(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5260533号
(P5260533)
(45)発行日　平成25年8月14日(2013.8.14)　(24)登録日　平成25年5月2日(2013.5.2)

(51)Int.Cl.　　F I
G06F 21/31 (2013.01)　　G06F 21/20 131A
H04L 9/32 (2006.01)　　G06F 21/20 131D
　　H04L 9/00 673A

請求項の数 39　(全 25 頁)

(21)出願番号　特願2009-534797 (P2009-534797)
(86)(22)出願日　平成19年10月22日 (2007.10.22)
(65)公表番号　特表2010-517121 (P2010-517121A)
(43)公表日　平成22年5月20日 (2010.5.20)
(86)国際出願番号　PCT/US2007/082088
(87)国際公開番号　WO2008/051905
(87)国際公開日　平成20年5月2日 (2008.5.2)
審査請求日　平成22年10月20日 (2010.10.20)
(31)優先権主張番号　11/552,555
(32)優先日　平成18年10月25日 (2006.10.25)
(33)優先権主張国　米国 (US)

(73)特許権者　509119902
サイファーロック　テクノロジー　コーポレーション
アメリカ合衆国　コネチカット州　０６８２４　フェアフィールド　サードフロア　ポストロード　１２６１
(73)特許権者　310009867
シター　ポール
アメリカ合衆国　コネチカット州　０６４６８　モンロー　ジョッキーホロウロード　６３

最終頁に続く

(54)【発明の名称】ユーザ認証システム及びその方法

(57)【特許請求の範囲】
【請求項１】
デバイス、サービス、アプリケーション、機能、またはシステムにユーザがアクセスするのを認証する方法であって、
認証システムによって提供される一組の変数及び演算子から選択されるユーザ式として認証キーを生成するステップと、
前記ユーザ式を前記認証システムに保存するステップと、
前記認証システムによって生成された変数の配列を前記ユーザに提示するディスプレイを利用するステップと、
を含み、
前記変数の配列は、各々に値が割り当てられている前記ユーザ式の前記変数を含んでいて、
前記方法は更に、
前記ユーザ式の一致している変数に前記割り当てられた値を当てはめて第１の結果を計算するステップと、
前記第１の結果の複数のキャラクタの中に１つ以上の付加キャラクタを加えるステップと、
前記付加キャラクタを有する前記第１の結果を前記認証システムに伝えるステップと、
を含み、
前記認証システムによって計算される前記ユーザ式の別個で独自の計算の第２の結果が

、前記付加キャラクタを有する第１の結果において見出されかつ前記付加キャラクタが一組の指定制限事項を満たしている場合に、前記認証システムは前記ユーザを認証することを特徴とする方法。
【請求項２】
前記一組の指定制限事項は無効であることを特徴とする請求項１記載の方法。
【請求項３】
前記認証システムによって生成された前記変数の配列は、前記ユーザのためにカスタマイズされていることを特徴とする請求項１記載の方法。
【請求項４】
前記変数は、任意の英数字、キャラクタ、マーク、シンボル、記号、または画像を含むことを特徴とする請求項１記載の方法。
【請求項５】
前記値は、ランダムに生成された数値を含むことを特徴とする請求項１記載の方法。
【請求項６】
ユーザ式をつくる際の支援を前記ユーザに提供するステップ含むことを特徴とする請求項１記載の方法。
【請求項７】
前記ユーザ式は、１つ以上のカスタム演算子を含むことを特徴とする請求項１記載の方法。
【請求項８】
前記第１の結果を受け取るための変数を有するローカル式と前記ユーザ式を有するリモート式とを生成するステップと、
前記ローカル式の計算が前記リモート式の計算に一致する場合に前記ユーザを認証するステップと、
を含むことを特徴とする請求項１記載の方法。
【請求項９】
前記ローカル式はトランスポート可能であることを特徴とする請求項８記載の方法。
【請求項１０】
前記ローカル式の前記計算は、ローカルコンピュータデバイスによって行われ、前記リモート式の前記計算は、前記ローカルコンピュータデバイスから離隔した制御装置によって行なわれることを特徴とする請求項８記載の方法。
【請求項１１】
請求項１記載の認証セッションを開始するラッパーを提供するステップと、
前記ラッパー内にデータとともにメッセージを封入するステップと、
前記メッセージを開封する試みがあると、メッセージ受信者に対する第１の認証セッションとメッセージ送信者に対する第２の認証セッションとを開始するステップと、
前記第２の認証セッションから得られるユーザ式を判断するステップと、
前記第１の認証セッションに当該結果を与えるステップと、
認証があると、前記受取人が前記メッセージ及びデータにアクセスすることを認めるステップと、
をさらに含むことを特徴とする請求項１記載の方法。
【請求項１２】
デバイス、サービス、アプリケーション、機能、またはシステムにユーザがアクセスするのを認証する認証システムであって、
前記認証システムによって提供されかつ前記認証システムに保存されている一組の変数及び演算子から選択されるユーザ式としての認証キーと、
前記認証システムによって生成された変数の配列を前記ユーザに提示するディスプレイと、
を含み、
前記変数の配列は、各々に値が割り当てられている前記ユーザ式の前記変数を含み、

前記認証システムは更に、
前記割り当てられた値を前記ユーザ式の一致している変数に当てはめた第１の結果を含み、
前記第１の結果は、１つ以上の加えられた付加キャラクタを含み、前記認証システムに伝えられ、
前記認証システムは更に、
前記認証システム内に回路を含み、
前記回路は、前記認証システムによって計算される前記ユーザ式の別個で独自の計算の第２の結果が、前記付加キャラクタを有する前記第１の結果において見出され、前記付加キャラクタが一組の指定制限事項を満たしている場合に、前記ユーザを認証することを特徴とするシステム。
【請求項１３】
デバイス、サービス、アプリケーション、機能、またはシステムにユーザがアクセスするのを認証する方法であって、
認証システムによって提供される変数及び演算子を有するユーザ式として認証キーを生成するステップと、
前記ユーザ式を前記認証システムに保存するステップと、
変数及び値の配列を前記ユーザに提示するディスプレイを利用するステップと、
を含み、
前記変数及び値の配列は、前記ユーザ式の変数と各変数に付随する前記配列の特定の位置の値とを含んでいて、
前記方法は更に、
前記配列の前記変数に付随する前記特定の位置の前記値を前記ユーザ式の一致している変数に当てはめて第１の結果を計算するステップと、
前記第１の結果を前記認証システムに伝えるステップと、
を含み、
前記第１の結果が前記認証システムによって計算された前記ユーザ式の別個で独自の計算の第２の結果に一致する場合に、前記認証システムは前記ユーザを認証することを特徴とする方法。
【請求項１４】
各変数に付随する前記特定の位置は、前記ユーザ式に含まれることを特徴とする請求項１３記載の方法。
【請求項１５】
各変数に付随する前記特定の位置は、ユーザプロファイルに含まれることを特徴とする請求項１３記載の方法。
【請求項１６】
前記認証システムによって生成される前記変数の配列は、前記ユーザのためにカスタマイズされることを特徴とする請求項１３記載の方法。
【請求項１７】
前記変数は、任意の英数字、マーク、シンボル、記号、または画像を含むことを特徴とする請求項１３記載の方法。
【請求項１８】
前記値はランダムに生成された数値を含むことを特徴とする請求項１３記載の方法。
【請求項１９】
ユーザ式を生成する際の支援を前記ユーザに提供するステップを含むことを特徴とする請求項１３記載の方法。
【請求項２０】
前記ユーザ式は、１つ以上のカスタム演算子を含むことを特徴とする請求項１３記載の方法。
【請求項２１】

前記第１の結果を受け取るための変数を有するローカル式と前記ユーザ式を有するリモート式とを生成するステップと、
前記ローカル式の計算が前記リモート式の計算に一致する場合に前記ユーザを認証するステップと、
を含むことを特徴とする請求項１３記載の方法。
【請求項２２】
前記ローカル式はトランスポート可能であることを特徴とする請求項２１記載の方法。
【請求項２３】
前記ローカル式の前記計算は、ローカルコンピュータデバイスによって行われ、前記リモート式の前記計算は、前記ローカルコンピュータデバイスから離隔した制御装置によって行われることを特徴とする請求項２１記載の方法。
【請求項２４】
請求項１３記載の認証セッションを開始するラッパーを提供するステップと、
前記ラッパー内にデータとともにメッセージを封入するステップと、
メッセージを開封する試みがあると、メッセージ受信者に対する第１の認証セッションとメッセージ送信者に対する第２の認証セッションとを開始するステップと、
前記第２の認証セッションから得られるユーザ式を判断するステップと、
前記第１の認証セッションに当該結果を与えるステップと、
認証があると、前記メッセージ及びデータに前記受取人がアクセスすることを認めるステップと、
を更に含むことを特徴とする請求項１３記載の方法。
【請求項２５】
デバイス、サービス、アプリケーション、機能、またはシステムにユーザがアクセスするのを認証する認証システムであって、
前記認証システムによって提供されかつ前記認証システムに保存されている変数及び演算子を有するユーザ式としての認証キーと、
変数及び値の配列を前記ユーザに提示するディスプレイと、
を含み、
前記変数及び値の配列は、前記ユーザ式内の変数と各変数に付随している前記配列の特定の位置の値とを含み、
前記認証システムは更に、
前記配列内の前記変数に付随する前記特定の位置の前記値を前記ユーザ式の一致している変数に当てはめた第１の結果を含み、
前記第１の結果は前記認証システムへ伝えられ、
前記認証システムは更に、
前記第１の結果が前記認証システムによって計算された前記ユーザ式の別個で独自の計算の第２の結果と一致する場合に、前記ユーザを認証する前記認証システム内の回路を含むことを特徴とするシステム。
【請求項２６】
デバイス、サービス、アプリケーション、機能、またはシステムにユーザがアクセスするのを認証する方法であって、
認証システムによって提供される変数及び演算子を有するユーザ式として認証キーを生成するステップと、
前記ユーザ式を前記認証システムに保存するステップと、
変数及び値の配列を前記ユーザに提示するディスプレイを利用するステップと、
を含み、
前記変数及び値の配列は、前記ユーザ式の変数と各変数に付随している前記配列の特定の位置の値とを含み、
前記方法は、
前記配列内の前記変数に付随する前記特定の位置の前記値を、前記ユーザ式の一致して

いる変数に当てはめて第１の結果を計算するステップと、
１つ以上の付加キャラクタを前記第１の結果の複数のキャラクタの中に加えるステップと、
前記付加キャラクタを有する前記第１の結果を前記認証システムに伝えるステップと、
を含み、
前記認証システムによって計算される前記ユーザ式の別個で独自の計算の第２の結果が、前記付加キャラクタを有する前記第１の結果において見出されかつ前記付加キャラクタが一組の指定制限事項を満たしている場合、前記認証システムは前記ユーザを認証することを特徴とする方法。
【請求項２７】
前記一組の指定制限事項は無効であることを特徴とする請求項２６記載の方法。
【請求項２８】
各変数に付随する前記特定の位置は、前記ユーザ式に含まれることを特徴とする請求項２６記載の方法。
【請求項２９】
各変数に付随する前記特定の位置は、ユーザプロファイルに含まれることを特徴とする請求項２６記載の方法。
【請求項３０】
前記認証システムによって生成される前記変数の配列は、前記ユーザのためにカスタマイズされることを特徴とする請求項２６記載の方法。
【請求項３１】
前記変数は、任意の英数字、マーク、シンボル、記号、または画像を含むことを特徴とする請求項２６記載の方法。
【請求項３２】
前記値はランダムに生成された数値を含むことを特徴とする請求項２６記載の方法。
【請求項３３】
前記ユーザにユーザ式を生成する際の支援を提供するステップを含むことを特徴とする請求項２６記載の方法。
【請求項３４】
前記ユーザ式は、１つ以上のカスタム演算子を含むことを特徴とする請求項２６記載の方法。
【請求項３５】
前記第１の結果を受け取るための変数を有するローカル式と前記ユーザ式を有するリモート式とを生成するステップと、
前記ローカル式の計算が前記リモート式の計算に一致する場合に前記ユーザを認証するステップと、
を含むことを特徴とする請求項２６記載の方法。
【請求項３６】
前記ローカル式はトランスポート可能であることを特徴とする請求項２６記載の方法。
【請求項３７】
前記ローカル式の前記計算は、ローカルコンピュータデバイスによって行われ、前記リモート式の前記計算は、前記ローカルコンピュータデバイスから離隔した制御装置によって行われることを特徴とする請求項３５記載の方法。
【請求項３８】
請求項２６記載の認証セッションを開始するラッパーを提供するステップと、
前記ラッパー内にデータとともにメッセージを封入するステップと、
前記メッセージを開封する試みがあると、メッセージ受信者に対する第１の認証セッションとメッセージ送信者に対する第２の認証セッションとを開始するステップと、
前記第２の認証セッションから得られるユーザ式を判断するステップと、
前記第１の認証セッションに当該結果を提供するステップと、

認証があると、前記メッセージ及びデータに前記受信者がアクセスするのを認めるステップと、
を更に含むことを特徴とする請求項２６記載の方法。
【請求項３９】
デバイス、サービス、アプリケーション、機能、またはシステムにユーザがアクセスするのを認証する認証システムであって、
前記認証システムによって提供されかつ前記認証システムに保存されている変数及び演算子を有するユーザ式としての認証キーと、
変数及び値の配列を前記ユーザに提示するディスプレイと、
を含み、
前記変数及び値の配列は、前記ユーザ式の変数と各変数に付随する前記配列の特定の位置の値とを含み、
前記認証システムは更に、
前記配列内の前記変数に付随する前記特定の位置の前記値を前記ユーザ式の一致している変数に当てはめた第１の結果を含み、
前記第１の結果は、１つ以上の加えられた付加キャラクタを含み、前記認証システムに伝えられ、
前記認証システムは更に、
前記認証システム内に回路を含み、
前記回路は、前記認証システムによって計算された前記ユーザ式の別個で独自の計算の第２の結果が、前記付加キャラクタを有する前記第１の結果において見出されかつ前記付加キャラクタが一組の指定制限事項を満たしている場合に、前記ユーザを認証することを特徴とするシステム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、データの安全保護に関し、特に、ユーザの認証に関する。
【背景技術】
【０００２】
コンピュータシステムは、ユーザに対して様々なアプリケーションまたはサービスを提供できる。一般に、システムへのアクセスは、許可されたユーザに限られているかもしれない。ユーザの認証についての一例として、ユーザがユーザ名及びパスワードを入力することを求められるログインプロセスがあげられる。
【０００３】
技術の新たな進展にも関わらず、ユーザ名とパスワードとの組合せは、依然として最も一般的なアクセス制御手段のうちの１つである。しかしながら、パスワードは不利であるかもしれない。なんとなれば、容易に記憶されるパスワードは割り出すのが極めて容易であり、複雑で割り出すのに難しいものは容易に忘れられるからである。
【０００４】
この種のシステムの完全な状態は、概して、パスワードを秘密にしておくことに基づいている。しかしながら、パスワードを割り出す多くの公知の方法がある。公知の方法には、推測すること、一般的なパスワードまたは全ての知られている言葉についての辞書を用いること、文字・記号（キャラクタ）の全ての組合せを用いることを含むしらみつぶしの試み、サーバとやり取りしている間にパスワードに関してネットワークトラフィックを監視すること、「ショルダーサーフィン」（ログインの間にユーザの肩越しに見ること）、キーロギング（ログインの間にユーザのキー入力を記憶するかまたは伝えること）、その他を含む。
【０００５】
この種の攻撃に対する公知の防御策は、パスワードをより長くして推測するのをより難しくすることと、辞書の適用及びしらみつぶしの技術をより難しくすることとを含む。他

の防御策は、例えばユーザに関係のある名前、電話番号、生年月日、その他などの「意味がある」パスワードの使用を禁止すること、ユーザがパスワードを入力するときにアスタリスクなどの意味のないキャラクタを表示してショルダーサーファーにアスタリスクだけが見えるようにすること、ネットワークを介してパスワードを送信する前にパスワードを暗号化してネットワーク監視による探知を防ぐこと、を含む。

【０００６】

アクセス制御及び認証の１つの方法は、ワンタイムパスワード（ＯＴＰ）の使用である。ユーザはログインするたびに異なるパスワードを使用し、よって、上述の攻撃技術の多くを役に立たない状態にする。パスワードを傍受し、キーロギングし、そうでなければ割り出すことは、何らの効果ももたらさない。なんとなれば、取得されたパスワードを再び用いることができないからである。

【０００７】

最も一般的に利用可能なＯＴＰシステムは、多かれ少なかれ同じプロトコルを共有する。ログインプロセスの一部として、サーバはユーザにいわゆるチャレンジを送出する。いわゆるチャレンジは単に大きい乱数であってもよい。ユーザは、例えばＯＴＰを生成する特別な物理的な機器またはソフトウェアなどのＯＴＰ生成器に、この数を入力する。ユーザは該ＯＴＰを入力する。サーバも同様に、それ自体のＯＴＰ生成器に該チャレンジを入力する。サーバのＯＴＰとユーザのＯＴＰが一致すれば、ユーザは認証される。

【０００８】

ＯＴＰ生成器が物理的な機器（例えばスマートカード、トークン、バイオメトリック装置、その他）であるという点で、失われ、壊れ、または盗まれたＯＴＰ生成器についてのコスト及び不便さが関心事となるかもしれない。

【０００９】

パスワード生成アルゴリズムが全てのユーザに対して同じものである例では、各ユーザは、結果を一意のものにするために秘密のキーを割り当てられる。このキーは、通常、ユーザのＯＴＰ生成器に埋め込まれ、サーバのデータベースにも記憶される。このＯＴＰ生成スキームにはいくつかのバリエーションがある。例えば、時刻がチャレンジの代わりに用いられてユーザとサーバとを同期させてもよい。ほとんどの場合、安全確保はユーザの秘密のキーの完全性に依存する。キーの情報が漏洩されると、システムは無効になる。その結果、パスワードのように、最もよく知られているものの１つであるしらみつぶしを用いて、キーは様々な種類の攻撃の対象となる。安全確保のさらなる層が、ＯＴＰを計算するアルゴリズムを保護することにより提供されているが、アルゴリズムは執拗に割り出されて信頼できる安全確保の要素でない。

【００１０】

ネットワーク環境において、通常、サーバは様々なサービス及びアプリケーションを、ネットワークで結ばれた多数のユーザへ提供する。サーバは、特定のサービスまたはアプリケーションの使用を適切に許可するために動作してユーザを確かめる。通常、これは上記した標準のログインプロセスによって実施される。サーバはその時入力されたユーザ名及びパスワードを記憶されたユーザ名及びパスワードと照合する。

【発明の開示】

【発明が解決しようとする課題】

【００１１】

辞書アプリケーション、しらみつぶし攻撃、トラフィック監視、ショルダーサーフィン、キーロギング、及び様々な他の種類の攻撃に強固であって耐え得る認証システムを提供することが有利である。

【課題を解決するための手段】

【００１２】

１つの実施形態において、デバイス、サービス、アプリケーション、機能、またはシステムへのユーザのアクセスを認証する方法は、認証システムによって提供される一組の変数及び演算子から選択されてユーザ式として認証キーを生成するステップと、認証システ

ムにユーザ式を保存するステップと、各々に値が割り当てられているユーザ式の複数の変数を含んでいて認証システムによって生成された変数の配列をユーザに示すディスプレイを利用するステップと、を含む。該方法はまた、割り当てられた値をユーザ式の一致している変数に当てはめて第１の結果を計算するステップと、第１の結果の複数のキャラクタの中に１つ以上の付加キャラクタを加えるステップと、付加キャラクタを有する第１の結果を認証システムに伝えるステップと、を含み、第１の結果とともに伝えられた付加キャラクタの数が予め定められた閾値未満であって、かつ認証システムによって計算されたユーザ式とは別個で独自の計算の第２の結果に第１の結果が一致する場合に、認証システムはユーザを認証する。

【００１３】

別の実施形態では、デバイス、サービス、アプリケーション、機能、またはシステムにユーザがアクセスするのを認証する方法は、認証システムによって提供される変数及び演算を有するユーザ式として認証キーを生成するステップと、ユーザ式を認証システムに保存するステップと、各変数に付随する配列の特定の位置におけるユーザ式及び値における変数を含む変数及び値の配列をユーザに示すディスプレイを利用するステップと、を含む。該方法はまた、配列内の変数に付随する特定の位置における値をユーザ式の一致している変数に当てはめて第１の結果を計算するステップと、第１の結果を認証システムへ伝えるステップと、を含み、第１の結果が認証システムによって計算されたユーザ式の別個で独自の計算の第２の結果に一致する場合に、認証システムはユーザを認証する。

【００１４】

また別の実施形態では、デバイス、サービス、アプリケーション、機能またはシステムへユーザがアクセスするのを認証する方法は、認証システムによって提供される変数及び演算を有するユーザ式として認証キーを生成するステップと、認証システムにユーザ式を保存するステップと、ユーザ式の変数及び各変数に付随する配列の特定の位置の値を含む変数及び値の配列をユーザに示すディスプレイを利用するステップと、を含む。該方法はまた、配列内の変数に付随する特定の位置の値をユーザ式の一致している変数に当てはめて第１の結果を計算するステップと、第１の結果のキャラクタの中に１つ以上の付加キャラクタを加えるステップと、付加キャラクタとともに第１の結果を認証システムに伝えるステップと、を含み、第１の結果とともに伝えられた付加キャラクタの数が予め定められた閾値未満であって、第１の結果が認証システムによって計算されるユーザ式の別個で独自の計算の第２の結果に一致する場合、認証システムはユーザを認証する。

【００１５】

本実施形態の前述の態様及び他の特徴は、添付の図面に関連して成される以下の記述において説明される。

【図面の簡単な説明】

【００１６】

【図１】開示された実施形態によるユーザ認証システムの一例を示す図である。

【図２】本認証システムに付随する演算子のフローチャートを示す図である。

【図３】ユーザ認証システムとともに用いるユーザインタフェース画面の例を示す図である。

【図４】ユーザ認証システムとともに用いる管理画面の例を示す図である。

【図５】企業ネットワークにおいて実施される開示された実施形態を示す図である。

【図６】電子商取り引きまたはｅコマース用分散型システムにおける別の実施形態を示す図である。

【図７】メッセージによって送信されるデータを保護する実施形態を示す図である。

【図８】例示的なメッセージのブロック図を示す図である。

【図９】ユーザ認証システムとともに用いるユーザインタフェーススクリーンの別の例を示す図である。

【図１０】目標位置を利用する実施形態を示すフローチャートである。

【図１１】目標位置を利用する別の実施形態を示すフローチャートである。

【図１２】デコイキャラクタを利用する実施形態を示すフローチャートである。
【発明を実施するための形態】
【００１７】
図１は、開示した実施形態の特徴を包含するユーザ認証システム１００を示す。本実施形態は図面を参照して説明されるが、本実施形態は、多くの代替形式及び要素もしくは構成要素のいかなる適切なサイズ、形状、または種類を含んでもよいということが理解されなければならない。
【００１８】
図１に示すように、システム１００は、この例ではユーザインタフェース１１０で示されるユーザインタフェース機能と、この例では制御装置１１５で示される認証制御機能とを含む。
【００１９】
本発明は、ユーザ式として認証キーを生成するステップを含む。認証セッションが開始されると、ユーザは、各々が値を割り当てられている変数の配列を提示される。ユーザは、提示された変数に付随する値をユーザ式の一致している変数に当てはめて、結果を入力する。
【００２０】
図２のフローチャートを参照してさらに詳細に説明すると、ブロック３１０に示されるようにユーザ式が生成される。ユーザ式は、一組の変数及び演算子からユーザによって構築されてもよい。認証システムがアプリケーションを提供し、選択用の変数及び演算子のリストを提供することによってユーザを支援してもよい。認証システムは、また、ユーザのために自動的にユーザ式を生成できるアプリケーションを提供してもよい。得られる式は、ブロック３１５に示すように、通常、ユーザによって記憶され、認証システムによって保存される。
【００２１】
ユーザが、デバイス、サービス、アプリケーション、または機能へのアクセスを要求し、ブロック３２０に示すようにそのとき認証セッションが開始されてもよい。認証セッションが開始されると、認証システムはブロック３２５に示すように、各々に値が割り当てられている変数の配列をユーザに提示する。ユーザは、ユーザ式の変数に一致していて配列に示された変数を識別する。次にユーザは、ブロック３３０に示すように変数に割り当てられた値をユーザ式に当てはめ、ブロック３３５に示すように結果を入力する。
【００２２】
値は、ランダムに生成されて変数に割り当てられてもよく、通常各認証セッションとともに変化してもよい。認証システムは、変数に割り当てられた値を独自にユーザ式に当てはめて、ブロック３４０に示すように独自の結果を生成する。認証システムは、ブロック３４５に示すように独自の結果を入力された結果と比較する。結果が一致する場合、認証システムはユーザにサービスまたはアプリケーションへのアクセスの権利を与える（ブロック３５０）。結果が一致しない場合、アクセスが拒否される（ブロック３５５）。
【００２３】
例えば、ユーザは以下のユーザ式を構築してもよい。即ち、３＊（２＊Ｑ＋３＊Ｔ）を構成してもよい。認証セッションの間、変数及び値の配列が、ユーザに提示される。配列の変数Ｑが値３２を割り当てられ、配列の変数Ｔが値９を割り当てられると、ユーザ式は、３＊（２＊３２ ＋３＊９）、即ち数２７３を生じる。次にユーザは、数２７３を入力する。認証システムは変数及び値の配列を生成してユーザ式を保存したので、認証システムはユーザ式を用いて同じ計算をする。結果が一致すれば、ユーザは認証される。
【００２４】
上記した認証セッションに加えて、システム１００は、認証システムの一部として管理プロセスを提供してもよい。認証セッションは、上記したようなデバイス、サービス、アプリケーション、または機能へアクセスするためにユーザに資格を与えるステップを含む。通常、管理プロセスはユーザに、ユーザが式を設定することができるツールを提供し、

次の認証セッションのための式を記録する。さらに、例えばスペース及びディレクトリの割り当て、暗号化プロセス、プログラム間通信、その他などの他の設定プロセス及び管理プロセスを取り扱う。

【００２５】

上記したように、認証セッションの一部として、変数の配列が、ユーザに提示されてもよい。配列例が、図３に示される。この例では、配列３６０は、格子３６５、ユーザ名を入力する領域３７０及び、本発明によるユーザ式を当てはめた結果であるパスワードを入力する領域３７５を含む。格子３６５はセル３８０で構成されていて、各セルはユーザ式変数を表す文字または文字の組合せ３８５により示されてもよい。各変数は、値３９０を割り当てられる。上記したように、各変数に割り当てられた値は、配列がユーザに提示される度に変化してもよい。１つの実施形態では、各々の値は、配列が提示される度に、乱数生成器によって生成される。

【００２６】

上述した例示的な式３＊（２＊Ｑ＋３＊Ｔ）を用いると、ユーザは配列３６０を調べ、変数Ｑが６９という値を割り当てられていて、変数Ｔが４９という変数を割り当てられているとわかる。ユーザは、式に当てはめて、結果を入力する。

【００２７】

この例では、各セルは２つの構成要素、即ち変数及び値を含む。変数が文字に関連して記載されていて、値が数に関連して記載されているが、変数及び値は認識可能ないかなるマーク、シンボル、記号、または画像として示されてもよいということが理解されるべきである。

【００２８】

また、この例では、変数の配列が１０×１０のセル格子として示されている。しかしながら、配列はいかなる形であってもよく、いかなる数のセルまたは位置を含んでいてもよい。

【００２９】

ユーザ式が、例えば、足し算、引き算、乗算、除算、累乗、最大値、最小値、絶対値、連結、その他といった、いかなる数学的演算及び非数学的演算を含んでいてもよい。さらに、演算の順序を変える括弧を含んでいてもよい。認証システムはまた、カスタム演算子を提供して、望ましい式の変数に関するいかなる関数をもユーザが実行することを可能にしてもよい。

【００３０】

図４は、管理プロセスの一部としてユーザに提示されてもよい管理画面４００の例を示す。管理上プロセスは、例えば、ユーザ設定処理の各ステップを通してユーザをエスコートする「ウィザード」、及びユーザが式を設定するのを助ける式ビルダーといった多様なツールをユーザに提供してもよい。１つの実施形態において、式ビルダーは、ユーザに選択用の変数及び演算子のメニューを提供し、ユーザに対して一意の式を編集することでそのユーザを支援してもよい。

【００３１】

管理画面４００は、変数の配列４０５、数のキーパッド４１０、数学的関数キー４１５及び非数学的関数キー４２０、及び式のテスト用キー４２５、式の保存用キー４３０を含んでいてもよい。管理画面４００は、また、ユーザ名３７０及びユーザ式４４０を入力する領域を含んでいてもよい。ユーザは変数及び様々な演算子から選択してユーザ式を入力してもよい。

【００３２】

例えば、ユーザはキーボード１４５（図１）を用いてユーザ式をタイプしてもよい。ユーザが式をタイプするときに、ユーザ式がユーザ式領域４４０に表示されてもよい。あるいは、ユーザはポインティングデバイスを用いて、キャラクタ、変数、または演算子上でカーソルを位置決めし、マウスボタンをクリックするかまたはエンターキーを押して所望のキャラクタ、変数または演算子を選択してもよい。選択したものは、ユーザ式領域４４

０に表示される。ユーザは、ユーザ式が所望通り構築されるまで続ける。ユーザ式が完了すると、次にユーザは「セーブ」ボタン４３０を動作させて式を記憶してもよい。

【００３３】

１つの実施形態において、ユーザが、１つ以上のカスタム演算子を構築する関数を与えられていてもよい。例えば、演算子の１つがオフセット関数を含み、関数はユーザ式の変数に付随し、付随する変数からオフセットした配列の変数からの値を当てはめる。オフセット関数は、（Ｏｆｆｓｅｔ（ｘ、ｙ））で表され、ｘはｘ軸のオフセットをいい、ｙはｙ軸のオフセットをいう。オフセット関数を含む例示的なユーザ式は、Ａ＋Ｂ（Ｏｆｆｓｅｔ（１、１））であってもよい。図３を参照すると、ユーザは変数Ａに割り当てられた値を最初に見つけて用いる。次に、変数Ｂを見つけるが、この認証セッションにおいて座標（１、１）だけオフセットされた変数Ｍからの値を用いる。

【００３４】

オフセットが配列３６５の範囲内に提示されている変数を示している限り、ユーザは所望するいかなるオフセットをも使用できる。１つの例示的な実施例において、ユーザはユーザ式内で所望される「（Ｏｆｆｓｅｔ（ｘ、ｙ））」を単にタイプすることによってオフセット関数を入力する。別の例示的な実施例では、非数学的関数４２０の１つが「オフセット」と名付けられたボタンを含んでもよい。オフセットボタンを押すことによって、ユーザにオフセット座標を入力することを要求するダイアログボックスが開始されてもよい。座標を入力すると、例えば（Ｏｆｆｓｅｔ（１、１））などのオフセット指定が、ユーザ式領域４４０内に表示されるユーザ式に現れてもよい。

【００３５】

オフセット関数の別の展開では、ＩＸ関数といわれる特別のオフセットが決定されてもよい。ＩＸ関数は、配列の上側左手位置を示している座標として、変数に付随する値を利用する。例えば、ユーザがユーザ式２＊Ｂを用いることを望み、配列３６５の上側左手コーナーを特定するのに変数Ｋを指定することを望んでもよい。オフセットボタンを押した後に、座標に対する要求に応えて、ユーザはＩＸ（Ｋ）、即ち、特別のオフセット及び指定に対するいくつかの他の適当な指定で応答してもよい。

【００３６】

その後、ユーザがユーザ式３６５を用いてユーザ式の結果を判断するときに、ユーザは、変数Ｋが値「４３」を割り当てられているということがわかり、次に変数Ａのオフセット位置として座標（４、３）、変数Ｂのオフセット位置を指定する座標（５、３）、変数Ｃのオフセット位置を指定する座標（６、３）、その他、を考慮する。座標（５、３）の値を用いると、ユーザ式２＊Ｂは、そのときパスワード領域３７５において入力される「１０４」を生じる。

【００３７】

いかなる関数、演算子、または関数もしくは演算子の組合せを実行する他のカスタム演算子が生成されてもよい。

【００３８】

別の例として、管理画面４００は、１つ以上の変数に関して演算するカスタム関数を生成する選択を含んでいてもよい。カスタム関数は、数学、論理的（ＡＮＤ、ＯＲ、ＸＯＲ、その他）三角法、統計、その他の様々なタイプの演算子をいくつでも含んでいてもよい。ユーザは、カスタム関数を設計するためのテンプレートとして用いることができる１つ以上のスクリプトを提示されてもよい。同様にスクリプトが提供され、ボタンまたはメニュー項目をユーザに提示し、カスタム関数を呼び出して、ユーザ式においてカスタム関数を用いてもよい。

【００３９】

カスタム関数を生成する機能が有利である。なんとなれば、それはシステムが特定のユーザまたは企業の一部に対してカスタマイズされることを可能にするからである。システムの購入者は、他のシステムの購入者に利用可能でないかまたは知られていないカスタム関数及び演算子を生成することによって、更にシステムの安全確保を強化する機能を提供

される。
【００４０】
認証システムは、ＡｕｔｏＴｏｋｅｎ（登録商標）関数と称される、式内で式を生成する関数を提供することによって、より大きな安全確保の手段を提供してもよい。例えば、ユーザはＡｕｔｏＴｏｋｅｎ（登録商標）キー４３５（図４）を選択することによって、ＡｕｔｏＴｏｋｅｎ（登録商標）関数を呼び出す。ＡｕｔｏＴｏｋｅｎ（登録商標）関数は、ユーザ式領域４４０にユーザが入力するユーザ式をユーザに促す。
【００４１】
ＡｕｔｏＴｏｋｅｎ（登録商標）関数は、それぞれローカル式及びリモート式と称される２つの式を自動的に生成する。ローカル式及びリモート式の各々は、変数、定数及び演算子を含み、それらが演算式を形成する限り、ランダムに選択されてランダムに命令されてもよい。変数、定数及び演算子には、ユーザに提示される変数及び管理プロセスによって提供される演算子の配列からの変数を含んでもよい。ローカル式とリモート式とはいかなる複雑さ及び長さであってもよい。さらに、ローカル式はユーザによって入力されるユーザ式の結果を与えられる結果変数を含むがリモートユーザ式はユーザ式自体を含む、ということ以外は概して同じである。
【００４２】
リモート式は認証システムにより指定されるいかなる場所に保存されてもよい。ローカル式はユーザ近辺の場所に保存されてもよい。１つの実施形態では、ローカル式は、ユーザによって指定されるかまたは選択されるいかなる場所で保存されてもよい。
【００４３】
ローカル式は、異なる場所から、デバイス、サービス、アプリケーションまたは機能にアクセスするのに用いるためにトランスポート可能であってもよい。例えばローカル式は、磁気、光学、半導体、または他の適当な媒体などのいかなる種類の持ち運び可能な媒体上にローカル式を保存することを含むといったトランスポート可能であるように保存されてもよい。ローカル式は、ローカル式を記憶してアクセスするための、フロッピー（登録商標）ディスク、コンパクトディスク、フラッシュメモリーカード、ＵＳＢドライブ、またはいかなる適切な装置（例えば後述する図５の２４７）などに保存されてもよい。
【００４４】
１つの実施形態では、ローカル式は、必ずしも保存されないが、ユーザによる使用のために別の場所に運ばれるか伝送されてもよい。
【００４５】
ＡｕｔｏＴｏｋｅｎ（登録商標）関数を実施したユーザに対する認証セッションは以下のように進む。ユーザは、デバイス、サービス、アプリケーションまたは機能へのアクセスを要求し、認証セッションが開始される。システムはユーザに変数の配列を提示し、ユーザは自分のユーザ式の結果を入力する。この時またはこの時点より前のいつでも、ローカル式が可搬性媒体に記憶された場合、可搬性媒体がシステムに結合されてローカル式は認証システムによってアクセスされることが可能である。認証システムがローカル式の結果変数の位置に結果を挿入し、ローカル式の残りの部分に変数の配列からの値を挿入し、ローカル式の結果を計算する。認証システムは、また、変数の配列からの値を、リモート式の残りの部分だけでなくリモート式のユーザ式へ挿入し、リモート式の結果を計算する。
【００４６】
認証システムは結果を比較し、それらが一致すれば、ユーザは、所望するデバイス、サービス、アプリケーション、または機能へのアクセスを許可される。
【００４７】
なにかの理由のためにユーザのユーザ式が漏れた場合、ユーザは再びＡｕｔｏＴｏｋｅｎ（登録商標）関数を呼び出して、追加の支持リソースを要求されることなしに新しいローカル式、リモート式及びユーザ式を生成して、安全なアクセスの継続を確保する。
【００４８】

他の特徴として、認証システムは、通常、ユーザが他の関数内に関数を埋め込んでユーザ式の安全性を拡張することを可能にする。例えば、ユーザ式はＡ＋（ＡＶＥ（ＡＶＥ Ｂ＋Ｃ＋（ＡＶＥ Ｄ＋Ｅ＋Ｆ））＋Ｇ＋Ｈ）を含んでもよい。特殊関数が用いられて、配列３６５からの変数に割り当てられた値に基づいて、ユーザ式内でダミーのキャラクタを埋め込んでもよい。この関数は、「セット」関数として指定されてもよい。セット関数を用いた例示的なユーザ式は、
（ｓｅｔ Ｚ，１）[ユーザ式]
であってもよい。

【００４９】

変数Ｚに値５が割り当てられる配列では、ユーザ式の結果の最初の値を入力する前に５つのダミーのキャラクタをタイプしてもよい。このように、ダミーキャラクタがいくつでも、ユーザ式の結果内のいかなる位置に挿入されてもよい。

【００５０】

付加的な安全の特徴として、ユーザ式が、配列３６５の変数に割り当てられた値を用いて、秘密のフレーズの特定の言葉の中で、特定の文字を指定してもよい。例えば、ユーザは自分たちの秘密のフレーズを「the dog is lazy」と決定してもよく、ＡＢＣＤというユーザ式を決定してもよい。自分たちのユーザ式を構築するときに、ユーザはユーザ式領域４４０へ自分たちの秘密のフレーズ及び自分たちのユーザ式を指示するコマンドをタイプしてもよい。

【００５１】

あるいは、非数学的関数４２０は、ユーザが指示を選択することを可能にする関数を含んでいてもよい。認証の間、配列が提示されてもよい。例えば、Ａが値３１を割り当てられ、Ｂが値１４を割り当てられ、Ｃが値２１を割り当てられ、Ｄが値１３を割り当てられる。Ａ＝３１に対するフレーズに配列の値を用いることは、最初の語の３番目の文字を生じ、Ｂ＝１４は４番目の語の最初の文字を生じ、Ｃ＝２１は最初の語の２番目の文字を生じ、Ｄ＝１３は３番目の語の１番目の文字を生じる。このようにして、ユーザはＥＬＨＩを打ち込む。配列及びフレーズの秘密の性質を与えられると、この種の結果を解析する試みは、たぶん失敗するだろう。

【００５２】

認証システムは、ユーザ式内でリセット関数を提供することによって、より大きな安全手段を提供してもよい。このリセット関数は、ユーザに提示される変数の配列をリセットする働きをする。例えば、認証セッションの一部として、図３に示す変数の配列がユーザに提示される。ユーザは、配列を調べて、ユーザ式の第１の変数の値を識別して、第１の変数を入力する。第１の変数を入力した後に、リセット関数が、例えば、ユーザ式内のコマンドによって、またはコマンドをタイプすることによって起動される。そして、値及び変数が変更されて、ユーザは新しい配列を提示される。ユーザはユーザ式を利用し続けて、新しい配列から式の次の変数の値を識別する。ユーザが全ての値を識別して、ユーザ式の結果を計算して入力すると、ユーザは所望するようにアクセスを許可される。

【００５３】

リセット関数を用いるユーザ式の例は、
Ａ｜｜Ｂ｜｜＜ｒｅｓｅｔ＞Ｃ
であってもよい。ここで、変数Ａと関連する値が、Ｂに付随する値と連結され、変数の配列がリセットされて、ＡとＢとの連結は変数の新しい値Ｃに連結される。

【００５４】

リセット関数は、ユーザ式のいかなる位置に挿入されてもよく、ユーザ式の１つ以上の場所に挿入されてもよいということが理解されるべきである。リセット関数は様々な方法により起動されてもよい。例えば、特定のキーを押下することへの応答としてまたは値が入力された後に自動的に、であってもよい。

【００５５】

図４の管理画面を参照すると、リセット関数は、式ビルダーの一部としてまたはリセッ

ト関数を挿入するための順を追ったプロセスをユーザに提供する「ウィザード」として、ユーザに提示されてもよい。

【００５６】

上記したように、リセット関数は、ユーザに提示された変数の配列をリセットする働きをする。このことは、配列の変数に対する新しい値を再生するか、変数の位置を変更するか、またはその両方の組合せという形をとることができる。リセット関数は、式ビルダーまたはウィザード処理の間にユーザによって与えられるシード数または変数に基づく式を用いる新しい配列を生成してもよい。変数シードは、ユーザに提示される変数の配列からの変数であってもよい。

【００５７】

このように、リセット関数は、本発明に高い水準の安全性を提供する。例えば、ネットワーク化された環境において、デスクトップコンピュータとサーバーとの間の通信が妨害されると、変数の配列についてのデータが抜き出されるかもしれない。例えば、ある人は、妨害されたデータから変数の配列を、失敗はするが引き出そうとするかもしれない。リセット関数は、外部コミュニケーションを用いずに、局所的に変数の配列をリセットする働きをする。よって、通信を傍受することによって変数の配列を引き出す努力は役に立たなくなる。なんとなれば、新しい変数の配列が生成されて、リセットされた変数配列または新しい変数配列に付随する通信がないからである。

【００５８】

再び図１を参照すると、システム１００はユーザインタフェース１１０及び制御装置１１５を含むデスクトップコンピュータであってもよい。制御装置１１５は、１つ以上のプロセッサ１２０を含んでいてメモリ１２５から認証プログラム１３５を実行し、また、情報、データ及びプログラムを記憶するための記憶装置１３０を含んでいてもよい。制御装置１１５は、他のデバイスと通信するためのインタフェースも含んでいてもよい。ユーザインタフェース１１０は、情報をユーザに提示するディスプレイデバイス１４０と、情報、質問、応答及びコマンドを入力するための、例えばキーボード及びポインティングデバイスなどの１つ以上の入力装置１４５とを含んでいてもよい。

【００５９】

プロセッサ１２０は、認証プログラム１３５の制御下で認証サービスを提供し、認証されると、認証されたユーザがサービス１５０にアクセスするかまたは利用することを可能にしてもよい。本実施形態において、サービス１５０は局所的なサービスであってもよい。即ち、デスクトップコンピュータ１００の範囲内に存在してもよい。サービス１５０は、プロセッサ１２０またはシステム１００のユーザがアクセスを要求できるいかなるデバイス、サービス、アプリケーションまたは機能であってもよい。例えば、サービス１５０は、データ処理システム、コンピュータを利用したサービス、コンテンツ配信サービス、データベース、ファイルシステム、その他であってもよい。

【００６０】

工程の間に、ユーザは、制御装置１１５を介してサービス１５０にアクセスしようとしてもよい。制御装置１１５は、上記したような認証セッションを開始して、ユーザが有資格者であるか否か、許可を有するか否か、または一般にサービス１５０にアクセスすることを許されているか否か判断する。ユーザが適当な資格証明書、即ち、本明細書で説明したようなユーザ式へ割り当てられた値についての適当なアプリケーションを与える場合、制御装置１１５はサービス１５０へのアクセスを許可する。

【００６１】

図５は、分散型システム５００として示される本発明の別の実施形態を示す。システム５００は、企業または会社のワイドエリアネットワークまたはローカルエリアネットワークの一部であってもよく、一般的に、ユーザインタフェース２１０、制御装置２１５、及び通信ネットワーク２２５によって接続されたアプリケーションまたはサービス２２０を含む。ユーザインタフェース２１０は、通常、ローカルのコンピュータデバイス２３０の一部であって、制御装置２１５及びサービス２２０は通常、コンピュータデバイス２３０

から離隔している。ローカルコンピュータデバイス２３０は、記憶装置２４５に記憶されたプログラム２４０を実行する１つ以上のプロセッサ２３５を含んでいてもよい。コンピュータデバイス２３０は、また、ローカル式を記憶するための着脱自在の外部記憶装置２４７を含んでいてもよい。ユーザインタフェース２１０は、ユーザに情報を表示するディスプレイデバイス２５０と、情報、質問、応答、及びコマンドを入力するための例えばキーボード及びポインティングデバイスなどの１つ以上の入力装置２５５とを含んでいてもよい。

【００６２】

制御装置２１５が認証サーバとして働いてもよく、１つ以上のプロセッサ２６０及び認証プロセス及び認証セッションを制御するプログラムを記憶する記憶機能２６５を含んでいてもよい。認証サーバとして、制御装置２１５はコンピュータデバイス２３０またはコンピュータデバイス２３０のユーザを認証する働きをしてもよい。認証すると、制御装置２１５が動作してコンピュータデバイス２３０にサービス２２０を提供するかまたはコンピュータデバイス２３０がサービス２２０にアクセスすることを可能にする。制御装置２１５はまた、記憶設備２６５に記憶された命令又はプログラムの制御下でシステム２００の構成要素の間のトラフィックを指示する働きをしてもよい。制御装置２１５はまた、記憶設備２６５の中でコンピュータデバイス２３０のための記憶容量を提供してもよい。認証サーバとして、制御装置２１５は、他のコンピュータデバイス２７５_{1}・・・２７５_{n}を認証し、認証すると、他のコンピュータデバイス２７５_{1}・・・２７５_{n}にサービス２２０及び他のサービス２７０_{1}・・・２７０_{n}へアクセスさせてもよい。

【００６３】

本実施形態では、認証プロセス及び認証セッションを制御するプログラムが、記憶装置２４と記憶設備２６５との間で分散されてもよい。認証プロセス及び認証セッションの一部は、それぞれ記憶装置２４５及び記憶設備２６５に記憶されたプログラムの制御下でプロセッサ２３５及び２６０によって実施されてもよい。

【００６４】

サービス２２０は、コンピュータデバイス２３０またはコンピュータデバイス２３０のユーザがアクセスを要求できるいかなるアプリケーションまたはサービスであってもよい。例えば、サービス２２０は、データ処理システム、コンピュータを利用したサービス、コンテンツ配信サービス、データベース、ファイルシステム、その他であってもよい。サービス２２０は、コンピュータデバイス２３０または制御装置２１５内に存在するか、またはシステム２００内にまたはシステム２００の任意の構成要素と結合したいかなる場所に存在してもよい。

【００６５】

通信ネットワーク２２５は、例えばインターネット、一般加入電話網（ＰＳＴＮ）、無線ネットワーク、有線ネットワーク、仮想プライベートネットワーク（ＶＰＮ）、その他などの通信に適しているいかなるリンクまたはネットワークを含んでもよい。通信は、Ｘ．２５、ＡＴＭ、ＴＣＰ／ＩＰ、その他を含むいかなる適切なプロトコルを用いて実施されてもよい。

【００６６】

工程の間に、ユーザはサービス２２０にアクセスしようとするかもしれない。制御装置２１５は、試みられたアクセスを監視するかまたは報告される。例えば、制御装置２１５は、記憶設備２６５に記憶されたプログラムの制御下でサービス２２０にアクセスしようとする全ての試みを監視して傍受する。別の例として、サービス２２０が、全てのアクセスの試みを、処理のために制御装置２１５へ自動的に転送してもよい。サービス２２０へのアクセスを制御するために制御装置２１５を用いるいかなる他の適切な方法が実施されてもよい。

【００６７】

制御装置２１５は、認証セッションを開始して、ユーザが有資格者であるか否か、許可を有するか否か、または一般的にサービス２２０にアクセスすることが許されているか否

かを判断する。制御装置２１５は、データ及びコマンドをコンピュータデバイス２３０に与えて、表示２５０上に変数の配列を表示し、ユーザにユーザ式の結果を与えるように促す。コンピュータデバイスは、結果を制御装置２１５へ送信する。制御装置２１５も、ユーザ式及び変数の配列からの値を用いて結果を計算する。送信された結果と制御装置２１５によって計算された結果が一致する場合、制御装置２１５はサービス２２０へのアクセスを許可する。

【００６８】

本実施形態では、ユーザが上記したようなＡｕｔｏＴｏｋｅｎ（登録商標）関数を実施するときに、ローカル式が着脱自在の外部記憶装置２４７に記憶されてもよい。ローカル式における結果変数の代わりにユーザ式の結果を挿入すること、ローカル式の残りの部分へ変数の配列からの値を挿入すること、ローカル式の結果を計算すること、を含むローカル式に関する演算が、コンピュータデバイス２３０上で動作しているクライアントプログラムによって実行されてもよい。リモート式の残りの部分だけでなく、リモート式内のユーザ式へ変数の配列からの値を挿入すること、リモート式の結果を計算すること、を含むリモート式に関する演算が、制御装置２１５上のサーバプログラムによって実行されてもよい。

【００６９】

図６は、電子商取り引きまたはｅ‐コマース用の分散型システム６００として示される別の実施形態を示す。システム６００は、インターネットに基づくものであってもよく、共通の通信媒体としてワールドワイドウェブを用いてもよい。システム６００は、概して、先に述べた実施形態の全ての特徴を提供し、多くのユーザ６１０_{1}・・・６１０_{n}、制御装置６２０、及び多くのアプリケーションまたはサービス６５０_{1}・・・６５０_{n}を含む。ユーザ６１０_{1}・・・６１０_{n}、サービス６５０_{1}・・・６５０_{n}、及び制御装置６２０は、通常、インターネット６６０によって接続されている企業体などの独立した事業体を示す。例えば、ユーザ６１０_{1}・・・６１０_{n}はサービスにアクセスする個人であってもよいし、またはプログラムの制御下でサービスにアクセスするコンピュータデバイスであってもよい。１つの実施形態では、ユーザ６１０_{1}・・・６１０_{n}は料金を払って１つ以上のサービス６５０_{1}・・・６５０_{n}にアクセスしてもよく、制御装置６２０が認証を介してかかるアクセスを制御する働きをする。サービス６５０_{1}・・・６５０_{n}のオペレータが順にアクセス及び認証サービスに対して制御装置のオペレータに料金を払ってもよい。ユーザ、サービスオペレータ、及び制御装置のオペレータの間の他のビジネス構成も検討される。制御装置６２０が１つ以上のプロセッサ４２５を含んで、ユーザ認証を制御してサービス６５０_{1}・・・６５０_{n}にアクセスするプログラムを実行する。制御装置６２０は、ユーザ６１０_{1}・・・６５０_{n}を認証し、認証されたユーザに１つ以上のサービス６５０_{1}・・・６５０_{n}を提供する働きをする。サービス６５０_{1}・・・サービス６５０_{n}は、ユーザ６０１_{1}・・・６１０_{n}がｅ‐コマース取引を含むアクセスを要求するいかなるサービスを含んでもよい。例えば、サービス６５０_{1}・・・６５０_{n}は、商品購買システム、データ処理システム、コンピュータを利用したサービス、テキスト、オーディオまたはビデオその他を配信するコンテンツ配信サービス、インターネットなどのネットワークを介しての全ての商取引への参加型を含んでもよい。

【００７０】

システム６００において、１人以上のユーザ６１０_{1}・・・６１０_{n}が、サービス６５０_{1}・・・６５０_{n}に規定通りにアクセスしてもよい。制御装置６２０は、試みられたアクセスを監視するかまたは報告される。例えば、制御装置６２０はサービス６５０_{1}・・・６５０_{n}のいずれかにアクセスする全ての試みを監視し傍受してもよい。別の例では、サービス６５０_{1}・・・６５０_{n}が全てのアクセスの試みを、処理のための制御装置６２０へ自動的に送信するか、そうでなければ、試みられたアクセスについて制御装置６２０に報告してもよい。

【００７１】

それに応じて、制御装置６２０は各ユーザ６１０と認証セッションを開始し、当該ユー

ザが有資格者であるか否か、許可を有するか否か、または一般的に１つ以上のサービス６５０$_1$・・・６５０$_n$にアクセスすることを許可されているか否かを判断する。ユーザ６１０が適当な資格証明書、即ち本明細書で記載されているようなユーザ式の適当な結果を与える場合、制御装置６２０は所望のサービスまたは複数のサービスへのアクセスを許可する。

【００７２】

別の実施形態では、ユーザ６１０は、サービスへのアクセスが１回限りで許可される１つ以上のサービス６５０$_1$・・・６５０$_n$にアクセスしようと試みてもよい。制御装置６２０は、試みられたアクセスを報告されるかまたは積極的に監視する。それに応じて、制御装置６２０がユーザ６１０との認証セッションを開始する。プログラムまたはオペレータであってもよい管理者は、ユーザ６１０へ１回の使用に対してだけ有効であるユーザ式を送信する。ユーザ６１０は１回限りのユーザ式の結果を入力し、通常、１つ以上のサービス６５０$_1$・・・６５０$_n$にアクセスすることが許可される。

【００７３】

図７は、例えばｅメールなどのメッセージの一部として送信されるデータの安全を確保する実施形態を利用するシステム７００を示す。システム７００は、本明細書で開示された認証システム７１０を利用するメッセージ発信者７０５、受信者７１５、及び通信ネットワークを含む。発信者７０５及び受信者７１５の両方は、１つ以上のプロセッサ、記憶装置、及びメッセージ転送及び開示されたような認証動作を支援するプログラムを含む。発信者７０５は、例えばｅメールなどのメッセージを作成する。それは発信者７０５が安全確保することを望むデータを含む。かかるメッセージ８１０のブロック図が図８に示される。データ８２０はメッセージの一部またはメッセージに添付されたファイルとして含まれてもよい。認証システム７１０は、メッセージ８１０及びデータ８２０を有するラッパー８２５を含み、ラッパー８２５は、認証セッションを開始して受信者７１５が適当な資格証明書を生成しなければデータ８２０へのアクセスを阻止する。次にメッセージは、例えば標準のｅメールプロトコルを用いて、受信者７１５へ送信される。

【００７４】

受信すると受信者７１５はメッセージを開こうとする。ラッパーは認証セッションを開始して、図３に示す配列を表示する。発信者に対する受領通知も生成されて、それは発信者７０５に対して開始されるべき同じ認証セッションを生じる。

【００７５】

発信者７０５は、発信者のユーザ式の結果を判断し、次に、通常メッセージを送信するために用いられる方法と異なった方法を介して結果を受信者７１５へ送信する。受信者が結果を入力し、正しければ、ラッパー８２５はデータ８２０へのアクセスを許可する。一旦データが閉じられると、認証セッションは終了する。メッセージを開く試みがなされる度に、別の認証が新しい配列から始まる。このようにして、配列は変数に割り当てられる新しい値を含んで、発信者のユーザ式を当てはめた結果を再び判断することを発信者７０５に要求する。従って、受信者７１５が再びメッセージを開こうとするか、または別の人にメッセージを転送しようとすると、ユーザ式の前の結果はもはやメッセージを開くために使用可能でなく、発信者７０５に報告されてもよい。

【００７６】

ユーザに提示される配列の別の実施形態が、図９に示される。上記したように、認証セッションの一部として、変数の配列９００が、ユーザに提示されてもよい。配列９００は、各セル９２０に変数９１０及び多数の値９１５を含んでいてもよい。上記のように、変数及び値は、いかなる英数字も、またはいかなるマーク、シンボル（記号）、もしくは画像をも含むことができる。

【００７７】

この実施形態では、セル９２０は、各セルの各コーナーの値９１５とともに変数９１０で各々表示される。各セル内の任意の位置に変数９１０及び値９１５はいくつあってもよいということが理解されなければならない。例えば、各セルは、長方形などの幾何学的図

形であってもよいし、複数の値が各セルの複数のコーナーに置かれてもよい。別の例として、各セルは円い形状を有していてもよく、各セルの値の位置はある程度指定されていてもよい。

【００７８】

概して、認証プロセスの一部として変数に割り当てられることになっている値は、目標位置と称されるセル内の特定の場所を有していてもよい。変数Ｈを有する図９のセルを、例として用いることができる。Ｈの目標位置が上部左手コーナーである場合、Ｈに割り当てられる値は５である。

【００７９】

例示的実施形態では、前述のユーザセットアッププロセスの一部として、ユーザは、プロファイルと称される情報を提供することができる。ユーザプロファイルは、例えば名前、連絡先、仕事場所などの、ユーザに関する情報を含むことができる。プロファイルは、制御装置２１５（図５）、ローカルコンピュータデバイス２３０（図５）、記憶装置２６５（図５）、または他のいかなる適当な場所に保存されてもよい。ユーザプロファイルは、また、ユーザのユーザ式の変数についての１つ以上の目標位置を含むことができる。目標位置は、例えば「上部左コーナー」または「９０度」などの、各セル内の相対的な位置で指定されてもよい。その他の位置指定技術が用いられてもよい。

【００８０】

別の実施形態では、目標位置がユーザ式の一部として指定されてもよい。例えば、図９に示した実施形態の例示的なユーザ式は、Ｂ（ＵＬ）＋Ｃ（ＬＬ）であってもよい。ここで、ＵＬは、Ｂを含むセルの上部左コーナーの値を用いることを指定する目標であり、ＬＬは、Ｃを含むセルの下部左コーナーの値を用いることを指定する目標位置である。その他の指示が、セル内の目標位置を指定するために用いられてもよい。

【００８１】

認証セッションが開始されると、認証システム１００は、図９に示したような変数の配列をユーザに提示する。各セルは、１つの変数及びいくつかの値を有していてもよい。ユーザは、配列内に示されていてユーザ式の変数に一致する変数を識別する。ユーザはまた、変数に割り当てられることになっている値が置かれた目標位置が各変数にあるということを、理解することができる。ユーザは、各変数を識別し、その変数に対して指定された目標位置の値を変数に割り当て、ユーザ式の演算子を実行し、結果を入力する。認証システムは、その変数に対して指定された目標位置の値を変数に独自に割り当てて、ユーザ式の演算子を実行して独自の結果を生成する。認証システムは、独自の結果をユーザの入力した結果と比較して、結果が一致する場合、認証システムは、サービスまたはアプリケーションへユーザがアクセスできるようにする。結果が一致しない場合、アクセスは拒否される。

【００８２】

図１０は、ユーザプロファイルに保存された目標位置を利用する実施形態を説明するフローチャートを示す。ブロック１００５において、ユーザプロファイルは、上記のように生成される。ユーザ式は、ブロック１０１０において生成されて、ブロック１０１５において保存される。ブロック１０２０に示すように、認証セッションが開始される。ブロック１０２５において、認証システム１００は、ユーザに変数及び目標位置の配列を提示する。ブロック１０３０において、ユーザは、ユーザ式の変数に一致していて配列に提示された変数を識別して、その変数に対して指定された目標位置の値を変数に割り当てる。ブロック１０３５において、ユーザは、ユーザ式の結果を判断して、その結果を入力する。ブロック１０４０において、認証システムは、その変数に対して指定された目標位置の値を変数に独自に割り当て、ユーザ式の演算子を実行して独自の結果を生成する。ブロック１０４５において、認証システムは、独自の結果をユーザの入力した結果と比較して、結果が一致する場合、認証システムは、ブロック１０５０に示すようにサービスまたはアプリケーションへユーザがアクセスできるようにする。結果が一致しない場合、アクセスはブロック１０５５に示すように拒否される。

【００８３】
図１１は、ユーザ式の一部として目標位置を利用する実施形態を説明するフローチャートを示す。ブロック１１１０において、ユーザ式は、目標位置とともに生成される。ブロック１１１５において、ユーザ式は、記憶されて、保存される。認証セッションが、ブロック１１２０に示すように開始される。ブロック１１２５において、認証システム１００は、変数の配列及び目標位置をユーザに提示する。ユーザは、ユーザ式の変数に一致していて配列に提示された変数を識別し、ブロック１１３０に示すようにその変数に対して指定された目標位置の値を変数に割り当てる。ブロック１１３５において、ユーザはユーザ式の結果を判断して、その結果を入力する。ブロック１１４０において、認証システムは、その変数に対して指定された目標位置の値を変数に独自に割り当て、ユーザ式の演算子を実行して独自の結果を生成する。認証システムは、ブロック１１４５に示すように独自の結果をユーザが入力した結果と比較する。結果が一致する場合、ブロック１１５０において、認証システムは、サービスまたはアプリケーションにユーザがアクセスできるようにする。ブロック１１５５に示すように、結果が一致しない場合、アクセスは拒否される。

【００８４】
図９に戻ると、セルの配列は、長方形格子として示されているが、配列はいかなる形状を有していてもよく、いくつのセルまたは位置を含んでいてもよい。配列内のセルは、また、いかなる形状を有していてもよい。

【００８５】
別の実施形態では、認証システムは、概してデコイキャラクタと称されるダミーのキャラクタまたは特に数字用のデコイ数字をユーザがユーザ式結果に加えることができるようにしてもよい。この特徴は利点である。なんとなれば、ユーザ式結果を入力する前にユーザ式結果に自発的に付加キャラクタをさらに加えることによってユーザが動的にユーザ式結果を偽装するができるようにするからである。ユーザは、ユーザ式結果のどこにでもデコイキャラクタを加えることができる。よって、変数についてのユーザの動作及び変数の配列が観察されているかまたは記録されている場合、実際のユーザ式結果は、デコイキャラクタから識別できない。デコイキャラクタは、いかなる英数字、マーク、シンボル（記号）、または画像をも含むことができる。

【００８６】
１つの実施形態では、いくつのデコイキャラクタが、ユーザ式結果の複数のキャラクタの中に点在してもよい。別の実施形態では、許容されるデコイキャラクタに対する制限事項があってもよい。例えば、特定のデコイキャラクタまたはデコイキャラクタの組合せは、認められないかもしれない。他の実施形態では、許容されるデコイキャラクタの最大数が指定されてもよい。より具体的な例として、デコイキャラクタの最大数は、Ｎ／２であってもよい。ここで、Ｎは、デコイキャラクタを加える前にユーザ式結果におけるキャラクタ数である。デコイキャラクタに対する制限事項は、ユーザプロファイルの一部であってもよいし、または全てのユーザもしくは一群のユーザに対して指定されてもよい。デコイキャラクタの制限事項は、システム１００のメモリ、記憶場所、または記憶領域に保存されてもよい。

【００８７】
Ｎ／２の例を参照すると、ユーザは、変数の配列を提示されてもよく、ユーザ式結果をＡ６Ｂ４Ｃ３と計算してもよい。ユーザは認証システムにＡＡ６ＢＢ４Ｃ３３を提供し、よって、追加の「Ａ」、追加の「Ｂ」及び追加の「３」を元の結果に加える。この例では、認証システムは、上記の独自の計算から得られる元のユーザ式結果のキャラクタを判断して、ＡＡ６ＢＢ４Ｃ３３の文字列を解析する。認証システムは、元のユーザ式結果が提示されていると判断して、デコイキャラクタの数が３つであると判断する。認証システムは、デコイキャラクタの数(３)がデコイキャラクタの制限事項、即ち、Ｎ／２デコイキャラクタの最大数、を満たすということを確認する。次に、システムはアクセスを認める。デコイキャラクタの数がＮ／２を上回るか、または、元のユーザ式結果が文字列内に提示

されていない場合、認証システムはアクセスを拒否する。

【００８８】

他のデコイキャラクタ制限事項が指定されてもよく、例えば、Ｎ／３、Ｎ／４などのデコイキャラクタの他の最大数が用いられてもよい。

【００８９】

図１２は、デコイキャラクタを利用する実施形態を説明するフローチャートを示す。ユーザ式は、ブロック１２１０において生成される。ユーザ式は、上記のように目標位置を含んでもよいしまたは含まなくてもよい。ユーザ式は、ブロック１２１５において、記憶されて、保存される。認証セッションが、ブロック１２２０に示すように開始される。認証システム１００は、ブロック１２２５に示すように変数の配列をユーザに提示する。配列は、上記のように目標位置及び値を含んでいてもよいしまたは含んでいなくてもよい。ブロック１２３０において、ユーザは、ユーザ式の変数に一致している配列に示された変数を識別して、その変数に対して指定された値を変数に割り当てる。必要な場合、値は目標位置の値であってもよい。ブロック１２３５に示すように、ユーザは、ユーザ式の結果を判断して、１つ以上のデコイキャラクタを含んでいるその結果を入力する。ブロック１２４０において、認証システムは、変数に割り当てられた値を用いてユーザ式の演算子を独自に実行し、独自の結果を生成する。値は、目標位置から割り当てられてもよいしまたは割り当てられなくてもよい。ブロック１２５０において、システムは、ユーザが生成した結果を分析して、点在されたデコイキャラクタの中に独自の結果があるかどうかを見出す。結果が示されていない場合、ブロック１２６５に示すようにアクセスは拒否される。結果が見出されて一組のデコイキャラクタ制限事項が無効である場合、ブロック１２６０に示すようにアクセスは認められる。結果が見出されて何らかのデコイキャラクタ制限事項が指定されている場合、即ち、一組の制限事項が無効でない場合、システムは、ブロック１２５５に示すようにデコイキャラクタが制限事項を満たしているということを確認する。制限事項が満たされていない場合、アクセスは認められない（ブロック１２６５）。デコイキャラクタ制限事項が満たされている場合、アクセスが認められる（ブロック１２６０）。

【００９０】

再び図９を参照すると、認証システムの別の実施形態は、ユーザが、変数の配列の提示を変更するかまたはカスタマイズすることができるようにする。カスタム化は、特定のユーザにまたは一群のユーザに特有でもよい。ユーザインタフェースのカスタム化の後の認証セッションが開始されると、ユーザはそれらの特定のカスタムメイドの配列を提示される。このことは、ユーザが情報のやりとりをしているシステムが事実認証システムであって偽のシステムでないということをユーザが確認するのを可能にする。

【００９１】

ユーザは、例えば、カラースキーム、ツールバーのカラー、フィルカラー、背景、テキストのフォント、テキストのサイズ、テキストのカラーなどを含む配列の特徴のいくつでもカスタイマイズすることができてもよい。１つの実施形態では、ユーザは、例えば、配列の背景として、セルの背景として、変数として、または配列の任意の一部としてなどの、配列の一部として包含するための画像を提供することが可能であってもよい。

【００９２】

配列のカスタム機能は、上記したユーザのプロファイルの一部として保存されてもよい。１つの実施形態において、認証セッションの開始時に、ユーザは、それらのユーザ名または他のいくつかの一意の識別子をタイプすることによってログインすることができる。次に、認証システムは、ユーザ名を認証して、変数の配列を提供することができる。正当なユーザ名が与えられた場合、認証システムはユーザのプロファイルに付随するカスタム化された配列を供給することができ、よって、例えば、ユーザが認証システムと情報をやりとりしているという保証レベルをユーザに与えることができる。別の例では、正当なユーザ名が与えられて配列がユーザのカスタム化なしで表示される場合、ユーザはセッションを終えるように指示されてもよい。

【００９３】
１つの実施形態では、無効なユーザ名が提供される場合に、認証システムは一般的配列を提供し、潜在的な詐称者または攻撃者に警告するかまたは何らかの情報を提供することを避けることができる。
【００９４】
前述の説明は開示された実施形態を説明するだけであるということが理解されるべきである。様々な代替形及び変化形が、本明細書で開示された実施形態から逸脱することなく、当業者によって考え出され得る。従って、開示された実施形態は、添付された請求の範囲内にあたる全てのかかる代替形及び変化形を包含することを意図する。

【図１】

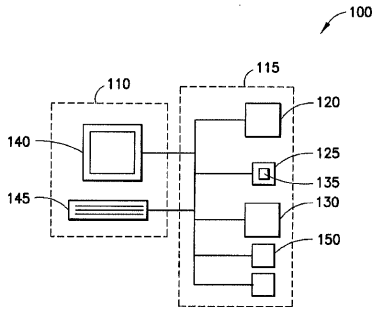
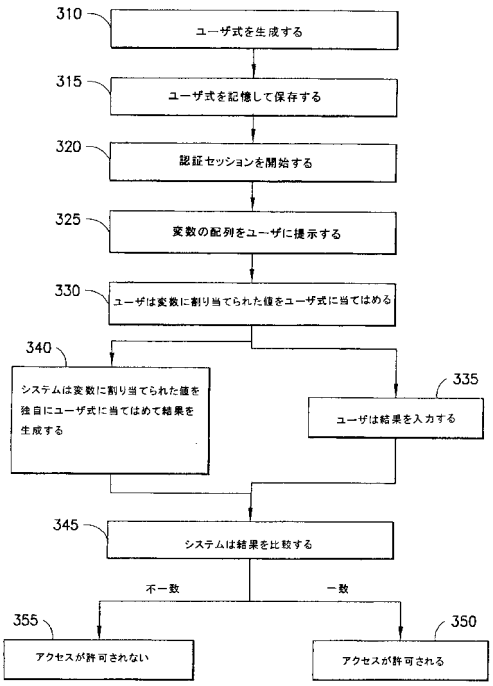


FIG.1

【図２】



【図３】

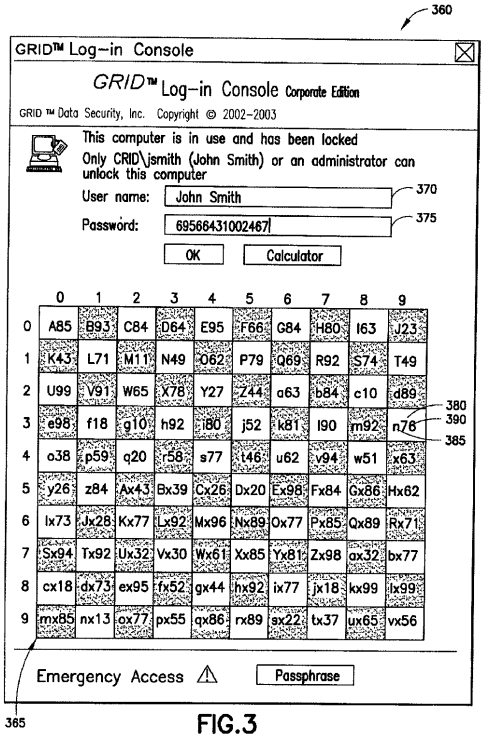


FIG.3

【図４】

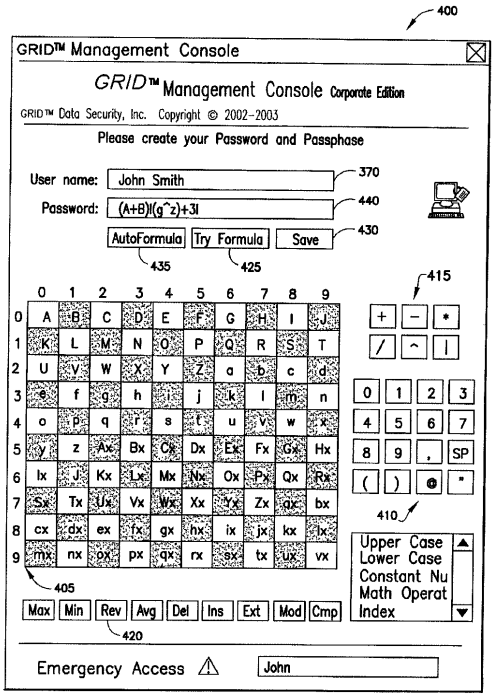


FIG.4

【図５】

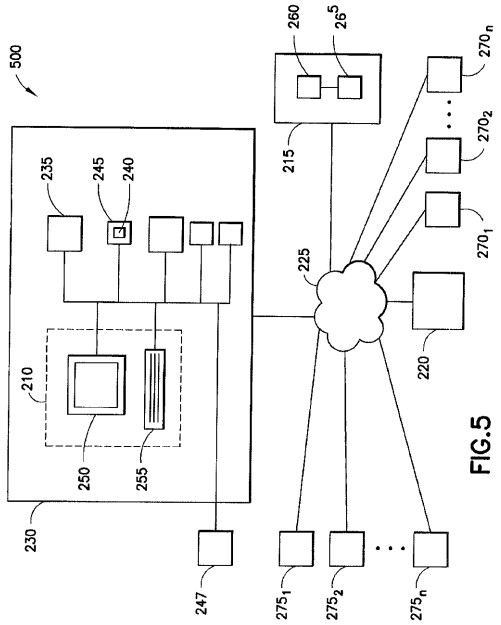


FIG.5

【図６】

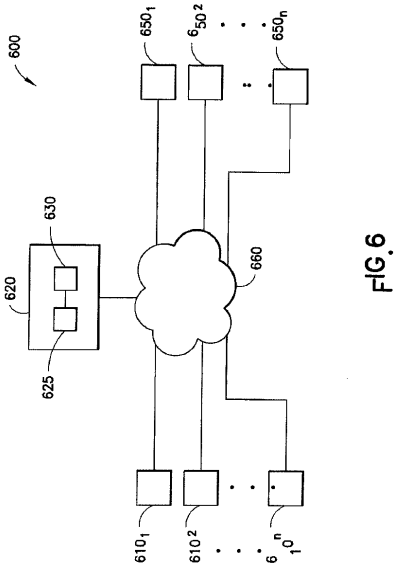


FIG.6

【図７】

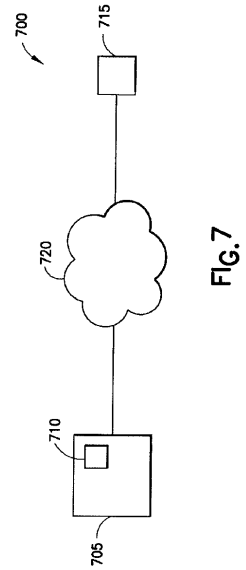


FIG.7

【図８】

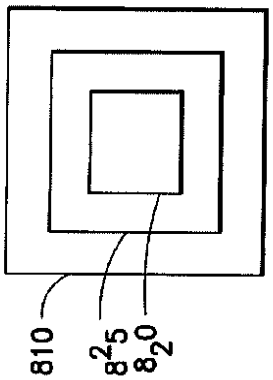


FIG.8

【図９】

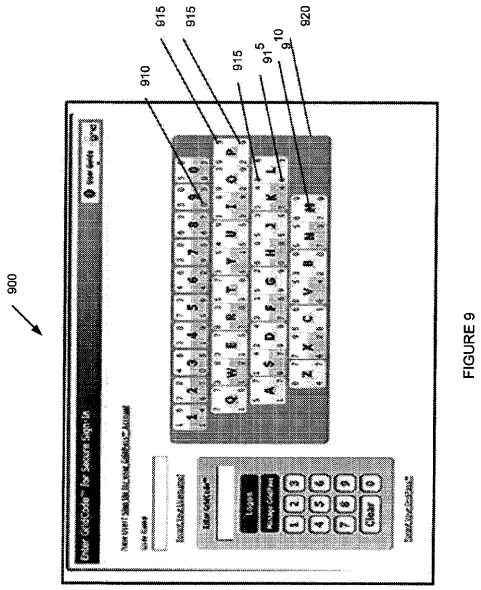
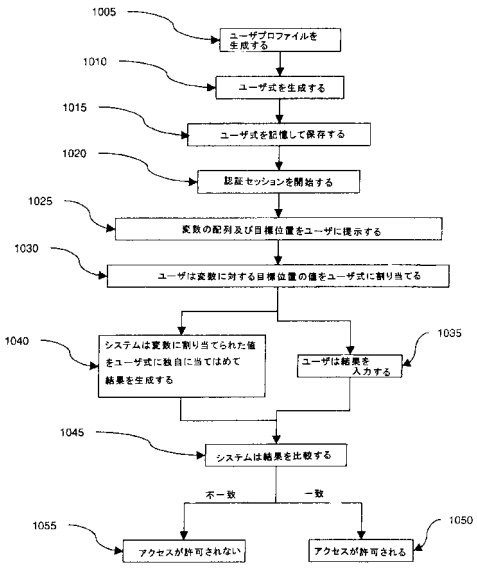
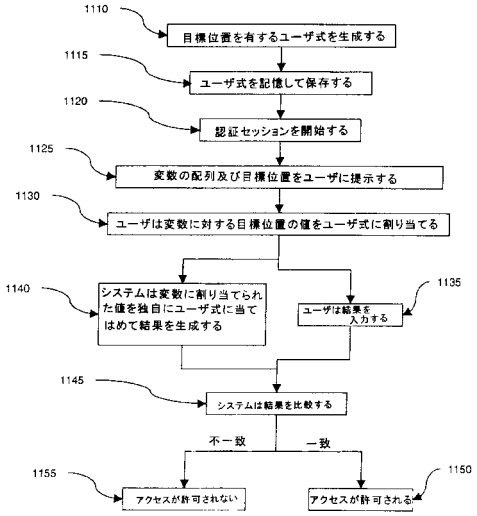


FIGURE 9

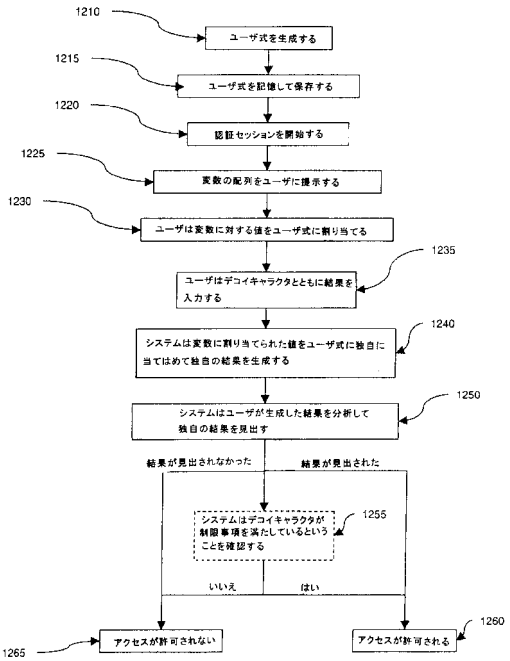
【図１０】



【図１１】


1110
目標位置を有するユーザ式を生成する
1115
ユーザ式を記憶して保存する
1120
認証セッションを開始する
1125
変数の配列及び目標位置をユーザに提示する
1130
ユーザは変数に対する目標位置の値をユーザ式に割り当てる
1140
システムは変数に割り当てられた値を独自にユーザ式に当てはめて結果を生成する
1135
ユーザは結果を入力する
1145
システムは結果を比較する
不一致
一致
1155
アクセスが許可されない
アクセスが許可される
1150

【図１２】


1210
ユーザ式を生成する
1215
ユーザ式を記憶して保存する
1220
認証セッションを開始する
1225
変数の配列をユーザに提示する
1230
ユーザは変数に対する値をユーザ式に割り当てる
1235
ユーザはデコイキャラクタとともに結果を入力する
1240
システムは変数に割り当てられた値をユーザ式に独自に当てはめて独自の結果を生成する
1250
システムはユーザが生成した結果を分析して独自の結果を見出す
結果が見出されなかった
結果が見出された
システムはデコイキャラクタが制限事項を満たしているということを確認する
1255
いいえ
はい
1265
アクセスが許可されない
アクセスが許可される
1260

フロントページの続き

(73)特許権者 310009878
フラナジン ジョージ ケリー
アメリカ合衆国 バージニア州 ２３２２５ リッチモンド ウッドバインロード １９０１
(73)特許権者 310009889
ギンズバーグ レヴ
アメリカ合衆国 ニュージャージー州 ０７８６６ ロッカウェイ ブラザートンアベニュー １６
(74)代理人 110001025
特許業務法人藤村合同特許事務所
(72)発明者 シター ポール
アメリカ合衆国 コネチカット州 ０６４６８ モンロー ジョッキーホロウロード ６３
(72)発明者 フラナジン ジョージ ケリー
アメリカ合衆国 バージニア州 ２３２２５ リッチモンド ウッドバインロード １９０１
(72)発明者 ギンズバーグ レヴ
アメリカ合衆国 ニュージャージー州 ０７８６６ ロッカウェイ ブラザートンアベニュー １６

審査官 和田 財太

(56)参考文献 国際公開第２００５／０３８５７３（WO，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ ２１／３１
Ｈ０４Ｌ ９／３２