(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6199506号
(P6199506)
(45)発行日　平成29年9月20日(2017.9.20)　(24)登録日　平成29年9月1日(2017.9.1)

(51)Int.Cl.　F I
G06F 21/41 (2013.01)　G06F 21/41

請求項の数 19　(全 45 頁)

(21)出願番号	特願2016-561901(P2016-561901)
(86)(22)出願日	平成27年11月25日(2015.11.25)
(86)国際出願番号	PCT/JP2015/082991
(87)国際公開番号	WO2016/084822
(87)国際公開日	平成28年6月2日(2016.6.2)
審査請求日	平成28年12月12日(2016.12.12)
(31)優先権主張番号	特願2014-240462(P2014-240462)
(32)優先日	平成26年11月27日(2014.11.27)
(33)優先権主張国	日本国(JP)
(31)優先権主張番号	特願2015-6662(P2015-6662)
(32)優先日	平成27年1月16日(2015.1.16)
(33)優先権主張国	日本国(JP)
(31)優先権主張番号	特願2015-33330(P2015-33330)
(32)優先日	平成27年2月23日(2015.2.23)
(33)優先権主張国	日本国(JP)

(73)特許権者　304021831
国立大学法人　千葉大学
千葉県千葉市稲毛区弥生町１番３３号
(73)特許権者　507328106
株式会社セフティーアングル
千葉県市川市真間５丁目１８－２１
(74)代理人　110000279
特許業務法人ウィルフォート国際特許事務所
(72)発明者　多田　充
千葉県千葉市稲毛区弥生町１番３３号　国立大学法人千葉大学　統合情報センター内
(72)発明者　糸井　正幸
千葉県市川市真間５丁目１８－２１　株式会社セフティーアングル内
最終頁に続く

(54)【発明の名称】複数のサービスシステムを制御するサーバシステム及び方法

(57)【特許請求の範囲】
【請求項１】
複数のユーザ端末及び複数のサービスシステムと通信可能なサーバシステムであって、
管理情報を記憶する記憶手段と、
前記記憶手段に接続された制御手段と
を有し、
前記複数のユーザ端末の各々は、前記サーバシステムとの通信のために実行されるアプリケーションプログラムであるAPPを実行するようになっており、
前記管理情報が、ユーザ毎に、
そのユーザが利用し得るサービスシステムのＩＤであるsysIDと、
サーバシステムとそのユーザのユーザ端末との間で共有されるＩＤであって当該ユーザ端末で実行されるAPPのＩＤであるaIDと、
サーバシステムとそのユーザが利用し得るサービスシステムとの間で共有されユーザ毎に異なるＩＤであるmIDと
を含むようになっており、
前記管理情報において、各aIDに、１以上のmIDと、１以上のsysIDと、１以上の判断用情報が関連付けられるようになっており、
前記制御手段は、初回登録のユーザ端末について、
当該ユーザ端末のAPPについてのaIDを生成し、
当該aIDを前記管理情報において第１のsysID及び第１のmIDと関連付け、

当該aIDを含んだ許可証であるPassを当該ユーザ端末に発行し、
前記制御手段は、２回目以降登録のユーザ端末について、
当該ユーザ端末から、当該ユーザ端末に格納されているPassを受け、
当該Pass内のaIDを前記管理情報において第２のsysID及び第２のmIDと関連付け、
前記制御手段が、
（Ａ）判断用情報及びPassが関連付けられているリクエストをユーザ端末から受信した場合、そのリクエストに関連付いている判断用情報と前記管理情報において関連付けられている判断用情報とが一致するか否かと、そのリクエストに関連付いているPassが正しいか否かとを判断し、
（Ｂ）（Ａ）の判断の結果が真であれば、そのリクエストに関連付けられているPass内のaIDに前記管理情報において関連付けられているmIDのうちの、前記受信したリクエストに基づく全てのmIDを特定し、
（Ｃ）（Ｂ）で特定されたmIDに関連付いているsysIDに対応したサービスシステムである特定サービスシステムに、（Ｂ）で特定されたmIDのうちその特定サービスシステムに対応したmIDと、そのサービスシステムに対する制御内容とが関連付いたリクエストを送信し、
前記リクエストに関連付けられている判断用情報は、前記ユーザの記憶情報又は非記憶情報をシードとした情報であり、
前記制御内容は、識別符号の制御と、情報連携とのうちの少なくとも１つであり、
前記受信したリクエストに関連付けられているPass内のaIDに、前記管理情報において関連付けられているmIDが、２以上である場合、前記受信したリクエストによって、前記受信したリクエストに基づく全てのmIDは、２以上になる、
サーバシステム。
【請求項２】
前記受信したリクエストは、識別符号の制御のリクエストである、
請求項１記載のサーバシステム。
【請求項３】
前記受信したリクエストには、ユーザにより選択されたサービスシステムのsysIDが関連付けられており、
（Ｂ）において、前記制御手段は、前記受信したリクエストに関連付けられているaID及びsysIDに前記管理情報において関連付けられているmIDを特定する、
請求項１又は２記載のサーバシステム。
【請求項４】
前記受信したリクエストに関連付いている判断用情報は、前記ユーザ端末にユーザにより入力されたパスワード又はそのパスワードに基づくパスワードでありそのリクエストの認証に使用されるパスワードであるtReqPwである、
請求項１乃至３のいずれか１項に記載のサーバシステム。
【請求項５】
前記初回登録において、前記制御手段が、
（ａ）サービスシステムから、そのサービスシステムのsysIDを受信し、そのユーザ及びそのサービスシステムに対応したmIDと、サーバシステムにおける制御装置のＩＤであるcIDとを、そのサービスシステムに送信し、受信したsysIDと送信したmIDとを前記管理情報に登録し、
（ｂ）前記ユーザ端末からのリクエストに応答して、前記生成したaIDと、前記tReqPwとを、（ａ）で登録されたsysID及びmIDに関連付け、（ａ）で登録されたsysID及びmIDを含む情報要素群のＩＤであるＳＮと、その関連付けられたaIDと、前記送信したcIDとを含んだ前記Passを、前記ユーザ端末に送信する、
請求項４記載のサーバシステム。
【請求項６】
前記tReqPwは、前記ユーザにより入力されたパスワードと前記ユーザ端末又は前記制御

手段により決定された乱数とを用いて生成されたパスワードである、
請求項４又は５記載のサーバシステム。
【請求項７】
前記リクエストは、識別符号の発行のリクエストである識別符号発行リクエストであり、
（Ｃ）において、前記制御手段が、全ての特定サービスシステムに共通の識別符号を生成し、
（Ｃ）において送信されるリクエストには、更に前記共通の識別符号が関連付けられ、
（Ｃ）において送信されるリクエストの制御内容は、前記共通の識別符号の登録であり、
前記共通の識別符号は、前記全ての特定のサービスシステムのいずれの特定サービスシステムに対しても前記ユーザ端末又は別のユーザ端末により入力される識別符号である、
請求項２乃至６のうちのいずれか１項に記載のサーバシステム。
【請求項８】
前記制御手段が、前記ユーザが利用し得るサービスシステムの各々から、そのサービスシステムに登録されているuID（ユーザＩＤ）がそのサービスシステムと前記ユーザ端末との間で共有されるsuKey（暗号／復号キー）で暗号化されたものである暗号化uIDを、（Ｃ）のリクエストの応答又はそれとは別のタイミングで受信し、
前記制御手段が、前記ユーザが利用し得るサービスシステムからそれぞれ受信した暗号化uIDを前記ユーザ端末に送信する、
請求項２乃至７のうちのいずれか１項に記載のサーバシステム。
【請求項９】
前記記憶手段及び前記制御手段を有する第１の制御装置と、
前記第１の制御装置及び複数のサービスシステムと通信可能な第２の制御装置と
を有し、
前記複数のサービスシステムは、前記第１の制御装置に登録されているsysIDに対応した第１のサービスシステムと前記第２の制御装置に登録されているsysIDに対応した第２のサービスシステムとを含み、
前記第１の制御装置が受信したリクエストは、識別符号の発行のリクエストである識別符号発行リクエストであり、
前記識別符号発行リクエストに関連付けられている全てのsysIDは、少なくとも第２のサービスシステムのsysIDを含み、
前記第１又は第２の制御装置が、前記第１の制御装置により発行された共通の識別符号についてのリクエストを、前記識別符号発行リクエストに関連付けられているsysIDに対応した第２のサービスシステムに送信する、
請求項１乃至８のうちのいずれか１項に記載のサーバシステム。
【請求項１０】
前記第１の制御装置が、前記識別符号発行リクエストに関連付けられているsysIDのうちの、第２のサービスシステムシステムに対応したsysIDを、前記第２の制御装置に送信し、その第２のサービスシステムに対応したmIDを前記第２の制御装置から受信し、受信したmIDと前記共通の識別符号とを関連付けたリクエストを、そのmIDに対応した第２のサービスシステムに送信する、
請求項９記載のサーバシステム。
【請求項１１】
前記第１の制御装置が、前記識別符号発行リクエストに関連付けられているsysIDのうちの、第２のサービスシステムシステムに対応したsysIDと、前記共通の識別符号とを、前記第２の制御装置に送信し、
前記第２の制御装置が、その第２のサービスシステムに対応したmIDと、前記共通の識別符号とを関連付けたリクエストを、そのmIDに対応した第２のサービスシステムに送信する、

請求項９記載のサーバシステム。
【請求項１２】
前記第１の制御装置が、前記識別符号発行リクエストに関連付けられているsysIDのうちの、第２のサービスシステムシステムに対応したsysIDを、前記第２の制御装置に送信し、
前記第２の制御装置が、その第２のサービスシステムに対応したmIDを含んだ情報であるアサーションを、その第２のサービスシステムに送信し、
前記第１の制御装置が、前記共通の識別符号を関連付けたリクエストを、その第２のサービスシステムに送信する、
請求項９記載のサーバシステム。
【請求項１３】
前記サービスシステムへ送信したリクエストに対し前記サービスシステムから受信した応答が、前記サービスシステムが保持する情報であって別のサービスシステムに公開することが許可されている情報要素を含む、
請求項１乃至１２のうちのいずれか１項に記載のサーバシステム。
【請求項１４】
前記受信したリクエストは、連携元サービスシステムの連携対象情報を連携先サービスシステムと共有することである情報連携を表しており、
前記受信したリクエストが情報連携を表している場合、
（Ｂ）において特定されたmIDは、前記連携元サービスシステム又は前記連携先サービスシステムのmIDを含み、
（Ｃ）において、前記特定サービスシステムが、前記連携元サービスシステムの場合、前記制御手段が、前記連携対象情報のリクエストであって、前記連携元サービスシステムのmIDと前記連携先サービスシステムのsysIDとが関連付けられたリクエストを、前記連携元サービスシステムに送信し、前記特定サービスシステムが、前記連携先サービスシステムの場合、前記制御手段が、前記連携対象情報のリクエストであって、前記連携先サービスシステムのmIDと前記連携元サービスシステムのsysIDとが関連付けられたリクエストを、前記連携先サービスシステムに送信する
請求項１乃至１３のうちのいずれか１項に記載のサーバシステム。
【請求項１５】
前記制御手段が、
（Ｐ）前記連携元サービスシステムから連携対象情報を受信し、
（Ｑ）前記受信した連携対象情報を前記連携先サービスシステムが取得可能になる前に、前記連携対象情報を前記ユーザ端末に送信し、
（Ｒ）前記受信した連携対象情報の連携ＮＧの回答を前記ユーザ端末から受信した場合、前記連携対象情報が前記連携先サービスシステムに取得されることを不可能にする、
請求項１４記載のサーバシステム。
【請求項１６】
前記制御手段が、
前記受信した連携対象情報が暗号化されている場合、その連携対象情報を復号すること無しに、格納又は送信し、
前記受信した連携対象情報が暗号化されていない場合、その連携対象情報のマルウェアの有無をチェックする、
請求項１５記載のサーバシステム。
【請求項１７】
（Ｃ）で送信される１以上のリクエストの各々に関連付けられている制御内容は、認証シャッターのopen又はclosedである、
請求項１乃至１６のうちのいずれか１項に記載のサーバシステム。
【請求項１８】
複数のサービスシステムと通信可能なサーバシステムと、

ユーザ端末で実行されるアプリケーションプログラムであり前記サーバシステムと通信するＡＰＰと
を有し、
前記サーバシステムが、管理情報を記憶し、
前記管理情報が、ユーザについて、
そのユーザが利用し得るサービスシステムのＩＤであるsysIDと、
サーバシステムとそのユーザのユーザ端末との間で共有されるＩＤであって当該ユーザ端末で実行されるAPPのＩＤであるaIDと、
前記サーバシステムとそのユーザが利用し得るサービスシステムとの間で共有されユーザ毎に異なるＩＤであるmIDと
を含むようになっており、
前記管理情報において、各aIDに、１以上のmIDと、１以上のsysIDと、１以上の判断用情報が関連付けられるようになっており、
前記サーバシステムは、初回登録のユーザ端末について、
当該ユーザ端末のAPPについてのaIDを生成し、
当該aIDを前記管理情報において第１のsysID及び第１のmIDと関連付け、
当該aIDを含んだ許可証であるPassを当該ユーザ端末に発行し、
前記サーバシステムは、２回目以降登録のユーザ端末について、
当該ユーザ端末から、当該ユーザ端末に格納されているPassを受け、
当該Pass内のaIDを前記管理情報において第２のsysID及び第２のmIDと関連付け、
前記サーバシステムが、
（Ａ）判断用情報及びPassが関連付けられているリクエストを前記ＡＰＰから受信した場合、そのリクエストに関連付いている判断用情報と前記管理情報において関連付けられている判断用情報とが一致するか否かと、そのリクエストに関連付いているPassが正しいか否かとを判断し、
（Ｂ）（Ａ）の判断の結果が真であれば、そのリクエストに関連付けられているPass内のaIDに前記管理情報において関連付けられているmIDのうちの、前記受信したリクエストに基づく全てのmIDを特定し、
（Ｃ）（Ｂ）で特定されたmIDに関連付いているsysIDに対応したサービスシステムである特定サービスシステムに、（Ｂ）で特定されたmIDのうちその特定サービスシステムに対応したmIDと、そのサービスシステムに対する制御内容とが関連付いたリクエストを送信し、
前記リクエストに関連付けられている判断用情報は、前記ユーザの記憶情報又は非記憶情報をシードとした情報であり、
前記制御内容は、識別符号の制御と、情報連携とのうちの少なくとも１つであり、
前記受信したリクエストに関連付けられているaIDに、前記管理情報において関連付けられているmIDが、２以上である場合、前記受信したリクエストによって、前記受信したリクエストに基づく全てのmIDは、２以上になる、
システム。
【請求項１９】
初回登録のユーザ端末について、
当該ユーザ端末のAPPについてのaIDを生成し、
当該aIDを管理情報において第１のsysID及び第１のmIDと関連付け、
当該aIDを含んだ許可証であるPassを当該ユーザ端末に発行し、
２回目以降登録のユーザ端末について、
当該ユーザ端末から、当該ユーザ端末に格納されているPassを受け、
当該Pass内のaIDを前記管理情報において第２のsysID及び第２のmIDと関連付け、
（Ａ）判断用情報及びPassが関連付けられているリクエストをユーザ端末から受信した場合、そのリクエストに関連付いている判断用情報と前記管理情報において関連付けられ

ている判断用情報とが一致するか否かと、そのリクエストに関連付いているPassが正しいか否かとを判断し、
前記管理情報が、ユーザについて、
そのユーザが利用し得るサービスシステムのＩＤであるsysIDと、
サーバシステムとそのユーザのユーザ端末との間で共有されるＩＤであって当該ユーザ端末で実行されるAPPのＩＤであるaIDと、
サーバシステムとそのユーザが利用し得るサービスシステムとの間で共有されユーザ毎に異なるＩＤであるmIDと
を含むようになっており、
前記管理情報において、各aIDに、１以上のmIDと、１以上のsysID、１以上の判断用情報とが関連付けられるようになっており、
（Ｂ）（Ａ）の判断の結果が真であれば、そのリクエストに関連付けられているPass内のaIDに前記管理情報において関連付けられているmIDのうちの、前記受信したリクエストに基づく全てのmIDを特定し、
（Ｃ）（Ｂ）で特定されたmIDに関連付いているsysIDに対応したサービスシステムである特定サービスシステムに、（Ｂ）で特定されたmIDのうちその特定サービスシステムに対応したmIDと、そのサービスシステムに対する制御内容とが関連付いたリクエストを送信し、
前記リクエストに関連付けられている判断用情報は、前記ユーザの記憶情報又は非記憶情報をシードとした情報であり、
前記制御内容は、識別符号の制御と、情報連携とのうちの少なくとも１つであり、
前記受信したリクエストに関連付けられているaIDに、前記管理情報において関連付けられているmIDが、２以上である場合、前記受信したリクエストによって、前記受信したリクエストに基づく全てのmIDは、２以上になる、
方法。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、概して、サービスシステムの制御に関する。
【背景技術】
【０００２】
認証のようなアクセス制御では、一般に、識別符号が使用される。「識別符号」には、認証等のアクセス制御に用いられるあらゆるデータが該当し得る。本明細書で言う「識別符号」は、不正アクセス禁止法（正確には、不正アクセス行為の禁止等に関する法律）で使用される「識別符号」の意味を含んでよい。識別符号の一例として、ワンタイムパスワードのようなパスワードが知られている。パスワードを用いた認証技術として、例えば特許文献１が知られている。
【先行技術文献】
【特許文献】
【０００３】
【特許文献１】特許第３６７８４１７号明細書
【発明の概要】
【発明が解決しようとする課題】
【０００４】
ユーザＩＤ及びパスワードの漏えいやパスワードクラッキング等により、ネットワーク上でのなりすまし犯罪が増加している。その為、サービス企業は、ユーザに対して、パスワード（及びユーザＩＤ）の厳重管理とパスワードに関しては定期的な変更を依頼している。
【０００５】
しかし、インターネット上で多くのサービスを受けるユーザが、多くのパスワード（及

びユーザＩＤ）を管理し（例えば、サービス毎に、パスワードを管理し）、更に、パスワードを定期的に変更することは、容易ではない。

【０００６】

多くのユーザは、利用している全てのサービスシステム（サービス）について全てのパスワード（及びユーザＩＤ）を記憶できない。このため、複数のサービスシステムで同一のパスワード（及びユーザＩＤ）を使用したりノートやパーソナルコンピュータ等にサービス毎のパスワード（及びユーザＩＤ）を記録したりしているのが実情である。しかし、この方法も安全とは言えない。

【０００７】

以上のような問題は、パスワード（及びユーザＩＤ）に限らず、他種の識別符号（例えば、ワンタイムパスワード）についてもあり得る。

【０００８】

また、１ユーザが複数のサービスシステムを利用するにあたり下記に示すような別の問題もあり得る。

【０００９】

例えば、利便性の観点では、ユーザは、第１のサービスシステムに情報を提供するために第２のサービスシステムからその情報を取得しその取得した情報を第１のサービスシステムに提供しなければならないという煩わしさがあり得る。

【００１０】

また、安全性の観点では、サービスシステムに対して他人により成り済まされることを心配するユーザも存在し得る。

【課題を解決するための手段】

【００１１】

複数のユーザ端末及び複数のサービスシステムと通信可能なサーバシステム（１以上の計算機）が構築される。サーバシステム（例えば制御センタ）は、各ユーザについて１以上の情報要素群を含んだ管理情報を保持する。１以上の情報要素群の各々が、サーバシステムとサービスシステムとの間で共有されユーザ毎に異なるＩＤ（mID）を含む。サーバシステムが、リクエストをユーザ端末から受信する。サーバシステムが、そのリクエストを基に１以上のサービスシステムにそれぞれ対応した１以上のmIDを、そのユーザ端末のユーザについて管理情報から特定する。サーバシステムが、その１以上のサービスシステムの各々に、特定された１以上のmIDのうちそのサービスシステムに対応したmIDと、そのサービスシステムに対する制御内容とが関連付いたリクエストを送信する。

【発明の効果】

【００１２】

複数のサービスシステムの利用について安全性を確保しつつ利便性を改善できる。

【図面の簡単な説明】

【００１３】

【図１】実施例１に係る認証プロセスの概略を示す。
【図２】U_Mの構成例を示す。
【図３】U_Pの構成例を示す。
【図４】$S_i^{(j)}$（$S_1^{(1)}$）の構成例を示す。
【図５】$C^{(j)}$（$C^{(1)}$）の構成例を示す。
【図６】$uList_i^{(j)}$（$uList_1^{(1)}$）の構成例を示す。
【図７】$aList^{(j)}$（$aList^{(1)}$）の構成例を示す。
【図８】pListの構成例を示す。
【図９】$sList^{(j)}$（$sList^{(1)}$）の構成例を示す。
【図１０】$cList^{(j)}$（$cList^{(1)}$）の構成例を示す。
【図１１】$C^{(1)}$によるtpw提供を示す。
【図１２】初回登録のフローの一例を示す。
【図１３】２回目以降登録のフローの一例を示す。

【図１４】実施例１に係るtpw発行フローの一例を示す。
【図１５】実施例２に係る認証システムの一例を示す。
【図１６】pListの一例を示す。
【図１７】実施例２に係るtpw発行フローの一例を示す。
【図１８】実施例３に係るtpw発行フローの一例を示す。
【図１９】図１８の具体例を示す。
【図２０】実施例４に係るtpw発行フローの一例を示す。
【図２１】実施例５に係るtpw発行フローの一例を示す。
【図２２】実施例６に係るtpw削除フローの一例を示す。
【図２３】実施例７に係る$uList_i^{(j)}$の構成例を示す。
【図２４】実施例７に係る$aList^{(j)}$の構成例を示す。
【図２５】実施例８に係る認証／連携フローの一例を示す。
【図２６】識別符号管理の概要の一例を示す。
【図２７】シャッターシステムの構成例を示す。
【図２８】認登録手続き１、登録手続き２、及び、認証シャッター操作手続きの各々のフローの一例を示す。
【図２９】ログイン手続きのフローの一例を示す。
【図３０】画面遷移の例を示す。
【図３１】実施例８に係る登録フローの一例を示す。
【発明を実施するための形態】
【００１４】
以下、幾つかの実施例を説明する。
【００１５】
その際、複数のサービスステムに共通の識別符号として、パスワードを例に取る。共通のパスワードには、後述するように、使用期限及び使用回数のうちの少なくとも１つのような制限が関連付けられる。実施例では、共通のパスワードは、パスワードが発行された当日間だけ無制限に使用可能なワンタイムパスワードを例に取る（実施例において、「ワンタイム」とは、使用期間が一時的及び使用回数が１回限りのうちの少なくとも前者を意味する）。以下、そのようなパスワードを、「共通1-dayパスワード」と呼ぶことがある。なお、後述するように、一部の実施例では、パスワードは、tpw（共通1-dayパスワード）でなくてもよい。例えば、一部の実施例では、パスワードは、tpwとは異なるタイプの一時的パスワード（例えばワンタイムパスワード）でもよいし、１つのサービスシステムでのみ使用可能な一般的な固定のパスワードでもよい。
【００１６】
以下の説明では、「ＡＡＡリスト」の表現にて情報を説明することがあるが、情報は、どのようなデータ構造で表現されていてもよい。すなわち、情報がデータ構造に依存しないことを示すために、「ＡＡＡリスト」を「ＡＡＡ情報」と呼ぶことができる。また、リスト（テーブル又はテーブルを含んだデータベース）の構成は一例であり、２以上のリストが１つのリストにまとめられたり、１つのリストが複数のリストに分割されたりしてもよい。
【００１７】
以下の説明では、「記憶部」は、メモリを含んだ１以上の記憶デバイスでよい。例えば、記憶部は、主記憶デバイス（典型的には揮発性のメモリ）及び補助記憶デバイス（典型的には不揮発性の記憶デバイス）のうちの少なくとも主記憶デバイスでよい。補助記憶デバイスは、例えば、ＨＤＤ（Hard Disk Drive）又はＳＳＤ（Solid State Drive)でよい。
【００１８】
以下の説明では、「プロセッサ」は、典型的にはマイクロプロセッサ（例えばＣＰＵ（Central Processing Unit））でよく、処理の一部（例えば暗号化又は復号化）を行う専用ハードウェア回路（例えばＡＳＩＣ（Application Specific Integrated Circuit））

を含んでもよい。

【００１９】

少なくとも１つの実施例では、サービスシステムとユーザ端末の２者間に、共通1-dayパスワードを発行する制御センタが介入して、３者間での認証が行われる。実施例の説明では、下記の表記ルールを採用する。なお、ユーザは、１以上存在するが、実施例ではユーザ同士の通信は必須ではないので、説明を分かり易くするために、１人のユーザを例に取る。

・tpw：共通1-dayパスワード
・$C^{(j)}$：制御センタ（jは１以上の整数（j＝１，２，３，…））（制御センタを管理する又は所有する者は、個人でも私企業でも官公庁でもよい）
・S_i：サービスシステム（iは１以上の整数（i＝１，２，３，…））（サービスシステムを管理する又は所有する者は、個人でも私企業でも官公庁でもよい）
・$S_i^{(j)}$：$C^{(j)}$に登録されているS_i
・U：ユーザ
・U_P：第１のユーザ端末（$S_i^{(j)}$の利用のためのユーザ端末（例えばパーソナルコンピュータ））
・U_M：第２のユーザ端末（tpwの発行リクエストのためのユーザ端末であり、例えばデバイス認証可能なユーザ端末（例えばスマートフォンのような携帯端末））
・APP：tpw発行リクエストなど$C^{(j)}$との通信のために実行されるアプリケーションプログラム
・suKey $_i^{(j)}$：U（例えばU_M）と$S_i^{(j)}$とに共有される鍵
・$cID^{(j)}$：$C^{(j)}$の制御センタＩＤ
・$sysID_i^{(j)}$：$S_i^{(j)}$のサービスシステムＩＤ
・$mID_i^{(j)}$：$S_i^{(j)}$の管理用ＩＤであり、$C^{(j)}$と$S_i^{(j)}$との間で共有される情報（U毎に異なる）
・$tReqPw^{(j)}$：tpwの発行リクエストのパスワード
・reqPw：$tReqPw^{(j)}$のシードとなる情報（ユーザが記憶する第１の情報）
・$uID_i^{(j)}$：$S_i^{(j)}$の利用のためのユーザＩＤ（ユーザが記憶する第２の情報）であり、Uと$S_i^{(j)}$との間で共有される情報
・$aID^{(j)}$：APPのＩＤ（但し、後述するように、関連付けを避けるために１つの$C^{(j)}$及び１つのAPPにつき異なる複数の$aID^{(j)}$が存在することもある）
・$uList_i^{(j)}$：$S_i^{(j)}$が記憶する管理リスト（Uに関する情報を保持するリスト）
・$aList^{(j)}$：$C^{(j)}$が記憶する第１の管理リスト（U_M等に関する情報を保持するリスト）
・$sList^{(j)}$：$C^{(j)}$が記憶する第２の管理リスト（$S_i^{(j)}$等に関する情報を保持するリスト）
・$cList^{(j)}$：$C^{(j)}$が記憶する第３の管理リスト（$C^{(j)}$等に関する情報を保持するリスト）
・pList：U_Mが記憶する管理リスト（$C^{(j)}$及び$S_i^{(j)}$等に関する情報を保持するリスト）
・$tpwInfo_i^{(j)}$：tpwの使用制限を表す情報を含むことができ$S_i^{(j)}$により決定されtpwに関連付けられる情報（以下の実施例では、tpwが共通1-dayパスワードのため、使用制限として、使用期限「tpwの発行日の00:00の直前まで」及び使用回数「無制限」をいずれの$tpwInfo_i^{(j)}$も含む）
・Ticket：$C^{(j)}$にUを登録することの電子的な許可証であり$C^{(j)}$により発行される情報
・$Pass_i^{(j)}$：tpwを発行することの電子的な許可証であり$C^{(j)}$により発行される情報

【００２０】

以下の実施例では、１ユーザにつきユーザ端末は２つであるが（又はそれより多いが）、１ユーザにつきユーザ端末は１つであってもよい。後者の場合、例えばU_Mが、第２ユーザ端末と第１ユーザ端末を兼ねてよい。

【００２１】

また、以下の説明では、$C^{(j)}$が１つであるか複数であるかに関わらず、reqPw、APP又はpListは、１つでもよいし、$C^{(j)}$毎にreqPw、APP又はpListが存在してもよい。以下の説明

では、reqPw、APP及びpListのいずれも、$C^{(j)}$の数に関わらず１つであるとする。

【００２２】

また、以下の説明では、APP等のプログラムを主語として処理を説明する場合があるが、プログラムがプロセッサ（例えばＣＰＵ（Central Processing Unit））によって実行されることで、定められた処理が、適宜に記憶部（例えばメモリ）及び／又はインターフェース部（例えば通信ポート）等を用いながら行われるため、処理の主語は、プロセッサとされてもよい。プログラムを主語として説明された処理は、プロセッサあるいはそのプロセッサを有する装置又はシステムが行う処理としてもよい。プログラムは、プログラムソースから計算機のような装置にインストールされてもよい。プログラムソースは、例えば、プログラム配布サーバまたは計算機が読み取り可能な記憶メディアであってもよい。プログラムソースがプログラム配布サーバの場合、プログラム配布サーバはプロセッサ（例えばＣＰＵ）と記憶部を含み、記憶部はさらに配布プログラムと配布対象であるプログラムとを記憶してよい。そして、プログラム配布サーバのプロセッサが配布プログラムを実行することで、プログラム配布サーバのプロセッサは配布対象のプログラムを他の計算機に配布してよい。

【実施例１】

【００２３】

以下、実施例１を説明する。実施例１では、制御センタが１つ（$C^{(1)}$のみ）である。

【００２４】

図１は、実施例１に係る認証プロセスの概略を示す。

【００２５】

サービスシステム１０３（図１では$S_1^{(1)}$のみ図示）とユーザ端末１０５（第１のユーザ端末１０５Ａ（U_P）、第２のユーザ端末１０５Ｂ（U_M））の２者間に、tpwを発行する制御センタ１０１（$C^{(1)}$）が介入して、３者間での認証が行われる。

【００２６】

ユーザ（U）は、自分が所有しているU_Mで実行されるAPPが表示する画面にreqPw（例えば値“xxxx”）を入力し、U_M（APP）が、入力されたreqPwを基に$tReqPw^{(1)}$を生成し、tpw発行リクエストを$C^{(1)}$に送信する（ステップ５０）。tpw発行リクエストには、生成された$tReqPw^{(1)}$と、事前登録において$C^{(1)}$により発行されU_Mに格納された$Pass_1^{(1)}$とが関連付いている（含まれている）。

【００２７】

$C^{(1)}$は、tpw発行リクエストを受信し、そのtpw発行リクエストに関連付いている$tReqPw^{(1)}$が、事前に登録された$tReqPw^{(1)}$と適合するか否かと、tpw発行リクエストに関連付いている$Pass_1^{(1)}$が正しいか否かとを判断する（ステップ５１）。いずれの判断の結果も肯定の場合、$C^{(1)}$は、tpw（例えば値“1234”）を決定し、U（U_M）と$S_1^{(1)}$に、決定したtpwを発行する（ステップ５３及び５４）。その際、$C^{(1)}$は、$S_1^{(1)}$に、$S_1^{(1)}$と$C^{(1)}$間の共通の$mID_1^{(1)}$と、決定したtpwとを含んだ情報セットを送信する（ステップ５３）。

【００２８】

U_M（APP）が、tpwを$C^{(1)}$から受信し、受信したtpw（例えば値“1234”）を出力（例えば表示）する（ステップ５５）。tpwの出力は、表示に代えて又は加えて、音声出力等の他種の出力でもよい。

【００２９】

U（U_P）は、$S_1^{(1)}$に対して、U_Mが受信した情報セット内のtpwと同じtpwと、Uが記憶している$uID_1^{(1)}$（例えば値“yyyy”）とを、入力する（ステップ５６）。

【００３０】

$S_1^{(1)}$は、$C^{(1)}$から受信した$mID_1^{(1)}$に対応するUを特定する。そして、$S_1^{(1)}$は、入力された$uID_1^{(1)}$が、事前に登録された$uID_1^{(1)}$に適合し、且つ、入力されたtpwが、$C^{(1)}$から受けたtpwに適合するか否かを判断する（ステップ５７）。その判断結果が肯定の場合、$S_1^{(1)}$は、Uに対してサービス提供を行う。

【００３１】

Uを特定する為に下記の３つのパラメータ（キー）がある。
・$C^{(1)}$とUとの間で共有されるtReqPw$^{(1)}$
・$S_1^{(1)}$とUとの間で共有される$uID_1^{(1)}$
・$C^{(1)}$と$S_1^{(1)}$との間で共有される$mID_1^{(1)}$
【００３２】
上記３つのＩＤは、それぞれ２者間でしか知りえない。すなわち、
・tReqPw$^{(1)}$を、$S_1^{(1)}$は知らない。
・$uID_1^{(1)}$を、$C^{(1)}$は知らない。
・$mID_1^{(1)}$を、Uは知らない。
【００３３】
このように、意図的に三すくみを作ることにより、どこから情報漏えいが生じても、同時に２箇所から漏えいしなければ、なりすまし犯罪が成立しないようになっている。
【００３４】
tpwを取得するために、U本人が所有するU_Mを使用するため、専用ハードが不要である。また、後述するように、U_Mの個体識別番号を送信することなく、U_Mであることを$C^{(1)}$が確認できる。本実施例では、記憶情報の認証（Uが記憶しているreqPwに基づき生成されたtReqPw$^{(1)}$の認証であるユーザ認証）と所有物の認証（登録において使用されたU_Mに格納されている$Pass_1^{(1)}$の認証であるデバイス認証）の２要素認証が可能となる。
【００３５】
以下、U_M、U_P、$S_i^{(j)}$（$S_1^{(1)}$）、$C^{(j)}$（$C^{(1)}$）、$uList_i^{(j)}$（$uList_1^{(1)}$）、$aList^{(j)}$（$aList^{(1)}$）、pList、$sList^{(j)}$（$sList^{(1)}$）及び$cList^{(j)}$（$cList^{(1)}$）の構成例を説明する。
【００３６】
図２は、U_Mの構成例を示す。
【００３７】
U_Mは、モバイル端末であり、例えば、スマートフォンである。スマートフォンは、スマートデバイスの一種である。スマートデバイスは、単なる計算処理だけではなく、多種多様な用途に使用可能な多機能のデバイスであり、典型的には、スマートフォン、又は、タブレットＰＣである。U_Mは、タッチパネル型ディスプレイ２１１と、記憶部２１３と、Ｉ／Ｆ（通信インターフェイスデバイス）２１４と、それらに接続されたプロセッサ２１２とを有する。タッチパネル型ディスプレイ２１１は、入力デバイスと表示デバイスの一例であり、入力デバイスと表示デバイスが一体になったデバイスである。記憶部２１３は、APP等のプログラムとpList等の情報とを記憶する。プロセッサ２１２は、APPを実行する。APPは、pListを参照又は更新したり、Ｉ／Ｆ２１４を介して$C^{(j)}$（$C^{(1)}$）等の外部装置と通信したりする。APPは、pListの少なくとも一部をタッチパネル型ディスプレイ２１１に表示してもよいし、受信したtpwを、無線等でU_Pに送信（入力）してもよい。
【００３８】
図３は、U_Pの構成例を示す。
【００３９】
U_Pは、記憶部３１１と、Ｉ／Ｆ３１３と、入力デバイス３１５と、表示デバイス３１４と、それらに接続されたプロセッサ３１２とを有する。入力デバイス３１５は、ユーザが情報を入力するために使用するデバイスであり、例えば、キーボード及びポインティングデバイスである。表示デバイス３１４は、情報を表示するデバイスであり、例えば液晶表示デバイスである。記憶部３１１は、Ｗｅｂブラウザ等のプログラムと、情報とを記憶する。プロセッサ３１４は、Ｗｅｂブラウザ等のプログラムを実行することで、Ｉ／Ｆ３１３を介して$S_i^{(j)}$（$S_1^{(1)}$）等の外部装置と通信する。
【００４０】
図４は、$S_i^{(j)}$（$S_1^{(1)}$）の構成例を示す。
【００４１】
$S_i^{(j)}$（$S_1^{(1)}$）は、ユーザ端末（例えばU_P）にサービスを提供するコンピュータシステ

ムであり、典型的には、サービス企業のコンピュータシステムである。$S_i^{(j)}$（$S_1^{(1)}$）は、１以上の計算機であり、記憶部４１１と、Ｉ／Ｆ４１３と、それらに接続されたプロセッサ４１２とを有する。記憶部４１１が、プログラムと、$uList_i^{(j)}$（$uList_1^{(1)}$）等の情報とを記憶する。プロセッサ４１２が、記憶部４１１内のプログラムを実行することで、$uList_i^{(j)}$（$uList_1^{(1)}$）を参照又は更新したり、Ｉ／Ｆ４１３を介してU_P等の外部装置と通信したりする。

【００４２】

図５は、$C^{(j)}$（$C^{(1)}$）の構成例を示す。

【００４３】

$C^{(j)}$（$C^{(1)}$）は、tpwを発行するコンピュータシステムである。$C^{(j)}$（$C^{(1)}$）は、１以上の計算機であり、記憶部５１１と、Ｉ／Ｆ５１３と、それらに接続されたプロセッサ５１２とを有する。記憶部５１１が、プログラムと、$aList^{(j)}$（$aList^{(1)}$）、$sList^{(j)}$（$sList^{(1)}$）及び$cList^{(j)}$（$cList^{(1)}$）等の情報とを記憶する。プロセッサ５１２が、記憶部５１１内のプログラムを実行することで、$aList^{(j)}$（$aList^{(1)}$）、$sList^{(j)}$（$sList^{(1)}$）又は$cList^{(j)}$（$cList^{(1)}$）を参照又は更新したり、Ｉ／Ｆ５１３を介してU_M又は$S_i^{(j)}$（$S_1^{(1)}$）等の外部装置と通信したりする。

【００４４】

図６は、$uList_i^{(j)}$（$uList_1^{(1)}$）の構成例を示す。なお、以下、図６～図１０において、リストにおける情報要素の名称は、アルファベット大文字で表記する。また、以下、リストにおける１行（レコード）を、「アカウント」と呼ぶ。

【００４５】

$uList_i^{(j)}$（$uList_1^{(1)}$）は、Uに関する情報を保持する。$uList_i^{(j)}$の各アカウントが保持する情報要素は、例えば、UID、MID、TPW、TPWINFO、SUKEY及びOTHERSである。UIDは、登録された$uID_i^{(j)}$である。MIDは、登録された$mID_i^{(j)}$である。TPWは、登録されたtpwである。TPWINFOは、登録された$tpwInfo_i^{(j)}$である。SUKEYは、登録された$suKey_i^{(j)}$である。OTHERSは、他の情報要素であり、例えば、Uのユーザ名等を含んでよい。

【００４６】

図７は、$aList^{(j)}$（$aList^{(1)}$）の構成例を示す。

【００４７】

$aList^{(j)}$（$aList^{(1)}$）は、U_M等に関する情報を保持する。$aList^{(j)}$の各アカウントが保持する情報要素は、例えば、SN、SYSID、MID、TREQPW、AID及びOTHERSである。SNは、登録されたシリアル番号（sn）である。SYSIDは、登録された$sysID_i^{(j)}$である。MIDは、登録された$mID_i^{(j)}$である。TREQPWは、登録された$tReqPw^{(j)}$である。AIDは、登録された$aID^{(j)}$である。$aID^{(j)}$は、１つのAPP及び１つの$C^{(j)}$につき１つであるが、１つのAPP及び１つの$C^{(j)}$につき異なる複数の$aID^{(j)}$が生成されてもよい。OTHERSは、他の情報要素であり、例えば、$C^{(j)}$による運用等に必要な情報を含んでよい。

【００４８】

図８は、pListの構成例を示す。

【００４９】

pList（pList）は、$C^{(j)}$及び$S_i^{(j)}$等に関する情報を保持する。pListの各アカウントが保持する情報要素は、例えば、SYSID、CID、RAND、AID、PASS、SUKEY及びOTHERSである。SYSIDは、登録された$sysID_i^{(j)}$である。CIDは、登録された$cID^{(j)}$である。RANDは、登録された乱数（以下、Randと表記）である。Randは、後述するように、$tReqPw^{(j)}$の生成（算出）に使用される。AIDは、登録された$aID^{(j)}$である。PASSは、登録された$Pass_i^{(j)}$である。$Pass_i^{(j)}$は、tpw発行の電子的な許可証である。$Pass_i^{(j)}$の詳細は後述する。SUKEYは、登録された$suKey_i^{(j)}$である。OTHERSは、他の情報要素であり、例えば、$C^{(j)}$との通信等に関する情報を含んでよい。

【００５０】

図９は、$sList^{(j)}$（$sList^{(1)}$）の構成例を示す。

【００５１】

sList$^{(j)}$（sList$^{(1)}$）は、$S_i^{(j)}$等に関する情報を保持する。sList$^{(j)}$の各アカウントが保持する情報要素は、例えば、SYSID及びOTHERSである。SYSIDは、登録されたsysID$_i^{(j)}$である。OTHERSは、他の情報要素であり、例えば、$S_i^{(j)}$の名称、$S_i^{(j)}$との通信に必要な情報（例えば、ＦＱＤＮ（Fully Qualified Domain Name）及びネットワークアドレス）等を含んでよい。

【００５２】

図１０は、cList$^{(j)}$（cList$^{(1)}$）の構成例を示す。

【００５３】

cList$^{(j)}$（cList$^{(1)}$）は、他のC$^{(j)}$等に関する情報を保持する（本実施例では、C$^{(j)}$は１つなので、cList$^{(j)}$はブランクである）。cList$^{(j)}$の各アカウントが保持する情報要素は、例えば、CID及びOTHERSである。CIDは、登録されたcID$^{(j)}$である。OTHERSは、他の情報要素であり、例えば、他のcID$^{(j)}$の名称、他のcID$^{(j)}$との通信に必要な情報（例えば、ＦＱＤＮ及びネットワークアドレス）等を含んでよい。

【００５４】

図１１は、C$^{(1)}$によるtpw提供を示す。

【００５５】

C$^{(1)}$は、U（U_M）から１つの$S_i^{(1)}$についてtpw発行リクエストを受けた場合、ユーザが契約している全ての$S_i^{(j)}$（特定されたユーザについてaList$^{(1)}$から特定された全てのsysID $_i^{(1)}$にそれぞれ対応した$S_i^{(1)}$）に、tpw（例えば値“1234”）（及びmID $_i^{(1)}$）の提供を行う。図１１の例によれば、ユーザが契約している$S_i^{(1)}$は、$S_1^{(1)}$、$S_2^{(1)}$及び$S_3^{(1)}$である。C$^{(1)}$は、$S_i^{(1)}$からのtpw問合せ無しにtpwを$S_i^{(1)}$に提供してもよいし、$S_i^{(1)}$からのtpw問合せに応答してtpwを$S_i^{(1)}$に提供してもよい。U（U_P）は、同じtpwで、tpwに関連付けられているtpwInfo$_i^{(1)}$が示す期限まで（例えばその日１日（必ずしも２４時間であったり、当日の23:59（翌日の00:00の直前の一例）であったりする必要はない））、契約しているいずれの$S_i^{(1)}$に対してもログインできる。tpwInfo$_i^{(1)}$は、$S_i^{(1)}$毎に異なっていてもよいし、複数の$S_i^{(1)}$においてtpwInfo$_i^{(1)}$が同一であってもよい。

【００５６】

以下、本実施例で行われる処理のフローを説明する。

【００５７】

＜事前登録＞

【００５８】

＜＜初回登録＞＞

【００５９】

図１２は、初回登録のフローの一例を示す。

【００６０】

初回登録とは、C$^{(1)}$に登録されていないUについて$S_i^{(1)}$を利用するための事前登録である。初回登録は、２段階の手続きを含む。第１段階が、Uと$S_i^{(1)}$との間で行われる手続きであり、第２段階が、UとC$^{(1)}$との間で行われる手続きである。

【００６１】

第１段階（Uと$S_i^{(1)}$との間で行われる手続き）は下記ステップ１２０１～ステップ１２０７である。ここでは、Uが$S_1^{(1)}$に利用申請するものとする。

【００６２】

（ステップ１２０１）U（U_P）は、$S_1^{(1)}$に利用申請を送信する。その際、U（U_P）は、$S_1^{(1)}$で使用するuID$_1^{(1)}$を決める。

【００６３】

（ステップ１２０２）$S_1^{(1)}$は、U（U_P）から利用申請を受信し、その申請に応答して、UとのsuKey$_1^{(1)}$を決定し、uList$_1^{(1)}$にアカウントを追加する。$S_1^{(1)}$は、追加したアカウントに、UIDとして、決定されたuID$_1^{(1)}$を登録し、SUKEYとして、決定されたsuKey$_1^{(1)}$を登録する。

【００６４】

（ステップ１２０３）$S_1^{(1)}$は、$sysID_1^{(1)}$を関連付けたユーザ追加リクエストを$C^{(1)}$に送信する。

【００６５】

（ステップ１２０４）$C^{(1)}$は、ユーザ追加リクエストを受信し、そのリクエストに応答して、$sysID_1^{(1)}$と追加されるUとの両方に対応付ける$mID_1^{(1)}$を決定し、$aList^{(1)}$にアカウントを追加する。$C^{(1)}$は、追加したアカウントに、SNとして、決定したsn（例えばアカウントの通し番号）を登録し、SYSIDとして、ユーザ追加リスクエストに関連付いている$sysID_1^{(1)}$を登録し、MIDとして、決定した$mID_1^{(1)}$を登録する。ここで決定されたsnを、以下、「sn1」と記載することがある。

【００６６】

（ステップ１２０５）$C^{(1)}$は、登録チケット（以下、Ticket）を生成し、生成したTicketと、ステップ１２０４で決定した$mID_1^{(1)}$とを、$S_1^{(1)}$に送信する。Ticketは、第１の電子署名（以下、Sign1）と、$cID^{(1)}$と、登録したsn1及び$sysID_1^{(1)}$とに基づいている。具体的には、例えば、Ticketは、Sign1と、$cID^{(1)}$と、sn1と、$sysID_1^{(1)}$とを含む（Ticket = (sn1, $cID^{(1)}$, $sysID_1^{(1)}$, Sign1)）。Sign1は、$cID^{(1)}$と、登録したsn1及び$sysID_1^{(1)}$とに基づいている。なお、Ticketにおいて、snは、$C^{(1)}$がユーザを特定するために使用される情報要素（例えば通し番号）である。$cID^{(1)}$は、どの$C^{(j)}$に登録にすればよいかをAPPが特定するために使用される情報要素である（$cID^{(j)}$が$C^{(j)}$との通信に必要な情報を含む等、何らかの方法で$C^{(j)}$との通信に必要な情報と$cID^{(j)}$とがAPPにおいて関連付けられればよい）。Ticketに$sysID_1^{(1)}$は無くてもよい。例えば、Sign1は、$cID^{(1)}$と、sn1と、$sysID_1^{(1)}$とを含む（Sign1 = sign(sn1, $cID^{(1)}$, $sysID_1^{(1)}$, aux)）。Ticketに$sysID_1^{(1)}$が含まれていなければ、Sign1に$sysID_1^{(1)}$が含まれていなくてもよい。Sign1は、$C^{(1)}$がその正しさを検証できさえすればよい。なお、aux（補助的な情報）は、$uList_1^{(1)}$内の何らかの情報要素（例えばOTHERSの少なくとも一部）を含んでよい。Sign1にauxは無くてもよい。

【００６７】

（ステップ１２０６）$S_1^{(1)}$は、Ticketと$mID_1^{(1)}$とを$C^{(1)}$から受信する。$S_1^{(1)}$は、ステップ１２０２で登録された$uID_1^{(1)}$と、受信した$mID_1^{(1)}$とを関連付ける。具体的には、$S_1^{(1)}$は、受信した$mID_1^{(1)}$を、ステップ１２０２で登録された$uID_1^{(1)}$があるアカウントにMIDとして登録する。

【００６８】

（ステップ１２０７）$S_1^{(1)}$は、受信したTicketと、ステップ１２０２で登録した$suKey_1^{(1)}$とを、U（U_P）に送信する。

【００６９】

第２段階（Uと$C^{(1)}$との間で行われる手続き）は下記ステップ１２０８～ステップ１２１１である。

【００７０】

（ステップ１２０８）Uが、reqPwを決定し、決定したreqPwと、U_Pで受信したTicket及び$suKey_1^{(1)}$とを、U_Mに入力する。U_MのAPPが、その入力に応答して、乱数（Rand）を決定し、$tReqPw^{(1)}$を生成する。$tReqPw^{(1)}$は、決定されたRandと、入力されたreqPwとに基づいている（ここで決定されたRandを、以下、「Rand1」と記載することがある。）。具体的には、例えば、$tReqPw^{(1)}$は、衝突困難一方向性関数（ハッシュ関数）及びRand1を用いて不可逆変換されたreqPwである（$tReqPw^{(j)} = h_j$ (Rand1, reqPw)）。$tReqPw^{(j)}$は、パスワードの役割を果たすが、衝突困難一方向性関数等によりreqPwが解読不能に暗号化されたものなので、reqPwの秘密性を維持できる。tReqPw生成のための関数hが、h_jの表記の通り、制御センタ毎に異なっていてよい。これにより、Uは、１つのreqPwを覚えるだけで、制御センタ毎に異なるtReqPwを登録できる。U_M（APP）は、Ticket及び$tReqPw^{(1)}$を、Ticket内の$cID^{(1)}$から特定された$C^{(1)}$に、送信する。なお、秘密性が落ちるが、U_Mが、(Rand及びreqPwを$C^{(1)}$に送信し、$C^{(1)}$が、U_MからのRand1及びreqPwを用いて、$tReqPw^{(1)}$を生成してもよい。また、Randは無くてもよいが、Randがあることで、$C^{(1)}$の$aList^{(1)}$にお

いて同一Uについて$tReqPw^{(1)}$が同じ値になってしまうことを避けることができる。

【００７１】

（ステップ１２０９）$C^{(1)}$は、Ticket及び$tReqPw^{(1)}$をU_M（APP）から受信する。$C^{(1)}$は、受信したTicket内のSign1が正しいか否かを判断することで、Ticketが正しいか否かを判断する。その判断結果が肯定の場合、$C^{(1)}$は、Ticket内のsnに適合するSNを含んだアカウントを$aList^{(1)}$から特定する。$C^{(1)}$は、Ticketの送信元のAPP（U_M）についての$aID^{(1)}$を生成し、特定したアカウントに、AIDとして、生成した$aID^{(1)}$を登録し、TREQPWとして、受信した$tReqPw^{(1)}$を登録する。$tReqPw^{(j)}$は、パスワードの役割を果たすが、衝突困難一方向性関数等によりreqPwが解読不能に暗号化されたものなので、$aList^{(1)}$から$tReqPw^{(j)}$が漏洩したとしても、reqPwの秘密性を維持できる。

【００７２】

（ステップ１２１０）$C^{(1)}$は、$Pass_1^{(1)}$を生成し、生成した$Pass_1^{(1)}$をU_M（APP）に送信する。$Pass_1^{(1)}$は、$aList^{(1)}$に既に登録されているsn1、$cID^{(1)}$及び$sysID_1^{(1)}$と、ステップ１２０９で登録した$aID^{(1)}$と、第２の電子署名（以下、Sign2）とに基づいている。具体的には、例えば、$Pass_1^{(1)}$は、sn1と、$cID^{(1)}$と、$sysID_1^{(1)}$と、$aID^{(1)}$と、Sign2とを含む（$Pass_1^{(1)}$ = (sn1, $cID^{(1)}$, $sysID_1^{(1)}$, $aID^{(1)}$, Sign2)）。$Pass_1^{(1)}$内の$aID^{(1)}$は、後にU_Mからtpw依頼リクエストを受信した場合にtpwの発行先となる全ての（又は一部の）$S_i^{(1)}$を特定するために使用される情報要素である（$aList^{(1)}$において同一の$aID^{(1)}$に複数の$sysID_i^{(1)}$が関連付けられている）。Sign2は、sn1、$cID^{(1)}$及び$sysID_1^{(1)}$と、ステップ１２０９で登録した$aID^{(1)}$とに基づいている。具体的には、例えば、Sign2は、sn1と、$cID^{(1)}$と、$sysID_1^{(1)}$と、$aID^{(1)}$とを含む（Sign2 = sign(sn1, $cID^{(1)}$, $sysID_1^{(1)}$, $aID^{(1)}$, aux)）。

【００７３】

（ステップ１２１１）U_M（APP）は、$Pass_1^{(1)}$を$C^{(1)}$から受信し、pListにアカウントを追加する。U_M（APP）は、追加したアカウントに、SYSIDとして、$Pass_1^{(1)}$（又はTicket）内の$sysID_1^{(1)}$を登録し、CIDとして、$Pass_1^{(1)}$（又はTicket）内の$cID^{(1)}$を登録し、RANDとして、ステップ１２０８で決定したRand1を登録し、AIDとして、$Pass_1^{(1)}$内の$aID_1^{(1)}$を登録しPASSとして、受信した$Pass_1^{(1)}$を登録し、SUKEYとして、ステップ１２０８で入力された$suKey_1^{(1)}$を登録する。なお、pListのアカウントに登録される情報要素のうち、例えば$cID^{(1)}$及び$sysID_1^{(1)}$以外の情報要素は、U_Mが記憶している情報（例えば、個体識別情報及び将来的にはマイナンバー（及びそれに付随する情報）のうちの少なくとも１つ）とUが記憶している情報（例えばreqPw）とのうちの少なくとも１つを暗号鍵として暗号化されてよい（$cID^{(1)}$及び$sysID_1^{(1)}$はオープンな情報要素のため暗号化されないでよい）。

【００７４】

＜＜２回目以降の登録＞＞

【００７５】

図１３は、２回目以降登録のフローの一例を示す。

【００７６】

既に$C^{(1)}$に登録されているUが、別のサービスシステム（例えば$S_2^{(1)}$）を利用するときは、初回登録時に入手された$aID^{(1)}$を使用できる。具体的には、第１段階は、初回登録の第１段階と同じである（ステップ１３０１～ステップ１３０７は、ステップ１２０１～ステップ１２０７とそれぞれ同じである）。第２段階（Uと$C^{(1)}$との間で行われる手続き）は下記である。主に、初回登録の第２段階との相違点を記載し、初回登録の第２段階との共通点については説明を省略又は簡略する。

【００７７】

（ステップ１３０８）Uが、Uが初回登録で使用したreqPw（Uが記憶している情報）と、U_Pで受信したTicket及び$suKey_2^{(1)}$とを、U_Mに入力する。U_M（APP）が、pListをタッチパネル型ディスプレイ２１１に表示し、Uから、利用するアカウントの選択を受ける。U_M（APP）は、Uにより選択されたアカウントからRand1、$cID^{(1)}$、$sysID_1^{(1)}$、$aID^{(1)}$及びPass

$_1{}^{(1)}$を取得する。U_M（APP）は、入力されたTicket内の$cID^{(1)}$が、選択されたアカウントから取得された$cID^{(1)}$と同じか否かを判断する。この判断結果が否定の場合、U_M（APP）は、登録失敗として停止してよい。一方、この判断結果が肯定の場合、U_M（APP）は、$tReqPw^{(1)}$（$=h_1$（取得されたRand1，入力されたreqPw）を生成し、生成した$tReqPw^{(1)}$と、アカウントから取得された$Pass_1{}^{(1)}$と、入力されたTicketとを、$C^{(1)}$に送信する。

【００７８】

（ステップ１３０９）$C^{(1)}$は、Ticket、$Pass_1{}^{(1)}$及び$tReqPw^{(1)}$をU_M（APP）から受信する。$C^{(1)}$は、受信したTicket内のSign1を検証することで、Ticketが正しいか否かを判断する。その判断結果が肯定の場合、$C^{(1)}$は、Ticket内のsn（以下、sn2）に適合するSNを含んだアカウントを$aList^{(1)}$から特定し、また、受信した$Pass_1{}^{(1)}$から$aID^{(1)}$を取得する。$C^{(1)}$は、特定したアカウントに、SNとして、Ticket内のsn2を登録し、AIDとして、取得した$aID^{(1)}$を登録し、TREQPWとして、受信した$tReqPw^{(1)}$を登録する。

【００７９】

（ステップ１３１０）$C^{(1)}$は、$Pass_2{}^{(1)}$（= (sn2, $cID^{(1)}$, sysID $_2{}^{(1)}$, $aID^{(1)}$, Sign2)）を生成し、生成した生成した$Pass_2{}^{(1)}$をU_M（APP）に送信する。$Pass_2{}^{(1)}$内のSign2は、Sign2 = sign(sn2, $cID^{(1)}$, sysID $_2{}^{(1)}$, $aID^{(1)}$, aux)である。

【００８０】

（ステップ１３１１）U_M（APP）は、$Pass_2{}^{(1)}$を$C^{(1)}$から受信し、pListにアカウントを追加する。U_M（APP）は、追加したアカウントに、SYSIDとして、$Pass_2{}^{(1)}$（又はTicket）内の$sysID_2{}^{(1)}$を登録し、CIDとして、$Pass_2{}^{(1)}$（又はTicket）内の$cID^{(1)}$（又は、ステップ１３０８で取得した$cID^{(1)}$）を登録し、RANDとして、ステップ１３０８で取得したRand1を登録し、PASSとして、受信した$Pass_2{}^{(1)}$を登録し、SUKEYとして、ステップ１３０８で入力された$suKey_2{}^{(1)}$を登録する。

【００８１】

以上のように、事前登録では、初回登録と２回目以降の登録とがある。初回登録であるか２回目以降の登録であるかは、UがU_M（APP）に明示してよい。例えば、APPが、初回登録と２回目以降登録のいずれであるかの選択をUから受け付ける画面（例えば、初回登録ボタンと２回目以降登録ボタンとを有するＧＵＩ（Graphical User Interface）を表示し、いずれのボタンが押されたかによって、初回登録と２回目以降登録のいずれの処理を実行するかを決定してよい。また、Uは、$C^{(1)}$に対して初回登録が済んだ後にいずれかの$S_i{}^{(1)}$を初めて利用する場合に、初回登録を選択してもよい。この場合、同一のUについて異なる複数の$aID^{(1)}$が$C^{(1)}$に登録されることになる。初回登録とするか２回目以降の登録とするかは、異なる複数の$S_i{}^{(1)}$に同一の$aID^{(1)}$を関連付けるか否かである。関連付けがされていれば、U_Mを紛失した又はreqPwを忘れた等の場合に、復旧が比較的容易である。なぜなら、Uは、いずれかの$S_i{}^{(1)}$にその旨を伝えれば、$S_i{}^{(1)}$が、そのUに対応した$mID_i{}^{(1)}$を$C^{(1)}$に送信し、$C^{(j)}$が、その$mID_i{}^{(1)}$に対応した$aID^{(1)}$を特定し、特定した$aID^{(1)}$に関連付いている全ての$sysID_i{}^{(1)}$を$aList^{(1)}$から特定できるためである。また、Uにとっても、pListにおいて同一の$aID^{(1)}$に複数の異なる複数の$sysID_i{}^{(1)}$が関連付いているので、Uにとっての$S_i{}^{(1)}$のグループを特定できる。一方、関連付けがされていなければ、Uがどの複数の$S_i{}^{(1)}$を利用しているかを$C^{(1)}$により$aList^{(1)}$から特定されることを避けることができる。実施例１では、関連付けをするか否かをUが選択できる。

【００８２】

＜tpw（共通1-dayパスワード）の発行＞

【００８３】

以下、Uが利用登録している$sysID_i{}^{(1)}$の全て（または一部）で利用できるtpwの発行のフローを説明する。

【００８４】

図１４は、実施例１に係るtpw発行フローの一例を示す。なお、以下の説明では、複数のSYSID（ここでは、pListに登録されている全てのSYSID）のグループを、「SYSIDGroup」と表記する。また、SYSIDGroupのうちの少なくとも１つのSYSIDを、「SYSIDPart」と表

記する。従って、SYSIDPartは、SYSIDPart⊂SYSIDGroupである（「SYSIDPart⊂SYSIDGroup」は、SYSIDPart＝SYSIDGroupであることも含む）。そして、SYSIDPart⊂SYSIDGroupについての$Pass_{SYSIDPart}$を、$\{Pass_i^{(1)}\}_K$とする。Kは、$sysID_i^{(1)} \in SYSIDPart$である。つまり、$Pass_{SYSIDPart}$の意味は、SYSIDPartを構成する$sysID_i^{(1)}$にそれぞれ対応した$Pass_i^{(1)}$の集合である。UがSYSIDPart⊂SYSIDGroupの全てに使用できるtpwの発行のフローは、以下の通りである。

【００８５】

（ステップ１４０１）U_M（APP）が、例えばpListの少なくとも一部の情報を表示し、pListのSYSIDGroupのうちのSYSIDPartの選択と、reqPwの入力とを、Uから受ける。U_M（APP）は、$Pass_{SYSIDPart}$から１つの$Pass_i^{(1)}$を選択する。また、U_M（APP）は、選択した$Pass_i^{(1)}$が登録されているアカウントからRandを取得し、取得したRandと入力されたreqPwとを用いてtReqPw$^{(1)}$を生成する。U_M（APP）は、Uにより選択されたSYSIDPartと、生成されたtReqPw$^{(1)}$と、選択した$Pass_i^{(1)}$とを関連付けたtpw発行リクエストを、選択された$Pass_i^{(1)}$に対応したcID$^{(1)}$から特定されたC$^{(1)}$に送信する。なお、SYSIDPartの選択は、Uに代えて、U_M（APP）により行われてもよい。

【００８６】

（ステップ１４０２）C$^{(1)}$は、tpw発行リクエストをU_M（APP）から受信し、そのリクエストに応答して、そのリクエストに関連付いているtReqPw$^{(1)}$が正しいか否かの第１の判断と、そのリクエストに関連付いている$Pass_i^{(1)}$が正しいか否かの第２の判断とを行う。第１の判断は、例えば、その$Pass_i^{(1)}$内のsnと一致するsnを保持したアカウント（aList$^{(1)}$内のアカウント）内のTREQPWと、リクエストに関連付いているtReqPw$^{(1)}$とが一致するか否かの判断である。第２の判断は、$Pass_i^{(1)}$内のsnと一致するsnを保持したアカウント（aList$^{(1)}$内のアカウント）内の情報要素（CID、SYSID、AID）と、$Pass_i^{(1)}$内の情報要素（cID$^{(1)}$, $sysID_1^{(1)}$, aID$^{(1)}$）とを用いて、$Pass_i^{(1)}$内のSign2が正しいか否かを判断することにより行われる。第１の判断の結果及び第２の判断の結果のうちの少なくとも１つが否定の場合、C$^{(1)}$は処理を中止してよい。第１の判断の結果及び第２の判断の結果のいずれも肯定の場合、C$^{(1)}$はステップ１４０３を行う。

【００８７】

（ステップ１４０３）C$^{(1)}$は、aList$^{(1)}$を参照し、正しいと判断された$Pass_i^{(1)}$内のaID$^{(1)}$と一致するAIDを有し、且つ、tpw発行リクエストに関連付いているSYSIDPart内のいずれかの$sysID_i^{(1)}$と一致するSYSIDを有するアカウントを全て特定する。C$^{(1)}$は、特定された全てのアカウントからそれぞれMID（$mID_i^{(1)}$）を取得する。ここで取得された$mID_i^{(1)}$の集合を、「MIDGroup」と表記する。MIDGroupは、$\{mID_i^{(1)}\}_L$である。Lは、$sysID_i^{(j)} \in SYSIDPart$, AID=aID$^{(1)}$である。

【００８８】

（ステップ１４０４）C$^{(1)}$は、tpwを決定する。tpwは、例えばランダムな値でよい。C$^{(1)}$は、各$sysID_i^{(1)}$（∈SYSIDPart）について、以下を行う。ステップ１４０４～ステップ１４０７の説明において、１つの$sysID_i^{(1)}$を例に取る。C$^{(1)}$は、$sysID_i^{(1)}$にに対応した$S_i^{(1)}$に、その$S_i^{(1)}$に対応する$mID_i^{(1)}$と、決定されたtpwとを送信する（$mID_i^{(1)}$とtpwとを関連付けたtpw登録リクエストを$S_i^{(1)}$に送信する）。ここでは、C$^{(1)}$は、tpwを、$S_i^{(1)}$からの問合せ無しに送信するが、上述したように、$S_i^{(1)}$からの問合せに応答してtpwを送信するようにしてもよい。

【００８９】

（ステップ１４０５）$S_i^{(1)}$が、その$S_i^{(1)}$に対応する$mID_i^{(1)}$と、決定されたtpwとをC$^{(1)}$から受信する。$S_i^{(1)}$は、受信した$mID_i^{(1)}$と一致するMIDが登録されているアカウントを$uList_i^{(1)}$から特定する。$S_i^{(1)}$は、特定したアカウントに、TPWとして、受信したtpwを登録する。また、$S_i^{(1)}$は、そのtpwについて$tpwInfo_i^{(1)}$を決定し、そのアカウントに、TPWINFOとして、決定した$tpwInfo_i^{(1)}$を登録する。$tpwInfo_i^{(1)}$は、そのtpwの使用期限及び使用可能回数等のtpw制限を表す情報を含んでよい。本実施例では、上述したように、tpwは、共通1-dayパスワードを意味するため、使用制限として、使用期限「tpwの発行

日の00:00の直前まで」及び使用回数「無制限」を、$tpwInfo_i^{(j)}$が含む。

【００９０】

（ステップ１４０６）$S_i^{(1)}$は、ステップ１４０５で特定したアカウントからSUKEY（$suKey_i^{(1)}$）を取得する。$S_i^{(1)}$は、登録した$tpwInfo_i^{(1)}$を含んだ情報$mes_i^{(j)}$（$mes_i^{(1)}$）を、取得した$suKey_i^{(1)}$で暗号化する。結果として、$eMes_i^{(1)}$（$mes_i^{(1)}$の暗号化情報）、すなわち、$Enc_{SUKEY}(mes_i^{(1)})$が得られる（$SUKEY=suKey_i^{(1)}$）。$S_i^{(1)}$は、得られた$eMes_i^{(1)}$を、$C^{(1)}$に送信する。なお、$mes_i^{(j)}$は、$tpwInfo_i^{(1)}$に加えて、その$S_i^{(1)}$に関する情報を含んでよい。その$S_i^{(1)}$に関する情報は、Uの$uID_i^{(1)}$（ステップ１４０５で特定したアカウントから取得されたUID）を含んでよい。暗号化関数（Enc）は、例えば、事前に定められた共通鍵暗号方式の暗号化関数でよい。$eMes_i^{(1)}$は、後述するように、$C^{(1)}$を通じてU_M（APP）に届く情報である。そして、$eMes_i^{(1)}$は、U_M（APP）により、暗号化に使用された$suKey_i^{(1)}$と同一の$suKey_i^{(1)}$を用いて復号化される。つまり、$mes_i^{(j)}$が得られる。U_M（APP）は、得られた$mes_i^{(j)}$内の情報の少なくとも一部（例えば$uID_i^{(1)}$）を、タッチパネル型ディスプレイ２１１に表示する。これにより、Uが$uID_i^{(1)}$を忘れてしまっていても、tpw発行リクエストの応答時という適切なタイミングで（$uID_i^{(1)}$の問合せをU_M（APP）がわざわざ発行すること無しに）、$uID_i^{(1)}$を知ることができる。

【００９１】

（ステップ１４０７）$C^{(1)}$は、$sysID_i^{(1)}$（∈SysysIDPart）にそれぞれ対応した全ての$S_i^{(1)}$から応答（$eMes_i^{(1)}$）を受信した場合に、それらすべての$eMes_i^{(1)}$（$= \{eMes_i^{(1)}\}_M$）と、ステップ１４０４で決定したtpwとを、U_M（APP）に送信する（$M = sysID_i^{(1)} \in SYSIDPart$）。

【００９２】

（ステップ１４０８）U_M（APP）が、$\{eMes_i^{(1)}\}_M$と、tpwとを$C^{(1)}$から受信する。U_M（APP）は、$\{eMes_i^{(1)}\}_M$に含まれる各$eMes_i^{(1)}$について、以下を行う。１つの$eMes_i^{(1)}$を例に取る。U_M（APP）は、$eMes_i^{(1)}$に対応するアカウントをpListから特定する。U_M（APP）は、特定したアカウントからSUKEY（$suKey_i^{(1)}$）を取得し、取得した$suKey_i^{(1)}$）を用いて、$eMes_i^{(1)}$を復号化する。それにより、$mes_i^{(1)}$が得られる。U_M（APP）は、得られた$mes_i^{(1)}$内の情報要素の少なくとも一部を、表示及び上記特定したアカウントに登録のうちの少なくとも一方を行う。U_M（APP）は、そのアカウントに、受信したtpwも登録してよい。U_M（APP）は、受信したtpwをタッチパネル型ディスプレイ２１１に表示してよい。

【００９３】

＜$S_i^{(1)}$の利用＞

【００９４】

フローは、図１を参照して説明したフローと同様である。具体的には、例えば下記である。以下、１つの$S_i^{(1)}$を例に取る（なお、$S_i^{(1)}$の利用段階では、既に、その$S_i^{(1)}$の$uList_i^{(j)}$に、Uに提供されたtpwが設定されている）。Uは、U_Pに、$uID_i^{(1)}$とtpwとを入力する。$S_i^{(1)}$は、U（U_P）から、サービス提供リクエストを受信する。サービス提供リクエストには、U_Pに入力された$uID_i^{(1)}$及びtpwが関連付いている。$S_i^{(1)}$は、その$uID_i^{(1)}$及びtpwの照合を行う。具体的には、$S_i^{(1)}$は、その$uID_i^{(1)}$及びtpwにそれぞれ一致するUID及びTPWが登録されているアカウントが$uList_i^{(1)}$にあるか否かを判断する。その判断結果が肯定の場合、$S_i^{(1)}$は、U（U_P）にサービスを提供する（例えばログインを許可する）。

【００９５】

複数の$S_i^{(1)}$に、その日１日は、同じtpwを使用できる（$S_i^{(1)}$に対するtpwの使用期限は、その$S_i^{(1)}$に対応しtpwに関連付けられている$tpwInfo_i^{(1)}$に従う）。なお、tpwの使用期限（tpwに関連付けられる$tpwInfo_i^{(1)}$が表す使用期限）は、必ずしも２４時間であったり、当日の23:59であったりする必要はない。また、tpwの制限として、使用期限に加えて、使用回数（Ｎ回（Ｎは１以上の整数のうちの任意の値））も定義されていてよい。$tpwInfo_i^{(j)}$は、$S_i^{(j)}$毎に異なっていてもよい。

【００９６】

また、U_M（APP）は、Uが利用している全て（又は一部）の$S_i^{(1)}$でそれぞれ使用するuID

$_i{}^{(1)}$を表示することができる。例えば、U_M（APP）は、Uからのリクエストに応答して、ユーザID問合せを$C^{(1)}$に発行してよい。ユーザID問合せの発行から応答までのフローは、tpw発行リクエストの発行から応答までのフローと同様でよい。その応答には、$S_i{}^{(1)}$から$C^{(1)}$を通じた暗号化ユーザＩＤ（$suKey_i{}^{(1)}$で暗号化された$uID_i{}^{(1)}$）が含まれていてよい。また、その応答には、Uが利用している全て（又は一部）にそれぞれ対応した１以上の暗号化ユーザＩＤが含まれていてよい。U_M（APP）は、$suKey_i{}^{(1)}$を用いて暗号化ユーザＩＤを復号化し、復号化されたユーザＩＤを表示してよい。

【００９７】

また、$C^{(1)}$が、少なくとも１つの$S_i{}^{(1)}$については、$S_i{}^{(1)}$からの問合せ無しにtpwを送信するのではなく、$C^{(1)}$自身が保持してもよい（例えば、その$S_i{}^{(1)}$に対応するアカウント（$aList^{(1)}$におけるアカウント）に、tpwを登録してよい）。この場合は、$S_i{}^{(1)}$が、U（U_P）からサービス提供リクエストを受信した場合に、$C^{(1)}$に、そのUについての$mID_i{}^{(1)}$を関連付けたtpw問合せを送信してよい。$C^{(1)}$は、そのtpw問合せを受信した場合、そのtpw問合せに関連付いている$mID_i{}^{(1)}$に対応したtpwを特定し、特定したtpwを、tpw問合せの送信元$S_i{}^{(1)}$に送信してよい。

【００９８】

以上、実施例１によれば、例えば下記のうちの少なくとも１つの効果を奏することができる。

【００９９】

（１）UがID及びパスワード管理の煩わしさから解放される。

１日１回tpw（共通1-dayパスワード）を取得すれば、その日１日は、同じtpwを使用して、Uが利用する全て（又は一部）の$S_i{}^{(1)}$へのログインが可能になる。このため、管理の煩わしさから解放される。また、$uID_i{}^{(1)}$を忘れても、$uID_i{}^{(1)}$がU_Mに表示される。この点も、管理の煩わしさの解放に貢献している。

【０１００】

（２）安全性が高まる。

tpwは、１日（$tpwInfo_i{}^{(1)}$が表す使用期限）で使えなくなる。このため、たとえ、tpwが盗まれても、そのtpwを翌日に使うことはできない。故に、安全性が高まる。また、tpwの使用期限に加えて使用可能回数を制限することで、更に安全性を高めることが期待できる。また、事前登録で使用したU_M以外のユーザ端末からではtpwを取得できない。なぜなら、U_M以外のユーザ端末には、事前登録のときに取得された情報要素が登録されているpListが存在しないためである。この点も、安全性の向上に貢献している。また、たとえ他人にU_Mが拾われても、tpw発行のリクエストの際にはUが記憶しているreqPwが必要なので、reqPwを他人に知られなければ、他人にtpwが取得されることが無い。

【０１０１】

（３）情報漏えいに強い。

Uは、$C^{(1)}$と$S_i{}^{(1)}$との間で共有される$mID_i{}^{(1)}$を知らない。$C^{(1)}$は、$S_i{}^{(1)}$とUとの間で共有される$uID_i{}^{(1)}$を知らない。$S_i{}^{(1)}$は、$C^{(1)}$とU間で共有される$tReqPw^{(1)}$を知らない。このように、意図的な三すくみにより、三者のいずれで情報漏えいが生じても、なりすましが成立しない。

【０１０２】

（４）$S_i{}^{(1)}$との利用が高まることが期待できる。

Uにとって、インターネット上のサービス利用は、ID及びパスワードを調べることから始まる。利用しているサービスが多ければ多いほど、ID及びパスワードの管理はUにとって億劫である。この煩わしさから解放されることにより、インターネットの活用が更に広がると期待できる。

【実施例２】

【０１０３】

以下、実施例２を説明する。その際、実施例１との相違点を主に説明し、実施例１との共通点については説明を省略又は簡略する。

【０１０４】
実施例２では、２以上の$C^{(j)}$が存在する。例えば、図１５に示すように、$C^{(1)}$及び$C^{(2)}$が存在するとする。また、$C^{(1)}$に、$S_1^{(1)}$及び$S_2^{(1)}$が登録されており、$C^{(2)}$に、$S_1^{(2)}$及び$S_2^{(2)}$が登録されているとする。そして、Uが、それら４つのサービスシステム（$S_1^{(1)}$、$S_2^{(1)}$、$S_1^{(2)}$及び$S_2^{(2)}$）に登録したとする。その際、Uは、$S_2^{(1)}$の登録では$S_1^{(1)}$の登録の際にpListに登録された情報を利用し、$S_2^{(2)}$の登録では$S_1^{(2)}$の登録の際にpListに登録された情報を利用しなかったとする。言い換えれば、$S_1^{(1)}$については初回登録が行われ、$S_2^{(1)}$については２回目以降の登録が行われたとする。また、$S_1^{(2)}$についても$S_2^{(2)}$についても初回登録が行われたとする。AIDが同じ値であればRANDも同じ値である。また、AIDが同じ値であれば、CIDも同じ値である。
【０１０５】
この結果、pListは、図１６に示す通りとなる。すなわち、$S_2^{(1)}$に対応付けられるAIDは、$aID^{(1)}$、すなわち、$S_1^{(1)}$に対応付けられたAIDと同じである。一方、$S_2^{(2)}$に対応付けられるAIDは、$aID^{(2')}$、すなわち、$S_2^{(1)}$に対応付けられたAIDと異なる。２以上の$C^{(j)}$が存在する場合、U_M（APP）が$C^{(j)}$毎に実施例１に係るtpw発行フローを行うことが考えられる。しかし、そうすると、$C^{(j)}$毎にtpwが異なってしまい、Uにとっての利便性が低い。
【０１０６】
そこで、実施例２では、tpwを２以上の$C^{(j)}$で共通にすることができる。
【０１０７】
図１７は、実施例２に係るtpw発行フローの一例を示す。
【０１０８】
U_M（APP）と$C^{(1)}$（その日初めてのtpw発行リクエストの送信先）との間に関して、実施例１に係るtpw発行フローが行われる。これにより、U_M（APP）は、$C^{(1)}$からtpwを受信する。
【０１０９】
tpwを受信したU_M（APP）は、Uが登録されている他の$C^{(J)}$（ここではJは２以上の整数）の各々との間で、以下の処理を行う。U_M（APP）は、$C^{(1)}$から受信したtpwを関連付けたtpw発行リクエストを$C^{(J)}$に送信する。$C^{(J)}$は、tpwが関連付けられたtpw発行リクエストを受信する。$C^{(J)}$は、tpwを発行せず、受信したtpw発行リクエストに関連付けられているtpwを、その$C^{(J)}$に登録されている各$S_i^{(j)}$に送信する。$C^{(J)}$は、各$S_i^{(J)}$から、$eMes_i^{(J)}$を含んだ応答を受信する。そして、$C^{(J)}$は、$\{eMes_i^{(J)}\}_M$を含んだ応答（$M = sysID_i^{(J)} \in SYSIDPart$）を、$U_M$（APP）に送信し、$U_M$（APP）が、その応答を受信する。
【０１１０】
このように、U_M（APP）が、$C^{(1)}$以外の全ての$C^{(j)}$の各々にtpwを通知し（tpwを関連付けたtpw発行リクエストを送信し）、$C^{(1)}$以外の全ての$C^{(j)}$の各々から（つまり各$C^{(J)}$から）、$\{eMes_i^{(J)}\}_M$を含んだ応答を受信する。この一連の処理が終わった場合に、Uは、その日１日、同じtpwを使用して、いずれの$C^{(j)}$（ここではjは１以上の整数）に登録されているいずれの$S_i^{(j)}$にもログイン可能である（サービスを受けることができる）。なお、Uが登録されている制御センタのうち$C^{(1)}$以外のいずれかの$C^{(j)}$との通信にエラーが生じた場合、U_M（APP）と$C^{(1)}$とのtpw発行フローから処理がやり直されてもよい。
【実施例３】
【０１１１】
以下、実施例３を説明する。その際、実施例１及び２との相違点を主に説明し、実施例１及び２との共通点については説明を省略又は簡略する。
【０１１２】
実施例２では、U_M（APP）が各$C^{(j)}$に対してtpw発行リクエストを送信する必要があるため、U_M（APP）が行う通信の回数が多くなる。
【０１１３】
そこで、実施例３では、$C^{(j)}$が情報をやり取りすることで、U_M（APP）が行う通信の回

数を減らすことができる（例えば、U_M（APP）は２以上の$C^{(j)}$のうち$C^{(1)}$とのみ通信を行なえばよい）。

【０１１４】

以下、実施例３を詳細に説明する。その際、記載を簡単にするため、以下の表記ルールを採用する。

・$SYSIDGroup^{(j)}{}_{SYSIDPart,\ aID}$：pListにおいて、AIDがaIDとなる全ての$sysID_x^{(j)}$（∈SYSIDPart）からなる集合（xは、iの値がいずれでもよいことを意味する）

・$AID_{SYSIDPart}$：pListにおける各$sysID_x^{(x)}$∈SYSIDPart⊂SYSIDGroupに対するAIDの集合（下付きのxは、iの値がいずれでもよいことを意味し、上付きのxは、jの値がいずれでもよいことを意味する）

・$Pass_{SYSIDPart,\ aID}$：SYSIDがSYSIDPartの元であり、AIDがaIDとなる全てのアカウントのPASSからなる集合

【０１１５】

図１８は、実施例３に係るtpw発行フローの一例を示す。

【０１１６】

（ステップ１８０１）Uは、SYSIDPart（⊂SYSIDGroup）を選択し、U_M（APP）にreqPw及びSYSIDPartを入力する。このとき、$AID_{SYSIDPart}$は、{aID1，…，aIDN}であるとする。以下、１つのaIDWを例に取る（1≦W≦N）である。aIDWに対応したjを、「JW」であるとする。U_M（APP）は、aIDWを保持したアカウントを１つ選び、tReqPwW（$= h_{JW}$（Rand，pSYSID））を計算し（ただし、そのアカウントのSYSID=$sysID_{IW}^{(JW)}$としRAND＝RandWとする）、PASS（$Pass_{IW}^{(JW)} \in Pass_{SYSIDPart,\ aIDW}$）を取得する。取得されたPASSを、PassWとする。その後、U_M（APP）は、SYSIDPart及び$\{tReqPwW, PassW\}_{1 \leqq W \leqq N}$をいずれかの$C^{(JW)}$（ここでは$C^{(J1)}$とする）に送信する。

【０１１７】

（ステップ１８０２）$C^{(J1)}$は、PassWが正しいか否かを判断する。

【０１１８】

（ステップ１８０３）ステップ１８０２の判断結果が肯定の場合、$C^{(J1)}$は、$aList^{(J1)}$を参照し、Pass1に含まれるaID1と同一のAIDを保持し且つSYSID（$sysID_i^{(J1)}$）がSYSIDPartの元となる各アカウントに対して、そのMID（$mID_i^{(J1)}$）を取得する。ステップ１８０２の判断結果が否定の場合、$C^{(J1)}$は、全ての$sysID_i^{(J1)} \in SYSIDGroup^{(J1)}{}_{SYSIDPart,\ aID1}$に各々について、状態$st_i^{(J1)}$の値を“false”とする。$C^{(J1)}$が、$S_i^{(j)}$毎に$st_i^{(J1)}$を管理する。$st_i^{(J1)}$は、tpwの登録が成功したか（true）か否か（false）を意味する。

【０１１９】

（ステップ１８０４）$C^{(J1)}$は、tpwを発行し、ステップ１８０２の判断結果が肯定の場合に特定された各$S_i^{(J1)}$に、tpw及び$mID_i^{(J1)}$を送信する。

【０１２０】

（ステップ１８０５）tpw及び$mID_i^{(J1)}$を受信した$S_i^{(J1)}$は、$mID_i^{(J1)}$が登録されているアカウントを$uList_i^{(J1)}$から特定し、$tpwInfo_i^{(J1)}$を定め、その$tpwInfo_i^{(J1)}$を含んだ$mes_i^{(J1)}$を生成する。$S_i^{(J1)}$は、特定したアカウントに、TPWとして、受信したtpwを登録し、TPWINFOとして、定めた$tpwInfo_i^{(J1)}$を登録する。また、$S_i^{(J1)}$は、$st_i^{(J1)}$の値を“true”とする。なお、$S_i^{(J1)}$における当該Uが存在しない等の場合、$st_i^{(J1)}$の値を“false”とする。

【０１２１】

（ステップ１８０６）各$S_i^{(J1)}$（∈SYSIDPart）は、当該アカウントに登録されているSUKEY（$suKey_i^{(J1)}$）を取得し、状態$st_i^{(J1)}$の値と、$eMes_i^{(J1)}=Enc_{SUKEY}(mes_i^{(J1)})$を$C^{(J1)}$に送信する（SUKEY= $suKey_i^{(J1)}$）。この段階で、$C^{(J1)}$は、$C^{(J1)}$に登録されている全ての$S_i^{(J1)}$（∈SYSIDPart）から$st_x^{(x)}$の値および$mes_x^{(x)}$を受け取ったことになる。この後、$C^{(J1)}$は、2≦W≦Nに対して以下を実行する。ここでは、各W（≠１）に対してJW≠J1とする。JW＝J1となるWが存在する場合は、$C^{(J1)}$自身が、各$S_i^{(JW)}$（$=S_i^{(J1)}$）に対して、tpwを新たに発行せず同一tpwを使い、ステップ１８０２～ステップ１８０６までと同様

の処理をすればよい。

【０１２２】

（ステップ１８０７）$C^{(J1)}$は、$SYSIDGroup^{(JW)}{}_{SYSIDPart,\ aIDJW}$、tReqPwW及びPassWを、$C^{(JW)}$に送信する。

【０１２３】

（ステップ１８０８）$C^{(JW)}$は、PassWが正しいか否かを判断する。この判断結果が肯定の場合、$C^{(JW)}$は、PassWに含まれるaIDWを用いてaList$^{(JW)}$からアカウントを特定し、MID（$\{mID_i{}^{(JW)}\}_B$）を取得し（B= SYSID∈$SYSIDGroup^{(JW)}{}_{SYSIDPart,\ aIDJW}$）、一時的に$st_i{}^{(JW)}$の値を“true”とする。PassWが正しくない場合は全てのサービスシステムについて（何らかの理由でMIDが取得できない場合は、MIDを取得できないサービスシステムについて）、$C^{(JW)}$は、$st_i{}^{(JW)}$の値を“false”とする。

【０１２４】

（ステップ１８０９）$C^{(JW)}$は、$st_i{}^{(JW)}$＝trueとなる各$S_i{}^{(JW)}$∈$SYSIDGroup^{(JW)}{}_{aIDw}$に対するアクセストークン（$token_i{}^{(JW)}$）を生成する。$C^{(JW)}$は、$token_i{}^{(JW)}$と、$st_i{}^{(JW)}$と、$mID_i{}^{(JW)}$とを、$C^{(J1)}$に送信する（$token_i{}^{(JW)}$が、$st_i{}^{(JW)}$、$mID_i{}^{(JW)}$を含んでもよい）。この段階で、$C^{(J1)}$は、$C^{(J2)}$,…, $C^{(JW)}$の各々から、$\{st_i{}^{(JW)}, mID_i{}^{(JW)}, token_i{}^{(JW)}\}_B$から受け取っている（B= SYSID∈$SYSIDGroup^{(JW)}{}_{SYSIDPart,\ aIDJW}$）。

【０１２５】

（ステップ１８１０）$C^{(J1)}$は、$st_i{}^{(JW)}$＝trueとなる$S_i{}^{(JW)}$に対してのみ、$mID_i{}^{(JW)}$、tpw及び$token_i{}^{(JW)}$を送信する。

【０１２６】

（ステップ１８１１）$mID_i{}^{(JW)}$、tpw及び$token_i{}^{(JW)}$を受信した各$S_i{}^{(JW)}$は、$token_i{}^{(JW)}$が正しいか否かを判断する。この判断結果が肯定の場合、$S_i{}^{(JW)}$は、$mID_i{}^{(JW)}$が登録されているアカウントを$uList_i{}^{(JW)}$から特定し、$tpwInfo_i{}^{(JW)}$を定め、その$tpwInfo_i{}^{(JW)}$を含んだ$mes_i{}^{(JW)}$を生成する。$S_i{}^{(JW)}$は、特定したアカウントに、TPWとして、受信したtpwを登録し、TPWINFOとして、定めた$tpwInfo_i{}^{(JW)}$を登録する。$S_i{}^{(JW)}$は、$eMes_i{}^{(JW)}=Enc_{SUKEY}(mes_i{}^{(JW)})$を生成する（SUKEY=$suKey_i{}^{(JW)}$）。$S_i{}^{(JW)}$は、$st_i{}^{(JW)}$の値を“true”とする。$S_i{}^{(JW)}$は、$st_i{}^{(JW)}$と$eMes_i{}^{(JW)}$とを$C^{(J1)}$に返す。なお、$token_i{}^{(JW)}$が正しくない等の場合、$S_i{}^{(JW)}$は、$st_i{}^{(JW)}$の値を“false”とし、その$st_i{}^{(JW)}$を$C^{(J1)}$に返してよい。

【０１２７】

（ステップ１８１２）$C^{(J1)}$は、$S_i{}^{(JW)}$から、$st_i{}^{(JW)}$と$eMes_i{}^{(JW)}$とを含んだ応答を受信する。

【０１２８】

（ステップ１８１３）$C^{(J1)}$は、各$S_i{}^{(JW)}$∈$SYSIDGroup^{(JW)}{}_{aIDw}$（2≦w≦N）から、$st_i{}^{(JW)}$と$eMes_i{}^{(JW)}$とを含んだ応答を受信した場合、ステップ１８０４で発行したtpwと、全ての（$st_i{}^{(JW)}$, $eMes_i{}^{(JW)}$）を、U_M（APP）に返す。

【０１２９】

U_M（APP）が各$eMes_i{}^{(JW)}$を復号化することにより、Uは、全ての$S_i{}^{(JW)}$⊂SYSIDPartで使用できるtpwと、各$S_i{}^{(JW)}$⊂SYSIDPartから送られてきた$tpwInfo_i{}^{(JW)}$（tpw使用期限等を含んだ情報）を得ることができる。

【０１３０】

図１８に示したtpw発行フローの具体例を、図１９に示す。すなわち、Uが、$S_1{}^{(1)}$、$S_2{}^{(1)}$、$S_1{}^{(2)}$、及び$S_2{}^{(2)}$に登録されており、Uが、$S_1{}^{(1)}$及び$S_2{}^{(2)}$についてのtpw（共通1-dayパスワード）の発行リクエストを送信するとき（SYSIDPart＝$\{S_1{}^{(1)}, S_2{}^{(2)}\}$ のとき）、U_M（APP）、$C^{(1)}$、$C^{(2)}$、$S_1{}^{(1)}$、$S_2{}^{(2)}$間のやり取りは、図１９の通りである（図１８に記載のステップ番号と同じステップ番号を使用）。図１９では、$C^{(J1)}$を$C^{(1)}$とし、$C^{(JW)}$を$C^{(2)}$としている。

【実施例４】

【０１３１】

以下、実施例４を説明する。その際、実施例１～３との相違点を主に説明し、実施例１

～３との共通点については説明を省略又は簡略する。

【０１３２】

実施例４では、複数の$C^{(JW)}$に登録されている複数の$S_i^{(JW)}$に共通のパスワード（tpw）の発行に関し、$C^{(J1)}$が、他の$C^{(JW)}$に登録されている$S_i^{(JW)}$に関する登録処理をその$C^{(JW)}$に任せる。

【０１３３】

図２０は、実施例４に係るtpw発行フローの一例を示す。図１９との相違点を主に説明する。その際、$C^{(J1)}$を$C^{(1)}$とし、$C^{(JW)}$を$C^{(2)}$とする。

【０１３４】

ステップ１８０１～ステップ１８０６と同じ処理が行われる（ステップ２００１～ステップ２００６）。$C^{(1)}$が、$sysID_2^{(2)}$、$tReqPw^{(2)}$及び$Pass_2^{(2)}$に加えてtpwを$C^{(2)}$に送信し（ステップ２００７）、$C^{(2)}$が、tpw、$sysID_2^{(2)}$、$tReqPw^{(2)}$及び$Pass_2^{(2)}$を$C^{(1)}$から受信し、$Pass_2^{(2)}$が正しいか否かを判断する（ステップ２００８）。その判断結果が肯定の場合、$C^{(2)}$が、tpw及び$mID_2^{(2)}$を、$S_2^{(2)}$に送信する（ステップ２００９）。$S_2^{(2)}$が、tpw及び$tpwInfo_2^{(2)}$を$uList_2^{(2)}$に登録し（ステップ２０１０）、$st_2^{(2)}$と$eMes_2^{(2)}$を$C^{(2)}$に返す（ステップ２０１１）。$C^{(2)}$が、その$st_2^{(2)}$と$eMes_2^{(2)}$を$C^{(1)}$に送信する（ステップ２０１２）。つまり、$st_2^{(2)}$と$eMes_2^{(2)}$が、$S_2^{(2)}$から$C^{(2)}$を通じて$C^{(1)}$に送られる。その後、$C^{(1)}$は、tpwと、$S_1^{(1)}$及び$S_2^{(2)}$からそれぞれ受信した（$st_1^{(1)}$, $eMes_1^{(1)}$）及び（$st_2^{(2)}$, $eMes_2^{(2)}$）とを、U_M（APP）に返す（ステップ２０１３）。

【０１３５】

$S_i^{(JW)}$（JW≠J1）は、$C^{(J1)}$に登録されたサービスシステムではないので、本来、$C^{(J1)}$は$S_i^{(JW)}$に対してtpwを登録できない。そこで、上述の実施例３では、$C^{(JW)}$が、自身の$sList_i^{(JW)}$に登録されている$S_i^{(JW)}$に対して、tpw登録できるためのアクセストークン（$token_i^{(JW)}$）を発行し、$S_i^{(JW)}$における$mID_i^{(JW)}$と共に$C^{(J1)}$に送信する。$C^{(JW)}$と各$S_i^{(JW)}$との間に秘密鍵$ckey_i^{(JW)}$が共有されていることで、$mID_i^{(JW)}$を暗号化して$C^{(J1)}$に送信できる。$token_i^{(JW)}$は、使い捨ての署名でもよいが、$token_i^{(JW)}$の使用期限や権限の制限等が$token_i^{(JW)}$に関連付けられていてよく、その場合、$C^{(J1)}$は、最初に受けた$sysID_i^{(JW)}$、$mID_i^{(JW)}$、$token_i^{(JW)}$を次回以降も使うことができる。このため、$C^{(J1)}$と$C^{(JW)}$間の通信、及び、$C^{(JW)}$と$S_x^{(JW)}$間の通信を、省略できる。

【実施例５】

【０１３６】

以下、実施例５を説明する。その際、実施例１～４との相違点を主に説明し、実施例１～４との共通点については説明を省略又は簡略する。

【０１３７】

実施例３及び４は、いわゆるＩＤ連携をベースとした方式が採用されるが（mIDが制御センタ間で連携される）、実施例５では、ＳＡＭＬ（Security Assertion Markup Language）のようなシングルサインオンをベースとした方式が採用される。$S_2^{(2)}$（$S_i^{(JW)}$）が、ポリシー実行ポイント２１００としての機能を有する。

【０１３８】

図２１は、実施例５に係るtpw発行フローの一例を示す。図１９との相違点を主に説明する。

【０１３９】

ステップ１８０１～ステップ１８０６と同じ処理が行われる（ステップ２１０１～ステップ２１０６）。$C^{(1)}$が、$sysID_2^{(2)}$、$tReqPw^{(2)}$及び$Pass_2^{(2)}$を$C^{(2)}$に送信する（ステップ２１０７）。$C^{(2)}$が、tpw、$sysID_2^{(2)}$、$tReqPw^{(2)}$及び$Pass_2^{(2)}$を$C^{(1)}$から受信し、$Pass_2^{(2)}$が正しいか否かを判断する（ステップ２１０８）。

【０１４０】

ステップ２１０８の判断結果が肯定の場合、$C^{(2)}$は、認証状態、属性（$mID_2^{(2)}$等）、利用権限（パスワード登録）などのアサーション（$mID_2^{(2)}$等を含んだ情報）を、$S_2^{(2)}$へ送信する（ステップ２１０９）。言い換えれば、$C^{(2)}$（$C^{(JW)}$）は、$uList_2^{(2)}$（$uList_i^{(J}$

$^{W)}$）に登録されているmID $_2^{(2)}$（$mID_i^{(JW)}$）を、$C^{(1)}$（$C^{(J1)}$）に通知する必要が無い。

【０１４１】

$S_2^{(2)}$が、ポリシー実行ポイント２１００によりアサーションが正しいか否かを判断する（ステップ２１１０）。$S_2^{(2)}$は、その判断結果が肯定の場合、その判断結果（OK）を$C^{(1)}$に通知してもよいし、その判断結果を$C^{(1)}$に通知せず保持しておいてもよい。

【０１４２】

$C^{(1)}$が、tpwを、$S_2^{(2)}$に通知する（ステップ２１１１）。例えば、$C^{(1)}$が、$sysID_2^{(2)}$に対応した$S_2^{(2)}$との通信に必要な情報を知っていてその情報を使用して$S_2^{(2)}$に通知を送信してもよいし、$C^{(2)}$が、$S_2^{(2)}$にアサーションを送信するとき等のタイミングで、$S_2^{(2)}$との通信に必要な情報を$C^{(1)}$に通知してもよい。また、$C^{(1)}$から$S_2^{(2)}$へのtpw通知は、$S_2^{(2)}$からの上記判断結果に応答して行われてもよいし、$S_2^{(2)}$からの上記判断結果無しに例えば定期的に行われてもよい。$S_2^{(2)}$が、$C^{(1)}$からtpwを受信した場合、$tpwInfo_2^{(2)}$を決定し、tpwと$tpwInfo_2^{(2)}$を$uList_2^{(2)}$に登録する（ステップ２１１２）。この登録は、ステップ２１１０の判断結果が肯定の場合に行われる。

【０１４３】

その後、$S_2^{(2)}$が、$st_2^{(2)}$と$eMes_2^{(2)}$を$C^{(1)}$に返す（ステップ２１１３）。$C^{(1)}$は、tpwと、$S_1^{(1)}$及び$S_2^{(2)}$からそれぞれ受信した（$st_1^{(1)}$, $eMes_1^{(1)}$）及び（$st_2^{(2)}$, $eMes_2^{(2)}$）とを、U_M（APP）に返す（ステップ２１１３）。

【実施例６】

【０１４４】

以下、実施例６を説明する。その際、実施例１～５との相違点を主に説明し、実施例１～５との共通点については説明を省略又は簡略する。

【０１４５】

実施例１～５では、tpw発行が行われる。実施例６では、tpw発行に代えて又は加えて、tpwに関する他種の制御、例えば、tpw変更、tpw削除等が行われる。具体的には、例えば、tpw発行リクエストは、tpw制御リクエストの一例である。tpw制御の一例が、tpw発行であり、制御センタ（識別符号制御装置又は識別符号制御システム）の一例が、制御センタである。tpw制御リクエストに関連付けられる情報要素は、tpw発行リクエストに関連付けられる情報要素と同じでよい。ＡＰＰは、tpw発行に加えてtpw発行以外のtpw制御にも使用される。以下、tpw制御リクエストの別の一例として、tpw削除を例に取り、tpw制御を説明する。なお、「tpw削除」とは、「tpw認証を無効化して、次にtpw発行依頼するまで、Uを含め誰もログインできないようにすること」を意味する。

【０１４６】

図６は、実施例６に係るtpw削除フローの一例を示す。

【０１４７】

（ステップ２２０１）U_M（APP）が、図１４のステップ１４０１と同様の処理を行う。但し、本実施例では、tpw発行リクエストに代えてtpw削除リクエストが送信される。

【０１４８】

（ステップ２２０２）$C^{(1)}$は、tpw削除リクエストをU_M（APP）から受信し、そのリクエストに応答して、そのリクエストに関連付いている$Pass_i^{(1)}$が正しいか否かを判断する。

【０１４９】

（ステップ２２０３）$C^{(1)}$は、ステップ２２０２の判断結果が肯定の場合、$aList^{(1)}$を参照し、正しいと判断された$Pass_i^{(1)}$内の$aID^{(1)}$と一致するAIDを有し、且つ、tpw削除リクエストに関連付いているSYSIDPart内のいずれかの$sysID_i^{(1)}$と一致するSYSIDを有するアカウントを全て特定する。$C^{(1)}$は、特定された全てのアカウントからそれぞれMID（$mID_i^{(1)}$）を取得する。

【０１５０】

（ステップ２２０４）$C^{(1)}$は、各$sysID_i^{(1)}$（∈SYSIDPart）について、以下を行う。ステップ２２０４～ステップ２２０７の説明において、１つの$sysID_i^{(1)}$を例に取る。$C^{(1)}$は、$sysID_i^{(1)}$にに対応した$S_i^{(1)}$に、その$S_i^{(1)}$に対応する$mID_i^{(1)}$を関連付けたtpw削除

リクエストを送信する。

【０１５１】

（ステップ２２０５）$S_i^{(1)}$が、$mID_i^{(1)}$が関連付いたtpw削除リクエストを$C^{(1)}$から受信する。$S_i^{(1)}$は、受信したリクエストに関連付いている$mID_i^{(1)}$と一致するMIDが登録されているアカウントを$uList_i^{(1)}$から特定する。$S_i^{(1)}$は、特定したアカウント上の認証要素tpw及びtpwInfoを削除する。

【０１５２】

（ステップ２２０６）$S_i^{(1)}$は、削除完了の応答を、$C^{(1)}$に送信する。

【０１５３】

（ステップ２２０７）$C^{(1)}$は、$sysID_i^{(1)}$（∈SYSIDPart）にそれぞれ対応した全ての$S_i^{(1)}$から応答を受信した場合に、tpw削除リクエストに対する応答を、U_M（APP）に送信する。U_M（APP）が、応答を$C^{(1)}$から受信する。

【０１５４】

実施例６によれば、選択された$Pass_i^{(1)}$に対応する$aID^{(j)}$と同一の$aID^{(j)}$を保持する全てのアカウントにそれぞれ対応した全ての$S_i^{(j)}$に対し、tpwについての制御を行うことができる。例えば、tpwの削除は、tpwに代えて使用期限及び使用回数に制限の無いパスワードが共通パスワードとして採用されている場合に有効であると考えられる（つまり、実施例では、採用されるパスワードは、共通1-dayパスワードであるが、そのような制限パスワードに限らず、使用期限及び使用回数等の制限の無いパスワードが採用されてもよい）。

【実施例７】

【０１５５】

以下、実施例７を説明する。その際、実施例１～６との相違点を主に説明し、実施例１～６との共通点については説明を省略又は簡略する。

【０１５６】

実施例７では、少なくとも１つの$S_i^{(j)}$は、特定の制御センタに、$Info_i^{(j)}$を送信する。「特定の制御センタ」は、例えば、その$S_i^{(j)}$が登録されている制御センタ、所定種類の情報要素（例えばtpw又は$mID_i^{(j)}$）の送信元の制御センタ、又は、U_M（APP）からtpw制御リクエストを受信した制御センタである。「$Info_i^{(j)}$」は、$Info_i^{(j)}$の発行元の$S_i^{(j)}$から出力された情報でありその$S_i^{(j)}$以外のサービスシステムに公開されてよい情報を含んだ情報である（$Info_i^{(j)}$に含まれる情報は、Uにより公開が許可された情報でよい）。$Info_i^{(j)}$は、例えば事前登録において$S_i^{(j)}$からの応答（例えば、図１２のステップ１２０３の応答、図１３のステップ１３０３の応答）に含まれてもよいし、tpw発行等の制御において$S_i^{(j)}$からの応答（例えば、図１４のステップ１４０６の応答、図１８のステップ１８１２の応答、図２０のステップ２０１１及びステップ２０１２のうちの少なくとも１つの応答、図２１のステップ２１１３）に含まれてもよい。これにより、図２３に示すように、$Info_i^{(j)}$を発行した$S_i^{(j)}$の$uList_i^{(j)}$には、その発行された$Info_i^{(j)}$が登録される（INFO）。また、特定の制御センタに、$Info_i^{(j)}$が集まり、図２４に示すように、その制御センタの$aList^{(j)}$に、$Info_i^{(j)}$が登録される。$Info_i^{(j)}$は、公開が許可された情報に関する情報として、許可された公開先サービスシステムに関する情報（例えば、$sysID_i^{(j)}$、サービスシステムを提供する企業の名称）、公開されている期間等を含んでよい。

【０１５７】

Uから申請を受けた$S_i^{(j)}$は、その申請の処理に所定種類の情報を必要とする場合、上記特定の制御センタ（又は、申請を受けた$S_i^{(j)}$が登録されている$C^{(j)}$）に、その所定種類の情報の問合せ（例えば、申請元のUに対応した$mID_i^{(j)}$が関連付けられた問合せ）を送信してよい（その問合せは、その問合せを$S_i^{(j)}$から受けた$C^{(j)}$から、上記特定の制御センタに転送されてもよい）。その問合せを受けた制御センタが、その問合せ応答して、$mID_i^{(j)}$に対応した$Info_i^{(j)}$内の情報であり公開が許可されている情報（例えば、履歴書、住民票）を、問合せ元の$S_i^{(j)}$に送信してよい。

【実施例８】
【０１５８】
以下、実施例８を説明する。その際、実施例１～７との相違点を主に説明し、実施例１～７との共通点については説明を省略又は簡略する。なお、実施例８は、実施例７の変形例又は具体例でよい。
【０１５９】
Uが登録されている個々のサービスシステムは、Uの個人情報（例えば、卒業証明書、資格証明書、履歴書、カルテ、マイナンバー（及びそれに付随する情報）等）を管理している。少なくともUが許可する範囲で、Uの個人情報が、サービスシステム間で連携されるようになっていると、利便性の向上が期待される。また、連携される情報は、Uの個人情報に代えて又は加えて、Uに関する他種の情報も考えられるが、少なくとも連携対象の情報の種類によっては、連携対象の情報の少なくとも一部が、不特定者（例えば、U及びUが許可する者（例えば、連携元と連携先）以外の者）に閲覧されてはならない。
【０１６０】
実施例８では、不特定者に情報が閲覧されること無しにその情報をサービスシステム間で連携できる。
【０１６１】
また、実施例８では、登録フローにおいて、Uは、$S_i^{(j)}$に情報が登録されたことを知ることができる。
【０１６２】
また、実施例８では、$C^{(j)}$と$S_i^{(j)}$に、認可情報の委譲に関する既存の仕様、例えばOAuthを適用可能である。
【０１６３】
以下、実施例８に係る登録フロー及び情報連携（Information Sharing）フローの各々の一例を説明する。
【０１６４】
図３１は、実施例８に係る登録フローの一例を示す。なお、以下、説明を分かり易くするため、$C^{(j)}$として、$C^{(1)}$のみが存在することとする（図３１は、複数の$S_i^{(1)}$のうち$S_1^{(1)}$のみを示す）。
【０１６５】
登録フローが終了した時点において、下記の情報要素がU_Mに保存されている。下記の情報要素は、pListに登録される。また、下記の情報要素のうちの少なくとも１つが、U_M固有の情報を含む情報を鍵として暗号化されてから保存されてよい。
・$Pass_i^{(1)}$：$C^{(1)}$に送信するリクエストの承認を依頼する情報（リクエスト依頼パス）。
・$suKey_i^{(1)}$：$S_i^{(1)}$と通信する際に必要な共有鍵。
【０１６６】
登録フローが終了した時点において、下記の情報要素が$S_i^{(1)}$に保存されている。下記の情報要素は、$uList_i^{(1)}$に登録される。下記の情報要素のうちの少なくとも１つは暗号化されてから保存されてもよい。
・$uID_i^{(1)}$：$S_i^{(1)}$の利用のためのユーザＩＤでありUと$S_i^{(1)}$との間で共有される情報。
・$authInfo_i^{(1)}$：Uの認証情報（例えばTempPw以外のパスワード（例えば固定パスワード））。
・$verAuthInfo_i^{(1)}$：$authInfo_i^{(1)}$を検証するための情報。
・$mID_i^{(1)}$：$S_i^{(1)}$の管理用ＩＤであり、$C^{(1)}$と$S_i^{(1)}$との間で共有される情報（U毎に異なる）。なお、情報連携の際には、連携元又は連携先の$mID_i^{(1)}$が保存される。
・$suKey_i^{(1)}$：U_Mと通信する際に必要な共有鍵。
・verRegToken：登録完了チェックトークン（regToken）を検証するための情報。
・TempPw：一時的なパスワード（例えばtpw）。
・TempPwInfo：TempPwの制限に関する情報であり、例えば、有効期限（period）、使用回数（TempPwTimes）及び使用可能回数（TempPwTimesMax）のうちの少なくとも１つを含む

。
・sID：連携ＩＤ。情報連携の際に使用されるＩＤであり連携を一意に識別するためのＩＤである。
・$AttList_i^{(1)}$：情報属性（att）のリスト（詳細は後述）。
【０１６７】
登録フローが終了した時点において、下記の情報要素が$C^{(1)}$に保存されている。下記の情報要素は、$aList^{(1)}$、$sList^{(1)}$及び$cList^{(1)}$のうちの少なくとも$aList^{(1)}$に登録される。下記の情報要素のうちの少なくとも１つは暗号化されてから保存されてもよい。
・$mID_i^{(1)}$：$S_i^{(1)}$の管理用ＩＤであり、$C^{(1)}$と$S_i^{(1)}$との間で共有される情報（U毎に異なる）。なお、情報連携の際には、連携元の$mID_i^{(1)}$と連携先の$mID_i^{(1)}$とが保存される。
・verTicket：$aList^{(1)}$のアカウントに対する登録チケット（ticket）の検証に必要な情報である。
・$aID^{(1)}$：APPのＩＤ。上述したように、１つの$C^{(j)}$及び１つのAPPにつき異なる複数の$aID^{(1)}$が存在することもある。
・tReqPw：リクエストパスワード。
・$verPass_i^{(1)}$：$Pass_i^{(1)}$の検証（U_Mの機器認証）に必要な情報。
・sID：連携ＩＤ。
・$sysID_i^{(1)}$：$S_i^{(1)}$のサービスシステムＩＤ。
・att：情報属性（例えば氏名、電子メールアドレス等）。attとして、提供可能なattと受入可能なattとが保存されている。１以上のatt値（attに従う値）を含んだ情報が連携対象情報（Info）である。
・eInfo：暗号化された連携対象情報（Info）。
・AccessToken：OAuthのアクセストークンであって、$C^{(1)}$と$S_i^{(1)}$との間での通信に使用されるトークン。
【０１６８】
実施例８に係る登録フローは、図３１に示す通り、下記の通りである。
【０１６９】
登録フローは、U と$S_i^{(1)}$間の手続きである第１の登録手続きと、U と$C^{(1)}$間の手続きである第２の登録手続きとで構成される。第１の登録手続きは、下記の（Ｒ１）～（Ｒ６）で構成され、第２の登録手続きは、下記の（Ｒ７）～（Ｒ１０）で構成される。
【０１７０】
（Ｒ１）U_M（例えばAPP）は、$S_i^{(1)}$の方針に従うユーザ情報を$S_i^{(1)}$に送信し、$S_i^{(1)}$にログインするための$uID_i^{(1)}$及び$authInfo_i^{(1)}$を定める。
【０１７１】
（Ｒ２）$S_i^{(1)}$は、（Ｒ１）で受け取ったユーザ情報を、必要に応じて変換し保存する。
【０１７２】
（Ｒ３）$S_i^{(1)}$は、$sysID_i^{(1)}$及び登録パスワード（rpw）が関連付けられたアカウント追加リクエストを$C^{(1)}$に送信する。なお、rpwは、U自身が決めてU_M（又はU_P）により$S_i^{(1)}$に知らせた情報もよいし、$S_i^{(1)}$により決められた情報でもよい。$C^{(1)}$は、$sysID_i^{(1)}$及びrpwが関連付けられているアカウント追加リクエストを受信する。
【０１７３】
（Ｒ４）$C^{(1)}$は、アカウント追加リクエストに応答して、次の処理を行う。すなわち、$C^{(1)}$は、アカウントを１つ作成し（例えば$aList^{(1)}$にアカウントを追加し）、そのアカウントに対して、$mID_i^{(1)}$を割り当てる（登録する）。更に、$C^{(1)}$は、そのアカウントに対する登録チケット（ticket）を生成する。その後、$C^{(1)}$は、割り当てた$mID_i^{(1)}$、受信した$sysID_i^{(1)}$、及び、verTicket（登録チケットの正当性を検証するために必要な情報）を、自身のデータベース（例えば$aList^{(1)}$）に登録する。ticketには、該当するアカウントを特定する情報が含まれている。$C^{(1)}$は、割り当てた$mID_i^{(1)}$、及び、生成したticketを、$S_i^{(1)}$に送信する。$S_i^{(1)}$は、$mID_i^{(1)}$及びticketを受信する。

【０１７４】
（Ｒ５）$S_i^{(1)}$は、アカウントを１つ追加し（$uList_i^{(1)}$にアカウントを１つ追加し）、U_Mとの暗号化通信に必要な鍵$suKey_i^{(1)}$を定め、$uID_i^{(1)}$、$mID_i^{(1)}$及び$suKey_i^{(1)}$をそのアカウントに登録する。さらに、$S_i^{(1)}$は、登録完了チェックトークン（regToken）を生成し，それを検証するために必要な情報（verRegToken）を、当該アカウントに登録する。
【０１７５】
（Ｒ６）$S_i^{(1)}$は、ticket、$suKey_i^{(1)}$及びregToken$を$U_M$に送信する。$U_M$は、ticket、$suKey_i^{(1)}$及びregTokenを受信する。なお、U自身がrpwを設定していない場合、$S_i^{(1)}$は、更にrpw$もU_M$に送信する。また、regTokenの設定及び送信は必須ではない。
【０１７６】
（Ｒ７）U_Mは、ticket、$suKey_i^{(1)}$、rpw、regToken及びreqPwを関連付けた登録リクエストを$C^{(1)}$に送信する。$C^{(1)}$は、ticket、$suKey_i^{(1)}$、rpw、regToken及びreqPwが関連付いている登録リクエストを受信する。ticket、$suKey_i^{(1)}$、rpw及びregTokenは、$S_i^{(1)}$から受信した情報でもよいし、Uにより入力された情報でもよい。reqPwは、U又はAPPにより定められた情報でよい。
【０１７７】
（Ｒ８）$C^{(1)}$は、登録リクエストに応答して、次の処理を行う。すなわち、$C^{(1)}$は、verTicket（及びrpw）を用いて、ticketの正当性を検証する。そのticketが正しい場合、$C^{(1)}$は、ticketからアカウントを識別し、識別されたアカウントに対して、$aID^{(1)}$及び$Pass_i^{(1)}$を生成し登録する。また、$C^{(1)}$は、その$aID^{(1)}$及び$Pass_i^{(1)}$と、登録リクエストに関連付いているreqPwとの検証に必要な情報（verTReqPw（tReqPwの検証に必要な情報）及び$verPass_i^{(1)}$（$Pass_i^{(1)}$の検証に必要な情報）を、識別されたアカウントに登録する。$Pass_i^{(1)}$には、$C^{(1)}$におけるアカウントを識別できる情報（例えば$aID^{(1)}$）、及び、Uが登録先$S_i^{(1)}$を識別できるための情報（例えば$sysID_i^{(1)}$）が含まれる。なお、$C^{(1)}$は、（Ｒ８）において、UにOAuth認証をさせて、その認証結果に基づくAccessTokenを暗号化してそのアカウントに登録してもよい。
【０１７８】
（Ｒ９）$C^{(1)}$は、$mID_i^{(1)}$及びregToken$をS_i^{(1)}$に送信する。$S_i^{(1)}$は、$mID_i^{(1)}$及びregTokenを受信し、受信した$mID_i^{(1)}$が登録されているアカウントにおけるverRegTokenを用いることにより、regTokenを検証する。regTokenが正当な場合、$S_i^{(1)}$は、そのアカウントが３者間認証を利用できる状態になったと認識する。
【０１７９】
（Ｒ１０）$C^{(1)}$は、$Pass_i^{(1)}$をU_Mに送信する。U_Mは、$Pass_i^{(1)}$を受信し、$Pass_i^{(1)}$及び$suKey_i^{(1)}$を保存する。
【０１８０】
以上が、実施例８に係る登録フローの説明である。なお、実施例８において、登録フローは、図３１を参照して説明した登録フローに代えて、他の実施例での登録フローが適用されてもよい。或いは、実施例８に係る登録フローは、他の実施例で適用されてもよい。また、実施例８に代えて又は加えて他の実施例でもOAtuthが適用されてもよいが、少なくともOAtuthは本発明に必須ではない。
【０１８１】
図２５は、実施例８に係る認証／連携フローの一例を示す。なお、以下の説明では、$S_i^{(j)}$として、$S_1^{(1)}$及び$S_2^{(1)}$を含む複数の$S_i^{(1)}$が存在することとする。また、以下の説明では、Uが、$S_1^{(1)}$（サービスＡ）の利用にあたり、$S_1^{(1)}$が所望する情報が$S_2^{(1)}$（サービスＢ）に保持されている情報と同じため、$S_2^{(1)}$に保持されている情報を$S_1^{(1)}$に提供したいとする。従って、$S_2^{(1)}$が、連携元サービスシステムであり、$S_1^{(1)}$が、連携先サービスシステムである。また、以下の説明では、冒頭に「（認証）」が付いている処理は、tpwのようなTempPw発行の場合のみ実行される処理である。冒頭に「（連携）」が付いている処理は、情報連携の場合のみ実行される処理である。冒頭に「（認証）」も「（連携）」も付いていない処理は、TempPw発行の場合と情報連携の場合のいずれの場合も実行される

処理である。

【０１８２】

（Ｐ１）

U_M（APP）は、opの選択をUから受ける。「op」は、リクエスト対象のオペレーション種類であり、具体的には、例えば、認証、情報連携、又はその両方である。「認証」が選択された場合、以降、冒頭に「（認証）」が付いている処理が行われることになる。「情報連携」が選択された場合、以降、冒頭に「（連携）」が付いている処理が行われることになる。「両方」が選択された場合、以降、冒頭に「（認証）」が付いている処理も「（連携）」が付いている処理も行われることになる。なお、冒頭に「（認証）」が付いている処理と冒頭に「（連携）」が付いている処理の重複部分は、一方の処理で行われたならば他方の処理では行われないでもよい。

U_M（APP）は、U_Mに保存されている全ての$Pass_i^{(1)}$から特定される$sysID_i^{(1)}$のリストを表示する。

（認証）：U_M（APP）は、表示したリストから、$aID^{(1)A}$（又は$sysID_1^{(1)}$）の選択を受ける。$aID^{(1)A}$は、Uがログイン先とする$S_1^{(1)}$（サービスＡ）の$sysID_1^{(1)}$が登録されているアカウントにおける$aID^{(1)}$である。

（連携）：U_M（APP）は、表示したリストから、$aID^{(1)A}$（又は$sysID_1^{(1)}$）及び$aID^{(1)B}$（又は$sysID_2^{(1)}$）の選択を受ける。$aID^{(1)A}$は、情報の連携先$S_1^{(1)}$の$sysID_1^{(1)}$が登録されているアカウントにおける$aID^{(1)}$である。$aID^{(1)B}$は、情報の連携元$S_2^{(1)}$の$sysID_2^{(1)}$が登録されているアカウントにおける$aID^{(1)}$である。

U_M（APP）は、選択されたopと、選択されたアカウントに対するPass（$Pass_1^{(1)}$及び$Pass_2^{(1)}$のうちの少なくとも$Pass_1^{(1)}$）と、tReqPwとを関連付けたリクエストを、$C^{(1)}$に送信する。tReqPwは、（Ｐ１）においてUから入力されたreqPw又はそれに基づく情報である。$C^{(1)}$は、op、Pass及びtReqPwが関連付いているリクエストを受信する。

【０１８３】

（Ｐ２）

$C^{(1)}$は、受信したリクエストに応答して、次の処理を行う。すなわち、$C^{(1)}$は、受信したPass及びtReqPwが登録されているアカウント（以下、対象アカウント）におけるverPass及びverTReqPwを用いてtReqPw及びPassの正当性を検証する。それらが正当な場合、$C^{(1)}$は、Passを基に特定される$aID^{(1)A}$（及び$aID^{(1)B}$)に対応する$mID_1^{(1)}$（及び$mID_2^{(1)}$）をアカウント（例えば$aList^{(1)}$）から見つける。

（連携）：$C^{(1)}$は、$aID^{(1)A}$（$mID_1^{(1)}$）に対応する$S_1^{(1)}$に対して、受け入れ可能な情報属性（att）のリスト（$AttList_1^{(1)}$）を照会し、且つ、$aID^{(1)B}$（$mID_2^{(1)}$）に対応する$S_2^{(1)}$に対して、提供可能な情報属性の属性リスト（$AttList_2^{(1)}$）を照会する。「$AttList_i^{(1)}$」は、情報属性（att）のリストであり、受け入れ可能なattと提供可能なattとのうちの少なくとも一方を含む。$AttList_i^{(1)}$は、受け入れ可能なattと提供可能なattとのうちの両方を含んでいて、$C^{(1)}$からの照会に応答して提供される際に、受け入れ可能なattと提供可能なattとのうちの一方に絞られてもよい。$AttList_i^{(1)}$は、$S_i^{(1)}$から事前に登録されたリストでもよく、その場合、照会手続きは省略されてよい。$S_i^{(1)}$は、上述したように、提供可能なatt及び受け入れ可能なattを予め保存している。

【０１８４】

（Ｐ３）

（連携）：$C^{(1)}$は、$AttList_1^{(1)}$及び$AttList_2^{(1)}$の共通部分（att）をU_Mに送信し、U_Mが、共通部分（att）を表示する。U_Mは、Uから、その共通部分のうちの、連携する情報属性attの選択を受け、選択されたattを、$C^{(1)}$に送信する。$C^{(1)}$は、選択されたattを受信する。

【０１８５】

（Ｐ４）

（認証）：$C^{(1)}$は、対象アカウントに対するtpwを生成する。ここでは、tpwが生成されることとするが、tpw以外の種類のTempPwが生成されてもよい。

（連携）：$C^{(1)}$は、この認証／連携フローで実行される情報連携に対して一意的なsIDを生成する。

【０１８６】

（Ｐ５）

（連携）：$C^{(1)}$は、（Ｐ４）で生成したsID、$mID_2^{(1)}$、（Ｐ３）で受信したatt、及び、連携先$S_1^{(1)}$の$sysID_1^{(1)}$を関連付けたリクエスト（情報提供リクエスト）を、連携元$S_2^{(1)}$に送る。その際、$C^{(1)}$は、OAuthのAccessTokenも、連携元$S_2^{(1)}$に送信してよい。OAuthのAccessTokenには、$authInfo_1^{(1)}$無しに連携先$S_1^{(1)}$に送信されてよい情報属性（att）が記述されていてよい。連携元$S_2^{(1)}$が、sID、$mID_2^{(1)}$、att、及び$sysID_1^{(1)}$（及びAccessToken）が関連付いているリクエストを受信する。

【０１８７】

（Ｐ６）

（連携）：連携元$S_2^{(1)}$は、そのリクエストに応答して、次の処理を行う。すなわち、連携元$S_2^{(1)}$は、$mID_2^{(1)}$に対応するUに対するatt値（受信したattに従う値）を含んだ連携対象情報Infoを、連携先$S_1^{(1)}$が復号可能な鍵で暗号化する。ここでは、サービスＢ（$S_2^{(1)}$）から連携される情報という意味で、Infoを、「InfoB」と表記し、暗号化されたInfoBを、サービスＡ（$S_1^{(1)}$）に連携される情報という意味で、「eInfoBA」と表記する。連携元$S_2^{(1)}$は、InfoBを$suKey_2^{(1)}$で暗号化する。その暗号化されたInfoBを、Uと共有される鍵で暗号化されたという意味で、「eInfoUB」と表記する。$S_2^{(1)}$は、sID、eInfoBA、及び、eInfoUBを、$C^{(1)}$に送る。$C^{(1)}$は、sID、eInfoBA、及び、eInfoUBを受信する。$C^{(1)}$は、受信したsID、eInfoBA、及び、eInfoUBを記憶部５１１に格納してよい。

【０１８８】

（Ｐ７）

（認証）：$C^{(1)}$は、$mID_1^{(1)}$及びtpwを関連付けたリクエストを、$S_1^{(1)}$に送信する。$S_1^{(1)}$は、$mID_1^{(1)}$及びtpwが関連付いているリクエストを受信する。

（連携）：$C^{(1)}$は、$mID_1^{(1)}$及びsIDを関連付けたリクエストを、連携先$S_1^{(1)}$に送信する。その際、$C^{(1)}$は、OAuthのAccessTokenも連携先$S_1^{(1)}$に送信してよい。連携先$S_1^{(1)}$は、$mID_1^{(1)}$及びsID（及びAccessToken）が関連付いているリクエストを受信する。

【０１８９】

（Ｐ８）

（認証）：$S_1^{(1)}$は、$mID_1^{(1)}$に該当するアカウントに、tpwと、そのtpwについてのtpwInfo（例えば、period、tpwTimesMax）とを登録し、tpw及びtpwInfoを含んだ情報を$suKey_1^{(1)}$で暗号化し、暗号化された情報であるeTpwInfoを$C^{(1)}$に返す。

（連携）：$S_1^{(1)}$は、sID及び$mID_1^{(1)}$を、データベース（例えば$uList_1^{(1)}$）における該当アカウントに登録する。

【０１９０】

（Ｐ９）

（認証）：$C^{(1)}$は、eTpwInfo（暗号化されたtpwを含む）をU_Mに送る。

（連携）：$C^{(1)}$は、eInfoUBをU_Mに送る。

【０１９１】

（Ｐ１０）

【０１９２】

U_Mは、（Ｐ９）で受け取った情報（eTpwInfo及びeInfoUBのうちの少なくとも一方）を、$suKey_2^{(1)}$を用いて復号し、復号化された情報を表示する。

（連携）：表示された情報は、連携対象情報である。U_M（APP）は、連携対象情報の連携を承認する（OK）かキャンセルするか（NG）の回答を受け付け、受け付けた回答を、$C^{(1)}$に通知してよい。Uは、連携対象情報の少なくとも一部に誤りがある、或いは連携したくなくなった等の場合に、「NG」を回答すればよい。回答が「NG」（キャンセル）を意味する場合、$C^{(1)}$は、連携をキャンセルする、すなわち、連携対象情報が連携先$S_1^{(1)}$に取得されることを不可能とする。具体的には、例えば、$C^{(1)}$は、回答「NG」を受信した場合に

、記憶部５１１に格納されたeInfoUB（及びeInfoBA及びsID）を記憶部５１１から削除する、又は、連携対象情報のアクセス権限から連携先$S_1^{(1)}$を除外する。

【０１９３】

（Ｐ１１）

【０１９４】

U_Pは、$S_1^{(1)}$にアクセスし、例えばログインのために、$uID_1^{(1)}$及び$authInfo_1^{(1)}$を$S_1^{(1)}$に入力する。

（認証）：U_Pは、更にtpwを$S_1^{(1)}$に入力する。

【０１９５】

（Ｐ１２）

【０１９６】

入力された情報（$uID_1^{(1)}$及び$authInfo_1^{(1)}$）が正しい場合、$S_1^{(1)}$は、U_Pのログインを許可する。

【０１９７】

（Ｐ１３）

（連携）：$S_1^{(1)}$は、$S_1^{(1)}$に登録されている$mID_1^{(1)}$宛ての連携処理に対するsIDを$C^{(1)}$に送信する。$C^{(1)}$は、そのsIDに関連付けられているeInfo（例えばeInfoBA）を、$S_1^{(1)}$に送信する。$S_1^{(1)}$は、そのeInfo（例えばeInfoBA）を受信し復号化する（これにより、InfoBが得られる）。

【０１９８】

上述した情報連携フローによれば、情報の連携は、Uからのリクエスト（許可）により可能となる。また、連携対象の情報、連携元及び連携先のいずれもUが指定可能である。このため、連携対象情報、連携元及び連携先を、Uの許可した範囲に制限できる。

【０１９９】

また、上述した情報連携フローによれば、連携対象の情報は、暗号化された状態で、連携元及び連携先以外の者により管理される記憶部５１１に格納され、その情報は、連携先である$S_2^{(1)}$により復号される。このため、連携対象の情報が不特定者に閲覧されることを防ぐことができる。

【０２００】

なお、上述した情報連携フローにおいて、$C^{(1)}$が、eInfoBAに加えて、そのeInfoBAがサービスＢ（$S_2^{(1)}$）からの情報であることの証明書も記憶部５１１に格納してよい。それに代えて又は加えて、$C^{(1)}$が、eInfoBAに加えて、そのeInfoBAがサービスＢ（$S_2^{(1)}$）からの情報であることの証明書も、$S_1^{(1)}$に送信してもよい。

【０２０１】

また、連携される情報の少なくとも一部は、ユーザ端末（U_P及びU_Mのうちの少なくとも１つ）に表示される情報に代えて又は加えて、情報連携先のサービスシステムへのアクセスキー（例えばURL等）のようなリンクであってもよい。また、そのリンクも、表示される情報の少なくとも一部であってよい。

【０２０２】

また、連携元と連携先は、上記例のような１：１に限らず、１：N（Nは２以上の整数）でも、M：１（Mは２以上の整数）でもよい。

【０２０３】

また、eInfoは、$S_2^{(1)}$から$C^{(1)}$（記憶部５１１）経由で$S_1^{(1)}$に送られるが、それに代えて、下記の（ａ）～（ｃ）のうちのいずれかが採用されてもよい。

（ａ）$C^{(1)}$が、InfoBをサービスＡ（$S_1^{(1)}$）に送ることを$S_2^{(1)}$にリクエストする。$S_2^{(1)}$が、そのリクエストに応答して、eInfo（又はInfoB（暗号化されていない連携対象情報））を$S_1^{(1)}$に送る。

（ｂ）$C^{(1)}$が、InfoをサービスＢ（$S_2^{(1)}$）から取得することを$S_1^{(1)}$にリクエストする。$S_1^{(1)}$が、そのリクエストに応答して、eInfoBA（又はInfoB）を$S_2^{(1)}$から取得する。

（ｃ）$S_2^{(1)}$が、eInfoBA（又はInfoB）の存在する場所（$S_2^{(1)}$の中又は外のストレージ装

置）を表すリンクを$C^{(1)}$に送る。$C^{(1)}$が、そのリンクに従い、eInfoBA（又はInfoB）を取得し、そのeInfoBA（又はInfoB）を$S_1^{(1)}$に送るか、或いは、$C^{(1)}$が、そのリンクを$S_1^{(1)}$に送り、$S_1^{(1)}$が、そのリンクに従い、eInfoBA（又はInfoB）を取得する。

【０２０４】

実施例８に係る情報連携は、Uの証明資料（例えば、卒業証明書、資格証明書、納税証明書、不動産登記簿等）をその証明資料を管理している大学又は団体等から企業等に提出することや、医療関係のカルテ等を病院間で受け渡しすることや、マイナンバー（及びそれに付随する情報）を企業間で受け渡しすること等、様々なケースに適用することが期待できる。

【０２０５】

実施例８によれば、情報連携をUが安心して任せられることが期待できる。なぜなら、$S_i^{(1)}$は、$C^{(1)}$から信用度等の観点から認められた場合に$C^{(1)}$に登録されることが期待されるからである。

【０２０６】

実施例７及び８のうちの少なくとも１つにおいて、下記の（０１）～（０５）のうちの少なくとも１つが採用されてよい。

【０２０７】

（０１）連携対象情報の少なくとも一部は暗号化されないでもよい。連携対象情報の少なくとも一部を暗号化するか否かは、ユーザにより選択されてもよいし（例えば、ステップ２５０１で、連携対象情報毎に暗号化するか否かをユーザが指定してもよいし）、連携対象情報の重要度又は種別に応じて連携元サービスシステムにより暗号化するか否かが制御されてもよい。

【０２０８】

（０２）連携対象情報の$EK_1^{(1)}$（暗号鍵）は、$S_1^{(1)}$の公開鍵でよく、連携対象情報の$DK_1^{(1)}$（復号鍵）は、$S_1^{(1)}$の秘密鍵でよい。また、その暗号鍵／復号鍵は、公開鍵／秘密鍵に代えて、共通鍵等の他種の鍵でもよい。また、その鍵は、$S_1^{(1)}$及び$S_2^{(1)}$間でユーザ端末経由で受け渡しされてもよいし（具体的には、例えば、$S_2^{(1)}$から$C^{(1)}$に送信され、$C^{(1)}$からU_Mに送信され（U_MによりU_Mの画面に表示され）、U_Pに入力され、U_Pから$S_1^{(1)}$に送信されてもよいし）、$S_1^{(1)}$及び$S_2^{(1)}$間でユーザ端末非経由で受け渡しされてもよいし（具体的には、例えば、$S_2^{(1)}$から$C^{(1)}$経由（又は非経由）で$S_1^{(1)}$に送信されてもよいし）、$S_1^{(1)}$及び$S_2^{(1)}$間で事前に共有されてもよい。

【０２０９】

（０３）例えば連携対象情報の少なくとも一部が暗号化されていない場合、$C^{(1)}$は、連携対象情報が無害であるか否か（例えば表示させてよいか否か）のチェック、つまり、マルウェア（例えば、ウィルス又は遠隔操作プログラム等）の有無のチェックを行ってよい。

【０２１０】

（０４）実施例８では、tpw発行リクエストが、情報連携リクエスト（情報をサービスシステム間で共有することのリクエスト）を兼ねることができるが、情報連携リクエストは、tpw発行リクエストから独立していてよい。すなわち、U_Mは、tpw発行リクエストの発行とは別のタイミングで、情報連携リクエスト（例えば、サービスA（$S_1^{(1)}$）からサービスC（$S_2^{(1)}$）に情報を連携することのリクエスト）を$C^{(1)}$に送信してもよい。その場合、その情報連携リクエストに応答して、上述の情報連携が行われてよい。

【０２１１】

（０５）実施例８では、連携元も連携先もUにより選択されるが、連携元と連携先のうちの少なくとも１つが、Uが利用し得る全てのサービスシステム（$C^{(1)}$がUについてaList$^{(1)}$から特定できる全てのサービスシステム）であってもよい。

【０２１２】

以下、上述した実施例１～８を総括する。なお、総括の説明において、適宜、実施例１～８のうちの少なくとも１つの実施例の変形例等の新たな記載を追加することができる。

【０２１３】
実施例１～８によれば、$S_i^{(j)}$は、$C^{(j)}$から$mID_i^{(j)}$及びtpwを受信した場合に、Uからサービスのリクエスト（例えばログインのリクエスト）を受け付け可能な状態になり、tpwの使用期限（有効期限）が過ぎた場合に、Uからサービスのリクエスト（例えばログインのリクエスト）を受け付け不可能な状態になる。前者の状態は、認証シャッターがopenの状態であり、後者の状態は、認証シャッターがclosedの状態である。「認証シャッター」とは、認証リクエストの受け付けを制御するための論理的なシャッターである。$S_i^{(j)}$は、認証シャッターがopenであれば、$uID_i^{(j)}$及びtpwと共に認証リクエストを受けた場合に、その$uID_i^{(j)}$及びtpwが正しいか否かの判断（認証）を行う。一方、$S_i^{(j)}$は、認証シャッターがclosedであれば、$uID_i^{(j)}$及びtpwが正しいか否かの判断を行うこと無しにその認証リクエストを拒否する。tpwの使用期限が過ぎたことが、認証シャッターの状態がopenからclosedに変わった意味するが、認証シャッターのopenからclosedの変更は、Uからのリクエストに応答して行われてもよい。

【０２１４】
図２６は、識別符号管理の概要の一例を示す。

【０２１５】
図２６において、「TempPw」とは、上述したように一時的なパスワードの意味であり、tpwに限らず、一般的なotp（ワンタイムパスワード）を含む概念である。図２６によれば、TempPwと制御方式の関係がわかる。

【０２１６】
TempPwが必要なケースでは、TempPwの使用可能期間（使用期限までの期間）が短い（例えば数分）か長い（例えば「短い」に該当する期間より長い）かと、TempPwの使用可能回数が固定か無制限かによって、使用されるTempPwの種類が異なる。具体的には、例えば、TempPwの使用可能期間が「短い」であり、TempPwの使用可能回数が「固定」の場合、使用されるTempPwは、一般的なotp（例えば使用可能回数が１回に制限されたotp）でよい。TempPwの使用可能期間が「長い」であり、TempPwの使用可能回数が「無制限」の場合、使用されるTempPwは、上述したtpwであることが好ましい。

【０２１７】
TempPwは必ずしも必要ではない。TempPwが不要なケースもある。そのケースでは、上述した認証シャッターを用いた制御だけでもよい。認証シャッターとTempPwの併用も可能である。

【０２１８】
以下、TempPw（例えばtpw）が使用されない認証シャッター制御を説明する。なお、以下、説明を分かり易くするため、$C^{(j)}$として、$C^{(1)}$のみが存在し、$S_i^{(j)}$として、$S_1^{(1)}$及び$S_2^{(1)}$を含む複数の$S_i^{(1)}$が存在することとする。

【０２１９】
図２７の参照符号２７００－１に示すように、$S_i^{(1)}$は、認証シャッターの開閉を制御するシャッター管理サーバ２７０１－ｉと、認証に成功した場合にサービスを提供するサービス提供サーバ２７０２－ｉと、認証を行う認証サーバ２７０３－ｉという複数の機能を有する。すなわち、$S_1^{(1)}$は、シャッター管理サーバ２７０１－１、サービス提供サーバ２７０２－１、及び、認証サーバ２７０３－１を有し、$S_2^{(1)}$は、シャッター管理サーバ２７０１－２、サービス提供サーバ２７０２－２、及び、認証サーバ２７０３－２を有する。

【０２２０】
シャッター管理サーバ２７０１－ｉ、サービス提供サーバ２７０２－ｉ、及び、認証サーバ２７０３－ｉのうち、シャッター管理サーバ及び認証サーバ２７０３－ｉのいずれも、複数の$S_i^{(1)}$で共有とすることができる。

【０２２１】
具体的には、例えば、図２７の参照符号２７００－２に示すように、認証サーバ２７０３が、$S_1^{(1)}$及び$S_2^{(1)}$の外部に存在し、且つ、認証サーバ２７０３が、$S_1^{(1)}$及び$S_2^{(1)}$に

共有されてよい。更に、図２７の参照符号２７００－３に示すように、シャッター管理サーバ２７０１も、$S_1^{(1)}$及び$S_2^{(1)}$の外部に存在し、且つ、シャッター管理サーバ２７０１が、$S_1^{(1)}$及び$S_2^{(1)}$に共有されてよい。

【０２２２】

以下、参照符号２７００－１が示す構成を例に取り、認証シャッター制御を説明する。なお、以下の説明では、$S_1^{(1)}$及び$S_2^{(1)}$のうち、$S_1^{(1)}$を例に取る。

【０２２３】

認証シャッター制御では、登録手続き１、登録手続き２、認証シャッター操作手続き、ログイン手続きが行われる。

【０２２４】

登録手続き１では、図２８の参照符号２８００－１に示すフローが行われる。

【０２２５】

すなわち、U_Pは、リクエスト（Req_S）を、サービス提供サーバ２７０２－１に送信する（ステップ２８０１）。サービス提供サーバ２７０２－１は、そのリクエストに応答して、$sysID_1^{(1)}$を関連付けたユーザ追加リクエストを$C^{(1)}$に送信する（ステップ２８０２）。

【０２２６】

$C^{(1)}$は、一意的なmID（$mID_1^{(1)}$）を生成し、$sysID_1^{(1)}$と当該アカウント（Uのアカウント）に関する情報（例えば、アカウント作成日時等、当該アカウントに関する不変の情報で$C^{(1)}$が保持するリストに保存される情報）とに対する電子署名Signを生成し、認証シャッター制御アプリケーションパス（Pass = (mID, sysID, Sign)）を生成する。更に、$C^{(1)}$は、鍵を生成し、その鍵を用いてPassを暗号化する。暗号化されたPassを、E(Pass)と言う。なお、$C^{(1)}$がPassを暗号化するのはこのときの一度きりであり、そのPassを復号するのは$C^{(1)}$自身であり、かつ、Pass自体はそれほど大きなサイズにはならないので、鍵は使い捨ての鍵としてVernam暗号が採用されてもよい。

【０２２７】

また、$C^{(1)}$が、当該アカウントに対して、ust（Uの状態）の値を、「halfway」（登録中）とする。ust（Uの状態）は、例えば、$aList^{(1)}$のOTHERSに含まれてよい。$C^{(1)}$が、snに関連付けてmID、鍵、及びustを、例えば$aList^{(1)}$に保持する。$C^{(1)}$が、sn、mID及びE(Pass)をサービス提供サーバ２７０２－１に送る（ステップ２８０３）。

【０２２８】

サービス提供サーバ２７０２－１は、$uList_1^{(1)}$に、$uID_1^{(1)}$及びmIDを登録し、sst（認証シャッターの状態）の値を「closed」（閉の状態を意味する値）とし、period（認証シャッターがclosedの状態になる時刻）の値を、「Undefined」とする。sst及びperiodは、$uList_1^{(1)}$のTPWINFO及びOTHERSのうちの少なくとも一方に含まれている。その後、サービス提供サーバ２７０２－１は、sn及びE(Pass)をU_Pに送る（ステップ２８０４）。

【０２２９】

登録手続き２では、図２８の参照符号２８００－２に示すフローが行われる。

【０２３０】

U_Pが受信したsn及びE(Pass)は、Uにより、U_Mに入力される。U_Pが受信した情報のU_Mへの入力は、二次元バーコード等が利用されてもよいし、マニュアルでの入力が利用されてもよい。Sn及びE(Pass)は、U_Mの例えばAPPに入力される。

【０２３１】

その後、Uにより、U_Mに、認証シャッター制御パスワード(reqPw)が入力される。ここの説明では、簡単のため、制御センタ（C）を１つとし、tReqPw = reqPwとする。U_Mは、sn、reqPw及びE(Pass)を$C^{(1)}$に送信する（ステップ２８１１）。$C^{(1)}$が、snからアカウントを特定し、そのアカウント情報として登録されているustが「halfway」の場合に限り、当該アカウントの鍵を用いてE(Pass)を復号しPassを得る。その後、$C^{(1)}$が、そのPassの正当性を検証し、正しい場合は、hreqPwの値を「h(reqPw)」（reqPwに対して不可逆変換処理を施した値）とし、ustの値を「active」（登録済を意味する値）とする（ステップ２

８１２）。ustに加えて、hreqPwも、例えば、aList$^{(1)}$のOTHERSに含まれてよい。なお、ustが既に「active」の場合や、Passが正しくない場合、C$^{(1)}$が、登録失敗としてその時点で手続きを停止してよい。

【０２３２】

Passが正しい場合、C$^{(1)}$が、そのPassをU$_M$に送信する（ステップ２８１３）。U$_M$は、受け取ったPassを、U$_M$固有情報（例えば、MACアドレス、UUID等）を鍵として暗号化した上で保存する（ステップ２８１４）。

【０２３３】

認証シャッター操作手続き（Uが認証シャッターを開けるとき又は閉じるとき）では、図２８の参照符号２８００－３に示すフローが行われる。

【０２３４】

U$_M$が、U$_M$固有情報を用いて、Pass等の暗号化されている情報を復号する。U$_M$は、sysID$_1$$^{(1)}$（認証シャッターを操作するサービスシステム（S$_1$$^{(1)}$）のシステムID）、操作内容（open又はclose（O/C））及びreqPwの入力をUから受け、それらの情報とPassとをC$^{(1)}$に送信する（ステップ２８２１）。

【０２３５】

C$^{(1)}$は、Passに含まれているmIDからアカウントを特定し、Pass及びreqPwの正しさを検証する。正しい場合、C$^{(1)}$は、シャッター管理サーバ２７０１－１に、mIDおよび操作内容（O/C）を送信する（ステップ２８２２）。

【０２３６】

シャッター管理サーバ２７０１－１は、操作内容がopenであれば、認証シャッターを閉める時刻tを決定し、Uに対応したperiod（mIDをキーに特定されるperiod）の値を「t」とする。認証シャッターを開けるタイミングは、Uがこれから$S_1$$^{(1)}$を利用しようとしているときと考えられるので、「t」は、操作内容を受信してから数分先の時刻でよい。シャッター管理サーバ２７０１－１は、操作内容がcloseであれば、Uに対応したperiodの値を「Undefined」とする。

【０２３７】

その後、シャッター管理サーバ２７０１－１は、Uに対応したsst及びperiodを更新し、periodをC$^{(1)}$に返す（ステップ２８２３）。C$^{(1)}$は、そのperiodをU$_M$に送信する（ステップ２８２４）。

【０２３８】

ログイン手続きでは、図２９に示すフローが行われる。

【０２３９】

U$_P$が、Uからの指示に応答して、uID$_1$$^{(1)}$及びpwをサービス提供サーバ２７０２－１に送信する（ステップ２９０１）。pwは、固定パスワードでもTempPwでもよい。サービス提供サーバ２７０２－１は、uID$_1$$^{(1)}$を関連付けた照会（Uに対する認証シャッターの状態の照会）をシャッター管理サーバ２７０１－１に送信する（ステップ２９０２）。

【０２４０】

シャッター管理サーバ２７０１－１は、uID$_1$$^{(1)}$をキーとしてsst及びperiodを特定する。時刻がperiodを過ぎていない場合は、シャッター管理サーバ２７０１－１は、sstの値（「open」又は「closed」)を、サービス提供サーバ２７０２－１に返す（ステップ２９０３）。時刻がperiodを過ぎている場合は、シャッター管理サーバ２７０１－１は、sstの値として「closed」をサービス提供サーバ２７０２－１に返す。また、uID$_1$$^{(1)}$が存在しない場合、又は、periodの値が「Undefined」となっている場合は、シャッター管理サーバ２７０１－１は、sstの値として「closed」をサービス提供サーバ２７０２－１に返す。

【０２４１】

サービス提供サーバ２７０２－１は、sstの値として「open」が返ってきた場合のみ、(uID$_1$$^{(1)}$, pw)を、認証サーバ２７０３－１に照会する（ステップ２９０４）。sstの値として「open」が返ってこなかった場合、サービス提供サーバ２７０２－１は、ログイン認

証失敗として、手続きを終了してよい。

【０２４２】

認証サーバ２７０３－１は、($uID_1^{(1)}$, pw)に応じて、Yes又はNoを、サービス提供サーバ２７０２－１に返す（ステップ２９０５）。

【０２４３】

サービス提供サーバ２７０２－１は、Yesが返ってきた場合のみ、U_Pにサービスを提供する（例えばログイン認証成功とする）。

【０２４４】

多くのWebアプリケーションが、認証が成功した際、UのブラウザにCookieを渡すように、認証シャッター制御の場合も、認証が成功した際にサービス提供サーバ２７０２－１がU_PにCookieを渡せば、U_Pがサイト内を移動する度に認証手続きを実行する必要はない。認証成功の場合（Yesが返ってきた場合）、サービス提供サーバ２７０２－１がシャッター管理サーバ２７０１－１に認証シャッターを閉じるリクエスト(CloseShutter)を送ることにより、Uがログインした後は他者によるなりすましログインを防ぐこともできる。

【０２４５】

図３０は、U_M又はU_Pでの画面遷移の例を示す。

【０２４６】

参照符号３０００－１は、tpwの使用可能期間が短く使用可能回数が固定のケースの画面遷移例である。このケースでは、上述したように、一般的なotpが使用可能である。このため、例えば、Uが、U_Mの画面に、$tReqPw^{(1)}$（正確には$reqPw^{(1)}$）と所望のサービスシステム（サービスA）を入力すれば、$C^{(1)}$により、サービスAに対してのみ使用可能なOTP「1234」が発行され、そのOTPがU_Mに表示される。

【０２４７】

参照符号３０００－２は、tpwの使用可能期間が長く使用可能回数が無制限のケースの画面遷移例である。このケースでは、上述したように、共通のtpwが使用されるが、参照符号３０００－２は、サービス毎に異なるパスワードが発行された例を示す。例えば、Uが、U_Mの画面に、$tReqPw^{(1)}$と所望の１以上のサービスシステム（サービスA及びサービスC）を入力すれば、$C^{(1)}$により、サービスA及びサービスCにそれぞれ対応したパスワード「1234」及び「5678」が発行され、それらのパスワードがU_Mに表示される。

【０２４８】

参照符号３０００－３は、tpwの使用可能期間が長く使用可能回数が無制限のケースの画面遷移例である。このケースでは、上述したように、pwが使用される。例えば、Uが、U_Mの画面に、$tReqPw^{(1)}$とtpwを共有する所望の１以上のサービスシステム（サービスA及びサービスC）を入力すれば、$C^{(1)}$により、サービスA及びサービスCに共通のtpw「1234」が発行され、そのtpwがU_Mに表示される。その際、図示のように、tpwに関連付けられているtpwInfoが含むperiodが表す使用期限や、そのtpwInfoが含むuID（Uにより選択されたサービスシステム毎のuID）も表示されてよい。

【０２４９】

参照符号３０００－４は、認証シャッターの開閉のケースの画面遷移例である。例えば、Uが、U_Mの画面に、操作内容（例えばClose）と所望の１以上のサービスシステム（サービスA及びサービスC）を入力すれば、$C^{(1)}$により、サービスA及びサービスCの各々の認証シャッターの状態（sst）がUについて操作内容通りの状態にされ、その結果が、U_Mに表示される。その際、図示のように、periodの他にユーザが選択したサービスシステム毎のuIDを含んだtpwInfoがU_Mに送られ、そのtpwInfoが含むuID（Uにより選択されたサービスシステム毎のuID）も表示されてよい。

【０２５０】

参照符号３０００－５は、認証／連携の画面遷移例である。例えば、参照符号３０００－５に示すように、Uが、U_Mの画面に、連携元サービスシステム（From）（例えば図２５の$S_2^{(1)}$）、連携先サービスシステム（To）（例えば図２５の$S_1^{(1)}$）、及び連携対象情報（例えば「X証明書」）を入力（例えば選択）し、U_M（APP）が、それらを$C^{(1)}$に送信する

。ここでは、「X証明書」が、連携対象情報でもあり、情報連携において、att値でもある。つまり、この図の例では、連携対象情報は１つのatt値である。このように、Uにより所望のattが指定され、そのattについて、提供可能か受け入れ可能かの双方のチェックが行われてもよい。U_M（APP）が、$C^{(1)}$からのtpwの他に、uIDと、連携対象情報の少なくとも一部と、回答ボタン（OKボタン及びNGボタン）とを表示する。連携対象情報の鍵がユーザ端末経由で受け渡しされる場合、鍵もU_M（APP）により表示されてよい。OKボタンが押された場合、Uが、U_Pを用いて、連携先サービスシステムにアクセスしてよい。

【０２５１】

以上、幾つかの実施例を説明したが、本発明はそれらの実施例に限定されない。

【０２５２】

例えば、携帯端末の生体情報による認証が一般化した場合は、それとの連携を行うことにより、記憶情報を用いない２要素認証、又は、３要素認証が期待できる。例えば、U_Mの生体認証（例えば、指紋認証又は虹彩認証）を経てU_Mが使用可能になった場合、U_Mからの$tReqPw^{(1)}$の生成に、Uの生体情報（例えば、指紋情報又は虹彩情報）が利用されてよい。例えば、reqPwに代えて又は加えて、Uの生体情報が利用されてよい。利用される生体情報は、U_Mにより検出された情報であってもよいし、U_Mに予め登録されている情報でもよい。

【０２５３】

また、$tpwInfo_i^{(j)}$は、$S_i^{(j)}$がUに提供する画面（例えば、ログイン画面等の申請受付画面、銀行口座番号等の入力受付画面）に表示される電子的な身元証明オブジェクト（例えば、テキスト又は画像）を含んでよい。$tpwInfo_i^{(j)}$内の身元証明オブジェクトは、U_M（APP）によりディスプレイ２１１に表示されてよい。Uは、$S_i^{(j)}$から提供された画面に情報を入力する前に、その画面上の身元証明オブジェクトと、U_M（APP）によりディスプレイ２１１に表示された身元証明コード（$tpwInfo_i^{(j)}$内の身元証明オブジェクト）とを比較する。それらが一致していれば、Uに提供された画面は確かに$S_i^{(j)}$から提供された画面であることがわかる。これにより、不正なシステムに対してUが情報を提供してしまうこと（例えばフィッシングの被害に合うこと）を避けることができる。

【０２５４】

また、tpw発行リクエスト等のtpw制御リクエストに関連付けられる$sysID_i^{(j)}$は、Uに手動で選択されたサービスシステムの$sysID_i^{(j)}$に代えて、pListに登録されておりU_M（APP）により自動で選択された全て（又は一部）の$sysID_i^{(j)}$でよい。

【０２５５】

また、tpwの制限の少なくとも１つ（例えばtpwの使用期限及び使用回数のうちの少なくとも１つ）は、サービスシステムに代えて、tpwを発行する制御センタにより決められてもよい。tpwの使用期限を例に取ると、次の通りである。すなわち、tpwの使用期限が、制御センタにより決定され、制御センタに決定された使用期限が、サービスシステムに、別の制御センタ経由で又は非経由で、送信される。具体的には、例えば、$C^{(1)}$は、tpwの使用期限を、SYSIDPart内の各々の$sysID_i^{(j)}$について決定する（例えばステップ１４０２～１４０４のいずれかにおいて）。使用期限は、SYSIDPart内の全ての$sysID_i^{(j)}$について同じでもよいし、SYSIDPart内の$sysID_i^{(j)}$毎に異なっていてよい。例えば、tpw使用期限を決定した$C^{(1)}$の配下にある$S_1^{(1)}$に対応したtpw使用期限（$Period_1^{(1)}$）は、$C^{(1)}$から$S_1^{(1)}$に送信される。また、例えば、$C^{(1)}$とは別の制御センタ$C^{(2)}$の配下にある$S_1^{(2)}$に対応したtpw使用期限（$Period_1^{(2)}$）は、$C^{(1)}$から$C^{(2)}$経由又は非経由で$S_1^{(2)}$に送信される。$S_i^{(j)}$は、受信したtpw使用期限（$Period_i^{(j)}$）を、$tpwInfo_i^{(j)}$の少なくとも一部として$uList_i^{(j)}$に登録する（例えばステップ１４０５）。以上の処理は、tpwの使用期限以外の制限（例えば使用回数）についても適用されてよい。

【０２５６】

また、tpwの制限の少なくとも１つ（例えばtpwの使用期限及び使用回数のうちの少なくとも１つ）は、サービスシステムに代えて、ユーザにより決められてもよい。tpwの使用期限を例に取ると、次の通りである。tpwの使用期限が、UによりU_M（APP）に入力され、U_M（APP）から制御センタに送信され、制御センタからサービスシステムに、別の制御セン

タ経由で又は非経由で、送信される。具体的には、例えば、U_M（APP）が、SYSIDPart内の各々の$sysID_i^{(j)}$について、tpwの使用期限（$Period_i^{(j)}$）の入力をUから受ける（例えばステップ１４０１）。使用期限は、SYSIDPart内の全ての$sysID_i^{(j)}$について同じでもよいし、SYSIDPart内の$sysID_i^{(j)}$毎に異なっていてよい。SYSIDPart内の各々の$sysID_i^{(j)}$のtpw使用期限（$Period_i^{(j)}$）が、U_M（APP）から$C^{(1)}$に送信される（例えばステップ１４０１）。その後、例えば、tpw使用期限をU_Mから受信した$C^{(1)}$の配下にある$S_1^{(1)}$に対応したtpw使用期限（$Period_1^{(1)}$）は、$C^{(1)}$から$S_1^{(1)}$に送信される。また、例えば、$C^{(1)}$とは別の制御センタ$C^{(2)}$の配下にある$S_1^{(2)}$に対応したtpw使用期限（$Period_1^{(2)}$）は、$C^{(1)}$から$C^{(2)}$経由又は非経由で$S_1^{(2)}$に送信される。$S_i^{(j)}$は、受信したtpw使用期限（$Period_i^{(j)}$）を、$tpwInfo_i^{(j)}$の少なくとも一部として$uList_i^{(j)}$に登録する（例えばステップ１４０５）。以上の処理は、tpwの使用期限以外の制限（例えば使用回数）についても適用されてよい。

【０２５７】

また、$C^{(j)}$、$S_i^{(j)}$、U_P及びU_Mの各々が行う上述した処理の少なくとも一部は、上述したように、コンピュータプログラムをプロセッサが実行することにより行われる。また、上述した「サーバ」は、コンピュータシステムで実行される機能（例えば仮想サーバ）に代えて、物理的なサーバマシンであってもよい。$C^{(j)}$及び$S_i^{(j)}$は、典型的には、異なる者（エンティティ）により所有又は管理されるが、同一の者により所有又は管理されてもよい。

【０２５８】

また、少なくとも登録フェーズでのUと$S_i^{(j)}$間のやり取りは、Webベースに限らず、紙ベースで行われてもよい。なお、上述の説明において、U_Pから$C^{(j)}$へのリクエストに応答して行われる処理におけるテーブル操作によれば、テーブルにレコード（アカウント）が追加され、U_Mから$C^{(j)}$へのリクエストに応答して行われる処理におけるテーブル操作によって、そのレコードに情報が登録される。

【０２５９】

また、$aID^{(j)}$のように複数のサービスシステムを統合するキーは、U_Mと$C^{(j)}$のうちの少なくとも１つに保持されてよい。

【０２６０】

また、$aID^{(j)}$は必須ではない。例えば、$S_i^{(j)}$が同一でもUが異なれば$mID_i^{(j)}$は異なるため、$mID_i^{(j)}$が$aID^{(j)}$として使用されてもよい。しかし、Uが利用する$S_i^{(j)}$の数が多い場合、Uが利用する２以上の$S_i^{(j)}$に同一の$aID^{(j)}$を関連付けることができるので、$aID^{(j)}$の存在により効率化が期待できる。

【０２６１】

また、U_Mが受信する$tpwInfo_i^{(j)}$には、サービスシステム毎に（例えば、tpwの発行先のサービスシステム毎に、又は、連携対象情報の連携先サービスシステム毎に）、そのサービスシステムへのリンク（例えばURL）が含まれていてよい。U_M（又はU_P）は、$tpwInfo_i^{(j)}$内のリンクを指定することでサービスシステムへアクセスしてもよい。なお、$tpwInfo_i^{(j)}$に含まれるリンク（URL）には、ユーザを識別する情報が含まれていてもよい。そのリンクを指定してU_M（又はU_P）からアクセスされたサービスシステムは、入力欄に情報（例えばuIDと認証情報）が入力された画面をアクセス元のU_M（又はU_P）に提供してよい。

【０２６２】

また、tpwが使用される少なくとも１つの実施例において、U_P（又はU_M）から$S_i^{(j)}$に送信されるリクエスト（例えばログインリクエスト）には、tpwに加えて、その$S_i^{(j)}$に固有のパスワードが使用されてもよい。また、少なくとも１つの実施例において、電子署名は必須でない。

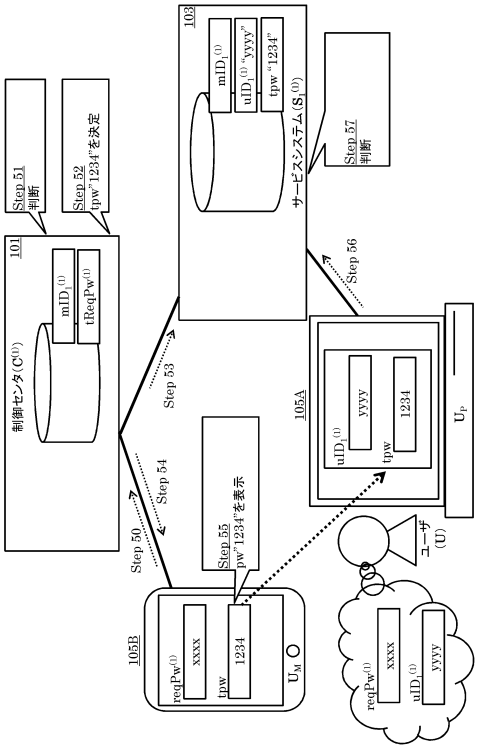
【符号の説明】

【０２６３】

１０１…制御センタ、１０３…サービスシステム、１０５…ユーザ端末

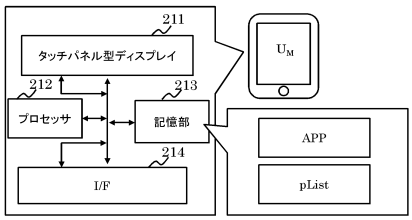
【図１】

FIG. 1



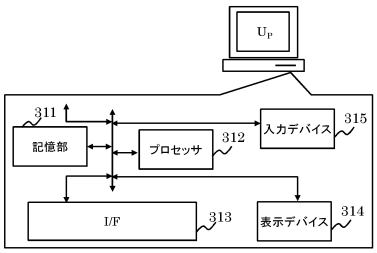
【図２】

FIG. 2



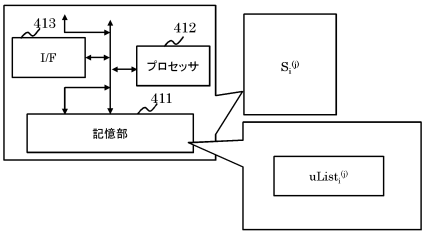
【図３】

FIG. 3



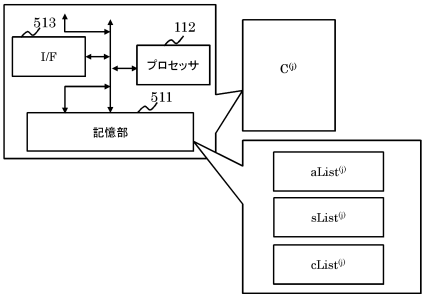
【図４】

FIG. 4



【図５】

FIG. 5



【図６】

FIG. 6

$uList_i^{(j)}$ (in $S_i^{(j)}$)

UID	MID	TPW	TPWINFO	SUKEY	OTHERS
…	…	…	…	…	…

【図７】

FIG. 7

$aList^{(j)}$ (in $C^{(j)}$)

SN	SYSID	MID	TREQPW	AID	OTHERS
…	…	…	…	…	…

【図８】

FIG. 8

pList (in U_M)

SYSID	CID	RAND	AID	PASS	SUKEY	OTHERS
…	…	…	…	…	…	…

【図９】

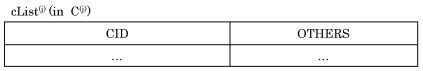
FIG. 9

$sList^{(j)}$ (in $C^{(j)}$)

SYSID	OTHERS
…	…

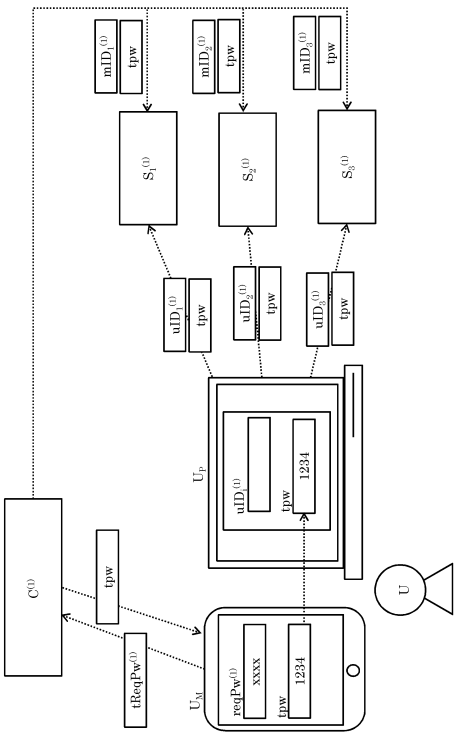
【図１０】

FIG. 10



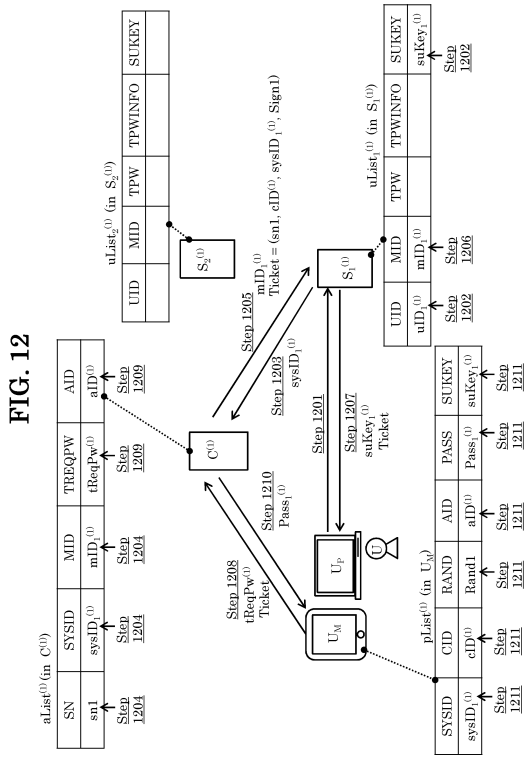
【図１１】

FIG. 11



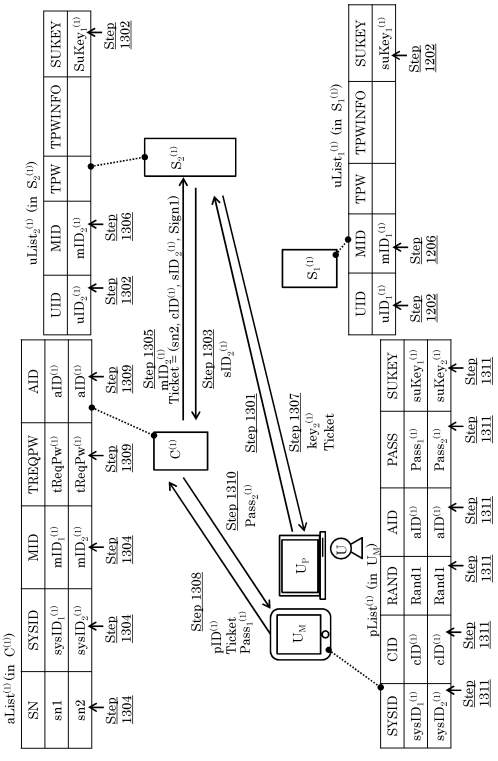
【図１２】

FIG. 12



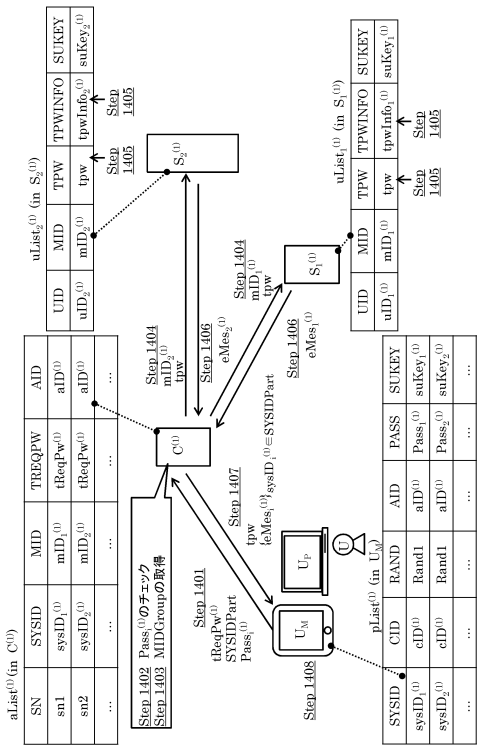
【図１３】

FIG. 13



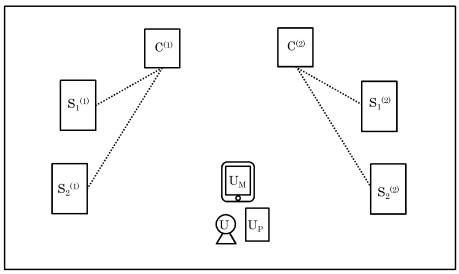
【図１４】

FIG. 14



【図１５】

FIG. 15



【図１６】

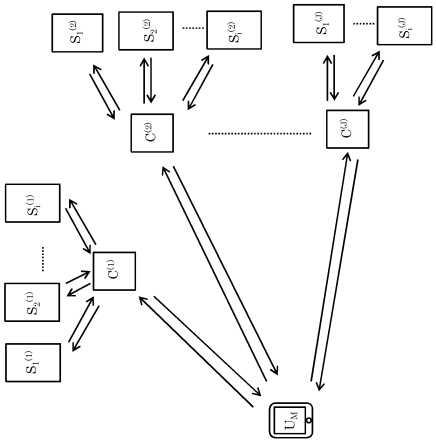
FIG. 16

pList (in U_M)

SYSID	CID	RAND	AID	PASS	SUKEY
$sysID_1^{(1)}$	$cID^{(1)}$	$Rand^{(1)}$	$aID^{(1)}$	$Pass_1^{(1)}$	$suKey_1^{(1)}$
$sysID_2^{(1)}$	$cID^{(1)}$	$Rand^{(1)}$	$aID^{(1)}$	$Pass_2^{(1)}$	$suKey_2^{(1)}$
$sysID_1^{(2)}$	$cID^{(2)}$	$Rand^{(2)}$	$aID^{(2)}$	$Pass_1^{(2)}$	$suKey_1^{(2)}$
$sysID_2^{(2)}$	$cID^{(2)}$	$Rand^{(2)}$	$aID^{(2)}$	$Pass_2^{(2)}$	$suKey_2^{(2)}$

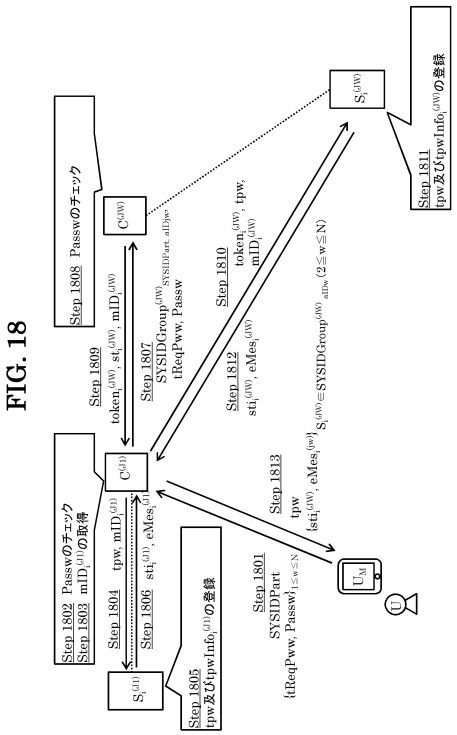
【図１７】

FIG. 17



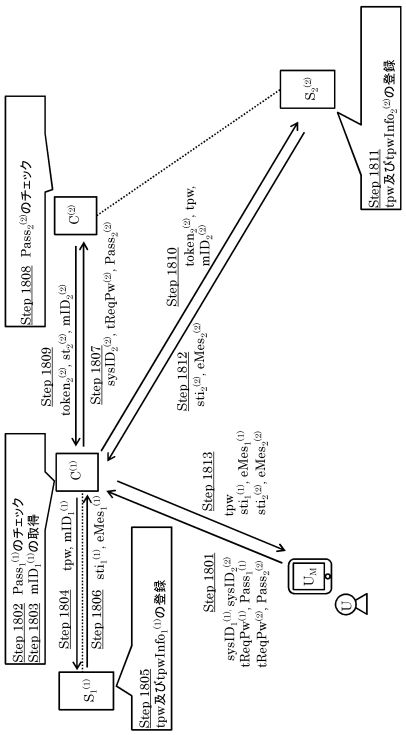
【図１８】

FIG. 18



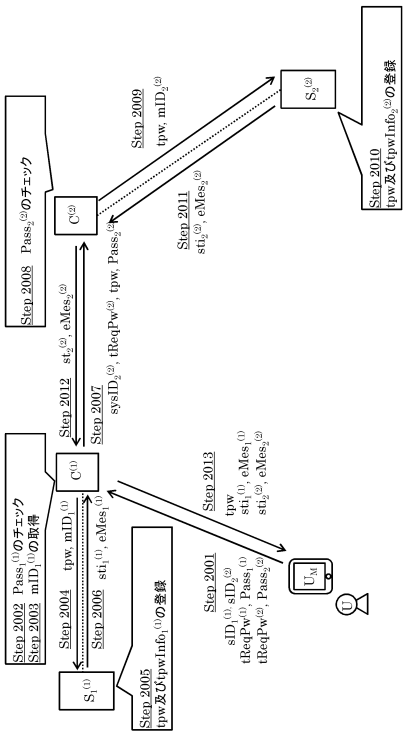
【図１９】

FIG. 19



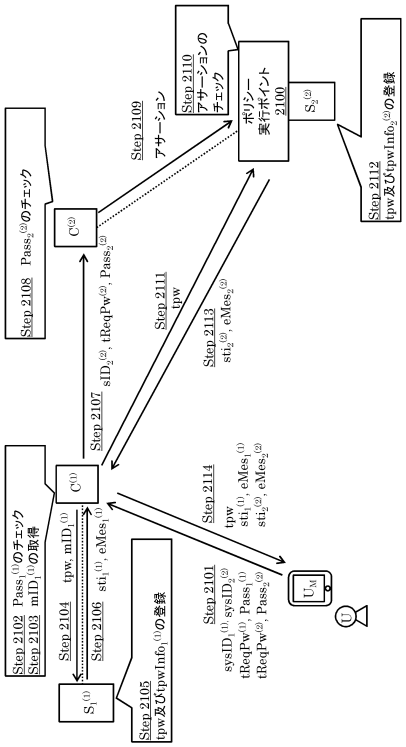
【図２０】

FIG. 20



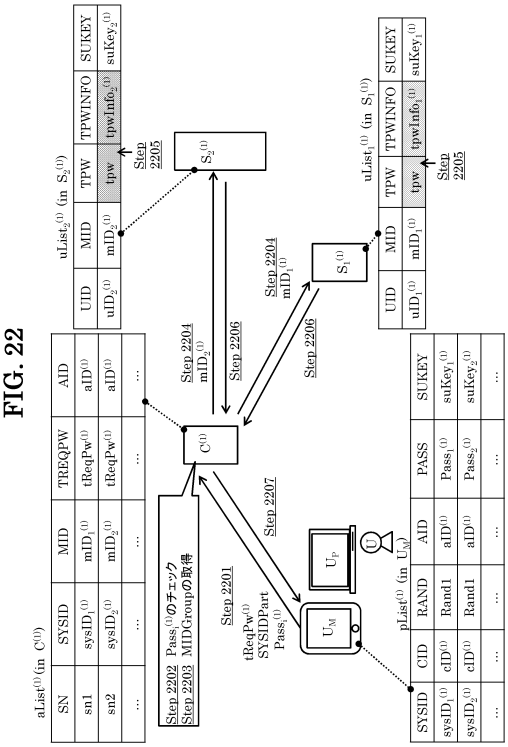
【図２１】

FIG. 21



【図２２】

FIG. 22



【図２３】

FIG. 23

$uList_1^{(j)}$ (in $S_1^{(j)}$)

UID	MID	TPW	TPWINFO	INFO	SUKEY	OTHERS
…	…	…	…	…	…	…

【図２４】

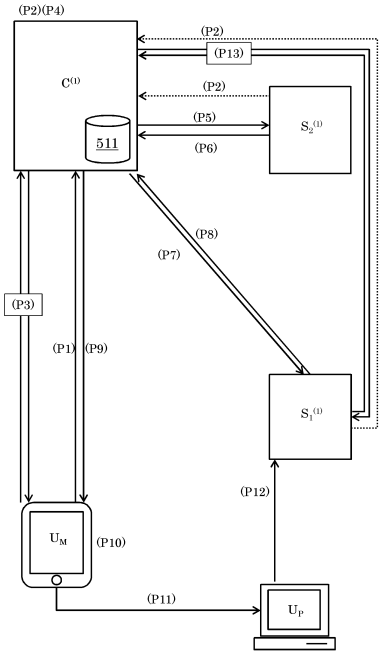
FIG. 24

$aList^{(j)}$ (in $C^{(j)}$)

SN	SYSID	MID	TREQPW	INFO	AID	OTHERS
…	…	…	…	…	…	…

【図２５】

FIG. 25



【図２６】

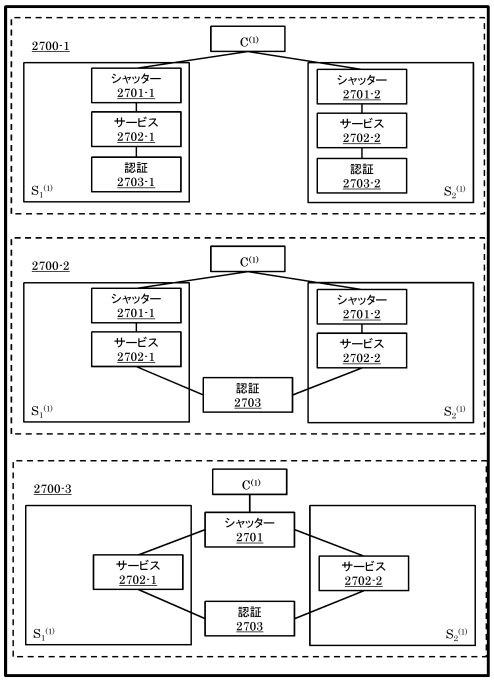
FIG. 26

TempPwの種類		使用可能回数	
		固定	無制限
使用可能期間	短い	otp1	otp2
	長い		tpw

TempPw	制御方式
必要	(*)
不要	認証シャッター

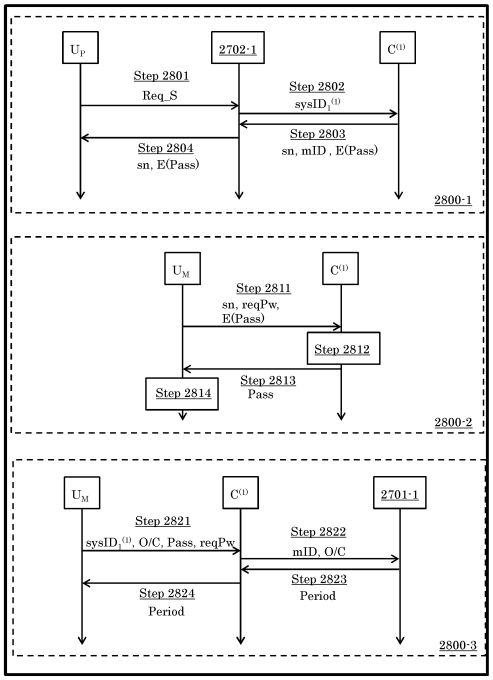
【図２７】

FIG. 27



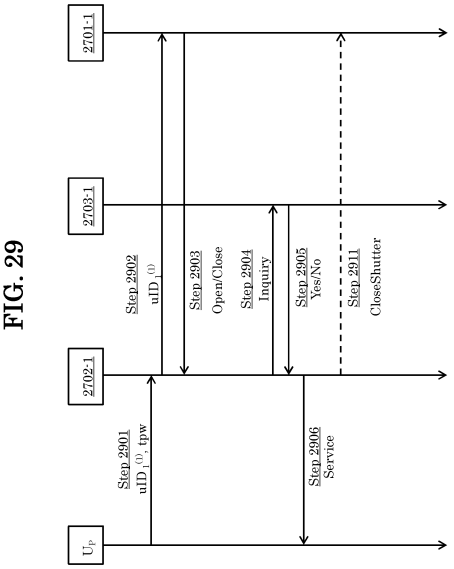
【図２８】

FIG. 28



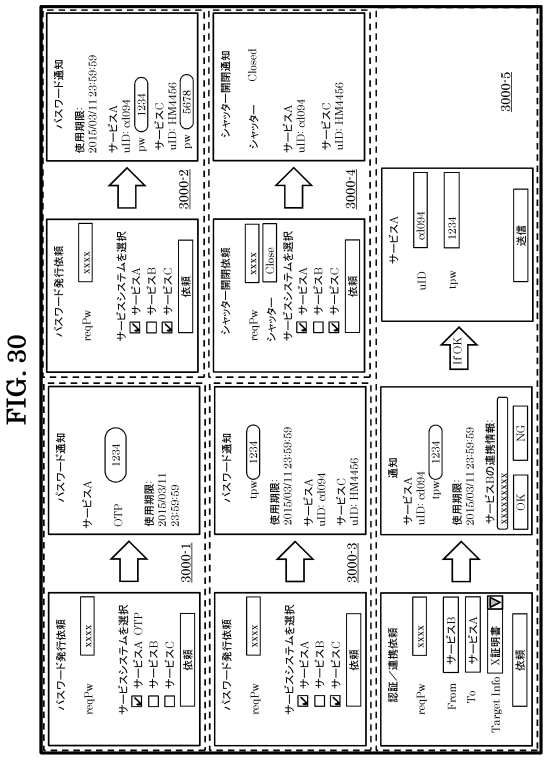
【図２９】

FIG. 29



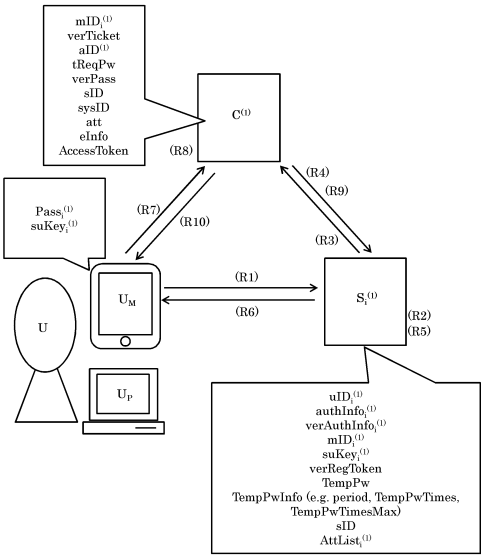
【図３０】

FIG. 30



【図３１】

FIG. 31



フロントページの続き

(31)優先権主張番号　特願2015-187644(P2015-187644)
(32)優先日　平成27年9月25日(2015.9.25)
(33)優先権主張国　日本国(JP)

早期審査対象出願

審査官　中里　裕正

(56)参考文献　特開平０８－２２１３６４（ＪＰ，Ａ）
特開２００４－０７０８１４（ＪＰ，Ａ）
垣野内将貴 他，プライバシーを考慮したワンタイムパスワード認証システムの実装，2012年暗号と情報セキュリティシンポジウム講演論文集，２０１２年　1月３０日，p.1-6
高田哲司，Authentication Shutter:個人認証に対する攻撃を遮断可能する対策の提案，コンピュータセキュリティシンポジウム２０１４論文集，２０１４年１０月１５日，p.883-890

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／４１