(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2013-30157
(P2013-30157A)
(43)公開日　平成25年2月7日(2013.2.7)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/62	(2013.01)	G06F	21/24	165A	
G06Q 50/22	(2012.01)	G06F	17/60	126A	
G06F 21/31	(2013.01)	G06F	21/20	131A	
G06F 21/44	(2013.01)	G06F	21/20	144C	
G06F 21/60	(2013.01)	G06F	21/24	160C	

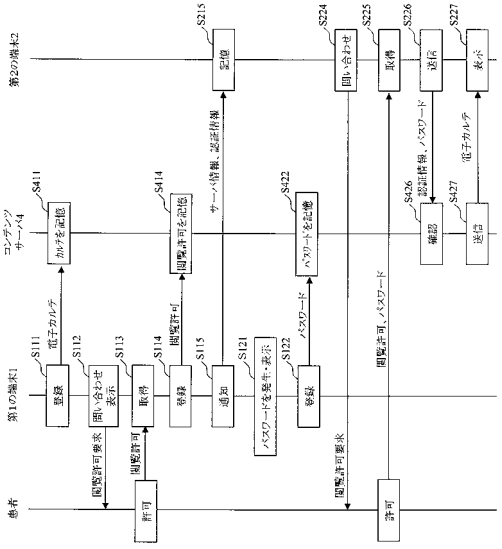
審査請求 未請求　請求項の数 16　ＯＬ　（全 24 頁）

(21)出願番号　特願2012-117274 (P2012-117274)
(22)出願日　平成24年5月23日 (2012.5.23)
(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)

(71)出願人　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
(74)代理人　100119677
弁理士　岡田　賢治
(74)代理人　100115794
弁理士　今下　勝博
(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

(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)【要約】
【課題】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。
【解決手段】本発明は、第１の端末１が、特定の者に関する非公開情報をコンテンツサーバ４に登録する非公開情報登録ステップと、第１の端末１が、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、コンテンツサーバ４がパスワードを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、コンテンツサーバ４が、第２の端末２からパスワードを受信し、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非公開情報を第２の端末２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。
【選択図】図２



【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、
を順に有する非公開情報閲覧方法。
【請求項２】
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するか、或いは、
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の端末が表示するか、或いは、
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記非公開情報に関連付けて記憶する、
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５】

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４に記載の非公開情報閲覧方法。

【請求項６】

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７】

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６に記載の非公開情報閲覧方法。

【請求項８】

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３、５又は７に記載の非公開情報閲覧方法。

【請求項９】

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、

を備える非公開情報閲覧システム。

【請求項１０】

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

記憶するか、或いは、
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の端末が表示するか、或いは、
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記非公開情報に関連付けて記憶する、
ことを特徴とする請求項９に記載の非公開情報閲覧システム。
【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９又は１０に記載の非公開情報閲覧システム。
【請求項１２】
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、
を備える非公開情報閲覧システム。
【請求項１３】
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１２に記載の非公開情報閲覧システム。
【請求項１４】
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１５】
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１４に記載の非公開情報閲覧システム。
【請求項１６】
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１１、１３又は１５に記載の非公開情報閲覧システム。
【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、患者といろいろな相談をした上で、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で手渡しされていた。
【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。
【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
【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。
【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。

【００１１】

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。

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。

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。

【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。

【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

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】

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。

【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。

【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。

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。

【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。
【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。
【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。
【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。
【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。

【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）。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）。

【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）。

【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。

【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。

【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。

【００５３】

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（Ｓ１４１）。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３の端末３に送信し（Ｓ４４２）、パスワードを電子カルテに関連付けて記憶する（Ｓ４４３）。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（Ｓ３４２）。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。

【００５４】

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（Ｓ２４４）、患者からの閲覧許可を取得する（Ｓ２４５）。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（Ｓ３４６）、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（Ｓ２４６）。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。

【００５５】

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（Ｓ２４７）。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（Ｓ４４７）。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（Ｓ４４８）。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（Ｓ２４８）。

【００５６】

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。

【００５７】

（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。

【００５８】

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（Ｓ３５１）。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（Ｓ４５１）。

【００５９】

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（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）。

【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】

（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】

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。

【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】

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。

【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。

【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。

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。

【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）。

【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。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。
【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】
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。
【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）
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。

【００８８】

スキャナ３００は、スキャン開始指示を取得する（ステップＰ４）。次に、画像変換ステップでは、スキャナ３００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、カルテ２００及びコード１０１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３００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、手書きカルテ及びＱＲコード（登録商標）を電子カルテに変換する。次に、スキャナ３００は、カルテ２００及びコード１０１の画像データをコンピュータ４００に送信する（ステップＰ５）。次に、コンピュータ４００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に対して、ＩＤ又はパスワードなどによる認証を実行し、当該認証が成功すればカルテ２００及びコード１０１の画像データを送信する（ステップＰ６）。

【００８９】

属性情報設定ステップでは、認証サーバ５００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。電子カルテシステムでは、認証サーバ５００は、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し（ステップＰ７）、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Ｐ８）。

【００９０】

格納認証ステップでは、認証サーバ５００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、認証サーバ５００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Ｐ９）、電子カルテの格納を承認する（ステップＰ１０）。具体的には、認証サーバ５００は、コンピュータ４００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４００は、認証サーバ５００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。

【００９１】

カルテ追加ステップでは、認証サーバ５００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、認証サーバ５００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）。

【００９２】

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５００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５００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。

【００９３】
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２００を透明ケース１００に格納し、カルテ２００を透明ケース１００に格納した状態で、スキャン開始指示をスキャナ３００に与えるのみでよい。よって、カルテ２００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２００が透明ケース１００に格納されたかどうかを確認したうえで、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、手書きで作成されたカルテ２００であっても、本願カルテの格納方法を導入する前に作成されたカルテ２００であっても、本願カルテの格納方法を用いて容易に電子化することができる。

【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。

【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）。

【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）。

【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の更新の度に変更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の更新の度に変更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の更新の度に変更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。

【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。

【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、ブライダル産業、メディア産業に利用することができる。

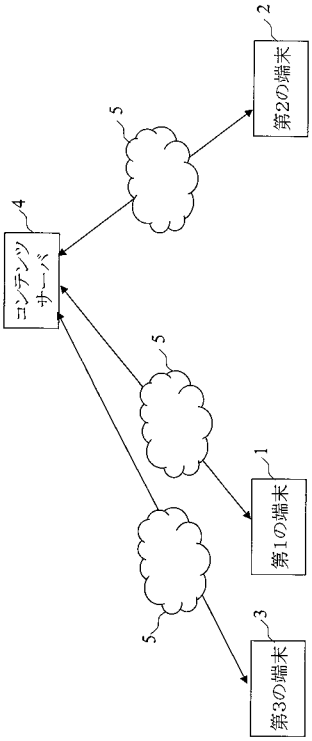
【符号の説明】

【０１０３】

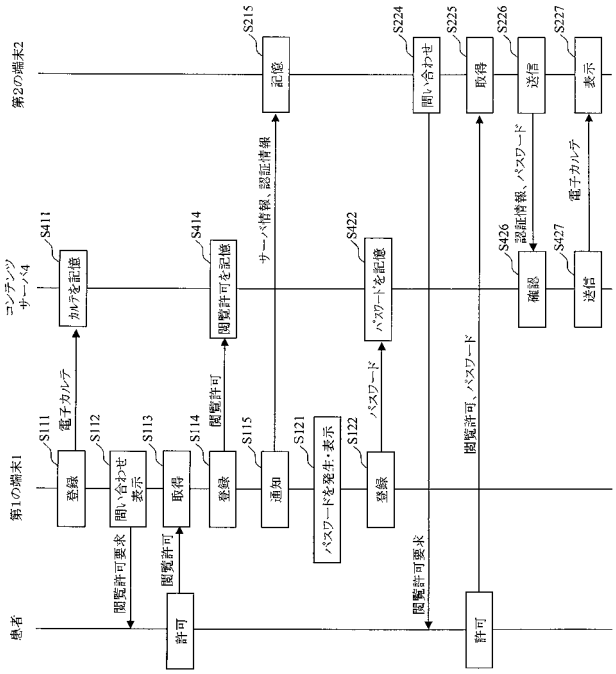
１：第１の端末
２：第２の端末
３：第３の端末
４：コンテンツサーバ
５：通信ネットワーク
１００：透明ケース
２００：カルテ
３００：スキャナ
４００：コンピュータ

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
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

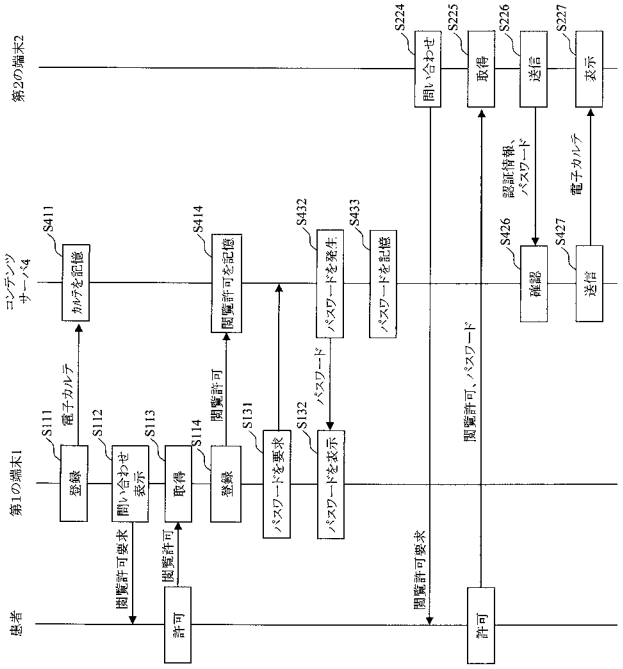
【図１】



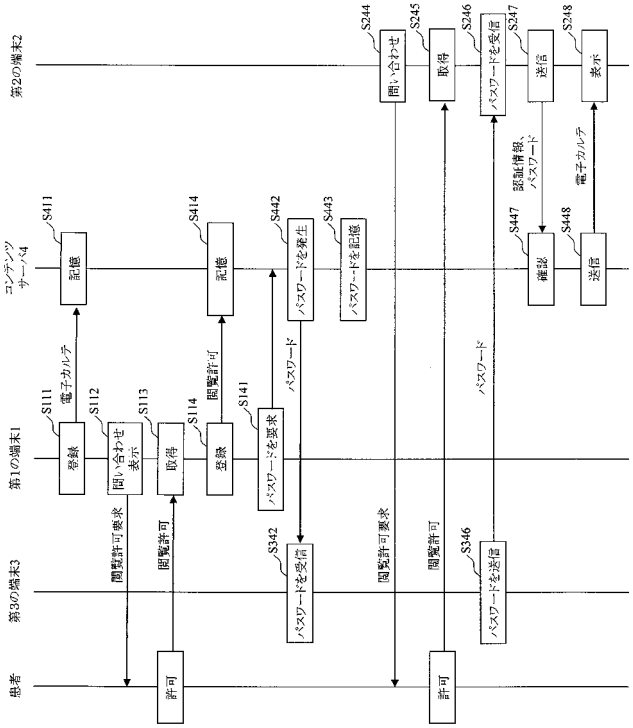
【図２】



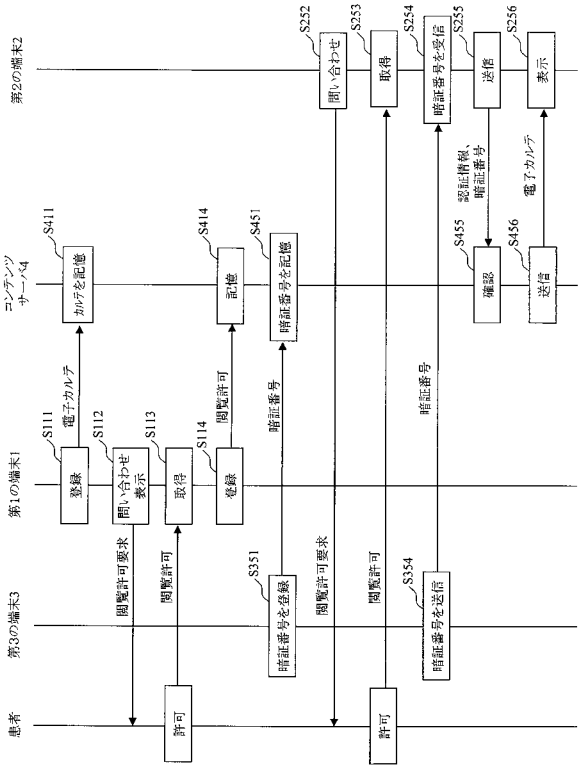
【図３】


患者
第1の端末1
第2の端末2
コンテンツサーバ4
登録
問い合わせ表示
取得
閲覧許可要求
閲覧許可
電子カルテ
カルテを記憶
閲覧許可を記憶
パスワードを要求
パスワードを発生
パスワードを表示
パスワードを記憶
問い合わせ
確認
送信
表示
閲覧許可、パスワード
認証情報、パスワード
電子カルテ

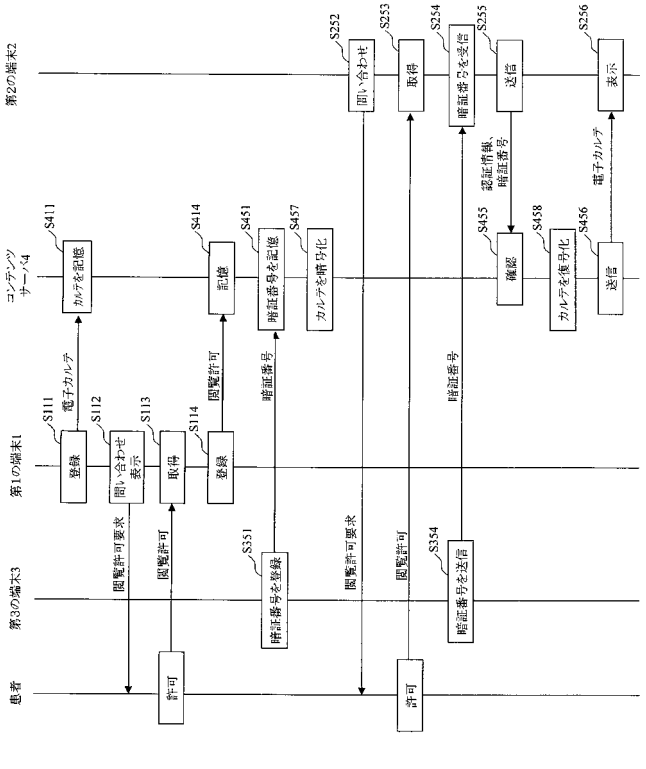
【図４】


患者
第1の端末1
第2の端末2
第3の端末3
コンテンツサーバ4
登録
問い合わせ表示
取得
閲覧許可要求
閲覧許可
電子カルテ
記憶
パスワードを要求
パスワードを発生
パスワードを記憶
パスワードを受信
パスワードを送信
問い合わせ
確認
送信
表示
パスワード
認証情報、パスワード
電子カルテ

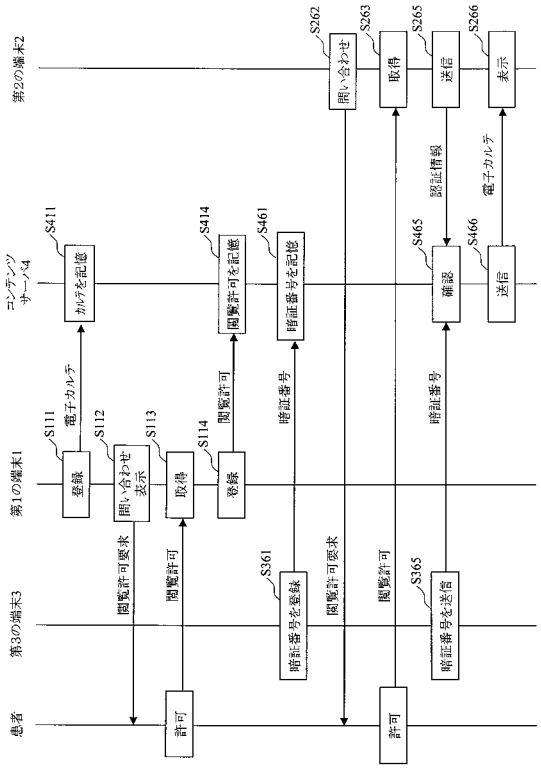
【図５】


患者
第1の端末1
第2の端末2
第3の端末3
コンテンツサーバ4
登録
問い合わせ表示
取得
閲覧許可要求
閲覧許可
電子カルテ
カルテを記憶
記憶
暗証番号を記憶
暗証番号を登録
暗証番号を送信
暗証番号を受信
問い合わせ
確認
送信
表示
暗証番号
認証情報、暗証番号
電子カルテ

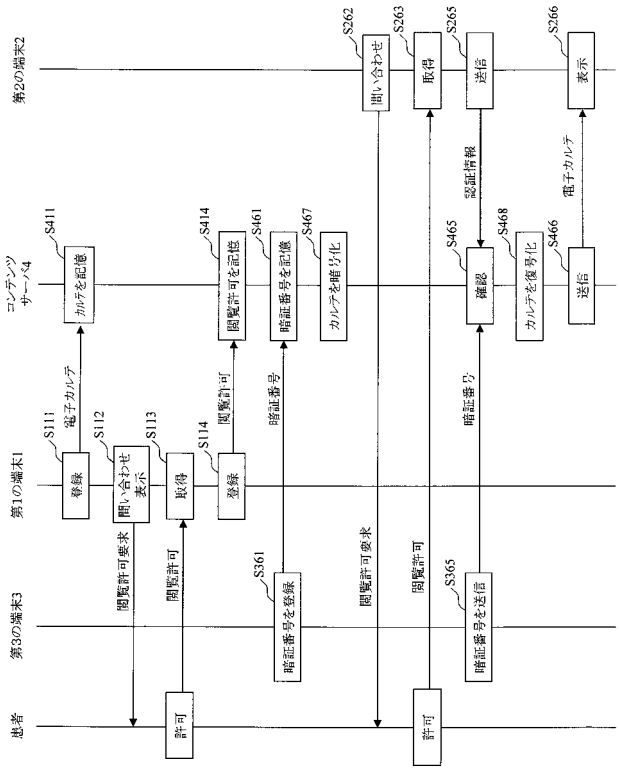
【図６】


患者
第1の端末1
第2の端末2
第3の端末3
コンテンツサーバ4
登録
問い合わせ表示
取得
閲覧許可要求
閲覧許可
電子カルテ
カルテを記憶
記憶
暗証番号を記憶
暗証番号を登録
暗証番号を送信
暗証番号を受信
問い合わせ
確認
送信
表示
暗証番号
認証情報、暗証番号
電子カルテ
カルテを暗号化
カルテを復号化

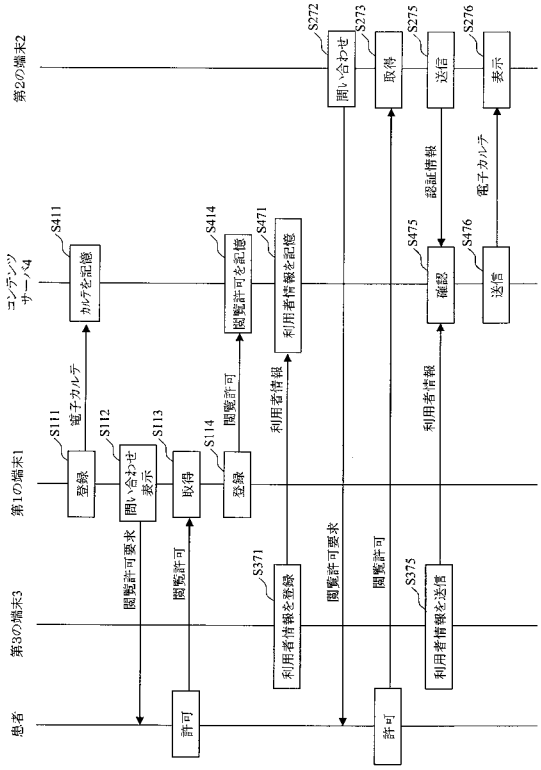
【図７】


患者
第3の端末3
第1の端末1
コンテンツサーバ4
第2の端末2
S111 登録 電子カルテ
S112 問い合わせ表示
S113 取得
S114 登録 閲覧許可
S361 暗証番号を登録
S365 暗証番号を送信
S411 カルテを記憶
S414 閲覧許可を記憶
S461 暗証番号を記憶
S465 確認
S466 送信 電子カルテ
S262 問い合わせ
S263 取得
S265 送信 認証情報
S266 表示
閲覧許可要求
閲覧許可
許可
暗証番号

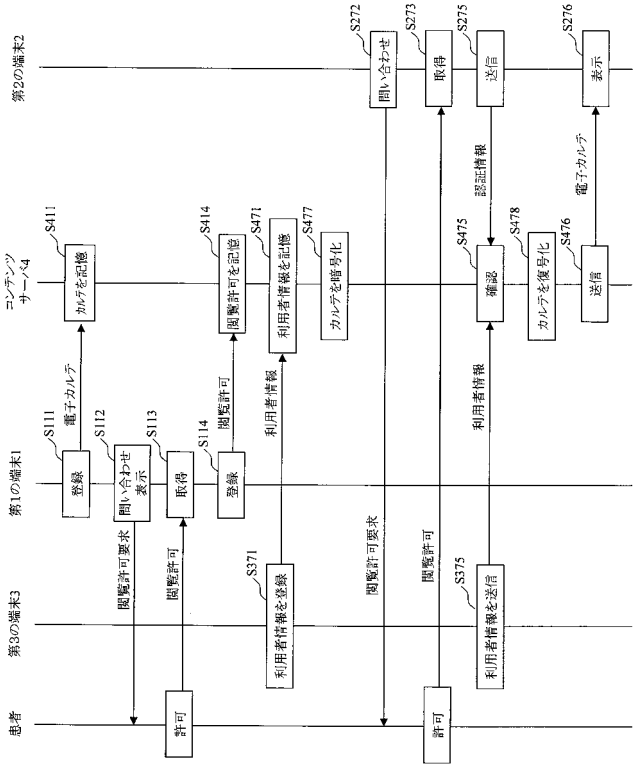
【図８】


患者
第3の端末3
第1の端末1
コンテンツサーバ4
第2の端末2
S111 登録 電子カルテ
S112 問い合わせ表示
S113 取得
S114 登録 閲覧許可
S361 暗証番号を登録
S365 暗証番号を送信
S411 カルテを記憶
S414 閲覧許可を記憶
S461 暗証番号を記憶
S465 確認
S466 送信 電子カルテ
S467 カルテを暗号化
S468 カルテを復号化
S262 問い合わせ
S263 取得
S265 送信 認証情報
S266 表示
閲覧許可要求
閲覧許可
許可
暗証番号

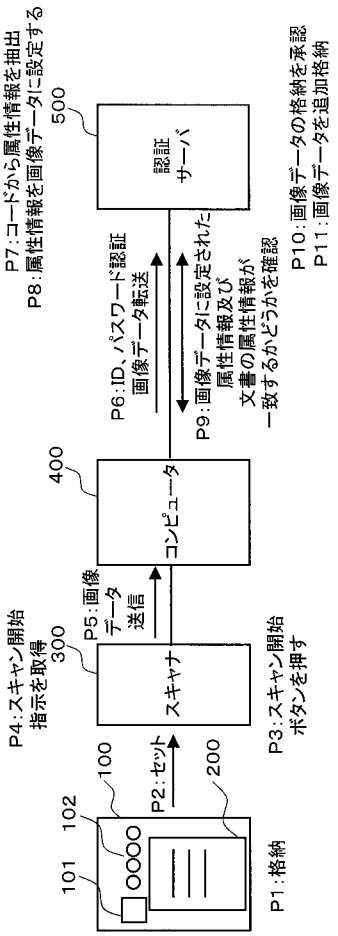
【図９】


患者
第3の端末3
第1の端末1
コンテンツサーバ4
第2の端末2
S111 登録 電子カルテ
S112 問い合わせ表示
S113 取得
S114 登録 閲覧許可
S371 利用者情報を登録
S375 利用者情報を送信
S411 カルテを記憶
S414 閲覧許可を記憶
S471 利用者情報を記憶
S475 確認
S476 送信 電子カルテ
S272 問い合わせ
S273 取得
S275 送信 認証情報
S276 表示
閲覧許可要求
閲覧許可
許可
利用者情報

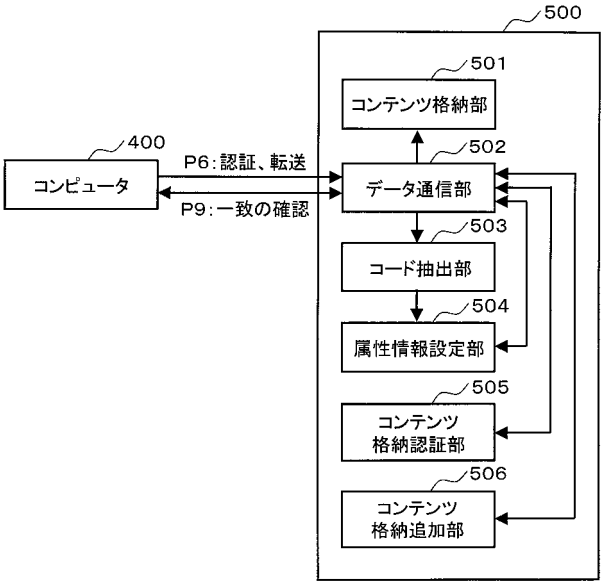
【図１０】


患者
第3の端末3
第1の端末1
コンテンツサーバ4
第2の端末2
S111 登録 電子カルテ
S112 問い合わせ表示
S113 取得
S114 登録 閲覧許可
S371 利用者情報を登録
S375 利用者情報を送信
S411 カルテを記憶
S414 閲覧許可を記憶
S471 利用者情報を記憶
S475 確認
S476 送信 電子カルテ
S477 カルテを暗号化
S478 カルテを復号化
S272 問い合わせ
S273 取得
S275 送信 認証情報
S276 表示
閲覧許可要求
閲覧許可
許可
利用者情報

【図１１】


P7:コードから属性情報を抽出
P8:属性情報を画像データに設定する
500
認証
サーバ
P6:ID、パスワード認証
画像データ転送
P9:画像データに設定された
属性情報及び
文書の属性情報が
一致するかどうかを確認
P10:画像データの格納を承認
P11:画像データを追加格納
400
コンピュータ
P5:画像
データ
送信
P4:スキャン開始
指示を取得
300
スキャナ
P3:スキャン開始
ボタンを押す
100
P2:セット
200
102
101
OOOO
P1:格納

【図１２】


500
501
コンテンツ格納部
400
コンピュータ
P6:認証、転送
P9:一致の確認
502
データ通信部
503
コード抽出部
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