(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2009-528582
(P2009-528582A)
(43)公表日　平成21年8月6日(2009.8.6)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/20	(2006.01)	G06F	15/00	330B	5B285
H04L 9/32	(2006.01)	G06F	15/00	330E	5J104
G09C 1/00	(2006.01)	H04L	9/00	675A	
H04L 9/08	(2006.01)	G09C	1/00	640E	
		H04L	9/00	601C	

審査請求 未請求　予備審査請求 未請求　（全 10 頁）

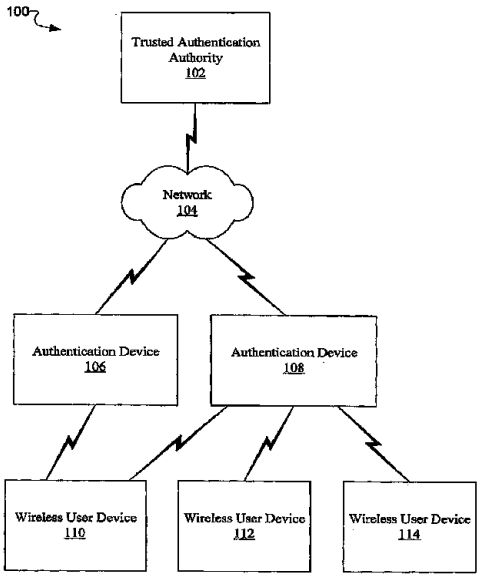
(21)出願番号　特願2008-546009 (P2008-546009)
(86)(22)出願日　平成18年12月13日 (2006.12.13)
(85)翻訳文提出日　平成20年8月13日 (2008.8.13)
(86)国際出願番号　PCT/US2007/047695
(87)国際公開番号　WO2007/112133
(87)国際公開日　平成19年10月4日 (2007.10.4)
(31)優先権主張番号　11/300,570
(32)優先日　平成17年12月13日 (2005.12.13)
(33)優先権主張国　米国(US)

(71)出願人　500046438
マイクロソフト　コーポレーション
アメリカ合衆国　ワシントン州　９８０５２－６３９９　レッドモンド　ワン　マイクロソフト　ウェイ
(74)代理人　100077481
弁理士　谷　義一
(74)代理人　100088915
弁理士　阿部　和夫
(72)発明者　ラッセル　アイ．サンチェス
アメリカ合衆国　９８０５２　ワシントン州　レッドモンド　ワン　マイクロソフト　ウェイ　マイクロソフト　コーポレーション　インターナショナル　パテンツ内

最終頁に続く

(54)【発明の名称】無線認証

(57)【要約】
保護されたリソースへのアクセスを許可する前にユーザを認証するための無線認証システムがここで説明される。認証デバイスは、保護されたリソースへのアクセスの意図の指示を受け取る。認証デバイスは鍵の要求を送る。無線ユーザデバイスおよび認証デバイスは鍵交換を採用できる。認証デバイスは、鍵交換を介して取得された１または複数の鍵が有効であるかどうかを判定し、１または複数の鍵が有効である場合に保護されたリソースへのアクセスを許可できる。認証デバイスは、鍵保有者検証などのユーザの識別のさらなる検証を要求できる。鍵および鍵保有者検証が有効である場合に、認証デバイスは、保護されたリソースへのアクセスを許可できる。



【特許請求の範囲】
【請求項１】
保護されたリソースにアクセスすることを意図するモバイルユーザデバイスから指示を受け取るステップと、
前記リソースにアクセスする前記意図の前記モバイルユーザデバイスからの前記指示に応答して、前記モバイルユーザデバイスとの鍵交換を要求するステップと、
前記モバイルユーザデバイスと１または複数の鍵を交換するステップであって、前記１または複数の鍵はユーザのセキュリティ証明書を提供する、交換するステップと、
前記鍵交換を介して取得された前記１または複数の鍵が有効であるかどうかを検証するステップと、
前記鍵交換を介して取得された前記１または複数の鍵が有効である場合に、前記保護されたリソースへのアクセスを認証するステップと
を実行するためのデバイスが実行可能な命令を含む１または複数のデバイス可読媒体。
【請求項２】
前記保護されたリソースへのアクセスを意図する指示は、受動の動作を備えたことを特徴とする請求項１に記載の１または複数のデバイス可読媒体。
【請求項３】
前記受動の動作は、認証デバイスへ近づくことを備えたことを特徴とする請求項２に記載の１または複数のデバイス可読媒体。
【請求項４】
前記保護されたリソースへのアクセスを意図する指示は、明白な動作を備えたことを特徴とする請求項１に記載の１または複数のデバイス可読媒体。
【請求項５】
前記明白な動作は、鍵所有者検証の表示を備えたことを特徴とする請求項４に記載の１または複数のデバイス可読媒体。
【請求項６】
前記明白な動作は、認証デバイスに触ることを備えたことを特徴とする請求項４に記載の１または複数のデバイス可読媒体。
【請求項７】
前記ステップは、鍵保有者検証を要求するステップをさらに備えたことを特徴とする請求項１に記載の１または複数のデバイス可読媒体。
【請求項８】
前記鍵保有者検証はＰＩＮを備えたことを特徴とする請求項７に記載の１または複数のデバイス可読媒体。
【請求項９】
前記鍵検証は、一連のキーストロークを備えたことを特徴とする請求項７に記載の１または複数のデバイス可読媒体。
【請求項１０】
前記鍵保有者検証は、ジェスチャーを備えたことを特徴とする請求項７に記載の１または複数のデバイス可読媒体。
【請求項１１】
前記ステップは、前記鍵保有者検証が有効であるかどうかを検証するステップをさらに備えたことを特徴とする請求項７に記載の１または複数のデバイス可読媒体。
【請求項１２】
前記保護されたリソースへのアクセスを認証するステップは、前記鍵および前記鍵保有者検証の両方が有効である場合に、前記保護されたリソースへのアクセスを認証するステップを備えたことを特徴とする請求項１１に記載の１または複数のデバイス可読媒体。
【請求項１３】
ユーザに関連付けられたセキュリティ証明書を格納する鍵を含む無線ユーザデバイスと、

前記無線ユーザデバイスに通信的に結合された認証デバイスであって、前記認証デバイスは、１または複数のリソースへのアクセスを保護するためのロックを含み、前記認証デバイスは、前記１または複数のリソースへのアクセスのユーザの意図を認識し、前記無線ユーザデバイスから前記鍵を取得し、前記鍵が有効かどうかを検証し、前記鍵が有効な場合に前記１または複数のリソースへのアクセスを許可する認証デバイス
を備えたことを特徴とするシステム。
【請求項１４】
前記認証デバイスに通信的に結合されたサーバをさらに備え、前記サーバは、前記認証デバイスから受け取られたセキュリティ証明書の検証の後に、追加のリソースへのアクセスを許可することを特徴とする請求項１３に記載のシステム。
【請求項１５】
リソースへのアクセスを保護する第一のデバイスのロック設定をトリガするステップであって、前記ロックをトリガするステップは、前記リソースへのアクセスの意図の指示を提供するステップを備える、トリガするステップと、
第２のデバイスでロックを解除する鍵の要求を受け取るステップと、
セキュアな鍵交換を介して、前記第２のデバイスから前記第１のデバイスに前記鍵を送るステップと、
前記鍵が有効である場合に、前記リソースへのアクセスを受け取るステップと
を備えたことを特徴とする方法。
【請求項１６】
リソースへのアクセスを保護する第１のデバイスのロック設定をトリガするステップは、前記第１のデバイスの近接に入り込むステップを備えることを特徴とする請求項１５に記載の方法。
【請求項１７】
前記第１のデバイスの前記近接を開放するステップ、および前記リソースへのアクセスを防ぐための再ロックを前記ロックに引き起こすステップをさらに備えたことを特徴とする請求項１６に記載の方法。
【請求項１８】
鍵保有者検証の要求を受け取るステップ、および鍵保有者検証を提供することをユーザに促すステップをさらに備えたことを特徴とする請求項１５に記載の方法。
【請求項１９】
前記第１のデバイスへの前記鍵保有者検証を送信するステップをさらに備えたことを特徴とする請求項１８に記載の方法。
【請求項２０】
前記リソースへのアクセスを受け取るステップは、前記鍵および前記鍵保有者認証の両方が有効である場合に、前記リソースへのアクセスを受け取るステップを備えることを特徴とする請求項１９に記載の方法。
【発明の詳細な説明】
【技術分野】
【０００１】
パスワードのみを使用する認証は、価値のある企業リソースへの十分なセキュリティを提供しない。１つの解決法は、スマートカードなどのセキュリティカードを使用することである。しかしこれらのカードは、使用するのに不便であることが多く、よりセキュアでない技術を使用する。また使用の不便さは、ぴったり付いてドアを通ることにより、およびモバイルデバイス上に証明書を格納することによるなど、セキュリティを妨害することを試すことをユーザに導く。
【発明の開示】
【発明が解決しようとする課題】
【０００２】
以下は、読み手に基本的な理解を提供するために開示の簡易化された概要を示す。この

概要は、開示の広い全体ではなく、本発明の重要な要素を特定せず、または本発明の範囲を線引きしない。この唯一の目的は、以降で示されるより詳細な説明への前置きとして、簡易化された形式でここに開示されたいくつかの概念を示すことである。

【課題を解決するための手段】

【０００３】

ここで説明されるのは、無線認証のための方法およびシステムに向けられた様々な技術および技法である。説明された技術の１つの実装に従って、認証デバイスは、保護されたリソースへのアクセスを意図する指示を受け取るとき、前記認証デバイスは鍵の要求を送る。認証デバイスおよび無線ユーザデバイスはその後、セキュアな鍵交換に従事することができる。認証デバイスは鍵が有効であるかどうかを判定し、鍵が有効である場合に保護されたリソースへのアクセスを許可できる。説明された技術の別の実装において、認証デバイスは、カード保有者検証などのユーザの特定のさらなる検証を要求できる。認証デバイスは、鍵検証および鍵保有者検証の両方が有効である場合に、保護されたリソースへのアクセスを許可できる。

【０００４】

添付の図面と併せて考慮される以下の詳細な説明を参照することにより、より理解されるようになるのと同じように、多くの付帯する特徴が読んでより理解できるであろう。

【発明を実施するための最良の形態】

【０００５】

この説明は、添付の図面と照らし合わせて読まれる以下の詳細な説明から、よりよく理解できる。

【０００６】

似たような参照番号は、添付の図面において似たような部分を指定するように使用される。

【０００７】

添付の図面と併せて以下で提供される詳細な説明は、本発明の例を説明するものとして意図され、この例が構成または利用されうる唯一の形式を表すことを意図しない。詳細な説明は、例の機能および例を構成および動作するステップのシーケンスを説明する。しかし、同じまたは同等の機能およびシーケンスは異なる例により達成できる。

【０００８】

図１は無線認証のための例示的なシステム１００のブロック図である。システム１００は、１０６および１０８などの１または複数の認証デバイスを含む。それぞれの認証デバイスを、１１０、１１２および１１４などの１または複数の無線ユーザデバイスに通信的に結合できる。無線ユーザデバイスのそれぞれを、１または複数の認証デバイスに通信的に結合できる。１１０などの無線ユーザデバイスでユーザは、保護されたリソースへのアクセスの意図を明示できる。認証デバイス１０６が保護されたリソースへのアクセスの意図のこの指示を受け取るとき、認証デバイスは認証処理を開始する。認証デバイス１０６は、ユーザデバイス１１０との鍵交換を要求する。ユーザデバイス１１０はその後、認証デバイス１０６と鍵をセキュアに交換することができる。鍵はユーザのセキュリティ証明書を提供する。認証デバイス１０６はその後、鍵交換を介して取得される鍵の有効性を検証できる。鍵の有効性はローカルで、またはネットワーク１０４を介して信頼された認証局１０２と通信することにより検証できる。鍵が有効である場合、認証デバイス１０６はリソースへのアクセスを許す。信頼された認証局１０２は、追加のセキュリティ証明書を要求でき、リソースへのアクセスが許される前に、認証デバイス１０６はこれらの証明書を提供する。

【０００９】

さらなる検証のために、認証デバイス１０６は、ユーザの特定のさらなる検証のために、ユーザから鍵保有者検証を追加で要求できる。鍵保有者検証の例は、ＰＩＮ、一連のキーストローク（keystroke）、ジョイスティックトリガ、動きまたはジェスチャーの組合せを含むことができるが、これらに限られない。認証デバイス１０６が鍵保有者検証を受

け取るとき、認証デバイス１０６はローカルでまたは信頼された認証局１０２と通信することにより、カード保有者検証の有効性をチェックできる。鍵が有効で鍵保有者検証が有効である場合、認証デバイス１０６はリソースへアクセスを許すことができる。

【００１０】

鍵保有者検証の有効性を将来のアクセスのために格納できる。これらはカード保有者検証の失効ポリシーセットであるかもしれない。失効ポリシーの例は、期限、多くのアクセスもしくは鍵の使用またはリソースの種類を含むことができるがこれらに限られない。たとえば、期限が設定される場合、鍵保有者検証は設定された期限までの期間について有効のままであることができる。期限が到達する前に鍵が使用される場合、鍵保有者認証は有効のままであり、ユーザは鍵保有者検証を提供する必要がない。期限が到達した後、ユーザはリソースにアクセスする前に、もう一度鍵保有者検証を提供することを要求する。多くのユーザが設定される場合、その後鍵保有者検証は、鍵がユーザの設定数まで使用されるまで有効であることができる。失効ポリシーはリソースの種類に基づいて変更することもできる。失効ポリシーを設定するために他の基準を使用できる。失効ポリシーは信頼された認証機関、認証デバイスまたは他のデバイスもしくは機関により設定できる。

【００１１】

図２は、無線認証のための例示的な認証デバイス２３０および例示的な無線ユーザデバイス２４０のブロック図である。認証デバイス２３０は、プロセッサ２０４、送信器２０６、受信機２０８、ロック２０２、１または複数の鍵２１２およびストレージ要素２１０を含む。ロック２０２は１または複数のリソースへのアクセスを保護する。認証デバイス２３０は、無線ユーザデバイス２４０に通信的に接続される。無線ユーザデバイス２４０は、プロセッサ２２２、送信器２１６、受信機２１８、１または複数の鍵２２０およびストレージ要素２１４を含む。１または複数の鍵２２０は、ユーザについてのセキュリティ証明書を含む。これらのセキュリティ証明書はロック２０２を解除するのに使用でき、ロック２０２により保護された１または複数のリソースへのアクセスを提供する。無線ユーザデバイスの例は、バッジ、ウェアラブルデバイス、またはユーザが携帯できる任意の他のモバイルデバイスを含むことができるが、これらに限られない。

【００１２】

例示的な実装によって、認証デバイス２３０はＰＣ、ノートブックコンピュータ、携帯電話、ＰＤＡまたはＶＯＩＰ電話などのコンピューティングデバイスであることができる。ロック２０２および任意の他の必要なモジュールは、コンピューティングデバイスに組み込むことができ、あるいはＳＤＩＯカード、ＵＳＢキー、ＰＣＭＣＩＡカード、コンパクトフラッシュ（登録商標）またはＰＣＩカードなどの様々なプラグインのアクセサリインタフェースを介してコンピューティングデバイスとのインターフェースを取ることができる。

【００１３】

代替として、認証デバイス２３０は、ドア、キャビネットまたはロッカーなどの物理的アクセスを防ぐために装置に統合できる。認証デバイス２３０はプリンタ、コピー機、現金レジ、電話会議装置、ローン用装置またはプレゼンテーション装置などの装置に統合することもできる。さらに、認証デバイス２３０は、他の任意の価値のある資産または文書を保護するために統合することができる。

【００１４】

例示的な実装において、認証デバイス２３０は、無線ユーザデバイスに投じることができる。他の例示的な実装において、カメラまたは動きセンサーなどの動き検知デバイスは、認証デバイス２３０の周りの動きを検知するのに使用できる。これらまたは他の実装において、リソースへアクセスすることの意図の指示は、認証デバイス２３０のある近接に入ってくる無線ユーザデバイス２４０であることができる。認証デバイス２３０がリソースへのアクセスの意図のこの指示を受け取るとき、認証デバイス２３０は認証処理を開始できる。たとえば、無線ユーザデバイス２４０を有するユーザがユーザのラップトップの近接に入ってくるとき、ラップトップはリソースへのアクセスすることのユーザの意図を

認識し、その後、無線ユーザデバイスからユーザの鍵を自動的に取得する。ラップトップは、ユーザの特定(identity、アイデンティティ)を検証するためのＰＩＮをユーザに促すこともできる。鍵およびＰＩＮは、有効性について検証されることができ、ラップトップは、ＯＳならびにネットワークへのユーザを認証することができる。ユーザがラップトップの付近を離れる場合、ラップトップは、ＯＳおよびネットワークから認証しないことができる。ユーザがあるタイムリミット内にラップトップの近接に戻るとき、ラップトップはＰＩＮの再入力をユーザに促すことなく、解除および再認証できる。

【００１５】

代替として、リソースへのアクセスの意図の指示は、コンピューティングデバイス上のキーボード上のタイピング、ドアのハンドルに触れること、コピー機のボタンを押すことなどの物理的な動作であることができる。物理的動作は、認証デバイスに認証処理を開始することを促す。認証デバイスは、ユーザデバイスから鍵を要求できる。認証デバイスは、ユーザから鍵保有者検証を要求することもできる。鍵および／または鍵保有者検証が有効であると決定された後、リソースへのアクセスを許すことができる。

【００１６】

代替として、カード保有者検証それ自身を表す動作は、リソースへのアクセスを意図する通信を提供することもできる。この場合、認証デバイスは明確にカード保有者検証を要求する必要がないが、むしろ鍵交換を開始することにより、カード保有者検証の表示に応答する必要がある。リソースへのアクセスの意図の他の表示は、他の実装で使用でき認識できることを理解されたい。

【００１７】

無線ユーザデバイスは、ユーザの位置およびユーザの数をトラック(track)するのにも使用できる。たとえば、ドアを通して入るまたは出る人々の数をトラックできる。無線ユーザデバイスは、会議の出席を判定するのに使用できる。無線ユーザデバイスは人々を見つけ、そして人々に知らせるのにも使用できる。

【００１８】

無線ユーザデバイスは、ユーザが認証したい１または複数の認証デバイスに対応する１または複数のプロファイルを含むことができる。無線ユーザデバイスがそのプロファイルを有さない認証デバイスの近接内に無線ユーザデバイスが入ってくるとき、無線ユーザデバイスは認証デバイスとの認証を試みない。無線ユーザデバイスが近接の新しい認証デバイスを探索する発見機能を含むことができる。新しい認証デバイスが見つかるとき、ユーザは無線ユーザデバイスに新しい認証デバイスプロファイルを追加するための選択を有する。ユーザが新しいデバイスプロファイルを追加することを選ぶ場合、ユーザにカード保有者検証を入力することを促すことができる。一度新しい認証デバイスプロファイルが追加されると、無線ユーザデバイスが新しい認証デバイスの近接に入ってくるとき、新しい認証デバイスは認証処理を自動的に開始する。

【００１９】

図３は、無線認証の例示的な処理を示すフロー図である。図３のこの説明が他の図面を参照してなされる一方で、図３に示される例示的な処理は特定の１つの図面または複数の図面の任意のシステムまたは他の中身と関連付けられて限定されることを意図しないことを理解されたい。さらに、図３の例示的な処理が操作実行の特定の順番を示す一方で、１または複数の代替の実装において、操作を異なって順序付けられるかもしれないことを理解されたい。さらに、図３の例示的な処理に示されるいくつかのステップおよびデータは、いくつかの実装においては必要ではなく、省くことができる。最終的に、図３の例示的な処理が多数の分離したステップを含む一方で、いくつかの環境においてこれらの操作のいくつかは同時に結合され実行されることを認識されたい。

【００２０】

３１０において、デバイスはリソースにアクセスする意図の指示を受け取る。リソースへのアクセスの意図の指示は、認証デバイスの近接に入ってくる無線ユーザデバイスなどの受動の動作、カード保有者検証の表示などの明白な動作、認証デバイスに触れるなどの

リソースへのアクセスの意図を明示する物理的な動作、またはリソースへアクセスの意図を示す他の動作であることができる。３２０において、認証デバイスは、鍵交換および／またはカード保有者検証の要求を送る。鍵交換の例は、ＰＧＰ（Ｐｒｅｔｔｙ Ｇｏｏｄ Ｐｒｉｖａｃｙ）、ＧＰＧ（Ｇｎｕ Ｐｒｉｖａｃｙ Ｇｕａｒｄ）またはＰＫＣ（Ｐｕｂｌｉｃ Ｋｅｙ Ｃｒｙｐｔｏｇｒａｐｈｙ）を含むがこれらに限られない。３３０において、ユーザデバイスは、認証デバイスと鍵を交換する。カード保有者検証が要求される場合、ユーザデバイスまたは認証デバイスは、ユーザにカード保有者検証を提供することを頼むことができる。３４０において、認証デバイスは、鍵交換を介して取得された１または複数の鍵が有効であるかどうかを決定する。カード保有者検証が要求され提供される場合、認証デバイスはカード保有者検証が有効であるかどうかも決定する。３５０において、１または複数の鍵および／またはカード保有者検証が有効である場合、ユーザにリソースへのアクセスを許可することができる。鍵またはカード保有者検証のいずれかが無効である場合、３６０において、リソースへのアクセスを拒否できる。

【００２１】

図４は、本発明のある態様が実装される例示的なコンピューティング環境を示す。コンピューティング環境４００がここで説明される様々な技術を採用できる適切なコンピューティング環境の唯一の例であり、ここで説明される技術の使用または機能性の範囲に関してなんらかの限定を提案することを意図しないことを理解されたい。また、コンピューティング環境４００はここで示されるコンポーネントのすべてを要求する必要はないものとして解釈される。

【００２２】

ここで説明された技術は、膨大な他の一般目的または特定目的のコンピューティング環境または構成で使用できる。ここで説明される技術の使用に適するであろう周知のコンピューティング環境および／または構成の例は、パーソナルコンピュータ、サーバコンピュータ、ハンドヘルドまたはラップトップデバイス、タブレットデバイス、マルチプロセッサシステム、マイクロプロセッサベースのシステム、セットトップボックス、プログラマブル家電、ネットワークＰＣ、ミニコンピュータ、メインフレームコンピュータ、上述のシステムまたはデバイスの任意を含む分散コンピューティング環境などを含むがこれらに限られない。

【００２３】

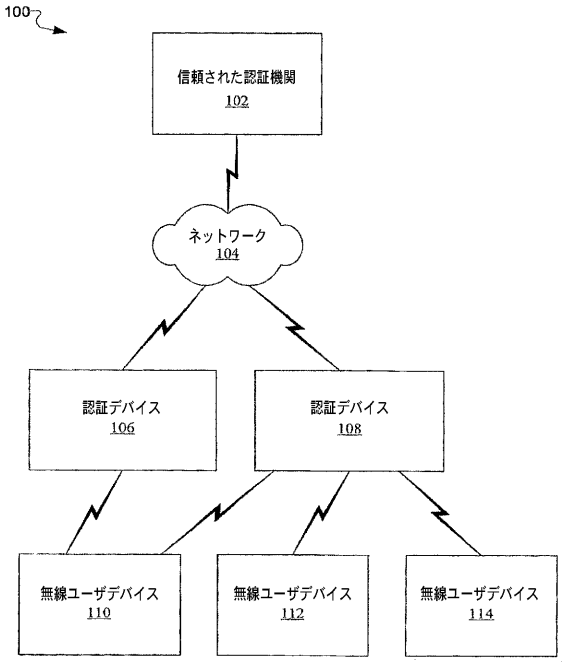
図４を参照して、コンピューティング環境４００は、一般目的のコンピューティングデバイス４１０を含む。コンピューティングデバイス４１０のコンポーネントは、処理ユニット４１２、メモリ４１４、ストレージデバイス４１６、入力デバイス４１８、出力デバイス４２０および通信接続４２２を含むがこれらに限られない。

【００２４】

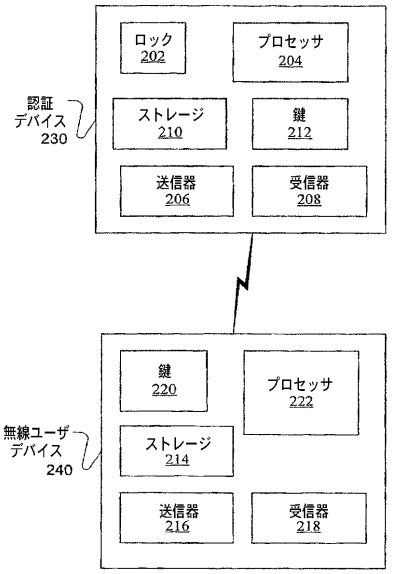
コンピューティングデバイスの構成および種類によって、メモリ４１４は、（ＲＡＭなどの）揮発性、（ＲＯＭ、フラッシュメモリなどの）不揮発性またはこれら２つの組合せであることができる。コンピューティングデバイス４１０は、磁気もしくは光ディスクまたはテープを含むがこれらに限られない（リムーバブルおよび／またはリムーバブルでない）追加のストレージを含むこともできる。このような追加のストレージはストレージ４１６により図４に示される。コンピュータストレージメディアは、コンピュータが読取り可能な命令、データ構造、プログラムモジュールまたは他のデータなどの情報の格納のための任意の方法または技術において実装される、揮発性および不揮発性、リムーバブルおよびリムーバブルでないメディアを含む。メモリ４１４およびストレージ４１６はコンピュータストレージメディアの例である。コンピュータストレージメディアは、ＲＡＭ、ＲＯＭ、ＥＥＰＲＯＭ、フラッシュメモリもしくは他のメモリ技術、ＣＤ－ＲＯＭ、ＤＶＤもしくは他の光ストレージ、磁気カセット、磁器テープ、磁気ディスクストレージもしくは他の磁気ストレージデバイス、または所望の情報を格納するのに使用でき、コンピューティングデバイス４１０によりアクセスできる任意の他のメディアを含むが、これらに限られない。このようなコンピュータストレージメディアはコンピューティングデバイス４

１０に一部であることができる。
【００２５】
コンピューティングデバイス４１０は、ネットワーク４３０を通して他のコンピューティングデバイスなどの他のデバイスと通信することをコンピューティングデバイス４１０に可能にする通信接続４２２も含むこともできる。通信接続４２２は、通信メディアの一例である。通信メディアは通常、コンピュータが読取り可能な命令、データ構造、プログラムモジュールまたは搬送波または他の転送メカニズムなどの変調されたデータ信号における他のデータを組み込み、任意の情報配送メディアを含む。「変調されたデータ信号」という用語は、１または複数のその特性を有する信号を意味し、信号内の情報をエンコードするような方式で設定または変化する信号を意味する。例としてであり限定ではなく、通信メディアは、有線ネットワークまたは直接有線接続などの有線メディア、アコースティック、無線周波、赤外線および他の無線メディアなどの無線メディアを含む。ここで使用されるようにコンピュータ可読記憶媒体という用語は、ストレージメディアを含む。
【００２６】
コンピューティングデバイス４１０は、キーボード、マウス、ペン、音声入力デバイス、タッチ入力デバイスおよび／または任意の他の入力デバイスなどの入力デバイス４１８を有することもできる。１または複数のディスプレイ、スピーカ、プリンタおよび／または任意の他の出力デバイスなどの出力デバイス４２０もまた含まれうる。
【００２７】
本発明が多くの例示的な実装に関して説明されてきたが、本発明が説明された実装に限定されないが、添付の特許請求の範囲の精神および範囲内で修正および変更できることを当業者は認識する。この説明はしたがって、限定の代わりに例示として見なされることとなる。
【図面の簡単な説明】
【００２８】
【図１】無線認証のための例示的なシステムのブロック図である。
【図２】無線認証のための例示的なデバイスのブロック図である。
【図３】無線認証のための例示的な処理を示すフロー図である。
【図４】本発明のある態様が実装される例示的なコンピューティング環境を示す図である。

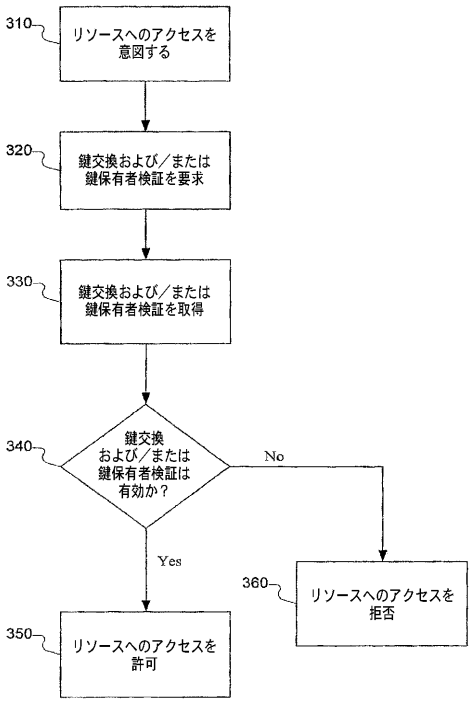
【図１】


100
信頼された認証機関
102
ネットワーク
104
認証デバイス
106
認証デバイス
108
無線ユーザデバイス
110
無線ユーザデバイス
112
無線ユーザデバイス
114

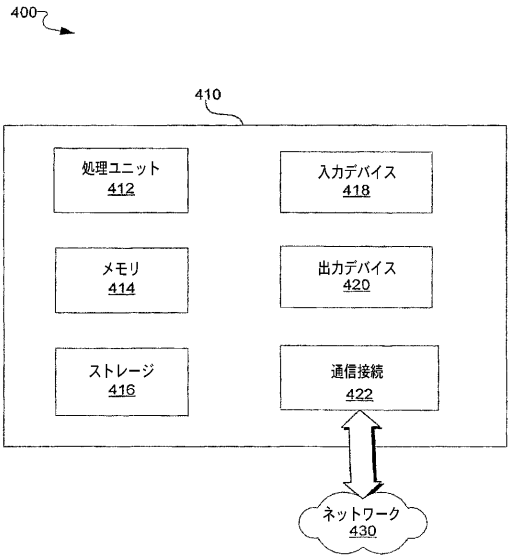
【図２】


認証デバイス
230
ロック
202
プロセッサ
204
ストレージ
210
鍵
212
送信器
206
受信器
208
無線ユーザデバイス
240
鍵
220
プロセッサ
222
ストレージ
214
送信器
216
受信器
218

【図３】


310
リソースへのアクセスを意図する
320
鍵交換および／または鍵保有者検証を要求
330
鍵交換および／または鍵保有者検証を取得
340
鍵交換および／または鍵保有者検証は有効か？
No
Yes
360
リソースへのアクセスを拒否
350
リソースへのアクセスを許可

【図４】


400
410
処理ユニット
412
入力デバイス
418
メモリ
414
出力デバイス
420
ストレージ
416
通信接続
422
ネットワーク
430

フロントページの続き

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

(72)発明者 ドナルド アール．トンプソン
アメリカ合衆国 ９８０５２ ワシントン州 レッドモンド ワン マイクロソフト ウェイ マイクロソフト コーポレーション インターナショナル パテンツ内
(72)発明者 ディヴィッド エム．リーマン
アメリカ合衆国 ９８０５２ ワシントン州 レッドモンド ワン マイクロソフト ウェイ マイクロソフト コーポレーション インターナショナル パテンツ内

Ｆターム(参考) 5B285 AA01 BA02 BA08 CA02 CA04 CA41 CA43 CB02 CB55 CB56
CB59 CB62 CB63 CB73 CB76 CB84 CB92 DA03
5J104 AA07 AA16 EA04 EA15 EA16 JA21 KA02 KA05 NA02 NA27
NA37 NA38