(19)日本国特許庁(JP)

# 再公表特許(A1)

(11)国際公開番号
WO2003/069489

発行日 平成17年11月4日(2005.11.4)

(43)国際公開日 平成15年8月21日(2003.8.21)

| (51)Int.Cl.[7] | F I | | |
|---|---|---|---|
| G06F 15/00 | G06F | 15/00 | 330E |
| H04L 9/32 | H04L | 9/00 | 673C |

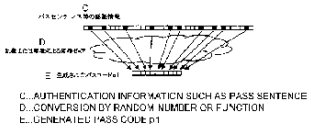
審査請求 未請求 予備審査請求 未請求 (全 21 頁)

出願番号 特願2003-568545 (P2003-568545)
(21)国際出願番号 PCT/JP2002/001256
(22)国際出願日 平成14年2月14日(2002.2.14)
(81)指定国 AP(GH,GM,KE,LS,MW,MZ,SD,SL,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,MD,RU,TJ,TM),EP(AT,BE,CH,CY,DE,DK,ES,FI,FR,GB,GR,IE,IT,LU,MC,NL,PT,SE,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AT,AU,AZ,BA,BB,BG,BR,BY,BZ,CA,CH,CN,CO,CR,CU,CZ,DE,DK,DM,DZ,EC,EE,ES,FI,GB,GD,GE,GH,GM,HR,HU,ID,IL,IN,IS,JP,KE,KG,KP,KR,KZ,LC,LK,LR,LS,LT,LU,LV,MA,MD,MG,MK,MN,MW,MX,MZ,NO,NZ,OM,PH,PL,PT,RO,RU,SD,SE,SG,SI,SK,SL,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VN,YU,ZA,ZM,ZW

(71)出願人 597011762
若山 裕典
埼玉県さいたま市本郷町１５５５－３
(71)出願人 505288192
田中 芳樹
埼玉県さいたま市浦和区領家７－２８－２－７０２
(71)出願人 505288044
島田 憲一
埼玉県秩父市宮側町１５－１４
(72)発明者 若山 裕典
埼玉県さいたま市北区本郷町１５５５－３番地

(54)【発明の名称】本人認証の方法

(57)【要約】
「モニタリング問題を除く認証におけるあらゆる問題に対処可能な認証方法」と、「モニタリングはされないが認証する側による成済ましの可能性及び認証装置からの認証情報盗難による成済ましの可能性があり且つそれぞれ認証内容に個別の問題を持つ認証方法」とを、一つの本人認証処理において二段階で行うことにより通信のインターセプト、モニタリング、盗み見、総当り攻撃、およびユーザの管理外且つシステム外における認証情報の漏洩、複製および偽造による成済ましを防止し、且つ後者の認証方法において「ユーザの発する認証情報と認証装置に登録する認証情報の間に照合可能な非可逆的関係を設けて、認証する側による成済ましや認証装置上からの認証情報盗難による成済ましを防止するようにした」ことによって、本人認証に関し想定し得る全ての問題に対し、少なくとも個別に対処できるようにした。



【特許請求の範囲】
【請求項１】
「モニタリング問題を除く認証におけるあらゆる問題に対処可能な認証方法」と、「モニタリングはされないが認証する側による成済ましの可能性及び認証装置からの認証情報盗難による成済ましの可能性があり且つそれぞれ認証内容に個別の問題を持つ認証方法」とを、一つの本人認証処理において二段階で行うことにより、通信のインターセプト、モニタリング、盗み見、総当り攻撃、およびユーザの管理外且つシステム外における認証情報の漏洩、複製および偽造による成済ましを防止し、且つ後者の認証方法において「ユーザの発する認証情報と認証装置に登録する認証情報の間に照合可能な非可逆的関係を設けて、認証する側による成済ましや認証装置上からの認証情報盗難による成済ましを防止する」ようにしたことによって、本人認証に関し想定し得る全ての問題に対し、少なくとも個別に対処できるようにしたことを特徴とする本人認証の方法。
【請求項２】
「モニタリングを除くあらゆる認証における問題に対処可能な認証方法」について、記数法における大きな基底を持つ値を図形などを用いて表記し、該値を用いることにより少ない要素数で大きな組み合わせ数を持つパスワードを作成できるようにしたことを特徴とする請求の範囲第１項記載の本人認証の方法。
【請求項３】
ユーザからの認証要求があると、認証装置は乱数を生成して認証装置に登録されているパスワードを並べ替えてユーザに提示し、且つ認証装置は認証装置に登録されたユーザのパスワードから該乱数を用いて並べ替えるための配列順を生成し、ユーザは提示されたパスワードのためのキャラクタを、ユーザが登録したパスワードの配列に並べ替えるための配列順を認証装置に通知し、認証装置はユーザから送られてきた配列順と、ユーザからの認証要求時に認証装置が生成した配列順とを照合することによって認証を行うようにしたことを特徴とする請求の範囲第１項および請求の範囲第２項に記載の本人認証の方法。
【請求項４】
「ユーザの発する認証情報と認証装置に登録する認証情報の間に照合可能な非可逆的関係を設けて、認証する側による成済ましや認証装置上からの認証情報盗難による成済ましを防止する」ことについて、認証装置がユーザ毎にユニークな乱数または一方向関数によって、ユーザ毎にユニークなパスセンテンス等の文字列情報、バイオメトリクス情報または鍵情報などの認証情報から非可逆的に変換することにより生成したパスコードｐ１をユーザＩＤおよび該ユニークな乱数または一方向関数と共に認証装置上に登録し、ユーザがユーザ端末からユーザＩＤと共に該文字列情報または鍵情報などの認証情報を送信するか、または認証用端末からバイオメトリクス情報または携帯物に登録された鍵情報などの認証情報を入力することによって認証装置に認証要求を出した場合、認証装置はユーザＩＤによって認証装置に登録されている該ユニークな乱数または一方向関数を呼出し、該ユニークな乱数または一方向関数を使ってユーザ端末または認証用端末から送られてきた該文字列情報、バイオメトリクス情報または鍵情報などの認証情報からパスコードｐ１を生成し、生成されたパスコードｐ１と認証装置上に登録されているパスコードｐ１を照合することにより認証するようにしたことを特徴とする請求の範囲第１項記載の本人認証の方法。
【発明の詳細な説明】
技術分野
この発明は、オープンな通信ネットワーク上から固定型若しくは携帯型の情報通信端末機器を用いて、公開鍵暗号などで信頼性を保証された他の情報端末システム若しくはサーバシステムに対してアクセスするユーザの本人認証の方法と認証に使用する認証情報の形式及び処理方法に関する。
背景技術
古来より、特に軍事・商業の分野において合言葉による相互認証や、例えば「開け胡麻」のようなパスワードによる本人認証及びパーミッションの付与などが行われてきた。また、複数の者が共通の暗号表若しくは仲間内でのみ通用する特殊な文字などによって通信文

を記述することで、関係者間という閉じられた系の中において平分の暗号化および復号化を行い、そのことによって通信文の帰属性の証明即ち相互認証と通信内容の秘匿を行ってきた。この方法は近代になって電信や電話などの電気的通信技術が発達・普及するとともに社会に広く普及した。更に近年、コンピュータ及びデータ通信が発達し普及すると、暗号化・復号化を数学的に処理することにより、処理を自動化し高速化すると共に第三者による解読の困難性を高め、より確実な本人認証を行うようになった。その後、数学的処理による方式は広く社会に普及したが、情報処理技術のハードウェア・ソフトウェア両面にわたる技術革新は、そうした方式を一つひとつ無力化していった。そこで最終兵器のように登場したのが素因数分解問題や離散対数問題を応用した二重鍵暗号システムであった。これは暗号鍵の第三者による解読を数学的に困難にすると共に、鍵そのものを公開鍵と秘密鍵に二重化し、開かれた通信ネットワーク上での通信情報の秘匿性を高めると同時にユーザ認証に対しても用いるものであった。ところが、近年開発されあるいは開発されつつあるＤＮＡコンピュータや量子コンピュータによる超並列処理技術は、これら高度な数学的暗号システムさえも無力化することとなった。つまり、ＤＮＡコンピュータ技術の確立により、公開鍵暗号による暗号化は最早安全とは言えなくなり、その結果、情報通信ではインターセプトされることを前提としなければならなくなったという問題がある。また、公開鍵暗号技術を認証に用いた場合、鍵の解読が可能となったことにより成済ましが容易になったと言う問題がある。こうした状況下において現在、「量子力学的もつれ（量子のエンタングルド状態）」に基づく、量子暗号と呼ばれる、理論的に第三者には解読不能な暗号システムの開発が進められている。しかしながら、公開鍵暗号の場合も、あるいは将来、量子暗号や量子テレポーションによる通信方法が開発された場合における暗号化と相互の認証においても、認証はいずれも端末機器もしくは端末上のシステムに依存して行われる。従って、端末機器を不特定多数の人々が利用可能な企業等公の場で利用する場合や、盗難・紛失の危険に晒され易い携帯端末で利用する場合については、誰でもその端末機器を操作可能であることから、単純にこの認証だけで通信相手がこちらの想定している本人であると認証することは困難である。即ち、暗号鍵システム単独では単なる端末認証にとどまってしまうという問題がある。

本人認証の問題に関しては、これまでにパスワードはもとよりＩＣカードや磁気カードなどによる本人認証システム、あるいは指紋や網膜パターンなどのバイオメトリクス情報を用いて本人認証を行うシステムが開発されている。なかでもバイオメトリクス情報は本人に固有の情報であるため、本人認証には最も適していると考えられ、すでにバイオメトリクス情報を数値化する技術が多数開発されている。

しかしながら、バイオメトリクス情報による本人認証は、認証する側にも同じバイオメトリクス情報を保存する方式であるため、認証する側が、登録されたバイオメトリクス情報を使用することは容易であり、認証する側に成済ます動機がある状況では安全とはいえないという問題、即ち認証装置上からの漏洩の問題がある。また、バイオメトリクス情報が電子化されていることにより、該データそのものが認証装置外部に流出する可能性、即ち認証装置上からの漏洩の問題がある。一方、ユーザが事故等により認証に用いるための当該身体部分を失った場合、バイオメトリクス情報の唯一性が逆に代替利用できる身体的特徴採用を制限してしまうことで、認証データを盗まれたユーザが社会的に抹殺されるなどの社会的問題を惹き起こしかねないという問題、即ち唯一性と代替物の問題がある。更に、犯罪に暴力的に採り入れられた場合、認証に用いる体部分の切除など従来の犯罪よりも陰惨になる可能性がある。

一方、バイオメトリクス情報を本人認証に用いる場合の根本的な問題として、本来唯一物であるはずのバイオメトリクス情報の利用も、その技術はＣＧや音声合成などの情報処理技術と共通の基盤上において進化、向上するものであることから、電子的に偽造可能であるという問題がある。このことはバイオメトリクス情報の解析技術イコール認証技術イコール偽造技術であることを示しており、即ち認証技術が確立すると同時に偽造技術も確立してしまうという、永遠に解決不能の問題であると考えられる。即ち、バイオメトリクス情報は単独で本人認証のための完結した手段として成立するのではなく、最善の状況にお

いても本人認証手段の一部分になりうるに過ぎないことを示している。
更に、バイオメトリクス情報による本人認証に関してそれぞれの技術を個別に見ると、指紋については指紋採取されればシリコンゴムなどによって簡単に複製されてしまうという問題、即ちユーザの管理外且つシステム外における認証情報漏洩の問題がある。また、指紋採取を公的に行いうる公安機関等から指紋データが流出若しくは国家権力そのものが利用することによっても成済ましは簡単にできてしまうという問題、即ちユーザの管理外且つシステム外における認証情報漏洩の問題がある。更に照合に用いる指を事故等で失ったり、指の腹に怪我をしただけでも認証ができなくなってしまうという問題、即ち唯一性と代替物の問題がある。声紋についても同様に、録音機等で簡単に複製されるという問題、即ちユーザの管理外且つシステム外における認証情報漏洩の問題、あるいは情報処理技術により認証情報そのものを生成できてしまうという問題、即ち電子的に偽造可能であるという問題がある。筆跡を本人認証に用いるについては、筆跡そのものが体調や精神状態によって大きな差異が生まれるため安定しづらいと言う問題があり、また、計測技術や数値制御技術などのロボット技術などを応用すれば安定的に再現することも可能であるという問題、即ち電子的に偽造可能であるという問題がある。顔貌を本人認証に用いる場合については、リアルワールドにおいて画像情報を作成することは容易という問題、即ちユーザの管理外且つシステム外の問題があり、またＣＧ等によって合成あるいは生成することも容易と言う問題、即ち電子的に偽造可能であると言う問題がある。
ＩＣカード等の携帯物で認証する認証方法は、手軽である一方、紛失や盗難の危険性が高いという問題、即ちユーザの管理内且つシステム外の問題がある。更に、紛失や盗難があっても、所有者がすぐには気がつきづらいという問題がある。即ち結果として、事故が拡大する可能性が高い。また、こうした携帯物による認証方法の特性から、事故若しくは犯罪の実行者について、当該携帯物の盗難によって第三者に成済まされたものか、カード所有者の狂言によるものか証明しづらいという、認証技術上の欠陥問題も生ずることになる。また、基本的な問題として、携帯物による認証方法では、該携帯物の記憶部に公開鍵方式における秘密鍵、あるいはＤＮＡ情報などによる秘密鍵、またあるいは共通鍵とユーザＩＤなどの鍵情報が書き込まれており、これを認証装置上の鍵情報と照合することにより認証する形態を採る事が多く、その場合公開鍵方式などの鍵方式における場合と同様に、秘密鍵を用いた成済まし問題や端末認証問題、インターセプト問題があり、また認証する側に成済ます動機がある状況では安全とはいえないという問題がある。
こうした問題を補うためにパスワードによって当該カードの所有者であることを認証する方法もあるが、その時にはパスワードによる認証方法における問題がそのままカード等による認証方法の問題として持ち込まれることになる。一方、ＩＣチップ等を体内に埋め込む方法では紛失の可能性はないものの、バイオメトリクスによる場合と同様、犯罪に暴力的に採り入れられた場合は従来の犯罪よりも陰惨になる可能性がある。
パスワードは従来、暗証番号のような４桁の数字や、多くても６桁から８桁の数字とアルファベットの組み合わせで利用されていた。これはかつてコンピュータの処理能力が低かった時代からの名残であると同時に、人にとって記憶が苦手であることによるものと考えられる。しかしながら、このことが総当り攻撃に対する脆弱性を生み出している。また、メモ書きからの漏洩、即ちユーザの管理内且つシステム外における漏洩や、入力時に盗み見られることによっても漏洩しやすいと言う問題がある。また、モニタリングによって入力情報が盗み見られることによって認証情報が漏洩すると言う問題がある。更に、パスワードは認証する側にも同じパスワードが保存されるため、認証する側に成りすます動機がある状況では安全とはいえないという問題がある。別に、パスワードにはサーバの発行する文字列によってユーザのパスワードを暗号化するワンタイムパスワードと呼ばれる認証方法もあるが、通信の暗号化に主眼が置かれた認証方法であり、本人認証そのものには従来のパスワードを使用しているため、本人認証の問題に関しては従来のパスワードと同じ問題を抱えている。
以上これまで述べたように従来の本人認証技術においては第一に、認証に用いる鍵を解析することの容易性の問題があった。超並列処理の可能なＤＮＡコンピュータの開発成功に

よって素因数分解問題や離散対数問題の解析を可能とし、その結果、公開鍵暗号による暗号化や認証は、秘密鍵を使った成済ましが可能となった。また、パスワードにおいても桁数の不足から可能な組み合わせ数が少なく、容易に総当り攻撃によって解読されてしまうため、成済ましの問題があった。
第二に、公開鍵暗号の解析が可能となったことは、インターセプトの脅威が復活したことを意味する。
第三に、公開鍵暗号等、端末あるいは携帯物に鍵情報を登録して用いる認証方法は、単に秘密鍵の搭載された端末機器を認証しているに過ぎず、ユーザ本人を認証しているわけではないという問題がある。
第四に、バイオメトリクス情報や携帯物による認証、あるいはパスワードによる認証において、認証する側に成済ましの動機がある状況においては容易に成済まされてしまうという問題、あるいは、認証装置上からの認証情報の漏洩の問題がある。これはユーザの発する認証情報と、認証装置上に登録されている認証情報との間に、照合可能な非可逆的関係があるか否かの問題に帰結する。
第五に、バイオメトリクス情報による認証において唯一性と代替物の問題がある。
第六に、バイオメトリクス情報や体内に埋め込んだ携帯物による認証においては、犯罪に暴力的に採り入れられた場合には陰惨な結果を惹き起こす可能性があるという問題がある。
第七に、バイオメトリクス情報において電子的偽造の可能性の問題がある。
第八に、バイオメトリクス情報による認証において、ユーザ管理外且つシステム外における認証情報漏洩の問題がある。
第九に、携帯物やパスワードによる認証において、ユーザの管理内且つシステム外における認証情報漏洩の問題がある。
第十に、パスワードによる認証において盗み見やモニタリングの問題がある。
従来の認証方法には大別して以上のような１０項目の問題点があるが、この内、第五、第六、第七、第八はバイオメトリクス情報による認証の方法に特有の問題である。特に第六の問題は、他の認証方法との併用によってのみ危険を軽減できる可能性がある。
そこで、本発明においては、第一に、鍵に解読不能性を与えるため、パスワードによる認証方法において総当り攻撃に対し十分に解読不能な組み合わせ数を持つ方法の提供を目的としている。
第二に、インターセプトによっても解析不能な認証方法の提供を目的としている。
第三に、端末機器ではなくユーザ本人を認証する方法の提供を目的としている。
第四に、ユーザの発する認証情報と認証装置上に登録されている認証情報との間に照合可能な非可逆的関係を構築する方法の提供を目的としている。
第五に、バイオメトリクス情報を認証に用いる場合及び携帯物による認証方法の場合は、該方法の持つ問題点を補いうる他の認証方法と併用することによって本人を認証する方法を提供することを目的としている。
第六に、認証情報がユーザの管理外且つシステム外において、漏洩、複製あるいは偽造されない、情報若しくは情報形式による認証方法の提供を目的としている。
第七に、複雑でありながらユーザにとって覚えやすく、しかし他人には説明しづらい、即ちユーザにとって管理しやすく、自ら漏洩することの困難なパスワードによる認証方法の提供を目的とする。
第八に、ユーザによる認証情報の入力若しくは認証情報を引き出すための情報の入力をモニタリングされることによって漏洩しても、成済ますことのできない認証方法の提供を目的としている。

発明の開示

本発明においては、課題として第一に、パスワードによる認証方法において総当り攻撃に対し十分に解読不能な組み合わせ数を持ちうるパスワード記述の方法を提供する。
第二に、入力情報を認証要求の都度ランダムに変え且つ認証装置に登録された情報と照合可能とすることにより、認証情報が通信中にインターセプトされて漏洩しても、漏洩した

情報だけでは認証情報を再現できない方法を提供する。
第三に、第一に記載の課題及び第二に記載の課題に述べる、パスワードによる認証方法を用いた、端末機器ではなくユーザ本人を認証する方法を提供する。
第四に、ユーザの発するユーザ固有の認証情報若しくは当該ユーザのみが知り得る認証情報と認証装置上に登録される該ユーザの認証情報との間に、照合可能、且つ非可逆的関係若しくは認証装置上の認証情報からユーザの発する認証情報を引き出すことが理論的にまたは実質的に困難な関係を成立させることにより、認証する側による成済ましや認証装置上からの認証情報盗難による成済ましを防ぐ方法を提供する。
第五に、ユーザに固有の認証情報若しくは当該ユーザのみが知り得る認証情報によって認証を行うことで、ユーザが認証情報を発するために該ユーザの使用する情報端末機器が盗難されても、それだけでは成済ますことの困難な方法を提供する。
第六に、当該ユーザだけが知りうる認証情報によって認証を行うことで、認証情報がユーザの管理外且つシステム外において、漏洩、複製あるいは偽造されない、情報若しくは情報形式を用いる方法を提供する。
第七に、記数法における大きな基底を持つ値を図形によって表したパスワード表記を用いることにより、複雑でありながらユーザにとって覚えやすく、しかし他人には説明しづらい、即ちユーザにとって管理しやすく、自ら漏洩することの困難なパスワードによる認証方法を提供する。
第八に、端末上に登録された認証情報若しくはワンタイムパスワードで保護された認証情報を用いることによって、ユーザによる認証情報の入力若しくは認証情報を引き出すための情報の入力をモニタリングされることによって漏洩しても、成済ますことのできない方法を提供する。
上記課題を解決するための好ましい方法として、以下のような３つの方法を採ることとした。
第１に、第一、第三、第四、第六および第八に記載の課題を解決する方法として、ユーザ毎にユニークな乱数または関数により非可逆的に変換したユーザの認証情報を、該ユニークな乱数または関数と共に認証装置上に登録し、認証要求に基づくユーザからの認証情報を該乱数または関数によって変換し、認証装置上に登録された情報と照合することにより、認証装置上から認証情報の漏洩や認証する側による成済まし、インターセプトによる漏洩に対応した。例えば、認証情報にパスセンテンスのような長いパスワードを用いる場合には、ユーザの申請したパスセンテンスからそのユーザ毎にユニークな乱数によって文字列（以下、パスコードｐ１という）を抽出し、該抽出された文字列をユーザＩＤと共に認証装置に記憶し、該ユーザから認証要求が出され、ユーザＩＤとともにパスセンテンスが送られてくると認証装置はユーザＩＤから登録されたパスコードｐ１を呼び出すとともに、対応するユニークな乱数を呼び出し、ユーザから送信されてきたパスセンテンスを認証装置に登録されているユニークな乱数を使ってパスコードｐ１に変換し、変換されたパスコードと認証装置に登録されているユーザＩＤに対応するパスコードｐ１を比較することによって本人の認証を行うようにした。尚、認証情報はパスセンテンス以外に、携帯物に搭載された情報、あるいはバイオメトリクス情報などその他の個人に付随する情報を利用あるいは併用することができる。
第２に、第一、第二、第三、第五、第六および第七に記載の課題を解決する方法として、パスワードの構造に関し、記数法における基底の値を大きくすることによって小さな桁数でも大きな組み合わせ数を確保し、そのことにより総当り攻撃によってパスワードが解読されることの困難な方法とした。また、パスワードに用いるキャラクタの表記方法として、相互に類似した若しくは全く同じ、図形などのキャラクタ（以下、Ｆキャラクタという）を用いることにより盗み見によってパスワードが解読されることのないパスワードによる方法とした。更に、認証方法として、認証装置が乱数を使ってパスワードの配列を変更してユーザに提示し、ユーザは正規の配列にするための順位（以下、パスコードｐ２という）を入力し、認証装置はユーザの入力したパスコードｐ２と認証装置が生成したパスコードｐ２を比較して認証するようにしたことにより、盗み見や通信のインターセプトによ

って破られることのない方法とした。
第３に、第１に記載の解決方法の内、バイオメトリクス情報をモニタに表示することなく認証情報として用いる方法を使用するか、あるいは第１に記載の解決方法の内、パスセンテンスを端末上に登録して用いる方法または公開鍵等その他の端末認証方法により、端末上に記憶した認証情報をそのままモニタに表示することなく認証に用いることにより、モニタリングされても成済まされることのない認証方法とし、且つ第２に記載の解決方法によってユーザの記憶に基づく認証情報を認証要求の都度ユーザが入力する方法を採るか、またはパスワードに第１に記載の解決方法を用いたワンタイムパスワード方法を利用することにより、認証情報入力者が登録されたユーザ本人であることを認証し、端末上に記憶したデータを用いる認証方法とユーザの記憶に基づく認証情報を認証要求の都度入力する認証方法の両者が同時に成立することを本人認証の条件としたことで、第一、第二、第三、第四、第五、第六、第七および第八に記載の課題を解決する本人認証方法とした。
従来の技術との関連において有する有利な効果として、第一に、パスワードに関して、記数法における大きな基底の値をＦキャラクタによって表し、且つ、予めユーザが登録した限定された数のＦキャラクタからパスコードｐ２を選択・作成できるようにしたことにより、少ない桁数で大きな組み合わせ数を確保しつつ直感的記憶のしやすさを獲得し、パスコードｐ２入力のためのパスワードキャラクタを表示することによりユーザの記憶を助け、第三者に対して口頭でもスケッチでも表現し伝達することの難しさから該ユーザ本人による漏洩の可能性を減少し、且つ入力する値をパスコードｐ２としたことにより、入力の容易性を実現した。
第二に、情報処理技術の進展による解析性能の向上に対し、第２に記載の解決方法では、ユーザによるパスワード登録時において認証する側が提供するＦキャラクタの数を大きくして記数法における基底の値を大きくすることで容易に複雑性を増大させる対応を可能とした。第１に記載の解決方法の内、パスセンテンス作成による方法では、情報処理装置の機能向上による解析性能の向上に対しパスセンテンスの長さをより長くすることにより、容易に複雑性を増大させる対応を可能とした。また、パスセンテンスを用いる方法は、端末認証の為の秘密鍵やＩＣカード等の携帯物に搭載する秘密鍵にも用いることができる。
第三に、第１の方法において、パスセンテンスを用いる場合は、パスセンテンスをユーザが記憶することによっても利用できることから、直接入力も可能であり、世界中どこからでもネットワークに接続された端末があれば第２および第３に記載の解決方法と併用することにより、本人認証が可能である。このことにより、端末が盗難された時などの緊急時において、ユーザの周囲にあるネットワークに接続された端末からパスセンテンスを入力することによりパスワードを変更するなどの緊急対応が可能である。
第四に、長いパスセンテンスや、Ｆキャラクタ等による大きな基底の値を直接使用せず、照合においては非可逆的に変換された文字列（以下、パスコードという）の形に変換して用いられるので、認証の照合処理速度が速い。
第五に、パスセンテンスは、例えば日記などから抜粋して作ることもできるのでユーザにとって作成が容易であり、且つ、第三者がそのパスセンテンスを推定することは困難である。
発明を実施するための最良の形態
本発明をより詳細に説述するために、添付の図面に従ってこれを説明する。
図１は、電子情報機器の使用に際し本人認証を行う為の、または情報通信ネットワーク上において本人認証を行う為の、この発明にかかる好ましい処理方式の全体を概念的に示すフローチャートであるが、システム全体を一覧的に表示するためにシステム構成の主要部分および各処理段階において使用するパスワードによる方法の原理を合成して示している。
図１（ｂ）は端末認証に用いられるパスワード方法を表しており、図１（ａ）のパスコードｐ１認証処理過程（１０）において該パスワードによる方法を実行する。図１（ａ）のパスコードｐ１認証処理過程（１０）において、最初に、ユーザが端末上に独自のパスセンテンス（２１２）を登録し、認証装置５は認証装置がユーザ毎に発行したユニークな乱

数（６２２３）を用いてパスコードｐ１生成モジュール（５９）において、ユーザから送信されたパスセンテンス（２１２）から抽出されたパスコードｐ１を認証装置データベース部６２にパスコードｐ１（６２２２）として登録する。次に、ユーザから認証の要求があった場合、認証装置はユーザ端末から送られてきたパスセンテンス（２１２）をパスコードｐ１生成モジュール（５９）において該ユニークな乱数（６２２３）によってパスコードｐ１に変換し、そのパスコードｐ１と既に認証装置上に登録されているパスコードｐ１（６２２２）を照合モジュール（５２）において照合することによりユーザ端末の認証を行う。パスセンテンスとパスコードｐ１の関係が非可逆的に決定されており、且つ認証装置上にはパスコードｐ１のみが登録されていることにより、認証装置上からパスコードｐ１が盗まれても盗んだ第三者はパスセンテンスそのものを復元することができず、従って成済ましができない認証方法となっている。更に、パスセンテンスの桁数を十分大きくすれば、総当り攻撃に対して実質的に解読を不能とすることができる。一方、ユーザ端末上に登録されたデータをモニタに表示することなく利用することにより、モニタリング行為によってパスセンテンスが盗まれることはない。また、パスセンテンスはパスワードのような短い文節あるいは数字と文字の組み合わせではなく文章なので物語性を持たせることや韻を踏むことができることから、ユーザ本人にとっては従来のパスワードよりも記憶しやすく、端末そのものが盗難された場合には他の端末から認証装置にアクセスして登録データを変更し、被害を未然に防ぐことが可能であり、公開鍵における秘密鍵や端末機器のコードを端末認証に利用するよりも融通性に富む。

図１（ｄ）は本人認証処理に用いられるパスワードによる方法を表しており、図１（ａ）のパスコードｐ２認証処理過程（１１）において該パスワードによる方法を実行する。最初に、ユーザは認証装置（５）が提供する記数法における大きな基底を持つＦキャラクタの中からパスワードとなるＦキャラクタを、認証装置によって設定された数だけ選択し、配列順を決めて認証装置（５）に送信し、認証装置（５）は該Ｆキャラクタと該配列順をデータベース部（６２）にパスワード＿Ｆキャラクタ（６２２４）およびＦキャラクタ配列（６２２５）として登録する。次に、ユーザから認証要求があると、認証装置（５）はユーザに対し配列組替の為の乱数を生成し、該乱数によりパスワード＿Ｆキャラクタ（６２２４）の配列順を組替えてユーザ端末に送信する。この時、同時に配列組替の為の乱数（６３６）を一時記憶部に登録する。ユーザは事前に登録した配列順をパスコードｐ２として入力モジュール（２３）から入力し認証装置（５）に送信する。認証装置（５）はユーザＩＤ（６２２１）からパスワードとなるＦキャラクタ（６２２４）及びその配列順であるＦキャラクタ配列（６２２５）を呼び出し、一時記憶部にある配列組替乱数（６３６）によってパスコードｐ２を生成し、ユーザから送られてきたパスコードｐ２と照合モジュール（５２）において比較照合することにより本人認証を行う。Ｆキャラクタは形や色が類似の、あるいは全く同じ図形などから構成されることにより、Ｆキャラクタを提供者する側＝認証する側にとって作成が容易であり、且つ、使用時において盗み見によってどのＦキャラクタを用いているのか判断することが困難であり、またユーザが他人にユーザ本人が選択しているＦキャラクタと他のＦキャラクタの違いを際立たせて説明することも難しく、しかしながらユーザ本人にとっては語数が少ないためわかり易いという特性を持つ。このＦキャラクタをユーザが認証時に使用する分だけ事前に登録することにより、ユーザ本人は少ない選択肢の中からパスワード配列を作成することができるのでユーザにとって取り扱いが容易である。更に、ユーザからの認証要求毎に認証装置が新しい乱数によって配列順を組替えた登録済みのＦキャラクタをユーザに送信し、ユーザはＦキャラクタの配列順をパスワード配列となるように組替順を作成し、この組替順をパスコードｐ２として認証に用いることにより、パスコードｐ２がインターセプトされることがあってもパスワードを再現することはできないという特性を持つ。

図１（ａ）は、この発明が、端末上に登録されたパスワードとして大きな桁数を持つパスセンテンスに基づく認証処理をパスコードｐ１認証処理過程（１０）が行い、ユーザ本人の記憶に基づくパスワードであって記数法における基底の値を大きくすることで少ない語数でも大きな組み合わせ数を持ちうるＦキャラクタを用いたパスワードによる認証処理を

パスコードｐ２認証処理過程（１１）が行い、両者が同時に成立することを認証の要件としたことにより、認証装置上からの認証鍵の盗難、モニタリング、盗み見、通信インターセプト、ユーザの管理外且つシステム外における漏洩、電子的偽造、および総当り攻撃等、従来技術の持っていた全ての問題に対処しうる本人認証の方法および装置であることを示している。端末機器が盗まれた場合には、認証要求時において認証装置からユーザに提示されるＦキャラクタの数は事前にユーザによって登録された数しかないので、当該端末機器を入手した第三者が該端末機器を用いて総当り攻撃することによりパスワードを解読することが可能である。しかしながら、端末機器が盗まれ若しくは紛失した段階でユーザが他の端末機器からパスセンテンスを直接入力してパスコードｐ１処理過程及びパスコードｐ２処理過程を行うことにより、パスワード等の登録データを変更して被害を防ぐことができる。

尚、（ｂ）及び（１０）は、他の端末認証の方法、例えば端末機器毎にユニークに割り振られた機器コードや、あるいは公開鍵方式における秘密鍵など、ユーザ端末を特定しうる、端末上に登録された他のユニークな情報、あるいは携帯物に登録された鍵情報などで代用することができる。また、（ｂ）および（ｄ）は、それぞれ単独での本人認証システムとしても機能しうる。

（ｃ）は、この発明にかかるＦキャラクタの構成と作成方法について、好ましい方法を表を用いて概念的に示している。Ｆキャラクタは基本形とそのカラーバリエーション及び形態バリエーションにより構成される。作成方法は最初にいくつかの基本バリエーションを作成し、その基本バリエーションに部分的なあるいは全体的な色彩の変化をつけることでカラーバリエーションを作成し、更に各バリエーションの形あるいは配置に小さな変化を加えることで大量のバリエーションを生み出すものである。あるいは同一図形に対し単に別の新しいキャラクタコードを設定するだけで新たなバリエーションとすることもできる。

例えばここで基本形のバリエーションｘを１００種類、基本形のカラーバリエーションｙを１６，７７７，２１６種類、各基本形のバリエーションｚを２０種類とすると、その組み合わせｘｙｚは３３，５５４，４３２，０００種類となり、これで6桁のパスワードを作成すると、その組み合わせは３３，５５４，４３２，０００$^{6}$ ≒１．４３×１０$^{6\,3}$ 通りあるので、総当り攻撃でこのパスワードを解読することは現在の技術においては実質的に不可能である。また将来の技術に対しても、組み合わせ数を増やすことは、例えばカラーバリエーションにおける色の組み合わせを１色増やすだけで１．７×１０$^{7}$ 倍になり、容易に複雑性を高めることができる。Ｆキャラクタの表記方法を用いた認証処理の方法について、パスワードの配列順を示すパスコードｐ２を用いることで、モニタリングまたは端末機器を盗難して総当り攻撃する以外の方法では決して解読することのできないパスワードによる認証方法となりうる。

また、この発明によれば、パスコードｐ２を作成するには、画面上に表示されているユーザ自身が事前に登録したパスワードのＦキャラクタの中から選択するわけであるから、ユーザの記憶を呼び覚ます為のヒントが常に表示されていることと同じ状況であり、従って、ユーザがパスワードを忘れて認証を受けられなくなる可能性は従来のパスワードによる認証方法よりも低いものとなる。

尚、シーケンス図（図９、図１０、図１１、図１２、図１３）に記載の暗号化のための公開鍵及び秘密鍵の部分は、パスコードｐ１またはパスコードｐ２またはパスコードｐ１を生成するためのパスワードまたはパスコードｐ２を作成するためのパスワードから生成される秘密鍵を用いても良い。

産業上の利用可能性

電子商取引において、電子マネーや電子財布、あるいはクレジットカードの真のホルダーであること証するための本人認証や、電子政府等における各種証明書発行のための本人認証あるいはその他の個人データの取り扱い時における本人認証に対して、十分な本人認証性能を提供し得る。

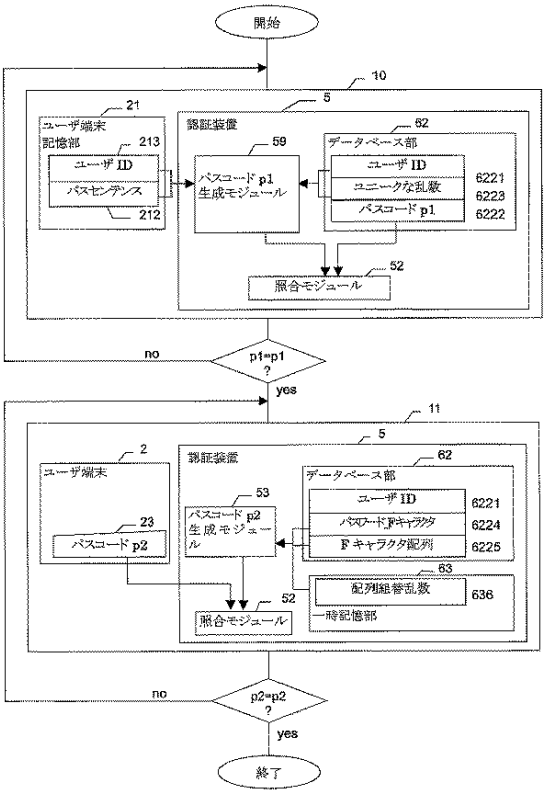
【図面の簡単な説明】

図１は、この発明にかかる好ましい本人認証方法の全体を概念的に示すフローチャートであるが、システム全体を一覧的に表示するためにシステム構成の主要部分を合成して示している。
図２は、この発明にかかる図１に示す本人認証処理の実施例であり、本人認証過程全体を示す、暗号化処理除くフローチャートである。
図３は、この発明にかかる実施例として図２に示す本人認証処理の内、パスコードｐ１認証処理過程のために端末上に保存する認証情報を認証装置に登録する処理方式を示す、暗号化処理を除くフローチャートである。
図４は、この発明にかかる実施例として図２に示す本人認証処理の内、パスコードｐ２認証処理過程のための認証情報を認証装置に登録する処理方式を示す、暗号化処理を除くフローチャートである。
図５は、この発明にかかる実施例として図２に示す本人認証処理のシステムの全体構成図である。
図６は、この発明にかかる実施例として図５に示す本人認証処理のシステム構成図の内、ユーザ及びユーザ端末のシステム構成図である。
図７は、この発明にかかる実施例として図５に示す本人認証処理のシステム構成図の内、サービス提供者端末のシステム構成図である。
図８は、この発明にかかる実施例として図５に示す本人認証処理のシステム構成図の内、認証装置のシステム構成図である。
図９は、この発明にかかる実施例として図３に示す、パスコードｐ１認証処理過程のための、端末上に保存する認証情報を認証装置に登録する処理方式のシーケンス図である。
図１０は、この発明にかかる実施例として図２、図３、図４、図５、図６、図７、図８、図９に示す本人認証方法の実社会における本人認証との関係に関するシーケンス図である。
図１１は、この発明にかかる実施例として図４に示す、パスコードｐ２認証処理過程のための認証情限を認証装置に登録する処理方式のシーケンス図である。
図１２は、この発明にかかる実施例として図２に示す本人認証方法の内、パスコードｐ１認証処理過程示すシーケンス図である。
図１３は、この発明にかかる実施例として図２に示す本人認証方法の内、パスコードｐ２認証処理過程示すシーケンス図である。
図１４は、図１（ｃ）及び（ｄ）に示すこの発明にかかる好ましいパスコードｐ２認証処理過程のフローチャートである。
図１５は、図１（ｂ）に示すこの発明にかかる好ましいパスコードｐ１認証処理過程のフローチャートである。
符号の説明
（ａ）…この発明にかかる好ましい本人認証方法の全体を概念的に示すフローチャートであるが、システム全体を一覧的に表示するためにシステム構成の主要部分を合成して示している。
（ｂ）…この発明にかかる好ましいパスコードｐ１の生成方法の原理を示す図。
（ｃ）…この発明にかかる記数法における大きな基底を持つ値を表示するための、好ましい表記方法の原理を示す図。
（ｄ）…（ｃ）に記載するパスワード用キャラクタからパスコードｐ２の生成方法の原理を示す図。
１０…パスコードｐ１認証処理過程のシステム構成図
１１…パスコードｐ２認証処理過程のシステム構成図
２…ユーザ端末
２１…ユーザ端末記憶部
２１２…ユーザ端末記憶部に登録されたパスセンテンス
２１３…ユーザ端末記憶部に登録されたユーザＩＤ
２３…ユーザ端末キーボード

5…認証装置
５２…認証装置の照合モジュール
５３…認証装置のパスコードｐ２生成モジュール
５９…認証装置のパスコードｐ１生成モジュール
６２…認証装置のデータベース部
６２２１…認証装置のデータベース部に登録されたユーザＩＤ
６２２２…認証装置のデータベース部に登録されたパスコードｐ１
６２２３…認証装置のデータベース部に登録されたユニークな乱数
６２２４…認証装置のデータベース部に登録されたパスワード＿Ｆキャラクタ
６２２５…認証装置のデータベース部に登録されたパスワード＿Ｆキャラクタの配列
６３…認証装置の一時記憶部
６３６…認証装置の一時記憶部に登録された、Ｆキャラクタの配列変換に用いた乱数

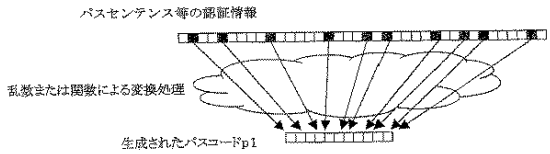
【図１（ａ）】

図１（a）



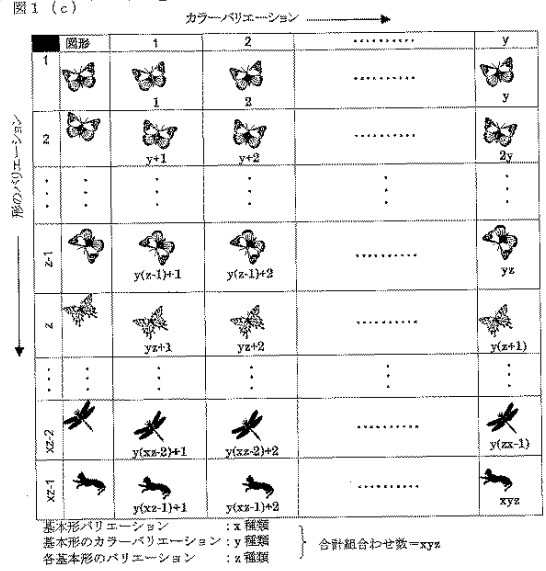

【図１（ｂ）】

図１（b）



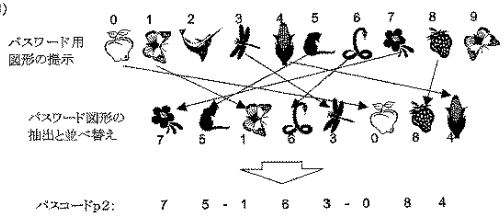

【図１（ｃ）】

図１（c）



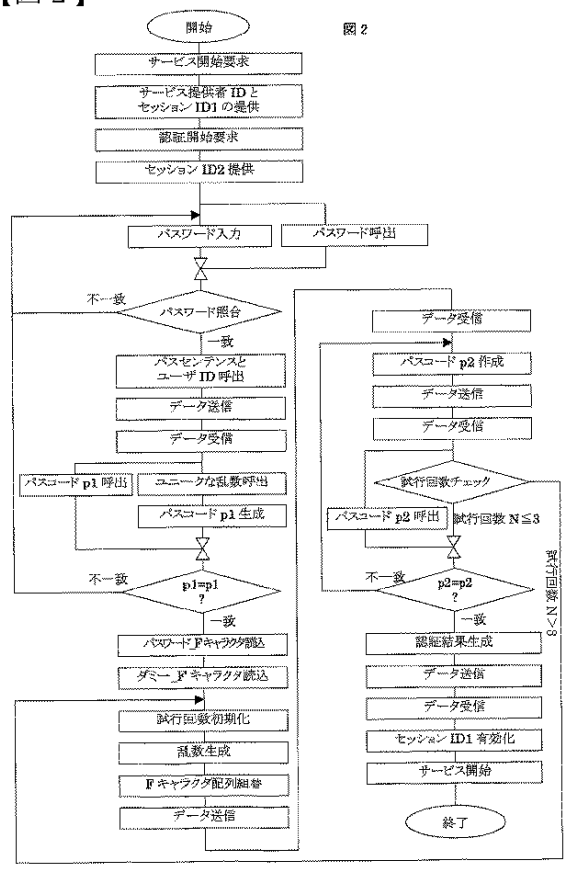
【図１（ｄ）】

図1（d）



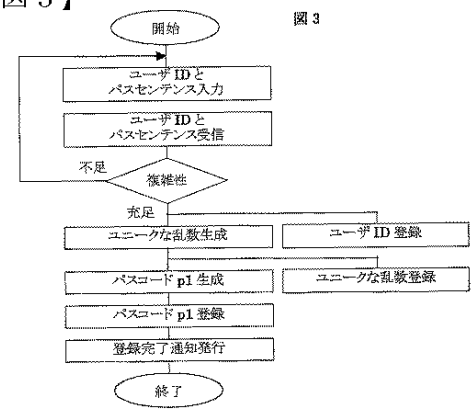

【図２】

図２



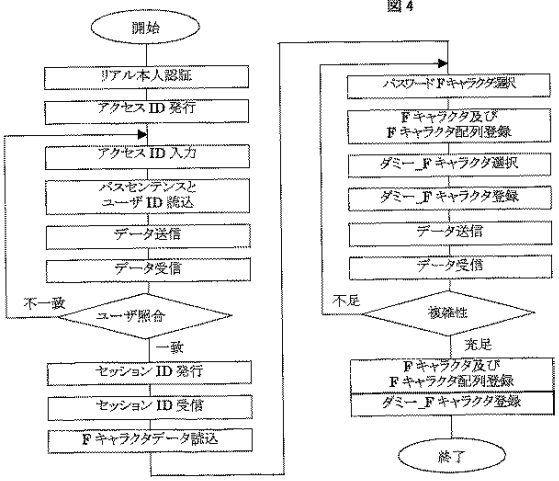

【図３】

図３



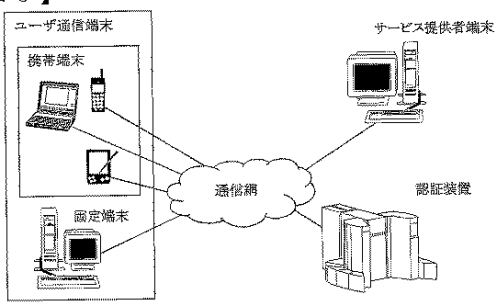

【図４】

図４



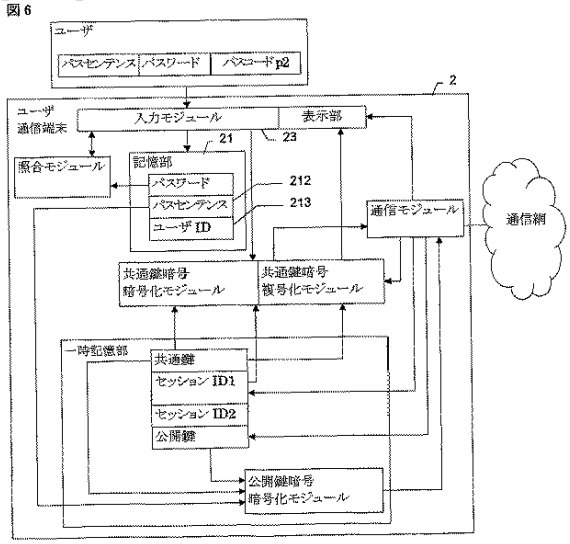

【図５】

図５



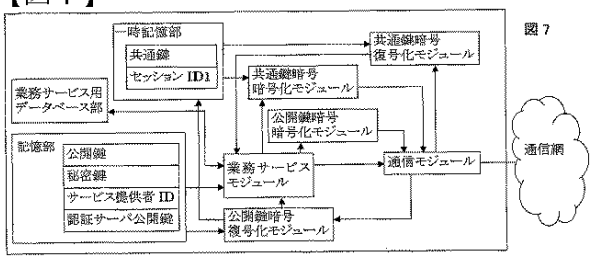
【図６】

図６



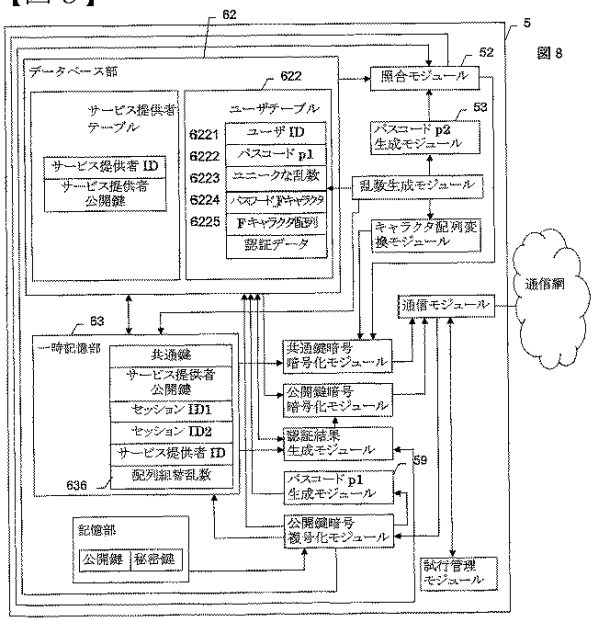

【図７】

図７



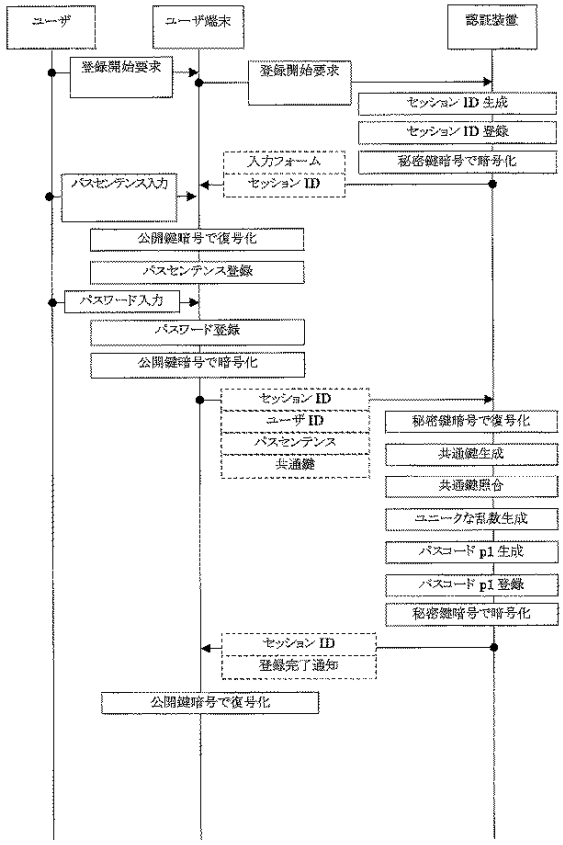

【図８】

図８



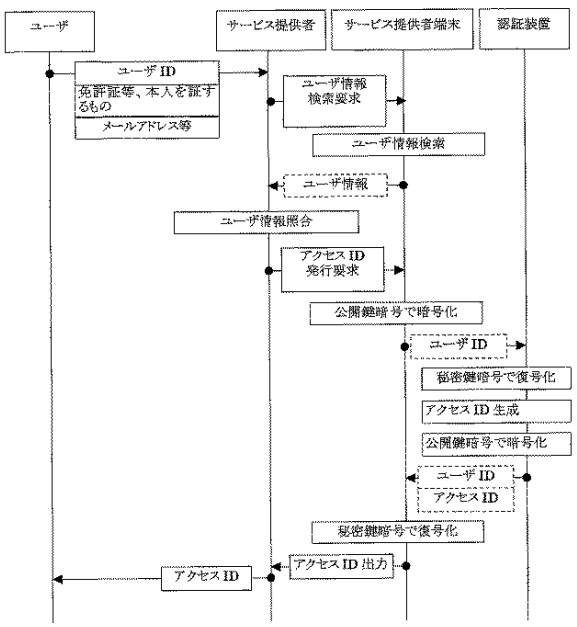

【図９】

図９

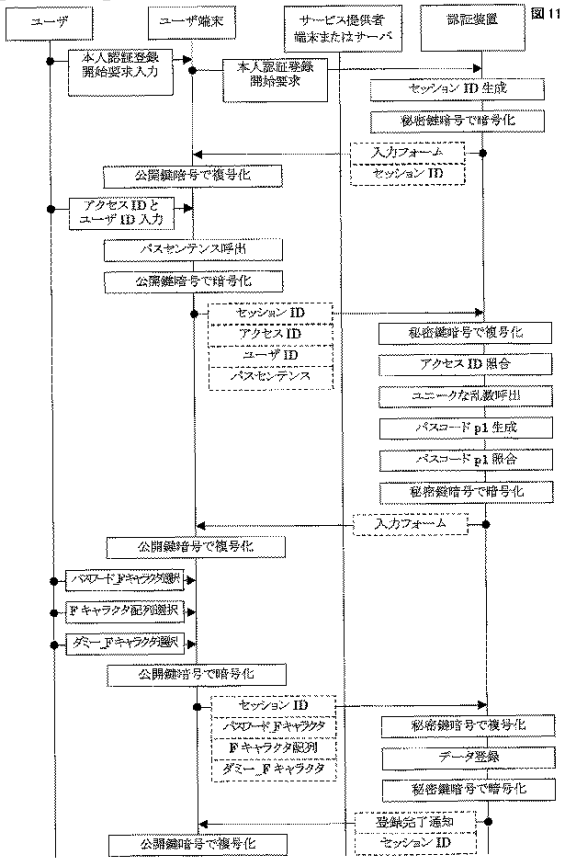



【図１０】

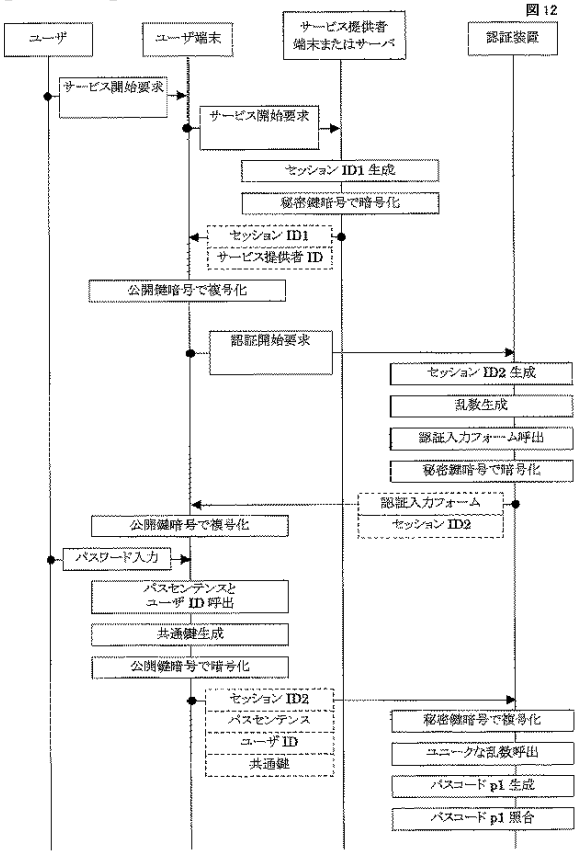
図10



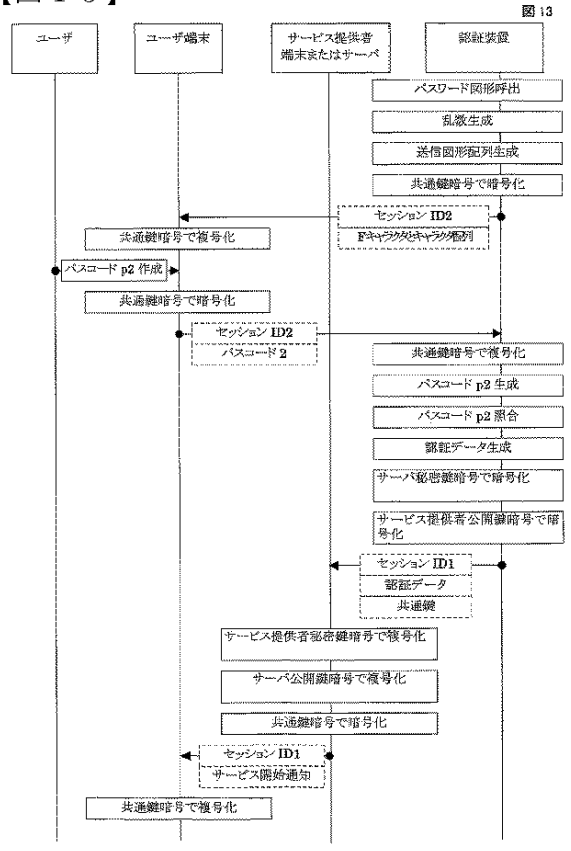
【図１１】



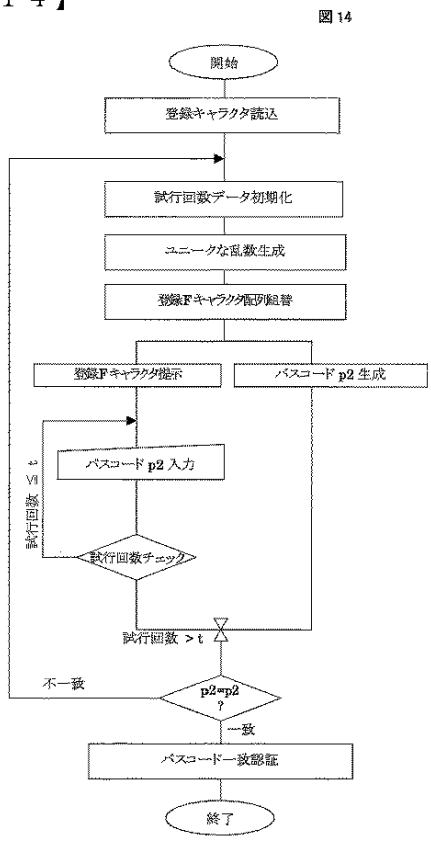

【図１２】




【図１３】

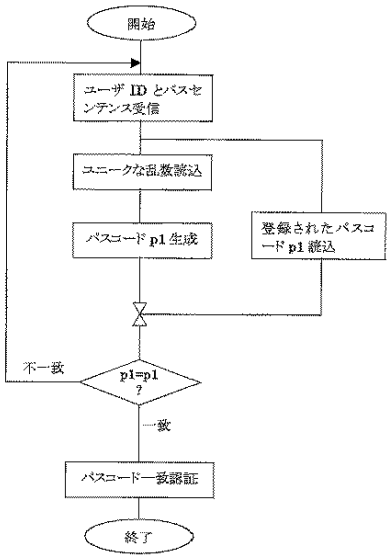



【図１４】



【図１５】

図 15




【手続補正書】
【提出日】平成14年6月28日(2002.6.28)
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】特許請求の範囲
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
パスコードｐ１認証処理過程（１０）において二重鍵暗号方式やバイオメトリクス方式、ワンタイムパスワード方式あるいは文章のように長文化されたパスワードであるところのパスセンテンス方式等を用い「『モニタリングはされないが認証する側による成済ましの可能性』及び『認証装置からの認証情報盗難による成済ましの可能性』があり且つそれぞれ認証内容に個別の問題点を持つ認証」を行うことにより「『通信のインターセプトによる認証情報の漏洩』、『モニタリングによる認証情報の漏洩』、『盗み見による認証情報の漏洩』、『総当り攻撃による認証情報の漏洩』、および『ユーザの管理外且つシステム外における認証情報の漏洩』、『認証情報の複製または偽造』による成済まし」を防止し、同時に「ユーザの発する認証情報と認証装置に登録する認証情報の間に乱数等を用いて照合可能な非可逆的関係を設けて、『認証する側による成済まし』や『認証装置上からの認証情報盗難による成済まし』を防止する」ようにしたことにより、本人認証に使用するユーザＩＤ等の記録された通信端末機器若しくは通信端末機器に装着して使用する電子的ＩＤカード等ユーザＩＤの記録された装置等、通信ネットワークに接続されたユーザＩＤ搭載装置を認証し、
而して、パスコードｐ２認証処理過程（１１）において大きな組合わせ数を持つパスワード等当該認証鍵情報所有者本人の意思によらずしては成済ましが不可能であるところの本

人を特定しうる事実を用いて「認証する側による成済まし」、「認証装置からの認証情報盗難による成済まし」および「『通信のインターセプトによる認証情報の漏洩』、『盗み見による認証情報の漏洩』、『総当り攻撃による認証情報の漏洩』、『認証情報の複製および偽造』および『ユーザＩＤ搭載装置盗難』による成済まし」に対し安全を確保した認証を行うことによりユーザ本人を認証し、
「ユーザ本人の認証」と「通信に接続されたユーザＩＤ搭載装置の認証」を２段階で行うことにより本人認証に関し「認証する側による成済まし」、「認証装置からの認証情報盗難による成済まし」、「『モニタリングによる認証情報の漏洩』、『通信のインターセプトによる認証情報漏洩』、『盗み見による認証情報漏洩』、『総当り攻撃による認証情報漏洩』、『ユーザの管理外且つシステム外における認証情報の漏洩』、『認証情報の複製或いは偽造』および『ユーザＩＤ搭載装置盗難』による成済まし」に対し、少なくとも個別に対処できるようにしたことを特徴とする本人認証の方法。
【請求項２】
「大きな組合わせ数を持つパスワード」に関し、記数法における大きな基底を持つ値を文字或は無限に作成しうる図形（ｃ）などのキャラクタを用いて表記すると共に、各キャラクタ毎にそれぞれ一つまたは複数のユニークなキャラクタコードを割り付け、該値をパスワード表記に用いることによって少ない要素数のパスワード配列でも容易且つほぼ無制限に大きな組合わせ数を持たせることができると同時に、総当り攻撃に対して論理的に限界のない強度を持ち、またパスワード入力を盗み見られることによっても容易に漏洩せず、且つ当該パスワード所有者自身からも漏洩することが困難なパスワード方式としたことを特徴とする請求の範囲第１項に記載の本人認証の方法。
【請求項３】
「大きな組合わせ数を持つパスワード」に関し、ユーザからの認証要求があると、認証装置は乱数を生成し、認証装置に登録されているパスワードを該乱数により並べ替えてユーザに提示（ｄ　「パスワード用図形の提示」）し、且つ認証装置は認証装置に登録されたユーザのパスワードから該乱数を用いて並べ替えるための配列順を生成（ｄ　「パスワード図形の抽出と並べ替え」）し、
ユーザは提示されたパスワードのためのキャラクタを、ユーザが登録したパスワードの配列に並べ替えるための配列順（ｄ　「パスコードｐ２」）を認証装置に通知し、
認証装置はユーザから送られてきた配列順とユーザからの認証要求時に認証装置が生成した配列順とを照合することによって、入力の盗み見や通信のインターセプトによるパスワード不正使用をほぼ無力化したことを特徴とする請求の範囲第１項および請求の範囲第２項に記載の本人認証の方法。
【請求項４】
「ユーザの発する認証情報と認証装置に登録する認証情報の間に照合可能な非可逆的関係を設けて、認証する側による成済ましや認証装置上からの認証情報盗難による成済ましを防止する」ことについて、
ユーザ毎にユニークなパスセンテンス等の文字列情報、あるいはバイオメトリクス情報またはその他の鍵暗号情報や端末機器番号などの認証情報を、認証装置がユーザ毎にユニークな乱数または一方向関数を用いて非可逆的に変換することによりパスコードｐ１（ｂ）として生成し、生成したパスコードｐ１をユーザＩＤおよび該ユニークな乱数または一方向関数と共に認証装置上に登録し、
ユーザが、ユーザ端末からユーザＩＤと共に該文字列情報または鍵情報などの認証情報を送信するか、または認証用端末からバイオメトリクス情報またはＩＣカードなどの携帯物に登録された鍵情報などの認証情報を入力し送信することによって認証装置に認証要求を出し、認証装置はユーザＩＤによって認証装置に登録されている該ユニークな乱数または一方向関数を呼出し、
該ユニークな乱数または一方向関数を使ってユーザ端末または認証用端末から送られてきた該文字列情報、バイオメトリクス情報またはその他の鍵暗号情報や端末機器番号などの認証情報からパスコードｐ１を生成し、生成されたパスコードｐ１と認証装置上に登録さ

れているパスコードｐ１を照合することにより本人認証に使用するユーザＩＤ等の記録された通信端末機器若しくは通信端末機器に装着して使用する電子的ＩＤカード等ユーザＩＤの記録された装置等、通信ネットワークに接続されたユーザＩＤ搭載装置を認証するようにしたことを特徴とする請求の範囲第１項記載の本人認証の方法。

【国際調査報告】

## INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP02/01256

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] G06F15/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] G06F15/00, H04L9/00, G09C1/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1926-1996 Jitsuyo Shinan Toroku Koho 1996-2002
Kokai Jitsuyo Shinan Koho 1971-2002 Toroku Jitsuyo Shinan Koho 1994-2002

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| Y<br>A | WO 97/20265 A1 (Casio Computer Co., Ltd.),<br>05 June, 1997 (05.06.97),<br>Full text; all drawings<br>& JP 09-152991 A & EP 807284 A<br>& US 5928364 A1 | 1,2<br>3 |
| Y<br>A | Naoki TABUCHI, "Juyosei Masu Joho Security no Kakuritsu", Nikkei Computer, 09 August, 1993 (09.08.93), No.316, pages 111 to 121<br>Page 117 "Password no Roken·Suisoku Boshi Taisaku" | 1,2<br>4 |
| A | JP 2001-282738 A (Microsoft Corp.),<br>12 October, 2001 (12.10.01),<br>Full text; all drawings<br>(Family: none) | 1-3 |

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

| Date of the actual completion of the international search | Date of mailing of the international search report |
|---|---|
| 23 April, 2002 (23.04.02) | 14 May, 2002 (14.05.02) |
| Name and mailing address of the ISA/<br>Japanese Patent Office<br><br>Facsimile No. | Authorized officer<br><br>Telephone No. |

Form PCT/ISA/210 (second sheet) (July 1998)

| 国際調査報告 | 国際出願番号 PCT／JP02／01256 |
|---|---|

A. 発明の属する分野の分類（国際特許分類（IPC））

Int. Cl⁷ G06F15／00

B. 調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））

Int. Cl⁷ G06F15／00, H04L9／00, G09C1／00

最小限資料以外の資料で調査を行った分野に含まれるもの

| | |
|---|---|
| 日本国実用新案公報 | 1926－1996年 |
| 日本国公開実用新案公報 | 1971－2002年 |
| 日本国実用新案登録公報 | 1996－2002年 |
| 日本国登録実用新案公報 | 1994－2002年 |

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C. 関連すると認められる文献

| 引用文献のカテゴリー＊ | 引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示 | 関連する請求の範囲の番号 |
|---|---|---|
| Y<br>A | WO 97／20265 A1 (CASIO COMPUTER CO.,LTD.) 1997.06.05, 全文, 全図<br>& JP 09－152991 A & EP 807284 A & US 5928364 A1 | 1, 2<br>3 |
| Y<br>A | 田渕治樹, 重要性増す情報セキュリティの確立, 日経コンピュータ, 1993.08.09, 第316号, p. 111－p. 121<br>p. 117「パスワードの露見・推測防止対策」参照 | 1, 2<br>4 |

☒ C欄の続きにも文献が列挙されている。　☐ パテントファミリーに関する別紙を参照。

＊ 引用文献のカテゴリー
「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

| 国際調査を完了した日 | 国際調査報告の発送日 |
|---|---|
| 23.04.02 | 14.05.02 |

| 国際調査機関の名称及びあて先 | 特許庁審査官（権限のある職員） | | |
|---|---|---|---|
| 日本国特許庁（ISA／JP）<br>郵便番号100－8915<br>東京都千代田区霞が関三丁目4番3号 | 宮司 卓佳 | 5B | 9555 |
| | 電話番号 03－3581－1101 内線 3545 | | |

様式PCT／ISA／210（第2ページ）（1998年7月）

| 国際調査報告 | 国際出願番号 PCT／JP02／01256 |
|---|---|

C（続き）. 関連すると認められる文献

| 引用文献のカテゴリー＊ | 引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示 | 関連する請求の範囲の番号 |
|---|---|---|
| A | JP 2001－282738 A（マイクロソフト コーポレイション）2001．10．12，全文，全図（ファミリーなし） | 1－3 |

| | | | |
|---|---|---|---|
| 专利名称(译) | 重组抗骨桥蛋白抗体及其用途 | | |
| 公开(公告)号 | JPWO2003027151A1 | 公开(公告)日 | 2005-01-06 |
| 申请号 | JP2003530737 | 申请日 | 2002-09-25 |
| [标]申请(专利权)人(译) | 株式会社 免疫生物研究所 | | |
| 申请(专利权)人(译) | 株式会社 免疫生物研究所<br>藤泽制药有限公司 | | |
| [标]发明人 | 上出利光<br>今重之<br>山本宣哉<br>樋口浩文<br>鳥飼正治<br>時枝養之<br>中島敏博<br>前田浩明 | | |
| 发明人 | 上出 利光<br>今 重之<br>山本 宣哉<br>樋口 浩文<br>鳥飼 正治<br>時枝 養之<br>中島 敏博<br>前田 浩明 | | |
| IPC分类号 | C07K16/18 C12N15/09 A61K39/00 A61K39/395 A61P19/02 A61P29/00 A61P37/00 A61P37/02 A61P37/06 C07K14/52 C07K16/24 C07K16/28 C07K16/46 C12N1/15 C12N1/19 C12N1/21 C12N5/10 C12N15/13 C12N15/63 C12P21/08 G01N33/15 G01N33/50 G01N33/53 G01N33/566 G01N33/577 | | |
| CPC分类号 | A61K39/00 A61K2039/505 A61P19/02 A61P29/00 C07K14/52 C07K16/24 C07K16/2842 C07K16/2848 C07K2317/34 | | |
| FI分类号 | C12N15/00.ZNA.A A61K39/395.U A61P29/00.101 A61P37/06 C07K16/18 C07K16/46 C12N1/15 C12N1/19 C12N1/21 C12P21/08 G01N33/15.Z G01N33/50.Z G01N33/53.D G01N33/53.M G01N33/566 G01N33/577.B C12N5/00.A | | |
| 代理人(译) | 大野信夫<br>高桥 德明 | | |
| 优先权 | 2001290700 2001-09-25 JP | | |
| 外部链接 | Espacenet | | |


摘要(译)

一种抗体，其中至少重链和轻链的恒定区被转化为人源的抗体，其抑制识别RGD序列的整联蛋白与骨桥蛋白或其片段与SVVYGLR序列或其相应序列之间的结合本发明公开了抑制整联蛋白与骨桥蛋白或其片段结合的方法。该抗体可用作自身免疫疾病的治疗剂，风湿病或类风湿性关节炎的治疗剂，并提供治疗自身免疫疾病，风湿病或类风湿性关节炎的方法。该骨桥蛋白抗体也可用于风湿病诊断剂和诊断方法。

1 （c）

カラーバリエーション ⟶

| | 図形 | 1 | 2 | ・・・・・・・・・・ | y |
|---|---|---|---|---|---|
| 1 |  |  1 |  2 | ・・・・・・・・・・ |  y |
| 2 |  |  y+1 |  y+2 | ・・・・・・・・・・ |  2y |
| ・・・ | ・・・ | ・・・ | ・・・ | ・・・ | ・・・ |
| z-1 |  |  y(z-1)+1 |  y(z-1)+2 | ・・・・・・・・・・ |  yz |
| z |  |  yz+1 |  yz+2 | ・・・・・・・・・・ |  y(z+1) |
| ・・・ | ・・・ | ・・・ | ・・・ | ・・・ | ・・・ |
| xz-2 |  |  y(xz-2)+1 |  y(xz-2)+2 | ・・・・・・・・・・ |  y(xz-1) |
| xz-1 |  |  y(xz-1)+1 |  y(xz-1)+2 | ・・・・・・・・・・ |  xyz |

基本形バリエーション　　：x 種類
基本形のカラーバリエーション：y 種類
各基本形のバリエーション　　：z 種類

} 合計組合わせ数＝xyz