(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第6574168号
(P6574168)

(45)発行日　令和1年9月11日(2019.9.11)　(24)登録日　令和1年8月23日(2019.8.23)

(51)Int.Cl.　F I
H04L 9/32 (2006.01)　H04L 9/00 675B
H04L 9/00 673B

請求項の数 14　(全 21 頁)

(21)出願番号　特願2016-516736(P2016-516736)
(86)(22)出願日　平成26年5月27日(2014.5.27)
(65)公表番号　特表2016-521932(P2016-521932A)
(43)公表日　平成28年7月25日(2016.7.25)
(86)国際出願番号　PCT/US2014/039590
(87)国際公開番号　WO2014/193841
(87)国際公開日　平成26年12月4日(2014.12.4)
審査請求日　平成29年5月17日(2017.5.17)
(31)優先権主張番号　201310200130.5
(32)優先日　平成25年5月27日(2013.5.27)
(33)優先権主張国・地域又は機関
中国(CN)

(73)特許権者　510330264
アリババ・グループ・ホールディング・リミテッド
ＡＬＩＢＡＢＡ　ＧＲＯＵＰ　ＨＯＬＤＩＮＧ　ＬＩＭＩＴＥＤ
英国領，ケイマン諸島，グランド・ケイマン，ジョージ・タウン，ワン・キャピタル・プレイス，フォース・フロア，ピー．オー．ボックス　８４７
(74)代理人　110001243
特許業務法人　谷・阿部特許事務所

最終頁に続く

(54)【発明の名称】端末識別方法、ならびにマシン識別コードを登録する方法、システム及び装置

(57)【特許請求の範囲】
【請求項１】
サービスネットワークによって、署名または証明書の検証が実行されるようにするための第１の要求を端末から受信することと、
前記サービスネットワークによって、前記第１の要求から、前記端末のマシン識別コード識別子のための信頼された機関の署名または証明書を取得することであって、前記マシン識別コード識別子は、前記信頼された機関によって前記端末のマシン識別コードに割り当てられた識別子であり、前記信頼された機関の前記署名または証明書は、ユーザのユーザ識別子と前記端末の前記マシン識別コード識別子とを、前記署名または証明書に関連付けられた情報として含む、取得することと、
前記サービスネットワークによって、前記取得された署名または証明書を検証し、前記取得された署名または証明書が正当であると検証される場合に、前記署名または証明書から取得される前記マシン識別コード識別子を使用することによって前記端末を識別することと、
前記端末の前記マシン識別コード識別子、および、対応するマシン識別コードまたはその派生コードをデータベースに記憶させることと、
前記サービスネットワークが、前記端末から、マシン識別コードの検証が実行されるようにするための第２の要求を受信することと、
前記サービスネットワークが、前記端末の前記マシン識別コードと署名または証明書とを前記第２の要求から取得し、前記署名または証明書が正当であることを検証した後で、

前記署名または証明書から取得される前記マシン識別コード識別子に基づいて、前記データベース内の前記対応するマシン識別コードまたは前記派生コードをクエリすることと、

前記第２の要求から取得される前記マシン識別コードまたは派生コードが、前記クエリすることによって前記データベース内で見つけられる前記マシン識別コードまたは前記派生コードと異なる場合、前記第２の要求を拒否すること、

を含む、端末識別方法。

【請求項２】

前記第１の要求は、匿名のユーザからの匿名ログイン要求及び／または実名のユーザからの実名ログイン要求を含む、

請求項１に記載の端末識別方法。

【請求項３】

前記サービスネットワークが、前記署名または証明書から取得された前記マシン識別コード識別子を使用することによって前記端末を識別した後、前記端末識別方法は、

前記サービスネットワークが前記端末にログインを許可して前記端末とのセッションを確立する場合、前記サービスネットワークが、前記セッションと前記マシン識別コード識別子との間の対応関係を記録することと、

前記サービスネットワークが、前記マシン識別コード識別子の前記端末から送信された要求として前記セッションを介して受信される後続の要求を識別することと、

を更に含む、

請求項２に記載の端末識別方法。

【請求項４】

前記第１の要求に前記署名または証明書が含まれない場合、

前記サービスネットワークが、前記端末に対し、それの前記マシン識別コードを報告するように通知し、前記端末によって報告された前記マシン識別コードを、登録のために前記信頼された機関に提示し、前記信頼できる機関によって発行された署名または証明書を記憶用に前記端末に送信すること、あるいは

前記サービスネットワークが、前記マシン識別コードの登録処理のためのインターフェースを前記端末に提供し、前記インターフェースを通じて、登録のための前記信頼された機関に、前記端末が、それの前記マシン識別コードを提示して、前記信頼された機関によって発行される前記署名または証明書を取得して記憶するように促すこと、

によって、前記サービスネットワークが、前記端末の前記マシン識別コードの登録処理を開始する、

請求項１に記載の端末識別方法。

【請求項５】

前記端末の前記マシン識別コードの前記登録処理は、

前記端末が、直接的なまたは前記サービスネットワークを介した登録のために、前記信頼された機関に、ユーザのユーザ情報およびそれの前記マシン識別コードを提示することを更に含み、前記信頼できる機関によって発行された前記署名または証明書は、前記署名と関連付けられた情報として前記ユーザのユーザ識別子および前記端末の前記マシン識別コード識別子を含む、

請求項４に記載の端末識別方法。

【請求項６】

前記サービスネットワークまたは前記信頼された機関が、前記信頼された機関によって発行される署名または証明書を記憶用に前記端末に送信することは、

前記端末によって前記サービスネットワークへと送信される前記第１の要求及び前記第２の要求の少なくとも１つに含まれるパラメータとして、記憶用に前記端末に前記署名または証明書を送信することを含む、

請求項４に記載の端末識別方法。

【請求項７】

前記第２の要求は、

前記端末を使用するユーザのユーザ情報を含む実名登録要求、
匿名ユーザからの匿名ログイン要求、
所定のセキュリティレベルより高いセキュリティレベルを要する要求、
無作為化アルゴリズムに基づく要求であって、マシン識別コードが検証の対象として設定される要求、及び
テストサイクルに従う要求であって、マシン識別コードが検証の対象として設定される要求
のうちの１つ以上を含む、
請求項１に記載の端末識別方法。
【請求項８】
１以上のプロセッサと、前記１以上のプロセッサにより実行可能な命令であって、実行されたときに前記１以上のプロセッサに以下の動作を実行させる命令を含むメモリとを備える端末識別システムであって、前記動作は、
端末から要求を受信することと、
署名または証明書の検証が実行されるようにするための第１の要求を前記端末から受信した後、前記端末のマシン識別コード識別子のための信頼された機関の署名または証明書を前記第１の要求から取得して検証することであって、前記マシン識別コード識別子は、前記信頼された機関によって、前記端末のマシン識別コードに割り当てられる識別子であり、前記信頼された機関の前記署名または証明書は、ユーザのユーザ識別子および前記端末の前記マシン識別コード識別子を、前記署名または証明書に関連付けられた情報として含む、ことと、
前記署名または証明書が正当であることを検証した後、前記署名または証明書から取得された前記マシン識別コード識別子を使用することによって前記端末を識別することと、
前記端末の前記マシン識別コード識別子と、対応するマシン識別コードまたはその派生コードをデータベースに記憶させることと、
前記端末から、マシン識別コードの検証が実行されるようにするための第２の要求を受信することと、
前記端末の前記マシン識別コードと署名または証明書とを前記第２の要求から取得し、前記署名または証明書が正当であることを検証した後で、前記署名または証明書から取得される前記マシン識別コード識別子に基づいて、前記データベース内の前記対応するマシン識別コードまたは前記派生コードをクエリすることと、
前記第２の要求から取得される前記マシン識別コードまたは派生コードが、前記クエリすることによって前記データベース内で見つけられる前記マシン識別コードまたは前記派生コードと異なる場合、前記第２の要求を拒否することと、
を含む、端末識別システム。
【請求項９】
前記第１の要求が、匿名のユーザからの匿名ログイン要求及び／または実名のユーザからの実名ログイン要求を含む、
請求項８に記載の前記端末識別システム。
【請求項１０】
前記署名または証明書から取得された前記マシン識別コード識別子を使用することによって前記端末を識別し、前記端末が、成功裏にログインし、サービスネットワークとのセッションを確立した後、前記動作は、前記セッションと前記マシン識別コード識別子との間の対応関係を記録し、前記セッションを介して受信される後続の要求を、前記マシン識別コード識別子を有する前記端末から送信された要求として識別することをさらに含む、
請求項９に記載の前記端末識別システム。
【請求項１１】
前記動作は、
前記第１の要求に前記署名または証明書が含まれないときに、前記端末の前記マシン識別コードの登録処理を初期化することを、

前記端末に、それの前記マシン識別コードを報告するように通知し、前記端末によって報告された前記マシン識別コードを、登録のために前記信頼された機関に提示し、前記信頼された機関によって発行された署名または証明書を記憶用に前記端末に送信すること、あるいは

前記マシン識別コードの登録処理のためのインターフェースを前記端末に提供し、前記インターフェースを通じて、登録のために前記信頼された機関に前記端末がそれの前記マシン識別コードを提示し、前記信頼できる機関によって発行された前記署名または証明書を記憶用に取得するように促すこと、

によって行うことを含む、請求項８に記載の前記端末識別システム。

【請求項１２】

前記信頼された機関によって発行された前記署名または証明書を記憶用に前記端末に送信することは、前記端末によってサービスネットワークへと送信される前記第１の要求および前記第２の要求の少なくとも１つに含まれるパラメータとして、前記署名または証明書を前記端末に記憶用に送信することを含む、請求項１１に記載の前記端末識別システム。

【請求項１３】

マシン識別コードの検証が実行されるようにするための第２の要求を前記端末から受信し、前記第２の要求から取得された署名および証明書を検証した後、前記動作は、

前記端末の前記マシン識別コード識別子と、対応するマシン識別コードまたはそれの派生コードとを記憶することと、

前記第２の要求における前記署名または証明書が正当であると確認されたときに、前記署名または証明書から取得された前記マシン識別コード識別子に従って、前記データベース内の前記対応するマシン識別コードまたは前記派生コードをクエリし、

前記第２の要求から取得された前記マシン識別コードまたは前記派生コードが、前記クエリすることによって前記データベース内で見つかった前記マシン識別コードまたは前記派生コードと同じであるかどうかを判定し、同じである場合には正当性を示す前記マシン識別コードの検証結果を、その他の場合には非正当性を示す前記マシン識別コードの検証結果を設定することと、

判定結果が相違を示すときに、前記第２の要求を拒否することと、

を更に含む、

請求項８に記載の前記端末識別システム。

【請求項１４】

前記第２の要求は、

前記端末を使用するユーザのユーザ情報を含む実名登録要求、

匿名ユーザからの匿名ログイン要求、

所定のセキュリティレベルより高いセキュリティレベルを必要とする要求、

無作為化アルゴリズムに基づく要求であって、マシン識別コードが検証の対象として設定される要求、及び

テストサイクルに従う要求であって、マシン識別コードが検証の対象として設定される要求

のうちの１以上を含む、請求項１３に記載の前記端末識別システム。

【発明の詳細な説明】

【技術分野】

【０００１】

関連出願の相互参照

この出願は、２０１３年５月２７日に出願され、「Ｔｅｒｍｉｎａｌ Ｉｄｅｎｔｉｆｉｃａｔｉｏｎ Ｍｅｔｈｏｄ，ａｎｄ Ｍｅｔｈｏｄ，Ｓｙｓｔｅｍ ａｎｄ Ａｐｐａｒａｔｕｓ ｏｆ Ｒｅｇｉｓｔｅｒｉｎｇ Ｍａｃｈｉｎｅ Ｉｄｅｎｔｉｆｉｃａｔｉｏｎ Ｃｏｄｅ」と題された中国特許出願第２０１３１０２００１３０．５号に対する外国優先権を主張するものであり、それは、それの全体が参照によって本明細書に組み

込まれる。

【０００２】

本開示は、端末識別技術に関するものであり、特に、マシン識別コードに基づいて端末を識別する方法及び関連したネットワークに関するものである。

【背景技術】

【０００３】

社会の継続的な開発と共に、インターネットが、急速に開発されており、我々の日々の生活の不可欠な部分になってきている。何千もの人間が、日々、オンライン購入をしたり、ニュースを閲覧したりしている。既存のコンピュータネットワークにおいて、ユーザは、ウェブサイト上で多くの異なるＩＤを登録し得、異なるタスクを実行するために異なるサービスネットワークにログインし得る。どの端末がログインのためにこれらのＩＤによって使用されるかを決定することは、事業管理、ユーザ管理、リスク管理、及び商業用知的分析を効率的に実行するために非常に重要である。

【０００４】

したがって、多数の端末識別技術が、既存の技術において現れている。既存の識別技術は、基本的には、ユーザがサービスネットワーク（例えばウェブサイトまたはプラットフォームなど）にアクセスするときに、ユーザによって使用された端末と関連付けられたデータを収集して、ネットワークにおけるサーバまたはコンピュータを使用して、このデータに基づいて、端末であって、その端末からそのデータが発生する、端末を決定する。それの最も広く採用されたものは、識別を達成するためにＭＡＣアドレスを取得するブラウザと関連付けられた制御構成要素を使用することである。しかしながら、ＭＡＣアドレスは、登録リストから取得されて、人間による改ざんや偽造を受け易い。したがって、そのように取得されたＭＡＣアドレスの不正確さまたは虚偽性の問題が存在する。

【０００５】

公開番号ＣＮ１０３０２４０９０Ａ号を有する中国特許公報は、端末識別のための異なる方法及びシステムを開示する。この方法は、ブラウザと関連付けられたソフトウェア情報または端末のハードウェアＩＯ層から取得されたハードウェア情報を端末のマシン識別コードとして使用して、このマシン識別コードに基づいて端末を識別する。識別の間に、端末は、サービスネットワークに送信するためにそれのマシン識別コードをフェッチする。サービスネットワークは、データベースに記憶される異なる端末と関連付けられたデータ情報にマシン識別コードをマッチングさせて、最も良くマッチングした端末を識別された端末と見なす。

【０００６】

このマシン識別コードをベースとする端末識別方法は、ハードウェアＩＯ層からハードウェア情報を取得して、それは、ＭＡＣアドレスと比べると、より正確であり、かつ妨害されたり改ざんされたりすることがより困難である。しかしながら、端末は、各要求の間にマシン識別コードをフェッチする必要があるので、サービスネットワークは、識別の間にデータベース内の端末のデータ情報とのマシン識別コードのマッチングの度合いを計算する必要があり、この方法は、大量の通信及び計算リソースを消費して、それ故、ユーザ経験を悪化させる。その上、フェッチされたマシン識別コードは、伝送や記憶の処理の間に逆コンパイル、妨害及び違反を受け易く、それ故、ユーザマシンの識別コードのプライバシ保護に好ましくない。

【発明の概要】

【０００７】

この発明の概要は、発明を実施するための形態において以下に更に説明される簡略化された形態で概念の選択を導入するために提供される。この発明の概要は、特許請求された主題の全ての重要な特徴または本質的な特徴を特定することを意図されるものではないし、特許請求された主題の範囲を決定する際の助けとして単独で使用されることを意図されるものでもない。用語「技法」は、上記文脈によって及び本開示全体を通して許容されるような、例えば、（複数の）デバイス、（複数の）システム、（複数の）方法及び／また

はコンピュータで読み取り可能な命令のことを指し得る。

【０００８】

本開示によって解決されることになる技術的問題は、より少数のリソースを占有する、かつ、より良いプライバシ保護を容易にする端末識別方法、関連したサービスネットワーク、及び端末を提供することである。

【０００９】

この問題を解決するために、本開示は、端末識別方法であって、

サービスネットワークが、端末から、第１の要求であって、その第１の要求のために署名または証明書検証が実行されることになる、第１の要求を受信することと、

サービスネットワークが、第１の要求から端末のマシン識別コード識別子のために信頼できる機関の署名または証明書を取得することであって、マシン識別コード識別子が、信頼できる機関によって端末のマシン識別コードに割り当てられた識別子である、取得することと、

サービスネットワークが、取得された署名または証明書を検証して、検証結果が正当性を示す場合、署名または証明書から取得されたマシン識別コード識別子を使用して端末を識別することと、を含む、端末識別方法を提供する。

【００１０】

一実施形態において、第１の要求が、匿名ログイン要求及び／または実名ログイン要求を含む。

【００１１】

いくつかの実施形態において、サービスネットワークが、署名または証明書から取得されたマシン識別コード識別子を使用して端末を識別した後、本方法は、

サービスネットワークが、端末がログインすることを可能にして、端末とのセッションを確立する場合、サービスネットワークが、セッションとマシン識別コード識別子との相関関係を記録することと、

サービスネットワークが、マシン識別コード識別子の端末から送信された要求としてセッション経由で受信される後続の要求を識別することと、を更に含む。

【００１２】

一実施形態において、サービスネットワークが、第１の要求から署名または証明書を取得しない場合、サービスネットワークが、以下のアプローチに従って、端末マシン識別コードのための登録処理を開始する。

【００１３】

サービスネットワークが、端末にそれのマシン識別コードを報告することを通知して、端末によって報告されたマシン識別コードを登録のために信頼できる機関に提示して、信頼できる機関によって発行された署名または証明書を記憶のために端末に送信する。

【００１４】

あるいは、サービスネットワークが、ネットワークによって提供されるマシン識別コード登録のインターフェースを通して登録のために信頼できる機関にそれのマシン識別コードを提示するように端末を促して、信頼できる機関によって発行された署名または証明書を取得して記憶する。

【００１５】

いくつかの実施形態において、端末マシン識別コードの登録処理は、

端末が、直接的にまたはサービスネットワーク経由で登録のために信頼できる機関にユーザのユーザ情報及びそれのマシン識別コードを提示することを更に含み、信頼できる機関によって発行された署名または証明書が、署名と関連付けられた情報としてユーザのユーザ識別子及び端末のマシン識別コード識別子を含む。

【００１６】

一実施形態において、サービスネットワークまたは信頼できる機関が、記憶のために署名または証明書を端末に送信することは、

端末によってサービスネットワークに送信された要求に含まれることになるパラメータ

として、記憶のために署名または証明書を端末に送信することを含む。
【００１７】
更に、端末識別方法が、
端末のマシン識別コード識別子及び対応するマシン識別コードまたはそれの派生コードをデータベース内に記憶することと、
サービスネットワークが、端末から、第２の要求であって、その第２の要求のためにマシン識別コードの検証が実行されることになる、第２の要求を受信することと、
サービスネットワークが、第２の要求から端末のマシン識別コード及び署名または証明書を取得して、署名または証明書が正当であることを検証した後、署名または証明書から取得されたマシン識別コード識別子に基づいて、データベース内の対応するマシン識別コードまたは派生コードを照会することと、
第２の要求から取得されたマシン識別コードまたは派生コードが、照会において見付けられるマシン識別コードまたは派生コードとは異なる場合、要求を断ることと、を更に含む。
【００１８】
一実施形態において、端末から送信された各要求が、第２の要求であり、または第２の要求が、以下の要求、すなわち、
実名ログイン要求、
匿名ログイン要求、
所定のセキュリティレベルより高いセキュリティレベルを有する要求、
マシン識別コードが、無作為化アルゴリズムに基づく検証のために設定されるという要求、及び
マシン識別コードが、テストサイクルに従う検証のために設定されるという要求のうちの１以上を含む。
【００１９】
それに応じて、本開示は、サービスネットワークの端末識別システムであって、
端末から要求を受信するために使用される受信モジュールと、
受信モジュールが、第１の要求であって、その第１の要求のために署名または証明書検証が実行されることになる、第１の要求を端末から受信した後、第１の要求から端末のマシン識別コード識別子のために信頼できる機関の署名または証明書を取得して検証するために使用される第１の検証モジュールであって、マシン識別コード識別子が、信頼できる機関によって端末のマシン識別コードに割り当てられた識別子である、第１の検証モジュールと、
第１の検証モジュールの検証結果が正当性を示すときに、署名または証明書から取得されたマシン識別コード識別子を使用して端末を識別するために使用される識別モジュールと、を含む、端末識別システムを更に提供する。
【００２０】
一実施形態において、受信モジュールによって受信される第１の要求が、匿名登録要求及び／または実名登録要求を含む。
【００２１】
いくつかの実施形態において、識別モジュールが、署名または証明書から取得されたマシン識別コード識別子を使用して端末を識別した後に、端末が、成功裏にログインしてサービスネットワークとのセッションを確立する場合、セッションとマシン識別コード識別子との相関関係が記録されて、セッション経由で受信される後続の要求が、マシン識別コード識別子を有する端末から送信された要求として識別される。
【００２２】
一実施形態において、システムは、第１の検証モジュールが、以下のアプローチに従って、第１の要求から署名または証明書を取得しないときに、端末マシン識別コードの登録処理を初期化するために使用される登録初期化モジュールを更に含む。すなわち、
端末にそれのマシン識別コードを報告することを通知して、端末によって報告されたマ

シン識別コードを登録のために信頼できる機関に提示して、信頼できる機関によって発行された署名または証明書を記憶のために端末に送信すること、あるいは
端末に、ネットワークによって提供されるマシン識別コード登録のインターフェースを通して登録のために信頼できる機関にそれのマシン識別コードを提示して、記憶のために信頼できる機関によって発行された署名または証明書を取得することを促すこと。

【００２３】

いくつかの実施形態において、登録開始モジュールが、信頼できる機関によって発行された署名または証明書を記憶のために端末に送信することが、サービスネットワークに端末によって送信された要求に含まれることになるパラメータとして、署名または証明書を記憶のために端末に送信することを含む。

【００２４】

一実施形態において、第１の検証モジュールは、受信モジュールが、第２の要求であって、その第２の要求のためにマシン識別コード検証が実行されることになる、第２の要求を端末から受信した後に、それの署名または証明書を検証するために更に使用される。

【００２５】

端末識別システムが、
端末のマシン識別コード識別子及び対応するマシン識別コードまたはそれの派生コードを記憶するために使用されるデータベースと、
第１の検証モジュールが、第２の要求における署名または証明書が正当であることを確認するときに、署名または証明書から取得されたマシン識別コード識別子に従って、データベース内の対応するマシン識別コードまたは派生コードを照会して、第２の要求から取得されたマシン識別コードまたは派生コードが、照会において見付けられたマシン識別コードまたは派生コードと同じであるかどうかを決定して、同じである場合には正当性あるいはその他の場合には非正当性を示すマシン識別コードの検証結果を設定するために使用される第２の検証モジュールと、
第２の検証モジュールの決定結果が相違を示すときに、要求を拒否するために使用されるアクセス制御モジュールと、を更に含む。

【００２６】

一実施形態において、端末によって送信された各要求が第２の要求であり、または第２の要求が、以下の要求、すなわち、
実名ログイン要求、
匿名ログイン要求、
所定のセキュリティレベルより高いセキュリティレベルを有する要求、
マシン識別コードが、無作為化アルゴリズムに基づく検証のために設定されるという要求、及び
マシン識別コードが、テストサイクルに従う検証のために設定されるという要求のうちの１以上を含む。

【００２７】

前述のスキームにおいて、サービスネットワークは、マッチングを実行する必要なく、端末によって報告される署名または証明書におけるマシン識別コード識別子に基づいて、端末を識別する。その上、端末は、マシン識別コードを毎回フェッチして伝送する必要がなく、それ故、マシン識別コードの偽造を回避して、通信及び計算上のリソースを節約する。加えて、（サービスネットワークだけが知る）マシン識別コード識別子は、マシン識別コードの代わりに、端末が記憶して伝送するものであるので、ユーザマシン識別コードのためのプライバシ保護が強化される。

【００２８】

本開示によって解決されることになる別の技術的問題は、端末のマシン識別コードの登録方法及び対応する信頼できる機関を提供することである。

【００２９】

この問題を解決するために、本開示は、信頼できる機関における適用のための、端末の

マシン識別コードの登録方法であって、
端末のマシン識別コードを含む登録要求を受信することと、
マシン識別コードを検証して、正当であることが検証される場合、マシン識別コード識別子をマシン識別コードに割り当てることと、
マシン識別コード識別子を含む情報のための署名を行って、署名またはその署名を含む証明書を登録要求の要求元に送信することと、を含む方法を提供する。
【００３０】
一実施形態において、登録要求が、端末を使用するユーザのユーザ情報を更に含む。
【００３１】
方法は、
ユーザ情報を検証して、正当であることが検証される場合、ユーザ識別子及びマシン識別コード識別子のための署名を共に行うことを更に含み、ユーザ識別子が、ユーザ情報から取得されるか、あるいはユーザ情報に従って割り当てられる。
【００３２】
それに応じて、本開示は、
端末のマシン識別コードを含む登録要求を受信するように構成された受信モジュールと、
マシン識別コードを検証するように構成された検証モジュールと、
検証モジュールの検証結果が正当性を示すときに、マシン識別コード識別子をマシン識別コードに割り当てるように構成された割り当てモジュールと、
マシン識別コード識別子を含有する情報のための署名を行って、登録要求の要求元に署名またはその署名を含有する証明書を送信するように構成された発行モジュールと、を含む、信頼できる機関を更に提供する。
【００３３】
一実施形態において、受信モジュールによって受信される登録要求が、端末を使用するユーザのユーザ情報を更に含む。
【００３４】
検証モジュールが、ユーザ情報とマシン識別コードを同時に検証する。
【００３５】
発行モジュールが、ユーザ識別子及びマシン識別コード識別子のための署名を行って、ユーザ識別子が、ユーザ情報から取得されるか、あるいはユーザ情報に従って割り当てられる。
【００３６】
前述のスキームは、端末のマシン識別コード識別子の割り当て及び対応する署名または証明書の発行を実現して、それは、端末のマシン識別コード識別子が本物であることを証明するために適用され得る。端末のマシン識別コードの検証は、非正当な端末の登録を拒否し得、端末の信頼性を向上し得る。
【図面の簡単な説明】
【００３７】
【図１】本開示の第１の実施形態に従う端末識別の方法のフローチャートである。
【図２】本開示の第１の実施形態に従う端末識別のシステムの機能図である。
【図３】本開示の第１の実施形態に従う端末のマシン識別コードの登録方法のフローチャートである。
【図４】本開示の第１の実施形態に従う信頼できる機関の機能図である。
【図５】本開示の第２の実施形態に従うマシン識別コードの検証方法のフローチャートである。
【図６】図２において説明されるようなシステムの実施例の構造図である。
【図７】図４において説明されるような信頼できる機関の実施例の構造図である。
【発明を実施するための形態】
【００３８】

目的をより良く理解するために、本開示の技術的スキーム、利益及び実施形態が、添付の図面を参照にして詳細に説明されることになる。本開示の実施形態及び実施形態における特徴は、矛盾が存在しないときに、互いにかつ自由裁量によって組み合わされ得ることに留意するべきである。

【００３９】

本開示の典型的な構成において、端末、サービスネットワークと関連付けられた装置、及び信頼できる機関は、中央処理装置（ＣＰＵ）、入出力インターフェース、ネットワークインターフェース、及び内部記憶装置のうちの１以上を含み得る。

【００４０】

内部記憶装置は、コンピュータで読み取り可能な媒体、例えば、非永続的な記憶デバイス、ランダムアクセスメモリ（ＲＡＭ）、及び／または不揮発性内部記憶装置、例えば、読み取り専用メモリ（ＲＯＭ）もしくはフラッシュＲＡＭなどの形態を含み得る。内部記憶装置は、コンピュータで読み取り可能な媒体の実施例である。

【００４１】

コンピュータで読み取り可能な媒体は、永続的または非永続的な種類の、取り外し可能あるいは取り外し不可能な媒体を含み得、それは、任意の方法または技術を使用して情報の記憶を達成し得る。情報は、コンピュータで読み取り可能なコマンド、データ構造、プログラムモジュール、または他のデータを含み得る。コンピュータ記憶媒体の実施例は、限定されるものではないが、相変化メモリ（ＰＲＡＭ）、静的ランダムアクセスメモリ（ＳＲＡＭ）、動的ランダムアクセスメモリ（ＤＲＡＭ）、他の種類のランダムアクセスメモリ（ＲＡＭ）、読み取り専用メモリ（ＲＯＭ）、電子的に消去可能でプログラム可能な読み取り専用メモリ（ＥＥＰＲＯＭ）、高速フラッシュメモリまたは他の内部記憶技術、コンパクトディスク読み取り専用メモリ（ＣＤ－ＲＯＭ）、デジタル多用途ディスク（ＤＶＤ）または他の光記憶装置、磁気カセットテープ、磁気ディスク記憶装置または他の磁気記憶デバイス、あるいは任意の他の非伝送媒体を含み、それらは、コンピューティングデバイスによってアクセスされ得る情報を記憶するために使用され得る。本明細書において定義される際、コンピュータで読み取り可能な媒体は、一時的な媒体、例えば変調データ信号及び搬送波などを含まない。

【００４２】

第１の実施形態

この実施形態のシステムは、端末、サービスネットワーク及び信頼できる機関を含む。端末は、ユーザデバイス、例えば、ＰＣ、スマートホン、ＰＤＡ等であり得る。サービスネットワークは、ネットワークサービスを端末に提供するために使用されて、例えば、ウェブサイトシステムまたはネットワークプラットフォームのうちの１以上を含み得る。サービスネットワークは、要求を送信した端末を識別し得る。信頼できる機関が、マシン識別コード識別子を端末のマシン識別コードに割り当てて、署名または証明書を発行するために使用される。信頼できる機関が、サービスネットワークにおけるノード、またはサービスネットワークの外側のノードであり得ることに留意するべきである。

【００４３】

図１に示されるように、本実施形態における端末識別の方法が、以下を含む。

【００４４】

ブロック１１０で、サービスネットワークが、署名または証明書検証が実行されることになるという第１の要求を端末から受信する。

【００４５】

署名または証明書検証が実行されることになるという第１の要求が、サービスネットワークによって定義されて、例えば、匿名ログイン要求及び／または実名ログイン要求を含み得、ならびに、この開示において限定されない他の要求もまた含み得る。第１の要求が匿名ログイン要求を含むとき、サービスネットワークは、ユーザが匿名でログインするときに端末を識別して、それ故、匿名のログインの状況下で端末と関連付けられた活動についての統計を計算する。

【００４６】
ブロック１２０で、サービスネットワークは、第１の要求から端末のマシン識別コード識別子のために信頼できる機関の署名または証明書を取得する。マシン識別コード識別子が、信頼できる機関によって端末のマシン識別コードに割り当てられた識別子である。
【００４７】
この実施形態におけるマシン識別コードが、端末を一意的に識別できるハードウェア及び／またはソフトウェア情報を含む。ハードウェア情報は、例えば、端末のハードウェアＩＯ層から取得されるハードウェア情報を含み得、ソフトウェア情報は、例えば、端末のブラウザのソフトウェア情報等を含み得る。
【００４８】
端末のマシン識別コード識別子のための署名は、例えばマシン識別コード識別子などの情報のために信頼できる機関の秘密鍵によって生成された署名に対応しており、sig_{CA}（ＵＭＩＣ＿ｉｄ）として表わされ得、ここで、「ＣＡ」は、信頼できる機関を表わし、ＵＭＩＣ＿ｉｄは、端末のマシン識別コード識別子を表わす。署名と関連付けられた情報は、限定されるものではないが、マシン識別コードを含み、他の情報、例えばユーザ識別子等を更に含み得る。ユーザ識別を含む署名は、sig_{CA}（ＵＭＩＣ＿ｉｄ||Ｕｓｅｒ＿ｉｄ）として表わされ得、ここで、「Ｕｓｅｒ＿ｉｄ」は、ユーザ識別子を表わす。
【００４９】
証明書は、署名を含む証明書である。署名の情報がＵＭＩＣ＿ｉｄ及びＵｓｅｒ＿ｉｄを含むとき、証明書は、
【００５０】
【表１】

証明書バージョン番号
証明書連続番号
ＵＭＩＣ＿ｉｄ
Ｕｓｅｒ＿ｉｄ
sig_{CA}（ＵＭＩＣ＿ｉｄ‖Ｕｓｅｒ＿ｉｄ）
タイムスタンプ

表１

【００５１】
として表わされ得る。
【００５２】
注釈：上記表は、証明書に含まれる情報の一部だけを示す。証明書は、Ｘ．５０９標準に従い得るが、それに限定されるものではない。
【００５３】
ブロック１３０で、決定が、署名または証明書が取得されるかどうかについてなされる。取得された場合、ブロック１５０が実行される。その他の場合には、ブロック１４０が実行される。
【００５４】
ブロック１４０で、端末のマシン識別コードの登録処理が開始される。処理が終了する。
【００５５】
この実施形態において、サービスネットワークが第１の要求から署名または証明書を取得しない場合、端末マシン識別コードの登録処理が、以下のアプローチに従って開始される。すなわち、サービスネットワークが、端末にそれのマシン識別コードを報告することを通知して、端末によって報告されたマシン識別コードを登録のために信頼できる機関に提示して、信頼できる機関によって発行された署名または証明書を記憶のために端末に送信する。他の実施形態において、サービスネットワークが、端末に、ネットワークによっ

て提供されるマシン識別コード登録のインターフェースを通して登録のために信頼できる機関にそれ自体のマシン識別コードを提示するように、ならびに信頼できる機関によって発行された署名または証明書を取得して記憶するように、促し得る。

【００５６】

一実施形態において、登録処理では、サービスネットワークまたは信頼できる機関が、端末からサービスネットワークに送信された要求に含まれることになるパラメータとして、記憶のために署名または証明書を端末に送信し得、例えば、クッキー（Ｃｏｏｋｉｅ）におけるパラメータとして、端末に送信する。

【００５７】

本開示は、端末のマシン識別コードの登録をどのように開始するかについて限定がないことに留意するべきである。上記２つのアプローチ以外で、端末は、要求が署名または証明書を含まないときにサービスネットワークが登録を開始する必要なく、そのような署名または証明書が取得されていないときに信頼できる機関に自発的に登録し得る。

【００５８】

ブロック１５０で、検証が、署名または証明書のために実行される。検証結果が正当性を示す場合、ブロック１７０が実行される。その他の場合には、ブロック１６０が実行される。

【００５９】

このブロックにおいて、サービスネットワークは、信頼できる機関の公開鍵を使用して署名を復号して、署名の検証を達成する。証明書の検証は、既存の証明書検証方法、例えば、証明書の有効期間についての検証を追加すること、あるいは証明書が証明書データベースに存在するかどうかを利用し得る。

【００６０】

署名または証明書の検証が、マシン識別コード識別子が信頼できる機関によって実際に割り当てられたマシン識別コード識別子であることを確保して、非正当なユーザが、マシン識別コードを偽造または改ざんすることを効果的に防ぐ。

【００６１】

ブロック１６０で、第１の要求が拒否される。処理が終了する。

【００６２】

署名または証明書の検証結果が、非正当性を示す場合には、端末が、信頼できる機関から正当の署名または証明書を取得していないことを示しており、第１の要求は、この時に拒否され得る。第１の要求を拒否するとき、ブロック１４０で端末のマシン識別コードの登録処理が、設計ニーズに基づいて開始され得る。

【００６３】

ブロック１７０で、端末が、署名または証明書から取得されたマシン識別コード識別子を使用して識別される。

【００６４】

端末を識別するためにマシン識別コード識別子を使用することは、同じマシン識別コード識別子を有する端末が、同じ端末として識別されることを暗示する。したがって、同じ端末によって送信された要求と関連付けられた時間及び回数の統計が、正しく計算され得、それは、端末がネットワークサービスにアクセスすることを許可されるかどうかを決めるために使用され得る。

【００６５】

第１の要求以外の要求の場合、サービスネットワークは、端末識別を実行してもよいし、または実行しなくてもよい。一実施形態例において、１つのセッションにおいて端末が変えられることは困難であるので、セッションとマシン識別コード識別子との相関関係は、サービスネットワークが、端末がブロック１７０の後にログインすることを可能にして端末とのセッションを確立する場合に、記録され得る。セッション経由で受信される後続の要求が、マシン識別コード識別子を有する端末によって送信された要求として識別されて、それ故、計算上のリソースを節約する。あるいは、別の実施形態において、端末から

送信された各要求が、第１の要求として取り扱われ得、より信頼できる識別を達成するために、その第１の要求から署名または証明書が検証のために取得される。

【００６６】

サービスネットワークは、上記端末識別方法を実装するために、図２に示されるような端末識別システムを利用し得る。識別システムは、以下を含む。

【００６７】

受信モジュール１１は、端末から要求を受信するために使用される。

【００６８】

第１の検証モジュール１２は、受信モジュールが、第１の要求であって、その第１の要求のために署名または証明書検証が実行されることになる、第１の要求を端末から受信した後、第１の要求から端末のマシン識別コード識別子のために信頼できる機関から署名または証明書を取得して検証するために使用される。ここで、マシン識別コード識別子は、端末のマシン識別コードに信頼できる機関によって割り当てられた識別子である。一実施形態において、受信モジュールによって受信される第１の要求が、匿名ログイン要求及び／または実名ログイン要求を含む。

【００６９】

識別モジュール１３は、第１の検証モジュールの検証結果が正当性を示すときに、署名または証明書から取得されたマシン識別コード識別子を使用して端末を識別するために使用される。端末が、成功裏にログインしてサービスネットワークとのセッションを確立した後、識別モジュールは、セッションとマシン識別コード識別子との相関関係を記録し得、マシン識別コード識別子を有する端末から送信された要求として、セッション経由で受信される後続の要求を取り扱い得る。

【００７０】

（任意選択的である）登録開始モジュール１４は、以下のアプローチ、すなわち、端末にそれのマシン識別コードを報告するために通知して、端末によって報告されたマシン識別コードを登録のために信頼できる機関に提示して、信頼できる機関によって発行された署名または証明書を記憶のために端末に送信することであって、署名または証明書が、一実施形態において、端末からサービスネットワークに送信された要求に含まれることになるパラメータとして、記憶のために端末に送信される、当該アプローチを使用して、第１の検証モジュールが第１の要求から署名または証明書を取得しないときに、端末マシン識別コードの登録処理を開始すること、あるいはネットワークによって提供されるマシン識別コード登録のインターフェースを通して登録のために信頼できる機関にそれのマシン識別コードを提示するように、ならびに信頼できる機関によって発行された署名または証明書を取得して記憶するように、端末を促すことのために使用される。

【００７１】

実装の間に、上記モジュールが、異なる実体に分散されてもよいし、または同じ実体内に分散されてもよい。

【００７２】

それに応じて、図３に示されるように、信頼できる機関によって端末のマシン識別コードを登録する方法は、以下を含む。

【００７３】

ブロック２１０は、端末のマシン識別コードを含む登録要求を受信する。

【００７４】

ブロック２２０は、マシン識別コードを検証して、正当であることが検証される場合、マシン識別コード識別子をマシン識別コードに割り当てる。

【００７５】

ここで、マシン識別コードの検証は、例えば、汎用装置の正当性を検査すること、例えば、ハードディスクが現実の製造業者の装置であるかどうかを、連続番号等を通してチェックすることなどであり得る。この場所における検証は、端末識別のために任意選択的であることに留意するべきである。しかしながら、追加的な検証が、非正当な端末の登録を

拒否し得、それ故、端末の信頼性を上げる。

【００７６】

ブロック２３０は、マシン識別コード識別子を含有する情報のための署名を行って、署名またはその署名を含有する証明書を登録要求元に送信する。

【００７７】

図４に示されるように、信頼できる機関が、

端末のマシン識別コードを含む登録要求を受信するように構成された受信モジュール２１、

マシン識別コードを検証するように構成された検証モジュール２２、

検証モジュールの検証結果が正当性を示すときに、マシン識別コード識別子をマシン識別コードに割り当てるように構成された割り当てモジュール２３、ならびに

マシン識別コード識別子を含有する情報にサインするように、及び署名またはその署名を含有する証明書を登録要求元に送信するように構成された発行モジュール２４を含む。

【００７８】

受信された登録要求が、端末を使用するユーザのユーザ情報を更に含むとき、検証モジュールが、ユーザ情報とマシン識別コードの両方のために検証を実行する。発行モジュールは、ユーザ識別子とマシン識別コード識別子の両方のために署名を行う。ここで、ユーザ識別子が、ユーザ情報から取得されるか、またはユーザ情報に従って割り当てられる。

【００７９】

同様に、上記検証モジュールは、任意選択的である。検証モジュールが含まれない時の状況下で、割り当てモジュールは、登録要求に含まれるマシン識別コードにマシン識別コード識別子を直接的に割り当て得る。その上、信頼できる機関に含まれる上記モジュールが、１つの実体に位置してもよく、あるいは様々な実体に分散されてもよいことに留意するべきである。信頼できる機関は、これらの機能を実装するモジュールで構成された論理実体である。

【００８０】

上記実施形態において、マシン識別コードは、ユーザ識別子に縛られず、また、マシン識別コードを取り替える攻撃を受け易い。例えば、第２の端末が、ユーザ間で第１の端末及び第３の端末を用いてセキュリティチャネルを別個に確立した後、第２の端末は、第１の端末から受信されたマシン識別コードをそれ自体のマシン識別コードとして第３の端末に送信して、第３の端末は、第２の端末から送信されたこのマシン識別コードが、第２の端末のマシンコードではないことを識別することができない。したがって、上記実施形態に基づいて、端末は、一実施形態において、端末マシン識別コードの登録処理の間に登録のために信頼できる機関に直接的にまたはサービスネットワークを通してユーザのユーザ情報及びそれ自体のマシン識別コードを提示し得る。ここで、ユーザ情報は、ユーザによって入力され得、あるいはローカルに記憶され得る。登録要求がユーザ情報を含むとき、信頼できる機関は、登録の間にユーザ情報を検証し得る。検証が正当性を示す場合、ユーザ識別子及びマシン識別コード識別子が、署名を行うためにサインされることになる情報として見なされる。ユーザ識別子は、ユーザ情報から取得され得、あるいはユーザ情報に従って割り当てられ得る。そのように、ユーザ識別子及びマシン識別コード識別子は、署名または証明書において共に縛られて、それ故、マシン識別コードを取り替える上記攻撃を効果的に回避する。

【００８１】

第２の実施形態

第１の実施形態におけるサービスネットワークが、端末の識別子としてマシン識別コード識別子を取り扱い、端末の識別を実現する。しかしながら、非正当なユーザは、多数のジャンク署名または証明書を記憶する既存のジャンクアカウントに類似して、信頼できる機関によって発行された多数の署名または証明書を同じマシン内に記憶し得、相違点は、既存のジャンクアカウントの登録と比べて高い費用である。要求は、悪意のあるプログラムを通してサービスネットワークに送信されて、異なる署名または証明書が、異なる要求

において使用される。この場合において、サービスネットワークは、端末の効果的な識別を実現することができない。したがって、本実施形態が、第１の実施形態の先頭上にマシン識別コードの検証処理を追加する。

【００８２】

この実施形態において、マシン識別コード識別子及び対応するマシン識別コードまたはそれの派生コードが、データベース内に記憶されることを必要とされる。具体的には、信頼できる機関は、割り当てられた端末のマシン識別コード及びマシン識別コード識別子をそれによってそれに応じてデータベース内に記憶し得、維持し得る。あるいは、信頼できる機関は、端末のマシン識別コード及びマシン識別コード識別子をデータベース内への記憶とサービスネットワークによる保守のためにサービスネットワークに送信し得る。端末のマシン識別コードのプライバシをより良い手法で保護するために、マシン識別コードの派生コードは、マシン識別コードの代用になり得、代わりにデータベース内に記憶され得る。マシン識別コードの派生コードは、マシン識別コードのために実行された計算に基づいて取得されたコードのことを指す。例えば、マシン識別コードが、Ｎビットハードウェア情報及び／またはＭビットブラウザソフトウェア情報を含むとき、Ｎビットハードウェア情報及び／またはＭビットブラウザソフトウェア情報のハッシュ値が、そのマシン識別コードの派生コードとして見なされ得る。

【００８３】

図５に示されるように、この実施形態においてマシン識別コードを検証する処理は、以下を含む。

【００８４】

ブロック３１０は、サービスネットワークによって端末から送信された要求を受信する。

【００８５】

ブロック３２０は、受信された要求が、マシン識別コード検証を必要とする第２の要求であるかどうかを決定する。そうではない場合、ブロック３３０が実行される。その他の場合には、ブロック３４０が実行される。

【００８６】

この実施形態において、マシン識別コード検証を必要とする第２の要求が、サービスネットワーク及び端末によって前もって合意されて、あるいは他の実施形態において、サービスネットワークまたは端末によって設定され得る。第２の要求が端末によって設定されるとき、サービスネットワークは、要求が、端末のマシン識別コード及び署名／証明書を含むかどうかを検査することによって、要求が第２の要求であるかどうかを決定し得る。第２の要求がサービスネットワークによって設定されるとき、サービスネットワークは、マシン識別コード及び署名／証明書を報告することを端末に通知し得る。本開示は、どのような要求が第２の要求として見なされるかに関して限定がない。

【００８７】

例えば、高いセキュリティ要件を有するサービスネットワークのために、端末から送信された全要求が、端末の信頼性を確保する及びネットワークサービスのセキュリティレベルを向上するための第２の要求として設定され得る。

【００８８】

別の実施例として、以下の１以上の種類の要求が、第２の要求として見なされ得る。

【００８９】

実名登録要求、

匿名登録要求、

所定のセキュリティレベルより高いセキュリティレベルを有する要求、例えば、アカウント間の支払いや振替を含む要求など、

マシン識別コードが、無作為化アルゴリズム、例えば、端末が、特定の要求を第２の要求として無作為に決定し得ることに基づく検証のために設定されるという要求、

マシン識別コードが、テストサイクル、例えば、１つのテストを完了した後、端末が、

所定の時間区分内、すなわち、テストサイクル内に、テストを再び実行しないことに従う検証のために設定されるという要求、ならびにこのテストサイクルが第２の要求として決定された後に送信された要求。

【００９０】

一実施形態において、データセキュリティのための要件が低いというシナリオにおいて、この実施形態におけるマシン識別コードの検証が、飛ばされ得る。

【００９１】

ブロック３３０は、他の要求のための処理方法に従う処理を実行する。処理が終了する。

【００９２】

要求が第１の要求である場合、署名または証明書の検証が、端末を識別するためにこの時に実行され得る。他の要求の場合、端末の識別は、実行される必要がなくてもよく、または端末は、マシン識別コード識別子とセッションとの記録された相関関係に基づいて識別され得る。

【００９３】

ブロック３４０は、第２の要求から端末のマシン識別コード及び署名または証明書を取得して、署名または証明書が、正当であることが検証される場合、署名または証明書から取得されるマシン識別コード識別子に基づいて、データベースから対応するマシン識別コードあるいはそれの派生コードを照会する。

【００９４】

ブロック３５０は、取得されるマシン識別コードまたは派生コードが、見付けられるマシン識別コードまたは派生コードと同じであるかどうかを決定する。そうではない場合、ブロック３６０が実行される。その他の場合には、ブロック３７０が実行される。

【００９５】

データベースがマシン識別コードを記憶する場合、サービスネットワークは、データベース内の対応するマシン識別コードと取得されたマシン識別コードを比較する必要だけがある。データベースがマシン識別コードの派生コードを記憶する場合、サービスネットワークは、最初に同じアルゴリズムに従って取得されたマシン識別コードから派生コードを計算して取得する必要があり、データベース内の対応する派生コードとその派生コードを比較する。

【００９６】

ブロック３６０は、この要求を拒否する。処理が終了する。

【００９７】

要求を拒否した後、他の処理は実行され得ず、またはユーザは、マシン識別コードの登録を再び実行することを促され得る。あるいは、マシン識別コード識別子が、無効または非正当として設定され得、それぞれの署名または証明書においてこのマシン識別コード識別子を含む後続の受信される要求が、全て拒否され得る。

【００９８】

ブロック３７０は、ネットワークサービスのアクセスに関して別の決定を実行することを進める。

【００９９】

ここで、ネットワークサービスのアクセスに関して別の決定が、例えば、端末から送信された要求の間隔及び回数についての統計を計算して、端末の要求が、悪意のあるコンピュータプログラム等から送信されたかどうかを決定することであり得る。

【０１００】

第２の要求がまた第１の要求である場合、第１の要求のための他の処理、例えば、署名または証明書におけるマシン識別コード識別子に基づいて端末を識別することが、完了される必要があることに留意するべきである。

【０１０１】

この実施形態において、サービスネットワークにおける端末識別システムが、第１の実

施形態の先頭上に、以下の機能及び機能モジュールを追加する。すなわち、
第１の検証モジュールは、受信モジュールが、マシン識別コードが端末から検証される必要があるという第２の要求を受信するときに、署名または証明書の検証を実行するように更に構成される。
【０１０２】
その上、端末識別システムが、
端末のマシン識別コード識別子及び対応するマシン識別コードまたはそれの派生コードを記憶するように構成されたデータベースと、
第１の検証モジュールが、第２の要求における署名または証明書が正当であることを検証したときに、署名または証明書において取得されたマシン識別コード識別子に従って、データベース内の対応するマシン識別コードまたは派生コードを照会して、第２の要求から取得されたマシン識別コードまたは派生コードが、照会から見付けられるマシン識別コードまたは派生コードと同じであるかどうかを決定して、同じである場合には正当あるいはその他の場合には非正当としてマシン識別コードのための検証結果を設定するように構成された、第２の検証モジュールと、
第２の検証モジュールの検証結果が非正当として設定されるときに、要求を拒否するように構成されたアクセス制御モジュールと、を更に含む。
【０１０３】
図６は、システムの実施例６００、例えば、上記したようなシステムなどをより詳細に例示する。一実施形態において、システム６００は、限定されるものではないが、１以上のプロセッサ６０１、ネットワークインターフェース６０２、メモリ６０３、及び入出力インターフェース６０４を含むことができる。
【０１０４】
メモリ６０３は、揮発性メモリ、例えばランダムアクセスメモリ（ＲＡＭ）など、及び／または不揮発性メモリ、例えば読み取り専用メモリ（ＲＯＭ）もしくはフラッシュＲＡＭなどの形態で、コンピュータで読み取り可能な媒体を含み得る。メモリ６０３は、コンピュータで読み取り可能な媒体の実施例である。
【０１０５】
コンピュータで読み取り可能な媒体が、例えばコンピュータで読み取り可能な命令、データ構造、プログラムモジュール、もしくは他のデータなどの情報の記憶のために任意の方法または技術において実装された揮発性及び不揮発性の、取り外し可能なならびに取り外し不可能な媒体を含む。コンピュータ記憶媒体の実施例は、限定されるものではないが、相変化メモリ（ＰＲＡＭ）、静的ランダムアクセスメモリ（ＳＲＡＭ）、動的ランダムアクセスメモリ（ＤＲＡＭ）、他の種類のランダムアクセスメモリ（ＲＡＭ）、読み取り専用メモリ（ＲＯＭ）、電気的に消去可能でプログラム可能な読み取り専用メモリ（ＥＥＰＲＯＭ）、フラッシュメモリまたは他のメモリ技術、コンパクトディスク読み取り専用メモリ（ＣＤ－ＲＯＭ）、デジタル多用途ディスク（ＤＶＤ）または他の光記憶装置、磁気カセット、磁気テープ、磁気ディスク記憶装置または他の磁気記憶デバイス、あるいはコンピューティングデバイスによるアクセスのための情報を記憶するために使用され得る任意の他の非伝送媒体を含む。本明細書において定義される際、コンピュータで読み取り可能な媒体が、一時的な媒体、例えば変調データ信号及び搬送波などを含まない。
【０１０６】
メモリ６０３は、プログラムモジュール６０５及びプログラムデータ６０６を含み得る。一実施形態において、プログラムモジュール６０５は、受信モジュール６０７、第１の検証モジュール６０８、第２の検証モジュール６０９、識別モジュール６１０、登録モジュール６１１、及びアクセス制御モジュール６１２を含み得る。いくつかの実施形態において、メモリ６０３が、データベース６１３を更に含んでもよい。これらのプログラムモジュールについての詳細は、上記した前述の実施形態において見付けられ得る。
【０１０７】
図７は、信頼できる機関の実施例７００、例えば上記したような信頼できる機関などを

より詳細に例示する。一実施形態において、信頼できる機関７００は、限定されるものではないが、１以上のプロセッサ７０１、ネットワークインターフェース７０２、メモリ７０３、及び入出力インターフェース７０４を含むことができる。メモリ７０３は、揮発性メモリ、例えばランダムアクセスメモリ（ＲＡＭ）など、及び／または不揮発性メモリ、例えば読み取り専用メモリ（ＲＯＭ）もしくはフラッシュＲＡＭなどの形態で、コンピュータで読み取り可能な媒体を含み得る。メモリ７０３は、コンピュータで読み取り可能な媒体の実施例である。

【０１０８】

メモリ７０３は、プログラムモジュール７０５及びプログラムデータ７０６を含み得る。一実施形態において、プログラムモジュール７０５は、受信モジュール７０７、検証モジュール７０８、割り当てモジュール７０９、及び発行モジュール７１０を含み得る。これらのプログラムモジュールについての詳細は、上記した前述の実施形態において見付けられ得る。

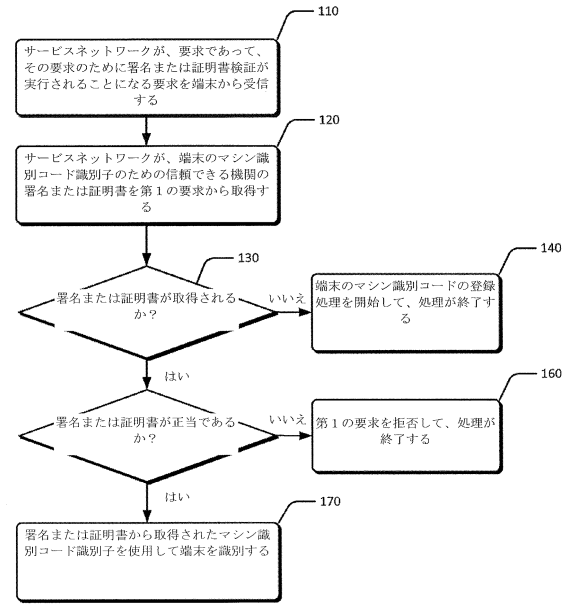
【０１０９】

当業者は、前述の方法の全てまたは一部が、関連のあるハードウェア構成要素に命令するプログラムによって実行され得ることを理解することができる。プログラムは、コンピュータで読み取り可能な記憶媒体、例えば、読み取り専用メモリ、磁気ディスク、または光ディスクなどの中に記憶され得る。任意選択的に、前述の実施形態の全てまたは一部が、１以上の集積回路を使用して実装され得る。したがって、前述の実施形態の各モジュール／ユニットは、ハードウェアまたはソフトウェア機能モジュールの形態で実装され得る。本開示は、ハードウェアとソフトウェアの組み合わせの任意の特定の形態に限定されない。

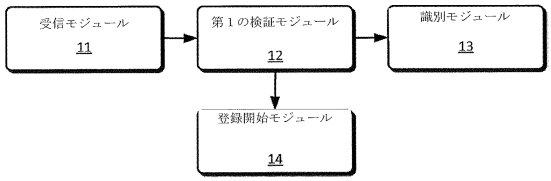
【０１１０】

上記したものは、本開示の単に好適な実施形態に過ぎず、本開示の限定として解釈されるべきではない。当業者のために、開示された方法及びシステムが、種々の変更や修正に適応できる。本開示の趣旨及び原理内にある任意の変更、等価物及び改善等が、本開示の保護の下で包含される。

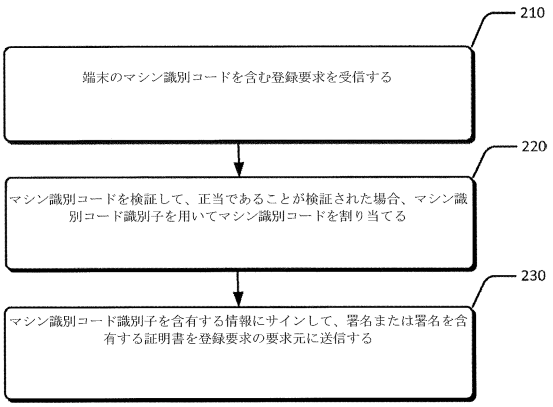
【図１】



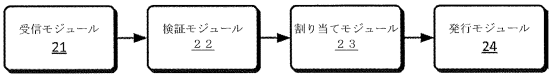
【図２】



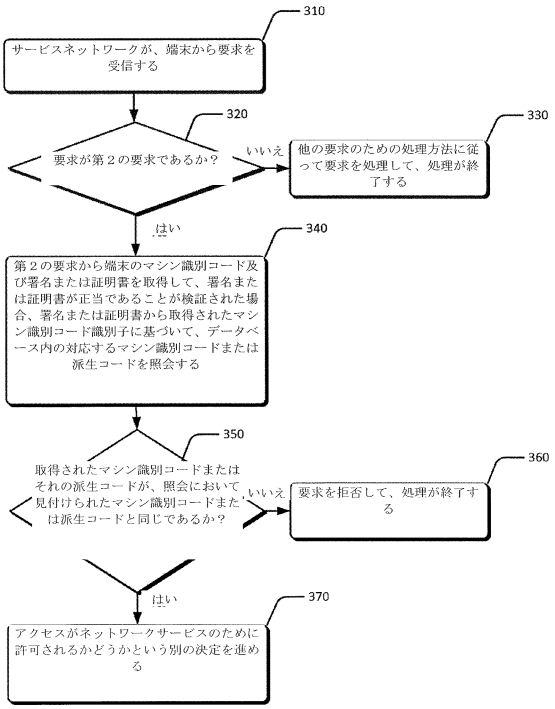
【図３】



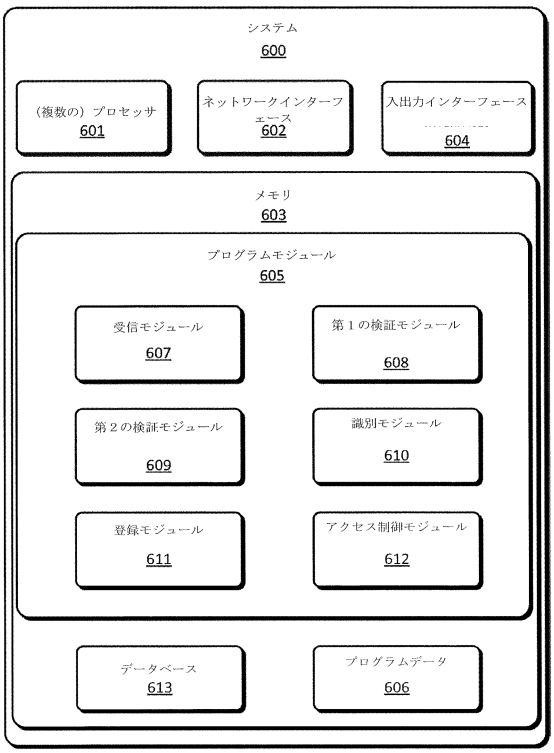
【図４】



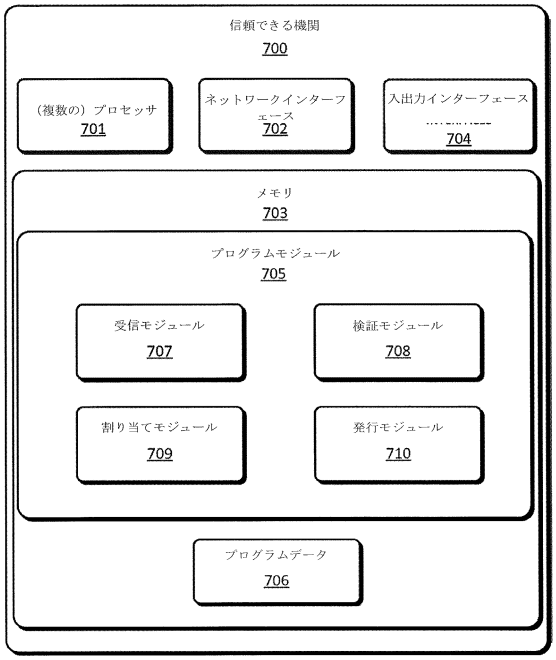
【図５】



【図６】



【図７】


信頼できる機関
700
（複数の）プロセッサ
701
ネットワークインターフェース
702
入出力インターフェース
704
メモリ
703
プログラムモジュール
705
受信モジュール
707
検証モジュール
708
割り当てモジュール
709
発行モジュール
710
プログラムデータ
706

フロントページの続き

(72)発明者 インフォン フー
中華人民共和国 ３１１１２ ハンチョウ ユー ハン ディストリクト ウェスト ウェン イー ロード ナンバー ９６９ ビルディング ３ ５／エフ アリババ グループ リーガル デパートメント内
(72)発明者 ユードン ジャン
中華人民共和国 ３１１１２ ハンチョウ ユー ハン ディストリクト ウェスト ウェン イー ロード ナンバー ９６９ ビルディング ３ ５／エフ アリババ グループ リーガル デパートメント内
(72)発明者 ジェンユエン ジャン
中華人民共和国 ３１１１２ ハンチョウ ユー ハン ディストリクト ウェスト ウェン イー ロード ナンバー ９６９ ビルディング ３ ５／エフ アリババ グループ リーガル デパートメント内
(72)発明者 ジエン リウ
中華人民共和国 ３１１１２ ハンチョウ ユー ハン ディストリクト ウェスト ウェン イー ロード ナンバー ９６９ ビルディング ３ ５／エフ アリババ グループ リーガル デパートメント内

審査官 和平 悠希

(56)参考文献 特開２００８－２３４６０６（ＪＰ，Ａ）
国内No. 1のデバイス証明書発行管理サービス 端末識別情報を基に証明書を安全に登録, BUSINESS COMMUNICATION, ２０１３年 5月 1日, Vol. 50, No. 5, pp. 96-97

(58)調査した分野(Int.Cl., ＤＢ名)
Ｈ０４Ｌ ９／３２