(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4699461号
(P4699461)
(45)発行日　平成23年6月8日(2011.6.8)　(24)登録日　平成23年3月11日(2011.3.11)

(51)Int.Cl.　F I
H04L 12/66 (2006.01)　H04L 12/66 B

請求項の数 15　(全 16 頁)

(21)出願番号	特願2007-523678 (P2007-523678)	(73)特許権者	508320505
(86)(22)出願日	平成17年7月22日 (2005.7.22)		バークレイズ・キャピタル・インコーポレーテッド
(65)公表番号	特表2008-508797 (P2008-508797A)		アメリカ合衆国・ニューヨーク・１００１９・ニュー・ヨーク・セヴンス・アヴェニュー・７４５
(43)公表日	平成20年3月21日 (2008.3.21)	(74)代理人	100108453
(86)国際出願番号	PCT/US2005/026215		弁理士　村山　靖彦
(87)国際公開番号	WO2006/014842	(74)代理人	100064908
(87)国際公開日	平成18年2月9日 (2006.2.9)		弁理士　志賀　正武
審査請求日	平成19年4月10日 (2007.4.10)	(74)代理人	100089037
(31)優先権主張番号	10/903,941		弁理士　渡邊　隆
(32)優先日	平成16年7月30日 (2004.7.30)	(74)代理人	100110364
(33)優先権主張国	米国(US)		弁理士　実広　信哉
前置審査			

最終頁に続く

(54)【発明の名称】確実なネットワーク接続性のためのシステム及び方法

(57)【特許請求の範囲】
【請求項１】
内部のネットワークへの遠隔コンピュータのアクセスを許容する方法であって、
遠隔コンピュータからアクセス要求を受信するステップと、
遠隔コンピュータの構成状態を表わす構成情報を要求して受信するステップであって、該要求された構成情報は、遠隔コンピュータから受信されたアクセス要求に少なくとも基づくものである前記ステップと、
遠隔コンピュータから受信された構成情報に少なくとも基づく安全政策との遠隔コンピュータの順応性を決定するステップと、
遠隔コンピュータが安全政策と順応しないならば、遠隔コンピュータの構成状態を表わす追加の構成情報を要求して受信するステップであって、追加の構成情報要求は、受信された構成情報及び安全政策に少なくとも基づくものである前記ステップと、
遠隔コンピュータが、安全政策と順応するならば、内部のネットワークへの遠隔コンピュータのアクセスを許容するステップと、
を含む方法。
【請求項２】
受信された追加の構成情報が、禁止された構成状態を含むならば、内部のネットワークへのアクセスを拒否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】
内部のネットワークへの遠隔コンピュータのアクセスを許容するステップは、遠隔コン

ピュータにアクセストークンを送信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】
アクセストークンは、所定の期間後に満了する請求項３に記載の方法。
【請求項５】
アクセス要求は、内部のネットワークによって維持される複数のアクセス・レベルから選択された要求されたアクセス・レベルを含み、複数のアクセス・レベルの各々は、ネットワークへのアクセスを認可する請求項３に記載の方法。
【請求項６】
送信されたアクセストークンは、認可されたアクセス・レベルを含む請求項５に記載の方法。
【請求項７】
受信された構成情報に基づいて、遠隔コンピュータが要求されたアクセス・レベルに関連した安全政策に順応（一致）しないが、認可されたアクセス・レベルに関連した安全政策と順応（一致）するときに、認可されたアクセス・レベルは、要求されたアクセス・レベルでない請求項６に記載の方法。
【請求項８】
遠隔コンピュータから安全化された内部のネットワークにアクセスする方法であって、
（ａ）内部のネットワークと通信してゲートウェイ・サーバにアクセス要求を送信するステップと、
（ｂ）ゲートウェイ・サーバから構成情報要求を受信するステップと、
（ｃ）要求された構成情報をサーバに送信するステップと、
（ｄ）アクセストークンがゲートウェイ・サーバから受信されるまでステップ（ｂ）－（ｃ）を繰り返すステップと、
（ｅ）内部のネットワークにアクセスするために、受信されたアクセストークンを送信するステップと、
を含み、アクセス要求は、要求されたアクセス・レベルを含み、該要求されたアクセス・レベルは、内部のネットワークによって維持される複数のアクセス・レベルから選択され、複数のアクセス・レベルの各々は、ネットワーク・リソースへのアクセスを認可し、アクセストークンは、遠隔コンピュータの構成状態を表わす構成情報が内部のネットワークの安全政策と順応する場合に、遠隔コンピュータへ送信される方法。
【請求項９】
受信されたアクセストークンは、認可されたアクセス・レベルを含む請求項８に記載の方法。
【請求項１０】
送信された構成情報に基づいて、遠隔コンピュータが要求されたアクセス・レベルに関連した安全政策に順応（一致）しないが、認可されたアクセス・レベルに関連した安全政策と順応（一致）するときに、認可されたアクセス・レベルは、要求されたアクセス・レベルでない請求項９に記載の方法。
【請求項１１】
構成情報要求を受信するステップは、さらに、
ゲートウェイ・サーバからプログラムを受信するステップと、
該プログラムを実行するステップと、
を含む請求項８に記載の方法。
【請求項１２】
受信されたアクセストークンは、所定の期間後に満了する請求項８に記載の方法。
【請求項１３】
外部ネットワークを介して遠隔コンピュータによる内部のネットワークへのアクセスを許容するようコンピュータを制御するための命令を含むコンピュータ読取り可能媒体であって、
遠隔コンピュータからのアクセス要求を受信し、

アクセス要求に少なくとも基づく少なくとも遠隔コンピュータの構成状態を表わす構成情報要求を遠隔のコンピュータに送り、
遠隔コンピュータから構成情報要求に対する応答を受信し、
遠隔コンピュータから受信された応答に基づいて該遠隔コンピュータが内部のネットワークの安全政策と順応することを確認し、
受信された応答が安全政策と順応しないならば、遠隔コンピュータに追加の構成情報要求を送り、該追加の構成情報は、遠隔コンピュータの構成状態を表わすとともに、受信された応答及び安全政策に少なくとも基づいて要求され、そして
遠隔コンピュータが内部のネットワークの安全政策と順応するならば、遠隔コンピュータの内部のネットワークへのアクセスを許容する
ことにより、外部ネットワークを介して遠隔コンピュータによる内部のネットワークへのアクセスを許容するようコンピュータを制御するための命令を含むコンピュータ読取り可能媒体。
【請求項１４】
受信された応答が禁止された構成状態を含むならば、内部のネットワークへのアクセスを拒否するための命令をさらに含む請求項１３に記載のコンピュータ読取り可能媒体。
【請求項１５】
安全化されたネットワークであって、
内部の通信ネットワークと、
該内部の通信ネットワーク及び外部の通信ネットワークに接続されるゲートウェイ・コンピュータと、を備え、該ゲートウェイ・コンピュータは、外部の通信ネットワークを介して遠隔コンピュータから内部の通信ネットワークに接続するための要求を受信するよう適合され、そして、さらに、遠隔コンピュータの内部の通信ネットワークへのアクセスを許容する前に、遠隔コンピュータの構成状態を表わす構成情報が複数の安全政策の少なくとも１つと順応するのを確認するよう適合されている安全化されたネットワーク。
【発明の詳細な説明】
【背景技術】
【０００１】
ユーザが内部の会社のネットワーク及びリソースに外部からアクセスするのを多くの会社が許容する。このような１つの方法は、仮想私設ネットワーク（ＶＰＮ）接続を用いる。代表的なシナリオにおいては、遠隔のコンピュータで働いているユーザがインターネットに接続して、顧客側のＶＰＮプログラムを開始する。ＶＰＮプログラムは、会社のＶＰＮゲートウェイ・コンピュータにアクセスするために、受容可能なネットワーク・プロトコルを用いる。ゲートウェイ・コンピュータ、例えばＶＰＮサーバは、ユーザを認証して、遠隔のユーザのための遠隔ネットワーク・セッションを創設する。このようなＶＰＮセッションの１つの利点は、遠隔のユーザのコンピュータが、会社のネットワークに直接存在しているように見えることである。
【０００２】
内部の会社のネットワークは、安全性の理由のために外部のネットワークもしくはインターネットから通常バッファリングもしくは隔離される。内部のネットワークへの及び内部のネットワークからのインターネット・トラフィックは、会社の安全政策に基づいてフィルタリングされ得る。安全政策は、ファイル及びデータベースのアクセスに制限され得るか、もしくは制限されないインターネット・アクセスを有するコンピュータに対して任意の会社のリソースへのアクセスを制限するかまたは禁止し得る。例えば、或るユーザもしくはコンピュータだけが外部のネットワーク接続を創設して外部の世界と通信し得るように許容され得る。しかしながら、これらのコンピュータは、顧客のデータを記憶するデータベースにアクセスすることから妨げられ得る。これは、ウィルス及び存在するほかの脅威から会社のリソース及びコンピュータを保護するために行われる。他の安全政策は、内部のネットワークにログオンするのに先立って会社の安全性チェックでの検証及び承認を必要とし得る。

【０００３】
この形態の内部的な隔離は、代表的には、どんな遠隔のユーザも内部の会社のネットワークに接続することを許容されない場合には適切である。しかしながら、会社の安全政策の要件を実施しつつ内部の会社のリソースへの遠隔ユーザのアクセスを許容するという基本的な問題がある。これは、遠隔のコンピュータが代表的には、適所にフィルタを持たない、もしくは、単にファイアウォールを持たないインターネットにアクセスするという点において明白である。この状況においては、遠隔のコンピュータがＶＰＮ接続を介して会社のサーバに接続するとき、会社は、顧客のコンピュータにその内部安全政策を実施することができない。従って、遠隔のコンピュータは、重要なデータにアクセスすることができ、すなわち、それは、同じ内部安全要件に叶うことなく、かつ、外部の脅威からバッファリングされることなく、内部のネットワークに直接接続されるように見える。このことは、信用の無い遠隔コンピュータが会社のネットワークに無制限にアクセスするであろうという点において会社の安全にとって関心事である。

【０００４】
この危険は、遠隔コンピュータがＶＰＮを使用しつつ適正に保護され、そして、信用の無いものではない場合には緩和され得る。しかしながら、遠隔コンピュータは、会社の直接制御下にないので、現在の顧客駆動安全方法では、このことを確実にすることができない。

【０００５】
これらの問題を扱うために種々の試みが行われてきたが、会社の安全政策に厳密に密着したものは完全には提供されていない。殆どの解決法は、ＶＰＮアクセスを許容する前に、顧客のコンピュータ安全政策、または、安全政策の顧客が行う強化に頼っている。例えば、多くのＶＰＮ顧客プログラムは、ウィルス・スキャナ及び可能な場合には遠隔の顧客の機械上の個人のファイアウォールの存在をチェックする。この情報は、サーバにとって有用であり得るが、それは、顧客のコンピュータが信用の無いものではないということを確実にはしない。さらに、或るウィルスは、ウィルス・チェッカー及びファイアウォールを迂回し得、もしくは、遠隔コンピュータが能動的なＶＰＮセッション中に信用の無いものになり得る。

【０００６】
他の安全チェックは、今日までのデータ・ウィルス定義を確認することのように、もしくは、製品のＢｌａｃｋＩＣＥ™ファミリーのような安全プログラムが存在するということを確実にするように、顧客のコンピュータ上で実行され得る。しかしながら、これらの解決法は、未だに、顧客によって開始された認証に頼っており、そして顧客によって認証された情報がサーバに提起される。顧客のコンピュータが信用の無いものである場合には、不正確な情報がサーバに通され得る。

【発明の開示】
【発明が解決しようとする課題】
【０００７】
従って、遠隔コンピュータが内部のネットワークにアクセスするのを許容する前に、遠隔のコンピュータの構成状態を確認するためのシステム及び方法に対する必要性が存在する。

【課題を解決するための手段】
【０００８】
本発明の実施形態は、ＶＰＮ接続を行う遠隔コンピュータが適正に保護されるのを確実にするための方法を提供する。従って、一実施形態においては、遠隔コンピュータのサーバ駆動される安全チェックが何等かのＶＰＮ接続を許容する前に必要とされる。これらのサーバ駆動されるチェックは、安全なＶＰＮ接続を提供するよう適合可能でありかつ構成可能であることが好ましい。サーバ駆動される安全チェックは、何が確認すべきか、確認は如何に行われるべきかでもって構成され得る。サーバは、最初に、任意の数の遠隔ユーザ・アクセス・レベルで構成され得る。サーバ駆動される安全チェックは、次に、アクセ

スが各アクセス・レベルで認可される前に、該アクセス・レベルとの順応性を確認するよう構成され得る、すなわち、サーバへの制限されたアクセスのためのチェックは、サーバへの無制限のアクセスのためのチェックよりも代表的には厳しいものではない。この方法で、顧客及びサーバ・リソースの双方は、必要なレベルのアクセスを認可するために効率的に用いられ得る。さらに、安全性チェックは、一度にすべてのレベルに対する確認よりもむしろ、アクセス・レベルの繰り返し確認を必要とし得る。さらに、安全性チェックは、顧客との各通信が独立的に処理され、累積情報が各サーバ－顧客通信サイクルに含まれるように構成され得る。

【０００９】

もう１つの実施形態においては、安全性チェックは、ＶＰＮアクセスが許容される前に追加の情報が必要とされるか否かを決定するために、遠隔コンピュータから受信された情報に適合する。例えば、特定のプログラムまたはプロセスが活動しているという情報を顧客が送信する場合、安全性チェックは、プログラムまたはプロセスによって使用中の．ｄｌｌ　ｆｉｌｅｓまたは関連のレジストリ・エントリを顧客が送信することを適合的に必要とし得る。特定のプログラムまたはプロセスが安全であるということをサーバが満足したとき、サーバは、次に、顧客のコンピュータ上の適所における、任意の他のプログラム、プロセス、等を適合的に確認し得る。

【００１０】

構成された安全性チェック及び適合された安全性分析に基づいて、ＶＰＮアクセスは遠隔コンピュータに認可される。一実施形態において、トークンが、サーバによって顧客コンピュータに提供される。顧客コンピュータは、ＶＰＮサーバへのログオンのときに用いるために、ＶＰＮ顧客プログラムまたはＶＰＮアプリケーションにこのトークンを通し得る。遠隔コンピュータが会社の安全政策と順応し続けるということを確実にするために、トークンが或る時間間隔、例えば、１０秒、１分、及び１時間で更新されるということをサーバは必要とし得る。さらに、トークンは、サーバ駆動される安全性チェックの分析に基づいて遠隔コンピュータを認可するために、アクセスのレベルに関する情報を含んでいても良い。

【００１１】

このようなサーバ駆動される確認の利点は、顧客のコンピュータを更新する必要無しで、ユーザ及びグループの安全プロフィル（profile）を容易に構成可能であるということを含んでいる。さらに、複数のアクセス・レベルの１つは、一致性もしくは順応性テストに基づいて認可され得る。さらに、新しく発見された弱点に対するタイムリーな応答を許容するよう、一致性もしくは順応性テストを追加したり修正したりし得、そしてパスワードは、リプレイ・アタック（replay attacks）を阻止するよう任意の時間間隔で変更され得る。

【００１２】

本発明の一実施形態は、内部のネットワークへの遠隔コンピュータのアクセスを許容する方法であって、

遠隔コンピュータからアクセス要求を受信するステップと、

遠隔コンピュータの構成状態を表わす情報を要求して受信するステップであって、該要求された情報は、遠隔コンピュータから受信されたアクセス要求に少なくとも基づくものである前記ステップと、

遠隔コンピュータから受信された情報に少なくとも基づく安全政策との遠隔コンピュータの順応性を決定するステップと、

遠隔コンピュータが安全政策と順応しないならば、追加の情報を要求して受信するステップであって、追加の情報要求は、受信された情報及び安全政策に少なくとも基づくものである前記ステップと、

遠隔コンピュータが、安全政策と順応するならば、内部のネットワークへの遠隔コンピュータのアクセスを許容するステップと、

を含む方法に向けられている。

【００１３】
本発明のもう１つの実施形態は、サーバ・コンピュータへのアクセスを提供するための方法であって、
初期のトークン要求を受信するステップと、
構成可能な安全政策との順応性のために初期のトークン要求を評価するステップと、
初期のトークン要求が構成可能な安全政策と順応しないならば、構成可能なトークン・データ要求を送信し、構成可能なトークン・データ要求に応答してもう１つのトークン要求を受信し、構成可能な安全政策との順応性のために受信されたもう１つのトークン要求を評価し、そして、受信されたもう１つのトークン要求が構成可能な安全政策と順応するまで、送信し受信しそして評価するステップを繰り返すステップと、
トークンを送信するステップと、
前記トークンを備えたサーバ・ログイン要求を処理するステップと、
を含む方法に向けられている。
【００１４】
本発明もう１つの実施形態は、遠隔コンピュータからサーバ・コンピュータへのアクセスを提供するための方法であって、サーバは複数のアクセス・レベルを有し、各レベルは１つのアクセス・レベルに対応するユーザ・プロフィルを備え、当該方法は、
（ａ）トークン要求を受信するステップと、
（ｂ）複数のアクセス・レベルの少なくとも１つとの順応性のためのトークン要求を評価するステップと、
（ｃ）トークン要求が複数のアクセス・レベルの少なくとも１つと順応しないならば、
（ｉ）受信されたトークン要求に少なくとも基づいて少なくとも１つの安全データ要求を送信し、
（ｉｉ）少なくとも１つの安全データ要求への応答を受信し、そして
（ｉｉｉ）複数のアクセス・レベルの少なくとも１つとの順応性のために受信された応答を評価するステップと、
（ｄ）受信された応答が複数のアクセス・レベルの少なくとも１つと順応するまで、ステップ（ｃ）を繰り返すステップと、
（ｅ）少なくとも１つの順応するアクセス・レベルに対応するトークンを送信するステップと、ここに、前記トークンはサーバ・コンピュータにアクセスするために用いられ
（ｆ）トークンに含まれるユーザ・プロフィルに従ってサーバへのアクセスを提供するステップと、
を含む方法に向けられている。
【００１５】
本発明のもう１つの実施形態は、内部のネットワークへの遠隔コンピュータのアクセスを許容する方法であって、
遠隔コンピュータからのアクセス要求を受信するステップと、
遠隔コンピュータによる実行のためのプログラムを遠隔コンピュータに送信するステップと、
プログラムにより発生されるデータを受信するステップと、
受信されたデータに基づいて内部のネットワークの安全政策との遠隔コンピュータの順応性を確認するステップと、
遠隔コンピュータが安全政策と順応するならば、内部のネットワークへの遠隔コンピュータのアクセスを許容するステップと、
を含む方法に向けられている。
【００１６】
本発明のもう１つの実施形態は、遠隔コンピュータから安全化された内部のネットワークにアクセスする方法であって、
（ａ）内部のネットワークと通信してゲートウェイ・サーバにアクセス要求を送信するステップと、

（ｂ）ゲートウェイ・サーバからデータ要求を受信するステップと、
（ｃ）要求されたデータをサーバに送信するステップと、
（ｄ）トークンがゲートウェイ・サーバから受信されるまでステップ（ｂ）－（ｃ）を繰り返すステップと、
（ｅ）内部のネットワークにアクセスするために、受信されたトークンを送信するステップと、
を含む方法に向けられている。

【００１７】

本発明のもう１つの実施形態は、外部ネットワークを介して遠隔コンピュータによる内部のネットワークへのアクセスを許容するようコンピュータを制御するための命令を含むコンピュータ読取り可能媒体であって、
遠隔コンピュータからのアクセス要求を受信し、
アクセス要求に少なくとも基づく少なくとも１つのデータ要求を遠隔のコンピュータに送り、
遠隔コンピュータからデータ要求に対する応答を受信し、
遠隔コンピュータから受信された応答に基づいて該遠隔コンピュータが内部のネットワークの安全政策と順応することを確認し、
受信された応答が安全政策と順応しないならば遠隔コンピュータに追加のデータ要求を送り、該追加のデータは受信された応答及び安全政策に少なくとも基づいて要求され、そして
遠隔コンピュータが内部のネットワークの安全政策と順応するならば、遠隔コンピュータの内部のネットワークへのアクセスを許容する
ことにより、外部ネットワークを介して遠隔コンピュータによる内部のネットワークへのアクセスを許容するようコンピュータを制御するための命令を含むコンピュータ読取り可能媒体に向けられている。

【００１８】

本発明のもう１つの実施形態は、安全化されたネットワークであって、
内部の通信ネットワークと、
該内部の通信ネットワーク及び外部の通信ネットワークに接続されるゲートウェイ・コンピュータと、を備え、該ゲートウェイ・コンピュータは、外部の通信ネットワークを介して遠隔コンピュータから内部の通信ネットワークに接続するための要求を受信するよう適合され、そして、さらに、遠隔コンピュータの内部の通信ネットワークへのアクセスを許容する前に、遠隔コンピュータが複数の安全政策の少なくとも１つと順応するのを確認するよう適合されている安全化されたネットワークに向けられている。

【発明を実施するための最良の形態】

【００１９】

図１は、本システム及び方法の１つの好適な実施形態を示す。図１には、インターネット１１０を介して複数の顧客のコンピュータ１０４Ａ－１０４Ｎと通信するよう適合されたサーバ１０２Ａ－１０２Ｎが示されている。ファイアウォール１１４もまた、図１に示されたインターネットと各顧客のコンピュータとの間、もしくは、サーバ１０２とインターネット（図示せず）との間に接続されても良い。

【００２０】

また、図１には、サーバ１０２に接続された会社のデータベース（１０８Ａ－１０８Ｎ）と内部の会社のネットワーク（１１２Ａ－１１２Ｎ）とが示されている。当業者には認識されるであろうように、フェールオーバ及び負荷平衡サーバを含む多くのサーバが存在し得る。さらに、任意の適切なネットワーク接続が、インターネット１１０の適所に履行され得るが、ＨＴＴＰまたはＨＴＴＰＳを用いた接続が好適である。さらに、他の会社のリソースが、サーバ１０２を介してアクセス可能であり得るが、これらのリソースは図１に示されていない。会社のリソースの例は、それに制限されるものではないが、プリンタ、ｅメール・サーバ、アプリケーション・サーバ、プロキシ・サーバ、及びスキャナであ

って良い。

【００２１】

図２は、本システム及び方法の態様を詳細に示している。要素１０２、１０４及び１１０は、図１に示されたのと同一の要素に対応している。サーバ１０２は、接続２００を介してインターネットに接続されるのが好ましい。上述したように、任意の適切なネットワーク接続が、サーバと顧客との間の通信を容易にするために履行され得る。

【００２２】

さらに図２には、顧客１０４が示されている。各顧客または遠隔のコンピュータは、実行しているオペレーティング・システム、並びに複数のアプリケーション２０６を有している。オペレーティング・システムは、オペレーティング・システムとアプリケーションとの構成情報を収容するレジストリを含み得る。これらのアプリケーションは、文書処理アプリケーション、インターネット・ブラウザ、オーディオまたはビデオ・アプリケーション、ｅメール・プログラム、アンチ－ウィルス・プログラム、ゲーム、またはユーザがインストールするために選択し得る他のアプリケーションであって良い。各顧客は、好ましくは、ＶＰＮ顧客アプリケーション２０４を含む。ＶＰＮ顧客アプリケーションは、遠隔コンピュータとサーバとの間の通信を容易にし、一度ＶＰＮ接続が創設されると、ユーザに会社のネットワーク・リソースにアクセスする能力を提供する。ＶＰＮ顧客アプリケーションは、好ましくは、サーバ１０２によって必要とされる安全性チェックを行うよう適合されている。認識されるように、他の補助アプリケーション（２０６）が、Ｃｉｓｃｏ　ＶＰＮ　Ｃｌｉｅｎｔ（登録商標）のようなＶＰＮ接続を行うために用いられ得る。ＶＰＮ顧客プログラム、または補助ＶＰＮアプリケーションは、利用可能なサーバのリスト及び利用可能なゲートウェイ場所（例えば、ニューヨーク、ロンドン、東京、等）のリストで構成され得る。

【００２３】

以下に詳細に説明するように、サーバ１０２は、会社のリソースへの変化するアクセス・レベルを許容するユーザ・グループまたはプロフィルで構成され得る。以下に詳細に説明するように、プロフィルは、種々のアクセス・レベル、会社のリソースの制限並びに特定のアクセス・レベルにおいてＶＰＮに接続することが必要とされるグループ名及びグループ・パスワードによってウェブ・グループを限定する。認識されるように、顧客のコンピュータに許可される下位のアクセス・レベルは、代表的には、会社のネットワークに対して課される危険性が少ない。

【００２４】

一実施形態においては、遠隔のコンピュータは、サーバ１０２から特定のプロフィルを要求する。サーバは、好ましくは、該プロフィルに対応する会社の安全政策と一致すると顧客が確認された後、要求されたプロフィルを顧客に割り当てる。もう一つの実施形態においては、サーバは、安全政策の順応性の顧客の実際のレベルに基づいて顧客にプロフィルを割り当てる。さらにもう一つの実施形態においては、サーバは、構成された安全政策によって創設されたデフォルト・プロフィルを顧客に割り当て得る。

【００２５】

各ユーザ・グループは、また、保護されたパスワードであっても良い。従って、顧客は、サーバが遠隔コンピュータに要求されたグループを割り当てる前に、パスワードを提供することが要求され得る。グループ・パスワードは、周期的に変更されても良く、プロフィルは、ユーザがプロフィルを取得してそれを用いてサーバ（リプレイ）に接続して、それにより、適所での安全性チェックをバイパスするのを避けるように更新されても良い。パスワードは、プログラム的に変更され得るので、会社は、例えば、１０秒、１分または１時間のような任意の間隔でグループ・パスワードを更新し得、それにより、リプレイ・アタックの効果を減少する。

【００２６】

一実施形態においては、サーバ１０２は、ログイン要求を有したトークンを必要とし得る。このトークンは、好ましくは、サーバに割り当てられたプロフィルを含む。これらの

ログイン・トークンは、好ましくは、顧客が特定のアクセス・レベルと一致したということをサーバが決定した後に、サーバから顧客に通される。もう一つの実施形態においては、プロフィルそれ自体が顧客に送信されて、ログイン・プロセスで用いられる。認識されるであろうように、サーバは、ユーザ名及びパスワード、安全性ＩＤ番号、または当該技術で知られている他のユーザ安全性有効情報のような遠隔コンピュータのログインのための他のデータを必要とし得る。さらに、サーバは、プロフィルまたはトークンがログイン要求に含まれることを要求し得、そして任意の時点で、安全政策順応性、グループ・パスワード、顧客プロフィル割り当て、等を再有効化もし得る。

【００２７】

図３は、遠隔コンピュータのログオンのためのシステム動作を示す好適な実施形態を示すフロー図である。好適な実施形態において、コンピュータ読取り可能媒体上に記憶されたプログラムを実行するコンピュータは、システム動作を維持する。図３に示されるように、ステップ３０２において、ＶＰＮ顧客２０４の場合が遠隔コンピュータ上で開始される。一実施形態において、ＶＰＮ顧客は、サーバ１０２にログインすることを試み得、そして動作はステップ３０６に直接流れるであろう。しかしながら、上述したように、サーバ１０２は、ログイン要求を有したトークンを提出するように遠隔コンピュータに要求し得る。従って、好適な実施形態においては、ＶＰＮ顧客は、サーバ１０２からのトークンを要求する（ステップ３０４）。さらに、他の実施形態においては、遠隔コンピュータは、特定のＶＰＮゲートウェイ・サーバ、特定のプロフィル・サーバ、またはそのトークン要求を有した特定のＶＰＮエントリ・ポイントを要求する。代表的には、プロフィルに関連した情報は、各ユーザごとに予め構成されるが、これらのパラメータは、例えば、ユーザが旅行しているときに、変えられ得る。

【００２８】

ＶＰＮ顧客がトークンを要求した後、または、サーバにログインすることを試みた後、遠隔コンピュータは、ステップ３０６においてサーバからデータを受信する。ステップ３０８において、ＶＰＮ顧客のアプリケーションは、トークン（または、プロフィル）が、受信されたデータ内に存在するか否かを決定する。もしトークン（またはプロフィル）が存在するならば、動作はステップ３１４に進む。もしトークン（またはプロフィル）が存在しなければ、顧客アプリケーションは、サーバから受信されたデータを処理する。

【００２９】

一実施形態において、データは、要求されたまたは割り当てられたユーザ・グループに関連したデータを顧客が収集するための要求を含む。データ要求は、ＸＭＬ、ＨＴＭＬまたは他の適切なフォーマット方法でフォーマッテイングされ得る。データ要求は、遠隔コンピュータが安全または他の情報を収集する必要とし、そして遠隔コンピュータが行うべきまたは行わなければならない動作を含む。一実施形態において、データ要求にはどんな実行可能な動作も含まれない。他の実施形態においては、サーバは、遠隔コンピュータ上で実行されるべきプログラムを提供し得る。プログラムは、例えば、アプリケーション、スクリプト、またはネットワーク化されたプログラムへのリンクであって良い。幾つかの実施形態においては、プログラムは、遠隔コンピュータ上に常駐し得る。幾つかの実施形態においては、サーバにより提供されるプログラムは、ユーザの直接の介在無しで遠隔コンピュータ上で自動的に実行され得る。

【００３０】

サーバによって要求されるデータ収集は、それに制限されるものではないが、レジストリ・キーが存在するか否かのチェック（該キーの特性を得る）；レジストリ・キーのリスト・サブキー；レジストリ・キーにおける値のリスト；レジストリ・キーにおける値；ディスク・ディレクトリの属性；ディレクトリにおけるリスト・ファイル；ディスク・ファイルの戻り属性；ディスク・ファイルの内容（ハードコード化されたサイズ限界）；遠隔機械上にインストールされたサービスのリスティング（現在の状況を含む）；特定のサービスまたはプロセスの詳細；送信先機械上で実行しているプロセスまたは送信先機械上で利用可能なアプリケーションのリスト：現在のユーザの環境変数のリスト：汎用機械及び

オペレーティング・システム情報（バージョン、サービス・パックを構築）；及び、一般顧客プログラム（ＶＰＮＣｏｎｎｅｃｔ）情報、を含み得る。

【００３１】

顧客が行う動作は、それに制限されるものではないが、ユーザにメッセージを表示すること、並びに任意選択的に、ユーザによって要求された場合には、ウェブＵＲＬを開くこと、を含み得る。ＵＲＬが、ｈｔｔｐ、ｈｔｔｐｓ、またはｆｔｐでないならば、顧客は、このＵＲＬが開くために安全ではないかもしれないという余分な警告を表示し得る。代表的には、ＵＲＬは、顧客コンピュータがネットワークにアクセスするのを許容されて抗ウィルス定義の更新を実行する前に顧客コンピュータによって満足されなければならない条件を一層詳細に記載したウェブ・ページにユーザを向ける方法として意図される。

【００３２】

ＶＰＮ顧客アプリケーションは要求を処理し、データが処理されて収集された後に、データは、ステップ３１２においてサーバに送信される。トークンまたはプロフィルが受信されるまで、点線の枠３２０によって示される、ステップ３０６－３１２が繰り返される。ステップ３１４において、トークンまたはプロフィルがＶＰＮ顧客に通され、顧客は、ステップ３１６においてサーバにログオンする。

【００３３】

図４は、サーバのログイン処理のためのシステム動作を示す好適な実施形態を示すフロー図である。図４に示されるように、ステップ４０２において、サーバは、ＶＰＮアクセスのために構成される。一実施形態において、サーバは、異なったアクセス・レベルを有する定義されたユーザ・グループまたはプロフィルで構成される。これらのアクセス・レベルは、それに制限されるものではないが、完全アクセス、中間アクセス、最小アクセス及び無アクセスを含み得、該無アクセスは、さらに、デフォルト・アクセス・レベルであるようさらに定義され得る。各アクセス・レベルまたはグループの構成は、サーバ上で任意の時間において変更され得、この方法で、会社の安全政策は、新しい脅威に、それらが生じるときに適合し得る。プロフィルは、それに制限されるものではないが、グループ・アクセス・レベル、リソース・アクセス・レベル、プロフィルに基づいたゲートウェイ・アクセス、ＶＰＮサーバのためのＩＰアドレス、プロフィルまたはトークンの経年数、及び特定のアクセス制限を含み得る。図５は、本発明の好適な実施形態におけるユーザ・レベル・アクセス選択の例示的なスクリーンショットを示す。

【００３４】

各サーバ１０２は、また、特定のアクセス・レベルに対して行われるべきテストを限定する１つまたは２つ以上の安全制御ファイル（安全チェック）及び任意の安全テストが失敗した場合に適応し得るアクセス・レベル制限でもって構成される。認識されるであろうように、テストの失敗がアクセスの拒否に帰結するということは必要でなく、むしろ、適所の安全政策が次の一層低いレベルへのアクセス、すなわち、中間のアクセスから低いレベルへのアクセス、を単に制限し得る。例としてだけのために、制御ファイルは、また、以下の任意のものを含み得る：拒否に帰結するファイルのリスト；拒否に帰結するレジストリ・エントリ、キーまたは値のリスト；特定のレベルにおけるアクセスのための必要とされるファイル；特定のレベルにおけるアクセスのための必要とされるレジストリ・エントリ、キーまたは値；特定のレベルにおけるアクセスのための必要とされるプロダクト・バージョン；特定のレベルにおけるアクセスのための必要とされるサービス状態；遠隔コンピュータ上の表示のためのメッセージ、を含み得る。

【００３５】

さらに、制御ファイルは、オペレーティング・システムが、インストールされた今日までのパッチまたは安全フィックスを有するということを必要とし得る。未知のまたは定義されていないプログラム、プロセス、レジストリ・エントリ、等が、遠隔コンピュータ上に配置されるとき、安全政策は、内部のネットワークへのアクセスを否定もしくは制限するよう、かつ同じものを示すメッセージをユーザに同時に送信するよう構成され得る。遠隔コンピュータ上の或る第３者のアプリケーション、レジストリ・エントリ、レジストリ

・キー、またはレジストリ値は、サーバが内部のネットワークへのアクセスを否定もしくは制限するように定義され得る。図６は、内部ネットワークへのアクセスを否定もしくは制限するために本発明の幾つかの実施形態において用いられ得る、かかる例示的な（exemplar）禁止された構成情報または状態のリストを示す。

【００３６】

さらに認識されるように、任意の数のプロフィルが、サーバ上に、もしくはサーバにアクセス可能に存在し得る。各プロフィルは、サーバが遠隔コンピュータに該プロフィルを配分する前に、異なったレベルのセキュリティの順応性（compliance）を必要とし得る。例えば、アプリケーションへの完全アクセスだけを許容するプロフィルは、ｅメール・サーバへの完全アクセスだけを許容するプロフィルよりも一層厳密な安全要件を有し得る。会社のネットワークのための最も適用可能な安全政策を提供するために、グループ・アクセス・レベル及び会社のリソースの任意の組み合わせを履行し得る。例えば、プリンタ、ｅメール・サーバ、アプリケーション、プロキシ（代理）・サーバ、等のようなリソースは、所望のユーザ・グループの各々内で任意の安全政策の制限でもって定義され得る。

【００３７】

代替的な実施形態においては、トークン要求は、ＶＰＮゲートウェイ・サーバとは（物理的にまたは論理的に）独立して存在する別のプロフィル・サーバに送信される。プロフィル・サーバは、好ましくは、ＶＰＮゲートウェイ場所ごとのプロフィル及びリソース安全情報、すなわち各ＶＰＮゲートウェイごとの各アクセス・レベルごとに１つのプロフィル、を含む。該プロフィルは、ＶＰＮ顧客が如何にＶＰＮサーバに接続するべきであるかに関する情報を含み得る。この情報は、場所に対して適切なＶＰＮサーバのＩＰアドレスまたはＤＮＳ名、並びにプロフィルのアクセス・レベル及び対応のパスワードに対応するこれらのサーバに関するグループ名を含み得る。トークンは、プロフィル・サーバから遠隔コンピュータに通され、そして、これらのトークンは、ＶＰＮゲートウェイ・サーバへの接続のために用いられ得る。この方法で、ＶＰＮサーバのリソースは、プロフィル割り当て及び他の安全関連のタスクのためには使用されない。

【００３８】

ステップ４０４において、サーバ１０２は、遠隔コンピュータからのトークンまたはログイン要求を受信する。サーバ１０２は、トークン要求を構文解析して、ステップ４０６において、安全制御ファイルに基づくデータにテストを行う。該テストは、内部のネットワークの安全要件に対応し、そして、遠隔コンピュータが欠陥を生じたものではないことを確認する。例えば、テストは、レジストリ・キーまたはエントリ、デスク及びディレクトリ属性、アプリケーション属性、ファイル属性、インストールされたサービス、処理の実行、ユーザ環境変数、遠隔機械及びオペレーティング・システム情報、ＶＰＮ顧客情報、アンチ－ウィルス・プログラム情報、もしくは遠隔コンピュータのウィルス定義情報を確認し得る。上述したように、これらのテストは、変更されても良いし、また、新しい安全脅威を処理するかもしくは異なったプロフィルまたはアクセス・レベルを提供するように、新しいテストが任意の時点で追加されても良い。さらに、これらのテストの任意の組み合わせが所望レベルの安全を提供するために履行され得る。

【００３９】

受信されたデータが、要求されたまたは割り当てられたプロフィルの安全政策に応じるものであるならば、サーバは、ステップ４１２において顧客にトークンを送信する。該データが応じないものであるならば、サーバは、ステップ４０８において、順応性（応じるものであること）を決定するために必要とされる追加の情報を決定し得る。認識されるであろうように、初期のトークン要求と共にほとんどもしくは全く情報が存在しない。この状況において、サーバは、全てのテストが行われるべきであることを決定し得、従って、サーバは、遠隔コンピュータからの対応のデータを要求する。追加のデータのための要求が、ステップ４１０において、遠隔コンピュータに送信される。

【００４０】

サーバは、フォロー・アップ情報を受信し、所定数の繰返しのために、または、順応性

テスト・データが受信されるまで、４０４－４１０のステップを通して処理が続く。図４における４２０で示された点線枠は、サーバにおいてデータを受信し、該データを評価し、新しい情報要求のために該データを処理し、そして、データ要求を送信するという繰返しプロセスを示す。

【００４１】

一実施形態において、サーバは、遠隔コンピュータとの交渉の状態を保持する。この方法で、各要求は、スタンドアロンのデータ・セットとして処理される。テスト・データが不完全であるならば、要求されたデータの全リストは、顧客に返信される。もう一つの実施形態においては、要求された追加のテスト・データだけが遠隔コンピュータから要求される。好適な実施形態においては、サーバによって要求される全ての情報を要求が含む前に、遠隔コンピュータが、該要求を２倍または３倍に拡張することが必要とされ得る。

【００４２】

もう一つの実施形態においては、サーバが特定の遠隔コンピュータから初期のトークン要求を受信してしまった後まで、サーバが特定の遠隔コンピュータからどんな情報を必要とするかをサーバは知らないかもしれない。該サーバは、トークン要求を構文解析し、顧客に特定のプロフィルを認可するために行われるべき安全テストを識別する。該サーバは、識別されたデータを遠隔コンピュータに送信し、そして、遠隔コンピュータから要求されたテストに対応するデータを受信する。サーバはデータを構文解析し、そして、該データがプロフィルを認可するのに充分であるか否かを決定する。このフォロー・アップ・データに関して、サーバは、追加の情報が要求されるかどうかを決定する。例えば、サーバは、ファイルが存在するということを示すレジストリまたはデスク・エントリを受信するまで、ファイルのための経路を要求することを知らないかも知れず、もしくは、サーバは、関連のプロセスまたはアプリケーション・データを受信するまで、．ｄｌｌファイル完全性またはマクロ（ｍａｃｒｏ）完全性を確認することを知らないかも知れない。

【００４３】

サーバは、追加のテストが実行されるべきであるか否かを決定するために、フォロー・アップ要求を評価する。もし、実行されるべきであるならば、サーバは、上述のステップ４２０を繰り返すことによって、追加のデータ要求を送信する。すべての適合性評価が行われてしまった後、サーバは、特定のプロフィルを認可し得る。しかしながら、すべての定義されたテストが行われてしまい、かつ安全性が未だ信用の無いものであり得るということをサーバが決定したならば、より低いプロフィル・レベルに関する一層低いレベルのアクセスまたは無アクセスが認可され得る。例えば、会社が特定のプロセスのためのテスト・パラメータを持っていないかも知れず、従って、サーバは、プロセスを評価できず、それ故、サーバは、会社のリソースへのアクセスを制限する。図７は、遠隔コンピュータ及びサーバ間の接続の創設に先立って、遠隔コンピュータとサーバとの間での情報の繰り返された交換を示す本発明の実施形態における顧客－サーバ通信サイクルの例示的スクリーンショットである。

【００４４】

本発明の少なくとも説明的な実施形態を記載したけれども、種々の変更及び改良が当業者には容易に行われ得るであろうし、それらも本発明の範囲内にあるものと意図されている。従って、前述の説明は、単に例示のためだけのものであり、制限するものとして意図されるものではない。本発明は、特許請求の範囲及びそれに等価なものに限定されるものとしてのみ制限される。

【図面の簡単な説明】

【００４５】

【図１】本発明のシステム及び方法の１つの好適な実施形態を示すブロック図である。

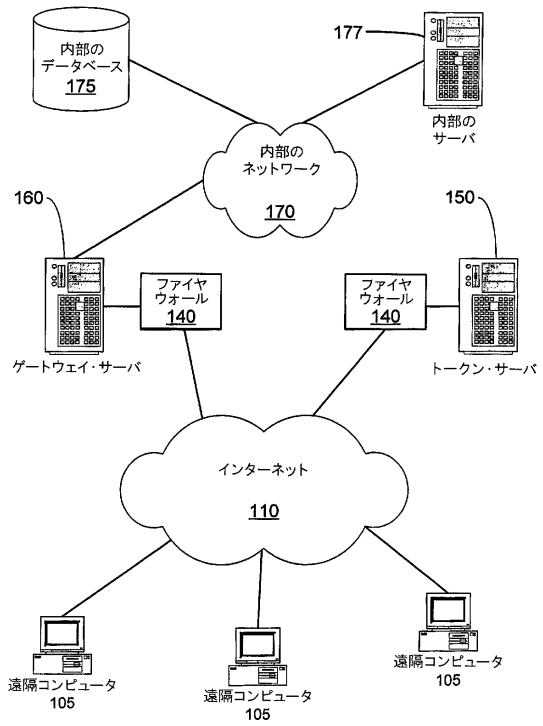
【図２】図１の好適な実施形態の態様を一層詳細に示すブロック図である。

【図３】本発明のシステム及び方法の１つの好適な実施形態におけるシステム動作の態様を示すフロー図である。

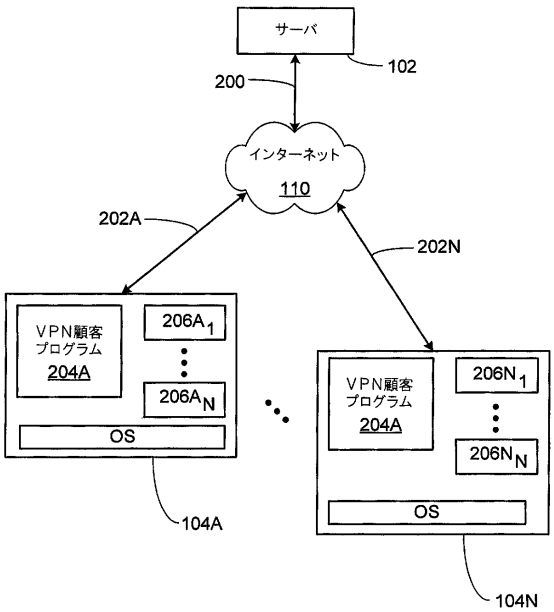
【図４】本発明のシステム及び方法のもう１つの好適な実施形態におけるシステム動作の

態様を示すフロー図である。
【図５】本発明のシステム及び方法の実施形態におけるユーザ・レベル・アクセス選択の例示的なスクリーンショットを示す図である。
【図６】本発明の幾つかの実施形態において用いられ得る構成情報のリストを示す図である。
【図７】本発明のシステム及び方法の実施形態における顧客－サーバ通信サイクルの例示的なスクリーンショットを示す図である。
【符号の説明】
【００４６】
１０２Ａ－１０２Ｎ　　サーバ
１０４Ａ－１０４Ｎ　　顧客のコンピュータ
１０５　　遠隔コンピュータ
１０８Ａ－１０８Ｎ
１１０　　インターネット
１１２Ａ－１１２Ｎ　　内部の会社のネットワーク
１１４　　ファイアウォール
２００　　接続
２０４　　ＶＰＮ顧客アプリケーション
２０６　　アプリケーション

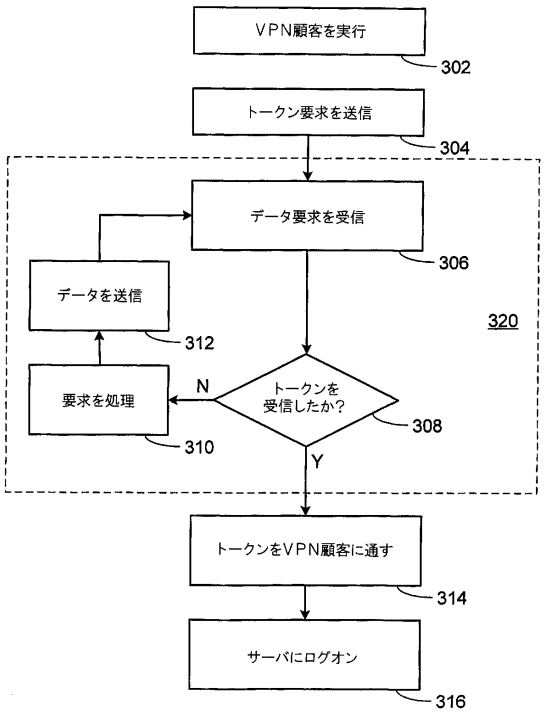
【図１】



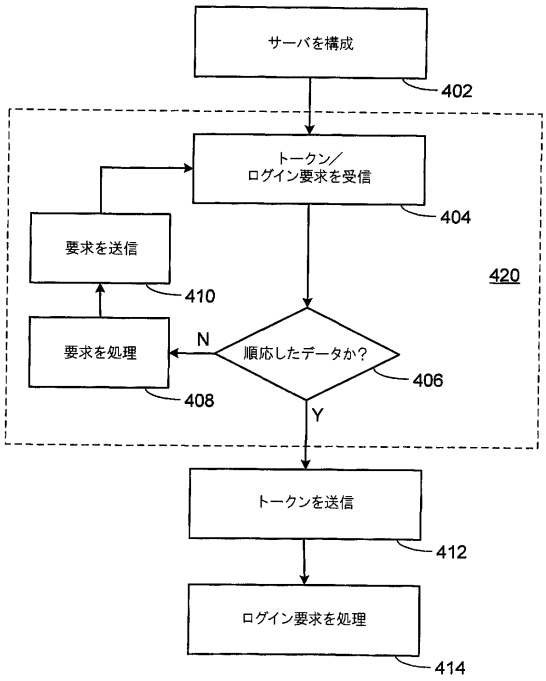
【図２】



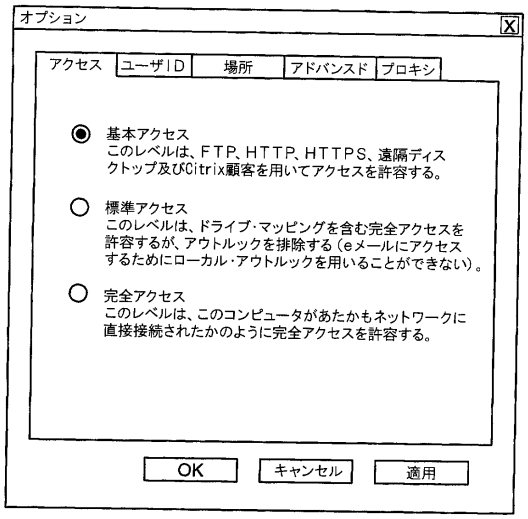
【図３】



【図４】



【図５】



【図６】

[Registry keys]
- HKLM\SOFTWARE\Classes\BonziBDY.Document=shell
- HKLM\SOFTWARE\Classes\daffile=shell
- HKLM\SOFTWARE\Classes\AIM=shell
- HKLM\SOFTWARE=Gator.com
- HKLM\SOFTWARE=Brilliant Digital Entertainment
- HKLM\SOFTWARE=Kazaa
- HKLM\SOFTWARE=CommonName
- HKLM\SOFTWARE=Cydoor
- HKLM\SOFTWARE=BearShare
- HKLM\SOFTWARE=WhenU
- HKLM\SOFTWARE=NeoModus
- HKLM\SOFTWARE=rdxr
- HKLM\SOFTWARE=Distributed Computing Technologies, Inc.
- HKLM\SOFTWARE=Qtrax
- HKLM\SOFTWARE=iMesh
- HKLM\SOFTWARE=GoToMyPC

[Registry values or data]
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Audiogalaxy Satellite=UninstallString
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run=XupiterStartup
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run=SQUpdatesChecker
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{E499428A-E04F-4683-8A21-42A5E6D1C851}=UninstallString
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Trillian=UninstallString;
- HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon\AllowMultipleTSSessions=0

[Prohibited files]
- %ProgramFiles%\Gator.com*.*=
- %ProgramFiles%\PrecisionTime*.*=

Fig. 6

【図７】

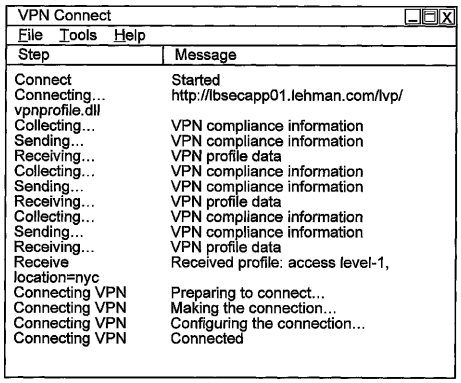

VPN Connect
File Tools Help
Step
Message
Connect
Started
Connecting...
http://lbsecapp01.lehman.com/lvp/
vpnprofile.dll
Collecting...
VPN compliance information
Sending...
VPN compliance information
Receiving...
VPN profile data
Collecting...
VPN compliance information
Sending...
VPN compliance information
Receiving...
VPN profile data
Collecting...
VPN compliance information
Sending...
VPN compliance information
Receiving...
VPN profile data
Receive
Received profile: access level-1,
location=nyc
Connecting VPN
Preparing to connect...
Connecting VPN
Making the connection...
Connecting VPN
Configuring the connection...
Connecting VPN
Connected

Fig. 7

フロントページの続き

(72)発明者　マイケル・ティー・エングル
アメリカ合衆国・ニュージャージー・０７０８７・ユニオン・シティー・マンハッタン・アヴェニュー・１００・アパートメント・１１３
(72)発明者　フレデリック・ヌウォコビア
アメリカ合衆国・ニュージャージー・０７０８３・ユニオン・ピルグリム・ウェイ・１８７
(72)発明者　ブラドリー・ディー・ノアック
アメリカ合衆国・ニュージャージー・０７０３０・ホボクン・クリントン・ストリート・７１１・＃５イー
(72)発明者　ジャージー・マコウィエッキ
アメリカ合衆国・ニュージャージー・０８８８９・ホワイトハウス・ステーション・ウィロー・コート・３

審査官　矢頭　尚之

(56)参考文献　特開２００４－０８６５３２（ＪＰ，Ａ）
特開２００３－１５０５５３（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
H04L　12/66
G06F　15/00