(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6453486号
(P6453486)
(45)発行日　平成31年1月16日(2019.1.16)　(24)登録日　平成30年12月21日(2018.12.21)

(51)Int.Cl.　F I
G06F 21/31 (2013.01)　G06F 21/31
G06F 21/46 (2013.01)　G06F 21/46

請求項の数 11　(全 24 頁)

(21)出願番号　特願2017-550703(P2017-550703)
(86)(22)出願日　平成28年3月16日(2016.3.16)
(65)公表番号　特表2018-514030(P2018-514030A)
(43)公表日　平成30年5月31日(2018.5.31)
(86)国際出願番号　PCT/US2016/022564
(87)国際公開番号　WO2016/160333
(87)国際公開日　平成28年10月6日(2016.10.6)
審査請求日　平成30年9月6日(2018.9.6)
(31)優先権主張番号　14/673,561
(32)優先日　平成27年3月30日(2015.3.30)
(33)優先権主張国　米国(US)

早期審査対象出願

(73)特許権者　507364838
クアルコム，インコーポレイテッド
アメリカ合衆国　カリフォルニア　９２１２１　サン　ディエゴ　モアハウス　ドライブ　５７７５
(74)代理人　100108453
弁理士　村山　靖彦
(74)代理人　100163522
弁理士　黒田　晋平
(72)発明者　ル・シャオ
アメリカ合衆国・カリフォルニア・９２１２１－１７１４・サン・ディエゴ・モアハウス・ドライヴ・５７７５

最終頁に続く

(54)【発明の名称】加速されたパスフレーズ検証

(57)【特許請求の範囲】
【請求項１】
コンピューティングデバイス上でユーザのセキュリティ資格情報を確認するための方法であって、
サーバ上でuserID値およびフルセキュリティストリングを含むユーザアカウントを作成するステップであって、前記フルセキュリティストリングが第1の文字で始まる、ステップと、
その後、
前記userIDを前記サーバに提供することと、
前記サーバから前記userIDに関連付けられた文字カウント値を受信することであって、前記文字カウント値が、前記コンピューティングデバイスの現在のコンテキストに基づくパスワード強度に対応する、受信することと、
ユーザから入力を受信することであって、前記入力が、前記第1の文字で始まる前記フルセキュリティストリングの中の連続する文字のサブセットからなる、受信することと、
前記入力の中の文字数が前記文字カウント値に等しいとき、前記入力を前記サーバに提供することとによって、
前記ユーザアカウントにアクセスするステップと
を備える方法。
【請求項２】

クライアントから受信されたアクセス要求を検証するための方法であって、
ユーザからユーザ識別情報およびフルセキュリティストリングを受信するステップであって、前記フルセキュリティストリングが第1の文字で始まる、ステップと、
複数のサブストリングを生成するステップであって、前記複数のサブストリングの各々が、前記第1の文字で始まる前記フルセキュリティストリングの中の連続する文字のサブセットからなり、前記複数のサブストリングの各々が、パスワード強度値および文字カウント値に関連付けられる、ステップと、
前記クライアントから前記アクセス要求を受信するステップであって、前記アクセス要求が前記ユーザ識別情報を含む、ステップと、
前記ユーザ識別情報および前記クライアントの現在のコンテキストに少なくとも部分的に基づいて、前記複数のサブストリングのうちの1つを決定するステップと、
前記複数のサブストリングのうちの前記1つに関連付けられた前記文字カウント値を前記クライアントに提供するステップと、
前記クライアントから入力サブストリングを受信するステップであって、前記入力サブストリングの長さが前記文字カウント値に対応する、ステップと、
前記入力サブストリングを検証するステップと、
前記入力サブストリングが有効である場合に前記アクセス要求を許可するステップと、
前記入力サブストリングが無効である場合に前記アクセス要求を拒否するステップと
を備える方法。
【請求項３】
前記現在のコンテキストが、前記クライアントの現在のロケーションを含む、請求項2に記載の方法。
【請求項４】
前記現在のコンテキストが、前記アクセス要求が受信された時刻を含む、請求項2に記載の方法。
【請求項５】
前記入力サブストリングを検証するステップが、前記入力サブストリングのためのサブストリングハッシュコードを決定するステップを含む、請求項2に記載の方法。
【請求項６】
前記ユーザ識別情報に少なくとも部分的に基づいて、ソルト値を決定するステップと、
前記入力サブストリングを前記ソルト値と組み合わせるステップであって、前記入力サブストリングと前記ソルト値の前記組合せに対して前記サブストリングハッシュコードが決定される、ステップと
をさらに備える、請求項5に記載の方法。
【請求項７】
メモリと、
前記メモリに動作可能に結合され、
サーバ上でuserID値およびフルセキュリティストリングを含むユーザアカウントを作成することであって、前記フルセキュリティストリングが第1の文字で始まる、作成することと、
前記userID値を提供した後に、前記サーバから文字カウント値を受信することであって、前記文字カウント値が、必要とされるパスワード強度に対応する、受信することと、
前記userID値および前記文字カウント値に等しい長さのサブストリングを提供することによって前記ユーザアカウントにアクセスすることであって、前記サブストリングが、前記第1の文字で始まる前記フルセキュリティストリングの中の連続する文字のサブセットを含む、アクセスすることと
を行うように構成された少なくとも1つのプロセッサと
を備える装置。
【請求項８】
前記少なくとも1つのプロセッサが、

前記装置についてのコンテキスト情報を決定することであって、前記必要とされるパスワード強度が前記コンテキスト情報に少なくとも部分的に基づく、決定することと、
前記コンテキスト情報、前記userID値、および前記サブストリングを提供することによって前記ユーザアカウントにアクセスすることと
を行うように構成される、請求項7に記載の装置。
【請求項９】
前記少なくとも1つのプロセッサが、前記userID値および前記コンテキスト情報を提供した後に、前記サーバから前記文字カウント値を受信するように構成される、請求項8に記載の装置。
【請求項１０】
前記コンテキスト情報が、前記装置の現在のロケーションを含む、請求項8に記載の装置。
【請求項１１】
前記コンテキスト情報が、現在の時刻を含む、請求項8に記載の装置。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、パスフレーズ検証に関する。
【背景技術】
【０００２】
高品質のデジタル符号化コンテンツ(たとえば、データ、音声、およびビデオ)を固定デバイスとモバイルデバイスの両方に配信することがサービスプロバイダおよび消費者によって望まれている。コンテンツへのアクセスは制限されることが多く、ユーザはセキュリティ資格情報を提供することを要求される場合がある。パスワード、パスフレーズ、パターン検証、ジェスチャおよび他のユーザ入力などの資格情報は、セキュリティが重要な使用事例において使用され得る。資格情報は、字、語、数、シンボル、ジェスチャ、または他のユーザ入力からなるストリングなどの複数の文字から構成され得る。一般に、より多くの文字を有する資格情報は、短いパスワードよりもセキュアである。
【０００３】
コンピュータネットワーク内のセキュリティを高めるために、コンピュータオペレーティングシステムは、256文字までのパスフレーズをサポートし得る。しかしながら、小型のタッチスクリーンを有するモバイルデバイスが使用されている場合は特に、ユーザが長いパスフレーズをキー入力することは不便であることが多い。非常に長いパスフレーズは、別個の、通常はより短い、パスワードに置き換えられることがある。しかしながら、より短いパスワードは、他の問題を有することがある。たとえば、簡単なパスワードは弱いが、強いパスワードは覚えるのが難しい。さらに、一定のクライアント側アプリケーションは、パスフレーズが強制される同じサーバと話すために、PCバージョンとモバイルフォンバージョンの両方を有することがある。PCバージョンにおいてパスフレーズが強制される場合、より短いパスワードを使用することによってモバイルバージョンにおける要件を緩和することは難しいことが多い。
【発明の概要】
【課題を解決するための手段】
【０００４】
本開示による、コンピューティングデバイス上でユーザのセキュリティ資格情報を確認するための例示的な方法は、フルセキュリティストリングが第1の文字で始まるように、サーバ上でuserID値およびフルセキュリティストリングを含むユーザアカウントを作成するステップと、サブストリングが第1の文字で始まるフルセキュリティストリングの中の連続する文字のサブセットを含むように、userID値およびサブストリングを提供することによってユーザアカウントにアクセスするステップとを含む。
【０００５】

本開示による、クライアントから受信されたアクセス要求を検証するための例示的な方法は、アクセス要求がユーザ識別情報を含むように、クライアントからアクセス要求を受信するステップと、ユーザ識別情報に少なくとも部分的に基づいて、文字カウント値を決定するステップと、文字カウント値をクライアントに提供するステップと、サブストリングの長さが文字カウント値に対応するように、クライアントからサブストリングを受信するステップと、サブストリングを検証するステップと、サブストリングが有効である場合にアクセス要求を許可するステップと、サブストリングが無効である場合にアクセス要求を拒否するステップとを含む。

【０００６】

そのような方法の実装形態は、以下の特徴のうちの1つまたは複数を含み得る。コンテキスト情報を受信するステップ、ならびに、ユーザ識別情報およびコンテキスト情報に少なくとも部分的に基づいて、文字カウント値を決定するステップ。コンテキスト情報は、クライアントの現在のロケーションを含み得る。コンテキスト情報は、アクセス要求が受信された時刻を含み得る。サブストリングを検証するステップは、サブストリングのためのサブストリングハッシュコードを決定するステップを含み得る。ソルト値は、ユーザ識別情報に少なくとも部分的に基づいて決定されてもよく、サブストリングは、サブストリングとソルト値の組合せに対してサブストリングハッシュコードが決定されるように、ソルト値と組み合わされてもよい。文字カウント値を決定するステップは、アクセス制御データベースがユーザ識別情報、ハッシュコードおよび文字カウント値を含むデータ構造であるように、アクセス制御データベースを照会するためにユーザ識別情報を使用するステップを含み得る。

【０００７】

本開示による例示的な装置は、メモリと、メモリに動作可能に結合され、フルセキュリティストリングを受信し、フルセキュリティストリングハッシュコードを生成し、フルセキュリティストリングハッシュコードをメモリに記憶し、フルセキュリティストリングの中の1つまたは複数の先頭文字に関連付けられたエントロピー値に基づいて、少なくとも1つのサブストリングを決定し、対応する文字カウント値が少なくとも1つのサブストリングの中の文字数と等しいように、少なくとも1つのサブストリングハッシュコードおよび少なくとも1つの対応する文字カウント値を生成し、少なくとも1つのサブストリングハッシュコードおよび少なくとも1つの対応する文字カウント値をメモリに記憶するように構成された少なくとも1つのプロセッサとを含む。

【０００８】

そのような装置の実装形態は、以下の特徴のうちの1つまたは複数を含み得る。フルセキュリティストリングハッシュコードを生成するために、第1のソルト値が生成され、フルセキュリティストリングと組み合わされてもよい。サブストリングハッシュコードを生成するために、第2のソルト値が生成され、サブストリングと組み合わされてもよい。フルセキュリティストリングは、ジェスチャ入力に対応する永続的データであってもよい。フルセキュリティハッシュコードを生成することは、フルセキュリティストリングに対して暗号化ハッシュを実行することを含み得る。少なくとも1つのサブストリングハッシュコードを生成することは、少なくとも1つのサブストリングに対して暗号化ハッシュを実行することを含み得る。サブストリングについてのエントロピー値は、少なくとも強いレベルの複雑度レベルとして評価される。

【０００９】

本開示による装置の一例は、メモリと、メモリに動作可能に結合され、フルセキュリティストリングが第1の文字で始まるように、サーバ上でuserID値およびフルセキュリティストリングを含むユーザアカウントを作成することと、userID値およびサブストリングを提供することによってユーザアカウントにアクセスすることであって、サブストリングが、第1の文字で始まるフルセキュリティストリングの中の連続する文字のサブセットを含む、アクセスすることとを行うように構成された少なくとも1つのプロセッサとを含む。

【００１０】

そのような装置の実装形態は、以下の特徴のうちの1つまたは複数を含み得る。文字カウント値は、userID値を提供した後に、サーバから受信されてもよい。装置についてのコンテキスト情報が決定されてもよく、コンテキスト情報、userID値、およびサブストリングを提供することによってユーザアカウントがアクセスされてもよい。文字カウント値は、userID値およびコンテキスト情報を提供した後に、サーバから受信されてもよい。コンテキスト情報は、装置の現在のロケーションおよび/または現在の時刻を含み得る。

【００１１】

本明細書で説明する項目および/または技法は、以下の機能のうちの1つまたは複数、ならびに言及されていない他の機能を提供し得る。ユーザアカウントは、システム上で作成される。システムは、ローカルデバイスまたはネットワークの一部であり得る。ユーザアカウントは、ユーザ識別情報(たとえば、userID)およびフルセキュリティストリングを含む。フルセキュリティストリングは、文字、ジェスチャ、パターン検証、または他のユーザ入力を含み得る。フルセキュリティストリングに対応するハッシュコードが記憶される。ソルト値は、ハッシュ関数の入力を形成するために、セキュリティストリングと一緒に使用され得る。フルセキュリティストリングの複雑度スコア(たとえば、強度値)が決定される。既製のアルゴリズムは、ストリングの複雑度(すなわち、強度)を評価するために使用され得る。たとえば、強度測定は、ストリングのエントロピーに基づき得る。フルセキュリティストリングの最初の「x」個の文字からなるサブストリングが決定される。サブストリングの強度が評価される。「x」の値は、サブストリングの対応する複雑度(すなわち、強度)に基づいて変化する。サブストリングに対応するハッシュコード(および任意選択のソルト値)が記憶される。複数のサブストリングが評価されてもよく、それらの対応するハッシュコードが記憶されてもよい。ユーザの資格情報は、サブストリングに基づいて確認される。すなわち、ユーザ検証は、フルセキュリティストリングの最初の「x」個の文字のみを用いて達成される。ユーザに関連付けられたコンテキストが決定されてもよい。コンテキストは、現在のロケーション、周囲雑音、挙動データおよび/または履歴データに基づいてもよい。サブストリングは、コンテキストに基づいて決定されてもよい。システムセキュリティポリシーは、いつ検証がフルセキュリティストリングの入力またはサブストリングの入力を必要とするかを設定してもよい。他の機能が提供されてもよく、本開示によるあらゆる実装形態が、説明する機能のすべてはもちろん、任意の特定の機能を提供しなければならないとは限らない。さらに、上記で言及した効果が言及したもの以外の手段によって達成される可能性があり得、言及した項目/技法は必ずしも言及した効果をもたらすとは限らないことがある。

【図面の簡単な説明】

【００１２】

【図１】モバイルデバイスの一実施形態の構成要素のブロック図である。

【図２】例示的なネットワーク化されたシステムのブロック図である。

【図３】コンピュータシステムの一例のブロック図である。

【図４】モバイルデバイス上でセキュリティ資格情報を提供するユーザの図である。

【図５Ａ】フルセキュリティストリングおよび対応するサブストリングを含むテーブルである。

【図５Ｂ】任意選択のソルト値を有するストリングの集合である。

【図６】例示的なクライアントサーバメッセージフローの流れ図である。

【図７】加速されたパスフレーズ検証とともに使用するためのデータ構造の一例である。

【図８】サブストリングハッシュコードを生成するプロセスのブロック流れ図である。

【図９】サーバ上での加速されたパスフレーズ検証のためのプロセスのブロック流れ図である。

【図１０】クライアント上での加速されたパスフレーズ検証のためのプロセスのブロック流れ図である。

【発明を実施するための形態】

【００１３】

ユーザ検証プロセスを加速するための技法について説明する。ユーザは、非常に長いセキュリティ資格情報(たとえば、ストリング、パスワード、パスフレーズ)をネットワークサーバに提供し得る。セキュリティ資格情報の中の最初の「x」個の文字の強度が評価され得る。たとえば、非常に長いセキュリティ資格情報の最初の6文字から8文字は、許容できる資格情報として働くのに十分なエントロピーを有し得る。資格情報は事実上、6文字から8文字だけで十分に強いので、非常に長いセキュリティ資格情報の中の後続の文字は、ユーザエクスペリエンスを改善するためにスキップされ得る(すなわち、ユーザは、追加の文字を入力する必要がない)。加速された資格情報検証を利用するシステムは、十分な強度(すなわち、エントロピー)が得られるまで、入力された資格情報の強度を最初の「x」個の文字を用いて評価し得る。システムは、最初の「x」個の文字の第1のハッシュ、ならびに省略されていないセキュリティ資格情報のハッシュを記憶することができ、パスワード検証は、特定のセキュリティポリシーに基づいて、最初の「x」個の文字のみまたは省略されていないセキュリティ資格情報を用いて達成され得る。セキュリティポリシーは、デフォルト設定、セットアップの間のユーザ選択、ロケーション/挙動のリアルタイム監視、または他のコンテキストとすることができる。動作の際、ユーザは元の資格情報(たとえば、パスフレーズ)を覚えていれば十分である。「x」の値(すなわち、十分なエントロピーを得るために入力されるべき文字数)は、ユーザによって知られていないことがある。すなわち、ソフトウェアは、資格情報セットアップの間に値「x」を決定し得る。「x」の値は、(たとえば、パブリックエリアまたはプライベートエリアにおける)コンテキストに基づいて変化し得る。値「x」は、複数のハッシュと一緒に記憶され得る。たとえば、第1のハッシュ(すなわち、最初の「x」個の文字用)および第2のハッシュ(すなわち、非常に長い資格情報全体用)は両方とも、同じuserIDに対して記憶される。「x」は少なくとも、エントロピーの許容できるレベルに対応すべきであることが必要とされる。元の各セキュリティストリングは、エントロピー評価に応じて、その特定の「x」の値を有し得る。ハッシュは、辞書攻撃を阻止するために、ソルト機構、すなわち、ハッシュ(パスフレーズ)=SHA-256(ソルト||パスフレーズ)を内部に含むことができ、式中、「||」はストリング連結を示す。最初の「x」個の文字を検証すると、ユーザインターフェース(UI)は、後続のユーザ入力の収集をスキップし、検証成功についてユーザに通知することができる。

【００１４】

図1を参照すると、本明細書の様々な技法が利用され得るモバイルデバイス100が示されている。モバイルデバイス100は、様々なモバイル通信デバイスおよび/またはコンピューティングデバイスの機能を含むか、または実装することができ、例としては、限定はしないが、現存するか将来開発されるかにかかわらず、携帯情報端末(PDA)、スマートフォン、ラップトップ、デスクトップまたはタブレットコンピュータなどのコンピューティングデバイス、自動車コンピューティングシステムなどがある。

【００１５】

モバイルデバイス100は、プロセッサ111(またはプロセッサコア)およびメモリ140を含む。モバイルデバイスは、場合によっては、公共バス101または私設バス(図示せず)によってメモリ140に動作可能に接続された信頼できる環境160を含み得る。信頼できる環境160は、プロセッサ111に統合され得るARM TrustZone(登録商標)技術などの信頼できる実行環境(TEE:Trusted Execution Environment)を含み得る。モバイルデバイス100はまた、通信インターフェース120と、ワイヤレスネットワーク上でワイヤレスアンテナ122を介してワイヤレス信号123を送信および受信するように構成されたワイヤレストランシーバ121とを含み得る。ワイヤレストランシーバ121は、バス101に接続される。ここで、モバイルデバイス100は、単一のワイヤレストランシーバ121を有するものとして示されている。しかしながら、モバイルデバイス100は、代替的に、Wi-Fi、CDMA、広帯域CDMA(WCDMA(登録商標))、ロングタームエボリューション(LTE)、BLUETOOTH(登録商標)短距離ワイヤレス通信技術などの複数の通信規格をサポートするために、複数のワイヤレストランシーバ121およびワイヤレスアンテナ122を有することができる。

【００１６】
通信インターフェース120および/またはワイヤレストランシーバ121は、複数のキャリア(異なる周波数の波形信号)上での動作をサポートし得る。マルチキャリア送信機は、被変調信号を複数のキャリア上で同時に送信することができる。各被変調信号は、符号分割多元接続(CDMA)信号、時分割多元接続(TDMA)信号、直交周波数分割多元接続(OFDMA)信号、シングルキャリア周波数分割多元接続(SC-FDMA)信号などであってもよい。各被変調信号は、異なるキャリア上で送られてもよく、パイロット、オーバーヘッド情報、データなどを搬送することができる。
【００１７】
モバイルデバイス100はまた、ユーザインターフェース150(たとえば、ディスプレイ、GUI)と、SPSアンテナ158を介して(たとえば、SPS衛星からの)衛星測位システム(SPS)信号159を受信するSPS受信機155とを含む。SPS受信機155は、単一のグローバルナビゲーション衛星システム(GNSS)または複数のそのようなシステムと通信することができる。GNSSは、限定はしないが、全地球測位システム(GPS)、Galileo、Glonass、Beidou(Compass)などを含むことができる。SPS衛星は、衛星、宇宙ビークル(SV)などとも呼ばれる。SPS受信機155は、SPS信号159を全体的にまたは部分的に処理し、これらのSPS信号159を使用してモバイルデバイス100のロケーションを決定する。プロセッサ111、メモリ140、DSP112および/または専用プロセッサ(図示せず)は、SPS受信機155と連携して、SPS信号159を全体的にもしくは部分的に処理するために、および/またはモバイルデバイス100のロケーションを計算するために利用されることもある。SPS信号159または他のロケーション信号からの情報の記憶は、メモリ140またはレジスタ(図示せず)を使用して実行される。1つのプロセッサ111、1つのDSP112および1つのメモリ140だけが図1に示されているが、これらの構成要素のいずれか、ペア、またはすべてのうちの2つ以上がモバイルデバイス100によって使用され得る。モバイルデバイス100に関連付けられたプロセッサ111およびDSP112は、バス101に接続される。
【００１８】
メモリ140は、1つまたは複数の命令またはコードとしての機能を記憶する(1つまたは複数の)非一時的コンピュータ可読記憶媒体を含むことができる。メモリ140を構成することができる媒体は、限定はしないが、RAM、ROM、FLASH、ディスクドライブなどを含む。メモリは、オペレーティングシステム141、アプリケーション142、データファイル143および認証モジュール144のためのコードを含み得る。一般に、メモリ140によって記憶された機能は、汎用プロセッサ111、専用プロセッサ、またはDSP112によって実行される。したがって、メモリ140は、説明する機能をプロセッサ111および/またはDSP112に実行させるように構成されたソフトウェア(プログラミングコード、命令など)を記憶する、プロセッサ可読メモリおよび/またはコンピュータ可読メモリである。代替的に、モバイルデバイス100の1つまたは複数の機能は、全体的にまたは部分的にハードウェアにおいて実行され得る。
【００１９】
モバイルデバイス100は、視界内の他の通信エンティティおよび/またはモバイルデバイス100が利用可能な情報に基づいて、様々な技法を使用して、関連するシステム内でのその現在の位置を推定することができる。たとえば、モバイルデバイス100は、1つもしくは複数のワイヤレスローカルエリアネットワーク(LAN)、BLUETOOTH(登録商標)もしくはZIGBEE(登録商標)などの短距離ワイヤレス通信技術を利用するパーソナルエリアネットワーク(PAN)、SPS衛星に関連付けられたアクセスポイント(AP)から取得された情報、および/または、マップサーバもしくはLCIサーバから取得されたマップ制約データを使用して、その位置を推定することができる。
【００２０】
次に図2を参照すると、例示的なネットワーク化されたコンピュータシステム200のブロック図が示されている。ネットワーク化されたコンピュータシステム200は、モバイルデバイス100およびパーソナルコンピュータ208などの複数のデータ処理デバイスを含む。デ

ータ処理デバイスは、ユーザ資格情報を受信することが可能な任意の適切な電子デバイス(たとえば、ノードブックコンピュータ、タブレットコンピュータ、ネットブック、モバイルフォン、ゲームコンソール、現金自動預払機(ATM)、キオスク、携帯情報端末(PDA)など)であってもよい。ネットワーク化されたコンピュータシステム200はまた、データ処理デバイスと通信し、1つまたは複数のネットワーク210との接続を可能にするように構成された、1つまたは複数のアクセスポイント212および/または基地局214を含み得る。たとえば、ネットワーク210は、ワイドエリアネットワーク(WAN)および/またはワイヤレスローカルエリアネットワーク(WLAN)であってもよく、インターネットへの接続をさらに含み得る。アクセスポイント212は、高度なWLANアクセスポイントであってもよく、基地局214は、電子的切替え機能を含んでもよく、メディアゲートウェイ(MGW)またはゲートウェイメディア交換センタサーバ(GMSC)として構成されてもよい。

【００２１】

ネットワーク210は、1つまたは複数のサーバ202への接続を提供し得る。サーバ202は、プロセッサおよびメモリを含むデータ処理デバイスであり、コンピュータ実行可能命令を実行するように構成される。たとえば、サーバ202は、プロセッサ、非一時的メモリ、ディスクドライブ、ディスプレイ、キーボード、マウスを含むコンピュータシステムを備え得る。プロセッサは、好ましくは、インテリジェントデバイス、たとえば、Intel(登録商標) CorporationまたはAMD(登録商標)によって製造されるものなどのパーソナルコンピュータ中央処理装置(CPU)、マイクロコントローラ、特定用途向け集積回路(ASIC)などである。メモリは、ランダムアクセスメモリ(RAM)および読取り専用メモリ(ROM)を含む。ディスクドライブは、ハードディスクドライブ、CD-ROMドライブ、および/またはジップドライブを含み、他の形態のドライブを含み得る。ディスプレイは、液晶ディスプレイ(LCD)(たとえば、薄膜トランジスタ(TFT)ディスプレイ)であるが、他の形態のディスプレイ、たとえば、陰極線管(CRT)が許容可能である。キーボードおよびマウスは、データ入力機構をユーザに提供する。サーバ202は、本明細書で説明する機能を実行するようにプロセッサを制御するための命令を含むプロセッサ可読、プロセッサ実行可能ソフトウェアコードを(たとえば、メモリに)記憶し得る。機能は、1つまたは複数のデータ処理デバイス上での加速された資格情報検証を支援する。機能は、たとえば、セキュリティストリングを受信すること、セキュリティストリングおよび対応するサブストリングの強度を決定すること、暗号学的にセキュアな擬似乱数を生成すること、暗号関数(たとえば、ハッシュコード)を生成し、記憶すること、文字カウント情報を決定すること、ユーザコンテキストデータを評価すること、ならびにデータアクセス要求を確認することを含み得る。ソフトウェアは、ネットワーク接続を介してダウンロードされること、ディスクからアップロードされることなどによって、メモリにロードされ得る。さらに、ソフトウェアは、直接的に実行可能ではなく、たとえば、実行前にコンパイルを必要とすることがある。サーバ202は、セキュリティ資格情報を記憶するために、アクセス制御データベース204(たとえば、データ構造、リレーショナルデータベース、フラットファイル)を含み得る。サーバ202はまた、ユーザに提供され得るデジタル符号化コンテンツ(たとえば、データ、音声、およびビデオ)を含むコンテンツデータベース206を含み得る。サーバ202、アクセス制御データベース204、およびコンテンツデータベース206の構成は例示的なものにすぎず、限定ではない。2つ以上のサーバおよびデータベースが使用され得る。

【００２２】

図3に示すコンピュータシステム300は、サーバ202の機能を少なくとも部分的に実装するために利用され得る。図3は、本明細書で説明するように、様々な他の実施形態によって提供される方法を実行することができ、かつ/またはモバイルデバイスもしくは他のコンピュータシステムとして機能することができるコンピュータシステム300の一実施形態の概略図を提供する。図3は、様々な構成要素の一般化された図を提供し、それらの構成要素のいずれかまたはすべては、適宜に利用され得る。したがって、図3は、個々のシステム要素が、比較的分離された方式または比較的より統合された方式で、どのように実装され得るかを広く示している。

【００２３】
バス305を介して電気的に結合され得る(または適宜に他の方法で通信し得る)ハードウェア要素を備えるコンピュータシステム300が示されている。ハードウェア要素は、限定はしないが、1つもしくは複数の汎用プロセッサおよび/または1つもしくは複数の(デジタル信号処理チップ、グラフィックス加速プロセッサなどの)専用プロセッサを含む1つまたは複数のプロセッサ310と、限定はしないが、マウス、キーボードなどを含むことができる1つまたは複数の入力デバイス315と、限定はしないが、ディスプレイデバイス、プリンタなどを含むことができる1つまたは複数の出力デバイス320とを含み得る。プロセッサ310は、たとえば、インテリジェントハードウェアデバイス、たとえば、Intel(登録商標) CorporationまたはAMD(登録商標)によって製造されるものなどの中央処理装置(CPU)、マイクロコントローラ、ASICなどを含むことができる。他のプロセッサタイプも利用され得る。

【００２４】
コンピュータシステム300は、1つまたは複数の非一時的記憶デバイス325をさらに含む(かつ/または非一時的記憶デバイス325と通信する)ことができ、非一時的記憶デバイス325は、限定はしないが、ローカルストレージおよび/もしくはネットワークアクセス可能なストレージを備えることができ、かつ/または、限定はしないが、ディスクドライブ、ドライブアレイ、光記憶デバイス、プログラム可能、フラッシュ更新可能などとすることができるランダムアクセスメモリ(「RAM」)および/もしくは読取り専用メモリ(「ROM」)などの固体記憶デバイスを含むことができる。そのような記憶デバイスは、限定はしないが、様々なファイルシステム、データベース構造などを含む、任意の適切なデータストアを実装するように構成され得る。

【００２５】
コンピュータシステム300はまた、通信サブシステム330を含む場合があり、通信サブシステム330は、限定はしないが、モデム、ネットワークカード(ワイヤレスまたはワイヤード)、赤外線通信デバイス、(BLUETOOTH(登録商標)短距離ワイヤレス通信技術トランシーバ/デバイス、802.11デバイス、WiFiデバイス、WiMaxデバイス、セルラー通信設備などの)ワイヤレス通信デバイスおよび/またはチップセットなどを含むことができる。通信サブシステム330は、データが、(一例を挙げると、以下で説明するネットワークなどの)ネットワーク、他のコンピュータシステム、および/または本明細書で説明する任意の他のデバイスと交換されることを可能にし得る。多くの実施形態では、コンピュータシステム300は、ここでのように、作業メモリ335をさらに備え、作業メモリ335は、上記で説明したように、RAMデバイスまたはROMデバイスを含むことができる。

【００２６】
コンピュータシステム300はまた、オペレーティングシステム340、デバイスドライバ、実行可能ライブラリ、および/または1つもしくは複数のアプリケーションプログラム345などの他のコードを含む、現在、作業メモリ335内に位置するように示されている、ソフトウェア要素を備えることができ、他のコードは、本明細書で説明するように、様々な実施形態によって提供されるコンピュータプログラムを備えてもよく、かつ/または、他の実施形態によって提供される方法を実装するおよび/もしくはシステムを構成するように設計されてもよい。単に例として、本明細書で説明する1つまたは複数のプロセスは、コンピュータ(および/またはコンピュータ内のプロセッサ)によって実行可能なコードおよび/または命令として実装され得る。たとえば、図3に示すように、認証モジュール322、アクセスコントローラ324、コンテキスト評価器326、および/または本明細書で説明する他の機能モジュールは、プロセッサ310を介して作業メモリ335から実行されるプロセッサ実行可能ソフトウェアコードを介して、コンピュータシステム300を介して実装され得る。そのようなコードおよび/または命令は、説明する方法に従って1つまたは複数の動作を実行するように汎用コンピュータ(または他のデバイス)を構成するおよび/または適合させるために使用され得る。

【００２７】

これらの命令および/またはコードのセットは、上記で説明した記憶デバイス325などのコンピュータ可読記憶媒体上に記憶され得る。場合によっては、記憶媒体は、コンピュータシステム300などのコンピュータシステム内に組み込まれ得る。他の実施形態では、記憶媒体は、記憶媒体がその上に記憶された命令/コードを用いて汎用コンピュータをプログラムする、構成するおよび/または適合させるために使用され得るように、コンピュータシステムから分離されてもよく(たとえば、コンパクトディスクなどのリムーバブル媒体)、かつ/またはインストールパッケージにおいて提供されてもよい。これらの命令は、コンピュータシステム300によって実行可能な実行可能コードの形態をとることができ、ならびに/または、ソースおよび/もしくはインストール可能コードの形態をとることができ、ソースおよび/もしくはインストール可能コードは次いで、(たとえば、一般に入手可能な様々なコンパイラ、インストールプログラム、圧縮/解凍ユーティリティなどのいずれかを使用する)コンピュータシステム300上でのコンパイルおよび/またはインストール時に実行可能コードの形態をとる。

【００２８】

図4を参照すると、モバイルデバイス上でセキュリティ資格情報を提供するユーザの図が示されている。モバイルデバイス100は、データ入力デバイスとしてのプログラマブルキーボード152を有するタッチスクリーンディスプレイ151と、視覚フィードバック機構としてのテキストボックスオブジェクト153とを含む。他のデータ入力およびディスプレイデバイス/オブジェクトが使用され得るので、ディスプレイ151、キーボード152、およびテキストボックスオブジェクト153は例示的なものにすぎず、限定ではない。動作の際、ユーザは、パスワード、パスフレーズ、ジェスチャ、または他の情報などのセキュリティコードをモバイルデバイス100上で実行されているアプリケーションに入力するよう促され得る。一例では、モバイルデバイス100はネットワーク化されたコンピュータシステム200の一部であり、ユーザはネットワークコンテンツ(すなわち、コンテンツデータベース206)にアクセスしようと試みている。ユーザは、以前にシステム200上でアカウントを設定した場合があるか、またはユーザのアカウント情報をリセットし、それぞれの時点でセキュリティ資格情報を提供した場合がある。システムにアクセスしようとする後続の試行において、ユーザは、キーボード152上でセキュリティ資格情報を入力するよう促される。セキュリティ資格情報の「x」個の文字数を入力した後(ここで、「x」は完全なセキュリティ資格情報よりも少ない文字である)、ユーザは、所望のコンテンツにアクセスすることが許可される。このようにして、ユーザがセキュリティ資格情報全体を入力する必要がないので、検証プロセスが加速される。ユーザは必ずしも「x」の値を知っているとは限らず、「x」の値はセキュリティ資格情報の中の文字に基づいて変化し得る。一実施形態では、「x」の値は、モバイルデバイス100が使用されているコンテキストに基づいて変化し得る。テキストボックスオブジェクト153の中の文字は、単にデモンストレーションとして示されており、セキュリティ資格情報の完全性を保持するのを助けるために一般的な記号(たとえば、ドット、アスタリスクなど)として表示され得る。

【００２９】

図1、図2および図4をさらに参照しながら図5Aおよび図5Bを参照すると、フルセキュリティストリングおよび対応するサブストリングを含むテーブル500が示されている。テーブル500は、フルセキュリティストリング/サブストリング列502、複雑度列504および文字列506を含む。フルセキュリティストリング/サブストリング列502の中のフィールドは、フルセキュリティストリング、およびフルセキュリティストリングからの異なる文字数を利用する6つのサブストリングの例である。文字列506は、フルセキュリティストリングおよびサブストリングの各々の中のそれぞれの文字数(たとえば、最初の「x」個の文字)を示す。複雑度列504は、それぞれのストリングに対するパスワード強度アルゴリズムの結果を表す。パスワード強度アルゴリズムは、ストリングのエントロピーを測定するように構成される。限定ではなく、一例として、パスワード強度アルゴリズムはwww.passwordmeter.comにおいて見出され得る。他のパスワード強度アルゴリズムおよび/またはエントロピー測定アルゴリズムも使用され得る。図5Bを参照すると、ユーザアカウントは、フルセ

キュリティストリング512と、第1のサブストリング514aと、第2のサブストリング514bと、第nのサブストリング514nとして示される任意の数の追加のサブストリングとを含むセキュリティストリングの集合510に関連付けられ得る。ストリングの集合の中のストリングの各々は、ストリング値をハッシュする前に、任意選択のソルト値と組み合わされ得る。たとえば、第nのサブストリング514nが第nのソルト値516nでソルトされ得るように、フルセキュリティストリング512には第1のソルト値516aがアペンドされてもよく、第1のサブストリング514aには第2のソルト値516bがアペンドされてもよく、第2のサブストリング514bには第3のソルト値516cがアペンドされてもよく、以下同様である。各ソルト値は通常、暗号学的にセキュアな擬似乱数生成器(CSPRNG:cryptographically secure pseudo-random number generator)を使用して生成されるが、ソルトのための他の値がセキュリティ計画または他のハードウェア考慮事項に基づいて使用され得る。ソルトは、辞書攻撃を阻止するためにストリングに追加される。ソルトは、ストリングをハッシュコードとして保存する前に、文字ストリングの先頭(すなわち、前)にプリペンドされてもよく、または文字ストリングの末尾(すなわち、後)にアペンドされてもよい。たとえば、ストリングの集合510および対応するソルトは各々、暗号化ハッシュ関数(たとえば、SHA256、SHA512、SHA3など)を介して変換されてもよく、得られたハッシュコードは、文字カウント列506からの対応する値とともに、アクセス制御データベース204上に記憶されてもよい。一実施形態では、ソルトおよび得られたハッシュコードのうちの1つまたは複数は、ローカルユーザ検証のために、信頼できる環境160に記憶されてもよい。認証モジュール144は、信頼できる環境160からソルト値を取り出し、テキストボックスオブジェクト153に与えられるデータをソルトし、ソルトされたストリングに対してハッシュ関数を実行し、その結果を信頼できる環境に記憶されたハッシュコードと比較するように構成される。

【００３０】

図1～図5をさらに参照しながら図6を参照すると、例示的なクライアントサーバメッセージフローの流れ図600が示されている。流れ図600は、クライアント602とサーバ604との間を流れる例示的なメッセージを示す。クライアント602はモバイルデバイス100であってもよく、サーバ604はサーバ202であってもよく、それぞれの例示的なメッセージはネットワーク210およびワイヤレス信号123を介して送信され得る。メッセージは、セキュアソケットレイヤ(SSL)またはハイパーテキスト転送プロトコルセキュア(HTTPS)などのセキュアインターネットプロトコルを介して交換され得る。ユーザは、サーバ604上でアカウントを作成するためにクライアント602を利用することができ、ユーザのアカウントを識別するuserIDなどのログイン情報を提供することができる。同様のプロセスは、以前にサーバ604上でアカウント(以前のuserIDを含む)を設定したユーザに対して行われ得るが、ユーザのセキュリティ資格情報をリセットしなければならない。1つまたは複数のアカウント作成メッセージ606がサーバ604と交換され得る。応答して、フルセキュリティストリングを提供するようユーザを促すために、サーバからセキュリティ情報要求メッセージ608が送られ得る。フルセキュリティストリングメッセージ610は、ユーザがアカウントアクセス要求を確認するためにセキュリティ資格情報として利用することを望む、非常に長いパスワード、パスフレーズ、一連のジェスチャ、または他の情報を含む。段階612において、サーバ604は、フルセキュリティストリングのためのハッシュコードを生成し、記憶するように構成される。サーバ604は、1つまたは複数のサブストリング(すなわち、フルセキュリティストリングの最初の「x」個の文字)のセキュリティ強度を評価し、それぞれのサブストリングハッシュコードおよび対応する文字カウント(すなわち、「x」の値)を生成し、記憶する。ハッシュコードは、userIDまたは他のインデックス情報を介してユーザに関連付けられ得る。

【００３１】

後続のログイン試行の際、ユーザは、ユーザのuserIDまたは他の識別情報を含むユーザIDログインメッセージ614を提供し得る。段階616において、サーバ604は、以前に決定されたサブストリングのうちのどれを加速された検証のために使用するかを決定するように構成される。サブストリングの選択は、モバイルデバイスのロケーション、現在の時刻、

または他の考慮事項などの現在のコンテキストに基づき得る。一実施形態では、フルセキュリティストリングごとに1つだけのサブストリングが記憶される。サブストリングに関連付けられた文字数が決定され(たとえば、アクセス制御データベース204から取り出され)、その数値が文字カウント情報メッセージ618を介してクライアント602に提供される。クライアント602は、フルセキュリティストリングを入力するようユーザを促し、ユーザによって入力されるときに各文字をカウントするように構成される。ユーザは、文字カウント情報メッセージ618の中の数値に気づいていない。ユーザによって入力された文字数が文字カウント情報メッセージ618において与えられた値に等しいとき、クライアント602は、入力された文字(すなわち、サブストリング)をサブストリングメッセージ620を介してサーバ604に提供するように構成される。ユーザは、サブストリングメッセージ620の交換に気づいていない。段階622において、サーバ604は、サブストリングメッセージ620において受信されたサブストリングを確認するように構成される。確認は、受信されたサブストリングのためのハッシュコードを生成することと、得られたハッシュコードをアクセス制御データベース204の中の以前に記憶されたハッシュコードと比較することとを含む。ソルト値も、前に説明したように使用され得る。確認の結果に基づいて、1つまたは複数の許可/拒否メッセージ624がクライアント602に提供される。確認が成功した場合、ユーザは、ユーザのフルセキュリティストリング全体を入力することなしに、ユーザのアカウントへのアクセスを与えられる。サブストリングメッセージ620はユーザが知らないうちに送信されるので、ユーザに対する効果は加速された検証プロセスである。段階622における確認プロセスが失敗した場合、許可/拒否メッセージ624は、アカウントへのアクセスが拒否さ
れたことをユーザに示すことができ、サーバ604は、失敗したアクセス試行を記録することができる。

【００３２】

図2および図5をさらに参照しながら図7を参照すると、加速されたパスフレーズ検証とともに使用するための例示的なデータ構造700が示されている。追加のテーブル、フィールド、インデックス、および関係が使用され得るので、データ構造700は例示的なものにすぎず、限定ではない。データ構造700は、サーバ202、またはネットワーク210上の他の記憶デバイスに残存することができ、アクセス制御データベース204およびコンテンツデータベース206などの1つまたは複数のデータベースを含むことができる。データベース204、206は、テーブルの集合を有する1つまたは複数のリレーショナルデータベースであり得る。データベース204、206内のデータの一部または全部は、モバイルデバイス100上にも記憶され得る。データベース204、206は、ユーザアカウントおよびログイン確認に関するデータフィールドを含む1つまたは複数のテーブル702、704を含むことができる。データフィールドは、当技術分野で知られているデータタイプ(たとえば、number、char、varchar、dateなど)とすることができる。アクセス制御データベース204の中に含まれる情報は、UserIDなどのユーザアカウントと、連絡先情報、課金情報、セキュリティの質問などのユーザ情報とを表す複数のフィールド(たとえば、Userinfo1、Userinfo2など)を含むアカウントテーブル702を含み得る。ユーザアカウントは、現在のコンテキストをユーザに関連付けるために、コンテキストデータベース(たとえば、Contextlink)にリンクされ得る。コンテキストは、位置情報、周囲音、ユーザ挙動、およびユーザ履歴データファイルに基づき得る。ユーザアカウントテーブルは、ユーザセキュリティデータを含んでもよく、または、ユーザセキュリティ情報を含むセキュリティテーブル704にリンクされてもよい。ユーザセキュリティ情報は、インデックス704a、リンクID704b、ソルト値704c、ハッシュコード704d、文字カウント値704e、およびコンテキスト選択基準704fなどのフィールドを含み得る。インデックス704aは、セキュリティテーブル704の中の個々の記録を識別するために使用されることがあり、リンクID704bは、対応する記録をアカウントテーブル702の中の記録にリンクさせるために使用されることがある。ソルト値704cは、ソルト値がセキュリティストリングの暗号ハッシュ化において使用される場合に必要とされる。ハッシュコード704dは、それぞれのソルト値704cを有するフルセキュリティストリング/サ

ブストリング列502の中の値の連結に対して実行されたハッシュ関数の結果である。図7のソルト値704cおよびハッシュコード704dは例にすぎず、図7の視覚的な審美性を高めるために短縮されている。文字カウント値704eは、文字カウント列506の中のそれぞれの値と一致する。コンテキスト選択基準704fは、クライアント602がアクセスを要求している現在のコンテキストに対応する相対値を表す。たとえば、現在のコンテキストがビジーエリア、または以前に訪問されていないロケーションに関連付けられる場合、ユーザは、ユーザのアカウントにアクセスできるようにするために、より大きいセキュリティサブストリングを提供することが必要とされ得る。逆に、ユーザが既存の使用パターンに準拠しているか、またはプライベートロケーションにいることをコンテキストが示す場合、より小さいセキュリティサブストリングが検証を可能にし得る。

【００３３】

ハッシュコード704dは、サブストリングおよびソルトに対してSHA256などの暗号化ハッシュ関数を実行した結果であり得る。たとえば、サブストリングが(たとえば、フルセキュリティストリング/サブストリング列502に示すように)8文字のストリング「Ju3Tou2W」であり、対応するソルト値704cが「4ece73a9bcbf066e」である(たとえば、図7の記録インデックス48を参照されたい)場合、対応するハッシュ関数は、

ハッシュコード=SHA256(ソルト||Ju3Tou2W)

であり、ここで、||は連結演算である。

図7のユーザセキュリティテーブルの中のハッシュコード704dの値は、視覚的な審美性のために短縮されている。ソルト値704cはランダムな16進数を含む一例であるが、ソルト値は他のデータ値を含み得る。他のソルト値および暗号アルゴリズムが使用され得るので、ソルト値704cおよびSHA256暗号化ハッシュ関数は例にすぎない。

【００３４】

図1～図7をさらに参照しながら図8を参照すると、コードを有するサブストリングを生成するためのプロセス800は、図示の段階を含む。しかしながら、プロセス800は一例にすぎず、限定的ではない。プロセス800は、たとえば、段階を追加、除去、再配置、結合、および/または同時に実行することによって、改変され得る。たとえば、第1のソルト値および/または第2のソルト値を生成することは任意選択であり、対応する段階は図8では破線で示されている。プロセス800は、クライアントサーバアプリケーションについてはサーバ202上で(たとえば、リモートログイン)、またはモバイルデバイス100上でローカルに(たとえば、ローカル認証)実行され得る。

【００３５】

段階802において、サーバ202は、フルセキュリティストリングを受信するように構成される。フルセキュリティストリングは、モバイルデバイス100に入力され、ネットワーク210を介してサーバに提供されてもよい。モバイルデバイス100も、フルセキュリティストリングを受信するように構成され得る。サーバ202およびモバイルデバイス100は、フルセキュリティストリングを受信するための手段である。フルセキュリティストリングは、パスワード、パスフレーズ、ジェスチャ、または他の情報などの、ユーザがコンピューティングデバイスに入力し得る比較的非常に長いセキュリティ資格情報である。図5に示すように、長さが21文字のフルセキュリティストリングの一例は、ストリング「Ju3Tou2Wang3Ming2Yue4」である。ジェスチャ入力(たとえば、ジェスチャ入力のASCII、16進法、および/またはバイナリ表現)に対応する永続的データなど、他の長さおよび要素が使用され得る。

【００３６】

段階804において、サーバ202上の認証モジュール322は、フルセキュリティストリングに基づいて、フルセキュリティストリングハッシュコードを生成し、記憶するように構成される。フルセキュリティストリングハッシュコードは、アクセス制御データベース204に記憶され得る。ローカル認証の場合、モバイルデバイス100上の認証モジュール144および信頼できる環境160も、フルセキュリティハッシュコードを生成し、記憶するように構成され得る。サーバ202またはモバイルデバイス100は、フルセキュリティハッシュコード

を生成し、記憶するための手段であり得る。フルセキュリティストリングハッシュコードは、段階806において生成されたソルト値を含み得る。ソルト値は任意選択であるが、一般的に、ルックアップテーブルおよびレインボーテーブルを使用して攻撃を阻止するために推奨される。任意の値がソルトとして使用され得るが、好ましい解決策は、暗号学的にセキュアな擬似乱数生成器(たとえば、Java(登録商標)の場合はjava.security.SecureRandom、MS dot NETの場合はsystem.security.cryptography.RNGCyptoServiceProvider、C/C++の場合はCryptGenRandom)を使用することである。ソルトは、段階802において受信されたフルセキュリティストリング値と連結され得る(たとえば、プリペンドする、アペンドする)。フルセキュリティストリングハッシュコードは、フルセキュリティストリングおよび存在する場合は連結されたソルトに対して暗号化ハッシュ関数を実行した結果である。暗号化ハッシュ関数の例としては、SHA256、SHA512、RipeMD、Whirlpoolがある。他の暗号化ハッシュ関数も使用され得る。得られたフルセキュリティハッシュコードは、アクセス制御データベース204などのメモリに記憶される。たとえば、フルセキュリティハッシュコードおよび任意選択のソルト値は、特定のユーザ(たとえば、アカウントテーブル702の中の記録)に関連付けられたセキュリティテーブル704に記憶され得る。フルストリングハッシュコードをユーザに関連付けるために、他のデータ構造も使用され得る。

【００３７】

段階808において、サーバ202上の認証モジュール322は、フルセキュリティストリングの中の1つまたは複数の先頭文字に関連付けられたエントロピー値に基づいて、少なくとも1つのサブストリングを決定するように構成される。ローカル認証の場合、モバイルデバイス100上の認証モジュール144および信頼できる環境160も、フルセキュリティストリングの中の1つまたは複数の先頭文字に関連付けられたエントロピー値に基づいて、少なくとも1つのサブストリングを決定するように構成され得る。サーバ202またはモバイルデバイス100は、フルセキュリティストリングの中の1つまたは複数の先頭文字に関連付けられたエントロピー値に基づいて、少なくとも1つのサブストリングを決定するための手段であり得る。フルセキュリティストリングの中の最初の「x」個の文字のエントロピーは、十分に強いレベルのサブストリングが実現されるまで、文字ごとに評価され得る。十分に強いという要件は、ネットワークセキュリティ設計要件に基づき得る。図5Aを参照すると、複雑度列504は、エントロピー複雑度レベルまたは強度レベルの相対的な指示(たとえば、弱い、良い、強い、非常に強い)を提供し、十分に強いサブストリングは、設計要件に基づいて、良い、強い、または非常に強い値に対応し得る。既製の強度メーターアルゴリズムは、ストリングの複雑度レベルを決定するために使用され得る。一例では、ストリング「Ju3Tou2W」は、「強い」の複雑度値に対応するエントロピーを有するので、十分に強いサブストリングと見なされる。サブストリング「Ju3Tou2W」は、フルセキュリティストリング「Ju3Tou2Wang3Ming2Yue4」の中の8つの先頭文字である。したがって、この例では、サブストリング「Ju3Tou2W」は、フルセキュリティストリングの中の1つまたは複数の先頭文字に関連付けられたエントロピー値に基づいて、少なくとも1つのサブストリングであると決定される。

【００３８】

段階810において、サーバ202上の認証モジュール322は、少なくとも1つのサブストリングハッシュコードおよび少なくとも1つの対応する文字カウント値を生成し、記憶するように構成される。ローカル認証の場合、モバイルデバイス100上の認証モジュール144および信頼できる環境160も、少なくとも1つのサブストリングハッシュコードおよび少なくとも1つの対応する文字カウント値を生成し、記憶するように構成され得る。サーバ202またはモバイルデバイス100は、少なくとも1つのサブストリングハッシュコードおよび少なくとも1つの対応する文字カウント値を生成し、記憶するための手段であり得る。上記の例を続けると、サブストリング「Ju3Tou2W」および(段階812において生成された)任意選択のソルト値は、(たとえば、前に説明したように暗号化ハッシュ関数を介して)サブストリングハッシュコードを作成するために使用され得る。図7に示すように、サブストリングハッシュコード、対応する文字カウント値、および任意選択のソルト値は、セキュリティ

テーブル704(すなわち、704c、704d、704e)に記憶され得る。ローカル認証実施形態では、セキュリティテーブル704は、モバイルデバイス上の信頼できる環境160に残存し得る。

【００３９】

図1～図7をさらに参照しながら図9を参照すると、サーバ上での加速されたパスフレーズ検証のためのプロセス900は、図示の段階を含む。しかしながら、プロセス900は一例にすぎず、限定的ではない。プロセス900は、たとえば、段階を追加、除去、再配置、結合、および/または同時に実行することによって、改変され得る。たとえば、コンテキスト情報を受信することは任意選択であり、したがって、段階906は破線で示されている。

【００４０】

段階902において、サーバ604上のアクセスコントローラ324は、アクセス要求がユーザ識別情報を含むように、クライアント602からアクセス要求を受信するように構成される。一例では、クライアント602はモバイルデバイス100であり、アクセス要求はネットワーク210を介して受信される。サーバ604は、クライアントからアクセス要求を受信するための手段である。ユーザ識別情報は、ユーザによって選択されたユーザ名に基づいてもよく、または特定のクライアントデバイス(たとえば、ネットワークインターフェースコントローラ(NIC)、加入者識別モジュール(SIM)、または他の一意のキー)に関連付けられてもよい。クライアント602は、コンテンツデータベース206上の情報にアクセスすることを要望する場合があり、サーバ202は、セキュリティパスフレーズなどの以前に提供された情報に基づいて、クライアントの資格情報を検証するように構成される。ユーザ識別情報は、セキュリティ資格情報を特定のクライアント/ユーザに関連付けるために使用される。

【００４１】

任意選択の段階906において、サーバ604上のコンテキスト評価器326は、コンテキスト情報を受信するように構成される。コンテキスト情報は、ロケーション情報(たとえば、モバイルデバイスの現在のロケーション)、またはモバイルデバイス100上のマイクロフォンを介してキャプチャされた周囲雑音などの他の同時期の環境情報であってもよい。コンテキスト情報は、段階902においてアクセス要求が受信された時刻であってもよく、コンテキスト評価器326は、その時刻をクライアントの使用履歴および前の挙動に対応するデータファイルと比較するように構成される。コンテキスト評価器326は、クライアント602がアクセスを要求している現在のコンテキストに対応するコンテキスト選択基準704fを割り当て得る。コンテキスト選択基準704fは、コンテキストに関連付けられたセキュリティニーズの相対的なスケールを示す、整数値、または他のデータタイプであってもよい。図7に示すように、セキュリティテーブル704は、高いコンテキスト選択基準704f(たとえば、10の値)は、ユーザを確認するためにフルセキュリティストリングの入力を必要とするが、より低いコンテキスト選択基準704f(たとえば、7の値)は、ユーザを確認するためにフルセキュリティストリングの最初の8文字(たとえば、サブストリング)のみが入力されることを必要とすることを示す。一実施形態では、アクセス制御データベース204は、クライアントについて2つのセキュリティストリングのみ(すなわち、フルセキュリティストリングおよび単一のサブストリング)を含み得る。コンテキスト情報がサーバ604によって受信された場合、コンテキスト情報は、フルセキュリティストリングまたはサブストリングが必要とされる(すなわち、2つのみのコンテキスト選択基準値が必要とされる)かどうかを決定するために使用され得る。コンテキスト選択は、ロケーションおよび時刻、または時刻および履歴などの(すなわち、アカウントにアクセスしようとする複数の試行を検出するための)1つまたは複数の要因に基づき得る。現在のコンテキスト値を決定するために、環境要因および挙動要因の他の組合せが使用され得る。サーバ604上のコンテキスト評価器326は、現在のコンテキスト値を決定するための手段である。

【００４２】

段階904において、サーバ604上のアクセスコントローラ324は、段階902において受信されたユーザ識別情報に少なくとも部分的に基づいて、文字カウント値を決定するように構成される。サーバ604上のアクセス制御データベース204は、文字カウント値を決定するための手段である。サーバ604は、(たとえば、記憶されたプロシージャまたは他のデータア

クセスコマンドを介して)アクセス制御データベース204を照会して文字カウント値を決定するために、ユーザ識別情報および任意選択のコンテキスト選択基準を利用し得る。文字カウント値704eは、対応するサブストリングの中の文字数(たとえば、図5Aでは、最初の「x」個の文字)である。フルセキュリティストリングおよび単一のサブストリングのみがユーザに関連付けられる場合、段階908においてサブストリングの文字カウントが選択され、クライアントに提供される。たとえば、クライアントは、ネットワーク210を介して文字カウント情報メッセージ618を受信し得る。

【００４３】

段階910において、サーバ604上のアクセスコントローラ324は、サブストリングの長さが文字カウント値に対応するように、クライアントからサブストリングを受信するように構成される。アクセスコントローラ324は、クライアントからサブストリングを受信するための手段である。クライアントは、対応する長さのサブストリングを含むサブストリングメッセージ620を送り得る。上記で説明した例を続けると、サーバ604が段階908において「8」の文字カウント値を提供した場合、クライアント602は、サブストリングメッセージ620の中にサブストリング「Ju3Tou2W」を含み得る。

【００４４】

段階912において、サーバ604上のアクセスコントローラ324は、段階910において受信されたサブストリングを検証するように構成される。アクセスコントローラ324は、サブストリングを検証するための手段である。受信されたサブストリングは、以前に記憶されたソルト値(たとえば、704c)と組み合わされてもよく、暗号化ハッシュコードが決定されてもよい。得られたハッシュコードは、アクセス制御データベース204の中のそれぞれの記録(たとえば、704d)と比較される。ハッシュコードが一致する場合、サブストリングは有効であり、段階914においてアクセス要求が許可される。ハッシュコードが一致しない場合、サブストリングは無効であり、段階914においてアクセス要求が拒否される。確認の許可された結果または拒否された結果に基づいたサーバ604の機能は、アプリケーションに基づいて変化し得る。一例では、失敗した確認の後、サーバ604は、文字カウント値に基づいて1つまたは複数の追加の試行を行うようユーザに求めるように構成されてもよく、次いで、後続の試行時にフルセキュリティストリングを入力するようユーザに要求してもよい。

【００４５】

図1～図7をさらに参照しながら図10を参照すると、クライアント上での加速されたパスフレーズ検証のためのプロセス1000は、図示の段階を含む。しかしながら、プロセス1000は一例にすぎず、限定的ではない。プロセス1000は、たとえば、段階を追加、除去、再配置、結合、および/または同時に実行することによって、改変され得る。モバイルデバイス100などのクライアント602は、プロセス1000を実行するための手段である。

【００４６】

段階1002において、モバイルデバイス100は、フルセキュリティストリングが第1の文字で始まるように、サーバ上でuserID値およびフルセキュリティストリングを含むユーザアカウントを作成するように構成される。userID値は、ユーザによって入力される、またはユーザに提供されるストリング(たとえば、電子メールアドレスまたは他の一意の識別子)であり得る。userIDは、NIC値またはSIM値などのシステム変数であり得る。フルセキュリティストリングは、連続した文字または他のデータ(たとえば、ジェスチャ入力に対応する永続的データ)の比較的非常に長いストリングであり得る。シーケンスは第1の文字で始まる。たとえば、図5で提供されるフルセキュリティストリング「Ju3Tou2Wang3Ming2Yue4」は、第1の文字「J」で始まる。フルセキュリティストリングは、ユーザによってタッチスクリーンディスプレイ151を介して、または他のタイプの入力デバイスを介して提供され得る。

【００４７】

段階1004において、モバイルデバイス100は、サブストリングが第1の文字で始まるフルセキュリティストリングの中の連続する文字のサブセットからなるように、userID値およ

びサブストリングを提供することによってユーザアカウントにアクセスするように構成される。ユーザは、その後、適切なセキュリティ資格情報を提供することによって、段階1002において作成されたユーザアカウントにアクセスしようと試みることができる。userIDは、userIDを適切なデータオブジェクトにタイプすることによって提供されるか、またはハードウェア構成(たとえば、NIC、SIM)に基づいてパッシブに提供され得る。次いで、ユーザは、ユーザが段階1002において提供したフルセキュリティストリングを入力し始めることができる。上記の例を続けると、ユーザは、第1の文字「J」を適切なデータオブジェクト(たとえば、テキストボックスオブジェクト153)に入力し、連続する文字を続ける。すなわち、ユーザによって提供されるサブストリングは、「J」の後に「u」が続き、その後に「3」が続き、その後に「T」が続き、その後に「o」が続き、その後に「u」が続き、その後に「2」が続き、その後に「W」が続く、といった具合である。少なくとも第1の文字「J」を入力した後の、ただしフルセキュリティストリングを入力する前の、このプロセスにおける任意の時点で、ユーザの資格情報が確認されるかまたは拒否される。入力されるべきサブストリングにおける文字数は、ユーザに知られていない。上記で説明したように、サブストリングにおける文字数は、サブストリングの以前に評価されたエントロピー(すなわち、強度)に基づいて変化し得る。一実施形態では、モバイルデバイスの現在のコンテキストも、サブストリングの長さを決定するために使用され得る。このようにして、プロセス1000を介して、加速されたパスフレーズ確認がモバイルデバイスによって実現される。

【００４８】

大幅な変形が特定の要望に従って行われる場合がある。たとえば、カスタマイズされたハードウェアが使用されることもあり、かつ/または特定の要素がハードウェア、ソフトウェア(アプレットなどのポータブルソフトウェアを含む)、もしくはその両方において実装されることがある。さらに、ネットワーク入力/出力デバイスなどの他のコンピューティングデバイスへの接続が用いられることがある。

【００４９】

(コンピュータシステム300などの)コンピュータシステムは、本開示による方法を実行するために使用され得る。そのような方法の手順の一部または全部は、作業メモリ335に含まれる(オペレーティングシステム340および/またはアプリケーションプログラム345などの他のコードに組み込まれる場合がある)1つまたは複数の命令の1つまたは複数のシーケンスをプロセッサ310が実行したことに応答して、コンピュータシステム300によって実行され得る。そのような命令は、記憶デバイス325のうちの1つまたは複数などの別のコンピュータ可読媒体から作業メモリ335に読み込まれ得る。単に例として、作業メモリ335に含まれる命令のシーケンスの実行は、プロセッサ310に、本明細書で説明する方法の1つまたは複数の手順を実行させ得る。

【００５０】

本明細書で使用する「機械可読媒体」および「コンピュータ可読媒体」という用語は、機械を特定の方式で動作させるデータを提供することに関与する任意の媒体を指す。モバイルデバイス100および/またはコンピュータシステム300を使用して実装される一実施形態では、様々なコンピュータ可読媒体は、実行のために命令/コードをプロセッサ111、310に提供することに関与することがあり、かつ/またはそのような命令/コードを(たとえば、信号として)記憶および/または搬送するために使用されることがある。多くの実装形態では、コンピュータ可読媒体は、物理的な記憶媒体および/または有形の記憶媒体である。そのような媒体は、限定はしないが、不揮発性媒体、揮発性媒体、および伝送媒体を含む、多くの形態をとることができる。不揮発性媒体は、たとえば、記憶デバイス140、325などの光ディスクおよび/または磁気ディスクを含む。揮発性媒体は、限定はしないが、作業メモリ140、335などのダイナミックメモリを含む。伝送媒体は、限定はしないが、バス101、305、ならびに通信サブシステム330(および/または通信サブシステム330が他のデバイスとの通信を提供する媒体)の様々な構成要素を備える電線を含む、同軸ケーブル、銅線および光ファイバを含む。したがって、伝送媒体は、波(限定はしないが、無線波デ

ータ通信および赤外線データ通信中に生成されるものなどの無線波、音波および/または光波を含む)の形態をとることもできる。

【００５１】

物理的なおよび/または有形のコンピュータ可読媒体の一般的な形態は、たとえば、フロッピーディスク、フレキシブルディスク、ハードディスク、磁気テープもしくは任意の他の磁気媒体、CD-ROM、ブルーレイディスク、任意の他の光媒体、パンチカード、紙テープ、穴のパターンを有する任意の他の物理媒体、RAM、PROM、EPROM、FLASH-EPROM、任意の他のメモリチップもしくはカートリッジ、以下で説明するような搬送波、またはコンピュータが命令および/もしくはコードを読み取ることができる任意の他の媒体を含む。

【００５２】

コンピュータ可読媒体の様々な形態は、実行のために1つまたは複数の命令の1つまたは複数のシーケンスをプロセッサ111、310に搬送することに関与することがある。単に例として、命令は最初に、リモートコンピュータの磁気ディスクおよび/または光ディスク上で搬送され得る。リモートコンピュータは、命令をそのダイナミックメモリ内にロードし、モバイルデバイス100および/またはコンピュータシステム300によって受信および/または実行されるべき命令を信号として伝送媒体を介して送ることができる。電磁信号、音響信号、光信号などの形態であってもよいこれらの信号はすべて、本発明の様々な実施形態による、命令が符号化され得る搬送波の例である。

【００５３】

上記で説明した方法、システム、およびデバイスは例である。様々な代替構成は、様々な手順または構成要素を適宜に省略、置換、または追加することができる。たとえば、代替方法では、段階は上記の説明とは異なる順序で実行されてもよく、様々な段階が追加、省略、または組み合わされてもよい。また、いくつかの構成に関して説明した特徴は、様々な他の構成において組み合わされてもよい。構成の異なる態様および要素は、同様の方法で組み合わされてもよい。また、技術は進化しており、したがって、要素の多くは例であり、本開示の範囲または特許請求の範囲を限定しない。

【００５４】

例示的な構成(実装形態を含む)の完全な理解を与えるために、説明において具体的な詳細が与えられている。しかしながら、構成は、これらの具体的な詳細なしに実践される場合がある。たとえば、構成を不明瞭にすることを避けるために、よく知られている回路、プロセス、アルゴリズム、構造、および技法は、不必要な詳細なしに示されている。この説明は、例示的な構成のみを提供し、特許請求の範囲の範囲、適用可能性、または構成を限定しない。むしろ、これらの構成の上述の説明は、説明した技法を実装するための有効な説明を当業者に提供することになる。本開示の趣旨または範囲から逸脱することなく、要素の機能および配置において様々な変更が行われ得る。

【００５５】

構成は、流れ図またはブロック図として示されるプロセスとして説明され得る。各々は動作について順次プロセスとして説明する場合があるが、動作の多くは並行してまたは同時に実行され得る。加えて、動作の順序は並べ替えられてもよい。プロセスは、図に含まれていない追加のステップを有してもよい。さらに、方法の例は、ハードウェア、ソフトウェア、ファームウェア、ミドルウェア、マイクロコード、ハードウェア記述言語、またはそれらの任意の組合せによって実装され得る。ソフトウェア、ファームウェア、ミドルウェア、またはマイクロコードにおいて実装されるとき、必要なタスクを実行するプログラムコードまたはコードセグメントは、記憶媒体などの非一時的コンピュータ可読媒体に記憶され得る。プロセッサは、説明したタスクを実行し得る。

【００５６】

特許請求の範囲を含め、本明細書で使用する場合、「のうちの少なくとも1つ」で始まる項目のリストで使用される「または」は、たとえば、「A、B、またはCのうちの少なくとも1つ」のリストがAもしくはBもしくはCもしくはABもしくはACもしくはBCもしくはABC(すなわち、AおよびBおよびC)、または2つ以上の特徴を有する組合せ(たとえば、AA、AAB

、ABBCなど)を意味するような、選言的リストを示す。

【００５７】

特許請求の範囲を含め、本明細書で使用する場合、別段に明記されていない限り、機能または動作が項目または条件「に基づく」という記述は、機能または動作が述べられた項目または条件に基づいており、述べられた項目または条件に加えて1つまたは複数の項目および/または条件に基づき得ることを意味する。

【００５８】

いくつかの例示的な構成について説明したが、様々な変更形態、代替構成、および等価物は、本開示の趣旨から逸脱することなく使用され得る。たとえば、上記の要素は、より大きいシステムの構成要素である場合があり、他の規則が、本発明の適用例よりも優先するか、またはさもなければ本発明の適用例を変更する場合がある。また、上記の要素が考慮される前、間、または後に、いくつかのステップが行われ得る。したがって、上記の説明は、特許請求の範囲を制限しない。

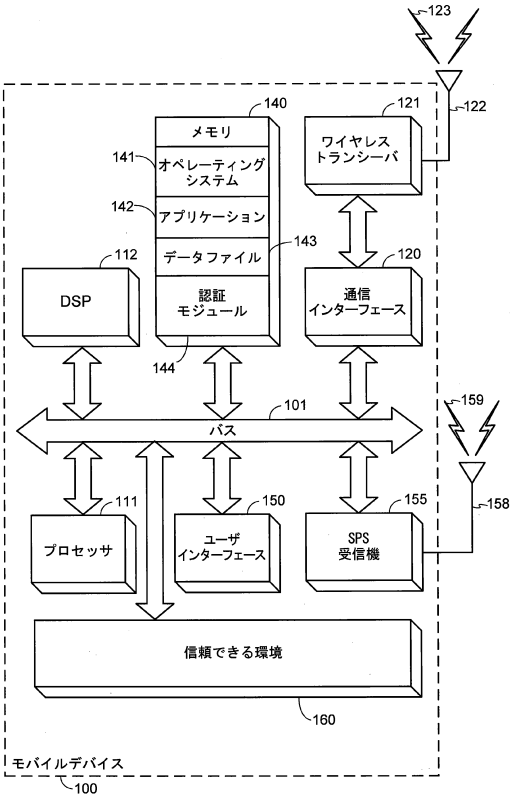
【符号の説明】

【００５９】

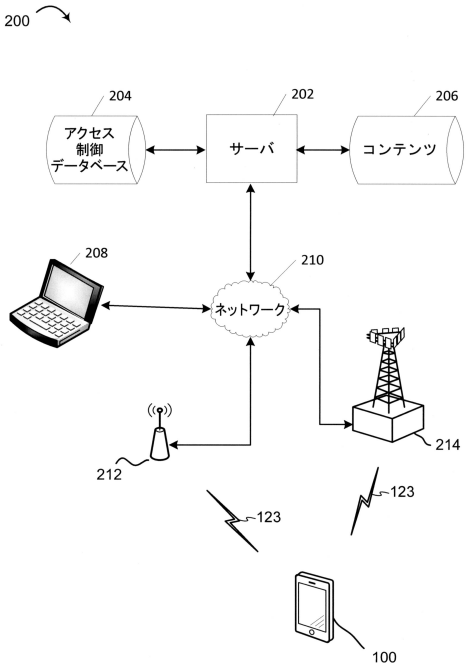
100 モバイルデバイス
101 公共バス、バス
111 プロセッサ、汎用プロセッサ
112 DSP
120 通信インターフェース
121 ワイヤレストランシーバ
122 ワイヤレスアンテナ
123 ワイヤレス信号
140 メモリ、記憶デバイス、作業メモリ
141 オペレーティングシステム
142 アプリケーション
143 データファイル
144 認証モジュール
150 ユーザインターフェース
151 タッチスクリーンディスプレイ、ディスプレイ
152 プログラマブルキーボード、キーボード
153 テキストボックスオブジェクト
155 SPS受信機
158 SPSアンテナ
159 衛星測位システム(SPS)信号、SPS信号
160 信頼できる環境
200 ネットワーク化されたコンピュータシステム、システム
202 サーバ
204 アクセス制御データベース、データベース
206 コンテンツデータベース、データベース
208 パーソナルコンピュータ
210 ネットワーク
212 アクセスポイント
214 基地局
300 コンピュータシステム
305 バス
310 プロセッサ
315 入力デバイス
320 出力デバイス
322 認証モジュール

324 アクセスコントローラ
325 非一時的記憶デバイス、記憶デバイス
326 コンテキスト評価器
330 通信サブシステム
335 作業メモリ
340 オペレーティングシステム
345 アプリケーションプログラム
500 テーブル
502 フルセキュリティストリング/サブストリング列
504 複雑度列
506 文字列
510 セキュリティストリングの集合、ストリングの集合
512 フルセキュリティストリング
514a 第1のサブストリング
514b 第2のサブストリング
514n 第nのサブストリング
516a 第1のソルト値
516b 第2のソルト値
516c 第3のソルト値
516n 第nのソルト値
600 流れ図
602 クライアント
604 サーバ
606 アカウント作成メッセージ
608 セキュリティ情報要求メッセージ
610 フルセキュリティストリングメッセージ
614 ユーザIDログインメッセージ
618 文字カウント情報メッセージ
620 サブストリングメッセージ
624 許可/拒否メッセージ
700 データ構造
702 テーブル、アカウントテーブル
704 テーブル、セキュリティテーブル
704a インデックス
704b リンクID
704c ソルト値
704d ハッシュコード
704e 文字カウント値
704f コンテキスト選択基準
800 プロセス
900 プロセス
1000 プロセス

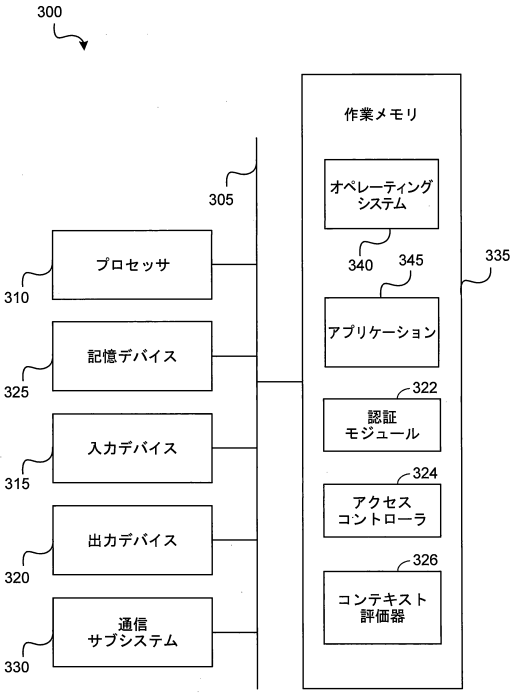
【図１】


123
122
140
メモリ
121
ワイヤレス
トランシーバ
141
オペレーティング
システム
142
アプリケーション
143
データファイル
112
DSP
認証
モジュール
120
通信
インターフェース
144
159
101
バス
158
111
プロセッサ
150
ユーザ
インターフェース
155
SPS
受信機
信頼できる環境
160
モバイルデバイス
100

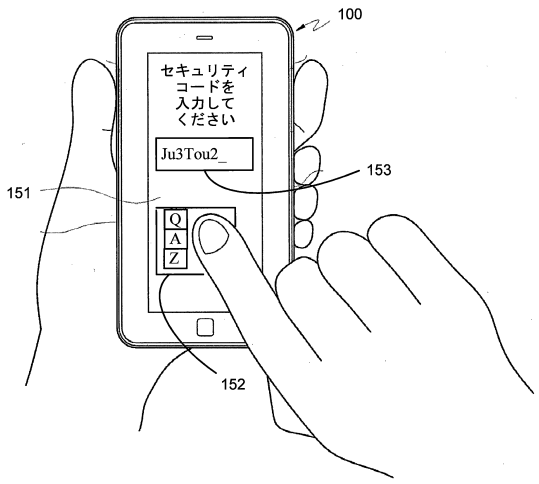
【図２】


200
204
アクセス
制御
データベース
202
サーバ
206
コンテンツ
208
210
ネットワーク
214
212
123
123
100

【図３】


300
作業メモリ
305
オペレーティング
システム
340
345
335
プロセッサ
310
アプリケーション
記憶デバイス
325
322
認証
モジュール
入力デバイス
315
324
アクセス
コントローラ
出力デバイス
320
326
コンテキスト
評価器
通信
サブシステム
330

【図４】

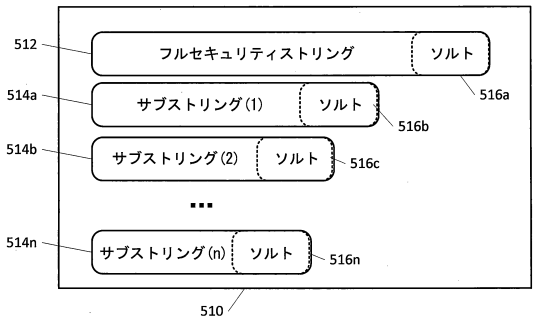

100
セキュリティ
コードを
入力して
ください
Ju3Tou2_
153
151
Q
A
Z
152

【図５Ａ】

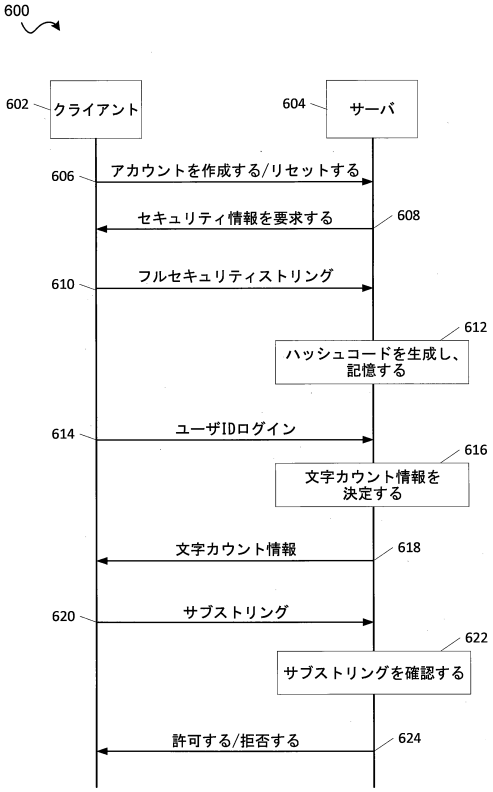
500

502 フルセキュリティストリング/サブストリング	504 複雑度	506 文字
Ju3Tou2Wang3Ming2Yue4	非常に強い	21
Ju3Tou2Wang3Ming2	非常に強い	17
Ju3Tou2Wang3	非常に強い	12
Ju3Tou2W	強い	8
Ju3Tou2	良い	7
Ju3Tou	良い	6
Ju3To	弱い	5

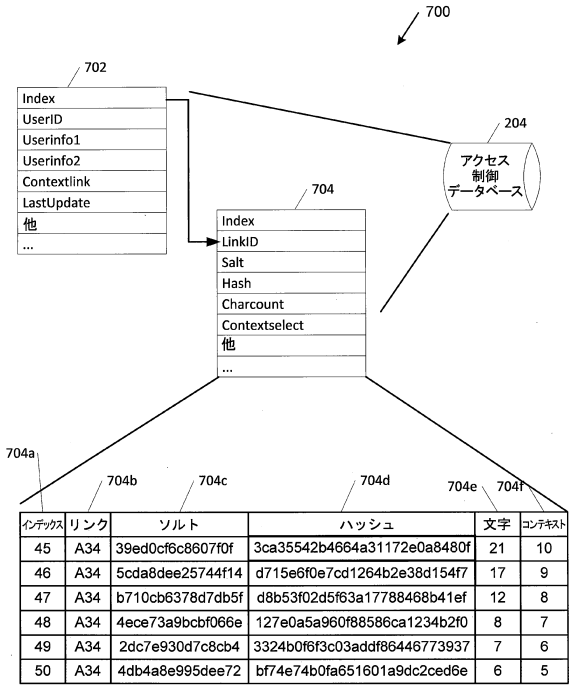
【図５Ｂ】



【図６】

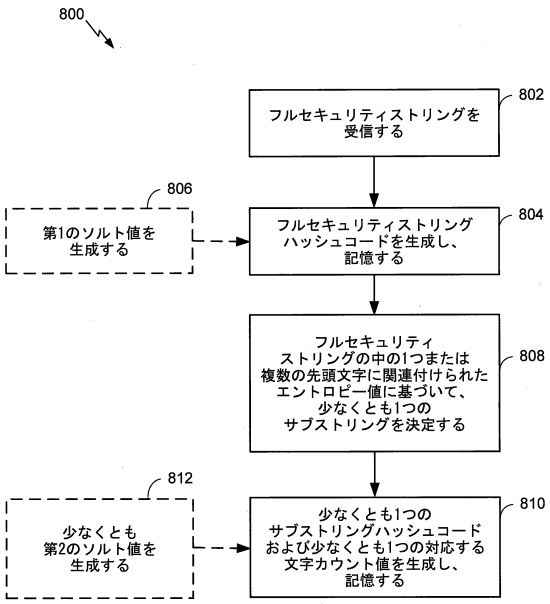


【図７】

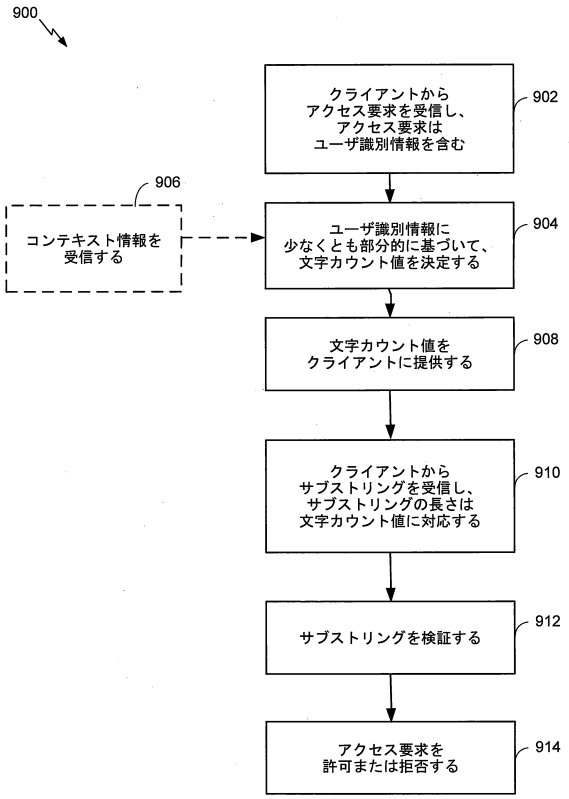


704a インデックス	704b リンク	704c ソルト	704d ハッシュ	704e 文字	704f コンテキスト
45	A34	39ed0cf6c8607f0f	3ca35542b4664a31172e0a8480f	21	10
46	A34	5cda8dee25744f14	d715e6f0e7cd1264b2e38d154f7	17	9
47	A34	b710cb6378d7db5f	d8b53f02d5f63a17788468b41ef	12	8
48	A34	4ece73a9bcbf066e	127e0a5a960f88586ca1234b2f0	8	7
49	A34	2dc7e930d7c8cb4	3324b0f6f3c03addf86446773937	7	6
50	A34	4db4a8e995dee72	bf74e74b0fa651601a9dc2ced6e	6	5

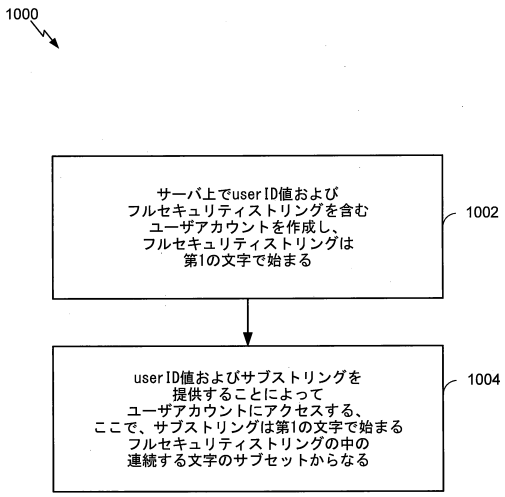
【図８】



【図９】


900
クライアントから
アクセス要求を受信し、
アクセス要求は
ユーザ識別情報を含む
902
906
コンテキスト情報を
受信する
ユーザ識別情報に
少なくとも部分的に基づいて、
文字カウント値を決定する
904
文字カウント値を
クライアントに提供する
908
クライアントから
サブストリングを受信し、
サブストリングの長さは
文字カウント値に対応する
910
サブストリングを検証する
912
アクセス要求を
許可または拒否する
914

【図１０】


1000
サーバ上でuserID値および
フルセキュリティストリングを含む
ユーザアカウントを作成し、
フルセキュリティストリングは
第1の文字で始まる
1002
userID値およびサブストリングを
提供することによって
ユーザアカウントにアクセスする、
ここで、サブストリングは第1の文字で始まる
フルセキュリティストリングの中の
連続する文字のサブセットからなる
1004

フロントページの続き

(72)発明者　サティアジット・パトネ
アメリカ合衆国・カリフォルニア・９２１２１－１７１４・サン・ディエゴ・モアハウス・ドライヴ・５７７５

審査官　宮司　卓佳

(56)参考文献　特開２０１３－１３１１６４（ＪＰ，Ａ）
特開平９－２８２２８２（ＪＰ，Ａ）
特開２００２－９１９２１（ＪＰ，Ａ）
特開２０１０－２５０４７５（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／３１－２１／４６