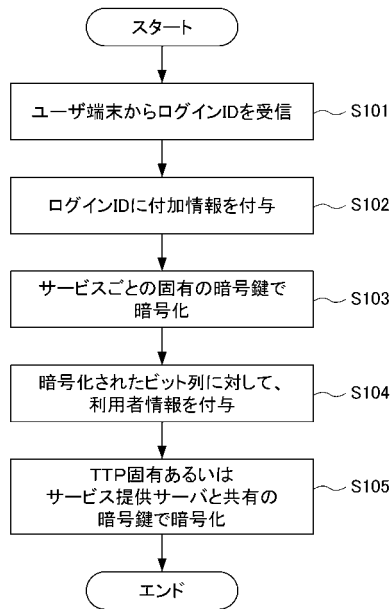
【図 1】



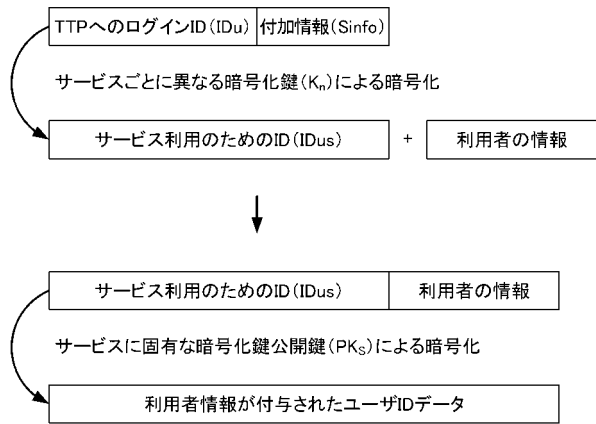
【図 2】



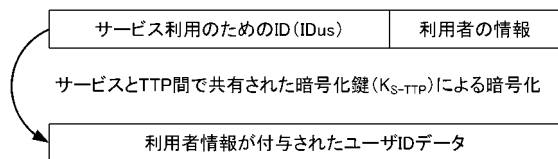
【図 3】



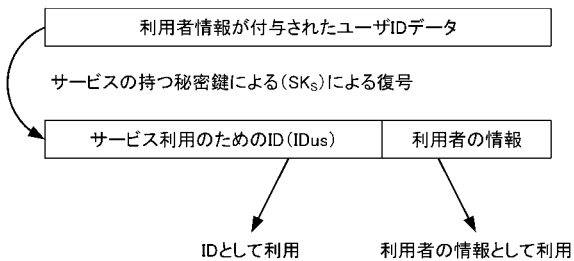
【図 4】



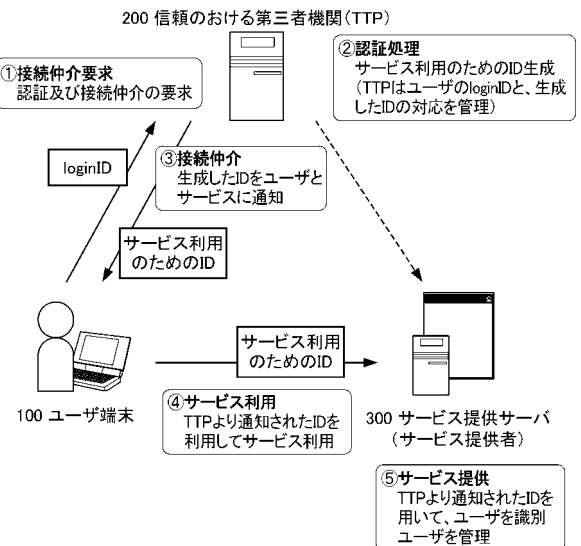
【図 5】



【図 6】



【図 7】



---

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

審査官 戸島 弘詩

- (56)参考文献 特開2006-244420(JP,A)  
特開2005-311904(JP,A)  
特開2005-056393(JP,A)

- (58)調査した分野(Int.Cl., DB名)
- G 0 6 F 2 1 / 2 0
  - G 0 9 C 1 / 0 0 - 5 / 0 0
  - H 0 4 K 1 / 0 0
  - H 0 4 L 9 / 0 0