

(19) 日本国特許庁 (JP)

(12) 特 許 公 報 (B2)

(11) 特許番号

特許第4638408号
(P4638408)

(45) 発行日 平成23年2月23日 (2011.2.23)

(24) 登録日 平成22年12月3日 (2010.12.3)

(51) Int. Cl.

F I

H O 4 W 4/02 (2009.01)

H O 4 Q 7/00 1 O 4

H O 4 M 11/00 (2006.01)

H O 4 M 11/00 3 O 2

請求項の数 33 (全 21 頁)

(21) 出願番号 特願2006-503644 (P2006-503644)
 (86) (22) 出願日 平成16年2月17日 (2004.2.17)
 (65) 公表番号 特表2006-518162 (P2006-518162A)
 (43) 公表日 平成18年8月3日 (2006.8.3)
 (86) 国際出願番号 PCT/US2004/004670
 (87) 国際公開番号 W02004/075594
 (87) 国際公開日 平成16年9月2日 (2004.9.2)
 審査請求日 平成19年2月16日 (2007.2.16)
 (31) 優先権主張番号 60/447,563
 (32) 優先日 平成15年2月14日 (2003.2.14)
 (33) 優先権主張国 米国 (US)
 (31) 優先権主張番号 60/490,765
 (32) 優先日 平成15年7月28日 (2003.7.28)
 (33) 優先権主張国 米国 (US)

(73) 特許権者 595020643
 クゥアルコム・インコーポレイテッド
 QUALCOMM INCORPORATED
 アメリカ合衆国、カリフォルニア州 92
 121-1714、サン・ディエゴ、モア
 ハウス・ドライブ 5775
 (74) 代理人 100108855
 弁理士 蔵田 昌俊
 (74) 代理人 100091351
 弁理士 河野 哲
 (74) 代理人 100088683
 弁理士 中村 誠
 (74) 代理人 100109830
 弁理士 福原 淑弘

最終頁に続く

(54) 【発明の名称】 移動局場所サービスのための増強されたユーザープライバシー

(57) 【特許請求の範囲】

【請求項 1】

移動局内で用いるためのプライバシー制御システムであって、前記移動局は無線通信システムと通信を行い、プライバシー制御システムは移動局に関連する地理的場所情報を与えるものであって、

a) 少なくとも一つのプライバシールールを有するプライバシーポリシー部を含み、移動局外部の場所要求者により発生された移動局の地理的場所に関する場所要求を受け取り、前記少なくとも一つのプライバシールールに基づいてこの場所要求に応じるか否かを決定するプライバシーエンジンと、

b) このプライバシーエンジンに作動的に結合されて応答し、移動局の地理的場所の推定を生成してプライバシーエンジンに与える場所決定モジュール (PDM) と、ここで、前記プライバシーエンジンはPDMからの地理的場所の推定を受け取り、この場所の推定を処理して前記場所要求に選択的に応答し、前記プライバシーポリシー部に従って応答メッセージを発生させる、

更に、前記プライバシーエンジンに作動的に結合されたユーザーインターフェースとを有し、このユーザーインターフェースはユーザーからの入力を受信し、このユーザーの入力はアップデートを有するプライバシーポリシーを変更するために使用されるように構成され、

更に、前記ユーザーインターフェースはプライバシーポリシーに応じてユーザーに対する場所要求の告知を与えるとともに、ユーザーからの前記場所要求の告知に応える応答を

10

20

受信するように構成される、
プライバシー制御システム。

【請求項 2】

前記 P D M は以下の方法、即ち全地球位置決定システム (G P S)、アシステッド G P S、アドバンスドフォワードリンク三辺測量、到達時間、高監視時間差、および移動局が動作中の無線通信セルの識別に応じた位置決め、のいずれか一つまたはそれ以上の方法により動作する、請求項 1 に記載のプライバシー制御システム。

【請求項 3】

更に、プライバシーエンジンと無線通信システムとに作動的に結合された無線ネットワーク通信モジュールを具備し、前記無線ネットワーク通信モジュールは、無線通信システムからの場所要求を受信して応答メッセージを無線通信システムに送信するとともに、無線通信システムからのデータおよびソフトウェア命令を受信しまたは前記無線通信システムに送信するように構成される、請求項 1 に記載のプライバシー制御システム。

10

【請求項 4】

前記プライバシーエンジンは、無線通信システムからダウンロードされたソフトウェアを有する、請求項 3 に記載のプライバシー制御システム。

【請求項 5】

前記プライバシーエンジンは、無線通信システムからダウンロードされたソフトウェアアップグレードによって変更される、請求項 3 に記載のプライバシー制御システム。

【請求項 6】

前記プライバシーポリシーは、無線通信システムからダウンロードされたソフトウェアを有する、請求項 3 に記載のプライバシー制御システム。

20

【請求項 7】

前記プライバシーポリシーは、無線通信システムからダウンロードされたアップデートにより変更される、請求項 3 に記載のプライバシー制御システム。

【請求項 8】

前記アップデートは、ユーザ特有のプライバシーポリシーデータを含む請求項 7 に記載のプライバシー制御システム。

【請求項 9】

前記場所要求は、無線通信システムに作動的に接続された外部アプリケーションから受信される、請求項 3 に記載のプライバシー制御システム。

30

【請求項 10】

前記場所要求は、移動局内で実行されるローカルソフトウェアアプリケーションから受信される、請求項 1 に記載のプライバシー制御システム。

【請求項 11】

更に、プライバシーエンジンと外部ローカルアプリケーションに作動的に結合されたローカル通信モジュールを具備し、前記ローカル通信モジュールは、外部ローカルアプリケーションからの場所要求を受信して応答メッセージを外部ローカルアプリケーションに送信するとともに、外部ローカルアプリケーションからデータおよびソフトウェア命令を受信してデータとソフトウェア命令を外部ローカルアプリケーションに送信するように構成される、請求項 1 に記載のプライバシー制御システム。

40

【請求項 12】

前記プライバシーエンジンは、外部ローカルアプリケーションからダウンロードされたソフトウェアを有する、請求項 11 に記載のプライバシー制御システム。

【請求項 13】

前記プライバシーエンジンは、外部ローカルアプリケーションからダウンロードされたソフトウェア命令によるソフトウェアアップグレードによって変更される、請求項 11 に記載のプライバシー制御システム。

【請求項 14】

前記プライバシーポリシーは、外部ローカルアプリケーションからダウンロードされた

50

ソフトウェアを具備する、請求項 1 1 に記載のプライバシー制御システム。

【請求項 1 5】

前記プライバシーポリシーは、前記外部ローカルアプリケーションからダウンロードされたアップデートにより変更される、請求項 1 1 に記載のプライバシー制御システム。

【請求項 1 6】

前記アップデートは、ユーザー特有のプライバシーポリシーデータを含む、請求項 1 5 に記載のプライバシー制御システム。

【請求項 1 7】

前記場所要求は外部ローカルアプリケーションから受信される、請求項 1 1 に記載のプライバシー制御システム。

【請求項 1 8】

前記アップデートはユーザー特有のプライバシーポリシーデータを含む、請求項 1 に記載のプライバシー制御システム。

【請求項 1 9】

前記プライバシーポリシーは複数のプライバシー等級を含み、このプライバシー等級はプライバシーエンジンによって受信された場所要求を分類し、更に前記プライバシーポリシーは各プライバシー等級に対する場所要求に応じた対応を決定するプライバシールールを含み、このプライバシールールは、

- a) 場所要求の許可又は禁止のデフォルトを要するルールと、
- b) 場所要求のユーザー告知を必要とするルールと、
- c) 要求されたサービスの内容に基づくユーザー告知を要するルールと、
- d) 場所要求が定期的なものか或いは必要時に発生されるものかに基づいたユーザー告知を要するルールと、
- e) 場所要求が発生した時間に基づくユーザー告知を要するルールと、
- f) ユーザー告知のために用いられる表示モードを指定するルールと、
- g) 与えられるべき場所推定の正確な範囲を指定するルールと、
- h) ユーザーがユーザー告知に回答しなかったときに応答メッセージの取り扱いのデフォルトを要するルールと、
- i) 移動局の現在の地理的場所に基づいた応答メッセージの取り扱いを決定するルールと、

のうちの少なくとも一つのルールを含む、請求項 1 に記載のプライバシー制御システム。

【請求項 2 0】

更に、着脱式のデータ記憶装置を具備し、このデータ記憶装置はプライバシーエンジンに作動的に結合されるとともに、ユーザー特有のプライバシーポリシーデータを受信し、記憶し、送信するように構成された、請求項 1 に記載のプライバシー制御システム。

【請求項 2 1】

前記着脱式のデータ記憶装置は加入者識別モジュール装置を具備する、請求項 2 0 に記載のプライバシー制御システム。

【請求項 2 2】

前記着脱式のデータ記憶装置はユニバーサル加入者識別モジュール装置を具備する、請求項 2 0 に記載のプライバシー制御システム。

【請求項 2 3】

前記着脱式のデータ記憶装置は着脱式のユーザー識別モジュール装置を具備する、請求項 2 0 に記載のプライバシー制御システム。

【請求項 2 4】

移動局の地理的場所情報に関して移動局内でプライバシー制御を与える方法であって、前記移動局は無線通信システムと通信を行い、この移動局はソフトウェア命令を有したプライバシーエンジンを含み、このプライバシーエンジンのソフトウェア命令は更にプライバシーポリシー命令を含み、移動局は更に移動局の地理的場所の推定を与えることができる位置決定モジュール(PDM)を含み、前記方法は、

a) 移動局の現在の地理的場所に関する場所要求を受信するステップと、
b) 前記プライバシーポリシー命令は受信した場所要求に応答するか否かを決定する少なくとも一つのプライバシールールを有し、この少なくとも一つのプライバシールールによる決定に基づいてこのプライバシールールを含むプライバシーエンジンのソフトウェア命令によりこの場所要求を処理するステップと、
c) 移動局の地理的場所の推定を取得するステップと、
d) この場所の推定を位置要求と、プライバシーエンジンのソフトウェア命令と、プライバシールールとに従って処理するステップと、
e) プライバシーエンジンのソフトウェア命令と、場所の推定と、プライバシールールとに対応して、場所要求に応答する応答メッセージを選択的に出力するステップと、
f) 更に、ユーザーに対して場所要求を告知するステップと、

を含むプライバシー制御方法。

10

【請求項 2 5】

前記場所要求を処理するステップ b) は、更に前記プライバシーポリシー命令をオーバーライドすることにより非常場所要求を処理して非常応答メッセージを出力するステップを含む、請求項 2 4 に記載のプライバシー制御方法。

【請求項 2 6】

前記場所要求を処理するステップ b) は、複数の現在場所要求を処理するステップを含む、請求項 2 5 に記載のプライバシー制御方法。

【請求項 2 7】

現在の場所要求は非常場所要求が処理されている間は中断される、請求項 2 6 に記載のプライバシー制御方法。

20

【請求項 2 8】

前記プライバシーポリシー命令は前記ステップ a) の処理の際に受信される場所要求を分類するプライバシー等級を含み、前記プライバシーポリシー命令は更に各プライバシー等級の場所要求に対する応答を決定するプライバシールールを含み、プライバシールールは、

a) 場所要求の許可又は禁止のデフォルトを要するルールと、
b) 場所要求のユーザー告知を要するルールと、
c) 要求されたサービスの内容に基づくユーザー告知を要するルールと、
d) 場所要求が定期的なものか或いは必要時に発生されるものかに応じたユーザー告知を要するルールと、
e) 場所要求が発生した時間に基づくユーザー告知を要するルールと、
f) ユーザー告知のために用いられる表示モードを指定するルールと、
g) 与えられるべき場所の推定の正確な範囲を決定するルールと、
h) ユーザーがユーザー告知に応答しなかったときに応答メッセージの取り扱いのデフォルトを要するルールと、
i) 移動局の現在の地理的場所に基づいた応答メッセージの取り扱いを指定するルールと、

30

のうちの少なくとも一つのルールを含む、請求項 2 4 に記載のプライバシー制御方法。

40

【請求項 2 9】

移動局の地理的場所情報に関して移動局内でプライバシー制御を与える装置であって、前記移動局は無線通信システムと通信を行い、この移動局はソフトウェア命令を有したプライバシーエンジンを含み、このプライバシーエンジンのソフトウェア命令は更にプライバシーポリシー命令を含み、移動局は更に移動局の地理的場所の推定を与えることができる位置決定モジュール (PDM) を含み、前記装置は、

a) 移動局の現在の地理的場所に関する場所要求を受信する手段と、
b) 前記プライバシーポリシー命令は受信した場所要求に応答するか否かを決定する少なくとも一つのプライバシールールを有し、この少なくとも一つのプライバシールールによる決定に基づいてこのプライバシールールを含むプライバシーエンジンのソフトウェア

50

命令によりこの場所要求を処理する手段と、

c) 移動局の地理的場所の推定を取得する手段と、

d) この場所の推定を、場所要求と、プライバシーエンジンのソフトウェア命令と、プライバシールールとに従って処理する手段と、

e) プライバシーエンジンのソフトウェア命令と、場所の推定と、プライバシールールとに従って場所要求に応答する応答メッセージを選択的に出力する手段と、

更に、ユーザーに場所要求の告知を行う手段と、

を含むプライバシー制御装置。

【請求項 30】

前記場所要求を処理する手段は、前記非常場所要求を処理するためにプライバシーポリシー命令をバイパスして非常応答メッセージを出力する手段を含む、請求項 29 に記載のプライバシー制御装置。

【請求項 31】

前記場所要求を処理する手段は更に複数の同時発生 of 場所要求を処理する手段を含む、請求項 30 に記載のプライバシー制御装置。

【請求項 32】

現在の場所要求は非常場所要求が処理されている間は中断される、請求項 31 に記載のプライバシー制御装置。

【請求項 33】

前記プライバシーポリシーは前記ステップ a) の処理の際に受信される場所要求を分類するプライバシー等級を含み、前記プライバシーポリシーは更に各プライバシー等級の場所要求に対する応答を決定するプライバシールールを含み、前記プライバシールールは、

a) 場所要求の許可又は禁止のデフォルトを要するルールと、

b) 場所要求のユーザー告知を要するルールと、

c) 要求されたサービスの内容に基づくユーザー告知を要するルールと、

d) 場所要求が定期的なものか或いは必要時に発生されるものかに応じたユーザー告知を要するルールと、

e) 場所要求が発生した時間に基づくユーザー告知を要するルールと、

f) ユーザー告知のために用いられる表示モードを指定するルールと、

g) 与えられるべき場所の推定の正確な範囲を決定するルールと、

h) ユーザーがユーザー告知に応答しなかったときに応答メッセージの取り扱いのデフォルトを要するルールと、

i) 移動局の現在の地理的場所に基づいた応答メッセージの取り扱いを指定するルールと、

のうちの少なくとも一つのルールを含む、請求項 29 に記載のプライバシー制御装置。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、米国で 2003 年 2 月 14 日に名称「移動局場所サービスのための増強されたユーザープライバシー」で出願された予備出願 No. 60/447,563 および 2003 年 7 月 28 日に提出された予備出願 No. 60/490,765 について 35 USC § 119(e) に基づく利益を受ける出願に係る発明であって、移動局に対する場所サービスの分野、特に場所要求に応答するプライバシーポリシーの増強されたユーザー制御に関する。

【背景技術】

【0002】

移動電話や無線デジタル通信装置（以下、移動局と称する）のための場所サービス（LoCation Servicesを短縮して L C S と称する）は無線通信プロバイダーにとってますます重要なビジネス分野となっている。この重要性は L C S における標準化や機能明細などの確立に反映されている。例えば 3 つの L C S 文献：2002 年 6 月の（3 G P P T

10

20

30

40

50

S 23.271V6.0.0)即ち、第3世代パートナーシッププロジェクト(3GPP)のテクニカルスペシフィケーショングループ(TSG)によるサービスとシステム問題に関する基本ステージ2(SA2)のリリース6によるLCSの説明;および2002年8月19日から23日までカナダのトロントで開催された3GPP TSG-SA2ミーティング#26のテクニカルドキュメント(TD)S2-022360;および2003年3月の(3GPP TSG23.271V6.3.0)即ち、第3世代パートナーシッププロジェクト(3GPP)のテクニカルスペシフィケーショングループ(TSG)によるサービスとシステム問題に関する基本ステージ2(SA2)のリリース6によるLCSの説明、がある。これらの文献は以下の説明では夫々、3GPP-R1、3GPP-R2、3GPP-R3として引用する。

10

【0003】

文献3GPP-R1と3GPP-R3はユーザープライバシーに関する章を含みLCSシステム全体の機能的モデルを説明している。文献3GPP-R2はネットワークエレメントを含み、これはプライバシープロファイルレジスタ(PPR)として説明され、加入者のLCSプライバシー情報を保持し、さらに対応するプライバシー機能を果たす。ここで述べられたこれらの文献はLCSと関連したLCSプライバシー動作に関連した最近の技術のスタンダードの全体像を示している。これらの文献によってLCSを加入者に供給する多くの方法と装置が通信の分野の当業者に知られている。

【0004】

無線通信システム中で移動局の位置を決定するための有効な方法は全地球位置測定システム(GPS)である。GPS装置(より一般的には、位置決定モジュールまたはPDM)を移動局に組み込むことにより高精度の位置決定が可能となる。PDMが移動局の場所情報を提供する主たる手段として用いられると、サービスプロバイダーネットワークは正確な場所要求を受信した時に移動局とコンタクトしなければならない。移動局のGPSのようなPDMを用いる場所サービス機能を使用する方法と装置は、無線通信分野の当業者によく知られている。GPSを用いた送受話器によるLCS機能が現在使用されている。移動局用のGPSシステムの例が、1998年の9月15日から18日の間に開かれたナビゲーションGPS学会1998の会報の333ページから344ページにM. MoegleinとN. F. Krasnerによる「スナップトラック(SnapTrack:商標)サービス用のGPS技術」と題する文献として記載されている。移動局に適するGPSシステムを記載した最近の特許出願として、2002年の5月2日付けの米国特許出願20020050944が、L. SheynblatとN. F. Krasnerによる「サテライト位置システム(SPS)信号の測定処理のための方法と装置」として出願されている。

20

30

【0005】

不都合なことに、現在のLCSプライバシー方法を用いたプライバシーポリシー情報のユーザー制御は、現在のLCSプライバシー方法がサービスプロバイダーネットワークによってユーザープライバシーを管理するために、非常に限定された非フレキシブルなものとなっている。例えば、従来のLCSプライバシー方法では、多くの等級の要求者のクライアントがサービスプロバイダーによって定義されており、これらの等級に基づく上記のPPRとして説明したユーザープライバシープロファイルがユーザーがサービスを受けるときに形成される。これらのLCSプライバシー方法により、ユーザー場所に対する無制限のアクセスを有する特定の要求者の等級、および制限されたアクセスを有する他の要求者の等級を指示する。このような制限は、例えば、特定の制限等級に対するLCS情報を自動的に拒否することを含む。この制限はまた、ユーザーが告知されることを要求し、また、特定の限定された等級の要求者によるLCSアクセス要求を許可(臨時的)する。これらの従来のシステムにおいて、プライバシープロファイルの変更は、プロバイダーとユーザーとの間のサービスの合意に基づいてのみ有効である。ユーザーの場所が移動局内のPDMによって主として決定されている場合には、PDMを無効にすることによって追加の変更オプションが可能となる。このオプションは、ユーザーによる正確な位置情報の取得を妨げることによりプライバシーを強めるが、PDMが再度有効になるまでは全ての要

40

50

求者の等級に対して正確な場所の取得ができないことから、この方法の有効性が非常に狭められることになる。

【 0 0 0 6 】

以下の説明は移動局内におけるＬＣＳプライバシー管理のための方法と装置に関して行われる。この説明は移動局ユーザーによる便利で柔軟性のあるＬＣＳ制御が可能であることを示している。

【 発明の開示 】

【 0 0 0 7 】

以下の説明は無線移動局の地理的場所を提供するための方法と装置に関し、特に場所情報の要求に対する応答を管理するプライバシーポリシーを強めたユーザー制御を提供するための方法と装置に関する。これらの要求は以下の説明においては場所要求、または位置要求としている。

【 0 0 0 8 】

この発明の一実施形態において、移動局のためのプライバシー制御システムは、プライバシーエンジンと、位置決定モジュール（ＰＤＭ）と、ユーザーインターフェースとを有する。プライバシーエンジンはソフトウェアモジュールであって、場所要求に対する移動局の応答を制御する。

【 0 0 0 9 】

プライバシーエンジンは更にプライバシーポリシーを含む。プライバシーポリシーは、場所要求者とそれに付随した場所要求とを分類するためのプライバシー等級と、各プライバシー等級において場所要求に対する応答を決定するプライバシールールとを含む。

【 0 0 1 0 】

プライバシー等級は場所要求者とアプリケーションのリストによって定義されている。場所要求者とアプリケーションとは、ＵＲＬのような識別情報、インターネットドメイン、または位置要求と共に供給される他のデータに基づいて個々に指定してもよいし、あるいはカテゴリー又は形式にグループ分けしてもよい。場所要求は、場所要求者に応じて分類される。これにより、場所要求は場所要求と共に供給される情報に基づいてプライバシー等級に割り当てられる。プライバシー等級の例としては、限定はされないが、未知又は未承認の場所要求アプリケーションおよび他の等級に含まれていない要求者の身元に対するデフォルトのプライバシー等級、信用のある場所要求アプリケーションおよび他の等級に含まれていない要求者の身元に対するデフォルトのプライバシー等級、及び、場所要求アプリケーションおよびＵＲＬまたは位置要求データとともに供給される他の識別データによって識別された要求者の身元を含むユーザー指定の等級等を含む。

【 0 0 1 1 】

各プライバシー等級は、それに付随して、場所要求に対するプライバシーエンジンの応答を決定するための一組のプライバシールールを有する。このルールの例としては、限定はされないが、無制限アクセスを規定するルールと、アクセス拒否のデフォルトのルールと、ユーザー告知と要求された許可を条件とするアクセスのためのルールと、ユーザー告知と要求された許可無しのアクセスのためのルールと、ユーザーが選択した時間内のアクセス拒否のルールと、場所の規定された近似のためのみのアクセスのためのルール等がある。プライバシーポリシー、プライバシー等級、及びプライバシールールは、プライバシーエンジンが夫々の、および全ての場所要求にどのように応答するかを決定する。

【 0 0 1 2 】

この発明によるユーザープライバシー方法と装置を用いることにより、特定の移動局に対するプライバシーポリシーは、移動局中のユーザーインターフェースを介してユーザーによって制御され、または変更することができる。一実施形態において、ユーザーインターフェースは適当な入力手段、例えば針、ポインティング装置またはキーパッドなどを有する。この発明概念の他の実施形態において、プライバシーポリシーは移動局を無線データネットワークを介して接続するネットワークアプリケーションを介して制御される。この発明方法の更に他の実施形態において、プライバシーポリシーはローカル装置にあるア

10

20

30

40

50

アプリケーションによって制御するようにできる。このローカル装置としてはラップトップコンピュータやパーソナルデジタルアシスタントなどであり、これらの装置は移動局に作動的に接続される。

【 0 0 1 3 】

初期プライバシーポリシーを含む移動局のプライバシーエンジンは無線データネットワークを介して移動局により受信（即ちダウンロード）することができる。

【 発明を実施するための最良の形態 】

【 0 0 1 4 】

以下の説明において実施形態と変形例とがこの発明の概念の使用と実施に付いて説明するために示されている。この説明はこの発明の概念の例示として行われているもので、ここに示されている概念の範囲を定めるものでないことは勿論である。

【 0 0 1 5 】

以下の図面において同様の参照番号および説明は同様の部分を示している。

【 0 0 1 6 】

図 1 はこの発明の概念を適用できる無線通信装置と無線通信システムのブロック図を示す。図 1 に示した実施形態は、ユーザーインターフェース 1 0 6 と無線ネットワーク通信モジュール 1 1 2 とアプリケーションブロック 1 1 4 とローカル通信モジュール 1 1 8 とプライバシーエンジン 1 2 0 と位置決定モジュール 1 2 2 と他のモジュール 1 2 4 とを有する移動局 1 0 2 を含む。

【 0 0 1 7 】

図 1 に示したように、この発明の一実施形態において、無線ネットワーク通信モジュール 1 1 2 は移動局 1 0 2 と外部データネットワーク 1 1 0 との間の無線データ接続を提供する。外部データネットワーク 1 1 0 は種々のネットワークシステムを含むことができる。例えば、ある実施形態では外部データネットワークは無線サービスプロバイダーネットワークを有することができる。他の実施形態では外部データネットワークは移動局とインターネットとの間のデータの受信と送信との接続を提供するインターネットサービスプロバイダーであってもよい。一般に、外部データネットワーク 1 1 0 は無線通信を用いて移動局に対してデータを送信し受信することができる種々のデータシステムを有する。図 1 に示したように、無線ネットワーク通信モジュール 1 1 2 は更にアプリケーションブロック 1 1 4 とプライバシーエンジン 1 2 0 とに作動的に結合されている。この無線通信モジュール 1 1 2 はアプリケーションブロック 1 1 4 とプライバシーエンジン 1 2 0 とからデータを受信し、送信する。

【 0 0 1 8 】

一実施形態においてアプリケーションブロック 1 1 4 は移動局の位置推定を要求する場所アプリケーションを有する。これらの場所アプリケーションは M S レジデントであり、これはネットワークとの相互通信を必要とせず、あるいはネットワーク（例えばモジュール 1 0 8）中の場所サーバとの間の相互通信を行い、従ってこの場所サーバは場所クライアントとして動作する。この典型的な実施形態においてアプリケーションブロック 1 1 4 はネットワークデータ通信及び移動局の他の機能に関する他のアプリケーションも有する。これらのアプリケーションの例としては、これらに限定するものではないが、データやデータファイルや移動局 1 0 2 に対するソフトウェア命令などを受信し、あるいはデータをダウンロードするための、e メールクライアント、ウェブブラウザズ、f t p クライアント、及び他のソフトウェアアプリケーションなどである。アプリケーションブロック 1 1 4 は無線通信モジュール 1 1 2 に結合されてデータを受信或いは送信し、外部データネットワーク 1 1 0 と通信を行う。アプリケーションブロック 1 1 4 は更にユーザーインターフェース 1 0 6 に作動的に結合されてデータを受信或いは送信し、種々のアプリケーションについてユーザー動作と通信を行う。アプリケーションブロック 1 1 4 は更にプライバシーエンジン 1 2 0 に作動的に結合されてデータの受信、送信を行う。このデータとしては場所要求や応答データを含む。このデータは更に受信即ちダウンロードされたソフトウェア命令を有し、これによりプライバシーエンジン 1 2 0 の機能や可能動作を作成し

、変更し、あるいは与える。更に、このようなプライバシーエンジン 120 の機能を作成し、変更し、或いは与えるためのデータは、データを受信し送信するように作動的に結合された無線通信モジュール 112 から直接受け取ることもできる。更に他の例として、プライバシーエンジン 120 の機能を作成し、変更し、或いは与えるためのデータを、図 1 には示していないが、移動局の構成部により受信し、実行するように構成してもよい。この構成部は通信分野の当業者に良く知られているもので、例えば、アプリケーションスペシフィック集積回路 (ASIC)、アプリケーションプログラミングインターフェース (API)、ランダムアクセスメモリ (RAM)、リードオンリーメモリ (ROM) 等を含む。無線ネットワークを介して移動局にアプリケーションをダウンロードして実行させるための方法とシステムの例が、2002 年の 12 月 5 日に公開されたランドブレード等による米国特許出願公開番号 2002/0183056 A1「無線環境におけるアプリケーションの安全な配布と実行」に開示されている。

10

【0019】

ローカル通信モジュール 118 は移動局 102 と外部ローカルアプリケーションモジュール 116 との間のデータ送受信を任意に行うための手段を提供する。この実施形態において外部ローカルアプリケーションモジュール 116 はパーソナルコンピュータやラップトップまたはパーソナルデジタルアシスタントなどのローカル接続された装置内に存在する。このモジュール 118 はローカル接続された装置との接続を行う。ローカル通信モジュール 118 は更にプライバシーエンジン 120 に作動的に結合されてデータの送受信を行う。このデータとしてはプライバシーエンジン 120 の機能や可能動作を作成し、変更し、あるいは与えるためのソフトウェア命令を含む。更に、これらのデータは場所アプリケーション (場所データを要求するアプリケーション) のための入出力データを含み、この場所アプリケーションは、無線通信モジュール 112 により与えられたネットワーク接続から分離した赤外線接続 MS、ブルートース、USB ケーブル、又は他の手段などに接続されたラップトップなどの分離された装置上で使用される。これらの場所データをプライバシーエンジン 120 に送ることにより、以下に述べるように、ローカルアプリケーションによる場所要求のプライバシー管理を容易に行うことができる。

20

【0020】

上述したように、プライバシーエンジン 120 は構成部 112、114、128 に結合されてデータの送受信を行う。プライバシーエンジン 120 はさらにユーザーインターフェース 106、位置決定モジュール 122、及び他の種々のモジュール 124 と結合されてデータの送受信を行う。このプライバシーエンジン 120 の機能と動作とは以下に説明する。

30

【0021】

ユーザーインターフェース 106 は移動局ユーザーに対して情報の受信、命令の供給、およびアプリケーションブロック 114 とプライバシーエンジン 120 のアプリケーションと機能の実行のための手段を与える。このユーザーインターフェース 106 は例えばグラフィカルユーザーインターフェースとタッチスクリーンやポインティング装置やキーボードなどの適切な入力手段を有する。更にユーザーインターフェース 106 はサウンドや音声コマンドの送信、受信の手段、あるいは移動局 102 に結合されたソフトウェアモジュールやアプリケーションやデジタル装置からの情報の受信、命令の送信、及びこれらの動作を行うための手段を有する。

40

【0022】

位置決定モジュール (PDM) 122 は移動局 102 の場所を示すデータを発生する。公知の適当な PDM は全地球位置決定システム (GPS) 装置または方法を使用する。しかしながら、移動局 102 に対して位置又は場所のデータを供給できる PDM であればどのようなものを用いることも可能である。例えば、この PDM として、アシステッド GPS (AGPS)、アドバンスドフォワードリンクトリラレーション (AFLT)、タイムオブアライバル (TOA)、エンハンスドオブザーブドタイムディファレンス (E-OTD)、および MS が動作している無線通信セルの識別に基づく位置決定などの公知の位

50

置決定方法を用いることができる。これらの方法は通信分野の当業者にとって公知であり、ここでは説明は行わない。

【0023】

他のモジュールブロック124は移動局の機能を実現しあるいは増強するためのソフトウェアとハードウェア要素を示している。これらのソフトウェアとハードウェア要素は、例えば、アプリケーションスペシフィック集積回路(ASIC)、アプリケーションプログラミングインターフェース(API)、ランダムアクセスメモリ(RAM)、リードオンリーメモリ(ROM)、加入者識別モジュール(SIM)またはユニバーサル加入者識別モジュール(USIM)、カメラなどを含む。他のモジュールブロック124の詳細は図1には示されていないが、この他のモジュールブロック124に含まれるモジュールと構成要素が要求される機能のために移動局内でどのように作動的に結合されているかは当業者ならば容易に理解できることである。

10

【0024】

図1における実施形態において、プライバシー管理サーバ104ソフトウェアアプリケーションを含み、これはデータの送受信のために外部データネットワーク110に結合される。このプライバシー管理サーバ104は外部データネットワーク110に結合されて無線ネットワーク通信モジュール112との間でデータの交換を行う。プライバシー管理サーバ104は外部データネットワーク110と無線ネットワーク通信モジュール112とを介してプライバシーエンジン120と通信を行う。このプライバシー管理サーバ104は外部データネットワーク110と無線ネットワーク通信モジュール112とを介してネットワークアプリケーションブロック114との間でデータの送受信を行う。プライバシー管理サーバ104とネットワークアプリケーションブロック114とプライバシーエンジン120との間で送信されるデータは、プライバシーエンジン120の機能および可能性を形成し、変更し、使用するためのソフトウェア命令を含むことができる。同様に、通信モジュール112を介してプライバシー管理サーバ104とプライバシーエンジン120との間を伝送されるデータも、プライバシーエンジン120の機能および可能性を形成し、変更し、使用するためのソフトウェア命令を含むことができる。一般に、プライバシー管理サーバ104と移動局102を含む構成要素との間で送信されるデータは、LCSとプライバシー管理を行いまたは関連する移動局102内でソフトウェアモジュールを形成し、変更し、使用するために用いられることができる。

20

30

【0025】

図1の場所要求アプリケーションブロック108は外部データネットワーク110を介して移動局102との間でデータの送受を行うように接続された場所要求アプリケーションを示す。場所要求アプリケーション108は外部データネットワーク110と無線ネットワーク通信モジュール112とを介してデータの授受をプライバシーエンジン120との間で行うように結合される。場所要求アプリケーションブロック108とプライバシーエンジン120との間の位置要求と位置応答データの授受を以下に説明する。

【0026】

典型的なプライバシーポリシー

この実施形態において、プライバシーエンジン120はソフトウェアモジュールであって、場所情報の要求に対する移動局の応答を制御するように動作する。これらの要求は以下の説明では場所要求であり、これはまた位置要求と同等である。

40

【0027】

プライバシーエンジンは更にプライバシーポリシーを含む。このプライバシーポリシーはプライバシーエンジンの構成要素であって、場所要求者とその対応する場所要求とを分類するプライバシー等級と、各プライバシー等級の場所要求に対する応答を決定するプライバシールールとを含む。

【0028】

プライバシー等級は場所要求者とアプリケーションとのリストにより定められる。場所要求者とアプリケーションとは、位置要求と共に供給されるURLやインターネットドメ

50

インや他のデータなどの識別情報に基づいて個々に分類され、あるいはカテゴリーまたは形式によってグループ分けされる。場所要求は場所要求者に応じて分類される。場所要求は、この場所要求と共に供給される情報に基づいてプライバシー等級に割り当てることができる。例えば、プライバシー等級は、これらに限定されないが、未知の又は未申告の場所要求アプリケーションと他の等級に含まれない要求者身元とに対するデフォルトプライバシー等級と、他の等級に含まれない信任された場所要求アプリケーションと要求者身元とに対するデフォルトプライバシー等級と、位置要求データとともに供給されるURLまたは他の識別データによって識別された場所要求アプリケーションと要求者身元とを含むユーザー別等級とを含む。

【0029】

各プライバシー等級は、場所要求に対するプライバシーエンジンの応答を決定するための関連する一組のプライバシールールを有する。例えば、限定されないが、無制限のアクセスを指定するルールと、アクセスのデフォルトの禁止を指定するルールと、ユーザー告知と要求された承認とを条件とするアクセスを指定するルールと、ユーザー告知はあるが要求された承認がないことを条件とするアクセスを指定するルールと、ユーザーが選択した時間内においてアクセス禁止を指定するルールと、場所の近似のためのみのアクセスを指定するルールとを含む。このプライバシーポリシーと、そのプライバシー等級と、そのプライバシールールとは、プライバシーエンジンがどのように夫々の、及び全ての場所要求に応答するかを決定するものである。

【0030】

典型的な初期化とソフトウェアアップグレード方法

この発明概念の一実施形態において、ユーザープライバシーの制御機能を持たない移動局は、ネットワークサーバからデータを受信またはダウンロードすることにより移動局LCS用の増強されたユーザープライバシーを使用するためのソフトウェアモジュールを初期設定することができる。プライバシーエンジン120(図1)をインストールして作動的に使用するためのソフトウェアデータと命令は初期プライバシーポリシーを含み、無線通信モジュール112を介してネットワークサーバ(例えば、図1のプライバシー管理サーバ104あるいは図示しない他のネットワークサーバ)から移動局102へ受信され、またはダウンロードされる。受信されまたはダウンロードされたデータの受信およびインストールは、ネットワークアプリケーションモジュール114中のブラウザ又は他の構成要素により、あるいは他のモジュール124に含まれる構成要素により遂行される。無線ネットワーク接続を介して移動局へアプリケーションやソフトウェアモジュールを受信しダウンロードする方法は無線通信技術の分野の通常の知識を持つ人にとって公知である。上述したように無線ネットワークを介して移動局にアプリケーションをダウンロードし実行させる方法とシステムとの一例がランドブレッド(Lundblade)の文献に記述されている。一実施形態においては、移動局はその移動局へのアプリケーションのインターフェースをアシストするためのソフトウェアプラットフォーム、例えばカリフォルニアのサンディエゴに本社のあるカルコム社により開発されたソフトウェアである無線用バイナリランタイムエンバイロメント(BREW)(商標)を含む。

【0031】

プライバシーエンジン120(図1参照)のためのアップグレード及び変更用のソフトウェア、およびプライバシーポリシーと他の移動局ソフトウェアとその構成要素とは上述したネットワークサーバから受信しダウンロードできる。特にユーザー(または許可された他の組織)はプライバシーポリシーを無線ネットワーク接続を介して更新できる。或いは、ユーザーはユーザーインターフェース106を介してプライバシーポリシーを更新できる。更にユーザーは、ローカル通信モジュール118を介して接続された外部ローカルアプリケーション(外部ローカルアプリケーションブロック116)を用いてデータを入力することによりプライバシーポリシーを更新できる。更に、ユーザーは着脱可能のデータ記憶装置(図1には図示せず)を用いてユーザー指定のプライバシーポリシーデータを入力できる。このユーザー指定のプライバシーポリシーデータは、移動局ユーザーの要求

または選択に応じて選択され、変更され、または形成されたプライバシー等級およびプライバシールールを含む。この発明概念の好ましい実施形態においては、移動局 102 は製造業者或いはサービスプロバイダーにより、総括的なプライバシーポリシーを含む初期設定されたデフォルトのプライバシーエンジンを提供されることになる。この総括的なプライバシーポリシーはユーザーにより以下の一つ或いは複数の方法によりカスタマイズされて、ユーザー指定のプライバシー等級とプライバシールールとを含むことになる。これらの方法は、1) ネットワークからユーザー指定のプライバシーポリシーデータをダウンロードする方法、2) ユーザーインターフェースを用いてユーザー指定のプライバシーポリシーデータを入力する方法、3) ローカル接続装置中にある外部ローカルアプリケーションを用いてユーザー指定のプライバシーポリシーデータを入力する方法、4) 着脱可能のデータ記憶装置を用いて予め記録されたユーザー指定のプライバシーポリシーデータを入力する方法などである。着脱可能のデータ記憶装置を用いる例としては、加入者識別モジュール、ユニバーサル加入者識別モジュール、あるいは着脱可能な識別モジュールなどがあり、以下に説明する。

10

【0032】

強化されたユーザープライバシー制御のための操作方法の例

図2(a) - 2(d) は移動局 LCS に用いるための増強されたユーザープライバシーの方法を例示するための統一化された流れ図を示す。図2(a) - 2(d) の流れ図間の接続は要素 214、220、230、232 によって示されている。同様に、図2(a) と図2(c) 間の接続は要素 202、208、223 によって示されている。図2(b) と図2(c) との接続は要素 258 によって示されている。図2(b) と図2(d) との間の接続は要素 214、246 によって示されている。図2(c) と図2(d) との接続は要素 246 によって示されている。

20

【0033】

図2(a) の要素 202 は、プライバシーエンジン 120 (図1) が場所データ情報の要求 (即ち位置要求) の受信を待ち受ける状態を示す。ステップ 204 において、プライバシーエンジン 120 は図1で説明されたデータ接続を介して位置要求を受信する。この実施形態の動作において、位置要求データは以下に示す情報、1) ネットワークアドレスと場所要求アプリケーションの形式、2) 要求者のカテゴリー (例えば、緊急サービス、商業サービス、個人など)、3) 可能な場合の要求者の身元、4) 要求者の身元の照合のためのコードワードまたはデジタル証明、5) 要求されたサービスの質 (QoS) を含む。通信分野の当業者にとって、この説明の範囲は、例えば地理的エリア情報、ユーザー情報、要求者情報、座標システムなど他のいろいろな実施形態に用いることができる他の形式の位置要求データを包含することは明らかである。

30

【0034】

図2(a) のステップ 206 において、位置要求カウンタがゼロの値に初期化される。このゼロの値はただ一つの位置要求が受信されたことを示している。第1の位置要求が処理されている間に次の位置要求が受信されると、位置要求カウンタが以下に説明するようにインクリメントあるいはデクリメントされる。この位置要求カウンタの目的は多くの位置要求が同時に発生したときの対応のためである。

40

【0035】

要素 208 は図2(c) からの流れ図の接続を示す。以下に説明するように、先行の位置要求が処理されているときに後続の位置要求が受信されたときにのみ、流れ図接続点 208 を介して図2(c) のステップ 286 に続く発明方法によって処理される。

【0036】

ステップ 210 において、プライバシーエンジン 120 (図1) は選択されたプライバシーポリシーに従って、ステップ 204 (または要素 208 を介して) の間に受信された位置要求にプライバシー等級を割り当てる。上述したように、プライバシーポリシーは、プライバシー等級を位置要求に対して割り当て、割り当てられたプライバシー等級に基づいてプライバシールールを決定するためのリストを有する。

50

【 0 0 3 7 】

図 1 において、プライバシーエンジン 1 2 0 は、アプリケーションモジュール 1 1 4、他のモジュール 1 2 4、または図示していない移動局モジュールと構成要素とを必要に応じて用いて、位置要求データの分類を行う。例えば、ネットワークアプリケーションはデジタル証明データを照合するために用いられる。

【 0 0 3 8 】

図 2 (a) において、ステップ 2 1 2 において、位置要求データは、位置要求が緊急サービス要求であるかどうかを決定するために調べられる。通常の法令上の要求に従って、緊急サービス要求はプライバシーポリシーに優先され、位置データができるだけ迅速に要求者に送信される。緊急サービス要求に対して、この方法のステップは流れ図の接続点 2 1 4 を介してステップ 2 5 6 (図 2 (b)) に進み、プライバシーポリシーをバイパスして迅速な応答を行う。非緊急要求に対してはステップ 2 1 6 に進む。

10

【 0 0 3 9 】

ステップ 2 1 6 において位置要求データは評価され、プライバシーポリシーに対して優先する必要がある他の要求であるかが調べられる。例えば、法の執行官又は政府のエージェントからの要求に対して優先的に処理する国もある。優先処理が要求されると、ステップは流れ図接続点 2 1 4 からステップ 2 5 6 に進んで迅速な処理が行われる。優先処理が要求されないときはステップ 2 1 8 に進む。

【 0 0 4 0 】

図 2 (a) に戻って、ステップ 2 1 8 でプライバシーエンジン 1 2 0 (図 1) は、位置要求がこの要求に割り当てられたプライバシー等級に付属するルールに基づいて拒否すべきか否かをプライバシーポリシーに基づいて決定する。位置要求情報の拒否は多くの条件に基づいて決定することができる。第 1 の例においては、この位置要求は要求者が商業的な組織であるとして拒否され、この商業的な組織に対して割り当てられたプライバシー等級は自動的な拒否を指示する。第 2 の例においては、要求者が私的な個人であるときであり、自動的に拒否されるように指定されたルールを持つプライバシー等級に分類されていて、その要求は拒否される。第 3 の例においては位置要求が要求者の身元を証明するデジタル証明またはパスワードを含まず、このカテゴリーのデフォルトプライバシー等級が自動的な拒否を指示するルールを含んでおり、その要求は拒否される。第 4 の例においては、緊急サービスに関する時以外に、全ての位置要求が特定時間の間は自動的な拒否を指示するプライバシー等級に含まれるように指示するようにユーザーが選択できる。無線通信の分野の当業者には、この説明の範囲内において多くの他の実施形態が含まれることが明らかである。

20

30

【 0 0 4 1 】

ステップ 2 1 8 において位置要求の拒否が決定されると、位置の計算が行われず、処理は次のステップ 2 2 2 に進み、拒否する旨のサービスメッセージが位置要求アプリケーションに送信される。図 2 (b) の流れ図を参照して以下に説明するように、ステップ 2 2 2 は更にステップ 2 3 8 又は 2 4 2 の後の流れ図接続点 2 2 0 を介して用いられる。ステップ 2 2 2 の後で、この発明の方法の処理は流れ図接続点 2 2 3 を介して図 2 (c) のステップ 2 8 2 に進む。更に詳細に説明するように、ステップ 2 8 2 において位置要求カウンタがチェックされ、アイドル状態ステップ 2 0 2 に復帰する前、または更に他の処理を行う前に他の要求が来ているか否かを決定する。

40

【 0 0 4 2 】

図 2 (a) に戻り、決定ステップ 2 1 8 において要求が拒否すべきでないと決定されたときは、プライバシーポリシーがステップ 2 2 4 で用いられて、ユーザー告知がなされたか否かが決定される。ステップ 2 2 4 においてユーザー告知が必要でないと決定されたときは、この発明の方法は更に他の処理のために流れ図接続点 2 3 0 を介して図 2 (b) のステップ 2 5 0 に進む。この説明は図 2 (b) を参照して以下に詳細に行う。

【 0 0 4 3 】

もしもユーザー告知が必要であるとステップ 2 2 4 で決定されると、ステップ 2 2 6 に

50

においてユーザーからの告知がユーザーインターフェース106(図1)を介して伝送される。ユーザーインターフェース106は音、映像、振動、またはユーザーの注意を引き付ける他の手段を用いてユーザーに位置要求が許可されたことを通知し、更に図形、テキストまたは音声による表示又は他のプレゼンテーションが、位置要求に関連する情報、例えば要求者のカテゴリー、要求者の身元、および/または要求されたQoSを伝送するために用いられる。

【0044】

ステップ228において、プライバシーエンジン120はプライバシーポリシーを用いて、ユーザー告知に加えて位置要求がユーザーの応答を必要とするか否かを決定する。もし必要が無いときは、この発明の方法は更に他の処理のために流れ図の接続点230を介して図2(b)のステップ250に進む。もしユーザー応答が必要であるときは、ユーザー応答のための待ち時間がステップ232において初期化される。

10

【0045】

図2(b)は図2(Aa)-2(c)の統一化された流れ図に接続される流れ図であり、ステップ232(ユーザー応答のための待ち時間)から処理が進められる。ステップ234、236、238はステップ232の待ち時間に終了するイベントを示している。ステップ240はステップ232の待ち時間の間に起こるイベントを示している。

【0046】

ステップ232においてユーザー応答のための待ち時間がステップ234で示されたイベントであるユーザーアクセプト要求により終了されると、位置要求データが更なる処理のためにステップ250に転送される。

20

【0047】

もしもステップ232においてユーザー応答のための待ち時間がユーザー応答がないためにステップ236のイベントであるタイムアップにより終了すると、位置要求データが送信され、さらに処理を行うためにステップ242に進む。このステップ242においてプライバシーポリシーが用いられてユーザー応答の欠落が拒否を要するものであるか否かを決定する。ユーザー応答の欠落が拒否を要求する場合は、この発明技術の流れ図の接続点220を介してステップ222(図2(a))に進む。もし、ユーザー応答の欠落が拒否を必要としないときは、更なる処理のためにステップ250に進む。

【0048】

30

もしステップ232におけるユーザー応答の待ち時間がステップ238(ユーザー無視要求)で示されるイベントにより終了すると、この発明による方法の処理は流れ図の接続点220を介して図2(a)のステップ222に進む。

【0049】

図2(b)に示したように、もしも新しい位置要求がステップ238の待ち時間の間に受信されると、即ちステップ240(待ちの間の新しい位置要求の到来)で示されるイベントがユーザー応答時間が終了する前に生じると、プライバシーエンジン120(図1)により受信された新しい位置要求データが送信され、処理はステップ244に進む。

【0050】

更に、図2(b)のステップ244において新しい位置要求が調べられ、この要求が緊急サービス要求であるか否かが決定される。緊急サービス要求に対して、流れ図の接続点246を介して処理がステップ288(図2(d))に進む。ステップ288において位置要求カウンタがインクリメントされ、処理はステップ290に進む。ステップ290において、前の位置要求に対する処理が中断され、以下に説明するように後続の処理のために待ちの状態に置かれる。他の実施形態(図示せず)において処理はステップ290における前の位置要求を停止させることもできる。更に他の実施形態(図示せず)においては、PDモジュール122(図1)が複数の同時要求を処理できる手段が提供される。ステップ290に続いて、処理は流れ図接続点214を介してステップ256(図2(b))に進み、緊急サービス要求に対する迅速な処理が行われる。新しい要求が緊急要求でない場合、処理はステップ244からステップ248(図2(b))に直接進む。

40

50

【 0 0 5 1 】

ステップ 2 4 8 において位置要求カウンタがインクリメントされる。処理はステップ 2 6 0 に進み、新しい位置要求データが次の処理のために伝送される。ステップ 2 6 0 において、新しい位置要求データが次の処理のためにデータ列内に配置される。ステップ 2 6 0 が終了すると、処理はステップ 2 3 2 に戻り、ユーザーからの応答を待つ。他の実施形態においては代替りの処理ステップを追加することができ、ステップ 2 4 8 の処理の前に使用できる。これにより、新しい位置要求を処理列に加える代わりに無視すべきか否かの決定を行うことができる。これらの実施形態においては、追加された処理ステップにより受理できない要求を無視することができるために、結果的に全体の処理効率が向上することになる効果が得られる。例えば、受理できない Q o S を示す要求は処理列に加える代わりに直ちに無視することができる。

10

【 0 0 5 2 】

図 2 (b) に示したように、ステップ 2 5 0 はステップ 2 3 4、2 4 2 のいずれかから、或いは (流れ図接続点 2 3 0 を介して) ステップ 2 2 8 (図 2 (a)) から処理に入ることができる。ステップ 2 5 0 において、Q o S を示す位置要求データは現在の位置要求に適用されているプライバシールールと比較される。実施形態の動作の説明のために、場所要求アプリケーションに戻されるべき位置データの精度を示すものとする。もしも位置要求データによって指定された Q o S が現在の位置要求のために適用されたプライバシールールによって指定された限度に対応する場合、処理はステップ 2 5 6 に進む。もしも位置要求データによって指定された Q o S がプライバシーポリシーの限度に対応しない場合は、ステップ 2 5 6 の処理に進む前にステップ 2 5 2 において対応するように変換される。Q o S 仕様の目的と使用の更に明確な説明は以下のアプリケーションの説明の章において行われる。

20

【 0 0 5 3 】

ステップ 2 5 6 において、図示した方法は P D モジュール 1 2 2 (図 1) を作動させ、位置要求データと現在のプライバシーポリシーの内容に応じて位置データを取り込む。ここまで述べたように、緊急またはプライバシー無視の要求が受信されると、ステップ 2 1 2、2 1 6 (図 2 (a)) またはステップ 2 9 0 (図 2 (d)) に続くステップ 2 5 6 が流れ図の接続点 2 1 4 を介して使用される。処理はその後ステップ 2 5 8 に進む。このステップ 2 5 8 において、P D M 1 2 2 からの応答の待ち時間の処理が行われる。

30

【 0 0 5 4 】

図 2 (c) は図 2 の流れ図の中に接続されており、ステップ 2 5 8 (図 2 (b)) における待ち時間 (P D M 応答の待ち時間) の処理の後に続く。ステップ 2 6 2 と 2 6 4 とはステップ 2 5 8 の待ち時間を終了させるイベントを示している。ステップ 2 6 6 もステップ 2 5 8 の待ち時間を終了させるイベントを示している。これらのステップは以下に詳細に説明する。

【 0 0 5 5 】

図 2 (c) に示したように、ステップ 2 5 8 の P D M 応答の待ち時間がステップ 2 6 2 のイベント、即ち P D M 1 2 2 がプライバシーエンジン 1 2 0 (図 1) に応答することによって終了すると、処理はステップ 2 6 2 から決定ステップ 2 7 0 に進む。もしステップ 2 5 8 の待ち時間がタイムアウト、即ちステップ 2 6 4 のイベント (タイムアウト) によって終了すると、処理はステップ 2 6 4 からステップ 2 7 2 に進み、エラーメッセージが場所要求アプリケーションに送信される。他の実施形態 (図示せず) において、予め記憶された位置情報をエラーメッセージの代わりに送信するようにしてもよい。ステップ 2 7 2 の後でステップ 2 8 2 に進み、新しい位置要求列の次の位置要求がテストされる。

40

【 0 0 5 6 】

図 2 (c) に示したように、もし新しい位置要求がステップ 2 5 8 の処理の間に発生すると、処理はステップ 2 6 6 (待ち時間の間に新しい位置要求の到来) に進む。ステップ 2 6 6 において新しい位置要求データがプライバシーエンジン 1 2 0 (図 1) に受信される。次のステップ 2 6 8 において新しい位置要求がテストされこの要求が緊急サービス要

50

求であるか否かが決定される。緊急サービス要求に対して処理は流れ図接続点 246 を介してステップ 288 (図 2 (d)) に進み、前述した処理が行われる。もしも新しい要求が緊急要求でないときは、処理はステップ 268 からステップ 274 に直接進む。

【0057】

ステップ 274 において、位置要求カウンタがインクリメントされる。次のステップ 278 において、新しい位置要求データがデータ列に加えられる。ステップ 278 が終了すると、処理はステップ 258 に戻り、待ち時間における PDM 応答待ちとなる。

【0058】

ステップ 258 の待ち時間がプライバシーエンジン 120 (図 1) に対する PDM 122 によって中断されると、図 2 (c) に示すようにステップ 258 からステップ 262 に進む。ステップ 262 において、PDM データがステップ 262 の PDM 122 からプライバシーエンジン 120 に伝送される。この PDM データは位置座標データと QoS データとを含む。ステップ 270 において、QoS を示す PDM データは現在の位置要求に関するプライバシー等級に関連するプライバシールールと比較される。この実施形態の説明において、QoS は場所要求アプリケーションに返送されるべき PDM 位置座標データの予測された精度を示している。PDM データは、例えば、位置推定の精度を示す QoS データに関連する緯度、経度データを含む。PDM データの QoS が現在位置要求のプライバシー等級に関するプライバシールールにより指定された限度に従っていれば、次の処理のためにステップ 280 に進む。PDM データにより指定された QoS が現在のプライバシーポリシーの限度に従っていないときは、QoS データはステップ 276 において変更される。位置推定がステップ 276 において変更されると、処理はステップ 280 に進む。QoS の目的、使用に関する更に詳細な説明は後でアプリケーションの例の章で行う。

【0059】

PDM データはステップ 280 において場所要求アプリケーションに伝送される。次に処理はステップ 282 に進み、新しい位置要求があるか否かが位置要求カウンタに問い合わせられる。カウンタの値がゼロであれば、新しい要求が無いことを示し、処理は待ち状態ステップ 202 (図 2 (a)) に移る。もしもカウンタ値がゼロ以上の整数であると、処理はステップ 284 に進む。ステップ 284 において、新しい位置要求データが新しい位置要求データ列から呼び出される。

【0060】

処理は次にステップ 286 に進み、位置要求カウンタがデクリメントされる。次いで、処理は (流れ図接続点 208 を介して) ステップ 210 (図 2 (a)) に進み、新しい位置要求データの処理を行う。

【0061】

アプリケーションの例

この発明の代表的なアプリケーションにおいて、いくつかのユーザーによる設定が可能なプライバシー等級およびこれらに属する規則やルールを規定することができる。図 1 を参照して説明したように、ユーザーによる設定は、プライバシーエンジン 120 とユーザーインターフェース 106 との間、プライバシー管理サーバ 104 (又は図示しない他のネットワークサーバ) との間、または外部ローカルアプリケーション 116 との間のデータ接続を介して行われる。プライバシーエンジン 120 とプライバシーポリシーとの設定と変更とは安全手段によってのみ許容されることが望ましい。例えば、この安全手段は安全はデジタル通信を行うための方法と手段、パスワードの使用、デジタル証明、及び他の公知の身元証明や真正証明方法などを含む。

【0062】

プライバシー等級は、限定されないが、以下の形式を含む。

【0063】

1. 未知又は未承認 (即ち非信任) の場所要求アプリケーションおよび他の等級に含まれていない要求者の身元に対するデフォルト、

2. 信用のある場所要求アプリケーションおよび他の等級に含まれていない要求者の身

10

20

30

40

50

元に対するデフォルト、

3. 場所要求アプリケーションおよび要求者の身元を含むユーザー指定の等級。

【0064】

各プライバシー等級は、限定されないが、以下のプライバシールールを含む。

【0065】

1. デフォルトの承認又は拒否の明細、または指定された制限に付随する承認、

2. ユーザー告知要求の明細、

2 a. 絶対的に要求され、または要求されないユーザー告知、および要求されたQoSに基づく告知（例えば、ユーザーは10メートルより高精度の位置推定の要求を告知するように指定する。これにより、もしも位置要求データが5メートル精度の位置推定でQoSを指定すると、ユーザーは告知される。）、及び

2 b. 要求が定期的なものか或いは必要に応じて発生されるものかに基づいた告知、

2 c. 発生時間、曜日、日付、または時間による限定に基づく告知。

【0066】

3. ユーザー告知のために用いられる表示モードの明細（例えば表示ユーザーインターフェース中のポップアップアイコン、音による告知、音楽又は他の音響、振動による告知、など）、および表示すべき情報（もしあれば）、

4. 定期的な要求に関して、定期的な要求の夫々に対して明白な告知が要求されているのか、あるいは定期的な要求の最初のものに対してのみ告知が要求されているのか、等の告知要求の明細、

5. 出力されるべきQoSまたは位置推定の精度の明細（例えば、プライバシーポリシー等級はジップコード精度で許容され、あるいは指定されたメートル数より大きい半径内の精度で許容される）、

6. もしもユーザーが告知に対して応答しなかった時のデフォルトの取り扱いの明細（例えば、ユーザーが“OK”ボタンを持つ場合と持たない場合のポップアップウインドウなどの告知に応答しなかったときの許可された要求または許可されなかった要求であって、数秒後に自動的に消去される）、

7. 移動局の場所または一日のうちの時間に基づいて形成される種々のルールの明細（例えば、ユーザーは特定の場所からの応答または一日の内の特定の時間帯の応答を変更または禁止するルールを形成することができる）。

【0067】

この発明概念の一実施形態において、移動局102（図1）は加入者身元モジュール（SIM）、ユニバーサル加入者身元モジュール（USIM）、または着脱可能なユーザー身元モジュール（RUIM）を含むことができる。SIM、USIM、およびRUIM装置は移動局のための着脱できる記憶装置であり、ユーザー特有の情報の安全な記憶装置である。図1を参照して説明したように、SIM、USIM、またはRUIM装置はその他のモジュールブロック112内に含まれる。この実施形態においては、ユーザー特有のプライバシーポリシーデータがSIM、USIM、またはRUIM装置に格納される。これらの装置はプライバシーエンジン120（図1では接続されていないが）と作動的に結合され、ユーザー特有のプライバシーポリシーデータが上述したプライバシーエンジンを用いた動作を行うためにプライバシーエンジン120に伝送される。ユーザー特有のプライバシーポリシーデータがプライバシーエンジンに格納されるために送信される。この格納動作はプライバシーポリシーデータが最初にSIM、USIM、またはRUIMに格納するために送信されるときに、あるいはデータ変更あるいは更新されるときに行われる。SIM、USIM、またはRUIMが移動局102から取り出されると、ユーザー特有のプライバシーポリシー情報はプライバシーエンジン120から都合よく自動的に消去される。移動局中でユーザー特有のデータの着脱可能な記憶装置としてSIM、USIM、またはRUIMを用いることは通信分野の当業者にとっては公知である。SIM装置の使用のための標準方式が、2001年6月の、第3世代パートナーシップ・プロジェクト（3G

10

20

30

40

50

P P)、テクニカル・スペシフィケーション (T S) グループ・ターミナル、加入者身元モジュール・アプリケーション・プログラミング・インターフェース (S I M A P I)、ステージ 1、リリース 1 9 9 9 (3 G P P T S 0 2 . 1 9 V 8 . 0 . 0) の文献に記載されている。この文献はこの明細書中で S I M 装置の説明としてその全てが引用されている。更に、当業者にとって、他の着脱式の記憶装置 (スマートカードまたはメモリスティックのような) を移動局に用いて、ユーザー特有のプライバシーポリシーデータを記憶してプライバシーエンジンと関連して使用する実施形態もこの発明の範囲に含まれることは自明である。

【 0 0 6 8 】

上記の説明に基づき、通信分野の当業者であれば、この明細書の教示範囲を拡大し、L C S に関する個人のプライバシー情報の制御と管理とに一般的に適用することは容易である。

10

【 0 0 6 9 】

更に、通信とコンピュータの分野の当業者にとって、記載された各実施形態の方法を有形化するためにコンピュータにより読み取り可能な媒体を用いることは自明のことである。例えば、図 2 (a) - 2 (c) を参照して説明された方法のステップは、コンピュータにより読み取り可能な媒体に記録された一連のコンピュータにより実行可能な命令として実施することができる。このような媒体は、限定されないが、R A M、R O M、E P R O M、E E P R O M、フロッピー (登録商標) ディスク、ハードディスク、C D - R O M などを含むことができる。この明細書の記載には更に、説明された各実施形態の方法のステップを、フィールドプログラマブルゲートアレイや、プログラマブルロジックアレイや、コンピュータプログラム命令を用いるように製造しまたは変更することができる他の集積回路のような集積回路中のデジタルロジックとして組み合わせる内容を含んでいる。

20

【 0 0 7 0 】

この明細書に記載された移動局 1 0 2 としては、限定されないが、無線電話、無線通信可能なパーソナルデジタルアシスタント、無線通信機能を持つラップトップ、および無線接続を介して個人通信を行うための他の種々のモバイルデジタル装置を含むことができる。

【 0 0 7 1 】

この発明概念の種々の実施形態が以上の説明に示されている。更に、ここで述べられた発明の範囲から逸脱しないで種々の変形が可能であることが分かる。例えば、この発明はソフトウェア又はハードウェアで実施可能であり、更にハードウェアとソフトウェアを組み合わせた実施形態により実施可能である。他の例として、一つのモジュールの部分として説明された機能は他のモジュールにおいて同様に遂行可能であることが分かる。更に他の例として、特定のシーケンス中で示されまたは述べられたステップ又は動作は、特定の順番のステップとして請求項の中で記載された場合に対応する実施形態を除いて、異なる順序で実行可能である。

30

【 0 0 7 2 】

従って、この発明の概念は説明された実施形態に限定されることはなく、請求項の範囲により限定されることが分かる。明細書の記載は請求項に記載されたものと同様の特徴の実施形態を示すが、そのような同様の特徴は、請求項の範囲を包含する本質部分と同一である場合を除き、請求項中の特徴と同じであると推定すべきでない。幾つかの場合において、請求項中の特徴と明細書中の特徴との意図された相違点は僅かに異なる用語によって強調されるものである。

40

【 図面の簡単な説明 】

【 0 0 7 3 】

【 図 1 】 この発明の概念を用いるために適用されたプライバシーエンジンを具えた移動局を含む典型的な通信システムのブロック図である。

【 図 2 (a) 】 移動局および他の無線通信装置によって用いられる位置サービスアプリケーションにおける強化されたユーザープライバシーを与えるための典型的な方法の流れ図

50

を示す。

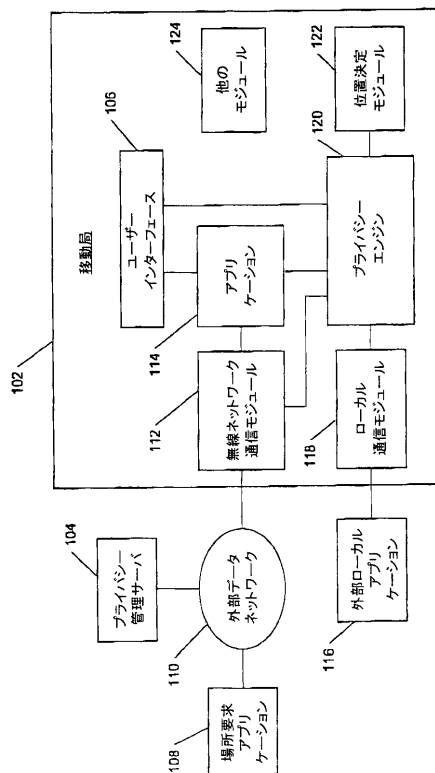
【図2(b)】移動局および他の無線通信装置によって用いられる位置サービスアプリケーションにおける強化されたユーザープライバシーを与えるための典型的な方法の流れ図を示す。

【図2(c)】移動局および他の無線通信装置によって用いられる位置サービスアプリケーションにおける強化されたユーザープライバシーを与えるための典型的な方法の流れ図を示す。

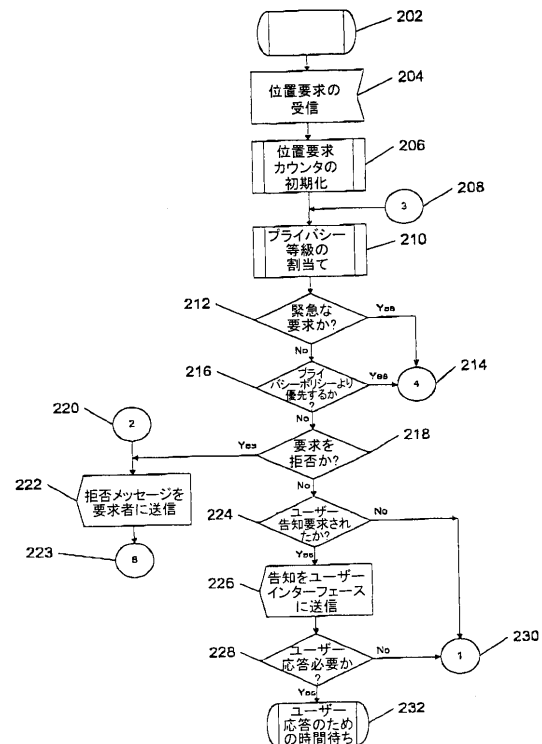
【図2(d)】移動局および他の無線通信装置によって用いられる位置サービスアプリケーションにおける強化されたユーザープライバシーを与えるための典型的な方法の流れ図を示す。

10

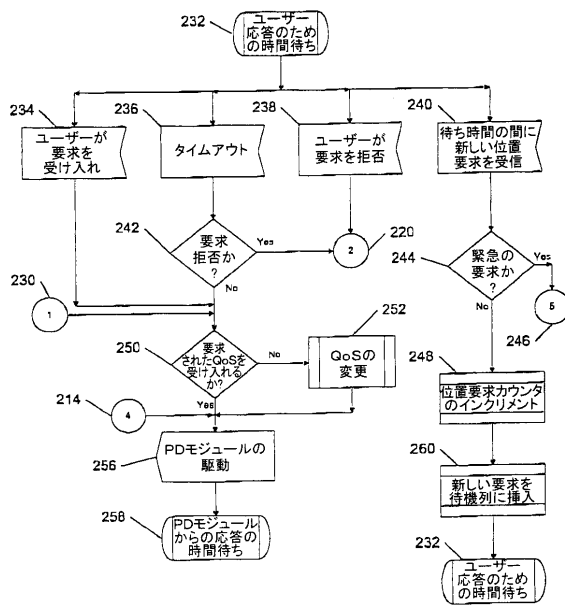
【図1】



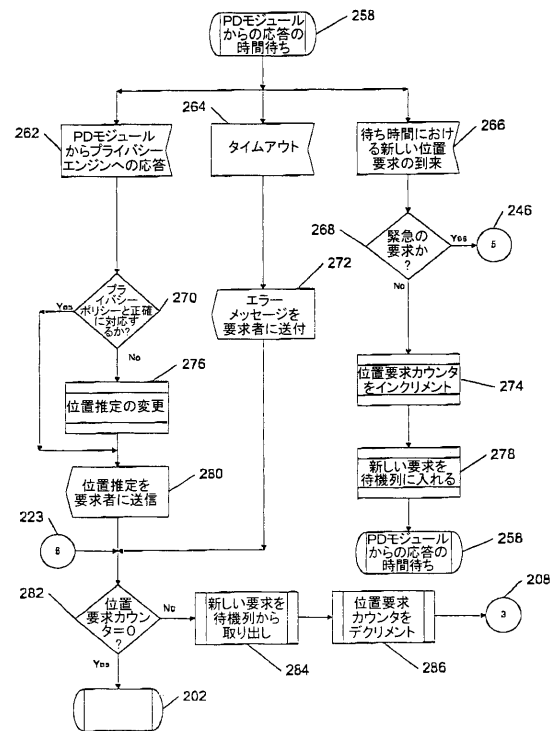
【図2a】



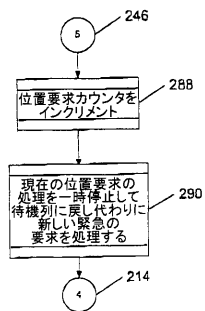
【図 2 b】



【図 2 c】



【図 2 d】



フロントページの続き

- (31)優先権主張番号 10/779,109
(32)優先日 平成16年2月13日(2004.2.13)
(33)優先権主張国 米国(US)

前置審査

- (74)代理人 100075672
弁理士 峰 隆司
(74)代理人 100095441
弁理士 白根 俊郎
(74)代理人 100084618
弁理士 村松 貞男
(74)代理人 100103034
弁理士 野河 信久
(74)代理人 100119976
弁理士 幸長 保次郎
(74)代理人 100153051
弁理士 河野 直樹
(74)代理人 100140176
弁理士 砂川 克
(74)代理人 100101812
弁理士 勝村 紘
(74)代理人 100124394
弁理士 佐藤 立志
(74)代理人 100112807
弁理士 岡田 貴志
(74)代理人 100111073
弁理士 堀内 美保子
(74)代理人 100134290
弁理士 竹内 将訓
(74)代理人 100127144
弁理士 市原 卓三
(74)代理人 100141933
弁理士 山下 元
(72)発明者 アーセンス、スザンヌ
アメリカ合衆国、カリフォルニア州 95051、サンタ・クララ、ナンバー365、ハルフォード・アベニュー 1760

審査官 望月 章俊

- (56)参考文献 米国特許第06360102(US,B1)
特開2003-021534(JP,A)

- (58)調査した分野(Int.Cl.,DB名)
H04W4/00-H04W99/00
H04B7/24-H04B7/26