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

特許第4571426号
(P4571426)

(45)発行日　平成22年10月27日(2010.10.27)　(24)登録日　平成22年8月20日(2010.8.20)

(51)Int.Cl.		F I		
G06F 21/20	(2006.01)	G06F	15/00	330F
G06K 17/00	(2006.01)	G06K	17/00	V
G06T 7/00	(2006.01)	G06T	7/00	510B
		G06T	7/00	530

請求項の数 4　(全 9 頁)

(21)出願番号　特願2004-106541 (P2004-106541)
(22)出願日　平成16年3月31日 (2004.3.31)
(65)公開番号　特開2005-293172 (P2005-293172A)
(43)公開日　平成17年10月20日 (2005.10.20)
審査請求日　平成19年1月31日 (2007.1.31)

(73)特許権者　000003562
東芝テック株式会社
東京都品川区東五反田二丁目１７番２号
(74)代理人　100091351
弁理士　河野　哲
(74)代理人　100088683
弁理士　中村　誠
(74)代理人　100108855
弁理士　蔵田　昌俊
(74)代理人　100084618
弁理士　村松　貞男
(74)代理人　100092196
弁理士　橋本　良郎

最終頁に続く

(54)【発明の名称】認証システム

(57)【特許請求の範囲】

【請求項１】

予め登録されている所定の認証精度を有する第１の生体認証情報を使用して部屋の入り口において該当する個人か否かの認証を行う第１の認証手段と、

部屋の入り口において該当する個人から生体情報を取得し、第１の生体認証情報よりも認証精度が低い第２の生体認証情報を作成する第１の認証情報作成手段と、

個人識別情報を発行する個人識別情報発行手段と、

前記第１の認証手段が該当する個人の認証を行うと、第２の生体認証情報を前記個人識別情報発行手段が発行した個人識別情報と関連付けて登録する個人情報登録部と、

室内において該当する個人から再び生体情報を取得して第２の生体認証情報と同じ種類の第３の生体認証情報を作成する第２の認証情報作成手段と、

室内において該当する個人の個人識別情報の入力によって前記個人情報登録部から読み出された第２の生体認証情報と第３の生体認証情報とを比較して該当する個人か否かの認証を行う第２の認証手段と

を備えたことを特徴とする認証システム。

【請求項２】

予め所定の認証精度を有する第１の生体情報が登録されるとともに、他の情報を書き込み可能なメモリカードと、

前記第１の生体認証情報を使用して部屋の入り口において該当する個人か否かの認証を行う第１の認証手段と、

部屋の入り口において該当する個人から生体情報を取得し、第１の生体認証情報よりも認証精度が低い第２の生体認証情報を作成する第１の認証情報作成手段と、
個人識別情報を発行する個人識別情報発行手段と、
前記第１の認証手段が該当する個人の認証を行うと、第２の生体認証情報を前記個人識別情報発行手段が発行した個人識別情報と関連付けて登録する個人情報登録部と、
前記第１の認証手段が該当する個人の認証を行うと、前記個人識別情報を前記メモリカードに書き込む書き込み手段と、
室内において該当する個人から再び生体情報を取得して第２の生体認証情報と同じ種類の第３の生体認証情報を作成する第２の認証情報作成手段と、
室内において前記メモリカードに記憶された該当する個人の個人識別情報が入力されることによって前記個人情報登録部から読み出し、この読み出した第２の生体認証情報と第３の生体認証情報とを比較して該当する個人か否かの認証を行う第２の認証手段と
を備えたことを特徴とする認証システム。

【請求項３】
前記第２の生体認証情報および前記第３の生体認証情報は、音声である
ことを特徴とする請求項１または請求項２に記載の認証システム。

【請求項４】
予め登録されている所定の認証精度を有する第１の生体認証情報を使用して部屋の入り口において該当する個人か否かを認証するステップと、
部屋の入り口において該当する個人から生体情報を取得し、前記第１の生体認証情報よりも認証精度が低い第２の生体認証情報を作成するステップと、
個人識別情報を発行するステップと、
前記認証の結果が該当する個人である場合に、前記作成した第２の生体認証情報を前記発行した個人識別情報と関連付けて登録するステップと、
室内において該当する個人から再び生体情報を取得して前記第２の生体認証情報と同じ種類の第３の生体認証情報を作成するステップと、
室内において該当する個人の個人識別情報の入力により前記登録分から読み出される第２の生体認証情報と前記作成された第３の生体認証情報との比較により該当する個人か否かを認証するステップと
を備えることを特徴とする認証方法。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、例えば、店舗等における従業員の入室や業務実行などの管理に適した認証システムに関する。
【背景技術】
【０００２】
従来、個人認証システムとして、生体情報を用いた個人認証システムが知られている。この認証システムは、サーバ端末と複数のクライアント端末を、ネットワークを介して接続し、各クライアント端末にそれぞれ生体認証情報照合装置を接続した構成になっている。サーバ端末は、認証動作を管理する生体認証情報管理サーバと、クライアント端末の端末ＩＤと認証対象者のユーザＩＤを関連付けて保存しておく端末情報ＤＢと、認証のための生体認証テンプレートデータや認証アルゴリズム、さらには端末ごとの照合精度などを保存しておく生体認証情報ＤＢとを備えている。また、各クライアント端末は、何らかの業務を行うアプリケーション及びアプリケーションから端末操作者の認証依頼を受け、サーバ端末に保存されている情報と生体認証情報照合装置を使用して端末操作者の認証を管理する生体認証管理クライアントを備えている（例えば、特許文献１参照）。
【０００３】
この様な認証システムでは、認証精度を上げる方法として、単独の高い認証精度を持つ生体認証情報を使って認証を行うか、指紋と声紋と顔といった複数の生体情報を併せて使

うことで精度の高い認証を行っている。
【特許文献１】特開２００３－１７８０３１号公報
【発明の開示】
【発明が解決しようとする課題】
【０００４】
このように従来の認証システムは、認証精度を上げる為にクライアント端末装置において、複数の生体認証情報についてそれぞれ照合するか、単独の高い認証精度を持つ生体認証情報を用いた端末操作者の認証を行うため、業務の実行に直接関わるクライアント端末装置での認証に手間が掛かり迅速な業務開始ができなかった。
【０００５】
そこで、本発明は、全体としての認証精度を高くできるとともに再度の個人認証を迅速に行うことができる認証システムを提供する。
【課題を解決するための手段】
【０００６】
本発明の認証システムは、予め登録されている所定の認証精度を有する第１の生体認証情報を使用して部屋の入り口において該当する個人か否かの認証を行う第１の認証手段と、部屋の入り口において該当する個人から生体情報を取得し、第１の生体認証情報よりも認証精度が低い第２の生体認証情報を作成する第１の認証情報作成手段と、個人識別情報を発行する個人識別情報発行手段と、第１の認証手段が該当する個人の認証を行うと、第２の生体認証情報を上記個人識別情報発行手段が発行した個人識別情報と関連付けて登録する個人情報登録部と、室内において該当する個人から再び生体情報を取得して第２の生体認証情報と同じ種類の第３の生体認証情報を作成する第２の認証情報作成手段と、室内において該当する個人の個人識別情報の入力によって上記個人情報登録部から読み出された第２の生体認証情報と第３の生体認証情報とを比較して該当する個人か否かの認証を行う第２の認証手段とを備える。すなわち、個人認証を２段階に分け、最初に認証精度が高い生体認証情報を使用して個人認証を行い、続いて、最初の認証時に作成した最初のものより認証精度の低い生体認証情報を使用して再び個人認証を行う。
【発明の効果】
【０００７】
本発明によれば、全体としての認証精度を高くできるとともに再度の個人認証を迅速に行うことができる。
【発明を実施するための最良の形態】
【０００８】
以下、本発明の実施の形態を、図面を参照して説明する。なお、この実施の形態は、本発明を、店舗の従業員管理に適用したものについて述べる。
（第１の実施の形態）
店舗内にネットワーク１を配置し、このネットワーク１に店舗サーバ２及び複数台のＰＯＳ端末３-1，…，３-nを接続している。前記店舗サーバ２は店舗の事務所などのバックヤードに設置され、前記各ＰＯＳ端末３-1～３-nは売場の端に設けられた精算所に設置されている。また、前記ネットワーク１に、店舗の従業員出入口近傍に設置された出退勤端末４を接続している。
【０００９】
前記店舗サーバ２は通信インターフェース（Ｉ／Ｆ）５を介して、例えば、センターに設置されている本部システムのコンピュータと通信するようになっている。前記店舗サーバ２にはデータベースを構成する個人情報登録部６が接続されている。
【００１０】
前記出退勤端末４に、予め登録されている認証精度が高い第１の生体認証情報を使用して個人認証を行う第１の認証手段として、例えば、指紋の生体認証情報を使用して個人認証を行う指紋認識装置７を接続している。なお、認証精度が高い生体認証情報としては、指紋の他に、虹彩や静脈の生体認証情報がある。

【００１１】
また、前記出退勤端末４に、該当する個人から生体情報、例えば、顔画像を撮影して入力する顔画像入力装置８を接続している。前記出退勤端末４は、第１の生体認証情報よりも認証精度が低い第２の生体認証情報を作成する第１の認証情報作成手段を備え、前記顔画像入力装置８が入力した顔画像によって第２の生体認証情報である顔画像の生体認証情報を作成するようになっている。なお、認証精度が低い生体認証情報としては、顔画像の他に、声紋や掌紋の生体認証情報がある。
【００１２】
また、前記出退勤端末４に、従業員９が所持しているメモリカードとしてのＲＦＩＤ（無線ＩＤ）カード１０に対する情報のリード、ライトを行うＲＦＩＤ－Ｒ／Ｗ装置１１を接続している。なお、メモリカードとしてはＲＦＩＤカード以外のＩＣカードなどであってもよい。
【００１３】
前記ＲＦＩＤカード１０には、予め該当する従業員の指紋の生体認証情報が登録されている。この登録は店側で行われ、例えば、暗号化されるなどのセキュリティがかけられ、第三者による不正な書き換えができないようになっている。なお、指紋の生体認証情報についてはプライバシー保護の関係から店側で保管しないで、従業員が所持するＲＦＩＤカード１０のみに登録されるようになっている。
【００１４】
前記各ＰＯＳ端末３-1～３-nに、室内において業務を実行するに当たり該当する従業員の個人認証を行う第２の認証手段としての顔認識装置１２を接続するとともに、従業員９が所持しているＲＦＩＤカード１０に対する情報のリード、ライトを行うＲＦＩＤ－Ｒ／Ｗ装置１３を接続している。
【００１５】
このシステムは、出退勤端末４が設置されている従業員出入口において、図２に示す手順に従って個人認証を行う。先ず、Ｓ１にて、従業員出入口から従業員９が入室すると、出退勤端末４はＲＦＩＤ－Ｒ／Ｗ装置１１に、従業員９が所持しているＲＦＩＤカード１０から無線で指紋の生体認証情報を取込ませる。また、指紋認識装置７に、入室した従業員９の指からセンサを使用して指紋を読取らせる。前記指紋認識装置７は、指紋を読取ると、この読取った指紋の生体認証情報とＲＦＩＤ－Ｒ／Ｗ装置１１がＲＦＩＤカード１０から取り込んだ指紋の生体認証情報とを照合し、一致しているか否かを判断する。そして、一致を判断すると正規の従業員であると認証し出退勤端末４に伝える。
【００１６】
この認証が終了すると、続いて、Ｓ２にて、顔画像入力装置８を制御して従業員９の顔画像を撮影する。そして、出退勤端末４は、顔画像入力装置８が撮影した顔画像から特徴部分を抽出し、指紋に比べて認証精度が低い顔画像の生体認証情報を作成する（第１の認証情報作成手段）。
【００１７】
また、Ｓ３にて、前記出退勤端末４は該当する従業員に対して個人識別情報を発行する（個人識別情報発行手段）。
なお、ここでは顔画像の生体認証情報の作成及び個人識別情報の発行を出退勤端末４で行ったが、顔画像入力装置８で行っても、あるいは店舗サーバ２で行ってもよい。
【００１８】
続いて、Ｓ４にて、出退勤端末４は、発行された個人識別情報をＲＦＩＤ－Ｒ／Ｗ装置１１を使用して従業員９が保持しているＲＦＩＤカード１０に書込むとともに、この個人識別情報と顔画像の生体認証情報を対として、ネットワーク１を介して店舗サーバ２に送信する。
Ｓ５にて、店舗サーバ２は、受信した個人識別情報と顔画像の生体認証情報の対を個人情報登録部６に登録する。
【００１９】

また、このシステムは、ＰＯＳ端末３-1～３-nが設置されている店舗内において従業員がＰＯＳ端末を操作する作業を開始する時には、図３に示す手順に従って個人認証を行う。

先ず、Ｓ１１にて、ＰＯＳ端末３-1～３-nは、ＲＦＩＤ－Ｒ／Ｗ装置１３を制御しＰＯＳ端末３-1～３-nの作業を開始する従業員９が所持しているＲＦＩＤカード１０から、このカードに入室時にＲＦＩＤ－Ｒ／Ｗ装置１１によって書込まれた個人識別情報を読取る。

【００２０】

続いて、Ｓ１２にて、ＰＯＳ端末３-1～３-nは、ＲＦＩＤ－Ｒ／Ｗ装置１３が読取った個人識別情報を、ネットワーク１を介して店舗サーバ２に送信する。そして、店舗サーバ２から、該当する顔画像の生体認証情報を受信する。このとき、店舗サーバ２はＰＯＳ端末から受信した個人識別情報に基づいて個人情報登録部６から該当する顔画像の生体認証情報を読み出し、ネットワーク１を介して該当するＰＯＳ端末に送信する制御を行う。

【００２１】

続いて、Ｓ１３にて、顔認識装置１２は、該当する従業員９の顔画像を撮影し、この撮影した顔画像から特徴部分を抽出して第３の生体認証情報である顔画像の生体認証情報を作成する。そして、この顔画像の生体認証情報と店舗サーバ２からＰＯＳ端末が受信した該当する顔画像の生体認証情報を比較し、本人か否かの認証を行う。

そして、顔認識装置１２が本人であると判断した場合は、ＰＯＳ端末はこの従業員９による操作を許可する。

【００２２】

このように、この認証システムによれば、迅速な認証が要求されない入室時には認証精度の高い指紋の生体認証情報を使用して厳密な個人認証が行われる。これにより、予め指紋を登録している従業員以外が入室することは困難となる。すなわち、不審者の入室を防止し、従業員のみを確実に入室させることができる。

【００２３】

そして、一旦入室した後においては従業員がＰＯＳ端末の作業を開始する場合に、顔画像という指紋に比べて認識精度が低い生体認証情報を使用して個人認証が行われる。これにより、入室時に一端認証された従業員がＰＯＳ端末で作業する場合には、低い認識精度の顔画像で迅速に個人認証されることになる。こうして、作業開始がスムーズに行われる。

【００２４】

また、低い認識精度の顔画像については、入室時に撮影した顔画像を登録し、この登録した顔画像を使用して行うので、たとえ従業員の顔画像が前日に比べて髪型や化粧などによって変化していても、その変化した顔画像を使用することになるので、充分に従業員を認識することができる。

【００２５】

このように、入室時には認証精度の高い指紋の生体認証情報を使用して厳密な個人認証を行い、一旦入室した後は入室時に撮影した顔画像を使用して個人認証を行うので、全体としての認証精度を高くできるとともにＰＯＳ端末での作業時に行われる再度の個人認証を迅速に行うことができる。

【００２６】

しかも、指紋情報は従業員が所持しているＲＦＩＤカード１０に登録され、店側の店舗サーバ２などには登録されていないので、あくまで個人管理となり、指紋情報がネットワーク上に流れて不当に利用される虞はない。

【００２７】

また、入室時に顔画像の生体認証情報を作成したときに個人識別情報を発行して従業員が所持しているＲＦＩＤカード１０に書込むと共に作成した顔画像の生体認証情報と個人識別情報を対として個人情報登録部６に登録し、その後ＰＯＳ端末の作業を開始する場合にＲＦＩＤカード１０から個人識別情報を読取って個人情報登録部６から該当する顔画像

の生体認証情報を取り出すようにしているので、ＲＦＩＤカード１０と顔画像の生体認証情報とは常に対応しており、他人のＲＦＩＤカード１０を使用してＰＯＳ端末の作業を開始するような不正な行為を確実に防止できる。

【００２８】

（第２の実施の形態）

なお、前述した実施の形態と同一の部分には同一の符号を付し詳細な説明は省略する。

図４に示すように、顔画像入力装置８に代えて音声入力装置１５を出退勤端末４に接続し、顔認識装置１２に代えて音声読取装置１６をＰＯＳ端末３-1～３-nにそれぞれ接続している。すなわち、第２の認証手段として音声読取装置１６を使用したものである。音声も顔画像と同様に指紋に比べて認証精度は低い。

【００２９】

前記音声入力装置１５は従業員９の音声を入力し、出退勤端末４は入力した音声から特徴部分を抽出して第２の認証手段である音声読取装置１６での照合に使用する音声の生体認証情報を作成するとともに個人識別情報を発行する。

【００３０】

前記出退勤端末４は、発行された個人識別情報をＲＦＩＤ－Ｒ／Ｗ装置１１を使用して従業員９が保持しているＲＦＩＤカード１０に書込むとともに、この個人識別情報と音声の生体認証情報を対として、ネットワーク１を介して店舗サーバ２に送信する。店舗サーバ２は受信した個人識別情報と音声の生体認証情報の対を個人情報登録部６に登録する。

【００３１】

ＲＦＩＤ－Ｒ／Ｗ装置１３はＰＯＳ端末３-1～３-nの作業を開始する従業員９が所持しているＲＦＩＤカード１０から個人識別情報を読取る。そして、ＰＯＳ端末はＲＦＩＤ－Ｒ／Ｗ装置１３が読取った個人識別情報を、ネットワーク１を介して店舗サーバ２に送信する。店舗サーバ２は受信した個人識別情報に基づいて個人情報登録部６から該当する音声の生体認証情報を読み出し、ネットワーク１を介して該当するＰＯＳ端末に送信する。

【００３２】

音声読取装置１６は従業員９の音声を読取り、この音声の特徴部分から音声の生体認証情報を作成し、この音声の生体認証情報とＰＯＳ端末が店舗サーバ２から受信した該当する従業員の音声の生体認証情報を照合して本人か否かの認証を行う。そして、両音声生体認証情報の一致を判断すると、本人であることを認証し従業員９によるＰＯＳ端末の操作を許可する。

【００３３】

このように、ＰＯＳ端末での認証に音声の生体認証情報を使用しているので迅速な個人認証ができる。そして、音声の生体認証情報は認識精度が低いが、入室時に音声を取込んで登録し、この登録した音声の生体認証情報を使用して行うので、最新の音声を使用して照合ができる。従って、音声情報を使用しても従業員を区別できる程度の十分な認証精度は得られる。

従って、本実施の形態においても前述した実施の形態と同様の作用効果が得られるものである。

【００３４】

なお、前述した各実施の形態では、入室時に指紋による個人認証を行った後、顔画像や音声の生体認証情報を作成するとともに個人識別情報を発行するものについて述べたが、個人識別情報については予め登録したものを使用しても、あるいは無くてもよい。予め登録したものを使用する場合は、例えば、従業員番号等が適している。また、個人識別情報を使用しない場合は個人情報登録部６に登録されている顔画像や音声の生体認識情報の全てを取込んだ顔画像や音声の生体認識情報と比較することになる。従って、登録する顔画像や音声の生体認識情報の量が少ない場合には適している。

また、この各実施の形態では、第２の認証手段をＰＯＳ端末に接続し、このＰＯＳ端末の作業を開始する従業員に対して個人認証を行うようにしたが必ずしもこれに限定するも

のではなく、例えば、決済端末やＦＡＸ、印刷、コピーなどの機能を備えた複合装置、在庫管理装置など店舗内に設置される端末や装置等に接続し、これら端末や装置等を使用する人に対して個人認証を行うものであってもよい。

なお、前述した各実施の形態は本発明を店舗の従業員管理に適用したものについて述べたがこれに限定するものでないのは勿論である。

【図面の簡単な説明】

【００３５】

【図１】本発明の、第１の実施の形態を示すブロック図。

【図２】同実施の形態における第１の認証手段による認証手順を示す流れ図。

【図３】同実施の形態における第２の認証手段による認証手順を示す流れ図。

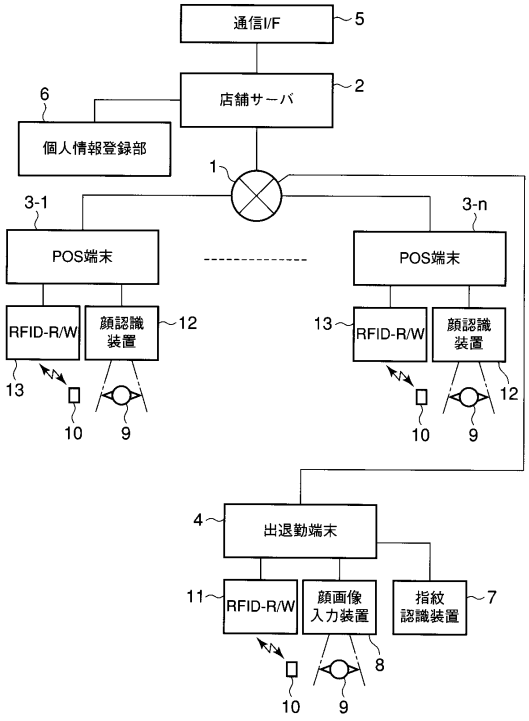
【図４】本発明の、第２の実施の形態を示すブロック図。

【符号の説明】

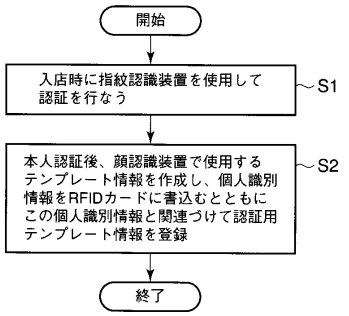
【００３６】

２…店舗サーバ、６…個人情報登録部、７…指紋認識装置、８…顔画像入力装置、１０…ＲＦＩＤカード、１１，１３…ＲＦＩＤ－Ｒ／Ｗ装置、１２…顔認識装置。

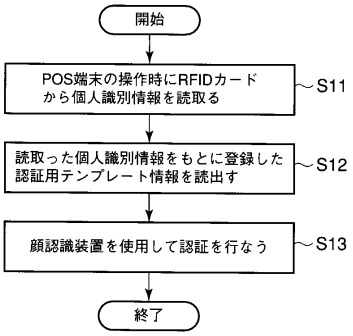
【図１】



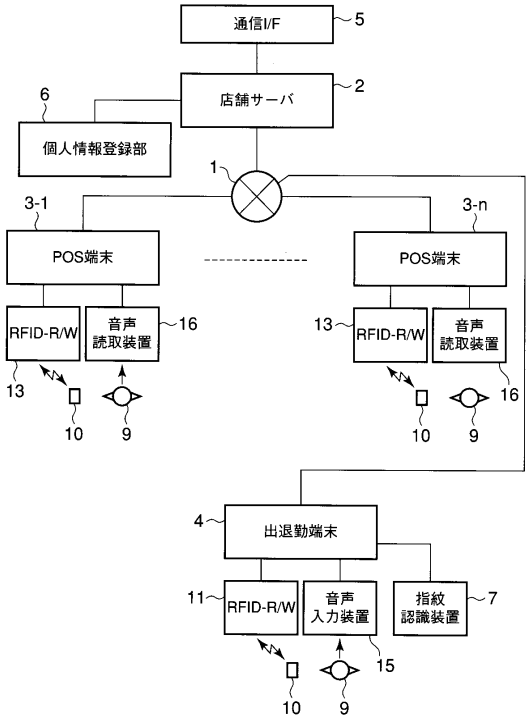
【図２】



【図３】



【図４】


通信I/F
5
店舗サーバ
2
6
個人情報登録部
1
3-1
3-n
POS端末
POS端末
RFID-R/W
音声
読取装置
16
13
10
9
13
RFID-R/W
音声
読取装置
16
10
9
4
出退勤端末
11
RFID-R/W
音声
入力装置
15
指紋
認識装置
7
10
9

フロントページの続き

(72)発明者　望月　啓希
静岡県三島市南町６番７８号　東芝テック株式会社三島事業所内
(72)発明者　渡邉　宏一
東京都中央区日本橋浜町３丁目２１番１号　日本橋Ｆタワー　東芝テック株式会社内

審査官　間野　裕一

(56)参考文献　特開２００１－２２９３５０（ＪＰ，Ａ）
特開２００３－１８６８４５（ＪＰ，Ａ）
特開平７－２０８００１（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／２０
Ｇ０６Ｋ　１７／００
Ｇ０６Ｔ　７／００