(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2005-539409
(P2005-539409A)
(43)公表日　平成17年12月22日(2005.12.22)

(51)Int.Cl.[7]	F I			テーマコード（参考）
H04L 12/28	H04L	12/28	310	5K033
H04Q 7/34	H04Q	7/04	C	5K067

審査請求 未請求　予備審査請求 未請求　（全 63 頁）

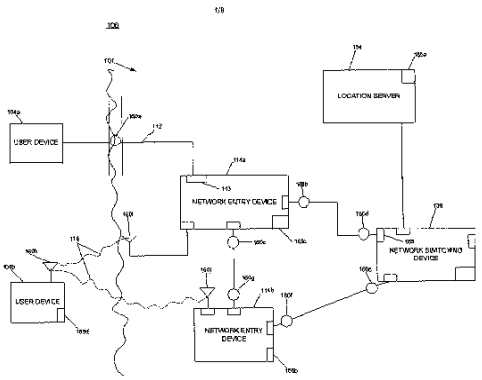
(21)出願番号	特願2003-573518 (P2003-573518)
(86)(22)出願日	平成15年2月28日 (2003.2.28)
(85)翻訳文提出日	平成16年11月1日 (2004.11.1)
(86)国際出願番号	PCT/US2003/006169
(87)国際公開番号	WO2003/075125
(87)国際公開日	平成15年9月12日 (2003.9.12)
(31)優先権主張番号	60/361,419
(32)優先日	平成14年3月1日 (2002.3.1)
(33)優先権主張国	米国 (US)
(31)優先権主張番号	60/361,421
(32)優先日	平成14年3月1日 (2002.3.1)
(33)優先権主張国	米国 (US)
(31)優先権主張番号	60/361,420
(32)優先日	平成14年3月1日 (2002.3.1)
(33)優先権主張国	米国 (US)

(71)出願人　501063117
エンテラシス　ネットワークス　インコーポレイテッド
アメリカ合衆国　マサチューセッツ州　01810－1008　アンドーバー　ミニットマン　ロード　50
(74)代理人　100082005
弁理士　熊倉　禎男
(74)代理人　100067013
弁理士　大塚　文昭
(74)代理人　100074228
弁理士　今城　俊夫
(74)代理人　100086771
弁理士　西島　孝喜

最終頁に続く

(54)【発明の名称】位置認識データネットワーク

(57)【要約】
ネットワークリンク型装置が接続されたネットワークにおいて物理的位置をそのような装置に関連付けるシステム。このシステムは、装置の位置を確立するための種々の技術を使用する。そのシステムコンフィギュレーションは、変更することができ、そしてLAM、MAN、ワイドエリアネットワーク（WAN）、パーソナルエリアネットワーク（PAN）、及びホームネットワークを含むいかなる形式のデータネットワークも含むことができる。又、システムは、特定装置の位置情報をネットワーク装置及びマネージメントへ供給し、これは、コンフィギュレーション精度、制御及びセキュリティを改善するために種々のやり方で使用することができる。又、この位置情報は、装置自体の制御又は保安のために使用してもよい。



【特許請求の範囲】
【請求項１】
データ通信ネットワーク内でクライアントの物理的な位置を決定する方法において、
クライアントが前記データネットワークと通信するときに通る接続ポイントの識別子を決定するステップと、
前記接続ポイントのその決定された識別子に基づいてクライアントの物理的な位置を決定するステップであって、前記接続ポイントの識別子と前記物理的な位置との間の記憶された関連性をアクセスすることを含むステップと、
を備えた方法。
【請求項２】
前記接続ポイントは、ケーブルベースの伝送媒体を経て前記クライアントへの通信経路を与える請求項１に記載の方法。
【請求項３】
物理的位置を決定する前記ステップは、前記クライアントが前記接続ポイントに接続するのに応答して行われる請求項１に記載の方法。
【請求項４】
接続ポイント識別子と各物理的位置との複数の関連性を記憶するステップであって、前記クライアントが前記接続ポイントに接続する前に接続ポイント識別子と物理的位置との間の関連性を記憶することを含むステップを更に備えた請求項１に記載の方法。
【請求項５】
前記データネットワーク内のネットワーク装置から前記クライアントへ接続情報を送信するステップを更に備え、接続ポイント識別子を決定する前記ステップは、前記接続情報を使用して接続ポイント識別子を決定することを更に含む請求項１に記載の方法。
【請求項６】
前記ネットワーク装置は、前記接続ポイントから前記データ通信ネットワーク内の他の装置への通信経路を与える請求項５に記載の方法。
【請求項７】
前記接続情報は、前記ネットワーク装置を識別する第１部分を含む請求項５に記載の方法。
【請求項８】
前記第１部分は、前記ネットワーク装置のアドレスを含む請求項７に記載の方法。
【請求項９】
前記第１部分は、前記ネットワーク装置のＭＡＣアドレスを含む請求項８に記載の方法。
【請求項１０】
前記第１部分は、前記ネットワーク装置のインターネットプロトコル（ＩＰ）アドレスを含む請求項８に記載の方法。
【請求項１１】
前記接続情報は、前記接続ポイントへの通信経路を与える前記ネットワーク装置の接続ポートを識別する第２部分を含む請求項５に記載の方法。
【請求項１２】
前記第２部分は、前記接続ポイントへの通信経路を与える前記接続ポートのＭＡＣアドレスを含む請求項１１に記載の方法。
【請求項１３】
前記第２部分は、前記装置ＩＤに含まれたインデックス属性を含む請求項１１に記載の方法。
【請求項１４】
物理的位置を決定する前記ステップは、更に、
前記クライアントから信号を受信する段階と、
前記データ通信ネットワークのネットワーク装置により前記信号の第１特性を測定する

段階と、
を含む請求項１に記載の方法。
【請求項１５】
物理的位置を決定する前記ステップは、更に、
前記測定された第１特性に基づいて物理的位置を決定する段階、
を含む請求項１４に記載の方法。
【請求項１６】
物理的位置を決定する前記ステップは、更に、
以前に測定された特性と各物理的位置との関連性を記憶する段階と、
前記測定された第１特性及び前記以前に測定された特性を使用して物理的位置を決定する段階と、
を含む請求項１４に記載の方法。
【請求項１７】
前記測定段階は、更に、
前記クライアントからケーブルベースの伝送媒体を経て受信した前記信号の前記第１特性を第１ネットワーク装置により測定する工程と、
前記クライアントからワイヤレス伝送媒体を経て受信した信号の第２特性を第２ネットワーク装置により測定する工程と、
を含み、物理的位置を決定する前記ステップは、更に、前記測定された第１特性及び前記測定された第２特性を使用して物理的位置を決定する段階を含む請求項１４に記載の方法。
【請求項１８】
位置データベースを使用して前記接続ポイント識別子と前記物理的位置との間の関連性を記憶するステップを更に備えた請求項１に記載の方法。
【請求項１９】
関連性を記憶する前記ステップは、集中型位置サーバーにおいて前記接続ポイント識別子と前記物理的位置との間の関連性を記憶する段階を含む請求項１８に記載の方法。
【請求項２０】
関連性を記憶する前記ステップは、前記接続ポイント識別子と、ネットワーク装置間に分散された前記物理的位置との間の関連性を記憶する段階を含む請求項１８に記載の方法。
【請求項２１】
前記接続ポイントはジャックを含む請求項１に記載の方法。
【請求項２２】
前記物理的位置と、ＭＡＣアドレス、ネットワーク層アドレス、電話番号、プロトコル形式、アセットＩＤ及び所有者の少なくとも１つとの間の関連性を記憶するステップを更に備えた請求項１に記載の方法。
【請求項２３】
前記決定された物理的位置を使用して認証を決定するステップを更に備えた請求項１に記載の方法。
【請求項２４】
前記決定された物理的位置を使用してサービスのレベルを決定するステップを更に備えた請求項１に記載の方法。
【請求項２５】
前記物理的位置を使用するセキュリティ機能を利用するステップを更に備えた請求項１に記載の方法。
【請求項２６】
セキュリティ機能を利用する前記ステップは、前記物理的位置に基づいてデータを暗号化する段階を含む請求項２５に記載の方法。
【請求項２７】

セキュリティ機能を利用する前記ステップは、前記物理的位置に関連した一時的キーを利用する段階を含む請求項２５に記載の方法。
【請求項２８】
物理的位置を決定する前記ステップは、更に、
前記決定された接続ポイント識別子に対して複数の記憶された関連性をサーチする段階と、
前記記憶された関連性において前記接続ポイント識別子に関連した物理的位置を識別する段階と、
を含む請求項１に記載の方法。
【請求項２９】
前記決定された物理的位置は、緯度及び経度フォーマット、緯度、経度、高度、及び精度フォーマット、位置識別番号、テクスチャストリング表示、及び関係情報を伴う相対的物理的位置、の少なくとも１つを含む請求項１に記載の方法。
【請求項３０】
前記決定された物理的位置を使用して接続ポリシーを確立するステップを更に備えた請求項１に記載の方法。
【請求項３１】
前記接続ポリシーを使用してユーザを認証するステップを更に備えた請求項３０に記載の方法。
【請求項３２】
前記決定された物理的位置を、前記接続ポイントに関連した装置へ送信するステップを更に備えた請求項１に記載の方法。
【請求項３３】
前記物理的位置に基づいて前記接続ポイントに関連した装置へコンフィギュレーション情報を送信するステップを更に備えた請求項１に記載の方法。
【請求項３４】
物理的位置を決定する前記ステップは、更に、前記接続ポイントに基づいて前記物理的位置を信頼性のある装置で決定する段階を含む請求項１に記載の方法。
【請求項３５】
前記信頼性のある装置は、ネットワークインフラストラクチャー内に配置される請求項３４に記載の方法。
【請求項３６】
前記物理的位置と信頼性レベルとの間の関連性を記憶するステップを更に備えた請求項１に記載の方法。
【請求項３７】
前記物理的位置を決定する装置を使用して前記物理的位置の信頼性レベルを決定するステップを更に備えた請求項３６に記載の方法。
【請求項３８】
複数の接続ポイントを含むデータネットワークインフラストラクチャーを調査する方法において、そのデータネットワークインフラストラクチャーへの複数の接続ポイントの各々に対して、
前記接続ポイントに対する物理的位置を決定するステップと、
前記接続ポイントに対する物理的位置を前記ネットワークインフラストラクチャーに与えるステップと、
を備えた方法。
【請求項３９】
前記接続ポイントとそれらの各決定された物理的位置との間の関連性を記憶するステップを更に備えた請求項３８に記載の方法。
【請求項４０】
前記接続ポイントを各接続ポイント識別子で識別するステップを更に備えた請求項３８

に記載の方法。
【請求項４１】
少なくとも幾つかの接続ポイントに対して、位置感知装置を前記接続ポイントに接続し、そして前記位置感知装置を使用して前記接続ポイントの物理的位置を決定するステップを更に備えた請求項３８に記載の方法。
【請求項４２】
前記位置感知装置は、グローバルポジショニングシステム（ＧＰＳ）受信器を含む請求項４１に記載の方法。
【請求項４３】
前記位置感知装置は、慣性ポジショニングシステムを含む請求項４１に記載の方法。
【請求項４４】
データ通信ネットワーク内でクライアントの物理的な位置を決定する方法において、
ケーブルベースの伝送媒体を経て接続ポイントへ前記クライアントを接続するステップと、
前記クライアントが通信する前記接続ポイントを識別するステップと、
前記識別された接続ポイントに基づいて前記クライアントの物理的位置を決定するステップと、
前記識別された接続ポイントと前記決定された物理的位置との間の関連性を記憶するステップと、
を備えた方法。
【請求項４５】
接続ポイント識別子を決定し、該接続ポイント識別子に基づいて物理的位置を決定するように構成され、前記接続ポイント識別子と前記物理的位置との間の記憶された関連性をアクセスすることも含むように構成された位置モジュールを備えたシステム。
【請求項４６】
前記位置モジュールと通信する位置クライアントを更に備えた請求項４５に記載のシステム。
【請求項４７】
前記位置クライアントは、通信プロトコルを使用して前記位置モジュールと通信する請求項４５に記載のシステム。
【請求項４８】
前記位置クライアントは、第３層プロトコルを使用して前記位置モジュールと通信する請求項４５に記載のシステム。
【請求項４９】
データネットワークインフラストラクチャー内の１つ以上の信頼性のあるネットワーク装置により、そのデータネットワークインフラストラクチャーへのアクセスを要求しているクライアント装置の物理的位置を決定して、信頼性のある物理的位置を発生するステップと、
前記信頼性のある物理的位置と前記クライアント装置との関連性を記憶するステップと、
を備えた方法。
【請求項５０】
前記データネットワーク内のネットワーク装置が信頼性のあるネットワーク装置であるかどうかを、偽の物理的位置データを与えるように前記ネットワーク装置を変更できる見込みに基づいて決定するステップを更に備えた請求項４９に記載の方法。
【請求項５１】
前記データネットワーク内の前記信頼性のあるネットワーク装置への物理的アクセスを制限するステップを更に備えた請求項４９に記載の方法。
【請求項５２】
１つ以上の信頼性のあるネットワーク装置が、スレッシュホールド以上の信頼性レベル

に各々関連付けられる請求項４９に記載の方法。
【請求項５３】
前記スレッシュホールドは、クライアント装置による要求の形式に依存する請求項５２に記載の方法。
【請求項５４】
前記信頼性のある物理的位置は、信頼性レベルに関連付けられる請求項４９に記載の方法。
【請求項５５】
前記１つ以上の信頼性のあるネットワーク装置の信頼性レベルを使用して前記信頼性のある物理的位置の信頼性レベルを決定するステップを更に備えた請求項５４に記載の方法。
【請求項５６】
信頼性レベルを決定する前記ステップは、前記１つ以上の信頼性のあるネットワーク装置と前記クライアント装置との間の通信の方法に基づいて信頼性レベルを決定することを含む請求項５５に記載の方法。
【請求項５７】
前記信頼性のある物理的位置を使用して前記クライアントのネットワークアクティビティを規制するステップを更に備えた請求項４８に記載の方法。
【請求項５８】
前記信頼性のある物理的位置を使用して前記クライアントによるアクセス要求に対する応答を決定するステップを更に備えた請求項４９に記載の方法。
【請求項５９】
前記信頼性のある物理的位置を使用して前記クライアントへ与えられるネットワークリソースを制御するステップを更に備えた請求項４９に記載の方法。
【請求項６０】
ネットワークリソースを制御する前記ステップは、前記ネットワークリソースへのアクセスを制限することを含む請求項５９に記載の方法。
【請求項６１】
前記信頼性のある物理的位置を緊急状態応答当局へ送信するステップを更に備えた請求項４９に記載の方法。
【請求項６２】
前記信頼性のある物理的位置を使用して前記クライアントへ情報を供給するステップを更に備えた請求項４９に記載の方法。
【請求項６３】
情報を供給する前記ステップは、前記信頼性のある物理的位置を使用して前記情報を選択することを含む請求項６２に記載の方法。
【請求項６４】
データネットワークインフラストラクチャー内の信頼性あるソースから第１の位置情報を送信するステップと、
前記ネットワークへのアクセスを要求しているクライアント装置から第２の位置情報を受信するステップであって、該第２の位置情報が前記第１の位置情報を使用するようなステップと、
前記第１及び第２の位置情報を使用して信頼性のある位置を決定するステップと、
を備えた方法。
【請求項６５】
前記信頼性のある物理的位置を使用して前記クライアントのネットワークアクティビティを規制するステップを更に備えた請求項６４に記載の方法。
【請求項６６】
前記信頼性のある物理的位置を使用して前記クライアントに与えられるネットワークリソースを制御するステップを更に備えた請求項６４に記載の方法。

【請求項６７】
装置の物理的な位置を特徴付ける値を決定するステップと、
前記決定された値に対応する信頼性レベルを決定するステップと、
前記信頼性レベルを前記物理的位置の値に関連付けるステップと、
を備えた方法。
【請求項６８】
信頼性レベルを決定する前記ステップは、更に、前記物理的位置の値を決定するのに使用される技術の精度を使用して信頼性レベルを決定することを含む請求項６７に記載の方法。
【請求項６９】
信頼性レベルを決定する前記ステップは、更に、前記物理的位置の値を決定するのに使用される考えられる値の範囲の粒度を使用して信頼性レベルを決定することを含む請求項６７に記載の方法。
【請求項７０】
信頼性レベルを決定する前記ステップは、更に、値の決定が物理的位置に対して偽の値を生じ得る確率を使用して信頼性レベルを決定することを含む請求項６７に記載の方法。
【請求項７１】
信頼性レベルを決定する前記ステップは、更に、前記物理的位置の値を決定するネットワーク装置の信頼性レベルを使用して信頼性レベルを決定することを含む請求項６７に記載の方法。
【請求項７２】
データネットワークインフラストラクチャー内に信頼性のあるネットワーク装置を備えたシステムであって、前記ネットワーク装置は、前記ネットワークインフラストラクチャーへのアクセスを要求するクライアント装置の信頼性のある物理的位置を決定し、そしてその信頼性のある物理的位置を前記クライアント装置に関連付けるように構成された位置モジュールを備えているシステム。
【請求項７３】
異なる物理的位置に複数の接続ポイントを含むデータネットワークインフラストラクチャーに接続された装置の物理的位置を決定する方法において、
前記接続ポイントの１つを通して前記データネットワークインフラストラクチャーと通信する装置との間でケーブルベースの伝送媒体を経て通過する通信信号の信号特性を測定するステップと、
前記測定された信号特性に基づいて前記装置の物理的位置を決定するステップであって、信号特性を接続ポイントに関連付ける記憶された情報をアクセスすることを含むステップと、
を備えた方法。
【請求項７４】
前記接続ポイントを各接続ポイント識別子で識別するステップを更に備えた請求項７３に記載の方法。
【請求項７５】
前記複数の接続ポイントの各々を通過する通信信号の信号特性を測定するステップと、
各測定された信号特性及びその各々の接続ポイントを関連付ける情報を記憶するステップと、
を更に備えた請求項７３に記載の方法。
【請求項７６】
物理的位置を決定する前記ステップは、信号特性に対する値を各物理的位置に関連させるファンクションを使用することを含む請求項７３に記載の方法。
【請求項７７】
前記信号特性は時間遅延を含む請求項７３に記載の方法。
【請求項７８】

前記信号特性は、時間遅延、時間ドメイン反射計測、信号減衰及びラウンドトリップ遅延、の少なくとも１つを含む請求項７３に記載の方法。

【請求項７９】

複数の接続ポイントを含むデータネットワークインフラストラクチャーを調査する方法において、そのデータネットワークインフラストラクチャーへのケーブルベースの通信経路を各々与える複数の接続ポイントの各々に対して、

前記接続ポイントに対する信号特性を決定するステップと、

前記接続ポイントに対する信号特性を前記ネットワークインフラストラクチャーに与えるステップと、

を備えた方法。

【請求項８０】

前記接続ポイントの各々とその信号特性との間の関連性を記憶するステップを更に備えた請求項７９に記載の方法。

【請求項８１】

前記接続ポイントの各々を各接続ポイント識別子で識別するステップを更に備えた請求項７９に記載の方法。

【請求項８２】

位置感知装置を前記接続ポイントの第１に接続し、そして前記位置感知装置を使用して前記接続ポイントの物理的位置を決定するステップを更に備えた請求項７９に記載の方法。

【請求項８３】

前記位置感知装置は、ＧＰＳ受信器を含む請求項８２に記載の方法。

【請求項８４】

前記第１の接続ポイントとその決定された物理的位置との間の関連性を記憶するステップを更に備えた請求項８２に記載の方法。

【請求項８５】

複数の接続ポイントの１つを通してデータネットワークインフラストラクチャーと通信している装置から動作信号特性を受信するように構成されたトランシーバと、

前記動作信号特性を、前記１つの接続ポイントに関連した記憶された信号特性と比較することにより、前記装置の物理的位置を決定するように構成された位置モジュールと、

を備えたシステム。

【請求項８６】

前記位置モジュールは、更に、前記信号特性に対する値を前記接続ポイントの各物理的位置に関連させるファンクションを使用するように構成される請求項８５に記載のシステム。

【請求項８７】

前記位置モジュールは、更に、前記接続ポイントの各々に対し信号特性とそれに対応する物理的位置との関連性を有する信号特性データベースを備えた請求項８５に記載のシステム。

【請求項８８】

位置に基づくアクセス制御情報を含むデータを供給するステップと、

前記位置に基づくアクセス制御情報に従って物理的位置におけるデータへのアクセスを制限するステップと、

を備えた方法。

【請求項８９】

前記データをアクセスする装置の物理的位置を決定し、そして前記決定された物理的位置に従って前記アクセスを制限するステップを更に備えた請求項８８に記載の方法。

【請求項９０】

データを供給する前記ステップは、データを暗号形態で供給することを含み、そしてデータへのアクセスを制限する前記ステップは、前記物理的位置に従ってデータの暗号解読

を行えるようにすることを含む請求項８８に記載の方法。
【請求項９１】
前記データは、コンピュータファイルで構成される請求項８８に記載の方法。
【請求項９２】
ファイルへのアクセスを制限する前記ステップは、オペレーティングシステムサービスを適用してアクセスを制限することを含む請求項９１に記載の方法。
【請求項９３】
ファイルへのアクセスを制限する前記ステップは、アプリケーションプログラムを使用してアクセスを制限することを含む請求項９１に記載の方法。
【請求項９４】
データネットワークを経て装置でデータを受信するステップと、
上記装置の物理的位置に基づいてそのデータへのアクセスを禁止するステップと、
を備えた方法。
【請求項９５】
物理的位置に基づいて制限ルート情報を含むデータを発生するステップを備えた方法。
【請求項９６】
前記制限ルート情報に従ってデータを送信するステップを更に備えた請求項９５に記載の方法。
【請求項９７】
データを受信するネットワーク装置が、前記制限ルート情報に従って制限された物理的位置に配置されている場合にデータを破壊するステップを更に備えた請求項９５に記載の方法。
【請求項９８】
前記制限ルート情報に従って制限された物理的位置に配置されているネットワーク装置へデータが送信されるのを禁止するステップを更に備えた請求項９５に記載の方法。
【請求項９９】
前記制限ルート情報に従って制限された物理的位置に配置されているクライアント装置によりデータがアクセスされるのを禁止するステップを更に備えた請求項９５に記載の方法。
【請求項１００】
前記制限ルート情報は、禁止された物理的位置を含む請求項９５に記載の方法。
【請求項１０１】
前記制限ルート情報は、許可された物理的位置を含む請求項９５に記載の方法。
【請求項１０２】
前記データは、データパケットを含む請求項９５に記載の方法。
【請求項１０３】
前記データは、ファイルを含む請求項９５に記載の方法。
【請求項１０４】
前記データは、ドキュメントを含む請求項９５に記載の方法。
【請求項１０５】
第１ネットワーク装置でデータを受信するステップと、
位置情報を使用して決定されたポリシーに基づいて第２ネットワーク装置へデータをルーティングするステップと、
を備えた方法。
【請求項１０６】
関連物理的位置をもつネットワーク装置と、
物理的位置に基づく制限ルート情報をもつデータと、
を備えたシステム。
【請求項１０７】
ネットワーク装置とそれらの各物理的位置との関連性を記憶するように構成された記憶

モジュールを含む物理的位置サーバーを更に備えた請求項１０６に記載のシステム。
【請求項１０８】
各ネットワーク装置は、その特定のネットワーク装置とその各物理的位置との関連性を記憶するように構成された記憶モジュールを含む請求項１０６に記載のシステム。
【請求項１０９】
各ネットワーク装置は、前記制限ルート情報に従ってデータを送信するように構成された位置モジュールを含む請求項１０６に記載のシステム。
【請求項１１０】
各ネットワーク装置は、データを受信する各ネットワーク装置が、前記制限ルート情報に従って制限された物理的位置に配置されている場合にデータを破壊するように構成された位置モジュールを備えた請求項１０６に記載のシステム。
【請求項１１１】
各ネットワーク装置は、前記制限ルート情報に従って制限された物理的位置に配置されている別のネットワーク装置へデータが送信されるのを禁止するように構成された位置モジュールを備えた請求項１０６に記載のシステム。
【請求項１１２】
各ネットワーク装置は、前記制限ルート情報に従って制限された物理的位置に配置されているクライアント装置によりデータがアクセスされるのを禁止するように構成された位置モジュールを備えた請求項１０６に記載のシステム。
【請求項１１３】
前記制限ルート情報は、禁止された物理的位置を含む請求項１０６に記載のシステム。
【請求項１１４】
前記制限ルート情報は、許可された物理的位置を含む請求項１０６に記載のシステム。
【請求項１１５】
前記データは、データパケットを含む請求項１０６に記載のシステム。
【請求項１１６】
前記データは、ファイルを含む請求項１０６に記載のシステム。
【請求項１１７】
前記データは、ドキュメントを含む請求項１０６に記載のシステム。
【請求項１１８】
物理的位置に基づく制限ルート情報を含むデータ。
【請求項１１９】
前記制限ルート情報を含むヘッダを更に含む請求項１１８に記載のデータ。
【請求項１２０】
前記制限ルート情報は、ネットワーク層情報を含む請求項１１８に記載のデータ。
【請求項１２１】
前記制限ルート情報は、トランスポート層情報を含む請求項１１８に記載のデータ。
【請求項１２２】
前記制限ルート情報は、禁止された物理的位置を識別する請求項１１８に記載のデータ。
【請求項１２３】
前記制限ルート情報は、許可された物理的位置を識別する請求項１１８に記載のデータ。
【請求項１２４】
データパケットを更に備えた請求項１１８に記載のデータ。
【請求項１２５】
ファイルを更に備えた請求項１１８に記載のデータ。
【請求項１２６】
ドキュメントを更に備えた請求項１１８に記載のデータ。
【請求項１２７】

隣接ネットワーク装置からの接続情報を第１装置で受信するステップと、
前記接続情報に基づいて前記第１装置の物理的位置を決定するステップと、
を備えた方法。
【請求項１２８】
前記隣接ネットワーク装置から送信された物理的位置を前記第１装置で受信するステップを更に備えた請求項１２７に記載の方法。
【請求項１２９】
前記物理的位置は、第１物理的位置であり、そして前記隣接ネットワーク装置は、第１隣接ネットワーク装置であり、前記方法は、更に、
第２の隣接ネットワーク装置から送信された第２物理的位置を前記第１装置で受信するステップと、
前記第１物理的位置を前記第２物理的位置と比較して、前記第１装置の前記決定された物理的位置の信用レベルを決定するステップと、
を備えた請求項１２８に記載の方法。
【請求項１３０】
前記隣接ネットワーク装置に基づき前記物理的位置に信頼性レベルを関連付けるステップを更に備えた請求項１２８に記載の方法。
【請求項１３１】
前記第１装置は、ルーター、スイッチ、ネットワークエントリー装置、ファイアウオール装置、ゲートウェイ、ワイヤレスアクセスポイント、及びコンピュータ装置より成るグループに属する請求項１２８に記載の方法。
【請求項１３２】
接続ポイントの物理的位置を決定し、そしてその物理的位置を、前記接続ポイントと通信しているクライアント装置に送信するように構成された位置モジュールを備えたシステム。
【請求項１３３】
前記クライアント装置は、前記物理的位置モジュールからの物理的位置を受信するように構成され、そして
前記クライアント装置と通信する隣接ネットワーク装置を更に備え、該隣接ネットワーク装置は、前記物理的位置モジュールを含む請求項１３２に記載のシステム。
【請求項１３４】
前記物理的位置は、第１の物理的位置であり、そして前記隣接ネットワーク装置は、第１の隣接ネットワーク装置であり、前記システムは、更に、
前記クライアント装置の第２の物理的位置を決定してその第２の物理的位置を前記クライアント装置に送信するように構成された物理的位置モジュールをもつ第２の隣接ネットワーク装置を備え、
前記ネットワーク装置は、更に、前記第２の物理的位置を受信し、そして前記第１の物理的位置を前記第２の物理的位置と比較して、前記クライアント装置の物理的位置の信用レベルを決定するように構成された請求項１３３に記載のシステム。
【請求項１３５】
前記隣接ネットワーク装置に基づく信頼性レベルが前記物理的位置に関連付けされる請求項１３３に記載のシステム。
【請求項１３６】
前記クライアント装置は、ルーター、スイッチ、ネットワークエントリー装置、ファイアウオール装置又はゲートウェイを含む請求項１３３に記載のシステム。
【請求項１３７】
機械が、隣接ネットワーク装置からの接続情報を第１装置で受信するようにさせ、そして前記接続情報に基づいて前記第１装置の物理的位置を決定するようにさせる実行可能な命令信号を記憶する機械読み取り可能な媒体を含む物品。
【請求項１３８】

クライアント装置からのネットワークアクセスの要求をネットワークインフラストラクチャーのネットワークエントリー装置で受信するステップと、
前記クライアント装置の物理的位置を前記ネットワークインフラストラクチャーにより決定するステップと、
前記物理的位置に基づいて前記クライアント装置の許可を決定するステップと、
を備えた方法。
【請求項１３９】
許可を決定する前記ステップは、更に、前記ネットワークエントリー装置により許可を決定することを含む請求項１３８に記載の方法。
【請求項１４０】
許可を決定する前記ステップは、更に、前記物理的位置を他のユーザ証明と共に許可装置へ供給することを含む請求項１３８に記載の方法。
【請求項１４１】
許可を決定する前記ステップは、更に、前記物理的位置に基づいてサービスレベルを決定することを含む請求項１３８に記載の方法。
【請求項１４２】
ユーザ証明を前記ネットワークエントリー装置で受信するステップを更に備え、
許可を決定する前記ステップは、更に、前記物理的位置及び前記ユーザ証明に基づいてサービスのレベルを決定することを含む請求項１４１に記載の方法。
【請求項１４３】
許可を決定する前記ステップは、更に、前記物理的位置に関連した信頼性レベルが規定のスレッシュホールド以上である場合には前記クライアント装置に関連したユーザを許可することを含む請求項１３８に記載の方法。
【請求項１４４】
許可を決定する前記ステップは、更に、ＩＥＥＥ８０２．１Ｘに基づいて通信することを含む請求項１３８に記載の方法。
【請求項１４５】
クライアント装置の物理的位置を決定するように構成されたネットワークインフラストラクチャーを備えたシステムにおいて、前記ネットワークインフラストラクチャーは、
クライアント装置からのネットワークアクセスの要求を受信しそして前記物理的位置に基づいて前記クライアント装置の許可を決定するように構成されたネットワークエントリー装置を含むシステム。
【請求項１４６】
前記ネットワークエントリー装置は、更に、前記物理的位置に基づいてサービスのレベルを決定するように構成される請求項１４５に記載のシステム。
【請求項１４７】
前記ネットワークエントリー装置は、更に、ユーザ証明を受信し、そして前記物理的位置及び前記ユーザ証明に基づいてサービスレベルを決定するように構成された請求項１４５に記載のシステム。
【請求項１４８】
前記ネットワークエントリー装置は、更に、前記物理的位置に関連した信頼性レベルが規定のスレッシュホールド以上である場合には前記クライアント装置に関連したユーザを許可するように構成される請求項１４５に記載のシステム。
【請求項１４９】
前記ネットワークエントリー装置は、更に、ＩＥＥＥ８０２．１Ｘに基づいて通信するように構成される請求項１４５に記載のシステム。
【請求項１５０】
機械が、クライアント装置からのネットワークアクセスの要求をネットワークインフラストラクチャーのネットワークエントリー装置で受信するようにさせ、
前記クライアント装置の物理的位置を前記ネットワークインフラストラクチャーにより

決定するようにさせ、そして
前記物理的位置に基づいて前記クライアント装置の許可を決定するようにさせる実行可能な命令信号を記憶する機械読み取り可能な媒体を含む物品。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、データネットワーク内の位置情報の決定及び使用に係る。
本出願は、次の米国仮特許出願に対する優先権を請求する。２００２年３月１日に出願された「A System for Network Definition Based on Device Location」と題する第６０／３６１，４１９号；２００２年３月１日に出願された「A System to Regulate Access as a Function of Device Location」と題する第６０／３６１，４２１号；２００２年３月１日に出願された「Systems and Methods to Define Location of a Network Device or a Networked Device」と題する第６０／３６１，４２０号；２００２年３月１日に出願された「A System and Method to Provide Security in a Network Based on Device Location Information」と題する第６０／３６１，３８０号；２００２年６月１０日に出願された「Location Discovery and Configuration Provisioning Server」と題する第６０／３８７，３３１号；及び２００２年６月１０日に出願された「System and Method for Switch Based Location Discovery and Configuration Provisioning of Network Attached Devices」と題する第６０／３８７，３３０号。これら特許出願の各々の全体的な内容を参考としてここに援用する。
【背景技術】
【０００２】
コンピュータシステムは、個人間で情報を交換するための有用なツールである。情報は、データ、音声、グラフィック及びビデオを含むが、これらに限定されない。交換は、コンピュータシステムを一緒にリンクする相互接続部を介して情報を表わす電子信号の転送を許すやり方で確立される。相互接続部は、ケーブル又はワイヤレスのいずれでもよい。ケーブル接続は、例えば、金属及び光ファイバ素子を含む。ワイヤレス接続は、例えば、赤外線、音響及び無線波送信を含む。
【０００３】
ある種の共通性を有する相互接続されたコンピュータシステムは、ネットワークとして表わされる。例えば、大学のキャンパスに関与した個人が各々コンピュータ装置を有してもよい。更に、キャンパス全体に点在した共用プリンタ及び遠隔配置のアプリケーションサーバーがあってもよい。全ての個人が何らかの状態で大学に関与しているという点で個人間に共通性がある。例えば、健康管理施設、製造場所及びインターネットアクセスユーザを含む他の環境においても、個人及びそれらのコンピュータ構成に対して同じことが言える。ネットワークは、共通グループの種々のコンピュータシステム間で、ある選択可能なやり方で通信又は信号交換を許す。これらコンピュータシステムと、システム間での交換を調整し容易にする装置との相互接続が、ネットワークを表わす。更に、ネットワークを互いに相互接続して、インターネットワークを確立してもよい。
【発明の開示】
【発明が解決しようとする課題】
【０００４】
ネットワーク又はインターネットワークの種々のコンピュータシステムが通信するプロセスは、一般に、ネットワークインターフェイスカード又は回路で実施される合意型信号交換規格及びプロトコルによって調整される。このような規格及びプロトコルは、複数の供給者から入手できるコンピュータシステムのアレー間で相互運用性を与える必要性及び要望から生れた。信号交換規格化の責任を果たしている２つの組織は、インスティテュート・オブ・エレクトリカル・アンド・エレクトロニック・エンジニアズ（ＩＥＥＥ）、及びインターネット・エンジニアリング・タスク・フォース（ＩＥＴＦ）である。特に、インターネットの運用性に関するＩＥＥＥ規格は、ローカルエリアネットワーク（ＬＡＮ）

及びメトロポリタンエリアネットワーク（ＭＡＮ）に関するＩＥＥＥ８０２コミッティーの権限のもとで確立され又は確立されつつある。

【課題を解決するための手段】

【０００５】

一般的な態様において、本発明は、ネットワークリンク型装置が接続されたネットワークにおいて物理的な位置をそのような装置に関連付けるシステムを特徴とする。このシステムは、装置の位置を確立するための種々の技術を使用する。システムコンフィギュレーションは、変更可能であるが、ＬＡＮ、ＭＡＮ、ワイドエリアネットワーク（ＷＡＮ）、パーソナルエリアネットワーク（ＰＡＮ）、及びホームネットワークを含む任意の形式のデータネットワークを備えることができる。このシステムは、特定の装置に対する位置情報をネットワーク装置及び管理部に供給するもので、コンフィギュレーション精度、制御及びセキュリティを改善するために種々のやり方で使用することができる。又、位置情報は、装置自体を制御し又は保安するのに使用されてもよい。

【０００６】

更に別の特徴は、ネットワークエントリー装置及び／又は中間装置が位置情報を取得するところのメカニズムに係る。これらメカニズムは、一般に、絶対及び相対位置情報を取得するための技術を含む。絶対位置情報は、座標系における既知の地理的識別子、例えば、緯度及び経度、推測航法(dead reckoning)、位置決めされるべき装置に固定されるか又はその付近にあるグローバル・サテライト・ポジショニング（ＧＰＳ）システム、慣性ロケーター、光学的ロケーター、及び他の技術を使用して得ることができる。相対位置は、既知の位置を有する装置からのベクトル処理、又は既知の位置からのベクトル処理により得ることができる。又、相対位置は、既知の無線ベース又は光学ベースの位置からの三角測量、ある範囲の位置を定義するための整相アレーサーチ、又はある範囲の位置へとマップされる信号強度減衰により得られてもよい。当該装置の位置を固定するための他の技術を使用してもよい。

【０００７】

装置が、それ自身の位置を決定し、そして始動時、接続時又は問合せ時に、その情報をネットワーク内のアプリケーションに中継することもできるし、或いはシステムが、装置の位置を決定し、その情報を記憶して、適当で且つ有用な場合にそれを装置に与えることもできる。又、絶対及び相対位置情報の両方が、位置情報が確実なものでシステムにより信頼され得るかどうか決定するための信頼レベルパラメータを含むことができる。その装置位置が絶対又は相対手段によって固定され、そしてファイル又はプログラムアーギュメントのような識別可能なやり方で装置に関連付けされると、装置位置を多数のやり方で使用して、システムのオペレーション又はシステムにより提供されるサービスを向上させることができる。例えば、どこでユーザの証明が必要になっても、装置の位置を要求することができる。換言すれば、装置の位置が、必要な証明の一部分となる。

【０００８】

１つの態様において、データ通信ネットワークにおいてクライアントの物理的な位置を決定する方法が提供される。この方法は、クライアントがデータネットワークと通信するときに通る接続ポイントの識別子を決定するステップと、接続ポイントのその決定された識別子に基づいてクライアントの物理的な位置を決定するステップであって、接続ポイントの識別子と物理的な位置との間の記憶された関連性をアクセスすることを含むステップとを備えている。

【０００９】

他の例において、この方法は、次の特徴の１つ以上を含むことができる。

接続ポイントは、ケーブルベースの伝送媒体を経てクライアントへの通信経路を与えることができる。ケーブルベースの伝送媒体は、例えば、ワイヤ導体又は光ファイバを含むことができる。

【００１０】

又、この方法は、クライアントが接続ポイントに接続するのに応答して物理的位置を決

定するステップも含むことができる。又、物理的位置は、タイマーの時間切れ、通信リンクの切断、通信セッションの終了、ユーザの証明の変更、ファイアウオールアラームのトリガー、新たなネットワーク装置のネットワークへの加入、マネージメントステーションによる促進、装置の特定の移動の検出、シャドー（ネットワークのユーザ又は装置）装置の検出、等の種々の事象の１つ以上に応答して決定することもできる。

【００１１】

この方法は、更に、接続ポイント識別子と各物理的位置との関連性を記憶するステップであって、クライアントが接続ポイントに接続する前に接続ポイント識別子と物理的位置との関連性を記憶することを含むステップを備えることもできる。

又、この方法は、更に、ネットワーク装置から接続情報を送信するステップを含むこともでき、ここで、接続ポイント識別子を決定するステップは、この接続情報を使用して接続ポイント識別子を決定することを更に含む。

【００１２】

この方法は、更に、ネットワーク装置を識別する接続情報の第１部分を決定するステップを含むことができる。この第１部分は、装置のＭＡＣアドレス又は装置のＩＰアドレスのようなネットワーク装置のアドレスを含むことができる。

この方法は、更に、接続ポイントへの通信経路を与えるネットワーク装置の接続ポートを識別する接続情報の第２部分を決定するステップを含むことができる。この第２部分は、例えば、接続ポートのＭＡＣアドレス、又は装置ＩＤに含まれたインデックス属性を含むことができる。

【００１３】

又、この方法は、更に、クライアントから信号を受信し、そしてその信号の第１特性をネットワーク装置により測定するステップを含むことができる。更に、この方法は、この第１特性に基づいて物理的位置を決定するステップを含むことができる。この方法は、更に、以前に測定された特性と各物理的位置との関連性を記憶し、そして第１特性及び以前に測定された特性に基づいて物理的位置を決定するステップを含むことができる。この方法は、更に、ケーブルベースの伝送媒体を経て受信した信号の第１特性を第１ネットワーク装置により測定し、そしてワイヤレス伝送媒体を経て受信した信号の第２特性を第２ネットワーク装置により測定するステップを含むことができる。この例では、物理的位置を決定するステップは、更に、測定された第１特性及び測定された第２特性に基づいて物理的位置を決定することを含むことができる。

【００１４】

この方法は、更に、物理的位置データベースを使用して接続ポイント識別子と物理的位置との間の関連性を記憶するステップを含むことができる。この方法は、更に、集中型物理的位置サーバーにおいて接続ポイント識別子と物理的位置との間の関連性を記憶するステップを含むことができる。この方法は、更に、接続ポイント識別子と、ネットワーク装置間に分散された物理的位置との間の関連性を記憶するステップを含むことができる。接続ポイントは、ジャックを含むことができる。この方法は、更に、物理的位置と、ＭＡＣアドレス、アドレス、電話番号、プロトコル形式、アセットＩＤ及び所有者の少なくとも１つとの間の関連性を記憶するステップを含むことができる。

【００１５】

又、この方法は、更に、物理的位置に基づいて認証を決定するステップを含むことができる。この方法は、更に、物理的位置に基づいてサービスのレベルを決定するステップを含むことができる。この方法は、更に、物理的位置に基づいてセキュリティ機能を使用するステップを含むことができる。この方法は、更に、物理的位置に基づいて送信データを暗号化するステップを含むことができる。この方法は、更に、物理的位置に関連した一時的キーを使用するステップを含むことができる。この方法は、更に、接続ポイント識別子に対して記憶された関連性をサーチし、そしてその記憶された関連性において接続ポイント識別子に関連した物理的位置を識別するステップを含むことができる。物理的位置は、緯度及び経度フォーマット、緯度、経度、高度、及び精度フォーマット、位置識別番号、

テクスチャストリング表示、及び／又は関係情報を伴う相対的物理的位置を含むことができる。

【００１６】

この方法は、更に、物理的位置に基づいて接続ポリシーを確立するステップを含むことができる。この方法は、更に、接続ポリシーに基づいてネットワークエントリー装置においてユーザを認証するステップを含むことができる。この方法は、更に、接続ポイントに関連した装置に物理的位置を送信するステップを含むことができる。この方法は、更に、物理的位置に基づいて、接続ポイントに関連した装置にコンフィギュレーション情報を送信するステップを含むことができる。この方法は、更に、接続ポイントに基づいて物理的位置を信頼性のある装置で決定するステップを含むことができる。この信頼性のある装置は、ネットワークインフラストラクチャー内に配置することができる。この方法は、更に、物理的位置と信頼性レベルとの間の関連性を記憶するステップを含むことができる。この方法は、更に、物理的位置を決定する装置に基づいて物理的位置の信頼性レベルを決定するステップを含むことができる。

【００１７】

別の態様において、複数の接続ポイントを含むデータネットワークインフラストラクチャーを調査する方法が提供される。この方法は、第１接続ポイントに対する物理的位置を決定するステップと、第１接続ポイントに対する物理的位置をネットワークインフラストラクチャーに与えるステップと、第２接続ポイントに対する物理的位置を決定するステップとを備えている。又、この方法は、第２接続ポイントに対する物理的位置をネットワークストラクチャーに与えるステップも含む。他の例では、この方法は、次の特徴を含むことができる。この方法は、更に、第１接続ポイントとその物理的位置との間の第１の関連性を記憶し、そして第２接続ポイントとその物理的位置との間の第２の関連性を記憶するステップを含むことができる。この方法は、更に、第１及び第２の接続ポイントを、各々第１及び第２の接続ポイント識別子で識別するステップを含むことができる。この方法は、更に、位置感知装置を第１接続ポイントに接続するステップを含むことができる。この位置感知装置は、例えば、ＧＰＳ受信器又は慣性ポジショニングシステムを含むことができる。

【００１８】

別の態様において、データ通信ネットワーク内のクライアントの物理的位置を決定する方法が提供される。この方法は、ケーブルベースの伝送媒体を経て接続ポイントへクライアントを接続するステップと、クライアントが通信するところの接続ポイントを決定するステップとを備えている。又、この方法は、接続ポイントに基づいてクライアントの物理的位置を決定するステップと、接続ポイントと物理的位置との間の関連性を記憶するステップも備えている。

【００１９】

別の態様において、接続ポイント識別子を決定し、その接続ポイント識別子に基づいて物理的位置を決定するように構成され、その接続ポイント識別子と物理的位置との間の記憶された関連性をアクセスすることも含むように構成された位置モジュールを備えたシステムが提供される。このシステムは、次の特徴を含むことができる。このシステムは、位置モジュールと通信する位置クライアントを更に含むことができる。この位置クライアントは、第２層プロトコルを使用して位置モジュールと通信することができる。位置クライアントは、第３層プロトコルを使用して位置モジュールと通信することができる。

【００２０】

別の態様において、データネットワークインフラストラクチャー内の１つ以上の信頼性のあるネットワーク装置により、そのデータネットワークインフラストラクチャーへのアクセスを要求しているクライアント装置の物理的位置を決定して、信頼性のある物理的位置を発生するステップと、その信頼性のある物理的位置とクライアント装置とを関連付けるステップとを備えた方法が提供される。

【００２１】

この方法は、候補ネットワーク装置が信頼性のあるネットワーク装置であるかどうかを、偽の物理的位置データを与えるように候補ネットワーク装置を変更できる確率に基づいて決定するステップを含むことができる。又、この方法は、次の特徴を含むこともできる。更に、この方法は、許可を受けた者以外の誰かが１つ以上の信頼性のあるネットワーク装置へアクセスするのを禁止するステップも含むことができる。

【００２２】

１つ以上の信頼性のあるネットワーク装置は、規定のスレッシュホールド以上の信頼性レベルに関連付けることができる。規定のスレッシュホールドは、クライアント装置による要求の形式に基づいて変更することができる。信頼性のある物理的位置は、信頼性レベルに関連付けることができる。この方法は、更に、１つ以上のネットワーク装置に基づいて信頼性のある物理的位置の信頼性レベルを決定するステップを含むことができる。この方法は、更に、１つ以上のネットワーク装置とクライアント装置との間の通信方法に基づいて信頼性レベルを決定するステップを含むことができる。この方法は、更に、信頼性のある物理的位置に基づいてクライアントのネットワークアクティビティを規制するステップを含むことができる。

【００２３】

又、この方法は、更に、信頼性のある物理的位置に基づいてクライアントによるアクセス要求に対する応答を決定するステップを含むことができる。この方法は、更に、信頼性のある物理的位置に基づいてクライアントへ与えられるネットワークリソースを制御するステップを含むことができる。この方法は、更に、信頼性のある物理的位置を緊急状態応答当局へ送信するステップを含むことができる。この方法は、更に、信頼性のある物理的位置に基づいてクライアントへ情報を供給するステップを含むことができる。この方法は、更に、物理的位置の規定の半径以内の当該ポイントを含む情報を供給するステップを含むことができる。

【００２４】

別の態様において、データネットワークインフラストラクチャー内の信頼性のあるソースから第１位置情報を送信するステップを含む方法が提供される。又、この方法は、ネットワークへのアクセスを要求するクライアント装置から第２の位置情報を受信するステップも含み、第２の位置情報は、第１の位置情報に基づくものであり、そして更に、第１及び第２の位置情報に基づいて信頼性のある位置を決定するステップも含む。他の例では、この方法は、次の特徴を含むことができる。この方法は、更に、信頼性のある物理的位置に基づいてクライアントのネットワークアクティビティを規制するステップも含むことができる。更に、この方法は、信頼性のある物理的位置に基づいてクライアントに与えられるネットワークリソースを制御するステップを含むことができる。

【００２５】

別の態様において、装置の物理的な位置に対する値を決定するステップを含む方法が提供される。又、この方法は、その決定された値に対応する信頼性のレベルを決定するステップと、信頼性のレベルを物理的位置の値と関連付けるステップとを含む。他の例では、この方法は、次の特徴を含むことができる。この方法は、更に、物理的位置の値を決定するのに使用される技術の精度に基づいて信頼性のレベルを決定するステップを含むことができる。この方法は、更に、物理的位置の値を決定するのに使用される考えられる値の範囲の粒度に基づいて信頼性のレベルを決定するステップを含むことができる。この方法は、更に、値の決定が物理的位置に対して偽の値を生じ得る確率に基づいて信頼性レベルを決定するステップを含むことができる。この方法は、更に、物理的位置の値を決定するネットワーク装置の信頼性レベルに基づいて信頼性レベルを決定するステップを含むことができる。

【００２６】

別の態様において、データネットワークインフラストラクチャー内に信頼性のあるネットワーク装置を備えたシステムであって、ネットワーク装置は、ネットワークインフラストラクチャーへのアクセスを要求するクライアント装置の信頼性のある物理的位置を決定

し、そしてその信頼性のある物理的位置をクライアント装置に関連付けるように構成された位置モジュールを備えているシステムが提供される。

【００２７】

１つの態様において、異なる物理的位置に複数の接続ポイントを含むデータネットワークインフラストラクチャーに接続された装置の物理的位置を決定する方法が提供される。この方法は、接続ポイントの１つを通してデータネットワークインフラストラクチャーと通信する装置から動作信号特性を受信するステップと、装置の物理的位置を決定するステップであって、信号特性と接続ポイントとの記憶された関連性をアクセスすることを含むステップとを備えている。他の例では、この方法は、次の特徴を含むことができる。この方法は、更に、接続ポイントを各接続ポイント識別子で識別するステップを含むことができる。前記装置は、ケーブルベースの伝送媒体を経て接続ポイントに接続することができる。

【００２８】

又、この方法は、更に、複数の接続ポイントの各々において信号特性を測定するステップと、複数の各接続ポイントに対して信号特性及びその各々の接続ポイントの関連性を記憶するステップとを含むことができる。この方法は、更に、信号特性に対する値を各物理的位置に関連させるファンクションを使用するステップを含むことができる。信号特性は時間遅延を含むことができる。又、信号特性は、時間遅延、時間ドメイン反射計測、信号減衰及び／又はラウンドトリップ遅延を含むことができる。

【００２９】

別の態様において、複数の接続ポイントを含むデータネットワークインフラストラクチャーを調査する方法が提供される。この方法は、第１接続ポイントに対する信号特性を決定するステップと、第１接続ポイントに対する信号特性をネットワークインフラストラクチャーに与えるステップとを備えている。又、この方法は、第２接続ポイントに対する信号特性を決定するステップと、第２接続ポイントに対する信号特性をネットワークインフラストラクチャーに与えるステップも備えている。

【００３０】

他の例において、この方法は、次の特徴を含むことができる。この方法は、更に、第１接続ポイントとその信号特性との間の第１関連性を記憶するステップと、第２接続ポイントとその信号特性との間の第２関連性を記憶するステップとを含むことができる。この方法は、更に、第１及び第２の接続ポイントを各第１及び第２の接続ポイント識別子で識別するステップを含むことができる。この方法は、更に、位置感知装置を第１の接続ポイントに接続するステップを含むことができる。位置感知装置は、ＧＰＳを含むことができる。この方法は、更に、第１接続ポイントとその物理的位置との間の第３関連性を記憶するステップを含むことができる。

【００３１】

別の態様において、トランシーバ及び位置モジュールを備えたシステムが提供される。トランシーバは、複数の接続ポイントの１つを通してデータネットワークインフラストラクチャーと通信している装置から動作信号特性を受信するように構成される。位置モジュールは、動作信号特性を、１つの接続ポイントに関連した記憶された信号特性と比較することにより、装置の物理的位置を決定するように構成される。他の例において、このシステムは、次の特徴を含むことができる。位置モジュールは、更に、信号特性に対する値を接続ポイントの各物理的位置に関連付けるファンクションを使用するように構成することができる。位置モジュールは、更に、接続ポイントの各々に対して信号特性とそれに対応する物理的位置との関連性を有する信号特性データベースを含むことができる。

【００３２】

別の態様において、位置に基づくアクセス制御情報を含むデータが供給される。ある物理的位置のデータへのアクセスは、位置に基づくアクセス制御情報に従って制限される。

この態様は、次の特徴の１つ以上を含むことができる。

データをアクセスする装置の物理的位置を決定することができ、そしてアクセスの制限

が、その決定された物理的位置に基づいて行なわれる。
データの供給は、データを暗号化形態で供給することを含み、そしてデータへのアクセスの制限は、物理的位置に基づいてデータの暗号解読を行なえるようにすることを含む。
【００３３】
この態様は、データを種々の位置に分布させることができるが、許可された位置でしかアクセスできないという効果を有することができる。このように、アクセスを行なうべき実際の位置を、例えば、データをアクセスするのを許すパスワードと共に、証明の一部分として使用することができる。例えば、ラップトップコンピュータのディスクにファイルがロードされる場合には、ラップトップコンピュータの位置で、ファイルをオープンできるかどうか決定することができる。データがコンピュータファイルの形態をとるときには、例えば、データをアクセスするオペレーティングシステムサービス又はアプリケーションプログラムにおいてアクセス制限をホスト処理することができる。
【００３４】
別の態様において、物理的位置に基づいて制限ルート情報を含むデータを発生する方法が提供される。他の例では、この方法は、次の特徴を含むことができる。この方法は、更に、制限ルート情報に基づいてデータを送信するステップを含むことができる。この方法は、更に、データを受信するネットワーク装置が、制限ルート情報に基づいて制限された物理的位置に配置されている場合にデータを破壊するステップを含むことができる。
この方法は、制限ルート情報に基づいて制限された物理的位置に配置されているネットワーク装置へデータが送信されるのを禁止するステップを含むことができる。
【００３５】
又、この方法は、更に、制限ルート情報に基づいて制限された物理的位置に配置されているクライアント装置によりデータがアクセスされるのを禁止するステップを含むことができる。制限ルート情報は、禁止された物理的位置を含むことができる。又、制限ルート情報は、許可された物理的位置を含むことができる。データは、データパケット、ファイル及び／又はドキュメントを含むことができる。
別の態様において、ネットワークを経て送信するためのデータであって物理的位置タグを含むデータを発生するステップを含む方法が提供される。
【００３６】
更に別の態様において、第１ネットワーク装置でデータを受信するステップと、第２ネットワーク装置の地理的な物理的位置に基づいて第２ネットワーク装置へのデータの送信を禁止するステップとを備えた方法が提供される。
別の態様において、装置でデータを受信するステップと、装置の物理的位置に基づいてそのデータへのアクセスを禁止するステップとを備えた方法が提供される。
【００３７】
更に別の態様において、ネットワーク装置及びデータを含むシステムが提供される。ネットワーク装置は、関連する物理的位置を有する。データは、物理的位置に基づく制限ルート情報を含む。他の例では、このシステムは、次の特徴を含むことができる。このシステムは、更に、ネットワーク装置とそれらの各物理的位置との関連性を記憶するように構成された記憶モジュールを有する物理的位置サーバーを含むことができる。各ネットワーク装置は、その特定のネットワーク装置とその各々の物理的位置との関連性を記憶するように構成された記憶モジュールを含むことができる。各ネットワーク装置は、制限ルート情報に基づいてデータを送信するように構成された位置モジュールを含むことができる。各ネットワーク装置は、データを受信する各ネットワーク装置が、制限ルート情報に基づいて制限された物理的位置に配置されている場合にデータを破壊するように構成された位置モジュールを含むことができる。
【００３８】
又、各ネットワーク装置は、制限ルート情報に基づいて制限された物理的位置に配置されている別のネットワーク装置へデータが送信されるのを禁止するように構成された位置モジュールも含むことができる。各ネットワーク装置は、制限ルート情報に基づいて制限

された物理的位置に配置されているクライアント装置によりデータがアクセスされるのを禁止するように構成された位置モジュールを含むことができる。制限ルート情報は、禁止された物理的位置を含むことができる。制限ルート情報は、許可された物理的位置を含むことができる。データは、データパケット、ファイル及び／又はドキュメントを含むことができる。

【００３９】

別の態様において、物理的位置に基づいて制限ルート情報を含むデータが提供される。このデータは、更に、制限ルート情報を含むヘッダを含むことができる。この情報は、例えば、位置情報の登録に基づいて情報を識別するために、明確に又はタグを使用して表わされてもよい。制限ルート情報は、ネットワーク層及び／又はトランスポート層に含ませることができる。制限ルート情報は、禁止された物理的位置を含むことができる。又、制限ルート情報は、許可された物理的位置を含むことができる。データは、データパケット、ファイル及び／又はドキュメントを含むことができる。

【００４０】

別の態様において、隣接ネットワーク装置からの接続情報を第１装置で受信するステップと、その接続情報に基づいて第１装置の物理的位置を決定するステップとを備えた方法が提供される。

この方法は、隣接ネットワーク装置から送信された物理的位置を第１装置で受信するステップを含むことができる。物理的位置は、第１の物理的位置であり、そして隣接ネットワーク装置は、第１の隣接ネットワーク装置である。この例では、この方法は、更に、第２の隣接ネットワーク装置から送信された第２の物理的位置を第１装置で受信するステップと、第１の物理的位置を第２の物理的位置と比較して、第１装置の実際の物理的位置の信用レベルを決定するステップとを含むことができる。この方法は、更に、隣接ネットワーク装置に基づいて物理的位置を信頼性レベルに関連付けするステップを含むことができる。第１装置は、ルーター、スイッチ、ネットワークエントリー装置、ファイアウオール装置、又はゲートウェイを含むことができる。

【００４１】

別の態様において、位置モジュールを備えたシステムが提供される。位置モジュールは、接続ポイントの物理的な位置を決定し、そしてその物理的な位置を、接続ポイントと通信するクライアント装置へ送信するように構成される。このシステムは、更に、物理的位置モジュールから物理的位置を受信するように構成されたクライアント装置と、該クライアント装置と通信する隣接ネットワーク装置とを含むことができ、この隣接ネットワーク装置は、物理的位置モジュールを含む。物理的位置は、第１の物理的位置であり、そして隣接ネットワーク装置は、第１の隣接ネットワーク装置である。この例では、システムは、更に、クライアント装置の第２の物理的位置を決定しそしてその第２の物理的位置をクライアント装置に送信するように構成された物理的位置モジュールをもつ第２の隣接ネットワーク装置を含むことができる。更に、クライアント装置は、第２の物理的位置を受信し、そして第１の物理的位置を第２の物理的位置と比較して、クライアント装置の実際の物理的位置の信用レベルを決定するように構成される。このシステムは、隣接ネットワーク装置に基づいて物理的位置を信頼性レベルに関連付けることができる。クライアント装置は、ルーター、スイッチ、ネットワークエントリー装置、ファイアウオール装置、ゲートウェイ、ワイヤレスアクセスポイント及び／又はコンピュータ装置を含むことができる。

【００４２】

別の態様において、クライアント装置からのネットワークアクセスの要求をネットワークインフラストラクチャーのネットワークエントリー装置で受信するステップを備えた方法が提供される。又、この方法は、クライアント装置の物理的な位置をネットワークインフラストラクチャーにより決定するステップと、その物理的な位置に基づいてクライアント装置の許可を決定するステップも含む。他の例では、この方法は、次の特徴を含むことができる。この方法は、更に、ネットワークエントリー装置により許可を決定するステッ

プを含むことができる。

【００４３】

この方法は、更に、物理的位置を他のユーザ証明と共に許可装置へ供給するステップを含むことができる。この方法は、更に、物理的位置に基づいてサービスのレベルを決定するステップを含むことができる。この方法は、更に、ユーザ証明をネットワークエントリー装置で受信するステップを含むことができ、ここで、許可を決定するステップは、物理的位置及びユーザ証明に基づいてサービスのレベルを決定することも含む。この方法は、更に、物理的位置に関連した信頼性レベルが規定のスレッシュホールド以上である場合にクライアント装置に関連したユーザを許可するステップを含むことができる。この方法は、更に、ＩＥＥＥ８０２．１Ｘに基づいて通信するステップも含むことができる。

【００４４】

別の態様において、ネットワークインフラストラクチャーを伴うシステムが提供される。ネットワークインフラストラクチャーは、クライアント装置の物理的な位置を決定するように構成される。ネットワークインフラストラクチャーは、クライアント装置からネットワークアクセスの要求を受け取りそして物理的位置に基づいてクライアント装置の許可を決定するように構成されたネットワークエントリー装置を備えている。又、このシステムは、次の特徴を含むことができる。ネットワークエントリー装置は、更に、物理的位置に基づいてサービスのレベルを決定するように構成できる。ネットワークエントリー装置は、更に、ユーザ証明を受け取り、そして物理的位置及びユーザ証明に基づいてサービスのレベルを決定するように構成することができる。ネットワークエントリー装置は、更に、物理的位置に関連した信頼性のレベルが規定のスレッシュホールド以上である場合にクライアント装置に関連したユーザを許可するように構成できる。ネットワークエントリー装置は、更に、ＩＥＥＥ８０２．１Ｘに基づいて通信するように構成することができる。

【００４５】

別の態様において、機械が上述した方法のいかなる組合せも実行するようにさせる実行可能な命令信号を記憶する機械読み取り可能な媒体を備えた製造物品が提供される。

本発明に関連した１つ以上の例の詳細を、添付図面を参照して以下に説明する。本発明の他の特徴、目的及び効果は、以下の説明、添付図面及び特許請求の範囲から明らかとなろう。添付図面全体にわたり同様の要素が同じ参照記号で示されている。

【発明を実施するための最良の形態】

【００４６】

１．０　概要（図１）

図１を参照すれば、位置認識システム１００は、該システム１００に関連したネットワークの一部分であるか又はそれを使用する装置の位置に基づいて動作してユーザにネットワークベースのサービスを提供する。システム１００は、多数のスイッチング装置を含むインフラストラクチャー１０１を備え、幾つかのスイッチング装置がインフラストラクチャー１０１の接続ポイント（例えば、１６０ａ－ｉ）に接続される。システム１００は、以下に述べる位置認識サービスを提供するためのハードウェア及びソフトウェア（例えば、サーバー１３４において実行されるアプリケーション）の両方を使用する。装置の位置は、装置の物理的な位置に関連付けることができ、これは、格子又はマップ座標（例えば、緯度、経度及び高度）、地域、或いは建築物、例えば、ビルの特定階床における座標又はビルの部屋番号を含む種々のやり方で特徴付けることができる。装置は、ユーザ装置１０４ａ及び１０４ｂのように、システム１００のインフラストラクチャー１０１の外部でもよい。又、装置は、ネットワークエントリー装置１１４ａ－ｂ（ネットワークのスイッチ又はエッジ装置と称されることもある）や、中央スイッチング装置１３６（例えば、ルーター）のように、インフラストラクチャー１０１の内部でもよい。ネットワークエントリー装置１１４は、ワイヤレスアクセスポイント１２０ａ－ｂを含み及び／又はそれに関連することができる。このワイヤレスアクセスポイント１２０は、１２０ａのように、ネットワークエントリー装置１１４に対して外部の個々の装置でもよいし、及び／又は１２０ｂのように、エントリー装置１１４に対して内部のものでもよい。

【００４７】
インフラストラクチャー１０１に対して内部及び外部の装置の幾つかは、位置モジュール１８５を含む。この位置モジュール１８５は、以下に詳細に述べるように、装置の位置を認識させるファンクションを含む。一例において、このファンクションは、位置情報を記憶するための位置データベースと、位置情報を他の装置へ通信するためのプロトコルと、位置に基づく規制を実施する（例えば、位置情報に基づいて規制することができる）ルールとを含む。又、このファンクションは、ここに述べる技術を使用して装置の位置を決定するのに必要なアルゴリズム及びプロセスも含むことができる。位置モジュール１８５は、システム１００のハードウェア及び／又はソフトウェアで実施することができる。例えば、装置において実行される特定のソフトウェアアプリケーションが位置ファンクションを提供／実施することができ、いずれかの装置のオペレーティングシステムが位置ファンクションを提供／実施することができ、及び／又はプログラマブルアレーのようなハードウェアモジュールを装置に使用して位置ファンクションを提供／実施することができる。

【００４８】
装置の位置を利用するために、システム１００は、先ず、その装置の位置を決定する。システム１００は、装置が他の装置と通信するのにケーブルベースの伝送媒体１１２を使用するか又はワイヤレス伝送媒体１１９を使用するかに基づいて、異なる技術を使用して装置の位置を決定する。ケーブルベースの伝送媒体１１２とは、光ケーブルや電線等の束縛された伝送媒体を指す。このようなケーブル伝送媒体は、多数の接続部（共用）、及び／又は２つの装置間のポイント対ポイント（専用）接続部に信号を供給することができる。ケーブルベースの媒体１１２は、システム１００のインフラストラクチャー１０１の一部分と考えることができる。通常、媒体１１２は、媒体の物理的な位置を容易に変更できないように設置される。例えば、ケーブルは、接続ポイント（例えば、ジャック）が固定位置となるように壁やコンジットを通して導かれる。ワイヤレス伝送媒体１１９とは、スルーフリーエアのような自由空間における伝送媒体を指す。ワイヤレス伝送媒体１１９は、一般に、伝送媒体が空気である通信、例えば、無線ベースの通信に係る。例えば、ＩＥＥＥ８０２．１１規格に基づく無線通信は、ワイヤレス伝送媒体１１９を使用する。ワイヤレス伝送媒体を使用する他のワイヤレス通信は、光通信（例えば、赤外線やレーザ等）、及び／又は音波や機械波のような空気中を通る他の通信の使用に係る。ワイヤレス媒体は、通信装置を配置することのできる非常に広い範囲の考えられる場所によって特徴付けられる。例えば、ＩＥＥＥ８０２．１１ベースのネットワークの場合には、移動装置が、環境に基づいて数百又は数千フィート離れたワイヤレスアクセスポイント１２０と通信することができる。

【００４９】
図１に示すシステム１００では、ユーザ装置１０４ａがケーブル１１２を使用して接続ポイント１６０ａ（例えば、壁内のジャック）を経てインフラストラクチャー１０１に接続する。同様に、ネットワークエントリー装置１１４ａ－ｂ及び中央スイッチング装置１３６がケーブルを使用して接続ポイント１６０ｂ－ｇに互いに接続される。ケーブルを使用するデータネットワークの一部分では、接続ポイント（例えば、１６０ａ－ｇ）は、装置に物理的に取り付けられるケーブルの端末である。接続ポート（例えば、１１３）は、ネットワーククライアントが通信するところの物理的ポートである。

【００５０】
上述したように、ケーブルに関連した接続ポイントは、一般に、位置が固定される。これらの接続ポイントの位置は、例えば、ケーブルが設置されるときに決定される。位置情報は、接続ポイントとそれに対応する位置との関連性を含む。システム１００は、位置モジュール１８５に位置情報を記憶する。位置モジュール１８５は、位置データベースを使用して位置情報を記憶することができる。集中型解決策の例では、システム１００は、システム１００のネットワークの全接続ポイントに対する位置情報を位置サーバー１３４の位置モジュール１８５ａに記憶する。別のセクションで以下に詳細に述べる分散型解決策

の例では、システム１００は、全接続ポイント又は接続ポイントの一部分に対する位置情報を位置モジュール１８５ａ－ｄの各々に記憶する。装置の位置を決定するための１つの解決策では、システム１００は、装置がネットワークインフラストラクチャー１０１に接続されるときに通る接続ポイント（例えば、１６０ａ－ｇ）を決定し、そしてその特定の接続ポイントに対応する記憶された位置情報を位置モジュール１８５において見出す。

【００５１】

ワイヤレス伝送媒体１１９を使用する装置は、接続ポイント１６０ｈ－ｉを経てインフラストラクチャー１０１に接続され、例えば、装置のトランシーバからネットワークエントリー装置１１４ａ－ｂのワイヤレスアクセスポイント１２０ａ－ｂへ各々通信する。接続ポイント１６０ａ－ｇと同様のこれらのワイヤレス接続ポイント１６０ｈ－ｉも、一般に、位置が固定される。しかしながら、ワイヤレス接続ポイント１６０ｈ－ｉに接続されるユーザ装置１０４の位置は、動的とすることができる。ユーザ装置１０４ｂの位置は、ユーザ装置１０４ｂが移動するときに変化する。固定のワイヤレス接続ポイント１６０ｈ－ｉは、ユーザ装置１０４ｂが立ち去ったときにユーザ装置１０４ｂともはや通信せず、従って、ある時間周期の後にユーザ装置１０４ｂに対する接続ポイントは、もはや存在しない。

【００５２】

ワイヤレス伝送媒体１１９を使用して装置の位置を決定する１つの解決策では、システム１００は、ユーザ装置１０４ｂから送信された信号を受信する通常多数のネットワーク装置（例えば、１２０ａ及び１２０ｂ）に対してユーザ装置１０４ｂの位置を決定する。システム１００は、異なるネットワーク装置で受信した信号の相対的時間遅延又は信号強度のような信号特性をワイヤレスアクセスポイント１２０ａ－ｂの既知の位置と組合せて使用する。システム１００は、他の既知の境界、例えば、そのユーザ装置１０４が動作しているビル内の壁を任意に使用して、ワイヤレス接続ポイント（例えば、１２０ａ又は１２０ｂ）に対するエリアの位置を更に制限する。システム１００は、１つ以上の接続ポイント１６０ｈ－ｉに関連したワイヤレスユーザ装置１０４ｂに対応する位置情報を位置モジュール１８５（例えば、集中型解決策の例では１８５ａ）に記憶する。システム１００は、ユーザ装置１０４ｂが移動するときに、対応する位置情報を更新する。

【００５３】

装置の位置が決定されると、システム１００は、その位置情報を種々のやり方で使用する。システム１００は、装置が追加又は移動されるときにそれらの位置に基づいてインフラストラクチャー１０１内又はインフラストラクチャー１０１の外部に装置を設けて構成することができる。これは、ネットワーク装置が、自動的な形態でその位置を学習し、そしてその位置に基づいて、それ自身を構成し、あるやり方で動作し、且つある位置に基づくルールを実施できるようにする。例えば、ネットワークエントリー装置１１４ａは、新たなネットワークエントリー装置であって、接続すると、その位置及びコンフィギュレーション、並びにその位置に基づく動作ルールを位置サーバー１３４から自動的な形態で学習するような新たな装置と置き換えることができる。

【００５４】

システム１００は、装置の位置に基づいて初期に連続的なベースである制限を実施することができる。システム１００は、ネットワークへのアクセス又はネットワークに記憶されたデータへのアクセスをユーザ装置１０４の位置に基づいて制限することができる。例えば、システム１００は、会計データベースへのアクセスを、会計部門オフィス内（例えば、あるビルのある階床のある座標内）に位置するユーザ装置１０４のみに制限する。更に、システム１００は、ユーザ装置１０４を１つの位置だけに基づいて認証できないように周期的及び／又は連続的にこれらの制限を規制し、次いで、その認証に基づいて別の非許可の位置で制限されたサービスにアクセスするように試みることもできる。又、位置は、例えば、速度及びサービスクオリティ（ＱｏＳ）のようなネットワークリソースの割り当てに使用されるユーザ識別又は装置形式に加えて、別のパラメータでもある。

【００５５】

又、システム１００は、インフラストラクチャー１０１を通るデータの流れを、そのデータの位置制限に基づいて制限する。例えば、システム１００は、会計データベースからのデータを会計部門オフィス（例えば、ある座標で定義されたエリア）内に留まるように制限することができる。このような制限を実施するための１つの解決策では、データは、位置制限（例えば、許可された位置及び／又は禁止された位置）を含むタグを有する。例えば、データを発生するアプリケーション、及び／又はネットワークを経てデータを搬送するためのデータパケットを発生するサーバーは、データ及び／又はパケットを発生しながらこのタグを追加することができる。システム１００内の装置及びアプリケーションは、許可された位置以外にある装置へデータをルーティングするのを許さず、許可された位置以外の位置にデータがある場合にそれを破壊し、及び／又は許可された位置以外のところにあるデータへのアクセス（例えば、読み取り、開放）を拒絶することにより、これらの制限を実施する。

【００５６】

又、システム１００は、位置情報を使用する他のサービス及びアプリケーションを提供することもできる。例えば、システム１００は、緊急事態に位置情報を使用することができ、この場合、装置はアラーム又はセンサであってもよい。システム１００は、アラーム装置の位置を決定し、そしてアラームに応答する当事者に位置情報を送信する。又、システム１００は、位置情報を使用して、盗まれたユーザ装置１０４を取り戻すこともできる。盗まれたユーザ装置１０４でネットワークにアクセスすると、システム１００は、盗まれた装置の位置を決定し、そして装置を探索しようとしている当事者にその位置情報を送信する。システム１００は、移動ユーザ装置（例えば、１０４ｂ）を追跡することができ、従って、そのユーザ装置に関連した何か（例えば、ユーザ、ファイル、物理的オブジェクト、等）も追跡することができる。システム１００は、位置情報の使用により、これら及び他のサービス及びアプリケーションを提供することができる。以下のセクションは、上記で概略的に述べた装置及び技術の詳細な例を示す。

【００５７】

２．０　装置位置決めの概要（図１、２及び３）

装置の位置を決定する際に、システム１００は、多数のメカニズム／技術の１つ以上を使用して、システム１００により位置情報を照合し信頼を置けるようにすることができる。これらメカニズムの１つの一般的な特徴は、インフラストラクチャー１０１の外部の装置がある位置にあることを宣言した場合でも、インフラストラクチャー１０１内の装置又はアプリケーションがそれら外部の装置を必ずしも信頼しないことである。即ち、装置の位置の決定は、装置自体により供給されるのではなく、ネットワークインフラストラクチャー１０１を使用してシステム１００により直接得られた情報に基づくのが好ましい。システム１００は、ネットワークと通信する装置の位置を決定するときに使用すべき情報を得るために種々の解決策を使用し、ケーブルベース又はワイヤレス伝送媒体には幾つかの特定の解決策を適用することができる。

【００５８】

一般的な概要において、ワイヤレス装置（例えば、ワイヤレス伝送媒体を経て通信する装置）の場合に、システム１００は、ネットワークインフラストラクチャー１０１の通常多数の装置（例えば、１２０ａ及び１２０ｂ）とワイヤレスユーザ装置（例えば、１０４ｂ）との間のワイヤレス通信の特性に基づいて装置を位置決めするのに使用される情報を維持する。一般に、この解決策は、三角測量と称され、これは、ワイヤレス装置の位置に基づく信号の時間遅延、信号強度及び方向性の変化に基づくものを含むと共に、分析又はモデルに基づく解決策や、種々の位置における送信及び伝播特性の以前の測定及び記録に基づく解決策を含む種々の全てのリモート位置決定及び近似を包含することが理解される。

【００５９】

ケーブルを経て接続される装置の場合に、システム１００は、ケーブル接続ポイントの位置を特徴付ける情報を、例えば、位置モジュール１８５に記憶された位置データベース

に維持する。このようなデータベースは、種々のやり方でポピュレーションされ、維持される。例えば、ネットワークインフラストラクチャー１０１が物理的に配置されると、全てのケーブル接続ポイントの調査を行なって、ネットワークインフラストラクチャー１０１における各ケーブル接続ポイント１６０及びその対応接続ポートに対応する物理的位置を記録することができる。次いで、装置又はネットワークインフラストラクチャーが、装置が接続されたケーブル接続ポイント１６０を識別するときに、システム１００は、位置データベースを使用して、その識別された接続ポイントに対応する位置を決定する。接続ポイントは、独特の接続ポイントＩＤを使用して識別される。接続ポイントＩＤの値は、例えば、数字、テキストストリング、又はインフラストラクチャー関連情報の組合せでよい。

【００６０】

これら技術の１つを使用して装置の位置を決定した後に、一例では、システム１００が、位置情報を位置モジュール１８５ａの位置データベースにおいて位置サーバー１３４に集中式に維持する。ワイヤレス装置の場合には、システム１００は、装置が移動するときに位置データベースに記憶された装置の位置を動的に変更する。システム１００は、ユーザ装置自体を追跡することができ、及び／又はワイヤレスユーザ装置が通信するときに経るところの最も近いネットワークエントリー装置（例えば、１１４）を追跡することができる。装置がケーブルを経て通信する状態では、システム１００は、装置があるケーブル接続ポイント（例えば、壁ジャック）から別のケーブル接続ポイントへ移動する場合及びそのときに、位置データベースを更新する。装置は、オープンシステムズインターコネクション（ＯＳＩ）通信モデルの第２層（データリンク層）又は第３層（ネットワーク層）を使用するプロトコルを用いて位置情報を互いに通信する。例えば、装置は、ＩＰバージョン４を使用して互いに通信する。他の層及びプロトコルを使用することもできる。装置を位置決めする付加的な及び別のメカニズムは、別のセクションで以下に説明する。

【００６１】

２．１　接続ポイントの位置を決定する技術（図１）

接続ポイントの位置を決定し、従って、これら接続ポイントを利用する装置の位置を決定する更に詳細なメカニズム／技術の例を以下に述べる。種々のメカニズムの詳細な説明は、ワイヤレス接続（即ちワイヤレス伝送媒体を使用する接続）に最も適用できるメカニズム、及びケーブル接続（即ちケーブルベースの伝送媒体を使用する接続）に最も適用できるメカニズムに分割されるが、一般に、これらのメカニズムは、両形式の接続に適用されてもよい。これらのメカニズムを他の形式の接続に適用できるときの例もある（例えば、ケーブル接続に対するメカニズムをワイヤレス接続に適用することもできる）。

【００６２】

２．１．１　ワイヤレス接続（図１）

上述したワイヤレス接続に対する幾つかの詳細な技術を参照すれば、これらの技術を説明するために選択されたワイヤレス通信の２つの例示的形式は、高周波によるもの又は赤外線周波数によるものである。システム１００は、これら通信形式の各々に対して異なるメカニズムを使用することができる。システム１００は、高周波により通信する装置（例えば、１０４、１１４）の位置を識別するためのメカニズム／技術の第１グループを使用することができる。例えば、システム１００は、図１に示すように、１１４ａ及び１１４ｂのようなネットワークエントリー装置１１４に各々関連した１２０ａ－ｂのような１つ以上のワイヤレスアクセスポイントを使用して装置の位置を三角測量する。別の例として、システム１００は、エントリー装置への接近度に基づいて装置の位置を決定する。ワイヤレス装置の位置を決定するためにシステム１００が使用できる種々の技術のリストを以下に示す。

【００６３】

システム１００は、信号強度、到着角度、及び相対的時間遅延解決策の使用を含む多数の既知の三角測量技術を使用することができる。システム１００は、例えば、データ交換に使用される周波数と交番する周波数において短い時間周期中に周波数ホップしてステー

ションを検出することによるオフ周波数サーチを使用することができる。例えば、ワイヤレスアクセスポイント１２０ａは、第１周波数ｆ１において動作することができる。ワイヤレスアクセスポイント１２０ｂは、第２周波数ｆ２において動作することもできる。周期的に且つ比較的短い時間中に、ワイヤレスアクセスポイント１２０ａが第２周波数ｆ２で動作し、ワイヤレスアクセスポイント１２０ｂと通信する装置の信号特性を検出し決定する。同様に、ワイヤレスアクセスポイント１２０ｂも、周期的に且つ比較的短い時間中に、第１周波数ｆ１で動作し、ワイヤレスアクセスポイント１２０ａと通信する装置の信号特性を検出し決定する。システム１００は、ローブベースの三角測量のために整相アレーサーチを使用することができる。即ち、ネットワークエントリー装置の無線アンテナは、サーチビーコンとしてローブの位置を最大又は少なくとも最適にするように向けられる。このようなローブ形成又はローブ操向は、ネットワークエントリー装置１１４が広いスイープを行なって、ある状態において充分なおおよその位置情報を得る段階的プロセスであってもよい。ネットワークエントリー装置１１４は、必要であれば、狭いローブでスイープを微調整して、より正確な位置を得ることができる。又、システム１００は、オフ周波数条件（例えば、周波数ホッピングと方向性サーチの組合せ）において整相アレーアンテナサーチを行うこともできる。

【００６４】

システム１００は、信号強度減衰の関数として既知のアクセスポイント（例えば、１２０ａ－ｂ）からの距離を近似する計算を実行することができる（例えば、信号が強度ｘであり、従って、装置はｙ－ｚフィート離れた範囲に配置されねばならない）。計算に加えて、システム１００は、信号特性及びそれに対応する位置の記憶された関連性をサーチすることもできる。この情報は、信号特性データベースに記憶することができる。ネットワークアドミニストレータは、異なる位置において規定の信号特性を測定し、そしてその測定された特性を位置ごとに記憶することによりこの信号特性データベースを発生する。ユーザ装置の位置を後で決定するときには、システム１００は、ある位置に等しく対応する信号特性を検出した場合に、ユーザ装置がその対応する位置にあると決定する。信号特性が同一でない場合には、システム１００は、データベース内の多数のエントリーを使用して、記憶された信号特性及び位置関連性に基づいてユーザ装置の位置情報を外挿することができる。この技術は、時々、ＲＦトレーニングと称される。

【００６５】

多数の周波数及び／又は接続ポイント及び／又はアンテナを使用すると、位置導出技術の精度を改善することができる。例えば、同じアクセスポイントが異なる周波数で使用された場合に、システム１００は、それら異なる周波数間の位置情報のエラーを使用して位置をより正確に推定することができる。更に、多数のアクセスポイントを使用すると（例えば、１２０ａで受信されたユーザ装置１０４ｂからの信号を、１２０ｂで受信された信号と比較して使用すると）、ある形式の三角測量又は信号強度インジケータの平均化において相対的位置精度を改善することができる。システム１００は、その目的に対して多数のアンテナを使用することができる。又、多数のアンテナ（図示せず）を使用して、ベアリングのラインを主張することもできる。この場合に、アンテナの相対的分離及び既知の間隔の精度の両方が位置精度の改善を与えることができる。又、システム１００は、超ワイドバンドの波を使用して、１つ以上の装置の相対的な位置を決定することもできる。これらの改良された技術を使用することにより位置導出の精度が高まるので、システム１００は、その位置に関連した信頼性パラメータのレベルに対して高い値を指定することができる。

【００６６】

又、システム１００は、ネットワークエントリー装置１１４ａ及び１１４ｂからの信号振幅の差を使用して、ネットワーク装置１１４ａ又は１１４ｂのアンテナに対するユーザ装置１０４ｂの相対的な位置を決定することもできる。システム１００は、信号振幅の差を使用するような技術を、上述した位相差技術と結合して、位置を決定することができる。ここに述べる位置技術は、特定形式のアンテナ技術に限定されない。システム１００は

、ワイヤレスアクセスポイント１２０に関連したアンテナ、或いは受信データから相対的位置を計算するのに使用されるネットワーク関連装置へ情報を中継するように設計されたパーソナルデジタルアシスタント又はラップトップコンピュータを含む（これらに限定されない）スタンドアローン装置に関連したアンテナを使用することができる。１つ以上のアンテナを、１つ以上のワイヤレスアクセスポイント１２０に配備することができる。又、システム１００は、ワイヤレスアクセスポイント１２０の送信強度を変更及び制限して、システム１００がその制限された送信強度による動作半径に基づいて相対的位置の半径を決定及び制御できるようにする。この相対的位置は、動作半径内の壁や立ち入れない場所のような他の物理的バリアにより動作半径から更に制限することができる。

【００６７】

又、システム１００は、赤外光線波及びレーザのような光学技術により通信するワイヤレス装置（例えば、１０４、１１４）の位置を識別するためのメカニズムの第２グループも使用することができる。より詳細には、赤外線送信器及び受信器を使用すると、前記制限された送信強度と同様に、ネットワークエントリー装置１１４ａ又は１１４ｂからユーザ装置１０４ｂが離れ得る実際の距離を制限することができる。従って、システム１００は、その最大距離限界をネットワークエントリー装置１１４ａ又は１１４ｂからの半径方向境界として使用してユーザ装置１０４ｂの相対的位置を決定する。更に、赤外線に対する視線要求は、境界を更に制限できるが、反射装置を使用してこのような制限を変更することもできる。上述したように、システム１００は、壁のような物理的バリアを使用して、赤外線装置の許容位置の決定された境界を制限することができる。

【００６８】

システム１００は、上述した技術を無線及び赤外線通信に使用してワイヤレス装置の位置を決定する。以下に詳細に述べるように、システム１００は、前記技術を使用して、ワイヤレスユーザ装置１０４ｂそれ自体の絶対的位置を決定してもよいし、或いは前記技術を使用して、ワイヤレスユーザ装置１０４ｂがワイヤレスアクセスポイント１２０ａ又は１２０ｂに接近しているかどうか決定すると共に、送信器強度及び物理的バリアのような他の既知のパラメータを使用して、相対的位置を決定してもよい。前記技術を使用してシステム１００により（例えば、アクセスポイント１２０ａ及び１２０ｂを経て）収集された位置情報は、その情報を収集するネットワーク制御装置（例えば、アクセスポイント１２０ａ及び１２０ｂ）が信頼できるものであれば、信頼性のある情報と考えてもよい。これら装置は、例えば、それがインフラストラクチャー１０１の一部分であり、且つ許可されたネットワークアドミニストレータ以外の者によりアクセス、移動及び／又は変更できない場合に、信頼できるとみなされる。ワイヤレス装置から位置を受信しそしてその受信した情報の精度に依存するのではなく、システム１００は、前記技術の１つ以上を使用して装置自体の位置を照合する。信頼できる装置（例えば、変更できないインフラストラクチャー１０１内の装置）により認証されたユーザに対する位置情報を決定すると、システム１００は、その位置情報に、信頼性レベルとして高い値を指定することができると共に、以下に詳細に述べるように、システム１００への許可されたアクセスに著しいセキュリティを与えることができる。

【００６９】

２．１．２　ケーブル接続（図１）

ケーブル接続を使用して装置の位置を決定するための幾つかの詳細な技術／メカニズムを参照すれば、システム１００は、位置データベースに予め記憶された接続ポイントの位置をサーチすることができ、及び／又はシステム１００は、ケーブルベースの伝送媒体を通る信号伝播の特性を使用することができる。一例において、システム１００は、位置データベースをサーチして、装置が接続された接続ポイントの位置を見出す。データベースは、位置サーバー１３４の位置モジュール１８５に配置される。以下に述べるように、システム１００は、各接続ポイント１６０に独特の識別子を指定する。装置がシステム１００に接続すると、システム１００は、その装置が接続されたケーブル接続ポイントの独特の識別子を決定する。そして無１００は、位置データベースをサーチしてその独特の識別

子で接続ポイントを見出し、そしてその接続ポイントに対応する位置を使用する。この技術を使用するために、位置データベースは、ケーブル接続ポイントが設置されたとき及び／又は接続ポイントが最初に使用されるときにポピュレートされる。

【００７０】

データベースを発生するためのプロセスは、手動でもよく及び／又は自動化されてもよい。手動プロセスの例では、ネットワークアドミニストレータが各接続ポイント及びそれに対応する位置に対する独特の識別子を位置データベースに入力する。例えば、ネットワークアドミニストレータは、マップ（例えば、フロアプラン、オフィスレイアウト等）を使用して、各設置された接続ポイントの位置情報を決定する。マップから得られて位置データベースに入力される位置情報は、接続ポイントの座標（例えば、緯度４２°、経度４８°）、接続ポイントのストリング記述（例えば、部屋１０、一階、ビル１）、等々を含むことができる。

【００７１】

自動化プロセスの例では、システム１００は、それ自身の位置決定システム（例えば、ＧＰＳ）をもつユーザ装置１０４を使用して、このユーザ装置１０４が各接続ポイント１６０に接続されたときに位置情報をシステム１００に与えるようにする。システム１００は、信頼性のあるユーザ装置（例えば、偽位置情報を与える確率がない／低いユーザ装置、又は常にネットワークアドミニストレータの制御下にあるユーザ装置）を使用するか、又は信頼性のないユーザ装置（例えば、ネットワークアドミニストレータの制御下にないユーザ装置）を使用することができる。

【００７２】

信頼性のないユーザ装置では、システム１００は、その信頼性のない装置から受信した位置情報を独立して照合するように試みることができる。例えば、その信頼性のない装置がケーブルベース及びワイヤレスの両伝送媒体を使用できる場合には（例えば、ネットワークカード、及びワイヤレス送信器又は赤外線ポートを伴うラップトップ）、システム１００は、前記ワイヤレス技術の１つ以上を使用して、その装置がケーブル接続ポイントを用いて通信する間に装置の位置を照合することができる。又、システム１００は、以下の信号特性技術の１つ以上を使用して、その装置がケーブル接続ポイントを用いて通信する間に装置の位置を照合することもできる。

【００７３】

それ自身の位置決定システムを伴う信頼性のあるユーザ装置では、システム１００は、その信頼性のあるユーザ装置が接続された接続ポイントを決定し、そしてその信頼性のあるユーザ装置で決定された位置を受け取ると、接続ポイント及びそれに対応する位置の関連性を位置データベースに追加する。信頼性のあるユーザ装置が付加的な接続ポイントに接続すると、システム１００は、全ての接続ポイントがその対応位置を有するまで位置データベースを更にポピュレーションする。関連性において、システム１００は、独特の識別子を使用して、接続ポイントの各々を識別することができる。

【００７４】

自動化プロセスの別の例では、システム１００は、ＧＰＳデータが存在しないところで機能し得るそれ自身の位置決定システムをもつ信頼性のあるユーザ装置１０４を使用する。システム１００は、規格に基づくＬＡＮ接続能力をもつユーザ装置を使用する。このユーザ装置は、ＧＰＳにより絶対三次元位置を決定することができると共に、おそらくは慣性ナビゲーションシステムにより、ＧＰＳデータが存在しないところでその絶対位置を決定する能力も有する。慣性ナビゲーションシステムが好ましいのは、ＧＰＳが衛星からの非常に低電力の送信を使用し、開発が激しい地域では屋内又は屋外の受信でも不充分であり又は受信できないことがあるためである。システム１００は、これが慣性ベースのシステムにスタート又は基準位置を与える場合に、外部の情報をもたずに非常に正確な三次元位置データを維持することができる。スタート位置に加えて、システム１００は、その位置情報が信頼できるものであることを確保するためにセキュリティ機能をユーザ装置に与えることができる。これは、例えば、キー及びレーザ技術を含むことができる。ユーザ装

置は、絶対位置情報を計算し、そしてその情報を、ＬＡＮを経、そのＬＡＮインターフェイスを経てＩＰ搬送するようにフォーマットする能力を有する。オペレータは、ＬＡＮへのアクセスを与えるポートへ行き、信頼性のあるユーザ装置をそのポートに接続し、そしてユーザ装置により導出された現在位置情報を位置サーバー１３４の位置データベースへ送信するよう指令することができる。この情報を受信すると、システム１００は、その接続ポイントに対する位置データベースにおける位置情報を更新する。

【００７５】

別の例では、別のセクションに詳細に述べるように、信頼性のある第三者が、接続ポイント１６０ａの位置を与えるエージェントとして働くことができる。例えば、接続ポイント１６０がユーザの家庭の電話ジャックである場合には、それに対応する電話番号を接続ポイントＩＤとして使用することができる。電話会社は、信頼性のあるエージェントとして働いて、その接続ポイントの位置（例えば、住所）を与えることができる。システム１００は、以下に述べるように、ソースの信頼度に基づきその位置情報に関連した信頼パラメータのレベルに値を指定する。システム１００が、例えば、電話会社である第三者エージェントを信頼すればするほど、システム１００は、より高い信頼性レベルをその与えられた位置情報に関連させる。

【００７６】

規定のデータベースとは別に又はそれに加えて、システム１００は、ケーブルベースの伝送媒体を通る信号伝播の特性を使用して、装置の位置を決定することができる。より詳細には、システム１００は、ケーブルベースの伝送媒体の長さと共に変化する信号の特性（例えば、時間遅延、時間ドメイン反射測定（ＴＤＲ）技術、信号減衰、ラウンドトリップ遅延等）を使用して、信号が進行するときに通るケーブルの長さを決定することができる。ある接続ポイントに対して、システム１００は、特定の信号特性を測定し、そしてその測定に基づいて、システム１００は、ケーブルの長さを決定する。ワイヤレス接続について上述したように、システム１００は、ルックアップテーブル、データベース、及び／又は特性測定をケーブル接続に対する位置に関連付けるファンクションも使用する。信号特性のデータ（例えば、ケーブルベースの媒体に対するラウンドトリップトレーニング）は、上述したように、信頼性のあるＧＰＳで接続ポイント１６０がマップされるのと同時に実行されて、位置が推定遅延だけに基づかないようにすることができる。

【００７７】

例えば、信号特性データベースは、測定された信号時間遅延がネットワークエントリー装置１１４ａからの特定のケーブル長さに対応するところの関連性を含む。システム１００は、インフラストラクチャーに含まれたケーブル１１２の長さを考慮する（例えば、差し引く）ことにより、その決定されたケーブル長さを接続ポイント１６０ａからの最大距離として使用して、ユーザ装置１０４ａの相対的な位置を決定する。更に、上述したように、システム１００は、ケーブル管路及び壁のような物理的なバリアを使用して、ユーザ装置１０４ａの許容位置の決定された境界を制限することができる。この技術は、長いケーブル長さを使用して、ひいては、接続ポイント１６０ａから実質的な距離だけ離れたところ（例えば、異なる部屋、及びおそらく非許可の部屋）にユーザ装置１０４ａを配置するのを許すようにして、ユーザ装置１０４ａが接続ポイント１６０ａに接続されたかどうか決定する際に有用である。例えば、システム１００は、上述した信号特性を使用して、ユーザ装置１０４ａとネットワークエントリー装置１１４ａとの間のケーブルが１０フィートであると決定する。システム１００は、接続ポイント１６０ａから１１４ａまでのケーブル長さが７フィートで、固定である（即ち、壁を通して延び、変更できない）という情報を有する。この結合情報を使用して、システム１００は、接続ポイント１６０ａからユーザ装置１０４ａまでのケーブルの長さが３フィートであり、従って、ユーザ装置１０４ａは、接続ポイント１６０ａが配置された部屋に拘束されることを決定する。

【００７８】

又、信号特性を使用すると、システム１００は、多数の接続ポイント（例えば、１０４ｉ及び１０４ｊ、図８）をもつケーブルに対してユーザ装置１０４がどの接続ポイントに

接続されたか決定することもできる。例えば、システム１００は、計算されたケーブル長さを使用して、ケーブル長さの範囲内でユーザ装置がどの接続ポイントにあるか決定することができる。接続ポイントが識別されると、システム１００は、位置データベースによりその位置を得て、ユーザ装置１０４の位置を決定することができる。システム１００がケーブル長さの範囲内で多数の接続ポイントを識別する場合もある。ある場合には、これでも、以下に詳細に述べるように、位置を認証するのに充分である。例えば、ケーブル長さは、ユーザ装置が２階の会議室１－５において接続ポイントの１つに接続されたことを指示できる。しかしながら、全ての会議室は、要求されたネットワークリソースに対して許可された位置であり、従って、この粒度及び精度は、この場合の認証として受け入れられる。

【００７９】

２．２　位置情報データベース（図１）

ワイヤレス及びケーブルベースの両伝送媒体について上述したように、システム１００は、該システム１００の接続ポイント（例えば、１６０ａ－ｉ）に関連した位置情報を位置データベースに維持して更新する。位置データベースに含まれた情報は、変化し得る。例えば、テーブル１は、位置データベースに含ませることのできる情報の形式を含むテーブルである。テーブル１に示すように、各行は、接続ポイントとそれに対応する位置との間の関連性を１つ以上のフォーマットで表わしている。「接続ポイントＩＤ」列は、特定の接続ポイントに関連した独特の識別子を含む。接続ポイントＩＤは、接続ポイントを独特に識別するいかなるＩＤでもよい。以下に詳細に説明されそしてテーブル１に示されたように、一例において、装置「媒体アクセス制御（ＭＡＣ）」アドレス（例えば、０００００１ｄ０００００１）及び装置内のポートＭＡＣアドレス（例えば、０００００１ｄ０００１０１）の組合せは、接続ポイントＩＤを決定する。テーブル１に含まれた位置は、各接続ポイントＩＤに対して２つのフォーマット形式で含まれる。第１の形式は、アメリカンナショナルスタンダードインスティテュート（ＡＮＳＩ）の位置識別番号（ＬＩＮ）であり、そして第２の形式は、緯度及び経度の座標である。（システム１００に使用できる幾つかの付加的なフォーマット例を以下の別のセクションで説明する。）

【００８０】

テーブル１の位置情報は、更に、任意のパラメータ「信頼性レベル」及び「装置ＩＤ」を含む。信頼性レベルは、以下で詳細に説明するように、規定範囲の値をもつパラメータであり、この範囲は、位置基準の信頼度を表わすものである。信頼性レベルは、一般に、接続ポイントの位置を与えるソースの信頼度に対応する。信頼性レベルの値が高いことは、位置基準が正確で、確実で、且つ通常許可されないアクセスを得るために誤って変更されたり発生されたりしない高い信用レベルを表わす。装置ＩＤは、接続ポイントに接続された装置を独特に識別する。装置ＩＤ情報は、システム１００が全てのネットワーク装置（例えば、１０４、１１４、１３６）の物理的位置のマップを記憶できるようにする。これは、システム１００に関連した装置で、それらの位置情報を取得及び／又は記憶するように構成されていない装置がある場合に有益である。システム１００は、この対応する装置情報を使用して、位置サーバー１３４が位置情報を位置認知アプリケーションへ送信することができるようにする。というのは、装置はそれ自体位置情報を送信できないからである。換言すれば、システム１００は、照合された位置情報を要求するアプリケーションに対して第三者の照合者として働くことができる。テーブル１は、装置ＩＤに加えて又はそれとは別に他の情報を含むことができる。例えば、テーブル１は、ＭＡＣアドレス、アドレス、電話番号、プロトコル形式、アセットＩＤ、所有者等を含むことができる。

【００８１】

接続ポイントＩＤ	位置ＩＤ形式	位置基準	位置ＩＤ形式	位置基準	信頼性レベル	装置ＩＤ
00001d000001: 00001d000101:	ANSI LIN	Xxxxxxxxxx1	緯度 経度	ｘ１° ｙ１°	2,256	モデル：ABC Ｓ／Ｎ：123
00001d000001: 00001d000102:	ANSI LIN	xxxxxxxxxx2	緯度 経度	ｘ２° ｙ２°	2,256	GUID: A82C3
00001d000001: 00001d000103:	ANSI LIN	xxxxxxxxxx3	緯度 経度	ｘ３° ｙ３°	2,256	
00001d000001: 00001d000104:	ANSI LIN	xxxxxxxxxx4	緯度 経度	ｘ４° ｙ４°	2,256	
00001d000001: 00001d000105:	ANSI LIN	xxxxxxxxxx5	緯度 経度	ｘ５° ｙ５°	2,256	
00001d000001: 00001d000106:	ANSI LIN	xxxxxxxxxx6	緯度 経度	ｘ６° ｙ６°	2,256	
00001d000001: 00001d000107:	ANSI LIN	xxxxxxxxxx7	緯度 経度	ｘ７° ｙ７°	2,256	
00001d000001: 00001d000108:	ANSI LIN	xxxxxxxxxx8	緯度 経度	ｘ８° ｙ８°	2,256	
00001d000001: 00001d000109:	ANSI LIN	xxxxxxxxxx9	緯度 経度	ｘ９° ｙ９°	2,256	
00001d000001: 00001d000110:	ANSI LIN	xxxxxxxxx10	緯度 経度	ｘ１０° ｙ１０°	2,256	

テーブル１

【００８２】

２．３　装置位置決めの特定例（図１、２、３及び８）

上述したように、位置データベースが確立されると、システム１００は、装置が接続ポイントに接続されたときに装置に位置情報を与えることができる。これは、インフラストラクチャー１０１の外部の装置及びインフラストラクチャー１０１内の装置に位置情報を与えることを含む。図２及び３は、システム１００が装置を位置決めする付加的な例を示す。図２は、システム１００への装置の接続を発見するところからネットワークへの装置アクセスを許すところまでシステム１００が実行するステップを広く示している。図３は、発見された装置の位置を決定するためにシステム１００が実行するステップをより詳細に示している。換言すれば、図３は、図２のステップの一部分をより詳細に示している。

【００８３】

図２は、システム１００への装置の接続を発見するところからネットワークへの装置アクセスを許すところまでシステム１００が実行する一連のステップの例を広く示している。図２の例示的位置識別プロセス２０１を参照すれば、システム１００は、ネットワークの関連付けに向けられた装置又は既にネットワークに関連付けられている装置をアクチベートするか、さもなければ、発見する（ステップ２１０）。システム１００は、位置情報について装置に問合せする（ステップ２１５）。この位置情報は、絶対的形式でも相対的形式でもよい。位置情報が存在しない場合には、システム１００は、装置がそれ自身の位置を識別できるかどうか問合せする（ステップ２２０）。位置情報が存在するか、又は装置が信頼し得る位置を与えることができる場合には、システム１００は、装置の位置情報を確立する（ステップ２３０）。位置は、例えば、システム１００が、規定のスレッシュ

ホールドより高い信頼性レベル値をその位置に対して指定する場合に、信頼できるものとなる。規定のスレッシュホールドは、装置が要求するネットワークリソースに基づいて変化し得る。例えば、要注意の情報やアプリケーションは、公開情報へのアクセスよりも相当に高いスレッシュホールドを必要とする。

【００８４】

装置がそれ自身の位置情報を与えることができないか、又は位置情報が、要求された特定のトランザクションに対してシステム１００に受け入れられる信頼性レベルに関連していない場合には、位置情報は、装置とは独立して、システム１００自体により又は信頼性のある第三者エージェントにより決定される（ステップ２２５）。信頼できる位置を決定した後に（ステップ２２５）、システム１００は、装置の位置情報を確立する（ステップ２３０）。

【００８５】

システム１００が装置からの位置情報を信頼できるかどうか（例えば、充分に高い信頼レベル値を位置に関連付ける）は、その位置情報のソースに依存し得る。例えば、位置情報が、変更を受け難いインフラストラクチャー１０１内の機密装置から到来した場合には、システム１００は、その位置情報を信頼し、そして位置情報に高い信頼レベル値を指定することができる。位置情報がＧＰＳから到来し、及び／又は偽の位置を与える確率レベルが低いことを考慮してセキュリティ機能を伴う第三者の証明で照合された場合には、システム１００は、位置情報を信頼できるが、位置情報がシステム１００自体から到来する場合より信頼レベル値が低い。信頼レベル値の範囲は、以下の制限アクセスセクションで詳細に説明する。

【００８６】

システム１００が装置の位置を決定し（ステップ２２５）、従って、高い信頼レベル値をその位置に指定する１つの例では、装置は、ネットワークエントリー装置（例えば、１１４ａ、１１４ｂ）から接続情報を受け取る。接続情報は、ネットワークエントリー装置が有する情報、例えば、ネットワークエントリー装置の識別子、及び接続ポイントに接続されたネットワークエントリー装置のポート番号を含む。装置は、受信した接続情報又はその一部分をシステム１００へ送信し、より詳細には、位置情報データベースを維持するネットワークの一部分（例えば、位置サーバー１３４）へ送信する。受信した情報（例えば、ネットワークエントリー装置の識別子及びポート番号）を使用して、位置サーバー１３４は、装置が接続された接続ポイントを決定する。一例では、ネットワークエントリー装置の識別子及びポート番号の組み合わせであるその接続ポートの独特の識別子を参照して、位置サーバー１３４は、その接続ポイントに関連した位置を検索する。位置サーバー１３４は、接続ポイントに関連した位置情報を装置へ送信する。

【００８７】

プロセス２０１の説明を続けると、システム１００は、任意であるが、データベースサーチ又はテーブル更新のいずれかにより付加的なパラメータの規定リストを確認する（ステップ２３５）。システム１００は、そのパラメータの規定リストを使用して、以下に述べるようにネットワークアクセスを定義してもよい。パラメータの規定リストは、接続の装置ポート番号、トラフィックアクティビティ及びリンク情報、ＭＡＣアドレス、ＩＰアドレス、タイムスタンプ、及びアクティビティステールネスを含むが、これらに限定されない。パラメータ及び装置位置情報の適当な規定リストが収集されたことがシステム１００で満足されると（ステップ２３５）、システム１００は、ネットワークアクセスを許す（ステップ２４０）。以下に述べるように、位置情報は、ＮＯＳ、ＲＡＤＩＵＳ、ＩＥＥＥ８０２．１Ｘ、ＩＥＥＥ８０２．１Ｑ、ファイアウオール及びＱｏＳメカニズムのように、既存のネットワーク使用制御手段に対する補足として使用されてもよい。更に、システム１００は、ネットワークの使用が、装置及び／又はデータに対する位置制限を含めて、これらメカニズム内に定義されたパラメータによりセットされた境界を越えることがないように確保するために、これらメカニズムに対して連続的に規制する。

【００８８】

一般に、別の一連のステップにおいて、システム１００は、装置の位置を確立すると共に、そして多数の入力の組合せに基づいてその確立した位置の信頼性レベルを確立し、上記入力は、装置自体に含まれた位置情報（例えば、ステップ２１５）、装置により識別された位置情報（例えば、ステップ２２０）、及び装置とは独立して収集された位置情報（例えば、ステップ２２５）を含むが、必ずしも図２に示すシーケンスをたどらない。

【００８９】

更に、図２は、装置の位置を決定すると共にその決定された位置に対して作用する単一の一連のステップを示している。一般に、このプロセス、及び以下に述べる装置位置を決定又は照合することを含む他のプロセスは、装置がネットワークに接続されている間に、攻撃が検出された場合に装置の位置に関する新たな情報がいつ入手できるようになるかを含めて位置の再決定が要求されるネットワークアドミニストレータにとって関心のある多数の理由のいずれかで、周期的に、或いはネットワークポリシーの内部又は外部ネットワーク事象又は他の事柄に基づいて、繰り返されてもよい。プロセスのこの繰り返しは、進行中ポリシー（規制）ファンクションを与える。例えば、このようなポリシーファンクションは、装置が１つの物理的位置で確立できず、その権利が相違する別の物理的位置へ移動するように、使用することができる。

【００９０】

上述したように、装置の位置を決定しそして確認するプロセスは、種々様々な事象で開始されてもよい。これらは、タイマーの時間切れ、通信リンクの切断、通信セッションの終了、ユーザの証明の変更、ファイアウオールアラームのトリガー、新たなネットワーク装置のネットワークへの加入、マネージメントステーションによる促進、装置の特定の移動の検出、シャドー（ネットワークのユーザ又は装置）装置の検出を含むことができるが、これらに限定されない。

【００９１】

図３を参照すれば、例示的プロセス３００は、発見された装置の位置を決定するためにシステム１００が実行するステップを示している。明瞭化及び単なる例示であるために、例示的プロセス３００のある部分は、位置サーバー及び位置クライアントを指す。位置サーバーは、システム１００の装置であって、この装置が位置情報を別のネットワーク装置へ与えることができるようにする位置モジュール１８５のファンクションを含むような装置を指す。これは、位置情報パラメータの記憶、パラメータに対する値を含む記憶装置へのアクセス、装置の位置を決定するアルゴリズム及びプロセス、並びに他の同様のファンクションのためのハードウェア及び／又はソフトウェアアプリケーションを含むことができる。更に、位置サーバーの位置モジュール１８５は、図３の任意のステップに示されたように、ネットワークにアタッチされた装置の位置に基づいて動作コンフィギュレーションパラメータを与えるように更に構成されてもよい。位置クライアントは、位置サーバーが位置を決定するように試みるところの装置を指す。図３のネットワークエントリーは、位置クライアントが通信するときに通るアクセスポートを含む中間装置を表わす。

【００９２】

図１を参照すれば、位置クライアントがユーザ装置１０４ａである例では、図３のネットワークエントリーは、ユーザ装置１０４ａが通信するときに通る接続ポート１１３を有するネットワークエントリー装置１１４ａである。位置クライアントがネットワークエントリー装置１１４ａである例では、図３のネットワークエントリーは、その装置１１４ａが通信するときに通る接続ポート１６５を有するスイッチング装置１３６である。これら２つの例で示すように、ネットワークエントリー装置１１４ａは、位置クライアント及び中間装置の両方として働くことができる。以下の別のセクションで分散型の例では、ネットワークエントリー装置１１４ａは、位置サーバーとして働くこともでき、従って、ネットワークエントリーと図３の位置サーバーとを単一の装置に結合することができる。

【００９３】

プロセス３００を参照すれば、ネットワークエンティティ（例えば、１１４ａ）は、接続情報（例えば、データパケットの形態）を位置クライアント（例えば、１０４ａ）へ送

信し（ステップ３０５）、これは、独特の接続ポイントＩＤの検出を許す。この接続情報は、接続情報が通常接続されるポートを表わすことができる。この接続情報は、多数の異なるプロトコルに適合するフォーマットにすることができる。位置クライアントは、接続情報を受信し（ステップ３１０）、そして接続ポイントＩＤを決定する（ステップ３１５）。例えば、位置クライアントは、例示的パケット形式の１つから接続ポイントＩＤを抽出することができる。

【００９４】

説明上、特定の例では、ＩＥＥＥスパニングツリーブリッジプロトコルデータユニット（ＢＰＤＵ）が使用される。ＩＥＥＥ８０２．１ＤスパニングツリーＢＰＤＵの例では、スパニングツリーがイネーブルされた各スイッチポートがＢＰＤＵを規則的な間隔で転送する（ステップ３０５）。ＢＰＤＵは、次の情報を含む。即ち、（ｉ）送信スイッチの一次ＭＡＣアドレス（ブリッジＩＤ）；（ii）送信ポートの識別子（ＢＰＤＵを送信するスイッチポートのＭＡＣアドレス）；（iii）送信スイッチがルートスイッチであると考えるところのスイッチの独特のブリッジＩＤ、及び（iv）送信ポートからルートまでの経路のコスト。位置クライアントは、ＩＥＥＥスパニングツリーＢＰＤＵを受信し（ステップ３１０）、そして独特のブリッジＩＤ及び送信ポートＩＤをその接続ポイントＩＤとしてデコードする。このデコードされた情報を使用して、位置クライアントは、接続ポイントＩＤ＝｛ブリッジＩＤ　ＭＡＣアドレス｝＋｛送信ポートＩＤ　ＭＡＣアドレス｝であることを決定する（ステップ３１５）。或いは又、位置クライアントは、これらの受信したパラメータを位置サーバーへ転送し、そして位置サーバーは、図２について述べたように、適用可能なパラメータを結合することにより接続ポイントＩＤを発生する。

【００９５】

この解決策は、特定のプロトコルフォーマットに基づいて変更を加えて、他の発見プロトコル及び技術に適用されてもよいことが明らかである。又、システム１００は、他の独特の識別子を使用することもできる。例えば、図８を参照すれば、電話ネットワーク１３２を経てシステム１００’に接続されたユーザ装置１０４ｈの場合に、システム１００’は、電話番号を使用して、ユーザ装置１０４ｈが接続された接続ポイント１６０ｋ（例えば、電話ジャック）を独特に識別することができる。同様に、ユーザ装置１０４ｇは、独特のＩＰアドレスが指定されたケーブルモデムを経てインターネット１４８に接続されたパーソナルコンピュータでよい。システム１００’は、この独特のアドレスを単独で又はＩＳＰ識別子と組合せて使用して、ユーザ装置１０４ｇに関連した接続ポイント１６０ｌ（例えば、ジャック、又はケーブルモデムに対するケーブルの端）を独特に識別することができる。

【００９６】

プロセス３００では、位置クライアントが接続ポイントＩＤを位置サーバーへ送信する（ステップ３２０）。位置サーバーは、接続ポイントＩＤに基づいて位置クライアントに対する位置情報を決定する（ステップ３２５）。この位置情報は、上述したように位置サーバー内の位置データベースにおいて定義することもできるし、或いは上述した技術を使用してネットワークインフラストラクチャー１０１’から発見することもできる。

【００９７】

位置情報を決定した後に（ステップ３２５）、位置サーバーは、位置情報を位置クライアントに送信する（ステップ３３０）。位置クライアントは、そのように構成されていれば、位置情報を将来の基準として記憶する（ステップ３３５）。受信したデータは、位置に加えて、位置情報の発生源に関連した対応する信頼レベル値を含んでもよい。又、位置情報及び付加的な情報は、セキュリティ機能で保護されてもよい。例えば、情報は、位置クライアントが接続された特定の接続ポイントのみに関連した一時的キーで暗号化されてもよい。

【００９８】

位置情報を決定するために（ステップ３２５）、位置サーバーは、接続ポイントＩＤ情報及び地理的情報を含む位置データベースを使用する。進歩型位置サーバーは、装置記憶

部として働くこともでき、装置（例えば、１０４、１１４）の独特の識別子を、前記テーブル１に示すように、それらに対応する接続ポイント及び地理的情報へとマップすることができる。図３に示すように、位置サーバーは、任意であるが、位置情報をネットワークエンティティの記憶モジュールに記憶することができる（ステップ３４０）。別の例では、ネットワークエンティティの記憶モジュール及び位置データベースが同じでよい。従って、トポロジーだけでなく、位置サーバーは、マップされた装置の物理的位置を伴う情報を記憶し及び／又はそれにアクセスする。

【００９９】

プロセス３００を参照すれば、位置クライアントは、規定長さの時間をカウントして（ステップ３２０）、その接続ポイントＩＤ情報を位置サーバーへ周期的に再送信し（ステップ３２０）、位置情報の精度を確保する。位置サーバーは、位置クライアントにより以前に送信された接続ポイントＩＤを参照した後（ステップ３２５）、位置クライアントに位置情報を送信する（ステップ３３０）。この周期的照合は、システム１００が位置情報を周期的に規制する一例である。又、換言すれば、位置クライアントが位置を変更していないことを周期的に照合する。

【０１００】

プロセス３００には、任意のステップ３５０及び３５５も示されており、これは、位置サーバーが位置基準以外の情報を準備し及び又はそれを位置データベースに記憶するように拡張された例を表わす。この例では、位置サーバーは、接続ポイントＩＤに基づくコンフィギュレーション及び／又はプロビジョン（準備）情報を得（ステップ３５０）、そしてこの付加的な情報を位置クライアントに送信する。この付加的な情報を使用して、位置クライアントは、位置に基づくこの付加的なデータに従ってそれ自体を構成することができる（ステップ３５５）。同様に、図示されていないが、ネットワークエンティティがそれ自体を構成することもできる。

【０１０１】

システム１００が位置情報を認証し、そして任意であるが、それらの位置に基づいて装置を構成した後に、システム１００は、インフラストラクチャー１０１のエッジでネットワークを連続的に規制して、位置情報に関するポリシーが実施されるようにする。プロセス３００のステップ３６５、３７０、３７５及び３８０は、システム１００によるエッジポリシーの一例を示す。例えば、位置クライアントが付加的なリソースを要求すると（ステップ３６５）、ネットワークエンティティ（例えば、エッジポリシーの場合には、ネットワークエントリー装置１１４）は、ここに述べる技術のいずれかを使用して、位置クライアントが、依然、認証されたときと同じ位置にいることを照合する（ステップ３７０）。もしそうでなければ、位置クライアントは、新たな位置で認証プロセスを繰り返すように強制される。データの要求に応答して、位置サーバー、又はネットワーク上の別のサーバー及び／又はアプリケーションは、その要求されたデータを、ネットワークエンティティを経て位置クライアントへ送信する（ステップ３６５）。以下に詳細に述べるように、ネットワークエンティティは、データに対して位置制限があるかどうか決定する。もしあれば、ネットワークエンティティは、例えば、位置クライアントが禁止された位置にいる場合に位置クライアントにデータを転送しないことにより、これらの位置制限を実施する（ステップ３８０）。図示されたように、ネットワークエンティティは、到来する要求及び出て行くデータの両方を、位置に基づくポリシーに従って規制する。

【０１０２】

３．０　装置位置を使用したネットワークオペレーション（図４、５、６及び７）

図３の任意のステップに示されたように、システム１００が装置の位置を決定すると、システム１００は、その位置情報を使用して、幾つかの自動オペレーションを与えることができる。換言すれば、位置認識のネットワークは、位置クライアント及び／又は位置データベースに記憶された情報を使用して、位置認識ネットワークのオペレーションを向上させることができる。システム１００は、上述した技術を使用して、装置が接続された接続ポイントを学習することができるので、システム１００は、それらの接続ポイントに関

連した位置に基づいて自動マネージメントを行うことができる。位置情報に基づいて自動マネージメントのためにシステム１００が行なうオペレーション及びサービスは変化し得る。幾つかの技術／メカニズムを以下に詳細に示す。

【０１０３】

３．１　準備及び構成

自動メカニズムの一形式は、装置がシステム１００に追加されたときの装置の準備及び構成（プロビジョニング及びコンフィギュレーション）を含む。追加時に、システム１００は、追加された装置の位置を決定し、次いで、その位置に基づいて、システム１００は、例えば、どんな特定のコンフィギュレーションでファイルを装置にロードしなければならないか、どんな形式のネットワークプライオリティを装置に指定しなければならないか、例えば、帯域巾、レイテンシー、ＱｏＳ、及び他の同様のネットワークポリシーを決定する。このメカニズムにより、システム１００は、各装置の位置に基づいてこれらポリシーのいずれかを実施することができる。以下の例は、システム１００が、準備及び／又は構成データを含むために位置データベース内でデータをいかに拡張できるかを示す。

【０１０４】

３．１．１　拡張された位置データベースを使用する準備／構成例

準備の１つの特定例において、位置サーバーは、位置情報及びネットワーク特有のコンフィギュレーションをボイスオーバーＩＰ（ＶｏＩＰ）ハンドセットに指定する。この情報は、電話において準備されるもので、例えば、バーチャルＬＡＮ（ＶＬＡＮ）ＩＤ、第２層又は第３層におけるトラフィックプライオリティ、並びにＥ９１１　ＬＩＮを含む。これは、例えば、ブランチオフィスでＶｏＩＰ電話における情報を簡単化する。準備パラメータは、位置サーバーの位置データベースにおいて位置情報に追加される。ＶｏＩＰ電話環境に対する拡張位置データベースは、次の情報を含むことができる。ボイスエンティティのＶＬＡＮメンバーシップ、ボイスペイロード／ボイスコントロール／非ボイストラフィックに対する第２層プライオリティマッピング、ボイスペイロード／ボイスコントロール／非ボイストラフィックに対するサービスマーキングの第３層クラス、位置クライアントのネットワーク層アドレス、ＡＮＳＩ　ＬＩＮナンバリング、緯度、経度、高度及び精度ファクタを含む地理的位置情報、ブートすべき装置マイクロコードファイル（例えば、ｂｏｏｔｐサーバーポインタ）、及び／又は他の同様のパラメータ。テーブル２は、ＶｏＩＰネットワークに対する付加的な準備パラメータを含む拡張位置データベースに含むことのできる情報形式の礼を含むテーブルである。接続ポイントＩＤ及び位置基準に加えて、テーブル２に示された位置データベースは、ボイスＶＬＡＮ　ＩＤ及びボイスプライオリティパラメータも含む。上述したように、位置データベースは、位置クライアントに関する装置ＩＤデータを含むこともできる。ＶｏＩＰの例では、これら任意の装置ＩＤパラメータは、ハンドセット拡張番号、ハンドセットモデル番号、ハンドセットバージョン、ハンドセットネットワークアドレス、及び／又はそれと同等のものを含むことができる。

【０１０５】

エントリー	接続ポイントＩＤ	位置ＩＤ形式	位置基準	ボイスＶＬＡＮＩＤ	ボイスプライオリティ	装置ＩＤ（任意）
1	00001d000001: 00001d000101:	ANSI LIN	xxxxxxxxxx1	101	5	拡張:7082 モデル: 123
2	00001d000001: 00001d000102:	ANSI LIN	xxxxxxxxxx2	101	5	
3	00001d000001: 00001d000103:	ANSI LIN	xxxxxxxxxx3	101	5	
4	00001d000001: 00001d000104:	ANSI LIN	xxxxxxxxxx4	101	5	
5	00001d000001: 00001d000105:	ANSI LIN	xxxxxxxxxx5	101	5	
6	00001d000001: 00001d000106:	ANSI LIN	xxxxxxxxxx6	101	5	
7	00001d000001: 00001d000107:	ANSI LIN	xxxxxxxxxx7	101	5	
8	00001d000001: 00001d000108:	ANSI LIN	xxxxxxxxxx8	101	5	
9	00001d000001: 00001d000109:	ANSI LIN	xxxxxxxxxx9	101	5	
10	00001d000001: 00001d000110:	ANSI LIN	xxxxxxxxx10	101	5	

テーブル２

【０１０６】

コンフィギュレーションの１つの特定例において、位置サーバーは、スイッチ及びルーターのような位置クライアントを自動構成することができる。しばしば、ネットワークスイッチは、複雑なコンフィギュレーションをサポートしなければならず、この複雑さが、ネットワークの周りでスイッチを移動させる能力を制限する。システム１００がネットワークスイッチを位置クライアントとすることができる場合には、ネットワークスイッチの構成を自動化することができる。この例では、ネットワークオペレータが配線室に入って、ネットワークスイッチを単に差し込むだけであり、このスイッチは、そのネットワーク層アドレスと、位置サーバーのネットワーク層アドレスしか含んでいない。ネットワークスイッチがパワーアップした後に、例えば、上述したように、ＩＥＥＥスパニングツリーＢＰＤＵを分析することによりその位置を検出し（ステップ３１０（図３））、その接続ポイントＩＤを決定する（ステップ３１５（図３））。ネットワークスイッチがその接続ポイントＩＤを決定すると（ステップ３１５（図３））、ネットワークスイッチは、位置サーバー１３４との会話を開始する（ステップ３２０）。この例では、位置サーバーが、その位置においてネットワークに接続することのあるネットワークスイッチのベースコンフィギュレーションファイルを表わす位置データベースフィールドに対して接続ポイントＩＤを参照する（ステップ３５０（図３））。テーブル３は、ネットワークスイッチを構成するための付加的なコンフィギュレーションパラメータを含む拡張位置データベースに含ませることのできる情報形式の例を含むテーブルである。接続ポイントＩＤ及び位置基準に加えて、テーブル３により表わされた位置データベースは、その対応位置において位置クライアントを構成するのに使用されるべきコンフィギュレーションファイルを識別するコンフィギュレーションファイルパラメータも含む。

【０１０７】

	接続ポイントＩＤ	位置ＩＤ形式	位置基準	構成ファイル
1	00001d000001:00001d000101	緯度－経度	ｘ1°，ｙ1°	closet1.cfg
2	00001d000001:00001d000102	緯度－経度	ｘ2°，ｙ2°	closet2.cfg
3	00001d000001:00001d000103	緯度－経度	ｘ3°，ｙ3°	closet3.cfg
4	00001d000001:00001d000104	緯度－経度	ｘ4°，ｙ4°	closet4.cfg
5	00001d000001:00001d000105	緯度－経度	ｘ5°，ｙ5°	closet1.cfg
6	00001d000001:00001d000106	緯度－経度	ｘ6°，ｙ6°	tftp:/1.1.1.1 /closet15.cfg
7	00001d000001:00001d000107	緯度－経度	ｘ7°，ｙ7°	closet1.cfg
8	00001d000001:00001d000108	緯度－経度	ｘ8°，ｙ8°	http:/2.2.1.1 /closet99.cfg
9	00001d000001:00001d000109	緯度－経度	ｘ9°，ｙ9°	closet1.cfg
10	00001d000001:00001d000110	緯度－経度	ｘ10°，ｙ10°	ftp://3.3.3.3 /closet10.cfg

テーブル３

【０１０８】

３．２　位置に基づく制限（図４、５及び６）

準備及び構成に加えて、システム１００のオペレーションは、位置に基づいて制限することができる。これらの制限は、システム１００のアクセス及び使用に対する制限を含むことができる。又、これらの制限は、システム１００をめぐる及びシステム１００を通るデータの送信も含むことができる。ネットワークアクセスに関する概要例として、ネットワーク内の位置情報は、位置に基づいて認証を行うことができる。位置情報は、システム１００が、ユーザにより与えられた証明に基づくだけでなく、ネットワークにアクセスするためにユーザにより使用される装置の位置にも基づいて、ユーザを認証できるようにする。装置の位置に基づいて、システム１００は、ある装置、情報、アプリケーション、信号交換プライオリティ等へのアクセスを許すか又は制限することができる。更に、装置及び又はそのユーザが、請求された装置位置をシステム１００へ供給する場合でも、システム１００は、ここに述べる技術を使用して、装置とは独立して位置を確認することができる。これは、装置の位置が、信頼性のあるソースから到来し（例えば、信頼性レベルパラメータに対して受け入れられる値を指定する）、そして確実に使用できることを保証する。

【０１０９】

データ制限に関する概要例として、システム１００は、情報を求める装置の位置の関数として又はユーザ及び位置情報の組合せとして、制限されたアクセスに対しネットワークに関連したデータ（例えば、所有権データベース）に１つ以上のパラメータを追加することができる。例えば、システム１００は、ネットワークエントリー装置から要求があったときに又は指定領域以外に位置する中間装置を通して到来するときに会社のビジネス情報へのアクセスを拒絶するようにプログラムされてもよい。又、システム１００は、位置情報を使用して、ファイルにアクセスする装置の位置に基づきファイルの変更を行うこともできる。特に、ファイルは、指定の位置以外からこれをオープンする試みがなされた場合にロックアウト指示子又は破壊指示子を含んでもよい。その一例は、重要な会社ビジネス情報である。認証された装置からこのような情報をアクセスする試みがなされた場合には、その認証された装置が指定の位置又は領域になければ、その情報又はファイルが破壊されることはない。この特徴は、許可されたユーザの所有でない装置に保持されるか又はそれによりアクセスされるファイルのセキュリティを維持する上で価値があることが明らかである。以下の例は、これらの概要例を更に詳細に説明する。

【０１１０】

３．２．１　ネットワークへのアクセスの制限（図４及び５）

概要例で述べたように、位置情報は、システム１００が、ネットワークにアクセスするためにユーザにより使用される装置の位置に基づいて、ユーザを認証しそして制限できるようにする。位置情報は、認証属性として通常の認証システムに追加することができる。ネットワークへのエントリー及びネットワークの使用は、通常、ＭＡＣ識別子に基づいてポートベースのネットワークアクセス制御を与える、ＩＥＴＦリクエスト・フォー・コメント（ＲＦＣ）２１３８及びＩＥＥＥ８０２．１Ｘ規格に説明されたネットワークオペレーティングシステム（ＮＯＳ）、リモート認証ダイヤルインユーザサービス（ＲＡＤＩＵＳ）のような認証システムを使用して調整される。ＮＯＳ及びＲＡＤＩＵＳの場合には、認証サーバー（例えば、１４２（図８））が、このような認証を確立するためのメカニズムを与える。ＩＥＥＥ８０２．１Ｘの場合には、ネットワークエントリー装置１１４は、この規格に詳細に説明されたように、このような認証能力を伴って構成されてもよい。ＩＥＥＥ８０２．１Ｑ規格は、ネットワークのアクセス及び使用を制御するための別の手段を与える。この規格は、ＶＬＡＮの確立及びオペレーションに向けられる。ＩＥＥＥ８０２．１Ｑ規格は、構成されたポートエントリーモジュールにおいてパケットの受信を許すためのネットワーク装置のコンフィギュレーションを定義する。ファイアウオール（例えば、１４０（図８））も、ネットワークの使用を調整する技術を与える。ファイアウオールは、主として、パケットを分析し、その分析から、ネットワークへの又はネットワークからのパケット送信が許されるかどうか決定するように設計されたコンピュータプログラムである。位置を認識することから、システム１００は、装置の物理的位置とこれらネットワークアクセス調整のいずれかとの関連性を、許可されたネットワークアクセスを評価するための属性として結合することができる。例えば、ＶＬＡＮを構成するためにネットワーク装置に分散されるＶＬＡＮポリシーテンプレートは、物理的位置の制約に付随させることができる。

【０１１１】

認証プロセスの一般的な概要において、ユーザ装置１０４は、接続ポイント１６０を経てネットワークインフラストラクチャー１０１に接続する。システム１００は、装置を認証する。システム１００は、装置１０４自体及び／又はインフラストラクチャー１０１から装置１０４の位置を受信する。システム１００は、ユーザ証明を受信し、そしてユーザを認証する。この認証の間に、システム１００は、ここに述べる技術を使用して装置１０４の位置を照合する。ユーザが認証され、そして位置が、要求されたネットワークリソースに対して照合及び認証された場合には、システム１００は、装置１０４がその要求されたリソースにアクセスするのを許すように動作を進める。システム１００は、これら事象の各々を管理使用のためにログすることができる。

【０１１２】

この概念をより詳細に説明するために、以下の例は、認証サーバー（例えば、１４２（図８））の使用を含む。この例では、種々のプロトコル、例えば、ＲＡＤＩＵＳ、ＴＡＣＡＣＳ＋、ダイアメータ、ＳｅｃｕｒｅＩＤ（登録商標）、ＥＡＰ／ＩＥＥＥ８０２．１Ｘ、及び／又はそれと同様のものを使用する認証サーバーは、位置サーバーのファンクションを含む。認証サーバー／位置サーバーは、位置データベースも含む。位置データベースは、ユーザ又はネットワーククライアントがある物理的位置からログインするよう試みるときに、認証サーバーが位置情報を考慮しなければならないかどうか指示する能力をサポートするように拡張される。

【０１１３】

例えば、機密の軍事及びインテリジェンス環境は、その機密位置で入手可能なコンピュータシステムの無断使用からある物理的位置を保護することを要求できる。各コンピュータシステムは、個々のユーザを認証するプロセスの間にコンピュータシステムが使用する位置クライアントを含む。拡張された位置データベースは、例えば、「機密エリア」又は「最小セキュリティレベル」真理値表のような属性を含んでもよい。ユーザが認証を試みると、認証／位置サーバーは、証明を確認するときに認証を要求するユーザの位置を使用する。認証／位置サーバーは、例えば、上述したように接続ポイントＩＤへの参照を使用

してこの情報を導出する。ユーザがその位置から認証するに充分な高いレベルのセキュリティクリアランスを有する場合には、認証プロセスが前進する。ユーザが、その特定位置に関連したセキュリティレベルを満足しない場合には、ネットワークが認証プロセスを停止し、アラームを鳴らし、及び／又は非許可ユーザの位置を報告することができる。

【０１１４】

図４は、位置に基づくネットワークアクセスの制限を適用できるかどうか決定するためにシステム１００が使用する例示的プロセス４０１を詳細に示す。より詳細には、図４に示す例示的位置識別プロセス４０１では、システム１００へのアクセスを求めるユーザは、最初に認証されるか（ステップ４０５）、さもなければ、システム１００によりフィルタされる。システム１００は、位置クライアント装置にいるエンドユーザに、名前及び１つ以上のパスワード（例えば、必要なユーザ証明）（これに限定されないが）を含むあるユーザ情報を供給するよう要求することにより、認証プロセスのこの部分を達成する。それに基づき（例えば、ユーザ名及びパスワードで）システム１００へのアクセスがユーザに許された場合には、システム１００は、ある情報やアプリケーション等へアクセスするためにユーザがシステム１００に問合せする（ステップ４１０）のを許す。それとは別に又はそれに加えて、システム１００は、要求されたアクセスを許す前に装置の位置を受け取る（ステップ４１５）。信頼性のあるユーザ装置（例えば、１０４）、ネットワークインフラストラクチャー装置（例えば、ネットワークエントリー装置１１４）及び／又は位置サーバーは、ここに述べる技術を使用してユーザ装置の位置を供給することができる。

【０１１５】

位置情報を受け取った状態で、システム１００は、クライアント装置の物理的位置が、要求されたネットワークリソースへのアクセスに対して許容及び許可された位置であることを認証する（ステップ４２０）。一例において、システム１００は、クライアント装置の位置を識別できる信頼性のある装置のように、予め承認された位置識別機器を有する装置からの要求されたアクセスを許す。上述したように、これは、システム１００が以前に信頼度（例えば、偽の位置を与えることがない）について評価したクライアント装置に関連したＧＰＳ受信器を含むことができる。又、これは、上述した技術を使用して位置情報を与えることができる認証されたルーター又はスイッチ又は固定布線ＧＰＳ受信器のようなネットワークインフラストラクチャー１０１内の信頼性のある装置も含むことができる。又、信頼性のある装置の生成は、クライアント装置がその信頼性のある装置に対して配置され且つネットワーク又はネットワーク位置リソースが外方に構築された場合には反復ファンクションであってもよい。

【０１１６】

一般に、システム１００は、例えば、図４に示すプロセスを周期的に繰り返すか、或いは新たな情報が入手できるか又は外部事象によりトリガーされたときに繰り返すことにより、進行中ポリシーファンクションを遂行する。

【０１１７】

別の例において、システム１００は、信頼レベルパラメータを使用して、位置情報の信頼度を認証する（ステップ４２０）。信頼レベルパラメータの値は、変化及び成長を考慮するために充分に大きなスケール及びレンジを使用して変更することができる。例えば、１６ビットワードを使用して、システム１００は、２５６から３８４０までのスケールを使用することができ、２５６は、最低の信頼レベルに対応し、そして３８４０は、最高の信頼レベルに対応する。このレンジは、全１６ビットを使用しないので、システム１００が時間と共に開発されるときにレンジの成長に対する余裕を与える。最低の信頼レベルと最高の信頼レベルとの間のいかなるレベルも、信頼度の混合レベルを表わし、システム１００は、ユーザが要求するアクセスの形式に基づく混合レベルで位置情報を使用するかどうか決定する（例えば、問合せの結果（ステップ４１０（ステップ４１０））。より重要なアプリケーション及び／又は情報は、３０７２以上の信頼レベルを要求し、一方、一般的なアプリケーション及び／又は情報は、１０２３以上の信頼レベルを要求することがある。システム１００は、ユーザが信頼レベル値に関わらず公開情報にアクセスするのを許

すことができる。換言すれば、位置を認証するために要求される信頼レベル値は、クライアントがアクセスを要求するところのリソースの形式に基づいて変化し得る。

【０１１８】

一例において、システム１００は、位置情報の信頼レベルを、位置情報の発信者に基づいて決定する。位置情報が、公開アクセスを伴わずに且つネットワークアドミニストレータの制御のもとで、インフラストラクチャー１０１内の内部ルート装置から発信され、そして接続ポイントが壁内ジャックであって、壁を破壊せずに変更できない取り付けケーブルを伴う場合には、システム１００は、３８４０の最大信頼レベル値を指定することができる（即ち、この例では、２５６から３８４０のスケールが使用される）。この場合、位置情報が正しくない又は変更される確率は、非常に低いか又は存在しない。上述した技術を使用してユーザ装置の位置を決定するシステム１００内のワイヤレスアクセスポイント（例えば、１２０ｂ）から位置情報が発信される場合には、ワイヤレスアクセスポイント１２０がネットワークのインフラストラクチャー１０１内にあるので、ある程度の信頼性がある。しかしながら、信号操作の可能性も若干あり、従って、システム１００は、位置情報に２２５６の信頼レベル値を指定する。というのは、誤った位置情報である確率が、前記壁内のジャックより比較的高いからである。位置情報が、いたずら防止といわれているシステムを用いてユーザ装置自体から発信されるか、或いは第三者の承認で到来する場合には、システム１００は、これを若干信頼できるが、この場合も、信号を操作するために何を行い得るかが確かでなく、従って、システム１００は、１０２３の信頼レベル値をこれに指定する。位置情報が、ほとんど又は全く安全手段をもたない装置から発信される（例えば、いたずら防止技術をもたない内蔵ＧＰＳを使用して）場合には、システム１００は、位置情報に、信頼レベル値４５６（例えば、全ＧＰＳ信号を若干信頼する）又は２５６（例えば、信号のいたずらを防止するメカニズムがなく、従って、最低値を指定する）を指定することができる。

【０１１９】

図４を参照すれば、システム１００がユーザを認証し（ステップ４０５）、そして装置位置情報を認証すると（ステップ４２０）、システム１００は、アクセス要求を考慮する。システム１００は、ユーザが、要求されたサービスのレベルに対して適切な証明を有するかどうか決定する（ステップ４２５）。これを行なうために、システム１００は、ユーザ証明、位置情報、及び要求されたアクセスの条件（例えば、ある情報データベースに対する要求、あるアプリケーションに対する要求等）を、記憶された位置制限と比較する。システム１００が、特定の要求に対してユーザが認証されたと決定すると（ステップ４２５）、システム１００は、ユーザにより使用される装置が、その要求された情報、アプリケーション等を受信するために承認されるか又は許可された位置にあるかどうか決定する（ステップ４３０）。両方のスレッシュホールド質問（ステップ４２５及びステップ４３０）の答えが肯定である場合には、システム１００は、ユーザが、既知の位置にあるクライアント装置を経て、要求された資料にアクセスするのを許す。いずれかのスレッシュホールド質問（ステップ４２５及びステップ４３０）の答えが否定である場合には、システム１００は、ユーザのアクセスを拒絶し（ステップ４４０）、ネットワークマネージャーに通知することができる。アクセスを拒絶するのに加えて又はそれとは別に、システム１００は、アドミニストレータが当局に通知する等の付加的なアクションをとるための時間を与えるために、要求を発しているクライアントを歓待したり、魅力的なことで引き付けたり、及び／又はその他のやり方でディスエイブルし及び遅延を与えることもできる。別の例では、システム１００は、要求された資料へのアクセスを、装置の位置のみに基づいて行い、そしてユーザ識別情報に基づいて認証する任意のステップ（ステップ４０５及びステップ４２５）は、アクセスのための前条件ではない。上述したように、システム１００は、矢印４４０で示すように、ステップ４１５、４２０、４２５、４３０及び４３５をループすることにより、位置認証を連続的に規制することができる。

【０１２０】

図５は、別の例示的な認証プロセス５００を示す。ここに示すプロセス５００では、シ

ステム１００は、クライアント装置に対する位置情報を得る（ステップ５０５）。この場合に、システム１００は、適切なサービスレベルを決定するのに装置の位置だけを使用する。又、別の例では、システム１００は、位置に加えて、ユーザ証明（例えば、ユーザ名及びパスワード）も使用して、適切なサービスレベルを決定することができる。システム１００は、得られた位置が照合されたかどうか決定する（ステップ５１０）。システム１００は、位置が照合されないと決定すると（ステップ５１０）、規定のポリシーに基づいてアクセスを拒絶するか（ステップ５１５）又はアクセスを制限する（ステップ５１５）（例えば、いかなるアクセスも拒絶するか、或いは位置に関わらず一般大衆に利用できる装置、アプリケーション及びデータのみにアクセスを制限する）。システム１００は、位置が照合されたと決定すると（ステップ５１０）、位置が認証されたかどうか決定する（ステップ５２０）。システム１００は、位置が認証されなかったと決定すると（ステップ５２０）、その主張した位置を受け入れるべきかどうか決定する（ステップ５２５）。システム１００は、その主張した位置を受け入れないと決定すると（ステップ５２５）、規定のポリシーに基づいてアクセスを拒絶／制限する（ステップ５１５）。システム１００は、その主張した位置を受け入れると決定すると（ステップ５２５）、以下に述べるように、規定のポリシーに基づいて選択可能なサービスレベルでアクセスを許す（ステップ５３０）。

【０１２１】

システム１００は、位置が認証されたと決定すると（ステップ５２０）、ユーザ位置が要求レベルで認証されたかどうか決定する（ステップ５３５）。これは、例えば、要求されたアクセスレベルに対して最小の信頼レベルを有することを含む。システム１００は、ユーザ位置が要求レベルで認証されないと決定すると（ステップ５３５）、以下に述べるように、規定のポリシーに基づいて選択可能なサービスレベルでアクセスを許す（ステップ５３０）。システム１００は、ユーザ位置が要求レベルで認証されたと決定すると（ステップ５３５）、その認証されたレベルでアクセスを許す（ステップ５４０）。

【０１２２】

プロセス５００に関連して説明したように、システム１００は、位置情報に基づいて、選択可能なサービスレベルで、システム１００へのユーザアクセスを許す（例えば、ステップ５３０）。選択可能なサービスレベルは、例えば、アクセス拒絶；装置位置に関わらず許可されるスレッシュホールドアクセス；信頼性のあるユーザ及び装置位置が照合されたが認証されず、幾つかの制限サービスが許される；一般的な位置照合（例えば、公共のエリア、空港、国、都市、電話エリアコード又は交換）及び幾つかの制限アクセスの許可；照合ＩＳＰ及びユーザ照合；照合ＩＳＰ及びユーザ非照合、幾つかの制限アクセスの許可；以前に認証された位置、時間間隔に基づく再認証要求；認証位置及びユーザ、全ての規定許可を許す；及び再認証要求、を含むが、これらに限定されない。これらレベルの幾つかを組合せて、付加的なサービスレベルを含ませることもできる。例えば、再認証は、トポロジー変化、時間切れ、信頼されないネットワーク装置、位置データベースの変化、ケーブル切断、或いは侵入検出システム及びファイアウオールシステムからのローカル又はリモートトリガーを含む（これらに限定されない）何らかの理由でいつ要求されてもよい。システム１００は、例えば、図３に示したエッジポリシーを使用することにより、このような再認証ポリシーを実施することができる。これらのサービスレベルは、上述した信頼レベルに対応してもよい（例えば、サービスレベルは、位置情報の信頼レベルの最小値に依存する）。

【０１２３】

前記技術を使用すると、システム１００は、ユーザ及び／又はアクセスを求めているユーザに関連した装置の位置に基づいて、データ、アプリケーション、特定ネットワーク装置、データ及びネットワークサービス、ＱｏＳ（サービスクオリティ）レベル、ネットワークツール、ファンクション、ルール、等々へのアクセスを制限することができる。更に、前記技術に対し、システム１００は、位置情報を使用して、アクセス要求の変更を行うことができる。例えば、装置が、本来安全でないと思われる位置（例えば、空港のような

公共の施設）からネットワークアクセスを求めるときには、システム１００は、ユーザがバーチャルプライベートネットワーク（ＶＰＮ）のような改良型接続を開始するように促すこともできるし、或いは非安全エリアにいる間に補足的制限を適用することをユーザに通知することもできる。より一般的には、これは、個々のユーザに対するアクセスルールを、クライアント装置の位置及び／又は位置情報に関連した信頼レベルに基づいて適用してもよいという点でポリシーベースアクセスの拡張とみなすことができる。

【０１２４】

更に、前記技術に対し、システム１００は、位置クライアントが接続された接続ポイントに接続される特定ポートに基づいてネットワークへの制限アクセスを与えることもできる。一例において、システム１００は、位置クライアントにより供給される位置が正しいと仮定するのではなく、前記技術を使用して、その特定ポートに関連した接続ポイントの位置を決定する。位置が確立されて信頼できるようにされるその特定のポートに対して、システム１００は、送信データをエンコードし、その信頼性のある位置に関連したポート及びそのポートだけがそのエンコードされたデータを送信のために受け入れるようにする。ユーザが、意図的であるか偶発的であるかに関わらず、その特定ポートから解離する場合には、再認証を行わねばならない。

【０１２５】

この例では、システム１００は、暗号キープロセスを使用して認証及び再認証を実行する。より詳細には、ユーザ及び位置によりシステム１００が認証したエンドユーザには、暗号キーが与えられ、このキーは、それが供給されたポートにしか作用せず、他のポートには作用しないように設計される。即ち、このキーは、ユーザにより使用される装置が位置を移動する（例えば、接続ポイントを変更する）場合のように、異なるポートを通して得られて使用することはできない。キーは、ひっくり返したり、回転したり、等々をしてもよいことに注意されたい。一例において、ネットワークエントリー装置は、特定キーの知識をもたず、むしろ、ポート番号／論理的ポート番号、及びＭＡＣアドレス、ＩＰアドレス及びそれ自身発生した暗号キーの１つ以上、等々を使用して、送信を許可する。又、システム１００は、送信が正しいユーザから到来したもので（例えば、正しいキーの使用に基づき）、ネットワークエントリー装置（例えば、１１４ａ（図１））の特定のアクセスポート（例えば、１１３（図１））に対して認証された装置（例えば、位置／認証サーバー）により変更されたかどうかしか受信者が決定できないように、データパケットを変更することができる。別の例では、三方キーイングがある。クライアント装置、ネットワークエントリー装置からのポート、及びデータを供給するサーバーは、各々、それ自身の関連キーを有する。このように、サーバーは、例えば、クライアント及び認証されたポートの両方からのデータにおける符牒を照合することにより、クライアントから到来するデータが実際にその関連キーでポートを経て到来することを照合することができる。要約すれば、キーは、認証された位置においてそのユーザを認証するために特に確立されたポートに対して良好であるに過ぎない。このように、システム１００は、その許容位置に対するオリジナル暗号キーを取得した場合でも、エンドユーザの位置が変化したときにポートアクセスを拒絶することにより、ユーザが偽の許容位置を使用してアクセスを得るのを防止できる。

【０１２６】

４．２．１　データの位置の制限（図６）

アクセス制御に加えて、システム１００は、位置情報を使用して、データ送信に関する制限を実施することができる。概略例で述べたように、位置情報は、システム１００が、特定領域以外の位置クライアントから要求を受けたときにある重要な情報へのアクセスを拒絶するか、又は特定領域以外に配置された中間装置を経てデータが送信されるのを禁止することができる。図６は、これらのデータ送信制限を実施するためにシステム１００が使用する例示的プロセス６０１を示す。より詳細には、図６に示す例示的情報タグ付けプロセス６０１において、システム１００は、情報（例えば、ファイル、ドキュメント等の一般的なデータ）へアクセスするためのエンドユーザからの要求を受信する（ステップ６

０５）。これは、上述したように、エンドユーザが充分に認証されるか、さもなければ、ネットワークへのアクセスが許可されたと仮定する。次いで、システム１００は、要求されたデータが位置依存型であるかどうか決定する（ステップ６１０）。即ち、ある定義された境界（例えば、当該装置、部屋、ビル、キャンパス、都市、国等）を越えてデータを移動してはならないかどうか決定する。システム１００は、データが位置依存型でないと決定すると（ステップ６１０）、位置により制限されないデータへのアクセスを許可する（ステップ６１５）。

【０１２７】

システム１００は、データが位置依存型であると決定すると（ステップ６１０）、データにタグ付けする（ステップ６２０）。例えば、データを発生するアプリケーション、及び／又はネットワークを経てデータを搬送するためにデータパケットを発生するサーバーは、データ及び／又はパケットを発生する間にこのタグを追加することができる。一例において、タグは、位置の制限を識別するファイルヘッダを備えている。又、ファイルヘッダは、キーを含むこともできる。ある例では、エンドユーザは、重要なデータにタグを追加して、定義された位置（例えば、家、コーナーオフィス、法廷、病院、健康管理施設等）の外部へ送信できないように要求することができる。タグは、非許可の位置で送信データをオープンするのを拒絶し（ステップ６２０ａ）、又はデータが非許可の位置にあると決定されたときにデータを破壊する（ステップ６２０ｂ）ように構成されてもよい。ファイルヘッダは、それ自体コード化されてもよいし暗号化されてもよい。更に、この特殊なファイルヘッダを削除すると、位置に関わりなく、送信データをオープンすることが拒絶されるか、又はデータが強制的に破壊されるように、データ／ファイルが暗号化されてもよい。

【０１２８】

システム１００内の装置及び／又はデータそれ自体は、データが、許可された位置以外のところにあるかどうか決定する（ステップ６２５）。データが、許可された位置以外にない場合には、システム１００は、データへのアクセスを許可する（ステップ６１５）。データが、許可された位置以外にある場合には、システム１００は、アクセスを拒絶し（ステップ６３０）、及び／又はデータを破壊する（ステップ６３０）。データが、許可された位置以外の位置へと次のホップをルーティングされようとしている場合には、システム１００は、許可された位置以外のところにある装置へデータが送信されるのを禁止する。例えば、システム１００は、図３について述べたように、エッジポリシーを使用することができ、インフラストラクチャー１０１の装置は、データを要求している位置クライアントへデータが転送されるかどうか制御することによりアクセスを規制及び実施する。又、データそれ自体、又はデータにアクセスしようと試みるアプリケーションも、アクセスを実行しそしてその位置が禁止位置である場合にアクセスを禁止する装置の位置を許容信頼レベルと共に得る実行可能な手段を含ませることにより、これらの制限を規制及び実施することができる。

【０１２９】

システム１００は、任意であるが、ユーザが許可されたアクセスエリア以外に位置している場合に、タグ付きデータの破壊又はタグ付きデータへのアクセスの拒絶を防止するための付加的なセキュリティオーバーライド制御をエンドユーザに与えるように構成することもできる。この場合に、システム１００は、データへのアクセスを規制し、そして必ずしもシステムはデータを転送しない。この例では、データが許可された位置以外のところにある場合でも、システム１００は、タグをオーバーライドできるかどうか決定する（ステップ６３５）。タグをオーバーライドできる場合には、システム１００は、データへのアクセスを許可する（ステップ６１５）。この場合に、アクセス（ステップ６１５）は、アクセス制限される。例えば、ユーザは、データを搬送のためにユーザ装置にロードすることが許されるが、ユーザは、ユーザ装置が許可された位置に入るまでデータを読み取ったり又は編集したりすることができない。

【０１３０】

４．３　他のサービスの提供（図７）

位置認識インフラストラクチャーでは、システム１００は、信頼性のある位置情報を使用して、前記サービスに加えて他のサービスを提供することができる。例えば、システム１００は、緊急事態において位置情報を使用することができ、ここでは、装置がアラーム又はセンサである。システム１００は、アラーム装置の位置を決定し、そしてその位置情報を、アラームに応答する当事者に送信する。又、システム１００は、位置情報を使用して、盗まれたユーザ装置１０４を取り戻すこともできる。盗まれたユーザ装置１０４でシステム１００にアクセスするときには、システム１００は、盗まれた装置の位置を決定し、そしてその位置情報を、装置の探索を求めている当事者へ送信する。システム１００は、移動ユーザ装置（例えば、１０４ｂ）を追跡し、従って、そのユーザ装置に関連した何か（例えば、ユーザ、ファイル、物理的オブジェクト等）を追跡することができる。システム１００は、位置情報を使用することにより、これら及び他のサービス及びアプリケーションを提供することができる。以下の例は、システム１００が位置情報をいかに使用して、これら及び他のサービス及びアプリケーションを提供できるかを示す。

【０１３１】

一例において、図７は、位置情報に基づきネットワーク環境においてセキュリティサービスを確立するためのプロセス７００を示す。このプロセス７００では、クライアント装置は、物理的な侵入検出装置、煙検出器、火災警報器、ＥＭＴ装置、ワイヤレスパニックボタン等でよい。これらクライアント装置は、緊急事象を信号するように設計される。或いは又、装置は、故障又は切迫した故障の際に警報を送信するか、或いはそれに接続された装置が故障した場合に警報を送信するように構成されたある種のネットワーク接続装置でもよい。装置が位置モジュール１８５を含む場合には、位置サーバー１３４は、その装置の位置情報を与えてその装置自体に記憶することができる。

【０１３２】

一例において、街路の左側にある第５ビルの４階の煙検出器がある事象でトリガーされる（ステップ７０５）。このトリガーされた装置が接続されたシステム１００は、ここに述べた技術を使用して装置の位置を決定するか、又はトリガーされた装置の特定の位置情報を問合せする（ステップ７１０）。システム１００は、その問合せを装置自体へ向けるか、又は位置サーバー１３４へ向ける。システム１００は、位置情報を絶対位置又は相対位置のいずれかとして受け取る（ステップ７１５）。上述したように、位置情報は、信頼性のあるものでもよいし、ないものでもよい。システム１００は、位置情報を照合して、それを信頼性あるものにすることができ、又はシステム１００が提供する特定のセキュリティサービスに対して要求される信頼レベルを高めることもできる。システム１００は、その詳細な位置情報を適当な当局へ中継し（ステップ７２０）、潜在的に高い応答効率を導くようにする。ネットワーク関連性を有する位置クライアントは、装置の位置情報をその装置のオペレーションにリンクすることにより、更に有効なものとすることができる。

【０１３３】

セキュリティサービスシステム１００の別の例は、重要な装置を盗難から保護することである。例えば、ラップトップコンピュータが盗まれ、その犯人がシステム１００にアクセスしようとする場合に、システム１００は、エンドユーザがネットワークにアクセスしたときに、その位置情報が、そのクライアントから直接得られたものか又は位置サーバー１３４から得られたものか評価する。ネットワークエントリーが求められる場合には、要求を発しているクライアントの位置が取得される。システム１００は、その特定の位置クライアントが盗難にあったと決定できると仮定すれば、その位置情報を適当な当局に供給する。識別された位置に至るに充分な時間を当局に与えるために、システム１００は、要求を発している位置クライアントを歓待したり、魅力的なことで引き付けたり、及び／又はその他のやり方でディスエイブルし及び遅延を与えることもできる。従って、位置認識システム１００は、セキュリティ侵害に関連した正確な位置情報を交換し、潜在的に、その侵害に関連した影響を無効化するための有効な手段として使用することができる。

【０１３４】

更に、位置に基づくシステム１００及びここに述べる技術は、個人、装置、梱包等がネットワークインフラストラクチャー１０１の付近及びそれを通して移動するときに、それらの移動を調整し及び／又は正確に監視するのに使用されてもよい。システム１００と通信する電子装置（例えば、ユーザ装置）は、パス、ラベル、アセットタグ等に適用される。この装置は、例えば、上述した無線ベースの技術のような技術を使用してその位置を追跡できるようにする手段を含む。例えば、保安ファシリティへの全ての訪問者に、訪問者パスが支給される。この訪問者パスは、ファシリティ全体にわたって配置されたネットワークインフラストラクチャー１０１のワイヤレスアクセスポイント（例えば、１２０ｂ（図１））と通信できるトランシーバを備えている。これらのワイヤレスアクセスポイントは、タグ／パス／訪問者がファシリティ全体にわたって移動するときに、ネットワークインフラストラクチャー１０１が前記技術を使用して訪問者の位置を決定するように構成することができる。更に、警備員は、予定の終業時間に訪問者がファシリティ内に留まっているかどうか知ることができる。これは、ファシリティが、センサを伴う個別の追跡システムを維持する必要性を排除する。個別の追跡システムに代わって、ネットワークアクセスに使用される同じデータネットワークインフラストラクチャー１０１を、ネットワークインフラストラクチャー１０１と通信する各装置と位置を関連付けることにより、追跡に使用することができる。

【０１３５】

これらの技術は、ネットワークセキュリティを向上させ、装置セキュリティを向上させ、同様に緊急状態応答性を改善し、そしてネットワークに基づく組織的セキュリティを確立するのに使用できる。当該ネットワーク装置及びネットワーク接続装置の位置情報を、セキュリティ、保護及び応答作用と関連付けることにより、これら及び多数の他の効果が与えられる。又、システム１００は、上述しない位置に基づく他のサービスを提供することもできる。例えば、システム１００は、改善されたネットワークトポロジー発見及びマッピングを、それらの物理的位置に特有の装置マップ表示と共に与えることができる。例えば、システム１００は、位置情報を使用して、装置とそれらの物理的位置を関連付ける正確なマップを作成することができる。又、システム１００は、各装置を手動で個々に照合する必要なく、装置の在庫を位置により与えることもできる。上述したように、位置データベースは、装置ＩＤ情報をそれに対応する位置情報と共に含むように拡張することができる。

【０１３６】

更に、システム１００は、位置情報を使用して、ネットワークルールに従うことをチェックすることができる（例えば、配線設計が不正確で、補足又は変更しなければならない場合）。位置情報は、ＬＡＮマネージャーに対する値でよく、例えば、ケーブルモデム及び電話線終端の位置を知ることに関心のあるケーブルオペレータやインターネットサービスプロバイダー（ＩＳＰ）に対する値でよい。

【０１３７】

又、システム１００は、当該ユーザに、そのユーザの現在位置に基づいて情報を与えることもできる。例えば、移動中のエンドユーザが、ネットワークにダイヤルし、接続装置の位置情報を取得し又は供給するようにさせ、次いで、装置位置の規定の半径内で多数の選択可能な基準を満足するホテルやレストラン等へ向かうようにしてもよい。

【０１３８】

５．０　幾つかの追加例（図８）

図８を参照すれば、システム１００’は、位置認識ネットワークの別の例を与えるもので、業務組織又は他の形式の企業のためのデータ通信ネットワークとして働く企業用ネットワークとして説明する。企業は、位置に依存する態様を含んでもよい種々のポリシーに基づいてネットワークを動作する。例えば、アクセス制御ポリジーは、ネットワークにおいてサービスにアクセスする装置の位置に依存してもよい。種々のコンフィギュレーションにおいて、システム１００’は、第１マイルに対して１つ以上のＬＡＮ、ＭＡＮ、ＷＡＮ、ＰＡＮ及び／又はイーサネット（登録商標。以下同様。）を含み又は使用してもよい

（例えば、ＩＥＥＥ８０２．３ａｈ）。このようなネットワークの他の例では、装置の物理的及び論理的構成が、図１及び８に示すものと異なってもよい。

【０１３９】

システム１００’は、種々の形式の装置を含む。ある装置は、ネットワークエントリー装置１１４ｃ－ｊ、一般に１１４であり、これらは、ユーザ装置１０４ｃ－ｌ、一般に１０４に対してシステム１００’のインフラストラクチャー１０１’へのアクセスを与え、或いはインターネット１４８又は電話ネットワーク１３２のような外部ネットワークへのアクセスを与える。ユーザ装置１０４及び外部ネットワークを除くシステム１００’の部分をネットワークインフラストラクチャー１０１’と称する。このインフラストラクチャー１０１’は、システム１００’内でデータをスイッチング及びルーティングする装置であって、１つ以上の中央スイッチング装置１３６’を含む装置と、システム１００’内でデータへのアクセス及びルーティングをサポートする役割を果たすコンピュータであって、認証サーバー１４２、アプリケーションサーバー１３４’、及びドメインネームサーバー（図示せず）のような他のサーバーを含むコンピュータとを備えている。更に、システム１００’は、ユーザ装置及びネットワークインフラストラクチャー装置の両方の特性を幾つか有するプリンタ１２２及びファックスマシン１２３のような装置も含む。

【０１４０】

ネットワークエントリー装置１１４は、ケーブルベース又はワイヤレスを含む種々の形式の伝送媒体を経てネットワークインフラストラクチャー１０１’へのアクセスを与える。ケーブルベースの伝送媒体は、例えば、１００－ベース－Ｔイーサネットリンクに使用されるねじれ対ワイヤを含むことができる。又、ケーブルベースの伝送媒体は、３つ以上の装置を接続できる共有ケーブルベース伝送媒体でよい。例えば、１０－ベース－２イーサネットに使用される同軸ケーブル、多数の装置間の高周波数（例えば、ＨｏｍｅＰＮＡ）通信に使用される電話ケーブル、及び装置間のデータ通信（例えば、ＨｏｍｅＰｌｕｇ）に使用される電力ラインは、このような共有ケーブルベース伝送媒体を与える。

【０１４１】

エントリー装置１１４は、異なる媒体（例えば、ケーブル及び／又は無線スペクトルの一部分）に各々関連した多数のエントリーポートモジュール（例えば、１１３’及び１１８）を含む。例えば、システム１００’では、ネットワークエントリー装置１１４ｆのエントリーポートモジュール１１３’が、専用のケーブルベースの伝送媒体１１２’によりユーザ装置１０４ｃに接続される。ネットワークエントリー装置１１４ｇのエントリーポートモジュール１１８は、共用ワイヤレス伝送媒体１１９’によりユーザ装置１０４ｄ－ｆに接続される。ネットワークエントリー装置１１４ｄのエントリーポートモジュール１４６は、インターネット１４８及び共有伝送媒体１５２によりユーザ装置１０４ｇに接続される。更に、ネットワークエントリー装置１１４ｅのエントリーポートモジュール１２６、１２８及び１３０は、電話ネットワーク１３２及び共有伝送媒体１５４によりユーザ装置１０４ｈに接続されてもよい。又、ネットワークエントリー装置１１４ｅのエントリーポートモジュール１２６、１２８及び１３０は、セルラー電話（又はＰＣＳ）タワー１７５を使用してユーザ装置１０４ｍに接続されてもよく、このタワーは、ベースステーション１７８を経て電話ネットワーク１３２及び共有伝送媒体１５４に接続される。いずれのネットワークエントリー装置１１４も、異なるポートモジュールにより、共有及び専用の両伝送媒体、並びにケーブルベース及びワイヤレスの伝送媒体に接続されてもよい。

【０１４２】

ネットワークエントリー装置１１４及びエンドユーザ装置１０４は、種々様々な構成にすることができる。例えば、ユーザ装置１０４は、個々のコンピュータ、プリンタ、サーバー、セルラー電話、ラップトップ、ハンドヘルド電子装置、電話、インターネットプロトコル（ＩＰ）構成電話、スイッチ装置等を含むことができる。ネットワークエントリー装置１１４は、例えば、スイッチ、ルーター、ハブ、ブリッジ、中継器、ワイヤレスアクセスポイント、データ通信装置、サーバーコンピュータ、モデム、マルチプレクサ、構内交換機（ＰＢＸ）、実質上、データ装置又はエンド装置を相互接続するために使用される

任意の装置、等々を含むことができる。インフラストラクチャー１０１’の個別の境界は、例示のために過ぎない。例えば、システム１００’は、インフラストラクチャー１０１’の論理的な部分を残しながら、図示された境界の外部にサーバーを含んでもよい。別の例では、ネットワークインフラストラクチャー１０１’の一部分が、インターネット１４８のようなリモートネットワークに配置されたシステム１００’に接続されてもよい。

【０１４３】

システム１００’の特定の物理的構成において、各装置（例えば、１０４、１１４）は、接続ポイント（例えば、１６０ｃ、１６０ｄ、１６０ｅ、１６０ｆ及び１６０ｇ、一般に１６０）を有する。接続ポイント１６０は、関連装置がシステム１００’に接続され、従って、その装置の位置に対応する場所である。例えば、ケーブルを経て通信する装置（例えば、１０４ｃ、１０４ｇ、１０４ｈ及び１１４ｇ）については、それらの接続ポイント（例えば、各々、１６０ｏ、１６０ｌ及び１６０ｋ、及び１６０ｎ）は、各装置がネットワークへの接続をなすために物理的にアタッチされるケーブルのターミナル（例えば、壁ジャック）を表わす。例えば、接続ポイント１６０ｏは、ケーブル１１２’のターミナルを表わす。ワイヤレス装置１０４ｆについては、伝送媒体が空気であり、従って、各接続ポイント１６０ｍは、ワイヤレス装置から信号を受信する受信アンテナの位置を表わす。システム１００’の物理的な構成については、各接続ポイント１６０は、システム１００’の残り部分への接続を与えるネットワークインフラストラクチャー１０１’の接続ポートが関連される。例えば、接続ポイント１６０ｏにアタッチされた（媒体１１２’の端において）ユーザ装置１０４ｃは、接続ポイント１１３’に関連付けされる。例えば、媒体１１２’がポート１１３’から切断され、そして同じ装置又は異なる装置の異なるポートに再接続された場合に、システム１００’の物理的構成が変化すると、接続ポイント及び接続ポートの関連性も変化し得ることに注意されたい。上述したように、特に、接続ポイントＩＤを発生するときに接続ポイント及び接続ポートの関連性を維持すると、システム１００’における装置の位置を決定する方法が与えられる。

【０１４４】

５．１　分散型位置データベース

上述した技術／メカニズムの幾つかにおいて、システム１００は、位置サーバーファンクション及び位置データベースを含む集中型位置サーバー１３４を使用する。集中型システムとは別に、システム１００の位置認識部分は、分散型システムとして実施することもできる。分散型システムの例においては、位置サーバーファンクション及び位置データベースがネットワークの装置間に分散される。例示的分散型システムでは、位置モジュール１８５が、例えば、エントリー装置（例えば、１１４）、サーバー（例えば、１４２）、ファイアウオール（例えば、１４０）等を含むネットワークの例示的装置の１つ、一部分又は全部に存在する。図１及び８に示すように、幾つかの装置は、ハードウェアであるか、ファームウェアであるか又はソフトウェアであるかに関わらず、位置モジュール（例えば、１８５ａ－ｏ、一般に１８５）を備え、これは、異なるファンクション、及び位置情報を含む情報部片を有するように構成できる。以下に述べるように、分散型システム例では、ネットワークインフラストラクチャー１０１の内外の装置が、任意であるが、それらのオペレーションに影響する位置従属情報を維持することができる。

【０１４５】

５．１．１　ネットワーク内の分散

図１及び８は、例示のためにのみ装置の一部分において位置モジュール１８５を示している。上述したように、特定のネットワーク装置、或いは特定のネットワーク装置にアタッチされた１つ以上の装置の位置を表わす情報が、位置モジュール１８５にデータベースとして予めロードされてもよい。各装置における位置データベースは、システム１００の全位置データベースでもよいし、又は位置データベースの一部分でもよい。特に、装置の位置モジュール１８５に含まれたデータベースの一部分は、その特定の装置に適用できる位置を伴う一部分である。例えば、特定のネットワークエントリー装置のポートに関連した全ての接続ポイントである。或いは又、位置モジュール１８５は、システム１００への

追加又は削除、及び／又はシステム１００に関連した装置の移動と共に変化する更新可能なテーブルを含んでもよい。位置モジュール１８５は、位置情報を含むことができると共に、ここに述べる詳細なメカニズム／技術の１つ以上を与えるために、情報を測定、計算、推測、サーチ及び／又はその他取得するように構成することができる。又、位置モジュール１８５は、装置の位置情報に基づいて、ネットワークベースのデータ、アプリケーション、ＱｏＳ、ＴｏＳ、帯域巾等へのアクセスの調整（例えば、規制）を行なえるようにするアクセス制御モジュールであるように構成することもできる。例えば、図４に示すように、分散型システムの場合に、位置モジュール１８５は、ネットワークベースの情報、アプリケーション、レートサービス、レート形式等へのアクセスを許すための要求として装置位置を含むように構成される。このような分散型システムでは、各ネットワークエントリー装置（例えば、１１４）は、準認証サーバーとなる。図６に示すように、位置モジュール１８５は、位置依存型の情報／データにタグ付けしそしてそれに応じてそのタグに作用するための手段を含むように構成される。又、各位置モジュール１８５は、上述したセキュリティ、安全性、又は他のサービスを提供する目的で通信装置の位置を識別することもできる。

【０１４６】

分散型の例では、位置サーバーファンクションは、ネットワーク装置、マネージメントステーション、又はサーバー／認証サーバーの一部分でよい。位置サーバーファンクションは、ユーザ装置が通信するときに通るスイッチ又はネットワーク装置（例えば、１１４）内に共通配置されてもよい。分散型システムでは、装置は、位置クライアント及び位置サーバーの両方である各位置モジュール１８５におけるファンクションを含むことができる。遠隔オフィスでは、その遠隔オフィスをホームオフィスに接続するルーターが、例えば、Ｅ９１１アプリケーションに対して位置情報を与えるために必要となる位置サーバーファンクションを含むことができる。企業キャンパスネットワークのような他のアプリケーションでは、位置サーバーファンクションは、ダイナミックホストコンフィギュレーションプロトコル（ＤＨＣＰ）サーバーのような改善型ＩＰアドレスマネージメントシステム及び専用位置支給システムの一部分であってもよい。

【０１４７】

位置サーバーファンクションを含むことのできる幾つかの考えられる装置のリストを以下に示す（これらの装置だけに限定されない）。ネットワークスイッチ、データスイッチ、ルーター、ファイアウオール、ゲートウェイ、ネットワークファイルサーバー又は専用位置サーバーのようなコンピュータ装置、マネージメントステーション、ハイブリッドＰＢＸ及びＶｏＩＰコールマネージャーのようなネットワーク接続ボイスオーバーＩＰ／ボイスオーバーデータシステム、改善型ＤＨＣＰサーバーのようなネットワーク層アドレスコンフィギュレーション／システムコンフィギュレーションサーバー、改善型ブートストラッププロトコル（ｂｏｏｔｐ）サーバー、ＩＰｖ６アドレス自動発見イネーブルルーター、及び半径方向拡張可能認証プロトコル／ＩＥＥＥ８０２．１Ｘ等のようなサービスを提供するネットワークベースの認証サーバー。

【０１４８】

一例において、分散型位置データベースに位置情報を与えるために、システム１００は、シンプルネットワークマネージメントプロトコル（ＳＮＭＰ）を使用する。ネットワークアドミニストレータは、ネットワークケーブルのターミナルの位置情報をＳＮＭＰ ｉｆＤｅｓｃｒ変数において支給する（例えば、ｉｆＤｅｓｃｒは、読み出し専用の属性であるが、多くのシステムは、ネットワークオペレータがポートを「命名」することを許し、これが次いでこのフィールドに表示される）。装置の位置サーバーファンクションは、ＳＮＭＰを経てターミナル情報を読み取る。

【０１４９】

上述したように、位置クライアントは、その地理的位置を学習するように試み、及び／又はそれ自身を、クライアントの位置を知る必要のある別の装置へ識別する。又、進歩型位置クライアントは、位置認識システムから（例えば、コンフィギュレーション情報を付

加的に与えるように構成された位置サーバーから）その動作的コンフィギュレーションを受け取ることもできる。位置クライアントは、ネットワークエレメントと通信し、そしてここに述べる多数の考えられる方法の１つによりその接続ポイントＩＤを発見する。位置クライアントは、その接続ポイントＩＤが分かると、位置サーバーにコンタクトして、その実際の位置を発見することができるか、又はそれ自身を位置サーバーに登録し、これは、位置クライアントの位置の発見を求める他の通信エンティティに対するプロキシーとして働くことができる。又、位置サーバーが、位置クライアントの通信トラフィックを装置の位置情報で変更できる通信システムであることも考えられる。

【０１５０】

位置クライアントを含むことのできる幾つかの考えられる装置（これらに限定されない）のリストを以下に示す。ネットワークスイッチ、ルーター、ファイアウオール、ゲートウェイ、ネットワークファイルサーバー又はエンドユーザコンピュータ装置のようなコンピュータ装置、パーソナルデジタルアシスタント、スマート機器（ネットワークに接続できるトースター、冷蔵庫、又はコーヒーポット）、ハイブリッドＰＢＸ及びＶｏＩＰコールマネージャーのようなネットワーク接続ボイスオーバーＩＰ／ボイスオーバーデータシステム、又はボイスオーバーＩＰ／データハンドセット。

【０１５１】

５．１．２　ネットワーク外の分散

システム１００の装置間に分散されるのに加えて、システム１００は、ネットワークの外部にある信頼性のあるデータベース及び／又は第三者により維持された信頼性のあるデータベースからの位置情報も使用することができる。上述したように、システム１００は、システム１００の外部のデータベースから得られた全ての位置情報に対して信頼性レベルを指定することができる。例えば、独特の接続ポイントＩＤが電話番号である電話ネットワーク例において、位置サーバー１３４における位置サーバーファンクション、又は位置モジュール１８５に分散されたいずれかのファンクションが、ホワイトページ形式のデータベースを参照して、電話番号に対するアドレスを検索することができる。このアドレスが位置認識アプリケーションにより確認された位置フォーマットでない場合には、位置サーバーファンクションが別の第三者データベースを参照して、そのアドレスを、例えば、緯度及び経度座標に変換することができる。更に別の粒度を得ることができる。例えば、自営業の場合に、アドレスは、それに関連した２つの電話番号、即ち営業用電話番号と住居用電話番号を有してもよい。営業用電話番号で識別される接続ポイントの位置は、ホームオフィスとして確立された部屋である。これは、家の１階に配置されて、高度座標も与えることができる。住居用電話番号で識別される接続ポイントの位置は、家族のパーソナルコンピュータを含む部屋である。これは、家の別の階に配置されてもよい。同様に、位置サーバーファンクションは、接続ポイントが、ケーブルモデムに接続されたケーブルエンドポイントであり、且つＩＰアドレスが加入者のアドレスに関連付けされている場合に、アドレス、部屋、及び／又は地理的座標を得ることができる。システム１００は、何らかの入手可能なリソースを使用して、特定の接続ポイントの位置情報を更新し、その第三者ソースの信頼度に基づいて適切な信頼レベルを指定することができる。

【０１５２】

５．２　分散型ネットワークにおける位置アドバタイジングシステムの使用

１つの分散型の例では、システム１００は、位置アドバタイジングシステムを使用して、装置間に情報を通信する。位置アドバタイジングシステムは、通常、第２層又は第３層プロトコル（例えば、隣接部発見プロトコル）を使用して、ネットワークを経て位置クライアント装置へ装置位置情報及び／又はコンフィギュレーションを支給及び／又はアドバタイジングするネットワーク装置を備えている。又、位置アドバタイジングシステムは、ネットワークを経て位置クライアント装置を接続できる装置も備えている。位置アドバタイジングシステム装置の一例は、第２層又は第３層ＬＡＮスイッチとして動作するデータスイッチのような装置である位置アドバタイジングスイッチを含むことができる。位置アドバタイジングシステム装置の別の例は、ネットワークルーターを含む自動コンフィギュ

レーションサーバーとも称される位置アドバタイジングルーターを含むことができる。又、この装置は、遠隔企業オフィスにおけるＬＡＮスイッチ及び／又はワイヤレスアクセスポイントへコンフィギュレーションを与えることのできるブランチオフィスルーターも含むことができる。位置アドバタイジングシステムにおける他の装置は、ワイヤレスＬＡＮアクセスポイント、バーチャルプライベートネットワークシステム、トンネルサーバー、リモートクライアント、ゲートウェイ及び／又はそれと同等のものを含むことができる。位置アドバタイジングシステムとして働く装置は、種々の座標系又は物理的位置のテクスチャー表示に基づいて位置情報を分散してもよい。位置アドバタイジングシステムの装置は、物理的ケーブルを経てそれに物理的に接続された位置クライアントを有する装置であるときは、上記と同様に、物理的ネットワークアクセスポートに対応する接続ポイントのデータベースと、そのポートに接続されたネットワークケーブルのターミナルの対応する理知的位置情報とを含む。分散型システムに関連して説明するが、位置アドバタイジングシステムは、上述した集中型位置サーバーを使用する集中型システムにおいて実施することもできる。

【０１５３】

システム１００は、その位置アドバタイジングシステムにＬＡＮスイッチを使用するときには、位置及びコンフィギュレーション情報を位置クライアント装置に与えるだけでなく、ネットワークポリシーを、位置クライアント装置が接続されたポートへと自動的にマップすることもできる。このポリシーは、位置クライアントが検出されるや否や位置アドバタイジングスイッチに準備されてもよいし、或いは位置クライアントが適切に構成されそして照合された後にのみポリシー準備がイネーブルされてもよい。この特徴は、自己イネーブル型ポリシーと称される。

【０１５４】

位置アドバタイジングシステムがワイヤレスＬＡＮアクセスポイントを含むときには、ネットワークは、位置及びコンフィギュレーション情報を、装置特有の識別、例えば、ＩＥＥＥ　ＭＡＣアドレス、及びワイヤレスネットワークの動作中に与えられるＩＥＥＥ８０２．１１関連性ＩＤへとマップする。ネットワークは、位置座標を関連性ＩＤへとマップする。ワイヤレスネットワークは、クライアント装置の完全な移動性を与えるので、システムは、例えば、上述した技術のような技術を使用して、位置クライアントの座標をいつでも三角測量する。位置データベースは、クライアントの座標を潜在的に非常に頻繁に変更できるので、性質が動的である。

【０１５５】

５．２．１　位置アドバタイジングシステムを使用する特定例

位置アドバタイジングシステムを使用する自動ネットワークマネージメントの一例は、データネットワークにおいて隣接部発見プロトコルを伴うボイスオーバーＩＰハンドセットのコンフィギュレーションである。ボイスオーバーＩＰハンドセットは、通常、イーサネットスイッチと通信するように設計され、複雑なコンフィギュレーションを必要とする。位置アドバタイジングシステムを伴うネットワークは、隣接部発見プロトコルをボイスオーバーＩＰハンドセットと一体化して、コンフィギュレーション情報をハンドセットに与え、接続ポイントスイッチに記憶されるべき在庫情報を発見し、そして接続ポイントスイッチ／アクセスプラットホームにおいてポートパラメータを自動的に構成することができる。

【０１５６】

この例における自動ボイスハンドセットコンフィギュレーションシステムは、ボイスハンドセットに多数のパラメータを与えることができる。例えば、このシステムは、ボイス及び／又はファックスペイロード及び制御トラフィックに対してＶＬＡＮメンバーシップ及び分類ルールを与えることができる。又、このシステムは、非ボイスペイロード及び制御トラフィックに対してもＶＬＡＮメンバーシップ及び分類ルールを与えることができる。又、このシステムは、ボイスペイロード及び制御トラフィックのＩＥＥＥ８０２．１Ｑプライオリティ決めパケットマーキング情報も与えることができる。又、このシステムは

、非ボイスペイロード及び制御トラフィックのＩＥＥＥ８０２．１Ｑプライオリティ決めパケットマーキングも与えることができる。又、このシステムは、ボイスペイロードトラフィックに対してＩＰ形式のサービスフィールドマーキングを与えることもできる。又、このシステムは、ファックスペイロードトラフィックに対してＩＰ形式のサービスフィールドマーキングを与えることもできる。又、このシステムは、ボイス／ファックス制御トラフィックに対してＩＰ形式のサービスフィールドマーキングを与えることもできる。又、このシステムは、ＶｏＩＰ電話に含まれたボイスエンティティに対してインターネットアドレスを与えることもできる。又、このシステムは、ＡＮＳＩ　ＬＩＮ（位置識別番号）も与えることができる。又、このシステムは、ハンドセットの地理的位置を、測地線情報と共に、或いは高度又は相対的位置情報を含む他の地理的座標系と共に、与えることができる。

【０１５７】

この特定例の説明上、ユーザ装置１０４ｃ（図８）がＶｏＩＰハンドセットを表わし、そしてネットワークエンティティ装置１１４ｆがＬＡＮスイッチを表わすものとする。ＬＡＮスイッチ１１４ｆは、位置アドバタイジングシステムのファンクションを、例えば、位置モジュール１８５ｎの一部分として含む。又、ＬＡＮスイッチ１１４ｆは、在庫情報、地理的情報及びコンフィギュレーション情報を含む拡張データベースを位置モジュール１８５に含む。オペレーション中に、ボイスオーバーＩＰハンドセット１０４ｃは、ブートし、そして隣接部発見プロトコルパケットの送出をスタートする。これらのパケットは、ＶｏＩＰハンドセット１０４ｃが接続されたＬＡＮスイッチ１１４ｆをトリガーして、隣接部発見プロトコルパケットの送出をスタートさせる。ＬＡＮスイッチ１１４ｆは、その拡張データベースから得られる次のコンフィギュレーション情報でボイスハンドセット１０４ｃに応答する。ＩＥＥＥ８０２．１Ｑプライオリティマーキングコンフィギュレーション、ＩＥＥＥ８０２．１Ｑ　ＶＬＡＮメンバーシップコンフィギュレーションルール、インターネットプロトコル形式のサービス／区別化サービスマーキングルール、ボイスハンドセット１０４ｃが通常のオペレーションに必要なボイスコールマネージャー／ＩＰ　ＰＢＸ／ＩＰボイススイッチのＩＰアドレス、及びＡＮＳＩ　ＬＩＮ。ＬＡＮスイッチ１１４ｆは、スイッチが接続するポートにおいてポリシーマネージメントコンフィギュレーションをイネーブルする（例えば、自己イネーブル型ポリシー）。ボイスハンドセット１０４ｃは、隣接部発見プロトコルを使用し続けて、その装置特有情報をアドバタイジングし続ける。この装置特有情報は、例えば、モデル番号、装置形式、ＩＰアドレス、装置シリアル番号、ハンドセットにより使用されるマイクロコードバージョン、等を含むことができる。ＬＡＮスイッチ１１４ｆは、ボイスハンドセット１０４ｃにより送信された隣接部発見プロトコルパケットからのこの装置特有情報をデコードし、そしてアドバタイジングされた情報をローカル又はリモートネットワークマネージメントデータベースへ記録する。システム１００’は、この情報を使用して、在庫マネージメント及び装置位置アプリケーションをサポートする。

【０１５８】

位置アドバタイジングシステムを使用する自動ネットワークマネージメントの別の特定例は、配線室スイッチ又はワイヤレスアクセスポイントを構成するためのビヒクルとしてキャンパス又は企業ネットワークにネットワークＬＡＮスイッチを使用することを含む。多くの企業ネットワークでは、ＩＴ組織が、多量の時間と、ネットワークユーザに対して一次ネットワークエントリー装置として働くアクセススイッチ又はワイヤレスＬＡＮアクセスポイントを構成するリソースを消費する。これらのネットワークエントリー装置は、通常、単一コンフィギュレーションで準備されるが、時々、僅かなコンフィギュレーションミスがあると、データネットワークのオペレーションに多数の問題が生じることになる。位置アドバタイジングシステムを伴うネットワークは、ネットワークアドミニストレータが、どこでネットワークに接続されるかに基づいて適切なコンフィギュレーションでバックボーンネットワークがプロビジョンネットワークアクセススイッチ及びルーターを切り換えるときにネットワーク装置の有効性に関して心配することから解放する。

【０１５９】
この特定例の説明上、ネットワークエントリー装置１１４ｆ（図８）は、配線室を表し、又はコンフィギュレーションクライアントとして働くユーザアクセススイッチを表わすものとする。この環境では、ユーザスイッチ１１４ｆは、位置クライアントとして参加するように構成される（例えば、位置モジュール１８５ｎに位置クライアントファンクションを含む）。位置クライアント１１４ｆは、ネットワークエントリー装置１１４ｃ、ネットワークエントリー装置１１４ｇ及び中央スイッチング装置１３６’を経てネットワークインフラストラクチャー１０１’に接続される。これら他の装置（即ち、ネットワークエントリー装置１１４ｃ、ネットワークエントリー装置１１４ｇ及び中央スイッチング装置１３６’）のいずれかが位置アドバタイジングシステムとして働いて、位置、コンフィギュレーション及び他の情報を、この例では位置クライアントであるネットワークエントリー装置１１４ｆへスイッチし、ブロードキャストする。

【０１６０】
その物理的位置を決定するために、装置１１４ｆは、その隣接装置１１４ｃ、１１４ｇ及び１３６’の各々から位置情報を受け取る。装置１１４ｃは、隣接装置１１４ｆが接続ポイント１６０ｕに接続されているので、装置１１４ｃが位置Ｘ１、Ｙ１に配置されて、位置情報を装置１１４ｆへ送信することを決定する。同様に、装置１１４ｇは、隣接装置１１４ｆが接続ポイント１６０ｖに接続されているので、装置１１４ｃが位置Ｘ２、Ｙ２に配置されることを決定し、そして装置１３６’は、隣接装置１１４ｆが接続ポイント１６０ｗに接続されているので、装置１１４ｃが位置Ｘ３、Ｙ３に配置されることを決定する。装置１１４ｃは、その隣接部の各々から座標を受け取り、そしてそれらを互いに比較して、統計学的な信用レベルでその実際の物理的位置を決定する。この信用レベルは、受け取ったデータに基づいて計算された物理的位置に関連付けるために信頼レベルに変換される。例えば、３つの全隣接装置が同じ座標を与える場合には、システム１００’は、その物理的位置に最も高い信頼レベル値を関連付けることができる。

【０１６１】
コンフィギュレーションを決定するために、他の装置（即ち、ネットワークエントリー装置１１４ｃ、ネットワークエントリー装置１１４ｇ及び中央スイッチング装置１３６’）のいかなる組合せも、位置クライアント１１４ｆへコンフィギュレーションパラメータをアドバタイジングする。コンフィギュレーションパラメータは、例えば、次の属性を含むことができる。ユーザアクセススイッチのＩＰアドレス、ユーザアクセススイッチのＩＰサブネットマスク、ユーザアクセススイッチのデフォールトＩＰルート、ＳＮＭＰトラップ行先ＩＰアドレス、ＳＮＭＰリードオンリコミュニティストリング、ＳＮＭＰリードーライトコミュニティストリング、ユーザポートにおけるデフォールトＶＬＡＮ　ＩＤ、ユーザアクセストラフィックに対するデフォールトＩＥＥＥプライオリティマスク、イネーブル又はディスエイブルされたＩＥＥＥ８０２．１Ｄスパニングツリー、ＩＥＥＥ８０２．１Ｗ急速スパニングツリーイネーブル又はディスエイブル、ユーザポートにおけるイネーブルＩＥＥＥ８０２．１Ｘ認証、データセンター／コンフィギュレーションプロビジョンスイッチへのポートにおけるイネーブルＩＥＥＥ８０２．１Ｑ　ＶＬＡＮタグ付け、このポートに接続されたデータケーブルのターミナルの地理的座標、等々。テーブル４は、この位置アドバタイジングシステム例において拡張位置データベースに含ませることのできる幾つかのエントリーの例を示す。この例では、左から最初の５つの列（即ち、地理的位置までのエントリーポート）は、位置クライアントに対して準備された情報を表わす。左から最後の２つの列（即ち、クライアントスイッチＩＰアドレス及びシリアル番号）は、位置クライアントから得られ／学習された情報を表わす。

【０１６２】

エントリーポート	ユーザポートのデフォールトVLAN ID	デフォールトプライオリティ	位置データ受信ポートでのトリガーイネーブル	ケーブルターミナルの地理的位置	クライアントスイッチＩＰアドレス	シリアル番号
1	1024	0	真	緯度X1 経度Y1 高度Z1	1.1.2.1	xxxxxx1
2	1024	0	真	緯度X2 経度Y2 高度Z2	1.1.2.2	xxxxxx2
3	1025	0	真	緯度X3 経度Y3 高度Z3	1.1.3.1	xxxxxx3
4	1026	0	真	緯度X4 経度Y4 高度Z4	1.1.4.1	xxxxxx4

テーブル４

【０１６３】

又、プロビジョンスイッチにおける位置アドバタイジングシステムが、一時的インターネットアドレス及び／又は一体化リソースロケーター（ＵＲＬ）を、ネットワークにアタッチされた位置データベースに与え、そこで、位置クライアントが更に進歩したコンフィギュレーションファイルを検索できるようにすることも考えられる。例えば、前記テーブル３のエントリー６、８及び１０を参照されたい。コンフィギュレーションファイルは、トリビアルファイル転送プロトコル又はインターネットファイル転送プロトコルのような標準メカニズムを経て検索することができる。

【０１６４】

位置アドバタイジングシステムを使用する自動ネットワークマネージメントの別の特定例は、ブランチオフィスにおいてローカル及びワイドエリアルーターに対して基本的スイッチコンフィギュレーションを準備することである。この例では、ネットワークは、ブランチオフィスルーター及び地域オフィスをその位置アドバタイジングシステムの一部分として使用する。以下に述べるオペレーションの一例では、ユーザアクセススイッチは、ブランチオフィスルーターであり、そしてデータセンタースイッチは、地域オフィスルーターである。以下に述べるオペレーションの別の例では、ユーザアクセススイッチは、ブランチオフィスのネットワークエントリー装置であり、そしてデータセンタースイッチは、ブランチオフィスルーターである。

【０１６５】

オペレーションにおいて、ユーザアクセスＬＡＮスイッチがブートし、隣接部発見プロトコルパケットの送出をスタートする。これらパケットは、位置クライアントが接続されたデータセンターＬＡＮスイッチ／位置アドバタイジングスイッチをトリガーし、隣接部発見プロトコルパケットの送信をスタートする。データセンタースイッチ／位置アドバタイジングスイッチは、位置クライアント／ユーザアクセススイッチが接続されたポートに関連したコンフィギュレーションをアドバタイジングする。これは、スイッチが接続されたポートにおいてポリシーマネージメントコンフィギュレーションをイネーブルする（例えば、自己イネーブル型ポリシー）。ユーザアクセススイッチは、隣接部発見プロトコルパケットを送信し続けて、ネットワークマネージメントシステムによりアクセスできる在庫情報でデータセンタースイッチを更新する。

【０１６６】

５．３　位置のフォーマット

位置情報のフォーマットは、システムの異なるバージョンにおいて変化し得る。上述した例では、位置情報に対する幾つかのフォーマットが示された。次のフォーマットは、付加的な例として含まれる。位置情報は、定義されたマップ座標系においてグリッド又はマップ座標として確立されてもよい。例えば、位置情報は、絶対的（例えば、緯度ｘと経度ｙ、ＧＰＳ位置、ローラン、ローランＣ、軍用グリッド）、領域的（例えば、マサチューセッツ、ビル１、３階）、相対的（例えば、ｚ階においてドアｙからｘフィート、３階のオフィス５、ポイントＡから３０°の半径方向上）、及び／又は航空機システム、例えば、超高周波（ＶＨＦ）全方向レンジ（ＶＯＲ）又は緊急位置システム（ＥＬＳ）であると考えることができる。ＧＰＳ位置決めは、衛星及び地上ベースステーションを含むことに注意されたい。位置情報は、海面レベル又はある定義された位置より上の高度を含む三次元でもよい。位置情報は、緊急状態Ｅ９１１相互運営のための連邦通信委員会により要求されたように、第四次元である精度指示子を含むことができる。又、位置情報は、緊急状態Ｅ９１１相互運営のための連邦通信委員会により要求されたように、位置識別番号を含むこともできる。位置情報は、数値、ストリング等として形式分けすることができる。

【０１６７】

５．４　位置情報の通信（図１及び８）

位置及び他の情報を装置間で送信するために、装置は、考えられる特定のネットワーク解決策をベースとし得る種々のプロトコルを使用して、互いに通信することができる。上述した例では、情報交換に使用される幾つかのプロトコルが示された。以下のプロトコルは、付加的な例として含まれる。装置は、インターネットプロトコル（バージョン４又は６）を使用することができる。システム１００が位置情報をいかに分散するかに基づいて上位層プロトコルを使用することができる。例えば、システム１００が位置情報をテーブル又はファイルとして記憶する場合には、システム１００は、ライト・ウェイト・ディレクトリー・アクセス・プロトコル（ＬＤＡＰ）のような上位層プロトコルを使用して、位置情報をアクセスし、装置間に送信することができる。システム１００は、位置情報をデータベースとして記憶する場合には、ストラクチャード・クエリー・ランゲッジ（ＳＱＬ）又はオープン・データベース・コネクティビティ（ＯＤＢＣ）のような上位層プロトコルを使用して、インターネットプロトコルを経て装置と相互作用することができる。

【０１６８】

又、装置は、第２層プロトコル、又はＩＰアドレスをもつことに依存しないプロトコルを使用して、通信することもできる。これは、装置がネットワーク層アドレスを定義できるようにすると共に、２つの装置が、インターネットプロトコルで動作していないネットワークを経て通信できるようにする。又、装置は、エクステンシブル・オーセンティケーション・プロトコル（ＥＡＰ）又はＩＥＥＥ８０２．１Ｘを使用して、互いに通信することもできる。又、装置は、ＩＰ（又は他の第３層プロトコル）或いはＭＡＣ層プロトコルの上にのる所有権プロトコルを使用して通信することもできる。

【０１６９】

説明上、上述した位置決め装置セクションの特定例では、例えば、ＩＥＥＥブリッジ・スパニング・ツリー・プロトコルが使用された。この例は、他のプロトコルを用いて説明することもできる。例えば、別の例では、システム１００は、ニューハンプシャー州、ロチェスターのエンテレシス・ネットワークス・インクによるキャブレトロン・ディスカバリー・プロトコル（ＣＤＰ）である所有権付きネットワーク隣接部発見プロトコルを使用する。ＣＤＰの例では、ネットワーク装置は、このプロトコルを使用して、隣接部発見を行なう。ＣＤＰ発見パケットは、このような発見がイネーブルされた全てのポートから所定の間隔で送信される（ステップ３０５（図３））。位置クライアントは、これら発見パケットを受信し（ステップ３１０（図３））、そして装置ＩＤフィールドをデコードする。特に、ＣＤＰ発見パケットでは、装置ＩＤフィールドは、そのパケットが送信されたポートのＳＮＭＰ　ｉｆＩｎｄｅｘと共に一次スイッチＭＡＣアドレスをベースとする。このデコードされた情報を使用して、位置クライアントは、接続ポイントＩＤ＝｛一次スイッチＭＡＣ｝＋｛ＣＤＰソーシングポートのｉｆＩｎｄｅｘ｝であると決定する（ステッ

プ３１５（図３））。

【０１７０】

システム１００は、プロトコルの組合せを使用して、前記技術を更に自動化することができる。プロトコルの組合せを使用する一例は、集中型であるか分散型であるかに関わらず、位置データベースを接続ポイントＩＤでポピュレートする自動技術である。ＣＤＰ及びＩＥＥＥスパニング・ツリー・プロトコルは、両方とも、それらに関連したＩＥＴＦＳＮＭＰマネージメント情報ベース（ＭＩＢ）を有する。位置サーバーは、ＳＮＭＰクライアントでイネーブルされると、ネットワーク環境において接続ポイントＩＤのリストを発生することができる。

【０１７１】

ＩＥＥＥスパニング・ツリー・プロトコルが、位置クライアントの接続ポイントＩＤを発見するために使用されるメカニズムである環境においては、ネットワークがＩＥＴＦｄｏｔ１ｄＢｒｉｄｇｅＭＩＢを使用することができる。ネットワークは、ｄｏｔ１ｄＢａｓｅＢｒｉｄｇｅＡｄｄｒｅｓｓＭＩＢオブジェクトを使用して、独特のスイッチ識別を定義する。ネットワークは、ｄｏｔ１ｄＢａｓｅＰｏｒｔｉｆＩｎｄｅｘＭＩＢオブジェクトをポーリングすることにより物理的ポートのＭＡＣアドレスを導出することができる。このＭＩＢオブジェクトは、ＩＥＴＦ　ＳＮＭＰ　ＭＩＢ２インターフェイスＭＩＢにおけるｉｆＩｎｄｅｘポインタに対応する。ｉｆＩｎｄｅｘを知ることでｉｆＰｈｙｓＡｄｄｒｅｓｓ　ＭＩＢオブジェクトをルックアップすることにより、ネットワークマネージメント装置は、接続ＩＤリストをポピュレートすることができる（例えば、ＩＥＥＥ８０２．１Ｄ接続ＩＤ＝スイッチベースＭＡＣアドレス＋ポートＭＡＣアドレス）。

【０１７２】

ＣＤＰをプロトコルとして使用して接続ＩＤを検出するときには、ネットワークは、あるＳＮＭＰ変数をポーリングすることにより接続リストを発生することができる。ネットワークは、ｄｏｔ１ｄＢａｓｅＢｒｉｄｇｅＡｄｄｒｅｓｓＭＩＢオブジェクトを使用して、独特のスイッチｉｄを定義する。ネットワークは、ｄｏｔ１ｄＢａｓｅＰｏｒｔｉｆＩｎｄｅｘＭＩＢオブジェクトをポーリングすることにより物理的ポートのＭＡＣアドレスを導出する。このＭＩＢオブジェクトは、ＩＥＴＦ　ＳＮＭＰ　ＭＩＢ２インターフェイスＭＩＢにおけるｉｆＩｎｄｅｘポインタに対応する（例えば、ＣＤＰ接続ＩＤ＝スイッチベースＭＡＣ＋ｉｆＩｎｄｅｘ）。

【０１７３】

ある例においては、ネットワークスイッチがＳＮＭＰを使用して各スイッチポートに対し位置情報を記憶することができる。ボイスハンドセットＭＩＢは、スイッチが各ポートに対してＡＮＳＩ　ＬＩＮ番号を記憶するのを許す。このネットワークは、ＳＮＭＰセット又はローカルコマンドラインコンフィギュレーションを経てスイッチにこの情報を準備することができる。このネットワークは、この情報をポーリングし及び／又はそれを接続ポイントＩＤ情報にマップすることができる。

【０１７４】

５．５　他の種々の変形

前記例の他の変形を実施することができる。前記例における信頼性レベルは、個別の数値として説明した。１つの例示的変形は、システム１００がストリング形式及びファジー論理技術を使用して信頼性レベルを実施できることである。例えば、信頼性レベルは、非常に信頼できる、信頼できる、あまり信頼できない、中性、信頼できない、及び非常に信頼できない、である。

【０１７５】

別の例示的変形は、上述したプロセスが付加的なステップを含んでもよいことである。更に、プロセスの一部分として示されたステップの順序は、図示された順序に限定されない。というのは、これらステップは、他の順序で実施することもでき、そして１つ以上のステップが、１つ以上の他のステップ又はその一部分に対して直列又は並列に実行されてもよいからである。例えば、ユーザの照合及び位置の照合は、並列に実行されてもよい。

【０１７６】
更に、プロセス、そのステップ、並びにこれらプロセス及びステップの種々の例及び変形は、個々に又は組合せで、コンピュータプログラム製品として実施されてもよく、具体的には、コンピュータ読み取り可能な媒体、例えば、不揮発性記録媒体、集積回路メモリ素子又はその組合せにおけるコンピュータ読み取り可能な信号として実施されてもよい。このようなコンピュータプログラム製品は、具体的にコンピュータ読み取り可能な媒体において実施されるコンピュータ読み取り可能な信号を含んでもよく、このような信号は、例えば、コンピュータにより実行された結果として、コンピュータがここに述べる１つ以上のプロセス又はアクションを実行し、及び／又は種々の例、変形及びその組合せを実行するように命令する１つ以上のプログラムの一部分としてインストラクションを定義する。このようなインストラクションは、複数のプログラミング言語、例えば、Ｊａｖａ（登録商標）、ビジュアルベーシック、Ｃ、又はＣ＋＋、フォートラン、パスカル、エイフェル、ベーシック、ＣＯＢＯＬ、等のいずれか、又はその種々の組合せのいずれかで書くことができる。このようなインストラクションが記憶されるコンピュータ読み取り可能な媒体は、上述したシステム１００の１つ以上のコンポーネントにあってもよいし、１つ以上のこのようなコンポーネントにわたって分散されてもよい。

【０１７７】
本発明を例示するのに有用な多数の例を説明した。しかしながら、本発明の精神及び範囲から逸脱せずに種々の変形がなされ得ることが理解されよう。従って、特許請求の範囲内で他の実施形態も考えられる。

【図面の簡単な説明】

【０１７８】
【図１】位置情報を伴う例示的システムのブロック図である。
【図２】位置情報を使用する例示的プロセスのブロック図である。
【図３】位置情報を使用する別の例示的プロセスのブロック図である。
【図４】位置情報を使用する更に別の例示的プロセスのブロック図である。
【図５】位置情報を使用する更に別の例示的プロセスのブロック図である。
【図６】位置情報を使用する更に別の例示的プロセスのブロック図である。
【図７】位置情報を使用する更に別の例示的プロセスのブロック図である。
【図８】位置情報を伴う別の例示的システムのブロック図である。

【図１】

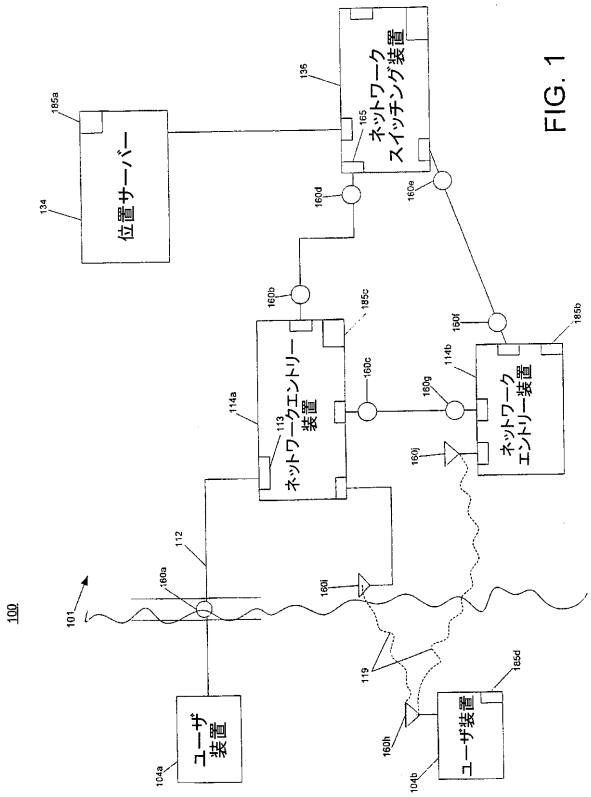


FIG. 1

【図２】

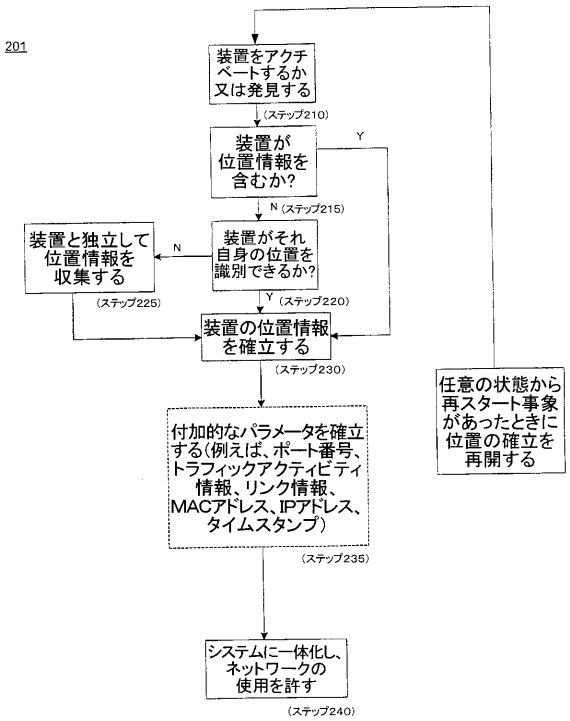


FIG. 2

【図３】

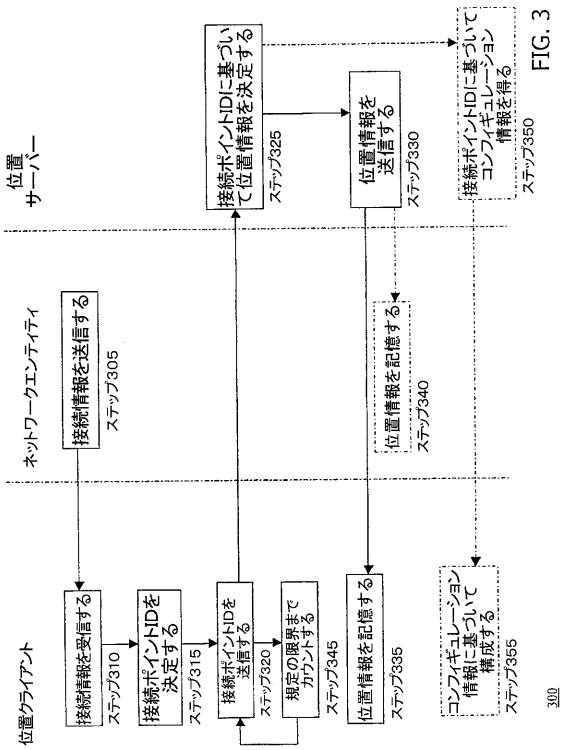


FIG. 3

【図４】

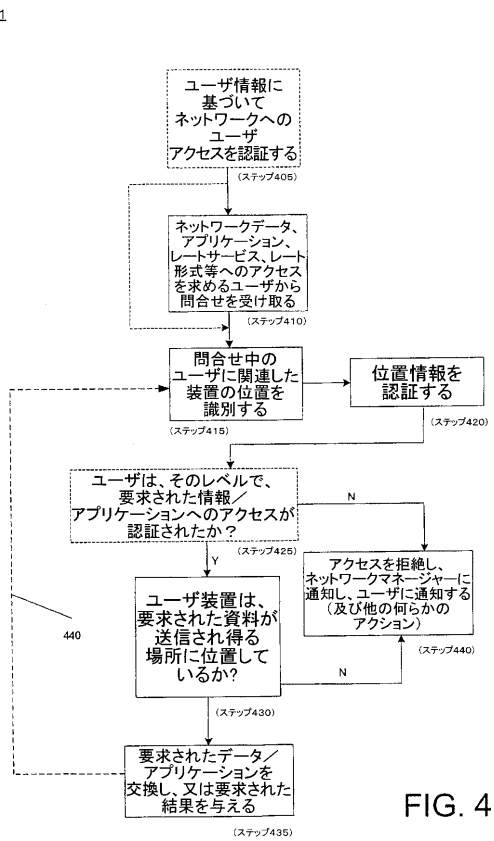


FIG. 4

【図５】

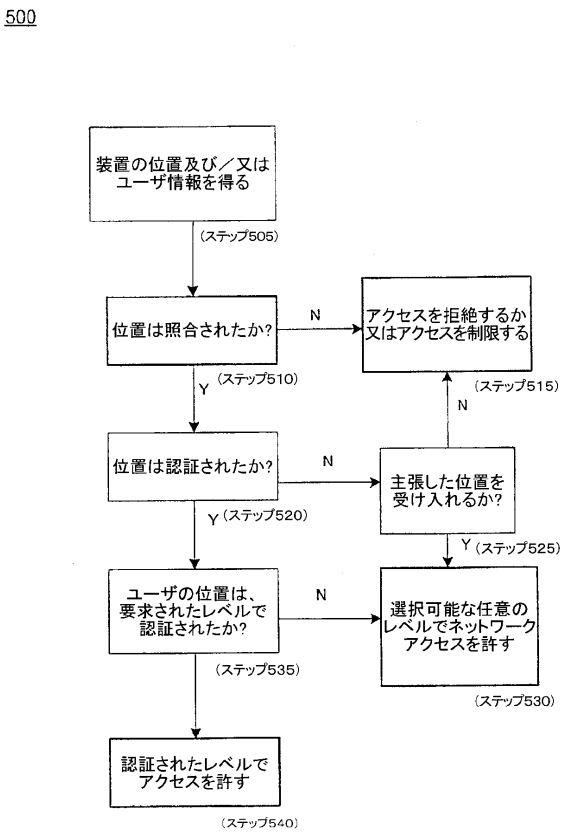


FIG. 5

【図６】

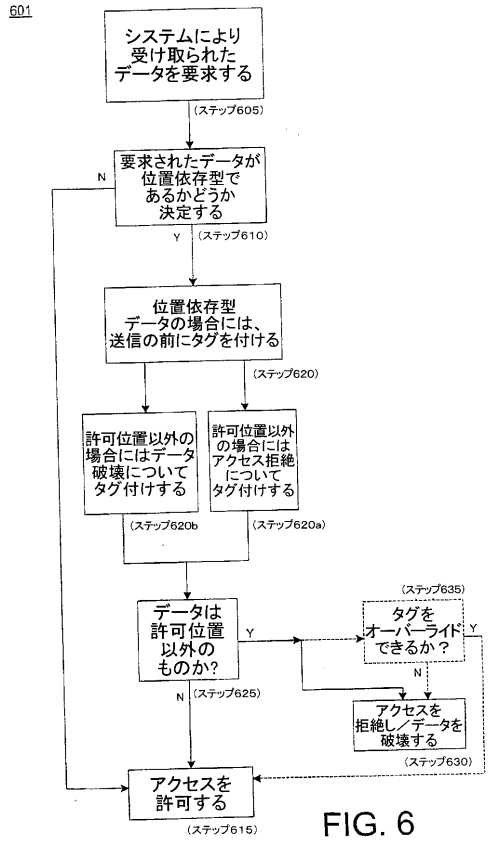


FIG. 6

【図７】

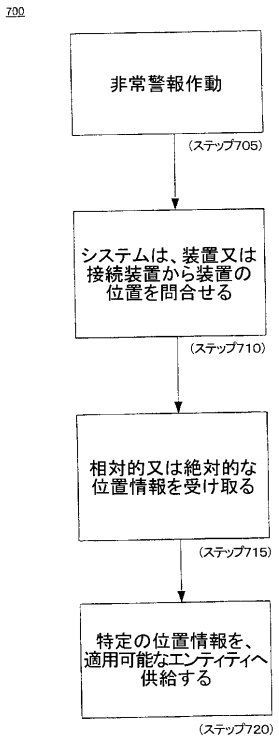


FIG. 7

【図８】

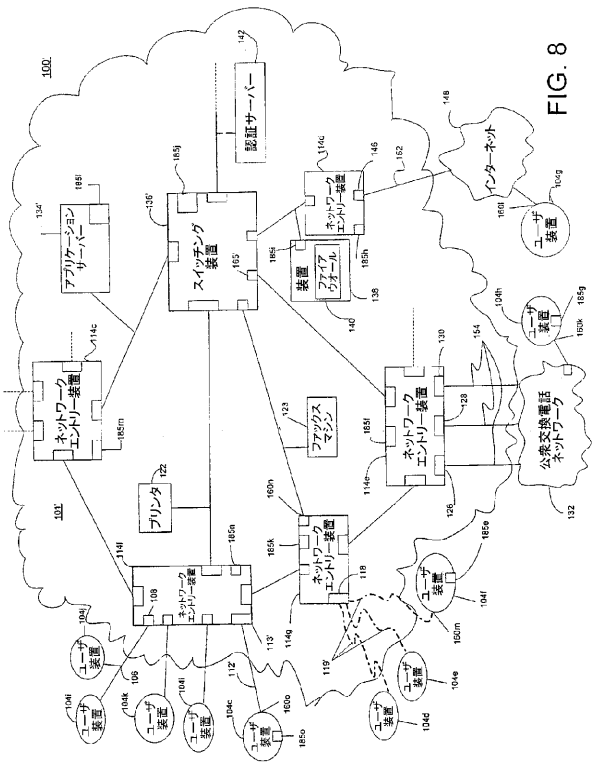


FIG. 8

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US03/06169

A. CLASSIFICATION OF SUBJECT MATTER
IPC(7) : G06F 15/173, 15/16, 15/177, 11/30; B60R 25/10; G08G 1/123; G01C 21/36
US CL : 709/220,223,225,229; 713/201; 340/988,426.19; 701/213
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 709/220,223,225,229; 713/201; 340/988,426.19; 701/213

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
Please See Continuation Sheet

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X,P --- Y,P	US 2002/0138632 A1 (BADE et al) 26 September 2002 (26.09.20020), paragraphs 21-29.	1, 73, 94, 127, 137, 150 --- 2-72, 74-93, 95-126, 128-136, 138-149
Y,P	US 6,523,064 B1 (AKATSU et al) 18 February 2003 (18.02.2003), column 15, lines 6-23; column 15 line 41 - column 16 line 57.	1-150
Y	US 6,167,513 A (INOUE et al) 26 December 2000 (26.12.2000), whole document, especially column 23, lines 8-25; column 24, lines 47-67; column 15, lines 24-41; column 16, lines 24-50.	1-72, 88-94, 138-150
A	US 6,115,754 A (LANDGREN) 05 September 2000 (05.09.2000).	
A,P	US 6,460,084 B1 (VAN HORNE et al) 01 October 2002 (01.10.2002).	1-48, 73-87, 127-137
A	US 6,012,088 A (LI et al) 04 January 2000 (04.01.2000).	1-48,73-87,127-137

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
29 September 2003 (29.09.2003)	27 OCT 2003
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (703)305-3230	Authorized officer Gregory G Todd Peggy Harwood Telephone No. (703)305-3900

Form PCT/ISA/210 (second sheet) (July 1998)

PCT/US03/06169

INTERNATIONAL SEARCH REPORT

C. (Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 6,151,631 A (ANSELL et al) 21 November 2000 (21.11.2000), columns 7-11.	1-150
Y,P	US 2002/0188842 A1 (WILLEBY) 12 December 2002 (12,12,2002), paragraphs 20-28.	1-150
Y,P	US 2003/0035544 A1 (HERLE et al) 20 February 2003 (20.02.2003)paragraphs 44-50.	1-48, 88-94, 138-150

INTERNATIONAL SEARCH REPORT

PCT/US03/06169

Continuation of B. FIELDS SEARCHED Item 3:
ACM
search terms: network and access and (control or manag or authoriz) and (gps) and topology and location

フロントページの続き

(31)優先権主張番号 60/361,380
(32)優先日 平成14年3月1日(2002.3.1)
(33)優先権主張国 米国(US)
(31)優先権主張番号 60/387,331
(32)優先日 平成14年6月10日(2002.6.10)
(33)優先権主張国 米国(US)
(31)優先権主張番号 60/387,330
(32)優先日 平成14年6月10日(2002.6.10)
(33)優先権主張国 米国(US)

(81)指定国 AP(GH,GM,KE,LS,MW,MZ,SD,SL,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,MD,RU,TJ,TM),EP(AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HU,IE,IT,LU,MC,NL,PT,SE,SI,SK,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AT,AU,AZ,BA,BB,BG,BR,BY,BZ,CA,CH,CN,CO,CR,CU,CZ,DE,DK,DM,DZ,EC,EE,ES,FI,GB,GD,GE,GH,GM,HR,HU,ID,IL,IN,IS,JP,KE,KG,KP,KR,KZ,LC,LK,LR,LS,LT,LU,LV,MA,MD,MG,MK,MN,MW,MX,MZ,NO,NZ,OM,PH,PL,PT,RO,RU,SD,SE,SG,SK,SL,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VN,YU,ZA,ZM,ZW

(72)発明者 ローズ ジョン ジェイ
アメリカ合衆国 ニューハンプシャー州 ０３８５７ ニューマーケット ムーディー ポイント ドライヴ ２１
(72)発明者 グラハム リチャード ダブリュー
アメリカ合衆国 ニューハンプシャー州 ０３０３８ デリー アイスランド ポンド ロード １８６
(72)発明者 ゴルスキー ジョン ポール
アメリカ合衆国 ニューハンプシャー州 ０３８６７ ローチェスター コンコード ウェイ ５
(72)発明者 ハーリントン デイヴィッド
アメリカ合衆国 ニューハンプシャー州 ０３８０１ ポーツマス ハーディング ロード ５０
(72)発明者 フラテュラ デイヴィッド
アメリカ合衆国 マサチューセッツ州 ０１８１０ アンドヴァー ミニットマン ロード ５０
(72)発明者 デュランド ロジャー ピー
アメリカ合衆国 ニューハンプシャー州 ０３０３１ アンハースト ウィリアムズバーグ ドライヴ １８
(72)発明者 フィー ブレンダン ジェイ
アメリカ合衆国 ニューハンプシャー州 ０３０６３ ナシュア ペンバートン ロード ３４
(72)発明者 アラン アンヤ アー
アメリカ合衆国 バージニア州 ２２０３３ フェアーファックス ドッグウッド ヒルズ レーン １２８０６

Ｆターム(参考) 5K033 CC01 DA01 DA19 DB12 DB20 EA03 EB03
5K067 BB21 CC08 DD17 DD20 EE02 EE16 HH22 HH23