(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第5090425号
(P5090425)

(45)発行日　平成24年12月5日(2012.12.5)　(24)登録日　平成24年9月21日(2012.9.21)

(51)Int.Cl.		F I		
G06F 21/20	(2006.01)	G06F	21/20	131A
G06Q 50/22	(2012.01)	G06F	17/60	126A
H04L 9/32	(2006.01)	H04L	9/00	673C

請求項の数 9　(全 30 頁)

(21)出願番号　特願2009-259286 (P2009-259286)
(22)出願日　平成21年11月12日 (2009.11.12)
(65)公開番号　特開2011-107779 (P2011-107779A)
(43)公開日　平成23年6月2日 (2011.6.2)
審査請求日　平成22年2月3日 (2010.2.3)

(73)特許権者　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目３番１号
(74)代理人　100108855
弁理士　蔵田　昌俊
(74)代理人　100080285
弁理士　小出　俊實
(74)代理人　100087963
弁理士　石川　義雄
(74)代理人　100075672
弁理士　峰　隆司
(74)代理人　100103034
弁理士　野河　信久

最終頁に続く

(54)【発明の名称】情報アクセス制御システム及び方法

(57)【特許請求の範囲】
【請求項１】
サーバ装置に記憶された第１のユーザの個人情報に対し、第２のユーザの端末から前記第１のユーザを識別するための情報を用いてアクセスする情報アクセス制御システムであって、
前記第１のユーザの端末から送信される発行要求に応じて、当該発行要求元のユーザを識別するための情報に加え、当該発行要求元ユーザの属性情報と、前記一時ユーザ指定子の発行元となるサーバ装置を特定するための識別情報と、解決要求元のユーザに提示するための提示情報のうちの少なくとも一つを含んだ、前記アクセスのために第２のユーザが第１のユーザを指定するために使用する、暗号化された一時ユーザ指定子を発行する発行手段と、
前記第２のユーザの端末から送信される解決要求に応じて、当該解決要求に含まれる前記発行された暗号化一時ユーザ指定子を復号して前記第１のユーザを識別するための情報に変換する解決手段と
を具備することを特徴とする情報アクセス制御システム。
【請求項２】
サーバ装置に記憶された第１のユーザの個人情報に対し規定されたアクセス制御ルールに対し、第１のユーザの端末から、前記個人情報のアクセスを許可する第２のユーザを識別するための情報を設定する機能を有する情報アクセス制御システムであって、
前記第２のユーザの端末から送信される発行要求に応じて、前記第２のユーザを識別す

るための情報の設定のために前記第１のユーザが第２のユーザを指定するために使用する、暗号化された一時ユーザ指定子を発行する発行手段と、
前記第１のユーザの端末から送信される解決要求に応じて、当該解決要求に含まれる前記発行された暗号化一時ユーザ指定子を復号して前記第２のユーザを識別するための情報に変換する解決手段と
を具備することを特徴とする情報アクセス制御システム。
【請求項３】
前記発行手段は、システム上で発行要求元のユーザの識別子と関連付けられた仮名を暗号化した一時ユーザ指定子を発行し、
前記解決手段は、前記発行された暗号化一時ユーザ指定子を復号して前記仮名に変換した後、この変換された仮名を前記発行要求元のユーザの識別子に変換することを特徴とする請求項１又は２記載の情報アクセス制御システム。
【請求項４】
前記発行手段は、前記一時ユーザ指定子に有効期間を表す情報を含め、
前記解決手段は、前記復号された一時ユーザ指定子に含まれる有効期間を表す情報をもとに、当該一時ユーザ指定子が有効か無効かを判定する手段を、さらに備えることを特徴とする請求項１又は２記載の情報アクセス制御システム。
【請求項５】
前記解決手段は、
失効リスト記憶手段と、
端末から送信される失効登録要求に応じて、当該失効登録要求により指定された一時ユーザ指定子を前記失効リスト記憶手段に記憶させる手段と、
前記復号された一時ユーザ指定子が前記失効リスト記憶手段に記憶されているか否かを判定し、記憶されている場合に当該一時ユーザ指定子を無効とする手段と
を、さらに備えることを特徴とする請求項１又は２記載の情報アクセス制御システム。
【請求項６】
前記解決手段は、端末から送信される失効削除要求に応じて、当該失効削除要求により指定される一時ユーザ指定子を前記失効リスト記憶手段から削除する手段を、さらに備えることを特徴とする請求項５記載の情報アクセス制御システム。
【請求項７】
前記発行手段は、当該発行手段が所有する秘密鍵を用いて一時ユーザ指定子に署名を行う手段を、さらに備え、
前記解決手段は、前記復号された一時ユーザ指定子の署名を、前記秘密鍵と対をなす公開鍵を用いて検証する手段を、さらに備えることを特徴とする請求項１又は２記載の情報アクセス制御システム。
【請求項８】
第１のユーザの個人情報を記憶するデータプロバイドサーバ装置と、ユーザが使用する端末と前記データプロバイドサーバ装置との間を連携する連携サーバ装置と、前記データプロバイドサーバ装置と連携サーバ装置との間を認証連携する認証サーバ装置とを備えるシステムを利用して、前記データプロバイドサーバ装置に記憶された第１のユーザの個人情報に対し、第２のユーザの端末から前記第１のユーザを識別するための情報を用いてアクセスする情報アクセス方法であって、
前記連携サーバ装置が、前記第１のユーザの端末から送信される発行要求に応じて、当該発行要求元のユーザを識別するための情報に加え、当該発行要求元ユーザの属性情報と、前記一時ユーザ指定子の発行元となるサーバ装置を特定するための識別情報と、解決要求元のユーザに提示するための提示情報のうちの少なくとも一つを含んだ、前記アクセスのために第２のユーザが第１のユーザを指定するために使用する、暗号化された一時ユーザ指定子を発行する過程と、
前記認証サーバ装置が、前記第２のユーザの端末から送信される解決要求に応じて、当該解決要求に含まれる前記発行された暗号化一時ユーザ指定子を復号して前記第１のユー

ザを識別するための情報に変換する過程と
を具備することを特徴とする情報アクセス制御方法。
【請求項９】
第１のユーザの個人情報を記憶するデータプロバイドサーバ装置と、ユーザが使用する端末と前記データプロバイドサーバ装置との間を連携する連携サーバ装置と、前記データプロバイドサーバ装置と連携サーバ装置との間を認証連携する認証サーバ装置とを備えるシステムを利用して、前記データプロバイドサーバ装置に記憶された第１のユーザの個人情報に対し規定されたアクセス制御ルールに対し、第１のユーザの端末から、前記個人情報のアクセスを許可する第２のユーザを識別するための情報を設定する機能を有する情報アクセス制御方法であって、
前記連携サーバ装置が、前記第２のユーザの端末から送信される発行要求に応じて、前記第２のユーザを識別するための情報の設定のために前記第１のユーザが第２のユーザを指定するために使用する、暗号化された一時ユーザ指定子を発行する過程と、
前記認証サーバ装置が、前記第１のユーザの端末から送信される解決要求に応じて、当該解決要求に含まれる前記発行された暗号化一時ユーザ指定子を復号して前記第２のユーザを識別するための情報に変換する過程と
を具備することを特徴とする情報アクセス制御方法。
【発明の詳細な説明】
【技術分野】
【０００１】
この発明は、例えば医療機関や保健関連機関、自治体等が保有するデータベースに保存されているユーザ情報を、本人もしくは本人が許可した第三者がアクセスして取得するサービスを実現するための情報アクセス制御システム及び方法に関する。
【背景技術】
【０００２】
近年、複数の医療機関・保健関連機関・自治体等が保有する医療や健康に係る情報を、通信ネットワークを介し、相互接続・共有することで統合的医療サービス・健康サービスを目指すＥＨＲ（Electronic Health Record）システムが提案されている。
ＥＨＲシステムにおいては、個人のプライバシーに関わる医療及び健康関連情報を扱う。プライバシーに関わる情報は、その扱いのミスが個人にとって大きな損害につながる場合があり、その流通と開示は必要最小限度にとどめる必要がある。そのため、従来型の個人情報を扱うシステムにおいては認証技術により本人確認を行い、本人に係る情報は本人のみが参照することを基本としている。
【０００３】
しかし、国民の誰もがＥＨＲを使えるようにするためには、本人に係わる情報を本人しか閲覧できないのでは不十分である。例えば、幼児や高齢者等の場合、本人から権限委譲された代理人が本人の代わりに操作できるようにする必要がある。また、医療健康関連の情報を本人しか閲覧できない状況では、その医療健康関連情報を活用することは困難であり、現代日本で目指されている地域に根ざした統合的医療サービスといったものの実現は難しい。例えば、医師に自身の情報を十分に閲覧してもらい、診断及び指導を受けるなど、他者に情報を閲覧してもらった上でその閲覧者から有益な情報を得ることができない。本人の医療健康関連の情報を活用するためには、情報開示したい相手には、簡単にそして過ちなく開示できるしくみが必要である。
【０００４】
そこで本発明者等は、ユーザごとにその医療健康関連情報の開示条件を規定したアクセス制御ルールを設定して、このアクセス制御ルールに医療健康関連情報の開示を許可した第三者ユーザの識別子を登録し、第三者ユーザから情報取得要求が送られた場合に上記アクセス制御ルールに基づいて情報開示の可否を判定するシステムを提案している。
【０００５】
しかし、個人情報に対しアクセスするためには、その所有者の識別情報（ユーザＩＤ）

を何らかの方法で取得する必要がある。また、情報開示を許可した第三者のユーザＩＤを登録する場合にも、第三者のユーザＩＤを何らかの方法で取得しなければならない。

【０００６】

第三者のユーザＩＤを取得する方法としては、例えば以下のようなものがある。すなわち、ＥＨＲのように医師や保健師等の業務用ユーザリスト（例えば担当患者リスト）が用意されている場合には、ユーザ本人がこの業務用ユーザリストの中から自己の医療健康関連情報の閲覧を許可する医師等を選択してそのユーザＩＤをアクセス制御リストに登録する。しかし、一般市民のような不特定多数のユーザが、利用範囲がシステム内のみに限定された業務用ユーザリストから医師や保健師等を指定してそのユーザＩＤを取得することは、医師や保健師のユーザＩＤ保護の観点から許されない。したがって、システム内に限定してユーザを安全に指定することは困難である。

一方、一般市民が自らの代理人を指定する場合、上記のような業務用ユーザリストから検索することはできない。また、システムが管理するユーザリストから氏名等で他の市民を検索することは個人情報保護の観点から許されない。一件まで絞り込んでから検索結果をていじするようにしたとしても、例えば同姓同名のユーザが存在する場合には誤検索の可能性があり非常に好ましくない。

【０００７】

また、システム上で登録済みのユーザを指定するその他の方法として、グループウェアにおける第三者ユーザを指定するものがある。この方法は、会社等の信頼できる特定ユーザのみが利用することを想定し、各ユーザはログインＩＤ、氏名、所属等を公開し、他者に参照させることを前提としている。このため、氏名やログインＩＤを直接指定して、システム上の第三者ユーザを特定することができる（例えば、非特許文献１を参照。）。

【０００８】

さらに、別の方法として、ＳＮＳ（Social Network Service）サービスにおける他者ユーザ指定方法がある。この方法は、不特定多数のユーザがそれぞれ自身のニックネームや氏名、性別、写真等の一部の個人情報（プロフィール）を公開し、他者に参照させるものとなっている。このため、プロフィール等に基づいて自分に近い趣向を持つ他者ユーザ等を検索することが可能となる（例えば、非特許文献２を参照。）。

【先行技術文献】

【非特許文献】

【０００９】

【非特許文献１】サイボウズ、インターネット＜URL: http://manual.cybozu.co.jp/office8/user/

【非特許文献２】GREE（グリー）、インターネット＜URL: http://www.gree.co.jp/privacy/

【発明の概要】

【発明が解決しようとする課題】

【００１０】

ところが、非特許文献１に記載された方法は、登録ユーザが信頼できることを前提としたものであり、不特定多数の見知らぬユーザが利用するサービスでは、個人情報に対する安全上の点で問題があり利用できない。また非特許文献２に記載された方法も、ＳＮＳのように、ユーザ同士の交流を目的とし、個人情報の一部を開示することを前提としたサービスでなければ利用できない。

【００１１】

この発明は上記事情に着目してなされたもので、その目的とするところは、ユーザを識別するための情報を公開したり無制限に検索させることなく、システム上で安全に所望のユーザを指定することを可能にした情報アクセス制御システム及び方法を提供することにある。

【課題を解決するための手段】

【００１２】

上記目的を達成するためにこの発明の第１の観点は、サーバ装置に記憶された第１のユーザの個人情報に対し、第２のユーザの端末から上記第１のユーザを識別するための情報を用いてアクセスする情報アクセス制御システムにあって、先ず上記第１のユーザの端末から送信される発行要求に応じて、上記アクセスのために第２のユーザが第１のユーザを指定するために使用する、暗号化された一時ユーザ指定子を発行する。この一時ユーザ指定子には、上記発行要求元のユーザを識別するための情報に加え、当該発行要求元ユーザの属性情報と、上記一時ユーザ指定子の発行元となるサーバ装置を特定するための識別情報と、解決要求元のユーザに提示するための提示情報のうちの少なくとも一つを含める。次に、上記第２のユーザの端末から送信される解決要求に応じて、当該解決要求に含まれる上記発行された暗号化一時ユーザ指定子を復号して上記第１のユーザを識別するための情報に変換し、この変換された第１のユーザを識別するための情報を用いて第１のユーザの個人情報にアクセスするように構成したものである。

【００１３】

したがって、第１のユーザの個人情報に対しアクセスするために必要な第１のユーザを識別するための情報は、第１のユーザ本人の要求に応じて一時ユーザ指定子として発行されるので、公開されることなくまた検索されることなく安全に第１のユーザから第２のユーザに渡すことができる。第２のユーザは、この渡された一時ユーザ指定子の解決をシステムに要求することで、システム上で第１のユーザを確実に指定してその個人情報をアクセスすることができる。

また、上記一時ユーザ指定子には、上記発行要求元のユーザを識別するための情報に加えて、当該発行要求元ユーザの属性情報と、上記一時ユーザ指定子の発行元となるサーバ装置を特定するための識別情報と、解決要求元のユーザに提示するための提示情報のうちの少なくとも一つが含められる。このため、ユーザ属性を含めた場合には、例えばアクセス制御ルールに第２のユーザを識別するための情報を設定する際に、同時に第２のユーザのユーザ属性情報、例えば所属組織や資格等を表す情報を設定することが可能となる。また、一時ユーザ指定子の発行元となるサーバ装置を特定するための識別情報を含めた場合には、一時ユーザ指定子発行元のサーバに限らず認証連携されたどのサーバでも一時ユーザ指定子の解決要求を受け付けることが可能となる。さらに、解決要求元のユーザに提示するための提示情報を含めた場合には、例えば発行元ユーザから入力されたニックネーム又は質問等を、一時ユーザ指定子の解決処理時に解決要求元ユーザに提示して確認させたり、質問に対する回答を要求することが可能となる。

【００１４】

一方、この発明の第２の観点は、サーバ装置に記憶された第１のユーザの個人情報に対し規定されたアクセス制御ルールに対し、第１のユーザの端末から、上記個人情報のアクセスを許可する第２のユーザを識別するための情報を設定する機能を有する情報アクセス制御システムにあって、先ず上記第２のユーザの端末から送信される発行要求に応じて、上記第２のユーザを識別するための情報の設定のために上記第１のユーザが第２のユーザを指定するために使用する、暗号化された一時ユーザ指定子を発行する。次に、上記第１のユーザの端末から送信される解決要求に応じて、当該解決要求に含まれる上記発行された暗号化一時ユーザ指定子を復号して上記第２のユーザを識別するための情報に変換し、この変換された第２のユーザを識別するための情報をアクセス制御ルールに設定するように構成したものである。

【００１５】

したがって、第１のユーザの個人情報に対応するアクセス制御ルールに設定するための第２のユーザの識別情報は、第２のユーザ本人の要求に応じて一時ユーザ指定子として発行される。このため、第２のユーザの識別情報は公開されることなくまた検索されることなく安全に第１のユーザに渡される。また、第１のユーザはこの渡された一時ユーザ指定子の解決を要求することで、システム上で第２のユーザを確実に指定してその識別情報を第１のユーザのアクセス制御ルールに設定することができる。

【００１６】

また、この発明の第１及び第２の観点は以下のような態様を備えることを特徴とする。

第１の態様は、上記発行手段により、システム上で発行要求元のユーザの識別子と関連付けられた仮名を暗号化した一時ユーザ指定子を発行し、上記解決手段により、上記発行された暗号化一時ユーザ指定子を復号して上記仮名に変換したのち、この変換された仮名を上記発行要求元のユーザの識別子に変換するものである。

このようにすると、上記暗号化された一時ユーザ指定子を復号するために使用する秘密鍵が流出して、一時ユーザ指定子が第三者に復号されても、システム上で使用されている実ＩＤ（ユーザＩＤやログインＩＤ）を第三者に知られるリスクを回避できる。

【００１７】

第２の態様は、上記発行手段により、一時ユーザ指定子に有効期間を表す情報を含め、解決手段により、上記復号された一時ユーザ指定子に含まれる有効期間を表す情報をもとに、当該一時ユーザ指定子が有効か無効かを判定するようにしたものである。

このようにすると、一時ユーザ指定子の用途に応じてその有効期間を設定することができる。例えば、医師等の場合には、一時ユーザ指定子を渡す相手が複数人に及ぶため、有効期限の長い一時ユーザ指定子を発行することで、複数人の相手のそれぞれに対しその都度一時ユーザ指定子を発行すめる場合と比べユーザの負担を軽減することができる。

【００１８】

第３の態様は、上記解決手段に失効リスト記憶手段を設け、端末から送信される失効登録要求に応じて、当該失効登録要求により指定された一時ユーザ指定子を上記失効リスト記憶手段に記憶させる。そして、解決要求を受信したときに、この要求に応じて復号された一時ユーザ指定子が上記失効リスト記憶手段に記憶されているか否かを判定し、記憶されている場合に当該一時ユーザ指定子を無効とするようにしたものである。

このようにすると、一時ユーザ指定子を紛失したり悪用された場合に、この一時ユーザ指定子を休止又は廃止することが可能になる。

【００１９】

第４の態様は、上記解決手段に、端末から送信される失効削除要求に応じて、当該失効削除要求により指定される一時ユーザ指定子を上記失効リスト記憶手段から削除する機能をさらに備えるようにしたものである。

このようにすると、一時的に使用を休止した一時ユーザ指定子の使用を再開させることが可能となる。

【００２１】

第５の態様は、上記発行手段により当該発行手段が所有する秘密鍵を用いて一時ユーザ指定子に署名を行い、解決手段により上記復号された一時ユーザ指定子の署名を上記秘密鍵と対をなす公開鍵を用いて検証するようにしたものである。

このようにすると、解決処理時に一時ユーザ指定子について署名検証を行うことが可能となり、これにより一時ユーザ指定子を紛失した場合のセキュリティを高めることができる。

【発明の効果】

【００２２】

すなわちこの発明によれば、ユーザを識別するための情報を公開したり無制限に検索させることなく、システム上で安全に所望のユーザを指定することを可能にした情報アクセス制御システム及び方法を提供することができる。

【図面の簡単な説明】

【００２３】

【図１】この発明の一実施形態に係わるユーザ指定方法を実施するためのシステムの機能構成を示すブロック図である。

【図２】図１に示したシステムで使用される一時ユーザ指定子（ＴＵＳ）の構成要素を示す図である。

【図３】図１に示したシステムで使用される一時ユーザ指定子（ＴＵＳ）の種類を示す図

である。
【図４】図１に示したシステムのＷｅｂ連携サーバに設けられるＴＵＳ発行手段の機能構成を示す図である。
【図５】図１に示したシステムのＷｅｂ連携サーバに設けられるＴＵＳ解決手段の機能構成を示す図である。
【図６】図１に示したシステムにおけるＴＵＳ発行処理手順とその内容（利用シーンＡの場合）を示すフローチャートである。
【図７】図１に示したシステムにおけるＴＵＳ受け渡し処理手順とその内容（利用シーンＡの場合）を示すフローチャートである。
【図８】図１に示したシステムにおけるＴＵＳ解決処理及びその利用手順とその内容（利用シーンＡの場合）を示すフローチャートである。
【図９】図１に示したシステムにおけるＴＵＳ発行処理手順とその内容（利用シーンＢの場合）を示すフローチャートである。
【図１０】図１に示したシステムにおけるＴＵＳ受け渡し処理手順とその内容（利用シーンＢの場合）を示すフローチャートである。
【図１１】図１に示したシステムにおけるＴＵＳ解決処理及びその利用手順とその内容（利用シーンＢの場合）を示すフローチャートである。
【図１２】図１に示したシステムにおけるＴＵＳ失効処理手順とその内容を示すフローチャートである。
【図１３】図１に示したシステムにおける失効済みＴＵＳ有効化処理手順とその内容を示すフローチャートである。
【図１４】図１に示したシステムにおいて各サーバが保有するユーザ識別子とそのサーバ間受け渡し処理の一例を示す図である。
【図１５】図６又は図９に示したＴＵＳ発行処理手順が実行されるときのＷｅｂ連携サーバ内の動作内容を示す図である。
【図１６】図８又は図１１に示したＴＵＳ解決処理手順が実行されるときのＷｅｂ連携サーバ及び認証サーバ内の動作内容を示す図である。
【図１７】図１２に示したＴＵＳ失効処理手順が実行されるときのユーザサポートセンタ及び認証サーバ内の動作内容を示す図である。
【図１８】図１２に示したＴＵＳ失効処理手順実行するために用いるＴＵＳ失効リストのレコードの構成要素を示す図である。
【図１９】この発明の他の実施形態に係わる発行済みＴＵＳを管理する機能を備えた場合のＴＵＳ解決処理の手順と内容を示すフローチャートである。
【発明を実施するための形態】
【００２４】
以下、図面を参照してこの発明に係わる実施形態を説明する。
この発明の一実施形態に係わる情報アクセス制御システムの全体構成を示す機能ブロック図である。
この一実施形態に係わる情報アクセス制御システムは、医療機関や保健関連機関、運動関連施設等がそれぞれ運用する複数のデータプロバイドサーバＤＰＳ１～ＤＰＳｎと、複数のＷｅｂ連携サーバＷＦＳ１～ＷＦＳｍと、認証サーバＩＤＰと、ユーザサポートセンタＵＳＣとを備え、これらのサーバ間及びこれらのサーバと図示しないユーザ端末との間を通信ネットワークを介して接続可能としたものである。
【００２５】
通信ネットワークは、例えばインターネットに代表されるＩＰ網と、このＩＰ網に対しアクセスするための複数のアクセス網とから構成される。アクセス網としては例えばＬＡＮ（Local Area Network）、無線ＬＡＮ、携帯電話網、有線電話網、ＣＡＴＶ（Cable Television）網が用いられる。
【００２６】
ユーザ端末には、患者等の一般ユーザが自宅等において使用する一般ユーザ用の端末と

、医師や保健師、薬剤師等のプロユーザが患者の依頼を受けて患者の医療情報等を取得するために、さらにはアクセス制御ルールを代行設定するために使用する業務用の端末と、ユーザサポートセンタＵＳＣに設けられるオペレータ用のコンソール端末が含まれる。これらの端末には一般にパーソナル・コンピュータが使用されるが、一般ユーザ用端末及びプロユーザ用端末としては携帯電話機やＰＤＡ（Personal Digital Assistant）等の携帯端末を使用することも可能である。

【００２７】

データプロバイドサーバＤＰＳ１～ＤＰＳｎは、中央制御ユニット（Central Control Unit；ＣＰＵ）に、バスを介してプログラムメモリと、各種データベースを保存するためのデータメモリと、通信インタフェースを接続したもので、その機能モジュールとして、認証連携モジュール１１と、情報流通モジュール１２と、情報提供モジュール１３と、アクセス制御ルール管理モジュール１４を備えている。これらの機能モジュールは何れも、上記プログラムメモリに格納されたプログラムを上記ＣＰＵに実行させることにより実現される。

【００２８】

データベースとしては、医療関連情報データベース１５と、アクセス制御ルールデータベース１６と、ローカルユーザデータベース１７を備えている。ローカルユーザデータベース１７には、各ユーザを識別し管理するためのユーザ情報が記憶される。ユーザ情報は、各ユーザに対しデータプロバイドサーバＤＰＳ１～ＤＰＳｎが独自に使用するローカルユーザＩＤと、ユーザ基本情報及びユーザ属性等からなる。医療関係情報データベース１５には、各ユーザの個人情報、例えば保健指導情報や健康診断情報等の医療健康関連情報が上記ユーザＩＤに対応付けられて格納される。

【００２９】

アクセス制御ルールデータベース１６には、医療関連情報データベース１５に格納されているユーザの医療健康関連情報について、当該情報の開示条件を規定するアクセス制御ルールを表す情報が記憶される。アクセス制御ルールには、情報の開示条件を表す複数のルール項目が記載されている。このルール項目は、例えば医療健康関連情報のオーナを示すデータ所有ユーザ（ユーザＩＤ等で管理される）と、アクセス制御対象とするデータ項目（「対象データ－項目」）と、何時から何時までの期間に登録されたデータをアクセス制御対象とするかを示す情報である「対象データ－期間」と、誰をアクセス制限又は許可の対象とするかを示す「対象ユーザ」と、どの組織をアクセス制限又は許可の対象とするかを示す「対象ユーザ－所属組織」と、どのような資格を持った者をアクセス制限又は許可の対象とするかを示す「対象ユーザ－ロール」と、情報所有者とどのような人間関係にある者を個人情報又はアクセス制御ルールに対するアクセス制限又は許可の対象とするかを示す「対象ユーザ－関係」とから構成される。「対象データ－項目」としては、例えば、病名、投薬名、体重、アレルギー情報がある。また、アクセス制御ルールには、上記各ルール項目に加え、上記アプリケーションデータベース１９に格納されているユーザの医療健康関連情報の読み取りの可否を表す項目と、当該医療健康関連情報の書き込みの可否を表す項目が記載されている。

【００３０】

なお、例えばアクセス制御対象とするユーザがＩＣカードとパスワードで認証された際にのみアクセスを許可するといったように、アクセスを許可する認証手段を限定する項目（「対象ユーザ－認証手段」）を含ませることも可能である。また、このアクセス制御ルール自体の有効期間を示す「ルール有効期間」項目を含ませ、これにより特定の期間にのみ情報を開示／非開示とすることも可能とする。

【００３１】

認証連携モジュール１１は、ローカルユーザデータベース１７に記憶されたユーザ情報に基づいてシングルサインオンのための処理を実行する。これによりユーザは一度のログインにより他のサーバには再度の認証なしにアクセスすることが可能となる。情報流通モジュール１２は、Ｗｅｂ連携サーバＷＦＳ１～ＷＦＳｍからの要求を受理して情報提供モ

ジュールに渡し、処理結果を受け取って要求元のＷｅｂ連携サーバＷＦＳ１～ＷＦＳｍに返送する。Ｗｅｂ連携サーバＷＦＳ１～ＷＦＳｍとデータプロバイドサーバＤＰＳ１～ＤＰＳｎとの間では、ＩＤＰから取得した認証情報とローカルユーザデータベース１７に格納されたＩＤ連携情報を用いてセキュアなデータ流通を行う。

【００３２】

情報提供モジュール１３は、認証連携されたＷｅｂ連携サーバＷＦＳ１～ＷＳＦｍから送信された情報取得要求を情報流通モジュール１２が受信したとき、この要求に応じて医療関連情報データベース１５に格納された情報、つまりローカルＩＤに関連付けられて管理されている医療関連情報を選択的に読み出して要求元へ送信する処理を行う。また、上記医療関連情報へアクセスする際に、情報提供モジュール１３はローカルユーザデータベース１７に記憶されたユーザＩＤと、アクセス制御ルールデータベース１６に記憶された対応するアクセス制御ルールに基づいて、要求元のユーザが開示条件を満足するユーザであるか否かを判断する。

【００３３】

アクセス制御ルール管理モジュール１４は、Ｗｅｂ連携サーバＷＦＳ１～ＷＦＳｍから送信された、アクセス制御ルールの登録、更新又は削除を要求するリクエストを受信した場合に、この受信されたリクエストに基づいてアクセス制御ルールデータベース１６に記憶されているアクセス制御ルールに対しルールの登録、更新又は削除処理を行う。

【００３４】

Ｗｅｂ連携サーバＷＦＳ１～ＷＦＳｍは、ＣＰＵにバスを介してプログラムメモリと、ローカルユーザデータベース２８を備えるデータメモリと、図示しないユーザ端末との間で通信を行うユーザインタフェース２１を接続したものからなる。ローカルユーザデータベース２８には、各ユーザを識別し管理するためにＷｅｂ連携サーバＷＦＳ１～ＷＦＳｍが独自に使用するローカルユーザＩＤが記憶される。

【００３５】

また、機能モジュールとしては、認証連携モジュール２２と、情報流通モジュール２３と、アクセス制御ルール管理要求モジュール２４と、情報取得要求モジュール２５を備え、さらにＴＵＳ発行モジュール２６及びＴＵＳ解決要求モジュール２７を備えている。これらの機能モジュールは何れも、上記プログラムメモリに格納されたプログラムを上記ＣＰＵに実行させることにより実現される。

【００３６】

認証連携モジュール２２は、ユーザ端末からのログイン要求を受信した場合に認証サーバＩＤＰに認証処理を委託し、認証サーバＩＤＰから認証結果情報を受け取る。情報取得要求モジュール２５は、認証後にユーザ端末から送信される情報取得要求をユーザインタフェース２１が受信したとき、この受信した情報取得要求を情報流通モジュール２３からデータプロバイドサーバＤＰＳ１～ＤＰＳｎへ送信する。そして、上記情報取得要求に対しデータプロバイドサーバＤＰＳ１～ＤＰＳｎから返送された医療関係情報を情報流通モジュール２３が受信したとき、この受信した医療関係情報ユーザインタフェース２１から要求元のユーザ端末へ送信する処理を行う。

【００３７】

アクセス制御ルール管理要求モジュール２４は、ユーザ端末から送信されたアクセス制御ルールの設定要求をユーザインタフェース２１が受信したとき、この受信した設定要求に応じてデータプロバイドサーバＤＰＳ１～ＤＰＳｎに対し情報流通モジュール２２からアクセス制御ルールの登録、更新または削除を要求する処理を行う。

【００３８】

ＴＵＳ発行モジュール２６は、ユーザ端末からの発行要求をユーザインタフェース２１が受信した場合に、他のサーバに問い合わせ等を行うことなくＷｅｂ連携サーバＷＦＳ１～ＷＦＳｍ内で一時ユーザ指定子（以下、ＴＵＳ：Temporary User Specifierと呼称する）を発行するもので、図４に示すようにＴＵＳ文字列生成処理部２６１と、暗号化処理部２６２とからなる。

【００３９】
ＴＵＳ文字列生成処理部２６１は、ＴＵＳの発行を要求したユーザを識別するための情報と、ＴＵＳの有効期間を表す情報と、乱数を含むＴＵＳ文字列を生成する。またＴＵＳ文字列には、ユーザ属性と、発行元となるＷｅｂ連携サーバＷＦＳ１～ＷＦＳｍのプロバイダＩＤと、表示名を含めることも可能である。
【００４０】
図２にＴＵＳの構成要素を示す。発行要求元ユーザを識別するための情報としては、システムユーザＩＤ、仮名等が用いられる。乱数は８桁のランダムな数値からなる。有効期間は有効期限開始日時とその終了日時とにより表される。ユーザ属性は、ログインユーザの所属組織情報とロール情報からなる。所属組織情報には、ログインユーザが所属する機関（病院、診療所、自治体等）を表す情報が含まれる。ロール情報には、ログインユーザが保有するロール（医療従事者資格など）が含まれる。
【００４１】
ＴＵＳにユーザ属性を埋め込むことは、特に医療従事者資格を有するプロユーザがＴＵＳを発行する場合において有用である。例えば、一般ユーザが自らのアクセス制御ルールに「Ａ病院の医師には自分の情報を開示する」というルールを記述したい場合、ＴＵＳに組織やロールを含めることによって、ユーザＩＤの設定と同様に所属組織とロール情報を設定することが可能となる。すなわち、ＴＵＳはその目的により使い分けることができる。図３はその目的別のＴＵＳの種類を示すものである。また、ＴＵＳにプロバイダＩＤを埋め込むことで、ＴＵＳ発行元のＷｅｂ連携サーバＷＦＳ１～ＷＦＳｍ以外でもＴＵＳ解決を受け付けることが可能となる。
【００４２】
さらに、ＴＵＳにニックネームや質問／回答等の表示名を埋め込むと、後述するＴＵＳの解決処理時に、ＴＵＳに埋め込んだニックネームを解決要求元のユーザ端末に表示して発行元のユーザを確認させることができる。また、質問に対する回答を要求することにより、発行要求元のユーザが、本当に自分が意図する相手のＴＵＳであることを解決要求元のユーザ端末に確認させることができる。すなわち、ＴＵＳに埋め込まれたユーザ識別情報が本当にＴＵＳを渡された実在の人物を指しているのかを解決要求元のユーザ端末が確認することができる。
【００４３】
暗号化処理部２６２は、上記生成されたＴＵＳ文字列を認証サーバＩＤＰの公開鍵を用いて暗号化する。またその際、セキュリティをさらに強化するため、Ｗｅｂ連携サーバＷＦＳ１～ＷＦＳｍの秘密鍵を用いてＴＵＳ文字列に署名を付与する。この暗号化処理がなされたＴＵＳは、ユーザインタフェース２１から発行要求元のユーザ端末へ返送される。
【００４４】
ＴＵＳ解決要求モジュール２７は、ユーザ端末から送信された暗号化ＴＵＳの解決要求をユーザインタフェース２１が受信した場合に、このユーザから受け取った暗号化ＴＵＳを認証サーバＩＤＰへ転送してＴＵＳの解決を要求する。そして、解決処理により変換されたＴＵＳを認証サーバＩＤＰから受信し、ユーザインタフェース２１から要求元のユーザ端末へ返送する。
【００４５】
認証サーバＩＤＰは、上記Ｗｅｂ連携サーバＷＦＳ１～ＷＦＳｍと同様に、ＣＰＵに対しバスを介してプログラムメモリと、データベースを記憶するデータメモリと、通信インタフェースを接続したもので、その機能モジュールとして認証モジュール３１と、認証連携モジュール３２と、情報流通モジュール３３と、管理用処理受付モジュール３４を備え、さらにＴＵＳ解決モジュール３５と、ＴＵＳ失効管理モジュール３６を備えている。これらの機能モジュールは何れも、上記プログラムメモリに格納されたプログラムを上記ＣＰＵに実行させることにより実現される。
【００４６】
またデータベースとしては、システムユーザデータベース３７と、ＴＵＳ失効リストデ

ータベース３８を備えている。システムユーザデータベース３７には、システムに登録されているユーザのシステムユーザＩＤ、システムログインＩＤ及びこれらのＩＤに関連付けられた仮名、つまりサーバ間のデータ送受信に用いられる連携用のＩＤが記憶される。また必要に応じてユーザＩＤと関連付けられてユーザの属性情報も記憶される。

【００４７】

ＴＵＳ失効リストデータベース３８にはＴＵＳ失効リストが格納される。ＴＵＳ失効リストには、システムユーザＩＤとＴＵＳが含まれる。なお、ＴＵＳ失効リストには、この他に要件に応じて失効日時、失効操作者、失効理由等を追加することも可能である。失効日時や失効操作者は監査時等の確認に、失効理由は失効済みＴＵＳを復活させる際の判断材料として用いることができる。

【００４８】

認証モジュール３１は、ユーザがログイン、情報取得要求及びアクセス制御ルールへのアクセス要求を送信したとき、当該要求元のユーザに対する認証処理を行うものである。具体的には、Ｗｅｂ連携サーバＷＦＳ１～ＷＦＳｍから認証要求が送られたとき、システムユーザデータベース３７に記憶されたユーザ情報を参照して、当該要求元のユーザの正当性を認証する。認証方式としては、ＩＤ／パスワード認証、ＩＣカード認証、公開鍵暗号基盤認証、多要素認証等の様々な認証方式を用いることができる。認証連携モジュール３２は、認証モジュール２１による認証処理の結果をＷｅｂ連携サーバＷＦＳ１～ＷＦＳｍに返す。

【００４９】

情報流通モジュール３３は、Ｗｅｂ連携サーバＷＦＳ１～ＷＦＳｍとデータプロバイドサーバＤＰＳ１～ＤＰＳｎとの間で情報流通、つまり医療関連情報の伝送やアクセス制御ルール管理要求／応答の伝送が行われる場合に、ＷＥｂ連携サーバＷＦＳ１～ＷＦＳｍからの要求に応じてデータプロバイドサーバＤＰＳ１～ＤＰＳｎの所在（ディレクトリ）を通知し、両サーバ間における情報流通を成立させるための仲介を行う。管理用処理受付モジュール３４は、後述するユーザサポートセンタＵＳＣからの要求を受け付け、システムユーザデータベース３７へのユーザ情報の登録、更新又は削除を行う。また、ＴＵＳ失効リスト管理要求（追加・削除）を受け付け、ＴＵＳ失効管理モジュール３６に渡す。

【００５０】

ＴＵＳ解決モジュール３５は、Ｗｅｂ連携サーバＷＦＳ１～ＷＦＳｍから受け取ったＴＵＳを解決して発行元ユーザのシステム上の識別子に変換する処理を行うもので、以下のような機能を備えている。図５はその機能構成を示すブロック図である。すなわち、ＴＵＳ解決モジュール３５は復号処理部３５１を有し、上記Ｗｅｂ連携サーバＷＦＳ１～ＷＦＳｍから受け取ったＴＵＳを、認証サーバＩＤＰが所持する秘密鍵を用いて復号する。また、ＴＵＳに署名が付与されている場合には、復号に先立ち発行元のＷｅｂ連携サーバＷＦＳ１～ＷＦＳｍの公開鍵を用いて署名を検証する。

【００５１】

すなわち、ＴＵＳは認証サーバＩＤＰの秘密鍵で暗号化されているため、ＴＵＳの解決は認証サーバＩＤＰのみが行える。また、ＴＵＳを解決してシステム上のユーザ識別子に変換してからでないと、ＴＵＳで示されるユーザに関するシステム上の機能、例えばそのユーザをアクセス制御ルールに追加する等を利用することができない。

【００５２】

ＴＵＳ解決モジュール３５は、次に有効期間判定部３５２において、現在時刻が上記復号されたＴＵＳに含まれる有効期間情報により表される期間内であるかどうかを判定する。この判定の結果、現在時刻が有効期間内であれば、失効リスト判定部３５３において、上記復号されたＴＵＳがＴＵＳ失効リストデータベース３８に存在しないかどうかを判定する。そして、存在しなければ、変換部３５４において、上記復号されたＴＵＳをシステム上のユーザ識別子（システムユーザＩＤまたは仮名等）に変換し、この変換されたユーザ識別子を要求元のＷｅｂ連携サーバＷＦＳ１～ＷＦＳｍへ返送する。

【００５３】

ＴＵＳ失効管理モジュール３６は、後述するユーザサポートセンタＵＳＣからＴＵＳの失効要求又は失効解除要求を管理用処理受付モジュール３４を介して受け取った場合に、これらの要求の内容に応じてＴＵＳ失効リストデータベース３８に失効対象のＴＵＳを追加したり、ＴＵＳ失効リストデータベース３８から失効解除となったＴＵＳを削除する処理を行う。

【００５４】

ユーザサポートセンタＵＳＣも、上記認証サーバＩＤＰ等と同様に、ＣＰＵにバスを介してプログラムメモリと、データメモリと、ユーザインタフェース４１を接続したもので、その機能モジュールとして、管理用処理要求モジュール４２と、ＴＵＳ失効管理要求モジュール４３を備えている。これらの機能モジュールは何れも、上記プログラムメモリに格納されたプログラムを上記ＣＰＵに実行させることにより実現される。

【００５５】

管理用処理要求モジュール４２は、図示しないオペレータ（システム管理者）の端末から送信される要求に応じて、認証サーバＩＤＰが管理するシステムユーザデータベース３７及び仮名の登録、更新又は削除を認証サーバＩＤＰに要求する処理を行う。また、データプロバイドサーバＤＰＳ１～ＤＰＳｎ及びＷｅｂ連携サーバＷＦＳ１～ＷＦＳｍがそれぞれ独自に使用する仮名をシステム共通のユーザＩＤに、又はシステム共通のユーザＩＤからそれぞれの仮名に変換する機能も持つ。また、ＴＵＳ失効管理要求モジュール４３からの要求を認証サーバＩＤＰへ転送する機能を持つ。

【００５６】

ＴＵＳ失効管理要求モジュール４３は、図示しないオペレータ端末から送信されたＴＵＳの失効要求又は失効解除要求をユーザインタフェース４１が受信した場合に、この受信されたＴＵＳの失効要求又は失効解除要求を管理用処理要求モジュール４２を介して認証サーバＩＤＰへ転送する処理を行う。

【００５７】

次に、以上のように構成されたシステムの動作を説明する。

（１）アクセス制御ルールへのユーザ登録（利用シーンＡ）

ここでは、例えばユーザＡの医療関係情報に対し設定されたアクセス制御ルールに、当該医療関係情報へのアクセスを許可するユーザとして、例えばユーザＡの家族或いは担当医師であるユーザＢを登録する場合を例にとって説明する。図６乃至図８はそのシーケンスを示す図、図１４はＴＵＳの発行からアクセス制御ルールへのユーザ情報の登録までの過程においてサーバ間で受け渡しされる制御データの一例を示す図である。

【００５８】

（１－１）ＴＵＳの発行

ユーザ情報の登録を依頼する側のユーザＢは、自身のユーザ端末において、図６に示すように先ずシステムに対しログインする（ステップＳ６１）。そうすると認証サーバＩＤＰにおいて上記ログインユーザの認証処理が行われ（ステップＳ６２）、ログインユーザの正当性が認められるとその応答がログイン元のユーザ端末に返送される。

【００５９】

この状態で、ユーザＢがユーザ端末においてＴＵＳの発行を要求するための操作を行ったとする（ステップＳ６３）。例えば、このときユーザ端末には図１４のＧ１に示すような操作画面が表示され、ユーザＢは表示されたメニューの中で「ＴＵＳ発行」を選択する。そして、ＴＵＳに含めるための図２に示した各構成要素（パラメータ）を任意に入力する。そうすると、ユーザ端末ではＴＵＳ発行要求が生成され、このＴＵＳ発行要求はＷｅｂ連携サーバＷＦＳ１へ送信される。

【００６０】

Ｗｅｂ連携サーバＷＦＳ１は、上記ＴＵＳ発行要求を受信するとステップＳ６４においてＴＵＳを発行して要求元のユーザ端末へ返送する。図１５はその処理手順と内容を示したものである。

同図において、ＴＵＳ発行要求はユーザインタフェース２１で受信され、ＴＵＳ発行モ

ジュール２６に転送される。ＴＵＳ発行モジュール２６は、上記ＴＵＳ発行要求を受け取ると、このＴＵＳ発行要求に含まれる入力パラメータ（図２の項番３～７）をチェックする。そして、情報流通モジュール２３を呼び出し、情報流通モジュール２３が管理する要求元ユーザの認証結果情報を取得する。

【００６１】

例えば、先ず入力パラメータにてロール情報（ロールＩＤ）又は所属組織情報（所属組織コード）が指定されている場合には、これらが上記認証結果情報の中に存在するか否かを判定する。この判定の結果、認証結果情報に含まれていれば、Ｗｅｂ連携サーバＷＦＳ１のローカルユーザＩＤと認証サーバＩＤＰのプロバイダＩＤを検索キーとしてローカルユーザデータベース２８に対しアクセスし、ローカルユーザＩＤに相当する仮名を読み出す。図１４では“Bwfs1”が読み出された場合を例示している。

【００６２】

続いて、情報流通モジュール２３を呼び出し、この情報流通モジュール２３が管理するＷｅｂ連携サーバ（自プロバイダ）ＷＦＳ１のプロバイダＩＤを取得する。そして、ＴＵＳを生成する各構成要素、つまり上記ユーザ端末から受信した入力パラメータ、上記取得された仮名及び乱数を連結する。各構成要素はKey=Value形式とし、ValueはＵＲＬエンコードを行う。

【００６３】

次に、上記連結されたＴＵＳの構成要素を認証サーバＩＤＰの公開鍵で暗号化する。例えば、BASE64エンコードを用いて文字列を生成する。そして、この生成された暗号化文字列に認証サーバＩＤＰのプロバイダＩＤと、上記取得た自己のＷｅｂ連携サーバＷＦＳ１のプロバイダＩＤを連結してＴＵＳとする。なお、暗号化にはＲＳＡ暗号などを使用する。最後に、上記生成された暗号化ＴＵＳを、ユーザインタフェース２１から要求元のユーザ端末へ返送する。

なお、上記ＴＵＳの受信後にユーザＢがログアウト操作を行うと（ステップＳ６５）、認証サーバＩＤＰにおいてログアウトが受け付けられて、ログアウト処理される（ステップＳ６６）。

【００６４】

（１－２）発行されたＴＵＳの受け渡し

Ｗｅｂ連携サーバＷＦＳ１から送られたＴＵＳは、図７に示すようにユーザＢのユーザ端末からユーザＡのユーザ端末へ例えば電子メールにより送信される（ステップＳ７１，Ｓ７２）。なお、上記ＴＵＳの受け渡しは、ＴＵＳをＦＤやＵＳＢメモリ等の記憶媒体に保存し、この記憶媒体をユーザＢからユーザＡに手渡しすることで行ってもよい。

【００６５】

このＴＵＳの受け渡しの具体例としては、以下のようなものが考えられる。

（１－２－１）市民が発行した短期の有効期限が設定されたＴＵＳの受け渡し

市民が短期の有効期限を設定したＴＵＳを自分の家族等に受け渡す場合には、発行されたＴＵＳのみ又はＴＵＳを発行したＷｅｂ連携サーバＷＦＳ１のＵＲＬと発行されたＴＵＳを埋め込んだＵＲＬを作成し、このＵＲＬを記述した電子メールをユーザＢの端末からユーザＡの端末へ送信する。

【００６６】

（１－２－２）医師が発行した長期の有効期限を設定したＴＵＳの受け渡し

医師など、業務においてシステムを利用し、情報を開示してもらう必要があるプロユーザ（自身のＴＵＳを渡す必要がある相手）が複数人におよぶ場合には、利便性向上のため、ＴＵＳの有効期限は長期（例えば、同一病院に勤めている期間）に設定し、次のような方法でＴＵＳを受け渡すことが考えられる。

【００６７】

すなわち、先ず医師に受診した後、患者が自宅でアクセス制御ルールに医師を登録するケースでは、医師が発行したＴＵＳ（文字列）またはＴＵＳの内容を二次元バーコードなどに変換したものを名刺に印刷し、患者（医師に対し情報を開示してほしい相手）に配布

する方法が考えられる。

【００６８】

また、病院において、受診前に患者が医師を自身のアクセス制御ルールに医師を登録するケースでは、医師が発行したＴＵＳを含むバーコードを受付で渡し、病院に設置された専用端末で患者がシステムにログインしてバーコードを読み込ませることで、アクセス制御ルールに医師を登録する。

【００６９】

尚、ＴＵＳは「開示してほしい側のユーザを示す指定子」であり、さらに業務でシステムを利用する医師などのプロユーザの場合、自身の医療関連情報を保有していないため、長期の有効期限が設定されたＴＵＳを複数人に配布しても、悪用される危険性は極めて少ない。

【００７０】

（１－３）ＴＵＳの解決とその利用

他者のユーザ情報を自身のアクセス制御ルールに登録しようとするユーザＡは、自身のユーザ端末において、図８に示すように先ずシステムに対しログインする（ステップＳ８１）。そうすると認証サーバＩＤＰにおいて上記ログインユーザの認証処理が行われ（ステップＳ８２）、ログインユーザの正当性が認められるとその応答がログイン元のユーザ端末に返送される。

【００７１】

この状態で、ユーザＡがユーザ端末において、ユーザＢから渡されたＴＵＳの解決を要求するための操作を行ったとする（ステップＳ８３）。そうすると、ユーザ端末ではＴＵＳ解決要求が生成され、このＴＵＳ解決要求はＷｅｂ連携サーバＷＦＳ２へ送信される。Ｗｅｂ連携サーバＷＦＳ２は、上記ＴＵＳ解決要求を受信するとステップＳ８４によりこのＴＵＳ解決要求を認証サーバＩＤＰへ転送する。認証サーバＩＤＰは、転送されたＴＵＳを解決し（ステップＳ８５）、その結果を要求元のユーザＡのユーザ端末へ返送する。図１６はその処理手順と内容を示したものである。

【００７２】

Ｗｅｂ連携サーバＷＦＳ２は、ユーザ端末から送信されたＴＵＳ解決要求をユーザインタフェース２１により受信すると、ＴＵＳ解決要求モジュール２７が要求されたＴＵＳに含まれる入力パラメータをチェックする。そして、情報流通モジュール２３を呼び出し、情報流通モジュール２３が管理する要求元ユーザの認証結果情報を取得する。続いて、認証サーバＩＤＰに送付するＴＵＳ解決要求電文を作成し、上記取得した要求元ユーザの認証結果と、上記作成されたＴＵＳ解決要求電文とを引数として情報流通モジュール２３を呼び出し、認証サーバＩＤＰへＴＵＳ解決要求電文を送信する。

【００７３】

認証サーバＩＤＰは、Ｗｅｂ連携サーバＷＦＳ２から送信されたＴＵＳ解決要求電文を情報流通モジュール３３により受信すると、ＴＵＳ解決モジュール３５が上記受信されたＴＵＳ解決要求電文をチェックする。そして、ＴＵＳ解決要求電文よりＴＵＳを取得し、認証サーバＩＤＰの秘密鍵で復号する。

【００７４】

次に、ＴＵＳ解決モジュール３５は、上記復号されたＴＵＳの有効期限をチェックする。このチェックの結果、有効期限開始日時が設定されない場合には、すでに解決処理が開始されているものとして扱う。また、有効期限終了日時が設定されない場合には無期限として扱う。

【００７５】

続いて、ＴＵＳ解決モジュール３５は、上記復号されたＴＵＳがＴＵＳ失効リストデータベース３８に記憶されていないか否かを判定する。つまり、上記復号されたＴＵＳが失効していないかどうかを確認する。この判定の結果、解決を要求されたＴＵＳが失効していなければ、上記復号されたＴＵＳの仮名と、ＴＵＳ解決要求電文に含まれるＴＵＳ発行元のＷｅｂ連携サーバＷＦＳ２のプロバイダＩＤを検索キーとして、情報流通モジュール

３３を介してシステムユーザデータベース３７に対しアクセスし、仮名及びプロバイダＩＤに対応するシステムユーザＩＤを取得する。例えば、いま仮名が“Bwfs1”、プロバイダＩＤが“Wfs1”であれば、図１４に示すようにシステムユーザＩＤとして“B@idp”が得られる。

【００７６】

続いて、ＴＵＳ解決モジュール３５は、上記取得されたシステムユーザＩＤと、ＴＵＳ解決要求電文にＴＵＳ解決要求元のＷｅｂ連携サーバＷＦＳ２のプロバイダＩＤを検索キーとして、情報流通モジュール３３を介してシステムユーザデータベース３７に対しアクセスし、これによりシステムユーザＩＤに該当する仮名を取得する。この処理により、ＴＵＳ発行元のＷｅｂ連携サーバＷＦＳ１とは異なるＷｅｂ連携サーバＷＦＳ２でも、ＴＵＳ解決要求を行うことができる。

【００７７】

続いて、ＴＵＳ解決モジュール３５は、上記取得された仮名と、ＴＵＳから抽出したロール情報（ロールＩＤ）、所属組織情報（所属組織コード）および表示名とを含む応答電文を作成する。そして、この作成された応答電文を情報流通モジュール３３から要求元のＷｅｂ連携サーバＷＦＳ２へ返送する。

【００７８】

認証サーバＩＤＰから応答電文を受け取ると、Ｗｅｂ連携サーバＷＦＳ２のＴＵＳ解決要求モジュール２７は、上記受け取ったＴＵＳ解決応答電文からＴＵＳの構成要素である仮名、所属組織情報、ロール情報、表示名を取得し、ＴＵＳの発行元ユーザのユーザ識別子を生成する。そして、この生成されたＴＵＳの発行元ユーザのユーザ識別子をユーザインタフェース２１から解決要求元のユーザ端末へ返送する。

【００７９】

上記ＴＵＳの発行元ユーザのユーザ識別子を受信すると、ユーザＡはこの受信したユーザ識別子を自身のアクセス制御ルールへ登録するための操作を行う（ステップＳ８６）。例えば、このときユーザ端末には図１４のＧ２に示すような操作画面が表示され、ユーザＡは表示されたメニューの中で「アクセス制御ルール設定」を選択する。そうすると、ユーザ端末ではアクセス制御ルール設定要求が生成され、このアクセス制御ルール設定要求はＷｅｂ連携サーバＷＦＳ２へ送信される。

【００８０】

Ｗｅｂ連携サーバＷＦＳ２は、上記ユーザ端末から送信されたアクセス制御ルール設定要求をユーザインタフェース２１により受信すると、アクセス制御ルール管理要求モジュール２４が、ユーザＡの認証結果情報と、上記受信されたアクセス制御ルール設定要求に含まれるユーザＢのユーザ識別子を引数として、情報流通モジュール２３を介して認証サーバＩＤＰからデータプロバイドサーバ向けのユーザＡ及びユーザＢの識別子を取得する。そして、この取得したデータプロバイドサーバ向けのユーザＡ及びユーザＢの識別子をもとに、アクセス先のデータプロバイドサーバＤＰＳ１へ情報流通モジュール２３からアクセス制御ルール設定要求を送信する（ステップＳ８８）。

【００８１】

データプロバイドサーバＤＰＳ１は、Ｗｅｂ連携サーバＷＦＳ２から送信された設定要求を情報流通モジュール１２により受信すると、アクセス制御ルール管理モジュール１４が、上記要求に応じてローカルユーザデータベース１７から該当するユーザＡのローカルユーザＩＤを読み出す。そして、この読み出されたローカルユーザＩＤをもとにアクセス制御ルールデータベース１６に対しアクセスし、上記ユーザＡの該当するアクセス制御ルールに、上記受信されたアクセス制御ルール設定要求に含まれる設定対象となるユーザＩＤ等を追加登録する（ステップＳ８８）。

【００８２】

上記登録処理が終了すると、その応答がデータプロバイドサーバＤＰＳ１の情報流通モジュール１２から要求元のＷｅｂ連携サーバＷＦＳ２の情報流通モジュール２３へ返送される。そして、さらにこのＷｅｂ連携サーバＷＦＳ２のアクセス制御ルール管理要求モジ

ュール２４の制御の下で、上記応答がユーザインタフェース２１からユーザＡのユーザ端末へ転送される。

【００８３】

（２）他者によるユーザの医療関係情報の取得（利用シーンＢ）

ここでは、例えばデータプロバイドサーバＤＰＳ１で管理されているユーザＡの医療関係情報を、例えばその家族或いは担当医師であるユーザＢが取得する場合を例にとって説明する。図９乃至図１１はそのシーケンスを示す図である。

【００８４】

（２－１）ＴＵＳの発行

医療関連情報を取得させようとするユーザＡは、自身のユーザ端末において、図９に示すように先ずシステムに対しログインする（ステップＳ９１）。そうすると認証サーバＩＤＰにおいて上記ログインユーザの認証処理が行われ（ステップＳ９２）、ログインユーザの正当性が認められるとその応答がログイン元のユーザ端末に返送される。

【００８５】

この状態で、ユーザＡがユーザ端末においてＴＵＳの発行を要求するための操作を行ったとする（ステップＳ９３）。この要求操作も、先に（１）で述べたアクセス制御ルールへのユーザ情報の登録の場合と同様に、ユーザ端末には操作画面が表示され、ユーザＡは表示されたメニューの中で「ＴＵＳ発行」を選択する。そして、ＴＵＳに含めるための図２に示した各構成要素（パラメータ）を任意に入力する。そうすると、ユーザ端末ではＴＵＳ発行要求が生成され、このＴＵＳ発行要求はＷｅｂ連携サーバＷＦＳ２へ送信される。

【００８６】

Ｗｅｂ連携サーバＷＦＳ２は、上記ＴＵＳ発行要求を受信するとステップＳ９４においてＴＵＳを発行して要求元のユーザ端末へ返送する。このＴＵＳの発行処理は以下のように行われる。

すなわち、Ｗｅｂ連携サーバＷＦＳ２は、ユーザ端末から送信されたＴＵＳ発行要求をユーザインタフェース２１で受信すると、ＴＵＳ発行モジュール２６により、先ず受信されたＴＵＳ発行要求に含まれる入力パラメータ（図２の項番３～７）をチェックする。そして、情報流通モジュール２３を呼び出し、情報流通モジュール２３が管理する要求元ユーザの認証結果情報を取得する。

【００８７】

例えば、先ず入力パラメータにてロール情報（ロールＩＤ）又は所属組織情報（所属組織コード）が指定されている場合には、これらが上記認証結果情報の中に存在するか否かを判定する。この判定の結果、認証結果情報に含まれていれば、Ｗｅｂ連携サーバＷＦＳ２のローカルユーザＩＤと認証サーバＩＤＰのプロバイダＩＤを検索キーとしてローカルユーザデータベース２８に対しアクセスし、ローカルユーザＩＤに相当する仮名を読み出す。続いて、情報流通モジュール２３を呼び出し、この情報流通モジュール２３が管理するＷｅｂ連携サーバ（自プロバイダ）ＷＦＳ２のプロバイダＩＤを取得する。そして、ＴＵＳを生成する各構成要素、つまり上記ユーザ端末から受信した入力パラメータ、上記取得された仮名及び乱数を連結する。

【００８８】

次に、上記連結されたＴＵＳの構成要素を認証サーバＩＤＰの公開鍵で暗号化する。そして、この生成された暗号化文字列に認証サーバＩＤＰのプロバイダＩＤと、上記取得た自己のＷｅｂ連携サーバＷＦＳ２のプロバイダＩＤを連結してＴＵＳとする。なお、暗号化にはＲＳＡ暗号などを使用する。最後に、上記生成された暗号化ＴＵＳを、ユーザインタフェース２１から要求元のユーザ端末へ返送する。

なお、上記ＴＵＳの受信後にユーザＢがログアウト操作を行うと（ステップＳ９５）、認証サーバＩＤＰにおいてログアウトが受け付けられて、ログアウト処理される（ステップＳ９６）。

【００８９】

（２－２）発行されたＴＵＳの受け渡し

Ｗｅｂ連携サーバＷＦＳ２から送られたＴＵＳは、図１２に示すようにユーザＡのユーザ端末からユーザＢのユーザ端末へ例えば電子メールにより送信される（ステップＳ１０１，Ｓ１０２）。なお、上記ＴＵＳの受け渡しは、ＴＵＳをＦＤやＵＳＢメモリ等の記憶媒体に保存し、この記憶媒体をユーザＡからユーザＢに手渡しすることで行ってもよい。このＴＵＳの受け渡しの具体例としては、発行されたＴＵＳのみ又はＴＵＳを発行したＷｅｂ連携サーバＷＦＳ２のＵＲＬと発行されたＴＵＳを埋め込んだＵＲＬを作成し、このＵＲＬを記述した電子メールをユーザＡの端末からユーザＢの端末へ送信する。

【００９０】

（２－３）ＴＵＳの解決とその利用

ユーザＡの医療関連情報を取得しようとするユーザＢは、自身のユーザ端末において、図１１に示すように先ずシステムに対しログインする（ステップＳ１１１）。そうすると認証サーバＩＤＰにおいて上記ログインユーザの認証処理が行われ（ステップＳ１１２）、ログインユーザの正当性が認められるとその応答がログイン元のユーザ端末に返送される。

【００９１】

この状態で、ユーザＢがユーザ端末において、ユーザＡから渡されたＴＵＳの解決を要求するための操作を行ったとする（ステップＳ１１３）。そうすると、ユーザ端末ではＴＵＳ解決要求が生成され、このＴＵＳ解決要求はＷｅｂ連携サーバＷＦＳ１へ送信される。Ｗｅｂ連携サーバＷＦＳ１は、上記ＴＵＳ解決要求を受信するとステップＳ１１４によりこのＴＵＳ解決要求を認証サーバＩＤＰへ転送する。認証サーバＩＤＰは、転送されたＴＵＳを解決し（ステップＳ１１５）、その結果を要求元のユーザＢのユーザ端末へ返送する。

【００９２】

Ｗｅｂ連携サーバＷＦＳ１は、ユーザ端末から送信されたＴＵＳ解決要求をユーザインタフェース２１により受信すると、ＴＵＳ解決要求モジュール２７が要求されたＴＵＳに含まれる入力パラメータをチェックする。そして、情報流通モジュール２３を呼び出し、情報流通モジュール２３が管理する要求元ユーザの認証結果情報を取得する。続いて、認証サーバＩＤＰに送付するＴＵＳ解決要求電文を作成し、上記取得した要求元ユーザの認証結果と、上記作成されたＴＵＳ解決要求電文とを引数として情報流通モジュール２３を呼び出し、認証サーバＩＤＰへＴＵＳ解決要求電文を送信する。

【００９３】

認証サーバＩＤＰは、Ｗｅｂ連携サーバＷＦＳ１から送信されたＴＵＳ解決要求電文を情報流通モジュール３３により受信すると、ＴＵＳ解決モジュール３５が上記受信されたＴＵＳ解決要求電文をチェックする。そして、ＴＵＳ解決要求電文よりＴＵＳを取得し、認証サーバＩＤＰの秘密鍵で復号する。

【００９４】

次に、ＴＵＳ解決モジュール３５は、上記復号されたＴＵＳの有効期限をチェックする。このチェックの結果、有効期限開始日時が設定されない場合には、すでに解決処理が開始されているものとして扱う。また、有効期限終了日時が設定されない場合には無期限として扱う。

【００９５】

続いて、ＴＵＳ解決モジュール３５は、上記復号されたＴＵＳがＴＵＳ失効リストデータベース３８に記憶されていないか否かを判定する。つまり、上記復号されたＴＵＳが失効していないかどうかを確認する。この判定の結果、解決を要求されたＴＵＳが失効していなければ、上記復号されたＴＵＳの仮名と、ＴＵＳ解決要求電文に含まれるＴＵＳ発行元のＷｅｂ連携サーバＷＦＳ２のプロバイダＩＤを検索キーとして、情報流通モジュール３３を介してシステムユーザデータベース３７に対しアクセスし、仮名及びプロバイダＩＤに対応するシステムユーザＩＤを取得する。

【００９６】

続いて、ＴＵＳ解決モジュール３５は、上記取得されたシステムユーザＩＤと、ＴＵＳ解決要求電文にＴＵＳ解決要求元のＷｅｂ連携サーバＷＦＳ１のプロバイダＩＤを検索キーとして、情報流通モジュール３３を介してシステムユーザデータベース３７に対しアクセスし、これによりシステムユーザＩＤに該当する仮名を取得する。この処理により、ＴＵＳ発行元のＷｅｂ連携サーバＷＦＳ２とは異なるＷｅｂ連携サーバＷＦＳ１でも、ＴＵＳ解決要求を行うことができる。

【００９７】

続いて、ＴＵＳ解決モジュール３５は、上記取得された仮名と、ＴＵＳから抽出したロール情報（ロールＩＤ）、所属組織情報（所属組織コード）および表示名とを含む応答電文を作成する。そして、この作成された応答電文を情報流通モジュール３３から要求元のＷｅｂ連携サーバＷＦＳ１へ返送する。

【００９８】

認証サーバＩＤＰから応答電文を受け取ると、Ｗｅｂ連携サーバＷＦＳ１のＴＵＳ解決要求モジュール２７は、上記受け取ったＴＵＳ解決応答電文からＴＵＳの構成要素である仮名、所属組織情報、ロール情報、表示名を取得し、ＴＵＳの発行元ユーザのユーザ識別子を生成する。そして、この生成されたＴＵＳの発行元ユーザのユーザ識別子をユーザインタフェース２１から解決要求元のユーザ端末へ返送する。

【００９９】

上記ＴＵＳの発行元ユーザのユーザ識別子を受信すると、ユーザＢはこの受信したユーザ識別子をもとにユーザＡの医療関連情報を取得するための操作を行う（ステップＳ１１６）。例えば、このときユーザ端末には操作画面が表示され、ユーザＢは表示されたメニューの中で「情報取得」を選択する。そうすると、ユーザ端末では情報取得要求が生成され、この情報取得要求はＷｅｂ連携サーバＷＦＳ１へ送信される。

【０１００】

Ｗｅｂ連携サーバＷＦＳ１は、上記ユーザ端末から送信された情報取得要求をユーザインタフェース２１により受信すると、情報取得要求モジュール２５が、ユーザＢの認証結果情報と、上記受信された情報取得要求に含まれるユーザＡのユーザ識別子を引数として、情報流通モジュール２３を介して認証サーバＩＤＰからデータプロバイドサーバ向けのユーザＡ及びユーザＢの識別子を取得する。そして、この取得したデータプロバイドサーバ向けのユーザＢ及びユーザＡの識別子をもとに、アクセス先のデータプロバイドサーバＤＰＳ１へ情報流通モジュール２３から情報取得要求を送信する（ステップＳ１１７）。

【０１０１】

データプロバイドサーバＤＰＳ１は、Ｗｅｂ連携サーバＷＦＳ１から送信された情報取得要求を情報流通モジュール１２により受信すると、情報提供モジュール１３が、上記要求に応じてローカルユーザデータベース１７から該当するユーザＡのローカルユーザＩＤを読み出す。そして、この読み出されたローカルユーザＩＤをもとに医療関連情報データベース１５に対しアクセスし、上記ユーザＡの該当する医療関連情報を読み出す。そして、この読み出された医療関連情報を、情報流通モジュール１２から要求元のＷｅｂ連携サーバＷＦＳ１へ送信する（ステップＳ１１８）。

【０１０２】

Ｗｅｂ連携サーバＷＦＳ１は、上記データプロバイドサーバＤＰＳ１から送信された医療関連情報を情報流通モジュール２３で受信すると、情報取得要求モジュール２５の制御の下で、この受信された医療関連情報をユーザインタフェース２１からユーザＢのユーザ端末へ転送する。

【０１０３】

（３）ＴＵＳ失効リストの管理

（３－１）ＴＵＳ失効処理

例えば、発行したＴＵＳの紛失や第三者への流出が判明した場合、当該ＴＵＳを失効させる必要がある。このＴＵＳの失効手続きは以下のように行われる。

ここでは、ユーザＡが自身のＴＵＳを失効させたい場合を例にとって説明を行う。図１

２はその処理手順と処理内容の概要を示すフローチャートである。

【０１０４】

ＴＵＳ失効管理は、システムの管理者であるオペレータがユーザからの依頼を受けて行う。ユーザＡはオペレータに対しＴＵＳ失効登録申請書を提出する（ステップＳ１２１）。オペレータは、ステップＳ１２２で上記ＴＵＳ失効登録申請書を受領すると、オペレータ用の端末からシステムにログインする（ステップＳ１２３）。上記ログイン要求を受信するとユーザサポートセンタＵＳＣは、先ずステップＳ１２４でユーザ認証を行う。そして、ログインユーザの正当性が確認されると、その結果をログイン元のオペレータ端末に返送する。

【０１０５】

上記認証結果の通知を受けてオペレータが、上記ＴＵＳ失効登録申請書の内容に基づいてＴＵＳ失効登録要求操作を行うと、オペレータ端末からユーザサポートセンタＵＳＣへＴＵＳ失効リストの追加登録要求が送信される（ステップＳ１２５）。ユーザサポートセンタＵＳＣは、上記ＴＵＳ失効リストの追加登録要求を受信すると、ステップＳ１２６において認証サーバＩＤＰへＴＵＳ失効リストの追加登録要求を転送する。認証サーバＩＤＰは上記ＴＵＳ失効リストの追加登録要求を受信すると、この受信された追加登録要求の内容に応じてＴＵＳ失効リストデータベース３８に失効対象のＴＵＳを追加登録する処理を実行する（ステップＳ１２７）。

【０１０６】

図１７は、上記ユーザサポートセンタＵＳＣ及び認証サーバＩＤＰ内における処理の流れを示す図である。同図において、ユーザサポートセンタＵＳＣは、上記ＴＵＳ失効リストの追加登録要求をユーザインタフェース４１により受信すると、ＴＵＳ失効リスト管理要求モジュール４３が先ず入力パラメータ、つまりＴＵＳおよび認証サーバのプロバイダＩＤをチェックする。続いて、管理用処理要求モジュール４２が認証サーバへＴＵＳ失効リスト追加要求電文を送信する。

【０１０７】

これに対し認証サーバＩＤＰは、上記ユーザサポートセンタＵＳＣから送られたＴＵＳ失効リスト追加要求電文を受信すると、以下のようにＴＵＳ失効リスト追加登録処理を実行する。

すなわち、先ず要求元のユーザサポートセンタＵＳＣのＩＰアドレスが、認証サーバＩＤＰの管理用処理受付モジュール３４で管理されている許可ＩＰアドレスリストに含まれるか否かをチェックする。続いて、入力パラメータ（ＴＵＳのリスト）をチェックする。そして、これらのチェックの結果、受付けの条件を満足すると、上記受信されたＴＵＳ失効リスト追加要求電文に含まれる暗号化されたＴＵＳを復号し、仮名、ＴＵＳの発行元のＷｅｂ連携サーバのプロバイダＩＤ、有効期限開始日時及び有効期限終了日時を抽出する。

【０１０８】

次に、ＴＵＳ失効リスト管理モジュール３６が、上記抽出されたＴＵＳの仮名とプロバイダＩＤを検索キーとして、情報流通モジュール３３を介してシステムユーザデータベース３７を検索し、仮名に相当するシステムユーザＩＤを取得する。続いて、この取得したシステムユーザＩＤを含むＴＵＳ失効リストのレコードを作成する。図１８は、作成されるＴＵＳ失効リストのレコードの一例を示すものである。同図に示すようにＴＵＳ失効リストのレコードは、ユーザＩＤと、ＴＵＳと、ＴＵＳから抽出した有効期間の開始日時及び終了日時と、レコードの作成日時及び更新日時とを含む。

【０１０９】

そして、ＴＵＳ失効リスト管理モジュール３６は、上記作成されたＴＵＳ失効リストのレコードを、ＴＵＳ失効リストデータベース３８のＴＵＳ失効リストに追加登録する。なお、入力パラメータに複数のＴＵＳリストが記載されている場合には、以上のレコード登録処理をこれらのＴＵＳリスト分繰り返す。そして、すべてのレコードの登録が完了すると、登録処理を終了する。

【０１１０】
上記登録処理が終了すると、認証サーバＩＤＰの管理用処理受付モジュール３４が、処理結果を表す応答を要求元のユーザサポートセンタＵＳＣへ返送する。上記処理結果を表す応答は、図１７に示すようにユーザサポートセンタＵＳＣを経由して要求元のオペレータ端末に転送される。
【０１１１】
オペレータは、上記応答を受けると自身の端末においてログアウト操作を行う（ステップＳ１２８）。そうするとユーザサポートセンタＵＳＣは、ステップＳ１２９においてログアウト処理を行い、その結果をオペレータ端末に通知する。オペレータは、上記ログアウト後にステップＳ１３０によりＴＵＳ失効情報を作成し、このＴＵＳ失効情報をユーザＡが使用するユーザ端末へ送信する（ステップＳ１３１）。
かくして、ＴＵＳ失効リストデータベース３８に失効対象のＴＵＳが登録され、以後このＴＵＳの使用は停止される。
【０１１２】
（３－２）失効済みＴＵＳの有効化
一時的に紛失したＴＵＳが見つかった場合、失効済みのＴＵＳの失効を解除することが可能である。この失効済みＴＵＳの有効化処理は以下のように行われる。図１３はその処理手順と処理内容の概要を示すフローチャートである。
【０１１３】
失効済みＴＵＳの有効化処理も、先に述べたＴＵＳ失効登録処理と同様に、システムの管理者であるオペレータがユーザからの依頼を受けて行う。ユーザＡはオペレータに対しＴＵＳ失効削除申請書を提出する（ステップＳ１４１）。オペレータは、ステップＳ１４２で上記ＴＵＳ失効削除申請書を受領すると、オペレータ用の端末からシステムにログインする（ステップＳ１４３）。上記ログイン要求を受信するとユーザサポートセンタＵＳＣは、先ずステップＳ１４４でユーザ認証を行う。そして、ログインユーザの正当性が確認されると、その結果をログイン元のオペレータ端末に返送する。
【０１１４】
上記認証結果の通知を受けてオペレータが、上記ＴＵＳ失効リストの閲覧要求操作を行うと、オペレータ端末からユーザサポートセンタＵＳＣへＴＵＳ失効リストの検索を求めるＴＵＳ失効管理要求が送信される（ステップＳ１４５）。ユーザサポートセンタＵＳＣは、上記ＴＵＳ失効リスト管理要求を受信すると、ステップＳ１４６において認証サーバＩＤＰへ上記ＴＵＳ失効リストの検索を求めるＴＵＳ失効リスト管理要求を転送する。認証サーバＩＤＰは上記ＴＵＳ失効リスト管理要求を受信すると、この受信された要求に応じてＴＵＳ失効リストデータベース３８から該当するＴＵＳ失効リストを読み出し、この読み出されたＴＵＳ失効リストをユーザサポートセンタＵＳＣを経由して要求元のオペレータ端末へ返送する（ステップＳ１４７）。
【０１１５】
オペレータは、自身の端末において、上記返送されたＴＵＳ失効リストの中から失効を削除する対象のＴＵＳを選択する（ステップＳ１４８）。そうすると、オペレータ端末はＴＵＳ失効管理要求モジュール４３によりＴＵＳ失効リストの削除を求めるＴＵＳ失効管理要求を生成し、このＴＵＳ失効管理要求をユーザサポートセンタＵＳＣへ送信する（ステップＳ１４８）。
【０１１６】
ユーザサポートセンタＵＳＣは、上記ＴＵＳ失効管理要求をユーザインタフェース４１により受信すると、ＴＵＳ失効管理要求モジュール４３の制御の下で、管理用処理要求モジュール４２から上記ＴＵＳの失効削除を求めるＴＵＳ失効管理要求を認証サーバＩＤＰへ転送する（ステップＳ１５０）。認証サーバＩＤＰは、上記ＴＵＳ失効リスト管理要求を受信すると、この受信された要求の内容に応じてＴＵＳ失効リストデータベース３８から該当する失効ＴＵＳの失効管理情報を削除する（ステップＳ１５１）。
【０１１７】

上記削除処理が終了すると、認証サーバＩＤＰの管理用処理受付モジュール３４が、処理結果を表す応答を要求元のユーザサポートセンタＵＳＣへ返送する。上記処理結果を表す応答は、ユーザサポートセンタＵＳＣを経由して要求元のオペレータ端末に転送される。オペレータは、上記応答を受けると自身の端末においてログアウト操作を行う（ステップＳ１５２）。そうするとユーザサポートセンタＵＳＣは、ステップＳ１５３においてログアウト処理を行い、その結果をオペレータ端末に通知する。オペレータは、上記ログアウト後にステップＳ１５４により削除処理後の新たなＴＵＳ失効情報を作成し、このＴＵＳ失効情報をユーザＡが使用するユーザ端末へ送信する（ステップＳ１５４）。

かくして、ＴＵＳ失効リストデータベース３８に記憶された失効対象ＴＵＳのうち、有効化すべきＴＵＳの失効状態は解除され、以後このＴＵＳは再び使用可能となる。

【０１１８】

以上詳述したように上記実施形態では、ユーザＡの個人情報に対し規定されたアクセス制御ルールに対し、ユーザＢが自身のユーザ情報の登録を要求する際に、先ずユーザＢの端末からＴＵＳ発行要求を送信して、Ｗｅｂ連携サーバＷＦＳ１により暗号化されたＴＵＳを発行する。次に、ユーザＡの端末からＴＵＳ解決要求を送信し、認証サーバＩＤＰにおいてこのＴＵＳ解決要求に含まれるＴＵＳを復号してユーザＢを識別するための情報に変換し、この変換されたユーザＢを識別するための情報をデータプロバイドサーバＤＰＳ１に送信して上記ユーザＡのアクセス制御ルールに設定するようにしている。

【０１１９】

したがって、ユーザＡの医療関係情報に対応するアクセス制御ルールに設定するユーザＢの識別情報は、ユーザＢ本人の要求に応じてＴＵＳとして発行される。このため、ユーザＢの識別情報を、公開されることなくまた検索されることなく安全にユーザＡに渡すことができる。また、ユーザＡはこの渡されたＴＵＳの解決を要求することで、システム上でユーザＢを確実に指定してその識別情報をユーザＡのアクセス制御ルールに設定することができる。

【０１２０】

またこの実施形態では、ユーザＡの医療関連情報を、ユーザＢが自身の端末からユーザＡの識別情報を用いて取得する際に、先ずユーザＡの端末からＴＵＳの発行要求を送信して、ユーザＡを他者に指定させるための暗号化されたＴＵＳをＷｅｂ連携サーバＷＦＳ２により発行する。次に、上記ユーザＢの端末からＴＵＳ解決要求を送信し、認証サーバＩＤＰにより当該解決要求に含まれる暗号化ＴＵＳを復号してユーザＡの識別情報に変換し、この変換されたユーザＡの識別情報を用いてデータプロバイドサーバＤＰＳ１からユーザＡの医療関係情報を取得するようにしている。

【０１２１】

したがって、ユーザＡの医療関連情報を取得するために必要なユーザＡの識別情報は、ユーザＡ本人の要求に応じてＴＵＳとして発行される。このため、ユーザＡの識別情報は、公開されることなくまた検索されることなく安全にユーザＡからユーザＢに渡すことができる。また、ユーザＢはこの渡されたＴＵＳの解決を自身の端末から要求することで、システム上でユーザＡを確実に指定してその医療関連情報を取得することができる。

【０１２２】

さらにこの実施形態では、ＴＵＳを発行する際に、システム上で発行要求元のユーザＩＤと関連付けられた仮名をＴＵＳに含め、ＴＵＳを解決する際に、上記発行された暗号化ＴＵＳを復号して上記仮名に変換したのち、この変換された仮名を上記発行要求元のユーザＩＤに変換するようにしている。したがって、上記暗号化されたＴＵＳを復号する秘密鍵が流出してＴＵＳが第三者により復号されても、システム上で使用されている実ＩＤ（ユーザＩＤやログインＩＤ）が第三者に知られるリスクを回避できる。

【０１２３】

さらにこの実施形態では、ＴＵＳを発行する際に、ＴＵＳに有効期間の開始日時と終了日時を表す情報を含め、このＴＵＳを解決する際に、復号されたＴＵＳに含まれる有効期間の開始日時と終了日時を表す情報をもとに、当該ＴＵＳが有効か無効かを判定するよう

にしている。したがって、ＴＵＳの用途に応じてその有効期間を任意に設定することができる。例えば、医師等の場合には、ＴＵＳを渡す相手が複数人に及ぶため、有効期間の長いＴＵＳを発行することで、複数人の相手のそれぞれに対しその都度ＴＵＳを発行する場合と比べユーザの負担を軽減することができる。

【０１２４】

さらにこの実施形態では、認証サーバＩＤＰにＴＵＳ失効リストデータベース３８を設け、オペレータ端末からＴＵＳ失効登録要求を送信して、認証サーバＩＤＰにより失効対象のＴＵＳを表す情報をＴＵＳ失効リストデータベース３８に登録する。そして、ユーザがＴＵＳ解決を要求したときに、この要求に応じてＴＵＳが上記ＴＵＳ失効リストデータベース３８に登録されているか否かを判定し、登録されている場合にはこのＴＵＳを使用無効とするようにしている。したがって、ＴＵＳを紛失したり悪用された場合に、このＴＵＳの使用を停止させることが可能になる。

【０１２５】

さらにこの方法を用いると、暗号化されたユーザの識別情報をＴＵＳに埋め込むことで、ＴＵＳを管理する必要がなくなり、ＴＵＳの発行数にも制限がないという利点がある。また、同一ユーザが複数のＴＵＳを発行することも可能である。

【０１２６】

さらにこの実施形態では、オペレータ端末からＴＵＳ失効削除要求を送信して、認証サーバＩＤＰにより失効中のＴＵＳの失効管理情報を削除するようにしている。このため、一時的に使用を停止させたＴＵＳの使用を、ユーザの申請に応じて再開させることが可能となる。

【０１２７】

さらにこの実施形態では、ＴＵＳを発行する際に、ＴＵＳに発行要求元のユーザの識別情報に加えて、発行要求元ユーザの属性情報、例えばユーザの所属組織や資格を表す情報を含めるようにしている。このようにすると、アクセス制御ルールにユーザＩＤを設定する際に、同時に当該設定要求元のユーザの所属組織や資格等を表す情報を設定することが可能となる。

【０１２８】

また、ＴＵＳにその発行元となるＷｅｂ連携サーバのプロバイダＩＤを含めるようにしてもよい。このようにすると、ＴＵＳ発行元のＷｅｂ連携サーバに限らず認証連携されたどのＷｅｂ連携サーバでもＴＵＳの解決要求を受け付けることが可能となる。

さらに、ＴＵＳにニックネームや質問／回答等の表示情報を含めることで、発行元ユーザが入力したニックネーム又は質問等を、ＴＵＳ解決処理時にその解決要求元ユーザに向けて表示してユーザ確認させることが可能となる。

【０１２９】

さらにこの実施形態では、ＴＵＳを発行する際に、Ｗｅｂ連携サーバが保持する秘密鍵を用いてＴＵＳに署名を行い、このＴＵＳを認証サーバＩＤＰが解決する際に、復号されたＴＵＳの署名を上記秘密鍵と対をなす公開鍵を用いて検証するようにしている。したがって、ＴＵＳの解決処理時にＴＵＳについて署名検証を行うことが可能となり、これによりＴＵＳを紛失した場合のセキュリティを高めることができる。

【０１３０】

なお、この発明は上記実施形態に限定されるものではない。例えば、上記実施形態ではＴＵＳの失効管理を行うようにしたが、それに加えてＴＵＳの発行管理も行うようにしてもよい。

ＴＵＳの失効管理のみを行う場合には、ＴＵＳ発行時にＷｅｂ連携サーバＷＦＳ１～ＷＦＳｍと認証サーバＩＤＰとの間の通信が発生しないし、またＴＵＳの発行数が制限されない等の利点がある反面、ユーザがＴＵＳを失効するためにはＴＵＳを提示することが必要となり、ＴＵＳを紛失した場合にＴＵＳの失効処理を行えないという課題がある。このことは、ＴＵＳ失効リストの内容を充実させることでも回避可能であるが、ＴＵＳの発行を管理することにより対処できる。以下、認証サーバＩＤＰにおいてＴＵＳを発行し、発

行したＴＵＳを管理する場合について述べる。

【０１３１】

認証サーバＩＤＰにおいて、ＴＵＳ失効リストに加え、「ＴＵＳ発行リスト」をデータベースにより管理する。ＴＵＳ発行リストでは、前記実施形態で述べたように、ＴＵＳに埋め込んでいた発行ユーザの識別子、所属組織情報、ロール情報、有効期間（開始日時及び終了日時）、表示名などの情報を保持する。また、ＴＵＳの種別などを保持することも可能である。これにより、ＴＵＳにはＴＵＳ発行リストとリンクさせるための情報のみを埋め込めばよいことになり、ユーザ個人に関連付けられた各種情報を格納する必要はなくなる。

【０１３２】

先ず、ＴＵＳの発行処理は次のように行われる。すなわち、ＴＵＳ発行モジュールはＷｅｂ連携サーバＷＦＳ１～ＷＦＳｍではなく認証サーバＩＤＰに配置し、代わりにＷｅｂ連携サーバＷＦＳ１～ＷＦＳｍにはユーザ端末からのＴＵＳ発行要求を、認証サーバＩＤＰへ転送するための処理を行うＴＵＳ発行要求モジュールを配置する。認証サーバＩＤＰにおけるＴＵＳ発行モジュールの処理機能は、図４に示した構成と同じである。但し、このＴＵＳ発行処理は、認証サーバＩＤＰで実行されるため、ＴＵＳに付与される発行元プロバイダＩＤは認証サーバＩＤＰを示すものとなる。またＴＵＳの暗号化は、前記実施形態と同様に認証サーバＩＤＰの公開鍵を用いて行うが、署名は認証サーバＩＤＰの秘密鍵を用いて行う。

【０１３３】

次に、ＴＵＳ解決処理は以下のように行われる。図１９はその処理手順と処理内容を示す図である。

すなわち、ＴＵＳ解決モジュール３５は前記実施形態と同様に認証サーバＩＤＰに設けられる。ＴＵＳ解決モジュール３５は、認証サーバＩＤＰの秘密鍵でＴＵＳをステップＳ２１１で復号し、そのＴＵＳがＴＵＳ発行リストに存在するか否かをステップＳ２２２により確認する。そして、存在する場合にはＴＵＳ発行リストデータベース３９から付随するユーザ属性情報などを取得し、ステップＳ２２３により対象ユーザのユーザ識別子を生成する。なお、ＴＵＳの復号処理は認証サーバＩＤＰの秘密鍵で、また署名は認証サーバＩＤＰの公開鍵を用いて行う。

【０１３４】

このようにＴＵＳの発行管理機能を設けると、以下のような効果が奏せられる。すなわち、認証サーバＩＤＰにおいてＴＵＳに関する情報を保持するため、仮名や有効期間などの各種情報をＴＵＳに格納する必要がなくなる。このため、ＴＵＳの文字列を短くすることができる。また、図３に示したようなＴＵＳの種類に関する情報も認証サーバＩＤＰ側で保持することができ、ＴＵＳの文字列自体を変更しなくても実現可能となる。さらに、ユーザ識別子から発行済みのＴＵＳを検索することができる。このため、ＴＵＳを紛失した場合には当該ＴＵＳを失効させることが可能になる。

【０１３５】

また、前記実施形態ではＴＵＳをこのＴＵＳに埋め込まれた有効期間情報により指定された期間内に限り有効とするようにしたが、ログインからログアウトされるまでの期間内に限り有効とするように制御してもよい。また、ＴＵＳは認証サーバで発行するようにしてもよく、その他データプロバイドサーバ、Ｗｅｂ連携サーバ、認証サーバの構成や機能等についても、この発明の要旨を逸脱しない範囲で種々変形して実施可能である。

【０１３６】

さらに、前記実施形態ではＥＨＲシステムを例にとって説明したが、利用するユーザが不特定多数で、本人が許可したユーザ以外には個人情報を一切公開することが許されないシステムであって、なおかつＥＨＲと同様に蓄積された本人の情報を第三者が代理操作したり参照することが要件となるシステムであれば、同様にこの発明を適用可能である。この種のシステムとしては、例えば既存もしくは今後普及が予測される公共サービスである、住民基本台帳ネットワークや、住民登録、運転免許管理、自動車登録、介護保険申請、

年金照会、税納付状況照会、電子私書箱等のシステムがあげられる。

【０１３７】

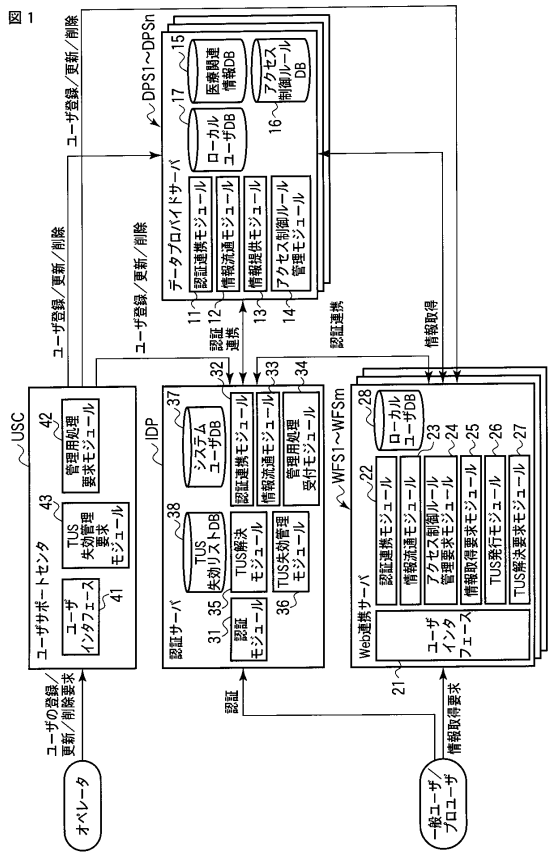
要するにこの発明は、上記各実施形態そのままに限定されるものではなく、実施段階ではその要旨を逸脱しない範囲で構成要素を変形して具体化できる。また、上記各実施形態に開示されている複数の構成要素の適宜な組み合せにより種々の発明を形成できる。例えば、実施形態に示される全構成要素から幾つかの構成要素を削除してもよい。さらに、異なる実施形態に亘る構成要素を適宜組み合せてもよい。

【符号の説明】

【０１３８】

ＤＰＳ１～ＤＰＳｎ…データプロバイドサーバ、ＷＦＳ１～ＷＦＳｍ…Ｗｅｂ連携サーバ、ＩＤＰ…認証サーバ、ＵＳＣ…ユーザサポートセンタ、１１，２２，３２…認証連携モジュール、１２，２３，３３…情報流通モジュール、１３…情報提供モジュール、１４…アクセス制御ルール管理モジュール、１５…医療関連情報データベース、１６…アクセス制御ルールデータベース、１７，２８…ローカルユーザデータベース、２１，４１…ユーザインタフェース、２４…アクセス制御ルール管理要求モジュール、２５…情報取得要求モジュール、２６…ＴＵＳ発行モジュール、２７…ＴＵＳ解決要求モジュール、３１…認証モジュール、３４…管理用処理受付モジュール、３５…ＴＵＳ解決モジュール、３６…ＴＵＳ失効管理モジュール、３７…システムユーザデータベース、３８…ＴＵＳ失効リストデータベース、４２…管理用処理要求モジュール、４３…ＴＵＳ失効管理要求モジュール。

【図１】



【図２】

図２

<TUSの構成要素>

項番	構成要素	説明
1	仮名	ログインユーザの識別子 (認証サーバとWeb連携サーバ間の仮名)
2	乱数	8桁のランダムな数値
3	所属組織情報（任意）	ログインユーザの所属組織情報
4	ロール情報（任意）	ログインユーザのロール情報
5	有効期限開始日時	YYYY/MM/DD hh:mm:ss 形式の文字列
6	有効期限終了日時	YYYY/MM/DD hh:mm:ss 形式の文字列
7	表示名	画面表示用の文字列

【図３】

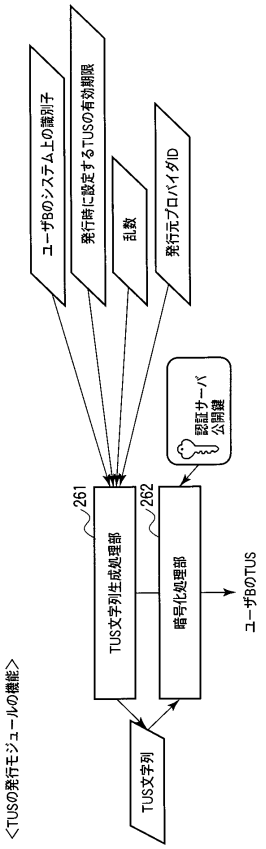
図３

<TUSの種類>

一時ユーザ指定子の種類	略称	含まれる情報	利用例
一時ユーザ指定子（ユーザ）	TUS（ユーザ）	・仮名	ユーザ関係登録やアクセス制御リスト登録時のユーザ指定
一時ユーザ指定子（組織）	TUS（組織）	・仮名 ・所属組織情報	ユーザ関係登録時のユーザ指定およびアクセス制御リスト登録時の組織指定
一時ユーザ指定子（ロール）	TUS（ロール）	・仮名 ・ロール情報	ユーザ関係登録時のユーザ指定およびアクセス制御リスト登録時のロール指定
一時ユーザ指定子（組織・ロール）	TUS（組織・ロール）	・仮名 ・所属組織情報 ・ロール情報	ユーザ関係登録時のユーザ指定およびアクセス制御リスト登録時の組織およびロール指定

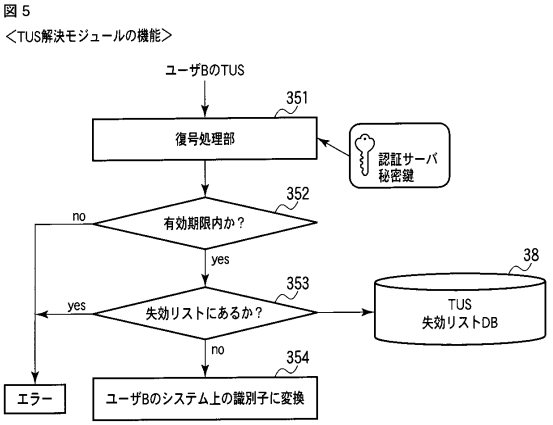
【図４】

図４



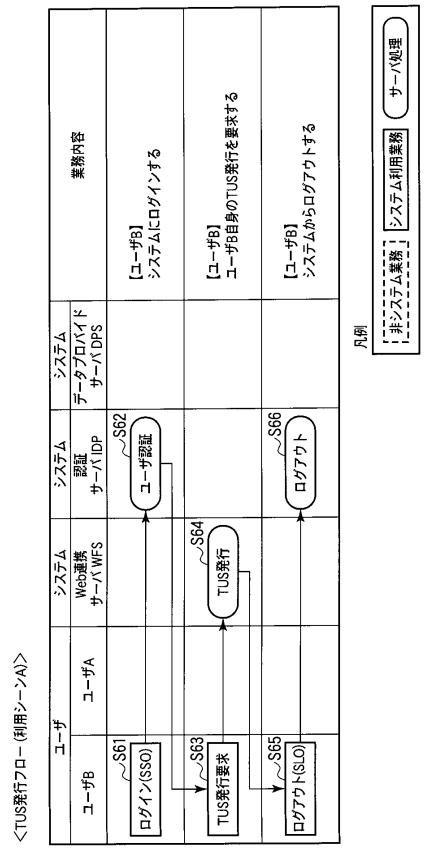
【図５】

図５



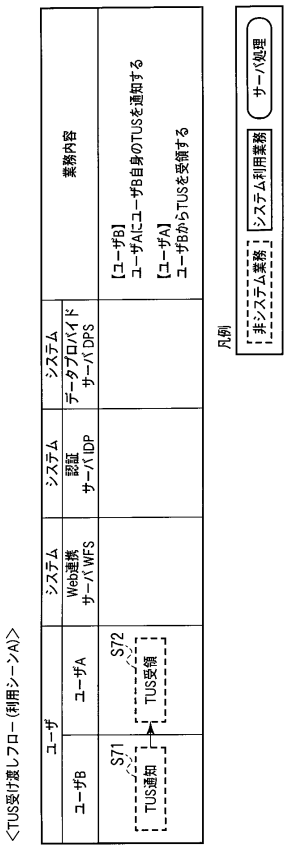
【図６】

図６



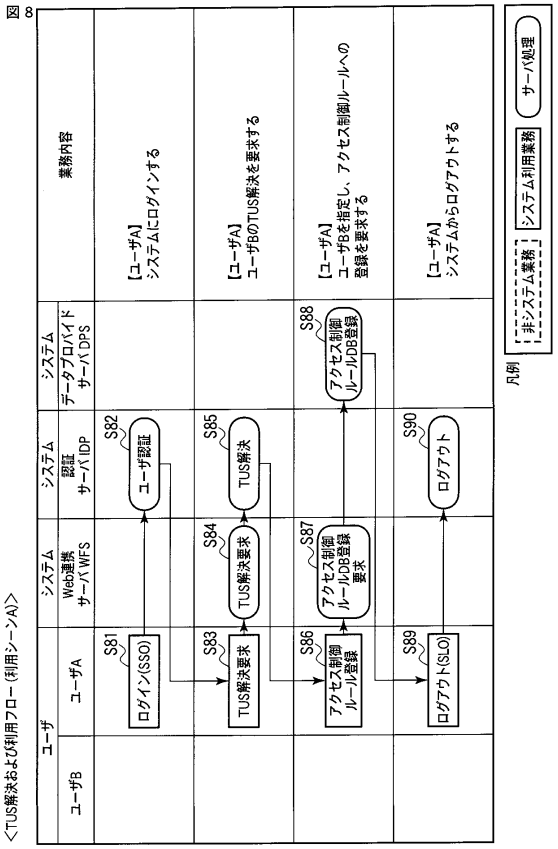
【図７】

図7



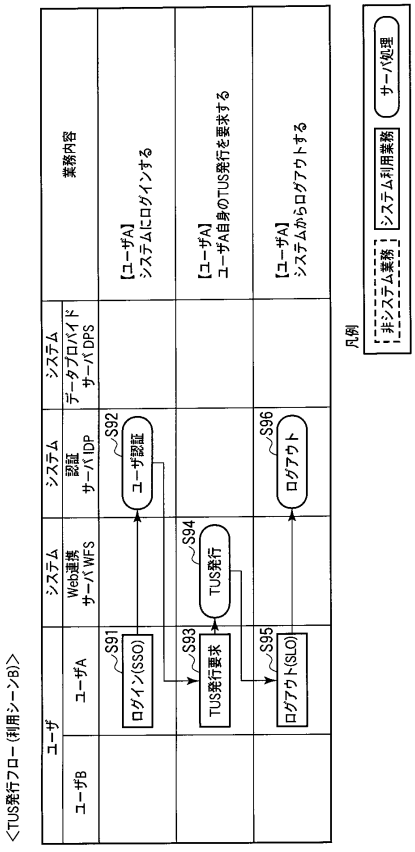
【図８】

図8



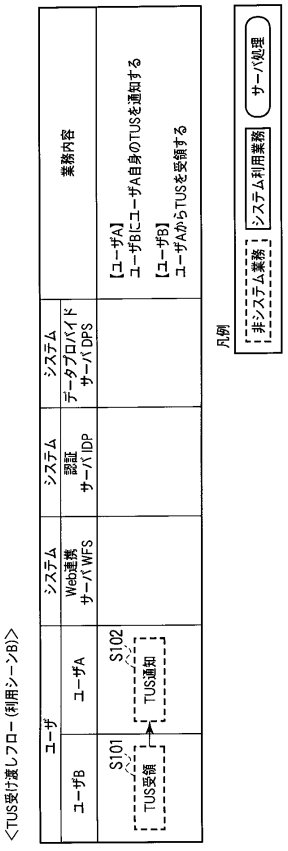
【図９】

図9

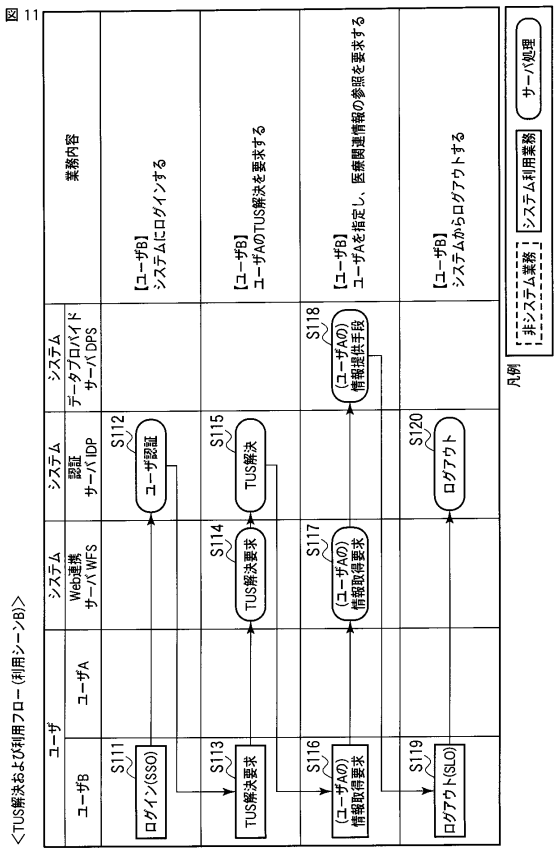


【図１０】

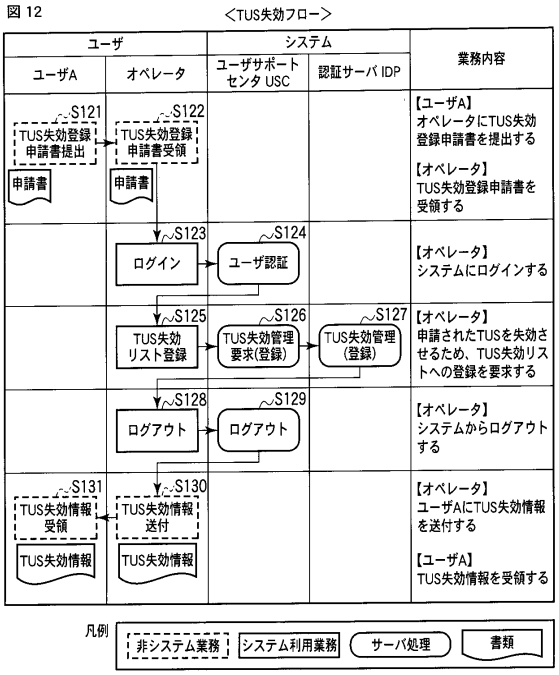
図10



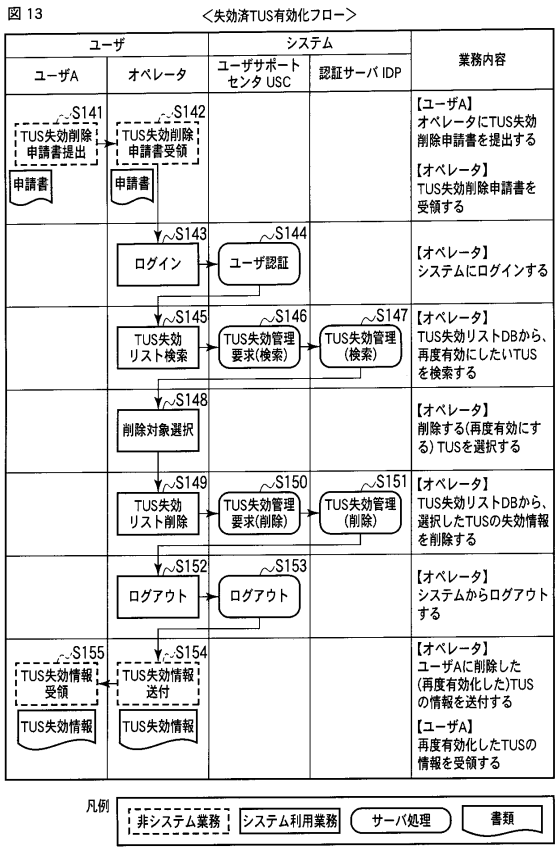
【図１１】



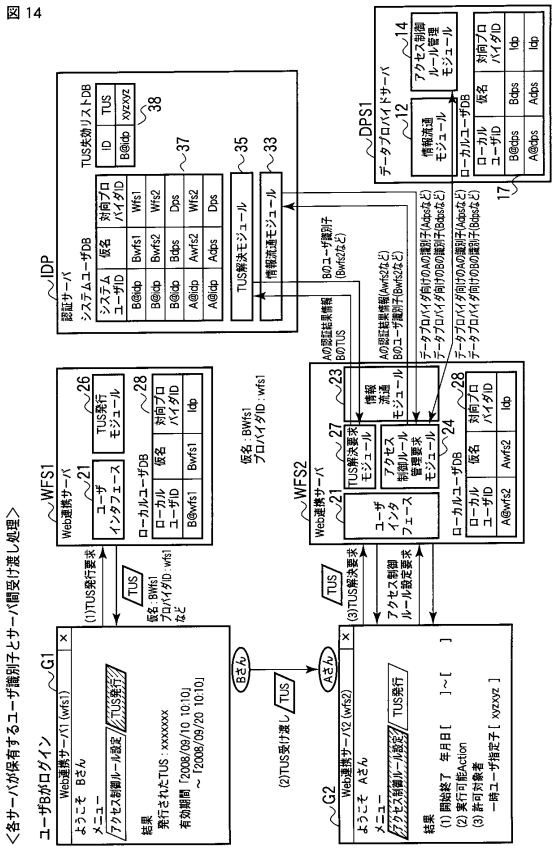
【図１２】



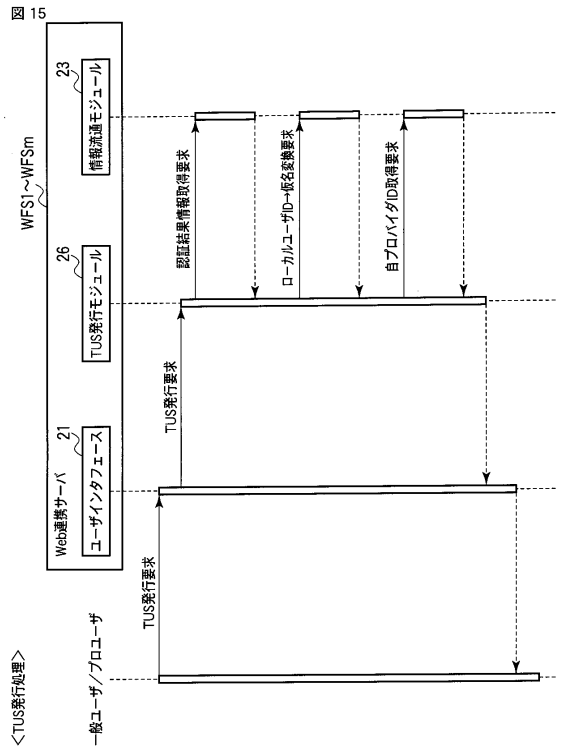
【図１３】



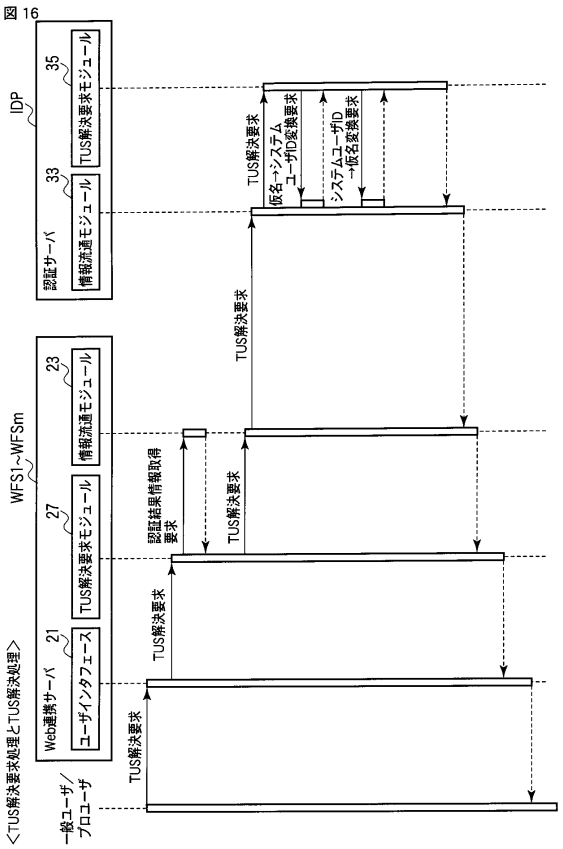
【図１４】



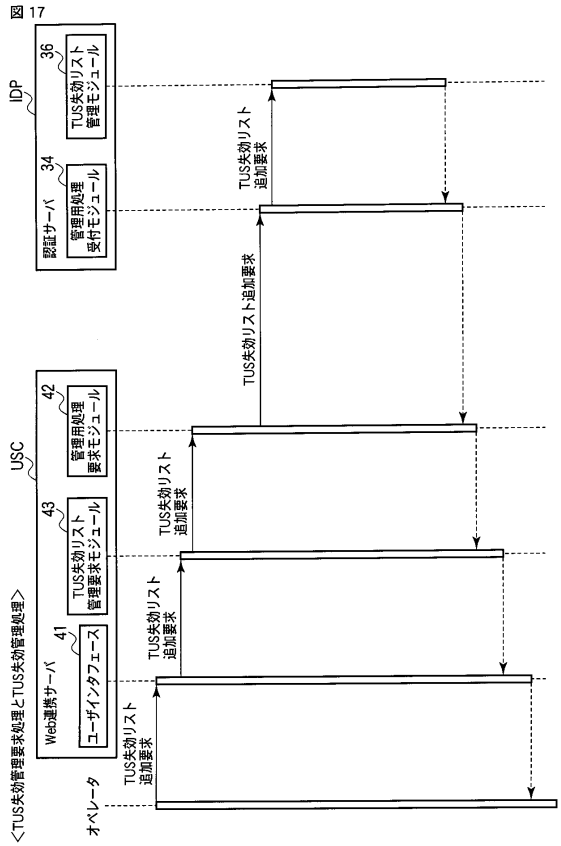
【図１５】



【図１６】



【図１７】



【図１８】

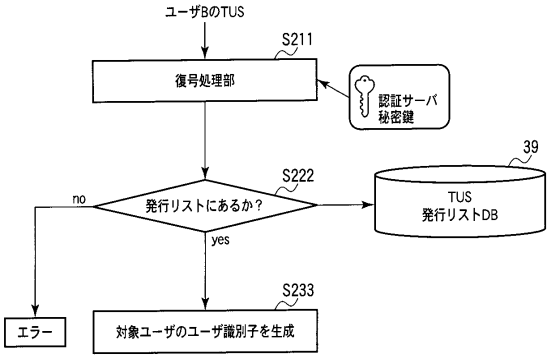
図 18

<TUS失効リストのレコードの構成要素>

項目	説明
userid	ユーザID
tus	TUS
expire_start_time	有効期限開始日時 TUSから取得
expire_end_time	有効期限終了日時 TUSから取得
create_time	作成日時 システムの現在日時を設定
update_time	更新日時 システムの現在日時を設定

【図１９】

図 19
<発行済TUSを管理する方式におけるTUS解決フロー>



フロントページの続き

(72)発明者　宮島　麻美
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(72)発明者　中村　亨
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(72)発明者　大野　浩
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(72)発明者　爰川　知宏
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(72)発明者　土川　仁
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(72)発明者　内藤　岳
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(72)発明者　前田　裕二
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内

審査官　▲吉▼田　耕一

(56)参考文献　特開２００２－２２９９５３（ＪＰ，Ａ）
特開２００５－０２５６７４（ＪＰ，Ａ）
特開２００２－３２４１９４（ＪＰ，Ａ）
特開２００７－２９９３０３（ＪＰ，Ａ）
特開２００４－２１３２６５（ＪＰ，Ａ）
特開２００３－０６６８３６（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／２０
Ｇ０６Ｑ　５０／２２
Ｈ０４Ｌ　９／３２