(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2009-123207
(P2009-123207A)
(43)公開日　平成21年6月4日(2009.6.4)

(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)	H04L	9/00	673A	5J104

審査請求 未請求　請求項の数 10　ＯＬ　（全 14 頁）

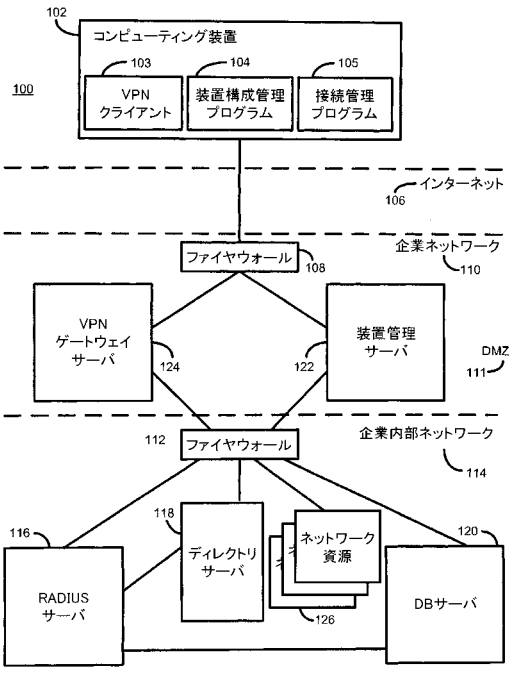
(21)出願番号　特願2008-285370 (P2008-285370)
(22)出願日　平成20年11月6日 (2008.11.6)
(31)優先権主張番号　07301555.4
(32)優先日　平成19年11月16日 (2007.11.16)
(33)優先権主張国　欧州特許庁 (EP)

(71)出願人　503003854
ヒューレット－パッカード　デベロップメント　カンパニー　エル．ピー．
アメリカ合衆国　テキサス州　７７０７０　ヒューストン　コンパック　センタ　ドライブ　ウエスト　１１４４５
(74)代理人　110000039
特許業務法人アイ・ピー・エス
(72)発明者　ブラウィ・サミル
フランス国３８０９０　ヴィルフォンテーヌ　ブールヴァール　スティーヴビコ　ヒューレット・パッカード・フランス内

最終頁に続く

(54)【発明の名称】ネットワークにアクセスする方法及び装置

(57)【要約】
【課題】ネットワークにアクセスする方法及び装置を提供する。
【解決手段】本発明に係る方法は、コンピューティング装置のネットワークへのアクセスを認証する方法であって、前記コンピューティング装置からユーザ識別子を含む認証データを受信することと、前記認証データの確認の許可が与えられているか否かを判断することと、前記認証データの確認の許可が与えられていると判断されるときに、前記認証データが確認されると、前記装置が前記ネットワークにアクセスするのを許可することとを含む。
【選択図】図１



【特許請求の範囲】
【請求項１】
コンピューティング装置のネットワークへのアクセスを認証する方法であって、
前記コンピューティング装置からユーザ識別子を含む認証データを受信することと、
前記認証データの確認の許可が与えられているか否かを判断することと、
前記認証データの確認の許可が与えられていると判断されるときに、前記認証データが確認されると、前記装置が前記ネットワークにアクセスするのを許可することと
を含む方法。
【請求項２】
前記認証データを受信する前に、
１つまたは複数のパラメータを受信することと、
受信された前記複数のパラメータのうちの少なくとも１つに対応するユーザ識別子をデータベースから取り出すことと、
取り出された前記ユーザ名に関連付けられる認証データの確認の許可を与えることと
をさらに含む請求項１に記載の方法。
【請求項３】
前記コンピューティング装置又は異なるコンピューティング装置のいずれかから前記複数のパラメータを受信すること
をさらに含む請求項１に記載の方法。
【請求項４】
前記許可することは、前記確認の許可が与えられる所定の期間内に、受信される前記認証データが受信されたと判断される場合にのみ実行される
請求項１～３のいずれかに記載の方法。
【請求項５】
前記許可を与えることは、
取り出された前記ユーザ識別子に関連付けられるデータベースレコードを取り出すことと、
所定数の受信された前記複数のパラメータが、取り出された前記データベースレコード内の対応する値に一致するか否かを判断することと
をさらに含む請求項２～４のいずれかに記載の方法。
【請求項６】
公衆インターネットを通じてアクセス可能な第１のサーバにおいて前記複数のパラメータを受信することと、
プライベートネットワーク内の第２のサーバにおいて前記認証データを受信することと
に適応する請求項１～５のいずれかに記載の方法。
【請求項７】
コンピューティング装置において遠隔ネットワークにアクセスする方法であって、
前記装置の特徴に関連する複数のパラメータから成る所定のセットを取得することと、
収集された前記複数のパラメータを第１のサーバに送信することと、
認証データを第２のサーバに送信することと
を含む方法。
【請求項８】
前記複数のパラメータを送信することは、公衆インターネットを介してアクセス可能なサーバに前記複数のパラメータを送信することに適応し、
前記認証データを送信することは、
前記遠隔ネットワーク上のサーバに前記認証データを送信することと、
収集された前記複数のパラメータの送信に後続する所定の時間期間内に前記認証データを送信することと
に適応する
請求項７に記載の方法。

【請求項９】
請求項１～６のいずれかに従って動作可能な認証サーバ。
【請求項１０】
請求項７または８に従って動作可能なコンピューティング装置。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は包括的には、コンピュータネットワークにアクセスする方法及び装置に関する。
【背景技術】
【０００２】
コンピューティング装置が公衆インターネットを介して企業コンピュータネットワーク又は他のプライベートコンピュータネットワークに遠隔接続することを可能にすることが既知である。
企業ネットワークにアクセスすることができる者を制御するために、ＩＴ管理者は様々な安全政策及び安全システムを使用し、管理しているコンピュータネットワークに許可されていないユーザが遠隔アクセスすることを阻止するのに役立てている。
【０００３】
遠隔ユーザは概して、適切なユーザ認証手順の遂行に成功しなければ企業ネットワークに遠隔アクセスすることができない。妥当なレベルの確実性でユーザを認証することを可能にするために、デュアルファクタ認証がＩＴネットワークの管理者によって十分に検討される。
デュアルファクタ認証は一般的に、「持っている或るもの」（例えばスマートカード又はハードウェアのトークン生成器）及び「知っている或るもの」（例えばパスワード）という主要な概念に基づいている。
【０００４】
企業ネットワークへの遠隔接続は通常、安全な仮想プライベートネットワーク（ＶＰＮ）を介して行われ、これによって、ユーザの装置と企業ネットワークとの間の通信が適度に安全であることが保証される。
この際、例えば適切な暗号技術が使用されるが、ＨＴＴＰＳの使用のような他のアクセス技法を使用してもよい。
【０００５】
ＶＰＮを介してコンピューティング装置を遠隔ネットワークに接続するために、コンピューティング装置のユーザは通常、与えられる正確なパスワード（「知っている或るもの」）に応答して認証トークンを生成するハードウェア又はソフトウェアのトークン生成器（「持っている或るもの」）を有する。
幾つかのトークン生成器は、認証トークンの生成に使用される暗号データを含む、ＰＩＮによって保護されるスマートカードを受け取るように構成されている。
この場合、このスマートカードは、「持っている或るもの」のファクタとみなすことができる。
生成された認証トークンは、ユーザが認証されたと判断するネットワークベースの認証システムに送信される。
【０００６】
デュアルファクタ認証技術又はマルチファクタ認証技術は、高いレベルのユーザ認証を提供するが、ユーザにとっては幾らか不便である。
例えば、ユーザは、ハードウェアのトークン生成器、スマートカード、又はそれらの両方を特定の構成に応じて別個に携帯しなければならない場合がある。
さらに、ＶＰＮを通じて接続することは通常、正確な順序で実行されなければならない多数の独立したステップを必要とする。
例えば、ユーザは、まず自身のオペレーティングシステムのユーザ名及びパスワードを

使用して自身のコンピュータをアンロックし、自身のスマートカードを自身のトークン生成器に挿入し、そのトークン生成器にパスワードを入力し、自身のＶＰＮクライアントアプリケーションを開き、生成された認証トークンをそのＶＰＮクライアントアプリケーションに手動で入力しなければならない場合がある。

【発明の開示】

【発明が解決しようとする課題】

【０００７】

したがって、本発明の１つの目的は、上記の問題のうちの少なくとも幾つかを克服、又は少なくとも軽減することである。

【課題を解決するための手段】

【０００８】

本発明の第１の態様によれば、コンピューティング装置のネットワークへのアクセスを認証する方法が提供される。

この方法は、コンピューティング装置からユーザ識別子を含む認証データを受信すること、認証データの確認の許可が与えられているか否かを判断すること、及び認証データの確認の許可が与えられていると判断される場合に、認証データが確認されると装置がネットワークにアクセスするのを許可することを含む。

【０００９】

本発明の第２の態様によれば、コンピューティング装置において遠隔ネットワークにアクセスする方法が提供される。

この方法は、装置の特徴に関連する複数のパラメータから成る所定のセットを取得すること、収集された複数のパラメータを第１のサーバに送信すること、及び認証データを第２のサーバに送信することを含む。

【００１０】

本発明の第３の態様によれば、上記方法ステップのうちの少なくとも幾つかに従って動作可能な認証サーバが提供される。

【００１１】

本発明の第４の態様によれば、上記方法ステップのうちの少なくとも幾つかに従って動作可能なコンピューティング装置が提供される。

【００１２】

次に、本発明の実施形態を、添付図面を参照して非限定的な例としてのみ説明する。

【発明を実施するための最良の形態】

【００１３】

図１は、本発明の一実施形態によるシステム１００の単純化されたブロック図を示す。

当業者は、明瞭にするために典型的なネットワークの全ての要素が示されていないことを理解するであろう。

【００１４】

コンピューティング装置１０２、例えば適切に備え付けられたパーソナルコンピュータ、ポータブルコンピュータ、携帯情報端末（ＰＤＡ）、携帯電話等は、適切な方法で公衆インターネット１０６に接続する。

このインターネットへの接続は、インターネットサービスプロバイダ（図示せず）を通じて行われ、ＩＳＰとの接続は任意の適切な方法、例えばＤＳＬ接続、無線ＬＡＮ接続、ＧＳＭベースのＧＰＲＳデータ接続等を通じて行われる。

【００１５】

企業ネットワーク１１０は、他の要素の中でも特に、遠隔認証ダイアルインユーザサービス（ＲＡＤＩＵＳ）サーバ１１６と、ディレクトリサーバ１１８と、データベースサーバ１２０と、ＶＰＮゲートウェイサーバ１２４と、装置管理サーバ１２２とを含む。

企業ネットワーク１１０は、一対のファイヤウォール１０８及び１１２と共に構成され、いわゆる非武装地帯（ＤＭＺ）１１１と安全な企業内部ネットワーク１１４とを形成する。

ＤＭＺ１１１内では、装置管理サーバ１２２及びＶＰＮゲートウェイサーバ１２４が配置され、これらの両方はインターネット１０６を通じて直接アクセス可能である。

【００１６】

当業者によく理解されるように、ＤＭＺ１１１内のネットワーク資源はインターネットを通じて直接アクセス可能であるが、企業内部ネットワーク１１４内のネットワーク資源は通常、認証に成功した遠隔ユーザのみがアクセス可能である。

【００１７】

コンピューティング装置１０２は、インターネット１０６に接続すると、この装置のユーザが適切に認証されることを条件として、企業内部ネットワーク１１４に遠隔接続することができ、その後企業内部ネットワーク１１４のネットワーク資源１２６にアクセスすることができる。

【００１８】

本実施形態では、コンピューティング装置１０２は、ＶＰＮクライアントアプリケーション１０３と、装置構成管理アプリケーション１０４と、接続管理アプリケーション１０５とをホストする。

【００１９】

装置構成管理プログラム１０４は、コンピューティング装置１０２から１つ又は複数の所定のパラメータを収集するように動作可能なソフトウェアアプリケーションである。

本明細書で使用される「パラメータ」という用語は、必要に応じて、パラメータ自体、パラメータの値、又はそれらの両方を指すものと理解される。

所定のパラメータは、物理的コンピューティング装置自体に関連することができ、例えば一意のハードウェア識別子（例えばこの装置が携帯電話である場合の、国際モバイル機器アイデンティティ、すなわちＩＭＥＩ）、ハードウェアシリアル番号、媒体アクセスコントローラ（ＭＡＣ）アドレス等である。

【００２０】

所定のパラメータは、コンピューティング装置１０２上の１つ又は複数のソフトウェアコンポーネントにも関連することができ、例えば装置構成管理アプリケーション１０４の一意の識別子（例えばＵＵＩＤ）、コンピューティング装置１０２上で実行されている又は当該装置にインストールされている他のソフトウェアアプリケーションの詳細（例えば、必要に応じて、それらのソフトウェアの名前、ＵＵＩＤ、バージョン番号等を含む）である。

【００２１】

企業内部ネットワーク１１４の管理者によって必要とされる安全レベルに応じて、装置構成管理プログラム１０４によって収集されるように構成されている所定のパラメータと、当該パラメータの収集される数とを変更することができる。

【００２２】

本実施形態では、コンピューティング装置１０２は適切には、携帯情報端末とＩＭＥＩを有する携帯電話との組み合わせである。

【００２３】

企業ネットワークの管理者によってコンピューティング装置１０２上で実行される初期構成プロセスの一部として、又は必要に応じて後に、企業ネットワーク１１０の管理者は、例えば構成管理プログラム１０４を通じて、コンピューティング装置１０２から１つ又は複数のパラメータを取得する。

取得されたパラメータは、ネットワーク管理者によって、この装置の指定されたユーザに与えられるユーザ名、又は他の適切なユーザ識別子に関連付けられる。

通常、指定されたユーザはこの装置の唯一の想定ユーザとなる。ユーザ名は例えばネットワークユーザ名とすることができる。

初期構成プロセス中、ＵＵＩＤを装置構成管理プログラム１０４に割り当てることができる。

【００２４】

取得されたパラメータ及びユーザ名は、このユーザ名を、これらのパラメータのうちの１つ又は複数を探索キーとして使用してデータベースを探索することによって取り出すことができるように、データベースサーバ１２０内に記憶される。

【００２５】

本実施形態では、装置構成管理プログラムは、コンピューティング装置１０２のＩＭＥＩと装置構成管理アプリケーション１０４のＵＵＩＤとを収集するように構成されている。

【００２６】

表１は以下において、例えばコンピューティング装置１０２が企業内部ネットワーク１１４の管理者によって構成されたときに取得された、データベースサーバ１２０に記憶される情報を示す。

【００２７】

【表１】

USER ID	vgiles
IMEI	35-209900-176148-1
UUID	550e8400-e29b-41d4-a716-446655440000

【００２８】

接続管理アプリケーション１０５は、コンピューティング装置１０２を企業内部ネットワーク１１４に接続するタスクを促進するソフトウェアアプリケーションである。

次に、コンピューティング装置１０２が企業内部ネットワーク１１４に接続する方法を、さらに図２、図３、及び図４を参照して説明する。

【００２９】

ユーザは適切な方法、例えば接続管理プログラムアイコンを「ダブルクリックすること」によって接続管理プログラム１０５を起動する。

起動時に、接続管理プログラム１０５は、コンピューティング装置１０２が現在インターネットに接続しているか否かを確認する。

インターネット接続が検出されない場合、接続管理プログラム１０５は、任意の適切な方法、例えば無線ＬＡＮ接続ポイントを通じてインターネット１０６への接続を確立するように試みることができるか、又は他の場合では、コンピューティング装置１０２のユーザに、コンピューティング装置１０２をインターネットに接続する方法を教えることができる。

【００３０】

インターネット接続が確認されると、接続管理プログラムは構成管理プログラム１０４から所定のパラメータを取得する（ステップ２０２）。

パラメータは、例えば、接続管理プログラム１０５による要求を受けて構成管理プログラム１０４が収集することができるか、又は代替的に、装置１０２が起動したときに、定期的に、若しくは他の任意の適切なときに収集することができ、後の取り出しのために記憶することができる。

【００３１】

ステップ２０４において、接続管理プログラム１０５は取得したパラメータを装置管理サーバ１２２に送信する。

パラメータは、任意の適切な方法、例えばＨＴＴＰ又はＨＴＴＰＳを使用して装置管理サーバ１２２に送信することができる。

さらなる一実施形態では、装置管理サーバ１２２は、取得されたパラメータの送信前に、適切に一致するユーザ名及びパスワードを提供するようにコンピューティング装置のユーザに要求することができる。

【００３２】

接続管理プログラム１０５は、装置管理サーバ１２２にパラメータを送信した後、ＶＰＮゲートウェイサーバ１２４との接続を確立するＶＰＮクライアントアプリケーション１０３を起動する。

ＶＰＮゲートウェイサーバ１２４は、ＶＰＮクライアントアプリケーション１０３を介して、コンピューティング装置のユーザに或る認証データを入力するように要求し、その後、当該認証データはＶＰＮゲートウェイサーバ１２４を通じてＲＡＤＩＵＳサーバ１１６に送信される。認証データは、例えばユーザのネットワークユーザ名、関連付けられているパスワード、アクセスコード等を含むことができる。

【００３３】

装置管理サーバ１２２は、パラメータを受信する（ステップ３０２）と、受信したパラメータのうちの１つ又は複数を探索キーとして使用してデータベースサーバ１２０の探索を実行する（ステップ３０４）。

本実施形態では、例えば、ステップ３０２において受信されたＵＵＩＤパラメータのみが探索キーとして使用されて、データベースサーバ１２０の探索が行われる。

そのＵＵＩＤを含むデータベースレコードが見つからない場合、さらなる動作は行われない（ステップ３０８）。データベースレコードが見つかった場合、そのデータベースレコードは取り出され（ステップ３０９）、当該データベースレコードからユーザ名が抽出される。ステップ３１０において、以下でさらに詳細に説明するように、抽出されたユーザ名に関連付けられる認証データの確認の許可が与えられる。

【００３４】

さらなる一実施形態では、認証データの確認の許可は、ステップ３０２において受信されたパラメータのうちの１つ又は複数が、取り出されたデータベースレコード内の対応するパラメータ値に一致する場合にのみ与えられる。

例えば、追加のチェックを行って、パラメータを送信したコンピューティング装置１０２のＩＭＥＩが、データベースレコードが作成されたときに使用されたＩＭＥＩと同じであるか否かを判断することができる。

このようにして、企業内部ネットワーク１１４の管理者はさらに、例えば所与の装置を使用する場合は所与のユーザのみがネットワークにアクセスするように要求することによって、或るユーザと対になっている或るコンピューティング装置にネットワーク１１４へのアクセスを制限することができる。

【００３５】

認証データの確認の許可は多数の方法で信号伝達することができる。

例えば、一実施形態では、許可がステップ３１０において与えられると、抽出されたユーザ名の詳細がＲＡＤＩＵＳサーバ１１６に送信される。

代替の一実施形態では、抽出されたユーザ名に許可が与えられたことを示すフラグが、データベースサーバ１２０内の抽出されたユーザ名の対応するデータベースレコード内に記憶される。

【００３６】

ＲＡＤＩＵＳサーバ１１６がステップ２０８において送信された認証データを受信する（ステップ４０２）と、認証データの確認の許可がステップ３１０において与えられたか否かを判断するチェックが行われる（ステップ４０４）。

許可されたユーザ名をＲＡＤＩＵＳサーバ１１６に送信することによって許可が与えられた実施形態では、ステップ４０２において認証データと共に受信されたユーザ名が装置管理サーバ１２２から受信されたユーザ名と同じであるか否かを判断するチェックが行われる。

データベースサーバ１２０内にフラグを設定することによって許可が与えられた実施形態では、ＲＡＤＩＵＳサーバは、許可のフラグが設定されたか否かを判断するために、ステップ４０２において受信されたユーザ名を使用してデータベースサーバ１２０を探索する。

認証データの確認の許可がステップ４０２において受信されたユーザ名に与えられてい

ないと判断された（ステップ４０４）場合は、ユーザ名の認証は失敗したとみなされ（ステップ４０６）、さらなる動作は行われない。

【００３７】

しかし、認証データの確認の許可が与えられたと判断された（ステップ４０４）場合は、ＲＡＤＩＵＳサーバは、ディレクトリサーバ１１８に、ステップ４０２において受信された認証データを確認する（ステップ４０８）ように要求する。

認証データの確認は、例えば受信されたユーザ名及びパスワードがディレクトリサーバ１１８に記憶されているユーザ名及びパスワードと一致するか否かを調べることのような適切な方法で実行することができる。

ディレクトリサーバが受信された認証データが認証されないと示す場合、ＲＡＤＩＵＳサーバ１１６は認証の試みを拒否する（ステップ４０６）。

他方、ディレクトリサーバ１１８が、認証データが認証されることを確認した（ステップ４０８）場合、コンピューティング装置１０２は、ディレクトリサーバ１１８において規定されたように、企業内部ネットワーク１１４のネットワーク資源１２６にアクセスすることを許可される。

当業者によく理解されるように、ＲＡＤＩＵＳサーバ１１６は、コンピューティング装置１０２のユーザを認証し、コンピューティング装置１０２が任意の適切な方法で企業内部ネットワーク１１４にアクセスすることを可能にする。

【００３８】

さらなる実施形態では、ステップ４０４におけるチェックは時間チェックを加えることによって拡張することができ、それによって、認証データの確認は、認証データの確認の許可が所定の時間期間内に与えられた場合にのみ実行される。

このような時間ベースのチェックは、例えば認証データの確認の許可と共にタイムスタンプデータを記録し、それによって、タイムスタンプデータが記録されてから経過した時間を計算することによって行うことができる。

【００３９】

所定のタイムアウト期間は任意の適切な値に設定することができ、所定のパラメータが装置管理サーバ１２２に提供されてから、コンピューティング装置１０２のユーザが自身のユーザ名及びパスワードを提供しなければならない適切な時間期間が与えられる。

時間期間は例えば３０秒～６０秒の間に適切に設定することができる。

より高い安全性が必要とされる場合、時間期間はより短く設定することができ、又は安全性をより緩めることが許可される場合、時間期間はより長く設定することができる。

【００４０】

別のさらなる実施形態では、装置管理サーバ１２２は、例えば公衆交換電話網（ＰＳＴＮ）若しくは公衆陸上移動網（ＰＬＭＮ）から、又はボイスオーバーＩＰ（ＶｏＩＰ）呼出のようなデータネットワークを介してアクセス可能な適切な音声アプリケーションに接続される。

上述した初期構成プロセスの一部として、又は必要に応じて後に、コンピューティング装置１０２又は当該コンピューティング装置のユーザのいずれかを識別するのに適切な識別子が、このユーザの割り当てられたユーザ名と共にデータベースサーバ１２０内に記憶される。

識別情報は、例えばコンピューティング装置１０２の発呼線識別番号（ＣＬＩＮ）、国際携帯電話加入者識別情報（ＩＭＳＩ）、ＳＩＰ　ＵＲＩ等とすることができる。

【００４１】

音声アプリケーションは、当該音声アプリケーションに対する呼出が行われたときに、発呼者の適切な識別情報を取得するように構成されている。

この実施形態では、コンピューティング装置１０２がＲＡＤＩＵＳサーバ１１６に接続する前に、ユーザが音声アプリケーションに関連付けられている電話番号に電話する。音声アプリケーションは、関連付けられている適切な発呼者識別情報を取得し、当該識別情報を装置管理サーバ１２２に渡す。

装置管理サーバ１２２は、上述したように、データベースサーバ１２０からユーザ名を取得するために、取得された識別情報を探索キーとして使用する。
音声アプリケーションが呼出を切ると、ユーザは、接続管理プログラムを通じて自身のユーザ名及びパスワードを入力し、当該ユーザ名及びパスワードは上述したようにＲＡＤＩＵＳサーバ１１６に送信される。
その後、ＲＡＤＩＵＳサーバ１１６は上述したようにユーザを認証することができる。
【００４２】
コンピューティング装置１０２は、例えば管理されているＩＴサービスの一部として、遠隔更新、例えばソフトウェアアプリケーション更新又はファームウェア更新を企業内部ネットワーク１１４から受信及びインストールすることができる場合がある。
この場合、後続の認証の試みのために、装置構成管理プログラム１０４によって取得されたパラメータがデータベースサーバ１２０内のパラメータと同期するように、コンピューティング装置１０２上で完了に成功したあらゆる更新の詳細もデータベースサーバ内に記録される。
【００４３】
装置管理サーバ１２２の機能は、ＲＡＤＩＵＳサーバ１１６と同じ場所に配置することができることを当業者は理解するであろう。
【００４４】
コンピューティング装置１０２が携帯電話であるか又は携帯電話として機能する場合、企業内部ネットワーク１１４は携帯電話ネットワークサービスプロバイダのネットワークから独立することができることにさらに留意されたい。
【００４５】
さらなる代替の一実施形態では、コンピューティング装置は、ファイヤウォール１１２を通じて、ＨＴＴＰＳのような安全な通信プロトコルを使用してネットワーク１１４に直接、すなわちＶＰＮを使用せずに接続することができる。ファイヤウォール１１２への最初の接続時、このファイヤウォールはＲＡＤＩＵＳサーバ１１６を通じてユーザを認証するように構成される。
ＲＡＤＩＵＳサーバ１１６は、上述したようにユーザを認証するように動作可能である。
【００４６】
ここで図５を参照すると、本発明のさらに別の実施形態のシステムのブロック図が示されている。図５のシステムは図１のシステムと共通の要素を有し、同様の参照符号は同様の要素を示す。
この実施形態では、ユーザは第１のコンピューティング装置５０２、例えばポータブルコンピュータ又はデスクトップコンピュータを有する。
当該コンピューティング装置を通じて、企業内部ネットワーク１１４へのアクセスは行われる。
ユーザは、第２のコンピューティング装置５０６、例えば携帯情報端末、スマートフォン等も有する。
ユーザは、第１のコンピューティング装置５０２を通じて企業内部ネットワーク１１４にアクセスすることを望む場合、第２の通信装置５０６上の接続管理プログラム５１０をまず起動する。
上述したように、接続管理プログラムは装置構成管理プログラム５０８から第２のコンピューティング装置５０６の複数のパラメータを取得し、これらのパラメータを装置管理サーバ１２２に送信する。
パラメータが第２のコンピューティング装置５０６から送信されると、ユーザは、例えば接続管理プログラム（図示せず）を通じてＶＰＮクライアントアプリケーション５０４を起動することができる。
当該ＶＰＮクライアントアプリケーションはユーザのユーザ名とパスワードとを要求する。ユーザの認証が上述したのと同じ方法で行われる。

第１のコンピューティング装置５０２及び第２のコンピューティング装置５０６の構成時にデータベースサーバ１２０内に最初に記憶されたパラメータは、適切には第２のコンピューティング装置５０６のパラメータであり、上述したようにユーザのユーザ名と関連付けられる。

このように、認証プロセス中に送信される認証データが、ネットワークへのアクセスを要求するコンピューティング装置以外の装置から来る。

【００４７】

上述の実施形態から明らかなように、本発明の実施形態は、簡単且つ安全な方法で、また企業ネットワーク１１４のユーザ及び管理者の両方に有利な方法で、コンピューティング装置のユーザが企業内部ネットワークに遠隔接続することを可能にする。

アクセス方法は必要に応じて単純化され、その最も単純な形態では、ユーザは、単に接続管理アプリケーション１０５を起動して、要求されたときに自身の通常のユーザ名とパスワードとを提供するだけである。

ユーザは、追加の又は別個のスマートカード又はハードウェア若しくはソフトウェアのトークン生成器を必要としない。

【００４８】

ネットワーク管理者は、ユーザがネットワークにアクセスするのを認証するためにデュアルファクタ認証が使用されるため満足する。

「知っているもの」のファクタはユーザのパスワードによって提供され、「持っているもの」のファクタは、コンピューティング装置１０２の特性であり、収集される１つ又は複数のパラメータによって提供され、接続管理プログラム１０５によって送信される。

さらに、装置構成管理プログラムがコンピューティング装置１０２の複数のパラメータを取得するように構成されている場合、単一の「持っているもの」のファクタよりも安全性を向上させることができる。

【００４９】

各遠隔ユーザに支給される別個のハードウェアのトークン発生器又はスマートカードを必要としないことによって、著しいコスト節約も達成することができる。

【００５０】

さらなる利点は、デュアル認証ファクタ、すなわち「持っているもの」のファクタ及び「知っているもの」のファクタの確認は、従来のデュアルファクタ認証手順におけるようにコンピューティング装置１０２上で局所的に実行されるのではなく、安全な企業内部ネットワークにおいて実行されるということである。

これは、コンピューティング装置１０２上の確認機構が危険に曝される可能性があるというリスクをさらに除去するため、安全性をさらに向上させるのに役立つ。

【００５１】

本発明の実施形態はハードウェア、ソフトウェア、又はハードウェアとソフトウェアとの組み合わせの形態において実現することができることが理解されるであろう。

任意のこのようなソフトウェアは、例えばＲＯＭのようなストレージ装置（消去可能か又は再書き込み可能か否かを問わない）のような揮発性若しくは不揮発性のストレージの形態で、又は例えばＲＡＭ、メモリチップ、装置、若しくは集積回路のようなメモリの形態で、又は例えばＣＤ、ＤＶＤ、磁気ディスク、若しくは磁気テープのような光学的若しくは磁気的に読み取り可能な媒体上に記憶することができる。

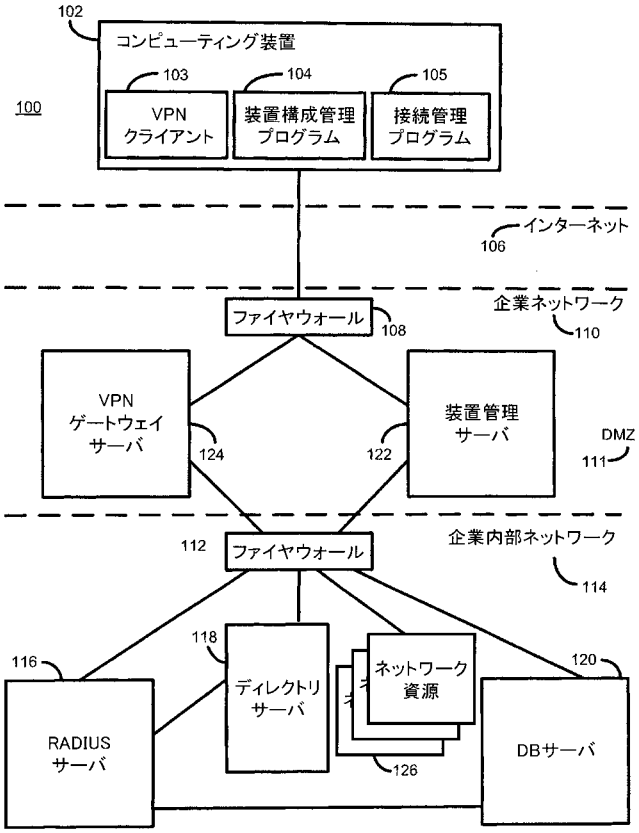
ストレージ装置及びストレージ媒体は、実行されたときに本発明の実施形態を実施する１つ又は複数のプログラムを記憶するのに適切な機械可読ストレージの実施形態であることが理解されるであろう。

したがって、実施形態は、任意の先行する請求項に記載のシステム又は方法を実施するためのコードを含むプログラムと、このようなプログラムを記憶する機械可読ストレージとを提供する。

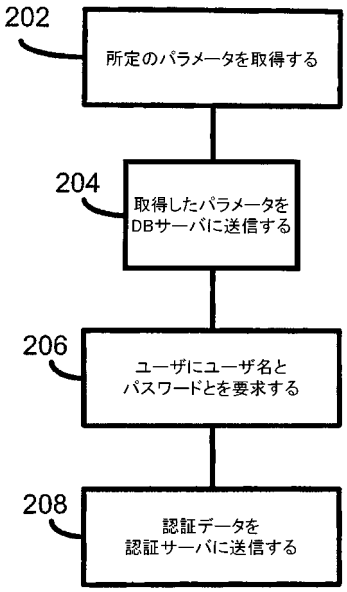
さらに、本発明の実施形態は、有線接続又は無線接続を介して搬送される通信信号のような任意の媒体を介して電子的に伝送することができ、実施形態は適切には、その任意の

媒体（the same）を包含する。
【図面の簡単な説明】
【００５２】
【図１】本発明の一実施形態によるシステム１００のブロック図である。
【図２】本発明の一実施形態による、コンピューティング装置によって行われる処理ステップ例を概略的に示すフロー図である。
【図３】本発明の一実施形態による、データベースサーバによって行われる処理ステップ例を概略的に示すフロー図である。
【図４】本発明の一実施形態による、認証サーバによって行われる処理ステップ例を概略的に示すフロー図である。
【図５】本発明の一実施形態によるシステム５００のブロック図である。
【符号の説明】
【００５３】
１００・・・システム
１０２・・・コンピューティング装置
１０３・・・ＶＰＮクライアント
１０４・・・装置構成管理プログラム
１０５・・・接続管理プログラム
１０６・・・インターネット
１０８、１１２・・・ファイヤウォール
１１０・・・企業ネットワーク
１１１・・・ＤＭＺ
１１４・・・企業内部ネットワーク
１１６・・・ＲＡＤＩＵＳサーバ
１１８・・・ディレクトリサーバ
１２０・・・ＤＢサーバ
１２２・・・装置管理サーバ
１２４・・・ＶＰＮゲートウェイサーバ
１２６・・・ネットワーク資源
５００・・・システム
５０２・・・コンピューティング装置１
５０４・・・ＶＰＮクライアント
５０６・・・コンピューティング装置２
５０８・・・装置構成管理プログラム
５１０・・・接続管理プログラム

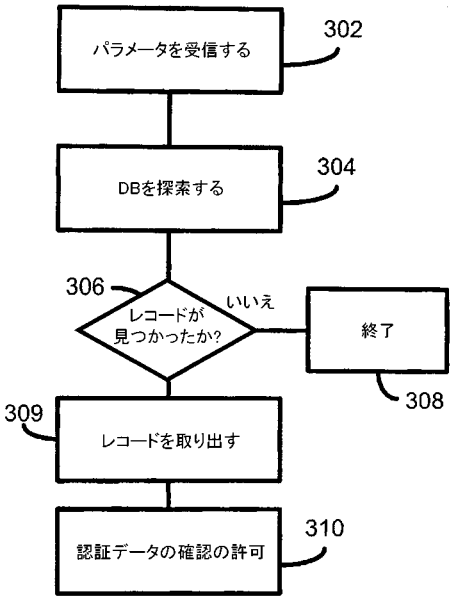
【図１】


102
コンピューティング装置
103
104
105
100
VPN
クライアント
装置構成管理
プログラム
接続管理
プログラム
インターネット
106
企業ネットワーク
ファイヤウォール
108
110
VPN
ゲートウェイ
サーバ
124
122
装置管理
サーバ
DMZ
111
112
ファイヤウォール
企業内部ネットワーク
114
118
116
120
ディレクトリ
サーバ
ネットワーク
資源
RADIUS
サーバ
DBサーバ
126

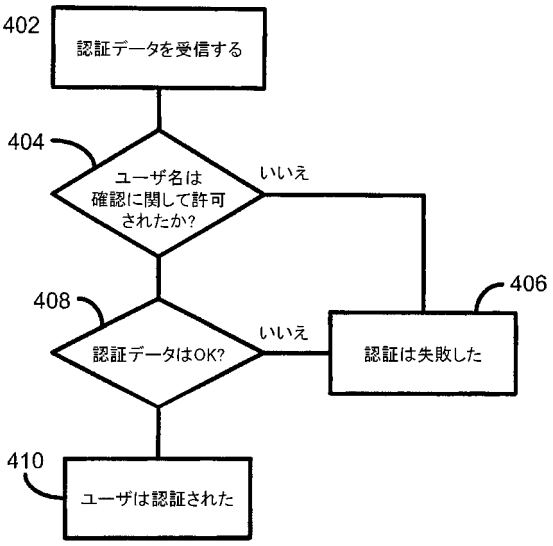
【図２】


202
所定のパラメータを取得する
204
取得したパラメータを
DBサーバに送信する
206
ユーザにユーザ名と
パスワードとを要求する
208
認証データを
認証サーバに送信する

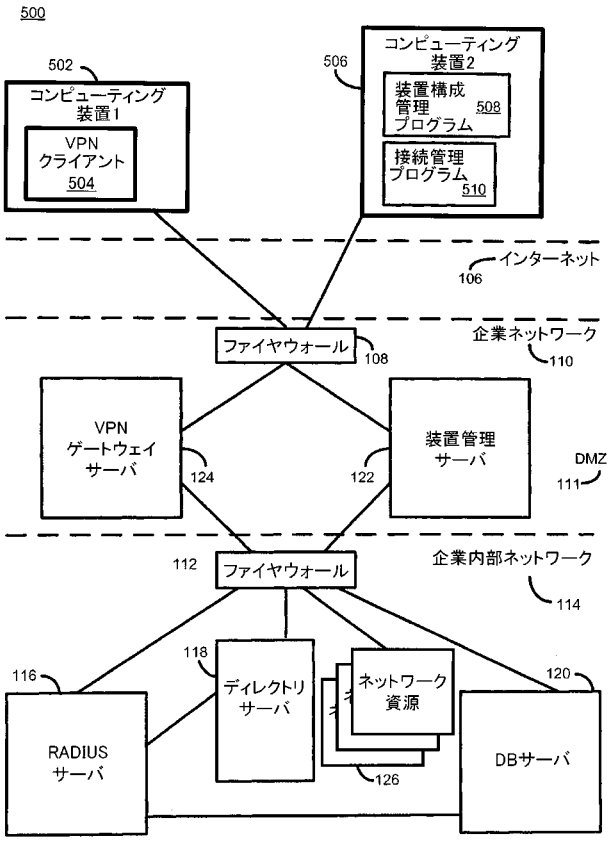
【図３】


パラメータを受信する
302
DBを探索する
304
306
レコードが
見つかったか?
いいえ
終了
308
309
レコードを取り出す
認証データの確認の許可
310

【図４】


402
認証データを受信する
404
ユーザ名は
確認に関して許可
されたか?
いいえ
406
408
認証データはOK?
いいえ
認証は失敗した
410
ユーザは認証された

【図５】


500
502
コンピューティング装置1
VPNクライアント 504
506
コンピューティング装置2
装置構成管理プログラム 508
接続管理プログラム 510
インターネット
106
企業ネットワーク
110
ファイヤウォール
108
VPNゲートウェイサーバ
124
122
装置管理サーバ
DMZ
111
112
ファイヤウォール
企業内部ネットワーク
114
116
RADIUSサーバ
118
ディレクトリサーバ
ネットワーク資源
126
120
DBサーバ

フロントページの続き

(72)発明者　ジル・ヴァンサン
フランス国３８０９０　ヴィルフォンテーヌ　ブールヴァール　スティーヴビコ　ヒューレット・パッカード・フランス内

Ｆターム(参考) 5B285 AA01 BA03 CA34 CB02 CB42 CB62 CB72 CB84 DA05 DA06 DA09
5J104 AA07 AA16 EA03 EA15 EA16 KA01 KA04 MA01 NA05 NA38 PA07