(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4097710号
(P4097710)
(45)発行日　平成20年6月11日(2008.6.11)　(24)登録日　平成20年3月21日(2008.3.21)

(51)Int.Cl.　F I
G06T 7/00 (2006.01)　G06T 7/00 510B

請求項の数 5 (全 11 頁)

(21)出願番号	特願平10-533957
(86)(22)出願日	平成10年1月19日(1998.1.19)
(65)公表番号	特表2001-508902(P2001-508902A)
(43)公表日	平成13年7月3日(2001.7.3)
(86)国際出願番号	PCT/GB1998/000154
(87)国際公開番号	WO1998/032093
(87)国際公開日	平成10年7月23日(1998.7.23)
審査請求日	平成17年1月18日(2005.1.18)
(31)優先権主張番号	97300328.8
(32)優先日	平成9年1月17日(1997.1.17)
(33)優先権主張国	欧州特許庁(EP)

(73)特許権者
ブリティッシュ・テレコミュニケーションズ・パブリック・リミテッド・カンパニー
イギリス国、イーシー１エー・７エージェイ、ロンドン、ニューゲート・ストリート　８１
(74)代理人
弁理士　鈴江　武彦
(74)代理人
弁理士　村松　貞男
(74)代理人
弁理士　橋本　良郎
(74)代理人
弁理士　白根　俊郎

最終頁に続く

(54)【発明の名称】セキュリテイ装置及び方法

(57)【特許請求の範囲】
【請求項１】
変りやすいディジタルシグネチャーに基づいて、ある人物がセキュリテイチェックを通過することを承認されるかどうかを判断する方法であって、該方法はプログラミングされたプロセッサで実行されるものであり、且つ、
該セキュリテイチェックを通過しようと試みる前記人物により提供されたディジタルシグネチャーを受領する段階と、
該受領したディジタルシグネチャーと第１のデータ記憶領域に記憶された基準のディジタルシグネチャーとの間の類似性の第１の測度を計算する段階と、
前記計算段階が該受領したディジタルシグネチャーと該基準ディジタルシグネチャーとの間の類似性の第１の測度が第１の所定の閾値よりも低いと判断する場合には、該人物は該セキュリテイチェックを通過することを承認されないことを示す信号を生成する段階と、
前記計算段階が該受領したディジタルシグネチャーと該基準ディジタルシグネチャーは十分に類似していると判断する場合には、該セキュリテイチェックを通過しようと以前に試みたときに提供された１又は複数の以前のディジタルシグネチャーにアクセスする段階であって、前記以前のディジタルシグネチャーは第２のデータ記憶領域に記憶されるものと、
該受領したディジタルシグネチャーと該１又は複数の以前のディジタルシグネチャーとの間の類似性の第２の測度を計算する段階と、
該受領したディジタルシグネチャーと１又は複数の以前のディジタルシグネチャーとの間

の類似性の第２の測度が第２の所定の閾値と同じまたは第２の閾値よりも高い場合には、該人物は該セキュリテイチェックを通過することを承認されないことを示す信号を生成する段階と、
該受領したディジタルシグネチャーと１又は複数の以前のディジタルシグネチャーとの間の類似性の第２の測度が該第２の所定の閾値よりも低い場合には、該人物は該セキュリテイチェックを通過することを承認されることを示す信号を生成する段階と、を備える方法。
【請求項２】
該受領したディジタルシグネチャーが１又は複数の以前のディジタルシグネチャーと同一である場合に、該人物は該セキュリテイチェックを通過することを承認されないことを示す信号が生成される請求項１記載の方法。
【請求項３】
前記受領したディジタルシグネチャーは生理学的情報を含む請求項１または２記載の方法。
【請求項４】
前記生理学的情報はアイリスコードを含む請求項３記載の方法。
【請求項５】
セキュリテイチェックを行う際に使用するための装置であって、
使用者により提供されたディジタルシグネチャーを受領するための入力手段と、
１又は複数の基準ディジタルシグネチャーと、該基準ディジタルシグネチャーを提供した承認された使用者を識別するそれぞれの関係する情報事項とを記憶するための第１の記憶手段と、
該識別された承認された使用者に属した以前の認識試行で得られた以前のディジタルシグネチャーを記憶するための第２の記憶手段と、
該第１の記憶手段にアクセスし、受領したディジタルシグネチャーと１又は複数の基準ディジタルシグネチャーとの間の類似性の第１の測度を計算し、該受領したディジタルシグネチャーと基準ディジタルシグネチャーとの間の計算された類似性の第１の測度が類似性の第１の所定のしきい値を越えている場合には、該使用者を受領したディジタルシグネチャーの作成者として識別するための第１の処理手段と、
第２の記憶領域にアクセスし、受領したディジタルシグネチャーを識別された承認された人物に属する以前の認識試行と関係する以前のシグネチャーとの間の類似性の第２の測度を計算して、受領した識別されたディジタルシグネチャーと以前のディジタルシグネチャーとの間の類似性の第２の測度が第２の所定のしきい値を越えない場合には該識別を承認するための第２の処理手段と、
受領したディジタルシグネチャーと基準ディジタルシグネチャーとの間の類似性の第１の測度が第１の所定のしきい値を越えていると第１の処理手段が判断する場合にのみ第２の処理手段を実行させるための制御手段であって、受領したディジタルシグネチャーと基準ディジタルシグネチャーとの間の類似性の測度が第１の所定のしきい値を越えていないと第１の処理手段が判断する場合に該使用者は該セキュリテイチェックを通過することを承認されないことを示す信号を生成するように構成された制御手段と、を備える装置。
【発明の詳細な説明】
この発明は、セキュリテイチェック（保安検査）を実施するときに使用される方法と装置とに関する。一回の使用から次の使用までに予期しない変化をするデータ列（シーケンス）に頼っている認識方法を用いる装置との関連で特別な有用性を備えている。
既知のセキュリテイチェックは、とりわけ、建物への出入り、保安状態にある計算機システムへのアクセスを管理したり、承認された人物にその者の銀行口座から現金を抽き出すことを許すようにしている。正規には、ユーザ（使用者）がアルファ数字のパスワード（これは例えば個人認識番号ＰＩＮで承認された人物の銀行口座と関係しているものでよい）を入力することが求められる。もしパスワードがその承認された人物と関係している記憶されたパスワードと符合すれば、その使用者はセキュリテイチェックを通過する。問題

が起るのは承認されていない人物がパスワードを知ってしまうことで、その者はセキュリテイチェックを簡単に通過できることである。
最近では、アルファ数字パスワードではなくディジタルシグネチャー（署名）の使用が示唆されている。ディジタルシグネチャーの多くの類型はある人物の生理学的特徴（バイオメトリック、生物測定として知られている）を反映している。こういったシグネチャーの下にある生理学的特徴は他人によっては作ることができず、したがって生物測定応用のディジタルシグネチャーは従来形のパスワードよりは大きなセキュリテイを提供している。示唆されている生物測定は指紋、音声サンプル、網膜走査、およびアイリス（虹彩）パターンがある。ディジタルシグネチャーの他の類型、たとえばある人物が書いた署名のディジタル化したバージョンもまた考慮されている。
アルファ数字パスワードに対して、同じディジタルシグネチャーを、例えば生物測定とか手書き署名（シグネチャー）の二つの試行から正確に得るという確率はときに低いものであり、このような不一致のディジタルシグネチャーに基いての認識は基準のディジタルシグネチャーに十分近いディジタルシグネチャーを得ることに依存している。例えば、認識と関連して、測定したアイリスコード間の差は、カメラの設定の違いとか、照明レベルの変動から生ずるし、あるいは部分的に眼瞼の閉じとか眼鏡上よごれやごみなどが原因することがある。手書きのシグネチャーの場合には、ディジタルシグネチャーの差はデータ捕捉の差が原因するだけでなく、書かれた署名そのものの変化も原因している。
欧州特許出願0 392 159は書かれた署名の確認方法を開示しており、この方法では使用者の書いた署名（シグネチャー）が基準シグネチャーであってその使用者がなりきろうとしている承認された人物により供給されたものと比較がされる。この基準シグネチャーは登録プロセスの際に供給される。もしある使用者により提供されたにわか作りの（インスタント）シグネチャーと使用者が意図している承認された人物により提供された基準シグネチャーとの間に顕著な差があれば、そのときはその使用者は詐称者と見なされる。基準シグネチャーと使用者のシグネチャーとの間の差が予想された程度である場合に限り、その使用者は承認された人物であると確認される。
多くのセキュリテイチェックに共通な問題は、セキュリテイのレベルであり、このレベルは登録時に用意することができるものであって、ある使用者が後にセキュリテイチェックを通過しようと試みることができる現場では承認された人物が整合をとれないということである。例えば、共用資源へのアクセスが遠隔地の使用者にできるようにしているシステムでは、パスワードとかディジタルシグネチャーでセキュリテイチェックが頼りとしているものはチェックされる前に通信リンクを介して送られていなければならず－この状態は銀行が用意する自動出納機と関係して発生する。さらに、ある状況では、書かれた署名や生物学的測定をディジタイズする装置は承認されていないアクセスを可能とするために変更されるということに対して無防備である。例えば、承認されていない使用者はポイント・オブ・セール（ＰＯＳ）デバイス内部のディジタルメモリに接続をとって後のこのデバイスを使用する承認された人物のパスワードとかディジタルシグネチャーを学習するかもしれない。
このような問題を回避するための一方法は各パスワードもしくはディジタルシグネチャーを送る前に時刻（タイム）スタンプをつけることである。しかし、時刻スタンプを用意するにはシステムの分散されたノードが同期をとる必要があり、これは実現が困難でもあるし、金もかかることでもある。
この発明の第１の特徴によると、一定でない変りやすい（コンスタントでない）ディジタルシグネチャーに基づいて、ある人物がセキュリテイチェックを通過することを承認されているかどうかを判断する方法が提供されていて、その方法は：記憶されたディジタルシグネチャーを備えるセキュリテイチェックを通過しようと試みる人物により提供されたにわか作りのシグネチャーを記憶されたディジタルシグネチャーと比較し；
該シグネチャーが十分に類似していると見る該比較に応答して、その人物を該記憶されたディジタルシグネチャーを提供した人物と同定する段階を含み；かつ、
前記方法は、

該にわか作りのディジタルシグネチャーとセキュリテイチェックを通過しようと以前に試みたときに提供された１又は複数の以前のディジタルシグネチャーとを比較し；かつ、
該にわか作りのシグネチャーが１または複数の以前のシグネチャーとは類似してはいそうもないと見る該比較に応答して同定を無効とすることを特徴とする方法である。
不安定なディジタルシグネチャーが前に提出されたシグネチャーのバージョンと密着した整合をとっていないことをチェックするように装置をしつらえることによって、盗聴者にとってシステムへの承認なしのアクセスができるようになるということの危険は軽減される。
ある実施態様では、にわか作りのシグネチャーが前のシグネチャーと同一であるときにだけ識別子が無効とされる。この場合には、前のディジタルシグネチャーを正確にコピィした盗聴者はセキュリティチェックを通過することを否定され、その一方で承認された人物が誤ってアクセスを否定される機会が減ることになる。
別な実施態様では、１又は複数の以前のシグネチャーと密接に整合しているにわか作りのディジタルシグネチャーでまた識別子が無効とされる。これは承認されていない使用者に優越するすなわち彼等の裏をかくもので、例えば指の型を用いて指紋を作ったり、アイリスパターンを作るのに眼の写真をとったり、手書き署名のファイクシミリなどを用いてセキュリテイチェックを破ろうとする使用者に対処できる。
好ましい実施例ではにわか作りのシグネチャーを基準シグネチャーと比較することには両シグネチャー間の類似性についての第１の測度を計算することを含み；類似性の第１の測度が所定の第１のしきい値を越えているとその使用者を承認された人物であると識別し；
にわか作りのディジタルシグネチャーを１又は複数の以前のディジタルシグネチャーと比較することには両シグネチャー間の類似性について１又は複数の第２の測度を計算することを含み；使用者の識別は類似性の第２の測度が第１のものよりも大きな所定の第２のしきい値を越えていて、しかも前記第１と第２のしきい値の少くとも一方が適応性をもっているときにはその使用者の識別子は無効とされる。これが承認された人物についてその者のディジタルシグネチャー内に本来的な偏位としてある差を補償するという利点を作り出している。加えて、承認された人物のディジタルシグネチャー内の差異で場所とか時間とかが原因で生ずることになるものもこの方法で補償される。
この発明の第２の特徴によると、セキュリテイチェックを行う際に使用するための装置が用意されていて、この装置の構成は：
使用者により提供されたディジタルシグネチャーを受取るための入力手段と；
１又は複数の基準ディジタルシグネチャーと、基準シグネチャーを提供した承認された人物を識別するそれぞれの関係する情報事項とを記憶するための第１の記憶手段と；
識別された承認された人物に属するとした以前の認識試行で得られた以前のディジタルシグネチャーを記憶するための第２の記憶手段と；
第１の記憶手段にアクセスし、受取ったディジタルシグネチャーを１又は複数の基準ディジタルシグネチャーと比較し、受取ったディジタルシグネチャーと基準ディジタルシグネチャーとの間の類似性の測度が類似性の第１の所定のしきい値を越えている場合には、その使用者を受取ったディジタルシグネチャーの作成者として識別するための第１の処理手段と；
第二の記憶領域にアクセスし、受取ったディジタルシグネチャーを識別された承認された人物に属するとした以前の認識試行と関係する以前のシグネチャーと比較して、受取ったディジタルシグネチャーと以前のディジタルシグネチャーとの間の類似性の第２の測度が第２の所定のしきい値を越える場合には識別子を無効とするための第２の処理手段とで成る。
さらに追加して以前の認識試行で提出されたディジタルシグネチャー間の類似性について考慮することにより、この装置は既知のセキュリテイチェック装置により提供されるよりも高度のセキュリテイを提供する。
下記の図面を参照して、例としてこの発明の実施態様を記述して行く。
図１は例示の人物識別、クライアント／サーバシステムの図である；

図２は図１のシステムのサーバ処理プラットホームの詳細を示す図である。
図３は使用者認識に必要とされるデータの構成を示す図である。
図４は使用者認識を演ずるのに必要とされる段階を示す流れ図である。
図５は承認された人物に対するアイリスコード認識の特性を示す流れ図である。
図１によると、アイリス（虹彩）コード生成器１００は使用者の眼１１０の画像を捕えるようにされている。アイリスコード生成器は手で持つ装置であり、出願人の未決特許出願PCT/GB97/01524，PCT/GB97/01525及びPCT/GB97/01526に記載されているものであり、ここで参照に供するものとする。生成器１００は捕えた画像を２５６バイトアイリスコードに変換するが、それはここで参照に供する米合衆国特許5,291,560に記載されている技術による。生成器１００はそこでアイリスコードをクライアント計算機システム１２０に送るがこのシステムはアイリスコードを受取って、後にアイリスコードを通信チャンネルを経て認識サーバ１６０に送る。将来の実施態様では生成器１００とクライアント計算機システムとは単一の専用ハードウェア装置として実施されるようになると思われる。
通信チャンネルは計算機１２０をセキュリテイのある私設データ網のような通信網１４０に接続するモデムを含む。網１４０はアイリスコードを第２のモデム１５０を経てサーバ１６０にルート設定する。サーバ１６０は外部記憶装置２７０例えばハードディスクドライブに接続されていて、以下に詳述するように、受取ったアイリスコードに基づいて認識処理をおこなう。
サーバ１６０は別な機能とかサースにアクセスをしたいと試みている承認されている人物を識別し、確認を与える。別な機能（図示せず）はセキュリテイのある通信網であって、肯定的な認識があった後にだけ認識サーバを経てアクセスできるものであるかもしれない。
図２は認識サーバ１６０の処理用プラットホーム２００の主成分を示す。サーバプラットホーム２００は、Sun（TM）SPARCステーション20/51のような通常の計算用プラットホームであり、UNIX（TM）オペレーテングシステムで動作し、Oracle（TM）データベース管理システムを作動させているものである。プラットホーム２００は中央処理装置２１０の標準的な特徴を含んでおり、中央制御装置２１０はアドレス及びデータバス２２０を経て主メモリ２３０と入力／出力（Ｉ／Ｏ）制御器２４０に接続されている。モデム１５０はＩ／Ｏ制御器２４０に直列接続２５０を経て接続されていて、またハードディスクドライブ１７０は並列ライン２６０を経てＩ／Ｏドライバ２４０に接続されている。
ディスクドライブ１７０は二つのOracleデータ記憶領域を含む。第１のデータ記憶領域２７３は複数の承認された人物に対する基準アイリスコードを含み、また第２のデータ記憶領域２７６は過去のアイリスコード情報でそれぞれの承認された人物各人についてのものを記憶する。
第１と第２のデータ記憶領域は図３により詳細に示されている。第１のデータ領域２７３は基準アイリスコード１ないしｎを単一のデータベース表３００内に含み、そこでは各アイリスコードは承認された人物１ないしｎと関係が付けられている。基準アイリスコードは適当な承認されている人物の登録プロセスによって得られたものである。このプロセスはいろいろな違った形式をとることができるが、一般には承認された人物が登録センタを訪ねて、そこで一連のアイリスコードが生成されて、単一の基準アイリスコードが選べるようにすることが必要とされる。
第２のデータ領域２７６はｎの別々なデータベース表３１０１ないし３１０ｎに分けられて、１つの表が各承認された人物に対する指標を付せられている。例示のように表３１０１は類似性のしきい値レベルに対する値と、承認された人物１に対するアイリスコードＡないしＤを含んでいる。アイリスコードＡないしＤは過去のアイリスコードで、承認された人物１に属するとした以前の認識試行でサーバ１６０により受取られたものである。承認された人物１に対する表の大きさは、後述するように、承認された人物１が認識される各度毎に１アイリスコード分だけ増えて行く。しかし実際には、データ記憶容量は無制限ではないから、記憶されるアイリスコードの数は例えば最新の百ということに制限されることになろう。

アイリス認識プロセスは図４の流れ図を参照して記述される。このプロセス自体は適当なソフトウェアプロセスとルーチンであってOracle SQLとC++で書かれたもので成る。
図４によると、段階４００では認識サーバ１６０はクライアント１２０からアイリスコードを受取る。アイリスコードは主メモリ２３０内の第一の一時的メモリ位置（ＴＥＭＰ（Temp）１）に記憶される。次に段階４０５では、第１のデータ記憶領域２７３内のデータ表が主メモリ２３０内に読取られる。データ表の大きさが主メモリよりも大きいとすると、そのときはファイルサーバ１６０は正常のやり方で必要とされているように、適当な大きさの表の一部を主メモリへ読取るようにしている。段階４１０，４１５，４２０では、サーバ１６０は主メモリ２３０をアクセスして読取り、各基準アイリスコードを一時メモリ位置（ＴＥＭＰ１）内に記憶されている受取ったアイリスコードと整合が見つかるまで比較する。この比較はビット毎ベースで（２５６×８ビットがある場合）行なわれ、整合するビットの数が各基準アイリスコードに対して求められる。この実施例では、整合は識別を構成していて、ビットの最大３０％が違っていても整合が得られる。
約３０％というしきい値は相当量の試行に基づいて帰納的に決められたもので、この結果についてはもっと詳細に次の文献で論じられている。“High confidence visual recognition of persons by a test of statistical independence”,Daugman J G,IEEE Transactions on pattern analysis and machine intelligence（PAMI）,vol.15,November 11,1993. 無論、数値とか比較方法とかは類型もしくは異類型間の変化が使用するアイリス捕捉装置１００にあるのでそれらに依存し、また画像捕捉環境とか、使用されるアイリスコード生成アルゴリズムとか、システムに求められるセキュリティのレベルとかといった他の要因に依存する。例えば、セキュリティが低い方のシステムでは短い、もっと詳細を含んでいないアイリスコードで動作することになろう。
段階４２０では、整合が見付からないときに、アイリスコードが識別されなかったとされて、段階４２５では適当な信号がクライアント１２０に戻される。
受取ったアイリスコードに対して整合が見付かったとすると、段階４３０ではそれぞれの基準アイリスコードと関係するサーバ１６０は承認された人物の識別子と第２の一時的なメモリ位置（ＴＥＭＰ２）へ読込む。整合する基準アイリスコードが承認された人物１と関係しているとすると、段階４３５ではサーバは第２のデータ記憶領域２７６にアクセスして、主メモリ２３０へ承認された人物１に属するものとされた過去のアイリスコードを含む表３１０１を読込む。また承認された人物１に対する類似性のそれぞれの測度に対するしきい値が第３の一時的なメモリ位置（ＴＥＭＰ３）へ読込まれる。
段階４４０では、各過去のアイリスコードが種メモリから読取られて受取ったアイリスコードと比較される。各アイリスコードの比較について、段階４４５では、もし正確な一致整合が見付かると、受取ったアイリスコードは詐欺的にものと見なされ、段階４５０では適当なメッセージがサーバ１６０によりクライアント１２０へ遅れて、プロセスは終る。
正確な一致整合が詐欺行為によるアイリスコードであると見る規準は２つのアイリスコードがたとえ同一の承認された人物から発したものであるとしても一致整合することはありそうもないという事実に由来する。したがって、正確な一致整合は、整合した過去のアイリスコードが承認されていない使用者によって傍受されて、承認された人物により試みられた以前の認識の際にサーバ１６０へ初めに送られたときにコピィされたとされる（承認されていない使用者はその後にこのアイリスコードをサーバに送って、例えばセキュリティのあるシステムへのアクセスを得るためにその承認を受けた人物のように仮面をつけているとされる）。傍受したデータを用いることにより承認された人物になりすますという試みのこの類型のものはときに再生攻撃（replay attack）として知られている。
正確な整合一致がなければ、そのときは整合するビットの百分率に対する値は（この場合は１００よりも小さくなる）が求められて第４の一時的なメモリ位置（ＴＥＭＰ４）に記憶される（段階４５５）。それから段階４６０で、もし第４の一時的なメモリ位置（ＴＥＭＰ４）内に記憶されている類似性の測度が第３の一時的なメモリ位置（ＴＥＭＰ３）内に記憶されている類似性についてのしきい値測度よりも大きいときは、受取ったアイリスコードは詐欺行為のものとみなされて、段階４５０では適当なメッセージがサーバ１６０

によりクライアント１２０へ送られて、このプロセスが終る。
もし受取ったアイリスコードが認識のための両規準を過去のアイリスコードに対して満たしていれば－正確に同じてなく、また類似しすぎてもいない－そのときは段階４６５で信号がサーバ１６０によってクライアント１２０に戻されて、承認された人物が同定識別されて認証が成功して行なわれたことを示す。最後に、段階４７０では、受取ったアイリスコードで第一の一時的なメモリ位置（ＴＥＭＰ１）に記憶されているものが過去のアイリスコードとして承認された人物１のためのデータベース表３１０１に書込まれる。
あるアイリスコードが詐欺行為によるものであるとする規準は、それが過去のアイリスコードへの類似性が類似性についての予め定めたしきい値レベルよりも大きいときには、正確な整合ほどでないとしても非常に近い整合はありそうもないという事実に由来する。
しきい値もまた以下に述べるように試行に基づいて発見的（帰納的）に決められる。この値はまた同じように使用されるアイリス画像捕捉装置１００の類型もしくは類型の変り方に依存したり、画像捕捉環境とかシステムに必要とされるセキュリテイのレベルとかのような他の要因に依存している。
認識の試験が１９９６年１０月に行なわれた。ここでは試験チームの訓練を受けたメンバーがその者達を整列させて、その者達を認識するために基本的な認識システムを作動させた。図５は使用者の眼が整列したときに作動させた５４６の認識に対する認識ハミング距離を示している。これらの認識に対する平均ハミング距離は０．０９０（すなわちビットの不一致で９％）であり、標準偏差は０．０４２であった。これらの結果が示しているのは使用者に対して認識ハミング距離の分布があることを示し、しかも同じような結果が商用アイリス認識システムで期待できることを示している。
図５のグラフを生成するために使用した結果を考慮すると、特定のしきい値に対してある人物を誤って認識することになる以下の確率が求められる。

しきい値（パーセント）	５４６の試行で期待される失敗数
2	3
3	9
4	30
5	83

例えば、しきい値が３パーセントに固定されているとすると、結果は５４６の認識試行が承認された人物によってされる度毎に９が無効とされることを示す。
実際には、サーバ１６０がアイリスコードのビットの９８％よりも大きなアイリスコードに接していると、プロセスを終了する代りに、クライアント１２０に要求して、識別して認証すべき使用者からの別なアイリスコードを得て戻すようにする。このクライアントは今度はアイリスコード生成器を制御して使用者の眼の照明のレベルを変えるとかアイリスコード生成器内部の光学系の焦点長を変えるとかの制御をしてから使用者の眼の他の像を捕捉することとする。このようにして変更したアイリス像を用いるという第２の機会を用意して、承認された人物がセキュリテイのある網へのアクセスを拒否される機会の数を減らさなければならない。
当業者は認証のために軽減された規準が上述のシナリオに適用されてもよいことに気付くであろう。例えば、正確な整合の場合にのみ第２のアイリスコードが要求される。ほかにもっと高度がアイリスコードを比較する実現法としてある種のビット不整合が相対的に起りそうな度合を勘案するか（アイリスコード内の全ビットが同じように変ることはなさそうである）、あるいはそのアイリスに対して以前の識別子についての統計的な一致を勘案することになろう。
実際には、もっと複雑な探索アルゴリズムが第１のデータ領域２７３を走査するための第１の処理段階で使われることになろう。例えば、アイリス認識の場合には、第１のデータ領域を数回走査することが整合するアイリスコードが見付かるまでに必要となり、例えば

その都度眼の違った回転を考慮することになる。違った眼の回転は使用者が頭を違った傾き角度でもって来ることにより生じ、またねじれた眼の回転が原因している。そこで専用のデータベース探索アルゴリズムで米合衆国特許5,291,560に記述されているものを第１の処理段階の目的で使うのがもっと有効である。
上述の米合衆国特許を用いて生成されたアイリスコードの性質は、アイリスコード内の全部のビットではないが、同じように信頼できぬものとなるようにしている。アイリスを符号化するために使用したアルゴリズムは各種のスケールレベル又は詳細もしくはその両方でアイリスの特徴を考慮して、これらの特徴を反映した情報を各アイリスコード内部の特定位置におけるビットに割当てている。そこで、もっと大きな立場でとらえた（マクロスコピックな）特徴に対応するアイリスコードのビットが不正確な設定をされる可能性を小さくすると仮定することが合理的となろう。逆に、あるアイリスの小さな、すなわち詳細に立入った特徴と対応するアイリスコード内のビットは不正確に設定される可能性が余計にあることになろう。
発明者らが認識していることは、特定のビットが不正確に設定される可能性の度合はクライアントのハードウェアの構成、使用される正確なアイリスコード生成アルゴリズム、照明の変化、フォーカスの僅かな違い、汚れや眼ぶたなどの原因でアイリスを閉じてしまうこと、あるいは使用者のある種の性質に非常に依存していることである。これはこういった原因に依存してアイリスコードが信頼できないものになるという異なる類型を期待することが合理的であるとする理由に基づいている。例えばまぶたを閉じることはアイリスの特定の大きさ部分に影響を与え、またごみやよごれといった粒子はもっと局部的なものである。フォーカスの差はアイリスの全部分に影響するが、アイリス像の高い方の空間周波数成分に大きな影響をもつことになる。クライアントハードウェアと関係した作像装置の光路内でのよごれは各認識についてのアイリスコードで同じ部分に影響を与えそうであり、（例えばＣＣＤチップ）からの雑音はその効果がもっと可変性をもっている。捕捉した像のアイリス部分を隔離するために使用される局部化ソフトウェア内の変化は今度はアイリスコード生成で使用される境界の位置に影響を与えることになろう。その結果は詳細な特徴を表わすビットが全体として顕微鏡的な（マイクロスコピックな）特徴に対応しているビットよりも余計に影響されることになろう。
このようにして、もっと総合的なこの発明の実施は不正確に設定されているアイリスコードの中で各ビット又はビット群の類似性を考慮している。不正確に設定されるようになっているビットの類似性を判断するには、判断プロセスが生成されたアイリスコードとクライアントと承認された人物との統計的な性質を使用できることは当業者には自明なことであろう。
さらに、基準アイリスコードもしくはいずれかのしきい値は識別もしくは認証特性あるいはその両方でのシフトに依存して時間がたつと変るかもしれない。例えば、もし特定の承認された人物が一般にいつも同じようなアイリスコード読取りを得ることが明らかになるとして、それが基準アイリスコードの２０パーセント以内であると、識別目的の類似性しきい値が７０パーセントから７５パーセントに上ることになろう。同じように、それ以上は受取ったアイリスコードと過去のアイリスコードとが同じであるとみなされるしきい値は２パーセントから１パーセントに減らされることになろう。パラメータにおけるこのような変化は定期的かつ自動的に認識サーバ１６０によって行なわれることになろう。逆に、もし承認された人物が貧弱なアイリスコード読取りが原因で一致して認識されないとすると、この承認された人物に対するしきい値は低下され、それはアイリスコード読取りがどのくらい貧弱であり、システムのセキュリテイがどの程度で妥協することになるかに依存している。
上述の実施例は使用者が承認された人物であるかないかについての判断を実行しているプロセッサを制御するためのソアトウェアプログラムの使用について記述されたが、少くともディジタルシグネチャー比較段階を実行するためにはハードウェア構成を用いてもよい。
また、上述の実施例の第１の比較段階は基準ディジタルシグネチャーの各々と順々に比較

することを含んでいる。したがって、記述した装置はどの承認されたた使用者がセキュリテイチェックを通過することを試みているかを判断することができる。この発明はまた、セキュリテイチェック用装置の目的が使用者の識別子を確認することである状態でのユーティリティを備えている。例えば、従来からある自動化された出納機（テラーマシン）の使用者は取引を実行する前に、データを記録した磁気ストリップを帯しているカードを挿入することが期待されている。実際には、このカードは識別子トークンとして機能していて、すなわち使用者はその者が入れた個人識別番号（ＰＩＮ）がカードを発給された承認されている人物と関連して記憶されたＰＩＮと整合すればそのときだけ経済取引を実行できることが許される。従来形装置内のＰＩＮの使用がディジタルシグネチャーの使用により置き換えられることになると、中央サーバはカードを発行された承認されている人物と関係している基準シグネチャーとその使用者のディジタルシグネチャーとが対応していること（もっとも似ていすぎないこと）が確認されることだけが必要となる。

上述の実施例は不安定なディジタルシグネチャーでの真性な（インヘレントな）可変性を探求している。したがって、幾分かパラドックス的（逆説的）なところであるが、この発明の実施例はディジタルシグネチャーを捕捉するために使用される装置を改良することによって悪化するかもしれない。例えば、アイリスパターンの像を捕捉するために使用された光学装置での改良は承認された人物のアイリス（虹彩）を捕えた像にほとんど変化がないものを生むかもしれない。これが今度は違った機会にある承認された人物によって作られた２つのアイリスコード間で密着した整合が発生する大きな機会をもたらすことになろう。詐欺行為の使用者と承認されたた人物との間の弁別はそこでもっとむづかしいものになることが想像される。

このような環境では上述の実施例は可変パラメータ（例えば瞳孔直径）をアイリスコードに加えて、セキュリテイチェックを通過しようとする承認された使用者の試みの間で著しく差が生ずるようなディジタルシグネチャーを用意するようにすることで改良ができよう。

【図１】

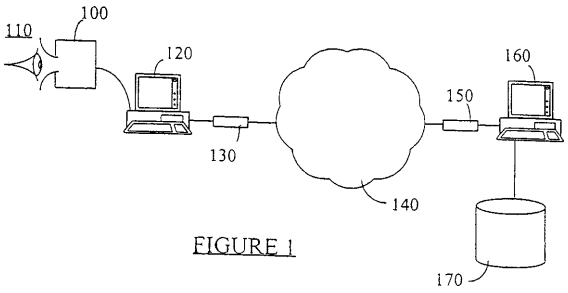

FIGURE 1

【図２】

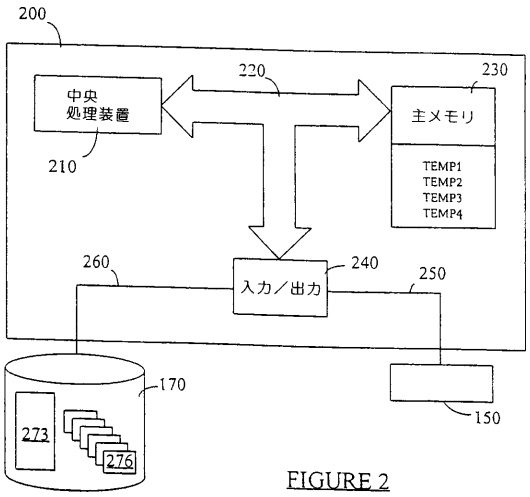

FIGURE 2

【図３】

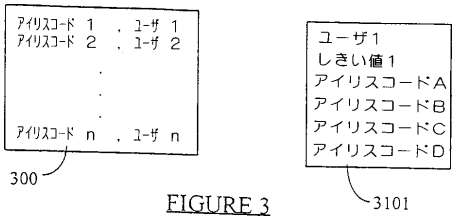

FIGURE 3

【図５】

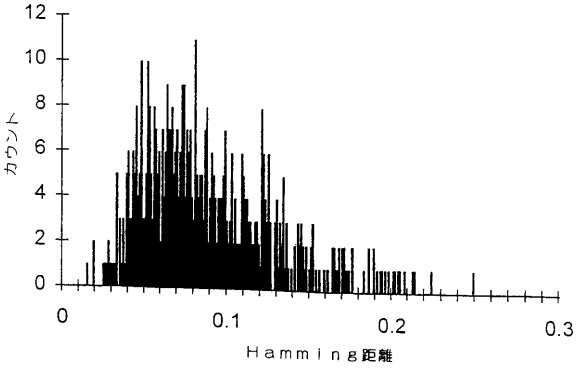

FIGURE 5

【図４】

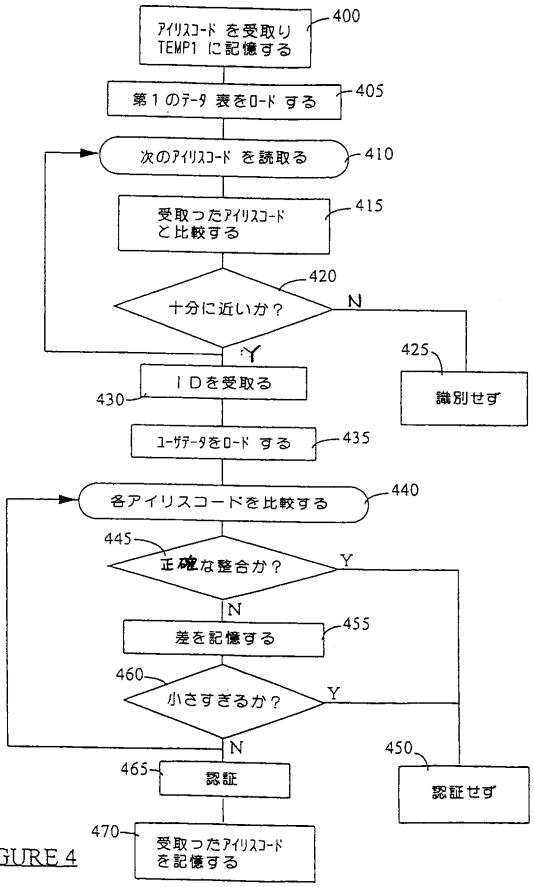
アイリスコード を受取り TEMP1 に記憶する
400
第１のデータ 表をロード する
405
次のアイリスコード を読取る
410
受取ったアイリスコード と比較する
415
十分に近いか？
420
N
Y
425
識別せず
ＩＤを受取る
430
ユーザデータをロード する
435
各アイリスコードを比較する
440
正確な整合か？
445
Y
N
差を記憶する
455
小さすぎるか？
460
Y
N
450
認証せず
認証
465
受取ったアイリスコード を記憶する
470

FIGURE 4

フロントページの続き

(72)発明者　シール、クリストファー・ヘンリー
イギリス国、アイピー１４・２ピーエフ、サフォーク、ストウマーケット、ヒントレスハム・クローズ　１６
(72)発明者　マッカートニー、デイビッド・ジョン
イギリス国、アイピー４・２ティーエイチ、サフォーク、イプスウィッチ、サウス・クローズ　５
(72)発明者　ギフォード、モーリス・マーリック
イギリス国、アイピー５・２ジーアール、イプスウィッチ、ケスグレイブ、ディッキンソン・テラス　１

審査官　松尾　俊介

(56)参考文献　特開昭６２－１７７６８０（ＪＰ，Ａ）
特開平０２－２６８３７３（ＪＰ，Ａ）
特開平１０－０１１５０９（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
G06T　7/00 ～ 7/60