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

特許第4913209号
(P4913209)

(45)発行日　平成24年4月11日(2012.4.11)　(24)登録日　平成24年1月27日(2012.1.27)

(51)Int.Cl.		F I		
H04W 4/22	(2009.01)	H04Q	7/00	135
H04W 8/26	(2009.01)	H04Q	7/00	160
H04W 84/12	(2009.01)	H04Q	7/00	630

請求項の数 7　(全 26 頁)

(21)出願番号	特願2009-508276 (P2009-508276)
(86)(22)出願日	平成19年3月26日 (2007.3.26)
(65)公表番号	特表2009-535948 (P2009-535948A)
(43)公表日	平成21年10月1日 (2009.10.1)
(86)国際出願番号	PCT/EP2007/052843
(87)国際公開番号	WO2007/124987
(87)国際公開日	平成19年11月8日 (2007.11.8)
審査請求日	平成20年10月29日 (2008.10.29)
(31)優先権主張番号	06360015.9
(32)優先日	平成18年4月29日 (2006.4.29)
(33)優先権主張国	欧州特許庁 (EP)

(73)特許権者　391030332
アルカテル－ルーセント
フランス国、７５００７・パリ、　アブニュ・オクターブ・グレアール、　３
(74)代理人　100094112
弁理士　岡部　讓
(74)代理人　100064447
弁理士　岡部　正夫
(74)代理人　100085176
弁理士　加藤　伸晃
(74)代理人　100096943
弁理士　臼井　伸一
(74)代理人　100101498
弁理士　越智　隆夫

最終頁に続く

(54)【発明の名称】ゲスト端末装置にＷＬＡＮへの緊急アクセスを提供する方法

(57)【特許請求の範囲】

【請求項１】

１つまたは複数のアクセス・ポイント（２０）と、第１のＳＳＩＤ（７）に関連付けられたＷＬＡＮ（２）のユーザ（７０乃至７３）からのデータ・パケットがＬＡＮ（３）に入ることを許すアクセス制御ファンクション（２１）とを含む該ＬＡＮ（３）への緊急アクセスを、該ＷＬＡＮ（２）を介して端末装置（１０）に提供する方法であって、

緊急の場合に前記ＬＡＮ（２）へのアクセスを許す専用の１つまたは複数の緊急ＳＳＩＤ（８）を定義するステップと、

選択された緊急ＳＳＩＤ（８）に関連付けられた端末装置（１０）から前記１つまたは複数のアクセス・ポイント（２０）の１つにデータパケットを送信することによって緊急コールを開始し、前記データ・パケットが端末装置（１０）によって、ＤＨＣＰ応答によって端末装置（１０）が受信した宛先アドレスにアドレス指定されるステップと、

前記アクセス制御ファンクション（２１）による、前記選択された緊急ＳＳＩＤ（８）に関連付けられた前記端末装置（１０）からの前記データ・パケットが、前記ＬＡＮ（３）に入ることを許すステップと、

前記選択されたＳＳＩＤ（８）に関連付けられた前記データ・パケットを、前記ＬＡＮ（３）に入ることを許された後、緊急応答ポイント（６０）にルーティングするステップとを含み、

前記方法は更に、

緊急応答ポイント（６０）への緊急コール確立の管理を負担するコール・マネージャ（

４０）のＩＰアドレスと前記コール・マネージャ（４０）がリッスンしているポートとを前記端末装置（１０）に供給する特定のＤＨＣＰオプションを、前記端末装置（１０）が要求するステップと、

前記コール・マネージャ（４０）の前記ＩＰアドレスと、前記コール・マネージャ（４０）がリッスンしているポートとを、前記端末装置（１０）がＤＨＣＰを使用してＤＨＣＰサーバーから受信するさらなるステップと、

前記選択された緊急ＳＳＩＤ（８）に関連付けられた前記端末装置（１０）が、データ・パケットを、前記コール・マネージャ（４０）の前記受信されたＩＰアドレスと、前記コール・マネージャ（４０）がリッスンしている前記ポートとでアドレス指定するステップとを更に含むことを特徴とする緊急アクセスを提供する方法。

【請求項２】

前記緊急ＳＳＩＤ（８）を２つ以上を異なる能力に、好ましくは、異なるコーデックに関連付けるさらなるステップと、

１つまたは複数の緊急ＳＳＩＤ（８）の前記ブロードキャストから抽出された情報に基づいて、緊急ＳＳＩＤ（８）を選択するさらなるステップとを含むことを特徴とする請求項１に記載の緊急アクセスを提供する方法。

【請求項３】

トラフィック指定処理または優先処理を使用することによって前記緊急コールを優先するさらなるステップを含むことを特徴とする請求項１又は２に記載の緊急アクセスを提供する方法。

【請求項４】

前記１つまたは複数のアクセス・ポイント（２０）から前記１つまたは複数の緊急ＳＳＩＤ（８）をブロードキャストするさらなるステップと、

前記端末装置（１０）による、前記１つまたは複数のブロードキャストされた緊急ＳＳＩＤ（８）の少なくとも１つを検出するさらなるステップと、

前記少なくとも１つの検出された緊急ＳＳＩＤから或る緊急ＳＳＩＤ（８）を選択するさらなるステップと、

前記端末装置（１０）による、前記選択された緊急ＳＳＩＤ（８）に関連付けられるさらなるステップとを含むことを特徴とする請求項１乃至３のいずれか１項に記載の緊急アクセスを提供する方法。

【請求項５】

前記１つまたは複数の緊急ＳＳＩＤ（８）の前記少なくとも１つを検出した後、前記端末装置（１０）において、前記ＷＬＡＮ（２）への緊急アクセスが利用可能であると前記端末装置（１０）のユーザ（１００）に知らせる通知を出力するさらなるステップを含むことを特徴とする請求項１乃至４のいずれか１項に記載の緊急アクセスを提供する方法。

【請求項６】

第１のＳＳＩＤ（７）に関連付けられたＷＬＡＮ（２）のユーザ（７０乃至７３）からのデータ・パケットが、ＬＡＮ（３）に入ることを許すアクセス制御ファンクション（２１）を含む、該ＷＬＡＮ（２）を介して該ＬＡＮ（３）に緊急アクセスを端末装置（１０）に提供する通信システム（１）であって、

前記少なくとも１つの検出された緊急ＳＳＩＤから選択された緊急ＳＳＩＤ（８）に関連付けられた端末装置（１０）からデータ・パケットを受信するように適合されたインタフェース（２０２）と、

前記選択された緊急ＳＳＩＤ（８）に関連付けられた前記端末装置（１０）からの受信された前記データ・パケットを、前記選択された緊急ＳＳＩＤ（８）に関連付けられた前記端末装置（１０）からの前記データ・パケットが、前記ＬＡＮ（３）に入ることを許す、前記アクセス制御ファンクション（２１）に転送するように適合された制御ユニット（２０３）とを含み、前記選択された緊急ＳＳＩＤ（８）に関連付けられた前記端末装置（１０）からの前記データ・パケットを、前記ＷＬＡＮ（２）に入ることを許した後、緊急応答ポイント（６０）にルーティングするように適合され、

前記データ・パケットはＤＨＣＰ応答によって端末装置（１０）が前記通信システム（１）から受信した宛先アドレスを保持し、
前記緊急アクセスを提供する通信システム（１）は、更に
緊急応答ポイント（６０）への緊急コール確立の管理を負担するコール・マネージャ（４０）、及び
前記端末装置（１０）からの対応する特定のＤＨＣＰオプションの要求に応答して、前記端末装置（１０）に、前記コール・マネージャ（４０）の前記ＩＰアドレスと、前記コール・マネージャ（４０）がリッスンしているポートとを、ＤＨＣＰを使用して提供し、それによって前記選択された緊急ＳＳＩＤ（８）に関連付けられた前記端末装置（１０）にて、データ・パケットを、前記コール・マネージャ（４０）のＩＰアドレスと、前記コール・マネージャ（４０）がリッスンしている前記ポートとでアドレス指定する、ＨＣＰサーバー（３０）を備えたことを特徴とする緊急アクセスを提供する通信システム（１）。

【請求項７】
緊急の場合に前記ＬＡＮ（３）へのアクセスを許すことに専用の１つまたは複数の緊急ＳＳＩＤ（８）を前記端末装置（１０）にブロードキャストするように適合された送信機（２０１）をさらに含むことを特徴とする請求項６に記載の緊急アクセスを提供する通信システム。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、無線ＬＡＮ（＝ＷＬＡＮ）を介する緊急アクセスを端末装置に提供するための方法、および前記方法を実行する通信システム（ＬＡＮ＝ローカル・エリア・ネットワーク）に関する。

【背景技術】
【０００２】
ＷＬＡＮは、ホテル、空港、鉄道の駅、会議施設などの公共の区域においても、企業の建物内などの占有の区域においても、ますます普及しているアクセス網になっている。企業は、企業の構内にＷＬＡＮを設置して、ＧＳＭ（＝Ｇｌｏｂａｌ Ｓｙｓｔｅｍ ｆｏｒ Ｍｏｂｉｌｅ Ｃｏｍｍｕｎｉｃａｔｉｏｎ）などの従来の無線網と比べて、比較的高い帯域幅を提供しながら、企業の従業員に移動の自由を許す。
【０００３】
過去数年の別の展開は、音声やビデオなどのリアルタイムのデータの伝送のためにＩＰベースのデータ網（ＩＰ＝インターネットプロトコル）が使用されることが増えてきたことである。コーデック標準Ｇ，７１１およびＧ．７２９、および伝送プロトコルＲＴＰ（ＶｏＩＰ＝ボイス・オーバＩＰ、コーデック＝符号化／復号、ＲＴＰ＝リアルタイムトランスポートプロトコル）などの、ＶｏＩＰアプリケーションを扱ういくつかの標準が、導入されている。
【０００４】
最近まで、加入者は、非リアルタイムのアプリケーションのために、例えば、加入者のブラウザをインターネットに接続するのにだけ、ＷＬＡＮを使用していた。しかし、今日のＷＬＡＮは、リアルタイムのアプリケーション、例えば、ＶｏＷＬＡＮ（ボイス・オーバＷＬＡＮ）も扱う作業も課題として与えられている。結局、ＶｏＷＬＡＮソリューションの加入者は、従来のＰＳＴＮ（公衆交換電話網）電話機またはＧＳＭ移動電話機の場合と同一の音声品質、信頼性、および機能を期待する。
【非特許文献１】ＩＥＥＥ８０２．１１－１９９９ Ｗｉｒｅｌｅｓｓ ＬＡＮ仕様書
【発明の開示】
【発明が解決しようとする課題】
【０００５】
本発明の目的は、緊急目的で遠隔通信サービスへのアクセスをゲスト端末装置に許可す

ることである。
【課題を解決するための手段】
【０００６】
本発明の目的は、１つまたは複数のアクセス・ポイントと、第１のＳＳＩＤに関連付けられたＷＬＡＮのユーザからのデータ・パケットがＬＡＮに入ることを許すアクセス制御ファンクションとを含むＬＡＮへの緊急アクセスを、ＷＬＡＮを介して端末装置に提供する方法によって達せられ、この方法は、緊急の場合にＬＡＮへのアクセスを許すことに専用の１つまたは複数の緊急ＳＳＩＤを定義するステップと、選択された緊急ＳＳＩＤに関連付けられた端末装置から１つまたは複数のアクセス・ポイントの１つにデータ・パケットを送信することによって、緊急コールを開始するステップと、アクセス制御ファンクションによる、選択された緊急ＳＳＩＤに関連付けられた端末装置からのデータ・パケットが、ＬＡＮに入ることを許すステップ（ＳＳＩＤ＝サービス・セット識別子）とを含む。
【０００７】
ＳＳＩＤに端末装置が関連付けられていることは、端末装置が、ＷＬＡＮの無線インタフェースを介する通信内で前記ＳＳＩＤを通知することを意味する。好ましくは、ＳＳＩＤは、無線インタフェースを介する通信のＭＡＣ層部分内で通知される。そのことは、端末装置が、無線インタフェースを介する通信中に、端末装置に関連付けられたＳＳＩＤをアクセス・ポイントにシグナルすることを意味する。
【０００８】
本発明の好ましい実施形態において、選択された緊急ＳＳＩＤに関連付けられた端末装置からのデータ・パケットは、ＬＡＮに入ることを許された後、緊急応答ポイントにルーティングされる。
【０００９】
本発明は、緊急事態の場合に、端末装置、つまり、ゲスト端末装置と許可された端末装置の両方に、ＷＬＡＮを介するＬＡＮへの確実でセキュアなアクセスをどのように提供するかという簡単な方法を提示する。
【００１０】
移動端末装置のユーザは、緊急コールを確立するために、公共でアクセス可能なＬＡＮに限定されず、企業ＬＡＮまたは専用ＬＡＮ、例えば、企業の構内ネットワークを使用することもできる。このため、制限されたアクセス権を有して、ネットワークにアクセスすることを通常許可されないゲスト端末装置さえも、このネットワークを介して緊急コールをセットアップすることができる。
【００１１】
さらに、本発明は、本発明が、緊急事態の場合に接続性および信頼性を提供する手段をＷＬＡＮに提供するので、ＶｏＷＬＡＮ技術の将来の受容に大きく寄与する。米国において、連邦通信委員会（＝ＦＣＣ）は、ＶｏＩＰサービスのプロバイダが、互いに接続されたすべてのＶｏＩＰコールが、完全な９－１－１能力を提供することを確実にするように義務付けており、９－１－１は、米国およびカナダ国における公式の全国的緊急番号である。同様の要求が、欧州の多くの国々において検討され、これらの国々において、公式の全国的緊急番号は、例えば、１－２－２である。提示される本発明により、中心的な緊急番号９－１－１および／または１－２－２をダイヤル呼び出しするいずれの発呼者も、救助が組織されるＰＳＡＰ（＝公共安全応答ポイント）に頼りになる仕方で転送されることを確信することができる。
【００１２】
緊急コールと関係するデータ・パケットのルーティングに関して、様々な方法が、利用可能である。したがって、実際の事態、および利用可能なインフラストラクチャ、トラフィック負荷などの状況に応じて、適切な方法が選択されることが可能である。
【００１３】
さらなる利点は、従属請求項によって示される本発明の実施形態によって実現される。
【００１４】

本発明の別の好ましい実施形態によれば、緊急コールを開始することを望む端末装置は、ＤＨＣＰ問い合わせによって、対応するデータ・パケットを送信すべき宛先アドレスを受け取ることができる（ＤＨＣＰ＝動的ホスト構成プロトコル）。したがって、端末装置は、選択された緊急ＳＳＩＤに関連付けられた端末装置からのデータ・パケットを、ＤＨＣＰ要求を介して受け取られた宛先アドレスでアドレス指定する。

【００１５】

ＤＨＣＰ概念は、好ましくは、デーモンとして実施され、クライアント要求をＵＤＰポート６７上で待つ（ＵＤＰ＝ユーザ・データグラム・プロトコル）ＤＨＣＰサーバを使用して実現されることが可能である。ＤＨＣＰサーバの構成ファイルが、配信されるべきアドレス・プールについての情報、およびネットワーク関連のパラメータについてのさらなるデータを含む。したがって、頻繁に変わる位置を有する端末装置は、誤りが生じやすい事前構成をなしで済ますことが可能である。端末装置は、ＷＬＡＮに対する接続を単に確立し、ＤＨＣＰサーバから、関係があるすべてのパラメータを要求する。

【００１６】

すると、選択された緊急ＳＳＩＤに関連付けられた端末装置からのデータ・パケットは、端末装置によって、そのＩＰアドレス、および緊急コールと関係するデータ・パケットをＰＳＡＰにルーティングするコール・マネージャのポートに送信される。好ましくは、端末装置は、ＤＨＣＰサーバから、コール・マネージャのアドレス関連のデータを受信する。

【００１７】

好ましくは、端末装置は、宛先アドレス、例えば、コール・マネージャのＩＰアドレスを端末装置に提供する或る特定のＤＨＣＰオプションを要求する。端末装置は、ＤＨＣＰ方法に関連するメッセージをＤＨＣＰサーバに送信して、緊急コールのデータ・パケットを送信すべき宛先アドレスを求めることができる。ＤＨＣＰサーバから宛先アドレスを受信した後、選択された緊急ＳＳＩＤに関連付けられた端末装置は、受信されたＩＰアドレスを、選択された緊急ＳＳＩＤに関連付けられた端末装置からのデータ・パケットの宛先アドレスとして設定する。好ましくは、宛先アドレスは、コール・マネージャのＩＰアドレスと、コール・マネージャがリッスンしているポートとを含む。

【００１８】

別の好ましい実施形態によれば、選択された緊急ＳＳＩＤに関連付けられた端末装置は、選択された緊急ＳＳＩＤに関連付けられた端末装置からのデータ・パケットを、任意のＩＰアドレスでアドレス指定する。ＷＬＡＮのＡＰに着信すると、そのＡＰに関連するＮＡＴファンクションが、これらのデータ・パケットのアドレスを、所定の宛先アドレスに変更する（ＡＰ＝アクセス・ポイント）。選択された緊急ＳＳＩＤに関連付けられたデータ・パケットは、宛先ＮＡＴ（＝ネットワーク・アドレス変換）を使用することによって、ＷＬＡＮインフラストラクチャ内で宛先アドレスにリダイレクトされる。ＮＡＴは、データ・パケットの中の第１のＩＰアドレスを別のＩＰアドレスで置き換えるＩＰ網における方法である。例えば、選択された緊急ＳＳＩＤに関連付けられたデータ・パケットは、ＮＡＴファンクションによって、コール・マネージャの宛先アドレスにリダイレクトされる。

【００１９】

さらに別の好ましい実施形態によれば、選択された緊急ＳＳＩＤに関連付けられた端末装置からのデータ・パケットは、所定のマルチキャスト・アドレスでアドレス指定される。このことは、端末装置において、またはＷＬＡＮに入った後、ネットワーク・ノードによって、例えば、ＡＰにおいて行われることが可能である。好ましくは、このマルチキャスト・アドレスは、コール・マネージャが加わったマルチキャスト・グループのマルチキャスト・アドレスであり、コール・マネージャがリッスンしている事前定義されたポートを含む。

【００２０】

好ましくは、ＲＴＰフローの宛先アドレスは、コール・マネージャが加わったマルチキ

ャスト・グループのマルチキャスト・アドレスである。このため、すべてのネットワーク・デバイスが、マルチキャストをサポートしなければならない。端末装置は、或る特定の緊急ＳＳＩＤに関連付けられると、或るマルチキャスト・グループに登録し、その後、端末装置が選択したＳＳＩＤに依存して、音声符号化／復号（＝ボコーダ）およびフレーミングを決定するＲＴＰフローを開始することができる。コール・マネージャは、いずれの種類のシグナリングもなしに、データ・パケットを直接に受信し、すなわち、緊急ＳＳＩＤに関連付けられた端末装置からのデータ・パケットの経路は、あらかじめ設定されており、接続は、あらかじめ確立されている。緊急コールと関係するデータ・パケットは、場合により、ＰＳＴＮなどの従来の電話網を介して、ＰＳＡＰにルーティングされる。

【００２１】

別の好ましい実施形態において、本発明によるコール・シグナリングは、ＳＩＰ、Ｈ．３２３などのようなすべてのタイプのコール処理クライアントを遵守する（ＳＩＰ＝セッション開始プロトコル）。この方法は、プロトコルに全くとらわれない。端末装置は、単に、ＲＴＰパケットをコール・マネージャに送信するだけでよい。コーデックもフレーミング・ネゴシエーションも存在しない。コール・マネージャは、或る特定のポート上で緊急サービス要求を常にリッスンする。好ましくは、コール・マネージャは、あらかじめ確立されたリンクを介して、選択された緊急ＳＳＩＤに関連付けられた端末装置からのデータ・パケットを受信し、緊急コールと関係するデータ・パケットを緊急応答ポイントにルーティングする。データ・パケット、例えば、ＲＴＰパケットは、符号化または復号なしに、さらにフレーミング・ネゴシエーションなしに、特定のシグナリング・スキームとは無関係に、ＬＡＮ、および関連するネットワークを介して伝送される。

【００２２】

本発明の好ましい実施形態によれば、緊急ＳＳＩＤに関連付けられた端末装置からのデータ・パケットは、ＬＡＮ網に入ることを許されると、緊急サービスまたは緊急応答ポイント、例えば、ＰＳＡＰにルーティングされる。好ましくは、このルーティングは、ＰＢＸまたはコール・マネージャによって実行される。コール・マネージャが、緊急コールを受信すると、コール・マネージャは、発信コールの地理的区域に関するコールを確立する。ＬＡＮに入る、緊急ＳＳＩＤに関連付けられた端末装置からのすべてのデータ・パケットは、好ましくは、これらのデータ・パケットの最初に示された宛先アドレスとは無関係に、緊急サービスまたは緊急応答ポイントにルーティングされる。緊急ＳＳＩＤに関連付けられた端末装置からのデータ・パケットは、緊急コールを確立するという目的に限って、ＬＡＮへのアクセスを許される。

【００２３】

本発明に沿って、前記ＬＡＮは、２つ以上のＷＬＡＮを介してアクセス可能なＬＡＮであることが可能である。ＷＬＡＮのそれぞれが、ＬＡＮ環境へのアクセス網の役割を果たし、別個のＳＳＩＤに関連付けられることが可能である。その場合、ＬＡＮは、第１のＳＳＩＤ、例えば、通常のＳＳＩＤによって第１のＷＬＡＮを介してアクセス可能であり、さらに第２のＳＳＩＤ，例えば、緊急ＳＳＩＤによって第２のＷＬＡＮを介してアクセス可能であることが可能である。

【００２４】

これに相応して、本発明は、許可されたユーザ、例えば、企業に所属するユーザの端末装置、ならびにゲスト・ユーザの端末装置を含む、いくつかのユーザ端末装置に、少なくとも２つのＷＬＡＮを介してアクセス可能なＬＡＮへのアクセスを提供する方法も提示する。前記第１のＷＬＡＮは、第１のＳＳＩＤに関連付けられたデータ・パケットにＬＡＮへのアクセスを提供する。第１のＷＬＡＮからのデータ・パケットは、或る暗号化方法を使用して選別されて、許可されたユーザの端末装置からの適切に暗号化されたデータ・パケットだけが、ＬＡＮに入ることを許され、他の端末装置からのデータ・パケットは破棄される。さらに、少なくとも１つの第２のＷＬＡＮが、すべてのユーザの端末装置を送信元とし、第２のＳＳＩＤに関連付けられたデータ・パケットに、ＬＡＮへのアクセスを提供する。第２のＷＬＡＮからのデータ・パケットは、選別されて、ＶｏＩＰ緊急コールを

伝送するデータ・パケットだけが許される。

【００２５】

緊急ＳＳＩＤに関連付けられたクライアントは、ゲスト・ユーザであることが可能であるので、暗号化および認証は、設定されることが可能でない。緊急ＳＳＩＤへの攻撃、または緊急ＳＳＩＤの許可のない使用を防止するのに、いくつかのセキュリティ手段が、設定されることが可能である。本発明の好ましい実施形態によれば、ユーザごとの帯域幅契約が、受け入れられることが可能である。パケットは、クライアントが、許された帯域幅を超えるパケットを送信した場合、ドロップされる。本発明の別の好ましい実施形態によれば、宛先ＮＡＴを使用して、パケットの宛先アドレスが、コール・マネージャＩＰアドレスであることを確信することができる。これにより、クライアントが、他のデバイスにパケットを送信することが防止される。プロトコル、サービス、使用される帯域幅、または選別されるべきデータ・パケットの送信元ＩＰアドレスもしくは宛先ＩＰアドレスに応じてパケットを選別することができるデバイスの存在により、音声通信だけが許される。

【００２６】

本発明の別の好ましい実施形態によれば、ＷＬＡＮへのアクセスは、第１のＳＳＩＤに関連付けられた端末装置からのデータ・パケット、すなわち、ＷＬＡＮの許可されたユーザを送信元とするデータ・パケット、およびＷＬＡＮのＡＰによってブロードキャストされた緊急ＳＳＩＤに関連付けられた端末装置からのデータ・パケットに限られる。このアクセス制限は、ファイアウォール規則を適用することによって、さらに／またはアクセス制御リスト（＝ＡＣＬ）および／またはプライベート仮想ローカル・エリア・ネットワーク（＝ＰＶＬＡＮ）の使用によって実施されることが可能である。また、アクセス制御ファンクションが、音声トラフィックだけしかＷＬＡＮに入ることを許さないことも可能である。

【００２７】

緊急サービスにおいて有するべき重要な情報は、緊急コールを開始したユーザの位置特定である。ＤＨＣＰトラッカの助けを借り、位置特定サーバにおいてホストされるＷｅｂサーバを使用して、この情報は、ＰＳＡＰに伝送されることが可能である。

【００２８】

本発明の目的は、１つまたは複数のアクセス・ポイントと、第１のＳＳＩＤに関連付けられたＷＬＡＮのユーザからのデータ・パケットがＬＡＮに入ることを許すアクセス制御ファンクションとを含むＬＡＮへの緊急アクセスを、ＷＬＡＮを介して有する端末装置を位置特定する方法によってさらに達せられ、この方法は、緊急の場合にＬＡＮへのアクセスを許すことに専用の１つまたは複数の緊急ＳＳＩＤを定義するステップと、選択された緊急ＳＳＩＤに関連付けられた端末装置から１つまたは複数のアクセス・ポイントの１つにデータ・パケットを送信することによって、緊急コールを開始するステップと、アクセス制御ファンクションによる、選択された緊急ＳＳＩＤに関連付けられた端末装置からのデータ・パケットが、ＬＡＮに入ることを許すステップと、端末装置の位置についての位置特定情報をコール・マネージャに伝送するステップとを含む。

【００２９】

好ましい実施形態において、端末装置は、位置特定情報を有するＳＯＡＰメッセージを、位置特定サーバまたはコール・マネージャに送信する（ＳＯＡＰ＝Ｓｉｍｐｌｅ Ｏｂｊｅｃｔ Ａｃｃｅｓｓ Ｐｒｏｔｏｃｏｌ）。位置特定情報を有するＳＯＡＰメッセージが、位置特定サーバに送信された場合、この位置特定情報は、コール・マネージャに転送されなければならない。このことは、コール・マネージャが、位置特定情報を提供するように位置特定サーバにポーリングを行うことによって、または位置特定サーバが、端末装置から位置特定情報を受信した後、コール・マネージャに、この位置特定情報をプッシュすることによって、行われることが可能である。

【００３０】

別の好ましい実施形態によれば、端末装置は、位置特定情報を有するＤＨＣＰ更新メッセージをＤＨＣＰサーバに送信する。次に、ＤＨＣＰサーバが、この位置特定情報を有す

るＳＯＡＰメッセージを位置特定サーバまたはコール・マネージャに送信する。やはり、位置特定情報を有するＳＯＡＰメッセージが、位置特定サーバに送信される場合、この位置特定情報は、コール・マネージャに転送されなければならない。このことは、コール・マネージャが、位置特定情報を提供するように位置特定サーバにポーリングを行うことによって、または位置特定サーバが、端末装置から位置特定情報を受信した後、コール・マネージャに、この位置特定情報をプッシュすることによって、行われることが可能である。

【００３１】

好ましい実施形態において、緊急コールに関する特定の緊急ＳＳＩＤが、コーデックなどの特定の能力と一緒に定義される。定義された緊急ＳＳＩＤのそれぞれは、異なる能力に、例えば、異なるコーデックに関連付けられる。このため、コールのために使用されるパラメータに依存して、いくつかの緊急ＳＳＩＤが、構成されることが可能であり、例えば、１つの緊急ＳＳＩＤが、Ｇ．７１１のために構成され、別の緊急ＳＳＩＤが、Ｇ．７２９のために構成されることが可能である。端末装置のユーザ、または端末装置のインテリジェンスが、関連付けられた能力に依存して、緊急ＳＳＩＤを選択することができる。或る特定の緊急ＳＳＩＤに関連付けられた能力についての情報は、緊急ＳＳＩＤのブロードキャストから抽出されることが可能である。これらの能力についての情報は、ＳＳＩＤ自体の中に含まれても、ＬＡＮの別個の情報要素から取得されてもよい。コール・マネージャは、ＲＴＰヘッダの中でデータ・パケットの処理についての情報を受信する。

【００３２】

好ましくは、緊急コールは、ボイス・オーバＷＬＡＮ電話コールに関連付けられたデータ・パケットを送信することによって開始される。ＶｏＷＬＡＮは、移動環境においてＶｏＩＰを可能にする。ＶｏＷＬＡＮは、概して建造物内で、ＩＥＥＥ８０２．１１ベースのＷＬＡＮに依拠する。ＶｏＷＬＡＮは、ＳＩＰまたはＨ．３２３などのコール・シグナリング・プロトコルに基づくＶｏＩＰ、およびサービス品質（＝ＱｏＳ）をサポートする８０２．１１ｅのバージョンにおけるＩＥＥＥ８０２．１１に準拠するＷＬＡＮなどのアプローチの統合を含む。さらに、ＵＭＴＳ網に対する直接接続が可能であり、このため、無線ベースのＬＡＮの範囲外のＶｏＷＬＡＮサービスの拡大が可能である。

【００３３】

本発明の別の好ましい実施形態によれば、端末装置は、８０２．１１ｅ方法またはWMM方法を使用して、緊急コールと関係するデータ・ストリームが、音声緊急優先度を有することを示す（WMM＝ＷｉＦｉマルチメディア、ＷｉＦｉ＝無線忠実度）。ネットワークへのコールの受け付け制御は、ＴＳＰＥＣ（＝トラフィック規格）の使用によってネゴシエートされる。この場合は端末装置である局が、局のトラフィック・フロー要件（データ転送速度、遅延限度、パケット・サイズ、およびその他）を指定し、ＡＤＤＴＳ（＝ＴＳＰＥＣ追加）管理動作フレームを送信することによって、ＴＳＰＥＣを作成するようＱＡＰ（＝ＱｏＳアクセス・ポイント）に要求する。ＱＡＰは、発行されたＴＳＰＥＣの現在のセットに基づいて、既存の負荷を計算する。現在の条件に基づいて、ＱＡＰは、新たなＴＳＰＥＣ要求を受け付ける、または拒否することができる。ＴＳＰＥＣが拒否された場合、ＱｏＳ局（＝ＱＳＴＡ）内の高優先度アクセス・カテゴリは、高優先度アクセス・パラメータを使用することを許されず、代わりに、ＱｏＳレベル・パラメータを使用しなければならない。

【００３４】

さらに、緊急コールを有利にするように先取りが使用されることが可能である。端末装置のユーザが、緊急番号などの優先番号をダイヤル呼び出しする場合、発呼側は、ＷＬＡＮが、通常の加入者会話より高い優先度を有する緊急のコールを処理するものと見込むことが可能である。ＡＰおよび／またはコール・マネージャは、この緊急コールの優先ステータスを認識し、この緊急コールを有利にするように、この緊急コールより低い優先度のコールに割り当てられたリソースを先取りする。

【００３５】

一般に、先取り機構およびＴＳＰＥＣ機構を使用して、緊急コールに関連付けられたデータ・パケットに或る特定のＱｏＳが保証されることが可能である。

【００３６】

好ましくは、端末装置は、緊急ＳＳＩＤが利用可能であることを端末装置が検出すると、或る特定の記号、例えば、「ＳＯＳ」という文字、または警察のパトロール・ランプを表すアイコンが、ソフトスクリーン上、またはダイヤルパッド上に表示されることが可能である、ディスプレイ・ユニット、例えば、スクリーンを含む。代替として、緊急ＳＳＩＤが利用可能である場合に、音響信号、例えば、ジングル、または或る特定のサウンドが、端末装置のスピーカから再生される。この特定のアイコンまたはサウンドを含むデータ・ファイルは、端末装置のメモリの中に格納されることが可能であり、このメモリから取得され、端末装置において出力されて、ＷＬＡＮへの緊急アクセスが利用可能であることを端末装置のユーザに知らせることが可能である。

【００３７】

本発明の別の好ましい実施形態によれば、１つまたは複数のアクセス・ポイントの少なくとも１つが、１つまたは複数の緊急ＳＳＩＤをブロードキャストする。端末装置が、ブロードキャストされた１つまたは複数の緊急ＳＳＩＤの少なくとも１つを検出し、この少なくとも１つの検出された緊急ＳＳＩＤから或る緊急ＳＳＩＤを選択する。

【００３８】

本発明の目的は、ＷＬＡＮを介するＬＡＮへの緊急アクセスを端末装置に提供するための通信システムによってさらに達せられ、この通信システムは、第１のＳＳＩＤを担持するＷＬＡＮの許可されたユーザからのデータ・パケットが、ＬＡＮに入ることを許すアクセス制御ファンクションを含み、この通信システムは、少なくとも１つの検出された緊急ＳＳＩＤから選択された緊急ＳＳＩＤに関連付けられた端末装置からデータ・パケットを受信するように適合されたインタフェースと、選択された緊急ＳＳＩＤに関連付けられた端末装置からの受信されたデータ・パケットを、アクセス制御ファンクションに転送するように適合された制御ユニットとを含み、アクセス制御ファンクションは、選択された緊急ＳＳＩＤに関連付けられた端末装置からのデータ・パケットが、ＬＡＮに入ることを許し、通信システムは、選択された緊急ＳＳＩＤに関連付けられたデータ・パケットを、ＬＡＮに入ることを許した後、緊急応答ポイントにルーティングするように適合される。

【００３９】

好ましくは、通信システムは、選択された緊急ＳＳＩＤに関連付けられた端末装置からのデータ・パケットを、これらのデータ・パケットが、ＤＨＣＰ要求を介して端末装置で受信された宛先アドレスで、端末装置においてアドレス指定されている場合に、ルーティングするように適合される。

【００４０】

別の好ましい実施形態によれば、通信システムは、ＷＬＡＮインフラストラクチャ内で、選択された緊急ＳＳＩＤに関連付けられた端末装置からのデータ・パケットを、所定の宛先アドレス、例えば、コール・マネージャのＩＰアドレスにリダイレクトするように適合されたＮＡＴファンクションをさらに含む。

【００４１】

さらに別の好ましい実施形態によれば、通信システムは、選択された緊急ＳＳＩＤに関連付けられた端末装置からのデータ・パケットを、これらのデータ・パケットが、宛先アドレスとしてコール・マネージャのＩＰアドレスで端末装置においてアドレス指定されている場合に、ルーティングし、前記ＩＰアドレスは、マルチキャスト・アドレスである。

【００４２】

本発明の目的は、ＷＬＡＮを介するＬＡＮへの緊急アクセスを端末装置に提供するための通信システムによってさらに達せられ、この通信システムは、第１のＳＳＩＤを担持するＷＬＡＮの許可されたユーザからのデータ・パケットが、ＬＡＮに入ることを許すアクセス制御ファンクションを含み、この通信システムは、少なくとも１つの検出された緊急ＳＳＩＤから選択された緊急ＳＳＩＤに関連付けられた端末装置からデータ・パケットを

受信するように適合されたインタフェースと、選択された緊急ＳＳＩＤに関連付けられた端末装置からの受信されたデータ・パケットを、選択された緊急ＳＳＩＤに関連付けられた端末装置からのデータ・パケットが、ＬＡＮに入ることを許す、アクセス制御ファンクションに転送するように適合された制御ユニットと、緊急事態固有のポート上で緊急要求を常にリッスンするように適合されたコール・マネージャとを含む。

【００４３】

さらに、本発明の目的は、ＷＬＡＮを介するＬＡＮへの緊急アクセスを端末装置に提供するための通信システムによってさらに達せられ、この通信システムは、第１のＳＳＩＤを担持するＷＬＡＮの許可されたユーザからのデータ・パケットが、ＬＡＮに入ることを許すアクセス制御ファンクションを含み、この通信システムは、少なくとも１つの検出された緊急ＳＳＩＤから選択された緊急ＳＳＩＤに関連付けられた端末装置からデータ・パケットを受信するように適合されたインタフェースと、選択された緊急ＳＳＩＤに関連付けられた端末装置からの受信されたデータ・パケットを、選択された緊急ＳＳＩＤに関連付けられた端末装置からのデータ・パケットが、ＬＡＮに入ることを許す、アクセス制御ファンクションに転送するように適合された制御ユニットとを含み、アクセス制御ファンクションは、サービスおよび／または帯域幅および／または宛先に関して、選択された緊急ＳＳＩＤに関連付けられた端末装置からのデータ・パケットに、ＬＡＮへのアクセスを制限するように適合される。

【００４４】

また、本発明の目的は、ＷＬＡＮを介するＬＡＮへの緊急アクセスを有する端末装置を位置特定するための通信システムによってさらに達せられ、この通信システムは、第１のＳＳＩＤを担持するＷＬＡＮの許可されたユーザからのデータ・パケットが、ＬＡＮに入ることを許すアクセス制御ファンクションを含み、この通信システムは、少なくとも１つの検出された緊急ＳＳＩＤから選択された緊急ＳＳＩＤに関連付けられた端末装置からデータ・パケットを受信するように適合されたインタフェースと、選択された緊急ＳＳＩＤに関連付けられた端末装置からの受信されたデータ・パケットを、選択された緊急ＳＳＩＤに関連付けられた端末装置からのデータ・パケットが、ＬＡＮに入ることを許す、アクセス制御ファンクションに転送するように適合された制御ユニットと、端末装置の位置特定情報を受信し、この位置特定情報と関係するデータを緊急応答ポイントに転送するように適合された位置特定サーバおよび／またはコール・マネージャとを含む。

【００４５】

好ましくは、この通信システムは、緊急の場合にＬＡＮへのアクセスを許すことに専用の１つまたは複数の緊急ＳＳＩＤを端末装置にブロードキャストするように適合された送信機をさらに含む。

【００４６】

本発明のこれら、ならびにさらなる特徴および利点は、添付の図面と併せて解釈される、現在、好ましいとされる例示的な実施形態の以下の詳細な説明を読むことによって、よりよく理解されよう。

【発明を実施するための最良の形態】

【００４７】

図１は、ＷＬＡＮ２と、ＬＡＮ３と、ネットワーク５と、コール・マネージャ４０と、ＰＳＡＰ６０とを含む通信システム１を示す。端末装置１０のユーザ１００が、緊急コールを介してＰＳＡＰ６０に接続されることを所望する。端末装置１０は、ＬＡＮ３に属するアクセス・ポイント２０のサービスエリア内に位置している。ＬＡＮ３は、アクセス制御ファンクション２１と、ＤＨＣＰサーバ３０と、位置特定サーバ３５と、コール・マネージャ４０とをさらに含む。ネットワーク５は、コール・マネージャ４０とＰＳＡＰ６０を接続する。第２のネットワーク５は、ＰＳＴＮ網などの通常の電話網であることが可能である。

【００４８】

端末装置１０は、アクセス網を介して遠隔通信網を確立するための移動デバイスである

ことが可能である。端末装置１０は、例えば、ＷＬＡＮインタフェースを有するＶｏＩＰクライアントを含む移動電話機またはラップトップ・コンピュータであることが可能である。端末装置１０は、検出ユニット１０１と、制御ユニット１０２と、ユーザ・インタフェース１０３とを含む。ユーザ・インタフェース１０３は、ユーザ１００が、端末装置１０に入力を与えることができるようにするとともに、端末装置１０から出力を受け取ることができるようにする手段を含む。好ましくは、ユーザ・インタフェース１０３は、入力キーを有するキーパッドと、マイクロホンと、ディスプレイと、スピーカとを含む。

【００４９】

ＬＡＮ３のアクセス・ポイント２０は、端末装置１０がＷＬＡＮ２に接続する通信ハブの役割をするハードウェア・デバイスまたはコンピュータ・ソフトウェアである。ＡＰ２０は、送信機２０１と、ＷＬＡＮ２に対するインタフェース、およびＬＡＮ３に対するインタフェースを有するインタフェース・モジュール２０２と、制御ユニット２０３とを含む。ＷＬＡＮ２に対するインタフェースは、ＷＬＡＮの端末装置を相手にデータを送受信する、すなわち、交換することができ、ＬＡＮ３に対するインタフェースは、ＬＡＮ３のネットワーク要素を相手にデータを送受信する、すなわち、交換することができる。

【００５０】

送信機２０１は、緊急の場合にＬＡＮ３へのアクセスを可能にすることに専用の１つまたは複数の緊急ＳＳＩＤをブロードキャストする。インタフェース２０２は、端末装置１０によって無線インタフェースを介してＬＡＮ３に送信されたデータ・パケットを受信する。制御ユニット２０３は、アクセス・ポイント２０に制御ファンクションおよびインテリジェンス・ファンクションを提供する。

【００５１】

ＷＬＡＮ２は、送信機のサービスエリア内の端末装置、ＷＬＡＮ２に対するインタフェース、ならびに端末装置と、ＷＬＡＮ２に対するインタフェース、すなわち、無線インタフェースとの間のデータ交換を伝送する媒体によって表されることが可能である。

【００５２】

ＳＳＩＤは、ＩＥＥＥ８０２．１１に基づく無線網を識別する。基本的にネットワークを識別する名前であるために、ネットワーク名としても知られるＳＳＩＤは、３２までの英数字の大文字小文字が区別される一意の文字列である。ＷＬＡＮ上のすべての無線デバイスは、互いに通信するために同一のＳＳＩＤを使用しなければならない。ＳＳＩＤは、ＷＬＡＮのＡＰにおいて構成され、ＡＰを介してＷＬＡＮにアクセスすることを所望するすべてのクライアントによって設定される。無線クライアント上のＳＳＩＤは、ＳＳＩＤをクライアント網設定に入力することによって手動で、またはＳＳＩＤを指定されないまま、つまり、空白にしておくことによって自動的に設定されることが可能である。

【００５３】

アクセス制御ファンクション２１は、ＬＡＮ３に対するアクセス制御を提供する。アクセス制御ファンクション２１は、ＷＬＡＮコントローラとして、好ましくは、スタンドアロンのデバイスとして実現されることが可能であり、あるいはＡＰ２０および／またはＡＰデバイスによって提供される機能に組み込まれることが可能である。アクセス制御ファンクション２１は、アクセス制御ファンクション２１を制御するため、ならびにＷＬＡＮ２の境界に着信するデータ・パケットに、メモリ・モジュール２０５の中に格納されたアクセス制御規則を適用するための制御ユニット２０４を含む。アクセス制御ファンクション２１は、着信するデータ・パケットがネットワーク２および３に入ることを許す前に、それらのパケットを選別する。

【００５４】

ＷＬＡＮ２は、ＩＰ網、例えば、ＤＨＣＰリレー・ファンクションを介するＬＡＮまたはインターネットであるネットワーク３を介して、ＤＨＣＰサーバ３０、位置特定サーバ３５、およびコール・マネージャ４０に接続される。ＤＨＣＰサーバ３０は、ＬＡＮ３にアクセスするデバイスに動的ＩＰアドレスを割り当てる。動的アドレス指定を使用して、デバイスは、ネットワークに接続するたびに、異なるＩＰアドレスを有することができる

。一部のシステムにおいて、デバイスのＩＰアドレスは、デバイスが依然として接続されている間に変わることさえ可能である。また、ＤＨＣＰは、静的ＩＰアドレスと動的ＩＰアドレスの混合もサポートする。

【００５５】

位置特定サーバ３５は、端末装置１０の位置を特定するサービス、好ましくは、ウェブ・サービスをホストする。このことは、端末装置１０から受信されたデータから情報を抽出することによって達せられることが可能である。端末装置１０の位置データを提供するように適合されたすべての情報が、「位置特定情報」という用語によって要約される。位置特定情報は、端末装置１０を位置特定するのに役立つことが可能である。

【００５６】

コール・マネージャ４０は、ＰＳＡＰ６０に対する緊急コール・セットアップを管理することを担う。コール・マネージャ４０は、１つまたは複数の互いにリンクされたコンピュータ、すなわち、ハードウェア・プラットフォーム、このハードウェア・プラットフォームに基づくソフトウェア・プラットフォーム、ならびにこのソフトウェア・プラットフォーム、およびこのハードウェア・プラットフォームによって形成されるシステム・プラットフォームによって実行されるいくつかのアプリケーション・プログラムから成る。コール・マネージャ４０の機能は、これらのアプリケーション・プログラムの実行によって提供される。これらのアプリケーション・プログラム、またはこれらのアプリケーション・プログラムの選択された部分が、システム・プラットフォーム上で実行されると、以下に説明されるとおりコール管理サービスを提供するコンピュータ・ソフトウェア製品を構成する。さらに、そのようなコンピュータ・ソフトウェア製品は、これらのアプリケーション・プログラム、またはアプリケーション・プログラムの前記選択された部分を格納する記憶媒体によって構成される。

【００５７】

図２は、本発明の第１の実施形態による端末装置１０、ＬＡＮ２のアクセス・ポイント２０、ＤＨＣＰサーバ３０、コール・マネージャ４０、およびＰＳＡＰ６０間の一連のメッセージを示す。第１のステップ９０１において、緊急サービスに専用である２つの緊急ＳＳＩＤが、検出ユニットを使用して端末装置１０が、これらのＳＳＩＤを検出することができるように、ＡＰ２０によってブロードキャストされる。端末装置１０による、ブロードキャストされた緊急ＳＳＩＤの検出の後、動作９０２において端末装置のディスプレイ・ユニット上にアイコン・パターンが表示されて、現在の位置において緊急サービスが利用可能であることを端末装置１０のユーザに知らせる。代替として、ユーザは、任意の通知機構を介して、緊急サービスの利用可能性について知らされてもよい。

【００５８】

示された緊急サービスを要求するのに、端末装置１０のユーザは、ステップ９０３において、端末装置１０のキーパッド上で、緊急サービスに関連する緊急サービス番号、例えば、北米において９－１－１という番号、または欧州において１－１－２という番号をダイヤル呼び出しする、あるいは端末装置１０上の緊急サービスに専用であるソフトキーを押すことができる。ソフトキーとは、特定の機能を実行する、端末装置のメイン・ディスプレイ・パネルの下のキーである。

【００５９】

動作９０３によってトリガされて、端末装置１０は、検出された緊急ＳＳＩＤのセットから或る緊急ＳＳＩＤを選択する。代替として、端末装置のユーザが、ユーザの選好に従って緊急ＳＳＩＤを選択し、キーを介して入力することによってユーザの選択を示すように促される。これに応じて、ステップ９０４で、端末装置１０が、選択された緊急ＳＳＩＤに関連付けられる。緊急コールのために使用されるコーデックは、選択された緊急ＳＳＩＤに応じて、Ｇ．７１１であることが可能である。端末装置１０が、最初、別のＳＳＩＤに関連付けられていた場合、端末装置１０は、前のＳＳＩＤから関連付け解除されて、その緊急ＳＳＩＤに関連付けられなければならない。次のステップ９０５において、端末装置１０は、ＤＨＣＰ　ＤＩＳＣＯＶＥＲメッセージをＤＨＣＰサーバ３０に送信する。

【００６０】
ＤＨＣＰサーバ３０は、端末装置１０に送信されるメッセージ９０６、例えば、ＤＨＣＰ　ＯＦＦＥＲメッセージでＤＣＨＰ要求に応答し、このメッセージ９０６は、コール・マネージャ４０のＩＰアドレスおよびポート、ならびに端末装置１０のＩＰアドレスを含む。端末装置は、そのオファーを選択し、ＤＨＣＰサーバに別の要求を送信し、肯定応答メッセージを受信することができる。このため、端末装置１０は、Ｇ．７１１コーデック標準におけるデータ・パケットを含むＲＴＰフロー９０７を、指定された宛先、つまり、コール・マネージャ４０に送信することができるようにされる。ＲＴＰフロー９０７の送信されたデータ・パケットは、選択された緊急ＳＳＩＤに関連付けられているので、アクセス制御ファンクション２１は、これらのパケットを通過させる。
【００６１】
ＡＰ２０を介してＬＡＮ３に入るすべてのデータ・パケットは、専用のスタンドアロンのアクセス制御サーバとして実施されることが可能なアクセス制御ファンクション２１を通過しなければならない。アクセス制御サーバは、１つまたは複数の互いにリンクされたコンピュータ、すなわち、ハードウェア・プラットフォーム、このハードウェア・プラットフォームに基づくソフトウェア・プラットフォーム、ならびにこのソフトウェア・プラットフォーム、およびこのハードウェア・プラットフォームによって形成されるシステム・プラットフォームによって実行されるいくつかのアプリケーション・プログラムによって構成されることが可能である。アクセス制御ファンクション２１は、これらのアプリケーション・プログラムの実行によって提供される。これらのアプリケーション・プログラム、またはこれらのアプリケーション・プログラムの選択された部分は、システム・プラットフォーム上で実行されると、以下に説明されるとおりアクセス制御サービスを提供するコンピュータ・ソフトウェア製品を構成する。さらに、そのようなコンピュータ・ソフトウェア製品は、これらのアプリケーション・プログラム、またはアプリケーション・プログラムの前記選択された部分を格納する記憶媒体によって構成される。
【００６２】
また、アクセス制御ファンクション２１が、ＬＡＮ３のネットワーク要素において、例えば、ＬＡＮ３のスイッチ、交換機、またはルータにおいて、さらなるタスクとして実施されることも可能である。また、アクセス制御ファンクション２１が、ＡＰ２０内に含まれることも可能である。アクセス制御ファンクション２１が、ＬＡＮ３の従来のネットワーク要素において実施される場合、アクセス制御ファンクション２１は、ネットワーク要素のその他のモジュールおよびユニットと協働してアクセス制御機能を提供する或る特定のモジュール内に含まれることが可能である。
【００６３】
アクセス制御ファンクション２１は、着信する各データ・パケットのヘッダ、特に、このヘッダ内に含まれるＳＳＩＤを読み取り、そのＳＳＩＤが、ＬＡＮ３に対して許可されているかどうかを調べる。例えば、アクセス制御ファンクション２１は、ＬＡＮ３、およびブロードキャストされた緊急ＳＳＩＤのいずれか、場合、許可されたユーザによって使用される最初のＳＳＩＤに関連付けられたすべてのデータ・パケットが入ることを許すように構成される。この目的で、アクセス制御ファンクション２１は、メモリ２０５の中に、承認されたＳＳＩＤのリストを有するアクセス制御リストを含むデータ・ファイルを格納していることが可能である。次に、アクセス制御ファンクション２１は、アクセス制御リストを調べ、着信したデータ・パケットのＳＳＩＤを、前記アクセス制御リストのＳＳＩＤと比較する。その結果に応じて、データ・パケットは、ＬＡＮ３に入ることを許される、または拒否される。同様に、前述したＡＣＬ方法が、アクセス制御ファンクション２１によって実現されることも可能である。
【００６４】
ＬＡＮ３へのアクセスを制御する別の仕方は、アクセス制御ファンクション２１によって、緊急ＳＳＩＤに関連付けられたデータ・パケットを送信するクライアントに制限された帯域幅を割り当てることであることが可能である。好ましくは、アクセス制御ファンク

ション２１は、緊急ＳＳＩＤに関連付けられたデータ・パケットを送信するすべてのクライアントと契約を結ぶ。この契約は、クライアントから受け入れられる帯域幅を制限する。このため、割り当てられ帯域幅を超える、端末装置によって送信されたデータ・パケットは、アクセス制御ファンクション２１によって単にドロップされる。このことは、ユーザが、緊急コールと関係するデータ・パケット以外のデータ・パケットを送信するためにＷＬＡＮへのユーザのアクセスを利用する危険を小さくする。

【００６５】

また、アクセス制御ファンクション２１は、使用されるプロトコル、送信元ＩＰアドレス、および宛先ＩＰアドレスに応じて、緊急ＳＳＩＤに関連付けられたデータ・パケットを選別することもできる。例えば、音声通信を伝送するデータ・パケットだけを許すことが可能である。一般に、サービス／プロトコル、および／または帯域幅、および／または送信元および／または宛先に関してデータ・パケットを選別することが可能である。

【００６６】

また、アクセス制御ファンクション２１は、緊急ＳＳＩＤに関連付けられたデータ・パケットが設定されている宛先ＩＰアドレスのアドレス変換を実行するＮＡＴファンクションによって実施されることも可能である。ＮＡＴファンクションは、例えば、制御ユニット２０４において実施されることが可能である。このため、ＮＡＴファンクションは、緊急ＳＳＩＤに関連付けられており、アクセス制御ファンクション２１に着信する任意のデータ・パケットの宛先ＩＰアドレスを、所定の宛先ＩＰアドレスに、例えば、コール・マネージャのＩＰアドレスに変更することができる。このことにより、クライアントが、緊急関連のデバイス以外のデバイスにパケットを送信することが防止される。

【００６７】

端末装置１０に、ＤＨＣＰソリューションによってＩＰアドレスが割り当てられることとは別に、端末装置１０は、遠隔通信ネットワーキングの分野で知られている他の方法によってＩＰアドレスを受け取ることも可能である。

【００６８】

緊急コールに関連付けられたデータ・パケットが、第１の局としてコール・マネージャ４０に伝送される方法は、使用されるプロトコルとは完全に独立である。確実で、迅速な伝送を確実にするのに、符号化および復号、フレーミングなどの、誤りが生じがちとなる可能性があるすべての変更は、省かれる。データ・パケットは、例えば、ＲＴＰパケットとして、端末装置１０から、或る特定のポート上で緊急サービス要求を常にリッスンするコール・マネージャ４０に単に転送される。

【００６９】

コール・マネージャ４０から、緊急コールと関係するデータ・パケットは、ＰＳＴＮ網を介して、ＰＳＡＰ６０にルーティングされる。したがって、緊急サービス番号のダイヤル呼び出し９０３により、端末装置１０が、地元の緊急の医療機関、消防機関、および警察機関に緊急コールをルーティングするように訓練されたＰＳＡＰにおける派遣係に迅速に接続される。

【００７０】

ＰＳＡＰコール・センタ６０において、オペレータが、発呼者の位置を検証し、緊急事態の性質を特定し、いずれの緊急応答チームに通知が行われるべきかを決定する。緊急派遣係が、ＬＢＳによって提供される位置情報を使用して、緊急事態に応答する公共安全スタッフに指示して、可能な最短の緊急応答時間を確実にする（ＬＢＳ＝位置ベースのサービス）。ときとして、単一の一次ＰＳＡＰが、地域全体を受け持つ。ほとんどの場合において、発呼者は、二次ＰＳＡＰに転送され、二次ＰＳＡＰから救助が送られる。二次ＰＳＡＰは、ときとして、消防派遣部署、自治体警察本部、または救急車派遣センタに配置される。コールが処理されると、ＰＳＡＰオペレータまたは派遣センタは、適切な緊急応答チーム、消防、救援、警察、派遣係に知らせる。

【００７１】

ＤＨＣＰオプションとは別に、インフラストラクチャは、宛先ＮＡＴを使用して、コー

ル・マネージャ４０のＩＰアドレスおよびポートにパケットをリダイレクトすることができる。ＮＡＴは、ローカル・エリア・ネットワークが、内部トラフィックに関して１つのＩＰアドレス・セットを使用し、外部トラフィックに関して第２のアドレス・セットを使用することを可能にするインターネット標準である。ＬＡＮがインターネットに出会う場所に配置されたＮＡＴボックスが、必要なすべてのＩＰアドレス変換を行う。この場合、ＮＡＴは、主に、内部ＩＰアドレスを隠すことによって或る種のファイアウォールを提供する役割をする。宛先ＮＡＴを使用する際、フローは、或る特定のポート上のホストに転送され、あるいは端末装置１０が、ＤＨＣＰオプションを使用して、コール・マネージャ４０にＲＴＰフロー９０７を直接に送信することができる。すべてのＲＴＰフローが、１つのポート上の、コール・マネージャ４０の特定のアドレスに向かわされる。１つのポート上に複数のソケットが作成される。このことは、マルチキャスト・ソケットまたはユニキャスト・ソケットに関して当てはまる。受動ソケットは、接続されるのではなく、新たな能動ソケットを生じさせる着信する接続を待つ。

【００７２】

端末装置１０は、ＡＰ２０によってアクセス可能にされたＬＡＮ３において知られていないので、暗号化を使用することはできない。しかし、侵害および／または攻撃からＬＡＮ３を保護するいくつかの仕方が、存在する。

【００７３】

主なセキュリティ上のリスクは、サービス拒否（＝ＤｏＳ）である。ＤｏＳ攻撃は、ホストのサービスの１つまたは複数を役に立たなくすることを目的とするホスト（サーバ）に対する攻撃である。通常、このことは、過負荷によって達せられる。通常、ＤｏＳ攻撃は、手動で実行されるのではなく、ネットワークの他のホストに無関係に拡散するバックドア・プログラムを使用して実行される。このため、攻撃者は、攻撃者のＤｏＳ攻撃の実行のために、さらなるホストを意のままにする。ＬＡＮ３などの８０２．１１インフラストラクチャ上で、攻撃からのいくらかの保護を提供するファイアウォール規則が、適用されることが可能である。ＤＨＣＰパケットおよびＲＴＰパケットだけが、ＬＡＮ３上の特定のホストに許されたフローである。他のプロトコルが使用された場合、そのユーザは、ブラックリストに載せられ、設定可能な時間中、ＡＰ２０に関連付けられることが可能でない。

【００７４】

代替として、ＤｏＳ－中間者（＝ＭＩＴＭ）検出－防御アプリケーションが、ＬＡＮ３上で実施されることが可能である。ＭＩＴＭ攻撃は、通信パートナの中間に物理的、または論理的に位置する攻撃者を出所とする。この位置において、ＭＩＴＭ攻撃者は、２名以上のネットワーク加入者の間のデータ・トラフィックを完全に支配し、交換される情報を自由に見る、または操作することさえできる。

【００７５】

攻撃からＬＡＮ３を保護するさらに別の仕方は、制限された帯域幅しか、ユーザに与えないことである。このことは、システムが、ＤｏＳから防御するのに役立つ可能性がある。宛先ＮＡＴを使用して、他のデバイスに攻撃が向けられることを防止することが、さらに可能である。

【００７６】

さらに別の実施形態において、すべてのゲスト・ユーザの関連付けが、仮想ローカル・エリア・ネットワーク（＝ＶＬＡＮ）ごとにＡＣＬを適用するために、これらのユーザに専用のＶＬＡＮにおいて使用されることが可能である。ネットワーク上のＶＬＡＮは、ブロードキャスト・ドメインである。そのＶＬＡＮ上のホストのすべては、同一のＶＬＡＮの他のメンバと通信することができる。プライベートＶＬＡＮ（＝ＰＶＬＡＮ）は、トラフィックが、ＯＳＩモデルのデータ・リンク層（層２）としてセグメント化されて、ブロードキャスト・ドメイン（ＯＳＩ＝開放型システム間相互接続）のサイズが制限されることを可能にする。ＡＣＬは、誰がＭＡＣ／ＩＰアドレス・アクセスを受け取るかを制御する。ＡＣＬは、例えば、特定のクライアントを、それらのクライアントのＩＰアドレスに

よって、ＬＡＮ３へのアクセスから除外することができるルータにおいて構成される。

【００７７】

また、攻撃からの保護は、スイッチ上、およびルータ上で実施されることも可能である。１つの可能性は、層２隔離のためにＰＶＬＡＮ環境を構成することである。ＰＶＬＡＮは、既存のＶＬＡＮ内でさらなる細分を提供し、個々のポートが、同一のＩＰサブネットを依然として共有しながら、他のポートから分離されることを可能にする。このことは、各デバイスに関して別個のＩＰサブネットを要求することなしに、デバイス間の分離が行われることを可能にする。最も単純な形態で、ＰＶＬＡＮは、隔離されたポート、およびプロミスキャス・ポートをサポートする。隔離されたポートは、プロミスキャス・ポートにだけ通信することができ、プロミスキャス・ポートは、いずれのポートにも通信することができる。この展開において、サブネットのメンバは、隔離されたポートであり、ゲートウェイ・デバイスは、プロミスキャス・ポートに接続される。このことにより、サブネット上のホストが、同一のサブネット上のメンバの要求に応じないことが可能になる。

【００７８】

別の可能性は、８０２．１ｘゲストＶＬＡＮを、層２隔離のためにＰＶＬＡＮに拡張する８０２．１ｘプライベート・ゲストＶＬＡＮフィーチャである。

【００７９】

８０２．１ｘプライベート・ゲストＶＬＡＮは、８０２．１ｘ　Ｓｕｐｐｌｉｃａｎｔなしに、ゲスト二次ＰＶＬＡＮを介する限られたネットワーク・アクセスをユーザに提供する。

【００８０】

別のかなり単純明快な方法は、ＡＣＬ技術を使用する、または単に、ＭＡＣアドレスの最大数をトランクポート上の個々のＶＬＡＮに制限することである。

【００８１】

本発明は、有害な意図のない不適切な関連付けを防止するいくつかの仕方をサポートする。例えば、緊急サービスＳＳＩＤに関連付けられるすべての端末装置は、或る時間内に緊急を要求するＴＳＰＥＣを送信しなければならず、さもなければ、ＡＰ２０によって関連付け解除され、さらに／またはブラックリストに載せられる。代替として、ＳＳＩＤは、隠されることが可能であり、能動的なスキャンが、緊急ＳＳＩＤに関連付けられるのに必須である。

【００８２】

緊急サービス・コールは、端末装置１０が、ＴＳＰＥＣトラフィック規格を使用して、ＲＴＰフローが、音声緊急優先度を有することを示すようにトリガすることによって、優先されることが可能である。また、先取り手続きを使用して、より低い優先度のコールに対して緊急コールが有利にされ得ることも可能である。

【００８３】

図３ａ乃至図３ｃは、緊急コールのパケットのルーティングと関係する異なる３つの例を示す。図３ａ乃至図３ｃのそれぞれにおいて、端末装置１０、ＬＡＮ３のアクセス・ポイント２０、アクセス・ポイント２０に関連するＮＡＴサーバ２２、ＤＨＣＰサーバ３０、コール・マネージャ４０、およびＰＳＡＰ６０の間で一連のメッセージが伝送される。

【００８４】

図３ａは、ＤＨＣＰ方法に基づくパケット・ルーティングと関係するメッセージ・フロー・シーケンスを示す。このＤＨＣＰ方法では、クライアントは、ＩＰアドレスを要求する際、コール・マネージャのＩＰアドレスをクライアントに与える或る特定のＤＨＣＰオプションを求める。この方法の第１のステップで、端末装置１０は、ＤＨＣＰ　ＤＩＳＣＯＶＥＲメッセージ２１０を送信する。端末装置１０が、ＤＨＣＰサーバ３０を利用することができるには、ＤＨＣＰリレーが使用されるのでない限り、両方のデバイスが、同一のＩＰ網内に存在しなければならない。両方のデバイスが、同一のＩＰ網内に存在していない場合、ＤＨＣＰサーバが配置されているネットワークに、ＤＨＣＰ関連のメッセージを中継し、さらに／または転送するＤＨＣＰリレー・ユニットまたはＤＨＣＰヘルパ・ユ

ニットなどのＤＨＣＰ支援デバイスが、使用されることが可能である。

【００８５】

端末装置１０によって送信されたＤＨＣＰ　ＤＩＳＣＯＶＥＲメッセージ２１０は、ＤＨＣＰサーバ３０に到達する。このことは、端末装置１０とＤＨＣＰサーバ３０が、同一のネットワーク内、例えば、ＶＬＡＮ内に存在する場合、ブロードキャストにおいてＤＨＣＰ　ＤＩＳＣＯＶＥＲメッセージ２１０を送信することによって、またはＤＨＣＰヘルパを介して、達せられることが可能である。ＤＨＣＰ　ＤＩＳＣＯＶＥＲメッセージ２１０によって、端末装置１０は、ＤＨＣＰサーバ３０からＩＰアドレスを要求する。好ましくは、ＤＨＣＰ　ＤＩＳＣＯＶＥＲメッセージ２１０は、端末装置１０のＭＡＣアドレスを含む（ＭＡＣ＝メディア・アクセス制御）。ＬＡＮアドレス、イーサネット（登録商標）ＩＤ、または空港ＩＤとしても知られるＭＡＣアドレスは、ネットワークのデバイスの一意ＩＤの役割をするネットワーク・デバイスのハードウェア・アドレスである。

【００８６】

好ましくは、端末装置１０は、利用可能なすべてのＤＨＣＰサーバへのネットワーク・ブロードキャストとしてＤＨＣＰ　ＤＩＳＣＯＶＥＲメッセージ２１０を送信する。いくつかのＤＨＣＰサーバが、同一のＩＰサブネットワーク内に配置されることが可能である。ＤＨＣＰ　ＤＩＳＣＯＶＥＲブロードキャスト・メッセージ２１０は、送信機ＩＰアドレスとして０．０．０．０を伝送することができ、送信する端末装置１０は、ＩＰアドレスを有していないが、それでも、到達可能なすべてのＤＨＣＰサーバに要求を向けるので、宛先アドレス２５５．２５５．２５５．２５５にアドレス指定されることが可能である。

【００８７】

ＤＨＣＰサーバ３０は、ＤＨＣＰ　ＤＩＳＣＯＶＥＲメッセージ２１０を受信し、要求する端末装置１０に関するＩＰアドレスのオファーを含むＤＨＣＰ　ＯＦＦＥＲメッセージ２１１で応答する。ＤＨＣＰ　ＯＦＦＥＲメッセージ２１１は、送信するＤＨＣＰサーバ３０を識別するサーバＩＤ、ならびにコール・マネージャ４０のＩＰアドレスおよびポートをさらに含む。端末装置１０が、異なるＤＨＣＰサーバから複数のオファーメッセージを受信することが可能である。このため、端末装置は、受信されたオファーの中から選択することができる。提案された１つまたは複数のオファーの１つを選択した後、端末装置は、ＤＨＣＰ　ＲＥＱＵＥＳＴメッセージ２１２によって、対応するサーバＩＤを使用して識別される適切なＤＨＣＰサーバ３０と連絡をとる。好ましくは、ＤＨＣＰ　ＲＥＱＵＥＳＴメッセージ２１２は、ブロードキャストされる。

【００８８】

これに応答して、ＤＨＣＰサーバ３０は、要求する端末装置１０にＤＨＣＰ　ＡＣＫ（＝肯定応答）メッセージ２１３を伝送する。伝送されるＤＨＣＰ　ＡＣＫメッセージ２１３は、端末装置１０のＩＰアドレスと、コール・マネージャ４０のＩＰアドレスと、コール・マネージャ４０が常にリッスンしているポートと、さらなる関係のあるデータとを含む。

【００８９】

このため、ステップ２１４で、端末装置１０は、端末装置１０自体のＩＰアドレスと、コール・マネージャ４０のＩＰアドレスと、コール・マネージャ４０がリッスンしているポートとを有する。端末装置１０は、緊急コールと関係するパケットにコール・マネージャ４０の宛先アドレスおよびポートでアドレス指定し、アドレス指定されたパケットをコール・マネージャ４０に送信する。端末装置１０とコール・マネージャ４０の間のＲＴＰフロー２１５が、確立される。コール・マネージャ４０は、緊急コールと関係するパケットを受信し、妥当なＰＳＡＰ６０に対するコール・セットアップ２１６を開始し、パケットをＰＳＡＰ６０に転送する。

【００９０】

図３ｂは、宛先ＮＡＴに基づくパケット・ルーティングと関係するメッセージ・フロー・シーケンスを示す。この宛先ＮＡＴ方法では、クライアントは、ＩＰアドレスを受信す

ると、任意の宛先アドレスにパケットを送信することができる。ＮＡＴサーバ２２は、このアドレスを、コール・マネージャ４０の１つに変更する。図３ｂのステップ２２０乃至２２４は、図３ａに示されるステップ２１０乃至２１４に対応する。図３ａに示される方法との唯一の違いは、ＤＨＣＰ　ＯＦＦＥＲメッセージ２２１およびＤＨＣＰ　ＡＣＫメッセージ２２３が、コール・マネージャ４０のＩＰアドレスおよびポートを含まないことである。

【００９１】

また、端末装置１０は、ＤＨＣＰを介する以外の別の方法を介してＬＡＮ３に参加するためのＩＰアドレスを受信することも可能である。

【００９２】

ステップ２２４で、端末装置１０は、端末装置のＩＰアドレスだけを取得する。端末装置１０は、宛先アドレスとして任意のＩＰアドレスで緊急コールと関係するパケットをアドレス指定し、このアドレス指定されたパケットを、ＡＰ２０に関連するＮＡＴサーバ２２に送信する。端末装置１０とＮＡＴサーバ２２との間のＲＴＰフロー２２５が、確立される。ＮＡＴサーバ２２は、端末装置１０からパケットを受信し、宛先アドレスを、コール・マネージャ４０のＩＰアドレスに変換する。ＮＡＴサーバ２２と、コール・マネージャ４０との間のＲＴＰフロー２２６が、確立される。コール・マネージャ４０は、緊急コールと関係する情報をパケット形態またはストリーム形態で受信し、妥当なＰＳＡＰ６０に対するコール・セットアップ２２７を開始し、パケットをＰＳＡＰ６０に転送する。

【００９３】

図３ｃは、マルチキャスト方法に基づくパケット・ルーティングと関係するメッセージ・フロー・シーケンスを示す。このマルチキャスト方法では、クライアントは、ＩＰアドレスを受信すると、コール・マネージャ４０がリッスンしている事前定義されたポート上のよく知られたマルチキャスト・アドレスにパケットを送信する。図３ｃのステップ２３０乃至２３４は、図３ａに示されるステップ２１０乃至２１４に対応する。図３ａに示される方法との唯一の違いは、ＤＨＣＰ　ＯＦＦＥＲメッセージ２３１およびＤＨＣＰ　ＡＣＫメッセージ２３３が、コール・マネージャ４０のＩＰアドレスおよびポートを含まないことである。

【００９４】

また、端末装置１０は、ＤＨＣＰを介する以外の別の方法を介してＬＡＮ３に参加するためのＩＰアドレスを受信することも可能である。

【００９５】

ステップ２３４で、端末装置１０は、端末装置１０のＩＰアドレスだけを取得する。端末装置１０は、宛先アドレスとしてマルチキャストＩＰアドレスで緊急コールと関係するパケットをアドレス指定し、このアドレス指定されたパケットをコール・マネージャ４０に送信する。端末装置１０とコール・マネージャ４０との間のＲＴＰフロー２３５が、確立される。コール・マネージャ４０は、緊急コールと関係する情報（パケット形態／ストリーム形態）を受信し、妥当なＰＳＡＰ６０に対するコール・セットアップ２３６を開始し、パケットをＰＳＡＰ６０に転送する。

【００９６】

図４は、端末装置７０乃至７３を含むＷＬＡＮ２の許可されたユーザのグループ７００を示す。許可されたユーザのグループ７００は、第１のＳＳＩＤ７を使用することによって緊急でないコールでＬＡＮ３にアクセスすることができる。同時に、グループ７００のメンバは、オープン・グループ８００のメンバでもある。オープン・グループ８００は、端末装置７０乃至７３を有する許可されたユーザと、端末装置１０乃至１３を有するＷＬＡＮ２の許可されていないユーザをともに含む。許可されたユーザのグループ７００だけが、第１のＳＳＩＤ７を使用することによって緊急でないコールでＬＡＮ３にアクセスする資格がある。しかし、グループ８００は、アクセス・ポイント２０のサービスエリア内に位置しているので、グループ７００のメンバとグループ８００のメンバの両方が、緊急ＳＳＩＤ８を使用することによって緊急コールでＬＡＮ３にアクセスすることができるよ

うにされる。グループ７００またはグループ８００の任意の端末装置、例えば、端末装置１０または端末装置７１が、緊急ＳＳＩＤ８を使用して、アクセス・ポイント２０を介してＬＡＮ３にアクセスすることができる。

【００９７】

したがって、アクセス・ポイント２０のサービスエリア内の任意の端末装置が、緊急ＳＳＩＤ８を使用することによって、緊急事態の場合にＬＡＮ３にアクセスすることができる。緊急でないコールの場合、ＷＬＡＮ２の許可されたユーザを含む許可されたグループ７００の端末装置だけが、アクセス・ポイント２０を介してＬＡＮ３にアクセスすることができる。緊急ＳＳＩＤ８に関連付けられたコールは、ＰＳＡＰ６０にルーティングされるが、例えば、端末装置７０を送信元とする緊急でないコールは、従来技術で知られている手続きにおいて別の通信パートナ９０にルーティングされることが可能である。

【００９８】

アクセス制御を実施するため、アクセス制御ファンクション２１が、許可されたＳＳＩＤに関連付けられた端末装置からのデータ・パケットに、ＬＡＮ３へのアクセスを制限することに加え、着信するデータ・パケットにさらなる規則を適用することができる。緊急ＳＳＩＤに関連付けられた端末装置からＬＡＮ２にデータ・パケットを送信する各ユーザには、ＰＳＡＰ６０に対する緊急コールをセットアップするのに十分であるが、他のコールを確立するだけ十分には広くない、制限された帯域幅が割り当てられることが可能である。このアクセス制御機構は、緊急コールが、データの量に関して多少、限定されている可能性があるので、機能することが可能である。

【００９９】

このアクセス制御機構と緊密に関係するのが、ＬＡＮ３に音声トラフィックだけしか入ることを許さない技術である。このため、ビデオのような帯域幅を消費するアプリケーションと関係するデータ・パケットは、データ・パケットが、緊急ＳＳＩＤを使用することによってＬＡＮ３に入ろうと試みた場合、ＬＡＮ３から閉め出される。

【０１００】

図５は、ＩＰパケットの伝送のためのネットワーク４００、およびネットワーク４００へのアクセスを提供するための２つの無線アクセス網４０１、４０２を示す。企業アクセス網４０１は、許可されたユーザ端末装置７０１、７０２だけによってアクセス可能な企業アクセス網であるのに対して、緊急アクセス網４０２は、緊急アクセス網４０２のサービスエリア内の任意の移動ユーザ端末装置によって、すなわち、許可されたユーザ端末装置７０１、７０２とゲスト・ユーザ端末装置８０１乃至８０３の両方によって、緊急目的でアクセス可能である。

【０１０１】

許可された端末装置７０１、７０２は、端末装置７０１、７０２が、アクセス網４０１２にデータ・パケットを伝送する前に、データ・パケットを適切に暗号化することができるようにする暗号化モジュール７０１０、７０２０を含むことが可能である。

【０１０２】

各アクセス網４０１、４０２は、それぞれのアクセス網に特有のＳＳＩＤを、送信機によって、例えば、ＡＰによってブロードキャストする。企業アクセス網４０１は、企業アクセス網４０１に関連する企業ＳＳＩＤをブロードキャストし、緊急アクセス網４０２は、緊急アクセス網４０１に関連する緊急ＳＳＩＤをブロードキャストする。ブロードキャストされたＳＳＩＤは、アクセス網４０１、４０２のサービスエリア内の任意の端末装置によって受信されることが可能である。

【０１０３】

企業アクセス網４０１は、アクセス制御ファンクション４０１１を含み、同様に、緊急アクセス網４０２も、アクセス制御ファンクション４０２１を含む。アクセス制御ファンクション４０１１、４０２１は、メモリ・モジュールの中に格納されたアクセス制御規則を含むスタンドアロンのサーバとして実施される。アクセス制御ファンクション４０１１、４０２１のそれぞれは、データ・パケットがアクセス網４０１、４０２に入ることを許

す前に、着信するデータ・パケットを選別する。

【０１０４】

緊急アクセス網４０２に関連する緊急ＳＳＩＤに関連付けられた端末装置からのデータ・パケットは、アクセス制御ファンクション４０２１によって緊急アクセス網４０２へのアクセスを許可される。許可されたユーザ端末装置７０１、７０２だけが、暗号化モジュール７０１０、７０２０を使用してデータ・パケットを適切に暗号化できることが可能である。アクセス制御ファンクション４０１１に着信するデータ・パケットは、企業アクセス網４０１に関連する企業ＳＳＩＤに関連付けられた端末装置を送信元としなければならず、アクセス網４０１に入ることを許されるように適切に暗号化されることが可能である。暗号化技術によって、アクセス制御ファンクション４０１１は、着信するデータ・パケットを選別し、許可されたユーザ端末装置を送信元としないデータ・パケットを破棄する。アクセス制御ファンクション４０１１は、選別－検査プロセスに関係のあるデータをデータベース４０１２から取得する。

【０１０５】

ゲスト・ユーザ端末装置８０１は、企業ＳＳＩＤに気付いており、この企業ＳＳＩＤを使用して、企業アクセス網４０１にアクセスする。企業アクセス網４０１のネットワーク管理者が、企業アクセス網４０１のアクセス・ポイント上に設定された公開企業ＳＳＩＤを構成し、範囲内のすべての無線デバイスにブロードキャストすることが可能である。このため、企業ＳＳＩＤは、企業アクセス網４０１によってオープンにブロードキャストされており、ゲスト・ユーザ端末装置８０１が、ブロードキャストされた企業ＳＳＩＤを拾い上げることによって企業ＳＳＩＤを受信している。

【０１０６】

しかし、ゲスト・ユーザ端末装置８０１が、企業アクセス網４０１によって提供される通信サービスを、許可されていない仕方で使用したいと欲する盗聴者に関連することも可能である。企業ＳＳＩＤの公開ブロードキャストは、セキュリティ上のリスクをもたらすので、企業アクセス網４０１のネットワーク管理者が、ネットワーク・セキュリティを向上させようとして、自動ＳＳＩＤブロードキャスト・フィーチャを無効したものと想定する。しかし、ＳＳＩＤブロードキャストの非活性化によって提供される保護は、ＳＳＩＤが、許可された端末装置７０１、７０２によって企業アクセス網４０１に送信されるデータ・パケットからプレーンテキストでスニフィングされる可能性があるので、盗聴者によって容易に裏をかかれる可能性がある。

【０１０７】

しかし、ゲスト・ユーザ端末装置８０１は、企業ＳＳＩＤを受信しており、この企業ＳＳＩＤに関連付けられ、企業アクセス網４０１にデータ・パケット・ストリーム３０１を送信する。ゲスト・ユーザ端末装置８０１は、データ・パケット３０１を適切に暗号化する手段を有さないので、アクセス制御ファンクション４０１１によってデータ・パケット・ストリーム３０１に対して実行される検査は、データ・パケット・ストリーム３０１の拒否をもたらす。

【０１０８】

他方、暗号化モジュール７０１０を含む許可されたユーザ端末装置７０１は、企業ＳＳＩＤに関連付けられた端末装置からであるとともに、適切に暗号化されているデータ・パケット１００１を企業アクセス網４０１に送信する。このため、アクセス制御ファンクション４０１１における検査プロセスは、アクセス網に入ることの許可をもたらす。同様に、その他の許可されたユーザ端末装置７０２を送信元とするデータ・パケット１００２も、企業アクセス網４０１に入ることを許される。

【０１０９】

許可されたユーザ端末装置７０２が、緊急ＳＳＩＤに関連付けられた端末装置からアクセス制御ファンクション４０２１にデータ・パケット５０２を送信すると、データ・パケット５０２は、緊急アクセス網４０２に入ることを許される。ゲスト・ユーザ端末装置８０２は、緊急ＳＳＩＤと関係するデータ・パケット・ストリーム５０１を企業アクセス網

４０１に送信するが、このデータ・パケット・ストリーム５０１は、適切なＳＳＩＤに関連付けられた端末装置からではなく、適切に暗号化されてもいないので、企業アクセス網４０１に入ることを許されない。しかし、緊急ＳＳＩＤに関連付けられたゲスト・ユーザ端末装置８０２が、緊急アクセス網４０２にデータ・パケット・ストリーム５０２を送信すると、データ・パケット５０３は、緊急ＳＳＩＤに関連付けられた端末装置からであるので、データ・パケット・ストリーム５０２は、アクセス制御ファンクション４０２１によって緊急アクセス網４０２に入ることを許される。

【０１１０】

企業ＳＳＩＤに関連付けられたゲスト・ユーザ端末装置８０３が、緊急アクセス網４０２にデータ・パケット３０２を送信すると、データ・パケット・ストリーム３０２は、アクセス制御ファンクション４０２１によって拒否される。アクセス制御ファンクション４０２１は、緊急ＳＳＩＤに関連付けられた端末装置からのデータ・パケットだけしか入ることを許さない。

【０１１１】

企業アクセス網４０１に入った後、データ・ストリーム１００１および１００２は、データ・ストリーム６０１および６０２としてネットワーク４００に転送され、データ・ストリーム６０１および６０２のデータ・パケットの中で示されるＩＰ宛先アドレスに従ってデータ・ストリーム６０１および６０２をルーティングする、または切り替えるネットワーク要素４００１、例えば、ルータまたはスイッチにルーティングされる。

【０１１２】

例えば、許可されたユーザ端末装置７０１のユーザが、企業通信パートナのＶｏＩＰ電話番号をダイヤル呼び出しすると、許可されたユーザ端末装置７０１のＶｏＩＰユーザ・エージェントが、これに応じて、対応するアドレスでデータ・パケット１００１、６０１をアドレス指定し、データ・パケット・ストリーム６０１は、ネットワーク要素４００１によって、そのアドレスを担当する別のネットワーク要素４００２にルーティングされる。接続の確立は、適切なルーティングおよびコール確立のためにシグナリング・メッセージおよび制御メッセージの交換を要求する。同様に、データ・パケット１００２も、ネットワーク要素４００１を介して別のネットワーク要素４００３にルーティングされる。事前確立されたルーティングは全く存在せず、代わりに、ネットワーク４００におけるそれぞれの次のホップは、各ネットワーク要素によって、データ・パケットの示されたアドレスに従ってデータ・パケットごとに個々に決定される。

【０１１３】

他方、緊急アクセス網４０２に着信し、入ることを許されたデータ・ストリーム５０２、５０３は、これらのデータ・パケットを緊急サービス応答ポイント６０、例えば、ＰＡＳＰにルーティングするコール・マネージャ４００１に、例えば、ＰＢＸにルーティングされる（ＰＢＸ＝構内交換機）。このルーティングは、シグナリング・トラフィックおよび制御トラフィックの必要なしに、事前確立された接続上で実行される。

【０１１４】

また、データ・パケットの実際のアドレスにかかわらず、緊急アクセス網４０２に入ることを許されたデータ・パケットの元の宛先アドレスは、データ・パケットから取り除かれ、緊急サービスに関連する事前設定された標準のアドレス、例えば、コール・マネージャ４００１のＩＰアドレスおよびポートで置き換えられ得ることも可能である。この標準化され、事前確立されたアプローチによって、緊急コールの迅速で、確実な応答が可能である。

【０１１５】

図６ａ乃至図６ｄは、緊急コールを開始する端末装置の位置特定と関係する、異なる４つの例を示す。図６ａ乃至図６ｄのそれぞれにおいて、端末装置１０、ＬＡＮ３のアクセス・ポイント２０、ＤＨＣＰサーバ３０、位置特定サーバ３５、コール・マネージャ４０、およびＰＳＡＰ６０の間で一連のメッセージが、伝送される。位置特定サーバ３５は、ＰＳＡＰに位置特定情報の伝送を提供するウェブ・サービスをホストする。

【０１１６】
図６ａは、第１の代替の実施形態による端末装置１０の位置特定と関係するメッセージ・フロー・シーケンスを示す。方法の第１のステップで、端末装置１０は、緊急ＳＳＩＤに関連付けられた後、ＡＰ２０を介して位置特定サーバ３５にＳＯＡＰプッシュ・メッセージ５１０を送信する。ＳＯＡＰプッシュ・メッセージ５１０は、端末装置１０の位置特定情報、例えば、端末装置がＬＡＮにアクセスするのを仲介するＡＰ２０のＢＳＳＩＤを含む（ＢＳＳＩＤ＝基本サービス・セット識別子）。ＢＳＳＩＤは、ＬＡＮにおけるＡＰの一意識別子である。ＩＥＥＥ８０２．１１－１９９９　Ｗｉｒｅｌｅｓｓ　ＬＡＮ仕様書が、ＢＳＳＩＤを、インフラストラクチャ・モードにおけるＡＰの局（ＳＴＡ）を識別するＭＡＣアドレスと定義する。このため、ＢＳＳＩＤは、各ＡＰを一意で識別し、このことは、同一のＳＳＩＤを有するＡＰを区別するために不可欠である。

【０１１７】
位置特定サーバ３５は、要求５１０の肯定応答の役割をする応答５１１によって応答する。端末装置１０が、ＳＯＡＰ要求メッセージ５１０を送信してから或る時間内に応答を受信しない場合、端末装置１０は、ＳＯＡＰ要求メッセージ５１０を再送することができる。

【０１１８】
コール・マネージャ４０が、緊急コールに気付くとすぐに、コール・マネージャは、位置特定サーバ３５にポーリング・メッセージ５１２を送信することによって、位置特定サーバ３５に定期的にポーリングすることを開始する。このポーリング・メッセージ５１２は、端末装置１０の位置特定情報と関係する更新情報をコール・マネージャ４０に報告するよう、位置特定サーバ３５をトリガする。位置特定サーバ３５は、常に位置特定情報で応答する。位置特定サーバ３５は、応答５１３を送信することによってポーリング・メッセージ５１２に応答する。応答５１３は、端末装置の位置に関する更新情報、または単に、利用可能な更新情報が存在しないことの指示を含む。コール・マネージャ４０は、単に、取得された位置特定情報をメッセージ５１４としてＰＳＡＰ６０に転送する、あるいは取得された位置特定情報を処理し、次に、処理された位置特定情報をメッセージ５１４としてＰＳＡＰ６０に送信する。

【０１１９】
例えば、位置特定サーバ３５は、例えば、ＬＡＮのＡＰのＢＢＳＩＤと、対応する位置とを含むデータベースを使用して、位置特定情報のＡＰ　ＢＢＳＩＤを地理的座標に変換することができる。次に、コール・マネージャは、これらの地理的座標をＰＳＡＰ６０に送信し、ＰＳＡＰ６０において、示された地理的位置に援助が送られることが可能である。

【０１２０】
図６ｂは、第２の代替の実施形態による端末装置１０の位置特定と関係するメッセージ・フロー・シーケンスを示す。ステップ５２０乃至５２１は、図６ａを参照して説明されるステップ５１０乃至５１１に対応する。前段で与えられた対応する説明は、図６ｂにも当てはまる。

【０１２１】
位置特定サーバ３５が、端末装置１０から位置特定情報、または位置特定情報の更新を受信し、好ましくは、端末装置１０に応答５２１を送信した後、位置特定サーバ３５は、メッセージ５２２によってコール・マネージャ４０に、この位置特定情報をプッシュする。メッセージ５２２に応答して、コール・マネージャ４０は、肯定応答のための応答メッセージ５２３を位置特定サーバ３５に送信する。

【０１２２】
コール・マネージャ４０は、図６ａに関連して前述したとおり、単に、取得された位置特定情報をＰＳＡＰ６０にメッセージ５２４として転送する、または取得された位置特定情報を処理し、次に、処理された位置特定情報をメッセージ５２４としてＰＳＡＰ６０に送信する。

【０１２３】
図６ｃは、第３の代替の実施形態による端末装置１０の位置特定と関係するメッセージ・フロー・シーケンスを示す。この方法の第１のステップで、端末装置１０は、緊急ＳＳＩＤに関連付けられた後、ＡＰ２０を介してコール・マネージャ４０にＳＯＡＰ要求メッセージ５３０を送信する。ＳＯＡＰ要求メッセージ５１０は、端末装置１０の位置特定情報、例えば、端末装置がＬＡＮにアクセスするのを仲介するＡＰ１０のＢＳＳＩＤを含む。
【０１２４】
コール・マネージャ４０は、要求５３０の肯定応答の役割をする応答５３１によって応答する。端末装置１０が、ＳＯＡＰ要求メッセージ５３０を送信してから或る時間内に応答を受信しない場合、端末装置１０は、コール・マネージャ４０にＳＯＡＰ要求メッセージ５３０を再送することができる。
【０１２５】
コール・マネージャ４０が、端末装置１０から位置特定情報、または位置特定情報の更新を受信し、好ましくは、端末装置１０に応答５３１を送信した後、コール・マネージャ４０は、図６ａに関連して前述したとおり、単に、取得された位置特定情報をメッセージ５３２としてＰＳＡＰ６０に転送する、または取得された位置特定情報を処理し、次に、処理された位置特定情報をメッセージ５３２としてＰＳＡＰ６０に送信する。
【０１２６】
図６ｄは、第４の代替の実施形態による端末装置１０の位置特定と関係するメッセージ・フロー・シーケンスを示す。この方法の第１のステップで、端末装置１０は、緊急ＳＳＩＤに関連付けられた後、ＤＨＣＰ更新要求５４０をＤＨＣＰサーバ３０に送信する。ＤＣＨＰ更新要求５４０は、端末装置１０の位置特定情報、例えば、端末装置がＬＡＮにアクセスするのを仲介するＡＰ１０のＢＳＳＩＤを含む。
【０１２７】
さらなる処理に関して、２つのオプションがある。ＤＨＣＰサーバ３０は、ＳＯＡＰメッセージ５４１を位置特定サーバ３５に送信するか、またはＳＯＡＰメッセージ５４６をコール・マネージャ４０に送信する。
【０１２８】
第１の場合、位置特定情報は、前述したとおり、好ましくは定期的なコール・マネージャからのポーリング・メッセージ５４２、および位置特定サーバ３５からの対応する応答５４３によって、または位置特定サーバ３５が、ＳＯＡＰメッセージ５４１を受信するとすぐに、位置特定サーバ３５からコール・マネージャ４０に、メッセージ５４４によって位置特定情報をプッシュすることによって、コール・マネージャ４０に伝送されることが可能である。この場合も、コール・マネージャ４０は、肯定応答５４５でメッセージ５４４に応答することができる。
【０１２９】
コール・マネージャ４０が、位置特定サーバ３５から位置特定情報を受信した後、コール・マネージャ４０は、図６ａに関連して前述したとおり、単に、取得された位置特定情報をメッセージ５４７としてＰＳＡＰ６０に転送する、または取得された位置特定情報を処理し、次に、処理された位置特定情報をメッセージ５４７としてＰＳＡＰ６０に送信する。
【０１３０】
ＤＨＣＰサーバ３０が、ＳＯＡＰメッセージ５４６をコール・マネージャ４０に直接に送信する後者の場合、コール・マネージャ４０は、やはり、取得された元の位置特定情報、または処理された位置特定情報をメッセージ５４７としてＰＳＡＰ６０に転送する。
【０１３１】
説明される方法選択肢および方法オプションは、可能な任意の組み合わせで実行されることが可能である。このため、単一の方法選択肢に関連して説明されるステップは、本発明の目標を実現するのに、別の方法選択肢のステップと組み合わされてもよい。例えば、

請求項１、８、１０、および１３が、互いに組み合わされてもよい。

【図面の簡単な説明】

【０１３２】

【図１】本発明の実施形態によるＬＡＮにアクセスする端末装置を示すブロック図である。

【図２】本発明の実施形態によるＬＡＮにアクセスする端末装置を示すメッセージ・フロー・シーケンスである。

【図３ａ】本発明の実施形態によるルーティング・オプションを示すメッセージ・フロー・シーケンスである。

【図３ｂ】本発明の実施形態によるルーティング・オプションを示すメッセージ・フロー・シーケンスである。

【図３ｃ】本発明の実施形態によるルーティング・オプションを示すメッセージ・フロー・シーケンスである。

【図４】本発明の別の実施形態によるＬＡＮにアクセスする端末装置を示すブロック図である。

【図５】本発明の別の実施形態によるＬＡＮにアクセスする端末装置を示す別のブロック図である。

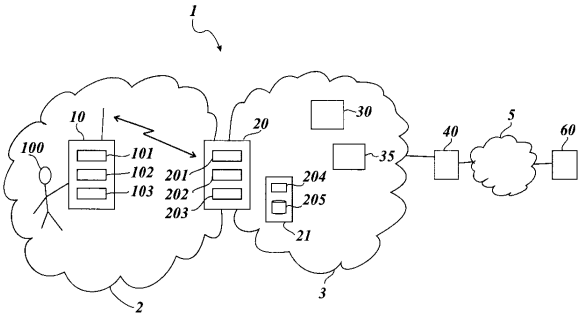
【図６ａ】本発明による位置特定関連のオプションを示すメッセージ・フロー・シーケンスである。

【図６ｂ】本発明による位置特定関連のオプションを示すメッセージ・フロー・シーケンスである。

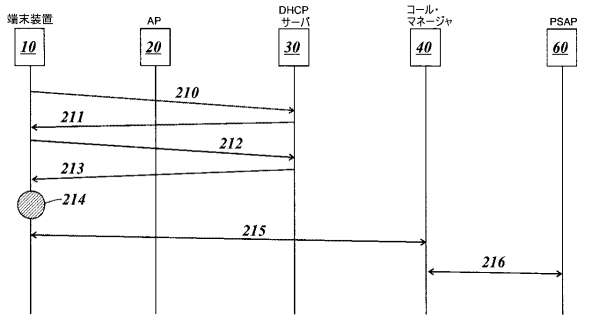
【図６ｃ】本発明による位置特定関連のオプションを示すメッセージ・フロー・シーケンスである。

【図６ｄ】本発明による位置特定関連のオプションを示すメッセージ・フロー・シーケンスである。

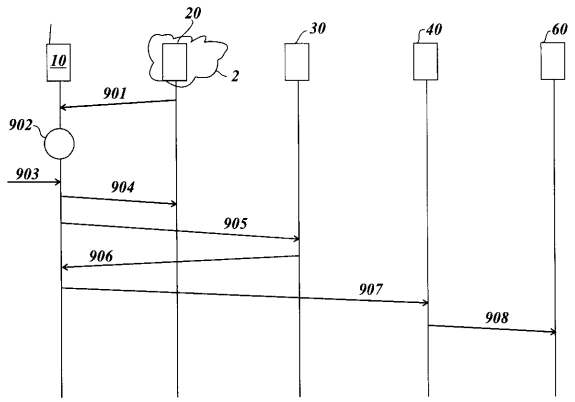
【図１】



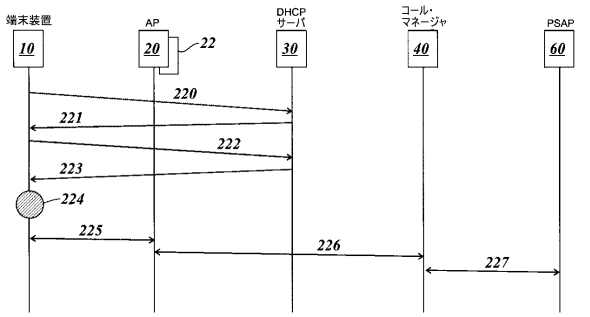
【図３ａ】



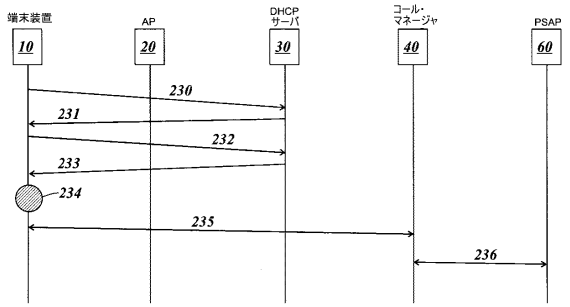
【図２】



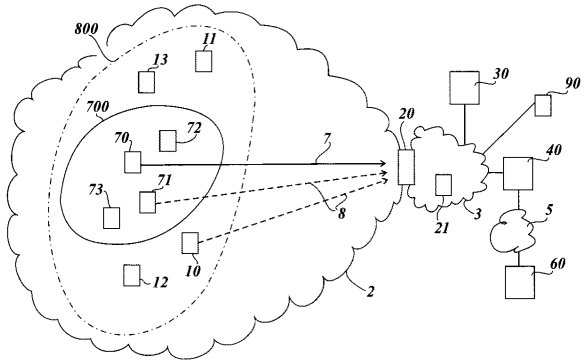
【図３ｂ】



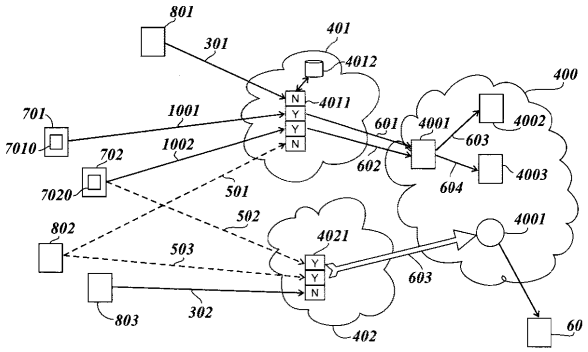
【図３ｃ】



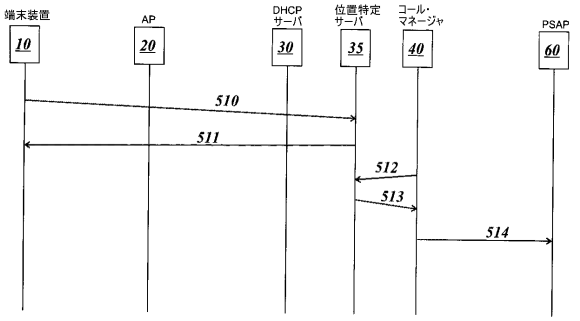
【図４】



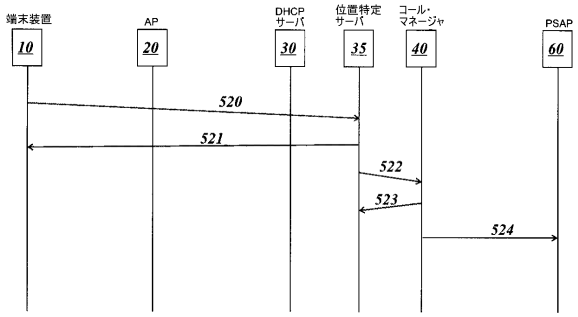
【図５】



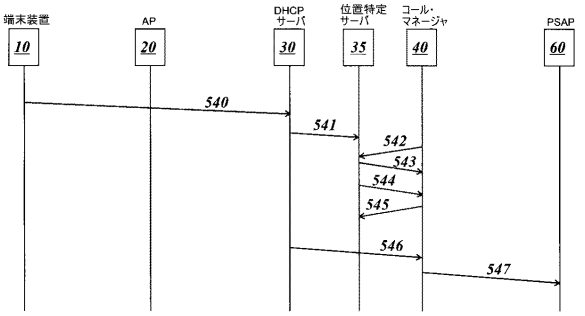
【図６ａ】



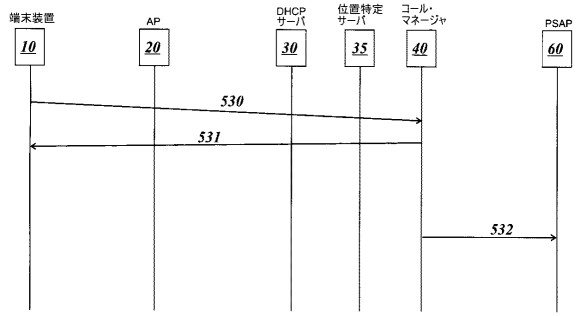
【図６ｂ】



【図６ｄ】



【図６ｃ】



フロントページの続き

(74)代理人 100104352
弁理士 朝日 伸光
(74)代理人 100128657
弁理士 三山 勝巳
(72)発明者 セリグナン，アンーロール
フランス エフー６７０００ ストラスブール，プティ リュ オーステルリッツ ４

審査官 齋藤 哲

(56)参考文献 Vivek Gupta, et al., Proposal for supporting Emergency Services, IEEE 802.11-05/1244r0 0, IEEE, ２００６年 3月, ＵＲＬ, https://mentor.ieee.org/802.11/dcn/06/11-06-0290-00 -000u-proposal-emergency-services.doc
Michael Montemurro, Emergency Services signalling for WLAN, IEEE 802.11-06/0003r0, IEE E, ２００６年 1月, ＵＲＬ, https://mentor.ieee.org/802.11/dcn/06/11-06-0003-00-000u- emergency-services-signaling-for-wlan.ppt
Stefano M. Faccin, et al., WiNOT TGu Proposal for Emergency Services Requirement, IEEE 802.11-06/0288r1, IEEE, ２００６年 3月, ＵＲＬ, https://mentor.ieee.org/802.11/dcn/ 06/11-06-0288-01-000u-emergency-services-requirement.doc

(58)調査した分野(Int.Cl., ＤＢ名)
H04B 7/24-7/26
H04W 4/00-99/00