

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2010-86080

(P2010-86080A)

(43) 公開日 平成22年4月15日(2010.4.15)

(51) Int.Cl.	F I	テーマコード (参考)
G 0 6 F 21/24 (2006.01)	G 0 6 F 12/14 5 3 0 B	5 B 0 1 7
G 0 6 Q 50/00 (2006.01)	G 0 6 F 17/60 1 2 6 Z	5 B 2 8 5
G 0 6 F 21/00 (2006.01)	G 0 6 F 15/00 3 3 0 Z	
	G 0 6 F 12/14 5 6 0 Z	

審査請求 有 請求項の数 11 O L (全 20 頁)

(21) 出願番号	特願2008-251815 (P2008-251815)	(71) 出願人	000004226
(22) 出願日	平成20年9月29日 (2008. 9. 29)		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	100058479
			弁理士 鈴江 武彦
		(74) 代理人	100108855
			弁理士 蔵田 昌俊
		(74) 代理人	100091351
			弁理士 河野 哲
		(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

最終頁に続く

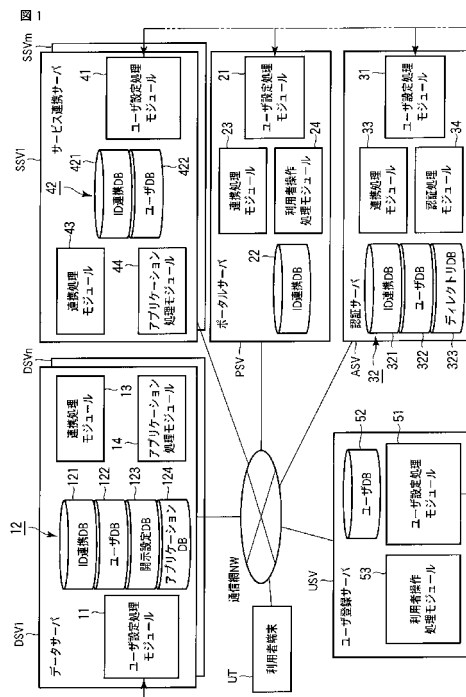
(54) 【発明の名称】 分散情報連携システム及び分散情報連携方法

(57) 【要約】

【課題】複数のデータサーバにより管理されている複数の個人データを必要なときにリアルタイムに収集でき、かつ大掛かりな設備と高度のセキュリティ管理が不要でスケーラビリティがあり、しかもユーザ情報間の連携情報の登録処理を効率良く行えるようにする。

【解決手段】ユーザ登録サーバUSVにおいて、利用端末UTからユーザ一括登録要求が送られた場合に、上記認証サーバASVと協働して他の各サーバが保有するユーザID間を連携するためのID連携情報を生成し、この生成されたID連携情報を上記データサーバDSV1～DSVn、及びサービス連携サーバSSV1～SSVnにそれぞれ送信して登録するようにしたものである。

【選択図】 図1



【特許請求の範囲】**【請求項 1】**

ユーザごとにその個人データを管理する複数のデータサーバと、サービス連携サーバと、認証サーバと、利用者端末とを通信ネットワークを介して接続可能とし、前記利用者端末からの情報取得要求に応じて、前記複数のデータサーバ、サービス連携サーバ及び認証サーバがそれぞれ管理するユーザ情報間を連携させるための連携情報と、前記認証サーバが管理する前記ユーザの認証情報とに基づいて、前記サービス連携サーバが前記複数のデータサーバから前記ユーザの個人データを収集し、この収集した個人データを前記通信ネットワークを介して前記要求元の利用者端末に配信する分散情報連携システムであって、

少なくとも前記複数のデータサーバ、サービス連携サーバ及び認証サーバに対し前記通信ネットワークを介して接続可能なユーザ登録サーバをさらに具備し、

このユーザ登録サーバは、前記利用者端末から発せられるユーザー一括登録要求に応じ、前記認証サーバと協働して連携情報を生成し、この連携情報を前記通信ネットワークを介して前記複数のデータサーバ、サービス連携サーバ及び認証サーバにそれぞれ送信し登録させる連携管理手段を、備えることを特徴とする分散情報連携システム。

【請求項 2】

前記連携管理手段は、

前記利用者端末からのユーザー一括登録要求に応じて、複数のデータサーバ、サービス連携サーバ及び認証サーバに対し、当該要求元のユーザに係わる連携情報が登録済みか否かを前記通信ネットワークを介して問い合わせる手段と、

前記問い合わせの結果、要求元のユーザに係わる連携情報が未登録と判定された場合に、前記認証サーバに対し連携情報の生成を要求して生成された連携情報を取得し、この取得した連携情報を前記通信ネットワークを介して前記未登録のデータサーバ、サービス連携サーバ及び認証サーバに送信して登録させる手段と

を備えることを特徴とする請求項 1 記載の分散情報連携システム。

【請求項 3】

前記連携管理手段は、前記問い合わせの結果、要求元のユーザに係わる連携情報が登録済と判定された場合に、前記利用者端末からのユーザー一括登録要求の内容が更新であれば、その更新内容を表す情報を含む更新要求を前記通信ネットワークを介して前記登録済のデータサーバ、サービス連携サーバ及び認証サーバに送信する手段を、さらに備えることを特徴とする請求項 2 記載の分散情報連携システム。

【請求項 4】

前記連携管理手段は、前記利用者端末からの一括登録要求の内容が削除であれば、削除要求を前記通信ネットワークを介して前記登録済のデータサーバ、サービス連携サーバ及び認証サーバに送信する手段を、さらに備えることを特徴とする請求項 2 記載の分散情報連携システム。

【請求項 5】

前記ユーザ登録サーバは、

前記利用者端末から送られる開示設定要求に応じて、この要求に含まれる個人データの開示の可否を指定するための開示設定情報を前記連携情報と共に前記通信ネットワークを介して該当するデータサーバに送信し設定させる手段を、さらに備えることを特徴とする請求項 1 記載の分散情報連携システム。

【請求項 6】

前記連携情報の登録及び開示設定情報の設定に使用する通信経路を、前記通信ネットワーク内の前記個人データの収集及び配信に使用する通信経路と異ならせることを特徴とする請求項 5 記載の分散情報連携システム。

【請求項 7】

ユーザごとにその個人データを管理する複数のデータサーバと、サービス連携サーバと、認証サーバと、利用者端末とを通信ネットワークを介して接続可能とし、前記利用者端末からの情報取得要求に応じて、前記複数のデータサーバ、サービス連携サーバ及び認証

10

20

30

40

50

サーバがそれぞれ管理するユーザ情報間を連携させるための連携情報と、前記認証サーバが管理する前記ユーザの認証情報とに基づいて、前記サービス連携サーバが前記複数のデータサーバから前記ユーザの個人データを収集し、この収集した個人データを前記通信ネットワークを介して前記要求元の利用者端末に配信する分散情報連携システムで使用される分散情報連携方法であって、

前記利用者端末からユーザ登録サーバにユーザ一括登録要求を送信する過程と、

前記送られたユーザ一括登録要求に応じて、前記ユーザ登録サーバが前記認証サーバと協働して連携情報を生成し、この生成された連携情報を前記通信ネットワークを介して前記複数のデータサーバ、サービス連携サーバ及び認証サーバにそれぞれ送信し登録させる過程と

10

を備えることを特徴とする分散情報連携方法。

【請求項 8】

前記連携情報を登録させる過程は、

前記利用者端末から送られたユーザ一括登録要求に応じて、前記ユーザ登録サーバが前記複数のデータサーバ、サービス連携サーバ及び認証サーバに対し、当該要求元のユーザに係わる連携情報が登録済みか否かを前記通信ネットワークを介して問い合わせる過程と、

前記問い合わせの結果、要求元のユーザに係わる連携情報が未登録と判定された場合に、前記ユーザ登録サーバが前記認証サーバに対し連携情報の生成を要求し、生成された連携情報を認証サーバから取得する過程と、

20

前記取得された連携情報を、前記ユーザ登録サーバが前記通信ネットワークを介して前記未登録のデータサーバ、サービス連携サーバ及び認証サーバへ送信して登録させる過程と

を備えることを特徴とする請求項 7 記載の分散情報連携方法。

【請求項 9】

前記連携情報を登録させる過程は、前記問い合わせの結果、要求元のユーザに係わる連携情報が登録済と判定された場合に、前記ユーザ登録サーバが前記利用者端末からのユーザ一括登録要求の内容が更新であれば、その更新内容を表す情報を含む更新要求を前記通信ネットワークを介して前記登録済のデータサーバ、サービス連携サーバ及び認証サーバに送信する過程を、さらに備えることを特徴とする請求項 8 記載の分散情報連携方法。

30

【請求項 10】

前記連携情報を登録させる過程は、前記利用者端末からの一括登録要求の内容が削除であれば、前記ユーザ登録サーバが削除要求を前記通信ネットワークを介して前記登録済のデータサーバ、サービス連携サーバ及び認証サーバに送信する手段を、さらに備えることを特徴とする請求項 8 記載の分散情報連携方法。

【請求項 11】

前記利用者端末から前記ユーザ登録サーバに開示設定要求を送信する過程と、

前記ユーザ登録サーバが、前記送られた開示設定要求に含まれる個人データの開示の可否を指定するための開示設定情報を、前記連携情報と共に前記通信ネットワークを介して該当するデータサーバに送信し設定させる過程と

40

を、さらに具備することを特徴とする請求項 7 記載の分散情報連携方法。

【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、運動関連施設等がそれぞれ保有する複数のデータベースにより管理されている医療等に関する個人データを、本人等の要求に応じて通信ネットワークを介して収集する分散情報連携システム及び分散情報連携方法に関する。

【背景技術】

【0002】

50

人は、罹病した場合や健康に不安を感じた場合、その症状等に応じて異なる医療機関を受診することがある。また、症状は同じでも居住地の移転や出張先等で罹病した場合にも、異なる医療機関を受診する。その結果、一人の患者の医療等に関する情報は複数の医療機関に分散して管理されることになる。

【 0 0 0 3 】

ところで、最近このように複数の医療機関で管理されている一人の患者の医療等に関する情報を通信ネットワークを介して収集して、遠隔地での診療や投薬等に役立てる、E H R (Electronic Health Recode) システムが提案されている。このシステムは、例えば複数の医療機関がそれぞれ保有するデータベースから、特定の患者に係わる様々な医療データを定期的に収集し、この収集した医療データを集中管理データベースに記憶して閲覧を可能にするものとなっている(例えば、特許文献1を参照。)

10

【 0 0 0 4 】

【特許文献1】特許第3903588号明細書

【発明の開示】

【発明が解決しようとする課題】

【 0 0 0 5 】

ところが、この従来提案されたシステムは、複数の機関で管理されている各医療データを、例えば月単位で夜間にバッチ処理により収集するものとなっている。このため、収集タイミングによっては医療データが古くなり、現時点の患者の状態に対応しないものになる場合がある。つまり、情報収集に対するリアルタイム性に難点がある。また、医療データは最高位の個人データであることから、集中管理データベースを保有する機関には厳格なセキュリティ管理が求められる。このため、機関の設備上及び管理上の負担が大きくなり、これがシステムの普及の妨げとなっている。さらに、集中管理データベースに負荷が集中することから、利用者数の増加や医療データを管理しているデータサーバ数の増加の要求に対応し難く、スケーラビリティに難点がある。

20

【 0 0 0 6 】

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、複数のデータサーバで管理されている複数の個人データを必要なときにリアルタイムに収集でき、かつ大掛かりな設備と高度のセキュリティ管理が不要でスケーラビリティがあり、しかもユーザ情報間の連携情報の登録処理を効率良く行うことが可能な分散情報連携システム及び分散情報連携方法を提供することにある。

30

【課題を解決するための手段】

【 0 0 0 7 】

上記目的を達成するためにこの発明の一観点は、ユーザごとにその個人データを管理する複数のデータサーバと、サービス連携サーバと、認証サーバと、利用者端末とを通信ネットワークを介して接続可能とし、上記利用者端末からの情報取得要求に応じて、上記複数のデータサーバ、サービス連携サーバ及び認証サーバがそれぞれ管理するユーザ情報間を連携させるための連携情報と、上記認証サーバが管理する上記ユーザの認証情報とに基づいて、上記サービス連携サーバが上記複数のデータサーバから上記ユーザの個人データを収集し、この収集した個人データを上記通信ネットワークを介して上記要求元の利用者端末に配信する分散情報連携システムであって、少なくとも上記複数のデータサーバ、サービス連携サーバ及び認証サーバに対し上記通信ネットワークを介して接続可能なユーザ登録サーバをさらに具備する。そして、ユーザ登録サーバに連携管理手段を設け、この連携管理手段により、上記利用者端末から送られるユーザ一括登録要求に応じ、上記認証サーバと協働して連携情報を生成し、この生成された連携情報を上記通信ネットワークを介して上記複数のデータサーバ、サービス連携サーバ及び認証サーバにそれぞれ送信し登録させるようにしたものである。

40

【 0 0 0 8 】

したがって、利用者端末から情報取得要求が送られると、登録されたユーザ情報間を連携させるための連携情報と、認証サーバが管理するユーザの認証情報とに基づいて、サー

50

ビス連携サーバにより各データサーバから上記ユーザの個人データが収集され、この収集された個人データが要求元の利用者端末に配信される。このため、ユーザはリアルタイムに自身に係わる個人データを取得することができる。また、要求に応じてその都度各データサーバから個人データが収集されるので、個人データを集中管理するためのデータベースが不要となる。このため、分散情報の連携配信サービスを提供しようとする際の設備上及び管理上の負担が軽減され、さらに利用者数の増加や医療データを管理しているデータサーバ数の増加要求にも対応し易くなり、これによりスケーラビリティのあるシステムを提供可能となる。

【 0 0 0 9 】

しかし、サービス連携サーバが複数のデータベースから個人データを収集するに当たっては、それぞれのデータベースにおいて個人データにアクセスするためのユーザID等のユーザ情報が必要となる。しかしながら、各データベースで使用される当該データベースに直接アクセスが可能なユーザID等のユーザ情報をサービス連携サーバが管理すると、不正アクセスを受けた場合などにデータが流出する範囲が広がってしまう可能性が高く、情報セキュリティ上問題である。

そこで、各データベースで使用されているユーザID等のユーザ情報を、そのデータベース外で管理するのではなく、連携用のユーザID、つまりID連携情報を用いて個人データを収集する方法が考えられている（例えば特開2007-299303号公報を参照）。しかし、このようなID連携処理を行うためには、各サーバに連携情報を事前に設定しておく必要がある。しかしながら、連携情報は各サーバにおいて個別に設定するしかなく、設定に手間が掛かると共に設定間違いを起こし易かった。

【 0 0 1 0 】

この発明は以上の点に着目してなされたもので、ユーザ登録サーバにより、すべてのサーバに対しユーザの管理情報間を連携させるための連携情報が一括して登録される。このため、きわめて効率良く連携情報の登録を行うことができ、かつ不慣れなユーザやオペレータであっても誤ることなく登録を行うことができる。

【 0 0 1 1 】

この発明は、以下のような各種具体的な実施態様を備えることも特徴とする。

第1の実施態様は、連携情報を登録させる際に、上記利用者端末から送られたユーザ一括登録要求に応じて、上記ユーザ登録サーバが上記複数のデータサーバ、サービス連携サーバ及び認証サーバに対し、当該要求元のユーザに係わる連携情報が登録済みか否かを上記通信ネットワークを介して問い合わせる。そして、この問い合わせの結果、要求元のユーザに係わる連携情報が未登録と判定された場合に、上記ユーザ登録サーバが上記認証サーバに対し連携情報の生成を要求して、生成された連携情報を認証サーバから取得し、この取得された連携情報を上記ユーザ登録サーバが上記通信ネットワークを介して上記未登録のデータサーバ、サービス連携サーバ及び認証サーバへ送信して登録させるものである。

このようにすると、要求元のユーザに係わる連携情報が未登録の場合にのみ、連携情報を新規登録手順を実行することができる。

【 0 0 1 2 】

第2の実施態様は、連携情報を登録させる際に、上記問い合わせの結果要求元のユーザに係わる連携情報が登録済と判定された場合に、上記ユーザ登録サーバが上記利用者端末からのユーザ一括登録要求の内容が更新であれば、その更新内容を表す情報を含む更新要求を上記通信ネットワークを介して上記登録済のデータサーバ、サービス連携サーバ及び認証サーバに送信するものである。

このようにすると、登録済みのユーザ情報に対し連携情報の更新処理を実行することができる。

【 0 0 1 3 】

第3の実施態様は、連携情報を登録させる際に、利用者端末からの一括登録要求の内容が削除であれば、上記ユーザ登録サーバが削除要求を上記通信ネットワークを介して上記

10

20

30

40

50

登録済のデータサーバ、サービス連携サーバ及び認証サーバに送信するものである。

このようにすると、登録済みの連携情報を削除することが可能となる。

【 0 0 1 4 】

第 4 の実施態様は、利用者端末からユーザ登録サーバに通信ネットワークを介して開示設定要求を送信し、ユーザ登録サーバが、上記送られた開示設定要求に含まれる個人データの開示の可否を指定するための開示設定情報を、上記連携情報と共に上記通信ネットワークを介して該当するデータサーバに送信し設定させる処理をさらに行うようにしたものである。

このようにすると、連携情報の一括登録処理と同時にデータサーバに対し個人データに対する開示設定処理を行うことが可能となり、これにより連携情報の登録処理と開示設定処理を効率良く行うことができる。

10

【 0 0 1 5 】

第 5 の実施態様は、連携情報の登録及び開示設定情報の設定に使用する通信経路を、通信ネットワーク内の上記個人データの収集及び配信に使用する通信経路と異ならせるようにしたものである。

このようにすると、連携情報の登録及び開示設定情報の設定のためのデータ転送を、個人データの収集及び配信のためのデータ転送と独立して行うことが可能となる。これにより、個人データの収集及び配信に使用する経路の通信トラフィックの影響を受けることなく安定に、しかも高いセキュリティ管理のもとで信頼性の高い登録又は設定処理を行い得る。

20

【 発明の効果 】

【 0 0 1 6 】

すなわち、この発明によれば、複数のデータサーバにより管理されている複数の情報を必要なときにリアルタイムに収集でき、かつ大掛かりな設備と高度のセキュリティ管理が不要でスケーラビリティがあり、しかもユーザ情報間の連携情報の登録処理を効率良く行うことが可能な分散情報連携システム及び分散情報連携方法を提供することができる。

【 発明を実施するための最良の形態 】

【 0 0 1 7 】

以下、図面を参照してこの発明に係わる一実施形態を説明する。

図 1 は、この発明の一実施形態に係わる分散情報連携システムの全体構成を示すブロック図である。この実施形態の分散情報連携システムは、医療機関や保健関連機関、運動関連施設等が運用する複数のデータサーバ $DSV1 \sim DSVn$ と、複数 (m 台) のサービス連携サーバ $SSV1 \sim SSVm$ と、ポータルサーバ PSV と、認証サーバ ASV と、ユーザ登録サーバ USV を備え、これらのサーバ $DS1 \sim DSn$, $SSV1 \sim SSVm$, PSV , ASV , USV 相互間、及びこれらのサーバと利用者端末 UT との間で、通信ネットワーク NW を介して通信可能としたものである。なお、 n はデータサーバの数であり自然数 (正の整数) 、 m はサーバ連携サーバの数であり自然数 (正の整数) である。

30

【 0 0 1 8 】

利用者端末 UT 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、薬剤師等が患者の依頼を受けて患者の医療データ等を取得するために使用する業務用の端末と、ユーザ登録サーバ USV に設けられるオペレータ用のコンソール端末 (図示せず) が含まれる。

40

【 0 0 1 9 】

通信ネットワーク NW は、例えばインターネットに代表される IP (Internet Protocol) 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。

【 0 0 2 0 】

データサーバ $DSV1 \sim DSVn$ は、中央制御ユニット (Central Control Unit ; CCU) に、バスを介してプログラムメモリ、データメモリ及び通信インタフェースを接続し

50

たもので、その機能モジュールとしてユーザ設定処理モジュール 1 1 と、データベース群 1 2 と、連携処理モジュール 1 3 と、アプリケーション処理モジュール 1 4 とを備えている。

【0021】

図 2 は、これらの機能モジュールの具体的な構成を示すブロック図である。データベース群 1 2 は、ID 連携データベース (ID 連携 DB) 1 2 1 と、ユーザデータベース (ユーザ DB) 1 2 2 と、開示設定データベース (開示設定 DB) 1 2 3 と、アプリケーションデータベース (アプリケーション DB) 1 2 4 とを備える。ユーザ DB 1 2 2 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、ユーザ ID、ユーザ基本情報及びユーザ属性等からなる。アプリケーション DB 1 2 4 には、各ユーザの保健指導情報及び健康診断情報が上記ユーザ ID に対応付けられて格納される。ID 連携 DB 1 2 1 には、ユーザ登録サーバ U S V から登録を要求された ID 連携情報が記憶される。このとき ID 連携情報とは、他サーバから自サーバのあるユーザの個人データにアクセスするための情報である。開示設定 DB 1 2 3 には、アプリケーション DB 1 2 4 に格納されているユーザの個人データ、つまり保健指導情報や健康診断情報について、当該情報を誰に対し開示するかを設定するための開示設定情報が記憶される。

10

【0022】

ユーザ設定処理モジュール 1 1 は、ユーザ登録サーバ U S V からの要求に応じて、自らの ID 連携 DB 1 2 1 及びユーザ DB 1 2 2 の検索、ID 連携 DB 1 2 1 への ID 連携情報の登録又は削除、ユーザ DB 1 2 2 へのユーザ情報の登録又は削除を行い、その結果をユーザ登録サーバ U S V に応答するもので、連携基盤配布部 1 1 1 と、個別カスタム部 1 1 2 を備える。

20

【0023】

例えば、検索要求の場合連携基盤配布部 1 1 1 は、ID 連携 DB 1 2 1 を検索すると共に、必要に応じて個別カスタム部 1 1 2 を介してユーザ DB 1 2 2 を検索し、その各検索結果をユーザ登録サーバ U S V に応答する。個別カスタム部 1 1 2 は、連携基盤配布部 1 1 1 からの要求に応じてユーザ DB 1 2 2 を検索し、その検索結果を連携基盤配布部 1 1 1 に応答する。また、登録要求の場合には、連携基盤配布部 1 1 1 は登録を要求された ID 連携情報を ID 連携 DB 1 2 1 に記憶させ、かつユーザ情報を個別カスタム部 1 1 2 を介してユーザ DB 1 2 2 に記憶させる。削除要求の場合には、ID 連携 DB 1 2 1 及びユーザ DB 1 2 2 に記憶された削除対象の ID 連携情報及びユーザ情報を削除する。

30

【0024】

連携処理モジュール 1 3 は、認証サーバ A S V から認証情報を取得し、ID 連携 DB 1 2 1 を用いて他のデータサーバ D S V、サービス連携サーバ S S V 1 ~ S S V m 又はポータルサーバ P S V との間で属性交換 (個人データの流通) を行うもので、S A M L (Security Assertion Markup Language) における S P 等の機能を有する認証連携部 1 3 1 と、ID - W S F (Identity Web Service Framework) における W S C (Web Service Consumer) 等の機能を有する属性交換部 1 3 2 とを備える。なお、ID - W S F (Identity Web Service Framework) 及び S A M L (Secure Assertion Markup Language) は、Liberty Alliance が定めている Web Service のための仕様である。

40

【0025】

アプリケーション処理モジュール 1 4 は、ユーザ DB 1 2 2、開示設定 DB 1 2 3 及びアプリケーション DB 1 2 4 を用いて、開示設定要求に基づく開示設定処理と、サービス連携サーバ S S V 1 ~ S S V m に対するデータ提供処理及び開示制御を行うもので、E H R 用 P F 接続部 1 4 5 と、データ提供部 1 4 4 と、開示設定部 1 4 2 と、開示制御部 1 4 3 とを備えている。

【0026】

E H R 用 P F 接続部 1 4 5 は、アプリケーション 1 4 1 から上記認証連携部 1 3 1 もしくは属性交換部 1 3 2 を利用することを容易にする。データ提供部 1 4 4 は、認証連携部 1 3 1 及び属性交換部 1 3 2 を通じてサービス連携サーバ S S V 1 ~ S S V m からの要求

50

を受理し、この要求に該当するデータをアプリケーションDB124から検索して、この検索データを属性交換部132を通じてサービス連携サーバSSV1～SSVmに返送する。開示設定部142は、ユーザ登録サーバUSVもしくはサービス連携サーバSSV1～SSVmからの要求に応じて、開示設定DB123への開示設定情報の追加、更新又は削除を行う。開示制御部143は、サービス連携サーバSSV1～SSVmからデータ収集要求を受信したときに、個人データをサービス連携サーバSSV1～SSVmへ送信するか否かを、開示設定DB123に記憶された開示設定情報に基づいて制御する。

【0027】

また、アプリケーション処理モジュール14は、アプリケーションDB124に格納された個人データ、つまり保健指導情報及び健康診断情報に基づいて、特定保健指導等を行うためのアプリケーション141を備える。このアプリケーション141は、EHR用PF接続部145に従って、データサーバ内の上記各機能モジュールを利用することができ、それ以外の部分は自由に作成できる。

【0028】

ポータルサーバPSVも、CPUにバスを介してプログラムメモリ、データメモリ及び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、ユーザ設定処理モジュール21と、ID連携データベース(ID連携DB)22と、連携処理モジュール23と、利用者操作モジュール24を備えている。

【0029】

図3は、上記ポータルサーバPSVの各機能モジュールの具体的な構成を示すブロック図である。ID連携DB22には、ユーザ登録サーバUSVから登録を要求されたID連携情報が記憶される。ユーザ設定処理モジュール21は連携基盤配布部を有する。この連携基盤配布部は、ユーザ登録サーバUSVからの要求が検索要求の場合は、自らのID連携DB22を検索してその検索結果をユーザ登録サーバUSVに対し応答する。また連携基盤配布部は、ユーザ登録サーバUSVからの要求が登録要求の場合には、登録を要求されたID連携情報をID連携DB22に記憶させる。これに対しユーザ登録サーバUSVからの要求が削除要求の場合には、ID連携DB22に記憶された削除対象のID連携情報を削除する。

【0030】

連携処理モジュール23は、認証サーバASVから認証情報を取得し、ID連携DB22を用いてデータサーバDSV1～DSVn、サービス連携サーバSSV1～SSVm又は他のポータルサーバとの間で属性交換を行うもので、認証連携部を有する。この認証連携部は、利用者操作画面を通じて利用者のログイン要求を受けた際に、認証サーバASVの認証部に認証を要求する。利用者操作モジュール24は複数の利用者操作部241～24Nを有する。これらの操作部はそれぞれ利用者端末UTにおけるユーザの操作を処理する。なお、Nは利用者操作部の数で、自然数(正の整数)である。

【0031】

認証サーバASVも、CPUに対しバスを介してプログラムメモリ、データメモリ及び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、ユーザ設定処理モジュール31と、データベース群32と、連携処理モジュール33と、認証処理モジュール34とを備えている。

【0032】

図4は、この認証サーバASVの機能モジュールの具体的な構成を示すブロック図である。データベース群32には、ID連携データベース(ID連携DB)321と、ユーザデータベース(ユーザDB)322と、ディレクトリデータベース(ディレクトリDB)323が設けられている。ユーザDB322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。ID連携DB321には、ユーザ登録サーバUSVから登録を要求されたID連携情報が記憶される。このID連携情報は、それぞれのユーザに対してサーバごとに設定される。ディレクトリDB323には、個人データの所在を表すディレクトリデータが記憶される。

10

20

30

40

50

【 0 0 3 3 】

ユーザ設定処理モジュール 3 1 は、ユーザ登録サーバ U S V からの要求に応じて、自らの I D 連携 D B 3 2 1 及びユーザ D B 3 2 2 の検索、 I D 連携 D B 3 2 1 への I D 連携情報の登録又は削除、ユーザ D B 3 2 2 へのユーザ情報の登録又は削除を行い、その検索結果をユーザ登録サーバ U S V に対し応答するもので、連携基盤配布部 3 1 1 及び個別カスタム部 3 1 2 を有する。

【 0 0 3 4 】

例えば、検索要求の場合、連携基盤配布部 3 1 1 は I D 連携 D B 3 2 1 を検索すると共に、必要に応じて個別カスタム部 3 1 2 を介してユーザ情報を検索し、これらの検索結果をユーザ登録サーバ U S V に応答する。個別カスタム部 3 1 2 は、連携基盤配布部 3 1 1 からの検索要求に応じてユーザ D B 3 2 2 を検索し、その検索結果を連携基盤配布部 3 1 1 に返す。また、登録要求の場合には、連携基盤配布部 3 1 1 は登録を要求された I D 連携情報を I D 連携 D B 3 2 1 に記憶させ、かつユーザ情報を個別カスタム部 3 1 2 を介してユーザ D B 3 2 2 に記憶させる。削除要求の場合には、 I D 連携 D B 3 2 1 及びユーザ D B 3 2 2 に記憶された削除対象の I D 連携情報及びユーザ情報を削除する。

【 0 0 3 5 】

連携処理モジュール 3 3 は、ユーザ D B 3 2 2、 I D 連携 D B 3 2 1 及びディレクトリ D B 3 2 3 を用いてデータサーバ D S V 1 ~ D S V n、サービス連携サーバ S S V 1 ~ S S V m 及びポータルサーバ P S V に対し、認証情報の提供及びディレクトリサービスの提供を行うもので、属性交換部 3 3 1 及び認証連携部 3 3 2 を有している。属性交換部 3 3 1 は、例えば I D - W S F における S P (Service Provider) の機能を有するもので、ディレクトリ D B 3 2 3 を利用してディレクトリサービスを提供する。認証連携部 3 3 2 は、 S A M L における I D P (Identity Provider) 等の機能を有する。

【 0 0 3 6 】

認証処理モジュール 3 4 はユーザに対する認証処理を行うもので、認証部を有する。認証部は、利用者端末 U T においてユーザが入力したユーザ情報をもとに、ユーザ D B 3 2 2 を参照して当該ユーザの正当性を認証する。認証方式としては、 I D / パスワード認証、公開鍵暗号基盤 (P K I ; Public Key Infrastructure) 認証、又は多要素認証等が用いられる。

【 0 0 3 7 】

サービス連携サーバ S S V 1 ~ S S V m も、 C P U にバスを介してプログラムメモリ、データメモリ及び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、ユーザ設定処理モジュール 4 1 と、データベース群 4 2 と、連携処理モジュール 4 3 と、アプリケーション処理モジュール 4 4 を備えている。

【 0 0 3 8 】

図 5 は、このサービス連携サーバ S S V 1 ~ S S V m の機能モジュールの具体的構成を示すブロック図である。データベース群 4 2 には、 I D 連携データベース (I D 連携 D B) 4 2 1 と、ユーザデータベース (ユーザ D B) 4 2 2 とが設けられている。 I D 連携 D B 4 2 1 には、ユーザ登録サーバ U S V から登録を要求された I D 連携情報が記憶される。ユーザ D B 4 2 2 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。

【 0 0 3 9 】

ユーザ設定処理モジュール 4 1 は、ユーザ登録サーバ U S V からの検索要求に応じて、自らの I D 連携 D B 4 2 1 及びユーザ D B 4 2 2 の検索、 I D 連携 D B 4 2 1 への I D 連携情報の登録又は削除、ユーザ D B 4 2 2 へのユーザ情報の登録又は削除を行い、その検索結果をユーザ登録サーバ U S V に対し応答するもので、連携基盤配布部 4 1 1 と、個別カスタム部 4 1 2 を備える。

【 0 0 4 0 】

例えば、検索要求の場合連携基盤配布部 4 1 1 は、 I D 連携 D B 4 2 1 を検索すると共に、必要に応じて個別カスタム部 4 1 2 を介してユーザ D B 4 2 2 を検索し、その各検索結果をユーザ登録サーバ U S V に応答する。個別カスタム部 4 1 2 は、連携基盤配布部 4

10

20

30

40

50

1 1からの検索要求に応じてユーザDB 4 2 2を検索し、その検索結果を連携基盤配布部 4 1 1に回答する。また、登録要求の場合には、連携基盤配布部 4 1 1は登録を要求されたID連携情報をID連携DB 4 2 1に記憶させ、かつユーザ情報を個別カスタム部 4 1 2を介してユーザDB 4 2 2に記憶させる。削除要求の場合には、ID連携DB 4 2 1及びユーザDB 4 2 2に記憶された削除対象のID連携情報及びユーザ情報を削除する。

【0041】

連携処理モジュール43は、認証サーバから認証情報を取得し、ID連携DB 4 2 1を用いて、データサーバDSV 1～DSV n、他のサービス連携サーバSSV又はポータルサーバPSVとの間で属性交換を行うもので、認証連携部431及び属性交換432を有している。認証連携部431は、SAMLにおけるSP等の機能を有する。属性交換432は、ID-WSFにおけるWSC等の機能を有する。

10

【0042】

アプリケーション処理モジュール44は、ユーザDB 4 2 2を用いてデータサーバDSV 1～DSV nに対して個人データの開示設定及び個人データの収集を要求するもので、EHR用プラットフォーム接続部(EHR用PF接続部)444と、データ収集部443と、開示設定要求部442とを備えている。EHR用PF接続部444は、アプリケーション441から認証連携部431もしくは属性交換部432を利用することを容易にする。データ収集部443は、ユーザの指定に応じてデータサーバDSV 1～DSV nから収集する個人データの抽出条件を設定し、認証連携部431及び属性交換部432を通じてデータサーバDSV 1～DSV nにデータの収集要求を送信する。開示設定要求部442は、ユーザからの開示設定要求に応じて、データサーバDSV 1～DSV nに対し開示設定DBへの開示設定情報の追加、更新又は削除を要求する。

20

【0043】

また、アプリケーション処理モジュール44は、個人に関する様々な医療・健康情報の一覧参照サービス等を行うためのアプリケーション441を備える。このアプリケーション441は、EHR用PF接続部444に従って、サービス連携サーバ内の上記各機能モジュールを利用することができ、それ以外の部分は自由に作成できる。

【0044】

ユーザ登録サーバUSVも、CPUにバスを介してプログラムメモリ、データメモリ及び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、ユーザ設定処理モジュール51と、各ユーザのユーザ情報を記憶するためのユーザデータベース(ユーザDB)52と、利用者操作処理モジュール53とを備えている。

30

【0045】

図6は、このユーザ登録サーバUSVが備える機能モジュールの具体的な構成を示すブロック図である。ユーザ設定処理モジュール51は、ユーザ管理部511と、ID連携管理部512と、サービス関連付け管理部513と、匿名ID管理部514と、ユーザ検索部515とを有する。

【0046】

ユーザ管理部511は、ユーザ(オペレータ)からの操作に応じて自らのユーザDB 52を更新すると共に、認証サーバASV、データサーバDSV 1～DSV n及びサービス連携サーバSSV 1～SSV mに対してユーザ登録、更新又は削除を要求する。

40

ID連携管理部512は、ユーザ(オペレータ)の操作に応じて、自らがユーザDB 52により管理するユーザIDと、認証サーバASV、データサーバDSV 1～DSV n及びサービス連携サーバSSV 1～SSV mがそれぞれ管理するユーザIDとの間の関連付けとその解除処理を行う。

【0047】

サービス関連付け管理部513は、ユーザ(オペレータ)の操作に応じて、データサーバDSV 1～DSV nを利用可能/不可能にするために、認証サーバASVに対してサービス関連情報の登録/解除を要求する。

匿名ID管理部514は、ユーザ(オペレータ)の操作に応じて、認証サーバASV、

50

データサーバDSV1～DSVn及びサービス連携サーバSSV1～SSVmに対し、匿名ID(SAML等)をユーザIDに、もしくはユーザIDから匿名ID(SAML等)に変換するよう要求する。

【0048】

ユーザ検索部515は、ユーザ(オペレータ)の操作に応じて自らが管理するユーザDB52を検索すると共に、認証サーバASV、データサーバDSV1～DSVn及びサービス連携サーバSSV1～SSVmに対し、指定された条件でユーザ検索を要求する。

利用者操作処理モジュール53はユーザによる操作を処理するもので、業務フローに応じて上記各機能部を効率的に呼び出す。

【0049】

次に、以上のように構成されたシステムによる分散情報収集動作を説明する。

(1) ユーザ情報及びその連携情報の一括登録処理

ここでは、例えば自治体の医療情報センタの職員(オペレータ)がユーザ登録サーバUSVに設けられたコンソール端末を操作して、指定した1つ以上の認証サーバASV、データサーバDSV1～DSVn、サービス連携サーバSSV1～SSVm又はポータルサーバPSVに対しユーザ情報の登録処理を行う場合を例にとって説明する。

【0050】

図8乃至図10は、このユーザ情報及びその連携情報の一括登録処理の手順を示すシーケンス図である。

(A) 先ず、コンソール端末において、オペレータがユーザ登録サーバUSVの所定のURL(Uniform Resource Locator)に対しアクセスすると、ユーザ登録サーバUSVからコンソール端末に対しユーザ一括登録画面がダウンロードされて表示される。図7に、表示されるユーザ一括登録画面の一例を示す。

この状態で、オペレータは、ユーザ登録を行いたいデータサーバDSV1～DSVn、サービス連携サーバSSV1～SSVm等を順に選択指定し、検索したいユーザ情報(ユーザID、ユーザ基本情報、ユーザ属性等)を入力する。なお、このユーザ情報の入力に際しては、ユーザ検索画面を利用することが可能である。

【0051】

(B) オペレータが入力したユーザ情報を用いて、ユーザ登録サーバUSVはユーザ検索部515により、図8に示すように各データサーバDSV1～DSVnに対して、該当するユーザ情報が既に登録されている否かの検索要求を行う。

(C) この検索の結果、データサーバDSV1～DSVn、サービス連携サーバSSV1～SSVmの検索結果一覧の中に、登録したいユーザのユーザ情報が既に存在した場合には、当該ユーザを選択する。これに対し存在しなかった場合には、オペレータは登録したいユーザのユーザ情報を手操作で入力する。

【0052】

(D) オペレータは、登録対象のすべてのデータサーバDSV1～DSVnに対し、上記(A)～(C)の処理を繰り返し行い、全ての操作が終了した後に一括登録を要求する。この一括登録の要求は、図9に示すようにコンソール端末からユーザ登録サーバUSVに送られる。

【0053】

(E) コンソール端末から上記一括登録要求が送られると、ユーザ登録サーバUSVはユーザ管理部511により、認証サーバASVに対して図9に示すようにユーザ登録を要求する。この要求に対し認証サーバASVは、連携基盤配布部311及び個別カスタム部312により、ID連携情報及びユーザ情報を検索し、自らが保持しているユーザIDをユーザ登録サーバUSVに返送する。

【0054】

(F) ユーザ登録サーバUSVは、上記認証サーバASVから返送されたユーザIDを使用して、ID連携管理部512により認証サーバASVに対してID連携情報の登録を要求する。この要求に対し認証サーバASVは、匿名IDを発行してユーザ登録サーバUS

10

20

30

40

50

Vに返送する。

【0055】

(G) ユーザ登録サーバUSVは、次にユーザ管理部511により、図9に示すようにサービス連携サーバSSV1～SSVmの1つに対してユーザ登録を要求する。この要求に対しサービス連携サーバSSV1～SSVmは、連携基盤配布部411及び個別カスタム部412により、ID連携情報及びユーザ情報を検索し、自らが保持しているユーザIDをユーザ登録サーバUSVに返送する。

【0056】

(H) ユーザ登録サーバUSVは、ID連携管理部512により、上記サービス連携サーバSSV1～SSVmから返送されたユーザIDと、上記(1-6)において認証サーバASVから取得した匿名IDを使用して、サービス連携サーバSSV1～SSVmに対してID連携情報の登録を要求する。この要求に対しサービス連携サーバSSV1～SSVmは、ID連携情報をID連携DB421に格納する。

10

(I) ユーザ登録サーバUSVは、上記(G)及び(H)の処理をサービス連携サーバSSV1～SSVmの数分だけ繰り返す。

【0057】

(J) ユーザ登録サーバUSVは、次にユーザ管理部511により、登録対象のユーザ情報がデータサーバDSV1～DSVnに未登録の場合、図10に示すようにデータサーバDSV1～DSVnの1つに対してユーザ登録を要求する。この要求に対しデータサーバDSV1～DSVnは、連携基盤配布部111及び個別カスタム部112により、ID連携情報及びユーザ情報を検索し、自らが保持しているユーザIDをユーザ登録サーバUSVに返送する。

20

【0058】

(K) またユーザ登録サーバUSVは、上記(E)により認証サーバASVから返送されたユーザIDを使用して、ID連携管理部512により認証サーバASVに対してID連携情報の登録を要求する。この要求に対し認証サーバASVは、匿名IDを発行してユーザ登録サーバUSVに返送する。

【0059】

(L) ユーザ登録サーバUSVは、次にID連携管理部512により、上記(J)によりデータサーバDSV1～DSVnから返送されたユーザIDと、上記(K)において認証サーバASVから取得した匿名IDを使用して、データサーバDSV1～DSVnに対してID連携情報の登録を要求する。この要求に対しデータサーバDSV1～DSVnは、ID連携情報をID連携DB121に格納する。

30

【0060】

(M) またそれと共にユーザ登録サーバUSVは、上記(1-5)により認証サーバASVから返送されたユーザIDを使用して、サービス関連付け管理部513により、図10に示すように認証サーバASVに対しデータサーバDSV1～DSVnのサービス関連付けを要求する。データサーバDSV1～DSVnは、この要求を受けると上記サービスの関連付けに関する情報を保存する。

(N) ユーザ登録サーバUSVは、上記(K)～(M)の処理を、データサーバDSV1～DSVnの数分だけ繰り返す。

40

(O) 以上の処理が終了すると、ユーザ登録サーバUSVはユーザ登録結果を表す情報を、図10に示すように登録要求元のコンソール端末に送信する。

【0061】

(2) ユーザID/匿名IDの問い合わせ処理

ユーザIDをもとにサーバ間の連携に使用している匿名IDを問い合わせる処理と、反対に匿名IDをもとにユーザIDを問い合わせる処理について、その手順を説明する。この処理機能を組み合わせることで、サーバ間のユーザIDの変換が可能となる。

図11は、このユーザID/匿名IDの問い合わせ処理の手順を示すシーケンス図である。

50

【 0 0 6 2 】

(2 - 1) ユーザ I D から匿名 I D の問い合わせ

(A) コンソール端末においてオペレータは、図 1 1 に例示するようにユーザ I D / 匿名 I D 問い合わせ画面が表示されている状態で、問い合わせ対象のサーバ (認証サーバ A S V 、データサーバ D S V 1 ~ D S V n 、サービス連携サーバ S S V 1 ~ S S V n 、ポータルサーバ P S V) と、ユーザ I D 及び連携先のサーバ (認証サーバ A S V 、データサーバ D S V 1 ~ D S V n 、サービス連携サーバ S S V 1 ~ S S V n 、ポータルサーバ P S V) をそれぞれ指定する。

【 0 0 6 3 】

(B) これに対しユーザ登録サーバ U S V は、オペレータが指定した上記各サーバの連携基盤配布部 1 1 1 , 3 1 1 , 4 1 1 に対して、ユーザ I D / 匿名 I D の変換処理要求を送信する。なお、ユーザ登録サーバ U S V にプロキシサーバの設定がある場合は、プロキシサーバ P S V 経由で要求を送信する。

10

【 0 0 6 4 】

(C) 上記ユーザ登録サーバ U S V からの要求を受信すると、各サーバの連携基盤配布部 1 1 1 , 3 1 1 , 4 1 1 は、I D 連携 D B 1 2 1 , 3 2 1 , 4 2 1 を参照し、ユーザ I D をキーとして対応する匿名 I D を読み出し、この読み出した匿名 I D をユーザ登録サーバ U S V へ返送する。

【 0 0 6 5 】

(D) ユーザ登録サーバ U S V は、サーバの連携基盤配布部 1 1 1 , 3 1 1 , 4 1 1 から、上記要求したユーザ I D / 匿名 I D の変換処理要求に対する変換結果を受信する。

20

(E) ユーザ登録サーバ U S V は、上記受信したユーザ I D から匿名 I D への変換結果をコンソール端末に送信し、表示させる。

【 0 0 6 6 】

(2 - 2) 匿名 I D からユーザ I D への問い合わせ

(A) コンソール端末においてオペレータは、図 1 1 に例示するようにユーザ I D / 匿名 I D 問い合わせ画面が表示されている状態で、問い合わせ対象のサーバ (認証サーバ A S V 、データサーバ D S V 1 ~ D S V n 、サービス連携サーバ S S V 1 ~ S S V n 、ポータルサーバ P S V) と、ユーザ I D 及び連携先のサーバ (認証サーバ A S V 、データサーバ D S V 1 ~ D S V n 、サービス連携サーバ S S V 1 ~ S S V n 、ポータルサーバ P S V) をそれぞれ指定する。

30

【 0 0 6 7 】

(B) これに対しユーザ登録サーバ U S V は、オペレータが指定した上記各サーバの連携基盤配布部 1 1 1 , 3 1 1 , 4 1 1 に対して、匿名 I D / ユーザ I D の変換処理要求を送信する。なお、ユーザ登録サーバ U S V にプロキシサーバの設定がある場合は、プロキシサーバ P S V 経由で要求を送信する。

【 0 0 6 8 】

(C) 上記ユーザ登録サーバ U S V からの要求を受信すると、各サーバの連携基盤配布部 1 1 1 , 3 1 1 , 4 1 1 は、I D 連携 D B 1 2 1 , 3 2 1 , 4 2 1 を参照し、匿名 I D をキーとして対応するユーザ I D を読み出し、この読み出したユーザ I D をユーザ登録サーバ U S V へ返送する。

40

【 0 0 6 9 】

(D) ユーザ登録サーバ U S V は、サーバの連携基盤配布部 1 1 1 , 3 1 1 , 4 1 1 から、上記要求した匿名 I D / ユーザ I D の変換処理要求に対する変換結果を受信する。

(E) ユーザ登録サーバ U S V は、上記受信した匿名 I D からユーザ I D への変換結果をコンソール端末に送信し、表示させる。

【 0 0 7 0 】

(3) ユーザ登録と同時に開示設定を行う処理

図 1 2 は、このユーザ登録と同時に開示設定を行う処理のシーケンスを示す図である。

50

ユーザ登録サーバUSVから、認証サーバASV、データサーバDSV1～DSVn、サービス連携サーバSSV1～SSVn及びポータルサーバPSVへ送信する要求の中で、付加情報を「キー＝値」の組み合わせで汎用的に保持可能な形態にする。

【0071】

先に(1)において説明したユーザ情報及びその連携情報の一括登録処理の手順に、以下の手順を追加する。

まず該当ユーザがデータサーバDSV1～DSVnに登録されたユーザだった場合には、ユーザ登録サーバUSVからサービス連携サーバSSV1～SSVnに対して、該当ユーザの開示設定情報の提供を要求し、その結果をコンソール端末に送信する。コンソール端末においてオペレータは、該当ユーザに対する追加開示設定情報を入力する。ユーザ登録サーバUSVは、データサーバDSV1～DSVnに対してユーザ登録要求を行う際に、付加情報として「開示設定情報＝add:userA」を要求に埋め込む。

10

【0072】

データサーバDSV1～DSVnは、ユーザ登録サーバUSVからユーザ登録、更新又は削除の要求を受信すると、当該要求に埋め込まれている付加情報に開示設定情報が含まれているか判定する。そして、付加情報に上記ユーザ属性が含まれていた場合には、この情報に基づいて、自らの開示設定DB123に対し開示設定情報を追加、更新又は削除する処理を行う。

【0073】

なお、以上(1)～(3)で述べたユーザ登録処理、ID変換処理及び開示設定処理は、いずれも通信ネットワークNW上において、サービス連携サーバSSV1～SSVnがデータサーバDSV1～DSVnから個人データを収集して利用者端末UTに配信するために使用される通信チャンネルとは異なる、登録・設定専用の通信チャンネルを介して行われる。

20

【0074】

以上述べたようにこの実施形態では、ユーザ登録サーバUSVにおいて、利用者端末UTからユーザ一括登録要求が送られた場合に、上記認証サーバASVと協働して他の各サーバが保有するユーザID間を連携するためのID連携情報を生成し、この生成されたID連携情報を上記データサーバDSV1～DSVn及びサービス連携サーバSSV1～SSVnにそれぞれ送信して登録するようにしている。

30

【0075】

したがって、各サーバにそれぞれ登録されたユーザID間を連携させるためのID連携情報と、認証サーバASVが管理するユーザの認証情報とに基づいて、サービス連携サーバSSV1～SSVnにより各データサーバDSV1～DSVnからユーザの個人データが収集され、この収集された個人データが要求元の利用者端末UTに配信される。このため、ユーザはリアルタイムに自身に係わる個人データを取得することができる。また、要求に応じてその都度各データサーバから個人データが収集されるので、個人データを集中管理するためのデータベースが不要となる。このため、分散情報の連携配信サービスを提供しようとする際の設備上及び管理上の負担が軽減され、さらに利用者数の増加や医療データを管理しているデータサーバ数の増加要求にも対応し易くなり、これによりスケラビリティのあるシステムを提供可能となる。

40

【0076】

しかも、ユーザ登録サーバUSVにより、すべてのサーバに対しユーザの情報間を連携させるためのID連携情報が一括して登録される。このため、きわめて効率良くID連携情報の登録を行うことができ、かつ不慣れなユーザやオペレータであっても誤ることなく登録を行うことができる。

【0077】

さらに、この実施形態では、各データサーバDSV1～DSVnに対する個人データの開示設定処理が、ユーザ一括登録処理と同時に行われる。このため、開示設定処理をユーザ一括登録処理とは別々に行う場合に比べ、開示設定の処理を効率良く行うことができる

50

。

【 0 0 7 8 】

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、ポータルサーバ P S V は設けても設けなくてもよく、またサービス連携サーバは複数台であっても 1 台であってもよい。その他、ユーザ登録サーバ、データサーバ、サービス連携サーバ及び認証サーバの構成、ユーザ一括登録処理の手順とその内容、開示設定処理の手順とその内容等についても、この発明の要旨を逸脱しない範囲で種々変形して実施できる。

【 0 0 7 9 】

要するにこの発明は、上記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わ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わせてもよい。

【 図面の簡単な説明 】

【 0 0 8 0 】

【 図 1 】 この発明の一実施形態に係わる分散情報連携システムの全体構成を示すブロック図である。

【 図 2 】 図 1 に示した分散情報連携システムにおけるデータサーバの機能構成を示すブロック図である。

【 図 3 】 図 1 に示した分散情報連携システムにおけるポータルサーバの機能構成を示すブロック図である。

【 図 4 】 図 1 に示した分散情報連携システムにおける認証サーバの機能構成を示すブロック図である。

【 図 5 】 図 1 に示した分散情報連携システムにおけるサービス連携サーバの機能構成を示すブロック図である。

【 図 6 】 図 1 に示した分散情報連携システムにおけるユーザ登録サーバ U S V の機能構成を示すブロック図である。

【 図 7 】 ユーザの一括登録処理において使用される利用者操作画面の一例を示す図である。

【 図 8 】 ユーザの一括登録処理の前半部分の処理手順と処理内容を示すシーケンス図である。

【 図 9 】 ユーザの一括登録処理の中間部分の処理手順と処理内容を示すシーケンス図である。

【 図 1 0 】 ユーザの一括登録処理の後半部分の処理手順と処理内容を示すシーケンス図である。

【 図 1 1 】 ユーザ I D / 匿名 I D 問い合わせ処理の処理手順と処理内容を示すシーケンス図である。

【 図 1 2 】 ユーザ登録と同時に開示設定を行う場合の処理手順と処理内容を示すシーケンス図である。

【 符号の説明 】

【 0 0 8 1 】

D S V 1 ~ D S V n ... データサーバ、 P S V ... ポータルサーバ、 A S V ... 認証サーバ、 S S V 1 ~ S S V m ... サービス連携サーバ、 U S V ... ユーザ登録サーバ U S V、 U T ... 利用者端末、 N W ... 通信網、 1 1 , 2 1 , 3 1 , 4 1 , 5 1 ... ユーザ設定モジュール、 1 2 , 2 2 , 3 2 , 4 2 , 5 2 ... データベース群、 1 3 , 2 3 , 3 3 , 4 3 ... 連携処理モジュール、 1 4 , 4 4 ... アプリケーション処理モジュール、 2 4 , 5 3 ... 利用者操作処理モジュール、 3 4 ... 認証処理モジュール、 1 1 1 , 2 1 1 , 3 1 1 , 4 1 1 ... 連携基盤配布部、 1 1 2 , 3 1 2 , 4 1 2 ... 個別カスタム部、 1 2 1 , 2 2 , 3 2 1 , 4 2 1 ... I D 連携データベース、 1 2 2 , 3 2 2 , 4 2 2 , 5 2 ... ユーザデータベース、 1 2 3 ... 開示設定データベース、 1 2 4 ... アプリケーションデータベース、 3 2 3 ... ディレクトリデータベ

10

20

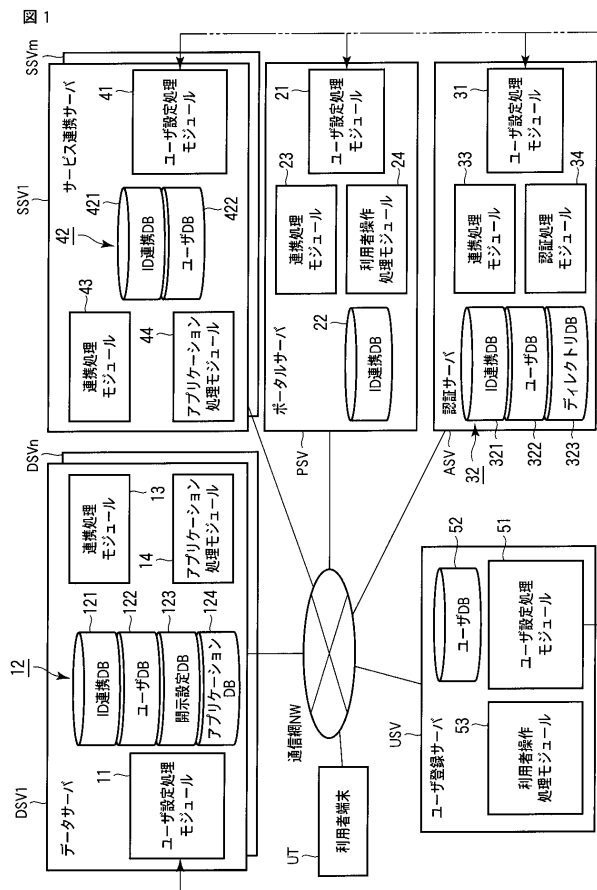
30

40

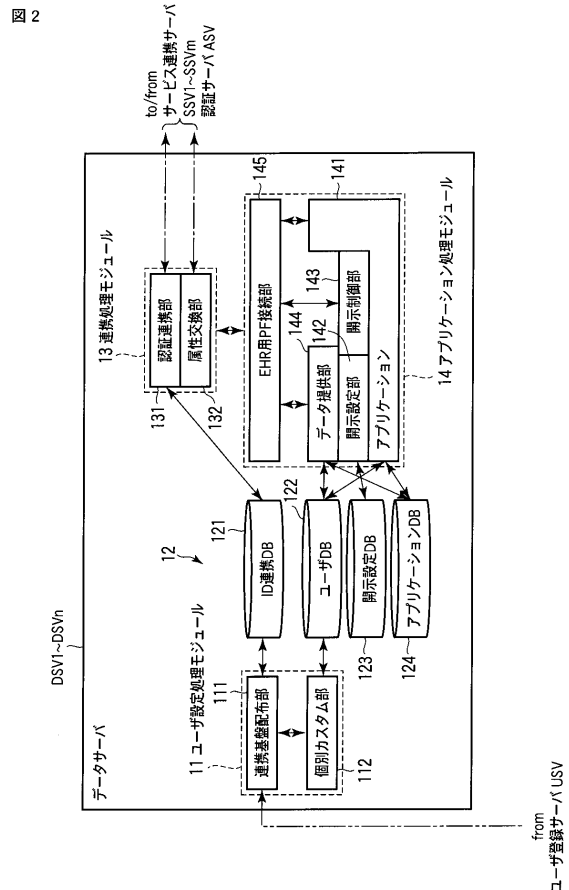
50

ース、131, 231, 332, 431... 認証連携部、132, 331, 432... 属性交換部、141, 441... アプリケーション、142... 開示設定部、143... 開示制御部、144... データ提供部、241~24n... 利用者操作部、341... 認証部、442... 開示設定要求部、443... データ収集部、444... EHR用PF接続部、511... ユーザ管理部、512... ID連携管理部、513... サービス関連付け管理部、514... 匿名ID管理部、515... ユーザ検索部。

【図1】

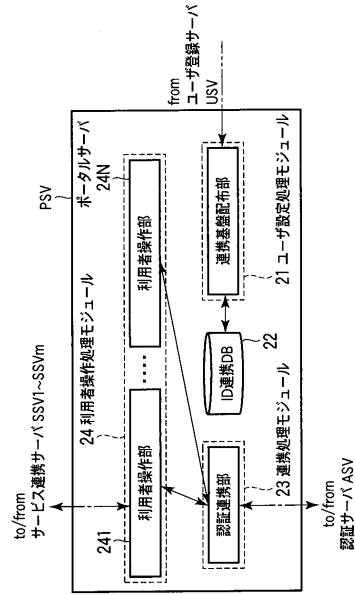


【図2】



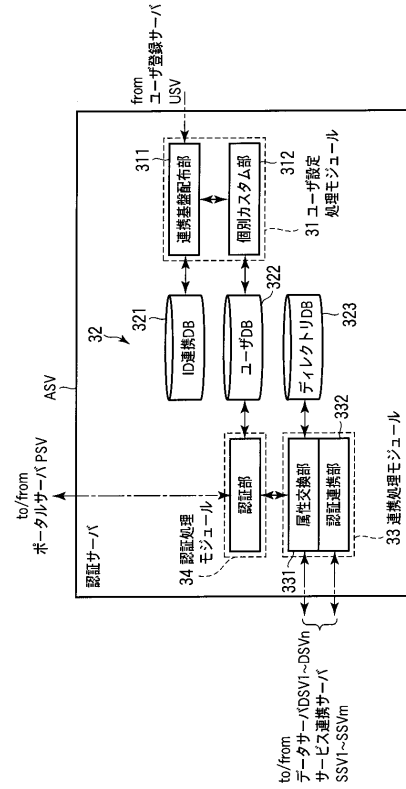
【図 3】

図 3



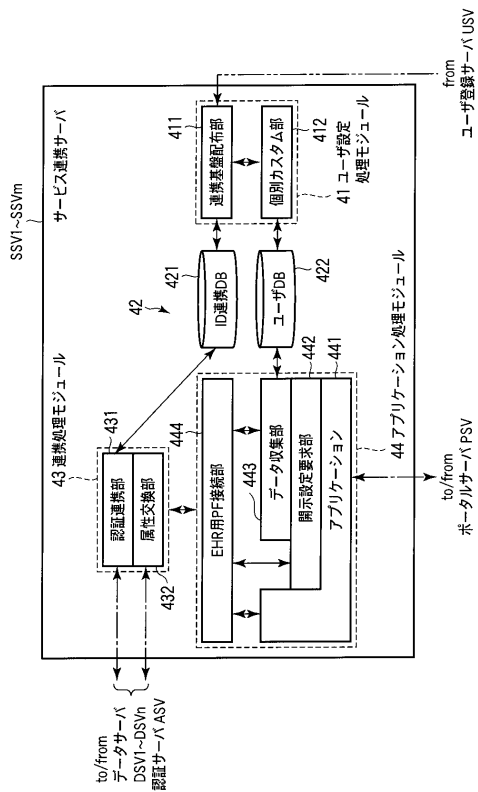
【図 4】

図 4



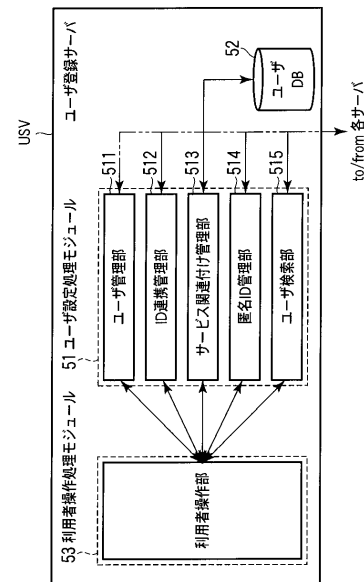
【図 5】

図 5



【図 6】

図 6



フロントページの続き

- (74)代理人 100103034
弁理士 野河 信久
- (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 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 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
- (72)発明者 小倉 賢治
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
- F ターム(参考) 5B017 AA08 BB09 CA16
5B285 BA08 BA10