

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第6032396号
(P6032396)

(45) 発行日 平成28年11月30日 (2016. 11. 30)

(24) 登録日 平成28年11月4日 (2016. 11. 4)

(51) Int. Cl.	F 1				
G06F 21/62	(2013. 01)	G06F	21/62	3 4 5	
G06F 21/31	(2013. 01)	G06F	21/31		
G06F 21/44	(2013. 01)	G06F	21/44		
G06Q 50/24	(2012. 01)	G06Q	50/24		

請求項の数 12 (全 24 頁)

(21) 出願番号	特願2012-117274 (P2012-117274)	(73) 特許権者	899000057 学校法人日本大学 東京都千代田区九段南四丁目8番24号
(22) 出願日	平成24年5月23日 (2012. 5. 23)	(74) 代理人	100119677 弁理士 岡田 賢治
(65) 公開番号	特開2013-30157 (P2013-30157A)	(74) 代理人	100115794 弁理士 今下 勝博
(43) 公開日	平成25年2月7日 (2013. 2. 7)	(72) 発明者	木原 雅巳 東京都千代田区九段南四丁目8番24号 学校法人日本大学内
審査請求日	平成27年5月1日 (2015. 5. 1)	審査官	平井 誠
(31) 優先権主張番号	特願2011-140887 (P2011-140887)		
(32) 優先日	平成23年6月24日 (2011. 6. 24)		
(33) 優先権主張国	日本国 (JP)		

最終頁に続く

(54) 【発明の名称】 非公開情報閲覧方法及び非公開情報閲覧システム

(57) 【特許請求の範囲】

【請求項1】

第1の端末が、特定の者に関する非公開情報をコンテンツサーバに登録する非公開情報登録ステップと、

前記第1の端末が、前記非公開情報の閲覧を許可するか否かを表示し、前記非公開情報の閲覧を許可する旨を取得する閲覧許可ステップと、

前記第1の端末と異なる第3の端末が暗証番号を取得して記憶し、当該暗証番号及び前記非公開情報を特定する情報を前記コンテンツサーバに送信し、前記コンテンツサーバが、前記第3の端末が前記特定の者に関連付けられた正規の端末であることを確認し、前記暗証番号を前記非公開情報に関連付けて記憶する暗証番号記憶ステップと、

前記第1の端末及び前記第3の端末とは異なる第2の端末が前記コンテンツサーバに記憶されている前記特定の者に関する非公開情報にアクセスするとともに前記暗証番号記憶ステップで前記第3の端末が記憶した暗証番号を取得して送信し、前記コンテンツサーバが、前記第2の端末から暗証番号を受信し、前記第2の端末が予め定められた正規の端末でありかつ受信した前記暗証番号が前記特定の者の非公開情報に関連付けられていることを確認し、当該確認ができた場合に前記特定の者の非公開情報を前記第2の端末に送信する暗証番号照合型非公開情報送信ステップと、

を順に有する非公開情報閲覧方法。

【請求項2】

前記暗証番号記憶ステップにおいて、前記非公開情報を前記暗証番号で暗号化し、

前記暗証番号照合型非公開情報送信ステップにおいて、前記確認ができた場合に前記暗証番号を用いて前記特定の者の非公開情報を復号化して前記第2の端末に送信する、ことを特徴とする請求項1に記載の非公開情報閲覧方法。

【請求項3】

前記閲覧許可ステップ以降前記暗証番号照合型非公開情報送信ステップの前までに、前記第1の端末が、前記非公開情報の閲覧を許可する旨を前記コンテンツサーバに登録することを特徴とする請求項1又は2に記載の非公開情報閲覧方法。

【請求項4】

第1の端末が、特定の者に関する非公開情報をコンテンツサーバに登録する非公開情報登録ステップと、

前記第1の端末が、前記非公開情報の閲覧を許可するか否かを表示し、前記非公開情報の閲覧を許可する旨を取得する閲覧許可ステップと、

前記第1の端末と異なる第3の端末が、当該第3の端末の記憶している前記特定の者に関する情報である利用者情報及び前記非公開情報を特定する情報を前記コンテンツサーバに送信し、前記コンテンツサーバが、前記第3の端末が前記特定の者に関連付けられた正規の端末であることを確認し、前記利用者情報を前記非公開情報に関連付けて記憶し、前記非公開情報を前記利用者情報で暗号化する利用者情報記憶ステップと、

前記第1の端末及び前記第3の端末とは異なる第2の端末が前記コンテンツサーバに記憶されている前記特定の者に関する非公開情報にアクセスし、前記コンテンツサーバが、前記第3の端末から前記利用者情報を受信し、前記第2の端末が予め定められた正規の端末でありかつ受信した前記利用者情報が前記特定の者の非公開情報に関連付けられていることを確認し、当該確認ができた場合に当該利用者情報を用いて前記特定の者の非公開情報を復号化して前記第2の端末に送信する利用者情報照合型非公開情報送信ステップと、を順に有する非公開情報閲覧方法。

【請求項5】

前記閲覧許可ステップ以降前記利用者情報照合型非公開情報送信ステップの前までに、前記第1の端末が、前記非公開情報の閲覧を許可する旨を前記コンテンツサーバに登録することを特徴とする請求項4に記載の非公開情報閲覧方法。

【請求項6】

前記非公開情報は、電子カルテであり、

前記第1の端末が、前記非公開情報の閲覧を許可する旨を前記コンテンツサーバに登録する際に、

スキャナが、カルテの属性情報を示すコードが付された透明ケースに前記カルテが格納された状態で、前記カルテ及び前記コードを画像データに変換する画像変換ステップと、

前記カルテの画像データの格納を承認する認証サーバが、前記カルテ及び前記コードの画像データから前記コードの画像を識別し、識別した前記コードの画像から前記カルテの属性情報を抽出し、抽出した前記カルテの属性情報を前記カルテの画像データの属性情報として設定する属性情報設定ステップと、

を順に有することを特徴とする請求項1から5のいずれかに記載の非公開情報閲覧方法。

【請求項7】

特定の者に関する非公開情報をコンテンツサーバに登録し、前記非公開情報の閲覧を許可するか否かを表示し、前記非公開情報の閲覧を許可する旨を取得する第1の端末と、

暗証番号を取得して記憶し、当該暗証番号及び前記非公開情報を特定する情報を前記コンテンツサーバに送信する、前記第1の端末とは異なる第3の端末と、

前記第1の端末から受信した前記非公開情報及び前記第3の端末から受信した前記暗証番号を格納し、前記第1の端末及び前記第3の端末とは異なる第2の端末がアクセスすると、前記第2の端末が予め定められた正規の端末でありかつ前記第2の端末から受信した暗証番号が前記特定の者の非公開情報に関連付けられていることを確認し、当該確認ができた場合に前記特定の者の非公開情報を前記第2の端末に送信するコンテンツサーバと、

10

20

30

40

50

前記コンテンツサーバに記憶されている前記特定の者に関する非公開情報にアクセスするとともに前記第 3 の端末の記憶している暗証番号を取得して送信し、前記コンテンツサーバから送信された前記特定の者の非公開情報を表示する前記第 1 の端末及び前記第 3 の端末とは異なる第 2 の端末と、

を備える非公開情報閲覧システム。

【請求項 8】

前記コンテンツサーバは、前記非公開情報及び前記暗証番号を格納する際に前記非公開情報を前記暗証番号で暗号化し、前記確認ができた際に前記暗証番号を用いて前記特定の者の非公開情報を復号化して前記第 2 の端末に送信することを特徴とする

請求項 7 に記載の非公開情報閲覧システム。

10

【請求項 9】

前記第 1 の端末が、前記非公開情報の閲覧を許可する旨を前記コンテンツサーバに登録することを特徴とする請求項 7 又は 8 に記載の非公開情報閲覧システム。

【請求項 10】

特定の者に関する非公開情報をコンテンツサーバに登録し、前記非公開情報の閲覧を許可するか否かを表示し、前記非公開情報の閲覧を許可する旨を取得する第 1 の端末と、

前記特定の者に関する情報である利用者情報を格納し、当該利用者情報及び前記非公開情報を特定する情報を前記コンテンツサーバに送信する、前記第 1 の端末と異なる第 3 の端末と、

前記第 1 の端末から受信した前記非公開情報及び前記第 3 の端末から受信した前記利用者情報を格納し、前記非公開情報を前記利用者情報で暗号化し、前記第 1 の端末及び前記第 3 の端末とは異なる第 2 の端末がアクセスすると、前記第 3 の端末から前記利用者情報を受信し、前記第 2 の端末が予め定められた正規の端末でありかつ受信した前記利用者情報が前記特定の者の非公開情報に関連付けられていることを確認し、当該確認ができた場合に当該利用者情報を用いて前記特定の者の非公開情報を復号化して前記第 2 の端末に送信するコンテンツサーバと、

20

前記コンテンツサーバに記憶されている前記特定の者に関する非公開情報にアクセスし、前記コンテンツサーバから送信された前記特定の者の非公開情報を表示する前記第 1 の端末及び前記第 3 の端末とは異なる第 2 の端末と、

を備える非公開情報閲覧システム。

30

【請求項 11】

前記第 1 の端末が、前記非公開情報の閲覧を許可する旨を前記コンテンツサーバに登録することを特徴とする請求項 10 に記載の非公開情報閲覧システム。

【請求項 12】

前記非公開情報は、電子カルテであり、

カルテの属性情報を示すコードが付された透明ケースに前記カルテが格納された状態で、前記カルテ及び前記コードを画像データに変換するスキャナをさらに備え、

前記コンテンツサーバは、前記カルテ及び前記コードの画像データから前記コードの画像を識別し、識別した前記コードの画像から前記カルテの属性情報を抽出し、抽出した前記カルテの属性情報を前記カルテの画像データの属性情報として設定することを特徴とする請求項 7 から 11 のいずれかに記載の非公開情報閲覧システム。

40

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、電子カルテなどの個人情報を含む非公開情報を第三者に閲覧させる非公開情報閲覧方法及び非公開情報閲覧システムに関する。

【背景技術】

【0002】

非公開情報としては、医療情報が記載されたカルテがある。カルテに記載された医療情報を第三者である紹介先の医師に閲覧させる場合、診察した医師が、患者といるいるな相

50

談をした上で、医療情報の記載された紹介状を作成して患者に手渡していた。そして、患者自身が、紹介状を紹介先の医師に手渡していた。従来の慣習では、この手順を踏むことで、診療した医師にとっても患者にとってもカルテが紹介先の医師以外の人に閲覧されない安心感を得ることができていた。このように、非公開情報は、情報の所有者が本人又は本人から依頼された人に紙の状態の手渡しされていた。

【0003】

一方で、カルテの電子化が進んでおり、電子カルテを閲覧可能にするシステムが提案されている（例えば、特許文献1及び2参照。）。

【0004】

特許文献1のシステムは、患者の診察内容を含む複数の異なる形式でそれぞれ作成された電子カルテを通信ネットワークを介して取得した電子カルテ管理サーバが、電子カルテ情報の項目を調整し、電子カルテの閲覧要求を受けると送信する。

10

【0005】

特許文献2のシステムは、紹介元の病院が出す紹介状情報と、紹介先の病院から出す診療情報の要求と、紹介元の病院から送る患者の診療情報と、をデータ管理サーバを介して送受信する。これにより、紹介先の医師によるカルテの閲覧を可能にしている。

【先行技術文献】

【特許文献】

【0006】

【特許文献1】特開2009-266077号公報

20

【特許文献2】特開2010-237834号公報

【発明の概要】

【発明が解決しようとする課題】

【0007】

特許文献1のシステムは、カルテをデータベース化しているが、患者の意思は考慮されていない。このため、特許文献1のシステムは、非公開情報の本人の安心感が得られない問題があった。

【0008】

特許文献2のシステムは、紹介先の医師がカルテを必要としているタイミングに紹介元の医師からカルテを送信する必要がある。このため、特許文献2のシステムは、非公開情報の所有者の負担になる問題があった。

30

【0009】

本発明は、非公開情報の本人の安心感が得られ、かつ非公開情報の所有者の負担にならない非公開情報閲覧方法及び非公開情報閲覧システムの提供を目的とする。

【課題を解決するための手段】

【0010】

前述の目的を達成するために、本願発明の非公開情報閲覧方法は、第1の端末が、特定の者に関する非公開情報をコンテンツサーバに登録する非公開情報登録ステップと、前記第1の端末が、前記非公開情報の閲覧を許可するか否かを表示し、前記非公開情報の閲覧を許可する旨を取得する閲覧許可ステップと、前記第1の端末又は前記コンテンツサーバが前記非公開情報を閲覧可能にするパスワードを発生させ、前記コンテンツサーバが前記パスワードを前記非公開情報に関連付けて記憶するパスワード記憶ステップと、前記第1の端末とは異なる第2の端末が前記コンテンツサーバに記憶されている前記特定の者に関する非公開情報にアクセスするとともに前記パスワード記憶ステップで発生させたパスワードを取得して送信し、前記コンテンツサーバが、前記第2の端末からパスワードを受信し、前記第2の端末が予め定められた正規の端末でありかつ受信した前記パスワードが前記特定の者の非公開情報に関連付けられていることを確認し、当該確認ができた場合に前記特定の者の非公開情報を前記第2の端末に送信するパスワード照合型非公開情報送信ステップと、を順に有する。

40

【0011】

50

本願発明の非公開情報閲覧方法は、非公開情報登録ステップと、閲覧許可ステップと、パスワード記憶ステップと、を有するため、非公開情報の本人と登録者との合意の上で、非公開情報の閲覧を許可する権限を前記特定の者に付与することができる。本願発明の非公開情報閲覧方法は、パスワード照合型非公開情報送信ステップを有するため、非公開情報の所有者が関与することなく前記特定の者の許可を取得するだけで、非公開情報を第2の端末で閲覧可能にすることができる。したがって、非公開情報の本人の安心感が得られ、かつ非公開情報の所有者の負担にならない非公開情報閲覧方法を提供することができる。

【0012】

本願発明の非公開情報閲覧方法では、前記パスワード記憶ステップにおいて、前記第1の端末が前記パスワードを発生させて表示するとともに前記コンテンツサーバに送信し、送信されたパスワードを前記コンテンツサーバが前記非公開情報に関連付けて記憶してもよい。

10

本発明は、非公開情報の登録者がパスワードを決定することができるため、非公開情報に直接関与した人がパスワードの管理をすることができる。

【0013】

また、本願発明の非公開情報閲覧方法では、前記パスワード記憶ステップにおいて、前記コンテンツサーバが前記パスワードを発生させて前記第1の端末に送信するとともに前記非公開情報に関連付けて記憶し、前記コンテンツサーバから送信された前記パスワードを前記第1の端末が表示してもよい。

20

本発明により、コンテンツサーバにおいてパスワードを一括管理することができるため、パスワードの重複を避けることができる。

【0014】

また、本願発明の非公開情報閲覧方法では、前記パスワード記憶ステップにおいて、前記コンテンツサーバが前記パスワードを発生させて前記第1の端末及び前記第2の端末とは異なる第3の端末に送信するとともに前記非公開情報に関連付けて記憶してもよい。

本発明により、コンテンツサーバにおいてパスワードを一括管理することができるため、パスワードの重複を避けることができる。さらに、第3の端末がパスワードを記憶するため、非公開情報の本人によるパスワードの紛失を防止することができる。

30

【0015】

本願発明の非公開情報閲覧方法では、前記閲覧許可ステップ以降前記パスワード照合型非公開情報送信ステップの前までに、前記第1の端末が、前記非公開情報の閲覧を許可する旨を前記コンテンツサーバに登録してもよい。

本発明により、非公開情報の登録者が許可しない情報については第三者による閲覧を防止することができる。

【0016】

前述の目的を達成するために、本願発明の非公開情報閲覧方法は、第1の端末が、特定の者に関する非公開情報をコンテンツサーバに登録する非公開情報登録ステップと、前記第1の端末が、前記非公開情報の閲覧を許可するか否かを表示し、前記非公開情報の閲覧を許可する旨を取得する閲覧許可ステップと、前記第1の端末と異なる第3の端末が暗証番号を取得して記憶し、当該暗証番号及び前記非公開情報を特定する情報を前記コンテンツサーバに送信し、前記コンテンツサーバが、前記第3の端末が前記特定の者に関連付けられた正規の端末であることを確認し、前記暗証番号を前記非公開情報に関連付けて記憶する暗証番号記憶ステップと、前記第1の端末及び前記第3の端末とは異なる第2の端末が前記コンテンツサーバに記憶されている前記特定の者に関する非公開情報にアクセスするとともに前記暗証番号記憶ステップで前記第3の端末が記憶した暗証番号を取得して送信し、前記コンテンツサーバが、前記第2の端末から暗証番号を受信し、前記第2の端末が予め定められた正規の端末でありかつ受信した前記暗証番号が前記特定の者の非公開情報に関連付けられていることを確認し、当該確認ができた場合に前記特定の者の非公開情報を前記第2の端末に送信する暗証番号照合型非公開情報送信ステップと、を順に有する

40

50

。 前記暗証番号記憶ステップにおいて、前記非公開情報を前記暗証番号で暗号化し、前記暗証番号照合型非公開情報送信ステップにおいて、前記確認ができた場合に前記暗証番号を用いて前記特定の者の非公開情報を復号化して前記第2の端末に送信してもよい。

【0017】

本願発明の非公開情報閲覧方法は、非公開情報登録ステップと、閲覧許可ステップと、暗証番号記憶ステップと、を有するため、非公開情報の本人と登録者との合意の上で、非公開情報の閲覧を許可する権限を前記特定の者に付与することができる。本願発明の非公開情報閲覧方法は、暗証番号照合型非公開情報送信ステップを有するため、非公開情報の所有者が関与することなく前記特定の者の許可を取得するだけで、非公開情報を第2の端
10
末で閲覧可能にすることができる。したがって、非公開情報の本人の安心感が得られ、かつ非公開情報の所有者の負担にならない非公開情報閲覧方法を提供することができる。

【0018】

本願発明の非公開情報閲覧方法では、前記閲覧許可ステップ以降前記暗証番号照合型非公開情報送信ステップの前までに、前記第1の端末が、前記非公開情報の閲覧を許可する旨を前記コンテンツサーバに登録してもよい。

本発明により、非公開情報の登録者が許可しない情報については第三者による閲覧を防止することができる。

【0019】

前述の目的を達成するために、本願発明の非公開情報閲覧方法は、第1の端末が、特定
20
の者に関する非公開情報をコンテンツサーバに登録する非公開情報登録ステップと、前記第1の端末が、前記非公開情報の閲覧を許可するか否かを表示し、前記非公開情報の閲覧を許可する旨を取得する閲覧許可ステップと、前記第1の端末と異なる第3の端末が、当該第3の端末の記憶している前記特定の者に関する情報である利用者情報及び前記非公開情報を特定する情報を前記コンテンツサーバに送信し、前記コンテンツサーバが、前記第3の端末が前記特定の者に関連付けられた正規の端末であることを確認し、前記利用者情報を前記非公開情報に関連付けて記憶し、前記非公開情報を前記利用者情報で暗号化する利用者情報記憶ステップと、前記第1の端末及び前記第3の端末とは異なる第2の端末が前記コンテンツサーバに記憶されている前記特定の者に関する非公開情報にアクセスし、
30
前記コンテンツサーバが、前記第3の端末から前記利用者情報を受信し、前記第2の端末が予め定められた正規の端末でありかつ受信した前記利用者情報が前記特定の者の非公開情報に関連付けられていることを確認し、当該確認ができた場合に当該利用者情報を用いて前記特定の者の非公開情報を復号化して前記第2の端末に送信する利用者情報照合型非公開情報送信ステップと、を順に有する。

【0020】

本願発明の非公開情報閲覧方法は、非公開情報登録ステップと、閲覧許可ステップと、利用者情報記憶ステップと、を有するため、非公開情報の本人と登録者との合意の上で、非公開情報の閲覧を許可する権限を前記特定の者に付与することができる。本願発明の非公開情報閲覧方法は、利用者情報照合型非公開情報送信ステップを有するため、非公開情報の所有者が関与することなく前記特定の者の許可を取得するだけで、非公開情報を第2
40
の端末で閲覧可能にすることができる。したがって、非公開情報の本人の安心感が得られ、かつ非公開情報の所有者の負担にならない非公開情報閲覧方法を提供することができる。

【0021】

本願発明の非公開情報閲覧方法では、前記閲覧許可ステップ以降前記利用者情報照合型非公開情報送信ステップの前までに、前記第1の端末が、前記非公開情報の閲覧を許可する旨を前記コンテンツサーバに登録してもよい。

本発明により、非公開情報の登録者が許可しない情報については第三者による閲覧を防止することができる。

【0022】

10

20

30

40

50

本願発明の非公開情報閲覧方法では、前記非公開情報は、電子カルテであり、前記第1の端末が、前記非公開情報の閲覧を許可する旨を前記コンテンツサーバに登録する際に、スキャナが、カルテの属性情報を示すコードが付された透明ケースに前記カルテが格納された状態で、前記カルテ及び前記コードを画像データに変換する画像変換ステップと、前記カルテの画像データの格納を承認する認証サーバが、前記カルテ及び前記コードの画像データから前記コードの画像を識別し、識別した前記コードの画像から前記カルテの属性情報を抽出し、抽出した前記カルテの属性情報を前記カルテの画像データの属性情報として設定する属性情報設定ステップと、を順に有してもよい。

本発明により、カルテを透明ケースに格納し、カルテを透明ケースに格納した状態で、スキャン開始指示をスキャナに与えるのみでよい。よって、カルテを画像データに変換するときに、画像データのファイル名を入力する必要がなくなる。そして、透明ケースを最初に準備すれば、透明ケースをその後使い回すことができる。さらに、透明ケースに付されたコードの位置は、カルテの更新の度に変更されることはないため、コードの画像を自動的に識別することができ、コードの認識率を高めることができる。

【0023】

前述の目的を達成するために、本願発明の非公開情報閲覧システムは、特定の者に関する非公開情報をコンテンツサーバに登録し、前記非公開情報の閲覧を許可するか否かを表示し、前記非公開情報の閲覧を許可する旨を取得する第1の端末と、前記第1の端末から受信した前記非公開情報及びパスワードを格納し、前記第1の端末とは異なる第2の端末がアクセスすると、前記第2の端末が予め定められた正規の端末でありかつ前記第2の端末から受信したパスワードが前記特定の者の非公開情報に関連付けられていることを確認し、当該確認ができた場合に前記特定の者の非公開情報を前記第2の端末に送信するコンテンツサーバと、前記コンテンツサーバに記憶されている前記特定の者に関する非公開情報にアクセスするとともに前記パスワードを取得して送信し、前記コンテンツサーバから送信された前記特定の者の非公開情報を表示する前記第1の端末とは異なる第2の端末と、を備える。

【0024】

本願発明の非公開情報閲覧システムは、第1の端末と、コンテンツサーバと、第2の端末と、を備えるため、非公開情報の所有者が関与することなく第2の端末の認証情報及びパスワードを入力するだけで、非公開情報を第2の端末で閲覧可能にすることができる。また、第1の端末が非公開情報の閲覧を許可する旨を取得した上でパスワードを発生させるため、非公開情報の本人と登録者との合意の上で、非公開情報の閲覧を許可する権限を前記特定の者に付与することができる。したがって、非公開情報の本人の安心感が得られ、かつ非公開情報の所有者の負担にならない非公開情報閲覧方法を提供することができる。

【0025】

本願発明の非公開情報閲覧システムでは、前記第1の端末が前記パスワードを発生させて表示するとともに前記コンテンツサーバに送信し、送信されたパスワードを前記コンテンツサーバが前記非公開情報に関連付けて記憶してもよい。

本発明は、非公開情報の登録者がパスワードを決定することができるため、非公開情報に直接関与した人がパスワードの管理をすることができる。

【0026】

本願発明の非公開情報閲覧システムでは、前記コンテンツサーバが前記パスワードを発生させて前記第1の端末に送信するとともに前記非公開情報に関連付けて記憶し、前記コンテンツサーバから送信された前記パスワードを前記第1の端末が表示してもよい。

本発明により、コンテンツサーバにおいてパスワードを一括管理することができるため、パスワードの重複を避けることができる。

【0027】

本願発明の非公開情報閲覧システムでは、前記コンテンツサーバが前記パスワードを発生させて前記第1の端末及び前記第2の端末とは異なる第3の端末に送信するとともに前

10

20

30

40

50

記非公開情報に関連付けて記憶してもよい。

本発明により、コンテンツサーバにおいてパスワードを一括管理することができるため、パスワードの重複を避けることができる。さらに、第3の端末がパスワードを記憶するため、非公開情報の本人によるパスワードの紛失を防止することができる。

【0028】

本願発明の非公開情報閲覧システムでは、前記第1の端末が、前記非公開情報の閲覧を許可する旨を前記コンテンツサーバに登録してもよい。

本発明により、非公開情報の登録者が許可しない情報については第三者による閲覧を防止することができる。

【0029】

前述の目的を達成するために、本願発明の非公開情報閲覧システムは、特定の者に関する非公開情報をコンテンツサーバに登録し、前記非公開情報の閲覧を許可するか否かを表示し、前記非公開情報の閲覧を許可する旨を取得する第1の端末と、暗証番号を取得して記憶し、当該暗証番号及び前記非公開情報を特定する情報を前記コンテンツサーバに送信する、前記第1の端末とは異なる第3の端末と、前記第1の端末から受信した前記非公開情報及び前記第3の端末から受信した前記暗証番号を格納し、前記第1の端末及び前記第3の端末とは異なる第2の端末がアクセスすると、前記第2の端末が予め定められた正規の端末でありかつ前記第2の端末から受信した暗証番号が前記特定の者の非公開情報に関連付けられていることを確認し、当該確認ができた場合に前記特定の者の非公開情報を前記第2の端末に送信するコンテンツサーバと、前記コンテンツサーバに記憶されている前記特定の者に関する非公開情報にアクセスするとともに前記第3の端末の記憶している暗証番号を取得して送信し、前記コンテンツサーバから送信された前記特定の者の非公開情報を表示する前記第1の端末及び前記第3の端末とは異なる第2の端末と、を備える。

前記コンテンツサーバは、前記非公開情報及び前記暗証番号を格納する際に前記非公開情報を前記暗証番号で暗号化し、前記確認ができた際に前記暗証番号を用いて前記特定の者の非公開情報を復号化して前記第2の端末に送信してもよい。

【0030】

本願発明の非公開情報閲覧システムは、第1の端末と、コンテンツサーバと、第2の端末と、を備えるため、非公開情報の所有者が関与することなく第2の端末の認証情報及び暗証番号を入力するだけで、非公開情報を第2の端末で閲覧可能にすることができる。また、第1の端末が非公開情報の閲覧を許可する旨を取得した上で第3の端末から暗証番号を送信するため、非公開情報の本人と登録者との合意の上で、非公開情報の閲覧を許可する権限を前記特定の者に付与することができる。したがって、非公開情報の本人の安心感が得られ、かつ非公開情報の所有者の負担にならない非公開情報閲覧方法を提供することができる。

【0031】

本願発明の非公開情報閲覧システムでは、前記第1の端末が、前記非公開情報の閲覧を許可する旨を前記コンテンツサーバに登録してもよい。

本発明により、非公開情報の登録者が許可しない情報については第三者による閲覧を防止することができる。

【0032】

前述の目的を達成するために、本願発明の非公開情報閲覧システムは、特定の者に関する非公開情報をコンテンツサーバに登録し、前記非公開情報の閲覧を許可するか否かを表示し、前記非公開情報の閲覧を許可する旨を取得する第1の端末と、前記特定の者に関する情報である利用者情報を格納し、当該利用者情報及び前記非公開情報を特定する情報を前記コンテンツサーバに送信する、前記第1の端末と異なる第3の端末と、前記第1の端末から受信した前記非公開情報及び前記第3の端末から受信した前記利用者情報を格納し、前記非公開情報を前記利用者情報で暗号化し、前記第1の端末及び前記第3の端末とは異なる第2の端末がアクセスすると、前記第3の端末から前記利用者情報を受信し、前記第2の端末が予め定められた正規の端末でありかつ受信した前記利用者情報が前記特定の

10

20

30

40

50

者の非公開情報に関連付けられていることを確認し、当該確認ができた場合に当該利用者情報を用いて前記特定の者の非公開情報を復号化して前記第2の端末に送信するコンテンツサーバと、前記コンテンツサーバに記憶されている前記特定の者に関する非公開情報にアクセスし、前記コンテンツサーバから送信された前記特定の者の非公開情報を表示する前記第1の端末及び前記第3の端末とは異なる第2の端末と、を備える。

【0033】

本願発明の非公開情報閲覧システムは、第1の端末と、コンテンツサーバと、第2の端末と、を備えるため、非公開情報の所有者が関与することなく第2の端末の認証情報及び利用者情報を入力するだけで、非公開情報を第2の端末で閲覧可能にすることができる。また、第1の端末が非公開情報の閲覧を許可する旨を取得した上で第3の端末から利用者情報を送信するため、非公開情報の本人と登録者との合意の上で、非公開情報の閲覧を許可する権限を前記特定の者に付与することができる。したがって、非公開情報の本人の安心感が得られ、かつ非公開情報の所有者の負担にならない非公開情報閲覧方法を提供することができる。

10

【0034】

本願発明の非公開情報閲覧システムでは、前記第1の端末が、前記非公開情報の閲覧を許可する旨を前記コンテンツサーバに登録してもよい。

本発明により、非公開情報の登録者が許可しない情報については第三者による閲覧を防止することができる。

【0035】

本願発明の非公開情報閲覧システムでは、前記非公開情報は、電子カルテであり、カルテの属性情報を示すコードが付された透明ケースに前記カルテが格納された状態で、前記カルテ及び前記コードを画像データに変換するスキャナをさらに備え、前記コンテンツサーバは、前記カルテ及び前記コードの画像データから前記コードの画像を識別し、識別した前記コードの画像から前記カルテの属性情報を抽出し、抽出した前記カルテの属性情報を前記カルテの画像データの属性情報として設定してもよい。

20

本発明により、カルテを透明ケースに格納し、カルテを透明ケースに格納した状態で、スキャン開始指示をスキャナに与えるのみでよい。よって、カルテを画像データに変換するときに、画像データのファイル名を入力する必要がなくなる。そして、透明ケースを最初に準備すれば、透明ケースをその後使い回すことができる。さらに、透明ケースに付されたコードの位置は、カルテの更新の度に変更されることはないため、コードの画像を自動的に識別することができ、コードの認識率を高めることができる。

30

【発明の効果】

【0036】

本発明によれば、非公開情報の本人の安心感が得られ、かつ非公開情報の所有者の負担にならない非公開情報閲覧方法及び非公開情報閲覧システムを提供することができる。

【図面の簡単な説明】

【0037】

【図1】本実施形態に係る非公開情報閲覧システムの一例を示す。

【図2】実施形態1に係る非公開情報閲覧システムのシーケンス図を示す。

【図3】実施形態2に係る非公開情報閲覧システムのシーケンス図を示す。

【図4】実施形態3に係る非公開情報閲覧システムのシーケンス図を示す。

【図5】実施形態4に係る非公開情報閲覧システムのシーケンス図を示す。

【図6】実施形態5に係る非公開情報閲覧システムのシーケンス図を示す。

【図7】実施形態6に係る非公開情報閲覧システムのシーケンス図を示す。

【図8】実施形態7に係る非公開情報閲覧システムのシーケンス図を示す。

【図9】実施形態8に係る非公開情報閲覧システムのシーケンス図を示す。

【図10】実施形態9に係る非公開情報閲覧システムのシーケンス図を示す。

【図11】画像データを格納する方法を示す図である。

【図12】認証サーバの構成を示す図である。

40

50

【発明を実施するための形態】**【0038】**

添付の図面を参照して本発明の実施形態を説明する。以下に説明する実施形態は本発明の実施の例であり、本発明は、以下の実施形態に制限されるものではない。なお、本明細書及び図面において符号が同じ構成要素は、相互に同一のものを示すものとする。

【0039】

図1に、本実施形態に係る非公開情報閲覧システムの一例を示す。第1の端末1、第2の端末2及び第3の端末3は、コンテンツサーバ4と通信ネットワーク5で接続されている。コンテンツサーバ4は、特定の者に関する非公開情報を格納する。第3の端末3は、特定の者の所有する携帯可能な移動端末であり、例えば、携帯電話、スマートフォン又はノートパソコンである。

10

【0040】

後述する実施形態1及び実施形態2に係る非公開情報閲覧システムは、第1の端末1と、第2の端末2と、コンテンツサーバ4と、を備える。後述する実施形態3から実施形態9に係る非公開情報閲覧システムは、第1の端末1と、第2の端末2と、第3の端末3と、コンテンツサーバ4と、を備える。

【0041】

本実施形態に係る非公開情報閲覧システムは、例えば、第1の端末1がコンテンツサーバ4に登録した電子カルテの情報を、第2の端末2で閲覧可能にする電子カルテ閲覧システムである。以下、本実施形態に係る非公開情報閲覧方法及び非公開情報閲覧システムが電子カルテ閲覧方法及び電子カルテ閲覧システムである場合について説明する。

20

【0042】**(実施形態1)**

図2に、実施形態1に係る非公開情報閲覧システムのシーケンス図を示す。本実施形態に係る非公開情報閲覧方法は、非公開情報登録ステップと、閲覧許可ステップと、パスワード記憶ステップと、パスワード照合型非公開情報送信ステップと、を順に有する。非公開情報登録ステップ、閲覧許可ステップ及びパスワード記憶ステップは、第1の医師による診察中に行う。パスワード照合型非公開情報送信ステップは、第2の医師による診察中に行う。

30

【0043】

非公開情報登録ステップでは、非公開情報閲覧システムは以下のように動作する。

第1の端末1が、特定の者に関する電子カルテをコンテンツサーバ4に登録する(S111)。例えば、第1の医師が、第1の端末1を用いて、新規患者のカルテをコンテンツサーバ4上に作成する。この患者の電子カルテがコンテンツサーバ4上に既に存在する場合は、最初のカルテの作成がこのステップに相当する。

【0044】

閲覧許可ステップでは、非公開情報閲覧システムは以下のように動作する。

第1の端末1が、電子カルテの閲覧を許可するか否かをディスプレイに表示する(S112)。第1の医師は、診察中の患者に、カルテを他の医師に開示してよいか否かの承諾を得る。承諾が得られたら、第1の医師は電子カルテの閲覧を許可する旨を第1の端末1に入力する。これにより、第1の端末1は、電子カルテの閲覧を許可する旨を取得し(S113)、電子カルテの閲覧を許可する旨をコンテンツサーバ4に登録する(S114)。コンテンツサーバ4は、電子カルテの閲覧を許可する旨を記憶する(S414)。このとき、閲覧を許可する第2の端末2を特定する。例えば、第2の端末2を使用する予定の第2の医師のもつIDを特定する。また、電子カルテのうちの公開してよい情報や公開してはいけない情報を指定する。

40

【0045】

ここで、第2の端末2がコンテンツサーバ4の所在を知らなかったり、第2の端末2にコンテンツサーバ4のアクセス権がない場合、第1の端末1は、コンテンツサーバ4にアクセスするのに必要なサーバ情報及び認証情報を、第2の端末2に通知する(S115)

50

。第2の端末2は、サーバ情報及び認証情報を受信して記憶する(S215)。この通知のタイミングは、閲覧許可ステップ以後パスワード照合型非公開情報送信ステップ前までの任意のタイミングで行うことができる。ステップS115及びステップS215を図示しない他の実施形態においても同様である。

【0046】

パスワード記憶ステップでは、非公開情報閲覧システムは以下のように動作する。

第1の端末1が電子カルテを閲覧可能にするパスワードを発生させ(S121)、ディスプレイに表示する。これにより、患者がパスワードを知ることができる。そして、第1の端末1がパスワードをコンテンツサーバ4に登録し(S122)、コンテンツサーバ4がパスワードを電子カルテに関連付けて記憶する(S422)。

10

【0047】

パスワード照合型非公開情報送信ステップでは、非公開情報閲覧システムは以下のように動作する。

患者が第2の医師の診察を受ける際、第2の端末2は、コンテンツサーバ4に記憶されているその患者の電子カルテにアクセスする。このとき、第2の端末2のディスプレイにパスワードを要求する旨が表示され、第2の医師は患者に対して電子カルテの閲覧許可の有無を問い合わせ(S224)、患者からの閲覧許可とともにパスワードを取得する(S225)。

【0048】

第2の端末2は、第2の端末2が正規の端末であることを示す認証情報と、患者から取得したパスワードをコンテンツサーバ4に送信する(S226)。コンテンツサーバ4は、受信した認証情報が正規の端末として登録されているか否かを確認する。そして、コンテンツサーバ4は、第2の端末2が予め定められた正規の端末でありかつ受信したパスワードが特定の者の電子カルテに関連付けられていることを確認する(S426)。この確認ができると、コンテンツサーバ4は、患者の電子カルテを第2の端末2に送信する(S427)。これにより、第2の端末2において患者の電子カルテの閲覧が可能になる(S227)。

20

【0049】

本実施形態に係る非公開情報閲覧システム及び非公開情報閲覧方法は、第1の医師と患者の双方の合意があったときにパスワードを発生させ、第2の医師に患者がパスワードを通知したときに電子カルテの閲覧が可能になる。このため、医師と患者の双方の合意とそれによる安心感が得られ、かつ紹介元の医師の負担の少ない非公開情報閲覧方法及び非公開情報閲覧システムを提供することができる。

30

【0050】

(実施形態2)

図3に、実施形態2に係る非公開情報閲覧システムのシーケンス図を示す。本実施形態に係る非公開情報閲覧方法は、パスワード記憶ステップが実施形態1と異なる。本実施形態では、異なる点のみ説明する。

【0051】

パスワード記憶ステップでは、非公開情報閲覧システムは以下のように動作する。

第1の端末1は、コンテンツサーバ4にパスワードを要求する(S131)。このパスワードの要求は、ステップS114と同時に行っても良い。コンテンツサーバ4は、この要求を受けると、パスワードを発生させて第1の端末1に送信し(S432)、パスワードを電子カルテに関連付けて記憶する(S433)。第1の端末1は、コンテンツサーバ4から送信されたパスワードを表示する(S132)。これにより、患者がパスワードを知ることができる。

40

【0052】

(実施形態3)

図4に、実施形態3に係る非公開情報閲覧システムのシーケンス図を示す。本実施形態に係る非公開情報閲覧方法は、パスワード記憶ステップ及びパスワード照合型非公開情報

50

送信ステップが実施形態 1 及び実施形態 2 と異なる。本実施形態では、異なる点のみ説明する。

【 0 0 5 3 】

パスワード記憶ステップでは、非公開情報閲覧システムは以下のように動作する。

第 1 の端末 1 は、コンテンツサーバ 4 にパスワードを要求する (S 1 4 1)。このパスワードの要求は、ステップ S 1 1 4 と同時に行っても良い。コンテンツサーバ 4 は、この要求を受けると、パスワードを発生させて第 3 の端末 3 に送信し (S 4 4 2)、パスワードを電子カルテに関連付けて記憶する (S 4 4 3)。第 3 の端末 3 は、コンテンツサーバ 4 から送信されたパスワードを受信して記憶する (S 3 4 2)。第 3 の端末 3 は患者の端末であるため、患者はパスワードを知ることができる。

10

【 0 0 5 4 】

パスワード照合型非公開情報送信ステップでは、非公開情報閲覧システムは以下のように動作する。

患者が第 2 の医師の診察を受ける際、第 2 の端末 2 は、コンテンツサーバ 4 に記憶されているその患者の電子カルテにアクセスする。このとき、第 2 の端末 2 のディスプレイにパスワードを要求する旨が表示され、第 2 の医師は患者に対して電子カルテの閲覧許可の有無を問い合わせ (S 2 4 4)、患者からの閲覧許可を取得する (S 2 4 5)。許可が得られたら、第 3 の端末 3 がパスワードを第 2 の端末 2 に送信し (S 3 4 6)、第 2 の端末 2 は第 3 の端末 3 からパスワードを受信する (S 2 4 6)。なお、第 3 の端末 3 がパスワードを表示し、表示されたパスワードを第 2 の端末 2 が取得してもよい。

20

【 0 0 5 5 】

第 2 の端末 2 は、第 2 の端末 2 が正規の端末であることを示す認証情報と、第 3 の端末 3 から受信したパスワードをコンテンツサーバ 4 に送信する (S 2 4 7)。コンテンツサーバ 4 は、第 2 の端末 2 が予め定められた正規の端末でありかつ受信したパスワードが特定の者の電子カルテに関連付けられていることを確認する (S 4 4 7)。この確認ができると、コンテンツサーバ 4 は、患者の電子カルテを第 2 の端末 2 に送信する (S 4 4 8)。これにより、第 2 の端末 2 において患者の電子カルテの閲覧が可能になる (S 2 4 8)。

【 0 0 5 6 】

本実施形態に係る非公開情報閲覧システム及び非公開情報閲覧方法は、コンテンツサーバ 4 が第 3 の端末 3 にパスワードを送信するため、患者はパスワードを書き留めたり記憶したりする必要はない。このため、患者によるパスワードの紛失を防止することができる。

30

【 0 0 5 7 】

(実施形態 4)

図 5 に、実施形態 4 に係る非公開情報閲覧システムのシーケンス図を示す。本実施形態に係る非公開情報閲覧方法は、実施形態 1 ~ 実施形態 4 におけるパスワード記憶ステップ及びパスワード照合型非公開情報送信ステップに代えて、暗証番号記憶ステップと、暗証番号照合型非公開情報送信ステップと、を有する。本実施形態では、暗証番号記憶ステップ及び暗証番号照合型非公開情報送信ステップについてのみ説明する。

40

【 0 0 5 8 】

暗証番号記憶ステップでは、非公開情報閲覧システムは以下のように動作する。

第 3 の端末 3 は、電子カルテを特定する情報をコンテンツサーバ 4 に送信して患者の電子カルテにアクセスする。この状態で、第 3 の端末 3 は、患者から入力された暗証番号を記憶し、当該暗証番号をコンテンツサーバ 4 に登録する (S 3 5 1)。コンテンツサーバ 4 は、第 3 の端末 3 が患者に関連付けられた正規の端末であることを確認し、暗証番号を電子カルテに関連付けて記憶する (S 4 5 1)。

【 0 0 5 9 】

暗証番号照合型非公開情報送信ステップでは、非公開情報閲覧システムは以下のように動作する。

50

患者が第2の医師の診察を受ける際、第2の端末2は、コンテンツサーバ4に記憶されているその患者の電子カルテにアクセスする。このとき、第2の端末2のディスプレイに暗証番号を要求する旨が表示され、第2の医師は患者に対して電子カルテの閲覧許可の有無を問い合わせ（S252）、患者からの閲覧許可を取得する（S253）。このとき、第3の端末3が暗証番号を送信し（S354）、第2の端末2は第3の端末3から暗証番号を受信する（S254）。

【0060】

第2の端末2は、第2の端末2が正規の端末であることを示す認証情報と、第3の端末3から受信した暗証番号をコンテンツサーバ4に送信する（S255）。コンテンツサーバ4は、第2の端末2が予め定められた正規の端末でありかつ受信した暗証番号が特定の者の電子カルテに関連付けられていることを確認する（S455）。この確認ができると、コンテンツサーバ4は、患者の電子カルテを第2の端末2に送信する（S456）。これにより、第2の端末2において患者の電子カルテの閲覧が可能になる（S256）。

10

【0061】

本実施形態に係る非公開情報閲覧システム及び非公開情報閲覧方法は、第3の端末3が暗証番号を入力するため、患者が暗証番号を決定することができる。このため、暗証番号を知っている者のみに、電子カルテを閲覧させることができる。また、患者自身が暗証番号を決定するため、患者の覚えやすい番号を暗証番号に用いることで、暗証番号の漏洩による電子カルテの情報の漏洩を防ぐことができる。

【0062】

20

（実施形態5）

図6に、実施形態5に係る非公開情報閲覧システムのシーケンス図を示す。本実施形態に係る非公開情報閲覧方法は、実施形態4における暗証番号記憶ステップ及び暗証番号照合型非公開情報送信ステップが異なる。本実施形態では、実施形態4と異なる点のみ説明する。

【0063】

本実施形態の暗証番号記憶ステップでは、電子カルテを暗証番号で暗号化する（S457）。これにより、コンテンツサーバ4に格納されている電子カルテに記載されている情報が第三者に漏洩する可能性を低くすることができる。

【0064】

30

本実施形態の暗証番号照合型非公開情報送信ステップでは、ステップS455における確認ができたなら、第2の端末2から送信された暗証番号を用いて電子カルテを復号化する（S458）。そして、コンテンツサーバ4は、患者の電子カルテを第2の端末2に送信する（S456）。これにより、第2の端末2において患者の電子カルテの閲覧が可能になる。

【0065】

（実施形態6）

図7に、実施形態6に係る非公開情報閲覧システムのシーケンス図を示す。本実施形態に係る非公開情報閲覧方法は、実施形態4における暗証番号照合型非公開情報送信ステップが異なる。本実施形態では、実施形態4と異なる点のみ説明する。

40

【0066】

本実施形態の暗証番号照合型非公開情報送信ステップでは、非公開情報閲覧システムは以下のように動作する。

患者が第2の医師の診察を受ける際、第2の端末2は、コンテンツサーバ4に記憶されているその患者の電子カルテにアクセスする。このとき、第2の端末2のディスプレイに暗証番号を要求する旨が表示され、第2の医師は患者に対して電子カルテの閲覧許可の有無を問い合わせ（S262）、患者からの閲覧許可を取得する（S263）。このとき、第3の端末3が暗証番号をコンテンツサーバ4に送信し（S365）、第2の端末2が第2の端末2の認証情報をコンテンツサーバ4に送信する（S265）。

【0067】

50

コンテンツサーバ4は、第2の端末2が予め定められた正規の端末でありかつ受信した暗証番号がアクセスしている患者の電子カルテに関連付けられていることを確認する(S465)。この確認ができると、コンテンツサーバ4は、患者の電子カルテを第2の端末2に送信する(S466)。これにより、第2の端末2において患者の電子カルテの閲覧が可能になる(S266)。

【0068】

(実施形態7)

図8に、実施形態7に係る非公開情報閲覧システムのシーケンス図を示す。本実施形態に係る非公開情報閲覧方法は、実施形態6における暗証番号記憶ステップ及び暗証番号照合型非公開情報送信ステップが異なる。本実施形態では、実施形態4と異なる点のみ説明する。

10

【0069】

本実施形態の暗証番号記憶ステップでは、電子カルテを暗証番号で暗号化する(S467)。これにより、コンテンツサーバ4に格納されている電子カルテに記載されている情報が第三者に漏洩する可能性を低くすることができる。

【0070】

本実施形態の暗証番号照合型非公開情報送信ステップでは、ステップS465における確認ができたなら、第3の端末3から送信された暗証番号を用いて電子カルテを復号化する(S468)。そして、コンテンツサーバ4は、患者の電子カルテを第2の端末2に送信する(S466)。これにより、第2の端末2において患者の電子カルテの閲覧が可能になる。

20

【0071】

(実施形態8)

図9に、実施形態8に係る非公開情報閲覧システムのシーケンス図を示す。本実施形態に係る非公開情報閲覧方法は、実施形態4～実施形態7における暗証番号記憶ステップ及び暗証番号照合型非公開情報送信ステップに代えて、利用者情報記憶ステップ及び利用者情報照合型非公開情報送信ステップを有する。本実施形態では、利用者情報記憶ステップ及び利用者情報照合型非公開情報送信ステップについてのみ説明する。

【0072】

利用者情報記憶ステップでは、非公開情報閲覧システムは以下のように動作する。

30

第3の端末3は、電子カルテを特定する情報をコンテンツサーバ4に送信して患者の電子カルテにアクセスする。この状態で、第3の端末3は、自己の記憶している利用者情報のなかから特定の情報を読み出してコンテンツサーバ4に登録する(S371)。コンテンツサーバ4は、第3の端末3が患者に関連付けられた正規の端末であることを確認し、利用者情報を電子カルテに関連付けて記憶する(S471)。

【0073】

ここで、利用者情報は、特定の者に関する情報であり、例えば、ID、パスワード、第3の端末3の所有者の固有情報である。第3の端末3の所有者の固有情報は、例えば、第3の端末3の位置、第3の端末3とコンテンツサーバ4との間の伝搬遅延特性、指紋又は虹彩などの生体認証情報である。

40

【0074】

利用者情報照合型非公開情報送信ステップでは、非公開情報閲覧システムは以下のように動作する。

患者が第2の医師の診察を受ける際、第2の端末2は、コンテンツサーバ4に記憶されているその患者の電子カルテにアクセスする。このとき、第2の端末2のディスプレイに利用者情報を要求する旨が表示され、第2の医師は患者に対して電子カルテの閲覧許可の有無を問い合わせ(S272)、患者からの閲覧許可を取得する(S273)。このとき、第3の端末3は、コンテンツサーバ4上の自己の電子カルテにアクセスし、利用者情報を送信する(S375)。これと同時に、第2の端末2は、第2の端末2が正規の端末であることを示す認証情報を送信する(S275)。

50

【0075】

コンテンツサーバ4は、第2の端末2が予め定められた正規の端末でありかつ受信した利用者情報が特定の者の電子カルテに関連付けられていることを確認する(S475)。この確認ができると、コンテンツサーバ4は、患者の電子カルテを第2の端末2に送信する(S476)。これにより、第2の端末2において患者の電子カルテの閲覧が可能になる(S276)。

【0076】

本実施形態に係る非公開情報閲覧システム及び非公開情報閲覧方法は、第3の端末3の利用者情報を暗号鍵として使用するため、患者は第3の端末3を第2の医師の診察室に持参すれば、電子カルテを閲覧させることができる。また、第3の端末3がない場所では電子カルテを閲覧することはできないため、患者本人以外の者にカルテが閲覧されるのを防ぐことができる。

【0077】

(実施形態9)

図10に、実施形態9に係る非公開情報閲覧システムのシーケンス図を示す。本実施形態に係る非公開情報閲覧方法は、実施形態8における利用者情報記憶ステップ及び利用者情報照合型非公開情報送信ステップが異なる。本実施形態では、実施形態8と異なる点のみ説明する。

【0078】

本実施形態の利用者情報記憶ステップでは、電子カルテを利用者情報で暗号化する(S467)。これにより、コンテンツサーバ4に格納されている電子カルテに記載されている情報が第三者に漏洩する可能性を低くすることができる。ここで、暗号化する利用者情報は、利用者情報の全部であってもよいし、一部であってもよい。

【0079】

本実施形態の利用者情報照合型非公開情報送信ステップでは、ステップS475における確認ができたら、第3の端末3から送信された利用者情報を用いて電子カルテを復号化する(S478)。そして、コンテンツサーバ4は、患者の電子カルテを第2の端末2に送信する(S476)。これにより、第2の端末2において患者の電子カルテの閲覧が可能になる(S276)。

【0080】

以上説明したように、実施形態1～実施形態10に係る発明は、単に電子カルテをサーバ上で共有するだけでなく、従来の医師間の紹介状のように、患者が自分の意思でカルテを紹介された医師に見せ、診療を受けることを可能にする。これにより、医師が勝手に他の医師が診療している患者のカルテを閲覧することを制限し、閲覧に関して、患者が他の医師の閲覧を許可したことを確実に記録することができる。

【0081】

実施形態1～実施形態10に係る発明は、医師間で行われているカルテ若しくは診療情報などの電子化された情報に関して、医師間での電子化情報の共有許可、医師と患者間での電子化情報の共有、他の医師への電子化情報の提供の許可などを、確実に記録することができる。また、現状の医師の診療におけるカルテの共有化、患者への他の医師の紹介など、現状行われているプロセスを変えることなく、カルテなどの電子化を進めることができる。

【0082】

実施形態1～実施形態10について、非公開情報が電子カルテである電子カルテ閲覧システムについて説明したが、これに限定されない。

例えば、非公開情報閲覧システムは、生徒の成績情報閲覧システムに適用することができる。この場合、非公開情報が学生の成績情報であり、第1の端末は生徒が所属する教育機関の端末であり、第2の端末は進学先や転校先等の教育機関又は就職先の企業の端末である。

例えば、非公開情報閲覧システムは、住民情報閲覧システムに適用することができる。

10

20

30

40

50

この場合、非公開情報が住民の住所や戸籍などの個人情報であり、第1の端末は住民を管轄する市区町村の端末であり、第2の端末は住民の住所や戸籍を確認する公共機関又は企業の端末である。

例えば、非公開情報閲覧システムは、結婚紹介情報閲覧システムに適用することができる。この場合、非公開情報が結婚希望者の情報であり、第1の端末は結婚希望者の所属する結婚紹介機関の端末であり、第2の端末は結婚希望者を紹介された他の結婚希望者の端末である。

例えば、非公開情報閲覧システムは、コンテンツ閲覧システムに適用することができる。この場合、非公開情報がコンテンツであり、第1の端末はコンテンツを管理している端末であり、第2の端末はコンテンツを利用する者の端末である。コンテンツは、著作権を保護すべき映像やゲームなどの任意の著作物である。

10

【0083】

(実施形態10)

本実施形態では、閲覧許可ステップ以降パスワード照合型非公開情報送信ステップの前までに、第1の端末1が、非公開情報の閲覧を許可する旨をコンテンツサーバ4に登録する。このときに非公開情報としてのカルテが電子化されていない場合、カルテを電子化した電子カルテをコンテンツサーバ4に格納する。電子カルテを格納する方法を図11に示す。電子カルテを格納する方法は、画像変換ステップと、属性情報設定ステップと、を順に行う。

【0084】

20

画像変換ステップでは、スキャナ300が、カルテ200の属性情報を示すコード101が付された透明ケース100にカルテ200が格納された状態で、カルテ200及びコード101を画像データに変換する。画像変換ステップでは、例えば、ステップP2～ステップP5を行う。

【0085】

属性情報設定ステップでは、カルテ200の画像データの格納を承認する認証サーバ500が、カルテ200及びコード101の画像データからコード101の画像を識別し、識別したコード101の画像からカルテ200の属性情報を抽出し、抽出したカルテ200の属性情報をカルテ200の画像データの属性情報として設定する。属性情報設定ステップでは、ステップP6～ステップP11を行う。

30

【0086】

(カルテを透明ケースに格納する方法)

まず、透明ケース100にカルテ200の属性情報を示すコード101及び文字102を付し、次に、透明ケース100にカルテ200を格納する。電子カルテシステムでは、透明ケース100は、クリアファイルであり、カルテ200は、手書きカルテであり、コード101は、QRコード(登録商標)であり、属性情報は、患者の氏名及びその振り仮名並びに患者の生年月日などの患者情報である。透明ケース100は、カルテ200の更新の度に準備する必要はなく、カルテ200の最初の登録において準備すればよい。

【0087】

(画像データを格納する方法)

40

画像データを格納する方法を図11に示す。最初に、透明ケース100を予め準備しておく。電子カルテシステムにおいては、医者又は看護師は、クリアファイルを予め準備しておく。次に、カルテ200を透明ケース100に格納する。電子カルテシステムでは、医者又は看護師は、文字102が示す患者情報及びカルテ200の患者情報が一致するように、手書きカルテをクリアファイルに挟む(ステップP1)。次に、透明ケース100に格納されたカルテ200をスキャナ300にセットする。電子カルテシステムでは、医者又は看護師は、クリアファイルに挟まれた手書きカルテをスキャナ300にセットする(ステップP2)。最後に、医者又は看護師は、スキャン開始ボタンを押す(ステップP3)。医者又は看護師は、ステップP3までの処理を行えばよく、以降の処理を行わなくてもよい。

50

【 0 0 8 8 】

スキャナ 3 0 0 は、スキャン開始指示を取得する（ステップ P 4）。次に、画像変換ステップでは、スキャナ 3 0 0 は、カルテ 2 0 0 の属性情報を示すコード 1 0 1 が付された透明ケース 1 0 0 にカルテ 2 0 0 が格納された状態で、カルテ 2 0 0 及びコード 1 0 1 を画像データに変換する。電子カルテシステムでは、スキャナ 3 0 0 は、手書きカルテの患者情報を示す Q R コード（登録商標）が付されたクリアファイルに手書きカルテが挟まれた状態で、手書きカルテ及び Q R コード（登録商標）を電子カルテに変換する。次に、スキャナ 3 0 0 は、カルテ 2 0 0 及びコード 1 0 1 の画像データをコンピュータ 4 0 0 に送信する（ステップ P 5）。次に、コンピュータ 4 0 0 は、カルテ 2 0 0 の画像データの格納を承認する認証サーバ 5 0 0 に対して、ID 又はパスワードなどによる認証を実行し、

10

【 0 0 8 9 】

属性情報設定ステップでは、認証サーバ 5 0 0 は、カルテ 2 0 0 及びコード 1 0 1 の画像データからコード 1 0 1 の画像を識別し、識別したコード 1 0 1 の画像からカルテ 2 0 0 の属性情報を抽出し、抽出したカルテ 2 0 0 の属性情報をカルテ 2 0 0 の画像データの属性情報として設定する。電子カルテシステムでは、認証サーバ 5 0 0 は、電子カルテから Q R コード（登録商標）の画像を識別し、識別した Q R コード（登録商標）の画像から手書きカルテの患者情報を抽出し（ステップ P 7）、抽出した手書きカルテの患者情報を電子カルテの患者情報として設定する（ステップ P 8）。

20

【 0 0 9 0 】

格納認証ステップでは、認証サーバ 5 0 0 は、カルテ 2 0 0 の画像データに設定された属性情報及びカルテ 2 0 0 の属性情報が一致するときに、カルテ 2 0 0 の画像データの格納を承認する。電子カルテシステムでは、認証サーバ 5 0 0 は、電子カルテに設定された患者情報及び手書きカルテの患者情報が一致するときに（ステップ P 9）、電子カルテの格納を承認する（ステップ P 1 0）。具体的には、認証サーバ 5 0 0 は、コンピュータ 4 0 0 に対して、これらの患者情報が一致するかどうかを確認する。そして、コンピュータ 4 0 0 は、認証サーバ 5 0 0 に対して、登録の権限を有する医者からの指示に応じて、これらの患者情報が一致するかどうかを応答する。

【 0 0 9 1 】

カルテ追加ステップでは、認証サーバ 5 0 0 は、カルテ 2 0 0 の画像データに設定された属性情報に基づいて、更新前のカルテ 2 0 0 の画像データを検索し、更新後のカルテ 2 0 0 の画像データを更新前のカルテ 2 0 0 の画像データに追加する。電子カルテシステムでは、認証サーバ 5 0 0 は、電子カルテに設定された患者情報に基づいて、更新前の電子カルテを検索し、更新後の電子カルテを更新前の電子カルテに追加する（ステップ P 1 1）。

30

【 0 0 9 2 】

同じ患者について、手書きカルテの更新の度に、同じクリアファイルが使い回されるため、同じ属性情報が設定された電子カルテが生成される。そこで、認証サーバ 5 0 0 は、更新後の電子カルテに設定された属性情報に基づいて、更新前の電子カルテを検索することができる。そして、認証サーバ 5 0 0 は、電子カルテの追加の形態として、更新前の電子カルテに加えて更新後の電子カルテを追加することもでき、更新前の電子カルテに代えて更新後の電子カルテを格納することもでき、初回の登録の際には新たなファイルを作成したうえで電子カルテを新たなファイルに格納することもできる。

40

【 0 0 9 3 】

画像変換ステップ及び属性情報設定ステップでは、カルテ 2 0 0 を透明ケース 1 0 0 に格納し、カルテ 2 0 0 を透明ケース 1 0 0 に格納した状態で、スキャン開始指示をスキャナ 3 0 0 に与えるのみでよい。よって、カルテ 2 0 0 を画像データに変換するときに、画像データのファイル名を入力する必要がなくなる。格納認証ステップでは、属性情報が一致した状態でカルテ 2 0 0 が透明ケース 1 0 0 に格納されたかどうかを確認したうえで、

50

画像データを格納することができる。カルテ追加ステップでは、認証サーバ500の自動処理を利用することにより、ユーザは、更新前のカルテ200を検索し、更新後のカルテ200を更新前のカルテ200に追加する必要がなくなる。

【0094】

透明ケース100は一度だけ準備しておけばよく何度でも使い回すことができ、カルテ200を更新するたびにコード101をカルテ200に付す必要はない。ここで、コード101がカルテ200に付されるとすれば、コード101の位置がカルテの更新の度に変更されることになるが、コード101は透明ケース100に付されるため、コード101の位置はカルテの更新の度に変更されることはない。よって、コード101の画像を自動的に識別することができ、コード101の認識率を高めることができる。さらに、手書き

10

【0095】

(認証サーバの構成)

認証サーバ500の構成を図12に示す。認証サーバ500は、コンテンツ格納部501、データ通信部502、コード抽出部503、属性情報設定部504、コンテンツ格納認証部505及びコンテンツ格納追加部506から構成される。コンテンツ格納部501は、画像データを格納しており、認証サーバ500に配置されていてもよく、認証サーバ500以外の装置に配置されていてもよい。データ通信部502は、ステップP6におけるID又はパスワードによる認証及び画像データの送信、並びにステップP9における属性情報の一致の確認について、コンピュータ400及び認証サーバ500の間でのインタフェースとなる。

20

【0096】

コード抽出部503は、カルテ200の属性情報を示すコード101が付された透明ケース100にカルテ200が格納された状態で作成されたカルテ200及びコード101の画像データから、コード101の画像を識別し、識別したコード101の画像から、カルテ200の属性情報を抽出する。電子カルテシステムでは、コード抽出部503は、手書きカルテの患者情報を示すQRコード(登録商標)が付されたクリアファイルに手書きカルテが挟まれた状態で作成された電子カルテから、QRコード(登録商標)の画像を識別し、識別したQRコード(登録商標)の画像から、手書きカルテの患者情報を抽出する(ステップP7)。属性情報設定部504は、抽出されたカルテ200の属性情報をカルテ200の画像データの属性情報として設定する。電子カルテシステムでは、属性情報設定部504は、抽出された手書きカルテの患者情報を電子カルテの患者情報として設定する(ステップP8)。

30

【0097】

コンテンツ格納認証部505は、カルテ200の画像データに設定された属性情報及びカルテ200の属性情報が一致するときに、カルテ200の画像データの格納を承認する。電子カルテシステムでは、コンテンツ格納認証部505は、電子カルテに設定された患者情報及び手書きカルテの患者情報が一致するときに、電子カルテの格納を承認する(ステップP9、P10)。コンテンツ格納追加部506は、カルテ200の画像データに設定された属性情報に基づいて、更新前のカルテ200の画像データを検索し、更新後のカルテ200の画像データを更新前のカルテ200の画像データに追加する。電子カルテシステムでは、コンテンツ格納追加部506は、電子カルテに設定された患者情報に基づいて、更新前の電子カルテを検索し、更新後の電子カルテを更新前の電子カルテに追加する(ステップP11)。

40

【0098】

本実施形態では、カルテ200の属性情報を示すコード101を、透明ケース100に付しているが、他の実施形態では、カルテ200の更新の度に変更される属性情報を示すコード101を、カルテ200に付してもよい。透明ケース100は更新の度に使い回さ

50

れるが、カルテ200は更新の度に作成されるため、カルテ200の更新の度に変更される属性情報を示すコード101を、透明ケース100ではなくカルテ200に付している。カルテ200の更新の度に更新される属性情報として、更新された日付及び変更された内容などに関する情報をあげることができる。

【0099】

画像変換ステップでは、スキャナ300は、カルテ200の更新の度に更新される属性情報を示すコード101がカルテ200に付された状態で、カルテ200及びコード101を画像データに変換する。コード抽出部503は、カルテ200の更新の度に更新される属性情報を示すコード101がカルテ200に付された状態で作成されたカルテ200及びコード101の画像データから、コード101の画像を識別し、識別したコード101の画像から、カルテ200の属性情報を抽出する。

10

【0100】

格納される画像データは、カルテ200のみの画像データであってもよく、カルテ200及びコード101の両方の画像データであってもよい。カルテ200のみの画像データが格納されるときには、カルテ200及びコード101の画像データからコード101の画像データが削除され、カルテ200のみの画像データを閲覧することができる。カルテ200及びコード101の両方の画像データが格納されるときには、画像データを容易に格納することができる。

【0101】

本実施形態では、コンピュータ400が認証サーバ500に対してID又はパスワードなどによる認証を実行しているが、他の実施形態では、コンピュータ400と関連付けられた携帯電話が認証サーバ500に対してID又はパスワードなどによる認証を実行してもよい。認証サーバ500は、コンピュータ400及び携帯電話を関連付けており、コンピュータ400から画像データの送信許可を要求されたときに、携帯電話に認証を要求する。携帯電話及び利用者は1対1に対応付けられているため、携帯電話が認証サーバ500に対して認証を実行することにより、認証のセキュリティを高めることができる。また、コンテンツサーバ4が認証サーバ500の機能を有していてもよい。

20

【産業上の利用可能性】

【0102】

本発明の非公開情報閲覧方法及び非公開情報閲覧システムは、電子カルテ閲覧システム、成績情報閲覧システム、住民情報閲覧システム、結婚紹介情報閲覧システム及びコンテンツ閲覧システムに適用することができるため、情報通信産業だけでなく、医療産業、教育産業、公共関与産業、プライダル産業、メディア産業に利用することができる。

30

【符号の説明】

【0103】

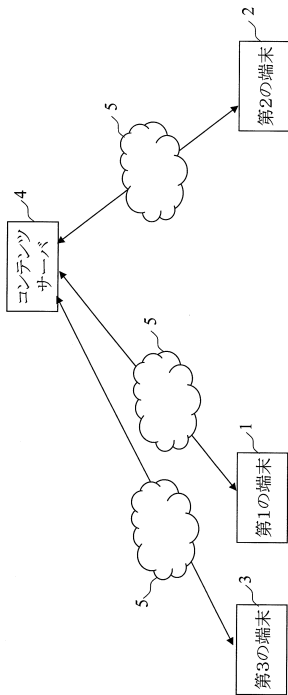
- 1：第1の端末
- 2：第2の端末
- 3：第3の端末
- 4：コンテンツサーバ
- 5：通信ネットワーク
- 100：透明ケース
- 200：カルテ
- 300：スキャナ
- 400：コンピュータ
- 500：認証サーバ
- 101：コード
- 102：文字
- 501：コンテンツ格納部
- 502：データ通信部
- 503：コード抽出部

40

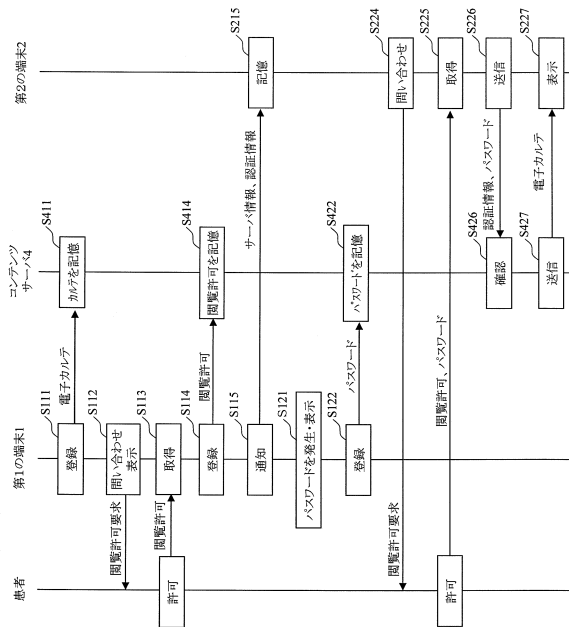
50

- 504 : 属性情報設定部
- 505 : コンテンツ格納認証部
- 506 : コンテンツ格納追加部

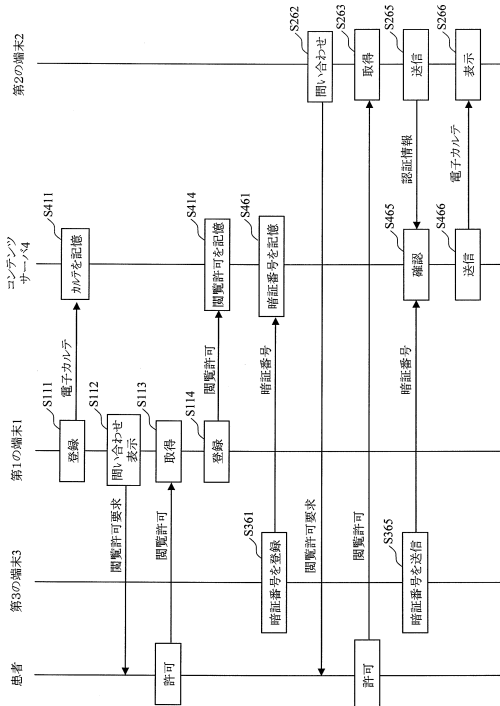
【図1】



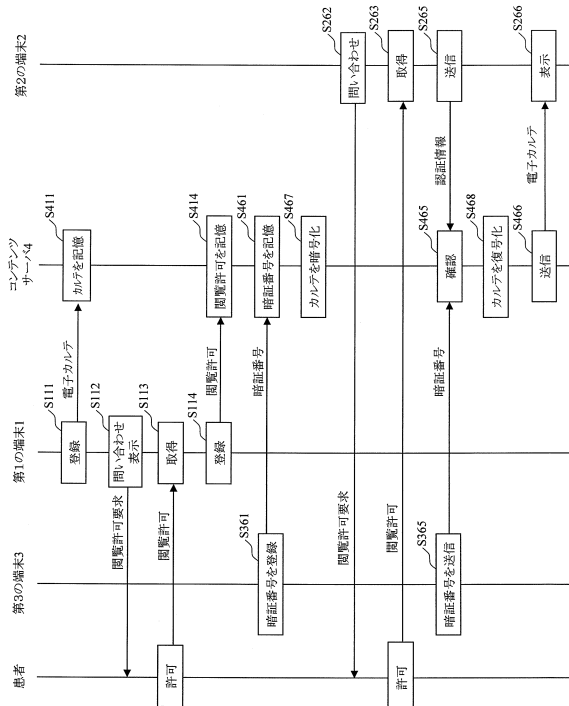
【図2】



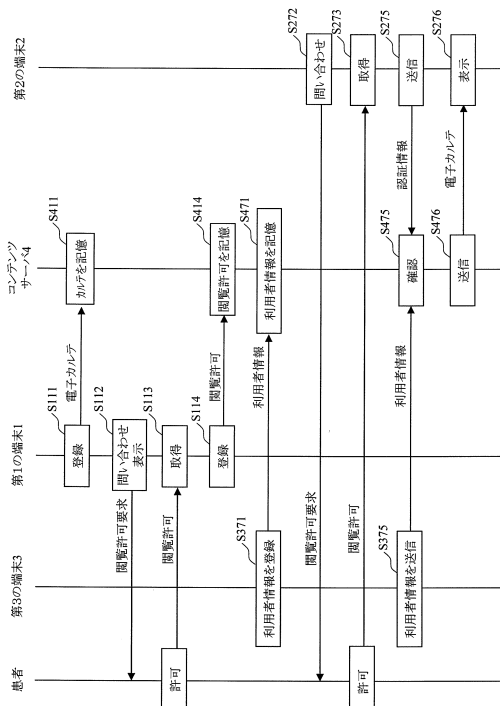
【図7】



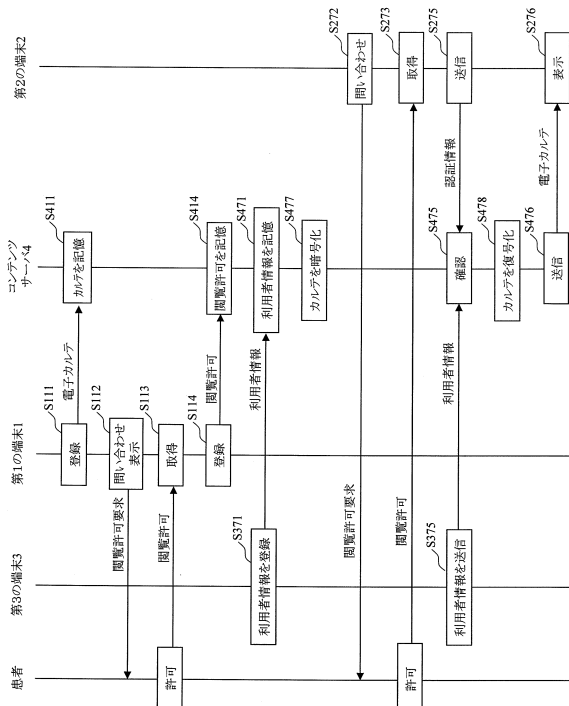
【図8】



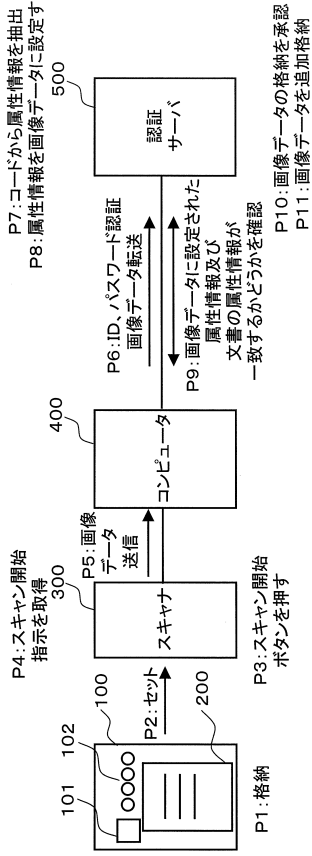
【図9】



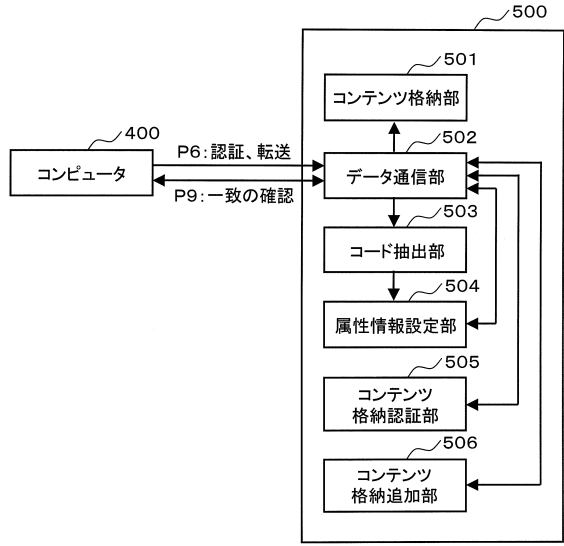
【図10】



【 図 1 1 】



【 図 1 2 】



フロントページの続き

- (56)参考文献 特開平 1 1 - 3 3 8 9 5 0 (J P , A)
特開 2 0 0 3 - 0 4 4 4 7 8 (J P , A)
特開 2 0 0 1 - 2 9 7 1 5 3 (J P , A)
特開 2 0 0 7 - 2 1 9 6 6 5 (J P , A)
特開 2 0 0 6 - 2 6 0 5 2 1 (J P , A)
特開 2 0 1 0 - 2 7 2 0 3 1 (J P , A)
牧亮介, 久保田洋彰, 木原雅巳, 地域医療における診療情報の電子化とその共有に関する検討,
平成23 年度 日本大学理工学部 学術講演会論文集, 2 0 1 1 年 1 1 月 2 6 日, p.551-552, ht
tp://www.cst.nihon-u.ac.jp/research/gakujutu/55/pdf/G-26.pdf

- (58)調査した分野(Int.Cl., D B 名)

G 0 6 F 2 1