(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2015-515218
(P2015-515218A)
(43)公表日　平成27年5月21日(2015.5.21)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 9/32	(2006.01)	H04L	9/00	673D	5J104
G06F 21/12	(2013.01)	H04L	9/00	673A	
G06F 21/31	(2013.01)	G06F	21/12	310	
		G06F	21/31		

審査請求 未請求　予備審査請求 未請求　（全 25 頁）

(21)出願番号　特願2015-506314 (P2015-506314)
(86)(22)出願日　平成24年4月20日 (2012.4.20)
(85)翻訳文提出日　平成26年11月26日 (2014.11.26)
(86)国際出願番号　PCT/IB2012/052006
(87)国際公開番号　WO2013/061171
(87)国際公開日　平成25年5月2日 (2013.5.2)

(71)出願人　514264950
フォーティコム、グループ、リミテッド
ＦＯＲＴＩＣＯＭ　ＧＲＯＵＰ　ＬＴＤ
オーストラリア連邦ビクトリア州、フランクストン、ハイランド、ドライブ、２６
(74)代理人　100117787
弁理士　勝沼　宏仁
(74)代理人　100082991
弁理士　佐藤　泰和
(74)代理人　100103263
弁理士　川崎　康
(74)代理人　100107582
弁理士　関根　毅
(74)代理人　100192577
弁理士　梶　大樹

最終頁に続く

(54)【発明の名称】抽象化およびランダム化された取引認証用ワンタイム使用パスワードのための方法およびシステム

(57)【要約】
ユーザのシステムへのアクセスを認証するセキュリティシステム及び方法が開示されている。セキュリティシステムは、ユーザからの認証要求を受信し、事前に記憶されたユーザキーワード及びユーザ選好データに基づいてセキュリティマトリクスを生成する。このセキュリティマトリクスは、各認証要求に対して異なる。セキュリティシステムは、ユーザにセキュリティマトリクスを送信し、セキュリティマトリクスに応答したワンタイムコードを待ち受ける。ユーザは、ユーザキーワード、ユーザ選好、及びセキュリティマトリクスに基づいてワンタイムコードを形成する。セキュリティシステムは、セキュリティマトリクス、キーワード、及びユーザ選好と照合してワンタイムコードを検証し、システムへのアクセスを許可又は拒否する認証結果をユーザに送信する。さらに、セキュリティシステムは、成功又は失敗メッセージをアクセスされたシステムに送信する。

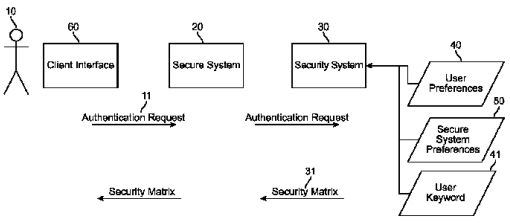


FIG. 1

【特許請求の範囲】
【請求項１】
セキュアシステムにアクセスするためのユーザ認証を検証する方法であって、
前記ユーザから認証要求を受信するステップと、
ユーザＩＤおよびユーザ選好データに基づいてセキュリティマトリクスを生成し、前記マトリクスを前記ユーザに送信するステップと、
前記セキュリティマトリクスに応答して前記ユーザからワンタイムコードを受信するステップと、
前記セキュリティマトリクス、前記ユーザＩＤ、少なくとも１つのユーザキーワード、およびユーザ選好データに基づいて前記ワンタイムコードを検証するステップと、
前記ワンタイムコードを検証後に、前記ユーザに認証結果を送信するステップであって、前記認証結果が前記ワンタイムコード、前記セキュリティマトリクス、前記ユーザＩＤ、前記ユーザキーワード、およびユーザ選好に基づいている、ステップと、
前記認証結果とは別に、前記認証結果に基づいて前記セキュアシステムに成功メッセージまたは失敗メッセージを送信するステップと
を含む方法。
【請求項２】
前記ユーザキーワードが暗号化された形式で記憶される請求項１に記載の方法。
【請求項３】
ユーザＩＤおよびユーザ選好データに基づいてセキュリティマトリクスを生成する前記ステップが、前記ユーザ選好データによって指定されるようにランダムに配置されたセキュリティマトリクスを生成することを含む請求項１に記載の方法。
【請求項４】
ユーザＩＤおよびユーザ選好データに基づいてセキュリティマトリクスを生成する前記ステップが、前記ユーザ選好データによって指定されるようにアルファベット順に配置されたセキュリティマトリクスを生成することを含む請求項１に記載の方法。
【請求項５】
前記認証要求がシステムＩＤを含み、
前記マトリクスの生成が、前記ユーザ選好データ、前記ユーザＩＤ、および前記システムＩＤに基づいている
請求項１に記載の方法。
【請求項６】
前記ユーザＩＤおよび前記ユーザ選好データに基づいてセキュリティマトリクスを生成する前記ステップが、前記セキュリティマトリクスのカスタム表現を構築することを含む請求項１に記載の方法。
【請求項７】
前記システムがシステム選好データを有し、
セキュリティマトリクスを生成する前記ステップが、前記ユーザＩＤ、前記ユーザ選好データ、および前記システム選好データに基づいている
請求項１に記載の方法。
【請求項８】
セキュリティマトリクスを生成する前記ステップが、事前に生成されたどのようなマトリクスとも異なるマトリクスを生成することを含む請求項１に記載の方法。
【請求項９】
前記認証結果が前記セキュアシステムによって使用されるセッションＩＤを含む請求項１に記載の方法。
【請求項１０】
前記ワンタイムコードを受信する前記ステップが、前記ユーザＩＤおよびシステムＩＤを受信することを含む請求項１に記載の方法。
【請求項１１】

前記ユーザキーワードが複数の文字からなり、
前記セキュリティマトリクスが前記キーワードの各文字に対応する数字をマップする
請求項１に記載の方法。
【請求項１２】
前記ユーザ選好データが、前記ユーザキーワードの文字がマップされている各数字を、オフセットを用いて変更することによって前記ワンタイムコードを形成する指示を含む請求項１１に記載の方法。
【請求項１３】
前記ユーザ選好データが、前記ユーザキーワードの文字がマップされている各数字を、クロールを用いて変更することによって前記ワンタイムコードを形成する指示を含む請求項１１に記載の方法。
【請求項１４】
前記ユーザ選好データが、前記ユーザキーワードの文字がマップされている各数字を、ジャンプを用いて変更することによって前記ワンタイムコードを形成する指示を含む請求項１１に記載の方法。
【請求項１５】
前記ユーザ選好データが、前記ユーザキーワードの文字がマップされている各数字を、マスクを用いて変更することによって前記ワンタイムコードを形成する指示を含む請求項１１に記載の方法。
【請求項１６】
前記ユーザ選好データが、前記ユーザキーワードの文字がマップされている各数字を、ユーザが選択した文字を用いて変更することによって前記ワンタイムコードを形成する指示を含む請求項１１に記載の方法。
【請求項１７】
前記ユーザ選好データが、前記ユーザキーワードの文字がマップされている各数字を、前記キーワードと等しい長さを有するユーザが選択した単語を用いて変更することによって前記ワンタイムコードを形成する指示を含む請求項１１に記載の方法。
【請求項１８】
前記セキュリティマトリクスに応答して前記ユーザからワンタイムコードを受信する前記ステップが、代替のキーワードに基づいて前記ワンタイムコードを生成することを含み、
前記ワンタイムコードを検証する前記ステップが、前記代替のキーワードに基づいて前記ワンタイムコードを検証することを含み、
前記成功メッセージまたは前記失敗メッセージを送信する前記ステップが、前記セキュアシステムが前記ユーザを保護するような、前記セキュアシステムへのパニック指示を含む
請求項１に記載の方法。
【請求項１９】
セキュアシステムにアクセスするためのユーザ認証を検証するセキュリティシステムであって、前記セキュリティシステムが、
ユーザキーワードおよびユーザ選好データを記憶すること、
前記セキュアシステムにアクセスするために前記ユーザからのユーザＩＤを含む認証要求を受信して、記憶された前記ユーザ選好データおよび前記ユーザＩＤに基づいた前記認証要求に応答してセキュリティマトリクスを生成すること、
前記セキュリティマトリクスを前記ユーザに送信し、前記ユーザからワンタイムコードを受信すること、
前記生成されたセキュリティマトリクス、前記ユーザキーワード、および前記ユーザ選好データを使用して前記ワンタイムコードを検証し、前記検証に基づいた認証結果を前記ユーザに送信すること、および、
前記認証結果とは別に、前記認証結果に基づいて前記セキュアシステムに成功メッセー

ジまたは失敗メッセージを送信することが
プログラムされているセキュリティコンピュータと、
前記ユーザが前記セキュアシステムにアクセスするための認証要求を前記セキュリティシステムに送信できるようにし、前記セキュリティマトリクスを受信して表示し、前記ユーザが前記ワンタイムコードを前記セキュリティシステムに送信できるようにする、クライアントインタフェースと
を含むセキュリティシステム。
【請求項２０】
前記セキュリティシステムが前記認証要求を、前記セキュアシステムを経由して受信する請求項１９に記載のセキュリティシステム。
【請求項２１】
前記セキュリティシステムが前記ユーザに前記セキュリティマトリクスを、前記セキュアシステムを経由して送信する請求項１９に記載のセキュリティシステム。
【請求項２２】
前記セキュリティシステムが前記セキュアシステムに前記セキュリティマトリクスを送信し、
前記セキュアシステムが前記セキュリティマトリクスのカスタム表現を生成して前記ユーザに送信する
請求項１９に記載のセキュリティシステム。
【請求項２３】
前記セキュリティシステムが前記ワンタイムコードを、前記セキュアシステムを経由して受信する請求項１９に記載のセキュリティシステム。
【請求項２４】
前記セキュリティシステムが前記認証結果を、前記セキュアシステムを経由して送信する請求項１９に記載のセキュリティシステム。
【請求項２５】
前記クライアントインタフェースがクライアントコンピュータシステム上で動作するブラウザである請求項１９に記載のセキュリティシステム。
【請求項２６】
前記クライアントインタフェースがＡＴＭ機である請求項１９に記載のセキュリティシステム。
【請求項２７】
前記クライアントインタフェースが売り場の端末装置である請求項１９に記載のセキュリティシステム。
【請求項２８】
前記クライアントインタフェースが、アクセスが要求される前記システムの顧客担当者によって操作されるコンピュータシステムのブラウザである請求項１９に記載のセキュリティシステム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、概して認証システムおよび方法に関し、より詳細には、高度に安全な認証システムに関する。
【背景技術】
【０００２】
現代の電子世界において、個人識別に関するセキュリティが、全ての取引の基本となっており、高いレベルの投資が、セキュリティや認証方法、それをサポートする技術、およびそのハッキングにも適用されている。銀行業界のほとんどは、システムにユーザを認証させるために、事前に配布されたユーザとシステムとの間に共有される秘密の数値パスワードである個人認証番号（ＰＩＮ）に依存しているが、全文のインタフェースを有するほ

とんどの電子システムは、パスワードに依存している。
【発明の概要】
【発明が解決しようとする課題】
【０００３】
暗号学的ハッシュ関数（ＣＨＦ）に大きな信頼をおく慣行が、一般的である。この決定論的手法は、任意のデータを取得し、このデータに一意である数学的に計算されたハッシュ値を返す。ＣＨＦの十分に立証された例としては、ＭＤ５アルゴリズムがある。ハッシュ関数およびクライアントとサーバ間のスマートなセキュリティ方法により、データの複製から個人のパスワードやＰＩＮをリバースエンジニアリングすることが困難になる。しかしながら、フィッシング技術を伴う目視手段により、ほとんどのパスワードやＰＩＮが危険な状態になり得、これにより、不正取引の処理が許可される。したがって、認証が危険な状態になり得る可能性を低減させるセキュリティスキームを有することが望ましい。
【課題を解決するための手段】
【０００４】
本発明の一実施形態は、ユーザがセキュアシステムに対して認証することを望むたびに、クライアントインタフェースとの相互作用を抽象化するための方法である。ランダム化されたキーワードに一致するＰＩＮを決定するために、事前に定義されたキーワードを、ユーザが使用できるような形式で、セキュリティシステムは、１回限りのランダム化された文字と数字の組み合わせをユーザに提示する。
【０００５】
より詳細には、本発明の実施形態は、セキュアシステムにアクセスするためのユーザ認証を検証するための方法である。この方法は、ユーザから認証要求を受信するステップと、ユーザＩＤおよびユーザ選好データに基づいてセキュリティマトリクスを生成し、このマトリクスをユーザに送信するステップと、セキュリティマトリクスに応答してユーザからワンタイムコードを受信するステップと、セキュリティマトリクス、ユーザＩＤ、少なくとも１つのユーザキーワード、およびユーザ選好データに基づいてワンタイムコードを検証するステップと、ワンタイムコードを検証後に、ワンタイムコード、セキュリティマトリクス、ユーザＩＤ、ユーザキーワード、およびユーザ選好に基づいた認証結果をユーザに送信するステップと、この認証結果とは別に、認証結果に基づいてセキュアシステムに成功メッセージまたは失敗メッセージを送信するステップとを含む。
【０００６】
さらに別の本発明の実施形態は、セキュアシステムにアクセスするためのユーザ認証を検証するためのセキュリティシステムである。このセキュリティシステムは、セキュリティコンピュータおよびクライアントインタフェースを含む。このセキュリティコンピュータは、ユーザキーワードおよびユーザ選好データを記憶すること、セキュアシステムにアクセスするためにユーザからのユーザＩＤを含む認証要求を受信して、記憶されたユーザ選好データおよびユーザＩＤに基づいた認証要求に応答してセキュリティマトリクスを生成すること、セキュリティマトリクスをユーザに送信し、ユーザからワンタイムコードを受信すること、生成されたセキュリティマトリクス、ユーザキーワード、およびユーザ選好データを使用してワンタイムコードを検証し、この検証に基づいて認証結果をユーザに送信すること、および、この認証結果とは別に、認証結果に基づいてセキュアシステムに成功メッセージまたは失敗メッセージを送信することが、プログラムされている。クライアントインタフェースは、ユーザがセキュアシステムにアクセスするための認証要求をセキュリティシステムに送信できるようにし、セキュリティマトリクスを受信して表示し、ユーザがワンタイムコードをセキュリティシステムに送信できるようにする。
【０００７】
本発明の方法の下で、ユーザのキーワードと自身を照合して検証するためにユーザに提供されるセキュリティマトリクスとの間に相関関係はない。セキュリティシステムはセキュリティマトリクスをランダムに構成し、ユーザは、ユーザおよびセキュリティマトリクスに有効であるワンタイムコードを決定するためにセキュリティマトリクスを採用する。

認証するための各要求によって、新しいセキュリティマトリクスは、キーワードを決定する確率を確実に最小にするように計算される結果となる。

【０００８】

本発明は、セキュリティ認証への新しいアプローチであり、ユーザが１つ以上のキーワードを定義することを許可している。そして、このキーワードは、個人選好として使用され、ランダム化されてシステムで生成されたセキュリティマトリクスから、ユーザがワンタイムコードを作成できる。キーワードは、どのような段階でも認証処理中に直接入力されることはなく、決して開示されたり共有されたりすることはない。

【０００９】

（ｉ）認証するための要求、（ｉｉ）認証情報の検証、および（ｉｉｉ）認可内容の伝送処理の、３つの段階に認証プロセスを分離することにより、セキュリティ方法が生み出される。これにより、全ての取引認証要求が、ユーザとクライアントインタフェースとセキュリティシステムとの間で監視され、記録され、そして分析されることが可能であるが、一方で、ユーザのキーワードが認識され得る可能性が低い状態を維持する。

【００１０】

セキュリティマトリクスの強度は、ユーザが照合して認証しているシステムによってではなく、ユーザがより単純にまたはより複雑に決定することによって変更され得る。

【００１１】

本発明の方法は、セキュアシステムやユーザ体験への変更を最小限にして、ユーザ認証を要求する任意のシステムに適用され得る。セキュリティマトリクスおよびワンタイムコードはキーワードから完全に抽象化されているため、いずれかの方向に送信するためにこれらをコード化するような緊急のセキュリティ要求はない。したがって、本発明の方法は、クライアントインタフェースとセキュアシステムとの間の接続が容易に観察すなわち監視され得る、どのようなシステムに対しても非常に適している。

【００１２】

この方法は、単一システムや複数システムに実装されるか、統合された公開検証システムとして実装されることが可能であり、自身の識別を検証するためにユーザに要求するどのような取引に対しても機能する。

【図面の簡単な説明】

【００１３】

本発明における、前述ならびに他の特徴、態様、および利点は、以下の説明、添付の特許請求の範囲、および添付の図面によって、より理解されよう。

【図１】認証要求を示す図である。

【図２】検証要求を示す図である。

【図３】オフセットが使用されるワンタイムコードの第１の例を示す図である。

【図４】オフセットおよびクロールが使用されるワンタイムコードの第２の例を示す図である。

【図５】クロールが使用されるワンタイムコードの第３の例を示す図である。

【図６】ジャンプが使用されるワンタイムコードの第４の例を示す図である。

【図７Ａ】ローカル認証用の内部セキュリティサーバの例示的な構成を示す図である。

【図７Ｂ】認証処理中のクライアントインタフェースの一部を示す図である。

【図８】遠隔からのウェブ認証用の内部セキュリティサーバの例示的な構成を示す図である。

【図９】遠隔からのウェブ認証用の外部セキュリティサーバの例示的な構成を示す図である。

【図１０】内部および外部のウェブ認証と内部システム認証のための、内部セキュリティサーバの例示的な構成を示す図である。

【図１１】メッセージの構造定義を示す図である。

【図１２】ユーザ選好を示す図である。

【図１３】セキュアシステム選好を示す図である。

【図１４】本発明の実施形態のフローチャート図である。
【図１５】ワンタイムコードを生成して送信する実施形態のフローチャート図である。
【発明を実施するための形態】
【００１４】
以下の説明では、次の識別が使用される。
【００１５】
セキュアシステム２０は、ユーザに、取引または情報要求の処理の際の前提条件として、認証することを要求するシステムである。
【００１６】
セキュリティシステム３０は、ユーザのキーワードおよび選好ならびにセキュアシステムの選好が記憶されているシステムであり、このセキュリティシステム３０でセキュリティシステムのインタフェースのための処理が実行される。
・認証要求１１
・セキュリティマトリクス３１
・ワンタイムコード１２
・認証結果３２
・成功メッセージ３３
【００１７】
ユーザ選好４０が表３に定義されており、セキュリティシステム３０によって内部に記憶される。
【００１８】
キーワード４１は、ユーザ１０によって定義されるアルファベット文字の線形文字列である。与えられた例において、キーワードは（Ａ～Ｚの）アルファベット文字にのみ限定されているが、本発明の方法およびシステムは、アルファベット文字（大文字と小文字を区別）、数字、記号、またはこれらの任意の組み合わせをサポートしている。
【００１９】
セキュアシステム選好５０が表４に定義されており、セキュリティシステム３０によって内部に記憶される。
【００２０】
クライアントインタフェース６０は、現金自動預払機やインターネットサービスへのログオン画面などの、ヒューマン・マシン・インタフェース（ＨＭＩ）であり、ユーザ１０は認証情報を提供するために、キーボード、タッチスクリーン、ピンパッド、または他の入力装置を用いて情報をやり取りすることを要求される。
【００２１】
図１において、ユーザ１０は、事前にユーザ選好４０とキーワード４１を、セキュリティシステム３０に提供している。キーワード４１は、暗号化された形式でセキュリティシステム３０に記憶され、任意の関数で送信されることは決してない。
【００２２】
図１において、ユーザ１０はクライアントインタフェース６０で認証することを要求し、クライアントインタフェース６０がこの認証要求１１を順番にセキュアシステム２０に送信し、セキュアシステム２０がこの認証要求１１をセキュリティシステム３０に転送する。
【００２３】
図２において、セキュアシステム選好データ５０は、要求される形式およびクライアントインタフェース６０の制限を決定するために使用される。ユーザ選好データ４０は、ユーザ１０が好むセキュリティマトリクス１１の複雑さを決定するために使用される。セキュリティシステム３０はセキュリティマトリクス３１を形成して、セキュアシステム２０に返送し、次に、セキュアシステム２０がセキュリティマトリクス３１を直接クライアントインタフェース６０に転送するか、または、セキュアシステム２０内の情報を利用してセキュリティマトリクス３１のカスタム表現を構築して、それから、セキュリティマトリ

クス３１をユーザ１０に提示する。ユーザＩＤの形式は、システムに依存せず、セキュリティサーバによってサポートされているあらゆるシステムにおいて、任意の一意のＩＤであり得る。ユーザＩＤの例としては、顧客ＩＤや電子メールアドレスがある。

【００２４】

図２において、ユーザ１０は、ワンタイムコード番号１２を決定するために提示されたセキュリティマトリクス３１を利用し、キーワード４１と関連付けてユーザ選好４０を適用することによって、認証する。ワンタイムコード番号１２がクライアントインタフェース６０に入力され、次にセキュアシステム２０に、その次にセキュリティシステム３０に送信される。セキュリティシステム３０で、ワンタイムコード１２、ユーザ１０が記憶したキーワード４１、およびユーザ選好４０と併せて、セキュリティマトリクス３１のデータを利用することによって、ワンタイムコード１２はセキュリティシステム３０によって検証される。要求に応答して次に、セキュリティシステム３０は、認証結果３２をセキュアシステム２０に戻し、その次にセキュアシステム２０はクライアントインタフェース６０に返送する。セキュアシステム選好５０に詳述されるように、認証が成功すると次に、セキュリティシステム３０は、セキュアシステム３０の成功通知ポイントに成功メッセージ３３を送ることを開始し、これと平行して、第２の相互作用が起こる。

【００２５】

あらゆる認証要求１１とあらゆるワンタイムコード１２の検証により、結果として、再利用されることを防ぐために再度ランダム化されたセキュリティマトリクス３１となる。認証要求１１およびワンタイムコード１２の要求のログが、ブルート・フォース・アタックを防ぐために与えられた時間枠での最大試行回数を制限するため、および、監査可能なトレースを提供するために、維持される。

【００２６】

図３の例が、セキュリティマトリクス３１、ユーザ選好データ４０、およびユーザキーワード４１を示している。ユーザ１０は、自身のキーワードとユーザ選好データ４０を使用して、ワンタイムコード１２を生成する。

【００２７】

この例では、（ａ）アルファベット順に表示されたセキュリティマトリクス３１、および（ｂ）キーワードの文字に対応する表示された数字に１を加算することを、ユーザ１０は好んでいる。

【００２８】

キーワードの各文字に対してのマトリクス値を取得すると、１７５７２が得られる。このマトリクス値の結果に＋１のオフセットを加算して、２８６８３をワンタイムコード１２として与える。

【００２９】

図４の例が、セキュリティマトリクス３１、ユーザ選好４０、およびユーザキーワード４１を示している。ユーザ１０は、自身のキーワードとユーザ選好４０を使用して、ワンタイムコード１２を生成する。

【００３０】

この例では、（ａ）ランダムな順序で表示されたセキュリティマトリクス３１、（ｂ）キーワードの文字に対して表示された数字に１を加算すること、および（ｃ）キーワードの１番目の文字にはさらに３を加算し、キーワードの２番目の文字にはさらに６を加算することなどを、ユーザ１０は好んでいる。

【００３１】

キーワードの各文字に対してのマトリクス値を取得すると、２８６７２が得られる。この値に＋１のオフセットを加算すると、３９７８３が得られる。さらに＋３のクロールを加算すると６５６０８が得られ、これがワンタイムコードとなる。この例での加算はモジュロ１０であるが、どのようなモジュロ加算であってもよいことに留意すべきである。

【００３２】

図５の例が、セキュリティマトリクス３１、ユーザ選好４０、およびユーザキーワード

４１を示している。ユーザ１０は、自身のキーワードとユーザ選好４０を使用して、ワンタイムコード１２を生成する。

【００３３】

この例では、（ａ）ランダムな順序で表示されたセキュリティマトリクス３１、（ｂ）キーワードの１番目の文字には２を加算し、キーワードの２番目の文字には４を加算することなど、および（ｃ）この例の２番目と４番目の数字はユーザが望む任意の数字であり、有効なワンタイムコードの応答は、ａ．４１２１５、ｂ．４２２２５、ｃ．４３２３５、ｄ．４１２３５、ｅ．４９２８５，ｆ．その他、であり、１番目と３番目と５番目の数字だけが関連していることを、ユーザ１０は好んでいる。

【００３４】

キーワードの各文字に対してのマトリクス値を取得すると、２＃８＃９が得られる。この値に＋２のクロールを加算して４＃２＃５を与え、これがワンタイムコードとなる。この加算もモジュロ１０であることに、留意すべきである。

【００３５】

図６の例が、セキュリティマトリクス３１、ユーザ選好４０、およびユーザキーワード４１を示している。ユーザ１０は、自身のキーワードとユーザ選好４０を使用して、ワンタイムコード１２を生成する。

【００３６】

この例では、（ａ）ランダムな順序で表示されたセキュリティマトリクス３１、（ｂ）キーワードの１番目の文字には１を加算し、キーワードの２番目の文字からは１を減算し、キーワードの３番目の文字には１を加算することなどを、ユーザ１０は好んでいる。

【００３７】

キーワードの各文字に対してのマトリクス値を取得すると、９８４２８が得られる。この値に＋１のジャンプを加算して０７５１９を与え、これがワンタイムコードとなる。この加算または減算もモジュロ１０である。

【００３８】

図７Ａにおいて、内部に提供されているセキュリティシステム３０は、ローカルネットワーク７０を経由してセキュリティシステム３０にログインするユーザ６０を検証するために、セキュアシステム２０によって利用される。ユーザは、有線または無線トランシーバ７２を介した無線のどちらかによって、このローカルネットワーク７０に接続されている。

【００３９】

ステップ１：ユーザが、セキュアシステムのログオンポータルにアクセスすると、図７Ｂの８２と８４に従って、電子メールアドレスであり得るユーザＩＤを提供するようにだけ要求される。

【００４０】

ステップ２：ユーザは、図７Ｂの８４のようにユーザＩＤを入力する。

【００４１】

ステップ３：セキュアシステムが、ユーザＩＤおよびシステムＩＤをセキュリティシステムに送信すると、このセキュリティシステムが検証を行い、図７Ｂの８６のようなセキュリティマトリクス３１を返送する。次に、このセキュリティマトリクス３１がセキュアシステム２０によってユーザ６０に戻って表示される。

【００４２】

ステップ４：ユーザは、図７Ｂの８６のように、ワンタイムコード１２を入力して、通常通りにログインする。セキュアシステム２０は、ワンタイムコード１２、ユーザＩＤ、およびシステムＩＤをセキュリティシステム３０に送信し、セキュリティシステム３０は、このコードを検証して、有効である場合、セッションＩＤをセキュアシステム２０に提供する。

【００４３】

図８において、内部に提供されているセキュリティシステム３０は、例えばモデム９６

を経由したインターネット９０を通じてセキュリティシステム３０にログインするユーザ６０を検証するために、セキュアシステム２０によって利用される。

【００４４】

ステップ１：遠隔ユーザが、セキュアシステムのログオンポータルにアクセスすると、図７Ｂの８２と８４に従って、電子メールアドレスであり得るユーザＩＤを提供するようにだけ要求される。

【００４５】

ステップ２：ユーザは、図７Ｂの８４のようにユーザＩＤを入力する。

【００４６】

ステップ３：セキュアシステムが、ユーザＩＤおよびシステムＩＤをセキュリティシステム３０に送信すると、このセキュリティシステム３０が検証を行い、セキュリティマトリクス３１を返送する。次に、このセキュリティマトリクス３１がセキュアシステム２０によってユーザ６０に戻って表示される。

【００４７】

ステップ４：ユーザは、図７Ｂの８６のように、ワンタイムコードを入力して、通常通りにログインする。セキュアシステム２０は、ワンタイムコード１２、ユーザＩＤ、およびシステムＩＤをセキュリティシステム３０に送信し、セキュリティシステム３０は、このコードを検証して、有効である場合、セッションＩＤをセキュアシステム２０に提供する。

【００４８】

図９において、公的に提供されているセキュリティシステム３０は、インターネット９０を通じてセキュリティシステム３０にログインするユーザ６０を検証するために、セキュアシステム２０によって利用される。この機器構成では、単一のセキュリティシステム３０が、複数のセキュアシステム２０にサービスを提供することが可能であり、ユーザ６０はあらゆる登録されたシステムに対して１つのキーワードを有することができる。前述同様に、遠隔ユーザ６０は、モデム９６を経由してインターネット９０に接続されている。

【００４９】

ステップ１：遠隔ユーザ６０が、セキュアシステム２０のログオンポータルにアクセスすると、図７Ｂの８２と８４に従って、電子メールアドレスであり得るユーザＩＤを提供するようにだけ要求される。

【００５０】

ステップ２：ユーザ６０は、図７Ｂの８４のようにユーザＩＤを入力する。

【００５１】

ステップ３：セキュアシステム２０が、ユーザＩＤおよびシステムＩＤをセキュリティシステム３０に送信すると、このセキュリティシステム３０が検証を行い、セキュリティマトリクス３１を返送する。次に、このセキュリティマトリクス３１がセキュアシステム２０によってユーザ６０に戻って表示される。

【００５２】

ステップ４：ユーザ６０は、ワンタイムコードを入力して、通常通りにログインする。セキュアシステム２０は、ワンタイムコード、ユーザＩＤ、およびシステムＩＤをセキュリティシステム３０に送信し、セキュリティシステム３０は、このコードを検証して、有効である場合、セッションＩＤをセキュアシステム２０に提供する。

【００５３】

図１０において、内部セキュリティシステム３０は、サービスを金融機関の事業全体にわたって提供するように構成されており、カウンタ、ＡＴＭ（現金自動預払機）、業者取引、またはインターネットでの、賃借システム用のパスワードおよびＰＩＮ番号等の標準的な認証システムに効果的に替わる構成である。上記の例は、（ａ）インターネット経由のインターネットバンキング、（ｂ）株式や外国為替等の他のインターネットサービス、（ｃ）ＡＴＭ、（ｄ）売り場、（ｅ）顧客サービスのパソコン、（ｆ）オフィスのパソコ

ンを示している。
【００５４】
上記のシステムは、以下に説明される。
インターネット経由のインターネットバンキング
【００５５】
ユーザが通常通りに銀行のインターネットポータル９０にログオンする場合、ただし、図７Ｂの８２と８４に従って、ログオン処理でユーザはユーザＩＤを提示することだけ要求される。ユーザＩＤを受信すると、銀行のコンピュータ２０が、セキュリティシステム３０にユーザＩＤと銀行のシステムＩＤを連絡する。ユーザＩＤとシステムＩＤを検証した上で、セキュリティシステム３０は、セキュリティマトリクスを生成し、銀行のコンピュータ２０に返送する。次に、銀行のコンピュータ２０は、図７Ｂの８６のようなワンタイムコードを入力するように要求すると共に、ユーザ１１０にセキュリティマトリクスを表示する。ユーザは、セキュリティマトリクスを使用して、ワンタイムコードを解き、システムに入力する。
ワンタイムコードは銀行のコンピュータ２０に返送され、次に、銀行のコンピュータ２０は、ワンタイムコード、ユーザＩＤ、および銀行のシステムＩＤを転送してセキュリティシステム３０に戻し、ここで、ワンタイムコードが検証される。ワンタイムコードが有効である場合、セッションＩＤが作成され、銀行のコンピュータ２０に返される。セッションＩＤは、次に、インターネットアプリケーション１１０に返され、銀行のコンピュータ２０への全ての後続要求の一部を形成する。
株式や外国為替等の他のインターネットサービス
【００５６】
ユーザは通常通りに銀行のインターネットポータルにログオンするが、ただし、図７Ｂの８２と８４に従って、ログオン処理でユーザはユーザＩＤを提示することだけ要求される。ユーザＩＤを受信すると、銀行のコンピュータ２０が、セキュリティシステム３０にユーザＩＤと銀行のシステムＩＤを連絡する。ユーザＩＤとシステムＩＤを検証した上で、セキュリティシステム３０は、セキュリティマトリクスを生成し、銀行のコンピュータ２０に返送する。次に、銀行のコンピュータ２０は、ワンタイムコードを入力するように要求すると共に、ユーザ１１２にセキュリティマトリクスを表示する。ユーザ１１２は、セキュリティマトリクスを使用して、ワンタイムコードを解き、システムに入力する。ワンタイムコードは銀行のコンピュータ２０に返送され、次に、銀行のコンピュータ２０は、ワンタイムコード、ユーザＩＤ、および銀行のシステムＩＤを転送してセキュリティシステム３０に戻し、ここで、ワンタイムコードが検証される。ワンタイムコードが有効である場合、セッションＩＤが作成され、銀行のコンピュータ２０に返される。セッションＩＤは、次に、インターネットアプリケーション１１２に返されて、銀行のコンピュータ２０への全ての後続要求の一部を形成する。
ＡＴＭ
【００５７】
ユーザは通常通りにＡＴＭカードまたはクレジットカードを銀行のＡＴＭ１０２ａ、１０２ｂに挿入すると、このＡＴＭは、ユーザＩＤおよびその他の関連情報を、銀行ＡＴＭのネットワーク１１６を経由して銀行のコンピュータ２０に送信する。銀行のコンピュータ２０は、セキュリティシステム３０にユーザＩＤと銀行のシステムＩＤを連絡する。ユーザＩＤとシステムＩＤを検証した上で、セキュリティシステム３０は、セキュリティマトリクスを生成し、銀行のコンピュータ２０に返送する。次に、銀行のコンピュータ２０は、セキュリティマトリクスをＡＴＭ１０２ａ、１０２ｂに返送してユーザに表示されるようにする。ユーザ１０２ａと１０２ｂは、セキュリティマトリクスを使用して、ワンタイムコードを解き、ＡＴＭのキーパッドに入力する。ワンタイムコードは銀行ＡＴＭのネットワーク１１６を経由して銀行のコンピュータ２０に返送され、次に、銀行のコンピュータ２０は、ワンタイムコード、ユーザＩＤ、および銀行のシステムＩＤを転送してセキュリティシステム３０に戻し、ここで、ワンタイムコードが検証される。ワンタイムコ

ードが有効である場合、セッションＩＤが作成され、銀行のコンピュータ２０に返されて、銀行のコンピュータ２０への全ての後続要求の一部を形成する。

売り場

【００５８】

ユーザが、ＡＴＭに入力するか、または業者の売り場のデバイス１０４にクレジットカードを通して、売買価格が業者によって通常通りに入力されると、情報が銀行クレジットカードのネットワーク１１４を経由して銀行のコンピュータ２０に返送される。銀行のコンピュータ２０は、セキュリティシステム３０にユーザＩＤと銀行のシステムＩＤを連絡する。ユーザＩＤとシステムＩＤを検証した上で、セキュリティシステム３０は、セキュリティマトリクスを生成し、銀行のコンピュータ２０に返送する。次に、銀行のコンピュータ２０は、セキュリティマトリクスを売り場のデバイス１０４に返送し、可能であれば画面に表示され、あるいは紙の領収書に印刷される。ユーザは、セキュリティマトリクスを使用して、ワンタイムコードを解き、売り場のキーパッド１０４に入力する。ワンタイムコードは銀行のコンピュータ２０に返送され、次に、銀行のコンピュータ２０は、ワンタイムコード、ユーザＩＤ、および銀行のシステムＩＤを転送してセキュリティシステム３０に戻し、ここで、ワンタイムコードが検証される。ワンタイムコードが有効である場合、セッションＩＤが作成され、銀行のコンピュータ２０に返されてから、銀行のコンピュータ２０が残りの取引を通常通りに処理する。

顧客サービスのパソコン

【００５９】

銀行の支店内の顧客サービス場所に近づいて、ユーザが銀行カードまたはその他の識別方法を利用して自身を識別させることによって、顧客サービス担当者は、ユーザのユーザＩＤを特定し、顧客のサービスポータル１０８にユーザＩＤを入力できるようにする。顧客サービスのパソコン１０８は、ユーザＩＤを銀行のコンピュータ２０に送信する。銀行のコンピュータ２０は、セキュリティシステム３０にユーザＩＤと銀行のシステムＩＤを連絡する。ユーザＩＤとシステムＩＤを検証した上で、セキュリティシステム３０は、セキュリティマトリクスを生成し、銀行のコンピュータ２０に返送する。次に、銀行のコンピュータ２０は、セキュリティマトリクスを顧客サービスのパソコン１０８に返送してユーザに表示されるようにする。ユーザは、提供された入力デバイスを使用して、ワンタイムコードを解き、顧客サービスのパソコン１０８に入力する。ワンタイムコードは銀行のコンピュータ２０に返送され、次に、銀行のコンピュータ２０は、ワンタイムコード、ユーザＩＤ、および銀行のシステムＩＤを転送してセキュリティシステム３０に戻し、ここで、ワンタイムコードが検証される。ワンタイムコードが有効である場合、セッションＩＤが作成され、銀行のシステム２０に返される。セッションＩＤは、次に、顧客サービスのパソコン１０８に返され、銀行のコンピュータへの全ての後続要求の一部を形成する。

オフィスのパソコン

【００６０】

通常のポータル１０６を通じてログインすることにより、ユーザは企業ネットワークにログオンするが、ただし、ログオン処理でユーザはユーザＩＤを提示することだけ要求される。ユーザＩＤを提示すると、銀行のコンピュータが、セキュリティシステム３０にユーザのＩＤと銀行のシステムＩＤを連絡する。ユーザＩＤとシステムＩＤを検証した上で、セキュリティシステム３０は、セキュリティマトリクスを生成し、銀行のコンピュータ２０に返送する。次に、銀行のコンピュータ２０は、ワンタイムコードを入力するように要求すると共に、ユーザにセキュリティマトリクスを表示する。ユーザは、セキュリティマトリクスを使用して、ワンタイムコードを解き、オフィスのパソコンのシステム１０６に入力する。ワンタイムコードは銀行のコンピュータ２０に返送され、次に、銀行のコンピュータ２０は、ワンタイムコード、ユーザＩＤ、および銀行のシステムＩＤを転送してセキュリティシステム３０に戻し、ここで、ワンタイムコードが検証される。ワンタイムコードが有効である場合、セッションＩＤが作成され、銀行のコンピュータ２０に返される。セッションＩＤは、次に、オフィスのパソコン１０６に返され、銀行のコンピュータ

２０への全ての後続要求の一部を形成する。
ユーザ・パニック・サポート
【００６１】
一実施形態において、セキュリティシステムは、パニックサポートができるようにさらに拡張される。この実施形態において、ユーザまたはシステム所有者は、特定の識別番号を使用するか、または、通常のキーワードの代わりに代替のキーワードを使用して、セキュリティマトリクスからワンタイムコードを形成する。セキュリティシステム３０は、ワンタイムコードを検証して、代替のキーワードが使用されたと判別した場合、セキュアシステム２０に渡されるパニック警告を出す。これにより、セキュアシステム２０は、例えば、インターネットまたはＡＴＭ１０２ａ、１０２ｂの利用可能残高が大幅に減ったことを示したり、業務システムへの「サンドボックス化」されたアクセスを提供しながらセキュリティに報告したりすることによって、脅威にさらされた人を保護する方法で応答する機会が提供される。
【００６２】
図１１は、メッセージの構造定義を示している。メッセージは、認証要求メッセージ１１、ワンタイムコードメッセージ、セキュリティ・マトリクス・メッセージ３１、認証結果３２、および成功メッセージ３３である。認証要求メッセージ１１は、一意のユーザＩＤを含み、いくつかの実施形態においては、認証を要求するシステムのＩＤを含む。ワンタイムコードメッセージは、一意のユーザＩＤを含み、いくつかの実施形態においては、認証を要求するシステムのＩＤ、およびユーザが入力するワンタイムコードを含む。セキュリティマトリクス３１は、セキュアシステム選好５０に従って構成されるキー、バリューペアの集合を含む。認証結果メッセージ３２は、いくつかの実施形態におけるセッションＩＤ、成功表示、またはエラー表示を含む。成功メッセージ３３は、一意のユーザＩＤを含み、いくつかの実施形態においては、照合して検証されたシステムのＩＤおよびセッションＩＤを含む。
【００６３】
図１２は、ユーザ選好を示している。ユーザ選好は、順序パラメータ、オフセットパラメータ、クロールパラメータ、ジャンプパラメータ、マスクパラメータおよびランダマイザを含む。順序パラメータによると、線形の抽象化とは、マトリクスがＡ～Ｚおよび０～９の線形順序で示されるキー文字を有することを意味する。ランダムな抽象化とは、マトリクスがランダム化された順序で示されるキー文字を有すること意味する。
【００６４】
オフセットパラメータは、正のオフセットまたは負のオフセットのどちらかを指定する。正のオフセットにより、正の量がキーに関連する各値に加算される。加算はモジュロ１０であり、文字はモジュロ２６であるため、Ｚ＋１＝Ａである。負のオフセットにより、負の量がキーに関連する各値に加算される。加算は、数字に対してモジュロ１０であり、文字に対してモジュロ２６である。
【００６５】
クロールパラメータは、正のインクリメントまたは負のインクリメントのどちらかを指定する。正のインクリメントとは、キーに関連する値に正の指定された量が加算され、そして、その次の加算では、指定された量だけインクリメントされる。負のインクリメントとは、キーに関連する値に負の指定された量が加算され、そして、その次の加算では、指定された量だけインクリメントされる。これも、加算は、数字に対してモジュロ１０であり、文字に対してモジュロ２６である。
【００６６】
ジャンプパラメータは、奇数または偶数のどちらかをジャンプするように指定する。奇数が指定される場合、次にキーワードの奇数インデックスでのキーに関連する全ての値に指定された量が加算され、キーワードの偶数インデックスに位置付けられている全ての値から指定された量が減算される。偶数が指定される場合、次にキーワードの奇数インデックスでのキーに関連する全ての値から指定された量が減算され、キーワードの偶数インデ

ックスに位置付けられている全ての値に指定された量が加算される。加算または減算は、数字に対してモジュロ１０であり、文字に対してモジュロ２６である。

【００６７】

マスクパラメータ、キーワードの１つ以上のインデックスに指定された文字が、他のパラメータによって変更されるべきではないことを指定する。さらに、キーワード内の位置でのハッシュマーク（＃）は、ワイルドカードの一致を表し、ユーザが任意の数字または記号をこの位置に入力できる。

【００６８】

ランダマイザは、１つの文字またはキーワードと同じ文字数を有する１つの単語のどちらかであり得る。ランダマイザが１つの文字の場合、マトリクスから得るその文字の数値が、キーワードの各数値にモジュロ１０加算される。ランダマイザが１つの単語の場合、ランダマイザの単語の各文字の値が、対応するキーワードの文字にモジュロ１０加算される。

【００６９】

図１３はセキュアシステム選好を示している。この選好は、リターン形式、キー範囲、および値の範囲を指定する。リターン形式は、ＸＭＬ、ＨＴＭＬ、画像、またはＣＳＶテキストのいずれかであり得る。キー範囲は、セキュリティシステムが、指定された文字を使用してセキュリティマトリクスキーを構築すべきであることを指定する。値の範囲は、セキュリティシステムが、指定された文字を使用してセキュリティマトリクス値を構築すべきであることを指定する。

【００７０】

図１４は、本発明の実施形態のフローチャート図である。このフローチャート図は、クライアントインタフェース、セキュアシステム、およびセキュリティシステムが、セキュアシステムへのアクセスを要求しているユーザを認証するために取るステップを説明している。ステップ１５０で、ユーザは、キーワードおよび自身のユーザ選好をセキュリティシステムに提供し、ステップ１５２で、セキュリティシステムがこのキーワードおよびユーザ選好を受信し、これを永続性記憶装置に保存する。

【００７１】

ステップ１５４で、ユーザは、クライアントインタフェースで認可要求を作成し、ステップ１５６で、クライアントインタフェースはセキュアシステムにこの要求を送信する。ステップ１５８で、セキュアシステムは、認証要求を受信し、この認証要求をシステムＩＤと共にセキュリティシステムに転送する。ステップ１６０で、セキュリティシステムはこの認証要求を受信する。次に、ステップ１６２で、セキュリティシステムは、セキュリティマトリクスを生成し、ステップ１６４ａまたは１６４ｂで、このマトリクスをセキュアシステムに送信する。ステップ１６４ａで、セキュアシステムはこのマトリクスをクライアントインタフェースに転送し、ステップ１６６で、クライアントインタフェースはこのマトリクスを受信する。ステップ１６４ｂで、セキュアシステムはセキュリティマトリクスのカスタム表現を構築して、これをクライアントインタフェースに送信し、ステップ１６６で、クライアントインタフェースはこのカスタム表現を受信する。

【００７２】

また、ステップ１６６で、ユーザは、セキュリティマトリクス、ユーザキーワード、およびユーザ選好を使用してワンタイムコードを作成し、ステップ１６８で、このワンタイムコードをクライアントインタフェースに入力する。次に、ステップ１７０で、クライアントインタフェースは、このワンタイムコードをセキュアシステムに送信する。ステップ１７２で、セキュアシステムはこのワンタイムコードを受信し、これをユーザＩＤおよびシステムＩＤと共にセキュリティシステムに転送して、ステップ１７４で、セキュリティシステムはこのワンタイムコードを受信する。ステップ１７４で、セキュリティシステムは、事前に送信されたセキュリティマトリクス、ユーザキーワード、およびユーザ選好を使用してこのワンタイムコードを検証する。認証結果が成功であった場合、ステップ１７６で、セキュリティシステムは、この認証の結果をセッションＩＤと共にセキュアシステ

ムに送信する。ステップ１７８で、セキュアシステムは、この結果をクライアントインタフェースに転送する。これとは別に、ステップ１８２で、セキュリティシステムは、成功メッセージまたは失敗メッセージをセキュアシステムに送信し、ステップ１８４で、セキュアシステムはこのメッセージを受信する。

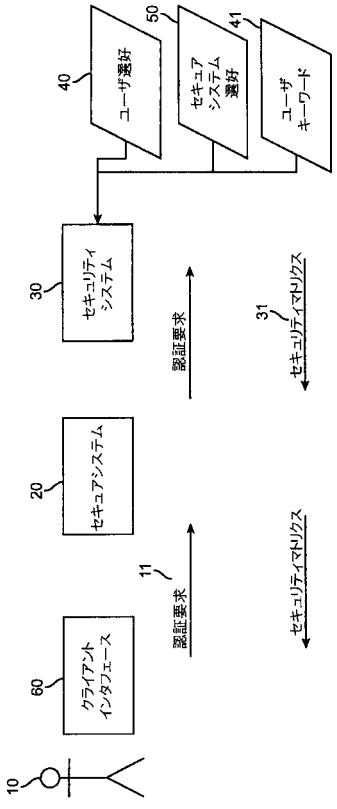
【００７３】

図１５は、ワンタイムコードを生成して送信する実施形態のフローチャート図である。ステップ１９０で、セキュリティマトリクスが、クライアントインタフェースに表示される。このマトリクスは、ユーザ選好によって指定されるように、アルファベット順またはランダムな順序のどちらかであり得る。ステップ１９２で、ユーザは、キーワード、セキュリティマトリクス、およびユーザ選好を使用してワンタイムコードを作成する。ワンタイムコードを形成するために、オフセット、クロール、ジャンプ、およびマスク、あるいはこれらの任意の組み合わせの、いずれが使用されるべきであるかを、ユーザ選好が指定する。ステップ１９４で、ユーザがワンタイムコードをクライアントインタフェースに入力することにより、このワンタイムコードはセキュアシステムに転送され得る。

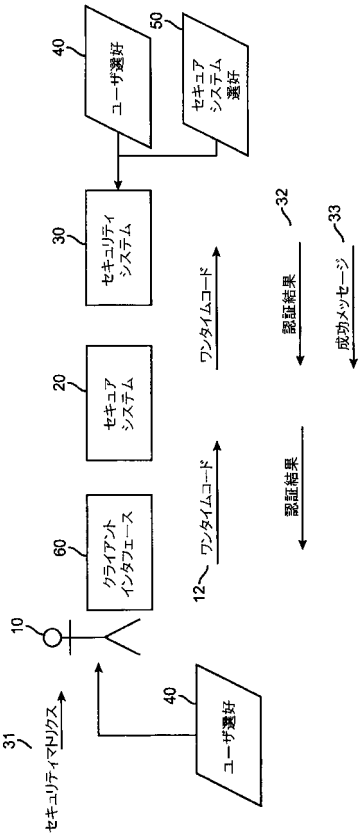
【００７４】

本発明は、発明の好ましい特定の形態を参照して、かなり詳細に説明されたが、他の形態も可能である。したがって、添付の特許請求の範囲の趣旨および範囲は、本明細書に含まれる好ましい形態の説明に限定されるべきではない。

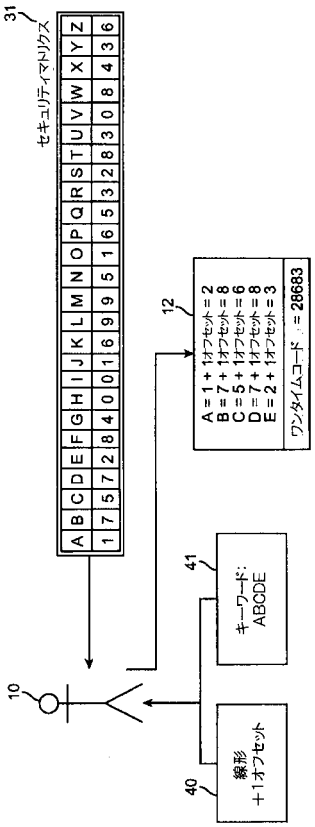
【図１】



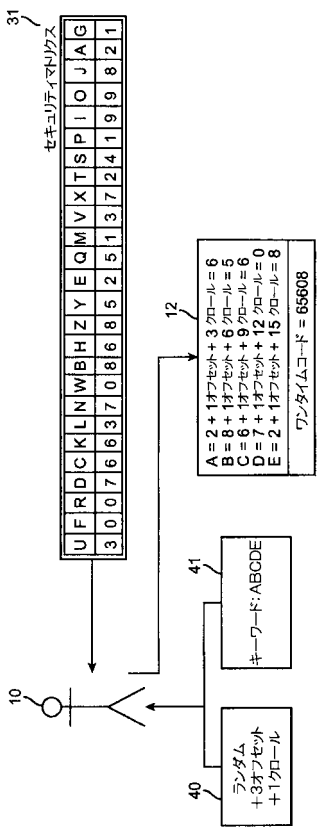
【図２】



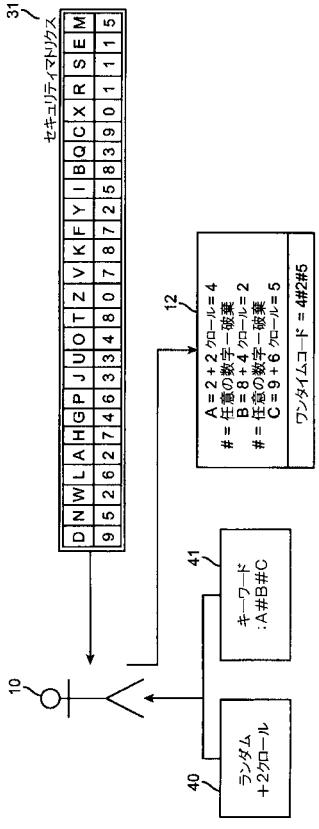
【図３】


31
セキュリティマトリクス
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
1 7 5 7 2 8 4 0 0 1 6 9 5 1 6 5 3 2 8 3 0 8 4 3 6
12
A = 1 + 1オフセット = 2
B = 7 + 1オフセット = 8
C = 5 + 1オフセット = 6
D = 7 + 1オフセット = 8
E = 2 + 1オフセット = 3
ワンタイムコード = 28683
41
キーワード:
ABCDE
10
40
線形
+1オフセット

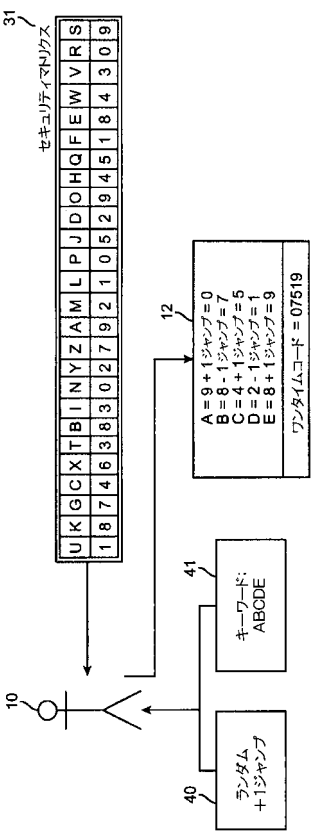
【図４】


31
セキュリティマトリクス
U F R D C K L N W B H Z Y E Q M V X T S P I O J A G
3 0 0 7 6 6 3 7 0 8 6 8 5 2 5 1 3 7 2 4 1 9 9 8 2 1
12
A = 2 + 1オフセット + 3 クロール = 6
B = 8 + 1オフセット + 6 クロール = 5
C = 6 + 1オフセット + 9 クロール = 6
D = 7 + 1オフセット + 12 クロール = 0
E = 2 + 1オフセット + 15 クロール = 8
ワンタイムコード = 65608
41
キーワード:ABCDE
10
40
ランダム
+3オフセット
+1クロール

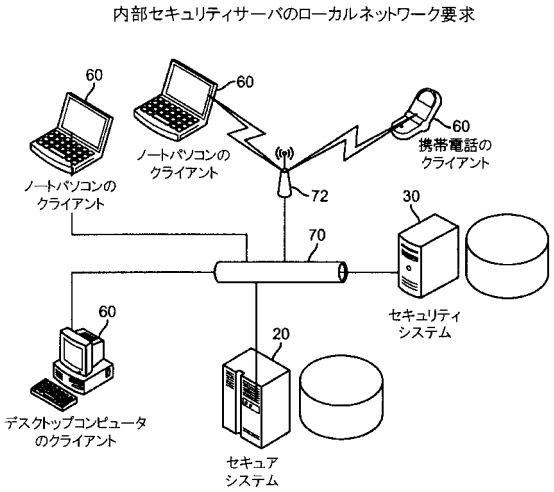
【図５】


31
セキュリティマトリクス
D N W L A H G P J U O T Z V K F Y I B Q C X R S E M
9 5 2 6 2 7 4 6 3 3 4 8 0 7 8 7 2 5 8 3 9 0 1 1 1 5
12
A = 2 + 2 クロール = 4
# = 任意の数字一破棄
B = 8 + 4 クロール = 2
# = 任意の数字一破棄
C = 9 + 6 クロール = 5
ワンタイムコード = 4#2#5
41
キーワード
:A#B#C
10
40
ランダム
+2クロール

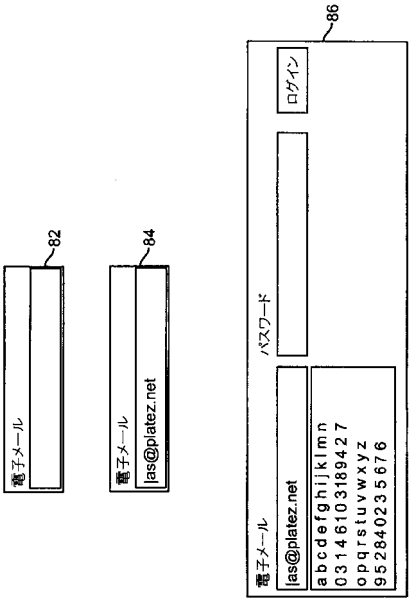
【図６】


31
セキュリティマトリクス
U K G C X T B I N Y Z A M L P J D O H Q F E W V R S
1 8 7 4 6 3 8 3 0 2 7 9 2 1 0 5 2 9 4 5 1 8 4 3 0 9
12
A = 9 + 1ジャンプ = 0
B = 8 + 1ジャンプ = 7
C = 4 + 1ジャンプ = 5
D = 2 + 1ジャンプ = 1
E = 8 + 1ジャンプ = 9
ワンタイムコード = 07519
41
キーワード:
ABCDE
10
40
ランダム
+1ジャンプ

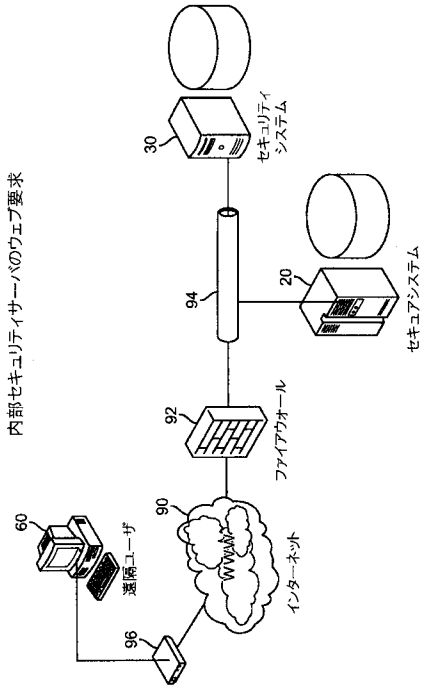
【図７Ａ】


内部セキュリティサーバのローカルネットワーク要求
60
ノートパソコンの
クライアント
60
ノートパソコンの
クライアント
60
携帯電話の
クライアント
72
30
70
セキュリティ
システム
60
デスクトップコンピュータ
のクライアント
20
セキュア
システム

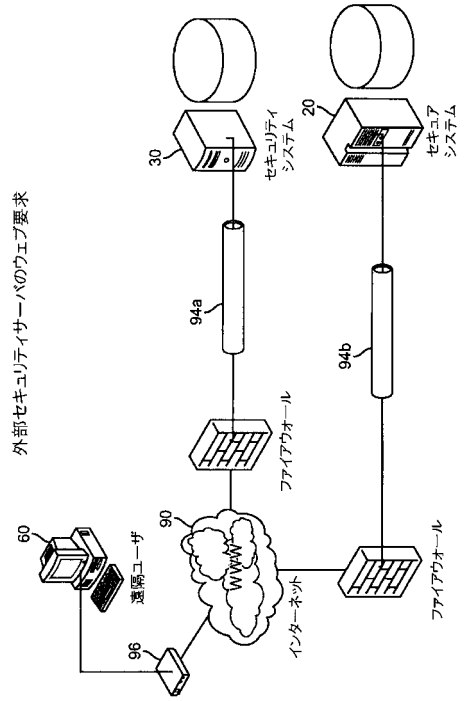
【図７Ｂ】


86
ログイン
パスワード
電子メール
las@platez.net
abcdefghijklmn
0314610318942 7
opqrstuvwxyz
952840235676
82
電子メール
84
電子メール
las@platez.net

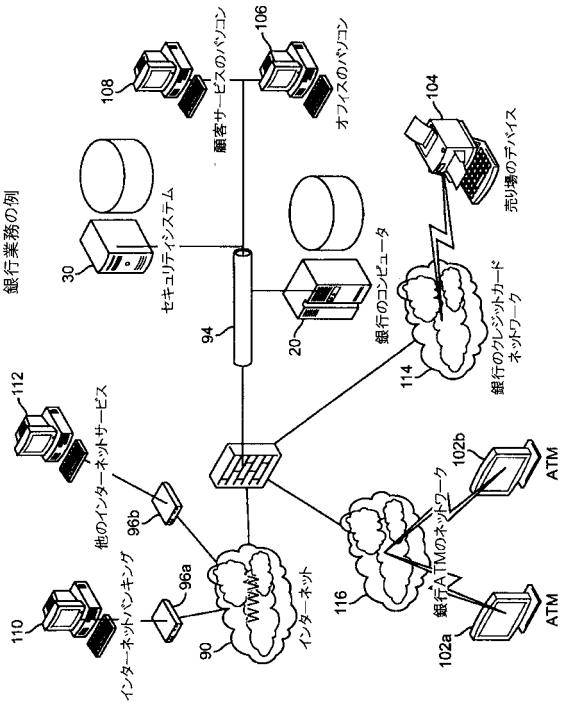
【図８】


内部セキュリティサーバのウェブ要求
30
セキュリティ
システム
20
セキュアシステム
94
92
ファイアウォール
60
遠隔ユーザ
90
インターネット
96

【図９】


外部セキュリティサーバのウェブ要求
30
セキュリティ
システム
20
セキュア
システム
94a
94b
ファイアウォール
60
遠隔ユーザ
90
インターネット
ファイアウォール
96

【図１０】



【図１１】

認証要求メッセージ *11*
一意のユーザID
認証を要求するシステムのID

ワンタイムコード *12*
一意のユーザ ID
検証を要求するシステムのID
エンドユーザが入力するワンタイムコード

セキュリティマトリクス *31*
セキュアシステム選好50に従って構成されるキー／バリューペアの集合

認証結果 *32*
セッションID、成功表示、エラー表示

成功メッセージ *33*
一意のユーザID
照会して検証されたシステムのID
セッションID

表 1

【図１２】

区 分	オプション	説明
順序	線形の抽象化	A～Z、0～9の線形順序で示されるキー文字
順序	ランダム化抽象化	ランダム化された順序で示されるキー文字
オフセット	正のオフセット	キーに関連する各値に加算される量。数字が9＋1＝0のようにラップし、文字がZ＋1＝Aのようにラップする、すなわち＋1
オフセット	負のオフセット	キーに関連する各値に減算される量。数字が0－1＝9のようにラップし、文字がA－1＝Zのようにラップする、すなわち－1
クロール	正のインクリメント	キーに関連する各値に加算されて、インクリメントされる量。数字が9＋1＝0のようにラップし、文字がZ＋1＝Aのようにラップする、すなわち＋1(係々に加算される連続した数0、1、2、3、4、5、6を引き起こす)
クロール	負のインクリメント	キーに関連する各値から減算されて、デクリメントされる量。数字が0－1＝9のようにラップし、文字がA－1＝Zのようにラップする、すなわち－1(係々に減算される連続した数0、－2、－4、－6、－8を引き起こす)
ジャンプ	奇数	キーワードの奇数インデックスに配置されている全ての値に指定された量が加算され、キーワードの偶数インデックスに配置されている全ての値から指定された量が減算される。
ジャンプ	偶数	キーワードの奇数インデックスに配置されている全ての値から指定された量が減算され、キーワードの偶数インデックスに配置されている全ての値に指定された量が加算される。
マスク	定義される	マスクはプレースホルダがキーワードの特定のインデックスに定義されるような、キーワードへのテンプレートの拡張である。このプレースホルダは、任意の数字、文字、記号であってもよく、その他のオプションによって影響されない。さらに、#記号がワイルドカードの一致を表し、ユーザが実際よりも長く見えるキーワードを定義できる。
ランダマイザ	単一	ユーザがキー範囲から単一キーを選択すると、次に、このキーに関連する値がキーワードNの各個別値を変更するために使用される。例えば、FRED＝6152がキーワード、P＝3が選択されたランダマイザの単一キーであって、他の変更子が適用されないと仮定すると、ワンタイムコードは9485である。
ランダマイザ	キー	ユーザがキーワードと同じ長さを有する第2のフルキーを選択すると、このランダマイザキー内の各トークンがキーワードNの各関連する値を変更するために使用される。例えば、FRED＝6152がキーワード、JOHN＝1493が選択されたランダマイザキーであって、他の変更子が適用されないと仮定すると、ワンタイムコードは7545である。

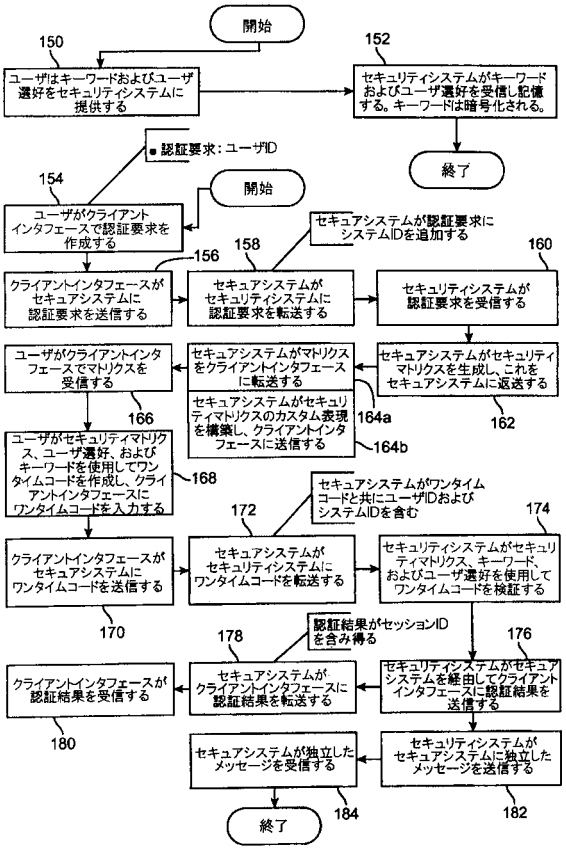
表 3

【図１３】

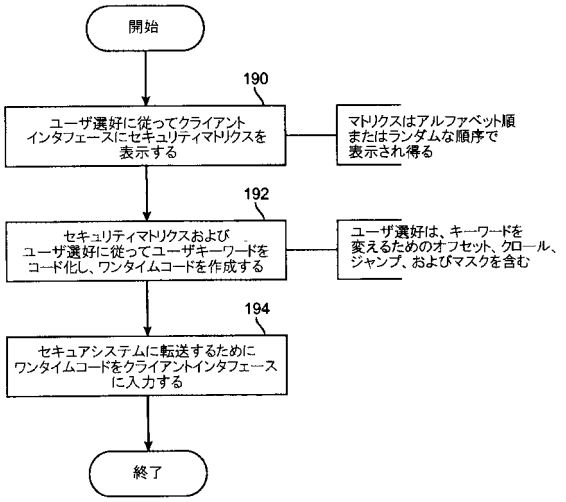
区分	オプション	説明
リターン形式	XML	セキュリティマトリクスがXML構造として返される。
リターン形式	HTML	セキュリティマトリクスがHTMLインクルードとして返される。
リターン形式	画像	セキュリティマトリクスが画像として返される。
リターン形式	CSV	セキュリティマトリクスがカンマ区切りのプレーンテキストとして返される。
キー範囲	A～Za～z,0～9 記号セット または画像	セキュリティシステムは、この選択した情報を使用してセキュリティマトリクスキーを構築する。また、この情報は、有効なキーワード構成を決定する。
値の範囲	A～Za～z,0～9 記号セット または画像	セキュリティシステムは、この選択した情報を使用してセキュリティマトリクス値を構築する。

表 4

【図１４】



【図１５】



【手続補正書】
【提出日】平成26年12月22日(2014.12.22)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
処理システム（３０）により実行されるユーザ認証方法であって、
認証セッションを開始するためのユーザからの要求を受信するステップ（１６０）であって、前記要求が前記ユーザの一意の識別子を含む、ステップと、
前記一意の識別子を使用して、メモリに記憶された前記ユーザと関連するレコードにアクセスするステップであって、前記記憶されたレコードが、少なくともコード値複雑さ選好データ（４０）およびユーザ定義のキーワード（４１）を含み、前記キーワードは、処理システムによってサポートされた１つ以上の記号セットから選択される所定の記号セットの要素を含む、記号の規則的配列からなり、前記規則的配列の前記記号は、事前に前記ユーザによって、他のユーザの選択とは独立して選択されている、ステップと、
前記認証セッション中の前記ユーザに対してだけ有効である１回限りのセキュリティマトリクスを生成するステップ（１６２）であって、前記１回限りのセキュリティマトリクスが前記記号セット内の各記号とコード値との間でのマッピングを含み、前記コード値は、前記認証セッションに特有であり、前記記号セットとは異なるコードセットからランダムに選択される、ステップと、
前記ユーザに提示するために、前記１回限りのセキュリティマトリクスを送信するステップ（１６４ａ）と、

前記１回限りのセキュリティマトリクスの提示に応答し、前記ユーザ定義のキーワードおよび前記コード値複雑さ選好データに基づいて、前記１回限りのセキュリティマトリクスから選択され、前記ユーザによって入力されるコード値（１２）の規則的配列を受信するステップと、

対応するコード値の配列との比較によって、前記受信したコード値の規則的配列を検証するステップ（１７４）であって、前記対応するコード値の配列が、前記記憶されたレコード内の前記ユーザ定義のキーワード、前記コード値複雑さ選好データ、および前記１回限りのセキュリティマトリクスに基づいて前記処理システムによって生成されるが送信されない、ステップと、

前記比較に基づいて前記認証セッションの認証結果を生成するステップ（１７８）と、

を含むユーザ認証方法。

【請求項２】

前記１回限りのセキュリティマトリクスを生成する前記ステップが、前記記号セット内の前記記号をランダムな配列で配置することを含む請求項１に記載の方法。

【請求項３】

前記１回限りのセキュリティマトリクスを生成する前記ステップが、前記記号セット内の前記記号をアルファベット順に配置することを含む請求項１に記載の方法。

【請求項４】

前記ユーザからの前記要求を受信するステップが、前記処理システムとは別のセキュアシステムから前記要求を受信することを含み、前記セキュアシステムは、対応するセキュアシステムの識別子を有し、

前記要求が、前記セキュアシステムの識別子をさらに含み、

前記１回限りのセキュリティマトリクスを生成する前記ステップが、前記セキュアシステムの識別子と関連する選好に基づいている

請求項１に記載の方法。

【請求項５】

前記ユーザに提示するために前記１回限りのセキュリティマトリクスを送信するステップが、

前記１回限りのセキュリティマトリクスを前記セキュアシステムに送信すること、

前記セキュアシステムが前記１回限りのセキュリティマトリクスのカスタム表現を構築すること、および、

前記セキュアシステムが前記１回限りのセキュリティマトリクスの前記カスタム表現を前記ユーザに提示すること

を含む請求項４に記載の方法。

【請求項６】

前記１回限りのセキュリティマトリクスを生成する前記ステップが、前記セキュアシステムの識別子と関連する選好に従って決定されるコードセットから、コード値をランダムに選択することを含む請求項４に記載の方法。

【請求項７】

前記所定の記号セットがアルファベット文字を含み、前記コードセットが数値のセットである請求項１に記載の方法。

【請求項８】

前記ユーザと関連する前記記憶されたレコードがオフセット値を有するユーザ選好を含み、

前記受信したコード値の規則的配列を検証する前記ステップが、

前記記憶されたレコード内の前記ユーザ定義のキーワードに基づいて対応するコード値の配列を生成すること、

前記コードセットの前記数値に記号をマップしている前記１回限りのセキュリティマトリクスを生成すること、および、

前記オフセット値に基づいて変更されたコード値の計算すること、

を含む請求項７に記載の方法。
【請求項９】
前記ユーザと関連する前記記憶されたレコードがクロール値を有するユーザ選好を含み、
前記受信したコード値の規則的配列を検証する前記ステップが、
前記記憶されたレコード内の前記ユーザ定義のキーワードに基づいて対応するコード値の配列を生成すること、
前記コードセットの前記数値に記号をマップしている前記１回限りのセキュリティマトリクスを生成すること、および、
前記クロール値に基づいて変更されたコード値を計算すること、
を含む請求項７に記載の方法。
【請求項１０】
前記ユーザと関連する前記記憶されたレコードがジャンプ値を有するユーザ選好を含み、
前記受信したコード値の規則的配列を検証する前記ステップが、
前記記憶されたレコード内の前記ユーザ定義のキーワードに基づいて対応するコード値の配列を生成すること、
前記コードセットの前記数値に記号をマップしている前記１回限りのセキュリティマトリクスを生成すること、および、
前記ジャンプ値に基づいて変更されたコード値を計算すること、
を含む請求項７に記載の方法。
【請求項１１】
前記ユーザと関連する前記記憶されたレコードがマスク値を有するユーザ選好を含み、
前記受信したコード値の規則的配列を検証する前記ステップが、
前記記憶されたレコード内の前記ユーザ定義のキーワードに基づいて対応するコード値の順序を生成すること、
前記コードセットの前記数値に記号をマップしている前記１回限りのセキュリティマトリクスを生成すること、および、
前記マスク値に基づいて変更されたコード値を計算すること、
を含む請求項７に記載の方法。
【請求項１２】
前記ユーザと関連する前記記憶されたレコードが、前記所定の記号セットから選択される記号の規則的配列からなる代替のユーザ定義のキーワードを含み、
前記受信したコード値の規則的配列を検証する前記ステップが、
前記記憶されたレコード内の前記代替のユーザ定義のキーワード、前記コード値複雑さ選好データ、および前記１回限りのセキュリティマトリクスに基づいて、前記処理システムによって生成されるが送信されない、対応するコード値の配列との比較を実行すること、ならびに、
前記比較結果が一致する場合に、パニック指示を含む前記認証セッションの前記認証結果を生成すること、
をさらに含む請求項７に記載の方法。
【請求項１３】
データストアおよび処理装置を含むユーザ認証装置（３０）であって、
前記データストアが１つ以上のレコードを含み、前記各データストアは、一意の識別子によってユーザと関連し、少なくともコード値複雑さ選好データ（４０）およびユーザ定義のキーワード（４１）を含み、前記キーワードは、前記処理システムによってサポートされた１つ以上の記号セットから選択される所定の記号セットの要素を含む、記号の規則的配列からなり、前記記号の規則的配列は、事前に前記ユーザによって、他のユーザの選択とは独立して選択され、
前記処理装置が処理ユニットおよび記憶されたプログラム命令を含み、前記プログラム

命令が実行された場合、前記処理ユニットが、
認証セッションを開始するためのユーザからの要求を受信し（１６０）、前記要求は前記ユーザと関連する前記一意の識別子を含み、
前記ユーザと関連する前記一意の識別子と前記記憶されたレコードを使用して前記データストアにアクセスし、
前記認証セッション中の前記ユーザに対してだけ有効である、１回限りのセキュリティマトリクスを生成し（１６２）、前記１回限りのセキュリティマトリクスは前記記号セット内の各記号とコード値との間でのマッピングを含み、前記コード値は、前記認証セッションに特有であり、前記記号セットとは異なるコードセットからランダムに選択され、
前記ユーザへ提示するために、前記１回限りのセキュリティマトリクスを送信し（１６４ａ）、
前記１回限りのセキュリティマトリクスの提示に応答し、前記ユーザ定義のキーワードおよび前記コード値複雑さ選好データに基づいて、前記１回限りのセキュリティマトリクスから選択され前記ユーザによって入力されるコード値の規則的配列（１２）を受信し、
前記記憶されたレコード内の前記ユーザ定義のキーワード、前記コード値複雑さ選好データ、および前記１回限りのセキュリティマトリクスに基づいて生成されるが送信されない、対応するコード値の配列との比較によって、前記受信したコード値の規則的配列を検証し（１７４）、
前記比較に基づいて前記認証セッションの認証結果を生成する（１７８）
ユーザ認証装置（３０）。
【請求項１４】
請求項１３に記載のユーザ認証装置およびユーザが認証を要求するセキュアシステム（２０）を含むセキュリティシステムであって、
前記セキュアシステムが、
前記ユーザの一意の識別子を受信し、
認証セッションを開始するための要求を前記ユーザ認証装置に送信し、前記要求が前記ユーザの前記一意の識別子を含み、
前記ユーザ認証装置から前記１回限りのセキュリティマトリクスを受信し、
前記１回限りのセキュリティマトリクスを前記ユーザに提示し、
前記ユーザから、前記１回限りのセキュリティマトリクスから選択されたコード値の規則的配列を受信し、
前記コード値の規則的配列を前記ユーザ認証装置に送信し、
前記ユーザ認証装置から前記認証結果を受信する
セキュリティシステム。
【請求項１５】
前記セキュアシステムが、ウェブ・サーバ・インタフェース、現金自動預払機（１０２ａ、１０２ｂ）、または売り場の端末装置（１０４）の１つを含み、
前記ウェブ・サーバ・インタフェースは、前記ユーザからの入力を受信し、前記１回限りのセキュリティマトリクスが前記ユーザによって操作されるウェブブラウザ（１１０、１１２）を介して前記ユーザに提示される
請求項１４に記載のセキュリティシステム。

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IB2012/052006

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/32(2006.01)i

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)
H04L 9/32; G06F 21/00; G06F 7/04

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Korean utility models and applications for utility models
Japanese utility models and applications for utility models

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
eKOMPASS(KIPO internal) & Keywords: authentication, one-time, login and matrix.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 8041954 B2 (PLESMAN PAUL) 18 October 2011 See claim 1, column 7, lines 57-67, column 8, lines 11-13,22-26,32-36 and figures 3-4.	1-4,6,8-9,19-28
Y	US 8042159 B2 (BASNER CHARLES M. et al.) 18 October 2011 See claims 1-2,16.	1-4,6,8-9,19-28
A	US 2011-0197266 A1 (CHU RONALD KING-HANG et al.) 11 August 2011 See claims 1,11,18 and figures 1-5.	1-28

☐ 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 application or patent 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 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
21 JANUARY 2013 (21.01.2013)	**22 JANUARY 2013 (22.01.2013)**
Name and mailing address of the ISA/KR Korean Intellectual Property Office 189 Cheongsa-ro, Seo-gu, Daejeon Metropolitan City, 302-701, Republic of Korea Facsimile No. 82-42-472-7140	Authorized officer Yang, Jong Phil Telephone No. 82-42-481-8595

Form PCT/ISA/210 (second sheet) (July 2009)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/IB2012/052006

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 8041954 B2	18.10.2011	US 2009-013402 A1	08.01.2009
US 8042159 B2	18.10.2011	US 2008-229397 A1	18.09.2008
US 2011-0197266 A1	11.08.2011	None	

フロントページの続き

(81)指定国 AP(BW,GH,GM,KE,LR,LS,MW,MZ,NA,RW,SD,SL,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,MD,RU,TJ,TM),EP(AL,AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HR,HU,IE,IS,IT,LT,LU,LV,MC,MK,MT,NL,NO,PL,PT,RO,RS,SE,SI,SK,SM,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AO,AT,AU,AZ,BA,BB,BG,BH,BR,BW,BY,BZ,CA,CH,CL,CN,CO,CR,CU,CZ,DE,DK,DM,DO,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,GT,HN,HR,HU,ID,IL,IN,IS,JP,KE,KG,KM,KN,KP,KR,KZ,LA,LC,LK,LR,LS,LT,LU,LY,MA,MD,ME,MG,MK,MN,MW,MX,MY,MZ,NA,NG,NI,NO,NZ,OM,PE,PG,PH,PL,PT,QA,RO,RS,RU,RW,SC,SD,SE,SG,SK,SL,SM,ST,SV,SY,TH,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC,VN

(72)発明者 アントニー、スメールズ
オーストラリア連邦ビクトリア州、フランクストン、ハイランド、ドライブ、２６

Ｆターム(参考) 5J104 AA07 AA16 AA32 EA03 EA04 EA18 JA03 KA01 KA06 KA21
NA02 NA05 NA20 NA36 NA37 NA38 PA07