(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第5388036号
(P5388036)

(45)発行日　平成26年1月15日(2014.1.15)　(24)登録日　平成25年10月18日(2013.10.18)

(51)Int.Cl.　　F I
G06F 21/31 (2013.01)　　G06F 21/20 131A
H04L 9/32 (2006.01)　　G06F 21/20 131D
　　H04L 9/00 673A

請求項の数 10　(全 34 頁)

(21)出願番号　特願2009-144603 (P2009-144603)
(22)出願日　平成21年6月17日 (2009.6.17)
(65)公開番号　特開2011-2960 (P2011-2960A)
(43)公開日　平成23年1月6日 (2011.1.6)
審査請求日　平成24年1月23日 (2012.1.23)

(73)特許権者　505210115
国立大学法人旭川医科大学
北海道旭川市緑が丘東二条一丁目１番１号
(74)代理人　100115749
弁理士　谷川　英和
(72)発明者　吉田　晃敏
北海道旭川市緑が丘東二条一丁目１番１号
国立大学法人旭川医科大学内

審査官　和田　財太

(56)参考文献　特開２００７－２２００７５（ＪＰ，Ａ）
特開２００３－１６２５７８（ＪＰ，Ａ）

最終頁に続く

(54)【発明の名称】端末装置、情報システム、情報処理方法、およびプログラム

(57)【特許請求の範囲】
【請求項１】
端末装置の現在の位置を示す位置情報を取得する位置情報取得部と、
現在時刻を取得する時刻取得部と、
前記位置情報取得部が取得した位置情報および前記時刻取得部が取得した時刻に応じて、二以上ある認証方法のうちの一の認証方法を決定する認証方法決定部と、
前記認証方法決定部が決定した一の認証方法に対応する画面を出力する認証画面出力部と、
前記認証画面出力部が出力した画面に対する、ユーザからの情報である認証情報を受け付ける受付部と、
前記認証情報を用いて行われた認証処理の結果である認証結果を受け付ける認証結果受付部と、
前記認証結果を出力する認証結果出力部とを具備する端末装置。
【請求項２】
前記認証方法決定部は、
領域を示す情報である領域情報と時間に関する情報である時間情報とを対応付ける情報である領域認証情報を、２以上格納し得る領域情報格納手段と、
前記位置情報取得部が取得した位置情報および前記時刻取得部が取得した時刻が、前記領域情報格納手段に格納されているいずれかの領域認証情報が有する領域情報および時間情報に合致するか否かを判断する判断手段と、

前記判断手段が、前記位置情報および前記時刻がいずれかの領域認証情報が有する領域情報および時間情報に合致すると判断した場合に、前記二以上の認証方法のうちの一の認証方法を決定する認証方法決定手段とを具備する請求項１記載の端末装置。
【請求項３】
前記領域情報格納手段は、
領域情報と、時間情報と、当該領域情報に対応する認証方法を識別する認証方法識別情報とを対応付ける情報である領域認証情報を、２以上格納しており、
前記判断手段は、
前記位置情報取得部が取得した位置情報および前記時刻取得部が取得した時刻が、前記領域情報格納手段に格納されている２以上の領域認証情報のうちのいずれの領域認証情報が有する領域情報および時間情報に合致するか否かを判断し、
前記認証方法決定手段は、
前記判断手段が合致すると判断した領域認証情報に対応する認証方法識別情報を、前記領域情報格納手段から取得する請求項２記載の端末装置。
【請求項４】
請求項１から請求項３いずれか記載の端末装置と、サーバ装置を具備する情報システムであって、
前記端末装置は、
前記受付部が受け付けた認証情報を、前記サーバ装置に送信する認証情報送信部と、
前記認証結果が認証許可であった場合のみ、所定の処理を行う処理部とをさらに具備し、
前記サーバ装置は、
前記認証情報を受信する認証情報受信部と、
前記認証情報受信部が受信した認証情報を用いた認証処理を行い、認証結果を取得する認証部と、
前記認証部が取得した認証結果を、前記端末装置に送信する認証結果送信部を具備する情報システム。
【請求項５】
第一端末装置と第二端末装置とサーバ装置とを具備する情報システムを構成するサーバ装置であって、
前記第一端末装置は、
当該第一端末装置の位置を示す情報である第一位置情報を格納し得る第一位置情報格納部と、
前記第一位置情報を前記サーバ装置に送信する第一送信部と、
前記サーバ装置から認証結果を受信する第一受信部と、
前記認証結果を出力する第一出力部とを具備し、
前記第二端末装置は、
当該第二端末装置の位置を示す情報である第二位置情報を取得する第二位置情報取得部と、
前記第二位置情報を前記サーバ装置に送信する第二送信部とを具備し、
前記サーバ装置は、
前記第一端末装置から第一位置情報を受信する第一位置情報受信部と、
前記第二端末装置から第二位置情報を受信する第二位置情報受信部と、
前記第一位置情報と前記第二位置情報とが、予め決められた関係を有するか否かを判断し、予め決められた関係を有する場合には認証許可を示す認証結果を取得し、予め決められた関係を有しない場合には認証不許可を示す認証結果を取得する認証部と、
前記認証部が取得した認証結果を、前記第一端末装置に送信する認証結果送信部を具備する情報システムを構成するサーバ装置。
【請求項６】
前記予め決められた関係は、
前記第一位置情報が示す地点と前記第二位置情報が示す地点との距離が、予め決められた

距離より小さいこと、または予め決められた距離以内であることである請求項５記載のサーバ装置。
【請求項７】
位置情報取得部、時刻取得部、認証方法決定部、認証画面出力部、受付部、認証結果受付部、および認証結果出力部により実現される情報処理方法であって、
前記位置情報取得部により、端末装置の現在の位置を示す位置情報を取得する位置情報取得ステップと、
前記時刻取得部により、現在時刻を取得する時刻取得ステップと、
前記認証方法決定部により、前記位置情報取得ステップで取得された位置情報および前記時刻取得ステップで取得された時刻に応じて、二以上ある認証方法のうちの一の認証方法を決定する認証方法決定ステップと、
前記認証画面出力部により、前記認証方法決定ステップで決定された一の認証方法に対応する画面を出力する認証画面出力ステップと、
前記受付部により、前記認証画面出力ステップで出力された画面に対する、ユーザからの情報である認証情報を受け付ける受付ステップと、
前記認証結果受付部により、前記認証情報を用いて行われた認証処理の結果である認証結果を受け付ける認証結果受付ステップと、
前記認証結果出力部により、前記認証結果を出力する認証結果出力ステップを具備する情報処理方法。
【請求項８】
第一位置情報取得手段、第二位置情報取得部、および認証部により実現される情報処理方法であって、
前記第一位置情報取得手段が、第一端末装置の位置を示す第一位置情報を取得する第一位置情報取得ステップと、
前記第二位置情報取得部が、第二端末装置の位置を示す第二位置情報を取得する第二位置情報取得ステップと、
前記認証部が、前記第一位置情報と前記第二位置情報とが、予め決められた関係を有するか否かを判断し、予め決められた関係を有する場合には認証許可を示す認証結果を取得し、予め決められた関係を有しない場合には認証不許可を示す認証結果を取得する認証ステップとを具備する情報処理方法。
【請求項９】
コンピュータを、
端末装置の現在の位置を示す位置情報を取得する位置情報取得部と、
現在時刻を取得する時刻取得部と、
前記位置情報取得部が取得した位置情報および前記時刻取得部が取得した時刻に応じて、二以上ある認証方法のうちの一の認証方法を決定する認証方法決定部と、
前記認証方法決定部が決定した一の認証方法に対応する画面を出力する認証画面出力部と、
前記認証画面出力部が出力した画面に対する、ユーザからの情報である認証情報を受け付ける受付部と、
前記認証情報を用いて行われた認証処理の結果である認証結果を受け付ける認証結果受付部と、
前記認証結果を出力する認証結果出力部として機能させるためのプログラム。
【請求項１０】
コンピュータを、
第一端末装置から、当該第一端末装置の位置を示す情報である第一位置情報を受信する第一位置情報受信部と、
第二端末装置から、当該第二端末装置の位置を示す情報である第二位置情報を受信する第二位置情報受信部と、
前記第一位置情報と前記第二位置情報とが、予め決められた関係を有するか否かを判断し

、予め決められた関係を有する場合には認証許可を示す認証結果を取得し、予め決められた関係を有しない場合には認証不許可を示す認証結果を取得する認証部と、
前記認証部が取得した認証結果を、第一端末装置に送信する認証結果送信部として機能させるためのプログラム。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、位置により認証方法を変更する情報システム等に関するものである。
【背景技術】
【０００２】
従来、或る場所で或る時刻に存在したことの証明に役立つ認証技術を提供する認証システムがあった（例えば、特許文献１参照）。かかる認証システムは、携帯端末装置とサーバとを具備してなる認証システムで、前記携帯端末装置は、撮影手段と、位置情報獲得手段と、通信手段と、前記撮影手段で得た画像情報、前記位置情報獲得手段で得た位置情報、及び該携帯端末装置の識別情報を、前記通信手段を介して送信させる制御手段とを備え、前記サーバは、通信手段と、記憶手段と、タイマと、前記携帯端末装置から送信されて来た情報を該サーバの通信手段が受信した際の前記タイマによる受信時刻情報と、該サーバの通信手段が受信した情報とを関連付けて前記記憶手段に記憶させる制御手段とを備えるシステムである。
【先行技術文献】
【特許文献】
【０００３】
【特許文献１】特開２００９－３７６０号公報（第１頁、第１図等）
【発明の概要】
【発明が解決しようとする課題】
【０００４】
しかしながら、従来の情報システムにおいては、ユーザが居る位置に応じて、認証方法を変えることができなかった。
【課題を解決するための手段】
【０００５】
本第一の発明の端末装置は、端末装置の現在の位置を示す位置情報を取得する位置情報取得部と、位置情報取得部が取得した位置情報に応じて、二以上ある認証方法のうちの一の認証方法を決定する認証方法決定部と、認証方法決定部が決定した一の認証方法に対応する画面を出力する認証画面出力部と、認証画面出力部が出力した画面に対する、ユーザからの情報である認証情報を受け付ける受付部と、認証情報を用いて行われた認証処理の結果である認証結果を受け付ける認証結果受付部と、認証結果を出力する認証結果出力部とを具備する端末装置である。
【０００６】
かかる構成により、ユーザが居る位置に応じて、認証方法を変えることができる。そのため、例えば、普段、ユーザが存在する場所や、居ることが予想される場所では、簡易な認証方法を採用し、簡単、迅速な認証が可能となり、ユーザが行き慣れていない場所では、厳重な認証方法を採用することにより、高度なセキュリティーを担保できる。
【０００７】
また、本第二の発明の端末装置は、第一に対して、認証方法決定部は、領域を示す情報である領域情報を、１以上格納し得る領域情報格納手段と、位置情報取得部が取得した位置情報の示す位置が、領域情報格納手段に格納されている１以上の領域情報が示す１以上の領域のいずれかに含まれるか否かを判断する判断手段と、判断手段が、位置情報の示す位置が１以上の領域のいずれかに含まれると判断した場合に、二以上の認証方法のうちの一の認証方法を決定する認証方法決定手段とを具備する端末装置である。
【０００８】

かかる構成により、普段、ユーザが存在する場所や、居ることが予想される場所を登録することにより、かかる場所では、簡易な認証方法を採用し、簡単、迅速な認証が可能となり、ユーザが行き慣れていない場所等では、厳重な認証方法を採用することにより、高度なセキュリティーを担保できる。

【０００９】

また、本第三の発明の端末装置は、第二に対して、二以上の認証方法は、第一の認証方法、および第一の認証方法よりセキュリティーレベルの高い第二の認証方法を含み、認証方法決定手段は、判断手段が、位置情報の示す位置が１以上の領域のいずれかに含まれると判断した場合に、二以上の認証方法のうちの第一の認証方法に決定し、判断手段が、位置情報の示す位置が１以上の領域のいずれにも含まれないと判断した場合に、二以上の認証方法のうちの第二の認証方法に決定する端末装置である。

【００１０】

かかる構成により、普段、ユーザが存在する場所や、居ることが予想される場所を登録することにより、かかる場所では、簡易な認証方法を採用し、簡単、迅速な認証が可能となり、ユーザが行き慣れていない場所等では、厳重な認証方法を採用することにより、高度なセキュリティーを担保できる。

【００１１】

また、本第四の発明の端末装置は、第二に対して、領域情報格納手段は、領域情報と、領域情報に対応する認証方法を識別する認証方法識別情報とを対応付ける情報である領域認証情報を、２以上格納しており、判断手段は、位置情報取得部が取得した位置情報の示す位置が含まれる領域を、領域情報格納手段に格納されている１以上の領域情報を用いて判断し、認証方法決定手段は、判断手段が判断した領域に対応する領域情報と対応付けられた認証方法識別情報を、領域情報格納手段から取得する端末装置である。

【００１２】

かかる構成により、領域を３以上に分けた場合、その領域に適した３以上の認証方法を採用できる。

【００１３】

また、本第五の発明の端末装置は、第二に対して、二以上の認証方法は、第一の認証方法、および認証処理を行わない第二の認証方法を含み、認証方法決定手段は、判断手段が、位置情報の示す位置が１以上の領域のいずれかに含まれると判断した場合に、認証処理を行わない第二の認証方法に決定し、判断手段が、位置情報の示す位置が１以上の領域のいずれにも含まれないと判断した場合に、第一の認証方法に決定する端末装置である。

【００１４】

かかる構成により、特定の場所に居る場合のみ、認証処理を行わせることができる。

【００１５】

また、本第六の発明の情報システムは、端末装置と、サーバ装置を具備する情報システムであって、端末装置は、受付部が受け付けた認証情報を、サーバ装置に送信する認証情報送信部と、サーバ装置が行った認証処理の結果である認証結果を受信する認証結果受信部と、認証結果が認証許可であった場合のみ、所定の処理を行う処理部とをさらに具備し、サーバ装置は、認証情報を受信する認証情報受信部と、認証情報受信部が受信した認証情報を用いた認証処理を行い、認証結果を取得する認証部と、認証部が取得した認証結果を、端末装置に送信する認証結果送信部を具備する情報システムである。

【００１６】

かかる構成により、情報システムにおいて、ユーザが居る位置に応じて、認証方法を変えることができる。そのため、例えば、普段、ユーザが存在する場所や、居ることが予想される場所では、簡易な認証方法を採用し、簡単、迅速な認証が可能となり、ユーザが行き慣れていない場所では、厳重な認証方法を採用することにより、高度なセキュリティーを担保できる。

【００１７】

また、本第七の発明の情報システムは、第一端末装置と第二端末装置とサーバ装置とを

具備する情報システムであって、第一端末装置は、第一端末装置の位置を示す情報である第一位置情報を格納し得る第一位置情報格納部と、第一位置情報をサーバ装置に送信する第一送信部と、サーバ装置から認証結果を受信する第一受信部と、認証結果を出力する第一出力部とを具備し、第二端末装置は、第二端末装置の位置を示す情報である第二位置情報を取得する第二位置情報取得部と、第二位置情報をサーバ装置に送信する第二送信部とを具備し、サーバ装置は、第一端末装置から第一位置情報を受信する第一位置情報受信部と、第二端末装置から第二位置情報を受信する第二位置情報受信部と、第一位置情報と第二位置情報とが、予め決められた関係を有するか否かを判断し、予め決められた関係を有する場合には認証許可を示す認証結果を取得し、予め決められた関係を有しない場合には認証不許可を示す認証結果を取得する認証部と、認証部が取得した認証結果を、第一端末装置に送信する認証結果送信部を具備する情報システムである。

【００１８】

かかる構成により、例えば、ユーザが保持している第二端末装置と、病院などに設置されている第一端末装置が近く（例えば、同じ部屋に居る程度の近さ）に存在する場合、認証許可となり、第一端末装置に情報がダウンロードされ得る。

【発明の効果】

【００１９】

本発明による情報システムによれば、ユーザが居る位置に応じて、認証方法を変えることができる。

【図面の簡単な説明】

【００２０】

【図１】実施の形態１における情報システム１の概念図
【図２】同情報システムのブロック図
【図３】同端末装置の動作について説明するフローチャート
【図４】同サーバ装置の動作について説明するフローチャート
【図５】同領域認証情報管理表を示す図
【図６】同カルテ情報管理表を示す図
【図７】同認証画面の例を示す図
【図８】同第二端末１２に出力された第二認証情報の例を示す図
【図９】同第二の認証画面の例を示す図
【図１０】同認証画面の例を示す図
【図１１】同第二の認証画面の例を示す図
【図１２】同領域認証情報管理表を示す図
【図１３】同情報システムの別のブロック図
【図１４】実施の形態２における情報システムのブロック図
【図１５】同サーバ装置の動作について説明するフローチャート
【図１６】同第二の認証画面の例を示す図
【図１７】同コンピュータシステムの概観図
【図１８】同コンピュータシステムの内部構成を示す図

【発明を実施するための形態】

【００２１】

以下、情報システム等の実施形態について図面を参照して説明する。なお、実施の形態において同じ符号を付した構成要素は同様の動作を行うので、再度の説明を省略する場合がある。

【００２２】

（実施の形態１）

本実施の形態において、位置情報を取得し、当該位置情報により、認証方法を変更する情報システム１について説明する。また、本実施の形態において、時刻（時間帯）によっても、認証方法を変更する情報システム１について説明する。

【００２３】

図１は、本実施の形態における情報システム１の概念図である。情報システム１は、端末装置１１、第二端末１２、およびサーバ装置１３を具備する。端末装置１１および第二端末１２は、例えば、いわゆるパーソナルコンピュータまたは携帯端末（携帯電話を含む）である。サーバ装置１３は、端末装置１１および第二端末１２と通信可能な装置であり、認証処理を行う装置である。なお、情報システム１において、第二端末１２は必須ではない。つまり、情報システム１は、端末装置１１、およびサーバ装置１３を具備する構成でも良い。

【００２４】

図２は、本実施の形態における情報システム１のブロック図である。

【００２５】

端末装置１１は、受付部１１１、位置情報取得部１１２、認証方法決定部１１３、認証画面出力部１１４、認証情報送信部１１５、認証結果受付部１１６、認証結果出力部１１７、処理部１１８を具備する。

【００２６】

認証方法決定部１１３は、領域情報格納手段１１３１、判断手段１１３２、認証方法決定手段１１３３を具備する。

【００２７】

第二端末１２は、第二受付部１２１、第二送受信部１２２、第二出力部１２３を具備する。

【００２８】

サーバ装置１３は、データ格納部１３１、認証情報受信部１３２、認証部１３３、認証結果送信部１３４、データ送受信部１３５を具備する。

【００２９】

認証部１３３は、第一認証手段１３３１、第二認証手段１３３２、第三認証手段１３３３を具備する。なお、認証部１３３は、２つの認証手段だけでも良いし、４つ以上の認証手段を有しても良い。

【００３０】

受付部１１１は、ユーザからの入力を受け付ける。受付部１１１は、認証処理が必要な処理を実行する命令の入力を受け付ける。この命令は、例えば、サーバ装置１３にログインする命令や、サーバ装置１３にアクセスする命令である。受付部１１１は、例えば、認証画面出力部１１４が出力した画面に対する、認証情報を受け付ける。認証情報とは、認証処理に必要な情報である。認証情報は、通常、ユーザが入力した情報である。認証情報とは、例えば、ユーザIDとパスワードである。また、例えば、認証情報は、２つのＩＤを有しても良い。

【００３１】

認証情報等の入力手段は、キーボードやマウスやテンキーやメニュー画面によるもの等、何でも良い。受付部１１１は、キーボード等の入力手段のデバイスドライバーや、メニュー画面の制御ソフトウェア等で実現され得る。

【００３２】

位置情報取得部１１２は、端末装置１１の現在の位置を示す位置情報を取得する。位置情報は、例えば、（緯度、経度）の情報である。また、位置情報は、例えば、場所を特定する情報（例えば、住所や地名など）である。位置情報取得部１１２は、例えば、ＧＰＳ受信機である。また、位置情報取得部１１２は、例えば、携帯電話の３つの基地局からの電波の受信状況に応じて、位置情報を取得しても良い。また、位置情報取得部１１２は、例えば、近距離無線通信手段により、場所を特定する情報を受信する。

【００３３】

認証方法決定部１１３は、位置情報取得部１１２が取得した位置情報に応じて、二以上ある認証方法のうちの一の認証方法を決定する。認証方法決定部１１３は、位置情報取得部１１２が取得した位置情報および時刻に応じて、二以上ある認証方法のうちの一の認証方法を決定しても良い。認証方法決定部１１３は、時刻のみに応じて、二以上ある認証方

法のうちの一の認証方法を決定しても良い。認証方法決定部１１３は、時刻を用いる場合、自身が保持している時計、または外部のサーバ装置（例えば、ＮＴＰサーバ）から時刻を取得する。なお、図示しない時刻取得部は、現在時刻を取得しても良い。また、時刻とは、時間帯の情報（例えば、９：００～１９：００や、２２：００～８：００など）でも良い趣旨である。また、認証方法の決定とは、例えば、認証方法を識別する情報である認証方法識別情報を取得することである。また、認証方法の決定とは、例えば、複数ある認証方法を実現する処理のうち、一の処理へ移行する制御を言う。また、認証方法とは、端末装置１１の認証の方法、端末装置１１のユーザの認証の方法などである。複数の認証方法のうちの一の認証方法は、認証処理しない、ことを含んでも良い。認証方法決定部１１３は、通常、ＭＰＵやメモリ等から実現され得る。認証方法決定部１１３の処理手順は、通常、ソフトウェアで実現され、当該ソフトウェアはＲＯＭ等の記録媒体に記録されている。但し、ハードウェア（専用回路）で実現しても良い。

【００３４】

領域情報格納手段１１３１は、領域を示す情報である領域情報を、１以上格納し得る。領域情報は、例えば、矩形の領域を特定する左上の位置情報（経度１、緯度１）と、右下の位置情報（経度２、緯度２）である。また、領域情報は、地方公共団体の名称などでも良い。また、領域情報格納手段１１３１は、領域情報と認証方法識別情報とを対応付ける情報である領域認証情報を、２以上格納していても良い。認証方法識別情報とは、認証方法を識別する情報である。また、領域情報格納手段１１３１は、領域情報と時間情報と認証方法識別情報とを対応付ける情報である領域認証情報を、２以上格納していても良い。時間情報とは、時間に関する情報であり、時刻を示す情報や時間帯や曜日を示す情報などである。ここで、「領域情報と、認証方法識別情報とが対応付ける」とは、領域情報と認証方法識別情報の一方の情報から、他方の情報を取得できればよいという意味である。したがって、対応情報は、領域情報と認証方法識別情報とを組として含む情報を有してもよく、領域情報と認証方法識別情報とをリンク付ける情報であってもよい。後者の場合には、対応情報は、例えば、領域情報と認証方法識別情報の格納されている位置を示すポインタやアドレスとを対応付ける情報であってもよい。本実施の形態では、前者の場合について説明する。また、領域情報と認証方法識別情報とは、直接対応付けられていなくてもよい。例えば、領域情報に、第３の情報が対応しており、その第３の情報に認証方法識別情報が対応していてもよい。領域情報格納手段１１３１は、不揮発性の記録媒体が好適であるが、揮発性の記録媒体でも実現可能である。領域情報格納手段１１３１に領域情報等が記憶される過程は問わない。例えば、記録媒体を介して領域情報等が領域情報格納手段１１３１で記憶されるようになってもよく、通信回線等を介して送信された領域情報等が領域情報格納手段１１３１で記憶されるようになってもよく、あるいは、入力デバイスを介して入力された領域情報等が領域情報格納手段１１３１で記憶されるようになってもよい。

【００３５】

判断手段１１３２は、位置情報取得部１１２が取得した位置情報の示す位置が、領域情報格納手段１１３１に格納されている１以上の領域情報が示す１以上の領域のいずれかに含まれるか否かを判断する。また、判断手段１１３２は、位置情報取得部１１２が取得した位置情報の示す位置が含まれる領域を、領域情報格納手段１１３１に格納されている１以上の領域情報を用いて決定しても良い。また、判断手段１１３２は、位置情報取得部１１２が取得した位置情報と現在時刻が、領域情報格納手段１１３１に格納されている領域情報および時間情報に合致するか否かを判断する。判断手段１１３２は、通常、ＭＰＵやメモリ等から実現され得る。判断手段１１３２の処理手順は、通常、ソフトウェアで実現され、当該ソフトウェアはＲＯＭ等の記録媒体に記録されている。但し、ハードウェア（専用回路）で実現しても良い。

【００３６】

認証方法決定手段１１３３は、判断手段１１３２が、位置情報の示す位置が１以上の領域のいずれかに含まれると判断した場合に、二以上の認証方法のうちの一の認証方法を決

定する。また、認証方法決定手段１１３３は、判断手段１１３２が、位置情報取得部１１２が取得した位置情報と現在時刻が、領域情報格納手段１１３１に格納されている領域情報および時間情報に合致すると判断した場合に、二以上の認証方法のうちの一の認証方法を決定する。例えば、二以上の認証方法が、第一の認証方法、および当該第一の認証方法よりセキュリティーレベルの高い第二の認証方法を含む場合であり、かつ、判断手段１１３２が、位置情報の示す位置が１以上の領域のいずれかに含まれると判断した場合に、認証方法決定手段１１３３は、二以上の認証方法のうちの第一の認証方法に決定し、判断手段１１３２が、位置情報の示す位置が１以上の領域のいずれかに含まれないと判断した場合に、二以上の認証方法のうちの第二の認証方法に決定する。なお、第一の認証方法より第二の認証方法のセキュリティーレベルの高い、とは、例えば、ユーザが入力するデータの数や種類が第一の認証方法より第二の認証方法の方が多いことである。データの種類について、ＩＤとパスワードは異なるデータの種類である。また、第一の認証方法より第二の認証方法の方がセキュリティーレベルの高い、とは、例えば、利用する端末の数が、第一の認証方法より第二の認証方法の方が多いことである。また、第一の認証方法より第二の認証方法の方がセキュリティーレベルの高い、とは、例えば、利用する端末のセキュリティーのレベルが、第一の認証方法よりの方が高いことである。いわゆるＰＣのセキュリティーのレベルより、ユーザの特定が運用上なされている携帯電話の方がセキュリティーのレベルが高い。

【００３７】

認証方法決定手段１１３３は、判断手段１１３２が判断した領域に対応する領域情報と対応付けられた認証方法識別情報を、領域情報格納手段１１３１から取得することは好適である。

【００３８】

認証方法決定手段１１３３は、通常、ＭＰＵやメモリ等から実現され得る。認証方法決定手段１１３３の処理手順は、通常、ソフトウェアで実現され、当該ソフトウェアはＲＯＭ等の記録媒体に記録されている。但し、ハードウェア（専用回路）で実現しても良い。

【００３９】

認証画面出力部１１４は、認証方法決定部１１３が決定した一の認証方法に対応する画面を出力する。認証画面出力部１１４は、例えば、自身で格納している画面の情報のうち、認証方法決定部１１３が決定した一の認証方法に対応する画面の情報を用いて、画面を構成して、出力する。また、認証画面出力部１１４は、認証方法決定部１１３が決定した一の認証方法を識別する情報を用いて、サーバ装置１３にアクセスし、サーバ装置１３から、一の認証方法に対応する画面の情報を受信し、当該画面の情報を用いて、画面を構成して、出力しても良い。認証画面出力部１１４は、認証方法決定部１１３が決定した一の認証方法に対応する画面を、結果として出力すれば良く、その画面の元になる情報の存在場所や、画面の出力アルゴリズムは問わない。なお、ここで、画面とは、認証するための情報を入力する画面である。また、認証方法に応じた画面が存在することが好適であるが、画面は一つでも良い。画面が一つである場合、例えば、認証方法により、入力する情報（利用するｒフィールド）が異なることは好適である。また、認証方法が異なる場合でも、画面が同一でも良い。かかる場合、認証のアルゴリズムが異なることは好適である。

【００４０】

認証画面出力部１１４は、ディスプレイやスピーカー等の出力デバイスを含むと考えても含まないと考えても良い。認証画面出力部１１４は、出力デバイスのドライバーソフトまたは、出力デバイスのドライバーソフトと出力デバイス等で実現され得る。

【００４１】

認証情報送信部１１５は、受付部１１１が受け付けた認証情報を、サーバ装置１３に送信する。認証情報送信部１１５は、通常、無線または有線の通信手段で実現されるが、放送手段で実現されても良い。

【００４２】

認証結果受付部１１６は、認証情報を用いて行われた認証処理の結果である認証結果を

受け付ける。認証結果受付部１１６は、通常、サーバ装置１３から認証結果を受信する。ただし、端末装置１１が認証処理する場合などは、認証結果受付部１１６は、図示しない指針の認証処理手段が行った認証結果を取得する。ここで、認証結果とは、認証許可を示す情報（例えば「１」）、または不許可を示す情報（例えば「０」）などである。認証結果受付部１１６は、例えば、無線または有線の通信手段で実現されるが、放送手段で実現されても良い。

【００４３】

認証結果出力部１１７は、認証結果受付部１１６が受け付けた認証結果を出力する。ここで、出力とは、ディスプレイへの表示、プロジェクターを用いた投影、プリンタへの印字、音出力、外部の装置への送信、記録媒体への蓄積、他の処理装置や他のプログラム等への処理結果の引渡し等を含む概念である。認証結果出力部１１７は、ディスプレイやスピーカー等の出力デバイスを含むと考えても含まないと考えても良い。認証結果出力部１１７は、出力デバイスのドライバーソフトまたは、出力デバイスのドライバーソフトと出力デバイス等で実現され得る。

【００４４】

処理部１１８は、認証結果が認証許可であった場合のみ、所定の処理を行う。所定の処理とは、例えば、受付部１１１が受け付けた命令（例えば、サーバ装置１３上のデータベースへのアクセス命令）をサーバ装置１３に送信し、サーバ装置１３からデータを受信し、出力する処理である。なお、所定の処理とは、何でも良い。さらに、処理部１１８は、認証結果に応じて、異なる処理を行っても良い。処理部１１８は、通常、ＭＰＵやメモリ等から実現され得る。処理部１１８の処理手順は、通常、ソフトウェアで実現され、当該ソフトウェアはＲＯＭ等の記録媒体に記録されている。但し、ハードウェア（専用回路）で実現しても良い。

【００４５】

第二受付部１２１は、第二端末１２のユーザからの入力を受け付ける。例えば、第二受付部１２１は、第二端末１２のユーザから、ＩＤを受け付ける。かかる場合の入力手段は、キーボードやマウスやテンキーやメニュー画面によるもの等、何でも良い。第二受付部１２１は、キーボード等の入力手段のデバイスドライバーや、メニュー画面の制御ソフトウェア等で実現され得る。

【００４６】

第二送受信部１２２は、第二受付部１２１が受け付けた情報（入力）を、サーバ装置１３に送信する。また、第二送受信部１２２は、サーバ装置１３から情報を受信する。第二送信部１２２は、通常、無線または有線の通信手段で実現されるが、放送手段で実現されても良い。

【００４７】

第二出力部１２３は、サーバ装置１３から受信した情報を出力する。第二出力部１２３は、ディスプレイやスピーカー等の出力デバイスを含むと考えても含まないと考えても良い。第二出力部１２３は、出力デバイスのドライバーソフトまたは、出力デバイスのドライバーソフトと出力デバイス等で実現され得る。

【００４８】

データ格納部１３１は、各種のデータが格納され得る。各種のデータとは、例えば、端末装置１１のユーザごとのカルテ情報である。カルテ情報とは、例えば、氏名、年齢、性別、病歴、現在の病気、服用している薬、家族の病気情報等の情報である。データ格納部１３１は、不揮発性の記録媒体が好適であるが、揮発性の記録媒体でも実現可能である。

【００４９】

認証情報受信部１３２は、端末装置１１、または端末装置１１と第二端末１２から認証情報を受信する。認証情報受信部１３２は、通常、無線または有線の通信手段で実現されるが、放送を受信する手段で実現されても良い。

【００５０】

認証部１３３は、認証情報受信部１３２が受信した認証情報を用いた認証処理を行い、

認証結果を取得する。なお、２以上の認証情報を用いて、認証処理を行う場合もある。認証部１３３は、２以上の認証手段を有する。なお、ここでは、主として、認証部１３３は、第一認証手段１３３１、第二認証手段１３３２、および第三認証手段１３３３を有する、として説明する。また、２以上の各認証手段の認証方法は異なる。認証部１３３は、通常、ＭＰＵやメモリ等から実現され得る。認証部１３３の処理手順は、通常、ソフトウェアで実現され、当該ソフトウェアはＲＯＭ等の記録媒体に記録されている。但し、ハードウェア（専用回路）で実現しても良い。

【００５１】

第一認証手段１３３１は、例えば、端末装置１１のＩＤとパスワードからなる認証情報を用いて、認証を行う。つまり、第一認証手段１３３１は、ＩＤとパスワードの組を１以上格納しており、認証情報受信部１３２が受信した認証情報が有するＩＤとパスワードに一致する組を検索し、一致する組が存在すれば認証許可とし、一致する組が存在しなければ認証不許可として、認証結果に対応する情報（例えば、認証許可の場合は「１」、認証不許可の場合は「０」）を取得する。なお、ＩＤとパスワードの組は、例えば、データ格納部１３１が保持していても良い。

【００５２】

第二認証手段１３３２は、例えば、端末装置１１のＩＤとパスワードからなる認証情報、および第二端末１２に送信された第二認証情報（一時的な認証情報）を用いて、認証処理を行う。つまり、例えば、第二認証手段１３３２は、ＩＤとパスワードの組を１以上格納しており、認証情報受信部１３２が受信した認証情報が有するＩＤとパスワードに一致する組を検索し、一致する組が存在すれば、第二端末１２に第二認証情報を送信し、当該第二認証情報が端末装置１１から送信されてきた場合に、認証許可とする。一方、認証情報に一致する組がない場合、または端末装置１１から送信されてきた第二認証情報が第二端末１２に送信した第二認証情報と一致しない場合は、認証不許可とする。

【００５３】

第三認証手段１３３３は、例えば、端末装置１１の２つのＩＤと２つのパスワードからなる認証情報、および第二端末１２に送信された第二認証情報（一時的な認証情報）を用いて、認証処理を行う。なお、第三認証手段１３３３は、例えば、まず、第一のＩＤとパスワードにより、１回目の認証処理を行った後、第二のＩＤとパスワード、および第二認証情報を用いて、２回目の認証処理を行う。

【００５４】

第一認証手段１３３１、第二認証手段１３３２、および第三認証手段１３３３は、通常、ＭＰＵやメモリ等から実現され得る。第一認証手段１３３１等の処理手順は、通常、ソフトウェアで実現され、当該ソフトウェアはＲＯＭ等の記録媒体に記録されている。但し、ハードウェア（専用回路）で実現しても良い。

【００５５】

認証結果送信部１３４は、認証部１３３が取得した認証結果（最終的な認証結果）を、端末装置１１に送信する。認証結果送信部１３４は、通常、無線または有線の通信手段で実現されるが、放送手段で実現されても良い。

【００５６】

データ送受信部１３５は、端末装置１１から命令を受信し、当該命令に対応するデータを端末装置１１に送信する。なお、データは、データ格納部１３１に格納されているデータである。データ送受信部１３５は、通常、無線または有線の通信手段で実現されるが、放送を受信する手段で実現されても良い。

【００５７】

次に、情報システム１の動作について説明する。まず、端末装置１１の動作について、図３のフローチャートを用いて説明する。

【００５８】

（ステップＳ３０１）受付部１１１は、認証処理が必要な処理を実行する命令の入力を受け付けたか否かを判断する。かかる命令の入力を受け付ければステップＳ３０２に行き

、命令の入力を受け付けなければステップＳ３０１に戻る。

【００５９】

（ステップＳ３０２）位置情報取得部１１２は、端末装置１１の現在の位置を示す位置情報を取得する。また、図示しない時刻取得部は、現在時刻を取得する。なお、現在時刻の取得は必須ではない。

【００６０】

（ステップＳ３０３）認証方法決定部１１３は、ステップＳ３０２で取得された位置情報（または、位置情報と現在時刻）に応じて、二以上ある認証方法のうちの一の認証方法を決定する。認証方法の決定アルゴリズムは、例えば、以下である。つまり、判断手段１１３２は、ステップＳ３０２で取得された位置情報（または、位置情報と現在時刻）を用いて、領域情報格納手段１１３１を検索する。そして、認証方法決定手段１１３３は、ステップＳ３０２で取得された位置情報（または、位置情報と現在時刻）に合致する領域情報（または、領域情報および時間情報）に対応する認証方法識別情報を、領域情報格納手段１１３１から取得する。

【００６１】

（ステップＳ３０４）認証画面出力部１１４は、ステップＳ３０３で決定された認証方法が第一認証方法であるか否かを判断する。第一認証方法であればステップＳ３０５に行き、第一認証方法でなければステップＳ３０６に行く。

【００６２】

（ステップＳ３０５）認証画面出力部１１４は、第一認証方法に対応する認証のための画面（認証画面）を出力する。なお、例えば、認証画面出力部１１４は、第一認証方法に対応する画面定義情報（例えば、ＨＴＭＬのデータ）を読み込み、当該画面定義情報を解釈し、認証画面を出力する。なお、かかる場合、認証画面出力部１１４は、認証方法を識別する情報と対応付けて、画面定義情報を保持している。また、第一認証方法に対応する画面出力のプログラム（関数、メソッドなどでも良い）を呼び出しても良い。ステップＳ３０９に行く。

【００６３】

（ステップＳ３０６）認証画面出力部１１４は、ステップＳ３０３で決定された認証方法が第二認証方法であるか否かを判断する。第二認証方法であればステップＳ３０７に行き、第二認証方法でなければステップＳ３０８に行く。

【００６４】

（ステップＳ３０７）認証画面出力部１１４は、第二認証方法に対応する認証のための画面（認証画面）を出力する。ステップＳ３０９に行く。

【００６５】

（ステップＳ３０８）認証画面出力部１１４は、第三認証方法に対応する認証のための画面（認証画面）を出力する。ステップＳ３０９に行く。

【００６６】

（ステップＳ３０９）受付部１１１は、ユーザから、認証情報を受け付けたか否かを判断する。認証情報を受け付ければステップＳ３１０に行き、認証情報を受け付けなければステップＳ３０９に戻る。

【００６７】

（ステップＳ３１０）認証情報送信部１１５は、ステップＳ３０９で受け付けられた認証情報を、サーバ装置１３に送信する。

【００６８】

（ステップＳ３１１）認証結果受付部１１６は、認証情報を用いて行われた認証処理の結果である認証結果を、サーバ装置１３から受信したか否かを判断する。認証結果を受信すればステップＳ３１２に行き、受信しなければステップＳ３１１に戻る。

【００６９】

（ステップＳ３１２）認証結果出力部１１７は、認証結果受付部１１６が受け付けた認証結果を出力する。なお、ここでの認証結果は、最終的な認証結果である。なお、認証結

果の出力は必須ではない。

【００７０】

（ステップＳ３１３）処理部１１８は、認証結果が認証許可であるか否かを判断する。認証許可であればステップＳ３１４に行き、認証不許可であればステップＳ３０１に戻る。

【００７１】

（ステップＳ３１４）処理部１１８は、ユーザの入力に応じた、所定の処理を行う。ステップＳ３０１に戻る。

【００７２】

なお、図３のフローチャートにおいて、ステップＳ３１４における処理の内容は問わない。

【００７３】

また、図３のフローチャートにおいて、電源オフや処理終了の割り込みにより処理は終了する。

【００７４】

次に、第二端末１２の動作について説明する。第二端末１２の第二受付部１２１は、第二端末１２のユーザからの入力を受け付ける。そして、第二送受信部１２２は、第二受付部１２１が受け付けた情報（入力）を、サーバ装置１３に送信する。また、サーバ装置１３から情報を受信しても良い。そして、第二出力部１２３は、第二送受信部１２２が受信した情報を出力する。なお、この情報は、例えば、認証のために必要な情報である。

【００７５】

次に、サーバ装置１３の動作について、図４のフローチャートを用いて説明する。

【００７６】

（ステップＳ４０１）認証情報受信部１３２は、端末装置１１、または端末装置１１と第二端末１２から認証情報を受信したか否かを判断する。なお、認証情報には、例えば、認証方法を識別する認証方法識別情報が含まれる。

【００７７】

（ステップＳ４０２）認証部１３３は、認証情報受信部１３２が受信した認証情報に含まれる認証方法識別情報に対応する認証処理を行い、認証結果を取得する。認証処理の内容の例については、上述した通りである。

【００７８】

（ステップＳ４０３）認証結果送信部１３４は、ステップＳ４０２で取得された認証結果を、端末装置１１に送信する。ステップＳ４０１に戻る。

【００７９】

（ステップＳ４０４）データ送受信部１３５は、端末装置１１から命令（データ送信指示の命令）を受信したか否かを判断する。命令を受信すればステップＳ４０５に行き、命令を受信しなければステップＳ４０１に戻る。

【００８０】

（ステップＳ４０５）データ送受信部１３５は、ステップＳ４０４で受信された命令にしたがって、データ格納部１３１に格納されているデータを取得する。

【００８１】

（ステップＳ４０６）データ送受信部１３５は、ステップＳ４０５で受信したデータを、端末装置１１に送信する。

【００８２】

なお、図４のフローチャートにおいて、認証後に行われた処理は、データの検索、送信の処理であったが、処理の内容は問わない。

【００８３】

また、図４のフローチャートにおいて、電源オフや処理終了の割り込みにより処理は終了する。

【００８４】

以下、本実施の形態における情報システム１の具体的な動作について説明する。情報システム１の概念図は図１である。

【００８５】

今、領域情報格納手段１１３１は、図５に示す領域認証情報管理表を保持している。領域認証情報管理表は、「ＩＤ」「領域情報」「時間情報」「認証方法識別情報」の属性値を有するレコードを１以上保持している。「ＩＤ」は、レコードを識別する情報である。「ＩＤ＝１、２」の「領域情報」の（x_1，y_1）（x_2，y_2）は、それぞれ（緯度，経度）であり、矩形の領域を示す。なお、領域情報（x_1，y_1）（x_2，y_2）で示される矩形の領域は、端末装置１１のユーザ（ユーザ１～ユーザ３）が、かかりつけの病院（病院Ａ）の敷地の領域を示す。また、「ＩＤ＝３」の「その他」は、領域情報（x_1，y_1）（x_2，y_2）以外の場合に、適用されることを示す。つまり、領域認証情報管理表の「ＩＤ＝１」のレコードは、病院Ａの時間帯「９：００－１８：００」（例えば、通常の診療時間）における認証方法は、「方法１」を採用することを示す。また、領域認証情報管理表の「ＩＤ＝２」のレコードは、病院Ａの時間帯「１８：０１－８：５９」（例えば、診療時間外）における認証方法は、「方法２」を採用することを示す。さらに、領域認証情報管理表の「ＩＤ＝３」のレコードは、病院Ａ以外の領域では、「方法３」の認証方法が採用されることを示す。また、認証方法のセキュリティレベルは「方法１＜方法２＜方法３」である、とする。つまり、方法１は、第一認証手段１３３１により実現される。方法２は、第二認証手段１３３２により実現される。方法３は、第三認証手段１３３３により実現される。

【００８６】

また、データ格納部１３１は、図６に示すカルテ情報管理表を保持している。カルテ情報管理表は、患者の病歴などの情報（カルテ情報）や、認証に必要な情報を管理している。カルテ情報管理表は、「Ｎｏ．」「第一認証情報」「第二認証情報」「端末識別情報」「出力情報」を有するレコードを1以上保持している。「Ｎｏ．」は、レコードを識別する情報である。「第一認証情報」は、第一認証手段１３３１、第二認証手段１３３２、および第三認証手段１３３３が利用する「ＩＤ１」「ＰＷ１」を有する。「第二認証情報」は、第三認証手段１３３３のみが利用する「ＩＤ２」「ＰＷ２」を有する。「ＩＤ１」「ＩＤ２」は、サーバ装置１３にログインまたはアクセスするために必要なＩＤである。「ＰＷ１」「ＰＷ２」は、サーバ装置１３にログインまたはアクセスするために必要なパスワードである。「端末識別情報」は、第二端末１２を識別する情報であり、ここでは、第二端末１２の電話番号である。なお、第二端末１２は、ここでは、例えば、いわゆる携帯電話である。また、「出力情報」は、第二端末１２のユーザ（患者）の属性や、病気に関する情報であるカルテ情報（医療情報）などを有する。

【００８７】

かかる場合、以下の３つの具体例について説明する。

（具体例１）

【００８８】

ユーザ１は、かかりつけの病院Ａに病気を診てもらうために、かかりつけの医師Ｘの元に出かけた、とする。そして、医師Ｘは、病院Ａ内に設置された端末装置１１を利用して、本ユーザ１のカルテ情報を、サーバ装置１３から取得しようとする、とする。

【００８９】

そして、医師Ｘは、端末装置１１に対して、サーバ装置１３へのアクセスの命令の入力を行った。

【００９０】

次に、端末装置１１は、サーバ装置１３へのアクセスの命令の入力を受け付ける。そして、位置情報取得部１１２であるＧＰＳ受信機は、端末装置１１の現在の位置を示す位置情報（x_3，y_3）を取得する。また、図示しない時刻取得部は、現在時刻「９：４５」を取得する、とする。

【００９１】

次に、認証方法決定部１１３は、取得された位置情報（x_3，y_3）と現在時刻「９：４５」を用いて、図５に示す領域認証情報管理表を検索する。そして、認証方法決定部１１３は、位置情報（x_3，y_3）は、領域情報（x_1，y_1）（x_2，y_2）で示される矩形の領域内であることを検知する。そして、認証方法決定部１１３は、現在時刻「９：４５」が「９：００－１８：００」に合致する、と判断する。そして、認証方法識別情報「方法１」を取得する。

【００９２】

次に、認証画面出力部１１４は、決定された認証方法が認証方法識別情報「方法１」に対応する認証画面を、図７に示すように表示する。

【００９３】

そして、医師Ｘは、ユーザ１のカルテ情報にアクセスするために、ＩＤ「５６３１」、ＰＷ「ａｂｃ」を入力し、「ログイン」ボタンを押下した、とする。なお、例えば、医師Ｘは、ユーザ１からＩＤ「５６３１」、ＰＷ「ａｂｃ」を聞いて、入力しても良い。

【００９４】

すると、認証情報送信部１１５は、認証情報「方法１、ＩＤ：５６３１、ＰＷ：ａｂｃ」を構成し、当該認証情報を、サーバ装置１３に送信する。

【００９５】

次に、サーバ装置１３の認証情報受信部１３２は、認証情報「方法１、ＩＤ：５６３１、ＰＷ：ａｂｃ」を受信する。

【００９６】

そして、認証部１３３は、認証情報受信部１３２が受信した認証情報に含まれる「方法１」から、第一認証手段１３３１を呼び出し、第一認証手段１３３１に「ＩＤ：５６３１、ＰＷ：ａｂｃ」を渡す。

【００９７】

次に、第一認証手段１３３１は、「ＩＤ：５６３１、ＰＷ：ａｂｃ」に合致する第一認証情報が、図６のカルテ情報管理表に、存在するか否かを判断する。そして、第一認証手段１３３１は、図６のカルテ情報管理表の「ＩＤ＝１」のレコードが、「ＩＤ：５６３１、ＰＷ：ａｂｃ」に合致する、と判断する。

【００９８】

そして、認証部１３３は、認証結果「認証許可」を取得する。

【００９９】

次に、認証結果送信部１３４は、取得された認証結果「認証許可」を、端末装置１１に送信する。

【０１００】

次に、認証結果受付部１１６は、認証結果「認証許可」を、サーバ装置１３から受信する。そして、認証結果出力部１１７は、認証結果受付部１１６が受け付けた認証結果「認証許可」を出力する。

【０１０１】

以後、医師Ｘの端末装置１１の操作に応じて、ユーザ１のカルテ情報（図６のレコード「ＩＤ＝１」の情報）が、端末装置１１にダウンロードされ、出力される。

【０１０２】

そして、このかかりつけの医師Ｘは、容易に、ユーザ１のカルテ情報を閲覧しながら、医療行為ができる。

（具体例２）

【０１０３】

次に、ユーザ２は、夜中に急に具合が悪くなり、かかりつけの病院Ａに言った、とする。そして、病院Ａの医師Ｙ（ユーザ２のかかりつけの医者ではない医者）に診察してもらうことになった、とする。

【０１０４】

そして、医師Ｙは、端末装置１１に対して、サーバ装置１３へのアクセスの命令の入力

を行った。

【０１０５】

次に、端末装置１１は、サーバ装置１３へのアクセスの命令の入力を受け付ける。そして、位置情報取得部１１２であるＧＰＳ受信機は、端末装置１１の現在の位置を示す位置情報（x_3，y_3）を取得する。また、図示しない時刻取得部は、現在時刻「２２：１８」を取得する、とする。

【０１０６】

次に、認証方法決定部１１３は、取得された位置情報（x_3，y_3）と現在時刻「２２：１８」を用いて、図５に示す領域認証情報管理表を検索する。そして、認証方法決定部１１３は、位置情報（x_3，y_3）は、領域情報（x_1，y_1）（x_2，y_2）で示される矩形の領域内であることを検知する。そして、認証方法決定部１１３は、現在時刻「２２：１８」が「１８：０１－８：５９」に合致する、と判断する。そして、認証方法識別情報「方法２」を取得する。

【０１０７】

次に、認証画面出力部１１４は、決定された認証方法が認証方法識別情報「方法２」に対応する認証画面を、図７に示すように表示する。

【０１０８】

そして、医師Ｙは、ユーザ２のカルテ情報にアクセスするために、ＩＤ「１２２１」、ＰＷ「ｘｙ３」を入力し、「ログイン」ボタンを押下した、とする。なお、例えば、医師Ｙは、ユーザ２からＩＤ「１２２１」、ＰＷ「ｘｙ３」を聞いて、入力する。

【０１０９】

次に、認証情報送信部１１５は、認証情報「方法２、ＩＤ：１２２１、ＰＷ：ｘｙ３」を構成し、当該認証情報を、サーバ装置１３に送信する。

【０１１０】

次に、サーバ装置１３の認証情報受信部１３２は、認証情報「方法２、ＩＤ：１２２１、ＰＷ：ｘｙ３」を受信する。

【０１１１】

そして、認証部１３３は、認証情報受信部１３２が受信した認証情報に含まれる「方法２」から、第二認証手段１３３２を呼び出し、第二認証手段１３３２に「ＩＤ：１２２１、ＰＷ：ｘｙ３」を渡す。

【０１１２】

次に、第二認証手段１３３２は、「ＩＤ：１２２１、ＰＷ：ｘｙ３」に合致する第一認証情報が、図６のカルテ情報管理表に、存在するか否かを判断する。そして、第二認証手段１３３２は、図６のカルテ情報管理表の「ＩＤ＝２」のレコードが、「ＩＤ：１２２１、ＰＷ：ｘｙ３」に合致する、と判断する。

【０１１３】

そして、第二認証手段１３３２は、第二認証情報（一時的な認証情報）を、自動的に構成する。なお、第二認証手段１３３２は、例えば、「ＩＤ：１２２１、ＰＷ：ｘｙ３」を用いて、ｆ（１２２１，ｘｙ３）を実行し、第二認証情報（ａ８５ｂｑ９）を構成した、とする。そして、第二認証手段１３３２は、図示しない記憶手段に、第二認証情報（ａ８５ｂｑ９）を一時蓄積する。

【０１１４】

次に、第二認証手段１３３２は、「ＩＤ＝２」のレコードが有する端末識別情報「０８０－７７８８－１２３４」を、図６の表から読み出す。

【０１１５】

そして認証結果送信部１３４は、端末識別情報「０８０－７７８８－１２３４」で識別される第二端末１２に、第二認証情報（ａ８５ｂｑ９）を送信する。

【０１１６】

また、認証結果送信部１３４は、第一の認証処理の処理結果「認証許可」を、端末装置１１に送信する。

【０１１７】
次に、第二端末１２の第二送受信部１２２は、サーバ装置１３から第二認証情報（ａ８５ｂｑ９）を受信する。そして、第二出力部１２３は、サーバ装置１３から受信した第二認証情報（ａ８５ｂｑ９）を出力する。図８は、第二端末１２に出力された第二認証情報の例である。
【０１１８】
次に、端末装置１１の認証結果受付部１１６は、第一の認証処理の処理結果「認証許可」を受信する。
【０１１９】
そして、認証画面出力部１１４は、第二の認証を行うための第二の認証画面を出力する。かかる第二の認証画面は、図９である。
【０１２０】
そして、医師Ｙは、第二認証情報（ａ８５ｂｑ９）を図９の第二の認証画面の入力フィールドに入力し、「送信」ボタンを押下する。
【０１２１】
すると、受付部１１１は、第二認証情報（ａ８５ｂｑ９）を受け付け、認証情報送信部１１５は、受付部１１１が受け付けた第二認証情報（ａ８５ｂｑ９）を、サーバ装置１３に送信する。
【０１２２】
次に、サーバ装置１３の認証情報受信部１３２は、端末装置１１から第二認証情報（ａ８５ｂｑ９）を受信する。
【０１２３】
次に、第二認証手段１３３２は、第二認証情報（ａ８５ｂｑ９）が一時格納されている第二認証情報に合致するか否かを判断する。ここで、両データは合致するので、第二認証手段１３３２は、最終的な認証結果を「認証許可」と決定する。
【０１２４】
次に、認証結果送信部１３４は、最終的な認証結果「認証許可」を、端末装置１１に送信する。
【０１２５】
次に、認証結果受付部１１６は、最終的な認証結果「認証許可」を、サーバ装置１３から受信する。そして、認証結果出力部１１７は、認証結果受付部１１６が受け付けた認証結果「認証許可」を出力する。
【０１２６】
以後、医師Ｙの端末装置１１の操作に応じて、ユーザ２のカルテ情報（図６のレコード「ＩＤ＝２」の情報）が、端末装置１１にダウンロードされ、出力される。
【０１２７】
そして、医師Ｙは、容易に、ユーザ２のカルテ情報を閲覧しながら、医療行為ができる。
（具体例３）
【０１２８】
次に、ユーザ３は、道を歩いている際に具合が悪くなり、救急車に乗せられた、とする。そして、救急車の救急員Ｚの依頼で、ユーザ３がＩＤやパスワードを伝えて、ユーザ３のカルテ情報を見て、救急措置を行おうとする、とする。
【０１２９】
まず、救急員Ｚは、救急車内に設置されている端末装置１１に対して、サーバ装置１３へのアクセスの命令の入力を行った。
【０１３０】
次に、端末装置１１は、サーバ装置１３へのアクセスの命令の入力を受け付ける。そして、位置情報取得部１１２であるＧＰＳ受信機は、端末装置１１の現在の位置を示す位置情報（x_4，y_4）を取得する。また、図示しない時刻取得部は、現在時刻「１４：３３

」を取得する、とする。

【０１３１】

次に、認証方法決定部１１３は、取得された位置情報（x_4，y_4）と現在時刻「１４：３３」を用いて、図５に示す領域認証情報管理表を検索する。そして、認証方法決定部１１３は、位置情報（x_4，y_4）は、領域情報（x_1，y_1）（x_2，y_2）で示される矩形の領域外であることを検知する。そして、認証方法決定部１１３は、認証方法識別情報「方法３」を取得する。

【０１３２】

次に、認証画面出力部１１４は、決定された認証方法が認証方法識別情報「方法３」に対応する認証画面を、図１０に示すように表示する。

【０１３３】

そして、救急員Ｚは、ユーザ３のカルテ情報にアクセスするために、ＩＤ「７２１５」、ＰＷ「ａ３５」を入力し、「ログイン」ボタンを押下した、とする。なお、救急員Ｚは、ユーザ３から、ＩＤ「７２１５」、ＰＷ「ａ３５」を聞いて、入力した、とする。

【０１３４】

次に、認証情報送信部１１５は、認証情報「方法３、ＩＤ：７２１５、ＰＷ：ａ３５」を構成し、当該認証情報を、サーバ装置１３に送信する。

【０１３５】

次に、サーバ装置１３の認証情報受信部１３２は、認証情報「方法３、ＩＤ：７２１５、ＰＷ：ａ３５」を受信する。

【０１３６】

そして、認証部１３３は、認証情報受信部１３２が受信した認証情報に含まれる「方法３」から、第三認証手段１３３３を呼び出し、第三認証手段１３３３に「ＩＤ：７２１５、ＰＷ：ａ３５」を渡す。

【０１３７】

次に、第三認証手段１３３３は、「ＩＤ：７２１５、ＰＷ：ａ３５」に合致する第一認証情報が、図６のカルテ情報管理表に、存在するか否かを判断する。そして、第三認証手段１３３３は、図６のカルテ情報管理表の「ＩＤ＝３」のレコードが、「ＩＤ：７２１５、ＰＷ：ａ３５」に合致する、と判断する。

【０１３８】

そして、第三認証手段１３３３は、第二認証情報（例えば、「７８ｚｑｙ５」）を、自動的に構成する。そして、第二認証手段１３３２は、図示しない記憶手段に、第二認証情報（７８ｚｑｙ５）を一時蓄積する。

【０１３９】

次に、第三認証手段１３３３は、「ＩＤ＝３」のレコードが有する端末識別情報「０９０－１２２２－７７５３」を、図６の表から読み出す。

【０１４０】

そして認証結果送信部１３４は、端末識別情報「０９０－１２２２－７７５３」で識別される第二端末１２に、第二認証情報（７８ｚｑｙ５）を送信する。

【０１４１】

また、認証結果送信部１３４は、第一の認証処理の処理結果「認証許可」を、端末装置１１に送信する。

【０１４２】

次に、第二端末１２の第二送受信部１２２は、サーバ装置１３から第二認証情報（７８ｚｑｙ５）を受信する。そして、第二出力部１２３は、サーバ装置１３から受信した第二認証情報（７８ｚｑｙ５）を出力する。

【０１４３】

次に、端末装置１１の認証結果受付部１１６は、第一の認証処理の処理結果「認証許可」を受信する。

【０１４４】

そして、認証画面出力部１１４は、第二の認証を行うための第二の認証画面を出力する。かかる第二の認証画面は、図１１である。図１１において、第二のＩＤ，第二のパスワード、および第二認証情報の入力を求められている、とする。

【０１４５】

次に、救急員Ｚは、ユーザ３から第二のＩＤと第二のパスワードを聞いて、かつ、ユーザ３の第二端末１２のディスプレイに表示されている第二認証情報「７８ｚｑｙ５」を得る。

【０１４６】

そして、救急員Ｚは、第二のＩＤ「ｐｐｘｘ」と第二のパスワード「５５５」と第二認証情報「７８ｚｑｙ５」を、図１１の画面に入力し、「送信」ボタンを押下する。

【０１４７】

すると、受付部１１１は、第二のＩＤ「ｐｐｘｘ」と第二のパスワード「５５５」と第二認証情報「７８ｚｑｙ５」を受け付け、認証情報送信部１１５は、受付部１１１が受け付けた認証情報（第二のＩＤ：ｐｐｘｘ、第二のパスワード：５５５、第二認証情報：７８ｚｑｙ５）を、サーバ装置１３に送信する。

【０１４８】

次に、サーバ装置１３の認証情報受信部１３２は、端末装置１１から認証情報（第二のＩＤ：ｐｐｘｘ、第二のパスワード：５５５、第二認証情報：７８ｚｑｙ５）を受信する。

【０１４９】

次に、第三認証手段１３３３は、第二認証情報（７８ｚｑｙ５）が一時格納されている第二認証情報に合致するか否かを判断する。ここで、第三認証手段１３３３は、両データは合致する、と判断する。

【０１５０】

また、第三認証手段１３３３は、第二のＩＤ「ｐｐｘｘ」と第二のパスワード「５５５」が、ユーザ３のＩＤ２、ＰＷ２と合致するか否かを判断する。ここで、合致するので、第三認証手段１３３３は、最終的な認証結果を「認証許可」と決定する。

【０１５１】

次に、認証結果送信部１３４は、最終的な認証結果「認証許可」を、端末装置１１に送信する。

【０１５２】

次に、認証結果受付部１１６は、最終的な認証結果「認証許可」を、サーバ装置１３から受信する。そして、認証結果出力部１１７は、認証結果受付部１１６が受け付けた認証結果「認証許可」を出力する。

【０１５３】

以後、救急員Ｚの端末装置１１の操作に応じて、ユーザ３のカルテ情報（図６のレコード「ＩＤ＝３」の情報）が、端末装置１１にダウンロードされ、出力される。

【０１５４】

そして、救急員Ｚは、容易に、ユーザ２のカルテ情報を閲覧しながら、救急措置を行える。

【０１５５】

以上、本実施の形態によれば、位置の違いにより、認証方法を変更できる。例えば、良く居る場所では、簡易な認証方法で、サーバ装置１３にアクセスでき、普段とは異なる場所に移動した場合は、高いセキュリティー性を担保して、サーバ装置１３にアクセスできる。

【０１５６】

また、本実施の形態によれば、位置および時間帯等の違いにより、認証方法を変更できる。

【０１５７】

なお、本実施の形態において、位置等の違いにより３以上の認証方法を用いた。しかし

、位置の違いにより、２つの認証方法を切り替えるだけでも良い。かかる場合、例えば、領域情報格納手段１１３１は、図１２に示す領域認証情報管理表を保持している。図１２に示す領域認証情報管理表は、簡易な認証方法１を適用する位置情報のみを管理している。図１２の領域認証情報管理表は、「ＩＤ」「領域名」「領域情報」を有するレコードを１以上、格納している。「領域情報」は、「領域名」で示される地方公共団体の境界線上の（経度，緯度）である。図１２において、旭川市、札幌市などの一部の市の中で、サーバ装置１３にアクセスする場合、簡易な認証方法（例えば、上記の認証方法１）により、サーバ装置１３にアクセスできる。また、図１２の領域認証情報管理表に管理されていない領域では、厳しい認証方法（例えば、上記の認証方法２）により、サーバ装置１３にアクセスできる。なお、領域認証情報管理表の各レコードは、ユーザごとに設定されていることは好適である。

【０１５８】

また、本実施の形態において、認証方法の決定は、端末装置１１が行ったが、サーバ装置で行っても良い。また、本実施の形態において、認証方法に対応した認証画面の出力は、端末装置１１が行ったが、サーバ装置で行っても良い。かかる場合、情報システム２のブロック図は、図１３のようになる。つまり、サーバ装置２３は、端末装置１１の位置情報を受信する位置情報受信部２３１と、認証方法決定部１１３と、認証画面送信部２３２と、認証情報受信部１３２と、認証部１３３と、認証結果送信部１３４等を具備する。また、端末装置２１は、受付部１１１、位置情報取得部１１２、サーバ装置２３に位置情報を送信する位置情報送信部２１１、サーバ装置２３から認証画面を受信する認証画面受信部２１２、認証画面を出力する認証画面出力部２１３、認証情報送信部１１５、認証結果受付部１１６、認証結果出力部１１７、処理部１１８を具備する。

【０１５９】

さらに、本実施の形態における処理は、ソフトウェアで実現しても良い。そして、このソフトウェアをソフトウェアダウンロード等により配布しても良い。また、このソフトウェアをＣＤ－ＲＯＭなどの記録媒体に記録して流布しても良い。また、このソフトウェアまたは、このソフトウェアを記録した記録媒体は、コンピュータプログラム製品として流通しても良いことは言うまでもない。なお、このことは、本明細書における他の実施の形態においても該当する。なお、本実施の形態における端末装置を実現するソフトウェアは、以下のようなプログラムである。つまり、このプログラムは、コンピュータを、端末装置の現在の位置を示す位置情報を取得する位置情報取得部と、前記位置情報取得部が取得した位置情報に応じて、二以上ある認証方法のうちの一の認証方法を決定する認証方法決定部と、前記認証方法決定部が決定した一の認証方法に対応する画面を出力する認証画面出力部と、前記認証画面出力部が出力した画面に対する、ユーザからの情報である認証情報を受け付ける受付部と、前記認証情報を用いて行われた認証処理の結果である認証結果を受け付ける認証結果受付部と、前記認証結果を出力する認証結果出力部として機能させるためのプログラム、である。

【０１６０】

また、上記プログラムにおいて、前記認証方法決定部は、領域を示す情報である領域情報を、１以上記憶媒体に格納しており、前記位置情報取得部が取得した位置情報の示す位置が、前記記憶媒体に格納されている１以上の領域情報が示す１以上の領域のいずれかに含まれるか否かを判断する判断手段と、前記判断手段が、前記位置情報の示す位置が前記１以上の領域のいずれかに含まれると判断した場合に、前記二以上の認証方法のうちの一の認証方法を決定する認証方法決定手段とを具備するものとして、コンピュータを機能させるプログラムであることは好適である。

【０１６１】

また、上記プログラムにおいて、前記二以上の認証方法は、第一の認証方法、および当該第一の認証方法よりセキュリティーレベルの高い第二の認証方法を含み、前記認証方法決定手段は、前記判断手段が、前記位置情報の示す位置が前記１以上の領域のいずれかに含まれると判断した場合に、前記二以上の認証方法のうちの第一の認証方法に決定し、前

記判断手段が、前記位置情報の示す位置が前記１以上の領域のいずれかに含まれないと判断した場合に、前記二以上の認証方法のうちの第二の認証方法に決定するプログラムであることは好適である。

【０１６２】

また、上記プログラムにおいて、前記記憶媒体は、領域情報と、当該領域情報に対応する認証方法を識別する認証方法識別情報とを対応付ける情報である領域認証情報を、２以上格納しており、前記判断手段は、前記位置情報取得部が取得した位置情報の示す位置が含まれる領域を、前記記憶媒体に格納されている１以上の領域情報を用いて判断し、前記認証方法決定手段は、前記判断手段が判断した領域に対応する領域情報と対応付けられた認証方法識別情報を、前記記憶媒体から取得するプログラムであることは好適である。

【０１６３】

（実施の形態２）

本実施の形態において、２つの端末装置の位置が一定の条件を満たす場合のみ、認証許可となる情報システム３について説明する。一定の条件とは、例えば、２つの端末装置の位置が一定の距離以内であることや、同一の領域内に存在することである。

【０１６４】

本実施の形態における情報システム３の概念図は、図１と同様である。また、図１４は、本実施の形態における情報システム３のブロック図である。

【０１６５】

情報システム３は、第一端末装置３１、第二端末装置３２、サーバ装置３３を具備する。

【０１６６】

第一端末装置３１は、受付部１１１、第一位置情報格納部３１１、第一送信部３１２、第一受信部３１３、第一出力部３１４、処理部１１８を具備する。

【０１６７】

第二端末装置３２は、第二端末識別子格納部１２０、第二位置情報取得部３２１、第二送信部３２２を具備する。

【０１６８】

サーバ装置３３は、第一位置情報受信部３３１、第二位置情報受信部３３２、認証部３３３、認証結果送信部３３４、データ格納部１３１、データ送受信部１３５を具備する。

【０１６９】

第一端末装置３１は、例えば、ある場所に固定されている端末である。第一端末装置３１は、例えば、病院内で医師が患者の病歴などのカルテ情報を閲覧するための端末である。なお、第一端末装置３１は、携帯端末でも良い。

【０１７０】

また、第二端末装置３２は、例えば、患者が保持している携帯端末である。なお、第二端末装置３２は、ノートパソコンなどの他の形態の端末でも良い。

【０１７１】

さらに、サーバ装置３３は、認証処理を行う装置である。サーバ装置３３は、例えば、認証処理の結果、認証許可であった場合、第一端末装置３１に種々の情報をダウンロードするためのサーバ装置であっても良い。その他、サーバ装置３３が行う処理は問わない。

【０１７２】

第一位置情報格納部３１１は、第一端末装置３１の位置を示す情報である第一位置情報を格納し得る。第一端末装置３１は、第一位置情報を取得する手段を具備しており、かかる手段により取得された第一位置情報を、第一位置情報格納部３１１に格納していても良い。第一位置情報は、（緯度，経度）など、第一端末装置３１の位置を特定する情報であれば何でも良い。第一位置情報格納部３１１は、不揮発性の記録媒体が好適であるが、揮発性の記録媒体でも実現可能である。第一位置情報格納部３１１に第一位置情報が記憶される過程は問わない。例えば、記録媒体を介して第一位置情報が第一位置情報格納部３１１で記憶されるようになってもよく、通信回線等を介して送信された第一位置情報が第一

位置情報格納部３１１で記憶されるようになってもよく、あるいは、入力デバイスを介して入力された第一位置情報が第一位置情報格納部３１１で記憶されるようになってもよい。

【０１７３】

第一送信部３１２は、第一位置情報をサーバ装置３３に送信する。第一送信部３１２は、ユーザの指示により第一位置情報を送信しても良いし、定期的に第一位置情報を送信しても良い。また、第一送信部３１２は、第二端末装置３２を識別する第二端末装置識別子（例えば、第二端末装置３２の電話番号、ＩＰアドレスなど）と第一位置情報とを対にして送信することは好適である。第一送信部３１２は、通常、無線または有線の通信手段で実現されるが、放送手段で実現されても良い。

【０１７４】

第一受信部３１３は、サーバ装置３３から認証結果を受信する。認証結果は、例えば、認証許可（例えば「１」）または認証不許可（例えば「０」）である。第一受信部３１３は、通常、無線または有線の通信手段で実現されるが、放送を受信する手段で実現されても良い。

【０１７５】

第一出力部３１４は、認証結果を出力する。ここでの出力とは、ディスプレイへの表示、プロジェクターを用いた投影、プリンタへの印字、音出力、外部の装置への送信、記録媒体への蓄積、他の処理装置や他のプログラムなどへの処理結果の引渡しなどを含む概念である。第一出力部３１４は、ディスプレイやスピーカー等の出力デバイスを含むと考えても含まないと考えても良い。第一出力部３１４は、出力デバイスのドライバーソフトまたは、出力デバイスのドライバーソフトと出力デバイス等で実現され得る。

【０１７６】

第二位置情報取得部３２１は、第二端末装置３２の位置を示す情報である第二位置情報を取得する。第二位置情報は、例えば、（緯度，経度）である。また、第二位置情報取得部３２１は、例えば、ＧＰＳ受信機により実現され得る。

【０１７７】

第二送信部３２２は、第二位置情報をサーバ装置３３に送信する。第一送信部３１２は、通常、ユーザの指示により第二位置情報を送信する。また、第二送信部３２２は、第二端末装置３２を識別する第二端末装置識別子と第二位置情報とを対にして送信することは好適である。第二送信部３２２は、通常、無線または有線の通信手段で実現されるが、放送手段で実現されても良い。

【０１７８】

第一位置情報受信部３３１は、第一端末装置３１から第一位置情報を受信する。第一位置情報受信部３３１は、通常、無線または有線の通信手段で実現されるが、放送を受信する手段で実現されても良い。

【０１７９】

第二位置情報受信部３３２は、第二端末装置３２から第二位置情報を受信する。第二位置情報受信部３３２は、通常、無線または有線の通信手段で実現されるが、放送を受信する手段で実現されても良い。

【０１８０】

認証部３３３は、第一位置情報と第二位置情報とが、予め決められた関係を有するか否かを判断し、予め決められた関係を有する場合には認証許可を示す認証結果を取得し、予め決められた関係を有しない場合には認証不許可を示す認証結果を取得する。ここで、予め決められた関係とは、例えば、第一位置情報が示す地点と第二位置情報が示す地点との距離が、予め決められた距離より小さいこと、または予め決められた距離以内であることである。認証部３３３は、通常、ＭＰＵやメモリ等から実現され得る。認証部３３３の処理手順は、通常、ソフトウェアで実現され、当該ソフトウェアはＲＯＭ等の記録媒体に記録されている。但し、ハードウェア（専用回路）で実現しても良い。

【０１８１】

認証結果送信部３３４は、認証部３３３が取得した認証結果を、第一端末装置３１に送信する。認証結果送信部３３４は、通常、無線または有線の通信手段で実現されるが、放送手段で実現されても良い。

【０１８２】

次に、情報システム３の動作について説明する。まず、第一端末装置３１の動作について説明する。第一端末装置３１の受付部１１１は、第二端末識別子を受け付け、かつ、認証処理を開始する指示を受け付ける。すると、第一送信部３１２は、第一位置情報格納部３１１から第一位置情報を読み出す。そして、第一送信部３１２は、第一位置情報と、受け付けられた第二端末識別子とを対にして、サーバ装置３３に送信する。そして、かかる送信に対応して、第一受信部３１３は認証結果（認証許可または認証不許可）を受信する。次に、第一出力部３１４は認証結果を出力する。認証結果が認証許可である場合、以後、第一端末装置３１の第一受信部３１３は、ユーザ（例えば、医師）からの指示に従い、サーバ装置３３にアクセスし、情報（例えば、患者のカルテ情報）を受信する。そして、第一出力部３１４は、情報（例えば、患者のカルテ情報）を出力する。なお、処理部１１８が、受信した情報に対して、種々の処理を行ったりしても良い。

【０１８３】

次に、第二端末装置３２の動作について説明する。第二端末装置３２の図示しない手段（受付手段）がユーザ指示を受け付けると、第二位置情報取得部３２１は、第二位置情報を取得する。そして、第二送信部３２２は、第二位置情報と第二端末識別子格納部１２０の第二端末識別子とを対にして、サーバ装置３３に送信する。

【０１８４】

次に、サーバ装置３３の動作について、図１５のフローチャートを用いて説明する。

【０１８５】

（ステップＳ１５０１）第一位置情報受信部３３１は、第一位置情報を受信したか否かを判断する。第一位置情報を受信すればステップＳ１５０２に行き、第一位置情報を受信しなければステップＳ１５０９に行く。なお、ここで、第一位置情報受信部３３１は、第一位置情報と第二端末識別子とを受信しても良い。

【０１８６】

（ステップＳ１５０２）認証部３３３は、ステップＳ１５０１で受信された第一位置情報または、第一位置情報と第二端末識別子とを、図示しない記録媒体に少なくとも一時格納する。

【０１８７】

（ステップＳ１５０３）第二位置情報受信部３３２は、第二位置情報を受信したか否かを判断する。第二位置情報を受信すればステップＳ１５０４に行き、第二位置情報を受信しなければステップＳ１５０３に戻る。なお、ここで、第二位置情報受信部３３２は、第二位置情報と第二端末識別子とを受信しても良い。

【０１８８】

（ステップＳ１５０４）認証部３３３は、ステップＳ１５０３で受信された第二位置情報または、第二位置情報と第二端末識別子とを、図示しない記録媒体に少なくとも一時格納する。

【０１８９】

（ステップＳ１５０５）認証部３３３は、ステップＳ１５０１で受信された第一位置情報およびステップＳ１５０３で受信された第二位置情報が、予め決められた条件を満たすか否かを判断する。なお、ここで、認証部３３３は、第一位置情報と第二位置情報とを取得する場合、同一の第二端末識別子と対になる第一位置情報と第二位置情報とを取得しても良いし、他の情報でひも付けされた第一位置情報と第二位置情報とを取得しても良いし、時間的に最も近接した時間に受信された第一位置情報と第二位置情報とを取得しても良い。また、認証部３３３は、第一位置情報が示す位置と第二位置情報が示す位置との距離を算出し、当該距離が予め決められた距離（予め記録媒体に格納している）以内、またはより小さいか否かを判断しても良い。また、認証部３３３は、第一位置情報と第二位置情

報との両方が、予め決められた領域（予め記録媒体に格納している）内を示す情報であるか否かを判断しても良い。例えば、予め決められた領域が（ｘ１，ｙ１）を左上の位置、（ｘ２，ｙ２）を右下の位置とする矩形領域である場合を考える。かかる場合、認証部３３３は、第一位置情報（ｘ３，ｙ３）と第二位置情報（ｘ４，ｙ４）が以下の条件を満たすか否かを判断する。以下の条件とは、「ｘ１＜＝ｘ３＜＝ｘ２」かつ「ｙ１＜＝ｙ３＜＝ｙ２」かつ「ｘ１＜＝ｘ４＜＝ｘ２」かつ「ｙ１＜＝ｙ４＜＝ｙ２」である（但し、ｘ１＜ｘ２，ｙ１＜ｙ２とする）。認証部３３３は、判断結果が条件を満たすとの判断結果である場合はステップＳ１５０６に行き、条件を満たさないとの判断結果である場合はステップＳ１５０７に行く。

【０１９０】

（ステップＳ１５０６）認証部３３３は、変数「認証結果」に「認証許可」を代入する。ステップＳ１５０８に行く。

【０１９１】

（ステップＳ１５０７）認証部３３３は、変数「認証結果」に「認証不許可」を代入する。

【０１９２】

（ステップＳ１５０８）認証結果送信部３３４は、認証結果を第二端末装置３２に送信する。ステップＳ１５０１に戻る。なお、認証部３３３は、通常、第二端末装置識別子と第一端末識別子と認証結果とを対応付けて、図示しない記憶手段に格納する。

【０１９３】

（ステップＳ１５０９）データ送受信部１３５は、第二端末装置３２からデータ送信の指示を受信したか否かを判断する。データ送信の指示を受信すればステップＳ１５１０に行き、データ送信の指示を受信しなければステップＳ１５０１に戻る。なお、データ送信の指示は、通常、第二端末装置３２と通信するための第二端末装置識別子を含む。

【０１９４】

（ステップＳ１５１０）データ送受信部１３５は、ステップＳ１５０９で受信されたデータ送信の指示を送信してきた第一端末装置３１が認証許可された第二端末装置３２であるか否かを判断する。認証許可された第二端末装置３２であればステップＳ１５１１に行き、認証許可された第二端末装置３２でなければステップＳ１５０１に戻る。なお、データ送受信部１３５は、例えば、ステップＳ１５０９で受信されたデータ送信の指示に含まれる第二端末装置識別子と対になる認証結果を図示しない記憶手段から取得し、認証許可された第二端末装置３２であるか否かを判断する。

【０１９５】

（ステップＳ１５１１）データ送受信部１３５は、ステップＳ１５０９で受信されたデータ送信の指示に対応するデータをデータ格納部１３１から読み出す。

【０１９６】

（ステップＳ１５１２）データ送受信部１３５は、ステップＳ１５１１で取得したデータを第二端末装置３２に送信する。ステップＳ１５０１に戻る。

【０１９７】

なお、図１５のフローチャートにおいて、電源オフや処理終了の割り込みにより処理は終了する。

【０１９８】

また、図１５のフローチャートにおいて、サーバ装置３３は、第一位置情報を受信してから第二位置情報を受信した。しかし、第一位置情報と第二位置情報を受信する順序は問わない。

【０１９９】

以下、本実施の形態における情報システム３の具体的な動作について説明する。情報システム３の概念図は図１である。

【０２００】

今、第一端末装置３１は、病院に設置されている端末であり、医師が患者のカルテ情報

を閲覧するために利用する端末である、とする。また、第二端末装置３２は、患者が所有する携帯端末である。さらに、サーバ装置３３は、患者のカルテ情報を格納しており、認証許可された場合、許可された第二端末装置３２の所有者である患者のカルテ情報を、第一端末装置３１からの指示に応じて、許可された第一端末装置３１に送信する。

【０２０１】

そして、第一端末装置３１の第一位置情報格納部３１１は、病院（または病院の医師の診察室）の位置を示す第一位置情報（Ｘａ，Ｙａ）を格納している。

【０２０２】

また、第二端末装置３２の第二端末識別子格納部１２０は、第二端末装置３２の第二端末識別子「０９０１２２２７７５３」（ここでは、第二端末装置３２の電話番号）を格納している。さらに、サーバ装置３３のデータ格納部１３１は、図６に示すカルテ情報管理表を保持している。

【０２０３】

かかる状況において、第二端末装置３２の所有者（山本広子さん）は、本病院の医師（Ｙ）に診察してもらうために、本病院の医師（Ｙ）の診察室を訪れた、とする。

【０２０４】

そして、医師（Ｙ）は、第一端末装置３１の画面（図１６）に示すように、認証を行うため、患者（山本広子さん）から携帯電話の番号を聞き、当該携帯電話の番号を入力し、送信ボタンを押下した、とする。

なお、入力する情報は、携帯電話の番号に限られないことは言うまでもない。入力する情報は、患者または第二端末装置３２を識別する情報であれば良い。かかる情報として、例えば、患者の氏名および患者の生年月日でも良いことは言うまでもない。

【０２０５】

すると、第一端末装置３１の受付部１１１は、認証のための情報送信の指示を受け付ける。

【０２０６】

次に、第一送信部３１２は、第一位置情報格納部３１１から第一位置情報（Ｘａ，Ｙａ）を読み出す。そして、第一送信部３１２は、第一位置情報（Ｘａ，Ｙａ）と、受け付けられた第二端末識別子「０９０１２２２７７５３」とを対にして、サーバ装置３３に送信する。なお、ここで、サーバ装置３３が第一端末装置３１に認証結果を返送するために、第一端末装置３１は、第一端末装置３１の識別情報（例えば、ＩＰアドレスなど）も、一緒にサーバ装置３３に送信している。

【０２０７】

次に、患者は、自身の第二端末装置３２に対して、第二位置情報をサーバ装置３３に送信する指示を入力する。

【０２０８】

そして、第二端末装置３２の図示しない手段（受付手段）がユーザ指示（第二位置情報をサーバ装置３３に送信する指示）を受け付ける。次に、第二位置情報取得部３２１は、第二位置情報（Ｘｂ，Ｙｂ）を取得する。そして、第二送信部３２２は、第二位置情報（Ｘｂ，Ｙｂ）と第二端末識別子格納部１２０の第二端末識別子「０９０１２２２７７５３」とを対にして、サーバ装置３３に送信する。

【０２０９】

次に、サーバ装置３３の第一位置情報受信部３３１は、第一位置情報（Ｘａ，Ｙａ）と第二端末識別子「０９０１２２２７７５３」とを受信する。そして、認証部３３３は、受信された第一位置情報（Ｘａ，Ｙａ）と第二端末識別子「０９０１２２２７７５３」とを記録媒体に一時格納する。

【０２１０】

次に、第二位置情報受信部３３２は、第二位置情報（Ｘｂ，Ｙｂ）と第二端末識別子「０９０１２２２７７５３」とを受信する。そして、認証部３３３は、受信された第二位置情報（Ｘｂ，Ｙｂ）と第二端末識別子「０９０１２２２７７５３」とを記録媒体に一時格

納する。
【０２１１】
次に、認証部３３３は、第二端末識別子「０９０１２２２７７５３」と対になる、第一位置情報（Ｘａ，Ｙａ）と第二位置情報（Ｘｂ，Ｙｂ）とを記録媒体から読み出す。
【０２１２】
次に、認証部３３３は、第一位置情報が示す位置と第二位置情報が示す位置との距離（ｄ）を算出し、当該距離が予め決められた距離（ｄａ）以内か否かを判断する。ここで「ｄ＜ｄａ」であるとすると、認証部３３３は、第一位置情報が示す位置と第二位置情報が示す位置との距離（ｄ）を算出する。そして、認証部３３３は、予め格納している条件（当該距離が予め決められた距離（ｄａ）以内である）を構成する距離（ｄａ）を読み出す。そして、認証部３３３は、距離（ｄ）と距離（ｄａ）とを比較し、「ｄ＜ｄａ」から、第一位置情報が示す位置と第二位置情報が示す位置とが予め決められた距離以内であり、認証許可である、と判断する。
【０２１３】
そして、認証部３３３は、変数「認証結果」に「認証許可」を代入する。次に、認証結果送信部３３４は、認証結果「認証許可」を第二端末装置３２に送信する。
【０２１４】
次に、第一端末装置３１の第一受信部３１３は認証結果「認証許可」を受信する。次に、第一出力部３１４は認証結果「認証許可」を出力する。
【０２１５】
以後、医師（Ｙ）は、患者（山本広子さん）のカルテ情報を、サーバ装置３３から取得できる。かかるカルテ情報の取得処理は、公知技術であるので、説明を省略する。
【０２１６】
以上、本実施の形態によれば、２つの端末装置の位置関係が所定の位置関係である場合に、認証許可とできる。このことにより、情報提供側（例えば、患者）が確実に存在する状況のもと、情報閲覧側（例えば、医師）が情報を閲覧できる。したがって、情報提供側のプライバシーを担保できたり、機密情報の漏洩を防いだりできる。
【０２１７】
なお、本実施の形態によれば、第一位置情報と第二位置情報が予め決められた距離以内である（距離より小さい）場合に、認証許可とした。ただし、第一位置情報と第二位置情報が予め決められた距離以上である（距離より大きい）場合に、認証許可としても良い。かかる場合、情報を見せたくない人が、確実に近くに居ない状況で、情報を閲覧できたりする。また、上述したように、第一位置情報と第二位置情報との両方が、予め決められた領域内の地点である場合に、認証許可としても良い。かかる場合、第一位置情報に適用する領域と第二位置情報に適用する領域とが、異なる領域でも良い。さらに、第一位置情報と第二位置情報との両方が、予め決められた領域外の地点である場合に、認証許可としても良い。かかる場合も、第一位置情報に適用する領域と第二位置情報に適用する領域とが、異なる領域でも良い。
【０２１８】
また、図１７は、本明細書で述べたプログラムを実行して、上述した実施の形態の情報システム等を実現するコンピュータの外観を示す。上述の実施の形態は、コンピュータハードウェア及びその上で実行されるコンピュータプログラムで実現され得る。図１７は、このコンピュータシステム３４０の概観図であり、図１８は、コンピュータシステム３４０の内部構成を示す図である。
【０２１９】
図１７において、コンピュータシステム３４０は、ＦＤドライブ３４１１、ＣＤ－ＲＯＭドライブ３４１２を含むコンピュータ３４１と、キーボード３４２と、マウス３４３と、モニタ３４４とを含む。
【０２２０】
図１８において、コンピュータ３４１は、ＦＤドライブ３４１１、ＣＤ－ＲＯＭドライ

ブ３４１２に加えて、ＭＰＵ３４１３と、ＣＤ－ＲＯＭドライブ３４１２及びＦＤドライブ３４１１に接続されたバス３４１４と、ブートアッププログラム等のプログラムを記憶するためのＲＯＭ３４１５と、ＣＰＵ３４１３に接続され、アプリケーションプログラムの命令を一時的に記憶するとともに一時記憶空間を提供するためのＲＡＭ３４１６と、アプリケーションプログラム、システムプログラム、及びデータを記憶するためのハードディスク３４１７とを含む。ここでは、図示しないが、コンピュータ３４１は、さらに、ＬＡＮへの接続を提供するネットワークカードを含んでも良い。

【０２２１】

コンピュータシステム３４０に、上述した実施の形態の情報システム等の機能を実行させるプログラムは、ＣＤ－ＲＯＭ３５０１、またはＦＤ３５０２に記憶されて、ＣＤ－ＲＯＭドライブ３４１２またはＦＤドライブ３４１１に挿入され、さらにハードディスク３４１７に転送されても良い。これに代えて、プログラムは、図示しないネットワークを介してコンピュータ３４１に送信され、ハードディスク３４１７に記憶されても良い。プログラムは実行の際にＲＡＭ３４１６にロードされる。プログラムは、ＣＤ－ＲＯＭ３５０１、ＦＤ３５０２またはネットワークから直接、ロードされても良い。

【０２２２】

プログラムは、コンピュータ３４１に、上述した実施の形態の情報システム等の機能を実行させるオペレーティングシステム（ＯＳ）、またはサードパーティープログラム等は、必ずしも含まなくても良い。プログラムは、制御された態様で適切な機能（モジュール）を呼び出し、所望の結果が得られるようにする命令の部分のみを含んでいれば良い。コンピュータシステム３４０がどのように動作するかは周知であり、詳細な説明は省略する。

【０２２３】

なお、上記プログラムにおいて、情報を送信する送信ステップや、情報を受信する受信ステップなどでは、ハードウェアによって行われる処理、例えば、送信ステップにおけるモデムやインターフェースカードなどで行われる処理（ハードウェアでしか行われない処理）は含まれない。

【０２２４】

また、上記プログラムを実行するコンピュータは、単数であってもよく、複数であってもよい。すなわち、集中処理を行ってもよく、あるいは分散処理を行ってもよい。

【０２２５】

また、上記各実施の形態において、一の装置に存在する２以上の通信手段（端末情報送信部、端末情報受信部など）は、物理的に一の媒体で実現されても良いことは言うまでもない。

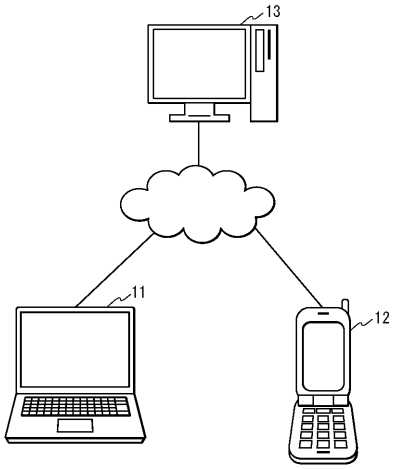
【０２２６】

また、上記各実施の形態において、各処理（各機能）は、単一の装置（システム）によって集中処理されることによって実現されてもよく、あるいは、複数の装置によって分散処理されることによって実現されてもよい。つまり、上記において、以下の情報処理方法を実現すれば良い。つまり、その情報処理方法は、位置情報取得部、認証方法決定部、認証画面出力部、受付部、認証結果受付部、および認証結果出力部により実現される情報処理方法であって、前記位置情報取得部により、端末装置の現在の位置を示す位置情報を取得する位置情報取得ステップと、前記認証方法決定部により、前記位置情報取得ステップで取得された位置情報に応じて、二以上ある認証方法のうちの一の認証方法を決定する認証方法決定ステップと、前記認証画面出力部により、前記認証方法決定ステップで決定された一の認証方法に対応する画面を出力する認証画面出力ステップと、前記受付部により、前記認証画面出力ステップで出力された画面に対する、ユーザからの情報である認証情報を受け付ける受付ステップと、前記認証結果受付部により、前記認証情報を用いて行われた認証処理の結果である認証結果を受け付ける認証結果受付ステップと、前記認証結果出力部により、前記認証結果を出力する認証結果出力ステップを具備する情報処理方法である。

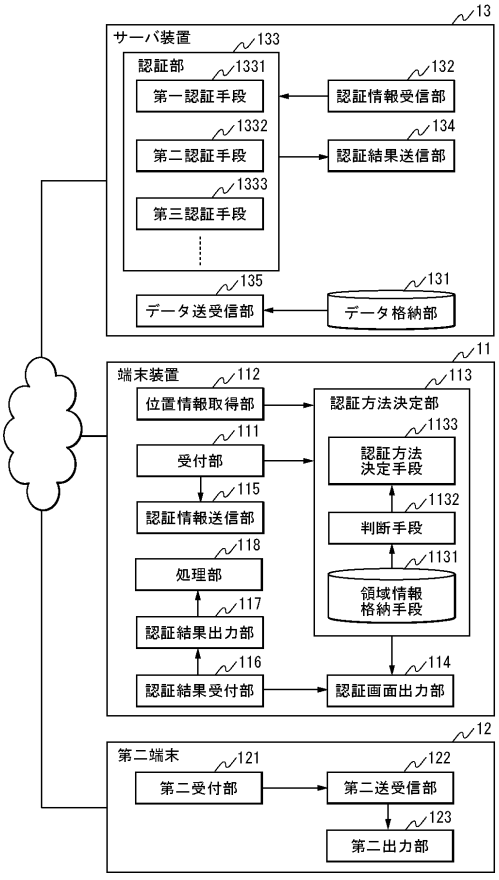
【０２２７】
本発明は、以上の実施の形態に限定されることなく、種々の変更が可能であり、それらも本発明の範囲内に包含されるものであることは言うまでもない。
【産業上の利用可能性】
【０２２８】
以上のように、本発明にかかる情報システムは、ユーザが居る位置に応じて、認証方法を変えることができる。そのため、例えば、普段、ユーザが存在する場所や、居ることが予想される場所では、簡易な認証方法を採用し、簡単、迅速な認証が可能となり、ユーザが行き慣れていない場所では、厳重な認証方法を採用することにより、高度なセキュリティーを担保できる、という効果を有し、電子カルテシステム等として有用である。
【符号の説明】
【０２２９】
１、２、３　情報システム
１１、２１　端末装置
１２　第二端末
１３、２３、３３　サーバ装置
３１　第一端末装置
３２　第二端末装置
１１１　受付部
１１２　位置情報取得部
１１３　認証方法決定部
１１４、２１３　認証画面出力部
１１５　認証情報送信部
１１６　認証結果受付部
１１７　認証結果出力部
１１８　処理部
１２１　第二受付部
１２２、３２２　第二送信部
１２２　第二送受信部
１２３　第二出力部
１３１　データ格納部
１３２　認証情報受信部
１３３、３３３　認証部
１３４、３３４　認証結果送信部
１３５　データ送受信部
２１１　位置情報送信部
２１２　認証画面受信部
２３１　位置情報受信部
２３２　認証画面送信部
３１１　第一位置情報格納部
３１２　第一送信部
３１３　第一受信部
３１４　第一出力部
３２１　第二位置情報取得部
３３１　第一位置情報受信部
３３２　第二位置情報受信部
１１３１　領域情報格納手段
１１３２　判断手段
１１３３　認証方法決定手段
１３３１　第一認証手段

１３３２　第二認証手段
１３３３　第三認証手段

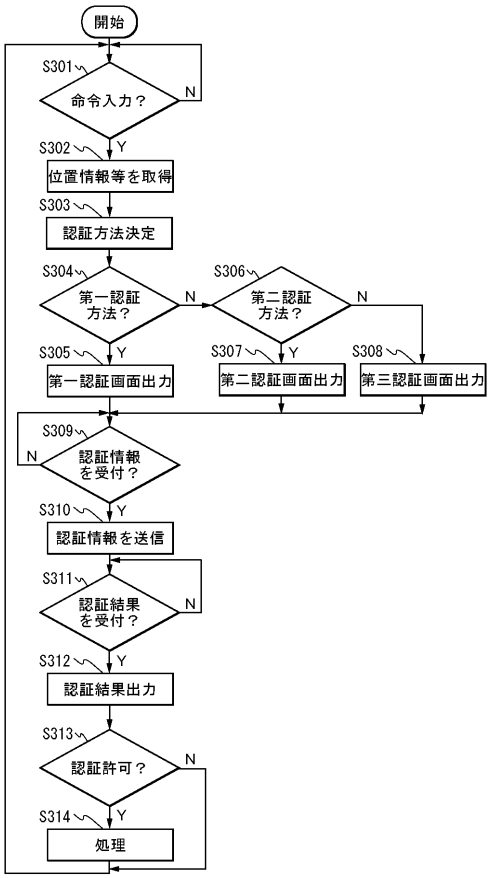
【図１】



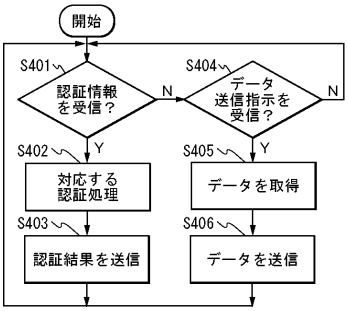
【図２】



【図３】



【図４】



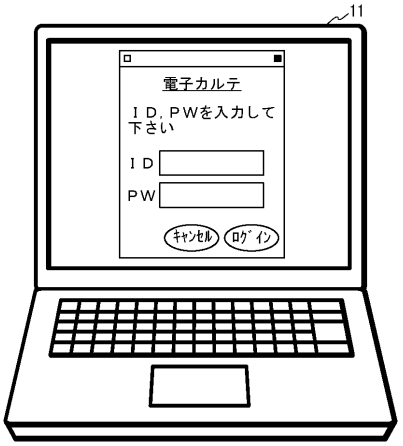
【図５】

ＩＤ	領域情報	時間情報	認証方法識別情報
1	（x_1，y_1）（x_2，y_2）	９：００－１８：００	方法１
2		１８：０１－８：５９	方法２
3	その他	——	方法３

【図６】

No	第一認証情報		第二認証情報		端末識別情報	出力情報					
	ＩＤ１	ＰＷ１	ＩＤ２	ＰＷ２		氏名	年齢	性別	病歴	通院中の病気	がん治療歴の有無
1	5631	abc	abcd	371	090-1234-5678	田中明子	48	女	20才 盲腸 28才 胃潰瘍 30才～糖尿病	糖尿病	無
2	1221	xy3	xyzw	172	080-7788-1234	山田和夫	34	男	15才 貧血 30才 高血圧	無	——
3	7215	a35	ppxx	555	090-1222-7753	山本広子	28	女	25才 盲腸	胃がん 胃潰瘍	有

【図７】

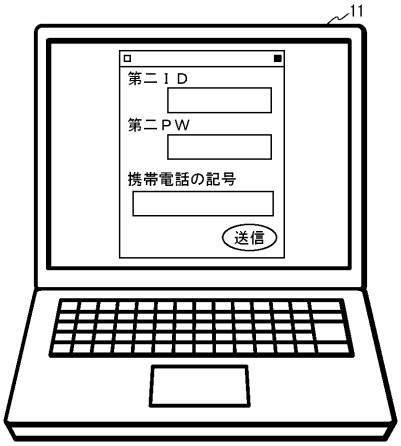


【図８】

【図９】

【図１０】

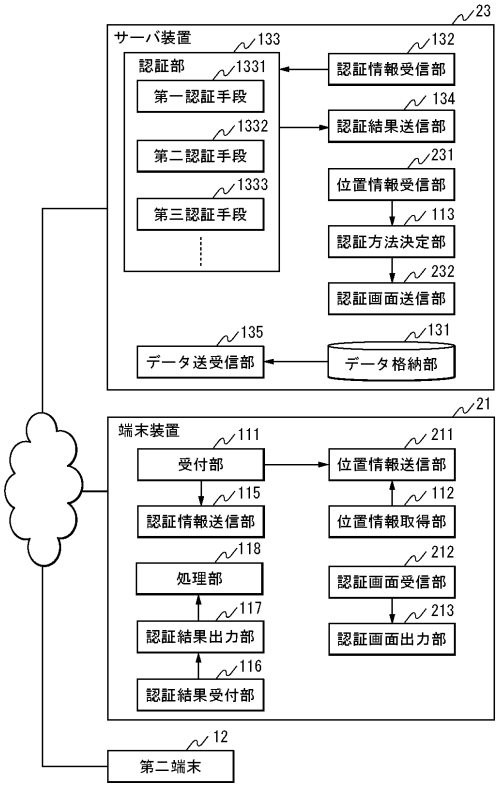
【図１１】



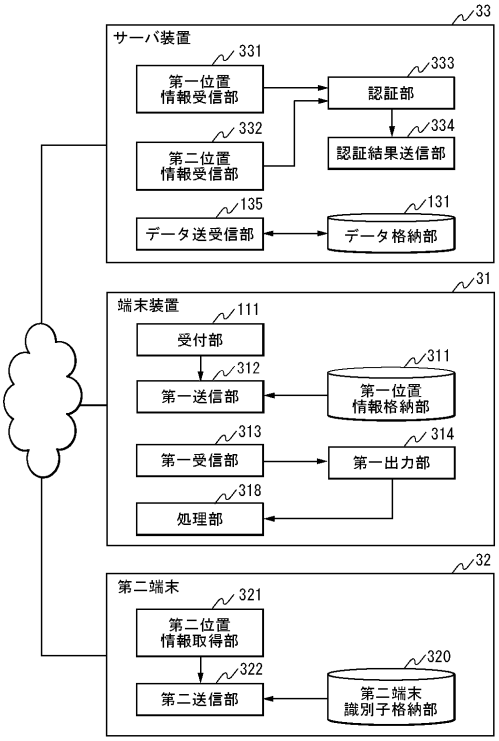
【図１２】

ＩＤ	領域名	領域情報
1	旭川市	(x_1, y_1) (x_2, y_2) (x_3, y_3) ・・・・・・
2	札幌市	(x_n, y_n) (x_{n+1}, y_{n+1}) ・・・・・・
⋮	⋮	⋮

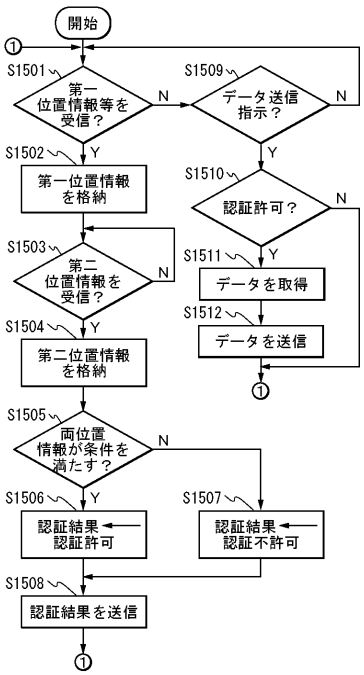
【図１３】



【図１４】

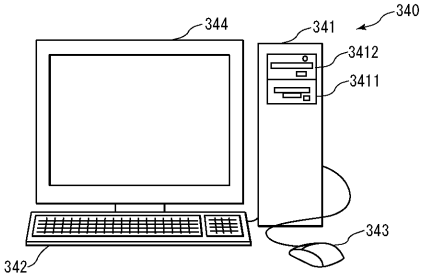


【図１５】

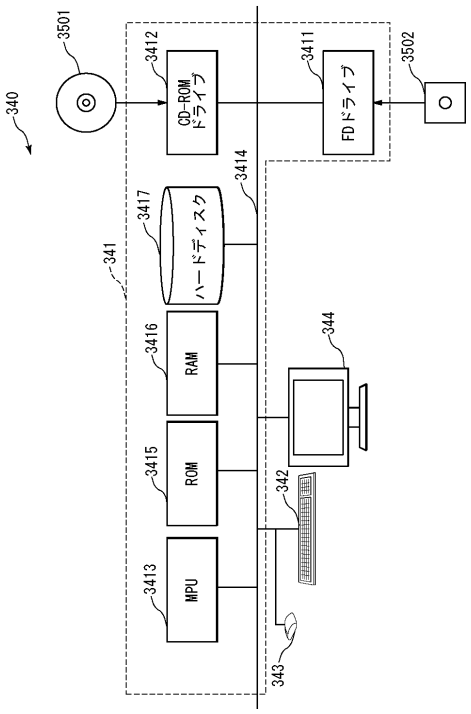


【図１６】

【図１７】



【図１８】


340
3501
3412
CD-ROM ドライブ
3411
FDドライブ
3502
3414
3417
ハードディスク
341
3416
RAM
344
3415
ROM
342
3413
MPU
343

フロントページの続き

(58)調査した分野(Int.Cl., ＤＢ名)
Ｇ０６Ｆ　２１／３１
Ｈ０４Ｌ　９／３２