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

特許第5038531号
(P5038531)

(45)発行日　平成24年10月3日(2012.10.3)　(24)登録日　平成24年7月13日(2012.7.13)

(51)Int.Cl.　　F I
G06F 21/20 (2006.01)　　G06F 21/20　131A
H04L 9/32 (2006.01)　　H04L 9/00　673A
　　G06F 21/20　144C

請求項の数 17　(全 19 頁)

(21)出願番号　特願2011-511684 (P2011-511684)
(86)(22)出願日　平成21年5月4日 (2009.5.4)
(65)公表番号　特表2011-522327 (P2011-522327A)
(43)公表日　平成23年7月28日 (2011.7.28)
(86)国際出願番号　PCT/US2009/042667
(87)国際公開番号　WO2009/148746
(87)国際公開日　平成21年12月10日 (2009.12.10)
審査請求日　平成24年1月24日 (2012.1.24)
(31)優先権主張番号　12/131,142
(32)優先日　平成20年6月2日 (2008.6.2)
(33)優先権主張国　米国 (US)

早期審査対象出願

(73)特許権者　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　100140109
弁理士　小野　新次郎
(74)代理人　100075270
弁理士　小林　泰
(74)代理人　100080137
弁理士　千葉　昭男
(74)代理人　100096013
弁理士　富田　博行
(74)代理人　100119781
弁理士　中村　彰吾

最終頁に続く

(54)【発明の名称】信頼できる機器に限定した認証

(57)【特許請求の範囲】

【請求項１】

アカウントネットワーク(account network)（１００）内でユーザーの多要素認証（multiple-factor authentication）を行なう方法であって、

前記アカウントネットワーク（１００）にアクセスするために前記ユーザーによって用いられる機器(device)（１０２）で生成(generated)された前記ユーザーのユーザー資格情報(user credentials)（２０４）および機器資格情報(device credentials)（２０４）を受け取るステップと、

前記ユーザー資格情報（２０４）のユーザー識別子(identifier)を前記機器資格情報（２０４）の機器識別子(identifier)に関連付け(associating)（２０６）て、前記ユーザーと前記機器との間の信頼関係(trust relationship)を表す(represent)ステップと、

前記ユーザー資格情報（２０４）および前記機器資格情報（２０４）を評価(evaluating)して、検証結果(verification results)を生成する（３１４）ステップと、

前記ユーザー資格情報（２０４）および前記機器資格情報（２０４）両方の前記検証結果に基づいて、前記ユーザーの識別(identity)の証拠(evidence)を提供する（３２０）ステップと、

前記ユーザー資格情報の検証は合格したが前記機器資格情報の検証が合格しない場合は、前記ユーザーによる前記ユーザー資格情報および前記機器資格情報を変更する試み(attempt)を阻止(blocking)するステップと、

前記ユーザ資格情報と前記機器資格情報との双方の識別の証拠が、検証の合格を示す場

合に、より高位の特権を許可し、前記ユーザ資格情報と前記機器資格情報とのいずれの識別の証拠も、検証の失敗を示す場合に、より低位の特権を許可するステップと、
を含み、
前記関連付けることが、前記ユーザ識別子と前記機器識別子を関連付けて、前記アカウントネットワーク内のユーザのアカウントに記録することを含み、
共有パラメータが、前記ユーザのアカウントに付加され、
前記共有パラメータが、遠隔ユーザを特定するために、及び、どの特権のレベルでの共有を希望するかを特定するために使用され、当該遠隔ユーザは、前記ユーザが、当該遠隔ユーザと、前記機器の共有を希望する者であり、
前記共有パラメータが、前記機器識別子と関連付けられる、
方法。

【請求項２】
前記ユーザーの識別の前記証拠は、前記ユーザー識別子および前記機器識別子の両方を含む、請求項１に記載の方法。

【請求項３】
前記関連付ける動作は、
前記ユーザー識別子および前記機器識別子と少なくとも１つの他の機器識別子を記録するステップであって、前記記録動作は、前記機器識別子および前記少なくとも１つの他の機器識別子で識別される前記機器を、前記ユーザーの信頼できる機器(trusted devices)として指定する、ステップ
を含む、請求項１に記載の方法。

【請求項４】
前記提供する動作は、
前記ユーザーの識別の前記証拠としてセキュリティトークンを生成するステップを含み、前記セキュリティトークンは、前記ユーザー識別子と前記機器識別子の両方を含む、請求項１に記載の方法。

【請求項５】
前記提供の動作は、
前記ユーザーの識別の前記証拠としてセキュリティトークンを生成するステップを含み、前記セキュリティトークンは、前記セキュリティトークンの受信者が前記セキュリティトークンから前記ユーザー識別子と前記機器識別子の両方にアクセスすることを可能にするプログラミングインタフェースを含む、請求項１に記載の方法。

【請求項６】
前記関連付け動作(associating operation)の後に前記機器識別子から前記ユーザー識別子の関連付けを解除(disassociating)して、前記機器を、ユーザーが信頼できるとされる機器から削除(remove)するステップをさらに含む、請求項１に記載の方法。

【請求項７】
前記提供動作(providing operation)は、前記ユーザー資格情報と前記機器資格情報両方の検証が合格した場合(upon successful verification)のみに、前記識別の証拠を提供(provides)する、
請求項１に記載の方法。

【請求項８】
前記提供動作は、前記ユーザー資格情報と前記機器資格情報両方の検証が合格した場合に、前記識別の証拠を提供する、
請求項１に記載の方法。

【請求項９】
前記提供動作は、前記ユーザー資格情報と前記機器資格情報両方の検証が合格した場合に、前記識別の証拠を提供し、
前記方法は、
結果として前記ユーザー資格情報の検証は合格したが前記機器資格情報の検証が合格し

なかった、前記ユーザー資格情報を使用した認証の試みを前記ユーザーに通知するステップ
をさらに含む、請求項１に記載の方法。
【請求項１０】
前記識別の証拠を受け取るのに応答してアカウントネットワークリソースによって付与(granted)される特権(privilege)のレベルは、前記識別の証拠が、前記機器資格情報の検証が合格したことを示すかどうかに応じて決まる、請求項１に記載の方法。
【請求項１１】
アカウントネットワーク内でユーザーの多要素認証を行なうコンピュータープロセスを行なうためのコンピューター実行可能命令を有するコンピューター可読記憶媒体（３１）であって、前記コンピュータープロセスは、
前記アカウントネットワーク（１００）にアクセスするために、前記ユーザーによって用いられる機器（１０２）で生成された前記ユーザーのユーザー資格情報（２０４）および機器資格情報（２０４）を受け取るステップであって、前記ユーザー資格情報（２０４）は、前記ユーザーのユーザー識別子を含み、前記機器資格情報（２０４）は、前記機器（１０２）の機器識別子を含むステップと、
前記アカウントネットワーク（１００）内の前記ユーザーのアカウント（１０６）に前記ユーザー識別子と前記機器識別子を組み合わせて記録する（２０６）ことにより、前記ユーザーと前記機器（１０２）との間の信頼関係を表すステップと、
前記ユーザー資格情報（２０４）および前記機器資格情報（２０４）を評価して、検証結果を生成するステップと、
前記ユーザー資格情報（２０４）および前記機器資格情報（２０４）両方の前記検証結果に基づいて、前記ユーザーの識別の証拠を提供する（３２０）ステップと、
前記ユーザー資格情報の検証は合格したが前記機器資格情報の検証が合格しない場合は、前記ユーザーによる前記ユーザー資格情報および前記機器資格情報を変更する試み(attempt)を阻止(blocking)するステップと、
前記ユザ資格情報と前記機器資格情報との双方の識別の証拠が、検証の合格を示す場合に、より高位の特権を許可し、前記ユザ資格情報と前記機器資格情報とのいずれの識別の証拠も、検証の失敗を示す場合に、より低位の特権を許可するステップと、
を含み、
前記関連付けることが、前記ユザ識別子と前記機器識別子を関連付けて、前記アカウントネットワーク内のユザのアカウントに記録することを含み、
共有パラメータが、前記ユザのアカウントに付加され、
前記共有パラメータが、遠隔ユザを特定するために、及び、どの特権のレベルでの共有を希望するかを特定するために使用され、当該遠隔ユザは、前記ユザが、当該遠隔ユザと、前記機器の共有を希望する者であり、
前記共有パラメータが、前記機器識別子と関連付けられる、
コンピューター可読記憶媒体（３１）。
【請求項１２】
前記ユーザーの識別の前記証拠は、前記ユーザー識別子および前記機器識別子の両方を含む、請求項１１に記載のコンピューター可読記憶媒体。
【請求項１３】
前記関連付けの動作は、
前記ユーザー識別子および前記機器識別子と少なくとも１つの他の機器識別子を記録するステップであって、前記記録動作は、前記機器識別子および前記少なくとも１つの他の機器識別子で識別される前記機器を、前記ユーザーの信頼できる機器として指定する、ステップ
を含む、請求項１１に記載のコンピューター可読記憶媒体。
【請求項１４】
前記提供する動作は、

前記ユーザーの識別の前記証拠としてセキュリティトークンを生成するステップを含み、前記セキュリティトークンは、前記ユーザー識別子と前記機器識別子の両方を含む、請求項１１に記載のコンピューター可読記憶媒体。

【請求項１５】

前記提供の動作は、

前記ユーザーの識別の前記証拠としてセキュリティトークンを生成するステップを含み、前記セキュリティトークンは、前記セキュリティトークンの受信者(recipient)が前記セキュリティトークンから前記ユーザー識別子と前記機器識別子の両方にアクセスすることを可能にするプログラミングインタフェースを含む、請求項１１に記載のコンピューター可読記憶媒体。

【請求項１６】

前記識別の証拠を受け取るのに応答してアカウントネットワークリソースによって付与される特権のレベルは、前記識別の証拠が、前記機器資格情報の検証が合格したことを示すかどうかに応じて決まる、請求項１１に記載のコンピューター可読記憶媒体。

【請求項１７】

アカウントネットワークリソース（１１０）にアクセスするためのあるレベルの特権をユーザーに許可する方法であって、

ユーザーが前記アカウントネットワークリソース（１１０）へのアクセスを試みる際に用いる機器（１０２）から識別の証拠（３２４）を受け取るステップと、

前記識別の証拠（３２４）を調べて（３２６）、前記識別の証拠が、前記アカウントネットワークリソース（１１０）に信頼できる認証提供者（１０４）による前記ユーザーのユーザー資格情報（２０４）および前記機器（１０２）の機器資格情報（２０４）両方の検証が合格したことを示すかどうかを判定するステップと、

前記ユーザー資格情報の検証は合格したが前記機器資格情報の検証が合格しない場合は、前記ユーザーによる前記ユーザー資格情報および前記機器資格情報を変更する試み(attempt)を阻止(blocking)するステップと、

前記識別の証拠が、前記認証提供者（１０４）による前記ユーザーの前記ユーザー資格情報（２０４）および前記機器（１０２）の前記機器資格情報（２０４）両方の検証が合格したことを示す場合は、第１のレベルの特権を付与する（３２６）ステップと、

前記識別の証拠（３２４）が、前記認証提供者（１０４）による前記ユーザーの前記ユーザー資格情報（２０４）および前記機器の前記機器資格情報両方の検証が不合格であったことを示す場合は、第２のレベルの特権を付与する（３２６）ステップと

を含み、

前記第1のレベルの特権が、前記第２のレベルの特権より高く、

前記識別の証拠は、前記アカウントネットワークリソースが前記ユーザー資格情報のユーザー識別子および前記機器資格情報の機器識別子にアクセスすることができるプログラミングインタフェースを提供するセキュリティトークンを含み、

前記関連付けることが、前記ユーザ識別子と前記機器識別子を関連付けて、前記アカウントネットワーク内のユーザのアカウントに記録することを含み、

共有パラメータが、前記ユーザのアカウントに付加され、

前記共有パラメータが、遠隔ユーザを特定するために、及び、どの特権のレベルでの共有を希望するかを特定するために使用され、当該遠隔ユーザは、前記ユーザが、当該遠隔ユーザと、前記機器の共有を希望する者であり、

前記共有パラメータが、前記機器識別子と関連付けられる、

方法。

【発明の詳細な説明】

【技術分野】

【０００１】

本願の実施例は、例えば、信頼できる機器に限定した認証に関する。

【背景技術】

【０００２】
[0001]典型的なユーザー認証機構では、ユーザーが、保護されたリソース（例えばインターネットを介してアクセスされるサーバー）へのアクセスを試みると、ユーザー名とパスワードを検証すること等により、ユーザーの資格情報が正しいことを確認する。しかし、そのような従来型の認証機構を使用すると、ユーザー名とパスワードが悪意ある者によって盗まれた場合、その者は、任意の機器を通じて世界のどこからでもユーザーのアカウントにアクセスすることができ、結果として望ましくないセキュリティ上の危険が生じる。

【発明の概要】
【発明が解決しようとする課題】
【０００３】
[0002]別の認証シナリオは、ユーザーがリモート機器へのログインを試みることを伴う。ユーザー認証機構でユーザーを認証することはできるが、そのリモート機器が実際に、ユーザーが期待する信頼できる機器であることを確かめることも関連する場合がある。例えば、ユーザーが、機密性のあるファイルをアップロードするためにリモートサーバーにログインしようとする場合がある。認証プロセスでユーザーの資格情報と機器の資格情報の両方を検証しない場合、ユーザーは、機密性のあるファイルを妥当でないサーバーにアップロードする可能性がある。アクセスしようとしている機器を間違えるという危険は、重大なセキュリティ上のリスクを招く。
【課題を解決するための手段】
【０００４】
[0003]本明細書に記載され、請求される実施は、機器の資格情報の検証をユーザーの資格情報の検証と組み合わせて、ユーザーにとって利便で、企業の境界を越えて有効である、より強固な認証機構を提供することにより、上述の問題に対処する。一実施では、ユーザーの資格情報の検証と機器の資格情報の検証が組み合わせられて、利便な２要素認証を提供する。一般に、ユーザーは、ユーザーの資格情報（例えばユーザー名とパスワード）を提供し、一方でユーザーの機器は、ユーザーと機器の両方に関連付けられた機器の資格情報を提供する。このようにすると、アカウント権限サービスまたは他の認証提供者は、両要素を検証し、ユーザーがアクセスしようとしているアカウントネットワークリソースのセキュリティポリシーに従ってセキュリティトークンを提供する。要求される要素が正しいことが確認されない場合、アカウント権限サービスは、別の要素（例えば指紋スキャン、網膜スキャン、ＨＩＰソリューション、秘密の質問等）による認証を要求することができる。対象のアカウントネットワークリソースによって付与される特権のレベルは、アカウント権限サービスで検証される要素の数および種類に応じて異なることができる。
【０００５】
[0004]一部の実施では、製造物品がコンピュータープログラム製品として提供される。コンピュータープログラム製品の一実装は、コンピューターシステムによる読み取りが可能で、コンピュータープログラムを符号化したコンピュータープログラム記憶媒体を提供する。コンピュータープログラム製品の別の実装は、コンピューティングシステムによって搬送波として具現化され、コンピュータープログラムを符号化したコンピューターデータ信号として提供されることができる。
【０００６】
[0005]この「課題を解決するための手段」は、以下の「発明を実施するための形態」でさらに説明される概念の一部を簡略化した形で紹介するために提供される。この「課題を解決するための手段」は、クレームに記載される主題の主要な機能または不可欠な機能を明らかにするものでも、クレームに記載される主題の範囲を限定することを意図するものでもない。
【図面の簡単な説明】
【０００７】
【図１】[0006]信頼できる機器に限定した認証を用いる例示的システムの図である。

【図２】[0007]信頼できる機器に限定した証明書を生成するための例示的動作および通信を示す図である。
【図３】[0008]信頼できる機器に限定した認証を使用してセキュアサーバーにアクセスするための例示的動作および通信を示す図である。
【図４】[0009] 信頼できる機器に限定した認証に基づいてリモート機器によるアクセスを提供する例示的システムの図である。
【図５】[0010]信頼できる機器に限定した認証に基づいてリモート機器によるアクセスを提供するための例示的動作および通信を示す図である。
【図６】[0011]本明細書に記載される技術を実施する際に有用である可能性がある例示的システムの図である。
【発明を実施するための形態】
【０００８】
[0012]図１に、信頼できる機器に限定した認証を用いる例示的システム１００を示す。ユーザーは、ユーザーアカウントを作成する際に、ユーザー機器１０２を操作して、通信ネットワーク１０８を介してアカウント権限サービス１０４と通信する。一実施では、ユーザーアカウントは、各種のネットワークサービスやリソース（「アカウントネットワークリソース」と総称する）にアクセスする際に使用されることができる。例えば、アカウント権限サービス１０４にアカウントを作成することにより、ユーザーは、１つの資格情報セットを設定することができ、その資格情報は、アカウントネットワーク内の電子メールサービス、予定表サービス、インスタントメッセージサービス、テキストメッセージサービス、ブログサービス、オンライン音楽サービス、写真共有サービス、各種の電子商取引サイト、各種のリモート機器等へのアクセスに使用されることができる。（用語「アカウントネットワーク」は、アカウント権限サービスとの間に信頼関係を有するアカウントネットワークリソースのネットワークを指す。）アカウント権限サービス１０４は、アカウントネットワーク内におけるユーザーアカウントの初期化および維持を管理する。アカウント権限サービス１０４は、それらアカウントネットワークリソース各々との間にも信頼関係を維持し、各アカウントネットワークリソースは、アカウント権限サービス１０４にから提供される識別の表現（例えばセキュリティトークン）に基づいてユーザーアクセスを許可する。一実施では、アカウント権限サービスは、使用条件、セキュリティポリシー等の契約上の同意、および、アカウント権限サービスと各アカウントネットワークリソースの間の通信を保護する暗号鍵の組合せに基づいて、アカウントネットワークリソースとの間に上記信頼関係を確立し、維持する。
【０００９】
[0013]例えばセキュリティトークンは、一意の秘密を使用して１つまたは複数のエンティティ（例えばユーザーおよび／または機器）の識別の証拠を提供する。セキュリティトークンを別のエンティティに提供することにより、提供側のエンティティは、自身の識別の証拠を与えていることになる。そのセキュリティトークンに基づいてあるレベルの特権を提供側エンティティに許可するかどうかを決定することは、受け取り側のエンティティに任される。さらに、セキュリティトークンは、有効期限がある場合があり、その期限後は信頼できなくなる。一実施では、セキュリティトークンは、コンピューティング機器がそのトークンを調査する（例えばセキュリティトークンがユーザー名および／または機器ＩＤを含んでいるかどうかを判定する）ことを可能にするＡＰＩ（アプリケーションプログラミングインタフェース）をサポートする。ユーザー名はユーザーＩＤの一例であり、他のユーザーＩＤが用いられてよいことは理解されたい。他の例には、電子メールアドレス、およびゲーマータグを含むエイリアスが含まれる。
【００１０】
[0014]一実施では、ユーザーは、ユーザー資格情報（例えばユーザー名およびユーザーパスワード）を提供してアカウントを作成するが、ユーザーアカウントの作成には他の情報の組合せも用いられてよい。アカウント情報は、アカウント権限サービス１０４からアクセス可能なデータリポジトリー１０６に格納される。例えば、アカウントレコードは、

データ項目の中でも特に、ユーザー名、パスワード、対応する機器パスワードを伴う１つまたは複数の機器ＩＤ、およびユーザーフレンドリーな機器名を含むことができる。ユーザーが自身のアカウントへのログインを試みると、アカウント権限サービス１０４は、ユーザーのアカウント情報を検索し、アカウント情報に格納された資格情報に照らしてユーザーの資格情報を検証する。例えば、アカウント権限サービス１０４は、提供されたユーザー名を使用してユーザーのアカウント情報を検索する。そして、アカウント権限サービス１０４は、ユーザーの資格情報（例えばユーザー名およびパスワード）を認証して、ユーザーのアカウントへのアクセスを許可する。

【００１１】

[0015]アカウントの作成時に提供される場合であっても、その後に提供される場合であっても、機器の資格情報（例えば機器識別子（ＩＤ）および機器パスワード）も、ユーザー機器１０２からアカウント権限サービス１０４に送信され、ユーザー資格情報と関連付けてアカウント情報として記憶されることができる。機器ＩＤとは、機器に対して生成されるグローバル一意の機器識別子である。機器ＩＤは、各種方法を使用して生成されることができる。一実施では、機器ＩＤは、機器ＩＤが別の機器ＩＤと衝突しないように、大きな値の集合を用いるグローバル一意識別子（ＧＵＩＤ）などの無作為に生成された数とすることができる。別の実施は、機器自体の固有の特徴を考慮することを含むことができる。例えばパーソナルコンピューター機器の場合は、ハードディスクとＢＩＯＳの組合せにより、機器ＩＤの生成に寄与するために使用することが可能な、一意で不変の何らかのパラメーターまたは特徴が得られる。一般には変化しない、オペレーティングシステム内のユーザー設定には、他の特徴が関連する可能性がある。そのような不変の特徴を用いると、機器ＩＤを実際の機器自体に近づけることができ、機器ＩＤがなりすましにくくなり、損失から回復するのが容易になる。

【００１２】

[0016]一実施では、ユーザーは、ユーザー機器１０２が信頼できる機器であることを指定し、ユーザー機器１０２で実行されるクライアントソフトウェアが機器ＩＤおよび機器パスワードを生成し、それをユーザー機器１０２が機器の資格情報としてアカウント権限サービス１０４に送信する。ユーザーは、ユーザー（および可能性としては他のユーザー）が将来ユーザー機器１０２を識別できるように、機器の資格情報と関連付けてユーザーフレンドリーな機器名も提供してよい。

【００１３】

[0017]一実施では、アカウント権限サービス１０４は、ユーザー名と関連付けて機器ＩＤをデータリポジトリー１０６に記録して、ユーザーとユーザー機器１０２との間に信頼関係を確立する。この処理を通じて、ユーザーは、ユーザー機器１０２が、アカウント権限サービス１０４と提携したアカウントネットワーク内で、自身の信頼できる機器の１つであることを宣言したことになる。ユーザーは同様の処理を通じて、複数の信頼できる機器を指定してもよいことを理解されたい。

【００１４】

[0018]さらに、ユーザーは、自分のアカウント中の自身の信頼できる機器のリストから機器を削除することもでき、これは、機器が盗まれ、ユーザーが盗まれた機器を通じた認証を阻止したい場合に有用である。例えば、ユーザーは、指定された機器ＩＤとの自身のユーザーＩＤの関連付けを解除する要求をアカウント権限サービス１０４に送信することができる。それに対して、アカウント権限サービス１０４は、ユーザーのアカウントから指定された機器の機器ＩＤを削除するか、または、ユーザーＩＤがもはや機器ＩＤと関連付けられないことを他の方法で指定することができる。この仕組みは、例えばユーザーが自分のコンピューターまたは携帯電話を更新する際に有用であることが考えられ、例えば、古い方のユーザー機器を通じた要求で「この機器を私の信頼できる機器のリストから削除する」ように指定することができる。ただし、状況によっては、ユーザーは、信頼できる機器リストから削除すべきユーザー機器をもはや持っていない場合もある（例えばユーザー機器が損傷、紛失、または盗まれた場合）。そのような状況では、ユーザーは、自分

の信頼できる機器のリストを要求することができ、機器はユーザーフレンドリーな機器名でリストされることができ、ユーザーはそのリストから削除する機器を選択することができる。あるいは、ユーザーは単にアカウント権限サービス１０４への削除要求でユーザーフレンドリーな機器名を提供することもできる。

【００１５】

[0019]一実施では、ユーザーがアカウント権限サービス１０４に自身のアカウントを作成していて、ユーザー機器１０２の機器ＩＤにユーザーが関連付けられている場合、ユーザーは、ユーザー機器１０２に関連付けられた機器証明書を要求することができる。一般に、機器証明書は、機器ＩＤに公開鍵をバインドするデジタル証明書である。機器証明書は、公開鍵が、その機器ＩＤで識別される機器に属することの証拠を提供する。例えば、ユーザーは、公開鍵と秘密鍵の対を生成し、対象機器の参照（例えばユーザーフレンドリーな機器名、機器ＩＤ等）と共に公開鍵をアカウント権限サービス１０４に送信することができる。公開鍵は、機器の資格情報および／またはユーザー資格情報と共に提出されて、証明書要求が信頼できる機器および／またはユーザーによってなされたことを保証する。公開鍵は、アカウントの作成と同時に、またはその後のいずれかの時に、アカウント権限サービス１０４に送信されることができる。アカウント権限サービス１０４は、公開鍵を使用して機器ＩＤを暗号化して機器証明書を作成し、自身の秘密鍵を使用して機器証明書に署名し、署名済みの機器証明書をユーザー機器１０２に送り返す。このトランザクションの結果、ユーザー機器１０２は、その機器が機器ＩＤで識別される機器であるという信頼できる証拠（例えば機器証明書）を所有することになる。

【００１６】

[0020]ユーザーが電子商取引サーバー１１０等のアカウントネットワークリソースへのアクセスを開始したいとき、ユーザーのブラウザーは、電子商取引サーバー１１０に移動することができ、電子商取引サーバー１１０は、ユーザーのブラウザーをアカウント権限サービス１０４にリダイレクトする。ユーザー機器１０２は、電子商取引サーバー１１０にアクセスするためのセキュリティトークンの要求で、ユーザー資格情報と機器証明書をアカウント権限サービス１０４に提供することができる。一実施では、セキュリティトークンは、ユーザー名および／または機器ＩＤを含むことができ、アカウントネットワークリソースは、ＡＰＩを通じてそれらユーザー名および／または機器ＩＤにアクセスすることができる。一実施では、アカウント権限サービス１０４は、ユーザー資格情報、機器証明書、および電子商取引サーバー１１０のセキュリティポリシーを評価して、電子商取引サーバー１１０にアクセスするためのセキュリティトークンをユーザー機器１０２に与えるかどうかを決定する。一般に、セキュリティポリシーは、セキュリティ保護された活動の条件としてサーバーが定義した事柄を定義する。セキュリティポリシーは、諸機能とそれらの間の流れの制約、外部システムおよびプログラムを含む敵対者によるアクセスの制約、およびユーザーによるデータへのアクセスの制約を扱う。別の実施では、アカウント権限サービス１０４は、ユーザー資格情報と機器資格情報の両方が認証されたかどうかも考慮に入れることができ、認証されていない場合は、アカウント権限サービス１０４はセキュリティトークンを保留してよい。この保留は、ネットワークサービスのセキュリティポリシーに従って行なわれるか、またはアカウント権限サービス自体によって決定されることができる。

【００１７】

[0021]ユーザー機器１０２がセキュリティトークンを受け取った場合、ユーザー機器１０２は、セキュリティトークンを電子商取引サーバー１１０に転送し、電子商取引サーバー１１０は、セキュリティトークンを評価した後に、決定されたレベルの特権下でユーザーのアクセスを許可する。ユーザーが電子商取引サーバー１１０へのアクセスを許された場合、その後ユーザー機器１０２と電子商取引サーバー１１０の間の通信は、サーバーのセキュリティポリシーとユーザーの特権レベルの条件下で行なわれることができる。

【００１８】

[0022]多要素認証（例えば２要素認証）は、単一要素認証より強いセキュリティを提供

することができる。一実施では、多要素は、ユーザー資格情報に加えて、信頼できる機器の資格情報を含むことができるが、他の要素の組合せも多要素認証で用いられることができる。ユーザーの名前とパスワードだけでは容易にフィッシングまたは盗取することが可能であるが、ユーザーがアカウントネットワークリソースにアクセスするために用いる物理的な信頼できる機器は、悪意のあるユーザーが入手し操作することがより難しいので、多要素証はより強い傾向がある。さらに、ユーザーの要素に加えて信頼できる機器の要素が認証されるかどうかに応じて、異なるセキュリティ上の決定がなされることができる。例えば、セキュリティポリシーは、未登録の機器からログインする試みがなされた場合はユーザーに通知すること、ユーザーのパスワードの変更は信頼できる機器を通じてのみ行なうよう要求すること、信頼できる機器の要素が認証されない場合は有効期限が短いセキュリティトークンを設定することなどができる。

【００１９】

[0023]一実施では、電子商取引サーバー１１０は、信頼できる機器の要素が認証されるかどうかに応じて、異なる特権レベルをユーザーに付与することができる。例えば、ユーザーの資格情報と機器の資格情報（例えば機器証明書で表される）の両方で認証を行なうユーザーには、追加的なストレージが与えられる、あるいは、ユーザー資格情報のみで認証するユーザーよりも人間対話型プロンプト（ＨＩＰ）または他のセキュリティプロンプトの回数を少なくすることができる。

【００２０】

[0024]ユーザーアカウントのセキュリティを強化するために、アカウント権限サービス１０４は、ユーザーがユーザー資格情報と信頼できる機器の機器資格情報の両方の検証を得ることができない場合には、ユーザー資格情報および／または機器資格情報を変更する試みを阻止することができる。実際には、この機能は、有効なユーザー名／パスワードを有するユーザーが、信頼できる機器を通じてアカウント権限サービス１０４にアクセスしていない場合は、アカウント権限サービス１０４を通じたユーザーアカウント情報の変更を行なえないようにすることができる。これに代えて、またはこれに加えて、ユーザーアカウント情報の変更を要求するユーザーがユーザー資格情報と信頼できる機器の機器資格情報両方の検証を得ることができなかった場合には、ユーザーアカウント情報を変更しようとする試みがユーザーに通知されることができる。

【００２１】

[0025]図２に、信頼できる機器に限定した証明書を生成するための例示的動作および通信（まとめて２００とする）を示す。この通信は、ユーザー機器と、アカウント権限サービスを運用するコンピューティングシステムとの間の、一般には通信ネットワークを通じて行なわれるデータ送信を表す。

【００２２】

[0026]一実施では、生成動作２０２で、ユーザー機器のクライアントソフトウェアが機器ＩＤおよび機器パスワード（「機器資格情報」）を生成し、両者はユーザー機器に関連付けられる。ユーザーは、機器ＩＤと関連付けてユーザーフレンドリーな機器名も提供することができる。送信動作２０４で、ユーザー機器は、ユーザー名／パスワードおよび機器ＩＤ／パスワード（および可能性としてはユーザーフレンドリーな機器名）を収集し、アカウントを作成する要求と関連付けてアカウント権限サービスに送信する。要求に応答して、作成動作２０６で、アカウント権限サービスはユーザーのアカウントを作成し、ユーザー名を機器ＩＤに関連付け、ユーザー名と機器ＩＤを、アカウント権限サービスからアクセス可能なデータストアーに記憶されたアカウント情報中に記録する。ユーザーパスワードと機器パスワードの両者もアカウント情報中に格納されることができ、典型的には暗号で保護される。

【００２３】

[0027]ユーザー名と機器ＩＤは、他の状況下でも関連付けできることを理解されたい。例えば、ユーザーのアカウントがすでに作成されており、ユーザーは、以前に作成されたアカウント内で関連付けるために後から機器資格情報を提供する場合がある。さらに、ユ

ーザー名は、複数の信頼できる機器ＩＤに関連付けられることができ、それらの関連付けがアカウント情報中に記録されることができる。

【００２４】

[0028]生成動作２０８で、ユーザー機器が公開鍵と秘密鍵の対を生成する。要求動作２１０で、ユーザー機器は、当該信頼できる機器に関連付けられた証明書を要求する。一実施では、ユーザー機器は、ユーザーフレンドリーな機器名および公開鍵をアカウント権限サービスに送信する。代替の実施では、ユーザー機器は、代わりにユーザー名／パスワードを送信して、要求が信頼できる機器からユーザーによって開始されたことを保証することができる。

【００２５】

[0029]生成動作２１２で、アカウント権限サービスは、機器ＩＤと公開鍵から機器証明書を作成し、次いで、アカウント権限サービスの秘密鍵を使用して証明書に署名して、ユーザー機器の公開鍵を機器ＩＤにバインドする。このようにすると、機器ＩＤがユーザー機器に属することを確認したいエンティティは、アカウント権限サービスの公開鍵を使用して証明書のデジタル署名を検証することにより、証明書を評価することができる。

【００２６】

[0030]一実施では、ユーザーは、複数の機器を「信頼できる」機器として指定することができる。したがって、信頼できる機器の各機器ＩＤが、ユーザーのユーザー名およびユーザーフレンドリーな名前と関連付けてアカウント情報中に記録される。このようにすると、ユーザーは、ユーザーフレンドリーな機器名を提供することにより、「信頼できる」機器として指定したい機器を識別する。機器証明書を要求する際、ユーザーはユーザーフレンドリーな機器名を提供することができ、アカウント権限サービスは、ユーザーのアカウントを見つけ、提供されたユーザーフレンドリーな機器名に対応する機器ＩＤを抽出することができる。アカウント権限サービスは次いで、機器ＩＤと公開鍵から機器証明書を作成し、自身の秘密鍵を使用して証明書に署名する。

【００２７】

[0031]アカウント権限サービスは、返却動作２１４で、生成した機器証明書をユーザー機器に返す。ユーザー機器は、受信動作２１６で機器証明書を受信する。ユーザー機器は、後に、その機器ＩＤで識別される機器である証明としてその機器証明書を使用することができる。

【００２８】

[0032]図３に、信頼できる機器に限定した認証を使用してセキュアサーバーにアクセスするための例示的な動作および通信（まとめて３００とする）を示す。この例では、ユーザーが自分のユーザー機器からセキュアサーバーにアクセスしたいと想定する。セキュアサーバーは、アカウント権限サーバーと信頼関係にあり、ユーザーおよび機器の認証をアカウント権限サーバーに依存する。この信頼関係の中で、アカウント権限サービスは、セキュアサーバーのセキュリティポリシーの知識を有し、セキュアサーバーへのアクセスのためにユーザーおよび／または機器を認証するように要求された際はそのポリシーを施行する。ユーザーがユーザー資格情報と機器資格情報の両方を提供するか、またはユーザー資格情報のみを提供するかに応じて、セキュアサーバーにアクセスするためにアカウント権限サービスからユーザーに付与される特権レベルは異なってよい。例えば、ユーザー資格情報と機器資格情報両方による認証では、アカウント権限サービスは、ユーザー資格情報だけによる認証の場合よりも高いレベルの特権をユーザーに付与する場合がある。

【００２９】

[0033]図の流れでは、ユーザーは、要求動作３０２でセキュアサーバーへのアクセスを要求する（例えばブラウザーをセキュアサーバーによって提供されるウェブページに移動することによる）。セキュアサーバー機器は、ユーザーがまだアカウント権限サービスによってアクセスの認証を受けていない（例えばユーザーのアクセス要求が、セキュアサーバーにアクセスするためのセキュリティトークンを含んでいなかった）ことを検出し、したがって、リダイレクト動作３０４で、認証のためにユーザーをアカウント権限サービス

にリダイレクトする。

【００３０】

[0034]アカウント権限サービスは、受信動作３０６で、リダイレクトされた要求（要求をリダイレクトしたセキュアサーバーの識別を含む）を受け取る。アカウント権限サービスにおける指示動作３０８では、ユーザーに資格情報を要求する。ユーザー機器は、受信動作３１０で指示を受け取り、送信動作３１２で資格情報を送出する。ユーザーは、自分のユーザー資格情報（例えばユーザー名およびパスワード）を送出することができ、これは一般的である。代替のシナリオでは、ユーザー機器は、機器証明書（または機器ＩＤと機器パスワード）も提出することができ、それにより認証のために２つの要素を提供する。

【００３１】

[0035]アカウント権限サービスとセキュアサーバーの間の信頼関係の一部として、アカウント権限サービスは、セキュアサーバーのセキュリティポリシーを知っている。したがって、アカウント権限サービスは、ユーザー機器から資格情報を受け取ると、その資格情報を認証し、資格情報がセキュアサーバーのセキュリティ要件を満たす場合（判定動作３１４で判定される）、アカウント権限サービスは、動作３２０でユーザー機器にセキュリティトークンを送信する。

【００３２】

[0036]ユーザー機器から供給された資格情報がセキュアサーバーのセキュリティ要件を満たさない場合、アカウント権限サービス３１６は、ユーザー機器に追加の資格情報を求めることができる。例えば、セキュアサーバーがユーザー資格情報と機器資格情報の両方等の２要素認証を要求する場合、アカウント権限サーバーは、信頼できる機器を介した認証をユーザーに要求することができる。あるいは、機器ＩＤ要素が満たされない場合は、セキュアサーバーは、ＨＩＰソリューションや秘密の質問の回答（例えば「母親の旧姓」）等の代替の第２の要素を受け付けることもできる。

【００３３】

[0037]他のシナリオでは、要求される数の要素が満たされない場合は、アカウント権限サービスによって付与される認証を何らかの形で縮小することができる。例えば、アカウント権限サービスは、第２の要素の認証が達成されない場合には、より早く期限が切れるセキュリティトークンを提供することができる。

【００３４】

[0038]ユーザー機器は、受信動作３２２でセキュリティトークンを受け取り、送信動作３２４でセキュアサーバーに転送する。付与動作３２６で、セキュアサーバーは、セキュリティトークンを調べて、アカウント権限サービスで行なわれた認証に基づいて、ユーザー／機器に許可する権限のレベルを決定する。一実施では、セキュアサーバーは、セキュリティトークンを調べて、アカウント権限サービスによる認証でユーザー資格情報と機器資格情報の両方が含まれていたかどうかを判定する。両方が含まれていた場合は、セキュアサーバーは、ユーザー機器を介して、より高いレベルの特権をユーザーに与えることができる。そうでない場合は、セキュアサーバーは、より低いレベルの特権をユーザーに与えるか、アクセスを一切許可しない。

【００３５】

[0039]図４に、信頼できる機器に限定した認証に基づいてリモート機器によるアクセスを提供する例示的システム４００を示す。ユーザーは、ユーザーアカウントを作成する際、ユーザー機器４０２を操作して、通信ネットワーク４０８を介してアカウント権限サービス４０４と通信する。一実施では、ユーザーアカウントは、各種のアカウントネットワークリソースにアクセスするために使用することができる。例えば、アカウント権限サービス４０４にアカウントを作成することにより、ユーザー機器４０２を操作するユーザーは、リモートユーザー機器４１２を介するリモートユーザー等、他のユーザーと共有してもよい、信頼できる機器のリストを公開することができる。アカウント権限サービス４０４は、アカウントネットワーク内のユーザーアカウントの初期化と維持を管理する。アカ

ウント権限サービス４０４は、ユーザー、ユーザー機器、およびアカウントネットワークに結合された他のユーザーおよび機器との間にも信頼関係を維持する。

【００３６】

[0040]一実施では、ユーザーは、ユーザー資格情報（例えばユーザー名およびユーザーパスワード）を提供してアカウントを作成するが、ユーザーアカウントの作成には他の情報の組合せも用いられることができる。アカウント情報は、アカウント権限サービス４０４からのアクセスが可能なデータリポジトリー４０６に格納される。ユーザーが自分のアカウントへのログインを試みると、アカウント権限サービス４０４は、ユーザーアカウント情報を検索し、提供されたユーザー資格情報をアカウント情報に格納された資格情報に照らして検証する。

【００３７】

[0041] アカウントの作成時に提供される場合であっても、またはその後提供される場合であっても、機器の資格情報（例えば機器識別子（ＩＤ）および機器パスワード）も、ユーザー機器４０２からアカウント権限サービス４０４に送信され、ユーザー資格情報と関連付けてアカウント情報として記憶されることができる。一実施では、ユーザーは、ユーザー機器４０２が信頼できる機器であることを指定し、ユーザー機器４０２で実行されるクライアントソフトウェアが機器ＩＤおよび機器パスワードを生成し、それをユーザー機器４０２が機器資格情報としてアカウント権限サービス４０４に送信する。ユーザーは、ユーザー自身（および可能性としては他のユーザー）が将来ユーザー機器４０２を識別できるように、ユーザーフレンドリーな機器名も提供してよい。

【００３８】

[0042]ユーザーは、機器共有命令を公開することにより、ユーザー機器４０２が別のリモートユーザーからアクセス可能であることも指定することができる。一実施では、ユーザーは、ユーザー機器４０２を他のユーザーからアクセス可能な機器として識別する共有パラメーターを、自身のアカウント情報中に設定する。別の実施では、ユーザーは、自身が機器を共有したいリモートユーザーとその際の特権レベルを共有パラメーターとして指定することもできる。共有パラメーターは、機器ＩＤに関連付けられ、アカウント権限サービス４０２は、機器ＩＤをユーザー機器４０４から受け取る。アカウント権限サービス４０４は、証明書に共有パラメーターを追加し、証明書に署名してからユーザー機器４０２に送り返すこともできる。

【００３９】

[0043]一実施では、アカウント権限サービス４０４は、機器ＩＤおよび共有パラメーターをユーザー名と関連付けてデータリポジトリー４０６に記録して、ユーザーとユーザー機器４０２との間に信頼関係を確立する。この処理を通じて、ユーザーは、ユーザー機器４０２が、アカウント権限サービス４０４と提携したアカウントネットワーク内で、自身の信頼できる機器の１つであることを宣言したことになる。

【００４０】

[0044]一実施では、ユーザーがアカウント権限サービス４０４に自身のアカウントを作成しており、ユーザーがユーザー機器４０２の機器ＩＤに関連付けられている場合、ユーザーは、ユーザー機器４０２に関連付けられた機器証明書を要求することができる。ユーザーは、公開鍵と秘密鍵の対を生成し、対象機器の参照（例えばユーザーフレンドリーな機器名、機器ＩＤ等）と共に公開鍵をアカウント権限サービス４０４に送信する。公開鍵は、アカウントの作成と併せて、またはその後のいずれかの時に、アカウント権限サービス４０４に送信されることができる。アカウント権限サービス４０４は、公開鍵を使用して機器ＩＤを暗号化して機器証明書を作成し、機器証明書をユーザー機器４０２に送り返す。このトランザクションの結果、ユーザー機器４０２は、その機器ＩＤで識別される機器であることの信頼できる証拠（例えば機器証明書）を所有することになる。

【００４１】

[0045]別のリモートユーザーがリモートユーザー機器４１２を通じてユーザー機器４０２に接続することを試みる際、リモートユーザー機器４１２は、アカウント権限サービス

４０４に、第１のユーザー（例えば第１のユーザーの電子メールアドレス、ゲーマータグ、ユーザー名等で識別される）に関連付けられた共有可能な機器のリストを要求する。アカウント権限サービス４０４は、第１のユーザーのアカウント情報を検索し、ユーザーの機器のうちどの機器が共有可能な機器として公開されているか、および要求側のリモートユーザーがその機器を共有する権限があるかどうかを判定する。リモートユーザーがそのような権限を有する場合、アカウント権限サービス４０４は、第１のユーザーに関連付けられ、リモートユーザーによる共有が可能な、共有可能機器のリストを返す。リモートユーザーは、共有可能機器の１つを選択し、その選択をアカウント権限サービス４０４に返すことができる。アカウント権限サービス４０４は、次いで、選択された機器の機器ＩＤをユーザーのアカウント情報から抽出し、その選択された機器の機器ＩＤをリモートユーザー機器４１２に返す。リモートユーザー機器４１２に返される情報は、ユーザー機器４０２の公開鍵およびＩＰアドレスを含むことができる。

【００４２】

[0046]選択した共有可能機器の機器ＩＤを信頼できるアカウント権限サービス４０４から取得すると、リモートユーザー機器４１２は、ユーザー機器４０２に接続することができる。一実施では、この接続は、ユーザー機器４０２のＩＰアドレスを用いて、ＴＣＰ／ＩＰ等の標準的なネットワークプロトコルを通じて実現される。リモートユーザー機器４１２がユーザー機器４０２との接続を達成すると、リモートユーザー機器４１２は、ユーザー機器４０２に機器証明書を要求し、アカウント権限サービス４０４で行なわれた署名を検証する。（このようにして、リモートユーザー機器４１２はユーザー機器４０２の公開鍵を得ることができる。リモートユーザー機器４１２は、アカウント権限サービス４０４からユーザー機器４０２の公開鍵も得ることができる。）

[0047]リモートユーザー機器４１２は、ユーザー機器４０２の公開鍵に一致する秘密鍵を提供するようにユーザー機器４０２に要求する。提供の方法は、ＳＳＬ等の標準的なプロトコルを通じて達成されることができるが、他の方法も用いられてよい。一実施では、ユーザー機器４０２は、リモートユーザー機器４１２とのネットワークチャレンジ／レスポンスハンドシェイクを行ない、その結果、ユーザー機器４０２が何らかのデータを自身の秘密鍵で署名および／または暗号化することになる。リモートユーザー機器４１２は次いで、ユーザー機器４０２の公開鍵を使用してそのデータを検証することができる。ユーザー機器４０２が真に秘密鍵を所有することを確認することにより、リモートユーザー機器４１２は、自身が接続しようとした機器に接続されたことを確認し、したがって双方の機器は安全に通信を続けることができる。検証が不合格の場合は、リモートユーザー機器４１２は、妥当でない機器に情報を提供する前、またはアクセス権を付与する前に、接続を切断することができる。

【００４３】

[0048]一実施では、ユーザー機器４０２は、リモートユーザー機器４１２の識別を確かめることができるように、リモートユーザー機器４１２がアカウント権限サービス４０４から受け取った機器４１２のセキュリティトークンを送信することも要求することができる。セキュリティトークンは、証明書形式の公開鍵と秘密鍵の対であってもよく、その場合機器４０２は、署名を検証し、リモートユーザー機器４１２によって秘密鍵が所有されている証明を取得する同様の処理を経る。

【００４４】

[0049]図５に、信頼できる機器に限定した認証に基づいてリモート機器によるアクセスを提供するための例示的動作および通信（まとめて５００とする）を示す。発見要求動作５０２で、リモートユーザーは、（リモートユーザー機器を介して）アカウント権限サービスに、別のユーザーに関連付けられた共有可能機器のリストを要求し、ユーザーの電子メールアドレス、ゲーマータグ、ユーザー名等のユーザー識別子を使用してユーザーを指定する。リスト発見動作５０４で、アカウント権限サービスは、要求を受け取り、指定されたユーザーのアカウントにアクセスして、指定されたユーザーに関連付けられた共有可能機器のリストを取得する。アカウント権限サービスは、指定されたユーザーによって提

出された機器名（通例はユーザーフレンドリーな機器名）を収集してリストにまとめ、そのリストを送信動作５０６でリモートユーザー機器に送り返す。

【００４５】

[0050]リモートユーザーは、選択動作５０８で、共有可能機器のリストを閲覧し、対象となる機器を選択することができる。送信動作５１０で、リモートユーザー機器は、共有可能機器の選択をアカウント権限サービスに返す。アカウント権限サービスは、抽出動作５１２で、相手のユーザーのアカウント情報にアクセスして、選択された機器の機器ＩＤを抽出し、送信動作５１４でリモートユーザー機器に返す。リモートユーザー機器は、受信動作５１６で機器ＩＤを受け取る。

【００４６】

[0051]リモートユーザー機器は、接続動作５１８で、選択した機器に接続する。前述のように、この接続は、ＴＣＰ／ＩＰなどの標準的なネットワークプロトコルを通じて得ることができるが、他の方法も用いられてよい。共有可能なユーザー機器は、接続動作５２０で接続を受け付け、このことは、そのユーザー機器の秘密鍵を所有していることの証明にもなる。リモートユーザー機器は、秘密鍵の所持の主張（例えば機器証明書）を受け取り、ユーザー機器の秘密鍵がその秘密鍵の所持の主張で使用されたことを確認する。この検証機構は、秘密鍵／公開鍵の対に基づいて（例えばＳＳＬを介して）実装されることができる。リモートユーザー機器は、機器証明書のアカウント権限の署名を確認してもよい。

【００４７】

[0052]リモートユーザー機器が機器ＩＤを介して共有可能ユーザー機器の識別を確認することができる場合、リモートユーザー機器は、自身が接続された機器が、共有可能機器のリストから選択した機器であることを保証される。そのため、リモートユーザー機器と共有可能ユーザー機器は、動作５２６および５２８で対話することができる。リモートユーザー機器が、共有可能ユーザー機器の識別を、接続しようとした機器として確認することができない場合は、接続を終了してセキュリティ違反の可能性を低下させることができる。

【００４８】

[0053]本発明を実施するための図６の例示的なハードウェアおよび動作環境は、ゲーム機本体またはコンピューター２０、携帯電話、携帯情報端末（ＰＤＡ）、セットトップボックスの形態の汎用コンピューティング機器、または他の種類のコンピューティング機器を含む。図６の実施では、例えば、コンピューター２０は、処理装置２１、システムメモリー２２、および、システムメモリーを含む各種システム構成要素を処理装置２１に動作的に結合するシステムバス２３を備える。処理装置２１は、１つのみの場合も、２つ以上存在する場合もあり、コンピューター２０のプロセッサーは、単一の中央演算処理装置（ＣＰＵ）からなるか、または、一般に並列処理環境と呼ばれる、複数の処理装置からなる。コンピューター２０は、従来型のコンピューターでも、分散コンピューターでも、他の種類のコンピューターでもよい。本発明は、この点で限定されない。

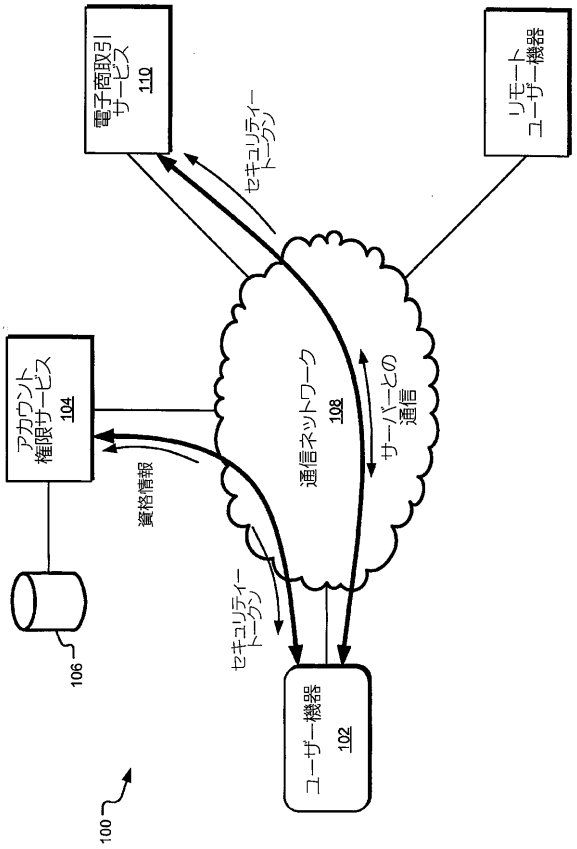
【００４９】

[0054]システムバス２３は、各種のバスアーキテクチャーを使用した、メモリーバスまたはメモリーコントローラー、ペリフェラルバス、スイッチファブリック、２地点間接続、およびローカルバスを含む、数種のバス構造のいずれでもよい。システムメモリーは、単にメモリーと呼ばれる場合もあり、読み取り専用メモリー（ＲＯＭ）２４およびランダムアクセスメモリー（ＲＡＭ）２５を含む。起動時等にコンピューター２０内の要素間の情報転送を助ける基本ルーチンを含んだ基本入出力システム（ＢＩＯＳ）２６は、ＲＯＭ２４に記憶される。コンピューター２０はさらに、図示しないハードディスクの読み書きを行なうハードディスクドライブ２７、取り外し可能磁気ディスク２９の読み取りまたは書き込みを行なう磁気ディスクドライブ２８、および、ＣＤ－ＲＯＭや他の光学媒体等の取り外し可能光ディスク３１の読み取りまたは書き込みを行なう光ディスクドライブ３０を備える。

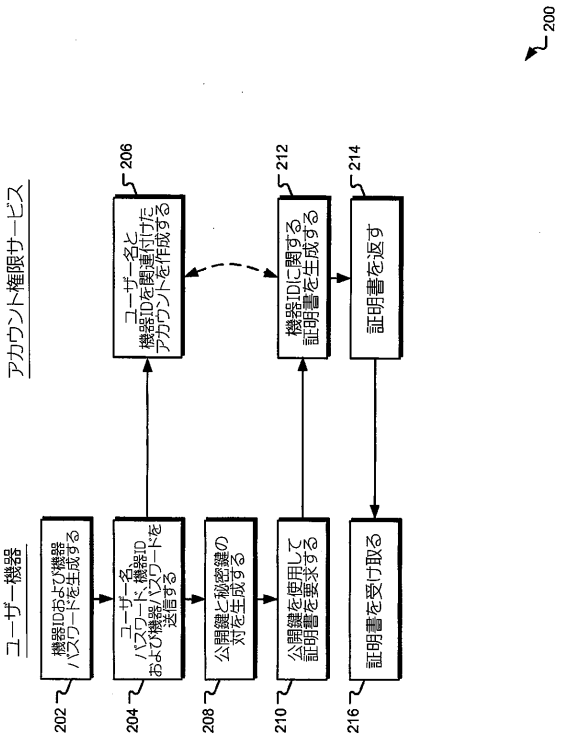
【００５０】
[0055]ハードディスクドライブ２７、磁気ディスクドライブ２８、および光ディスクドライブ３０は、それぞれ、ハードディスクドライブインタフェース３２、磁気ディスクドライブインタフェース３３、光ディスクドライブインタフェース３４でシステムバス２３に接続される。これらのドライブとそれに関連するコンピューター可読媒体は、コンピューター２０のコンピューター可読命令、データ構造、プログラムモジュール、および他のデータの不揮発性の記憶を提供する。当業者には、磁気カセット、フラッシュメモリーカード、デジタルビデオディスク、ランダムアクセスメモリー（ＲＡＭ）、読み取り専用メモリー（ＲＯＭ）等、コンピューターからアクセス可能なデータを記憶することができる任意の種類のコンピューター可読媒体が例示的動作環境で使用されてよいことが理解されよう。
【００５１】
[0056]ハードディスク、磁気ディスク２９、光ディスク３１、ＲＯＭ２４、またはＲＡＭ２５には複数のプログラムモジュールが記憶されることができ、それらのモジュールには、オペレーティングシステム３５、１つまたは複数のアプリケーションプログラム３６、他のプログラムモジュール３７、およびプログラムデータ３８が含まれる。ユーザーは、キーボード４０やポインティングデバイス４２等の入力装置を通じてコンピューター２０にコマンドおよび情報を入力することができる。他の入力装置（図示せず）には、マイクロフォン、ジョイスティック、ゲームパッド、衛星受信アンテナ、スキャナー等が含まれる。上記および他の入力装置は、多くの場合、システムバスに結合されたシリアルポートインタフェース４６を通じて処理装置２１に接続されるが、パラレルポート、ゲームポート、またはユニバーサルシリアルバス（ＵＳＢ）等の他のインタフェースで接続されることも可能である。モニター４７または他の種の表示装置も、ビデオアダプター４８等の表示インタフェースを介してシステムバス２３に接続される。モニターに加えて、コンピューターは通例、スピーカーやプリンター等の他の周辺出力装置（図示せず）を備える。
【００５２】
[0057]コンピューター２０は、リモートコンピューター４９等の１つまたは複数のリモートコンピューターとの論理接続を使用するネットワーク環境で動作することができる。これらの論理接続は、コンピューター２０に結合された、またはコンピューター２０の一部である通信装置によって達成されるが、本発明は、特定の種類の通信装置に限定されない。リモートコンピューター４９は、別のコンピューター、サーバー、ルーター、ネットワークＰＣ、クライアント、ピアデバイス、または他の一般的なネットワークノードであり、図６にはメモリー記憶装置５０のみを図示するが、通例は、上記でコンピューター２０に関して述べた要素の多くまたは全てを備える。図６に示す論理接続は、ローカルエリアネットワーク（ＬＡＮ）５１およびワイドエリアネットワーク（ＷＡＮ）５２を含む。このようなネットワーク環境は、オフィス内ネットワーク、企業規模のコンピューターネットワーク、イントラネット、およびインターネットに一般的に見られ、これらは全て、ネットワークの種類である。
【００５３】
[0058]ＬＡＮネットワーク環境で使用される場合、コンピューター２０は、ネットワークインタフェースまたはアダプター５３を通じてローカルネットワーク５１に接続される。アダプター５３は、通信装置の一種である。ＷＡＮネットワーク環境で使用される場合、コンピューター２０は通例、モデム５４、ネットワークアダプター、ある種の通信装置、またはワイドエリアネットワーク５２上に通信を確立するための他の種類の通信装置を備える。モデム５４は、内蔵される場合も外付け型の場合もあり、シリアルポートインタフェース４６を介してシステムバス２３に接続される。ネットワーク環境では、パーソナルコンピューター２０に関連して図示したプログラムモジュール、またはその一部は、リモートのメモリー記憶装置に記憶されることができる。図のネットワーク接続は例であり、コンピューター間に通信リンクを確立するための他の手段および装置が使用されてよいことが理解されよう。

【００５４】
[0059]例示的な実施では、アカウント権限サービスモジュールおよび他のモジュールは、メモリー２２および／または記憶装置２９もしくは３１に記憶され、処理装置２１で処理される命令によって実施されることができる。ユーザー名、パスワード、機器識別子、証明書、セキュリティトークン、および他のデータは、永続的なデータストアーとしてのメモリー２２および／または記憶装置２９または３１に記憶されることができる。
【００５５】
[0060]本明細書に記載される技術は、１つまたは複数のシステム内で論理動作および／またはモジュールとして実施される。論理動作は、１つまたは複数のコンピューターシステムで実行される、プロセッサー実施の一連のステップとして、および、１つまたは複数のコンピューターシステム内の相互接続されたマシンモジュールまたは回路モジュールとして実施される。同様に、各種構成要素モジュールの説明は、それらモジュールによって実行または実施される動作の点から提供されることができる。その結果得られる実施は、ここに記載される技術を実施する基礎システムの性能要件に応じて選択される事項である。したがって、本明細書に記載される技術の実施形態を構成する論理動作は、動作、ステップ、オブジェクト、またはモジュール等と、様々な呼び方がされる。さらに、論理動作は、明示的に要求されない限り、またはクレームの文言により特定の順序が本質的に必要とされない限りは、どのような順序で行なわれてもよいことを理解されたい。
【００５６】
[0061]上記の詳細な説明、例、およびデータは、本発明の例示的実施形態の構造および使用の完全な説明を提供する。本発明の各種実施形態についてある程度の詳細をもって、あるいは１つまたは複数の個々の実施形態を参照して上記で説明したが、当業者は、本発明の主旨または範囲から逸脱することなく、ここに開示される実施形態に多数の改変を行なうことができる。特に、ここに記載される技術はパーソナルコンピューターに依存せずに用いることが可能であることを理解されたい。したがって、他の実施形態が想定される。上記の説明に含まれ、添付図面に示される全ての内容は制限的なものではなく、単なる特定の実施形態の例示と解釈すべきことが意図される。以下の特許請求の範囲に定義される本発明の基本的要素から逸脱することなく詳細または構造の変更がなされることが可能である。
【００５７】
[0062]主題について構造的特徴および／または方法論的技術に固有の術語で説明したが、添付の特許請求の範囲に定義される主題は、必ずしも上記の具体的な特徴または動作に限定されないことを理解されたい。上記の具体的特徴および動作は、特許請求の範囲に記載される主題を実施する例示的形態として開示される。

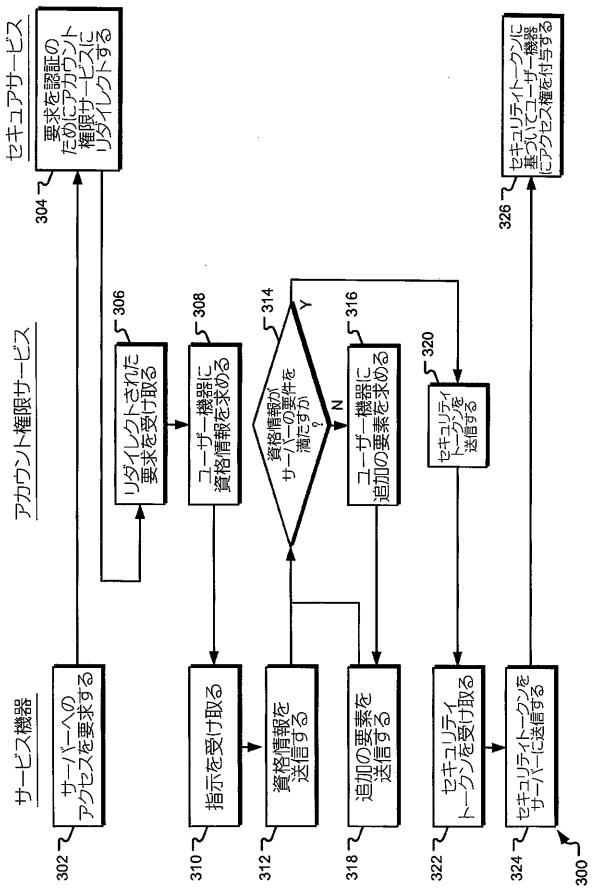
【図１】


電子商取引サービス 110
セキュリティートークン
リモートユーザー機器
アカウント権限サービス 104
通信ネットワーク 108
サーバーとの通信
資格情報
セキュリティートークン
106
ユーザー機器 102
100

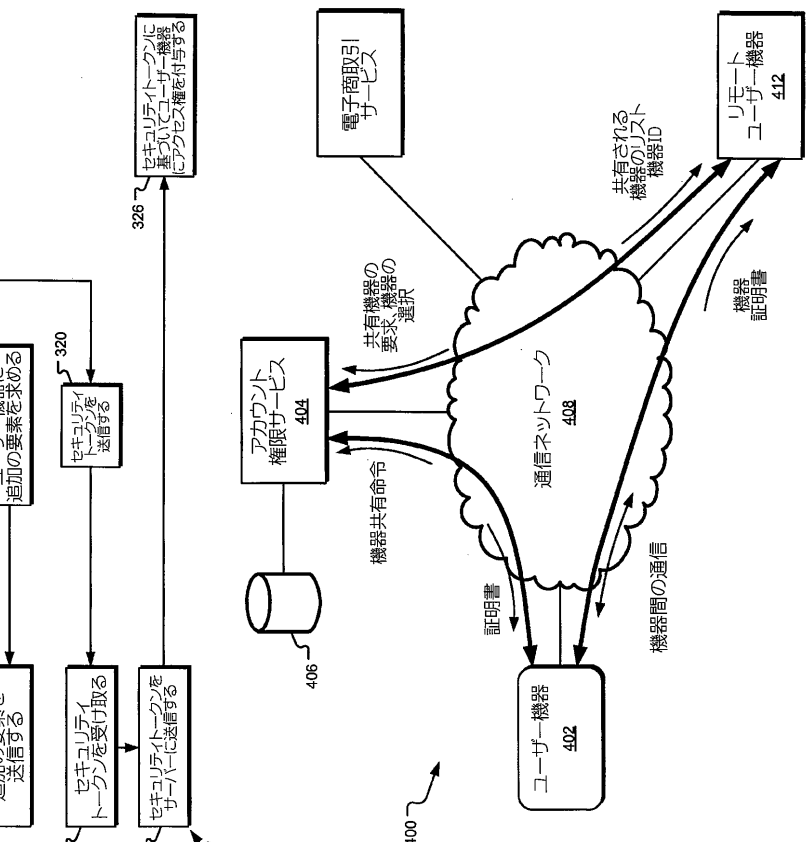
【図２】


200
アカウント権限サービス
ユーザー機器
機器IDおよび機器パスワードを生成する
ユーザー名、パスワード、機器IDおよび機器パスワードを送信する
公開鍵と秘密鍵の対を生成する
公開鍵を使用して証明書を要求する
証明書を受け取る
ユーザー名と機器ID関連付けたアカウントを作成する
機器IDに関する証明書を生成する
証明書を返す
202
204
206
208
210
212
214
216

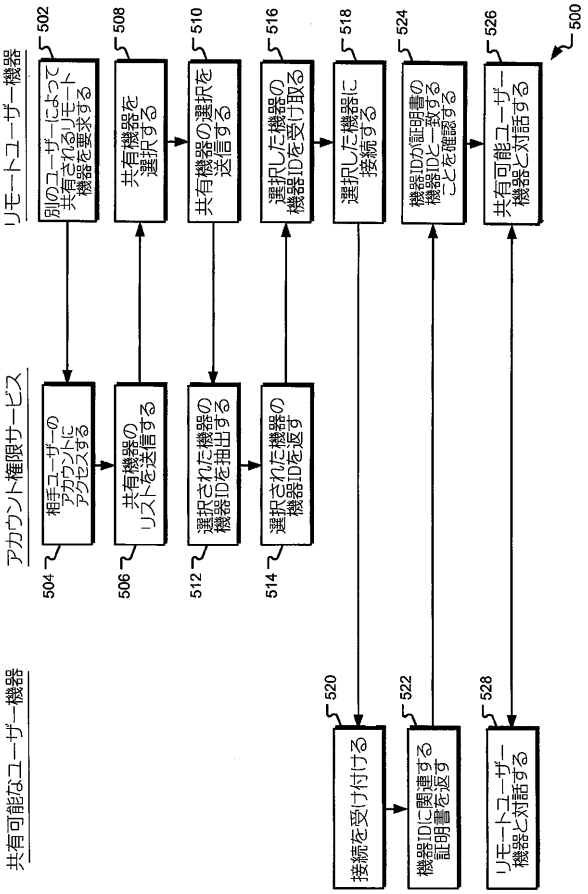
【図３】


セキュアサービス
アカウント権限サービス
サービス機器
要求を認証のためにアカウント権限サービスにリダイレクトする
リダイレクトされた要求を受け取る
ユーザー機器に資格情報を求める
資格情報がサーバーの要件を満たすか？
Y
N
ユーザー機器に追加の要素を求める
セキュリティートークンを送信する
セキュリティトークンに基づいてユーザー機器にアクセス権を付与する
サーバーへのアクセスを要求する
指示を受け取る
資格情報を送信する
追加の要素を送信する
セキュリティトークンを受け取る
セキュリティトークンをサーバーに送信する
302
304
306
308
310
312
314
316
318
320
322
324
326
300

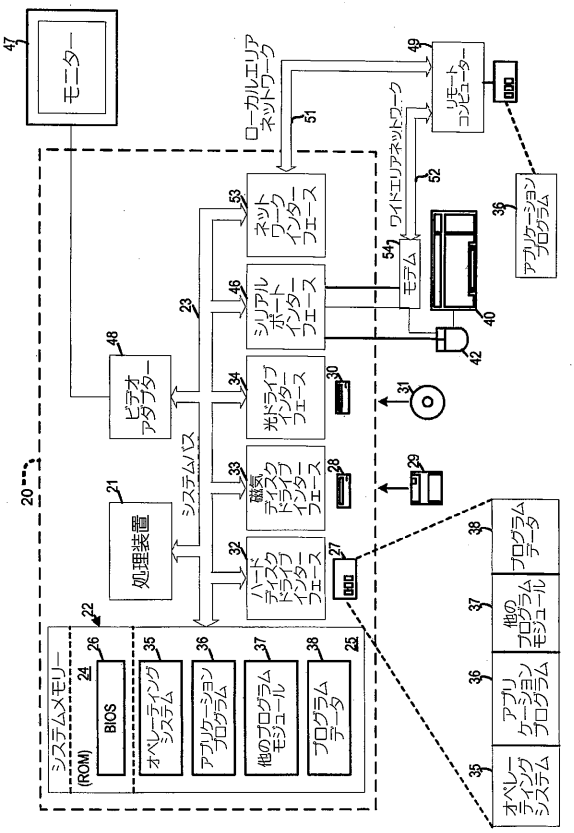
【図４】


電子商取引サービス
リモートユーザー機器 412
共有される機器のリスト機器ID
機器証明書
共有機器の要求、機器の選択
アカウント権限サービス 404
通信ネットワーク 408
機器共有命令
証明書
機器間の通信
406
ユーザー機器 402
400

【図５】


リモートユーザー機器
アカウント権限サービス
共有可能なユーザー機器
500
502 別のユーザーによって共有されるリモート機器を要求する
504 相手ユーザーのアカウントにアクセスする
506 共有機器のリストを送信する
508 共有機器を選択する
510 共有機器の選択を送信する
512 選択された機器の機器IDを抽出する
514 選択された機器の機器IDを返す
516 選択した機器の機器IDを受け取る
518 選択した機器に接続する
520 接続を受け付ける
522 機器IDに関連する証明書を返す
524 機器IDが証明書の機器IDと一致することを確認する
526 共有可能ユーザー機器と対話する
528 リモートユーザー機器と対話する

【図６】


モニター
ローカルエリアネットワーク
リモートコンピューター
ワイドエリアネットワーク
モデム
ネットワークインターフェース
シリアルポートインターフェース
ビデオアダプター
光ドライブインターフェース
磁気ディスクドライブインターフェース
ハードディスクドライブインターフェース
システムバス
処理装置
システムメモリー
(ROM)
BIOS
オペレーティングシステム
アプリケーションプログラム
他のプログラムモジュール
プログラムデータ
オペレーティングシステム
アプリケーションプログラム
他のプログラムモジュール
プログラムデータ

フロントページの続き

(72)発明者　グオ，ウエイ－チアーン（マイケル）
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，マイクロソフト　コーポレーション，エルシーエイ－インターナショナル・パテンツ
(72)発明者　ロウスコン，ヨルダン
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，マイクロソフト　コーポレーション，エルシーエイ－インターナショナル・パテンツ
(72)発明者　チェン，ゥルイ
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，マイクロソフト　コーポレーション，エルシーエイ－インターナショナル・パテンツ
(72)発明者　ウォン，プイ－イン・ウィンフレッド
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，マイクロソフト　コーポレーション，エルシーエイ－インターナショナル・パテンツ

審査官　平井　誠

(56)参考文献　特開２００４－２５８８４７（ＪＰ，Ａ）
特開平１０－２６０９３９（ＪＰ，Ａ）
特開２００５－３２３０７０（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
G06F　21/20
H04L　9/32