

(11) 特許出願公開番号

特開2015-201049

(P2015-201049A)

(43) 公開日 平成27年11月12日(2015.11.12)

(51) Int.Cl.

G06F 21/60 (2013.01)

F 1

G06F 21/24 160C

テーマコード (参考)

審査請求 未請求 請求項の数 6 O.L. (全 13 頁)

(21) 出願番号 特願2014-79674 (P2014-79674)

(22) 出願日 平成26年4月8日 (2014.4.8)

(71) 出願人 000004226

日本電信電話株式会社

東京都千代田区大手町一丁目5番1号

(74) 代理人 100108855

弁理士 蔵田 昌俊

(74) 代理人 100103034

弁理士 野河 信久

(74) 代理人 100075672

弁理士 峰 隆司

(74) 代理人 100179062

弁理士 井上 正

(72) 発明者 白石 将浩

東京都千代田区大手町一丁目5番1号 日本電信電話株式会社内

[最終頁に続く](#)

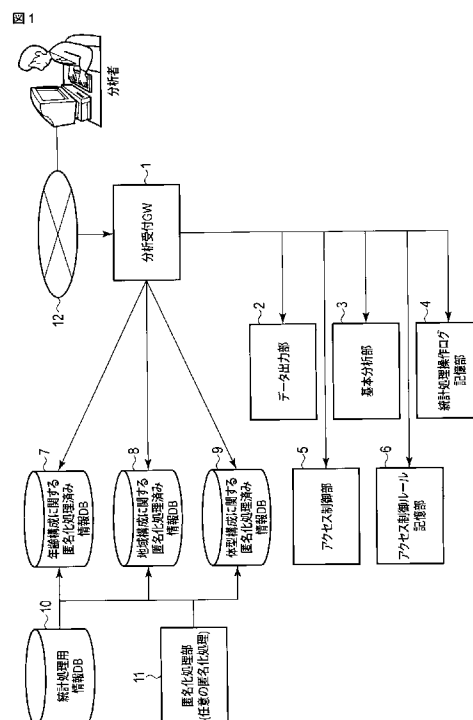
(54) 【発明の名称】 アクセス権限処理システム、アクセス権限処理方法、及びプログラム

(57) 【要約】

【課題】 1つの母集団から生成された複数種類の匿名化情報の分析結果から匿名化された個人情報に絞込まれたり、推測されたり、或いは特定されたりするのを防止することが可能なアクセス権限処理システムを提供することにある。

【解決手段】アクセス権限処理システムは、匿名化処理により得られる匿名化情報の分析要求を受付ける受付手段と、前記分析要求に基づきログを抽出する抽出手段と、前記分析要求に基づき制御ルールを参照する参照手段と、前記ログ及び前記制御ルールに基づき前記匿名化情報へのアクセスの可否を判定する判定手段と、前記匿名化情報へのアクセス許可の判定に基づき前記匿名化情報の分析結果を提供する情報提供手段と、を備える。

【選択図】 図1



【特許請求の範囲】**【請求項 1】**

匿名化処理により得られる匿名化情報の分析要求を受付ける受付手段と、
前記分析要求に基づきログを抽出する抽出手段と、
前記分析要求に基づき制御ルールを参照する参照手段と、
前記ログ及び前記制御ルールに基づき前記匿名化情報へのアクセスの可否を判定する判定手段と、
前記匿名化情報へのアクセス許可の判定に基づき前記匿名化情報の分析結果を提供する情報提供手段と、
を備えるアクセス権限処理システム。

10

【請求項 2】

前記抽出手段は、前記分析要求に基づき、前記匿名化情報の母集団に関する操作ログを抽出し、
前記参照手段は、前記分析要求に基づき、前記母集団に関するアクセス制御ルールを参照し、
前記判定手段は、前記操作ログ及び前記アクセス制御ルールに基づき前記匿名化情報へのアクセスの可否を判定する請求項 1 のアクセス権限処理システム。

【請求項 3】

前記操作ログは、前記母集団から生成される 1 種類以上の匿名化情報に対して何種類の統計処理を実施したかを示す情報を含み、
前記アクセス制限ルールは、前記母集団から生成される 1 種類以上の匿名化情報に対して何種類の統計処理までであれば前記匿名化情報へのアクセスを許容するかを示す情報を含む請求項 2 のアクセス権限処理システム。

20

【請求項 4】

前記情報提供手段は、前記匿名化情報へのアクセス許可の判定に基づき分析処理部へ前記匿名化情報の分析を要求し、前記匿名化情報の前記分析結果を受け取り、前記分析結果を提供する請求項 1 乃至 3 の何れか 1 つのアクセス権限処理システム。

【請求項 5】

匿名化処理により得られる匿名化情報の分析要求を受け、
前記分析要求に基づきログを抽出し、
前記分析要求に基づき制御ルールを選択し、
前記ログ及び前記制御ルールに基づき前記匿名化情報へのアクセスの可否を判定し、
前記匿名化情報へのアクセス許可の判定に基づき前記匿名化情報の分析結果を提供するアクセス権限処理方法。

30

【請求項 6】

請求項 1 乃至 4 の何れか 1 つのアクセス権限処理システムが備える各手段の処理をコンピュータに実行させるプログラム。

【発明の詳細な説明】**【技術分野】****【0001】**

この発明は、医療情報などの機密情報を処理するアクセス権限処理システム、アクセス権限処理方法、及びプログラムに関する。

40

【背景技術】**【0002】**

医療情報を流通させ、統計分析などに 2 次利用することが考えられている。例えば、流通しているデータを集め、統計処理をすることによって、地域ごとの疾病状況、及びある年のインフルエンザの流行状況を検出し、将来の製薬や公衆衛生管理の参考とするといったユースケースである。

【0003】

医療情報は、「医療情報を受託管理する情報処理事業者向けガイドライン (<http://www>

50

.meti.go.jp/policy/it_policy/privacy/iryoughlv2.pdf) 」などの各種ガイドラインや個人情報保護法に従った形式で保管・流通される必要がある。統計分析などの2次利用として収集したデータであっても個人が特定される形式でデータを保管することは、個人情報保護の観点から適切ではない。収集したデータについても、第三者に個人を特定されないように分析に利用してもらうことと保管することが重要である。

【0004】

収集したデータを用いて、第三者に個人を特定されない形式で分析利用させる技術として、匿名化技術が知られている。匿名化技術は様々あるが、基本的には個人が特定されるような情報（氏名、性別）をマスクする、あるいはぼかした値にする処理を行う。マスクする場合、個人名を全く異なる値に書き替える、住所などの情報を県単位に書き替える。ぼかした値にする場合、年齢が23才であっても、23才の人が一人であれば、全体的に20才代と表現する様に値を書き替える。

10

【先行技術文献】

【特許文献】

【0005】

【特許文献1】特開2006-324076

【特許文献2】特許4843325

【発明の概要】

【発明が解決しようとする課題】

【0006】

20

上記匿名化技術によって、個人情報保護された情報（母集団）からの分析処理（例えば統計処理）が可能となる。しかしながら、1つの母集団の情報に対する複数種類の匿名化処理により得られる複数種類の匿名化情報（から生成される複数種類の分析結果）を無制限に提供すると、一人の人物が複数種類の匿名化情報（又は複数種類の分析結果）を入手し、これら複数種類の匿名化情報（又は複数種類の分析結果）を組み合わせる分析することにより、匿名化された個人情報に絞込まれたり、推測されたり、或いは特定されたりする可能性がある。そのため、このような分析から匿名化された個人情報が絞込まれたり、推測されたり、或いは特定されたりするのを防止する仕組みが要望されている。

【0007】

この発明は上記事情に着目してなされたもので、1つの母集団から生成された複数種類の匿名化情報の分析結果から匿名化された個人情報に絞込まれたり、推測されたり、或いは特定されたりするのを防止することが可能な情報処理システム、アクセス権限処理方法、及びプログラムを提供することにある。

30

【課題を解決するための手段】

【0008】

上記目的を達成するためにこの発明のアクセス権限処理システム、アクセス権限処理方法、及びプログラムは、以下のように構成されている。

【0009】

（1）アクセス権限処理システムは、匿名化処理により得られる匿名化情報への分析要求を受付ける受付手段と、前記分析要求に基づきログを抽出する抽出手段と、前記分析要求に基づき制御ルールを参照する参照手段と、前記ログ及び前記制御ルールに基づき前記匿名化情報へのアクセスの可否を判定する判定手段と、前記匿名化情報へのアクセス許可の判定に基づき前記匿名化情報の分析結果を提供する情報提供手段と、を備える。

40

【0010】

（2）さらに、上記（1）のアクセス権限処理システムの前記抽出手段は、前記分析要求に基づき、前記匿名化情報の母集団に関する操作ログを抽出し、前記参照手段は、前記分析要求に基づき、前記母集団に関するアクセス制御ルールを参照し、前記判定手段は、前記操作ログ及び前記アクセス制御ルールに基づき前記匿名化情報へのアクセスの可否を判定する。

【0011】

50

(3) さらに、上記(2)のアクセス権限処理システムの前記操作ログは、前記母集団から生成される1種類以上の匿名化情報に対して何種類の統計処理を実施したかを示す情報を含み、前記アクセス制限ルールは、前記母集団から生成される1種類以上の匿名化情報に対して何種類の統計処理までであれば前記匿名化情報へのアクセスを許容するかを示す情報を含む。

【0012】

(4) さらに、上記(1)乃至(3)の何れか1つのアクセス権限処理システムの前記情報提供手段は、前記匿名化情報へのアクセス許可の判定に基づき分析処理部へ前記匿名化情報の分析を要求し、前記匿名化情報の前記分析結果を受け取り、前記分析結果を提供する。

10

【0013】

(5) アクセス権限処理方法は、匿名化処理により得られる匿名化情報の分析要求を受け付け、前記分析要求に基づきログを抽出し、前記分析要求に基づき制御ルールを参照し、前記ログ及び前記制御ルールに基づき前記匿名化情報へのアクセスの可否を判定し、前記匿名化情報へのアクセス許可の判定に基づき前記匿名化情報の分析結果を提供する。

【0014】

(6) プログラムは、上記(1)乃至(4)の何れか1つのアクセス権限処理システムが備える各手段の処理をコンピュータに実行させる。

【発明の効果】

【0015】

20

すなわちこの発明によれば、1つの母集団から生成された複数種類の匿名化情報の分析結果から匿名化された個人情報に絞込まれたり、推測されたり、或いは特定されたりするのを防止することが可能なアクセス権限処理システム、アクセス権限処理方法、及びプログラムを提供することができる。

【0016】

上記(1)のアクセス権限処理システム、上記(5)のアクセス権限処理方法、及び上記(6)のプログラムによれば、ログ及び制御ルールに基づき、分析要求される第1の匿名化情報へのアクセスの可否を判定し、アクセスが許可された場合に、第1の匿名化情報の分析結果を提供するので、1つの母集団の情報に対して実行される複数種類の匿名化処理により匿名化された複数種類の匿名化情報から生成される複数種類の分析結果を得ることに制限を持たせることができる。これにより、制限された分析結果しか提供されないので、許可される数を超えて分析結果を集めて第1の匿名化情報を復元しようとする行為を防止することができる。

30

【0017】

上記(2)のアクセス権限処理システムによれば、前記匿名化情報の母集団に関する操作ログ及び前記母集団に関するアクセス制御ルールに基づき前記匿名化情報へのアクセスを制限することができる。

【0018】

上記(3)のアクセス権限処理システムによれば、前記母集団から生成される1種類以上の匿名化情報に対して何種類の統計処理を実施したかを示す情報及び前記母集団から生成される1種類以上の匿名化情報に対して何種類の統計処理までであれば前記匿名化情報へのアクセスを許容するかを示す情報に基づき前記匿名化情報へのアクセスを制限することができる。

40

【0019】

上記(4)のアクセス権限処理システムによれば、アクセスが許可された場合に前記匿名化情報の分析結果を受け取るので、アクセスが許可されない場合には分析結果を提供しないことにより、前記匿名化情報の元となる医療情報等の機密情報を安全に管理することができる。

【図面の簡単な説明】

【0020】

50

【図 1】実施形態に係るアクセス権限処理システムの概略構成を示す図である。

【図 2】統計処理操作ログの一例を示す図である。

【図 3】統計処理操作ログアクセス制御ルールの一例を示す図である。

【図 4】実施形態に係るアクセス権限処理システムによる処理シーケンスの一例を示す図である。

【図 5】実施形態に係るアクセス権限処理システムによるログ検索条件取得及び過去ログ検索の一例を示すフローチャートである。

【図 6】実施形態に係るアクセス権限処理システムによるアクセス判定（S T 1 4）の一例を示す図である。

【発明を実施するための形態】

10

【0021】

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。

【0022】

図 1 は、実施形態に係るアクセス権限処理システムの概略構成を示す図である。図 1 に示すように、アクセス権限処理システムは、分析受付 G W（Gateway）1、データ出力部 2、基本分析部 3、統計処理操作ログ記憶部 4、アクセス制御部 5、アクセス制御ルール記憶部 6、年齢構成に関する匿名化処理済み情報 D B（Data Base）7、地域構成に関する匿名化処理済み情報 D B 8、体型構成に関する匿名化処理済み情報 D B 9、統計処理用（医療）情報 D B 10、匿名化処理部 11 を備える。

【0023】

20

ここで、アクセス権限処理システムを構成する各部の詳細について簡単に説明する。なお、各部の詳細については後に説明する。分析受付 G W 1 は、インターネット 12 を介して、分析者のパーソナルコンピュータ等からのアクセス（医療情報の分析要求等）を受付けることができる。データ出力部 2 は、分析者のパーソナルコンピュータ等からのアクセス（医療情報の分析要求等）に対応して、分析結果（匿名化された医療情報の統計処理結果等）を提供することができる。基本分析部 3 は、分析者のパーソナルコンピュータ等からのアクセス（医療情報の分析要求等）に対応して、年齢構成に関する匿名化処理済み情報、地域構成に関する匿名化処理済み情報、又は体型構成に関する匿名化処理済み情報を分析する。なお、本実施形態では、複数の匿名化処理として、年齢構成に関する匿名化処理、地域構成に関する匿名化処理、及び体型構成に関する匿名化処理について説明するが、これらに限定されるものではなく、さらに他の匿名化処理と組み合わせることもできる。

30

【0024】

統計処理操作ログ記憶部 4 は、図 2 に示す統計処理操作ログ（分析処理操作ログ）を記憶し、統計処理操作に応じて統計処理操作ログを更新する。アクセス制御ルール記憶部 6 は、図 3 に示す統計処理操作ログアクセス制御ルール（以下、アクセス制御ルール）を記憶する。アクセス制御部 5 は、分析者のパーソナルコンピュータ等からのアクセス（医療情報の分析要求等）に対応して、図 2 に示す統計処理操作ログ及び図 3 に示すアクセス制御ルールに基づき、アクセスの可否を判定し、アクセス可能判定に基づき年齢構成に関する匿名化処理済み情報、地域構成に関する匿名化処理済み情報、又は体型構成に関する匿名化処理済み情報へのアクセスを許可し、アクセス不能判定に基づきこれら情報へのアクセスを許可しない。なお、アクセス制御ルールはアクセス制御ルール記憶部 6 に記憶され、このアクセス制御ルールにおいて定義を設定する方法は、S Q L（Structured Query Language）等でアクセス制御ルール記憶部 6 に記憶されたアクセス制御ルールを直接編集してもよいし、G U I（Graphical User Interface）等を分析受付 G W 1 に用意し、G U I 等からアクセス制御ルール記憶部 6 に記憶されたアクセス制御ルールを編集するようにしてもよい。

40

【0025】

統計処理用情報 D B 10 は、医療情報（母集団の情報）を記憶する。匿名化処理部 11 は、匿名化処理（任意の匿名化処理）により、統計処理用情報 D B 10 に記憶された医療

50

情報から匿名化処理済みの医療情報を生成する。例えば、匿名化処理部 11 は、医療情報（母集団の情報）に対する年齢構成に関する匿名化処理により、医療情報から年齢構成に関する匿名化処理済みの医療情報を生成する。また、匿名化処理部 11 は、医療情報（母集団の情報）に対する地域構成に関する匿名化処理により、医療情報から地域構成に関する匿名化処理済みの医療情報を生成する。匿名化処理部 11 は、医療情報（母集団の情報）に対する体型構成に関する匿名化処理により、医療情報から体型構成に関する匿名化処理済みの医療情報を生成する。年齢構成に関する匿名化処理済み情報 DB 7 は、年齢構成に関する匿名化処理済みの医療情報を記憶する。地域構成に関する匿名化処理済み情報 DB 8 は、地域構成に関する匿名化処理済みの医療情報を記憶する。体型構成に関する匿名化処理済み情報 DB 9 は、体型構成に関する匿名化処理済みの医療情報を記憶する。なお、匿名社処理済みの医療情報は、分析処理終了後に削除される。

10

【0026】

なお、本実施形態では、医療情報を処理するアクセス権限処理システムについて説明するが、処理する情報は医療情報に限定されるものではなく、機密性が高く且つ一部の情報を隠す必要のある情報について適用可能である。

【0027】

図 4 は、図 1 に示すアクセス権限処理システムによる処理シーケンスの一例を示す図である。図 4 に示すように、分析者は、例えばパーソナルコンピュータにより、ネットワーク 12 を介して分析受付 GW 1 へアクセスし、公開分析処理一覧を要求する（ST1）。分析受付 GW 1 は、分析処理要求に応じた匿名化処理済み情報 DB（年齢構成に関する匿名化処理済み情報 DB 7、地域構成に関する匿名化処理済み情報 DB 8、又は体型構成に関する匿名化処理済み情報 DB 9）を検索し（ST2）、匿名化処理済み情報 DB からの検索結果の返却を受信する（ST3）。さらに、分析受付 GW 1 は、基本分析部 3 に対して、基本分析機能の有無を検索し（ST4）、検索結果の返却を受信する（ST5）

20

分析者が、例えばパーソナルコンピュータにより、ネットワーク 12 を介して分析受付 GW 1 へアクセスし、分析処理（匿名化情報の分析処理）を要求すると（ST6）、分析受付 GW 1 は、分析処理要求に基づき、ログ出力（いつ、どこからのアクセスでどの組織の、誰がどの母集団に対して、どういう匿名化した情報をどうしたいか）を要求し、アクセス制御判定を要求する（ST8）。例えば、アクセス制御判定要求は、アクセス元（グローバル IP アドレス（124.5.x.13）及びドメイン名の少なくとも一方）、組織名（Xx 研究所）、担当者（氏名 a）、母集団（A 年度全国医療情報）、匿名化等の情報処理（地域構成別医療費統計）、出力形態（グラフ出力）等の情報を含む。なお、利用者は、あらかじめ分析受付 GW の利用に関する申請（アクセス権限処理システムへのアカウント登録）を済ませていることが前提となる。また、母集団の情報に対してラベル（A 年度全国医療情報）が付けられている場合に、このラベルを使ったログ管理及びアクセス制御判定が可能となる。

30

【0028】

アクセス制御部 5 は、アクセス制御判定要求に基づき、アクセス制御ルール記憶部 6 に記憶されているアクセス制御ルールを検索し（ST9）、検索結果の返却を受信する（ST10）。アクセス制御部 5 は、ログ検索条件を取得し（ST11）、統計処理操作ログ記憶部 4 に対して該当するログ（統計処理操作ログ等）を検索し（ST12）、検索結果の返却を受信する（ST13）。アクセス制御部 5 は、アクセス制御ルール及び統計処理操作ログに基づき、アクセス可否を判定し（ST14）、判定結果を送信する。

40

【0029】

例えば、分析処理要求が母集団（A 年度全国医療情報）の分析処理要求を含む場合、アクセス制御判定要求が母集団（A 年度全国医療情報）のアクセス制御判定要求を含み、母集団（A 年度全国医療情報）に関する操作ログが取得され、母集団（A 年度全国医療情報）に関するアクセス制御ルールが取得される。これにより、アクセス制御部 5 は、母集団（A 年度全国医療情報）に関する操作ログ及び母集団（A 年度全国医療情報）に関するアクセス制御ルールに基づき、アクセス可否を判定する。

50

【0030】

例えば、母集団（A年度全国医療情報）に関する操作ログが、母集団から生成される1種類以上の匿名化情報に対して何種類の統計処理を実施したかを示す情報を含む。また、母集団（A年度全国医療情報）に関するアクセス制御ルールが、母集団から生成される1種類以上の匿名化情報に対して何種類の統計処理までであれば匿名化情報へのアクセスを許可するかを示す情報を含む。

【0031】

例えば、操作ログが、4種類の統計処理を実施したことを示す情報を含み、アクセス制御ルールが、5種類の統計処理までであれば前記匿名化情報へのアクセスを許可することを示す情報を含む場合、アクセス制御部5は、母集団（A年度全国医療情報）から生成された匿名化情報へのアクセスを許可する。操作ログが、5種類の統計処理を実施したことを示す情報を含み、アクセス制御ルールが、5種類の統計処理までであれば前記匿名化情報へのアクセスを許可することを示す情報を含む場合、アクセス制御部5は、次の統計処理が6種類目の統計処理でなければ、母集団（A年度全国医療情報）から生成された匿名化情報へのアクセスを許可し、次の統計処理が6種類目の統計処理であれば、母集団（A年度全国医療情報）から生成された匿名化情報へのアクセスを許可しない。さらに、アクセス制御ルールが、「過去いつまでの間に」という条件文を含むこともできる。例えば、アクセス制御ルールが、「過去1年の間に」という条件文を含む場合、アクセス制御部5は、次の統計処理が過去1年の間で6種類目の統計処理でなければ、母集団（A年度全国医療情報）から生成された匿名化情報へのアクセスを許可し、次の統計処理が過去1年の間で6種類目の統計処理であれば、母集団（A年度全国医療情報）から生成された匿名化情報へのアクセスを許可しない。

【0032】

分析受付GW1は、アクセス制御部5からの判定結果を受け取り、年齢構成に関する匿名化処理済み情報DB7、地域構成に関する匿名化処理済み情報DB8、又は体型構成に関する匿名化処理済み情報DB9に対して、分析処理要求に応じたデータ抽出を要求し（ST16）、抽出結果の返却を受信し（ST17）、基本分析部3に対して抽出データの基本分析を要求する（ST18）。基本分析部3が抽出データを分析し、分析結果を返却し、分析受付GW1が分析結果を受信する（ST19）。分析受付GW1は、データ出力部2を介して、分析結果を閲覧可能として提供し、分析者のパーソナルコンピュータ等からのアクセス（閲覧）を受け付けることができる（ST20）。

【0033】

例えば、分析受付GW1は、匿名化処理により母集団から生成された匿名化情報を受け取り、基本分析部3がこの匿名化情報を分析し、分析受付GW1は、データ出力部2を介して、分析結果を閲覧可能として提供する。

【0034】

上記のように、アクセス制御部5が、アクセス制御ルール及び統計処理操作ログに基づき、アクセスを許可した場合に限り、匿名化情報に基づく分析結果が提供されるので、複数種類の匿名化処理により一つの母集団から生成される複数種類の匿名化情報に基づく複数種類の分析結果を無制限に提供しない。これにより、複数種類の匿名化情報に基づく複数種類の分析結果から母集団の情報を復元するような不正を防止することができる。なお、アクセス制御のデフォルト判定を全分析拒否とし、安全性を確保するようにしてもよい。システム管理者は、利用者からの分析受付GWの利用に関する申請（アクセス権限処理システムへのアカウント登録）に基づき、アクセス制御ルールに対して申請された利用者の利用を許可するための定義情報を設定する。これにより、利用者によるシステムの利用が可能となる。

【0035】

図5は、図1に示すアクセス権限処理システムによるログ検索条件取得（ST11）及び過去ログ検索（ST12）の一例を示すフローチャートである。アクセス制御部5は、アクセス制御判定要求に基づき（ST101）、分析処理要求内容を取得し（ST102

）、検索範囲定義情報を取得する（S T 1 0 3）。分析処理要求内容は、統計処理操作ログ構成要素を含む。検索範囲定義情報とは、アクセス制御ルールとは別で管理されている検索範囲を定義するファイル或いはテーブルである。定義されている内容は、〔母集団、検索範囲〕であり、例えば、〔母集団：A年度全国医療情報、検索範囲：1年〕、〔母集団：B年度〇×健保組合医療情報、検索範囲：6ヶ月〕である。

【0036】

アクセス制御部5は、定義ファイルを取得し（S T 1 0 4、Y E S）、定義ファイルに基づき検索範囲をセットし（S T 1 0 5）、アクセスログから状況等を検索する（S T 1 0 6）。

【0037】

例えば、分析処理要求内容が、A年度全国医療情報の分析処理要求であり、定義ファイルが〔母集団：A年度全国医療情報、検索範囲：1年〕を含む場合、ログ検索は、分析処理要求内容の要求元の情報から判明するアクセス元からの過去1年のA年度全国医療情報に対するアクセス状況及び処理状況が検索される。

【0038】

また、分析処理要求内容が、C年度〇〇県医療情報の分析処理要求であり、定義ファイルが未定義の場合、検索範囲はセットされず、ログ検索は、分析処理要求内容の要求元の情報から判明するアクセス元からの過去すべてのC年度〇〇県医療情報に対するアクセス状況及び処理状況が検索される。

【0039】

図6は、図1に示すアクセス権限処理システムによるアクセス判定（S T 1 4）の一例を示すフローチャートである。

【0040】

アクセス制御部5は、ルール検索結果とログ検索結果を呼び出し、ルール検索結果とログ検索結果に基づき、当該母集団に関する匿名化処理の種類数はルールに許可されている範囲の種類数以内であれば次の判定へ移行し（S T 2 0 2、Y E S）、種類数を越えるならばアクセス権限無しと判定する（S T 2 0 7）。

【0041】

さらに、アクセス制御部5は、ルール検索結果とログ検索結果に基づき、当該母集団に関する結果はルールに許可として記載された要求形式であれば次の判定へ移行し（S T 2 0 3、Y E S）、要求形式でなければアクセス権限無しと判定する（S T 2 0 7）。

【0042】

さらに、アクセス制御部5は、ルール検索結果とログ検索結果に基づき、アクセス元はルールに許可として記載された利用者属性であれば次の判定へ移行し（S T 2 0 4、Y E S）、利用者属性でなければアクセス権限無しと判定する（S T 2 0 7）。

【0043】

さらに、アクセス制御部5は、ルール検索結果とログ検索結果に基づき、アクセス元はルールに許可として記載された利用者個人であればアクセス権限有りとして判定し（S T 2 0 5）、利用者属性でなければアクセス権限無しと判定する（S T 2 0 7）。

【0044】

以下、アクセス権限処理システムのアクセス制御を適用しないケースを説明し、これに対比してアクセス権限処理システムのアクセス制御の作用効果について説明する。上記のアクセス制御を実行しない場合、個人情報保護のため一つの母集団の情報へのアクセスが制限されていたとしても、複数種類の匿名化処理により一つの母集団の情報から複数種類の匿名化情報を生成し、これら複数種類の匿名化情報から生成される複数種類の統計情報を分析することにより（例えば複数種類の統計情報を様々な形式で結びつけることにより）、匿名化された情報（個人情報）が推測又は復元されることがある。

【0045】

例えば、年齢構成に関する匿名化処理済み情報を統計処理した結果、地域構成に関する匿名化処理済み情報を統計処理した結果、及び体型構成に関する匿名化処理済み情報を統

10

20

30

40

50

計処理した結果を組み合わせると、匿名化処理されたはずの個人情報等を絞り込んだり、推測したり、或いは特定したりすることができる場合がある。

【0046】

本実施形態の医療情報システムは、上記したアクセス制御を実行するので、匿名化された情報を復元しようとして複数種類の匿名化情報から生成される複数種類の統計情報を入手しようとした場合に、制限がかかるので（例えば図3に示すようにA年度全国医療情報の統計処理は5種類まで、B年度〇×健保組合医療情報の統計処理は4種類まで）、制限された種類数を越えた統計処理の処理結果を入手させない。これにより、上記したように、匿名化された情報（個人情報）が絞り込まれたり、推測されたり、或いは特定されたりするのを防止できる。

10

【0047】

さらに上記説明した実施形態に対して、ダミー処理及び匿名化処理済みデータを一時的に提供する処理を組み合わせることもできる。

【0048】

オリジナルの医療情報を平文で保管することは、安全性の面から適切ではない。しかしながら、予め匿名化処理により匿名化された医療情報を保管すると、オリジナルの医療情報に含まれていた一部の情報が欠落するため、統計処理に支障が出たり、統計処理の用途が限定されたりすることが考えられる。

【0049】

例えば、オリジナルの医療情報を保管せず、年齢構成に関する匿名化処理済みの医療情報、地域構成に関する匿名化処理済みの医療情報、及び体型構成に関する匿名化処理済みの医療情報を保管するケースを想定する。この場合、安全性については向上するものの、例えば、年齢構成に関する匿名化処理済みの医療情報に着目すると、年齢構成については外れ値が除去されるため、年齢構成を使った統計の精度が低下することが考えられ、統計処理の用途が限定されてしまう。地域構成に関する匿名化処理済みの医療情報、及び体型構成に関する匿名化処理済みの医療情報についても同様である。従って、オリジナルの医療情報を安全に保管する技術が要望される。

20

【0050】

そこで、オリジナルの医療情報をそのまま保管する方法に替えて、ダミー処理によりダミーデータを混在させた医療情報を保管することにより、一定水準での医療情報の安全性を確保することができる。ここで、ダミー処理について説明する。アクセス権限処理システムは、ダミーデータ管理テーブルを保持し、ダミーデータ管理テーブルに基づき医療情報（種類など）に応じたダミー処理を選択し、選択したダミー処理に基づきオリジナルの医療情報からダミーデータを含む医療情報を生成し、ダミーデータを含む医療情報を保管する。これにより、例えば、悪意のある人物により、保管されている医療情報が抜き取られたとしても、抜き取られた医療情報にはダミー処理によりダミーデータが混在されているので、抜き取られた医療情報から正しい情報をつかむことは容易ではない。ダミーデータ管理テーブルは、医療情報の提供元及び医療情報の種類等に応じたダミー処理を指定する情報を含む。

30

【0051】

統計処理（オリジナルの医療情報）が要求された場合、アクセス権限処理システムは、ダミーデータ管理テーブルに基づきダミーデータを含む医療情報からオリジナルの医療情報を生成し、オリジナルの医療情報を匿名化し、匿名化された医療情報を統計処理し、統計結果（分析結果）を提供（出力）する。また、匿名化された医療情報の提供は一時的なものとし、統計処理後に匿名化された医療情報を削除する。以上により、医療情報から個人情報等が流出するのを防止することができる。

40

【0052】

なお、上記アクセス制御、統計処理（分析処理）、ダミー処理、匿名化処理等の処理の全ての手順はソフトウェアによって実行することが可能である。このため、上記処理の手順を実行するプログラムを格納したコンピュータ読み取り可能な記憶媒体を通じてこのプ

50

プログラムを通常のコンピュータにインストールして実行するだけで、上記処理を容易に実現することができる。

【0053】

例えば、アクセス権限処理システム（分析受付GW1）は、上記プログラムをダウンロードし、ダウンロードしたプログラムを記憶し、プログラムのインストールを完了することができる。これにより、上記コンピュータに相当するアクセス権限処理システム（基本分析部3、アクセス制御部5等）は、インストールされた上記プログラムに基づき、上記処理を容易に実現することができる。

【0054】

また、アクセス権限処理システムは、コンピュータ読み取り可能な記憶媒体から上記プログラムを読み取り、読み取ったプログラムを記憶し、プログラムのインストールを完了することができる。これにより、アクセス権限処理システムは、インストールされた上記プログラムに基づき、上記処理を容易に実現することができる。

10

【0055】

その他にも、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。

【0056】

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。

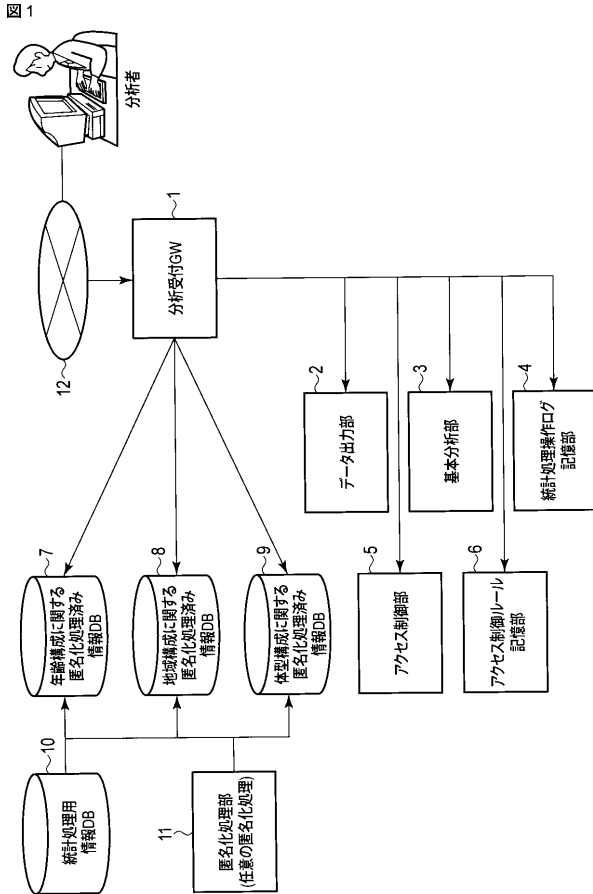
20

【符号の説明】

【0057】

1…分析受付GW、2…データ出力部、3…基本分析部、4…統計処理操作ログ記憶部、5…アクセス制御部、6…アクセス制御ルール記憶部、7…年齢構成に関する匿名化処理済み情報DB、8…地域構成に関する匿名化処理済み情報DB、9…体型構成に関する匿名化処理済み情報DB、10…統計処理用情報DB、11…匿名化処理部。

【図 1】



【図 3】

図 3

統計処理操作ログアクセス制御ルール

No.	どの母集団は	どういう用途で匿名化した情報を	どれだけ実施した	結果をどうした場合	どこからのアクセスの	どの組織の	誰であれば	当該母集団のどういう用途で匿名化した情報を	統計処理するかどうか
1	A年度 全国医療情報	どの用途でも	5種類	どうして	どこからでも	どの組織でも	だれでも	同一情報の別用途では	統計処理することはできない
2	B年度 〇×健康組合 医療情報	どの用途でも	4種類	どうして	どこからでも	どの組織でも	だれでも	同一情報の別用途では	統計処理することはできない
3	C年度 〇〇県 医療情報	どの用途でも	4種類	どうして	どこからでも	どの組織でも	だれでも	同一情報の別用途では	統計処理することはできない
4	すべての 情報を	どの用途でも	3種類	表で表示した	124.5 x 13	-	-	同一情報の別用途では	統計処理することはできない
5	すべての 情報を	どの用途でも	3種類	表で表示した	-	YY コンサルティング	だれでも	同一情報の別用途では	統計処理することはできない
6	C年度 〇〇県 医療情報	どの用途でも	4種類	どうして	-	Zz市役所	市ヶ谷良美	同一情報の別用途では	統計処理することはできない
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮

【図 2】

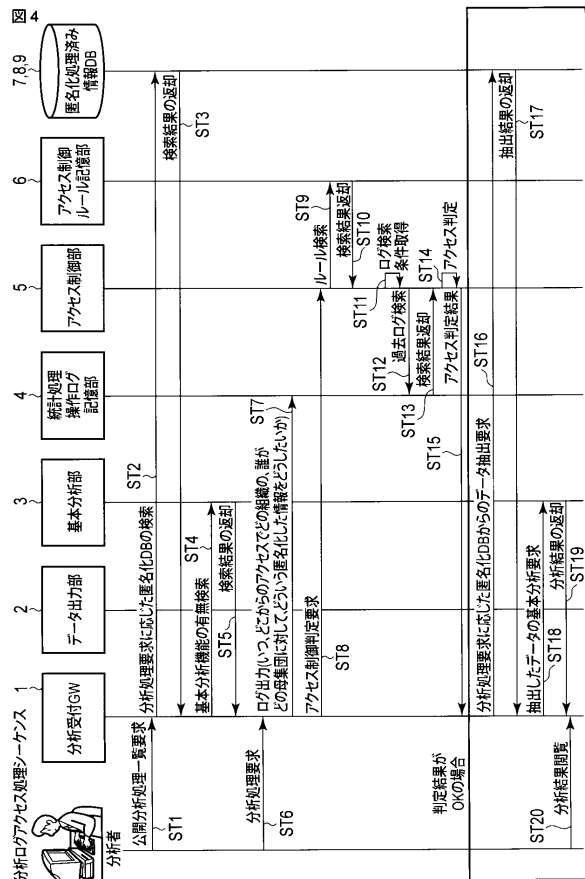
図 2

統計処理操作ログ構成要素

いつ	どこからのアクセスで	どの組織の	誰が	どの母集団に対して	どういう用途で匿名化した情報を	どうした	備考
2013/10/3	124.5 x 13	Xx研究所	氏名 a	A年度 全国医療情報	地域構成別 医療費統計	グラフにして 出力した	
2013/10/3	124.5 x 13	Xx研究所	氏名 a	A年度 全国医療情報	年代構成別 医療費統計	グラフにして 出力した	
2013/10/4	34 x 7.23	YYコンサルティング	氏名 b	B年度〇× 健康組合医療情報	年代構成別 医療費統計	表にして 出力した	
2013/10/4	34 x 7.23	YYコンサルティング	氏名 b	B年度〇× 健康組合医療情報	疾病構成別 医療費統計	表にして 出力した	
2013/10/23	217 x 4.87	Zz市役所	氏名 c	C年度〇〇 県医療情報	地域構成別 疾病件数	表にして 出力した	
2013/10/23	217 x 4.87	Zz市役所	氏名 c	C年度〇〇 県医療情報	性別構成別 疾病件数	表にして 出力した	
2013/10/23	217 x 4.87	Zz市役所	氏名 c	B年度〇〇 県医療情報	地域構成別 疾病件数	グラフにして 出力した	
2013/10/23	217 x 4.87	Zz市役所	氏名 c	B年度〇〇 県医療情報	性別構成別 疾病件数	グラフにして 出力した	
⋮	⋮	⋮	⋮	⋮	⋮	⋮	

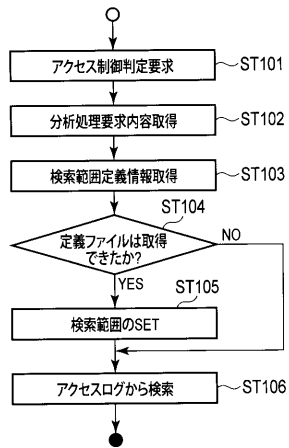
【図 4】

図 4



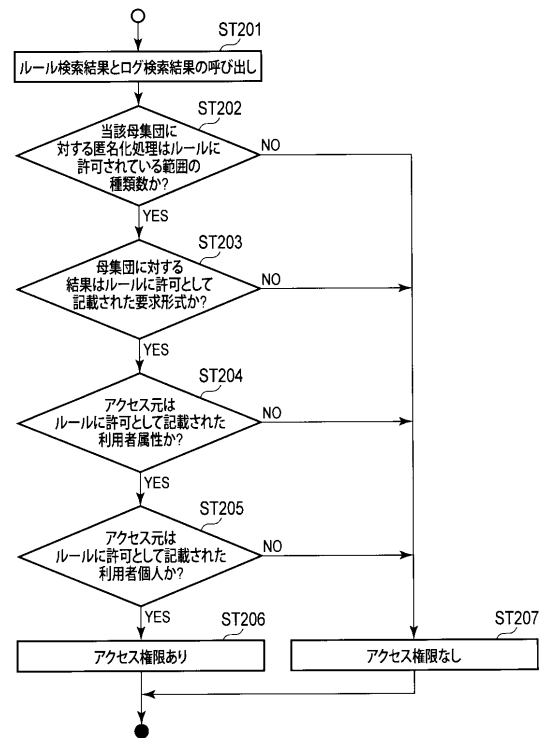
【図 5】

図 5



【図 6】

図 6



フロントページの続き

- (72)発明者 伊藤 良浩
東京都千代田区大手町一丁目5番1号 日本電信電話株式会社内
- (72)発明者 林 真弓
東京都千代田区大手町一丁目5番1号 日本電信電話株式会社内
- (72)発明者 池田 美穂
東京都千代田区大手町一丁目5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一丁目5番1号 日本電信電話株式会社内