

明 細 書

発明の名称：

通信装置、リマインダ装置、ならびに、情報記録媒体

技術分野

[0001] 本発明は、サーバ装置を利用するためのパスワード等の秘密情報を安全に管理するのに好適な通信装置、リマインダ装置、ならびに、これをコンピュータにより実現するためのプログラムを記録した非一時的な情報記録媒体に関する。

背景技術

[0002] 従来から、ユーザがパスワードを入力することによって利用が開始できるような各種のサーバ装置が提案されている。このようなサーバ装置を複数利用する場合には、安全性を向上させるために、サービスごとに異なるパスワードを利用することが望ましい。ここで、多数のパスワードをユーザが自身の頭に記憶するのは煩雑であり、特許文献 1 に開示される技術では、一つのマスターパスワードを入力すると、各サービス用のパスワードが読み出せるような記憶媒体を利用することとしている。

先行技術文献

特許文献

[0003] 特許文献1：特開 2 0 0 4 - 2 8 0 2 4 5 号公報

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、たとえばインターネットカフェなどでこのような記憶媒体を利用すれば、各サービス用のパスワードが読み出せることとなるため、安全性が低くなってしまふ。また、記憶媒体を紛失すると、各サービス用のパスワードがわからなくなってしまうという問題もある。

[0005] 一方で、現在、各家庭には、家庭内無線 LAN (Local Area Network) 等を実現するためのルータ装置等、インターネットからアクセス可能な各種の

通信装置が配置されている。

また、インターネットに接続可能な携帯電話やスマートフォン等はもちろん、パーソナル・コンピュータ等の各種の通信装置が多数提供されている。これらの通信装置には、家庭用ルータ装置に匹敵しうるような通信能力、計算能力を持つものも多い。

[0006] そこで、これらの通信機器を利用することにより、ユーザの各パスワードを安全にサーバ装置に提供できるようにするとともに、パスワードをそのまま記憶させた記憶媒体を持ち歩かなくとも、パスワードの利用ができるようにパスワード管理をしたい、という要望は強い。

[0007] 本発明は、上記のような課題を解決するもので、サーバ装置を利用するためのパスワード等の秘密情報を安全に管理するのに好適な通信装置、リマインダ装置、ならびに、これをコンピュータにより実現するためのプログラムを記録した非一時的な情報記録媒体を提供することを目的とする。

課題を解決するための手段

[0008] 以上の課題を解決するため、本発明の原理にしたがって、下記の発明を開示する。

[0009] 本発明の第1の観点に係る通信装置は、

サーバ名と、所定の行数ならびに所定の列数のパスワード表と、が、対応付けられて記憶される記憶部、

サーバ名を指定する認証要求を受信する受信部、

所定の行数ならびに所定の列数のランダム表を生成する生成部、

生成されたランダム表を、ユーザに提示する提示部、

提示されたランダム表の要素をユーザに対応付けられる選択順序で選択して並べることにより得られるキーを、当該ユーザから受け付ける受付部、

受け付けられたキーと、生成されたランダム表と、から、ユーザに対応付けられる選択順序を同定する同定部、

認証要求に指定されたサーバ名に対応付けて記憶部に記憶されるパスワード表から、当該パスワード表に含まれる要素を同定された選択順序で選択し

て並べることにより得られる要素列から、パスワードを取得する取得部、
認証要求に指定されたサーバ名のサーバ装置をユーザが利用できるように
するためのパスワードとして、取得されたパスワードを出力する出力部
を備えるように構成する。

[0010] また、本発明の通信装置において、
認証要求に指定されるサーバ名のサーバ装置は、時刻同期型ワンタイムパ
スワードにより、ユーザが当該サーバ装置を利用できるか否かを判定し、
取得部は、得られた要素列からなるシードと、現在の時刻と、に、所定の
一方向性関数を適用した結果を、パスワードとして取得する
ように構成することができる。

[0011] また、本発明の通信装置において、
取得部は、得られた要素列をパスワードとして取得する
ように構成することができる。

[0012] また、本発明の通信装置において、
出力部は、ユーザに対して取得されたパスワードを表示することにより、
取得されたパスワードを出力する
ように構成することができる。

[0013] また、本発明の通信装置において、
出力部は、取得されたパスワードを指定する利用要求を、認証要求に指定
されたサーバ名のサーバ装置に送信することにより、取得されたパスワード
を出力する
ように構成することができる。

[0014] また、本発明の通信装置において、
受信部は、認証要求を、ユーザが利用する第1の端末から受信し、
提示部は、生成されたランダム表を、ユーザが利用する第2の端末に提示
し、
受付部は、キーを、第1の端末から受け付け、
出力部は、ユーザが第1の端末によりサーバ装置を利用できるようにする

ため、利用要求を送信する

ように構成することができる。

[0015] また、本発明の通信装置において、

受信部は、認証要求を、ユーザが利用する第 1 の端末から受信し、

提示部は、生成されたランダム表を、ユーザが利用する第 1 の端末に提示し、

受付部は、キーを、第 2 の端末から受け付け、

出力部は、ユーザが第 1 の端末によりサーバ装置を利用できるようにするため、利用要求を送信する

ように構成することができる。

[0016] また、本発明の通信装置において、

認証要求に指定されたサーバ名に対応付けられるパスワード表が記憶部に記憶されていない場合、所定の行数ならびに所定の列数の新たなパスワード表を生成し、当該新たなパスワード表の各要素をランダムに定めて、当該サーバ名に対応付けて、当該新たなパスワード表を記憶部に記憶させることにより、記憶部を更新する更新部

をさらに備え、

出力部が利用要求を認証要求に指定されたサーバ名のサーバ装置に送信することにより、当該ユーザを当該サーバ装置に登録する

ように構成することができる。

[0017] また、本発明の通信装置において、

認証要求に指定されたサーバ名に対応付けられるパスワード表が記憶部に記憶されていない場合、所定の行数ならびに所定の列数の新たなパスワード表を生成し、ユーザからパスワードの入力を受け付け、当該受け付けられたパスワードを分割して当該新たなパスワード表の同定された選択順序の要素に順に格納し、それ以外の要素をランダムに定めて、当該サーバ名に対応付けて、当該新たなパスワード表を記憶部に記憶させることにより、記憶部を更新する更新部

をさらに備えるように構成することができる。

[0018] なお、本発明に係る通信装置から、サーバ名に係る要素ならびに通信に係る要素を省略した形態は、パスワードやシードを含む各種の秘密情報のリマインダ装置として機能する。

[0019] 本発明のその他の観点に係るコンピュータ読取可能な非一時的情報記録媒体において、当該情報記録媒体に記録されるプログラムは、コンピュータを、上記の通信装置やリマインダ装置の各部として機能させるように構成する。

[0020] また、上記の通信装置やリマインダ装置におけるキーは、より一般には、ユーザがパスワード表や秘密情報表の要素を選択する選択順序に対応付けられる情報と考えることができる。すなわち、キーから選択順序が一意に導出できるのであれば、必ずしもランダム表を利用する必要はない。

[0021] また、上記プログラムは、コンパクトディスク、フレキシブルディスク、ハードディスク、光磁気ディスク、デジタルビデオディスク、磁気テープ、半導体メモリ、動作中のRAM (Random Access Memory) 等のコンピュータ読取可能な非一時的情報記憶媒体に記録することができる。

[0022] 上記プログラムは、プログラムが実行されるコンピュータとは独立して、コンピュータ通信網の信号線、すなわち、一時的信号媒体を介して、配布・販売することができる。また、上記情報記憶媒体は、コンピュータとは独立して配布・販売することができる。

発明の効果

[0023] 本発明によれば、サーバ装置を利用するためのパスワード等の秘密情報を安全に管理するのに好適な通信装置、リマインダ装置、ならびに、これをコンピュータにより実現するためのプログラムを記録した非一時的な情報記録媒体を提供することができる。

図面の簡単な説明

[0024] [図1]本発明の実施形態に係る通信装置及びこれに接続される各種の機器の概要構成を示す説明図である。

[図2]本実施形態に係る通信装置の概要構成を示す説明図である。

[図3]あるユーザのあるサーバ名に対するパスワード表の例を示す説明図である。

[図4]あるユーザのあるサーバ名に対するパスワード表に対するランダム表の一例を示す説明図である。

[図5]本実施形態の一つの例に係る通信の様子を示す説明図である。

[図6]本実施形態の他の例に係る通信の様子を示す説明図である。

発明を実施するための形態

[0025] 以下に本発明の実施形態を説明するが、以下に説明する実施形態は説明のためのものであり、本願発明の範囲を制限するものではない。したがって、当業者であればこれらの各要素もしくは全要素をこれと均等なものに置換した実施形態を採用することが可能であるが、これらの実施形態も本発明の範囲に含まれる。

実施例 1

[0026] 図1は、本発明の実施形態に係る通信装置を含む通信システムの概要構成を示す説明図である。以下、本図を参照して説明する。

[0027] 通信システム101においては、通信装置121が、LAN 141とインターネット161との間の通信の中継を行うルータとして機能する。

[0028] ユーザは、LAN 141内のコンピュータ151から通信装置121を介してインターネット161にアクセスすることが可能であるほか、インターネット161側から通信装置121にアクセスすることも可能である。

[0029] インターネット161側から通信装置121にアクセスする手法としては、ユーザが所有する携帯電話やスマートフォン等の移動端末171を利用する手法のほか、LAN 141外のインターネットカフェなどに用意された不特定多数の利用者が利用する端末装置181を使用する態様もありうる。

[0030] また、インターネット161には、各種のサーバ装置191が接続されている。本実施形態では、ユーザがLAN 141内のコンピュータ151や、インターネットカフェなど外部のネットワーク内の端末装置181などが

ら、サーバ装置 191 を利用しようとする際に、通信装置 121 を用いて、当該ユーザのパスワードをサーバ装置 191 へ伝達するのである。

[0031] さて、本実施形態に係る通信装置 121 は、ルータ用のコンピュータにて所定のプログラムを実行することによって実現される。

[0032] 典型的なルータ用のコンピュータは、CPU (Central Processing Unit) の制御の下、一時的な記憶領域として RAM を、不揮発な記憶領域として EEPROM (Electrically Erasable Programmable Read Only memory) や HDD (Hard Disk) を使用し、2つの NIC (Network Interface Card) を使用して、インターネット 161 や LAN 141 内のコンピュータ 151 との間で通信する。CPU は、RAM や EEPROM、HD 等を参照し、あるいは NIC を使用して、各種のデータの取得、提供、演算等の処理を行う。

[0033] ルータ用のコンピュータが無線ルータの機能を有する場合には、2つの NIC の一方が無線 LAN のアクセスポイントとなり、LAN 141 内のコンピュータ 151 と、インターネット 161 との間の通信を中継する。

[0034] インターネット 161 側からルータ用のコンピュータにアクセスする際には、ルータ用のコンピュータに割り振られた固定ホスト名や固定グローバル IP (Internet Protocol) アドレスや、DDNS (Dynamic Domain Name System) による固定ホスト名ならびに動的グローバル IP アドレスを利用することも可能である。

[0035] ルータ用のコンピュータは、LAN 141 内の他のコンピュータのブラウザ等からアクセスしたり、ルータ用コンピュータに接続されるキーボードやマウスなどからの指示を受けて、各種の維持管理がなされる。

[0036] 上記のプログラムは、HD や EEPROM に記録され、RAM に読み出されて実行される。また、その配布には、NIC 経由でインターネット内の他の機器からダウンロードしたり、DVD-ROM (Digital Versatile Disk ROM) を利用したり等が可能である。

[0037] (通信装置の基本構成)

図 2 は、本実施形態に係る通信装置 121 の概要構成を示す説明図である

。以下、本図を参照して説明する。

[0038] 通信装置 1 2 1 は、記憶部 2 0 1、受信部 2 0 2、生成部 2 0 3、提示部 2 0 4、受付部 2 0 5、同定部 2 0 6、取得部 2 0 7、出力部 2 0 8、更新部 2 0 9 を備える。

[0039] なお、一般には、通信装置 1 2 1 は、複数のユーザのパスワードを管理するが、以下の説明では、理解を容易にするため、特定の一人のユーザに関する情報の管理について説明する。複数のユーザのそれぞれについて同様の処理を実行することにより、複数のユーザのパスワードを管理することが可能である。また、複数のユーザが利用する場合には、種々の情報のやりとりにおいて、当該ユーザのユーザ名やユーザが使用するコンピュータ 1 5 1 や移動端末 1 7 1 の個体識別番号など、ユーザを識別するための識別情報を指定することとなる。

[0040] 通信装置 1 2 1 にパスワードを管理されるユーザには、所定の行数、所定の列数の表の要素から、所定の個数の要素を選択する選択順序が割り当てられている。この選択順序が、ユーザの認証に利用される。

[0041] (パスワード表)

さて、記憶部 2 0 1 には、サーバ名と、所定の行数ならびに所定の列数のパスワード表と、が、対応付けられて記憶され、本実施形態では、E E P R O M や H D により構成される。

[0042] サーバ名は、当該ユーザが利用可能なサーバ装置 1 9 1 の名前であり、本実施形態では、当該サーバ装置 1 9 1 のドメイン名や I P アドレスを採用する。

[0043] 図 3 は、あるユーザのあるサーバ名に対するパスワード表の例を示す説明図である。以下、本図を参照して説明する。

[0044] 本図に示すパスワード表 3 0 1 は、5 行 5 列の 2 5 個の要素 3 0 2 からなり、パスワード表 3 0 1 の要素 3 0 2 には、それぞれ、3 文字のランダムな英数字が埋め込まれている。以下、パスワード表 3 0 1 内の各要素を表す際には、符号「3 0 2」の末尾に英小文字の添字を付すものとし、添字がない

場合は、総称を意味するものとする。

[0045] 上記のように、パスワード表 301 のユーザには、5 行 5 列の表からある個数の要素を順に選び出すための選択順序が割り当てられている。ここでは、当該ユーザに、選択順序として「まず 1 行 1 列目を選び、次に 2 行 5 列目を選び、最後に 4 行 2 列目を選ぶ」という選択順序が割り当てられているものとする。

[0046] 本実施形態では、当該ユーザの当該サーバ名に対する実際のパスワードが、パスワード表 301 の 1 行 1 列目の要素 302 a の 3 文字「L m j」、パスワード表 301 の 2 行 5 列目の要素 302 b の 3 文字「a 8 i」、パスワード表 301 の 4 行 2 列目の要素 302 c の 3 文字「6 z h」を連結することにより、「L m j a 8 i 6 z h」のように得られるのである。

[0047] パスワード表 301 のうち、選択順序に含まれない要素 302 には、ランダムな英数字が埋め込まれている。したがって、通信装置 121 に対する侵入が生じてパスワード表 301 全体が漏洩してしまっても、当該ユーザの当該サーバ名に対する実際のパスワードが直ちに侵入者に知得されてしまう、ということはない。ここに、本実施形態の特徴の一つがある。

[0048] さて、本実施形態では、ユーザがサーバ装置 191 を利用しようとする際には、その利用に供される LAN 141 内のコンピュータ 151 や LAN 141 外の端末装置 181 等からサーバ装置 191 のサーバ名を指定する認証要求を送信する。

[0049] すると、受信部 202 は、サーバ名を指定する認証要求を受信する。したがって、CPU の制御の下、NIC が受信部 202 として機能する。

[0050] (ランダム表)

認証要求が受信されると、生成部 203 は、当該ユーザの認証要求に指定されたサーバ名について記憶部 201 に記憶されているパスワード表 301 と同じ行数ならびに同じ列数のランダム表を生成する。本実施形態では、CPU がこの生成処理を実行する。

[0051] 図 4 は、あるユーザのあるサーバ名に対するパスワード表に対するランダ

ム表の一例を示す説明図である。

- [0052] 本図に示すランダム表401は、パスワード表301と同じ行数、同じ列数、すなわち、5行5列の表で、ランダム表401の要素402には、それぞれ、ランダムな2桁の数字が埋め込まれている。ここで、各要素402に埋め込まれている数字は互いに異なる。
- [0053] このようにして生成されたランダム表401は、提示部204がユーザに提示する。たとえば、ルータ用のコンピュータのCPUが、ユーザがサーバ装置191へのアクセスに利用しようとしているLAN 141内のコンピュータ151やLAN 141外の端末装置181等に、NICを用いて指示を出して、モニタ画面にランダム表401を表示させることにより、本提示処理が行われる。
- [0054] さて、ランダム表401の提示を受けたユーザは、ランダム表401の各要素402から、自身の選択順序にしたがって選択を行う。上記の例によれば、ランダム表401の1行1列目の要素402aの2桁数字「13」、ランダム表401の2行5列目の要素402bの2桁数字「02」、ランダム表401の4行2列目の要素402cの2桁数字「31」が選択される。
- [0055] そして、ユーザは、当該ユーザが所有する移動端末171等から、これらを連結した6桁数字「130231」からなるキーを通信装置121に送付する。
- [0056] 通信装置121の受付部205は、このキー「130231」を当該ユーザから受け付ける。したがって、NICが、CPUの制御の下、受付部205として機能する。
- [0057] さらに、同定部206は、受け付けられたキーと、生成されたランダム表401と、から、ユーザに対応付けられる選択順序を同定する。
- [0058] 本例では、受け付けられたキーを2桁ごとに分離すれば、「13」「02」「31」が得られる。ランダム表401の各要素402は互いに異なるから、これら3つの2桁数字をランダム表401の各要素402から探せば、当該ユーザの選択順序が「まず1行1列目を選び、次に2行5列目を選び、

最後に4行2列目を選ぶ」であることが同定されるのである。

[0059] この他、ランダム表401の各要素に絵を入れたり、各要素は空白のままとする形態もありうる。この形態では、ランダム表401の各要素の行番号、列番号をユーザに入力させても良い。

[0060] また、ランダム表401の各要素に絵を表示するとともに、各要素には画面に表示されないランダムな数字を割り当てておき、ユーザが絵を指示すると、その要素に割り当てられた数字が選択される、という態様を採用することもできる。

[0061] すなわち、図4に示すようなランダム表401を画面に表示するのではなく、ランダム表401と行数、列数が同じで、要素内に各種の絵やシンボル、イラストを配置した表を画面に表示する。

[0062] そして、絵等が描かれた要素をユーザが指示（たとえば、画面がタッチスクリーンで構成されている場合には、要素を直接ユーザが指でタップすれば良い。また、キーボードやマウスを利用して画面内のカーソルを移動させた上で、決定キーやマウスボタンを操作することで、要素を指示する手法を採用することもできる。）すると、その要素と同じ行番号、列番号の位置に配置された図4のランダム表401の数値が選択されることとする。

[0063] この態様では、ユーザに親しみやすい絵等を用いることで、ランダム表401のユーザによる選択を容易にする、という効果がある。

[0064] ついで、取得部207は、認証要求に指定されたサーバ名のサーバ装置191に対するアクセスを希望するユーザのパスワードを取得する。すなわち、上記のように同定された選択順序により、当該パスワード表301からパスワード表301の1行1列目の要素302aの3文字「L m j」、パスワード表301の2行5列目の要素302bの3文字「a 8 i」、パスワード表301の4行2列目の要素302cの3文字「6 z h」を選択して、これらを連結することにより、パスワード「L m j a 8 i 6 z h」を取得するのである。したがって、CPUがEEPROMやHDと共働して、取得部207として機能する。

[0065] このように、本実施形態では、選択順序そのものは、通信装置 1 2 1 内に記録しない。したがって、通信装置 1 2 1 に対する侵入が生じたとしても、パスワード表 3 0 1 全体が漏洩してしまっても、当該ユーザの当該サーバ名に対する実際のパスワードが直ちに侵入者に知得されてしまう、ということはない。ここに、本実施形態の特徴の一つがある。

[0066] さて、出力部 2 0 8 は、取得されたパスワードを指定する利用要求を認証要求に指定されたサーバ名のサーバ装置 1 9 1 に送信して、当該ユーザが当該サーバ装置 1 9 1 を利用できるようにする。

[0067] すなわち、通信装置 1 2 1 は、サーバ装置 1 9 1 に対するログインの代理サーバとして機能する。

[0068] ユーザが利用する L A N 1 4 1 内のコンピュータ 1 5 1 や携帯電話等の移動端末 1 7 1 から、通信装置 1 2 1 を介して、サーバ装置 1 9 1 にパスワードが送信され、ログインに成功した後も、当該サーバ装置 1 9 1 に対する通信装置 1 2 1 をプロキシサーバとして利用し続けることとしても良いし、openIDなどの認証技術と同様に、通信装置 1 2 1 による代理を解除して、L A N 1 4 1 内のコンピュータ 1 5 1 や携帯電話等の移動端末 1 7 1 と、サーバ装置 1 9 1 との間で、通信を行うこととしてもよい。

[0069] 図 5 は、このような、本実施形態の一つの例に係る通信の様子を示す説明図である。以下、本図を参照して説明する。

[0070] 上記のように、本例では、

(1) 第 1 の端末として L A N 1 4 1 内のコンピュータ 1 5 1 や L A N 1 4 1 外の端末装置 1 8 1 を採用して、認証要求の送信 (5 0 1) 元、ランダム表 4 0 1 の提示 (5 0 2) 先、サーバ装置 1 9 1 への利用 (5 0 3) 元として利用し、

(2) 第 2 の端末として携帯電話等の移動端末 1 7 1 を採用して、キーの送付 (5 0 4) 元として利用することとして、ランダム表 4 0 1 が表示される機器と、キーを入力する機器を分離している。

[0071] この態様では、携帯電話等の移動端末 171 においても、キーの他、当該ユーザのユーザ名やサーバ名を入力させる態様が最も単純である。

[0072] このほか、記憶部 201 において、当該ユーザの携帯電話等の移動端末 171 のメールアドレスやショートメッセージアドレスを管理し、本セッションに対するキーを入力するための入力フォームを表す URL (Universal Resource Locator) を通知して、携帯電話等の移動端末 171 のブラウザでユーザにアクセスさせる態様を採用することもできる。

[0073] このほか、ランダム表 401 の提示先とキーの送付元を入れ換えることとしても良い。図 6 は、このような、本実施形態の他の例に係る通信の様子を示す説明図である。以下、本図を参照して説明する。

[0074] すなわち、

(1) 第 1 の端末として、LAN 141 内のコンピュータ 151 や LAN 141 外の端末装置 181 を採用し、認証要求の送信 (501) 元、キーの送付 (504) 元、サーバ装置 191 への利用 (503) 元として利用し、

(2) 第 2 の端末として、携帯電話等の移動端末 171 を採用し、ランダム表 401 の提示 (502) 先として利用することとして、ランダム表 401 が表示される機器と、キーを入力する機器を分離する。

[0075] この態様では、記憶部 201 において、当該ユーザの携帯電話等の移動端末 171 のメールアドレスやショートメッセージアドレスを管理し、本セッションに対する電子メールやショートメッセージの本文にランダム表 401 を記載して提示することとしても良いし、ランダム表 401 を表示するための入力フォームを表す URL を通知して、携帯電話等の移動端末 171 のブラウザでユーザにアクセスさせる態様を採用することもできる。

[0076] これらの態様を採用することにより、端末装置 181 に対するモニタ画面の表示やキーボードの操作の履歴などを侵入者が追跡したとしても、サーバ装置 191 に対するパスワードは漏洩しないこととなる。したがって、セキュリティを格段に向上させることができる。

- [0077] このほか、LAN 141内のコンピュータ151から通信装置121を介してサーバ装置191へのアクセスをする場合に限っては、LAN 141内のコンピュータ151に、認証要求の送信元、ランダム表401の提示先、キーの送付元サーバ装置191への利用元の役割りを担わせても良い。
- [0078] 通信装置121が家庭内LAN用のルータとして機能している場合には、これらの情報のやりとりをしたとしても、LAN 141内のコンピュータ151は信頼性が高いものと考えられるからである。
- [0079] 勿論、LAN 141内のコンピュータ151から通信装置121を介してサーバ装置191へのアクセスをする場合であっても、上記のように、第1の端末と第2の端末とに役割を分離する形態を採用しても良い。
- [0080] さらに、これらの認証の際に、通信装置121が、ユーザ名や携帯電話等の移動端末171の個体識別番号等、ユーザを識別するための情報のチェックをあわせて行うこととしても良い。
- [0081] また、パスワード表301の行数や列数、各要素302に含まれる文字列の長さは、上記のものに限定されるわけではなく、種々変更が可能である。一般には、一人のユーザに対して各種のサーバ装置191用の複数のパスワード表301が用意されるので、これらの複数のパスワード表301で行数と列数は共通とする。また、各要素302内の文字列の長さは、そのパスワード表301に対するサーバ装置191に必要なパスワードの長さでユーザの選択順序に基づいて選択される要素302の個数から定める。
- [0082] このほか、ランダム表401の行数や列数は、パスワード表301と共通とする必要があるが、各要素402に含まれる文字列の種類や長さは適宜変更が可能である。ランダム表401とキーから、ユーザの選択順序が求められるように構成するため、全要素402について文字列の長さを共通とし、要素402が互いに異なるように構成するのが一般的である。
- [0083] なお、パスワード表301の各要素302に含まれる文字列や、ランダム表401の各要素402に含まれる文字列を、接頭符号とすることで、これらの文字列の長さを可変とすることも可能である。すなわち、表内の要素の

各文字列は、表内の他のいずれの要素の文字列の接頭部になっていない、という性質を持つように、これらの表をランダムに構成すれば良い。接頭符号を用いることで、キーから選択順序が一意に復元できるようになる。

[0084] 上記の実施例では、出力部 208 が、サーバ装置 191 へ、パスワードを指定する利用要求を送信することにより、パスワードを出力していた。

[0085] このほか、第 1 の端末（コンピュータ 151 や端末装置 181）、第 2 の端末（移動端末 171）を通信装置 121 と一体に構成した場合には、通信装置 121 は、パスワード・リマインダーとして機能する。

[0086] 典型的には、この態様の通信装置 121 は、キーボードやタッチパネル等の入力装置と、ディスプレイ等の表示装置と、を備え、インターネット接続可能な通信機能を有する携帯電話やスマートフォン等により実現される。

[0087] この態様では、認証要求は、通信装置 121 の入力装置を介してユーザから与えられる（501）。

[0088] ランダム表は、表示装置に表示され（502）、ユーザに提示される。

[0089] ユーザは、表示されたランダム表に変換を施して、認証用のキーを、入力装置を介して通信装置 121 に与える（504）。

[0090] すると、通信装置 121 の出力部 208 は、取得されたパスワードを表示装置に表示して、所望のサーバ装置用のパスワードをユーザに知らせる。

[0091] 本態様のパスワード・リマインダーでは、通信装置 121 を構成するスマートフォン等が盗難された場合であっても、記憶部 201 には、パスワードがそのまま記憶されているわけではないので、直ちにパスワードが漏洩することはない。

[0092] また、通信装置 121 にはユーザの変換規則は記録されていないから、スマートフォン等を入手した第三者が悪用を試みたとしても、表示装置に表示された「パスワード」が当該サーバ装置において実際に利用可能なものとなる危険性は低い。

[0093] 本発明の原理に基づくパスワード・リマインダーの種々の態様については、後述する実施例 3 において、さらに説明する。

[0094] (サーバ装置への新規登録)

さて、上記の説明では、記憶部201にすでにパスワード表301が記憶されている状況を想定していたが、以下では、あるサーバ名のサーバ装置191に対するあるユーザのパスワード表301を新たに生成するための手法について説明する。

[0095] すなわち、認証要求に指定されたサーバ名に対応付けられるパスワード表が記憶部201に記憶されていない場合、更新部209は、所定の行数ならびに所定の列数の新たなパスワード表を生成して、当該新たなパスワード表を記憶部201に記憶させることにより、記憶部201を更新する。

[0096] 新たなパスワード表301の各要素302に定められる文字列の長さ(文字数)や文字の種類は、当該ユーザの選択順序の諸元、ならびに、対応するサーバ装置191が許容するパスワードの種類に応じて定める。

[0097] ユーザの選択順序により、N個の要素302が選択され、サーバ装置191用のパスワードの長さがM文字である場合、各要素302に格納する文字列の長さLは、

$$L \times (N-1) < M \leq L \times N$$

を満たすように定める。

[0098] パスワードの長さがある範囲に含まれば良いシステムでは、上記不等式のうちの等号が成立するように、M, Lを定めることが望ましい。

[0099] パスワードの長さが固定されている場合で、上記不等式のうちの等号が成立しない場合には、以下のような手法がありうる。

(1) 当該サーバ名に対応付けて、パスワード表301のほかに、パスワードの長さMを記憶する手法。選択順序にしたがって得られるL×N文字の文字列から、いずれかのM文字を規則的に抽出して、これをパスワードとして利用する手法である。具体的な規則としては、先頭M文字を抽出したり、末尾M文字を抽出する手法がある。このほか、整数の加減算のみでM対L×Nの傾きの線分を描くブレゼンハムのアルゴリズムを適用して、誤差カウンタが繰り上がる毎に1文字を抽出する、という手法もある。

(2) 当該サーバ装置 191 で利用できない文字を適宜挿入し、 $L \times N$ 文字の文字列からこの利用できない文字を除去すると、パスワードが得られるようにする手法。たとえば、一般的なパスワードでは、文字コード 32 ~ 127 の ASCII 文字が利用可能であり、タブ文字や改行文字は利用できないのが一般的である。そこで、これらの利用不可能文字をパスワード表 301 の各要素 302 にランダムに挿入しておく手法である。パスワード表 301 の全要素 302 中の文字数と、パスワード表 301 の全要素 302 に出現する利用可能文字の文字数との比ができるだけ M 対 $L \times N$ に一致するように、ランダムに各要素 302 を定めることが望ましい。

[0100] このようにして、当該ユーザの当該サーバ名に対する新たなパスワード表 301 を生成して記憶部 201 に記憶させた後は、出力部 208 が、認証要求に指定されたサーバ名のサーバ装置 191 に、利用要求を送信することにより、当該ユーザを当該サーバ装置 191 に登録する。

[0101] すなわち、出力部 208 は、上記のように、記憶済みのパスワード表 301 からパスワードを得た場合には、「サーバ装置 191 のユーザとして登録済みのユーザがログインするためのパスワード」として、当該パスワードをサーバ装置 191 に送信する。

[0102] 一方、更新部 209 により新たに生成されて記憶部 201 に記憶されたばかりのパスワード表 301 からパスワードを得た場合には、「サーバ装置 191 のユーザとして未登録のユーザを新規に登録する際のログイン用パスワード」として、当該パスワードをサーバ装置 191 に送信する。

[0103] なお、サーバ装置 191 におけるパスワードに有効期限があり、パスワードの切り替えが必要な場合にも、本態様は有用である。すなわち、取得部 207 が、古いパスワードを既存のパスワード表 301 から得て、新たなパスワードを新たに生成したパスワード表 301 から得て、出力部 208 が両者をサーバ装置 191 に送信することにより、パスワードの更新を行う。

[0104] 本態様では、ユーザは、第三者から推測されにくく、自分が記憶しやすいパスワードをわざわざ考える必要はない。ユーザのサーバ装置 191 に対す

るパスワードは、ランダムに生成され、誰からも推測しにくいものとなるからである。したがって、ユーザが自分でパスワードを選択するよりも、サーバ装置 191 に対するパスワードの安全性をより一層高めることができるようになる。

[0105] なお、本実施形態に係る通信装置 121 は、ルータ用のコンピュータ上に実装するのが最も典型的であるが、必ずしも、ルータとして機能する必要はない。たとえば、サーバ装置 191 に対するプロキシとして機能するようなコンピュータにより、通信装置 121 を実現することも可能であり、そのような態様も、本発明の範囲に含まれる。

実施例 2

[0106] 上記の実施形態では、サーバ装置 191 に対して新規にユーザ登録を行う場合を想定していたが、本実施形態は、別途サーバ装置 191 にユーザ登録を行っており、パスワードが定められている場合に対応するものである。

[0107] この場合、認証要求に指定されたサーバ名に対応付けられるパスワード表は記憶部 201 に記憶されていないことになる。

[0108] すると、更新部 209 は、上記実施形態と同様に、所定の行数ならびに所定の列数の新たなパスワード表 301 を生成して、当該サーバ名に対応付けて、当該新たなパスワード表 301 を記憶部 201 に記憶させることにより、記憶部 201 を更新する。

[0109] ただし、パスワード表 301 の各要素 302 に埋め込む文字列の構成方法が少々異なる。

[0110] すなわち、更新部 209 は、ユーザから当該サーバ装置 191 に対するパスワードの入力を受け付ける。セキュリティを向上させる観点から、ユーザが当該パスワードの入力を行う機器は、通信装置 121 が管理する LAN 141 内のコンピュータ 151 に限定することが望ましい。

[0111] LAN 141 内のコンピュータ 151 において、ユーザがユーザ名やサーバ名を入力し、これらを指定する認証要求が通信装置 121 に送信される。すると、通信装置 121 の更新部 209 は、ユーザに当該サーバ装置 19

1用のパスワードを入力するよう、当該コンピュータ151に求め、当該コンピュータ151から送信されたパスワードを受け付ける。

[0112] このほか、ユーザが、ユーザ名やサーバ名とあわせて、パスワードを入力してしまう態様もありうる。この場合には、認証要求に対する付加的な情報として、当該サーバ装置191に対するパスワードが付加されることになる。更新部209は、認証要求に付加されたパスワードを受け付ける。

[0113] そして、ランダム表401の生成や提示、ユーザによるキーの入力、当該ユーザの選択順序の同定は、上記実施形態と同様に行われる。

[0114] このようにしてサーバ装置191用の既存のパスワードが得られたら、当該既存のパスワードを選択順序により選択される要素の個数に分割する。分割の長さが一定とならない場合には、上記実施形態と同様に、パスワードそのものの長さを記憶部201に保持するか、パスワード内に改行文字などを埋め込んで長さを調整する。

[0115] そして、更新部209は、同定された選択順序にしたがって、パスワード表301の要素にパスワードを分割することにより得られた断片を順に格納していく。

[0116] この後、パスワード表301の選択順序に関らない各要素302に、パスワードの断片と同じ長さのランダムな文字列を生成して埋め込む。この際には、パスワードに現れた文字の種類、たとえば、英字、数字、記号等のほか、挿入された改行文字等の出現頻度に応じて、ランダムな文字列を生成することにより、パスワード表301が漏洩した場合であっても、パスワードが第三者に推定されてしまうことを防止できる。

実施例 3

[0117] 上記の通信装置121は、ユーザとサーバ名に対応付けられたパスワード表301を管理する。しかも、パスワード表301がそのまま画面に表示されたとしても、当該ユーザの当該サーバ装置191に対するパスワードが、直ちにわかってしまうことはない。当該ユーザの選択順序とパスワード表301が揃って初めて、当該サーバ装置191に対するパスワードが得られる

。

[0118] したがって、ユーザがLAN 141内のコンピュータ151から、通信装置121にアクセスし、ユーザとサーバ名に対応付けられるパスワード表301を要求した場合に、通信装置121が、

(a) 当該パスワード表301をLAN 141内のコンピュータ151に応答して、LAN 141内のコンピュータ151の画面に表示させる、あるいは、

(b) 当該ユーザに対してあらかじめ設定された携帯電話等の移動端末171等の電子メールアドレスに、パスワード表301を記載した電子メールを送信する

ことにより、いわゆるパスワード・リマインダを実現することができる。

[0119] このほか、携帯電話等の移動端末171から、ユーザとサーバ名に対応付けられるパスワード表301を要求した場合に、通信装置121は、当該携帯電話等の移動端末171の個体識別番号のチェックを行った上で、当該携帯電話等の移動端末171に対応付けられる電子メールアドレスに、パスワード表301を記載した電子メールを送信する、という態様も考えられる。

[0120] すなわち、上記実施形態においては、通信装置121からランダム表401を移動端末171に送信することとしているが、通信装置121そのものに対する認証（通常のパスワードによる認証を採用しても良いし、上記の例のように、ランダム表と選択順序を利用した認証を採用して、選択順序そのものをパスワードとしても良い。）が成功した後は、通信装置121からパスワード表301が移動端末171に送信できることとするのである。

[0121] 一般的なブラウザには、あるサイトに対するパスワードを記憶して、次のログインに備えるものがあり、このような機能を有するブラウザでは、パスワードそのものを画面に表示する機能を提供していることも多いが、本実施形態では、パスワードそのものが直接画面に表示されるわけではない。

[0122] したがって、従来よりも安全なパスワード・リマインダを実現することができる。

実施例 4

- [0123] 上記実施形態は、パスワード表 301 の要素 302 を並べた要素列が、そのままサーバ装置 191 を利用するためのパスワードとして利用されるものであった。
- [0124] 本実施形態は、ユーザに割り当てられた規則に基づいてパスワード表 301 から選んだ要素 302 を並べてできる要素列を、ワンタイムパスワード用のシードとして利用するものである。以下、まず、従来から、時刻同期型のワンタイムパスワードシステムについて説明する。
- [0125] 従来のシステムでは、各ユーザに、トークンと呼ばれる電子機器が提供される。
- [0126] トークン内には、当該ユーザに割り当てられたシードが不揮発に記録されている。一般には、シードは、文字列もしくは数字列である。
- [0127] トークンは、リアルタイムクロック等を参照して現在時刻（典型的には、特定の基準時刻からの経過時間により表現される。）を取得し、取得された現在時刻と、不揮発に記憶されたシードと、に、所定の一方向関数を適用して、文字列や数字列（今日広く利用されているシステムでは、6桁の数字列である。）を計算してワンタイムパスワードを得て、これを液晶ディスプレイに表示する。
- [0128] 一方、サーバ装置では、各ユーザに割り当てられたシードと、現在時刻と、から、当該所定の一方向関数を適用することにより、各ユーザに対するワンタイムパスワードを計算できるようになっている。
- [0129] そこで、サーバ装置は、端末装置から送られたユーザ名とワンタイムパスワードとの組み合わせが、当該ユーザ名に対するシードと現在時刻との組み合わせから計算されるワンタイムパスワードと一致するか否かによって、認証を行う。
- [0130] 本実施形態では、このようなワンタイムパスワードシステムにおいて、専用のトークンをユーザが持ち歩くのではなく、携帯電話やスマートフォン、モバイル・コンピュータ等をトークンとして利用する際に、シードが流出す

るのを防止するために本発明を適用する。

[0131] 本実施形態においては、通信装置 121 の記憶部 201 に記憶されるパスワード表 301 には、当該ユーザのシードを当該ユーザの規則に基づいた個数に分断して、当該ユーザの規則に基づいた要素に埋め込み、他の要素にはほぼ同じ長さのランダムな列を埋め込むこととする。

[0132] 通信装置 121 の受信部 202 は、ユーザからのキーボード操作やタッチパネル操作に基づく認証要求を、当該ハードウェアの電子回路の信号線経由で受け付ける。

[0133] 生成部 203 は、上記実施形態と同様にランダム表 401 を生成する。提示部 204 は、通信装置 121 が備えるディスプレイに生成されたランダム表 401 を表示する。

[0134] 受付部 205 は、ユーザからのキーボード操作やタッチパネル操作に基づいて入力されたキーを受け付け、同定部 206 は、当該ランダム表 401 と当該キーに基づいて、当該ユーザの変換規則を同定する。

[0135] 取得部 207 は、当該ユーザの変換規則に基づいて、パスワード表 301 から要素を順に取り出して並べることにより、シードを得る。さらに、取得部 207 は、リアルタイムクロック等を参照して、現在の時刻を得る。そして、取得部 207 は、シードと現在時刻に所定の一方向関数を適用して当該ユーザ用のワンタイムパスワードを計算する。

[0136] 出力部 208 は、計算されたワンタイムパスワードをディスプレイに表示する。なお、この他の構成は、上記実施形態と同様とすることができる。

[0137] LAN 141 のルータ装置などを本発明の通信装置 121 として利用する際にも、同様に、このような時刻同期型ワンタイムパスワードシステムに、本発明を適用することが可能である。

[0138] 本実施形態は、上記実施形態におけるユーザのパスワードとして、ワンタイムパスワードのシードを利用するものと考えることができる。本実施形態においても、上記実施例と同様に、従来のワンタイムパスワードシステムのサーバ装置をそのまま利用することが可能である。

実施例 5

- [0139] 上記の各通信装置 1 2 1 は、通信機能を備えるコンピュータにより実現が可能であるが、パスワード・リマインダとして機能させる場合には、必ずしも通信機能を備える必要はない。すなわち、インターネット 1 6 1 への接続ができないような状況下であっても、コンピュータ 1 5 1 や移動端末 1 7 1、端末装置 1 8 1 等において所定のプログラムを動作させることにより、パスワード・リマインダとして機能させることが可能である。
- [0140] ここで、パスワードやシードは、第三者に秘密にすべき情報である。したがって、上記実施例におけるパスワード・リマインダは、より一般的に、秘密情報のリマインダと考えることが可能である。
- [0141] すなわち、秘密情報を複数の断片に分割し、これらをパスワード表 3 0 1 に格納することにより、種々の秘密情報のリマインダ装置として機能させることが可能である。本態様のパスワード表 3 0 1 は、上記態様と同様の構成を持つが、パスワードを含む各種の秘密情報の断片が埋め込まれた秘密情報表として機能する。
- [0142] 本実施形態のリマインダ装置において、複数の種類の秘密情報を記憶させる場合には、受信部 2 0 2 によりユーザから受け付けられた情報に基づいて必要な秘密情報の種類を識別する。すなわち、本態様のリマインダ装置は、受信部 2 0 2 において、サーバ名にかえて、秘密情報の種類の名称をユーザに入力させる。
- [0143] また、秘密情報が 1 種類に限られる場合には、受信部 2 0 2 を省略することも可能である。この場合には、定期的に、あるいは、ユーザからの指示に基づいて、生成部 2 0 3 によるランダム表の生成が行われる。
- [0144] 出力部 2 0 8 による出力は、液晶ディスプレイへの表示のほか、当該リマインダ装置として機能するコンピュータにおける各種の認証機能に、秘密情報をパスワードとして自動的に与えることとしても良いし、通信機能を介して外部のサーバ装置に秘密情報を与えることとしても良い。
- [0145] 秘密情報としては、パスワードやシードのほか、ユーザの社会保証番号や

保険証番号、クレジットカード番号、銀行口座番号など、種々のものをリニアインク装置に記憶させることが可能である。これらの秘密情報は、単純に分断して秘密情報表（パスワード表301）に格納することとしても良いし、秘密情報を暗号化して別途記憶し、暗号化された秘密情報を復号するための鍵を秘密情報表（パスワード表301）に格納する形態を採用することもできる。

[0146] なお、上記の通信装置121やリニアインク装置におけるキーは、より一般には、ユーザがパスワード表301や秘密情報表の要素を選択する選択順序に対応付けられる情報と考えることができる。すなわち、キーから選択順序が一意に導出できるのであれば、必ずしもランダム表401を利用する必要はない。

[0147] たとえば、画面にパスワード表301をそのまま表示する態様を採用することも可能である。また、ランダム表401における各要素が、常に固定されているような態様を採用することもできる。

[0148] 本願においては、2010年8月31日出願の日本国特許出願特願2010-194234に基づく優先権を主張するものとし、指定国の法令が許す限り、当該基礎出願の内容をすべて本願に取り込むものとする。

産業上の利用可能性

[0149] 本発明によれば、サーバ装置を利用するためのパスワード等の秘密情報を安全に管理するのに好適な通信装置、リニアインク装置、ならびに、これをコンピュータにより実現するためのプログラムを記録した非一時的な情報記録媒体を提供することができる。

符号の説明

[0150] 101 通信システム
121 通信装置
141 LAN
151 LAN内のコンピュータ
161 インターネット

- 1 7 1 移動端末
- 1 8 1 端末装置
- 1 9 1 サーバ装置
- 2 0 1 記憶部
- 2 0 2 受信部
- 2 0 3 生成部
- 2 0 4 提示部
- 2 0 5 受付部
- 2 0 6 同定部
- 2 0 7 取得部
- 2 0 8 出力部
- 2 0 9 更新部
- 3 0 1 パスワード表
- 3 0 2 パスワード表の要素
- 4 0 1 ランダム表
- 4 0 2 ランダム表の要素

請求の範囲

- [請求項1] サーバ名と、所定の行数ならびに所定の列数のパスワード表と、が、対応付けられて記憶される記憶部、
- サーバ名を指定する認証要求を受信する受信部、
- 前記所定の行数ならびに前記所定の列数のランダム表を生成する生成部、
- 前記生成されたランダム表を、ユーザに提示する提示部、
- 前記提示されたランダム表の要素を前記ユーザに対応付けられる選択順序で選択して並べることにより得られるキーを、当該ユーザから受け付ける受付部、
- 前記受け付けられたキーと、前記生成されたランダム表と、から、前記ユーザに対応付けられる選択順序を同定する同定部、
- 前記認証要求に指定されたサーバ名に対応付けて前記記憶部に記憶されるパスワード表から、当該パスワード表に含まれる要素を前記同定された選択順序で選択して並べることにより得られる要素列から、パスワードを取得する取得部、
- 前記認証要求に指定されたサーバ名のサーバ装置を前記ユーザが利用できるようにするためのパスワードとして、前記取得されたパスワードを出力する出力部
- を備えることを特徴とする通信装置。
- [請求項2] 請求項1に記載の通信装置であって、
- 前記認証要求に指定されるサーバ名のサーバ装置は、時刻同期型ワントタイムパスワードにより、前記ユーザが当該サーバ装置を利用できるか否かを判定し、
- 前記取得部は、前記得られた要素列からなるシードと、現在の時刻と、に、所定の一方方向性関数を適用した結果を、前記パスワードとして取得する
- ことを特徴とする通信装置。

- [請求項3] 請求項 1 に記載の通信装置であって、
前記取得部は、前記得られた要素列を前記パスワードとして取得する
ことを特徴とする通信装置。
- [請求項4] 請求項 1 に記載の通信装置であって、
前記出力部は、前記ユーザに対して前記取得されたパスワードを表示することにより、前記取得されたパスワードを出力する
ことを特徴とする通信装置。
- [請求項5] 請求項 1 に記載の通信装置であって、
前記出力部は、前記取得されたパスワードを指定する利用要求を、
前記認証要求に指定されたサーバ名のサーバ装置に送信することにより、前記取得されたパスワードを出力する
ことを特徴とする通信装置。
- [請求項6] 請求項 5 に記載の通信装置であって、
前記受信部は、前記認証要求を、前記ユーザが利用する第 1 の端末から受信し、
前記提示部は、前記生成されたランダム表を、前記ユーザが利用する第 2 の端末に提示し、
前記受付部は、前記キーを、前記第 1 の端末から受け付け、
前記出力部は、前記ユーザが前記第 1 の端末により前記サーバ装置を利用できるようにするため、前記利用要求を送信する
ことを特徴とする通信装置。
- [請求項7] 請求項 5 に記載の通信装置であって、
前記受信部は、前記認証要求を、前記ユーザが利用する第 1 の端末から受信し、
前記提示部は、前記生成されたランダム表を、前記ユーザが利用する第 1 の端末に提示し、
前記受付部は、前記キーを、第 2 の端末から受け付け、

前記出力部は、前記ユーザが前記第 1 の端末により前記サーバ装置を利用できるようにするため、前記利用要求を送信することを特徴とする通信装置。

[請求項 8]

請求項 5 に記載の通信装置であって、

前記認証要求に指定されたサーバ名に対応付けられるパスワード表が前記記憶部に記憶されていない場合、前記所定の行数ならびに前記所定の列数の新たなパスワード表を生成し、当該新たなパスワード表の各要素をランダムに定めて、当該サーバ名に対応付けて、当該新たなパスワード表を前記記憶部に記憶させることにより、前記記憶部を更新する更新部

をさらに備え、

前記出力部が前記利用要求を前記認証要求に指定されたサーバ名のサーバ装置に送信することにより、当該ユーザを当該サーバ装置に登録する

ことを特徴とする通信装置。

[請求項 9]

請求項 1 に記載の通信装置であって、

前記認証要求に指定されたサーバ名に対応付けられるパスワード表が前記記憶部に記憶されていない場合、前記所定の行数ならびに前記所定の列数の新たなパスワード表を生成し、前記ユーザからパスワードの入力を受け付け、当該受け付けられたパスワードを分割して当該新たなパスワード表の前記同定された選択順序の要素に順に格納し、それ以外の要素をランダムに定めて、当該サーバ名に対応付けて、当該新たなパスワード表を前記記憶部に記憶させることにより、前記記憶部を更新する更新部

をさらに備えることを特徴とする通信装置。

[請求項 10]

コンピュータを、請求項 1 に記載の通信装置の各部として機能させることを特徴とするプログラムを記録したコンピュータ読取可能な非一時的情報記録媒体。

- [請求項11] 所定の行数ならびに所定の列数の秘密情報表が、記憶される記憶部、
- 、
- 前記所定の行数ならびに前記所定の列数のランダム表を生成する生成部、
- 前記生成されたランダム表を、ユーザに提示する提示部、
- 前記提示されたランダム表の要素を前記ユーザに対応付けられる選択順序で選択して並べることにより得られるキーを、当該ユーザから受け付ける受付部、
- 前記受け付けられたキーと、前記生成されたランダム表と、から、
- 前記ユーザに対応付けられる選択順序を同定する同定部、
- 前記記憶部に記憶される秘密情報表から、当該秘密情報表に含まれる要素を前記同定された選択順序で選択して並べることにより得られる要素列から、秘密情報を取得する取得部、
- 前記取得された秘密情報を出力する出力部
- を備えることを特徴とするリマインダ装置。
- [請求項12] 所定の行数ならびに所定の列数の秘密情報表が、記憶される記憶部、
- 、
- 前記秘密情報表の要素を選択する選択順序に対応付けられるキーを、ユーザから受け付ける受付部、
- 前記受け付けられたキーから、前記ユーザに対応付けられる選択順序を同定する同定部、
- 前記記憶部に記憶される秘密情報表から、当該秘密情報表に含まれる要素を前記同定された選択順序で選択して並べることにより得られる要素列から、秘密情報を取得する取得部、
- 前記取得された秘密情報を出力する出力部
- を備えることを特徴とするリマインダ装置。