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

特許第4813595号
(P4813595)

(45)発行日　平成23年11月9日(2011.11.9)　(24)登録日　平成23年9月2日(2011.9.2)

(51)Int.Cl.		F I		
H04L 12/56	(2006.01)	H04L	12/56	H
G06F 21/20	(2006.01)	G06F	15/00	330B
		G06F	15/00	330C

請求項の数 13　(全 12 頁)

(21)出願番号	特願2009-501699 (P2009-501699)
(86)(22)出願日	平成19年3月20日 (2007.3.20)
(65)公表番号	特表2009-530991 (P2009-530991A)
(43)公表日	平成21年8月27日 (2009.8.27)
(86)国際出願番号	PCT/US2007/064412
(87)国際公開番号	WO2007/109671
(87)国際公開日	平成19年9月27日 (2007.9.27)
審査請求日	平成21年9月29日 (2009.9.29)
(31)優先権主張番号	60/784,183
(32)優先日	平成18年3月21日 (2006.3.21)
(33)優先権主張国	米国 (US)
(31)優先権主張番号	11/517,167
(32)優先日	平成18年9月7日 (2006.9.7)
(33)優先権主張国	米国 (US)

(73)特許権者　500088667
日本通信株式会社
東京都品川区南大井６丁目２５番３号
(74)代理人　100083806
弁理士　三好　秀和
(74)代理人　100095500
弁理士　伊藤　正和
(74)代理人　100111235
弁理士　原　裕子
(72)発明者　三田、　フランク　エス.
日本国１０８－００７４東京都港区高輪４－５－１２
(72)発明者　福田　尚久
日本国１４１－００１東京都品川区北品川６－１－８　ナンバー４０５

最終頁に続く

(54)【発明の名称】取引のためのセキュアな通信を提供するシステムおよび方法

(57)【特許請求の範囲】

【請求項１】

電子取引のためのセキュアな通信を提供する方法であって、

容量管理アプリケーションおよびセッションマネージャアプリケーションを備える接続サーバにおいてクライアント装置から接続開始信号を受信するステップであって、前記容量管理アプリケーションが、前記クライアント装置とリモートサーバとの間で送信されるパケットを管理することにより通信コストを選択的に低減することが出来るように、前記クライアント装置と前記リモートサーバとの間の情報トラフィックを制御するステップ、

直接接続を介して前記接続サーバと前記クライアント装置の間で通信リンクを確立するステップ、

前記セッションマネージャアプリケーションを用いて前記接続サーバから前記リモートサーバへの接続信号を開始するステップ、

第２の直接接続を介して前記接続サーバと前記リモートサーバの間で第２の通信リンクを確立するステップ、および

前記接続サーバを介しておよび前記直接接続と前記第２の直接接続とを介して、前記クライアント装置と前記リモートサーバの間に、電子取引を実施するためのセキュアな私設網を生成するステップ

を含む、方法。

【請求項２】

前記接続サーバが前記クライアント装置およびクライアント装置ユーザの識別を認証す

るステップをさらに含む、請求項１に記載の方法。
【請求項３】
前記接続サーバが前記クライアント装置上で取引インターフェースアプリケーションを起動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４】
前記接続サーバと前記リモートサーバの間の前記第２の直接接続が専用回線接続である、請求項１に記載の方法。
【請求項５】
前記接続サーバと前記クライアント装置の間の前記通信リンクが電気通信提供者サーバを含み、前記直接接続が前記接続サーバと前記電気通信提供者サーバとの間のものである、請求項１に記載の方法。
【請求項６】
前記接続サーバと前記電気通信提供者サーバの間の前記直接接続が専用回線接続である、請求項５に記載の方法。
【請求項７】
直接接続を介して接続サーバとクライアント装置との間に通信リンクを確立し、かつ第２の直接接続を介して前記接続サーバとリモートサーバとの間に第２の通信リンクを確立するセッションマネージャアプリケーションと、
前記クライアント装置と前記リモートサーバとの間で送信されるパケットを管理することにより通信コストを選択的に低減することが出来るように、前記クライアント装置と前記リモートサーバとの間の情報トラフィックを制御する容量管理アプリケーションと
を備える接続サーバであって、
前記通信リンクおよび前記第２の通信リンクを介して、前記クライアント装置と前記リモートサーバの間に、電子取引を実施するためのセキュアな私設網を生成する、接続サーバ。
【請求項８】
前記セッションマネージャアプリケーションが、前記クライアント装置およびクライアント装置ユーザの識別を認証するように適合されている、請求項７に記載の接続サーバ。
【請求項９】
前記リモートサーバとの前記第２の直接接続が専用回線接続である、請求項７に記載の接続サーバ。
【請求項１０】
前記セッションマネージャアプリケーションが、前記直接接続を介して電気通信提供者装置と前記通信リンクを確立することによって、前記クライアント装置との前記直接接続を介する前記通信リンクを確立し、
前記クライアント装置が前記電気通信提供者装置に接続されている、請求項７に記載の接続サーバ。
【請求項１１】
前記電気通信提供者装置との前記直接接続が専用回線接続である、請求項１０に記載の接続サーバ。
【請求項１２】
前記セッションマネージャアプリケーションが実行可能コードである、請求項７に記載の接続サーバ。
【請求項１３】
前記セッションマネージャアプリケーションを実行するプロセッサをさらに備える、請求項１２に記載の接続サーバ。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、一般に、コンピュータネットワーキングに関し、より詳細には、取引のため

のセキュアな通信を提供するシステムおよび方法に関する。
【０００２】
（関連出願データ）
本願は、２００６年3月２１日に出願された米国仮出願第６０／７８４，１８３号の利益を主張する、２００６年9月７日に出願された米国特許出願第１１／５１７，１６７号の利益を主張するものであり、両出願の全文を参照により本明細書に組み込むものである。
【背景技術】
【０００３】
人々が、ますます、インターネット上で金融その他の機密情報を扱う電子取引を行うようになってきている。電子取引には、電子的手段による勘定支払い、インターネットバンキング、電子オークション、電子振替、および電子証券取引が含まれ得る。加えて、人々は、その雇用者ネットワークなどのネットワークへのリモートアクセスも望んでいる。目下のところ、電子取引のためのリモートアクセスを含めて、リモートアクセスは、インターネットなどの公衆広域ネットワークを介し、パーソナルコンピュータなどのクライアント装置によって行われている。同様に、インターネット上での取引および通信に関連してますます大量の不正行為も行われるようになっている。
【発明の開示】
【発明が解決しようとする課題】
【０００４】
目下のところ、インターネット上の不正行為は、基本的には２つの発生源、すなわち、１）インターネット接続自体と、２）Ｍｉｃｒｏｓｏｆｔ（登録商標）オペレーティングシステムベースのクライアント装置など、オペレーティングシステムベースのクライアント装置とで発生している。これらの発生源は、典型的なオンライン電子取引を不正行為にさらすものである。第１の発生源、すなわちインターネット接続では、インターネットが公衆網であり、そのために、一般大衆が多くのポートを利用し、これらにアクセスすることができる。インターネットアクセスネットワーク技術の趨勢、進歩、およびその使用により、ユーザが利用できる帯域幅が増大している。帯域幅が増大するほど、インターネットアクセスは高速になる。この趨勢はユーザの「常時接続」使用行動を助長し、「常時接続」使用行動は固定料金によってさらに助長される。これは、ユーザが、オペレーティングシステムおよびネットワーク接続を開始するという面倒な処理を行わなくて済むように、インターネットアクセスを常につないだままにし得ることを意味する。この状況は、便利さを提供し得るが、同時に、複数の開放ポートを介してクライアント端末に望ましくないソフトウェアを侵入させるのに最適な環境も提供する。ポート保護技術も利用できるが、ほとんどの場合、その使用に伴う技術的課題は、大衆による使用を緩和させる。加えて、金融機関のＷｅｂページなどＷｅｂページ上のコードはＨＴＭＬコードであり、一般に公開されている。よって、ハッカーらは、インターネットのアクセスしやすさを利用して電子取引の情報を獲得することができる。
【０００５】
従来のリモートアクセス解決策の大部分は、インターネットを利用してクライアント装置上のユーザとサーバの間の接続を可能にする。専用回線接続または直接回線接続を利用するリモートアクセス解決策も提供されているが、普通のユーザにとっては費用がかかりすぎる。一般には、住宅などの遠隔地から組織のネットワークおよびサーバへの直接回線接続を備えることができるのは組織の幹部だけである。
【０００６】
第２に、大部分のクライアント装置がマイクロソフト社のＷｉｎｄｏｗｓ（登録商標）オペレーティングシステムを利用するものと仮定すると、大部分の不正行為実行者は、主に、これらの装置に存在する彼らの目的ためのソフトウェアを作成することに集中することになる。この種のソフトウェアは、一般に「スパイウェア」または「マルウェア」に分類され、Ｗｉｎｄｏｗｓ（登録商標）オペレーティングシステムベースの装置上にあって

待機することができる。そうしたスパイウェアは、その場合、そのユーザには知られずに、不正行為を活動化し得る一定の状況において作動することができる。スパイウェアは、「セキュアな」サイトへの望ましくないアクセスを容易にするために、キー入力を記録したり、別のやり方でユーザの機密情報を取り込んだりすることができる。したがって、電子取引のためのセキュアな通信を提供する解決策が求められている。

【課題を解決するための手段】

【０００７】

本発明の実施形態は、セキュアな通信を提供するシステムおよび方法を示すものである。本発明の一実施形態の一態様では、インターネットを利用せず、無線モデム、およびクライアント装置とリモートサーバの間の少なくとも１つの直接接続を利用してリモートサーバまたはネットワークへの仮想専用接続を生成する。本発明の一実施形態の別の態様では、垂直機能オペレーティングシステムがクライアントオペレーティングシステムに取って代わってリモートサーバとの通信を処理する。本発明の一実施形態の別の態様は、無線モデムおよび少なくとも１つの直接接続を介してリモートサーバとの接続を確立し、第１のオペレーティングシステムをシャットダウンし、第２のセキュアなオペレーティングシステムを始動し、第２のオペレーティングシステムでインターフェースアプリケーションを起動してリモートサーバとの電子取引を実施するクライアント装置を備える。

【０００８】

これらの例示的実施形態に言及するのは、本発明を限定し、または定義するためではなく、本発明の理解に役立つ例を示すためである。例示的実施形態については「発明を実施するための最良の形態」において論じ、そこで本発明をさらに説明する。本発明の様々な実施形態が提供する利点は、本明細書を吟味すればさらに理解されるであろう。

【０００９】

本発明の上記その他の特徴、態様、および利点は、以下の「発明を実施するための最良の形態」を添付の図面を参照して読めばより適切に理解されるものである。

【発明を実施するための最良の形態】

【００１０】

本発明の実施形態は、電子取引のためのセキュアな通信を提供するシステムおよび方法を示すものである。本発明には複数の実施形態がある。はじめの例として、本発明の１つの例示的実施形態は、クライアント装置上のユーザがリモートサーバとインターフェースするための私設網を提供するシステムおよび方法を示す。リモートサービスは、電子取引を実施する、金融機関またはその他の金融仲介機関と関連付けられた金融取引サーバとすることもでき、私設網と関連付けられたサーバとすることもできる。

【００１１】

一実施形態では、クライアント装置は、保護されていない公衆網にアクセスせずに、私設網上などのリモートサーバにアクセスする。クライアント装置は無線モデムを備え、無線モデムにより無線ネットワークを介して電気通信提供者のデータセンタにあるサーバへの接続を確立し得る。その場合、この電気通信提供者のサーバは、例えば、専用回線接続などによって接続サーバに直接接続されていてもよい。接続サーバは、専用回線接続などの直接接続などによってリモートサーバに接続されていてもよい。これにより、クライアント装置のためのセキュアな私設網が生成される。次いでクライアント装置は、リモートサーバとセキュアなやり方で通信することができる。次いでクライアント装置は、リモートサーバが金融機関と関連付けられている場合には、ユーザの金融口座にアクセスしてその金融口座で取引を行うことができ、オークションや小売業者の財貨やサービスに対する支払いをすることもでき、組織のリモートネットワーク上にある専有の情報にアクセスすることもできる。

【００１２】

一実施形態では、接続サーバ上の容量管理アプリケーションが、リモートサーバとクライアント装置の間の情報トラフィックを制御する。

【００１３】

一実施形態では、このような私設網が確立されたときに、クライアント装置上のアクセスエンジンが他のすべてのアプリケーションをシャットダウンする。また、接続サーバは、リモートサーバ上の許可されたアプリケーションだけのためにクライアント装置を認証することもできる。

【００１４】

クライアント装置は、任意のＷｉｎｄｏｗｓ（登録商標）ベースのスパイウェアまたはその他のマルウェアがアプリケーションサーバとの電子取引の間に機密情報を獲得するのを防ぐために、リモートサーバとの接続が行われる前、行われる間、または行われた後に、Ｗｉｎｄｏｗｓ（登録商標）オペレーティングシステムからオペレーティングシステムを切り換えることができる。また、代替として、クライアント装置は、Ｌｉｎｕｘなど、相対的によりセキュアなオペレーティングシステムで動作し、マイクロソフト社のＷｉｎｄｏｗｓ（登録商標）オペレーティングシステムを使用していなくてもよい。実施形態によっては、クライアント装置が保護されていないＬｉｎｕｘオペレーティングシステムで動作することもある。

【００１５】

この導入部は読者に本願の全般的主題について紹介するためのものである。本発明は決してかかる主題だけに限定されるものではない。以下で例示的実施形態について説明する。

【００１６】

［システムアーキテクチャ］

本発明による様々なシステムを構築することができる。次に図面を参照すると、図１には、本発明のシステムの１つの例示的実施形態が示されている。システム１００は、モデム１０４などの通信装置を備えるクライアント装置１０２を含む。モデム１０４は、無線モデムとすることができ、無線ネットワークを介して電気通信提供者サーバ１１０への接続を確立することができる。電気通信提供者サーバ１１０は、専用回線接続などの直接接続１１２によって接続サーバ１２０に接続されていてもよい。接続サーバ１２０は、さらに、専用回線接続などの直接接続１１４によってリモートサーバ１３０に接続されていてもよい。別の実施形態では、システム１００は接続サーバ１２０を含まず、提供者サーバ１１０は、専用回線接続によってリモートサーバ１３０に直接接続されている。

【００１７】

図１はただ１つのクライアント１０２と提供者サーバ１１０と接続サーバ１２０とリモートサーバ１３０とを含むが、本発明の一実施形態は、複数のクライアント１０２を含み、複数の提供者サーバ１１０、接続サーバ１２０、リモートサーバ１３０を含んでいてもよい。

【００１８】

クライアント装置１０２の例としては、パーソナルコンピュータ、情報端末、携帯情報端末、セルラ電話機、移動電話機、スマートフォン、ページャ、ディジタルタブレット、ラップトップコンピュータ、インターネット家電、およびその他のプロセッサベースの装置がある。一般に、クライアント装置１０２は、モデム１０４などの通信装置によってデータを送受信することができ、１つまたは複数のアプリケーションプログラム１０６、１０７と対話する、任意の適切な種類のプロセッサベースのプラットフォームとすることができる。クライアント装置１０２は、アプリケーションプログラム１０６を含むことのできる、ＲＡＭなどのコンピュータ可読媒体１０５に結合されたプロセッサ１０３を含むことができる。一実施形態では、クライアント装置１０２は、アクセスエンジンアプリケーション１０７と２つのオペレーティングシステム１０８、１０９を含む。例えば、クライアント装置１０２は、主に、Ｍｉｃｒｏｓｏｆｔ（登録商標）Ｗｉｎｄｏｗｓ（登録商標）オペレーティングシステムを動作させるが、電子取引時にリモートサーバ１３０に接続されるときにはＬｉｎｕｘオペレーティングシステム上で動作する。第２のオペレーティングシステム１０９は、図示のようにメモリ１０５内に位置していてもよく、取引インターフェースアプリケーション用の組み込みオペレーティングシステムとすることもできる

。アクセスエンジン１０７は、クライアント装置１０２と、提供者サーバ１１０との、最終的にはリモートサーバ１３０とのセットアップおよび接続を制御することができる。また、アクセスエンジン１０７は、第１のオペレーティングシステム１０８から第２のオペレーティングシステム１０９への切り換えも制御することができる。

【００１９】

一実施形態では、アクセスエンジン１０７は、共にこの参照により本明細書に組み込まれる、米国特許出願第１１／１６７，７４４号明細書（２００５年６月２７日出願）と第１１／１６８，８４７号明細書（２００５年６月２８日出願）に記載されている日本通信株式会社（Japan Communications, Inc.）のｂＡｃｃｅｓｓ（商標）システムなどのアクセスシステムの一部である。このアクセスシステムは、オペレーティングシステムのドライバレベルより下、オペレーティングシステムのコア部分より上で動作することができる。例えばこのアクセスシステムは、アクセスエンジン１０７を、接続サーバ１２０および提供者サーバ１１０を介してクライアント装置１０２のリモートサーバ１３０への接続を確立するように、Ｗｉｎｄｏｗｓ（登録商標）オペレーティングシステムのドライバレベルより下で動作させることができる。

【００２０】

ユーザ１０１は、例えば、キーボード、ポインティング装置、ディスプレイ（不図示）などによってクライアント装置１０２と対話することができる。モデム１０４は、例えば簡易型携帯電話システム（「ＰＨＳ」）ネットワークや符号分割多元接続（「ＣＤＭＡ」）ベースのネットワークといった無線通信ネットワークを介して通信することのできるセルラモデムを備えた、ＰＣＭＣＩＡカードなどとすることができる。実施形態によっては、第３世代移動電話技術（「３Ｇ」）ネットワークを使用してもよい。

【００２１】

モデム１０４が無線モデムである場合、クライアント装置からの通信は、モデム１０４を経由し、ＰＨＳやＣＤＭＡネットワークなどの無線ネットワークを介して、電気通信提供者のデータセンタ内にある提供者サーバ１１０に渡される。ディジタル無線通信は、ハードウェア識別方式である堅固なセキュリティ規格を提供する。例えば、無線装置は、装置内にあって暗号化に使用される電子的通し番号を使用する。実施形態によっては、モデムは、ケーブルモデムまたはディジタル加入者線（「ＤＳＬ」）モデムとすることもでき、クライアント装置１０２と、ユーザのインターネットサービス提供者（ＩＳＰ）のところにあるサーバ１１０との間で通信をやりとりするのに使用することもできる。

【００２２】

また、サーバは、１つまたは複数のアプリケーションプログラムを含むことのできるＲＡＭやその他の種類のメモリといったコンピュータ可読媒体に結合されたプロセッサを含む、プロセッサベースのサーバ装置とすることもできる。例えば、接続サーバ１２０は、コンピュータ可読媒体１１８にアクセスできるプロセッサ１１６を含むことができる。コンピュータ可読媒体１１８は、専用回線による提供者サーバ１１０およびリモートサーバ１３０との接続の確立を円滑に行わせることのできる、セッションマネージャアプリケーションプログラム１２２を含むことができる。また、セッションマネージャアプリケーション１２２は、ユーザ１０１およびクライアント装置１０２の認証機能を行ってもよい。加えて、コンピュータ可読媒体１１８は、リモートサーバ１３０とクライアント装置１０２の間の情報トラフィックを制御する容量管理アプリケーション１２４も含むことができる。

【００２３】

リモートサーバ１３０は、他のサーバ装置およびデータベースと対話してもよく、電子取引を実施するためにクライアント装置と対話させるアプリケーションプログラムを含んでいてもよい。実施形態によっては、ｂＡｃｃｅｓｓ（商標）ソフトウェアを使って、クライアント装置上で利用できるアプリケーションを取引用に設計された特定のアプリケーションだけに制限し、かつ／またはクライアント装置とリモートサーバ１３０の間の対話を最適化してもよい。クライアント装置から利用できるアプリケーションを制限すること

により、対話の性能を相対的に向上させ、クライアント装置とリモートサーバ１３０の間の有効な通信に必要な帯域幅を相対的に低減させることもできる。必要な帯域幅が減少すると、クライアント装置とリモートサーバ１３０の間の通信コストも減少し得る。電子取引には、例えば、電子的手段による勘定支払い、電子振替、および証券その他の金融商品取引などが含まれ得る。リモートサーバ１３０は、銀行や仲介業者などの金融機関と関連付けられていてもよい。また、リモートサーバは、ＰａｙＰａｌ（登録商標）などの金融仲介機関と関連付けられていてもよい。リモートサーバ１３０は、ユーザ名、パスワード、口座番号、その他の認証技術などによってユーザ１０１を認証する。クライアント装置１０２は、リモートサーバ１３０と対話するためにＷｅｂブラウザアプリケーションを実行することができる。ユーザには、ユーザが金融機関のＷｅｂサイトと対話しているように見えるが、その接続はセキュアな直接接続によるものである。

【００２４】

実施形態によっては、リモートサーバは、企業ネットワークなどの私設網と関連付けられていてもよい。この実施形態では、ユーザ１０１は、セキュアな接続によって私設網と通信することができ、セキュアなやり方で機密情報にアクセスすることができる。

【００２５】

前述のようなセキュアな接続の確立により、これまでは上級企業幹部だけしか利用できなかった同じ機能（リモートサーバへの直接接続）を、一般大衆が利用できるようになる。トランスポートアプリケーションを、特定のアプリケーションだけのためにユーザを認証する（ｂＡｃｃｅｓｓインターフェースなどの）インターフェースおよび接続サーバを介したものに限定することによってコスト削減が達成される。（モバイルデータカード無線モデムなどの）モデム１０４がクライアント装置１０２に接続されると、アクセスエンジン１０７および／または接続サーバ１２０は、クライアント装置１０２上で実行されるアプリケーションを、リモートサーバ１３０へのアクセスのために指定されたものだけに制限する。クライアント装置１０２とリモートサーバ１３０の間の通信経路は、モデム１０４、アクセスエンジン１０７、および接続サーバ１２０のうちの１つまたは複数によって制御される。この私設網を流れる実際のパケット数を管理することにより、さらなるコスト削減および低価格を実現することができる。

【００２６】

［セキュアな通信を提供する例示的方法］

本発明の実施形態による様々な方法を実行することができる。図２に、図１に示すセッションマネージャ１２２またはアクセスエンジン１０７によって実施され得るセキュアな通信を提供する例示的方法２００を示す。この例示的方法は例として示すにすぎず、本発明による方法を実行するやり方には様々なものがある。図２に示す方法２００は、様々なシステムの１つまたはそれらの組み合わせによって実行し、または他のやり方で実施することができる。例示のために前述の図１に示すシステムを使用する。

【００２７】

ステップ２０２で、通信サーバとの接続を開始する。一実施形態では、接続の開始がクライアント装置１０２のモデム１０４の作動によって行われる。例えば、モデム１０４がＰＣＭＣＩＡカードである場合、モデム１０４をクライアント装置１０２に接続すると接続サーバ１２０との接続が開始される。

【００２８】

ステップ２０４で、接続を確立する。一実施形態では、モデム１０４は、ＰＨＳやＣＤＭＡなどの無線ネットワークを介して提供者サーバ１１０に接続する。提供者サーバ１１０は、専用回線接続１１２を介して接続サーバ１２０に接続される。一実施形態では、接続サーバ１２０は、提供者サーバ１１０を介してクライアント装置１０２から開始された接続を受け取る。前述のように、アクセスエンジン１０７は、この接続を確立するのにオペレーティングシステムのドライバレベルより下で動作することができる。例えば、一実施形態では、Ｗｉｎｄｏｗｓ（登録商標）オペレーティングシステムが実行されている間、アクセスエンジン１０７は、Ｗｉｎｄｏｗｓ（登録商標）オペレーティングシステムの

ドライバレベルより下、同オペレーティングシステムのコアより上で動作して接続を確立する。

【００２９】

ステップ２０６で、接続サーバ１２０は、クライアント装置１０２およびユーザを検証し、かつ／または認証する。接続サーバ１２０は、セッションマネージャアプリケーション１２２を利用してクライアント装置１０２からの接続を受け取り、クライアント装置１０２およびユーザを検証し、かつ／または認証してもよい。実施形態によっては、接続サーバ１２０は、クライアント装置１０２およびユーザの検証も認証も行わない。このような実施形態では、接続サーバ１２０は、クライアント装置１０２から開始された接続を受け取った後でリモートサーバ１３０との接続を確立し、次いで、リモートサーバ１３０がクライアント装置１０２およびユーザを認証してもよい。

【００３０】

ステップ２０８で、通信サーバ１２０は、セッションマネージャアプリケーション１２２を利用してリモートサーバ１３０との直接接続を確立する。例えば、セッションマネージャアプリケーション１２２は、リモートサーバ１３０への信号を開始し、リモートサーバ１３０から、通信サーバ１２０とリモートサーバ１３０の間で直接接続が確立されることを示す信号を受け取ることができる。この信号は、接続サーバ１２０の識別、直接接続の確立を求める要求、および／またはクライアント装置１０２の識別といった情報のパケットとすることができる。一実施形態では、接続サーバ１２０は、専用回線接続１１４を介してリモートサーバ１３０に接続される。

【００３１】

ステップ２１０で、クライアント装置１０２上で取引インターフェースアプリケーションを起動する。一実施形態では、インターフェースアプリケーションは、Ｗｅｂブラウザアプリケーションであり、クライアント装置のメモリ１０５内に置くことができる。一実施形態では、セッションマネージャアプリケーション１２２は、クライアント装置１０２上で取引インターフェースアプリケーションを起動させることができる。リモートサーバ１３０は、インターフェースアプリケーションを介してクライアント装置１０２とインターフェースすることができる。例えば、リモートサーバ１３０は、ＨＴＭＬ　Ｗｅｂページを使ってユーザ１０１と対話することができる。クライアント装置１０２とリモートサーバの間の接続は専用の直接接続であり、インターネットなどの公衆網を利用しない。リモートサーバ１３０は、無線ネットワークを介して送信されるデータ量を低減するために、クライアント装置１０２に必要なデータだけを送信することができ、それによってセキュアな通信方法のコストを低減することができる。接続サーバ１２０は、通信コストを低減する目的で、容量管理アプリケーション１２４を利用して各接続を経由して送信されるパケットを管理してもよい。

【００３２】

図３に、図１に示すセッションマネージャ１２２またはアクセスエンジン１０７によって実施され得るセキュアな通信を提供する別の例示的方法３００を示す。ステップ３０２で、リモートサーバとの接続を開始する。一実施形態では、接続の開始がクライアント装置１０２のモデム１０４の作動によって行われる。例えば、モデム１０４がＰＣＭＣＩＡカードである場合、クライアント装置１０２へのモデム１０４の接続により、接続サーバ１２０を介したリモートサーバ１３０との接続が開始される。

【００３３】

ステップ３０４で、リモートサーバ１３０との接続を確立する。一実施形態では、モデム１０４は、ＰＨＳやＣＤＭＡなどの無線ネットワークを介して提供者サーバ１１０に接続する。提供者サーバ１１０は、専用回線接続１１２を介して接続サーバ１２０に接続される。接続サーバ１２０は、クライアント装置１０２から開始された接続を受け取り、リモートサーバ１３０との接続を開始する。

【００３４】

ステップ３０６で、第１のオペレーティングシステムがシャットダウンする。一実施形

態では、前述のように、クライアント装置１０２がＷｉｎｄｏｗｓ（登録商標）オペレーティングシステムを実行しており、Ｗｉｎｄｏｗｓ（登録商標）オペレーティングシステムを実行している間にリモートサーバ１３０との接続を確立する。この実施形態では、接続サーバ１２０はＷｉｎｄｏｗｓ（登録商標）オペレーティングシステムをシャットダウンすることができる。別の実施形態では、アクセスエンジン１０７がＷｉｎｄｏｗｓ（登録商標）オペレーティングシステムをシャットダウンすることができる。Ｗｉｎｄｏｗｓ（登録商標）オペレーティングシステムがシャットダウンされている間、リモートサーバ１３０への接続はモデムを用いて維持することができる。アクセスエンジン１０７は、リモートサーバ１３０との接続を確立しようとするのと同時に、Ｗｉｎｄｏｗｓ（登録商標）オペレーティングシステムをシャットダウンし始めることができる。別の実施形態では、Ｗｉｎｄｏｗｓ（登録商標）オペレーティングシステムは、リモートサーバとの接続が確立される前にシャットダウンされる。ユーザ１０２がリモートサーバ１３０との任意の取引を行う前にＷｉｎｄｏｗｓ（登録商標）オペレーティングシステムをシャットダウンさせ、または休眠状態に入らせることが望ましい。このようにして、Ｗｉｎｄｏｗｓ（登録商標）オペレーティングシステムに組み込まれているスパイウェアやその他のマルウェアが機能できなくなる。別の実施形態では、Ｗｉｎｄｏｗｓ（登録商標）などの第１のオペレーティングシステムがシャットダウンせず、Ｌｉｎｕｘなどの第２のオペレーティングシステムが、第１のオペレーティングシステムのプロセスとして実行される。この実施形態では、第２のオペレーティングシステムは、第１のオペレーティングシステムの上で実行される。第２のオペレーティングシステムは、メモリの少なくとも一部分にアクセスし、スパイウェアまたはマルウェアを排除することができる。

【００３５】

別の実施形態では、第１のオペレーティングシステムを完全にシャットダウンしない。そうではなく、アクセスエンジン１０７は、セキュアな接続の間に特定のアプリケーションだけを実行する。接続サーバ１２０は、さらに、クライアント装置１０２およびユーザ１０１を認証し、クライアント装置１０２上で適切なアプリケーションだけが実行され、クライアント装置１０２がリモートサーバ１３０との適切な通信に従事するよう保証してもよい。

【００３６】

次に図１に戻ると、第１のオペレーティングシステムをシャットダウンした後、ステップ３０８で、第２のオペレーティングシステムを始動する。一実施形態では、接続サーバ１２０が第２のオペレーティングシステムを始動することができる。例えば、Ｗｉｎｄｏｗｓ（登録商標）オペレーティングシステムをシャットダウンまたは休眠させた後で、Ｌｉｎｕｘオペレーティングシステムやその他のセキュアなオペレーティングシステムを始動することができる。これは、リモートサーバ１３０への接続が行われる前でも接続時でも接続後でも行うことができる。第２のオペレーティングシステム１０９は、図１に示すメモリ１０５に置き、そこから実行することができる。代替として、第２のオペレーティングシステムは、取引インターフェースアプリケーション用の組み込みオペレーティングシステムとすることもできる。Ｌｉｎｕｘなどのオープンソースオペレーティングシステムを使用すれば、通信方法２００を使った電子取引時に個人機密情報を獲得し得る有害なマルウェアをコンピュータ上に常駐させる可能性が低減される。

【００３７】

ステップ３１０で、クライアント装置１０２上で取引インターフェースアプリケーションを起動する。一実施形態では、インターフェースアプリケーションはＷｅｂブラウザアプリケーションであり、クライアント装置のメモリ１０５内に置くことができる。リモートサーバ１３０は、インターフェースアプリケーションを介してクライアント装置１０２とインターフェースすることができる。例えば、リモートサーバ１３０は、ＨＴＭＬＷｅｂページを使ってユーザ１０１と対話することができる。クライアント装置１０２とリモートサーバの間の接続は専用の直接接続であり、インターネットなどの公衆網を利用しない。リモートサーバ１３０は、無線ネットワークを介して送信されるデータ量を低減する

ために、クライアント装置１０２に必要なデータだけを送信することができ、それによってセキュアな通信方法のコストを低減することができる。接続サーバ１２０は、通信コストを低減する目的で、容量管理アプリケーション１２４を利用して各接続を経由して送信されるパケットを管理してもよい。

【００３８】

［一般原則］

以上の本発明の実施形態の説明は例示と説明の目的で示しているにすぎず、網羅的であることも、本発明を開示通りの形に限定することも意図するものではない。当業者には、本発明の精神および範囲を逸脱することなく、これらの実施形態の多数の変形形態および適合形態が明らかになるであろう。

【図面の簡単な説明】

【００３９】

【図１】本発明の一実施形態を実施するための例示的環境を示すブロック図である。

【図２】セキュアな通信を提供するプロセスを示す流れ図である。

【図３】セキュアな通信を提供するプロセスの別の実施形態を示す流れ図である。

【図１】

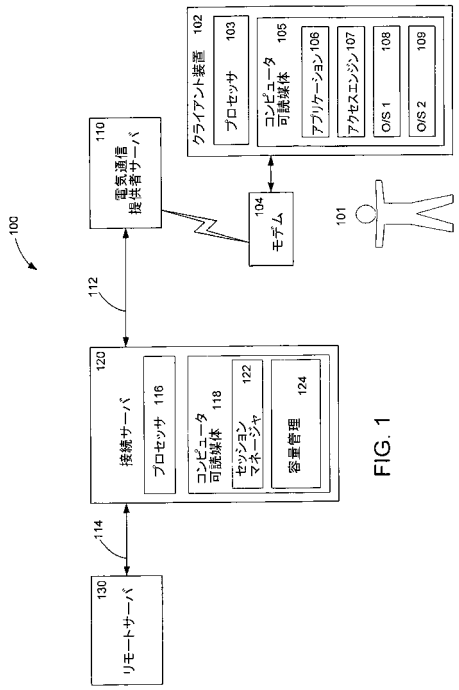

FIG. 1

【図２】

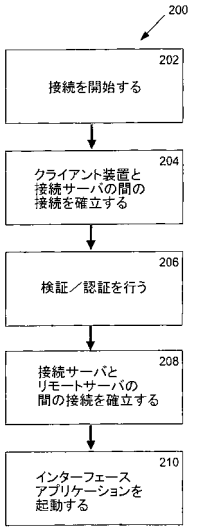

FIG. 2

【図３】

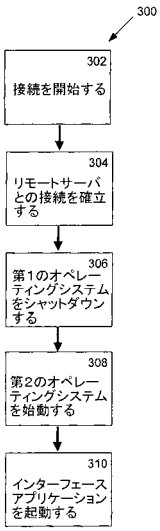
300
302
接続を開始する
304
リモートサーバとの接続を確立する
306
第1のオペレーティングシステムをシャットダウンする
308
第2のオペレーティングシステムを始動する
310
インターフェースアプリケーションを起動する

FIG. 3

フロントページの続き

(72)発明者　ウィン、　マーク
アメリカ合衆国　３０３０６　ジョージア州　アトランタ　カンバーランド　ロード　エヌ．イー．　１０３２
(72)発明者　岡崎　光輝
日本国神奈川県大和市中央林間２－１８－７　マホロバーハイム　１０３
(72)発明者　ロイヤー、　ポール
アメリカ合衆国　８０１１８　コロラド州　ラークスパー　ポンチョ　サークル　７３５４

審査官　玉木　宏治

(56)参考文献　特開２００４－１５８０２５（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
H04L 12/00-66
G06F 21/20