(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2019-512961
(P2019-512961A)
(43)公表日　令和1年5月16日(2019.5.16)

| (51)Int.Cl. | | | F I | | | テーマコード（参考） |
|---|---|---|---|---|---|---|
| H04L | 9/32 | (2006.01) | H04L | 9/00 | 675A | 5J104 |
| G09C | 1/00 | (2006.01) | G09C | 1/00 | 640E | |
| H04L | 9/08 | (2006.01) | H04L | 9/00 | 601B | |
| | | | H04L | 9/00 | 601E | |

審査請求 未請求　予備審査請求 未請求　（全 35 頁）

(21)出願番号　特願2018-549219 (P2018-549219)
(86)(22)出願日　平成29年3月17日 (2017.3.17)
(85)翻訳文提出日　平成30年11月8日 (2018.11.8)
(86)国際出願番号　PCT/AU2017/050240
(87)国際公開番号　WO2017/156590
(87)国際公開日　平成29年9月21日 (2017.9.21)
(31)優先権主張番号　2016901019
(32)優先日　平成28年3月18日 (2016.3.18)
(33)優先権主張国　オーストラリア(AU)

(71)出願人　514264950
フォーティコード、リミテッド
ＦＯＲＴＩＣＯＤＥ　ＬＩＭＩＴＥＤ
オーストラリア連邦ビクトリア州、メルボルン、ウィリアム、ストリート、２２、レベル、７
(74)代理人　100112737
弁理士　藤田　考晴
(74)代理人　100136168
弁理士　川上　美紀
(74)代理人　100196117
弁理士　河合　利恵

最終頁に続く

(54)【発明の名称】改善されたセキュリティーを伴うユーザ認証のための方法およびシステム

(57)【要約】
分散処理システムにおけるユーザ認証方法が、認証セッションを開始したいという要求（１００４）を第１の処理ユニット（１０８）において受信することによって開始し、この要求は、認証を必要としているユーザの一意の識別子を含む。第１の処理ユニットは、認証セッション中に有効である認証データ（４１２、１７１２）の少なくとも１つのアイテムを取得する。認証データは、ユーザによって操作される端末デバイスに関連付けられている第２の処理ユニット（１０６）へ送信される（１００６）。第２の処理ユニットは、１つまたは複数のセッション固有の認証ファクタ（４０４、１７０４）に基づいて変換アルゴリズムを使用して認証データを変換して、認証セッションの、およびユーザの特徴である変換された認証データを生成する。変換された認証データは、第３の処理ユニット（１０８）へ送信され（１００８）、第３の処理ユニット（１０８）は、変換された認証データが、ユーザに、および１つまたは複数のセッション固有の認証ファクタの所定の値に対応することを検証する。第３の処理ユニットは、検証に基づいて認証セッ

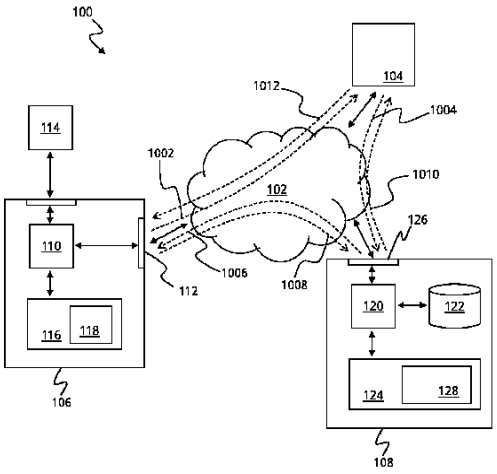



Figure 1

【特許請求の範囲】
【請求項１】
認証セッションを開始したいという要求を第１の処理ユニットにおいて受信するステップであって、前記要求が、認証を必要としているユーザの一意の識別子を含むステップと、
前記第１の処理ユニットが、前記認証セッション中に有効な認証データの少なくとも１つのアイテムを取得するステップと、
前記ユーザによって操作される端末デバイスに関連付けられている第２の処理ユニットへ前記認証データを送信するステップと、
前記第２の処理ユニットが、１つまたは複数のセッション固有の認証ファクタに基づいて変換アルゴリズムを使用して前記認証データを変換し、前記認証セッションの、および前記ユーザの特徴である変換された認証データを生成するステップと、
前記変換された認証データを第３の処理ユニットへ送信するステップと、
前記変換された認証データが、前記ユーザに、および前記１つまたは複数のセッション固有の認証ファクタの所定の値に対応することを前記第３の処理ユニットが検証するステップと、
前記第３の処理ユニットが、前記検証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と
を有する分散処理システムによるユーザ認証方法。
【請求項２】
秘密のキーワードが、前記ユーザに関連付けられており、前記秘密のキーワードが、所定のシンボル・セットから選択されたシンボルの順序付けられたシーケンスから構成されており、
認証データの前記少なくとも１つのアイテムが、前記シンボル・セット内のそれぞれのシンボルと、前記シンボル・セットとは別個のものであるコード・セットから選択される、前記認証セッションに固有であるコード値との間におけるマッピングを含むセキュリティー・マトリックスを含み、
前記セキュリティー・マトリックスが、前記第１の処理ユニットによって前記１つまたは複数のセッション固有の認証ファクタの前記所定の値に基づいて変換アルゴリズムを使用して変換されて、前記シンボル・セットおよび変換されたコード値を含む変換されたセキュリティー・マトリックスが生成され、
前記第２の処理ユニットの前記変換アルゴリズムが、前記セキュリティー・マトリックスの前記コード値を復元するように構成されている逆変換アルゴリズム、ならびに、前記セキュリティー・マトリックスから選択されたコード値のシーケンス、および前記ユーザによる入力を受信するためのユーザ入力ステップを含み、前記コード値が、前記秘密のキーワードに対応し、
前記検証するステップが、前記ユーザ入力ステップにおいて受信されたコード値の前記シーケンスを、前記秘密のキーワード、およびそれの前記セキュリティー・マトリックス内の前記コード値へのマッピングに対応するコード値の予想されるシーケンスとの比較によって確認するステップを含む請求項１に記載のユーザ認証方法。
【請求項３】
前記認証データが、前記１つまたは複数のセッション固有の認証ファクタの前記所定の値によってパラメータ化される変換アルゴリズムを使用して前記第１の処理ユニットによって暗号化されているセッション固有のワンタイム・コード・ワードを含み、
前記第２の処理ユニットの前記変換アルゴリズムが、前記セッション固有のワンタイム・コード・ワードを復号するように構成されている逆変換アルゴリズム、および前記ユーザのプライベート暗号化キーが適用されて、前記セッション固有のワンタイム・コード・ワードの署名されたコピーを含む前記変換された認証データが生成される暗号署名ステップを含み、
前記検証するステップが、前記ユーザのパブリック暗号化キーが適用されて、前記ユー

ザによって操作される前記端末デバイスに関連付けられている前記第２の処理ユニットによって前記セッション固有のワンタイム・コード・ワードの前記署名されたコピーが生成されたことが確認される暗号検証を含む請求項１に記載のユーザ認証方法。
【請求項４】
前記１つまたは複数のセッション固有の認証ファクタが、
前記ユーザによって操作される前記端末デバイスの地理的ロケーション、
前記ユーザによって操作される前記端末デバイスにとって見えるワイヤレス・ネットワークの１つまたは複数のサービス・セット識別子（ＳＳＩＤ）、
前記端末デバイスが接続されているワイヤレス・ネットワークのＳＳＩＤ、
前記端末デバイスが接続されているモバイル・セルラー・キャリアの識別情報、
前記ユーザによって操作される前記端末デバイスに関連付けられている一意の識別子、
前記ユーザの前記一意の識別子、
所定のデバイスまたはユーザに固有のキー値、
所定のアルゴリズムに従って生成される変化する値、
時刻および／または日付、
前記端末デバイスにとってアクセス可能なローカル・ビーコンまたはネットワーク接続デバイスによって提供されるデータ、ならびに
前記ユーザのバイオメトリック・データのうちの少なくとも１つを含む請求項１に記載のユーザ認証方法。
【請求項５】
前記第１の処理ユニットが、サービス・プロバイダ・コンピュータ・システムのプロセッサおよび／または認証サーバ・システムのプロセッサ上で実行する命令コードを含み、
前記第２の処理ユニットが、前記ユーザによって操作される前記端末デバイスのプロセッサ上で実行する命令コードを含む請求項１に記載のユーザ認証方法。
【請求項６】
前記ユーザによって操作される前記端末デバイスが、前記ユーザによって携帯されるポータブル・デバイスである請求項５に記載のユーザ認証方法。
【請求項７】
前記第３の処理ユニットが、サービス・プロバイダ・コンピュータ・システムのプロセッサおよび／または認証サーバ・システムのプロセッサ上で実行する命令コードを含む請求項１に記載のユーザ認証方法。
【請求項８】
プロセッサと、
該プロセッサに動作可能に関連付けられているネットワーク・インターフェースと、
前記プロセッサによってアクセス可能な少なくとも１つのコンピュータ可読ストレージ・デバイスと
を含む認証システムであって、
前記ストレージ・デバイスが、前記プロセッサによって実行可能な命令コードを含み、該命令コードが、
認証セッションを開始したいという要求を、前記ネットワーク・インターフェースを介して受信するステップであって、前記要求が、認証を必要としているユーザの一意の識別子を含むステップと、
前記認証セッション中に有効な認証データの少なくとも１つのアイテムを取得するステップと、
前記ユーザによって操作される端末デバイスに関連付けられている処理ユニットへ前記ネットワーク・インターフェースを介して前記認証データを送信するステップと、
前記ユーザによって操作される前記端末デバイスに関連付けられている前記処理ユニットによって生成された変換された認証データを、前記ネットワーク・インターフェースを介して受信するステップであって、前記変換された認証データが、前記認証セッションの、および前記ユーザの特徴である、ステップとを含む方法を前記プロセッサに実施させ

るように構成されており、
前記変換された認証データが、自分が前記ユーザに、および前記１つまたは複数のセッション固有の認証ファクタの所定の値に対応する旨の検証を可能にするように構成されており、
前記検証に基づいて前記認証セッションに関して認証結果が生成されることが可能である認証システム。
【請求項９】
前記プロセッサによって実行可能な前記命令コードが、
セッション固有のワンタイム・コード・ワードを生成するステップと、
前記１つまたは複数のセッション固有の認証ファクタの前記所定の値を前記少なくとも１つのコンピュータ可読ストレージ・デバイスから取り出すステップと、
前記１つまたは複数のセッション固有の認証ファクタの前記所定の値によってパラメータ化される変換アルゴリズムを使用して前記ワンタイム・コード・ワードを暗号化するステップとによって、認証データの前記少なくとも１つのアイテムを取得する前記ステップを前記プロセッサに実施させるように構成されている請求項８に記載の認証システム。
【請求項１０】
前記変換された認証データは、自分が、前記ユーザのプライベート暗号化キーを使用して暗号で署名されている前記セッション固有のワンタイム・コード・ワードに対応することを確認することによる検証を可能にするように構成されている請求項９に記載の認証システム。
【請求項１１】
プロセッサと、
該プロセッサに動作可能に関連付けられているネットワーク・インターフェースと、
前記プロセッサによってアクセス可能な少なくとも１つのコンピュータ可読ストレージ・デバイスと
を含むポータブル個人認証デバイスであって、
前記ストレージ・デバイスが、前記プロセッサによって実行可能な命令コードを含み、該命令コードが、
認証セッション中に有効である認証データを認証システムから前記ネットワーク・インターフェースを介して受信するステップと、
１つまたは複数のセッション固有の認証ファクタに基づいて変換アルゴリズムを使用して前記認証データを変換して、前記認証セッションの、およびユーザの特徴である変換された認証データを生成するステップと、
前記ネットワーク・インターフェースを介して前記認証システムへ前記変換された認証データを送信するステップとを含む方法を前記認証デバイスのユーザの認証セッションにおいて前記プロセッサに実施させるように構成されており、
前記変換された認証データが、自分が前記ユーザに、および前記１つまたは複数のセッション固有の認証ファクタの所定の値に対応する旨の検証を可能にするように構成されており、
前記検証に基づいて前記認証セッションに関して認証結果が生成されることが可能であるポータブル個人認証デバイス。
【請求項１２】
前記認証データが、暗号化されたセッション固有のワンタイム・コード・ワードを含み、前記プロセッサによって実行可能な前記命令コードが、
前記ポータブル個人認証デバイスの現在のコンテキストに基づく前記１つまたは複数のセッション固有の認証ファクタの値を特定するステップと、
前記１つまたは複数のセッション固有の認証ファクタの前記特定された値によってパラメータ化されるアルゴリズムを適用して、前記認証データを復号し、前記セッション固有のワンタイム・コード・ワードを復元するステップと、
前記ポータブル個人認証デバイスのセキュア・ストレージ内に保持されている前記ユー

ザのプライベート暗号化キーを適用して、前記認証システムへの送信のために前記セッション固有のワンタイム・コード・ワードの署名されたコピーを生成するステップとによって、前記認証データを変換する前記ステップを前記プロセッサに実施させるように構成されている請求項１１に記載のポータブル個人認証デバイス。

【請求項１３】

前記１つまたは複数のセッション固有の認証ファクタが、

前記ユーザによって操作される端末デバイスの地理的ロケーション、

前記ユーザによって操作される前記端末デバイスにとって見えるワイヤレス・ネットワークの１つまたは複数のサービス・セット識別子（ＳＳＩＤ）、

前記端末デバイスが接続されているワイヤレス・ネットワークのＳＳＩＤ、

前記端末デバイスが接続されているモバイル・セルラー・キャリアの識別情報、

前記ユーザによって操作される前記端末デバイスに関連付けられている一意の識別子、

前記ユーザの前記一意の識別子、

所定のデバイスまたはユーザに固有のキー値、

所定のアルゴリズムに従って生成される変化する値、

時刻および／または日付、

前記端末デバイスにとってアクセス可能なローカル・ビーコンまたはネットワーク接続デバイスによって提供されるデータ、ならびに

前記ユーザのバイオメトリック・データのうちの少なくとも１つを含む、請求項１２に記載のポータブル個人認証デバイス。

【請求項１４】

格納されているプログラム命令を含む有形のコンピュータ可読メディアであって、前記プログラム命令が、認証システムのプロセッサによって実行されたときに、

認証セッションを開始したいという要求を、前記認証システムのネットワーク・インターフェースを介して受信するステップであって、前記要求が、認証を必要としているユーザの一意の識別子を含む、ステップと、

前記認証セッション中に有効な認証データの少なくとも１つのアイテムを取得するステップと、

前記ユーザによって操作される端末デバイスに関連付けられている処理ユニットへ前記ネットワーク・インターフェースを介して前記認証データを送信するステップと、

前記ユーザによって操作される前記端末デバイスに関連付けられている前記処理ユニットによって生成された変換された認証データを、前記ネットワーク・インターフェースを介して受信するステップであって、前記変換された認証データが、前記認証セッションの、および前記ユーザの特徴である、ステップとを含む方法を前記認証システムに実施させ、

前記変換された認証データが、自分が前記ユーザに、および前記１つまたは複数のセッション固有の認証ファクタの所定の値に対応する旨の検証を可能にするように構成されており、

前記検証に基づいて前記認証セッションに関して認証結果が生成されることが可能である有形のコンピュータ可読メディア。

【請求項１５】

格納されているプログラム命令を含む有形のコンピュータ可読メディアであって、前記プログラム命令が、ポータブル個人識別デバイスのプロセッサによって実行されたときに、

認証セッション中に有効である認証データを認証システムから前記デバイスのネットワーク・インターフェースを介して受信するステップと、

１つまたは複数のセッション固有の認証ファクタに基づいて変換アルゴリズムを使用して前記認証データを変換して、前記認証セッションの、およびユーザの特徴である変換された認証データを生成するステップと、

前記ネットワーク・インターフェースを介して前記認証システムへ前記変換された認証

データを送信するステップとを含む方法を前記デバイスに実施させ、
前記変換された認証データが、自分が前記ユーザに、および前記１つまたは複数のセッション固有の認証ファクタの所定の値に対応する旨の検証を可能にするように構成されており、
前記検証に基づいて前記認証セッションに関して認証結果が生成されることが可能である有形のコンピュータ可読メディア。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、全般的には認証システムおよび方法に関し、より詳細には、改善されたセキュリティーおよび柔軟性を伴うマルチファクタ認証システムに関する。
【背景技術】
【０００２】
個人の身元の信頼できるセキュアな認証は、多くのオンライン・システムの必須の要素である。一般に、オンライン・システムまたはサービスの承認されるユーザは、少なくともユーザ識別子、たとえばユーザ名またはコードと、パスワードもしくは暗証番号（ＰＩＮ）などのさらなる「秘密の」コードとを提供することを必要とされる。ＰＩＮまたはパスワードは、ユーザが、認証のために、秘密、すなわち、パスワード、フレーズ、またはＰＩＮの知識を証明することを必要とされる知識ファクタの例である。
【０００３】
知識ファクタは、たとえば傍受による攻撃の影響を受けやすい。傍受の最も基本的な形態は、パスワードまたはＰＩＮを入力しているときのユーザを観察することを含み得る。観察は、直接に実行されることが可能であり、または隠されたカメラの使用を含み得る。より技術的に洗練された傍受技術は、いわゆる「中間者」攻撃を含み、「中間者」攻撃においては、悪意あるソフトウェアが、暗号化されていないパスワードがデータ送信中にアクセスされることが可能であるシステム・コンポーネントをターゲットとして、端末機器および／または中間ネットワーク・ノードにインストールされる。ユーザは、たとえばフィッシング攻撃を介して、知識ファクタを明らかにすることへと欺かれる可能性もある。
【０００４】
強化されたセキュリティーを伴う認証方法は、２ファクタ認証を含み、２ファクタ認証においては、ユーザは、身元の証明として１つまたは複数のさらなるファクタを提供することを必要とされる。たとえば、知識ファクタに加えて、所有ファクタ（「ユーザが持っている何か」）が最も一般的に使用されている。所有ファクタの例は、クレジット・カードなどを含み、それらは、取引システムにアクセスするためにはＰＩＮと併せて提示されなければならない。所有ファクタのその他の形態は、ユーザによる入力のための定期的に更新される乱数を表示するディスコネクトされたトークン（ｄｉｓｃｏｎｎｅｃｔｅｄ　ｔｏｋｅｎ）、およびセルラー・モバイル電話またはスマートフォンなどの一意に識別可能な個人のアイテムを含む。所有ファクタは、セキュリティーを著しく高めるが、それでもなお盗難および複製（たとえばカード・スキミング）の影響を受けやすい。
【０００５】
傍受に対するさらなる保護を提供する、知識ファクタのセキュリティーにおける改良が、本発明者の本願の譲受人に譲渡された特許文献１および特許文献２において開示されており、これらの特許文献の両方は、それらの全体が参照によって本明細書に組み込まれている。そのようなシステムは、所有ファクタなどのさらなるファクタの使用を通じてさらに強化されることが可能である。しかしながら、認証システムおよび方法に対するさらなる改良のための余地が残っている。たとえば、ユーザの身元以外のファクタに基づいて、セキュア・システムへのアクセスを制御または制限することが望ましいかもしれない。たとえば、ユーザが、承認されたデバイスを使用してしかセキュア・システムにアクセスできないことを確実にすること、および／またはセキュアなロケーションにユーザがいる間しかアクセスできないことを確実にすることが望ましいかもしれない。同時に、ユーザ・

クレデンシャルおよびその他のファクタが中間者攻撃などの傍受によって取得されることが不可能であることを確実にすることが望ましいかもしれない。そのようなさらなるセキュリティーが、エンドユーザにとってトランスペアレントである様式で提供され、それによって、正当な承認されているユーザに提示されるさらなる不便または障害がないことが好ましい。

【先行技術文献】

【特許文献】

【０００６】

【特許文献１】米国特許第８，８６９，２５５号明細書

【特許文献２】米国特許第９，５１９，７６４号明細書

【発明の概要】

【発明が解決しようとする課題】

【０００７】

したがって、本発明の目的は、強化された認証システムおよび方法に対する前述の必要性に対処することである。

【課題を解決するための手段】

【０００８】

一態様においては、本発明は、認証セッションを開始したいという要求を第１の処理ユニットにおいて受信するステップであって、この要求が、認証を必要としているユーザの一意の識別子を含む、ステップと、第１の処理ユニットが、認証セッション中に有効な認証データの少なくとも１つのアイテムを取得するステップと、ユーザによって操作される端末デバイスに関連付けられている第２の処理ユニットへ認証データを送信するステップと、第２の処理ユニットが、１つまたは複数のセッション固有の認証ファクタに基づいて変換アルゴリズムを使用して認証データを変換して、認証セッションの、およびユーザの特徴である変換された認証データを生成するステップと、変換された認証データを第３の処理ユニットへ送信するステップと、変換された認証データが、ユーザに、および１つまたは複数のセッション固有の認証ファクタの所定の値に対応することを第３の処理ユニットが検証するステップと、第３の処理ユニットが、検証に基づいて認証セッションの認証結果を生成するステップとを有する分散処理システムによるユーザ認証方法を提供する。

【０００９】

有利なことに、認証データの変換におけるセッション固有の認証ファクタの使用は、認証セッションの現在のコンテキストに関連付けられている情報がユーザ検証へと組み込まれることを可能にする。たとえば、第２の処理ユニットは、適切なソフトウェアを稼働させる専用のデジタル・アクセス・デバイス、または便利なことに、本発明の態様を具体化する必要とされる命令コードを提供するインストールされているアプリケーション（すなわち「アプリ」）を有するスマートフォンもしくはその他のパーソナル・デバイスなど、ユーザによって操作されるポータブル・パーソナル・デバイスのプロセッサ上で実行する命令コードを含むことができる。したがって、現在のコンテキスト情報は、デバイスの地理的ロケーション、デバイスにとって見えるワイヤレス・ネットワークのサービス・セット識別子（ＳＳＩＤ）、および／またはデバイスに関連付けられている一意の識別子などのファクタに対応する値を含むことができる。より一般的には、デバイス上で実行するソフトウェア・コードにとってアクセス可能な任意のコンテキスト固有の情報が、セッション固有の認証ファクタとして採用されることが可能である。

【００１０】

いくつかの実施形態においては、秘密のキーワード（たとえば、パスワードまたはパスフレーズ）が、ユーザに関連付けられており、この秘密のキーワードは、所定のシンボル・セットから選択されたシンボルの順序付けられたシーケンスから構成されており、認証データの少なくとも１つのアイテムは、シンボル・セット内のそれぞれのシンボルと、シンボル・セットとは別個のものであるコード・セットから選択される、認証セッションに固有であるコード値との間におけるマッピングを含むセキュリティー・マトリックスを含

み、セキュリティー・マトリックスは、第１の処理ユニットによって１つまたは複数のセッション固有の認証ファクタの所定の値に基づいて変換アルゴリズムを使用して変換されて、シンボル・セットおよび変換されたコード値を含む変換されたセキュリティー・マトリックスが生成され、第２の処理ユニットの変換アルゴリズムは、セキュリティー・マトリックスのコード値を復元するように構成されている逆変換アルゴリズム、ならびに、セキュリティー・マトリックスから選択されたコード値のシーケンス、およびユーザによる入力を受信するためのユーザ入力ステップを含み、コード値は、秘密のキーワードに対応し、検証ステップは、ユーザ入力ステップにおいて受信されたコード値のシーケンスを、秘密のキーワード、およびそれのセキュリティー・マトリックス内のコード値へのマッピングに対応するコード値の予想されるシーケンスとの比較によって確認するステップを含む。

【００１１】

そのような実施形態においては、本願の譲受人に譲渡された特許文献１および特許文献２において開示されているタイプのキーワードベースのユーザ認証方法においてシンボルとコード値との間におけるマッピングを「エンコードする」ためにセッション固有の認証ファクタが適用される。したがって第２の処理ユニット（たとえば、ユーザによって操作されるポータブル・パーソナル・デバイス）は、マッピングを正しく「デコードする」ためにセッション固有の認証ファクタの同じコンテキストベースの値を特定して適用しなければならない。たとえば、ロケーションベースの認証ファクタが適用される場合には、第１の処理ユニットは、ユーザが成功裏に認証されることが可能であるロケーションのＧＰＳ座標など、このファクタの所定の値を使用して、マッピングをエンコードすることになる。ポータブル・デバイス（すなわち、第２の処理ユニット）は、たとえば内蔵ＧＰＳ受信機ハードウェアを使用することによって、自分自身のロケーションを特定し、結果として生じる座標を適用してマッピングをデコードすることになる。デバイスは、マッピングをエンコードするために使用されたＧＰＳ座標の値を知らず、自分自身のロケーションがそれらの座標にマッチした場合にのみ、正しいデコードされたマッピングを入手することになる。したがってユーザは、承認されたロケーションに存在する場合にのみ、成功裏に認証することが可能になる。

【００１２】

代替実施形態においては、認証データは、１つまたは複数のセッション固有の認証ファクタの所定の値によってパラメータ化される変換アルゴリズムを使用して第１の処理ユニットによって暗号化されているセッション固有のワンタイム・コード・ワードを含み、第２の処理ユニットの変換アルゴリズムは、セッション固有のワンタイム・コード・ワードを復号するように構成されている逆変換アルゴリズム、およびユーザのプライベート暗号化キーが適用されて、セッション固有のワンタイム・コード・ワードの署名されたコピーを含む変換された認証データが生成される暗号署名ステップを含み、検証ステップは、ユーザのパブリック暗号化キーが適用されて、ユーザによって操作される端末デバイスに関連付けられている第２の処理ユニットによってセッション固有のワンタイム・コード・ワードの署名されたコピーが生成されたことが確認される暗号検証を含む。

【００１３】

そのような実施形態の特定の利点は、ユーザがセキュア・システムにアクセスするために秘密のキーワード（たとえば、パスワードまたはパスフレーズ）を提供するためのいかなる要件からも独立してセッション固有の認証ファクタが適用されることが可能であるということである。例示的なシナリオにおいては、ユーザは、雇用主によって提供されているリモート・デスクトップ・サービスなどのオンライン・サービスにアクセスしたいと望む場合があるが、ホーム・オフィスなど、認可されたロケーション以外でこれを行うことを制限される場合がある。ユーザによってサービスにログインする試みに際して、第２の処理ユニット（たとえば認証サーバ）は、たとえば２５６ビットまたは５１２ビットの乱数など、セッション固有のワンタイム・コード・ワード（すなわちノンス）を生成することができる。次いで第２の処理ユニットは、ユーザのホーム・オフィスのＧＰＳ座標など

、セッション固有の認証ファクタの所定の値からキーが導き出される対称暗号化アルゴリズムを使用してノンスを暗号化することができる。結果として生じる認証データを受信すると、ユーザのポータブル・デバイス（すなわち第２の処理ユニット）は、自分自身のロケーションを特定し、結果として生じる座標を適用して、ノンスを復号するために対称暗号化アルゴリズムにおいて使用するためのキーを生成することになる。デバイスは、元の暗号化キーを生成するために使用されたＧＰＳ座標の値を知らず、自分自身のロケーションがそれらの座標にマッチした場合にのみ、ノンスを成功裏に復号することになる。格納されているプライベート・キーを用いて、結果として生じる復号されたノンスに署名することによって、デバイスは、自分がノンスを成功裏に復号することができた旨のその後の検証を可能にする。したがってユーザは、承認されたロケーションに自分のポータブル・デバイスを伴って存在する場合にのみ、成功裏に認証することが可能になる。

【００１４】

別の態様においては、本発明は、プロセッサと、プロセッサに動作可能に関連付けられているネットワーク・インターフェースと、プロセッサによってアクセス可能な少なくとも１つのコンピュータ可読ストレージ・デバイスとを含む認証システムを提供し、ストレージ・デバイスは、プロセッサによって実行可能な命令コードを含み、この命令コードは、認証セッションを開始したいという要求を、ネットワーク・インターフェースを介して受信するステップであって、その要求が、認証を必要としているユーザの一意の識別子を含む、ステップと、認証セッション中に有効な認証データの少なくとも１つのアイテムを取得するステップと、ユーザによって操作される端末デバイスに関連付けられている処理ユニットへネットワーク・インターフェースを介して認証データを送信するステップと、ユーザによって操作される端末デバイスに関連付けられている処理ユニットによって生成された変換された認証データを、ネットワーク・インターフェースを介して受信するステップであって、変換された認証データが、認証セッションの、およびユーザの特徴である、ステップとを含む方法をプロセッサに実施させるように構成されており、変換された認証データは、自分がユーザに、および１つまたは複数のセッション固有の認証ファクタの所定の値に対応する旨の検証を可能にするように構成されており、検証に基づいて認証セッションに関して認証結果が生成されることが可能である。

【００１５】

いくつかの実施形態においては、プロセッサによって実行可能な命令コードは、セッション固有のワンタイム・コード・ワードを生成するステップと、１つまたは複数のセッション固有の認証ファクタの所定の値を少なくとも１つのコンピュータ可読ストレージ・デバイスから取り出すステップと、１つまたは複数のセッション固有の認証ファクタの所定の値によってパラメータ化される変換アルゴリズムを使用してワンタイム・コード・ワードを暗号化するステップとによって、認証データの少なくとも１つのアイテムを取得するステップをプロセッサに実施させるように構成されている。

【００１６】

変換された認証データは、自分が、ユーザのプライベート暗号化キーを使用して暗号で署名されているセッション固有のワンタイム・コード・ワードに対応することを確認することによる検証を可能にするように構成されることが可能である。

【００１７】

さらに別の態様においては、本発明は、プロセッサと、プロセッサに動作可能に関連付けられているネットワーク・インターフェースと、プロセッサによってアクセス可能な少なくとも１つのコンピュータ可読ストレージ・デバイスとを含むポータブル個人認証デバイスを提供し、ストレージ・デバイスは、プロセッサによって実行可能な命令コードを含み、この命令コードは、認証セッション中に有効である認証データを認証システムからネットワーク・インターフェースを介して受信するステップと、１つまたは複数のセッション固有の認証ファクタに基づいて変換アルゴリズムを使用して認証データを変換して、認証セッションの、およびユーザの特徴である変換された認証データを生成するステップと、ネットワーク・インターフェースを介して認証システムへ、変換された認証データを送

信するステップとを含む方法を認証デバイスのユーザの認証セッションにおいてプロセッサに実施させるように構成されており、変換された認証データは、自分がユーザに、および１つまたは複数のセッション固有の認証ファクタの所定の値に対応する旨の検証を可能にするように構成されており、検証に基づいて認証セッションに関して認証結果が生成されることが可能である。

【００１８】

本発明の実施形態においては、認証データは、暗号化されたセッション固有のワンタイム・コード・ワードを含み、プロセッサによって実行可能な命令コードは、ポータブル個人認証デバイスの現在のコンテキストに基づく１つまたは複数のセッション固有の認証ファクタの値を特定するステップと、１つまたは複数のセッション固有の認証ファクタの特定された値によってパラメータ化されるアルゴリズムを適用して、認証データを復号し、セッション固有のワンタイム・コード・ワードを復元するステップと、ポータブル個人認証デバイスのセキュア・ストレージ内に保持されているユーザのプライベート暗号化キーを適用して、認証システムへの送信のためにセッション固有のワンタイム・コード・ワードの署名されたコピーを生成するステップとによって、認証データを変換するステップをプロセッサに実施させるように構成されている。

【００１９】

さらなる態様においては、本発明は、格納されているプログラム命令を含む有形のコンピュータ可読メディアを提供し、それらのプログラム命令は、認証システムのプロセッサによって実行されたときに、認証セッションを開始したいという要求を、認証システムのネットワーク・インターフェースを介して受信するステップであって、その要求が、認証を必要としているユーザの一意の識別子を含む、ステップと、認証セッション中に有効な認証データの少なくとも１つのアイテムを取得するステップと、ユーザによって操作される端末デバイスに関連付けられている処理ユニットへネットワーク・インターフェースを介して認証データを送信するステップと、ユーザによって操作される端末デバイスに関連付けられている処理ユニットによって生成された変換された認証データを、ネットワーク・インターフェースを介して受信するステップであって、変換された認証データが、認証セッションの、およびユーザの特徴である、ステップとを含む方法を認証システムに実施させ、変換された認証データは、自分がユーザに、および１つまたは複数のセッション固有の認証ファクタの所定の値に対応する旨の検証を可能にするように構成されており、検証に基づいて認証セッションに関して認証結果が生成されることが可能である。

【００２０】

さらに別の態様においては、本発明は、格納されているプログラム命令を含む有形のコンピュータ可読メディアを提供し、それらのプログラム命令は、ポータブル個人識別デバイスのプロセッサによって実行されたときに、認証セッション中に有効である認証データを認証システムからデバイスのネットワーク・インターフェースを介して受信するステップと、１つまたは複数のセッション固有の認証ファクタに基づいて変換アルゴリズムを使用して認証データを変換して、認証セッションの、およびユーザの特徴である変換された認証データを生成するステップと、ネットワーク・インターフェースを介して認証システムへ、変換された認証データを送信するステップとを含む方法をデバイスに実施させ、変換された認証データは、自分がユーザに、および１つまたは複数のセッション固有の認証ファクタの所定の値に対応する旨の検証を可能にするように構成されており、検証に基づいて認証セッションに関して認証結果が生成されることが可能である。

【００２１】

本発明の実施形態のさらなる態様、利点、および特徴は、さまざまな実施形態についての以降の説明から、関連した技術分野における技術者にとって明らかになるであろう。しかしながら、本発明は、記述されている実施形態には限定されず、それらの実施形態は、前述の言明において、および添付の特許請求の範囲において定義されている本発明の原理を例示するために、ならびに当業者がこれらの原理を実際に実施するのを支援するために提供されているということが理解されるであろう。

【００２２】
次いで本発明の実施形態が、添付の図面を参照しながら記述されることになり、それらの図面においては、同様の参照番号は、同様の特徴を示している。
【図面の簡単な説明】
【００２３】
【図１】本発明を具体化する例示的なシステムを示す概略図である。
【図２】本発明の第１の実施形態による認証サーバにおいて実行されるユーザ認証方法のフローチャートである。
【図３】第１の実施形態によるエンドポイント・デバイスにおいて実行されるユーザ認証方法のフローチャートである。
【図４】第１の実施形態によるセッション固有の変換プロセスのフローチャートである。
【図５】第１の実施形態によるセッション固有のチャレンジ・メンションを構築するプロセスのフローチャートである。
【図６】第１の実施形態によるセッション固有の変換／暗号化キーを生成するための例示的な方法を示すフローチャートである。
【図７】第１の実施形態による例示的なセッション固有の逆変換プロセスを示すフローチャートである。
【図８】本発明を具体化する第１のチャレンジ・メッセージ・フォーマットの概略図である。
【図９】図８のメッセージ・フォーマットを具体化する例示的なＸＭＬコードを示す図である。
【図１０】第１の実施形態によるエンドポイント・デバイス、セキュア・システム、および認証サーバの間における通信のタイムラインを示す図である。
【図１１】第１の実施形態によるエンドポイント・ユーザ認証インターフェースの概略図である。
【図１２】例示的なユーザ・レコードを示す図である。
【図１３】例示的なセキュア・システム・レコードを示す図である。
【図１４】本発明を具体化する代替のユーザ認証システムおよび方法を示す概略図である。
【図１５】本発明のさらなる実施形態による認証サーバにおいて実行されるユーザ認証方法を示すフローチャートである。
【図１６】さらなる実施形態によるポータブル・デバイスにおいて実行されるユーザ認証方法を示すフローチャートである。
【図１７】さらなる実施形態によるセッション固有の暗号化プロセスを示すフローチャートである。
【図１８】さらなる実施形態によるセッション固有のチャレンジ・メッセージを構築するプロセスを示すフローチャートである。
【図１９】図１５および図１６の方法におけるセッション固有の暗号化／復号キーを生成するための例示的な方法を示すフローチャートである。
【図２０】ポータブル・デバイスによって生成された応答メッセージを受信したことに応答して認証サーバによって実行される認証の例示的なプロセスを示すフローチャートである。
【図２１】さらなる実施形態によるチャレンジ・メッセージ・フォーマットの概略図である。
【図２２】図２１のメッセージ・フォーマットを具体化する例示的なＸＭＬコードを示す図である。
【図２３】さらなる実施形態によるエンドポイント・デバイス、セキュア・システム、および認証サーバの間における通信のタイムラインを示す図である。
【発明を実施するための形態】
【００２４】

図１は、本発明を具体化するシステム１００を示すブロック図である。インターネットなどの公衆通信ネットワーク１０２が、セキュア・システム１０４、１つまたは複数のユーザ・エンドポイント・デバイス１０６、および認証サーバ１０８の間におけるメッセージングのために採用されている。一般的に言えば、ユーザ・エンドポイント・デバイス１０６は、たとえばウェブ・ブラウザ・ソフトウェアおよび／またはその他の接続されているアプリケーションを使用して、インターネット１０２を介して通信する能力を有している任意の適切なコンピューティング、通信、および／または処理アプライアンスであることが可能である。エンドポイント・デバイス１０６は、現金自動支払機（たとえばＡＴＭ）、ＰＯＳ（ｐｏｉｎｔ－ｏｆ－ｓａｌｅ）端末、自動販売機等などのその他のタイプの端末装置を含むこともできる。さらに、例示的なシステム１００は、すべての処理デバイスおよびシステムの間における通信のための単一の共有されているセキュアでないネットワーク１０２を含むが、本発明の実施形態は、金融取引ネットワーク、プライベート・ネットワーク、仮想プライベート・ネットワーク（ＶＰＮ）、セルラー・テレフォニー・ネットワーク、またはこれらおよび／もしくはその他の形態の通信システムの混合物など、その他のタイプの通信および／または取引ネットワークを含むことができる。

【００２５】

本明細書においては、「プロセッサ」、「コンピュータ」等などの用語は、文脈によってその他の形が必要とされていない限り、デバイス、装置、ならびに、ハードウェアおよびソフトウェアの組合せを含むシステムのある範囲の可能な実施態様を指すものとして理解されるべきである。これは、同一場所に配置されることまたは分散されることが可能である協働するハードウェアおよびソフトウェア・プラットフォームを含むポータブル・デバイス、デスクトップ・コンピュータ、およびさまざまなタイプのサーバ・システムを含むシングルプロセッサおよびマルチプロセッサ・デバイスおよび装置を含む。ハードウェアは、従来のパーソナル・コンピュータ・アーキテクチャー、またはその他の汎用ハードウェア・プラットフォームを含むことができる。ソフトウェアは、さまざまなアプリケーションおよびサービス・プログラムと組み合わされた市販のオペレーティング・システム・ソフトウェアを含むことができる。あるいは、コンピューティングまたは処理プラットフォームは、カスタムのハードウェアおよび／またはソフトウェア・アーキテクチャーを含むことができる。強化された拡張性のために、コンピューティングおよび処理システムは、物理的なハードウェア・リソースがサービス需要に応じて動的に割り当てられることを可能にするクラウド・コンピューティング・プラットフォームを含むことができる。これらのバリエーションのすべてが本発明の範囲内に収まるが、説明および理解を容易にするために、本明細書において記述されている例示的な実施形態は、シングルプロセッサの汎用コンピューティング・プラットフォーム、一般的に利用可能なオペレーティング・システム・プラットフォーム、および／または幅広く利用可能な消費者製品、たとえば、デスクトップＰＣ、ノートまたはラップトップＰＣ、スマートフォン、タブレット・コンピュータなどに基づいている。

【００２６】

とりわけ、「処理ユニット」という用語は、本明細書（特許請求の範囲を含む）においては、認証データを生成および送信すること、認証データを受信および処理すること、または認証データを受信および確認することなど、特定の定義されているタスクを実行するように構成されているハードウェアおよびソフトウェアの任意の適切な組合せを指すために使用されている。そのような処理ユニットは、単一の処理デバイス上の単一のロケーションにおいて実行する１つの実行可能コード・モジュールを含むことができ、または複数のロケーションにおいておよび／もしくは複数の処理デバイス上で実行する複数の協働する実行可能コード・モジュールを含むことができる。たとえば、本発明のいくつかの実施形態においては、認証処理が、認証サーバ１０８上で実行するコードによってもっぱら実行されることが可能であり、その一方でその他の実施形態においては、対応する処理が、セキュア・システム１０４および認証サーバ１０８上で実行する各コード・モジュールによって協働して実行されることが可能である。たとえば、本発明の実施形態は、セキュア

・システム１０４に認証サービスを提供するために、認証サーバ１０８上で実行するコード・モジュールと協働して動作するように構成されている、セキュア・システム１０４において、または別のサードパーティー・システムにおいてインストールされているアプリケーション・プログラミング・インターフェース（ＡＰＩ）コード・モジュールを採用することができる。

【００２７】

本発明の特徴を具体化するソフトウェア・コンポーネントは、ソフトウェア・エンジニアリングの技術分野における技術者にとっては馴染みがあるであろう任意の適切なプログラミング言語、開発環境、または言語および開発環境の組合せを使用して開発されることが可能である。たとえば、適切なソフトウェアは、Ｃプログラミング言語、Ｊａｖａプログラミング言語、Ｃ＋＋プログラミング言語、Ｇｏプログラミング言語、および／または、ネットワークもしくはウェブベースのサービスの実施に適しているある範囲の言語、たとえば、ＪａｖａＳｃｒｉｐｔ、ＨＴＭＬ、ＰＨＰ、ＡＳＰ、ＪＳＰ、Ｒｕｂｙ、Ｐｙｔｈｏｎなどを使用して開発されることが可能である。これらの例は、限定することを意図されているものではなく、システム要件に従って好都合な言語または開発システムが採用されることが可能であるということが理解されるであろう。

【００２８】

例示的なシステム１００においては、エンドポイント・デバイス１０６はそれぞれ、プロセッサ１１０を含む。プロセッサ１１０は、通信インターフェース１１２、１つまたは複数のユーザ入力／出力（Ｉ／Ｏ）インターフェース１１４、ならびに、揮発性および不揮発性ストレージの組合せを含むことができるローカル・ストレージ１１６にインターフェース接続されているか、またはその他の形で動作可能に関連付けられている。不揮発性ストレージは、読み取り専用メモリ（ＲＯＭ）、フラッシュ・メモリ等などのソリッドステート不揮発性メモリを含むことができる。揮発性ストレージは、ランダム・アクセス・メモリ（ＲＡＭ）を含むことができる。ストレージ１１６は、エンドポイント・デバイス１０６のオペレーションに関連しているプログラム命令および一時データを含む。いくつかの実施形態においては、エンドポイント・デバイス１０６は、（図１においては示されていない）ハード・ディスク・ドライブ、光ドライブ等などの大容量の不揮発性ストレージへのインターフェースなどのさらなる周辺インターフェースを含むことができる。

【００２９】

エンドポイント・デバイス・ストレージ１１６は、デバイス１０６の通常のオペレーションに関連したプログラムおよびデータ・コンテンツを含むことができる。これは、（たとえば、Ｗｉｎｄｏｗｓ、Ａｎｄｒｏｉｄ、ｉＯＳ、またはＭａｃＯＳオペレーティング・システムに関連付けられている）オペレーティング・システム・プログラムおよびデータ、ならびに本発明には全般的に関連していないその他の実行可能なアプリケーション・ソフトウェアを含むことができる。ストレージ１１６はまた、プログラム命令１１８を含み、プログラム命令１１８は、プロセッサ１１０によって実行されたときに、たとえば、以降で図３、図６、図７、図１１、および図１４を参照しながら記述されているような本発明の実施形態に関連しているオペレーションを実行するようエンドポイント・デバイス１０６に指示する。

【００３０】

図１においても示されているように、認証サーバ１０８は、プロセッサ１２０を含む。プロセッサ１２０は、不揮発性メモリ／ストレージ・デバイス１２２にインターフェース接続されているか、またはその他の形で動作可能に関連付けられており、不揮発性メモリ／ストレージ・デバイス１２２は、ハード・ディスク・ドライブであることが可能であり、および／またはＲＯＭ、フラッシュ・メモリ等などのソリッドステート不揮発性メモリを含むことができる。プロセッサ１２０はまた、認証サーバ１０８のオペレーションに関連しているプログラム命令および一時データを含むＲＡＭなどの揮発性ストレージ１２４にインターフェース接続されている。

【００３１】

従来の構成においては、ストレージ・デバイス１２２は、認証サーバ１０８の通常のオペレーションに関連した知られているプログラムおよびデータ・コンテンツを保持する。たとえば、ストレージ・デバイス１２２は、オペレーティング・システム・プログラムおよびデータ、ならびに、認証サーバ１０８の意図されている機能にとって必要なその他の実行可能なアプリケーション・ソフトウェアを含むことができる。ストレージ・デバイス１２２はまた、プログラム命令を含み、これらのプログラム命令は、プロセッサ１２０によって実行されたときに、以降で図２、図４、図５、および図６を参照しながらさらに詳細に記述されているような本発明の実施形態に関連しているオペレーションを実行するよう認証サーバ１０８に指示する。オペレーションにおいては、ストレージ・デバイス１２２上に保持されている命令およびデータは、要望に応じて実行用に揮発性メモリ１２４へ転送される。

【００３２】

プロセッサ１２０はまた、従来の様式で通信インターフェース１２６に動作可能に関連付けられている。通信インターフェース１２６は、データ通信ネットワーク１０２へのアクセスを容易にする。

【００３３】

使用においては、揮発性ストレージ１２４は、本発明の特徴を具体化する処理およびその他のオペレーションを実行するように構成されている、ストレージ・デバイス１２２から転送されるプログラム命令の対応する本体１２８を含む。

【００３４】

セキュア・システム１０４は、エンドユーザのためにアクセスを許可することおよび／または取引を実行することの前にそれらのユーザの認証を必要とする任意のコンピューティングまたは処理システムであることが可能である。本発明の実施形態によって提供されるサービスを採用することができるセキュア・システムは、バンキング・システム（たとえば、オンライン・バンキング・ポータル）、ｅコマース支払いポータル、セキュア・コンピューティング・プラットフォーム（たとえば、政府または雇用主のシステム）、およびユーザのセキュアな認証を必要とするその他のシステムを含むが、それらには限定されない。

【００３５】

システム１００において示されている破線は、本発明を具体化する、エンドポイント・デバイス１０６、セキュア・システム１０４、および認証サーバ１０８の間における通信を表している。これらの通信の詳細は、以降で、特に図１０および図２２を参照しながら提供される。本発明の目的のために、次いで図１を参照しながら、簡単な概要が提供される。

【００３６】

セキュア・システム１０４へのアクセスを必要とするエンドユーザは、エンドポイント・デバイス１０６または代替メカニズムのいずれかを使用して、アクセス要求１００２を開始することができる。セキュア・システム１０４は、要求されているアクセスをエンドユーザに提供するか否かを特定するために、認証サーバ１０８によって提供されるサービスを使用する。そのようなものとして、承認要求１００４が、セキュア・システム１０４によって認証サーバ１０８へ送信される。

【００３７】

認証サーバ１０８は、チャレンジ・メッセージ１００６を生成して、エンドポイント・デバイス１０６へ送信する。チャレンジ・メッセージは、認証サーバ１０８からエンドポイント・デバイス１０６へ直接に送信されることが可能であり、またはたとえばセキュア・システム１０４を介して、間接的に送信されることが可能である。チャレンジ・メッセージ１００６を回送する様式は、本発明の実施形態の全般的なオペレーションにとって重要ではない。

【００３８】

ユーザは、チャレンジ・メッセージに応答する入力を促され、対応する応答１００８が

、認証サーバ１０８へ返信される。認証サーバ１０８は、この応答を確認し、承認結果１０１０をセキュア・システム１０４へ返す。承認結果に応じて、セキュア・システム１０４は、エンドポイント・デバイス１０６を介してエンドユーザへのアクセスを許可または拒否するアクセス応答１０１２を送信することができる。あるいは、いくつかの実施形態においては、要求されているアクセスは、以降で図２２を参照しながら記述されている別のメカニズムを介して許可されることが可能である。

【００３９】

図２は、認証サーバ１０８の観点からの、本発明の第１の実施形態によるユーザ認証方法のさらなる詳細を示すフローチャート２００である。ステップ２０２において、認証サーバ１０８は、セキュア・システム１０４からの承認要求を受信し、この承認要求は、ユーザ名またはその他のユーザＩＤなど、エンドユーザの識別情報を含む。

【００４０】

ステップ２０４において、認証サーバ１０８は、所定のシンボル・セットのメンバーと、個別のコード・セットのメンバーとの間における「１回限りの」マッピングであるセキュリティー・マトリックスを生成する。一般には、シンボル・セットは複数のシンボルを含み、それらのシンボルからエンドユーザは、パスワードなどのキーワードもしくはフレーズ、または認証目的のために使用されるセットからのシンボルのその他のシーケンスを構築することができる。たとえば、シンボル・セットは、アルファベットの文字（大文字および／もしくは小文字）、数字、ならびに／または選択された句読点およびその他の特別な文字を含むことができる。

【００４１】

一般には、コード・セットは、個別の複数のコード値である。好ましくは、コード・セットのメンバーの数は、シンボル・セットのメンバーの数よりも少ない。コード・セットは、たとえば、１０進数０～９のセットであることが可能であり、これらのコード値のすべてがユーザによってＰＩＮパッドまたはテンキーのみを使用して入力されることが可能であるという利点を有している。

【００４２】

一般には、したがって、ステップ２０４において生成されたセキュリティー・マトリックスによって表されるマッピングは、「１対１」ではなく、それぞれのコード値は、シンボル・セットの複数のシンボルにマップされることが可能である。したがって、たとえばランダムまたは疑似ランダム・プロセスを介して、１回限りのマッピングを作成することによって、エンドポイント・デバイス１０６と認証サーバ１０８との間を通る通信メッセージの、またはエンドユーザのアクションを監視しているいかなる傍受者または観察者も、ユーザ認証のために使用されるキーワードまたはフレーズをいずれかの単一の観察で一意に特定することは可能ではない。さらに、それぞれの認証インスタンスごとに新たなセキュリティー・マトリックスが生成されるので、承認されたユーザによって以前に入力されたコードを単に再入力するだけでは、その後に認証の成功をもたらす結果にはならないであろう。

【００４３】

１回限りのセキュリティー・マトリックスを使用する認証の上述の方法はまた、本発明者の本願の譲受人に譲渡された特許文献１および特許文献２において開示されているシステムにおいて採用されており、これらの特許文献の両方は、それらの全体が参照によって本明細書に組み込まれている。

【００４４】

ステップ２０６において、認証サーバ１０８は、１つまたは複数のセッション固有のファクタに基づいてセキュリティー・マトリックス内のコード値を変換する。このステップのさらなる論考が、以降で図４を参照しながら提供されている。

【００４５】

コード値の変換に続いて、認証サーバ１０８は、変換されたセキュリティー・マトリックスを含むチャレンジ・メッセージ、およびその他の関連した情報を構築して、エンドポ

イント・デバイス１０６へ送信する。このステップは、以降で図５を参照しながらさらに詳細に論じられている。

【００４６】

ステップ２１０において、認証サーバ１０８は、エンドポイント・デバイス１０６からチャレンジ応答メッセージを受信する。チャレンジ応答メッセージは、エンドユーザによって提供された入力に対応している。エンドポイント・デバイス１０６が、ステップ２０６において認証サーバ１０８によって実行された変換を成功裏に反転させ、次いでユーザが、コード値の正しいシーケンスを入力している場合には、認証サーバ１０８は、認証サーバ・プロセッサ１２０にとってアクセス可能なデータベース内に保持されているユーザのキーワードのコピーに基づいて同じコード・シーケンスを複製することができるであろう。データベース内に保持されるユーザ・レコードのさらなる詳細が、以降で図１２を参照しながら論じられている。

【００４７】

したがって、ステップ２１２において、認証サーバ１０８は、受信されたコード・シーケンスを、対応するローカルに生成されたコード・シーケンスに照らして確認する。これから、認証結果２１４が生成される。受信されたコード・シーケンスと、ローカルに生成されたコード・シーケンスとの間におけるマッチのケースにおいては、肯定的な認証結果が生成されて、セキュア・システム１０４へ送信される。そうでない場合には、否定的な認証結果が生成されて、セキュア・システム１０４へ送信される。この認証結果に基づいて、セキュア・システム１０４は、エンドポイント・デバイス１０６を介して、エンドユーザへのアクセスを許可または拒否することができる。

【００４８】

次いで図３を参照すると、本発明を具体化する、エンドポイント・デバイスにおいて実行されるユーザ認証方法のフローチャート３００が示されている。方法３００は、ステップ２０８において認証サーバ１０８によって生成されたチャレンジ・メッセージを受信してこれに応答するためにエンドポイント・デバイス１０６によって実行される。

【００４９】

詳細には、ステップ３０２において、エンドポイント・デバイス１０６は、変換されたセキュリティー・マトリックスを含むチャレンジ・メッセージを認証サーバ１０８から受信する。ステップ３０４において、エンドポイント・デバイス１０６は、変換されたコード値に逆変換を適用するために、ステップ２０６において認証サーバ１０８によって採用されたのと同じセッション固有のファクタを適用する。この逆変換を実行すると、エンドポイント・デバイス１０６は、ステップ２０４において生成された元のセキュリティー・マトリックスに従って、シンボル・セットのシンボルと、コード・セットのコード値との間における元のマッピングを再生成したことになる。

【００５０】

ステップ３０６において、元のセキュリティー・マトリックスが、たとえばエンドポイント・デバイス１０６のＩ／Ｏデバイス１１４のディスプレイを介して、ユーザに提示される。ユーザは、マッピングに対応するコード値のシーケンスと、ユーザのパーソナル・キーワード（パスワード、パスフレーズ、または、シンボル・セットから選択されたシンボルのその他のシーケンス）とを入力することによって、表示されたセキュリティー・マトリックス（典型的には、適切なプロンプトを伴う）に応答することを可能にされる。ユーザ入力は、ステップ３０８においてエンドポイント・デバイス１０６によって受信され、次いでエンドポイント・デバイス１０６は、入力されたコード・シーケンスを含むメッセージを生成して、認証サーバ１０８へ返信する。このメッセージは、図２を参照しながら上述されているように、ステップ２１０において受信される。

【００５１】

図４は、本発明の一実施形態による、たとえばステップ２０６において認証サーバ１０８によって実行されるセッション固有の変換プロセスを示すフローチャート４００を示している。プロセス４００への入力は、ステップ２０４において生成されたセキュリティー

・マトリックス４０２である。とりわけ、ステップ４０６において、１つまたは複数のセッション固有のファクタ４０４が識別されて選択されるか、または取り出される。セッション固有のファクタは、典型的には、セキュア・システム１０４の要件に依存する。したがって、セッション固有のファクタは、セキュア・システム１０４に関連付けられているデータベース・レコードから取り出されることが可能である。セッション固有のファクタは、現在のセッションのその他の特徴、たとえば、特定のユーザ、エンドポイント・デバイスのロケーション、時刻／日付、および／またはセッションのその他の任意の識別可能な特性に依存することも可能である。

【００５２】

したがって、本発明の現在記述されている実施形態によれば、現在のセッションの事前に定義された特性にマッチするレコード４０６から１つまたは複数のセッション固有のファクタが取り出される。詳細には、変換方法４００において使用するために、セッション固有のファクタの対応する値が取り出されるか、または特定される。本発明の実施形態において採用されることが可能であるファクタのタイプおよび値の例は、下記のものを含むが、それらには限定されない。

・　ユーザＩＤによって表される現在のユーザ；

・　指定された精度まで特定されたＧＰＳ座標によって表されるエンドポイント・デバイス・ロケーション；

・　デジタル証明書、またはユーザもしくはデバイス登録プロセス中に生成されたランダム値など、エンドポイント・デバイス１０６および認証サーバ１０８の両方において事前に合意されて格納されている所定のデバイスまたはユーザ固有のキー；

・　ネットワーク・インターフェース（ＭＡＣ）アドレス、Ｗｉ－Ｆｉステーション ＩＤ、インターネット・プロトコル・バージョン６（ＩＰｖ６）アドレス、モバイル電話番号、ＳＩＭ識別子、またはその他のハードウェア・デバイス（たとえばＣＰＵ）シリアル・ナンバーなど、エンドポイント・デバイス１０６に関連付けられている１つまたは複数の一意の識別値；

・　ユーザまたはデバイス登録プロセス中に生成されたシードに基づく疑似ランダム・シーケンスなど、エンドポイント・デバイス１０６および認証サーバ１０８によって共有されているアルゴリズムに従って生成される変化する値；

・　エンドポイント・デバイス１０６にとって見えるワイヤレス・ネットワークの１つもしくは複数のサービス・セット識別子（ＳＳＩＤ）、および／または複数の見えるＳＳＩＤ；

・　エンドポイント・デバイス１０６が現在接続されているワイヤレス・ネットワークのＳＳＩＤ；

・　エンドポイント・デバイス１０６が接続されているモバイル・セルラー・キャリアの識別情報；

・　時刻および／または日付；

・　認証の時間／場所においてエンドポイント・デバイス１０６にとってアクセス可能なローカル・ビーコンまたはネットワーク接続デバイスによって提供されるデータ；

・　たとえばエンドポイント・デバイス１０６の指紋読取装置からのバイオメトリック・データ、および／またはエンドポイント・デバイス１０６のカメラによって取り込まれたイメージから入手された顔識別／分類データ；

【００５３】

ステップ４０８においては、ステップ４０４において取り出されたまたは特定されたファクタ値どうしが組み合わされて、セッション固有の変換／暗号化キーが形成される。任意の適切なアルゴリズムを使用して、ファクタどうしが組み合わされることが可能である。たとえば、組み合わされた各ファクタは、１つもしくは複数のセッション固有のファクタの値どうしの連結、１つもしくは複数のセッション固有のファクタの値から生成されたハッシュ、または入力されたセッション固有のファクタ値のすべてに基づく出力を生み出すその他の任意の適切な関数を含むことができる。

【００５４】
組み合わされた結果はさらに、セキュリティー・マトリックス４０２のコード値を変換するために任意の適切な様式で採用されることが可能である。たとえば、組み合わされた値は、コード値に適用される対称暗号化アルゴリズムにおいて暗号化キーとして使用されることが可能である。たとえば、シンプルな対称変換／暗号化アルゴリズムは、コード値とキー値との間におけるビット排他論理和（ＸＯＲ）演算によって、変換されたコード・シーケンスを算出することである。より洗練された対称暗号は、ＤＥＳ、３ＤＥＳ、ＡＥＳ－２５６、ＡＥＳ－５１２、およびＢｌｏｗｆｉｓｈを含む。そのような暗号とともに使用するための適切なキーは、ＳＨＡ－２５６またはＳＨＡ－５１２などの（これらには限定されない）適切なハッシング関数の使用によって、組み合わされたセッション固有のファクタ値から導き出されることが可能である。好ましくは、対称アルゴリズムが採用され、それによってエンドポイント・デバイス１０６は、セッション固有のファクタの組み合わされた値から同じ変換／暗号化キーを生成した後に変換を逆転させることができる。しかしながら、傍受者は、認証サーバ１０８およびエンドポイント・デバイス１０６によって共有されているがネットワーク１０２を介して送信されることはないセッション固有のファクタの値の知識を伴わずに逆転変換を実行することはできないであろう。

【００５５】
したがって、ステップ４１０において、セッション固有のファクタの組み合わされた、そして任意選択でハッシュされた値を含むキーが、セキュリティー・マトリックス４０２のコード値に適用され、変換されたセキュリティー・マトリックス４１２をもたらす結果となり、変換されたセキュリティー・マトリックス４１２は、送信ステップ２０８において使用するために提供される。

【００５６】
図５は、送信ステップ２０８における送信のためにセッション固有のチャレンジ・メッセージを構築するプロセスを示すフローチャート５００である。プロセス５００への入力は、変換されたセキュリティー・マトリックス４１２である。ステップ５０２において、セキュリティー・マトリックス４１２に含まれているシンボル・セットに基づいてメッセージのシンボル・セット部分が生成される。同様に、ステップ５０４において、変換されたセキュリティー・マトリックス４１２内の変換されたコード値に基づいてメッセージの変換されたコード・セット部分が生成される。

【００５７】
現在記述されている実施形態によれば、ステップ５０６において、有効なコード部分が生成される。メッセージの有効なコード部分の目的は、有効なコード値の完全なセット、たとえば１０進数０～９をエンドポイント・デバイス１０６へ通信することである。この情報がエンドポイント・デバイス１０６によって採用されることが可能である方法は、以降で図７を参照しながらさらに詳細に記述されている。

【００５８】
ステップ５０８において、コード値の変換を逆転させるために使用されることになるセッション固有のファクタ・タイプをエンドポイント・デバイス１０６に知らせるために、メッセージのファクタ選択部分が生成される。セッション固有のファクタの値は、プロセス５００によって構築されたメッセージ内にはなく、代わりに認証サーバ１０８とエンドポイント・デバイス１０６との間における共有されている「秘密の」情報を含むということに留意されたい。

【００５９】
ステップ５１０において、メッセージ部分どうしが組み合わされて、完全なチャレンジ・メッセージが構築され、次いでステップ５１２において送信される。

【００６０】
次いで図６を参照すると、１つまたは複数のセッション固有のファクタに基づいてセッション固有の変換／暗号化キーを生成するための例示的な方法を示すフローチャート６００が示されている。方法６００は、認証サーバ１０８における変換プロセス４００のステ

ップ４０８において使用されることが可能であり、次いで、対応する逆変換を実行するためのキーを生成するためにエンドポイント・デバイス１０６によって同様に採用されることが可能である。

【００６１】

ステップ６０２において、生成されたキーを含むためのストレージが初期化される。これは、メモリの対応するブロックをクリアすること、またはメモリのブロックを、認証サーバ１０８およびエンドポイント・デバイス１０６の両方に知られているその他の何らかの値に初期化することを含むことができる。いくつかのケースにおいては、初期化値は、それ自体が、たとえば一意のセッションＩＤに、または認証サーバ１０８およびエンドポイント・デバイス１０６のネットワーク・アドレスに基づくセッション固有のものであることが可能である。

【００６２】

例示的なプロセス６００においては、複数のセッション固有のファクタ値を組み合わせるために反復アルゴリズムが使用される。したがって、決定ステップ６０４において、依然として組み合わされるべきさらなるファクタ値があるかどうかを特定するためにチェックが実行される。そうである場合には、ステップ６０６において次のファクタが選択され、ステップ６０８において、対応するファクタ値が取り出されるか、または特定される。ステップ６１０において、新たなファクタ値が、たとえば連結またはその他のアルゴリズム的な方法によって、変換キーへと組み合わされる。次いで制御は、決定ステップ６０４へ戻って、特定されて組み合わされるべきファクタ値がさらにあるかどうかを特定する。

【００６３】

すべてのファクタ値が組み込まれると、任意選択の最終処理ステップ６１２が実行される。たとえば、最終処理ステップは、連結された各ファクタ値のハッシュ値を算出して、セキュリティー・マトリックス４０２内のコード値に適用される変換または暗号化プロセスの部分として使用されることになる知られている長さのキーを生み出すことを含むことができる。

【００６４】

図７は、本発明の実施形態による、エンドポイント・デバイス１０６において実行されることが可能であるセッション固有の逆変換プロセスを示すフローチャート７００である。ステップ７０２において、承認サーバ１０８によって採用されたのと同じプロセス６００に従って入手される変換キーが、逆変換における変換されたコード値に適用されて、候補コード値が生成される。これらは「候補コード値」として識別されるということに留意されたい。なぜなら、認証サーバ１０８によって、およびエンドポイント・デバイス１０６によって（たとえば、試みられた詐欺的な認証のケースにおいて）適用されるセッション固有のファクタ値どうしの間におけるいかなるミスマッチも、正しくないおよび／または無効なコード値の生成をもたらす結果となるからである。

【００６５】

とりわけ、逆変換プロセスにおける正しくない変換キーの適用は、無効なコード値である１つまたは複数の候補コード値をもたらす結果となる場合がある。たとえば、コード値が１０進数０～９に限定されている場合には、無効な逆変換は、その他の文字またはシンボルが生成される結果をもたらす場合がある。ステップ７０４において、そのような何らかの無効なコード値を探してチェックが実行される。ステップ５０６において生成されたチャレンジ・メッセージの無効なコード部分は、そのような無効なコード値を識別するためにエンドポイント・デバイス１０６によって使用されることが可能である。無効な値が存在している場合には、それらの無効な値は、ステップ７０６において、チャレンジ・メッセージの有効なコード部分から選択された有効なコードと置き換えられる。この選択は、ランダムであること、またはその他の任意の適切な方法を介して実行されることが可能である。この置き換えステップの結果として、ユーザは、有効と思われるセキュリティー・マトリックスを常に提示されることになり、したがって、詐欺的な認証の試みが検知および阻止されている可能性に気づかないであろう。

【００６６】
図８は、本発明の第１の実施形態によるチャレンジ・メッセージ・フォーマットの概略図８００を示している。例示的なチャレンジ・メッセージ８００は、図５を参照しながら上述されているように構築されたメッセージ部分に対応する複数のフィールドを含む。詳細には、メッセージ・フォーマット８００は、シンボル・セット８０２、変換されたコード・セット８０４、有効なコード・セット８０６、およびセッション固有のファクタ・リスト８０８を含む。セッション固有のファクタ・リスト８０８は、たとえば図６を参照しながら上述されているように、変換／暗号化キーを生成する際に採用されるセッション固有のファクタ、たとえば８０８ａ、８０８ｂを識別する１つまたは複数のサブフィールドを含む。

【００６７】
図９は、フォーマット８００に従ってチャレンジ・メッセージを具体化する例示的なＸＭＬコード９００を示している。示されている例においては、シンボル・セット９０２は、大文字のアルファベットの２６文字を含む。変換されたコード・セット９０４は、変換プロセス４００を２６個のコード値の対応するセットに適用した結果である。例示的なＸＭＬメッセージ９００においては、変換されたコード・セット９０４は、２６個の８ビット値を含み、それらのそれぞれは、２つの１６進数として表されている。

【００６８】
ＸＭＬコード９００はさらに、有効なコード値のセット９０６を含み、これは、この例においては１０進数０～９から構成されている。

【００６９】
ＸＭＬ要素９０８は、セッション固有のファクタ９１０、９１２、９１４のリストを囲んでいる。この例においては、３つのファクタが識別され、「ＩＤ」は、現在のユーザの識別子を表し、「ＧＰＳ：４」は、エンドポイント・デバイスのＧＰＳ座標を構成しているファクタを小数第４位の精度まで定義し、「ＰＳＫ」は、エンドポイント・デバイス１０６および認証サーバ１０８の両方に知られている事前共有キーを構成しているファクタを表す。

【００７０】
ＸＭＬコード９００によって表されている例においては、変換されたコード・セット９０４は、
・　正しいユーザＩＤがエンドポイント・デバイス上で使用されており、
・　小数第４位の精度でのＧＰＳ座標によって表されているエンドポイント・デバイスのロケーションが、認証サーバ１０８に知られている承認されたロケーションにマッチしており、
・　エンドポイント・デバイスによって採用されている事前共有キーが、認証サーバによって採用されているキーにマッチしている場合、たとえば、エンドポイント・デバイス上にインストールされているソフトウェアが、正当な、信頼されている、承認されたソースからのものである場合には、正しい元のコード・セットへ再び変換されることになる。

【００７１】
次いで図１０を参照すると、本発明を具体化する、エンドポイント・デバイス１０６、セキュア・システム１０４、および認証サーバ１０８の間における通信のタイムライン１０００が示されている。アクセス要求１００２が、エンドポイント・デバイス１０６からセキュア・サーバ１０４へ送信され、エンドポイント・デバイス・ユーザによって提供されたユーザＩＤまたはその他の識別情報を含むことができる対応する承認要求１００４が、セキュア・システム１０４から認証サーバ１０８へ送信される。この時点で、認証サーバ１０８は、アクセスが要求されている特定のセキュア・システム１０４、およびエンドポイント・デバイス１０６を介してアクセスを要求しているユーザの両方を識別することができると想定されることが可能である。

【００７２】
次いでセッション固有のチャレンジ・メッセージ１００６が、認証サーバ１０８からエ

ンドポイント・デバイス１０６へ送信される。セッション固有のチャレンジ・メッセージ１００６は、一般的なメッセージ・フォーマット８００を有しており、とりわけ、図９において示されているコード９００などのＸＭＬコードを含むことができる。

【００７３】

次いでエンドポイント・デバイス１０６は、コード値の元のシーケンスを復元するために変換を反転させ、キーワード・シンボルおよびコード値のペアを含むセキュリティー・マトリックスをエンドポイント・デバイスのユーザに表示する。ユーザは、ユーザ・キーワードに対応するコード値を入力し、対応するセッション固有のチャレンジ応答１００８が、エンドポイント・デバイス１０６から認証サーバ１０８へ送信される。

【００７４】

次いで認証サーバ１０８は、ユーザによって入力されたコード・シーケンスの確認を実行し、承認結果メッセージ１０１０を生成してセキュア・システム１０４へ送信する。承認結果メッセージ１０１０は、ユーザが成功裏に認証されたか否かを示すことになる。次いで、エンドポイント・デバイス１０６が、保護されているシステム１０４へのアクセスを許可されるかまたは拒否されるかを示す対応するアクセス応答メッセージ１０１２が送信される。

【００７５】

タイムライン１０００は、それぞれのユニットを実施するために使用されるロケーション、ハードウェア、およびソフトウェアの特定の組合せから独立して、３つの処理ユニットの間における通信の表示として、より一般的に解釈されることが可能である。第１の処理ユニットは、認証サーバ１０８に対応し、これは、認証を必要としているユーザの一意の識別子を含む要求を受信し、セッション固有の認証データ（すなわちチャレンジ）を生成し、この認証データを、エンドポイント・デバイス１０６に対応する第２の処理ユニットへ送信する。第２の処理ユニットは、認証セッションの、およびユーザの特徴である変換された認証データを生成し、これを、検証のために第３の処理ユニットへ送信する。タイムライン１０００によって表されている実施形態においては、第３の処理ユニットは、第１の処理ユニットと同じ認証サーバ・ハードウェア・プラットフォーム１０８上で実行する実行可能コード・モジュールであるが、一般には、この機能は、セキュア・システム１０４上で実行するＡＰＩコード・モジュールを伴って、または別の信頼されているプラットフォーム上になど、全体的にまたは部分的に別の場所に存在することが可能である。

【００７６】

図１１は、本発明を具体化するエンドポイント・ユーザ認証インターフェース１１００の概略図である。例示的なインターフェース１１００は、プロンプト１１０２、たとえば「ＰＩＮパッドを使用して、あなたのパスワードに対応する数字を入力してください」というテキストを含む。プロンプト１１０２の下には、セキュリティー・マトリックス１１０４が表示されている。セキュリティー・マトリックス１１０４は、ペアにされているシンボル値および対応するコード値を含む。例１１００においては、アルファベットの２６個の文字および４つの特別な文字を含む３０個のシンボル値があり、これらは、１０進数０～９を含むコード値とペアにされている。

【００７７】

したがってユーザは、ＰＩＮパッドまたはテンキー１１０６を介して、ユーザのパスワードのシンボル値に対応するコード値を入力することができる。キーパッド１１０６は、物理的なデバイスであることが可能であり、またはタッチスクリーン・ディスプレイ上で生成されることが可能である。音声認識、またはデータ入力のその他の手段など、ユーザ入力の代替形態が採用されることが可能である。

【００７８】

前述されているように、認証サーバ１０８はまた、１つまたは複数のデータベースを、たとえば、不揮発性ストレージ１２２、またはプロセッサ１２０にとってアクセス可能なその他の永続ストレージ内に保持する。認証サーバ１０８によって保持される１つまたは複数のデータベースは、ユーザ・レコードを含むデータベース、およびセキュア・システ

ム・レコードを含むデータベースを含む。ユーザ・レコードは、１つまたは複数のセキュア・システム、たとえば１０４へのアクセスを許可されることが可能であるユーザに対応する。セキュア・システム・レコードは、認証サーバ１０８が認証サービスを提供する１つまたは複数のセキュア・システム、たとえば１０４に対応する。

【００７９】

図１２は、認証サーバ１０８によってデータベース内に保持されることが可能である例示的なユーザ・レコード１２００のコンテンツを概略的に示している。例示的なユーザ・レコード１２００は、ユーザ識別子フィールド１２０２と、ユーザのキーワード／パスワードを含むフィールド１２０４とを含む。さらなるセキュリティーのために、キーワード／パスワード・フィールド１２０４は、ユーザによるセキュア・システム１０４への試みられたアクセスの認証のために認証サーバ１０８によってユーザのキーワードが必要とされるまで暗号化されることが可能である。ユーザ・レコード１２００は、１つまたは複数のユーザ情報フィールド１２０６を含むことができる。さらなるユーザ情報フィールド１２０６は、ユーザの本名、連絡先の詳細等などの個人情報を含むことができ、および／または承認の有効期日などのその他のシステム固有の情報、もしくは本発明の特定の実施態様において必要とされる場合があるその他の任意の情報を含むことができる。ユーザの１つまたは複数のパブリック暗号化キーを格納するためのフィールド１２０８も示されている。これらのパブリック・キーは、この実施形態においては必要とされないが、ユーザ・パブリック・キーの適用は、以降で図１５～図２２を参照しながら本発明のさらなる実施形態に関連してさらに詳細に記述されている。

【００８０】

図１３は、セキュア・システム・レコード１３００を概略的に示している。セキュア・システム・レコード１３００は、特定のセキュア・システム１０４に対応するシステム識別子１３０２を含むことができ、さらに認証情報１３０４を含むことができる。認証情報１３０４は、たとえば、セキュア・システム、たとえば１０４からの要求を識別および検証するために認証サーバ１０８によって使用されることが可能であるパスワード、パブリック・キー、またはその他の情報を含むことができる。

【００８１】

それぞれのセキュア・システム・レコード１３００はさらに、１つまたは複数のファクタ・リスト１３０６を含む。ファクタ・リスト１３０６は、選択基準１３０８を含むことができる。たとえば、特定のエンドポイント・デバイスもしくはロケーション、特定のユーザに関して、または特定の時刻において、特定のファクタ・リストが採用されることが可能である。したがって、認証サーバ１０８によって、対応するセキュア・システム１０４に関連して、現在の認証要求および／またはコンテキストのパラメータを選択基準１３０８に対してマッチさせることによって、適切なファクタ・リストが選択されることが可能である。

【００８２】

それぞれのファクタ・リスト１３０６は、１つまたは複数のファクタ・エントリー、たとえば１３１０ａ、１３１０ｂを含む。それぞれのファクタ・エントリーは、ファクタ・タイプ（たとえば、図９において例示されている「ＩＤ」、「ＧＰＳ：４」、「ＰＳＫ」）を含む。必要とされる場合には、ファクタ・エントリーは、ファクタ・タイプに対応するファクタ値を含むこともできる。ファクタ値は、たとえば、許可されているユーザＩＤ、承認されているエンドポイント・ロケーション、または事前共有キーの値（さらなるセキュリティーのために任意選択で暗号化される）を含むことができる。

【００８３】

セキュア・システム・レコード１３００を保持する認証サーバ１０８は、非常に多様な別々の使用事例用に構成されることが可能である。

【００８４】

１つの例示的な使用事例においては、セキュア・システム１０４は、特定のセキュアな建物内でのみ利用可能となる重要なレコードへのアクセスを提供することができる。これ

は、建物ロケーションに対応する値を伴うロケーション・ファクタを使用することによって実施されることが可能である。エンドポイント・デバイス１０６のロケーションが、対応するファクタ値にマッチしない場合には、認証は失敗することになり、アクセスは拒否されることになる。建物内に物理的に配置されている固定された端末に関連して使用するために代替のファクタ・リストが提供されることが可能である。たとえば、それぞれのそのような固定された端末のために、ＭＡＣアドレス、および／またはその他の一意のハードウェア・コンポーネント識別子など、その端末の物理的なパラメータに対応する１つまたは複数のファクタ・タイプを有するファクタ・リストが提供されることが可能である。したがって、たとえ固定された端末が、自分のロケーションを独立して特定する能力を一般には有することができないとしても、そのような端末からセキュア・システム１０４にアクセスする試みは、成功裏に認証されることが可能である。

【００８５】

別の例示的な使用事例においては、セキュア・システム１０４は、セキュアなコンピューティング・プラットフォーム、たとえば、承認されている、企業によって供給されているエンドポイント・デバイスからのみアクセスが許可されることが可能であるオフィス・サーバであることが可能である。たとえば、従業員は、会社のラップトップから、このラップトップのＭＡＣアドレス、および／またはその他の一意のハードウェア識別番号に基づいてサーバ１０４にアクセスすることを許可されることが可能である。複数のハードウェアベースのファクタを組み合わせることによって、認証サーバ１０８は、たとえ悪意あるユーザが、たとえば、承認されていないデバイス上でネットワーク・インターフェースのＭＡＣアドレスを変更することによってシステムをだますことを試みても、エンドポイント・デバイス１０６の一意のハードウェア署名に基づいてセキュア・システム１０４へのアクセスを規制することができる。

【００８６】

図１４を参照すると、本発明を具体化する代替のユーザ認証システムおよび方法を示す概略図１４００が示されている。実施形態１４００においては、エンドポイント・デバイス１４０２は、ユーザ・デバイス１４０４とは別個のものである。ユーザ・デバイス１４０４は、たとえば、スマートフォンまたはタブレットなどのポータブル・デバイスであることが可能である。固定されたエンドポイント・デバイス１４０２は、ディスプレイ１４０６を含む。ユーザがアクセスを要求した場合には、セッション固有のチャレンジ・メッセージ１００６が、エンドポイント・デバイス１４０２によってＱＲコードなどのマシン可読コードへと変換される。

【００８７】

ポータブル・デバイス１４０４上にインストールされているアプリケーションを使用して、ユーザは、マシン可読コードをスキャンし、このマシン可読コードは、アプリケーションによってデコードされる。次いでアプリケーションは、変換されたコード値の逆変換を実施し、結果として生じるセキュリティー・マトリックスをユーザに表示する。ユーザは、自分のキーワードに対応するコード値のシーケンスをポータブル・デバイス１４０４へと入力する。ユーザによって入力されたコードを含む、結果として生じるセッション固有の応答１００８が、認証サーバ１０８へ送信される。ユーザ・デバイス１４０４上のアプリケーションは、認証サーバの識別情報を伴って構成されることが可能であり、または関連した識別情報を、エンドポイント・デバイス・ディスプレイ１４０６から取得されたコードから入手することができる。認証が成功した場合には、ユーザは次いで、エンドポイント・デバイス１４０２を介してセキュア・システム１０４へのアクセスを提供される。

【００８８】

したがって実施形態１４００は、ユーザのパーソナル・デバイス１４０４を介して「アームズ・レングス」認証（‘ａｒｍ’ｓ　ｌｅｎｇｔｈ’　ａｕｔｈｅｎｔｉｃａｔｉｏｎ）を提供するという利点を有しており、ユーザは、認証情報を自分自身のデバイス１４０４内にのみ入力し、エンドポイント・デバイス１４０２内に入力することはない。この

アレンジは、ユーザがアクセスすることを試みているセキュア・システム１０４に対応するファクタ・リストにおいて定義されることが可能である任意のさらなるファクタとともに、ユーザが有している何か（ユーザのポータブル・デバイス１４０４）、ユーザが知っている何か（ユーザのキーワード）に応じて、強化されたマルチファクタ認証を可能にする。

【００８９】

次いで、ユーザの「所有ファクタ」としてのポータブル・デジタル・デバイスに基づくマルチファクタ認証に対するさらなる強化が、図１５～図２２を参照しながら本発明のさらなる例示的な実施形態を介して記述されている。このさらなる実施形態の一般的なシステム構成は、図１において１００と示されているのと変わらないが、エンドポイント・デバイス１０６は、ここでは、適切なソフトウェアを稼働させる専用のデジタル・アクセス・デバイス、または便利なことに、本発明の必要とされる機能性を具体化する必要とされる命令コードを提供するインストールされているアプリケーション（すなわち「アプリ」）を有するスマートフォンもしくはその他のパーソナル・デバイスなどのポータブル・パーソナル・デバイスである。さらに、デバイス１０６は、セキュア・システムへのアクセスを要求するためにユーザによって操作されることが可能であるが、アクセス要求は、デバイスから独立して生成されることが可能である。たとえば、ユーザは、オンライン・システムへのアクセスを、デスクトップ・コンピュータ上で実行するウェブ・ブラウザから、ユーザ名などの一意の識別子のみを入力することによって要求し、それによってリモート・セキュア・システム１０４をトリガーして、リモート認証サーバ１０８への認証要求を生成することができる。以降で図２２を参照しながらさらに詳細に記述されている、ポータブル・デバイス１０６との通信は次いで、認証結果がセキュア・システム１０４によって、またはセキュア・システム１０４に対して生成されることを可能にするための認証方法を実行する。

【００９０】

図１５は、認証サーバ１０８の観点からの、本発明のさらなる実施形態によるユーザ認証方法のさらなる詳細を示すフローチャート１５００である。ステップ１５０２において、認証サーバ１０８は、セキュア・システム１０４からの承認要求を受信し、この承認要求は、ユーザ名またはその他のユーザＩＤなど、エンドユーザの識別情報を含む。ステップ１５０４において、認証サーバ１０８は、当技術分野においては「ノンス」として一般的に知られているセッション固有のワンタイム・コード・ワードを生成し、これは、たとえば、適切な長さ、たとえば２５６または５１２ビットの乱数であることが可能である。

【００９１】

ステップ１５０６において、認証サーバ１０８は、１つまたは複数のセッション固有のファクタに基づいて暗号化キーを生成する。このステップのさらなる論考が、以降で図１７を参照しながら提供されている。暗号化キーは、たとえば、ＤＥＳ、３ＤＥＳ、ＡＥＳ－２５６、ＡＥＳ－５１２、またはＢｌｏｗｆｉｓｈなどの対称暗号を使用して、ステップ１５０６においてノンスを暗号化するために使用される。次いで、暗号化されたノンスおよびその他の関連した情報を含むチャレンジ・メッセージが、以降で図１８を参照しながらさらに詳細に論じられているようにポータブル・デバイス１０６へ送信される。その後に、ステップ１５２において、認証サーバ１０８は、ポータブル・デバイス１０６からチャレンジ応答メッセージを受信し、このチャレンジ応答メッセージは、元の復号されたノンスのデジタルに署名されたコピーを含む。エンドポイント・デバイス１０６が、ステップ１５０６において認証サーバ１０８によって実行されたキー生成を成功裏に複製して、署名のためにユーザのプライベート・キーを適用した場合には、認証サーバ１０８は、ステップ１５１４においてノンスを確認して、ユーザのパブリック・キー１２０８を使用して署名を検証することができるであろう。これから、認証結果１５１６が生成される。

【００９２】

次いで図１６を参照すると、本発明を具体化するコードを含むアプリを実行するスマートフォンなどのポータブル・デバイス１０６において実行されるユーザ認証方法のフロー

チャート１６００が示されている。詳細には、ステップ１６０２において、デバイス１０６は、暗号化されたノンスを含むチャレンジ・メッセージを認証サーバ１０８から受信する。ステップ１６０４において、デバイス１０６は、ノンスを暗号化するために使用された対称暗号化／復号キーを複製するために、ステップ１５０６において認証サーバ１０８によって採用されたのと同じセッション固有のファクタを適用する。ステップ１６０６において、このキーは、ノンスを復号するために使用される。復号されたノンスは次いで、ステップ１６０８において、ポータブル・デバイス内にセキュアに保持されているユーザのプライベート・キーを使用して署名される。たとえば、ポータブル・デバイスがスマートフォンであるケースにおいては、署名ステップは、Ａｎｄｒｏｉｄ Ｋｅｙｓｔｏｒｅ Ｓｙｓｔｅｍ、ｉＯＳ Ｋｅｙｃｈａｉｎ Ｓｅｒｖｉｃｅｓによって提供されている特徴、またはその他のオペレーティング・システムおよびハードウェア・プラットフォームのもとでサポートされている同等の機能性を使用してセキュアに実行されることが可能である。結果として生じる復号され署名されたノンスは次いで、ステップ１６１０において認証サーバ１０８へ送信される。

【００９３】

図１７は、本発明の一実施形態による、たとえばステップ１５０６および１５０８において認証サーバ１０８によって実行される、セッション固有の暗号化プロセスを示すフローチャート１７００を示している。プロセス１７００への入力は、ステップ１７０４において生成されるノンス１７０２である。とりわけ、ステップ１７０６において、図４および図１３を参照しながら前述されている第１の実施形態と同様の様式で、１つまたは複数のセッション固有のファクタ１７０４が識別され選択されるか、または取り出される。ステップ１７０８において、ステップ１７０６において取り出されるかまたは特定されたファクタ値どうしが組み合わされて、セッション固有の暗号化キーが形成され、このセッション固有の暗号化キーがステップ１７１０において使用されて、暗号化されたノンス１７１２が生成される。

【００９４】

図１８は、ステップ１５１０における送信のためのセッション固有のチャレンジ・メッセージを構築するプロセスを示すフローチャート１８００である。プロセス１８００への入力は、暗号化されたノンス１７１２である。ステップ１８０２において、復号キーの生成において使用されることになるセッション固有のファクタ・タイプをポータブル・デバイス１０６に知らせるために、メッセージのファクタ選択部分が生成される。上述の第１の実施形態の場合と同様に、セッション固有のファクタの「正しい」値は、プロセス１８００によってステップ１８０４において構築されたメッセージ内にはなく、代わりに認証サーバ１０８とポータブル・デバイス１０６との間における共有されている「秘密の」情報を含む。ステップ１８０６において、完成されたチャレンジ・メッセージが送信される。

【００９５】

次いで図１９を参照すると、１つまたは複数のセッション固有のファクタに基づいてセッション固有の暗号化／復号キーを生成するための例示的な方法を示すフローチャート１９００が示されている。方法１９００は、認証サーバ１０８における変換プロセス１５００のステップ１５０６において使用されることが可能であり、次いで、応答生成プロセス１６００のステップ１６０４においてポータブル・デバイス１０６によって同様に採用されることが可能である。ステップ１９０２において、生成されたキーを含むためのストレージが初期化される。例示的なプロセス１９００においては、プロセス６００におけるステップ６０４～６１０と同様の様式で複数のセッション固有のファクタ値を組み合わせるために反復アルゴリズム、すなわちステップ１９０４～１９１０が使用される。すべてのファクタ値が組み込まれると、次いで最終処理ステップ１９１２が実行され、最終処理ステップ１９１２は典型的に、組み合わされた各ファクタ値のハッシュ値を算出して、ノンス１７０２に適用される暗号化／復号プロセスの部分として使用されることになる知られている長さのキーを生み出すことを含むことができる。

【００９６】
図２０は、ポータブル・デバイス１０６によって生成された、復号され署名されたノンスを含むメッセージを２００２で受信したことに応答して認証サーバ１０８によって実行される認証のプロセスを示すフローチャート２０００である。最初にステップ２００４において、復号されたノンスが、はじめに生成されたノンス１７０２と比較される。決定ステップ２００６において、マッチしていると判明した場合には、認証サーバ１０８は、ユーザ・レコード１２００内に格納されているユーザのパブリック・キー１２０８を適用することによって、署名が有効であるということを検証することへ進む。決定ステップ２０１０において、マッチしていると判明した場合には、２０１２で、認証は成功したとみなされる。決定２００６において、復号されたノンスの値に、または決定２０１０においてデジタル署名にミスマッチがある場合には、２０１４で認証は失敗する。
【００９７】
図２１は、本発明のこの実施形態によるチャレンジ・メッセージ・フォーマットの概略図２１００を示している。例示的なチャレンジ・メッセージ２１００は、図１８を参照しながら上述されているように構築されたメッセージ部分に対応するフィールドを含む。詳細には、メッセージ・フォーマット２１００は、暗号化されたノンス２１０２、およびセッション固有のファクタ・リスト２１０４を含み、そしてセッション固有のファクタ・リスト２１０４は、暗号化／復号キーを生成する際に採用されるセッション固有のファクタ、たとえば２１０４ａ、２１０４ｂを識別する１つまたは複数のサブフィールドを含む。
【００９８】
同等の例示的なＸＭＬフォーマット・メッセージ・コンテンツ２２００が、図２２において示されている。示されている例においては、暗号化されたノンス２２０２は、６４個の８ビットの１６進数として表されている５１２ビット値を含む。セッション固有のファクタのリスト２２０４も、図９を参照しながら前述されているのと同じフォーマット内に存在している。
【００９９】
次いで図２３を参照すると、本発明のこの実施形態による、ポータブル・デバイス１０６、セキュア・システム１０４、および認証サーバ１０８の間における通信のタイムライン２３００が示されている。アクセス要求２３０２が、セキュア・サーバ１０４によって受信され、ユーザＩＤまたはその他の識別情報リクエスタを含むことができる対応する承認要求１００４が、セキュア・システム１０４から認証サーバ１０８へ送信される。次いでセッション固有のチャレンジ・メッセージ１００６が、認証サーバ１０８からポータブル・デバイス１０６へ送信される。この実施形態においては、セッション固有のチャレンジ・メッセージは、一般的なメッセージ・フォーマット２１００を有しており、とりわけ、図２２において示されているコード２２００などのＸＭＬコードを含むことができる。次いでエンドポイント・デバイス１０６は、セッション固有のファクタ（ＦＬ）を適用して、暗号化されたノンス（Ｎ）を復号するための復号キーを生成し、結果として生じる値に署名し、対応するセッション固有のチャレンジ応答１００８を認証サーバ１０８へ送信する。次いで認証サーバ１０８は、図２０を参照しながら前述されているように、署名されたノンスの確認を実行し、承認結果メッセージ１０１０を生成してセキュア・システム１０４へ送信する。セキュア・システム１０４は、この結果を使用して、要求を行っているユーザに２３１２でアクセスを許可するか否かを特定する。
【０１００】
本発明の特定の実施形態およびバリエーションが本明細書において記述されているが、関連した技術分野における技術者にとっては、さらなる修正および代替が明らかであろうということを理解されたい。とりわけ、例は、本発明の原理を例示するものとして、およびそれらの原理を実施するための複数の特定の方法およびアレンジを提供するために提示されている。一般には、本発明の実施形態は、検証コードが２つのリモート・ロケーションにおいて独立して生成されることが可能であって、かつ対応する変換／暗号化キーが、たとえば、認証サーバ・ロケーションにおいて、およびエンドポイント・デバイス・ロケ

ーションにおいて独立して生成されることも可能である技術的なアレンジを提供することに依存している。変換／暗号化キーは、１つまたは複数のセッション固有のファクタに依存しており、それによって、権限を伴わずにセキュア・システムにアクセスする試みが、広い範囲の基準に基づいて阻止されることが可能である。そのような基準は、エンドポイント・デバイス・ロケーション、エンドポイント・デバイス・ハードウェア署名、時刻などを含むが、それらには限定されない。

【０１０１】

したがって、記述されている実施形態は、本発明の一般的な特徴および原理を教示する目的で例として提供されているものとして理解されるべきであるが、添付の特許請求の範囲において定義されているとおりである本発明の範囲を限定するものとして理解されるべきではない。

【図１】

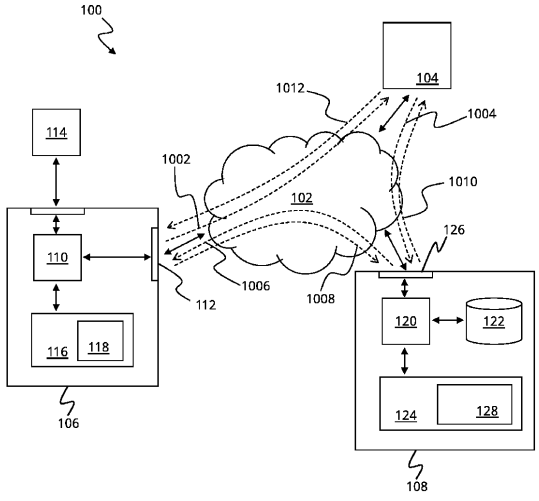
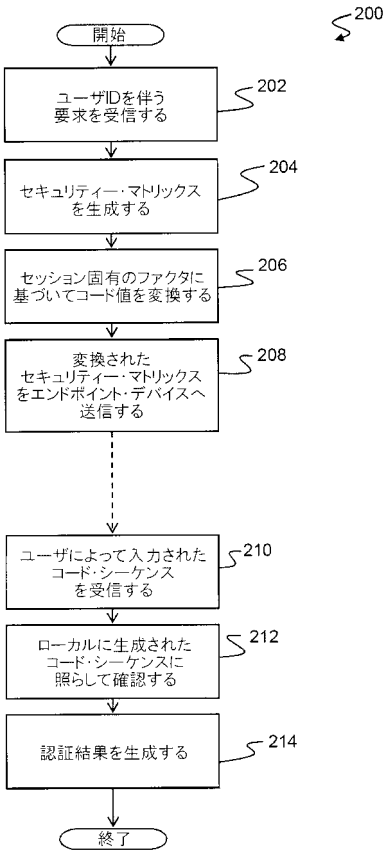
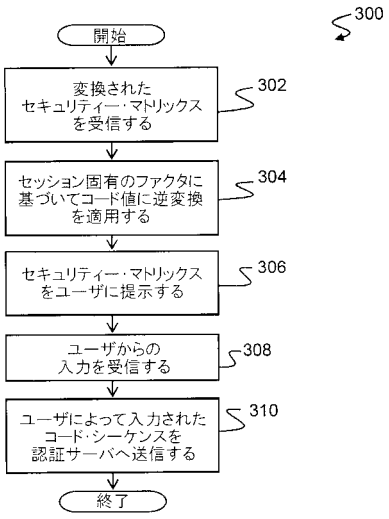



Figure 1

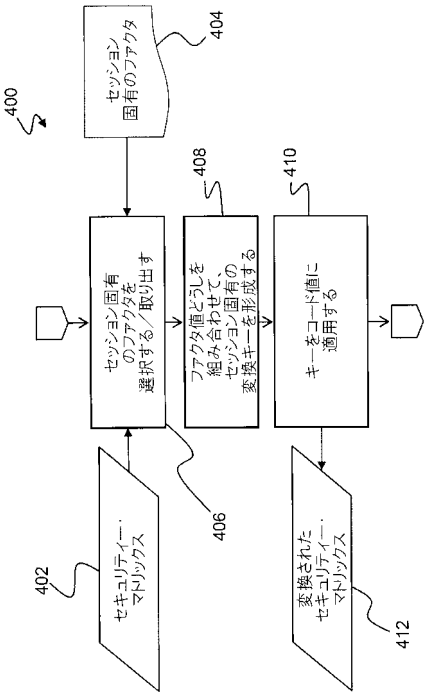
【図２】



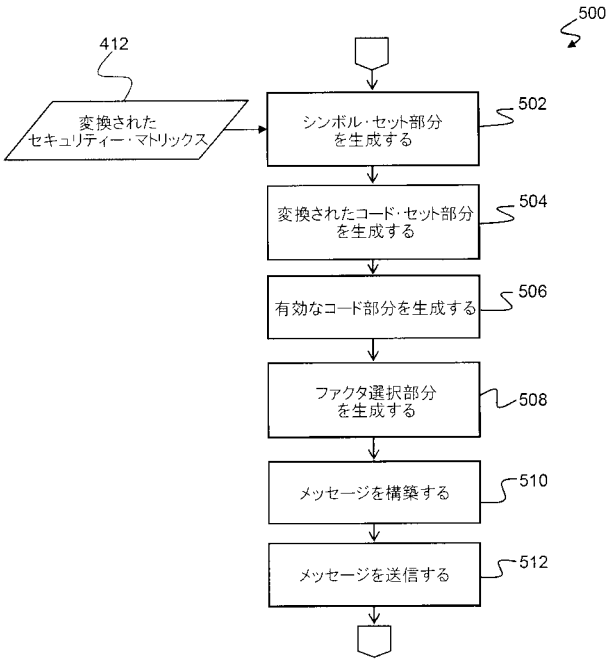
【図３】


300
開始
変換された
セキュリティー・マトリックス
を受信する
302
セッション固有のファクタに
基づいてコード値に逆変換
を適用する
304
セキュリティー・マトリックス
をユーザに提示する
306
ユーザからの
入力を受信する
308
ユーザによって入力された
コード・シーケンスを
認証サーバへ送信する
310
終了

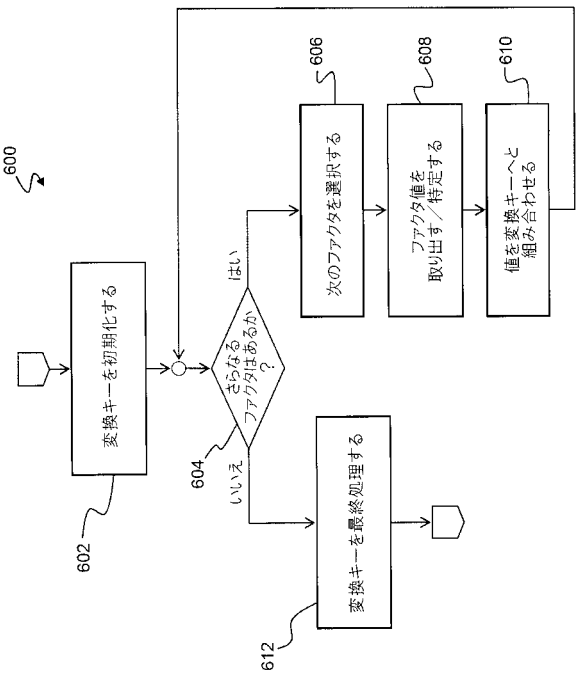
【図４】


400
セッション
固有のファクタ
404
408
410
セッション固有
のファクタを
選択する／取り出す
ファクタ値どうしを
組み合わせて
セッション固有の
変換キーを形成する
キーをコード値に
適用する
406
402
セキュリティー・
マトリックス
変換された
セキュリティー・
マトリックス
412

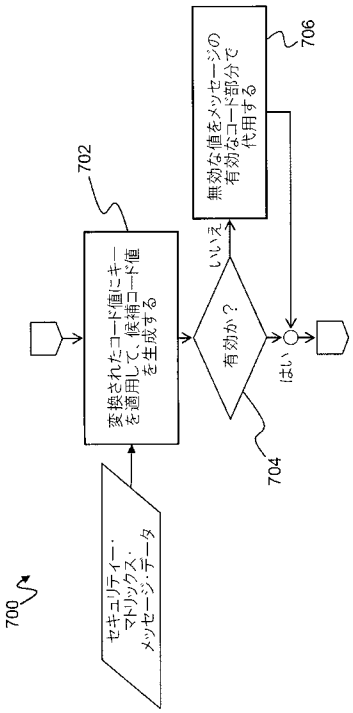
【図５】


500
412
変換された
セキュリティー・マトリックス
シンボル・セット部分
を生成する
502
変換されたコード・セット部分
を生成する
504
有効なコード部分を生成する
506
ファクタ選択部分
を生成する
508
メッセージを構築する
510
メッセージを送信する
512

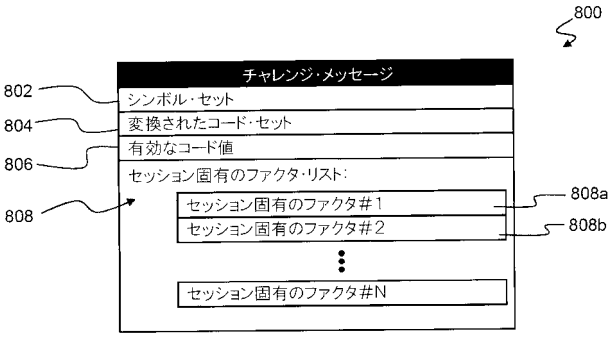
【図６】


600
変換キーを初期化する
602
さらなる
ファクタはあるか
？
はい
いいえ
604
次のファクタを選択する
606
ファクタ値を
取り出す／特定する
608
値を変換キーへと
組み合わせる
610
変換キーを最終処理する
612

【図７】




【図８】




【図９】

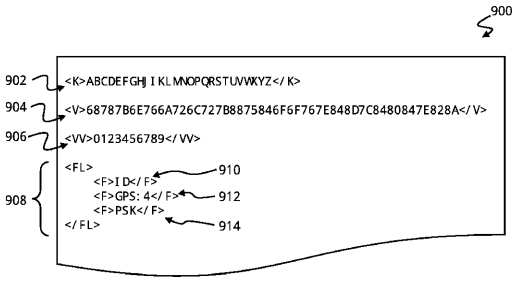
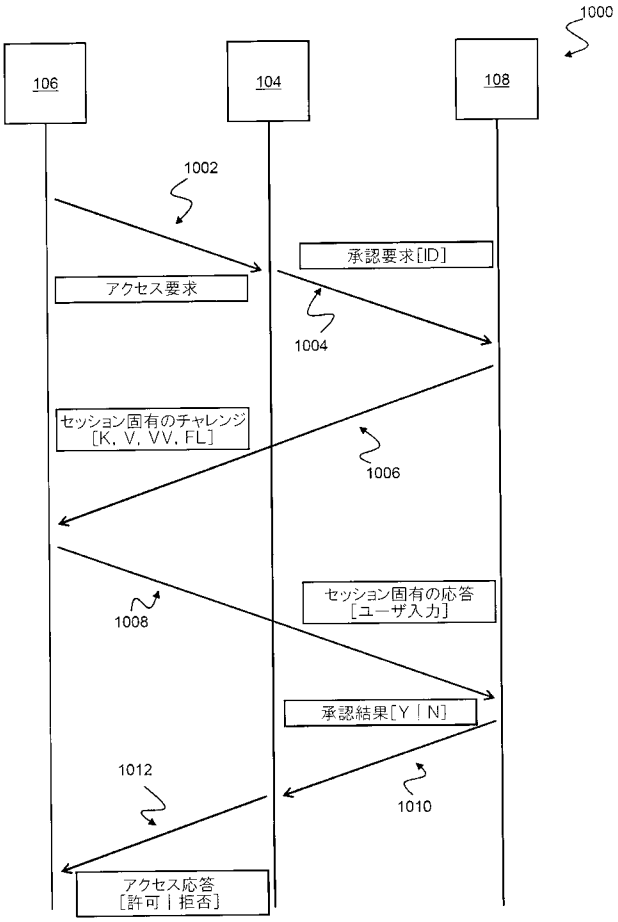
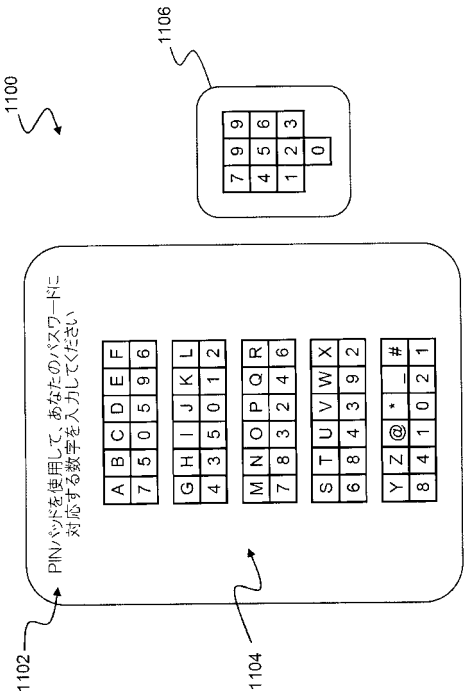



Figure 9

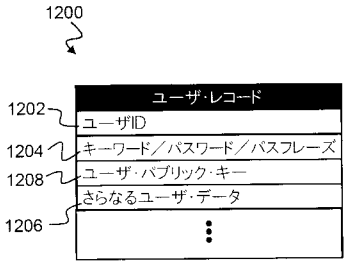
【図１０】



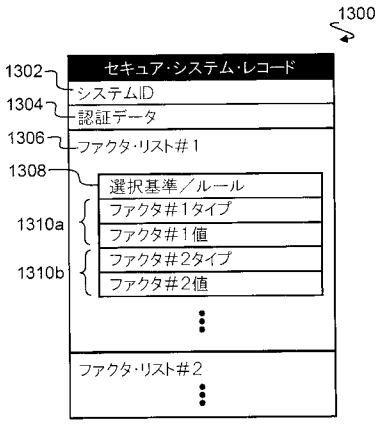

【図１１】



【図１２】




【図１３】




【図１４】

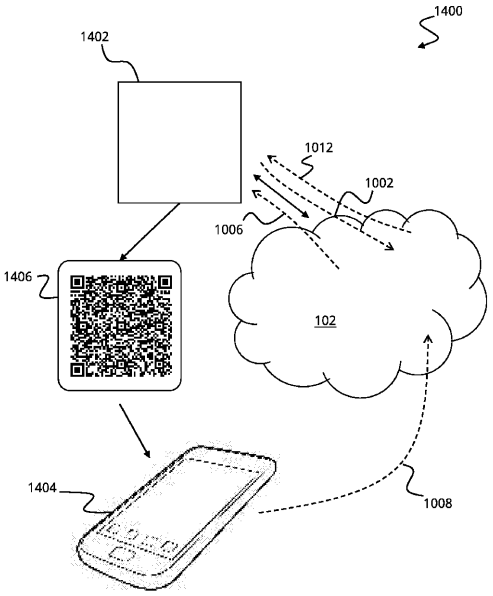
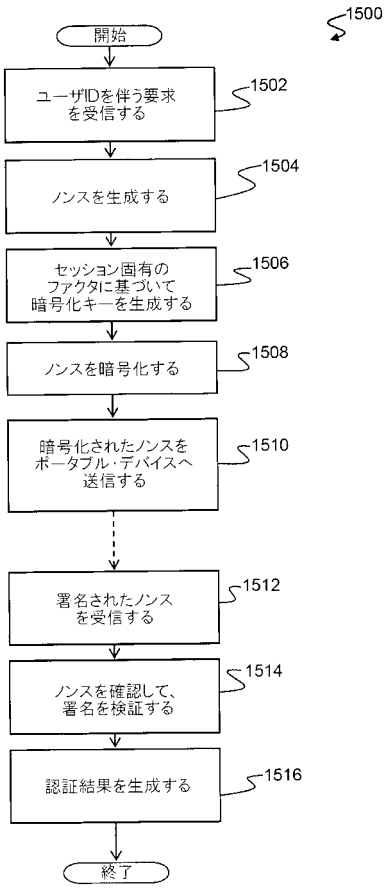
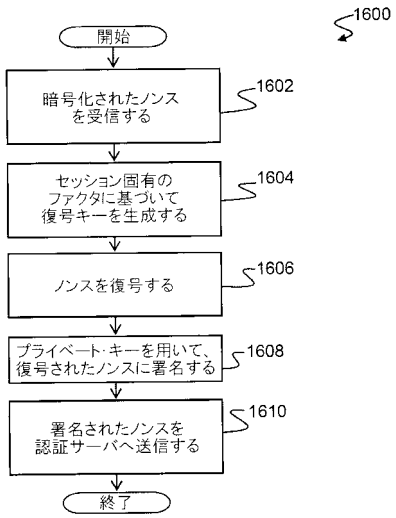



Figure 14

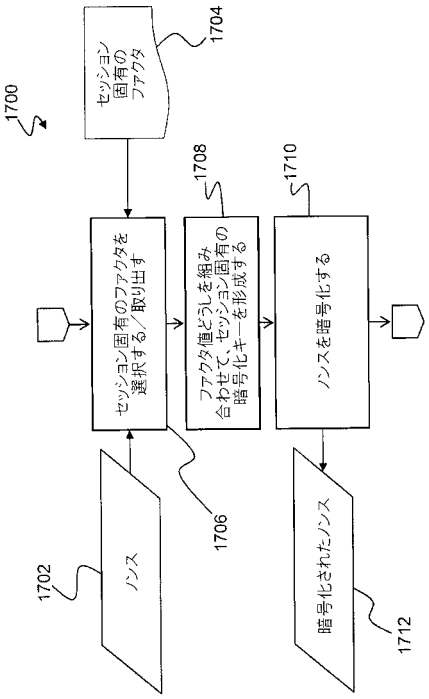
【図１５】



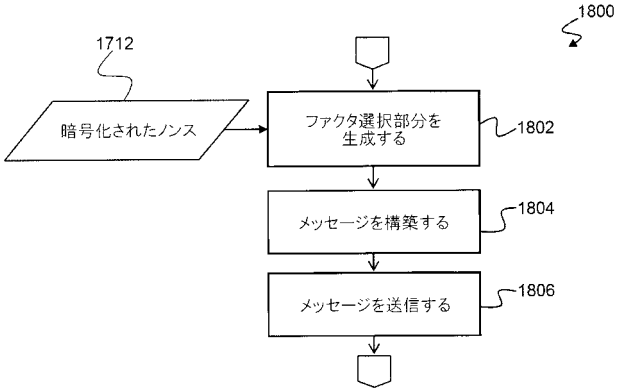

【図１６】



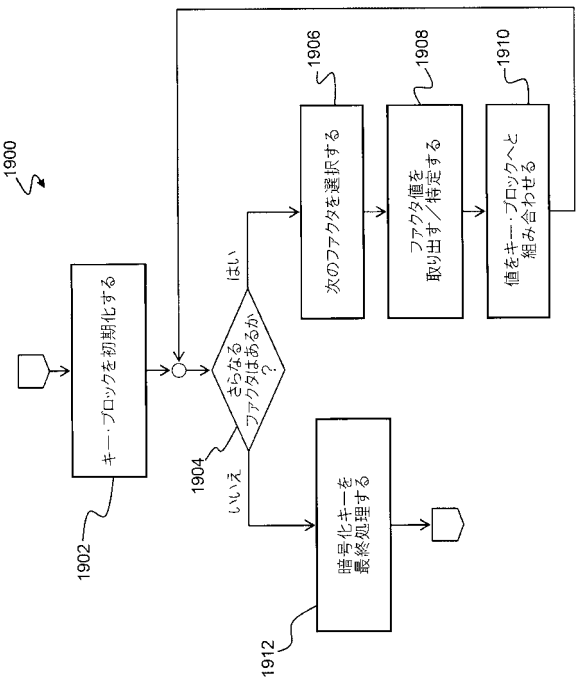
【図１７】



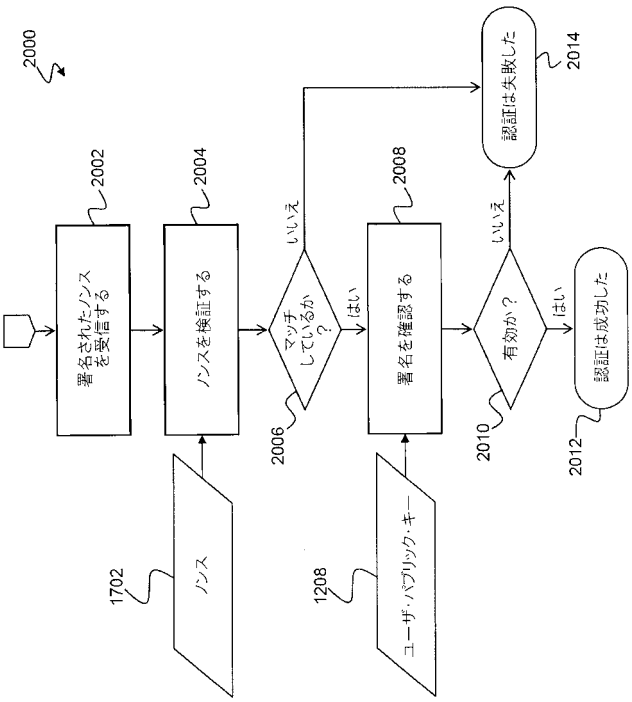

【図１８】



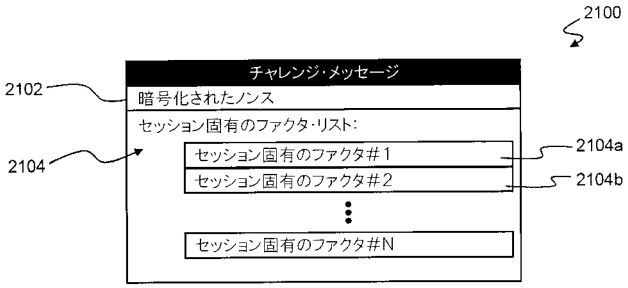

【図１９】




【図２０】



【図２１】




【図２２】

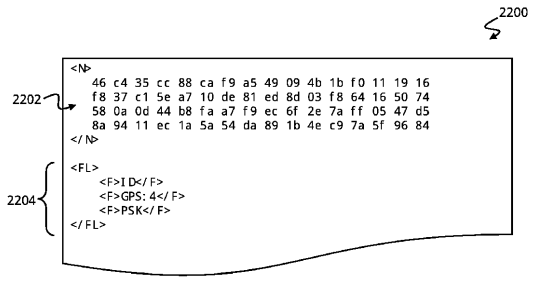
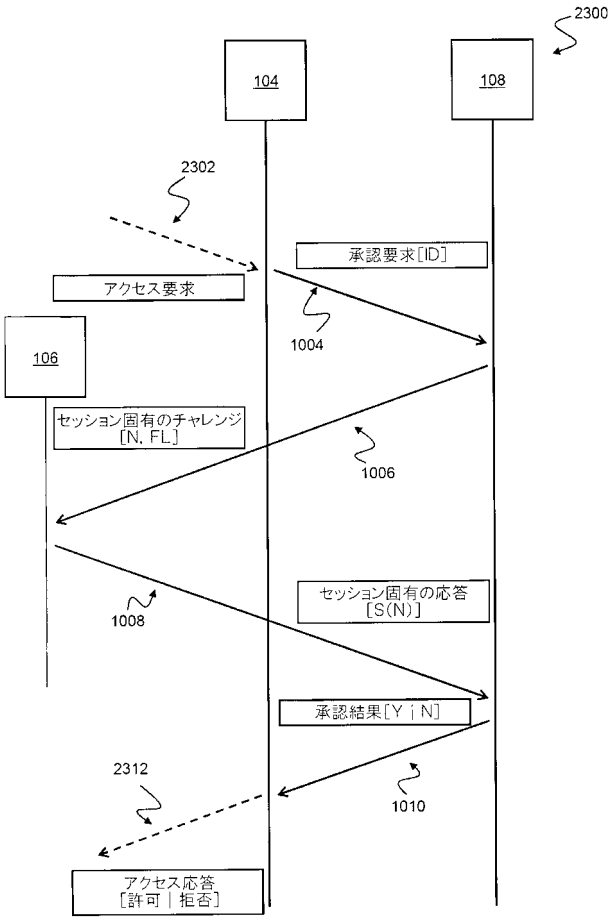



Figure 22

【図２３】



【国際調査報告】

**INTERNATIONAL SEARCH REPORT**

International application No.
**PCT/AU2017/050240**

**A. CLASSIFICATION OF SUBJECT MATTER**

**G06F 21/31(2013.01)i, G06F 21/46(2013.01)i, 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)
G06F 21/31; H04L 9/32; H04L 29/06; G06F 7/04; G06F 21/34; G06F 21/46

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: user authentication, authentication data, transform, verify

**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| Y | US 8869255 B2 (ANTONY SMALES) 21 October 2014<br>See column 5, lines 38-55; claim 1; and figures 7A-7B. | 1-15 |
| Y | US 5592553 A (RICHARD H. GUSKI et al.) 07 January 1997<br>See column 9, line 40 - column 10, line 52; claims 1, 11-12; and figure 6. | 1-15 |
| A | US 2013-0124292 A1 (NIRMAL JUTHANI) 16 May 2013<br>See paragraphs [0061]-[0065]; claims 1-11; and figures 6-8. | 1-15 |
| A | US 2011-0197266 A1 (RONALD KING-HANG CHU et al.) 11 August 2011<br>See paragraphs [0076]-[0091]; and figure 4. | 1-15 |
| A | US 2014-0040628 A1 (VASCO DATA SECURITY, INC.) 06 February 2014<br>See paragraphs [0108]-[0158]; and figures 3a-3b. | 1-15 |

☐ 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 another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents,such combination being obvious to a person skilled in the art
"&" document member of the same patent family

| Date of the actual completion of the international search | Date of mailing of the international search report |
|---|---|
| 13 June 2017 (13.06.2017) | **13 June 2017 (13.06.2017)** |

| Name and mailing address of the ISA/KR | Authorized officer |
|---|---|
| International Application Division<br>Korean Intellectual Property Office<br>189 Cheongsa-ro, Seo-gu, Daejeon, 35208, Republic of Korea | CHIN, Sang Bum |
| Facsimile No. +82-42-481-8578 | Telephone No. +82-42-481-8398 |

Form PCT/ISA/210 (second sheet) (January 2015)

**INTERNATIONAL SEARCH REPORT**
Information on patent family members

International application No.
**PCT/AU2017/050240**

| Patent document cited in search report | Publication date | Patent family member(s) | Publication date |
|---|---|---|---|
| US 8869255 B2 | 21/10/2014 | AU 2012-328082 A1 | 11/12/2014 |
| | | AU 2012-328082 B2 | 02/03/2017 |
| | | CA 2871049 A1 | 02/05/2013 |
| | | CL 2014002816 A1 | 31/07/2015 |
| | | CN 104541475 A | 22/04/2015 |
| | | EA 201491905 A1 | 31/03/2015 |
| | | EP 2839603 A1 | 25/02/2015 |
| | | EP 2839603 A4 | 13/01/2016 |
| | | HK 1207758 A1 | 05/02/2016 |
| | | JP 2015-515218 A | 21/05/2015 |
| | | KR 10-2015-0023268 A | 05/03/2015 |
| | | NZ 702130 A | 30/09/2016 |
| | | PH 12014502304 A1 | 22/12/2014 |
| | | SG 11201406706 A | 27/11/2014 |
| | | TW 201238315 A | 16/09/2012 |
| | | TW I526037 B | 11/03/2016 |
| | | US 2012-0137352 A1 | 31/05/2012 |
| | | US 2012-0137353 A1 | 31/05/2012 |
| | | US 2015-0040204 A1 | 05/02/2015 |
| | | US 9519764 B2 | 13/12/2016 |
| | | WO 2013-061171 A1 | 02/05/2013 |
| US 5592553 A | 07/01/1997 | EP 0636963 A2 | 01/02/1995 |
| | | EP 0636963 A3 | 14/04/1999 |
| | | JP 07-107086 A | 21/04/1995 |
| | | JP 3053527 B2 | 19/06/2000 |
| | | US 5661807 A | 26/08/1997 |
| US 2013-0124292 A1 | 16/05/2013 | CN 103370688 A | 23/10/2013 |
| | | CN 103370688 B | 09/11/2016 |
| | | EP 2598984 A1 | 05/06/2013 |
| | | EP 2598984 A4 | 19/04/2017 |
| | | US 9258296 B2 | 09/02/2016 |
| | | WO 2012-014231 A1 | 02/02/2012 |
| | | WO 2012-014231 A4 | 07/06/2012 |
| US 2011-0197266 A1 | 11/08/2011 | US 7904946 B1 | 08/03/2011 |
| | | US 9002750 B1 | 07/04/2015 |
| US 2014-0040628 A1 | 06/02/2014 | CN 104662864 A | 27/05/2015 |
| | | EP 2885904 A1 | 24/06/2015 |
| | | IN 466KON2015 A | 17/07/2015 |
| | | WO 2014-022778 A1 | 06/02/2014 |

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,ST,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,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,KM,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AO,AT,AU,AZ,BA,BB,BG,BH,BN,BR,BW,BY,BZ,CA,CH,CL,CN,CO,CR,CU,CZ,DE,DJ,DK,DM,DO,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,GT,HN,HR,HU,ID,IL,IN,IR,IS,JP,KE,KG,KH,KN,KP,KR,KW,KZ,LA,LC,LK,LR,LS,LU,LY,MA,MD,ME,MG,MK,MN,MW,MX,MY,MZ,NA,NG,NI,NO,NZ,OM,PA,PE,PG,PH,PL,PT,QA,RO,RS,RU,RW,SA,SC,SD,SE,SG,SK,SL,SM,ST,SV,SY,TH,TJ,TM,TN,TR,TT,TZ

（特許庁注：以下のものは登録商標）
１．ＪＡＶＡ
２．ＪＡＶＡＳＣＲＩＰＴ
３．ＡＮＤＲＯＩＤ
４．ＱＲコード
５．ＷＩＮＤＯＷＳ

(72)発明者 アントニー スメールズ
オーストラリア ３１９９ ヴィクトリア 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 EA15 KA01 KA04 NA02 NA38 PA07

【要約の続き】
ションの認証結果（１０１０）を生成する。