(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第3909289号
(P3909289)
(45)発行日　平成19年4月25日(2007.4.25)　(24)登録日　平成19年1月26日(2007.1.26)

(51)Int.Cl.		F I		
H04L 12/56	(2006.01)	H04L	12/56	H
G06F 13/00	(2006.01)	G06F	13/00	353C
G06F 15/00	(2006.01)	G06F	15/00	310D
G09C 1/00	(2006.01)	G09C	1/00	640E
		G09C	1/00	660E

請求項の数 23　(全 20 頁)

(21)出願番号　特願2002-551723(P2002-551723)
(86)(22)出願日　平成13年12月19日(2001.12.19)
(65)公表番号　特表2005-501432(P2005-501432A)
(43)公表日　平成17年1月13日(2005.1.13)
(86)国際出願番号　PCT/US2001/048993
(87)国際公開番号　WO2002/050695
(87)国際公開日　平成14年6月27日(2002.6.27)
審査請求日　平成16年11月11日(2004.11.11)
(31)優先権主張番号　60/257,480
(32)優先日　平成12年12月20日(2000.12.20)
(33)優先権主張国　米国(US)
(31)優先権主張番号　09/767,465
(32)優先日　平成13年1月22日(2001.1.22)
(33)優先権主張国　米国(US)

(73)特許権者　304019883
インテリシンク　コーポレイション
アメリカ合衆国　９５１３１　カリフォルニア州　サンノゼ　ノース　ファースト　ストリート　２５５０　スイート　５００
(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　デービッド　エル．サマーズ
アメリカ合衆国　８４１０５　ユタ州　ソルト　レイク　シティー　イースト　ダウンニントン　アベニュー　５３１

最終頁に続く

(54)【発明の名称】ポータブルデバイスと企業ネットワークとの間の自発的仮想専用ネットワーク

(57)【特許請求の範囲】
【請求項１】
リモート企業ネットワークと通信可能なデータセンタにおいて、前記データセンタは前記リモート企業ネットワークと関連付けられたファイアウォールの外部に位置し、ユーザが、前記データセンタと前記リモート企業ネットワークとの間の仮想専用ネットワークとして動作するデータトンネルを介して前記リモート企業ネットワークのネットワークデータにアクセスできるようにするための方法であって、
前記リモート企業ネットワークからデータ要求を受信する動作と、
前記データ要求に応答して、前記ファイアウォールを介して前記データセンタと前記リモート企業ネットワークとの間に、仮想専用ネットワークとして動作する前記データトンネルが確立されるように、進行中の回答データを前記リモート企業ネットワークに送信する動作と、
前記リモート企業ネットワークのネットワークデータにアクセスするための前記ユーザからのアクセス要求を受信する動作と、
前記アクセス要求を、前記データトンネルを使用して前記リモート企業ネットワークに送信する動作と、
前記ネットワークデータを、前記アクセス要求に応答して前記リモート企業ネットワークから受信する動作と、
前記ネットワークデータを前記ユーザに送信する動作とを含むことを特徴とする方法。
【請求項２】

前記データ要求が指定サーバによって受信され、当該指定サーバは前記データセンタの複数のサーバのうちの１つであることを特徴とする請求項１に記載の方法。
【請求項３】
前記データセンタのデータベースに、前記複数のサーバのうちのいずれが前記指定サーバであるかが通知され、前記指定サーバはデータトンネルが確立されたときにデータベースに通知することを特徴とする請求項２に記載の方法。
【請求項４】
前記アクセス要求は、前記データセンタの指定された電話ノードによって受信され、前記ユーザは電話システムを使用して前記アクセス要求を生成することを特徴とする請求項３に記載の方法。
【請求項５】
前記アクセス要求は、インターネットを介して前記データセンタの複数のサーバのうちの１つによって受信され、前記アクセス要求は、インターネットに接続されたデバイスを使用して前記ユーザによって生成されることを特徴とする請求項３に記載の方法。
【請求項６】
前記データセンタの前記指定された電話ノードは、前記アクセス要求を前記指定サーバに送信することを特徴とする請求項４に記載の方法。
【請求項７】
前記指定された電話ノードは、前記複数サーバのうち少なくとも１つと通信することによって、前記複数のサーバのうちのいずれが前記指定サーバであるかを判別することを特徴とする請求項６に記載の方法。
【請求項８】
前記指定された電話ノードは、前記データベースと通信することによって、前記複数サーバのうちのいずれが前記指定サーバであるかを判別することを特徴とする請求項６に記載の方法。
【請求項９】
前記ユーザから前記リモート企業ネットワークのネットワークデータにアクセスするためのアクセス要求を受信する前記動作は、前記ユーザのアイデンティティを認証する動作をさらに含むことを特徴とする請求項１に記載の方法。
【請求項１０】
前記ネットワークデータを前記ユーザに送信する前記動作は、
前記ネットワークデータを前記指定サーバから前記指定された電話ノードに送信する動作と、
前記ネットワークデータを前記指定された電話ノードから前記ユーザによって使用される前記電話システムに送信する動作とを含むことを特徴とする請求項４に記載の方法。
【請求項１１】
企業ネットワークと関連付けられたファイアウォールの外部に位置するリモートデータセンタネットワークと通信可能な前記企業ネットワークにおいて、ユーザが、前記リモートデータセンタと前記企業ネットワークとの間の仮想専用ネットワークとして動作するデータトンネルを介して前記企業ネットワークのネットワークデータにアクセスできるようにするための方法であって、
データ要求を前記リモートデータセンタに送信する動作と、
前記ファイアウォールを介して前記リモートデータセンタと前記企業ネットワークとの間に、仮想専用ネットワークとして動作する前記データトンネルが確立されるように、前記データ要求に応答して進行中の回答データを前記リモートデータセンタから受信する動作と、
前記リモートデータセンタから、前記企業ネットワークのネットワークデータにアクセスするためのアクセス要求を受信する動作とを含み、当該アクセス要求が前記ユーザから前記リモートデータセンタによって受信され、その後前記リモートデータセンタによって前記データトンネルを介して前記企業ネットワークに送信されるものであって、

さらに前記方法は、前記ユーザが前記ネットワークデータにアクセスできるようにするために、前記アクセス要求に応答して、前記ネットワークデータを前記リモートデータセンタに送信する動作を含むことを特徴とする方法。
【請求項１２】
前記データ要求はファイアウォールを介して送信されることを特徴とする請求項１１に記載の方法。
【請求項１３】
前記データ要求はプロキシサーバを介して送信されることを特徴とする請求項１２に記載の方法。
【請求項１４】
前記回答データはポート４４３を介して受信されることを特徴とする請求項１２に記載の方法。
【請求項１５】
前記回答データはセキュアソケットレイヤ（Secure Sockets Layer）プロトコルを使用して受信されることを特徴とする請求項１４に記載の方法。
【請求項１６】
前記回答データはポート８０を介して受信されることを特徴とする請求項１１に記載の方法。
【請求項１７】
前記ネットワークデータを前記リモートデータセンタに送信する前記動作は、
前記ネットワークデータをセキュアソケットレイヤ（Secure Sockets Layer）プロトコルに準拠するように暗号化する動作と、
前記ネットワークデータの送信が一時仮想専用ネットワークとして動作するように、前記ネットワークデータを第２のデータトンネルを介して前記リモートデータセンタに送信する動作と、
前記第２のデータトンネルを閉じる動作とを含むことを特徴とする請求項１１に記載の方法。
【請求項１８】
データセンタにおいて、ユーザが、前記データセンタとリモート企業ネットワークとの間の仮想専用ネットワークとして動作するデータトンネルを介して前記リモート企業ネットワークのネットワークデータにアクセスできるようにするための方法を実施するためのコンピュータプログラム製品であって、前記データセンタは前記リモート企業ネットワークと関連付けられたファイアウォールの外部に位置し、前記コンピュータプログラム製品は、
前記方法を実施するためのコンピュータ実行可能命令を搬送するコンピュータ読取り可能媒体を含み、前記コンピュータ実行可能命令は、
前記リモート企業ネットワークからデータ要求を受信するためのプログラムコード手段と、
前記データ要求に応答して、前記ファイアウォールを介して前記データセンタと前記リモート企業ネットワークとの間に、仮想専用ネットワークとして動作する前記データトンネルが確立されるように、進行中の回答データをリモート企業ネットワークに送信するためのプログラムコード手段と、
前記リモート企業ネットワークのネットワークデータにアクセスするための前記ユーザからのアクセス要求を受信するためのプログラムコード手段と、
前記アクセス要求を、前記データトンネルを使用して前記リモート企業ネットワークに送信するためのプログラムコード手段と、
前記ネットワークデータを、前記アクセス要求に応答して前記リモート企業ネットワークから受信するためのプログラムコード手段と、
前記ネットワークデータを前記ユーザに送信するためのプログラムコード手段とを含むことを特徴とするコンピュータプログラム製品。

【請求項１９】
前記コンピュータ実行可能命令は、前記ユーザのアイデンティティを認証するためのプログラムコード手段をさらに含むことを特徴とする請求項１８に記載のコンピュータプログラム製品。
【請求項２０】
前記コンピュータ実行可能命令は、前記データセンタの電話ノードが前記アクセス要求を受信し前記アクセス要求を指定サーバに送信できるようにするためのプログラムコード手段をさらに含み、前記指定サーバは前記進行中の回答データを前記リモート企業ネットワークに送信するものであることを特徴とする請求項１８に記載のコンピュータプログラム製品。
【請求項２１】
前記指定サーバは前記データセンタの複数のサーバのうちの１つであって、前記ユーザは電話システムを使用して前記アクセス要求を生成することを特徴とする請求項２０に記載のコンピュータプログラム製品。
【請求項２２】
前記コンピュータ実行可能命令は、前記データセンタのデータベースにネットワークデータのコピーをキャッシュするためのプログラムコード手段をさらに含むことを特徴とする請求項１８に記載のコンピュータプログラム製品。
【請求項２３】
前記コンピュータ実行可能命令は、前記ユーザからの前記アクセス要求の受信に応答して、前記ネットワークデータの前記キャッシュ済みコピーを前記ユーザに送信するためのプログラムコード手段をさらに含むことを特徴とする請求項１８に記載のコンピュータプログラム製品。
【発明の詳細な説明】
【０００１】
（発明の背景）
１．発明の分野
本発明は、ユーザが仮想専用ネットワークを介してデータにアクセスできるようにするための方法およびシステムに関する。より詳細に言えば、本発明は、自発的仮想専用ネットワークを介したネットワークデータへの制御されたモバイルリモートアクセスをユーザに提供するための方法およびシステムに関する。
【０００２】
２．背景および関連分野
今日のビジネス世界では、多くの企業が自社のネットワークインフラストラクチャにファイアウォール（firewall）を導入することにより、自社のデータへの未許可アクセスを防止している。典型的にファイアウォールは、識別されないユーザがリモート位置からネットワークデータにアクセスするのを防止するように構成される。ファイアウォールは一般に、企業が自社のネットワークデータにアクセスする人物をより適切に管理できるようにするのに非常に有益であるが、モバイル職業人が事務所を離れているか、そうでなければネットワークデータへのローカルアクセスが得られない場合に、彼らが重要かつ緊急のビジネス情報から切り離されてしまうという望ましくない結果を招くものでもある。
【０００３】
モバイル職業人がリモート位置からビジネス情報にアクセスできるようにするために、一部の企業では職業人の自宅またはサテライトオフィスからなどの、企業と指定のリモート位置との間に、仮想専用ネットワーク（ＶＰＮ）を導入している。ＶＰＮの機能は、企業ネットワークと指定のリモート位置との間に、企業ファイアウォールを介したセキュア接続を開くことである。ＶＰＮは、ネットワークデータへのリモートアクセスを提供するのには有益であるが、企業ネットワークにおいておよび時にはリモート位置において、費用のかかるハードウェアおよび／またはソフトウェアを導入しなければならない。
【０００４】

図１には、ＶＰＮを介したネットワークデータへのリモートアクセスを可能にするための、従来技術のシステムおよび方法の一実施形態が示されている。図に示されるように、ユーザ１０は、リモート位置からＶＰＮトンネル１４を介して企業ネットワーク１２と通信する。ＶＰＮトンネル１４の各端にはＶＰＮノード１６、１８がある。企業ネットワーク１２では、ＶＰＮノード１６は企業ネットワークのファイアウォール２０をまたいでいる。ネットワークデータ２２はＶＰＮノード１６にあるファイアウォール２０およびＶＰＮトンネル１４を介してユーザ１０に伝送される。従来技術によれば、リモート企業２３は、ＶＰＮノード１６とＶＰＮノード２６との間に示されるＶＰＮトンネル２４を介して企業ネットワーク１２と通信することも可能である。

【０００５】

ＶＰＮのハードウェアおよびソフトウェアは、ＶＰＮトンネルを介して伝送されるデータが傍受されないこと、およびユーザまたはリモート企業に企業ネットワークデータへのアクセスが許可されることを保証するために、ＶＰＮノードで暗号化技術および他のセキュリティ機能を使用する。ただし、ＶＰＮの利点は、適切なＶＰＮソフトウェアおよび／またはハードウェアが導入されたリモート位置が離散的である場合に限定される。したがって、現在のところＶＰＮは、企業ファイアウォールの背後に格納されたネットワークデータへのモバイルリモートアクセスはユーザに提供していない。具体的に言えば、従来技術のＶＰＮでは、移動車両で通勤中のユーザが電話からネットワークデータにアクセスすることはできない。

【０００６】

従来技術のＶＰＮの確立に関連付けられた必然的な結果もある。具体的に言えば、ＶＰＮは、企業ネットワークとリモートＶＰＮノードとの間でデータを伝送できるように、企業ファイアウォールにポートまたはホールを開ける必要がある。ＶＰＮポートでは、許可されたユーザのみがネットワークデータへのアクセスを与えられることを保証するためのハードウェアまたはソフトウェアを導入しなければならない。ただし、ＶＰＮにはユーザのアイデンティティを認証するためのセキュリティメカニズムがあるにもかかわらず、ハッカーが企業ネットワークへの未許可のアクセスを取得する可能性が増加している。たとえば、ハッカーは企業ＶＰＮノードのファイアウォールを攻撃するか、またはリモートＶＰＮノード位置にあるリモートユーザのコンピューティングデバイスに侵入することによって、ネットワークデータへの未許可のアクセスを取得する場合がある。ハッカーがネットワークデータへのアクセスを取得できないようにするために、多くの企業では２次ファイアウォールをインストールしており、ハッカーが第１のファイアウォールを通って入ってきた場合、２次ファイアウォールに突入する前で止められる可能性が高い。

【０００７】

図１は、ネットワークデータへの未許可のアクセスを防ぐための典型的なファイアウォール構成を示す図である。このファイアウォール構成には、１次ファイアウォール２０、２次ファイアウォール２８、および、１次ファイアウォール２０と２次ファイアウォール２８との間の領域である非武装地帯（ＤＭＺ）３０が含まれる。

【０００８】

多くの企業は、企業のファイアウォールインフラストラクチャを介して伝送されるデータを傍受およびフィルタリングするために、プロキシ（proxy）サーバを導入している。プロキシサーバは、他の多くの理由でも有益であり、その１つが、アクセス可能なインターネットサイトを企業が制限できるようにする一方で、企業ファイアウォールの背後からユーザがインターネットにアクセスできるようにすることである。さらにプロキシサーバは、ユーザ要求を伝送する際にプロキシとして働くことによって、インターネットユーザの真のアイデンティティを隠す。ユーザ要求を伝送する際にプロキシとして働くことにより、プロキシサーバはユーザ要求をフィルタリングすることが可能であり、その結果、認定された要求のみが受け付けられる。本質的には、プロキシサーバは、未許可の要求が受け付けられるのを禁止することによって、ファイアウォールインフラストラクチャの保護を強化することができる。インターネットアクセスのためにはファイアウォールインフラス

トラクチャに追加のホールまたはポートを開けなければならないため、従業員がインターネットにアクセスするのを許可している企業にとって、プロキシサーバは特に重要である。典型的には、これらのポートには「ポート８０」および「ポート４４３」が含まれる。ファイアウォールおよびプロキシサーバは協働して、ポートを介して伝送されるデータを定義済みプロトコルに必ず準拠させることにより、インターネット上の未許可のユーザが企業ネットワークを介した制御を取得しないようにする働きをする。企業内から開始されるインターネットアクセスは、典型的にはファイアウォールに「ポート８０」および「ポート４４３」を開ける必要があるが、適切なファイアウォールおよびプロキシサーバ構成を使用することによって、ハッカーが「ポート８０」および「ポート４４３」を介して企業ネットワークへの未許可のリモートアクセスを取得する可能性を大幅に制限することができる。

【０００９】

ただし、ＶＰＮによってファイアウォール内に作成されたホールは、たとえ有効なＶＰＮハードウェアおよびソフトウェアを使用しても警備するのは困難である。ＶＰＮは、企業ファイアウォール内に新しく開かれたＶＰＮポートおよびそれぞれのリモートＶＰＮノードを含み、監視しなければならないフロントの数も増加させる。したがって、ＶＰＮは許可されたユーザがリモート位置からネットワークデータにアクセスできるようにするのに有益ではあるが、同様に、リモート位置からのネットワークデータへの未許可のアクセスを容易にするので好ましくない。ＶＰＮは、企業ファイアウォールの警備を困難にし、プロキシサーバの使用を困難にするものであり、したがってファイアウォールを弱体化し、許可未許可にかかわらず、ユーザにネットワークデータについての過剰な管理を与えるものである。さらにＶＰＮは、導入および維持にかなりの費用がかかる。にもかかわらず、今日の企業はモバイル職業人がオフィスから離れた重要かつ緊急な情報にアクセスできるようにする必要があるため、多くの企業はリソースに対する出費や、ＶＰＮの確立に関連付けられたリスクを負うことをいとわない。

【００１０】

前述の内容に鑑みて、当分野では現在、企業ファイアウォールの背後に格納されたネットワークデータへの管理されたアクセスを、関連付けられたファイアウォールインフラストラクチャを弱体化させることなく、経済的な方法で、モバイル職業人に提供することが求められている。さらに、ＶＰＮを介したネットワークデータへのモバイルリモートアクセスをユーザに提供し、その結果、離散的な事前に定義されるリモートＶＰＮノード位置からネットワークデータを取得する必要がないようにすることも求められている。たとえば、モバイル職業人が移動車両で通勤中であっても、携帯電話デバイスからＶＰＮを介して電子メールメッセージにアクセスできるようにすることも、当分野での進歩となろう。

【００１１】

（発明の概要）

本発明は、企業ファイアウォールで費用のかかるソフトウェアまたはハードウェアを導入する必要なしに、またファイアウォールインフラストラクチャを弱体化させることになる企業のファイアウォールでの追加のポートまたはホールを開けることなしに、むしろ事前に開けられた（pre-opened）インターネットポートを介してセキュアなデータトンネルを確立することにより、仮想専用ネットワーク（ＶＰＮ）を介した企業ネットワークデータへの制御されたモバイルリモートアクセスをユーザに提供するための方法およびシステムに関する。

【００１２】

本発明は、モバイル職業人が、絶えず移動しながらも、費用のかかるＶＰＮソフトウェアおよびハードウェアで構成しなければならない事前に定義される離散的なＶＰＮノード位置からリモートアクセスを取得する必要なしに、電子メールなどの重要かつ緊急なビジネス情報に企業ファイアウォールの背後からリモートにアクセスできるようにするものである。

【００１３】

リモートユーザは、企業ネットワークとの確立されたデータトンネルを有するデータセンタと通信することにより、ビジネスまたは企業の位置からネットワークデータにアクセスすることができる。企業ネットワークが初期データ要求をデータセンタに送信し、データセンタが回答データの進行中の送信で回答すると、データトンネルが確立される。企業ネットワークは、インターネット「ポート８０」または「ポート４４３」などの事前に開かれたネットワークポートを介して、初期データ要求を送信し、回答データを受信する。データセンタはＷｅｂサーバを使用して企業ネットワークと通信し、企業ネットワークは自発的仮想専用ネットワーク（ＳＶＰＮ）モジュールを使用してデータセンタと通信する。

【００１４】

一実施形態では、ＳＶＰＮモジュールは企業ネットワーク内からデータ要求を開始し、結果として生じる通信チャネルが確実に開いたままであるようにこのチャネルを監視する。チャネルが何らかの理由で閉じた場合、ＳＶＰＮモジュールは再度データ要求を開始し、新しいチャネルを開く。データ要求には、統一資源識別子（ＵＲＩ／Ｕｎｉｆｏｒｍ　Ｒｅｓｏｕｒｃｅ　Ｉｄｅｎｔｉｆｉｅｒ）、またはデータセンタのＷｅｂサーバに関連付けられたリソースにアクセスするための要求が含まれる。データセンタのＷｅｂサーバは、この要求に応答してＵＲＬに関連付けられた回答データを進行中の方式で企業ネットワークに返送し、その結果データセンタと企業ネットワークとの間の通信チャネルが開かれたままになる。実際には、データセンタが企業ネットワークへの回答データの送信を完了することは決してない。Ｗｅｂサーバは、任意の開かれた通信チャネルの状況に関するデータセンタのデータベースも更新する。データベースは、データセンタが複数のＷｅｂサーバを含み、そのうちの１つのみが企業ネットワークとの開かれた通信チャネルを有する場合に、特に有用である。

【００１５】

データセンタと企業ネットワークとの間の通信のチャネルは、ＶＰＮトンネルとして動作するデータトンネルである。データは、伝送制御プロトコル／インターネットプロトコル（ＴＣＰ／ＩＰ）、セキュアソケットレイヤプロトコルを備えたハイパーテキスト転送プロトコル（ＨＴＴＰＳ）、およびＩＰセキュリティプロトコル（ＩＰｓｅｃ）を使用してパケットで暗号化され、企業ネットワークの「ポート４４３」を使用してデータトンネルを介して伝送される。他の実施形態では、データトンネルは「ポート８０」を介して確立され、データはＴＣＰ／ＩＰ、ＩＰｓｅｃ、および、セキュアソケットレイヤプロトコル（ＳＳＬ）を使用しないハイパーテキスト転送プロトコル（ＨＴＴＰ）を使用して暗号化される。一実施形態では、プロキシサーバが、ポートを介して伝送されるデータをスクリーニングして、定義済みプロトコルに確実に準拠させる。

【００１６】

企業ネットワークからのネットワークデータにアクセスしようとするリモートユーザは、インターネットに接続された電話デバイスまたはコンピュータデバイスなどの通信デバイスを使用して、データセンタとの通信回線を開く。次にユーザは、ネットワークデータにアクセスするための要求を生成し、この要求をデータセンタに伝送する。電話デバイスが使用される場合は、次にデータセンタがアクセス要求を電話ノードで受け取り、電話ノードがデータセンタ内に含まれるＷｅｂサーバのうちの１つにアクセス要求を伝送する。Ｗｅｂサーバが企業ネットワークとの確立されたデータトンネルを有する場合は、次にアクセス要求がデータトンネルを介してＷｅｂサーバから企業ネットワークのＳＶＰＮモジュールへと伝送される。ただし、Ｗｅｂサーバと企業ネットワークとの間に開かれたデータトンネルがない場合、Ｗｅｂサーバはデータベースをチェックして、確立されたデータトンネルを介して回答データを企業ネットワークに伝送している他のサーバがデータセンタにあるかどうかを調べる。企業ネットワークとの開かれたデータトンネルを維持している他のＷｅｂサーバがある場合、次に電話ノードに通知され、アクセス要求が他方のＷｅｂサーバに転送され、続いて他方のＷｅｂサーバから企業ネットワークのＳＶＰＮモジュールに伝送される。

【００１７】

企業ネットワークは、ネットワークデータに関してＳＶＰＮモジュールが許可するように構成された任意の動作を実行することにより、ＳＶＰＮモジュールで受け取られたアクセス要求を処理する。一実施形態では、アクセス要求の処理には、電子メールデータまたはＷｅｂページデータの受信およびユーザへのデータの返信が含まれる。他の実施形態では、ＳＶＰＮモジュールは、リモートユーザがアクセスおよび操作できるデータに対して企業の管理を保持しながら、事前に定義される機能がネットワークデータに関して実行できるように構成される。事前に定義される機能には、電子メールメッセージの削除および電子メールメッセージのユーザへのファックス送信が含まれるが、これらに限定されるものではない。

【００１８】

ＳＶＰＮモジュールは、任意の要求されたデータをデータセンタに伝送することによって、データセンタとの第２のデータトンネルを確立する。第２のデータトンネルは一時データトンネルであり、企業ネットワークと、第１のデータトンネルを介して企業ネットワークと通信しているものと同じＷｅｂサーバとの間に確立される。データセンタによってネットワークデータが受け取られるとすぐに、第２のデータトンネルは閉じられ、リモートユーザにネットワークデータへのアクセスが提供される。ユーザがデータセンタとの通信に電話デバイスを使用する場合、要求されたネットワークデータは、デジタル表示形式または音声形式などのわかりやすい形式で、Ｗｅｂサーバからデータセンタの電話ノードを介してユーザの電話デバイスに伝送される。たとえば、ネットワークデータが電子メールメッセージを含む場合、電子メールのテキストをユーザの電話デバイスの液晶ディスプレイ（ＬＣＤ）上に表示するか、または電話デバイスを介してユーザに読み上げることができる。あるいはユーザは、データセンタのＷｅｂサーバとの直接のインターネット通信リンクを開くことによって、インターネットを介してネットワークデータに直接アクセスすることができる。

【００１９】

一実施形態では、データセンタがユーザのアイデンティティを認証した後に、ユーザは要求されたネットワークデータにアクセスできるようになる。これは、ユーザに秘密の個人識別番号を入力するように要求することによって達成される。

【００２０】

前記内容に鑑みて、本発明は従来技術を超える改良であることを理解されたい。具体的に言えば、本発明は、企業がデータトンネルを介したネットワークデータへのアクセス許容量を制限する機能を保持しながら、ユーザがセキュアデータトンネルを介したネットワークデータへのモバイルリモートアクセスを有することができるようにするものである。

【００２１】

本発明の追加の特徴および利点については以下の説明で述べるものとし、一部は説明から明らかとなるか、または本発明の実施によって習得することができる。本発明の特徴および利点は、添付の特許請求の範囲で具体的に指摘された手段および組合せによって、理解および取得することができる。本発明のこれらおよび他の特徴は、以下の説明および添付の特許請求の範囲からより完全に明らかになるか、または以下で述べる本発明の実施によって習得することができる。

【００２２】

本発明の前述および他の利点および特徴が取得できる方法について記載するために、上記で簡単に述べた本発明について、添付の図面に示された特定の実施形態を参照しながらより具体的に説明する。これらの図面は本発明の典型的な実施形態のみを示したものであり、したがって本発明の範囲を限定するものとはみなされないことを理解した上で、添付の図面を使用して、本発明の追加の特性および詳細について記述および説明する。

【００２３】

（発明の詳細な説明）

本発明は、ユーザがポータブルデバイスを使用して、モバイルリモート位置から自発的仮想専用ネットワークを介して企業ネットワークのネットワークデータにアクセスできるよ

うにするための方法およびシステムの両方に及ぶものである。
【００２４】
ユーザは、電話またはコンピュータデバイスを使用して電子メールなどのネットワークデータへのアクセス要求を生成し、このアクセス要求をデータセンタに伝送する。データセンタはユーザのアイデンティティを認証し、仮想専用ネットワーク（ＶＰＮ）として動作する確立されたデータトンネルを介してアクセス要求を適切な企業ネットワークへ伝送する。データトンネルは、企業ネットワークからデータセンタに伝送されたデータ要求に応答して開かれる。アクセス要求が受信されると、企業ネットワークはネットワークデータを取り出し、このネットワークデータを第２のデータトンネルを介してデータセンタに伝送し、次にこのデータがユーザに伝送される。
【００２５】
本発明の実施形態は、コンピュータ実行可能命令またはデータ構造を格納したコンピュータ読取り可能媒体を含むか、またはこれに組み込まれる。コンピュータ読取り可能媒体の例には、ＲＡＭ、ＲＯＭ、ＥＥＰＲＯＭ、ＣＤ－ＲＯＭ、または他の光ディスク記憶装置、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、コンピュータ実行可能命令またはデータ構造の形で所望のプログラムコード手段を搬送または格納するために使用可能であり、汎用コンピュータまたは専用コンピュータがアクセス可能な、任意の他の媒体が含まれる。情報がネットワーク、トンネル、チャネル、または他の通信接続（ハードワイヤード、ワイヤレス、あるいは、ハードワイヤードまたはワイヤレスの組合せのいずれか）を介してコンピュータに転送または提供されるときに、コンピュータは接続をコンピュータ読取り可能媒体として適切にみなす。したがって任意のこうした接続は、厳密にコンピュータ読取り可能媒体と呼ばれる。前述の組合せも、コンピュータ読取り可能媒体の範囲内に含まれるものとする。コンピュータ実行可能命令は、たとえば、汎用コンピュータ、専用コンピュータ、または専用処理デバイスに一定の機能または機能グループを実行させる、命令およびデータを含む。コンピュータ実行可能命令および関連するデータ構造またはモジュールは、本明細書で開示された本発明のステップを実行するためのプログラムコード手段の一例を表す。
【００２６】
さらに本発明は、企業ネットワークファイアウォールの背後に格納された企業ネットワークのネットワークデータにリモートユーザがアクセスできるようにするための、コンピュータシステムにも及ぶ。これには、企業ネットワークとデータセンタとの間の仮想専用ネットワークとして動作するデータトンネルを開くこと、およびデータトンネルを介してネットワークデータを伝送することも含まれるが、これらに限定されるものではない。当分野の技術者であれば、本発明が、ポータブルコンピュータ、電話、ワイヤレス電話、ＰＤＡ、パーソナルコンピュータ、マルチプロセッサシステム、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などを含む、多くのタイプのコンピュータおよび電話システムを備えた、多くの環境で実施可能であることを理解されよう。
【００２７】
１．システム環境
図２は、ユーザ１０が、データセンタ４４と企業ネットワーク４０との間の仮想専用ネットワーク（ＶＰＮ）として動作するデータトンネル４２を介して企業ネットワーク４０のネットワークデータ２２にアクセスできるようにするための、本発明のシステムおよび方法の一実施形態を示す図である。一実施形態では、企業ネットワーク４０は、ファイアウォール２０および２８の背後で未許可のアクセスから保護されたネットワークデータ２２を含む、企業のコンピュータネットワークである。
【００２８】
本明細書で使用される場合、「企業ネットワーク」という用語は、相互にリンクされた処理デバイスによってタスクが実行される任意のコンピューティング環境を含むように、広義に解釈されるものとする。たとえば企業ネットワーク４０は、任意の企業、組合、個人、または他の団体のコンピューティング環境を含むことができる。企業ネットワーク４０

では、本発明の機能を実行するためのコンピュータ実行可能命令およびプログラムモジュールを、ローカルおよびリモートのメモリ記憶デバイス内に配置することができる。

【００２９】

「ネットワークデータ」および「企業ネットワークデータ」という用語は、ローカルおよびリモートのメモリ記憶デバイスに格納され、企業ネットワーク４０にアクセス可能な、任意のデータを含むように解釈されるものとする。たとえばネットワークデータ２２は、電子メールデータまたはＷｅｂページデータを含むことができる。一実施形態では、ネットワークデータ２２は、ファイアウォール２０および２８を含むファイアウォールインフラストラクチャの背後で保護される。ただし、ネットワークデータ２２は、たとえファイアウォールインフラストラクチャの背後で保護されていない場合でも、企業ネットワーク４０にアクセス可能な任意のデータを含むことができる。

【００３０】

「トンネル」という用語は、データがセキュアに伝送可能な任意のチャネルまたは他の通信回線を含むように解釈されるものとする。当分野の技術者であれば、トンネルを介して伝送されるデータが前記データへのアクセスを許可された識別済みユーザにのみ送達されるように、トンネルを介したセキュアな通信を可能にするために使用できる暗号化および認証の多数のプロトコルおよび方法があることを理解されよう。さらに、「トンネル」、「データトンネル」、および「チャネル」という用語は、本明細書で使用される場合は相互に交換可能であることも理解されたい。トンネルは、企業のファイアウォールインフラストラクチャを介したネットワークデータへのセキュアリモートアクセスを可能にすることによって、仮想専用ネットワークとして動作する。

【００３１】

本発明によれば、図３に示されるように、データトンネル４２は企業ネットワーク４０とデータセンタ４４との間に確立される。企業ネットワーク４０がデータ要求５０をデータセンタ４４に伝送し、データセンタ４４が回答データ５３の進行中の伝送で回答すると、データトンネル４２が開かれる。本明細書で使用される場合、「データ要求」という用語は、データセンタからのデータに関する要求を含むように広義に解釈されるものとし、Ｗｅｂページ、ハイパーテキストマークアップ言語（ＨＴＭＬ）データ、拡張可能マークアップ言語（ＸＭＬ）データ、またはＷｅｂサーバ６０の他のデータリソースへのアクセスを提供するためのデータセンタへの要求を表す、統一資源識別子（ＵＲＩ）を含むことができる。

【００３２】

図に示されるように、データ要求５０および回答データ５３は、企業ネットワーク４０のファイアウォール２０および２８を介して伝送される。当分野の技術者であれば、ファイアウォール２０および２８がハードウェア、ソフトウェア、またはその両方の組合せを含むことができることを理解されよう。本来ファイアウォールとは、ネットワークの指定されたポートを介したアクセスを禁止し、ネットワークデータが未許可のユーザによってファイアウォールの外部からアクセスされないことを保証する、セキュリティメカニズムである。

【００３３】

図３にも示されているように、データセンタ４４は、この実施形態ではＷｅｂサーバ６０を含むサーバでデータ要求５０を受信する。図２に示されるように、データセンタ４４は複数のＷｅｂサーバ６０、６０ａ、および６０ｂを含むことができることを理解されたい。複数のＷｅｂサーバ６０、６０ａ、および６０ｂは、データセンタ４４が複数の企業ネットワークと通信し、図示されていない複数のデータトンネルを維持できるようにするものである。本発明によれば、単一の企業ネットワークと単一のＷｅｂサーバとの間、または単一の企業ネットワークと複数のＷｅｂサーバとの間に、複数のデータトンネルを確立することができることを理解されたい。

【００３４】

ここで図３に戻ると、企業ネットワーク４０は自発的仮想専用ネットワーク（ＳＶＰＮ）

モジュール５２を使用して、実際にデータ要求５０をデータセンタ４４に伝送し、これに応答して回答データ５３を受信する。回答データ５３は、データ要求５０の受信に応答してデータセンタによって伝送され、データセンタ４４と企業ネットワーク４０との間のトンネル４２を開いたままにしておくように進行中の方法で伝送される、任意のデータを含むように解釈されるものとする。一実施形態では、これは企業ネットワーク４０がＷｅｂサーバ６０にＷｅｂページを開くように要求したときに達成され、Ｗｅｂページは、ＨＴＭＬ文書またはＸＭＬ文書などのＷｅｂサーバ６０によって提供される任意のタイプのデータリソースであってよい。これに応答して、Ｗｅｂサーバ６０はＷｅｂページの伝送を開始し、データの伝送が無期限の長い持続時間を有するような速度で、進行中の方法で伝送する。これにより、回答データ５３を企業ネットワーク４０に連続して伝送することによって、トンネル４２は開かれたままとなる。

【００３５】

ＳＶＰＮモジュール５２は、トンネル４２が確実に開いたままであるように監視する。何らかの理由でトンネル４２が閉じると、ＳＶＰＮモジュールは、新しいデータ要求をデータセンタ４４に伝送することによって、データセンタ４４との新しいデータトンネルを開く。本明細書では、具体的にはＳＶＰＮモジュール５２によって実行されるものとしていくつかの動作について述べるが、企業ネットワーク４０がＳＶＰＮモジュール５２を含む限りは、ＳＶＰＮモジュール５２によって実行される動作は、いずれも企業ネットワーク４０によって実行される動作でもあることを理解されたい。

【００３６】

ここで図２に戻ると、データセンタ４４はデータベース６２を含む。データベース６２は、Ｗｅｂサーバ６０によって維持される任意のデータトンネル４２を追跡する。Ｗｅｂサーバ６０はデータベース６２と通信し、データトンネル４２の状況をデータベース６２に通知する。これにより、データセンタ４４は、ネットワークデータ２２に関するユーザの要求を適切なＷｅｂサーバ６０に伝送することができる。ネットワークデータ２２に関するユーザ要求は、本明細書ではアクセス要求７０と呼ばれる。アクセス要求７０は、ユーザ１０によって開始された通信回線８４を介して、データセンタ４４によって受信される。

【００３７】

一実施形態では、ユーザ１０はアクセス要求７０を生成し、電話デバイスを使用してこのアクセス要求７０をデータセンタ４４に伝送する。この実施形態によれば、データセンタ４４の電話ノード８０がユーザ１０からのアクセス要求７０を受信する。アクセス要求７０を受信すると、電話ノード８０はＷｅｂサーバ６０と通信する。Ｗｅｂサーバ６０が、ネットワークデータ２２の要求元である適切な企業ネットワーク４０との確立されたデータトンネル４２を有する場合、アクセス要求７０はＷｅｂサーバ６０に伝送される。ただし、Ｗｅｂサーバ６０が適切な企業ネットワーク４０とのトンネル４２を確立していない場合、Ｗｅｂサーバ６０は、任意のＷｅｂサーバがあれば、どのＷｅｂサーバが適切な企業ネットワーク４０とのトンネル４２を確立しているかを判別するためにデータベース６２と通信し、この場合アクセス要求７０は適切なＷｅｂサーバに転送される。

【００３８】

代替実施形態では、電話ノード８０がデータベース６２と直接通信して、どのＷｅｂサーバが、アクセス要求７０がネットワークデータ２２へのアクセスを要求する適切な企業ネットワーク４０との確立されたトンネルを有するかを確認する。他の実施形態では、ユーザはＷｅｂサーバ６０との直接の通信回線８４を開始する。これはたとえば、ユーザがインターネットを介してＷｅｂサーバ６０にアクセスしたとき、またはＷｅｂサーバ６０のＷｅｂページが、パーソナルコンピュータまたはデータへのグラフィカルアクセスを提供できる他のデバイスを使用して、ユーザによってインターネットを介して開かれたときに達成される。

【００３９】

データセンタ４４と企業ネットワーク４０との間のデータトンネル４２は、伝送制御プロ

トコル／インターネットプロトコル（ＴＣＰ／ＩＰ）、セキュアソケットレイヤプロトコルを備えたハイパーテキスト転送プロトコル（ＨＴＴＰＳ）、およびＩＰセキュリティプロトコル（ＩＰｓｅｃ）を使用する。これらのプロトコルを使用して、データ要求、ネットワークデータ、回答データ、およびアクセス要求はパケットで暗号化され、企業ネットワークの図示されていない「ポート４４３」を使用してデータトンネル４２を介して伝送される。「ポート４４３」は、ユーザがファイアウォール２０および２８内の企業ネットワーク４０からインターネットにアクセスできるようにするために、すでに開かれている。

【００４０】

他の実施形態では、データトンネル４２が企業ネットワークの「ポート８０」を介して確立され、その結果、データ要求、ネットワークデータ、回答データ、およびアクセス要求はＴＣＰ／ＩＰ、ＩＰｓｅｃ、およびセキュアソケットレイヤプロトコル（ＳＳＬ）を使用しないハイパーテキスト転送プロトコル（ＨＴＴＰ）を使用して暗号化される。本発明は、レイヤ2転送（Ｌ２Ｆ／Ｌａｙｅｒ　Ｔｗｏ　Ｆｏｒｗａｒｄｉｎｇ）およびレイヤ２トンネリングプロトコル（Ｌ２ＴＰ／Ｌａｙｅｒ　Ｔｗｏ　Ｔｕｎｎｅｌｉｎｇ　Ｐｒｏｔｏｃｏｌ）を含む、任意のインターネットトンネリングプロトコルを使用できることを理解されたい。「ポート８０」も、企業ネットワーク４０のファイアウォールインフラストラクチャ内からのインターネットアクセスを可能にするために、すでに開かれている。この実施形態によれば、図３～４に示されるように、プロキシサーバ８２はデータパケットが定義済みのプロトコルに準拠していることを検証するために、データパケットをフィルタリングする。データ要求５０、ネットワークデータ２２、回答データ５３、またはアクセス要求１０が適切にパケット化されていない場合、プロキシサーバ８２はデータトンネル４２を通過させない。この方法では、プロキシサーバ８２が、許可されたデータ伝送および要求のみがデータトンネル４２を介して企業ネットワーク４０から外へまたは企業ネットワーク４０内部に確実に伝送されるようにすることにより、ファイアウォールインフラストラクチャの保護を強化する。

【００４１】

前述のように、本発明はファイアウォールインフラストラクチャ内に以前から存在する開かれたポートを使用して、リモートモバイル位置からのセキュアなＶＰＮタイプ通信を実行可能にする。したがって、本発明は、高度かつ費用のかかるＶＰＮハードウェアおよびソフトウェアを設置する必要が生じるような、ファイアウォールインフラストラクチャ内で追加ポートを開く必要がないため、従来技術を超える改良であることを理解されたい。さらに本発明は、プロキシサーバが、ポートを介して伝送されるどんなデータパケットも定義済みプロトコルに確実に準拠するようにフィルタリングできるようにするものである。

【００４２】

上記で述べたシステムおよび環境は、ユーザがポータブルデバイスを使用して、リモート位置から仮想専用ネットワークを介して企業ネットワークのネットワークデータにアクセスできるようにするための、本発明の方法を実施するための好適な環境およびシステムである。

【００４３】

２．ネットワークデータへのユーザアクセス

ユーザがリモート位置からネットワークデータにアクセスできるようにするための本発明の方法の一実施形態が、図４および５に示されている。ここで図４を見ると、リモート位置から企業ネットワーク４０のネットワークデータ２２にアクセスしようとするユーザ１０は、インターネットに接続された電話デバイスまたはコンピューティングデバイスなどの通信デバイスを使用して、データセンタ４４との通信回線８４を開く。データセンタ４４は、ユーザ１０が企業ネットワーク４０のネットワークデータ２２にアクセスする権限を有することを検証するために、ユーザ１０のアイデンティティを認証する。一実施形態では、ユーザが電話デバイスまたはインターネットコンピューティングデバイスを使用し

て個人識別番号を入力すると、ユーザのアイデンティティが認証される。他の実施形態では、ユーザ１０に割り当てられた対応する公開鍵および秘密鍵を有する対鍵（ｔｗｉｎ－ｋｅｙ）暗号化などの暗号化技術を使用し、インターネットを介してユーザのアイデンティティが確認される。当分野の技術者であれば、いずれも本発明に従って使用可能な、ユーザのアイデンティティを認証するためのさまざまな方法があることを理解されよう。ユーザのアイデンティティを認証するための他のこうした方法にはトークンおよびスマートカードが含まれるが、これらに限定されるものではない。

【００４４】

いったんユーザ１０のアイデンティティが認証されると、ユーザは、データセンタ４４にアクセス要求を伝送し、ここでＷｅｂサーバ６０によって受信される。アクセス要求７０は、ネットワークデータ２２へのアクセスを要求する任意の要求を含むことができる。たとえば、アクセス要求７０は、ファイアウォールインフラストラクチャの背後に保護されたかまたは企業ネットワークにアクセス可能な、電子メールメッセージ、Ｗｅｂページ、または企業ネットワークの他のデータへのアクセスを受信する要求を含むことができる。一実施形態では、ユーザ１０はコンピュータデバイスを使用して、インターネットを介してＷｅｂサーバ６０との通信回線８４を開く。この実施形態では、アクセス要求７０はＷｅｂサーバ６０によって直接受信される。他の実施形態では、ユーザ１０は電話デバイスを使用してデータセンタ４４にアクセス要求７０を伝送する。この代替実施形態によれば、図２を参照して上記で説明したように、アクセス要求は電話ノード８０を介してＷｅｂサーバ６０によって間接的に受信される。

【００４５】

アクセス要求７０を受信すると、Ｗｅｂサーバ６０は、図２および３を参照しながら上記で説明したように、企業ネットワーク４０の初期要求で開かれた確立されたデータトンネル４２を介してアクセス要求７０を企業ネットワーク４０に伝送する。アクセス要求７０は、回答データ５３と共にパケット化される。

【００４６】

アクセス要求７０は、ＳＶＰＮモジュール５２で企業ネットワーク４０によって受信される。企業ネットワーク４０は、アクセス要求７０によって要求されたネットワークデータ２２に関して任意の動作を実行することによって、アクセス要求７０を処理する。一実施形態では、ネットワークデータに関して実行可能な動作が、ＳＶＰＮモジュール５２の構成に従って事前に定義される動作に限定される。事前に定義される動作は、企業ネットワークがＳＶＰＮモジュール５２に実行可能にさせたい任意の動作を含むことができる。ネットワークデータ２２に関してどの動作が実行されるかをＳＶＰＮモジュール５２が制御できるようにすることによって、企業ネットワーク４０はネットワークデータ２２へのアクセス制御を維持し、ネットワークデータ２２が企業ネットワーク４０内でどのように操作されるかを制御することができる。事前に定義される動作は、電子メールヘッダの取出し、電子メールメッセージ本体の取出し、Ｗｅｂページデータの取出し、電子メールの削除、電子メールデータまたはＷｅｂページデータのユーザへのファックス送信、ネットワークデータ２２のデータセンタ４４への送信を含むことができるが、これらに限定されるものではない。ＳＶＰＮモジュール５２は、Ｐｏｓｔ Ｏｆｆｉｃｅ Ｐｒｏｔｏｃｏｌ（ＰＯＰ）またはＳｉｍｐｌｅ Ｍａｉｌ Ｔｒａｎｓｆｅｒ Ｐｒｏｔｏｃｏｌ（ＳＭＴＰ）を含むことができるがこれらに限定されることのない適切な手段を使用して、企業ネットワークからネットワークデータを取得する。

【００４７】

ＳＶＰＮモジュール５２は、第２のデータトンネル９０を介してネットワークデータ２２をデータセンタ４４に返信する。第２のデータトンネル９０は、企業ネットワーク４０とデータセンタ４４との間の一時仮想専用ネットワークとして動作する。データトンネル９０は、データトンネル４２に使用されるものと同じポート、インターネット「ポート４４３」を介して確立され、上記と同じプロトコルを使用して、データ伝送のセキュリティを保証する。他の実施形態では、対応するプロトコルと共に「ポート８０」が使用される。

プロキシサーバ８２は、所望のプロトコルが確実に準拠されるようにする。
【００４８】
データトンネル９０は、回答データ５３を企業ネットワーク４０に送信しているものと同じＷｅｂサーバ６０で確立されるか、またはデータセンタ４４の表示されていない別のＷｅｂサーバで確立される。データトンネル９０は閉じられ、ネットワークデータ２２がデータセンタ４４によって受信されると同時に、ネットワークデータ２２へのアクセスがユーザ１０に提供される。ユーザ１０によってデータセンタ４４と通信するために電話デバイスが使用される場合、ネットワークデータ２２は図２に示された電話ノード８０を介してＷｅｂサーバ６０からユーザに送信される。
【００４９】
本発明は、ユーザがネットワークデータへの音声アクセスを受け取れるようにするために、音声インターフェースを電子文書に提供するための方法と組み合わせて実施できることを理解されたい。一実施形態では、ネットワークデータ２２は電子メールメッセージを含み、データセンタ４４はユーザの電話デバイスを介して電子メールメッセージのテキストをユーザ１０に対して読み上げるか、あるいは電子メールメッセージをユーザの電話デバイス上に表示する。他の実施形態では、ユーザ１０は、Ｗｅｂサーバ６０と直接確立された通信回線８４からインターネットを介してネットワークデータ２２に直接アクセスする。
【００５０】
ユーザは、それぞれが別々に処理されるアクセス要求をいくつでも生成することができる。ユーザ要求を別々のトランザクションに分けることにより、本発明は、許可されたユーザまたは未許可のユーザのネットワークデータに関する管理が多くなり過ぎないようにすることで、ネットワークデータのセキュリティおよび管理を強化する。
【００５１】
図５は、本発明の一実施形態を示す流れ図である。図に示されるように、ステップ１００では、企業ネットワークがデータ要求をデータセンタに送信する。ステップ１０２でデータ要求を受信すると、データセンタはステップ１０４で進行中の回答データを企業ネットワークに返信する。一実施形態では、回答データにＨＴＭＬデータおよびＸＭＬデータなどのマークアップ言語データが含まれる。ステップ１０６では、企業ネットワークが進行中の回答データを受信する。ステップ１００～１０６で、企業ネットワークとデータセンタとの間にデータトンネルが確立される。一実施形態では、「ポート４４３」を介してデータトンネルが確立される。他の実施形態では、「ポート８０」を介してデータトンネルが確立される。
【００５２】
ユーザは、ステップ１０８でデータセンタへ最初に接続することによって、企業ネットワークのネットワークデータにアクセスする。次にユーザは、ステップ１１０でアクセス要求を生成し、データセンタに送信する。一実施形態では、アクセス要求はユーザによって電話デバイスを使用して生成される。代替の実施形態では、ユーザはコンピュータを使用してインターネットを介してアクセス要求を生成する。ステップ１１２でアクセス要求を受信すると、データセンタはステップ１１４で、ステップ１００～１０６で確立されたデータトンネルを介してアクセス要求を企業ネットワークに送信する。
【００５３】
企業ネットワークは、ステップ１１６でアクセス要求を受信し、ステップ１１８でアクセス要求が有効なアクセス要求であるかどうかを判別する。これは、アクセス要求が事前に定義される許可された動作のみがネットワークデータ上で実行されるように要求することの検証を含むことができる。ユーザのアイデンティティの妥当性検査動作を含むこともできる。限定的ではなく例示的なものとして、ステップ１１８では、意思決定の結果、電子メールメッセージの取出しが有効な要求であること、および添付の実行可能プログラムが有効な要求でないものとする。有効なアクセス要求の構成内容は事前に決定しておくことが可能であり、ＳＶＰＮモジュールによって制御される。アクセス要求が有効でない場合

、企業ネットワークは要求を処理せず、ステップ１２０で有効な要求が受信されるまで待機する。

【００５４】

アクセス要求が有効であり、ネットワークデータをユーザに返信するように要求する場合、ステップ１２４でネットワークデータが取り出され、その後、ステップ１２６に示された企業ネットワークとデータセンタの間に開かれた一時データトンネルを介して、ステップ１２８でデータセンタに送信される。この実施形態では、ステップ１２６で開かれる一時データトンネルは、ステップ１００～１０６で確立されたデータトンネルとは異なる。ただし、どちらのトンネルも、企業ネットワークの同じポートを介して確立できることを理解されたい。

【００５５】

ネットワークデータがデータセンタに送信された後、ステップ１３０で一時データトンネルが閉じられ、ステップ１２０で企業ネットワークは後続の有効な要求が受信されるまで待機する。アクセス要求が、電子メールの削除、電子メールメッセージのファックス送信、および電子メールの転送などの動作を実行するように要求するものであれば、企業ネットワークはステップ１３８で要求されたタスクを実行し、ステップ１２０で後続の有効な要求が受信されるまで待機する。

【００５６】

データセンタは、要求されたネットワークデータをステップ１３２で企業ネットワークから受信すると同時に、要求されたネットワークデータをステップ１３４でユーザに送信する。一実施形態では、これは要求されたデータをユーザが見ているＷｅｂページ上に表示することによって達成される。他の実施形態では、要求されたネットワークデータは、ユーザが使用している電話デバイスにデジタル形式または音声形式のいずれかで送信される。ユーザは要求されたネットワークデータをステップ１３６で受信し、ステップ１３８でデータセンタから切り離すか、またはステップ１１０で後続のアクセス要求をデータセンタに送信する。

【００５７】

本発明によれば、ユーザは、データセンタのデータベースにキャッシュされたネットワークデータにアクセスすることもできる。図２を参照しながら説明されるこの実施形態によれば、たとえユーザ１０がネットワークデータ２２に関するアクセス要求７０を生成する前であっても、ネットワークデータ２２はデータベース６２にキャッシュされる。この実施形態は、ネットワークデータ２２が切り離されているときに、ユーザ１０がネットワークデータ２２に即時にアクセスできるようにする場合に特に有用である。ネットワークデータ２２は、企業ネットワーク４０によって容易にまたは即時に取出し可能でない場合は必ず切り離される。たとえば、ネットワークデータ２２が企業ネットワーク４０内のかなりの大容量リモートメモリデバイスに格納される場合、ネットワークデータ２２を取り出すには数分かかる場合がある。切り離されている他のネットワークデータ２２には、電源が切断されているコンピュータのデスクトップまたはローカルコンピュータドライブに格納されたデータも含まれる。切り離されたネットワークデータの他の例には、ラップトップコンピュータまたはＰＤＡなどの、企業ネットワーク４０から定期的に切り離されるポータブルコンピュータまたは記憶デバイス上に格納された任意のデータもある。

【００５８】

この実施形態によれば、企業ネットワーク４０は、ＳＶＰＮ　５２とＷｅｂサーバ６０との間に新しい一時データトンネルを確立する。一時データトンネルは、図４を参照しながら説明したデータトンネル９０と同様の様式で確立される。一時データトンネルがいったん確立されると、ネットワークデータ２２が一時データトンネルを介してデータセンタ４４のデータベース６２にアップロードされる。ネットワークデータ２２のアップロードプロセスには、前述の確立されたプロトコルに従ってネットワークデータをパケット化する動作が含まれる。いったんネットワークデータ２２が受信されると、データセンタ４４はネットワークデータ２２のコピーをデータベース６２にキャッシュする。キャッシュされ

たネットワークデータ２２のコピーは、データベース６０がネットワークデータ２２の新しいバージョンを受信すると必ず更新される。ネットワークデータ２２の新しいバージョンが受信される頻度は、企業ネットワーク４０の許可および構成によって事前に決定される。

【００５９】

例示的なものであって限定的でない一例では、企業ネットワークは、企業ネットワークのすべてのユーザが受信する通知を生成する。この通知は、ユーザが自分の電子メール連絡、アドレスリスト、会社ファイル、および他の指定のネットワークデータ２２をアップロードすることを想起させるものであって、その結果、更新されたデータを企業ネットワーク４０から離れたオフサイトで取り出すことができる。この実施形態によれば、ユーザ１０は、どのネットワークデータ２２をデータセンタ４４に送信するか、およびユーザ１０がどのように応答するかによってどのネットワークデータ２２をデータベース６２にキャッシュするかを制御する。ユーザ１０は、たとえば通知を無視することによって応答することができる。あるいはユーザ１０は、ＳＶＰＮ　５２モジュールが指定されたネットワークデータ２２をデータセンタ４４のデータベース６２にアップロードできるようにするコマンドを開始することによって、応答することができる。前述のように、ネットワークデータの更新は、ＳＶＰＮ　５２モジュールとＷｅｂサーバ６０との間に確立された一時データトンネルを介して送信される。データパケットが受信されると、Ｗｅｂサーバ６０はユーザのネットワークデータ２２を復号し、これをデータベース６２に送信して、ここでキャッシュされる。

【００６０】

この実施形態は、ユーザが仮想専用ネットワークとして動作する一時データトンネルを介して切り離されたデータの同期をとれるようにするものであり、その結果、後でリモート位置からアクセスできるようにするものであることを理解されたい。この実施形態は、ネットワークデータが企業ネットワークから切り離されている場合、ユーザがデータセンタのデータベースにキャッシュされたネットワークデータのコピーに即時にアクセスできるようにするものでもある。たとえば、ネットワークデータが、ポータブルで物理的に切り離されたコンピュータ上に格納される場合、使用不能なネットワーク記憶ドライブに格納される場合、ネットワークの問題によってネットワークデータの取出しが困難な場合、および接続および処理の速度が遅いためにネットワークデータの取出しに長時間かかる場合などに、ネットワークデータが切り離される。

【００６１】

本実施形態によれば、ユーザ１０は、電話システムを使用してデータセンタ４４を呼び出すこと、およびネットワークデータ２２に関するアクセス要求７０を生成することにより、電子メール連絡などのネットワークデータ２２にアクセスする。データセンタ４４の電話ノード８０は、ユーザの呼出しおよび付随するアクセス要求７０を受信する。さらに電話ノード８０は、データベース６２からアップロードされたネットワークデータ２２を取り出し、アップロードされたネットワークデータ２２をユーザ１０に返信する。代替実施形態によれば、ユーザ１０はインターネットを介してデータセンタ４４に直接アクセスし、この場合、Ｗｅｂサーバ６０はユーザのアップロードされたネットワークデータ２２をデータベース６２から取り出して、ユーザ１０に返信する。

【００６２】

本実施形態は、ユーザ１０とデータセンタ４４との間に確立された通信回線８４を介して、データセンタ４４に直接コマンドを発行することによって、ユーザ１０がネットワークデータ２２を更新できるようにするものでもある。例示的なものとして、ユーザは、データセンタのデータベースに格納されたネットワークデータのキャッシュ済みコピーから、電子メール連絡を削除するコマンドを発行することができる。この例によれば、データセンタ４４は電子メール連絡を削除することによって応答し、これによって、データセンタでネットワークデータのキャッシュされたコピーを効率的に更新する。次にデータセンタ４４は、更新に関する情報を企業ネットワーク４０に送信する。これは、データトンネル

４２などの確立されたデータトンネルを介して企業ネットワーク４０に送信される更新情報を、回答データ５３に埋め込むことによって達成される。回答データ５３の送信は、図３および４を参照してより詳細に図示および記載される。

【００６３】

ＳＶＰＮモジュールはネットワークデータの更新を受信し、これに応じて企業ネットワークデータを更新する。これで、企業ネットワークデータ２２を、データセンタ４４のデータベース６２に格納されたネットワークデータのキャッシュされたコピーと同期させる。この実施形態は、リモートユーザが、データセンタのデータベースに格納されたネットワークデータを更新し、さらに企業ネットワークのネットワークデータをデータセンタに格納されたネットワークデータの更新済みキャッシュコピーと同期させることによって、企業ネットワークに格納されたネットワークデータを更新できるようにするものであることを理解されたい。

【００６４】

前述の内容に鑑みて、本発明は従来の技術を超える改良であることを理解されたい。具体的に言えば、本発明は、企業がデータチャネルを介したネットワークデータへのアクセス許容量を制限する機能を保持しながら、ユーザがセキュアデータチャネルを介したネットワークデータへのモバイルリモートアクセスを有することができるようにするものである。さらに本発明は、リモートユーザが企業ネットワークから切り離されたネットワークデータにアクセスできるようにするものでもある。さらに本発明は、ユーザがリモート位置から仮想専用ネットワークデータトンネルを介してネットワークデータを更新できるようにするものでもある。

【００６５】

本発明は、その精神または本来の特性を逸脱することなく、他の特有の形式で実施することができる。記載された実施形態は、すべての点において、限定的なものではなく単に例示的なものとみなされる。したがって本発明の範囲は、前述の説明によってではなく、添付の特許請求の範囲によって示される。特許請求の範囲と等価の意味および範囲内でのすべての変更は、その範囲内に包含されるものである。

【図面の簡単な説明】

【図１】　ユーザおよびリモート企業ネットワークが、仮想専用ネットワークトンネルを介して企業のデータにアクセスできるようにするための、従来技術のシステムを示す図である。

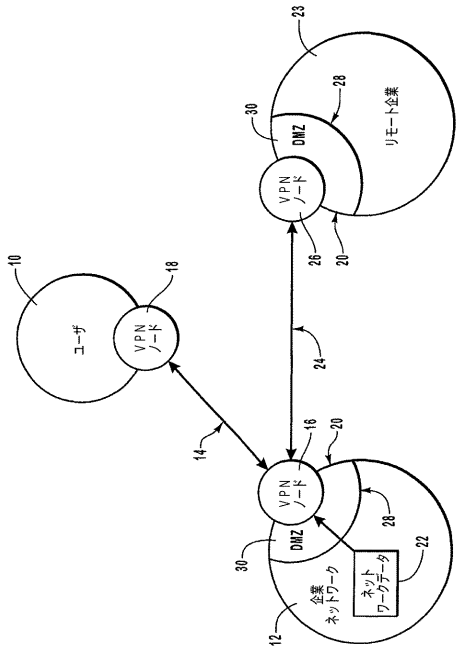
【図２】　本発明に好適なオペレーティング環境を提供する例示的システムにおいて、データセンタのＷｅｂサーバと通信する企業ネットワークと、データセンタの電話ノードと通信するユーザとを示す図である。

【図３】　企業ネットワークからデータセンタへデータ要求を送信することと、企業ネットワークがデータセンタから回答データを受信することを含む、企業ネットワークとデータセンタとの間にデータトンネルを確立するための方法を示す図である。

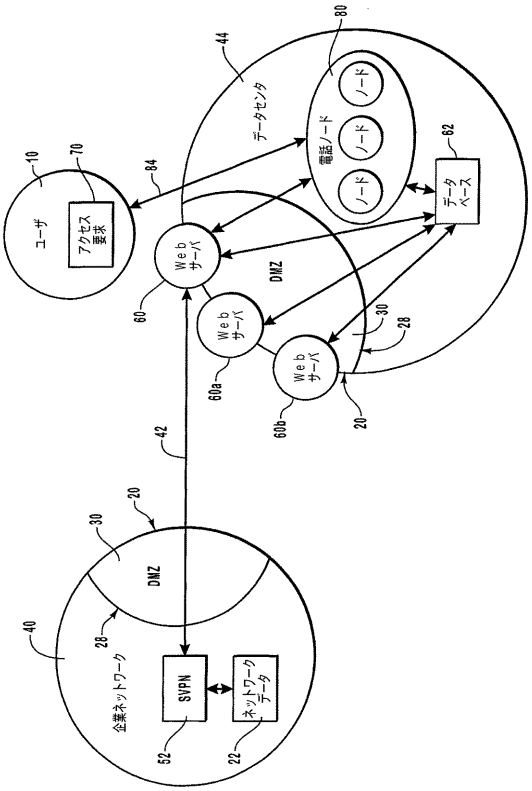
【図４】　ユーザがネットワークデータにアクセスできるようにするために企業ネットワークからデータセンタへネットワークデータを送信するための方法を示す図であって、ネットワークデータは企業ネットワークとデータセンタとの間のデータトンネルを介して伝送される。

【図５】　ユーザが企業ネットワークからのネットワークデータにアクセスできるようにするための本発明の方法の一実施形態を示す流れ図である。

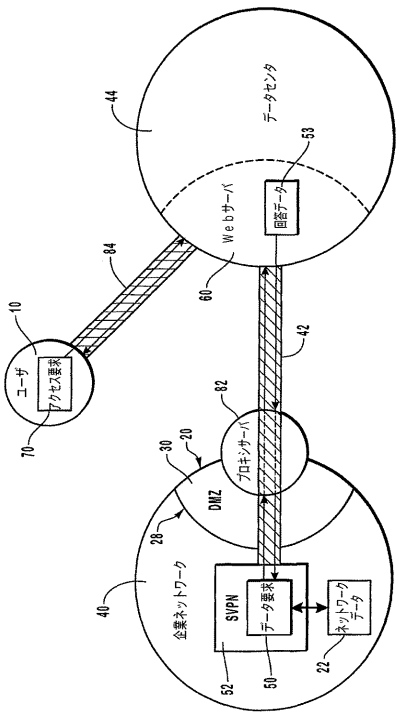
【図１】


ユーザ
VPN ノード
リモート企業
DMZ
企業 ネットワーク
ネット ワークデータ

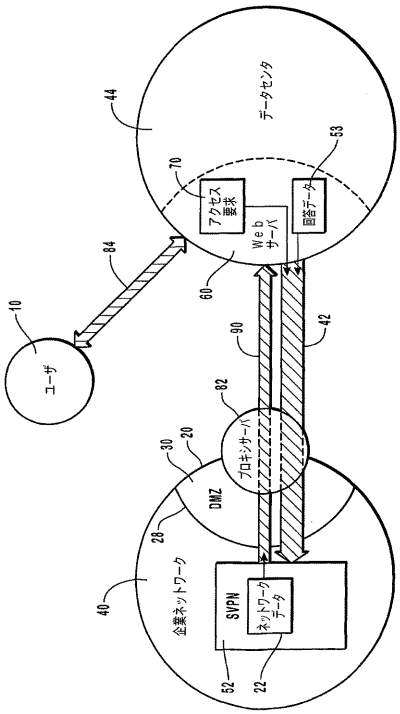
【図２】


ユーザ
アクセス要求
データセンタ
電話ノード
ノード
データ ベース
Web サーバ
DMZ
企業ネットワーク
SVPN
ネットワーク データ

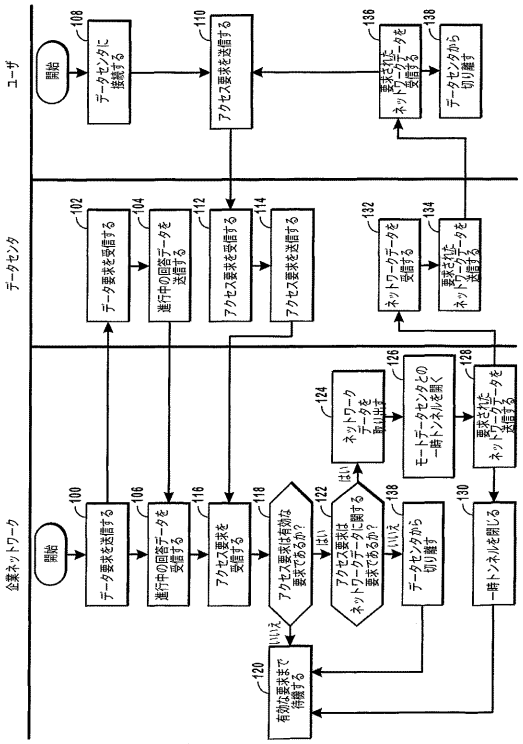
【図３】


ユーザ
アクセス要求
データセンタ
Web サーバ
回答データ
プロキシサーバ
DMZ
企業ネットワーク
SVPN
データ要求
ネットワーク データ

【図４】


ユーザ
データセンタ
アクセス要求
Web サーバ
回答データ
プロキシサーバ
DMZ
企業ネットワーク
SVPN
ネットワーク データ

【図５】


ユーザ
データセンタ
企業ネットワーク
開始
データセンタに接続する
データ要求を送信する
データ要求を受信する
進行中の回答データを送信する
進行中の回答データを受信する
アクセス要求を送信する
アクセス要求を受信する
アクセス要求を送信する
アクセス要求を受信する
アクセス要求は有効な要求であるか?
はい
いいえ
アクセス要求はネットワークデータに関する要求であるか?
はい
いいえ
ネットワークデータを取り出す
モートデータセンタとの一時トンネルを開く
要求されたネットワークデータを送信する
ネットワークデータを受信する
要求されたネットワークデータを受信する
データセンタから切り離す
一時トンネルを閉じる
有効な要求まで待機する
データセンタから切り離す

フロントページの続き

(72)発明者　ダレン　エル．ウエスマン
アメリカ合衆国　８４０５４－３３６８　ユタ州　ノース　ソルト　レイク　ノース　フェアーウェイ　ドライブ　２２９

審査官　清水　稔

(56)参考文献　米国特許第０６０８１９００（ＵＳ，Ａ）
特開平１０－２２４４０９（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
H04L 12/56
G06F 13/00
G06F 15/00
G09C 1/00