

(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2011-253322

(P2011-253322A)

(43) 公開日 平成23年12月15日(2011.12.15)

(51) Int.Cl.

G06Q 50/00 (2006.01)

F I

G06F 17/60 154

テーマコード (参考)

審査請求 未請求 請求項の数 12 O L (全 11 頁)

(21) 出願番号 特願2010-126296 (P2010-126296)
 (22) 出願日 平成22年6月1日(2010.6.1)

(71) 出願人 591106392
 石津 隆
 埼玉県久喜市青葉4-7-6
 (71) 出願人 510152792
 外越 照仁
 埼玉県南埼玉郡宮代町2103-176
 (71) 出願人 510153021
 吉田 和男
 東京都江戸川区西小岩5-10-4
 (74) 代理人 100110652
 弁理士 塩野谷 英城
 (72) 発明者 石津 隆
 埼玉県久喜市青葉4-7-6

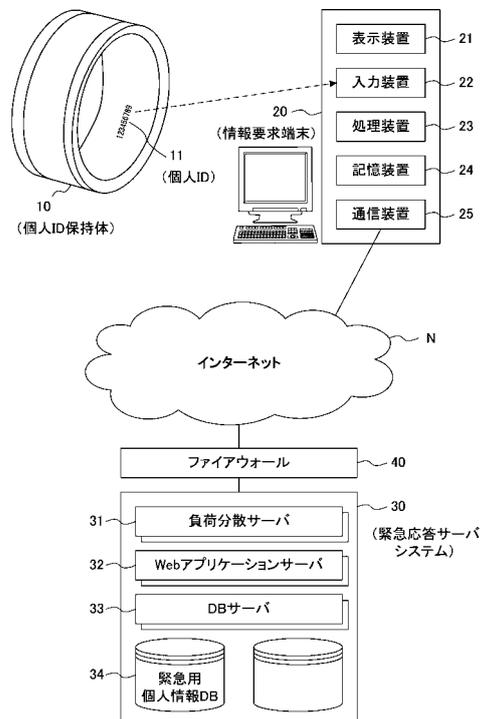
(54) 【発明の名称】 緊急時個人情報提供システムおよび方法

(57) 【要約】

【課題】意識不明等となった個人の個人情報を緊急に提供するシステムの実現。

【解決手段】本システムのユーザは、個人が身につける指輪等の個人ID保持体10から個人ID11を読み取り、情報要求端末20に与える。情報要求端末20は、緊急応答サーバ30に個人ID11を送信し個人ID11に対応する個人情報の提供を要求するが、緊急応答サーバ30は、情報要求端末20を操作するユーザを認証した上で、要求された個人情報を提供する。

【選択図】図1



【特許請求の範囲】**【請求項 1】**

個人IDに対応する個人情報を提供する緊急用個人情報提供システムであって、
個人を識別可能な個人IDを記録され当該個人が身につけるように構成された個人ID保持体と、

この個人ID保持体から読み取られた個人IDを緊急応答サーバシステムに送信する情報要求端末と、

各個人の個人IDと個人情報とを関連付けて記憶した緊急用個人情報DBを記憶装置に備え前記情報要求端末から送られた個人IDに対応する個人情報を前記緊急用個人情報DBから読み出して前記情報要求端末に提供する緊急応答サーバシステムとを備え、

前記情報要求端末は、前記緊急応答サーバシステムに送信する個人IDの所有者とは別人であるユーザの認証情報を前記緊急応答サーバシステムに送信し、

当該緊急応答サーバシステムは、同システムのユーザに予め発行した認証情報を記憶装置に記憶しており、前記情報要求端末から受信したユーザの認証情報と当該記憶装置に予め記憶している認証情報とが一致したことを条件として、前記個人IDに対応する個人情報を前記情報要求端末に提供し、

前記情報要求端末は、前記緊急応答サーバシステムから受信した個人情報を表示装置に表示する、緊急用個人情報提供システム。

【請求項 2】

前記個人ID保持体は、ネックレス、ブレスレット、指輪またはカードである、請求項1記載のシステム。

【請求項 3】

前記ユーザは、警察、消防署、病院、相談所または行政機関等の公の機関に所属するユーザである、請求項1又は2に記載のシステム。

【請求項 4】

前記個人情報は、保険証情報、本人証明写真、緊急連絡先、健康診断情報、身体検査情報、アレルギー情報、治療情報およびお薬手帳情報のうちの少なくとも1つを含む、請求項1乃至3のいずれかに記載のシステム。

【請求項 5】

前記ユーザの認証情報はユーザ毎に異なる値を発行する、請求項1乃至4のいずれかに記載のシステム。

【請求項 6】

前記緊急応答サーバシステムは、前記情報要求端末から個人情報を要求したユーザの識別情報と、当該個人情報に対応する個人IDと、当該要求に応じて個人情報を提供した日時とを関連付けて記憶装置内の情報提供ログに記録する、請求項5記載のシステム。

【請求項 7】

個人IDに対応する個人情報を提供する緊急用個人情報提供システムであって、
個人を識別可能な個人IDを記録され当該個人が身につけるように構成された個人ID保持体と、

この個人ID保持体から読み取られた個人IDを緊急応答サーバシステムに送信する情報要求端末と、

各個人の個人IDと個人情報とを関連付けて記憶した緊急用個人情報DBを記憶装置に備え前記情報要求端末から送られた個人IDに対応する個人情報を前記緊急用個人情報DBから読み出して前記情報要求端末に提供する緊急応答サーバシステムとを備えたシステムにおいて、

前記情報要求端末が、前記緊急応答サーバシステムに送信する個人IDの所有者とは別人であるユーザの認証情報を前記緊急応答サーバシステムに送信し、

当該緊急応答サーバシステムが、同システムのユーザに予め発行した認証情報を記憶装置に記憶しており、前記情報要求端末から受信したユーザの認証情報と当該記憶装置に予め記憶している認証情報とが一致したことを条件として、前記個人IDに対応する個人情

10

20

30

40

50

報を前記情報要求端末に提供し、

前記情報要求端末が、前記緊急応答サーバシステムから受信した個人情報を表示装置に表示する、緊急用個人情報提供方法。

【請求項 8】

前記個人 ID 保持体は、ネックレス、ブレスレット、指輪またはカードである、請求項 7 記載の方法。

【請求項 9】

前記ユーザは、警察、消防署、病院、相談所または行政機関等の公の機関に所属するユーザである、請求項 7 又は 8 に記載の方法。

【請求項 10】

前記個人情報は、保険証情報、本人証明写真、緊急連絡先、健康診断情報、身体検査情報、アレルギー情報、治療情報およびお薬手帳情報のうちの少なくとも 1 つを含む、請求項 7 乃至 9 のいずれかに記載の方法。

【請求項 11】

前記ユーザの認証情報はユーザ毎に異なる値を発行する、請求項 7 乃至 10 のいずれかに記載の方法。

【請求項 12】

前記緊急応答サーバシステムは、前記情報要求端末から個人情報を要求したユーザの識別情報と、当該個人情報に対応する個人 ID と、当該要求に応じて個人情報を提供した日時とを関連付けて記憶装置内の情報提供ログに記録する、請求項 11 記載の方法。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、特定の個人の個人情報が緊急に必要な場合、限られたユーザに対し、当該個人情報を提供するシステムに関する。

【背景技術】

【0002】

例えば急病人が救急車で病院に搬送される場合など、救急救命士などから個人情報の開示を求められる。しかし、その個人が自分の個人情報を自ら開示できない容体となっている場合がある。また、そこまでの容体でなくとも、自分の個人情報を自ら開示することが苦痛な容体となっている場合がある。

【0003】

この問題を解決する手段として、例えば特許文献 1 が開示されている。特許文献 1 では、請求項 14 に対応する発明において、利用者（意識不明者等）の電話機を第三者が操作し、短縮ダイヤルから緊急コールセンターに電話をかけると、その発信者番号から利用者が特定され、その利用者の個人情報が第三者に提供されるようになっている。その際、当該第三者は、利用者の電話機に表示される操作手順に従って短縮ダイヤルを発信する。

【0004】

しかし、これには以下の不都合を伴う。まず、第三者が緊急コールセンターの存在を事前に知っている必要がある。第三者が緊急コールセンターの存在を知らなければ、利用者の電話機を使って緊急コールセンターに電話をしようという行動を起させない。しかし、緊急コールセンターの存在を事前に知っているのは利用者だけであり、当該利用者に遭遇した第三者が緊急コールセンターの存在を事前に知っているとは限らない。また、第三者は使い慣れない他人（利用者）の電話機の操作に戸惑うだろう。電話機に短縮ダイヤルの操作手順を表示させるにしても、どうやってその操作手順を表示させたらよいか、第三者には分からないだろうし、そのような操作手順を表示できる特殊な電話機を利用者が持っていなければならない。そして、最大の問題は、利用者の電話機を操作できる第三者であれば、誰でも緊急コールセンターに電話をして利用者の個人情報を引き出せる可能性があるということである。利用者の容体とは関係なく、任意の第三者が利用者の電話機を利用し、偽って利用者の個人情報を引き出すおそれがある。このとき、第三者が偽れば、個

10

20

30

40

50

人情報を引き出した当該第三者を特定することができず、情報漏洩ルートの特定期間も困難となる。

【0005】

また、特許文献1では、請求項15に対応する発明において、第三者が任意の電話機から緊急コールセンターに発信し、利用者（意識不明者等）の身に付けた認識票に表示された登録ID番号を伝えると、当該利用者の個人情報が緊急コールセンターから第三者に提供されるようになっている。ここで、認識票はペンダント、ブレスレット、カードやシール等である。

【0006】

しかし、これにも以下の不都合を伴う。上記と同様に、第三者が緊急コールセンターの存在を事前に知っている必要がある。第三者が緊急コールセンターの存在を知らなければ、緊急コールセンターに電話をしようという行動を起こせない。しかし、緊急コールセンターの存在を事前に知っているのは利用者だけであり、当該利用者に遭遇した第三者が緊急コールセンターの存在を事前に知っているとは限らない。また、利用者の登録ID番号を知得した第三者であれば、誰でも緊急コールセンターに電話をして利用者の個人情報を引き出せる可能性がある。利用者の容体とは関係なく、任意の第三者が利用者の登録ID番号を利用し、偽って利用者の個人情報を引き出すおそれがある。登録ID番号を第三者に見つけてもらうために、利用者は認識票を見つけやすい個所に常時身に付けている必要があり、認識票に表示された登録ID番号は他人に知得されやすい。

10

【先行技術文献】

20

【特許文献】

【0007】

【特許文献1】特開2008-79082号公報

【発明の概要】

【発明が解決しようとする課題】

【0008】

本発明では、意識不明者等の個人情報を取得しようとする者が、当該個人情報を提供するセンターの存在を必ず事前に知っているようにし、かつ、個人を特定するIDが第三者に知られても、個人情報を取得する権限を持つ者だけが個人情報を取得できるようにすることを課題とする。

30

【課題を解決するための手段】

【0009】

この課題を解決するため、本発明では、まず、個人を識別可能な個人IDを記録され、当該個人が身につけるように構成された個人ID保持体を用いる。また、この個人ID保持体から読み取られた個人IDを緊急応答サーバシステムに送信する情報要求端末を用いる。さらに、各個人の個人IDと個人情報とを関連付けて記憶した緊急用個人情報DBを記憶装置に備え、情報要求端末から送られた個人IDに対応する個人情報を緊急用個人情報DBから読み出して情報要求端末に提供する緊急応答サーバシステムを備える。

【0010】

そして個人情報を取得する際、情報要求端末は、緊急応答サーバシステムに送信する個人IDの所有者とは別人であるユーザの認証情報を前記緊急応答サーバシステムに送信する。当該緊急応答サーバシステムは、同システムのユーザに発行した認証情報を記憶装置に予め記憶しており、情報要求端末から受信したユーザの認証情報と当該記憶装置に予め記憶している認証情報とが一致したことを条件として、個人IDに対応する個人情報を情報要求端末に提供する。情報要求端末は、緊急応答サーバシステムから受信した個人情報を表示装置に表示する。

40

【発明の効果】

【0011】

本発明によれば、特定の個人（意識不明者等）の個人情報を取得しようとする正規のユーザは、緊急応答サーバシステムにログインするための認証情報を予め発行されており、

50

当然に、緊急応答サーバシステムの存在を事前に知っており、緊急応答サーバシステムから個人情報を取得する方法も事前に知っている。よって、個人IDに基づいて緊急応答サーバから個人情報を取得する操作をスムーズに行うことができ、緊急の状況において必要な個人情報を速やかに取得することができる。また、正規のユーザは緊急応答サーバシステムにログインするための認証情報を予め発行されており、同システムの認証を受けなければシステムを利用できないので、人目に付きやすい個人IDが他人に知られても、その他人が本システムの正規ユーザでない限り、個人情報を取得することはできない。

【図面の簡単な説明】

【0012】

【図1】図1は緊急時個人情報提供システムの全体構成図である。

10

【図2】図2は緊急用個人情報DBのデータ構造図である。

【図3】図3は緊急時個人情報提供システムの動作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】

【0013】

[本実施形態の概要]

【0014】

まず図1に基づいて本実施形態の概要を説明する。例えば意識不明となった病人が救急搬送される場合、その病人の処置に必要な個人情報を緊急応答サーバシステム30から取得する。このため、例えば救急救命士が情報要求端末20から緊急応答サーバシステム30にログインし、病人が身に付ける指輪等の個人ID保持体10から個人ID11を読み取り、読み取った個人ID11を情報要求端末20から緊急応答サーバシステム30に送信する。

20

【0015】

緊急応答サーバシステム30は、受信した個人ID11に関連付けられた個人情報を緊急用個人情報DB34から検索し、検索結果を情報要求端末20に送信する。情報要求端末20は緊急応答サーバシステム30から受信した個人情報を表示する。

【0016】

これにより、救急救命士は、病人の処置に役立つ個人情報を速やかに得ることができる。この利用シーンにおいて、救急救命士は、緊急応答サーバシステム30にログインするための認証情報を事前に知っており、緊急応答サーバシステム30の存在も事前に知っている。病人が個人ID保持体10を身に付けているか否かをすぐに探し、病人が個人ID保持体10を身に付けていれば、緊急応答サーバシステム30を利用して速やかに病人の個人情報を取得できる。また、本システムの正規のユーザでは無い者が個人ID保持体10から個人ID11を取得したとしても、緊急応答サーバシステム30にログインするための認証情報を知らなければ、個人情報を不正に取得することはできない。

30

【0017】

上記の利用シーンは一例であり、種々のバリエーションについては後述する。

【0018】

[本実施形態のシステム構成]

【0019】

図1を参照しながら本実施形態のシステム構成を説明する。指輪等の個人ID保持体10には、個人ID11が表示されている。個人ID11は、各個人間で重複しない識別コードであり、情報要求端末20の入力装置から入力可能なデータにより構成されている。

40

【0020】

情報要求端末20は、コンピュータまたはコンピュータ機器であり、コンピュータディスプレイなどの表示装置21、キーボードなどの入力装置22、CPUなどの処理装置23、物理メモリやストレージなどの記憶装置24、およびインターネットNに接続するためのモデム等の通信装置25を備えている。

【0021】

処理装置23は、記憶装置24に格納されたOSを実行し、そのOS上でインターネッ

50

トブラウザを実行することによって、緊急応答サーバシステム30との間でデータ通信を行う。

【0022】

一方、緊急応答サーバシステム30は、ファイアウォール40を介してインターネットNに接続されている。ファイアウォール40は、Webアクセスの通信を許可しその他の侵入を拒否する通常のファイアウォールと、Webアクセスのデータをチェックしてアクセスの許否を決定するWebアプリケーションファイアウォールとの両方を備え、個人情報の不正な取得を防止する。

【0023】

緊急応答サーバシステム30は、負荷分散サーバ31と、Webアプリケーションサーバ32と、DBサーバ33と、緊急用個人情報DB34を含む記憶装置とを備え、各要素が2重化またはクラスタリングされることにより、システムの高可用性を実現し、ユーザから見てシステムが停止することなく、緊急時に確実に利用できるように構成されている。

【0024】

Webアプリケーションサーバ32は、ユーザのログイン要求に対する認証処理を実行する。また、Webアプリケーションサーバ32は、情報要求端末20からの要求に基づいて、DBサーバ33へ検索条件を入力する処理と、検索結果を情報要求端末20へ送信する処理等を実行する。

【0025】

DBサーバ33は、Webアプリケーションサーバ32から入力された検索条件に従って緊急用個人情報DB34を検索し、検索結果をWebアプリケーションサーバ32に返す。

【0026】

各サーバ31～33は、CPU等の処理装置がプログラムを実行することによって実現される。緊急用個人情報DB34を格納する記憶装置には、本システムにログインするユーザを認証するためのログインIDおよびパスワード等の認証情報も格納されている。情報要求端末20と緊急応答サーバシステム30との間の通信は、個人情報保護のためデータを暗号化して行う。

【0027】

[個人ID保持体の例]

【0028】

個人ID保持体10は、個人が意識することなく身につけていられる物であることが好ましく、指輪、ブレスレット、ネックレス、カード等が考えられる。

【0029】

[個人ID保持体への個人IDの記録方法]

【0030】

個人ID11は、個人ID保持体10に可視的に表示してもよいし、個人ID保持体10に添付したICチップにデータとして記録してもよい。後者の場合、情報要求端末20の入力装置22として、ICカードリーダーが必要となる。また、1次元または2次元のバーコードに変換した個人ID11を可視的に表示してもよい。個人ID11を2次元バーコードに変換して表示する場合、当該2次元バーコードに緊急応答サーバシステム30のURLを含めることもでき、例えば携帯カメラで撮影した2次元バーコードに基づいて、緊急応答サーバ30へのアクセスと個人ID11の送信とを同時に行うことも可能である。また、人体を個人ID保持体10と考え、個人ID11として指紋や静脈パターンを用いることも考えられる。

【0031】

[情報要求端末の種類]

【0032】

情報要求端末20は、デスクトップ型のコンピュータに限られず、ノート型コンピュー

10

20

30

40

50

タや、携帯電話機、スマートフォン、PDA等の携帯型コンピュータ機器でもよい。通信装置25は、情報要求端末20の種類に応じて、インターネットNへ接続するための有線通信装置または無線通信装置から選択される。

【0033】

[緊急用個人情報DBの構造]

【0034】

緊急応答サーバシステム30の緊急用個人情報DB34は、各個人の個人ID11と当該個人の個人情報とを関連付けて格納している。図2は、個人ID11に関連付けられる個人情報の例を示している。個人ID11に関連付けられる個人情報は、保険証情報51と、本人写真画像データ52と、緊急連絡先情報53と、健康診断情報(身体検査情報)54とを含む。さらに、アレルギー情報55と、治療情報56と、お薬手帳情報57とを含む。

10

【0035】

保険証情報51は、記号番号、氏名、生年月日、性別、住所および保険者番号を含む。緊急連絡先情報53は、複数登録することができ、例えば親族の連絡先、職場の連絡先、弁護士・行政書士・税理士等の専門家の連絡先を含む。健康診断情報(身体検査情報)54は、最近に受けた健康診断や身体検査の結果情報を含み、血液型も含まれる。アレルギー情報55は、副作用等の理由により本人に使用することができない薬品等の情報を含む。治療情報56は、現在治療中の病気や怪我について、かかりつけの病院の情報や当該病気や怪我の情報を含む。さらに、治療情報は、過去に治療した病気や怪我について、かかった病院の情報や当該病気や怪我の情報を含む。お薬手帳情報57は、現在服用中の薬の情報と、過去に服用した薬の情報とを含む。その他の個人情報が個人ID11に関連付けられていてもよい。

20

【0036】

[個人IDの発行と個人情報の登録]

【0037】

緊急応答サーバシステム30に個人情報を登録する個人は、緊急応答サーバシステム30における個人情報の取り扱い規約に同意した上で、緊急用個人情報DB34への掲載を許可する個人情報だけを本システムに登録する。図2に示した個人情報の一部だけの開示でもよい。

30

【0038】

登録の方法は幾つか考えられる。例えば、個人情報を登録したい本人が端末から緊急応答サーバシステム30にアクセスし、個人情報を直接入力してもよい。この場合、緊急応答サーバシステム30は、入力された個人情報に関連付ける個人IDを発行し、当該発行した個人IDと入力された個人情報とを関連付けて緊急用個人情報DB34に登録する。この場合、悪戯による個人情報の登録を防止するために、本システムの利用料金を本人名義のクレジットカードで決済させることが考えられる。

【0039】

また、他の方法として、個人情報を登録したい本人は、当該個人情報と本人確認書類とを運営会社に提出し、運営会社のオペレータが端末から緊急応答サーバシステム30にアクセスし、個人情報を入力してもよい。運営会社は、本人確認書類により個人情報の信頼性を判断した後、当該個人情報に関連付ける個人IDを発行する。オペレータは、発行された個人IDと個人情報とを関連付けて緊急用個人情報DB34に登録する。

40

【0040】

上記のいずれの場合でも、個人IDを発行した場合、その個人IDを記録した個人ID保持体を製作し、その個人IDの保有者に送付する。

【0041】

[本システムのユーザ]

【0042】

本システムのユーザ(情報要求端末20から緊急応答サーバシステム30にアクセスで

50

きるユーザ)は、特定の公の機関に所属する者に制限する。特定の公の機関とは、例えば、警察、消防署、病院、相談所、行政等である。

【0043】

本システムのユーザをこれらに制限するために、ユーザには緊急応答サーバシステム30へログインするための認証情報を運営会社から予め配布し、かつ緊急応答サーバシステム30の存在と利用方法も周知しておく。

【0044】

認証情報は、例えばログインIDとログインパスワードとから構成される。認証情報は、ユーザ間で共通の値を用いることも可能ではあるが、ユーザ毎に異なる値を発行することが好ましい。認証情報としてユーザ毎に異なる値を発行しておけば、あるユーザの認証情報が流出したとしても、そのユーザの認証情報だけを無効にすることで、他のユーザには影響を与えずに本システムの利用を継続させることができる。また、ユーザ毎に異なる認証情報を与えることによって、どのユーザにどの個人情報を提供したかというトラッキングを行うことができ、個人情報が流出した場合に、流出のルートを特定しやすくなる。

10

【0045】

[本実施形態の動作]

【0046】

次に、図3に基づいて本実施形態の動作を説明する。

【0047】

本システムの動作は、情報要求端末20と緊急応答サーバシステム30(以下、緊急応答サーバ30という)とが通信することによって実現する。前述したように本システムの利用シーンは種々考えられ、例えば、警察、消防署または病院が行う個人の人命救助、人物確認または応急処置に必要な個人情報を緊急に本システムからユーザへ提供し、さらにユーザが、提供された個人情報を利用し、本人の保護者、身元引受人や家族等の連絡先へ連絡をすることにも利用される。

20

【0048】

以下の動作説明では、分かりやすくするために、意識不明者が病院に救急搬送される場合を例として説明する。また、個人ID保持体10は指輪とし、情報要求端末20は、救急車両に装備されたモバイル通信端末とする。

【0049】

意識不明者(以下、病人という)のもとに救急車両が到着すると、本システムのユーザである救急救命士(以下、ユーザという)は、通常の救命処置に加え、病人の個人ID保持体10である指輪を外し、そこに記録された個人ID11を読み取る(S1)。次いで、ユーザは、救急車両に装備された情報要求端末20に緊急応答サーバ30への接続を指示する。例えば、情報要求端末20においてインターネットブラウザを起動し、ブラウザに予め登録された緊急応答サーバ30にアクセスするためのブックマークを開くことによって、緊急応答サーバ30への接続を指示する。情報要求端末20は、この指示を受けて緊急応答サーバ30に接続リクエストを送信する(S2)。このリクエストを受けた緊急応答サーバ30は、当該リクエストへの応答として、ユーザ認証情報の入力画面を表示するプログラムを記憶装置から読み出し、情報要求端末20に送信する(S3)。情報要求端末20は、ユーザ認証情報の入力画面を表示するプログラムを実行し、表示装置21にユーザ認証情報の入力画面を表示する(S4)。ユーザは、入力装置22を操作し、自分に与えられているユーザ認証情報を、入力画面に入力する。情報要求端末20は、入力されたユーザ認証情報を緊急応答サーバ30に送信する(S5)。緊急応答サーバ30は、情報要求端末20から受信した認証情報を、記憶装置に登録されているユーザ認証情報と照合する(S6)。認証情報が一致した場合は、情報要求端末20に、個人ID入力画面の表示プログラムを送信する(S7)。

30

40

【0050】

情報要求端末20は、受信した個人ID入力画面の表示プログラムを実行し、個人ID入力画面を表示装置21に表示する(S8)。

50

【 0 0 5 1 】

ユーザは、入力装置 2 2 を操作し、病人の個人 ID 保持体 1 0 から読み取った個人 ID 1 1 を入力画面に入力する。情報要求端末 2 0 は、入力された個人 ID 1 1 を緊急応答サーバ 3 0 に送信する (S 9)。緊急応答サーバ 3 0 は、情報要求端末 2 0 から受信した個人 ID 1 1 を、緊急用個人情報 DB 3 4 に登録されている個人 ID と照合する。個人 ID が一致した場合、当該個人 ID に関連付けられている個人情報を緊急用個人情報 DB 3 4 から読み出し、情報要求端末 2 0 に送信する (S 1 1)。

【 0 0 5 2 】

情報要求端末 2 0 は、緊急応答サーバ 3 0 から受信した個人情報を表示装置 2 1 に表示する (S 1 2)。ユーザである救急救命士は、表示装置 2 1 に表示された病人の個人情報を確認し、救命処置に利用する。また、個人情報に含まれる緊急連絡先に連絡をしてもよい。

10

【 0 0 5 3 】

一方、緊急応答サーバ 3 0 は、個人情報を要求したユーザの認証情報と、そのユーザに提供した個人情報に対応する個人 ID と、その個人情報を提供した日時とを関連付けて記憶装置内の情報提供ログに記録する (S 1 3)。例えば個人情報の流出事件が起きた場合に、情報提供ログを確認することによって、個人情報の流出元となったユーザを特定しやすくなる。以上により個人情報の要求に対する単位処理を完了する。実際には、沢山の情報要求端末 2 0 と沢山のユーザが存在し、緊急応答サーバ 3 0 には、個人情報を要求する多数のリクエストが送信される。緊急応答サーバ 3 0 は、個人情報を要求するリクエスト毎に、図 3 のフローチャートに示す単位処理をマルチタスクで実行する。

20

【 0 0 5 4 】

以上の動作説明において、情報要求端末 2 0 のすべての動作は、処理装置 2 3 が記憶装置 2 4 に格納されたプログラム (一時的に格納されたプログラムを含む) を実行することによって実現される。プログラムは、処理の遂行にあたり、記憶装置 2 4 に格納された種々のデータ (一時的に格納されたデータを含む) を利用する。また、緊急応答サーバ 3 0 のすべての動作は、処理装置が負荷分散サーバ 3 1、Web アプリケーションサーバ 3 2 および DB サーバ 3 3 のプログラムを実行することにより実現される。プログラムは、処理の遂行にあたり、緊急用個人情報 DB 3 4 を含む記憶装置内の種々のデータを利用する。

30

【 0 0 5 5 】

以上の動作説明では、救急救命士がユーザとなって本システムを利用するシーンを説明したが、本システムの利用シーンはこれに限らない。例えば救急救命士がユーザである病院の医師の指示で個人 ID を取得し、この個人 ID をユーザである医師に報告し、ユーザである医師が病院に設置された情報要求端末 2 0 から本システムを利用してもよい。

【 0 0 5 6 】

以上説明した本実施形態によれば、本システムのユーザは、本システムを利用するための認証情報を事前に取得しており、当然に本システムの存在と使用方法も知っているので、緊急事態に遭遇したユーザは、病人等の個人情報を必要とする場合に、当該病人等の身につけている個人 ID 保持体 1 0 を探し、そこから個人 ID 1 1 を取得し、本システムを利用して個人情報を取得する、という手順をスムーズに行うことができる。

40

【 0 0 5 7 】

また、本システムから個人情報を取得するためには、個人 ID を知っているだけでは足りず、本システムを利用するためのユーザ認証情報を知っている必要がある。よって、他人に個人 ID を知られたとしても、その他人が本システムを利用するための認証情報を知らない限り、個人情報が不正に引き出されることはない。

【 0 0 5 8 】

また、緊急応答サーバ 3 0 が情報提供ログを作成するので、個人情報の漏えいが起きた場合でも、情報提供ログを確認することによって、情報漏えいルートの特定が比較的容易になる。

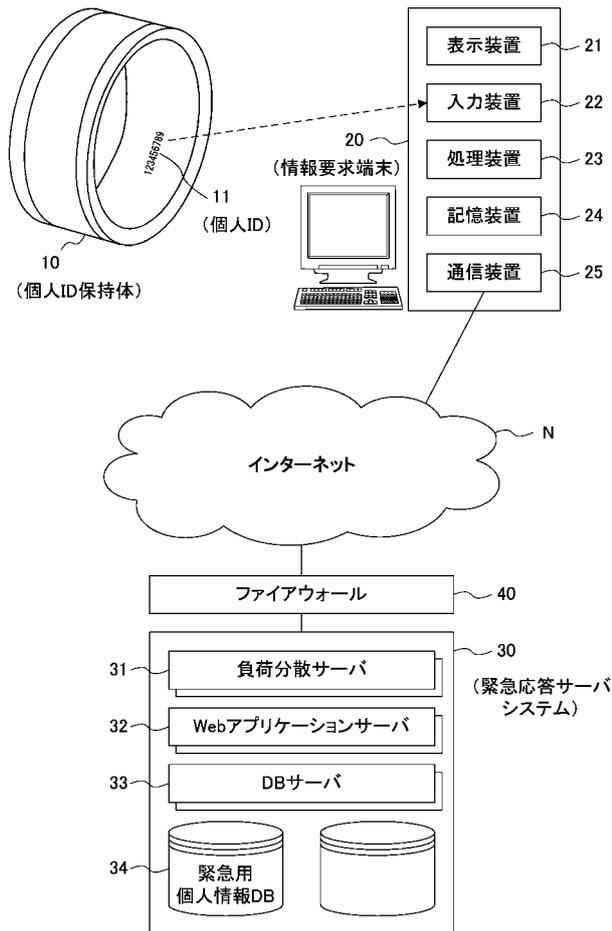
50

【符号の説明】

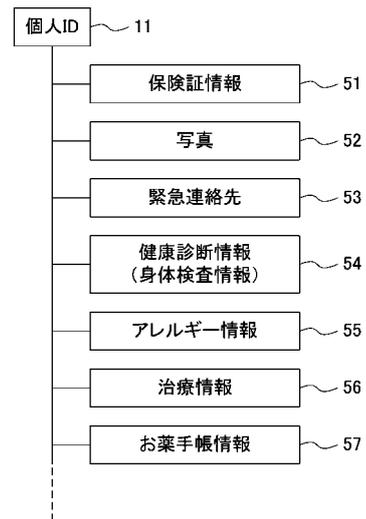
【0059】

- 10 個人ID保持体
- 11 個人ID
- 20 情報要求端末
- 21 表示装置
- 22 入力装置
- 23 処理装置
- 24 記憶装置
- 25 通信装置
- 30 緊急応答サーバシステム
- 31 負荷分散サーバ
- 32 Webアプリケーションサーバ
- 33 DBサーバ
- 34 緊急用個人情報DB

【図1】



【図2】



【 図 3 】

