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

特許第3970388号

(P3970388)

(45)発行日　平成19年9月5日(2007.9.5)　(24)登録日　平成19年6月15日(2007.6.15)

(51)Int.Cl.			F I		
H04Q	7/38	(2006.01)	H04B	7/26	109S
H04Q	7/06	(2006.01)	H04B	7/26	103A
H04Q	7/08	(2006.01)	H04L	9/00	673A
H04Q	7/12	(2006.01)			
H04L	9/32	(2006.01)			

請求項の数 12　(全 11 頁)

(21)出願番号　特願平9-177870
(22)出願日　平成9年7月3日(1997.7.3)
(65)公開番号　特開平10-66158
(43)公開日　平成10年3月6日(1998.3.6)
審査請求日　平成16年6月21日(2004.6.21)
(31)優先権主張番号　08/675029
(32)優先日　平成8年7月3日(1996.7.3)
(33)優先権主張国　米国(US)

(73)特許権者　390035493
エイ・ティ・アンド・ティ・コーポレーション
ＡＴ&Ｔ　ＣＯＲＰ.
アメリカ合衆国　１００１３－２４１２
ニューヨーク　ニューヨーク　アヴェニュー　オブ　ジ　アメリカズ　３２
(74)代理人　100064447
弁理士　岡部　正夫
(74)代理人　100085176
弁理士　加藤　伸晃
(74)代理人　100104352
弁理士　朝日　伸光
(74)代理人　100106183
弁理士　吉澤　弘司

最終頁に続く

(54)【発明の名称】アクセス制御システムに対するセキュリティ

(57)【特許請求の範囲】

【請求項１】

秘密保持システムへのアクセスをリクエストするユーザにそのアクセスの許可を保証する方法であって、前記ユーザは、ユーザが秘密保持システムへのアクセス資格を有するときには、実質的にユーザ独自のユーザ識別情報を有し、かつ実質的にユーザ独自の起動番号を有した無線通信装置を所持しており、該方法は、

ユーザ識別情報を該秘密保持システムに入力する段階からなり、該入力する段階が該ユーザにより行われ、該方法はさらに、

該ユーザ識別情報によって識別されたユーザが所持していなくてはならない無線通信装置の起動番号を識別する段階からなり、該識別する段階が該秘密保持システムによって行われ、該方法はさらに、

該ユーザ識別情報によって識別されたユーザが所持していなくてはならない無線通信装置の再認証情報を伝送する段階からなり、該伝送する段階が少なくとも該秘密保持システムによって行なわれ、該方法はさらに、

該再認証情報を該秘密保持システムに返送する段階からなり、該返送する段階が、該ユーザが所持していなくてはならない無線通信装置を該ユーザが所持しているときには、該ユーザによって行われ、そして、

該返送する段階において返送された再認証情報が該伝送段階において伝送された再認証情報と整合するかどうかを検出し、そして、整合するときには、該ユーザに該秘密保持システムへのアクセスを許容する段階とからなり、前記検出する段階が該秘密保持システム

によって行われることを特徴とする方法。
【請求項２】
請求項１に記載の方法において、該無線通信装置は該起動番号としてページャ番号を有するページャであり、そして、該識別する段階は、
該ユーザ識別情報によって識別されたユーザが所持していなくてはならないページャのページャ番号を識別する段階からなることを特徴とする請求項１に記載の方法。
【請求項３】
請求項２に記載の方法において、該伝送段階は、
該ページャ番号を有するページャに呼を行う段階と、
該再認証情報を該ページャに伝送する段階とからなることを特徴とする方法。
【請求項４】
請求項１に記載の方法において、該無線通信装置は該起動番号として電話番号を有する携帯電話であり、該識別する段階は、
該ユーザ識別情報によって識別されたユーザが所持していなくてはならない携帯電話の電話番号を識別する段階からなることを特徴とする方法。
【請求項５】
請求項４に記載の方法において、該伝送する段階は、
該電話番号を有する携帯電話に呼を行う段階と、
該再認証情報を該携帯電話に伝送する段階とからなることを特徴とする方法。
【請求項６】
請求項１に記載の方法において、該伝送する段階は、
ほぼ該伝送する段階が実行される度ごとに実質的に異なる再認証情報を発する段階からなることを特徴とする方法。
【請求項７】
請求項６に記載の方法において、該再認証情報は実質的に不規則な番号であることを特徴とする方法。
【請求項８】
請求項６に記載の方法において、該再認証情報は従来の電話番号の一般的な形式を有することを特徴とする方法。
【請求項９】
請求項１に記載の方法において、該入力する段階が、該再認証情報を該無線通信装置に伝送するのに使用する第二通信チャネルとは異なる、該ユーザと該秘密保持システムと間の第一通信チャネルを介して行われ、そして、該返送する段階は、該第一通信チャネルと該第二通信チャネルのうちの１つを使用して行われることを特徴とする方法。
【請求項１０】
請求項９に記載の方法において、該返送する段階が該第一通信チャネルを使用して実行されることを特徴とする方法。
【請求項１１】
請求項９に記載の方法において、該返送する段階が該第二通信チャネルを使用して実行されることを特徴とする方法。
【請求項１２】
請求項１に記載の方法であって、さらに、
該返送された再認証情報が該伝送された再認証情報と整合しないときには、該秘密保持システムへの該ユーザ接続を切断する段階からなることを特徴とする方法。
【発明の詳細な説明】
【０００１】
【発明の背景】
本発明は、必要であれば遠隔地からのアクセスが可能なシステムとすることが出来るアクセス制御システムに対するセキュリティに関するものである。本発明の利用可能システムは、例えば、コンピュータシステム、トランザクション処理システム、ボイスメール、音

声応答システム、他、同様のシステムである。本発明のセキュリティ面においては、秘密保持システムにアクセスしようとする人物がこれにアクセス出来るように認証されることを保証するものである。

【０００２】

アクセス制御システムには多くのタイプがある。そのようなシステムのほとんどはセキュリティのいずれかのフォームを用いて認証されていない人物がシステムにアクセスしてこれを利用するリスクを減じている。例えば、システムはそのシステムを使用しようとする人物に対し、最初にユーザ識別番号（ユーザＩＤ）、身分証明番号、もしくはパスワードを入力するよう要求する。このような上記の無形のセキュリティ情報だけでは、例えば認証されたユーザが入力する場面を見ていた悪用者により悪用される場合がある。他の場合では、このような無形のセキュリティ情報によって提供されうる上述のタイプのセキュリティよりもさらに高度なセキュリティを保証する場合がある。例えば、コンピュータシステム、ボイスメール、音声応答システムの管理ユーザやスーパーユーザは高度なセキュリティレベルを要求する。同様に、警備保障ビル、刑務所、空港、軍用施設の他、セキュリティ要求の高い場所への高レベルアクセスや管理アクセスの場合には、より高度なセキュリティレベルが要求されている。

【０００３】

よって本発明は、アクセス制御システムに対するセキュリティを改良することを目的とする。

【０００４】

また、本発明は特に、ユーザがシステムにアクセスを行う際に、単なる識別情報以上のものが必要とされるアクセス制御システムに対するセキュリティを提供する。

【０００５】

【発明の概要】

本発明のこれら目的及び他の目的は、本発明によるアクセス制御システムに対するセキュリティを提供することによって達成される。本発明のアクセス制御システムは、システムにアクセスを試みようとする人物（すなわちユーザ）に、ページャ(pager)のような特別の無線遠隔通信装置の所持を要求し、かつシステム側がユーザに対して要求した情報をその無線遠隔通信装置経由にて入力することを要求する。例えば、ユーザはパーソナルコンピュータから秘密保持システムにモデム接続を行う。そこでユーザはモデム接続経由で秘密保持システムに対しユーザ識別情報を入力する。秘密保持システムがユーザ識別情報が有効であることを認識した場合、システムは他の別の通信チャネル経由でユーザに再認証情報が送れるようにする。特に望ましい実施形態においては、再認証情報はその情報を受取る目的でユーザが所持していなくてはならない特別なページャに対し送られる。次に、システムはシステムに再認証情報を返送する（例えば、モデム接続経由で）タイミングをユーザに与える。システムは、ユーザが再認証情報を返送することが出来た場合にのみ、ユーザのアクセス要求を許可にする。ユーザが再認証情報を受取るために必要な特別な無線遠隔通信装置を所持している場合に、ユーザはその情報の受取りおよび返送が可能となり、かつ、それによる秘密保持システムへのアクセスが可能となる。ユーザが必要とされる無線遠隔通信装置を所持していない場合、そのユーザは再認証情報の受取りおよび返送が出来ないことから、秘密保持システムへのアクセスが不可能である。

【０００６】

本発明の別の側面においては、無線遠隔通信装置はユーザ以外の他の人物が所持する。この他の人物（ユーザ認証者）は、ユーザアクセスリクエストがなされた場合、秘密保持システムからの再認証情報を受取り、その情報をシステムに再伝送する。この場合、ユーザ認証者による決定を容易にするため、システムはユーザ認証者に対しユーザに関する追加情報を送ることも可能である（例えば、ユーザの識別情報、及び、ユーザがどこからアクセスを試みようとしているのかその所在場所に関する情報である。）。

【０００７】

【発明の詳細な記述】

図１に関し、ユーザ１０は通信リンク２０経由で秘密保持システム３０に対するアクセスを要求する。例えば、秘密保持システム３０はコンピュータシステムまたはコンピュータネットワークであり、ユーザはシステム３０へのアクセスを行うパーソナルコンピュータ（１０に含まれている）を所持している。また例えば、通信リンク２０は、ユーザがシステム３０の利用を望む場合、商用電話網を通してユーザが起動するモデム接続である。これらはあくまでも一例であり、他のタイプのユーザ装置１０、秘密保持システム３０、および通信リンク２０が可能である。

【０００８】

ユーザが最初に通信リンク２０を起動させる時に、一般的にシステム３０は、例えば、ユーザＩＤ、身分証明番号、もしくはパスワードなどのユーザを証明する情報を入力するようユーザに対し要求する。ここでは説明を行う上で、このような情報をまとめてユーザ識別情報と呼ぶことにする。システム３０はユーザ識別情報が有効かどうかのチェックを行う。そして、そのユーザ識別情報が有効であれば、以下に説明するように、システム３０はそのユーザが実際にシステムにアクセスする資格を有しているかどうかの確認プロセスを継続する。一方、システム３０が、ユーザが提供したユーザ識別情報が有効ではないと判断した場合（例えば、システム３０に保存されているユーザリストにそれと一致する情報がなかった場合）、システム３０は接続２０を終了させるか、またはユーザにもう一度情報を提供するよう指示を行う。そして所定回数の入力後、ユーザがユーザ識別情報を提供出来なかった場合、システム３０は接続２０を終了させる。

【０００９】

システム３０が、ユーザ１０が入力したユーザ識別情報が有効であると判断した場合（およびユーザもしくはユーザが要求したアクセスタイプによりさらにまだユーザ認証が必要であると判断した場合）、システム３０は、特定のユーザが所持していなくてはならない特別な無線遠隔通信装置７０を識別する。例えば、ユーザは特別のページャ番号を有したページャ、または特別の電話番号を有した携帯電話を所持することを求められる。ここでは説明上、ユーザ１０が所持する必要のあるこのような無線遠隔通信装置７０が「無線遠隔通信装置番号」または「起動番号」を有するという。装置７０は、実質的にこれによって起動される。このように、システム３０は、システム３０にアクセスするためにユーザ１０が所持していなくてはならない装置７０の無線遠隔通信装置番号を識別する。望ましくは、各ユーザ１０は、独自の、または実質的に独自の無線遠隔通信装置番号を有した装置７０と連動する。

【００１０】

システム３０がユーザ１０が所持していなくてはならない装置７０の番号を識別すると、システム３０は、装置７０と通信が可能な無線通信システム５０に（通信リンク４０経由で）メッセージを送る。システム３０からのこのメッセージによって、システム５０は装置７０に（無線通信リンク６０経由で）コールをし、「システム３０にアクセスを行うためユーザ１０はシステム３０に対し返送しなくてはならない。」というメッセージを装置７０に送る。例えば、システム３０は不規則な、またはほぼ不規則な番号（例えば、実際の規則的でない電話番号）をシステム５０に対し発し、通信リンク６０経由で装置７０に送信する。装置７０は、リンク８０で示すように、このメッセージを受取り、ユーザ１０に対しこれを示す。または、リンク８０は音声リンクであるかもしれない。ユーザ１０がこのメッセージを受取ると、ユーザは、例えば通信リンク２０経由にてそれをシステム３０に返送する。または、ユーザ１０はこのメッセージを他の方法で（例えば、７０、６０、５０、および４０部分が双方向通信可能であればこれら経由にて）システム３０に返送する。システム３０がユーザ１０からの再認証メッセージを受取ると、システム３０はユーザにアクセスするシステムを開く。

【００１１】

希望により、通信リンク２０、４０、および６０のいずれか、もしくは全部は、メッセージ暗号(message encryption)、またはパスワード交換のような従来のセキュリティの方法で保護可能であり、メッセージに信頼性を持たせ、第三者による傍受のリスクを減じるこ

とが可能である。

【００１２】

図２は、本発明による図１のシステムの動作ステップを示したものである。これらステップのある部分まではすでに説明を行っているので、その部分については幾らか説明を省略する。

【００１３】

ステップ１１０において、ユーザ１０は通信リンク２０経由で秘密保持システム３０へのアクセスをリクエストする。上述したように、一般的にこれにはシステム３０にユーザ識別情報を提供するユーザが含まれている。

【００１４】

ステップ１１２において、システム３０はユーザ１０によって提供されたユーザ識別情報が有資格ユーザの有効情報かどうかを判断する。この判断を行うためシステム３０は、ユーザから提供されたユーザ識別情報と全有資格ユーザリストとを比較する。図２のこれらのステップは、ユーザがこのテストをパスしたものと仮定したものである。しかし万一、パスしなかった場合、システム３０はステップ（上記にて提示した）を追加し、ユーザに再入力を行うよう指示を行うか、または、（直ちに、もしくはユーザが所定回数入力してもなお有効なユーザ識別番号を提供しなかった場合に）ユーザとの接続を終了する。

【００１５】

また、ステップ１１２において（ユーザが有効なユーザ識別番号を提供したとの仮定において）システム３０は、ユーザおよび／またはユーザアクセスリクエストが再認証を必要とするかどうかを判断する。すなわち、システム３０への比較的低レベルのアクセスについてのみの資格を有し、さらなるセキュリティの事前確認なしで許可されるユーザもいる。また、セキュリティの事前確認が必要なユーザが低レベルのアクセスのみをリクエストする場合もある。これらの場合は、セキュリティの事前確認を必要としない。しかしながら、図２に示すステップのほとんどは、システム３０がリクエストされたアクセスに応ずる前に、ユーザおよび／またはユーザアクセスリクエストがさらなるセキュリティの事前確認を必要とするとの仮定において示している。よって、ステップ１１４以降が実行されるべきであるとの仮定にたっている。

【００１６】

ステップ１１４において、システム３０は、システム３０にアクセスするためにユーザ１０が所持していなくてはならない無線遠隔通信装置７０の「起動番号」を識別する。もし装置７０がページャであれば、この番号は、コールがそのページャに着信しなくてはならない番号である。もし装置７０が携帯電話であれば、これはその電話番号である。

【００１７】

ステップ１１６において、システム３０は、４０、５０、６０、および７０部分を経由してユーザ１０に送られる再認証情報を発する。例えば、この再認証情報は不規則な、またはほぼ不規則な番号（例えば、不規則な、またはほぼ不規則な電話番号）である。

【００１８】

ステップ１１８において、システム３０は、無線通信システム５０に対し、ユーザ装置７０にコールし、そのユーザ装置に再認証情報を伝送するよう命令する。

【００１９】

ステップ１２０において、ユーザ装置７０はシステム５０経由でシステム３０からの再認証情報を受取り、ステップ１２２において、装置７０は受取った再認証情報をユーザに提供する。

【００２０】

ステップ１２４において、システム３０は装置７０から受取った再認証情報を入力するようユーザに指示を行う。このような指示は必要でない場合もあり、このステップは任意となる。

【００２１】

ステップ１２６において、ユーザは、装置７０から受取った再認証情報をシステム３０に

入力する。システム全体の構成により、ユーザによるこの情報入力は、通信リンク２０経由かまたは、７０、６０、５０、および４０部分を通るリターンチャネル経由のどちらか経由で行われる。例えば、装置７０がアンサーバック不可のページャである場合、ステップ１２６は通信リンク２０経由で行われる。また、装置７０がアンサーバックが可能なページャ、または携帯電話である場合、ステップ１２６は７０、６０、５０、および４０部分経由で行われる。

【００２２】

ステップ１２８において、システム３０は、ステップ１１６およびステップ１１８において送信した再認証情報と、ステップ１２６において返送された再認証情報とを比較する。それらがマッチした場合、ステップ１３０にて制御はステップ１３４に送られ、そこでシステム３０はユーザアクセスを許可する。一方、再認証情報が一致しなかった場合、ステップ１３０にて制御はステップ１３２に送られ、システム３０はユーザアクセスを（例えば、ユーザに対し適切なメッセージを送った後、ユーザとの接続を中断することにより）を終了させる。

本プロセスはステップ１３６において終了する。

【００２３】

図２におけるステップの順序はそれ程重要でない部分もある。例えば、ステップ１２４（システム３０がユーザに対し再認証情報入力を指示）は、プロセスのもっと早い段階であってもよい（例えば、ステップ１１６とステップ１１８の間でもよい。）。

【００２４】

このように前のステップにおくことで、装置７０経由にて再認証情報を受取る用意があることをユーザに知らせることが出来る点において望ましい。例えば、ユーザは装置７０をスタンバイさせるためにスイッチを入れる必要があるかもしれない。よって、指示ステップ１２４をより早い段階にするとこの点において有利である。

【００２５】

図３は、図１に示したシステムの別の形態である。図３は、４０’、５０’、６０’、７０’および８０’部分が、システム３０からユーザ１０方向へ、かつシステム３０に戻る方向への双方向通信が可能であることを図３において明示していること以外は、図１と同様の形態である。このように図３では、４０’、５０’、６０’、７０’および８０’部分経由でシステム３０から送られた再認証情報を、同通信チャネルのリバースパス経由でユーザからシステム３０に返送可能である全体のシステムタイプを明確に示している。また、図２の方法は図１及び図３のタイプのシステムに等しく適応する。

【００２６】

図４は、図１及び図３に示したシステムのまた別の形態である。図４において、ユーザ１０に連動する無線通信装置７０’は、そのユーザが所持するのではなく、他の人物（ユーザ認証者９０）が所持する。ユーザ１０がシステム３０へのアクセスをリクエストすると、このシステムは前述のように無線伝送を開始する。しかし、この場合、無線伝送はいくつかの再認証情報に加え、ユーザ１０を識別する情報をも含んでいる。例えば、ユーザ識別情報にはユーザの氏名や識別番号と同時に、ユーザ１０がシステム３０にアクセスを試みている電話の番号が含まれているかもしれない。このユーザ識別情報は、ユーザのアクセスリクエストを許可するかどうかを判断するユーザ認証者９０にとって役立つものである。ユーザ認証者９０が許可すると判断した場合、ユーザ許諾者は、７０’、６０’、５０’、および４０’部分を通るリバース通信チャネル経由で再認証情報をシステム３０に返送する。再認証情報がこうしてシステム３０に返送されると、システム３０は、ユーザ１０のアクセスを許可する。

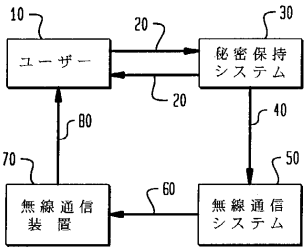
【００２７】

図５は、図４に示したシステムに図２の方法を適用させたものである。図５に示したステップのその多くは図２に示したステップと同様もしくは類似のものである。これら対応一致する部分は、図２及び図５に示した対応ステップと同じ下２桁の参照番号を使用することによって指示している。このように、すでに図２において対応したステップについて詳

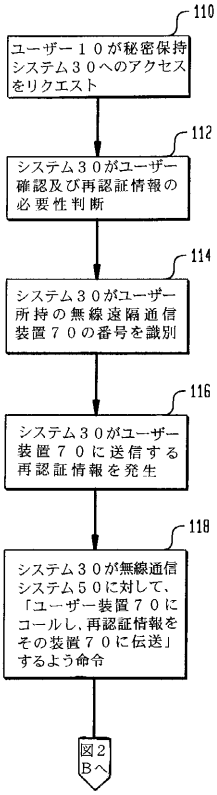
細説明を行っているので、図５においては説明を幾らか省略する。
【００２８】
ステップ２１０（図２のステップ１１０に対応）において、ユーザ１０は通信チャネル２０経由でシステムに対しアクセスをリクエストする。
【００２９】
ステップ２１２（図２のステップ１１２に対応）において、システム３０はユーザ１０が提供したユーザ識別情報を受諾し、このユーザアクセスリクエストには再認証情報が必要であると認識する。
【００３０】
ステップ２１４（図２のステップ１１４に対応）において、システム３０は、ユーザのアクセスリクエストを許可するユーザ認証者９０と連動する装置７０’の起動番号を識別する。
【００３１】
ステップ２１６（図２のステップ１１６に対応）において、システム３０は、装置７０’に伝送するユーザ識別情報および再認証情報を発する。上述のように、このユーザ識別情報にはユーザ１０の氏名、コード番号、ユーザがアクセスリクエストを行っている電話番号等が含まれる。この再認証情報は、本発明の他の実施形態の説明において使用している再認証情報と同様のものである。
【００３２】
ステップ２１８（図２のステップ１１８に対応）において、システム３０は、システム５０’に対し、装置７０’にコールし、ステップ２１６において発せられた情報を装置７０’に送信するよう命令する。
【００３３】
ステップ２２０（図２のステップ１２０に対応）において、装置７０’は、上記情報を受取り、ステップ２２２（図２のステップ１２２に対応）において、装置７０’はその情報をユーザ認証者９０に提供する。
【００３４】
ステップ２２６（図２のステップ１２６に対応）において、ユーザ認証者９０はユーザのアクセスリクエストを許可すると、再認証情報をシステム３０に返送する。
【００３５】
後続ステップ２２８、２３０、２３２、２３４、および２３６は、それぞれ、図２のステップ１２８、１３０、１３２、１３４、および１３６と同じであるため、ここでは説明を省く。
【００３６】
以上、本発明の実施の形態を詳細に説明したが、本発明の範囲を逸脱することなく他の方法でも具体化出来ることは当業者にとって明らかである。例えば、本発明においては、多くの別のタイプのユーザ端末装置１０、秘密保持システム３０、無線遠隔通信装置７０、および遠隔無線通信システム５０が使用可能である。繰返すと、本発明の使用可能例には、コンピュータシステム、トランザクション処理システム、ボイスメールまたは音声応答システムに対するアクセス制御、また、ビル、刑務所、軍用施設、高度安全保障場所等の警備保障施設へのアクセス制御が含まれる。よって、本発明は、管理ユーザ、またはスーパユーザのようなある特定のユーザのみにより使用されるであろう。
【図面の簡単な説明】
【図１】本発明に従って動作可能なシステムのブロック略図である。
【図２Ａ】本発明による方法を実行するステップのフローチャートを示す図である。
【図２Ｂ】本発明による方法を実行するステップのフローチャートを示す図である。
【図２Ｃ】本発明による方法を実行するステップのフローチャートを示す図である。
【図３】本発明に従って動作可能な別のシステムを示した図１に類似のブロック略図である。
【図４】本発明に従って動作可能なさらに別のシステムを示した図１および図３に類似の

ブロック略図である。
【図５Ａ】本発明による別の方法を実行するステップのフローチャートを示す図である。
【図５Ｂ】本発明による別の方法を実行するステップのフローチャートを示す図である。
【図５Ｃ】本発明による別の方法を実行するステップのフローチャートを示す図である。

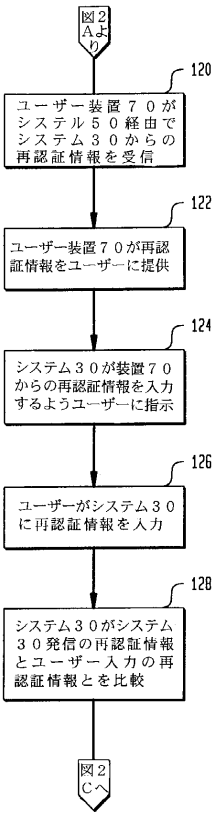
【図１】



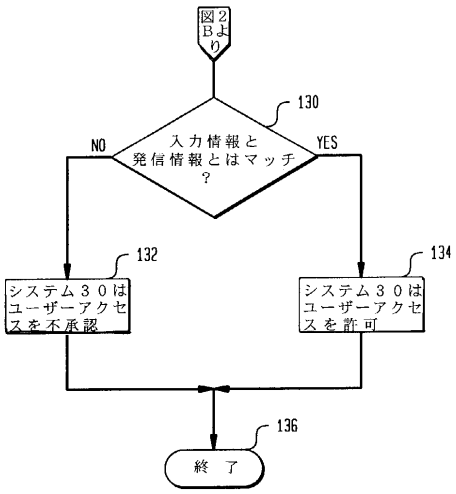
【図２Ａ】



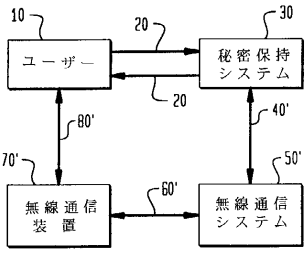
【図２Ｂ】



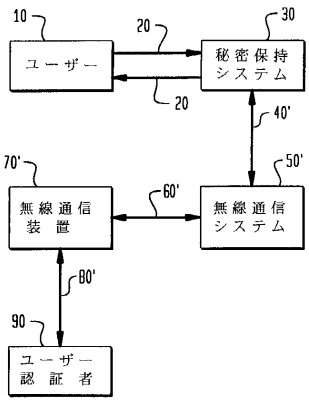
【図２Ｃ】



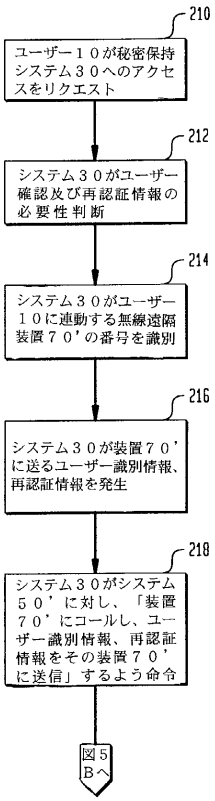
【図３】



【図４】



【図５Ａ】



【図５Ｂ】

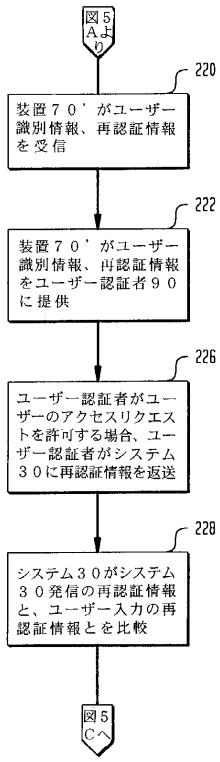


図5Aより
220
装置７０'がユーザー識別情報、再認証情報を受信
222
装置７０'がユーザー識別情報、再認証情報をユーザー認証者９０に提供
226
ユーザー認証者がユーザーのアクセスリクエストを許可する場合、ユーザー認証者がシステム３０に再認証情報を返送
228
システム３０がシステム３０発信の再認証情報と、ユーザー入力の再認証情報とを比較
図5Cへ

【図５Ｃ】

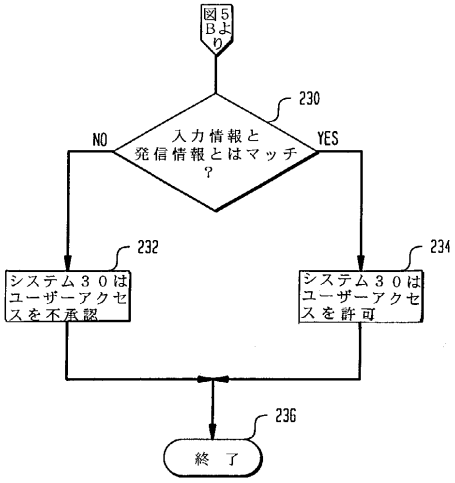


図5Bより
230
入力情報と発信情報とはマッチ？
NO
YES
232
システム３０はユーザーアクセスを不承認
234
システム３０はユーザーアクセスを許可
236
終了

フロントページの続き

(72)発明者　アンドリュー　フレデリック　バルファー
アメリカ合衆国　０７０４６　ニュージャーシイ，マウンテン　レイクス，ブウルヴァード　８５
(72)発明者　チャールズ　アーサー　ウィッツチョリック
アメリカ合衆国　６０５６３　イリノイズ，ネイパーヴィル，ノース　ルーミス　１１０４

審査官　望月　章俊

(56)参考文献　特表平１０－５０２１９５（ＪＰ，Ａ）
国際公開第９６／０００４８５（WO，Ａ１）
国際公開第９５／０１９５９３（WO，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
H04B7/24-7/26
H04Q7/00-7/38