(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5308459号
(P5308459)
(45)発行日　平成25年10月9日(2013.10.9)　(24)登録日　平成25年7月5日(2013.7.5)

(51)Int.Cl.　　F I
H04W 4/04 (2009.01)　　H04W 4/04 190
H04W 48/06 (2009.01)　　H04W 48/06

請求項の数 35　(全 16 頁)

(21)出願番号　特願2010-548003 (P2010-548003)
(86)(22)出願日　平成21年2月19日(2009.2.19)
(65)公表番号　特表2011-514063 (P2011-514063A)
(43)公表日　平成23年4月28日(2011.4.28)
(86)国際出願番号　PCT/EP2009/001214
(87)国際公開番号　WO2009/106265
(87)国際公開日　平成21年9月3日(2009.9.3)
審査請求日　平成22年8月27日(2010.8.27)
(31)優先権主張番号　08003753.4
(32)優先日　平成20年2月29日(2008.2.29)
(33)優先権主張国　欧州特許庁(EP)

(73)特許権者　504292093
コニンクリーケ・ケイピーエヌ・ナムローゼ・フェンノートシャップ
オランダ国エヌエル－２５１６　シーケイ・ザ・ヘーグ，マーンプレイン　５５
(73)特許権者　508351406
ネダーランゼ・オルガニサティ・フォーア・トゥーゲパスト－ナトゥールヴェテンシャッペリーク・オンデルゾエク・ティーエヌオー
オランダ国　２６２８　フェーカー・デルフト，ショエマカーストラート　９７
(74)代理人　100140109
弁理士　小野　新次郎

最終頁に続く

(54)【発明の名称】電気通信ネットワークおよび時間に基づくネットワーク・アクセス方法

(57)【特許請求の範囲】
【請求項１】
複数の端末にアクセスを提供するように構成される電気通信ネットワークであって、各端末は、当該電気通信ネットワークにアクセスするための一意の識別子を備えており、当該電気通信ネットワークが、
－少なくとも１つの端末の前記一意の識別子を、その間前記端末のアクセスが許可される少なくとも１つのアクセス許可時間間隔と組み合わせて格納するように構成されるレジスタと、
－アクセス要求を受信し、および前記端末から当該電気通信ネットワークにアクセスするために、前記一意の識別子を受信または判定するように構成されるアクセス要求受信機と、
－前記アクセス要求が前記アクセス許可時間間隔外において受信された場合、前記端末のアクセスを拒否するように構成されるアクセス・モジュールと、
を備えており、
前記電気通信ネットワークは、当該電気通信ネットワークのネットワーク負荷を得て、そして監視するように構成されており、当該電気通信ネットワークは、前記端末が前記アクセス許可時間間隔において当該電気通信ネットワークにアクセスできるように、当該電気通信ネットワークが制御情報を前記端末に送信することによって、前記ネットワーク負荷に応じて前記アクセス許可時間間隔を適応させるように構成される、電気通信ネットワーク。

【請求項２】
請求項１記載の電気通信ネットワークにおいて、当該電気通信ネットワークにおける前記ネットワーク負荷が、リアル・タイムに監視され、並びに／または数学的モデルおよび履歴データを用いて予期されるネットワーク負荷に基づく、電気通信ネットワーク。
【請求項３】
請求項１に記載の電気通信ネットワークにおいて、データ転送を直ちに行うことを要求しないマシン・ツー・マシンのアプリケーションが実行され、該アプリケーションを有する前記端末が、ピーク負荷時間中の当該電気通信ネットワークへのアクセスを拒否し、前記アクセス許可時間間隔がピーク負荷時間外である、電気通信ネットワーク。
【請求項４】
請求項１に記載の電気通信ネットワークにおいて、データ転送を直ちに行うことを要求しないマシン・ツー・マシンのアプリケーションが実行され、前記アクセス許可時間間隔がオフ・ピーク間隔であるか、または、当該電気通信ネットワークにより体験され若しくは予期されるネットワーク負荷に応じた可変時間間隔である、電気通信ネットワーク。
【請求項５】
端末の群が規定され、前記オフ・ピーク間隔の特定間隔が割り当てられる、請求項４に記載の電気通信ネットワーク。
【請求項６】
請求項１に記載の電気通信ネットワークにおいて、データ転送を直ちに行うことを要求しないマシン・ツー・マシンのアプリケーションが実行され、該アプリケーションを有する前記端末が、特定の端末または端末のグループに割り当てられる１またはそれ以上のアクセス許可時間間隔を有する、電気通信ネットワーク。
【請求項７】
請求項１に記載の電気通信ネットワークにおいて、当該電気通信ネットワークが、セルラ・ネットワークを備えており、前記レジスタが、前記セルラ・ネットワークにおけるホーム・ロケーション・レジスタまたはホーム加入者サーバである、電気通信ネットワーク。
【請求項８】
請求項１から７のいずれか１項に記載の電気通信ネットワークにおいて、当該電気通信ネットワークは、ネットワーク負荷モニタを備えており、該ネットワーク負荷モニタが当該電気通信ネットワークにおける前記ネットワーク負荷を監視するように構成される、電気通信ネットワーク。
【請求項９】
請求項７に記載の電気通信ネットワークにおいて、当該電気通信ネットワークが、前記セルラ・ネットワークにおける前記ホーム・ロケーション・レジスタまたは前記ホーム加入者サーバからネットワーク負荷情報を得る、電気通信ネットワーク。
【請求項１０】
請求項１から９のいずれか一項に記載の電気通信ネットワークにおいて、前記アクセス・モジュールが当該電気通信ネットワークへのネットワーク・アタッチを拒否するように構成される、電気通信ネットワーク。
【請求項１１】
請求項１から１０のいずれか一項に記載の電気通信ネットワークにおいて、前記アクセス・モジュールが、更に、前記端末の認証を行わずにアクセスを拒否するように構成される、電気通信ネットワーク。
【請求項１２】
請求項１から１１のいずれか一項に記載の電気通信ネットワークにおいて、更に、前記アクセス要求の受信に応答して、前記端末を認証するように構成される認証モジュールを備えており、前記アクセス・モジュールが、更に、前記端末から別のアクセス要求を受信したときに、ネットワーク・アタッチを拒否するように構成される、電気通信ネットワーク。

【請求項１３】
請求項１から１２のいずれか一項に記載の電気通信ネットワークにおいて、当該電気通信ネットワークがサービング・コントローラ・エンティティを備えており、該サービング・コントローラ・エンティティが、前記アクセス要求受信機と前記アクセス・モジュールとを備えており、前記サービング・コントローラ・エンティティが、更に、前記アクセス要求の受信に応答して前記レジスタから前記アクセス許可時間間隔を読み出すように構成されるデータ読み出しモジュールを備えており、前記アクセス・モジュールは、前記アクセス要求が前記読み出されたアクセス許可時間間隔外で受信された場合、前記電気通信ネットワークへのネットワーク・アタッチを拒否する、または前記端末とのパケット・データ・プロトコル・コンテキストを確立するのを拒否するように構成される、電気通信ネットワーク。
【請求項１４】
請求項１から１３のいずれか一項に記載の電気通信ネットワークにおいて、当該電気通信ネットワークが、前記アクセス・モジュールが当該電気通信ネットワークへのアクセスを拒否したことに応答して、アクセス拒否情報を前記端末に送信するように構成されているサービング・コントローラ・エンティティを備えている、電気通信ネットワーク。
【請求項１５】
請求項１から１４のいずれか一項に記載の電気通信ネットワークにおいて、当該ネットワークは、更に、別のネットワークへのゲートウェイを備えており、該ゲートウェイが、前記端末について更なる認証を可能にするように構成される、電気通信ネットワーク。
【請求項１６】
請求項１から１５のいずれか一項に記載の電気通信ネットワークにおいて用いるためのレジスタ。
【請求項１７】
請求項１２または１３に記載の電気通信ネットワークにおいて用いるためのサービング・コントローラ・エンティティ。
【請求項１８】
複数の端末にアクセスを提供するように構成される電気通信ネットワークであって、各端末は、当該電気通信ネットワークにアクセスするための一意の識別子を備えており、当該電気通信ネットワークが、
－少なくとも１つの端末の前記一意の識別子を、その間前記端末のアクセスが拒否される少なくとも１つのアクセス拒否時間間隔と組み合わせて格納するように構成されるレジスタと、
－アクセス要求を受信し、および前記端末から当該電気通信ネットワークにアクセスするために、前記一意の識別子を受信または判定するように構成されるアクセス要求受信機と、
－前記アクセス要求が前記アクセス拒否時間間隔内において受信された場合、前記端末のアクセスを拒否するように構成されるアクセス・モジュールと、
を備えており、
前記電気通信ネットワークは、当該電気通信ネットワークのネットワーク負荷を得て、そして監視するように構成されており、当該電気通信ネットワークは、前記端末が前記アクセス拒否時間間隔において当該電気通信ネットワークへのアクセスを禁止されるように、当該電気通信ネットワークが制御情報を前記端末に送信することによって、前記ネットワーク負荷に応じて前記アクセス拒否時間間隔を適応させるように構成される、電気通信ネットワーク。
【請求項１９】
電気通信ネットワークへのアクセスを制御するコンピュータ実装方法であって、前記電気通信ネットワークが複数の端末にアクセスを許可するように構成されており、各端末が前記電気通信ネットワークにアクセスするための一意の識別子を備えており、前記電気通信ネットワークが、少なくとも１つの端末の前記一意の識別子を少なくとも１つのアクセ

ス許可時間間隔と組み合わせて格納するように構成されているレジスタを備えており、当該方法が、
－前記電気通信ネットワークへのアクセスのために、アクセス要求および前記一意の識別子を前記端末から受信するステップと、
－前記一意の識別子を用いて、前記アクセス許可時間間隔においてアクセスするステップと、
－前記アクセス要求が前記アクセス許可時間間隔外において受信された場合、前記端末の前記電気通信ネットワークへのアクセスを拒否するステップと、
を備えており、更に、
－前記電気通信ネットワークのネットワーク負荷を監視するステップと、
－前記端末が前記アクセス許可時間間隔において当該電気通信ネットワークにアクセスできるように、前記電気通信ネットワークが制御情報を前記端末に送信することによって、前記監視したネットワーク負荷に応じて前記アクセス許可時間間隔を適応させるステップと、
を備えている、方法。
【請求項２０】
請求項１９記載の方法において、前記電気通信ネットワークのネットワーク負荷が、リアル・タイムに監視され、または予期されるネットワーク負荷に基づく、方法。
【請求項２１】
請求項１９に記載の方法において、データ転送を直ちに行うことを要求しないマシン・ツー・マシンのアプリケーションが実行され、前記アクセス許可時間間隔がオフ・ピーク間隔であるか、または、前記電気通信ネットワークにより体験され若しくは予期されるネットワーク負荷に応じた可変時間間隔である、方法。
【請求項２２】
請求項１９に記載の方法において、データ転送を直ちに行うことを要求しないマシン・ツー・マシンのアプリケーションが実行され、該アプリケーションを有する端末についての前記アクセス許可時間間隔が、前記電気通信ネットワークにより体験されまたは予期されるネットワーク負荷に応じてスケジュールされた可変時間間隔ｘ－ｙであり、前記ネットワーク負荷が特定の閾値未満となるか、特定の閾値未満となると予測される場合に、アクセスが前記端末に許可される、方法。
【請求項２３】
請求項１９に記載の方法において、データ転送を直ちに行うことを要求しないマシン・ツー・マシンのアプリケーションが実行され、該アプリケーションを有する前記端末が、特定の端末または端末のグループに割り当てられる１またはそれ以上のアクセス許可時間間隔を有する、方法。
【請求項２４】
請求項１９記載の方法において、前記電気通信ネットワークはセルラ・ネットワークであり、前記レジスタは該セルラ電気通信ネットワークにおけるホーム・ロケーション・レジスタまたはホーム加入者サーバである、方法。
【請求項２５】
請求項１９から２４のいずれか一項に記載の方法において、前記アクセス要求が前記時間間隔外において受信された場合、前記端末の前記電気通信ネットワークへのアクセスを拒否するステップが、前記電気通信ネットワークへのネットワーク・アタッチを拒否することを含む、方法。
【請求項２６】
請求項１９から２５のいずれか１項に記載の方法であって、更に、前記端末の認証を行わずに、前記電気通信ネットワークにおいて前記端末のアクセスを拒否するステップを備えている、方法。
【請求項２７】
請求項１９から２６のいずれか１項に記載の方法であって、更に、

－前記アクセス要求の受信に応答して、前記電気通信ネットワークにおいて前記端末を認証するステップと、
－前記端末から別のアクセス要求を受信したことに応答して、前記端末のネットワーク・アタッチを拒否するステップと、
を備えている、方法。
【請求項２８】
請求項１９に記載の方法であって、更に、
－サービング・コントローラ・エンティティにおいて、前記電気通信ネットワークに対する前記アクセス要求を受信するステップと、
－前記アクセス要求の受信に応答して、前記時間間隔を前記レジスタから前記サービング・コントローラ・エンティティに読み出すステップと、
－前記アクセス要求が前記読み出された時間間隔内で受信された場合、前記端末のネットワーク・アタッチを拒否する、または前記端末のパケット・データ・プロトコル・コンテキストを確立するのを拒否するステップと、
を備えている、方法。
【請求項２９】
請求項２８に記載の方法であって、更に、前記電気通信ネットワークへのアクセスを拒否することに加えて、アクセス拒否情報を前記端末に送信するステップを備えている、方法。
【請求項３０】
請求項２８に記載の方法であって、更に、前記アクセス許可時間間隔中における別のネットワークへのアクセスのために前記端末を認証するステップを備えている、方法。
【請求項３１】
電気通信ネットワークへのアクセスを制御するコンピュータ実装方法であって、前記電気通信ネットワークが複数の端末にアクセスを許可するように構成されており、各端末が前記電気通信ネットワークにアクセスするための一意の識別子を備えており、前記電気通信ネットワークが、少なくとも１つの端末の前記一意の識別子を少なくとも１つのアクセス拒否時間間隔と組み合わせて格納するように構成されているレジスタを備えており、当該方法が、
－前記電気通信ネットワークへのアクセスのために、アクセス要求および前記一意の識別子を前記端末から受信するステップと、
－前記一意の識別子を用いて、前記アクセス拒否時間間隔においてアクセスするステップと、
－前記アクセス要求が前記アクセス拒否時間間隔内において受信された場合、前記端末の前記電気通信ネットワークへのアクセスを拒否するステップと、
を備えており、更に、
－前記電気通信ネットワークのネットワーク負荷を監視するステップと、
－前記端末が前記アクセス拒否時間間隔において前記電気通信ネットワークへのアクセスが禁止されるように、前記電気通信ネットワークが制御情報を前記端末に送信することによって、前記監視したネットワーク負荷に応じて前記アクセス拒否時間間隔を適応させるステップと、
を備えている、方法。
【請求項３２】
電気通信ネットワークへのアクセスを制御するためのコンピュータ・プログラムであって、電気通信ネットワークにおいて起動すると、請求項１９から３１のいずれか１項に記載の方法を実行するように構成されるソフトウェア・コード部を備えている、コンピュータ・プログラム。
【請求項３３】
請求項３２記載のコンピュータ・プログラムを収容する担体。
【請求項３４】

請求項１から１５のいずれか１項に記載の電気通信ネットワークにおいて用いるための端末であって、前記電気通信ネットワークからのメッセージを受信するように構成されているメッセージ受信機を備えており、前記メッセージが、前記アクセス許可時間間隔に関する情報を備えており、前記端末が、更に、前記アクセス許可時間間隔にしたがって、前記アクセス要求を前記電気通信ネットワークに送信するように構成されているアクセス要求モジュールを備えている、端末。

【請求項３５】

請求項１８記載の電気通信ネットワークにおいて用いるための端末であって、前記電気通信システムからのメッセージを受信するように構成されているメッセージ受信機を備えており、前記メッセージが、前記アクセス拒否時間間隔に関する情報を備えており、前記端末が、更に、前記アクセス拒否時間間隔にしたがって、前記アクセス要求を前記電気通信ネットワークに送信するように構成されているアクセス要求モジュールを備えている、端末。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、電気通信の分野に関するものである。特に、本発明は、電気通信ネットワーク、および当該電気通信ネットワークへのアクセスを許可する方法に関するものである。

【従来技術】

【０００２】

過去数十年において、電気通信ネットワークのデータ容量に対する要求が益々増大してきている。電気通信提供事業者は、ＧＰＲＳのようなＧＳＭサービスおよび３Ｇサービスを拡張して提供するために、彼らのネットワークを適応させ、彼らの顧客の要求を満たすように更に多くのサービスを提供し続けている。

【０００３】

電気通信提供事業者は、ネットワーク・リソースを効率的に使用するために、彼らの顧客のふるまいに影響を及ぼす取り組みを行ってきた。一例として、移動体データ契約は、今日では多くの場合、ボリュームに基づく課金を用いて提供されており、ボリューム上限と組み合わせることもある。これによってネットワークを通じて送信するデータ量を、顧客に考慮させる。しかしながら、クライアントのふるまいおよび／または端末データ送信の制御、つまり、ネットワーク・リソースの使用が、なおも制限されていることには変わりない。

【発明の概要】

【発明が解決しようとする課題】

【０００４】

当技術分野では、電気通信ネットワーク、およびネットワーク・リソースの使用を取り締まる方法を改良することが求められている。

【課題を解決するための手段】

【０００５】

複数の端末に通信アクセスを提供するように構成された電気通信ネットワークを提案する。各端末は、この電気通信ネットワークにアクセスするための一意の識別子を備えている。この一意の識別子は、好ましくは、端末の加入、例えば、端末において利用可能なＳＩＭ（ＩＭＳＩ）の識別子と関連付けられている。電気通信ネットワークは、レジスタと、アクセス要求受信機と、アクセス・モジュールとを備えている。レジスタは、少なくとも１つの端末についての一意の識別子を、端末のアクセスが許可される、少なくとも１つのアクセス許可時間間隔、またはそれと同等のものと組み合わせて格納するように構成されている。アクセス要求受信機は、電気通信ネットワークにアクセスするためのアクセス要求を、端末から受信するように構成されている。アクセス要求は、一意の識別子またはテンポラリな識別子を含むことができる。アクセス・モジュールは、アクセス要求が前述の時間間隔またはそれと同等のもの以外で受信された場合、端末のアクセスを拒否するよ

うに構成されている。

【０００６】

このようなネットワークにおいて用いるためのレジスタおよびサービング・コントローラ・エンティティも提案する。

また、電気通信ネットワークへのアクセスを制御するコンピュータ実装方法も提案する。電気通信ネットワークは、複数の端末にアクセスを許可するように構成されており、各端末が電気通信ネットワークにアクセスするための一意の識別子を備えている。電気通信ネットワークは、少なくとも１つの端末の一意の識別子を少なくとも１つのアクセス許可時間間隔、またはそれと同等のものと組み合わせて格納するように構成されているレジスタを備えている。電気通信ネットワークへのアクセスのために、アクセス要求を前記端末から受信する。アクセス要求は、一意の識別子またはテンポラリな識別子を含むことができる。別のステップでは、一意の識別子を用いて、端末のアクセス許可時間間隔を検証する。アクセス要求が前記時間間隔以外で受信された場合、前記端末の前記電気通信ネットワークへのアクセスを拒否する。

【０００７】

また、前述の方法を実行するように構成されたプログラム・コード部を備えているコンピュータ・プログラム、およびこのようなコンピュータ・プログラムのための担体(carrier)も提案する。

前述のシステムおよび方法において用いるための端末も提案する。

【０００８】

尚、アクセス許可時間間隔と同等のものについては、電気通信ネットワークへのアクセスのためのアクセス要求を拒否すべき時間間隔を特定するアクセス拒否時間間隔を含むことは認められてしかるべきである。

【０００９】

アクセス要求は、回線交換アクセス要求、パケット交換アクセス要求、または組み合わせた要求であってもよい。

電気通信ネットワークにアクセスするステップは、例えば、３ＧＧＰ ＴＳ ２３．０６０（リリース７）において標準化されている。尚、電気通信ネットワークへのアクセスは、種々のアクセス・フェーズにおいて拒否できることは認められてしかるべきである。ネットワーク・アクセスを要求する第１フェーズは、通例、数個のステップを備えているネットワーク・アタッチ・プロシージャを伴う。好ましくは、電気通信ネットワークへのアクセスは、端末のネットワーク・アタッチを拒否することで拒否する。このフェーズにおいて拒否することにより、リソースの節約を最適化することが可能となる。

【００１０】

別のネットワーク・アクセス・フェーズは、ＰＤＰコンテキストの確立を伴う。ＰＤＰコンテキストの確立を拒否することもできる。前出のネットワーク・アタッチは既にネットワーク・リソースの使用を伴うが、ＰＤＰコンテキストの確立を禁止すると、電気通信ネットワークの事実上の使用を防止し、したがってリソースを節約することになる。尚、電気通信ネットワークへのアクセスのためというような、運用事業者によって決定される禁止事項（ＯＤＢ）は、既に３ＧＧＰ ＴＳ ２３．０１５、Ｖ．７．０．０に記載されている。禁止事項を可能にすることにより、ネットワーク運用事業者は、ある加入者の特定の宛先へのアクセスを拒否することができるようになる。

【００１１】

特定の端末または端末のグループに対して、電気通信ネットワークへのアクセスを許可する時間間隔を１つ以上指定する選択肢を設けることによって、ネットワーク・リソースの使用についてのネットワーク運用事業者の計画および制御が容易になる。時間間隔中にアクセスを拒否または遮断することは、種々の状況において有利であることを証明することができる。具体的には、マシン・ツー・マシン（Ｍ２Ｍ）アプリケーションには、データ転送を直ちに行う必要がないものもある。これらのアプリケーションが、例えば、ピーク負荷時間中に１つ以上のネットワーク・リソースを請求することを禁止されると、ネッ

トワーク・リソースを節約することができる。このような加入(subscription)は、例えば、加入料金を割引して提供するとよい。

【００１２】

Ｍ２Ｍアプリケーションは、通例、数百または数千ものデバイスを伴うが、これらのデバイスは希にしか電気通信ネットワークへのアクセスを要求しない。一例では、大規模顧客基地(large customer base)の家庭における、例えば、電気メータの電子的読み取りに関与する。

【００１３】

請求項２および１３の実施形態は、端末の識別子（１つまたは複数）および関連付けられた時間間隔（１つまたは複数）の組み合わせを利用可能にするために、電気通信ネットワークにおける適した場所を規定する。

【００１４】

請求項３および１４の実施形態は、電気通信ネットワークへのアクセスを許可／禁止する動的時間間隔（ならびに仮想および暗示的な時間間隔も可能）を規定する。これらの実施形態は、ネットワーク・リソースの最小限の使用に寄与する。

【００１５】

請求項４および１５の実施形態は、ネットワーク・リソースの使用改善に備える。

請求項５および１６の実施形態は、ネットワーク・リソースの使用改善に備える。

請求項６および１７の実施形態は、端末にアクセス許可時間間隔を通知する選択肢を設ける。このような情報は、問題の端末のみに送信すべきである。更に、１回の認証のみを許可することによって、ネットワーク・リソースを節約し、端末の電力を節約する。

【００１６】

請求項７および１８の実施形態は、電気通信ネットワークへのアクセスを許可するか否かについての判断（ネットワーク・アタッチまたはＰＤＰコンテキストの確立のいずれか）が、電気通信ネットワークの下位レベル、例えば、ＳＧＳＮに組み込まれ、ネットワーク・リソースの消費を削減することを確保する。アクセス許可時間規則をRADIUSサーバにおいて実施するというような、他の解決策では、様々なネットワーク機能、移動性管理、およびパケット・データ・プロトコル（ＰＤＰ）コンテキストの設定が必要となり、このため、アクセス許可時間間隔以外で端末が電気通信ネットワークにアクセスしたと判断した場合には、ネットワーク・リソースを不必要に消費する。

【００１７】

請求項８および１９の実施形態は、情報を端末に送信することを可能にする。このような情報は、適用可能なアクセス許可時間間隔に関する情報を含むことができる。可能性としては、この情報は、端末動作を制御するための制御情報を含むことができる。制御情報は、例えば、ネットワーク負荷が低いと予測される時間間隔中にログインするように、端末を制御することができる。好ましくは、この端末に対して認証手順を実行する。

【００１８】

請求項９および２０の実施形態は、アクセス許可時間間隔中において、より高いレベルでの認証、例えば、ＧＧＳＮを規定する。

以後、本発明の実施形態について更に詳しく説明する。しかしながら、これらの実施形態は、本発明の保護範囲を限定するように解釈してはならないことは、認められてしかるべきである。

【図面の簡単な説明】

【００１９】

【図１】図１は、本発明の一実施形態による電気通信ネットワークの模式図である。

【図２】図２は、図１の電気通信ネットワークのＨＬＲ、ＳＧＳＮ、およびＧＧＳＮを示す。

【図３Ａ】図３Ａは、図１の電気通信システムを用いる方法の種々の時間図を示す。

【図３Ｂ】図３Ｂは、図１の電気通信システムを用いる方法の種々の時間図を示す。

【図３Ｃ】図３Ｃは、図１の電気通信システムを用いる方法の種々の時間図を示す。

【図３Ｄ】図３Ｄは、図１の電気通信システムを用いる方法の種々の時間図を示す。
【図４】図４は、図１の電気通信ネットワークと共に用いる端末の模式図を示す。
【発明を実施するための形態】
【００２０】
図１は、パケット・サービス電気通信ネットワーク１を、データ通信のためにこの電気通信ネットワーク１にアクセスすることができる複数の端末Ａ～Ｄと組み合わせた模式図を示す。
【００２１】
電気通信ネットワーク１は、基地送受信局３を含む無線アクセス・ネットワーク２と、基地局コントローラ４とを備えている。無線アクセス・ネットワークは、移動体コア・ネットワークに接続されている。移動体コア・ネットワークは、サービング・コントローラ・エンティティ５、レジスタ６、および別のネットワーク８へのアクセスを提供するゲートウェイ７を含む。
【００２２】
サービング・コントローラ・エンティティ５は、サービングＧＰＲＳサポート・ノード（ＳＧＳＮ）または他のエンティティとすることができる。ＳＧＳＮ５は、電気通信ネットワーク１と端末Ａ～Ｄとの間の接続を制御する。尚、電気通信ネットワークは複数のＳＧＳＮを含むこともでき、ＳＧＳＮの各々は、通例、基地局コントローラ３に接続されて、これらが数カ所の基地局３を通じて端末にパケット・サービスを提供できるようになっていることは認められてしかるべきである。
【００２３】
レジスタ６は、ホーム・ロケーション・レジスタ（ＨＬＲ）、または別のレジスタ（ＩＭＳ用ホーム加入者サーバといった）とすることができる。
ゲートウェイ７は、例えば、インターネットに通ずるＧＰＲＳゲートウェイ・サポート・ノード（ＧＧＳＮ）とすることができる。その他の外部ネットワークには、企業内ネットワークまたは運用事業者の別のネットワークが含まれる。ＧＧＳＮ７は、コア・ネットワークを通じて、ＳＧＳＮ５に接続されている。
【００２４】
端末Ａ～Ｄが電気通信ネットワーク１にアクセスするには、多数のアクセス・フェーズを要する。
第１フェーズでは、端末Ａ～Ｄが電気通信ネットワーク１に対してアタッチを行うフェーズを伴う。このフェーズでは、種々の通信ステップが実行され、３ＧＧＰ　ＴＳ　２３．０６０（リリース７）において例示されるような、認証ステップが含まれる。認証ステップは、セキュリティ機能を実行し、認証トリプレット（ＧＰＲＳの場合）またはクインテット（ＵＭＴＳの場合）の交換を必要とする。
【００２５】
続くフェーズでは、電気通信ネットワーク１を通じてトラフィック・フローを搬送するために、パケット・データ・プロトコル（ＰＤＰ）コンテキストを確立することができる。ＰＤＰコンテキストは、通例、端末ＡとＳＧＳＮ５との間に設けられる無線アクセス・ベアラと、ＳＧＳＮ５とＧＧＳＮ７との間に設けられるパケット交換データ・チャネルまたはトンネルとを含む。次いで、端末Ａと相手側との間のセッションは、確立されたＰＤＰコンテキスト上で伝えられる。ＰＤＰコンテキストは、１つよりも多いトラフィック・フローを搬送することができるが、１つの特定のＰＤＰコンテキストの中にある全てのトラフィック・フローは、電気通信ネットワーク１を通じたそれらの送信に関する場合と同様に扱われる。
【００２６】
動作において、端末Ａは、ネットワーク・アタッチ・フェーズの後、ネットワークにおいてＰＤＰコンテキストを活性化することを要求するメッセージにおいて、ある外部ネットワーク８に対する基準点の選択のためのアクセス・ポイント名（ＡＰＮ）を示すことができる。ＳＧＳＮ５は、例えば、端末Ａによって与えられるアクセス・ポイント名または

ＳＧＳＮ５が知っているデフォルトＧＧＳＮにしたがって選択されたＧＧＳＮ７に、ＰＤＰコンテキスト作成要求を送ることができる。続いて、端末Ａおよび加入者アクセス・ポイントをサーブするＧＧＳＮ７によって用いられる、ＳＧＳＮ５におけるＰＤＰコンテキスト・データ構造を割り当てることによって、ＰＤＰコンテキストが活性化される。このデータ構造は、端末ＡのＩＰアドレス、端末ＡのＩＭＳＩ、ならびにＳＧＳＮ５およびＧＧＳＮ７双方におけるトンネルＩＤを含む。トンネルＩＤは、ＧＧＳＮ７によって割り当てられた番号であり、特定のＰＤＰコンテキストに関するデータを識別する。

【００２７】

通信セッションの間、ＳＧＳＮ５によって種々の機構(feature)を制御することができる。この制御は、加入と関連付けられＨＬＲ６に格納されている情報に基づくことができる。この情報は、ＳＧＳＮレベルでの制御を可能にするために、ＨＬＲ６からＳＧＳＮ５に読み出すことができる。

【００２８】

具体的には、これより図２を参照すると、ＨＬＲ６は、端末Ａ～Ｄ毎の加入と関連のある一意の識別子、例えば、端末Ａ～ＤのＳＩＭに格納されているＩＭＳＩを含む。各端末Ａ～Ｄには、電気通信ネットワーク１へのアクセスが許可される時間間隔が割り当てられている。

【００２９】

この例では、端末ＡおよびＢには、０８００～１１００ｐｍの間にアクセスが許可される。端末Ｃには、００００～０５００ａｍの間にアクセスが許可される。これらの時間間隔は、通例、１年の内の殆どの日におけるオフ・ピーク間隔である。端末群を定め、オフピーク時間の特定の間隔をこれらに割り当てることができる。端末Ｄには、電気通信ネットワーク１が体験したネットワーク負荷または電気通信ネットワーク１に予期されるネットワーク負荷に応じて、可変時間間隔ｘ－ｙがスケジューリングされる。ネットワーク負荷が特定の閾値未満に低下する場合、または低下することが予期される場合、端末Ｄにアクセスが許可される。

【００３０】

勿論、時間間隔は、電気通信ネットワーク１へのアクセスが拒否されるタイム・スロットに関係してもよい。即ち、アクセス拒否時間間隔でもよい。多数の時間間隔を１つの端末に割り当てることもできる。

【００３１】

電気通信ネットワーク１のリソース使用を制御するために、ＳＧＳＮ５は、以下で更に詳しく説明する動作を実行する数個のモジュールを含む。尚、これらのモジュールの内１つ以上は、プロセッサ（図示せず）上で実行するソフトウェア・モジュールとして実現してもよいことは、注記してしかるべきである。ＳＧＳＮ５は、更に、当業者には一般的に知られている態様でこれらの動作を実行するために、メモリおよびストレージ（図示せず）も含む。

【００３２】

ＳＧＳＮ５は、電気通信ネットワーク１へのアクセスのためのアクセス要求を端末Ａ～Ｄから受信するように構成されているアクセス要求受信機２０を備えている。端末のアクセス要求は、この端末において利用可能なＳＩＭのＩＭＳＩを含む。

【００３３】

ＳＧＳＮ５は、ある端末に対して許可されるアクセス時間間隔（１つまたは複数）以外（またはアクセス拒否間隔内）でアクセス要求が受信された場合に、その端末の電気通信ネットワーク１に対するアクセスを拒否するように構成されているアクセス・モジュール２１を有する。アクセス拒否は、ネットワーク・アタッチまたはＰＤＰコンテキストの確立に関係付けることができる。

【００３４】

更に、ＳＧＳＮ５は、データ読み出しモジュール２２を備えている。データ読み出しモジュール２２は、ＨＬＲ６からデータを読み出すように構成されており、具体的には、こ

のデータは該当するアクセス許可時間間隔であり、その間隔内でアクセス要求が受信され、端末Ａ～Ｄと関連のあるアクセス許可時間間隔である。しかしながら、ＳＧＳＮ５自体を特定の端末に関して予め構成しておき、したがってこれらの端末についてアクセス許可時間間隔（１つまたは複数）を既に備えていてもよいことは認められてしかるべきである。これは、特に、固定端末には有用となる場合がある。

【００３５】

また、ＳＧＳＮ５は、ＰＤＰコンテキスト確立モジュール２３、および認証部２４も備えている。

また、ＳＧＳＮ５は、電気通信ネットワーク１のネットワーク負荷を監視するように構成されているネットワーク負荷モニタ２５も有することができる。ネットワーク負荷情報は、他の情報源、例えば、電気通信ネットワーク１の他のＳＧＳＮまたはＨＬＲから得ることもできる。ネットワークの監視は、リアル・タイムでもよく、および／またはしかるべき負荷予測を得るために数学的モデルおよび履歴データを用いる、予測ネットワーク負荷に基づいてもよい。

【００３６】

これより、電気通信ネットワーク１、特にＳＧＳＮ５の動作について、図３Ａ～図３Ｄを参照しながら説明する。

図３Ａにおいて、ＳＧＳＮ５のアクセス要求受信機２０が、ステップ３０において、端末Ａからのアタッチ要求を０７００ｐｍに受信する。このアタッチ要求を処理できるためには、ＳＧＳＮはその端末において利用可能なＳＩＭのＩＭＳＩを必要とする。アタッチ要求は、このＩＭＳＩまたはＳＧＳＮによって端末Ａに割り当てられたＰ－ＴＭＳＩを含む場合がある。Ｐ－ＴＭＳＩは、セキュリティの理由から、無線経路を通じたＩＭＳＩの送信をできるだけ防止するために用いられる。端末Ａによって供給されたＰ－ＴＭＳＩがＳＧＳＮにおいて分かった場合、ＳＧＳＮはこのＩＭＳＩを得ることができる。あるいは、端末Ａによって供給されたが（新たな）ＳＧＳＮには知られていないＰ－ＴＭＳＩの場合、この新たなＳＧＳＮが要求すれば、古いＳＧＳＮまたは端末自体のいずれかによってＩＭＳＩが供給される。ＩＭＳＩは、データ読み出しモジュール２２が、ステップ３１においてアクセス許可時間間隔（０８００～１１００ｐｍ）をＨＬＲ６からＳＧＳＮ５に読み出すために用いられる。

【００３７】

アクセス許可時間間隔は、種々の方法で、ＨＬＲ６からＳＧＳＮ５に伝達することができる。

アタッチ要求３０に続いて、通例、ステップ３１において認証チェックが行われる。アクセス許可時間間隔は、認証トリプレットまたはカルテットと共に、ＳＧＳＮ５に送信することができる。

【００３８】

ネットワーク・アタッチ・フェーズの認証手順に続いて、通例、位置更新手順が行われる。最初に、位置更新要求３２がＳＧＳＮ５からＨＬＲ６に送信される。また、アクセス許可時間間隔も、ＨＬＲ６からの次の加入者データ挿入メッセージにおいてＳＧＳＮ５に送信することができる（ステップ３３）。ネットワーク・アタッチ・フェーズは、端末Ａへのアタッチ受入メッセージによって終了する（ステップ３４）。

【００３９】

ネットワーク・アタッチ・フェーズ（直前のパラグラフにおいて述べたステップ以外のステップを含む場合もある）を終了した後、ＰＤＰコンテキストを確立する。端末Ａは、ＰＤＰコンテキスト活性化要求３５において、ＰＤＰコンテキストの確立を要求する。

【００４０】

アクセス許可時間間隔を得る態様には関係なく、ＳＧＳＮ５のアクセス・モジュールは、アクセス要求がアクセス許可時間間隔以外で受信されたと判断する。その結果、ＰＤＰコンテキストは確立されない（ステップ３６において、ばつ印で示す）。ステップ３７において、端末Ａに拒否の通知がされる。

【００４１】
尚、ＳＧＳＮ５の認証部２４は、以上の状況において、端末Ａが認証されていてもいなくてもよいことを注記しておく。認証が要求されるのは、アクセス許可時間間隔が、位置更新メッセージ３２に応答してＨＬＲ６からＳＧＳＮ５に送信される場合である。しかしながら、アクセス許可時間間隔がＳＧＳＮ５において認証トリプレット／カルテットと共に得られた場合、認証を完了すべきでない。認証が優先されるのは、端末Ａへの拒否メッセージ３７が、アクセス許可時間間隔に関する情報を含む場合である。
【００４２】
ＳＧＳＮ５は、失敗したアクセス要求のデータを備えているか、または入手して維持する。これは、例えば、時間間隔を端末ＡのＩＭＳＩと組み合わせて格納することによって、または何らかの時間指示と組み合わせて一時的に端末Ａにフラグを立てることによって行うことができる。
【００４３】
枠０８００～１１００ｐｍ以外の時点における別のアクセス要求（ステップ３８）が、再度端末ＡのＩＭＳＩを含むか、またはこのアクセス要求の後に端末ＡのＩＭＳＩが続く場合、このアクセス要求を直接拒否することができる（ステップ３９）。この場合も、再度認証は行われない。
【００４４】
図３Ｂにおいて、端末Ａのネットワーク・アタッチが、０９００ｐｍにおいて受信される。ステップ４０～４５は、ステップ３０～３５に対応する。ネットワーク・アタッチ要求は、ここでは、端末Ａのアクセスのために割り当てられた時間間隔内であるので、アクセス・モジュール２１はＳＧＳＮ５のＰＤＰコンテキスト確立モジュール２３を制御して、端末ＡとのＰＤＰコンテキストを確立し、更にＧＧＳＮ７とのＰＤＰトンネルを確立する。具体的には、そういうものとして知られている態様で、ステップ４６はＰＤＰコンテキスト作成要求と関わりがあり、ステップ４７はＰＤＰコンテキスト作成応答と関わりがある。ステップ４８において、ＰＤＰコンテキスト活性化受入メッセージによって、端末Ａに通知する。すると、端末Ａは、例えば、別のネットワーク８におけるRADIUSサーバを用いて、別の認証手順に従うことができる（ステップ４９）。
【００４５】
ＳＧＳＮ５のネットワーク負荷監視モジュール２５は、電気通信ネットワーク１の（一部の）ネットワーク負荷を監視するか、または予測ネットワーク負荷を出力することができる。特定の時点または時間間隔における低ネットワーク負荷状況の存在を評価するために、ネットワーク負荷を負荷閾値と比較することができる。
【００４６】
図３Ｃにおいて、ステップ５０～５３は図３Ａのステップ３０～３３に対応する。端末Ｄの認証を実行し、ステップ５４において、低ネットワーク負荷が予期される時間間隔ｘ－ｙを端末Ｄに通知する。この情報は、端末Ｄがこのような低ネットワーク負荷時間間隔において電気通信ネットワーク１に再度アクセスする（ステップ５５）ように、端末Ｄを制御する制御情報を含む。ＰＤＰコンテキストを直ちに設定することができ（ステップ５６～５８）、RADIUSサーバへのアクセスが許可される。
【００４７】
前述のように、電気通信ネットワーク１へのアクセスの拒否は、ネットワーク・アタッチの間に行うことが好ましい。図３Ｄは、ステップ６０において、ＩＭＳＩを含む、端末Ａのネットワーク・アタッチ・メッセージを示す。次いで、認証手順が実行され（ステップ６１）、その間にアクセス許可時間間隔がＳＧＳＮ５において受け取られる。アクセス許可時間間隔およびＩＭＳＩは、ＳＧＳＮ５に格納される。あるいは、アクセス許可時間間隔は、位置更新手順（ステップ６２および６３）において得られる。ステップ６４において、ネットワーク・アタッチを拒否する。
【００４８】
前述のように、ＳＧＳＮ５は、それ自体が、端末Ａのアクセス許可時間間隔に関して予

め構成されている情報を備えることができる。あるいは、ステップ６１において、ＳＧＳＮは認証部２４を用いて端末Ａを認証し、アクセス許可時間間隔に関する情報を端末Ａに提供する。

【００４９】

図４は、端末Ａの模式図を示す。端末Ａは、電気通信ネットワーク１と通信するための送受信モジュール７０を備えている。更に、端末Ａはアクセス要求モジュール７１を有する。アクセス要求モジュールは、電気通信ネットワーク１から送受信モジュール７０を介してアクセス許可時間間隔に関する情報を受信し、アクセス許可時間間隔内の時点においてのみアクセス要求を電気通信ネットワークに送信するように構成されている。

【００５０】

尚、前述の電気通信ネットワークおよびシステムは、リソースを節約するには特に適していることは注記してしかるべきである。端末へのアクセスのふるまいに影響を及ぼす手法は他にもあり得るが、これらの方が浪費するリソースが多いと考えられる。

【００５１】

一例として、ネットワーク提供事業者は、ネットワークへのアクセスを全ての時点で許可するが、オフ・ピーク時間以外に送られたデータについては（非常に）高い料金を徴収することもできる。これは、ユーザがネットワークへの接続（即ち、ＰＤＰコンテキスト）を取り外す(tear down)ためのインセンティブにはならない。これは、料金の高いピーク時間中はデータを送らない動機を与えるに過ぎない。しかしながら、アクティブなＰＤＰコンテキストは、ＩＰアドレスを要求するだけでなく、移動体無線機およびコア・ネットワークにおいて多量のリソースを消費していることには変わりない。また、端末をネットワークにアタッチすることも要求しており、あらゆる種類の移動体管理機構が所定の位置になければならないことを意味する。更に、この解決策では、ある時点では料金を割増して課金することを可能にする、更に複雑な課金体系が必要となる。

【００５２】

別の例をあげるとすると、RADIUSサーバにおいてピーク時間中は原則的に端末へのアクセスを遮断することを含む。しかしながら、RADIUSサーバによってアクセスが遮断される前に、ネットワーク・リソースは既に消費されている。端末は、既にネットワークにアタッチすることを許可されており、ＳＧＳＮがＨＬＲから情報を既に読み出しており、移動体管理機能を実行していることを意味する。また、端末はＰＤＰコンテキストを確立することも許可されている。RADIUSサーバが外部データ・ネットワークへのアクセス要求を拒否すると、ＧＧＳＮはＰＤＰコンテキストを受け入れず、トンネルは解体される。しかしながら、ネットワークへのアタッチは、追加措置を講じなければ、継続する。

【図１】

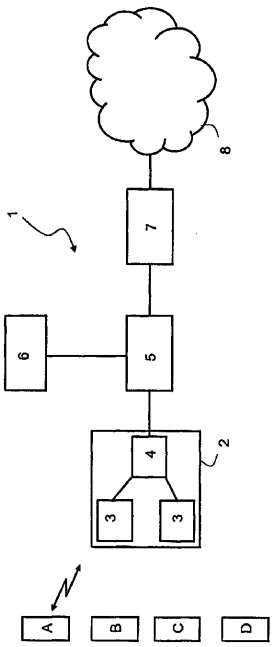

FIG. 1

【図２】

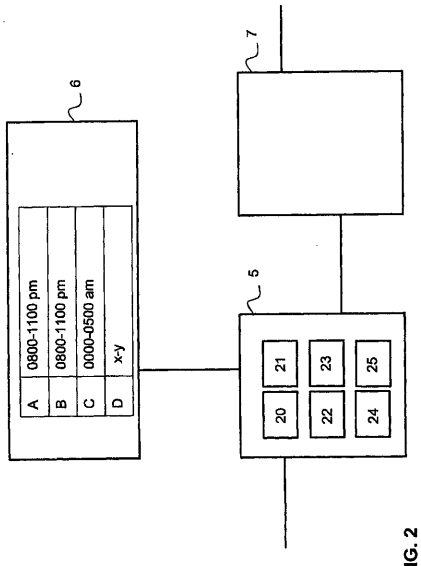

FIG. 2

【図３Ａ】

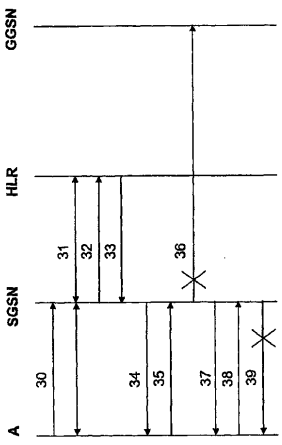

FIG. 3A

【図３Ｂ】

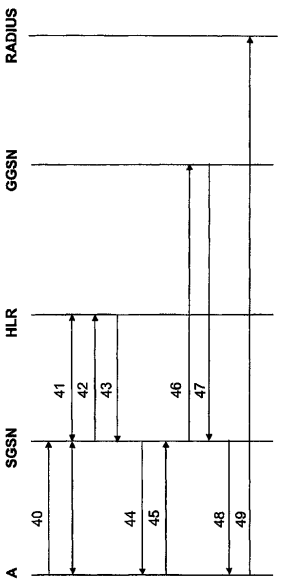

FIG. 3B

【図３Ｃ】

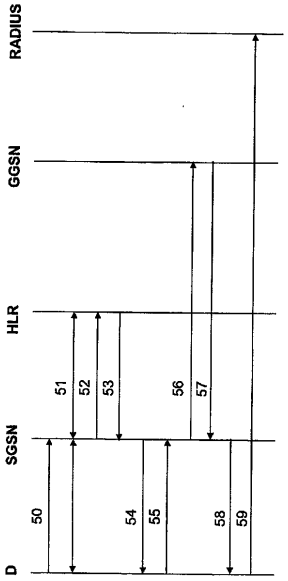

FIG. 3C

【図３Ｄ】

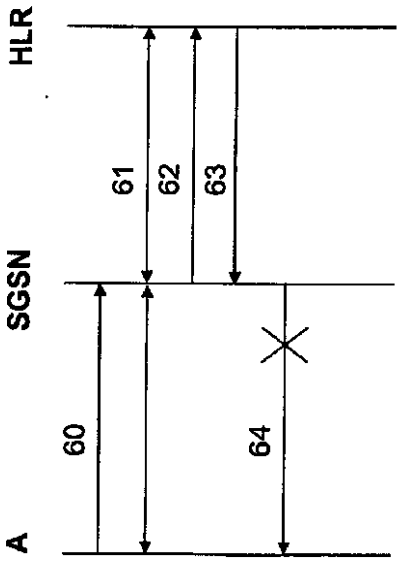

FIG. 3D

【図４】

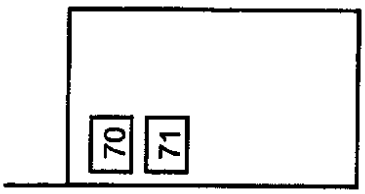

FIG. 4

フロントページの続き

(74)代理人 100089705
弁理士 社本 一夫
(74)代理人 100075270
弁理士 小林 泰
(74)代理人 100080137
弁理士 千葉 昭男
(74)代理人 100096013
弁理士 富田 博行
(74)代理人 100153028
弁理士 上田 忠
(72)発明者 ヴァン・ルーン, ヨハネス・マリア
オランダ国 ２７１９イェーエー ズーテメール, マコレハウト ３１
(72)発明者 シェンク, ミシェール・ロベルト
オランダ国 ２５１３ベーゼット ザ・ハーグ, クライネ・ノベルストラート ２８

審査官 齋藤 哲

(56)参考文献 特開２００２－０１６９７６（ＪＰ，Ａ）
特開２００７－１３５１９４（ＪＰ，Ａ）
特表２００３－５３３０７７（ＪＰ，Ａ）
特開２００５－０１２８０６（ＪＰ，Ａ）
特開２００６－１９７１３７（ＪＰ，Ａ）

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