

(19) 日本国特許庁(JP)

(12) 公表特許公報(A)

(11) 特許出願公表番号

特表2015-537401

(P2015-537401A)

(43) 公表日 平成27年12月24日(2015. 12. 24)

(51) Int.Cl.	F I	テーマコード (参考)
H04L 9/14 (2006.01)	H04L 9/00 641	5J104
H04W 64/00 (2009.01)	H04W 64/00 120	5K067
G06F 21/62 (2013.01)	H04W 64/00 140	
	G06F 21/62 363	

審査請求 未請求 予備審査請求 未請求 (全 45 頁)

(21) 出願番号 特願2015-531328 (P2015-531328)
 (86) (22) 出願日 平成25年9月10日 (2013. 9. 10)
 (85) 翻訳文提出日 平成27年4月13日 (2015. 4. 13)
 (86) 国際出願番号 PCT/US2013/059102
 (87) 国際公開番号 W02014/043147
 (87) 国際公開日 平成26年3月20日 (2014. 3. 20)
 (31) 優先権主張番号 61/699, 800
 (32) 優先日 平成24年9月11日 (2012. 9. 11)
 (33) 優先権主張国 米国 (US)
 (31) 優先権主張番号 14/010, 437
 (32) 優先日 平成25年8月26日 (2013. 8. 26)
 (33) 優先権主張国 米国 (US)
 (31) 優先権主張番号 14/023, 427
 (32) 優先日 平成25年9月10日 (2013. 9. 10)
 (33) 優先権主張国 米国 (US)

(71) 出願人 513114825
 ネクストナヴ, エルエルシー
 アメリカ合衆国カリフォルニア州94085,
 サニーベール, オークミード・パーク
 ウェイ 484
 (74) 代理人 100109634
 弁理士 舩谷 威志
 (74) 代理人 100129263
 弁理士 中尾 洋之
 (74) 代理人 100160369
 弁理士 黒田 仁志
 (74) 代理人 100163991
 弁理士 加藤 慎司
 (74) 代理人 100146374
 弁理士 有馬 百子

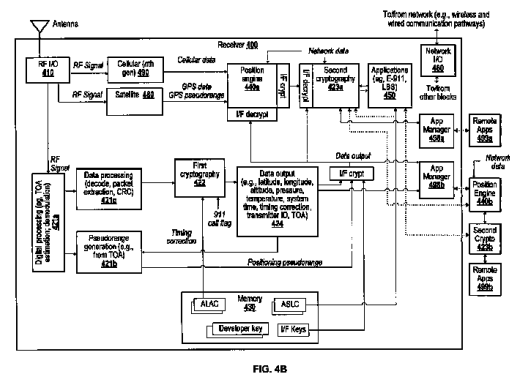
最終頁に続く

(54) 【発明の名称】 送信された情報への条件付きアクセスを提供するシステムおよび方法

(57) 【要約】

本開示は、特定のソフトウェアアプリケーションもしくはそのソフトウェアアプリケーションの配信者について、要求されたサービス種別、ユーザ種別、装置種別、ソフトウェアアプリケーション種別、課金および/またはその他の特性を含むさまざまな考慮事項に基づいて、受信機または受信機外部の他の装置における測位情報に対するアクセスを管理するシステム、方法、コンピュータプログラム製品および手段に関する。本開示はさらに、他のアプリケーションのうちの特定のアプリケーションについてセキュアなデータ送信を実行するシステム、方法、コンピュータプログラム製品および手段に関する。

【選択図】 図4B



【特許請求の範囲】**【請求項 1】**

少なくとも 1 つの処理部を含み、1 つ以上のアプリケーションによる位置情報へのアクセスを管理するシステムであって、前記処理部は、

地上波送信機のネットワークから受信した第 1 の組の暗号化された位置信号を第 1 の鍵を用いて復号し、

前記第 1 の組の復号された位置信号から位置情報を判別し、

第 1 の組の位置情報を識別し、該第 1 の組の位置情報は、第 1 のアプリケーションに対応する第 1 のサービスレベルに基づいて識別され、

前記第 1 の組の位置情報を第 2 の鍵を用いて暗号化し、

前記暗号化された第 1 の組の位置情報を前記第 1 のアプリケーションへ提供するように動作可能な、位置情報へのアクセスを管理するシステム。

10

【請求項 2】

前記第 1 の組の位置情報は、地上波送信機のネットワークからの 1 つ以上の送信機の位置座標、タイミング修正値および大気測定値のうち少なくとも 1 つを含む請求項 1 のシステム。

【請求項 3】

前記処理部はさらに、

前記復号された位置信号を用いて受信機の位置の推定座標を算出するように動作可能であり、前記第 1 の組の位置情報は前記受信機の推定座標を含む請求項 1 のシステム。

20

【請求項 4】

前記復号された位置信号は、前記地上波送信機のそれぞれにおける大気測定値を指定するデータを含み、前記推定座標は、前記復号された位置信号および前記受信機における少なくとも 1 つの大気測定値を用いて算出された高度座標を含む請求項 3 のシステム。

【請求項 5】

前記処理部はさらに、

前記復号された位置信号を用いて受信機の位置の推定座標を算出し、

前記第 1 のアプリケーションに許可された精度レベルに基づいて前記推定座標に基づく修正された座標を算出するように動作可能であり、

前記修正された座標は、前記受信機の位置の指定が前記推定座標より低精度であり、前記第 1 の組の位置情報は前記修正された座標を含む請求項 1 のシステム。

30

【請求項 6】

前記処理部はさらに、

第 2 の組の位置情報を識別し、該第 2 の組の位置情報は、第 2 のアプリケーションに対応する第 2 のサービスレベルに基づいて識別され、前記第 1 の組に含まれる特定の位置情報は前記第 2 の組に含まれず、

前記第 2 の組の位置情報を第 3 の鍵を用いて暗号化し、

前記第 2 の組の位置情報を前記第 2 のアプリケーションへ提供するように動作可能な請求項 1 のシステム。

【請求項 7】

40

前記処理部はさらに、

地上波送信機のネットワークから受信した第 2 の組の暗号化された位置信号を前記第 1 の鍵または第 3 の鍵を用いて復号し、前記第 1 の組の暗号化された位置信号は、前記受信機の第 1 の位置において受信され、前記第 2 の組の暗号化された位置信号は、前記受信機の第 2 の位置における受信機であり、

前記第 2 の組の復号された位置信号からさらなる位置情報を判別し、

第 2 の組のさらなる位置情報を識別し、該第 2 の組のさらなる位置情報は、第 2 のアプリケーションに対応する第 2 のサービスレベルに基づいて識別され、

前記第 2 の組の位置情報を第 4 の鍵を用いて暗号化し、

前記第 2 の組の位置情報を前記第 2 のアプリケーションへ提供するように動作可能な請

50

求項 1 のシステム。

【請求項 8】

前記処理部はさらに、

前記第 1 の組の位置情報の識別前に、前記第 1 のサービスレベルを指定する情報が前記受信機に蓄積されているかを判別し、

前記第 1 のサービスレベルを指定する情報が前記受信機に蓄積されていないと判別されると、前記第 1 のアプリケーションに対応する第 1 の開発者鍵にアクセスし、

該第 1 の開発者鍵をサーバへ送り、

該第 1 の開発者鍵の前記サーバへの送信に呼応して、前記第 1 のサービスレベルを指定する情報を受信するように動作可能な請求項 1 のシステム。

10

【請求項 9】

前記第 1 のサービスレベルを指定する情報は、前記第 1 のアプリケーションに対応する第 1 の認証済サービスレベル証明書に含まれ、該証明書は前記開発者鍵に対応する請求項 8 のシステム。

【請求項 10】

前記第 1 のサービスレベルは、前記第 1 の組の位置情報および任意の後続位置情報の任意の後続する組を前記第 2 の鍵を用いて暗号化することが可能な期間を指定する請求項 1 のシステム。

【請求項 11】

前記第 2 の鍵は、前記位置信号が復号された後に生成されるセッション鍵である請求項 1 のシステム。

20

【請求項 12】

第 1 のアプリケーションは遠隔サーバにて走行し、前記第 1 の組の位置情報は該遠隔サーバへ提供される請求項 1 のシステム。

【請求項 13】

前記処理部はさらに、

前記第 1 のアプリケーションに対応する第 1 の証明書において指定されたパラメータに基づいて前記第 1 のサービスレベルを判別するように動作可能な請求項 1 のシステム。

【請求項 14】

前記処理部はさらに、

保護されていない通信路を通して前記位置情報が送られる前に該位置情報をスクランブルし、

30

前記第 1 の組を識別する前に前記スクランブルされた位置情報をスクランブル解除するように動作可能な請求項 1 のシステム。

【請求項 15】

前記処理部はさらに、

保護されていない通信路を通して前記推定座標が送られる前に該推定座標をスクランブルし、

前記第 1 の組の暗号化前に前記スクランブルされた推定座標をスクランブル解除するように動作可能な請求項 3 のシステム。

40

【請求項 16】

前記処理部はさらに、

複数の鍵なかから前記第 1 の鍵を選択し、前記暗号化された位置信号の CRC フィールドは、前記第 1 の鍵を用いて前記第 1 の組の暗号化された位置信号を復号する場合にのみチェックを通過させるように動作可能な請求項 1 のシステム。

【請求項 17】

前記処理部はさらに、

複数の鍵のなかから前記第 1 の鍵を選択し、前記復号された位置信号のデータは、前記第 1 の鍵を用いて前記第 1 の組の暗号化された位置信号を復号する場合にのみ、予測される範囲の値と照合するように動作可能な請求項 1 のシステム。

50

【請求項 18】

前記第 1 の組の暗号化された位置信号は複数の送信機からのパケットデータを含み、前記処理部はさらに、

複数の鍵なかから前記第 1 の鍵を選択し、前記複数の送信機からの前記パケットデータは、前記第 1 の鍵を用いて前記第 1 の組の暗号化された位置信号を復号する場合にのみ、1 つ以上の整合性チェックを通過させるように動作可能な請求項 1 のシステム。

【請求項 19】

コンピュータで実行され、1 つ以上のアプリケーションによる位置情報へのアクセスを管理する方法であって、該方法は、

地上波送信機のネットワークから受信した第 1 の組の暗号化された位置信号を第 1 の鍵を用いて復号するステップと、

前記第 1 の組の復号された位置信号から位置情報を判別するステップと、

第 1 の組の位置情報を識別し、該第 1 の組の位置情報は、第 1 のアプリケーションに対応する第 1 のサービスレベルに基づいて識別されるステップと、

前記第 1 の組の位置情報を第 2 の鍵を用いて暗号化するステップと、

該暗号化された第 1 の組の位置情報を前記第 1 のアプリケーションへ提供するステップとを含み、少なくとも 1 つの処理部が前記ステップのうち少なくとも 1 つを実行する、コンピュータで実行される方法。

【請求項 20】

前記第 1 の組の位置情報は、地上波送信機のネットワークからの 1 つ以上の送信機の位置座標、タイミング修正値および大気測定値のうち少なくとも 1 つを含む請求項 19 のコンピュータで実行される方法。

【請求項 21】

前記方法は、

受信機の位置の推定座標を前記復号された位置信号を用いて算出するステップを含み、前記第 1 の組の位置情報は、前記受信機の推定座標を含む請求項 19 のコンピュータで実行される方法。

【請求項 22】

前記復号された位置信号は、前記地上波送信機のそれぞれにおける大気測定値を指定するデータを含み、前記推定座標は、前記復号された位置信号および前記受信機における少なくとも 1 つの大気測定値を用いて算出された高度座標を含む請求項 21 のコンピュータで実行される方法。

【請求項 23】

前記方法は、

受信機の位置の推定座標を前記復号された位置信号を用いて算出するステップと、

前記第 1 のアプリケーションに許可された精度レベルに基づいて前記推定座標に基づく修正された座標を算出するステップとを含み、該修正された座標は、前記受信機の指定が前記推定座標より低精度であり、前記第 1 の組の位置情報は前記修正された座標を含む請求項 19 のコンピュータで実行される方法。

【請求項 24】

前記処理部はさらに、

第 2 の組の位置情報を識別し、該第 2 の組の位置情報は、第 2 のアプリケーションに対応する第 2 のサービスレベルに基づいて識別され、前記第 1 の組に含まれる特定の位置情報は前記第 2 の組に含まれず、

前記第 2 の組の位置情報を第 3 の鍵を用いて暗号化し、

前記第 2 の組の位置情報を前記第 2 のアプリケーションへ提供するように動作可能な請求項 19 のコンピュータで実行される方法。

【請求項 25】

前記処理部はさらに、

地上波送信機のネットワークから受信した第 2 の組の暗号化された位置信号を前記第 1

10

20

30

40

50

の鍵または第 3 の鍵を用いて復号し、前記第 1 の組の暗号化された位置信号は、前記受信機の第 1 の位置において受信され、前記第 2 の組の暗号化された位置信号は、前記受信機の第 2 の位置における受信機であり、

前記第 2 の組の復号された位置信号からさらなる位置情報を判別し、

第 2 の組のさらなる位置情報を識別し、該第 2 の組のさらなる位置情報は、第 2 のアプリケーションに対応する第 2 のサービスレベルに基づいて識別され、

前記第 2 の組の位置情報を第 4 の鍵を用いて暗号化し、

前記第 2 の組の位置情報を前記第 2 のアプリケーションへ提供するように動作可能な請求項 19 のコンピュータで実行される方法。

【請求項 26】

10

前記処理部はさらに、

前記第 1 の組の位置情報の識別前に、前記第 1 のサービスレベルを指定する情報が前記受信機に蓄積されているかを判別し、

前記第 1 のサービスレベルを指定する情報が前記受信機に蓄積されていないと判別されると、前記第 1 のアプリケーションに対応する第 1 の開発者鍵にアクセスし、

該第 1 の開発者鍵をサーバへ送り、

該第 1 の開発者鍵の前記サーバへの送信に呼応して、前記第 1 のサービスレベルを指定する情報を受信するように動作可能な請求項 19 のコンピュータで実行される方法。

【請求項 27】

20

前記第 1 のサービスレベルを指定する情報は、前記第 1 のアプリケーションに対応する第 1 の認証済サービスレベル証明書に含まれ、該証明書は前記開発者鍵に対応する請求項 26 のコンピュータで実行される方法。

【請求項 28】

前記第 1 のサービスレベルは、前記第 1 の組の位置情報および任意の後続位置情報の任意の後続する組を前記第 2 の鍵を用いて暗号化することが可能な期間を指定する請求項 19 のコンピュータで実行される方法。

【請求項 29】

前記第 2 の鍵は、前記位置信号が復号された後に生成されるセッション鍵である請求項 19 のコンピュータで実行される方法。

【請求項 30】

30

第 1 のアプリケーションは遠隔サーバにて走行し、前記第 1 の組の位置情報は該遠隔サーバへ提供される請求項 19 のコンピュータで実行される方法。

【請求項 31】

前記方法は、前記第 1 のアプリケーションに対応する第 1 の証明書において指定されたパラメータに基づいて前記第 1 のサービスレベルを判別するステップを含む請求項 19 のコンピュータで実行される方法。

【請求項 32】

前記方法は、

保護されていない通信路を通して前記位置情報が送られる前に該位置情報をスクランブルするステップと、

40

前記第 1 の組を識別する前に前記スクランブルされた位置情報をスクランブル解除するステップとを含む請求項 19 のコンピュータで実行される方法。

【請求項 33】

前記方法は、

保護されていない通信路を通して前記推定座標が送られる前に該推定座標をスクランブルするステップと、

前記第 1 の組の暗号化前に前記スクランブルされた推定座標をスクランブル解除するステップとを含む請求項 21 のコンピュータで実行される方法。

【請求項 34】

前記方法は、

50

複数の鍵のなかから前記第 1 の鍵を選択し、前記暗号化された位置信号の CRC フィールドは、前記第 1 の鍵を用いて前記第 1 の組の暗号化された位置信号を復号する場合にのみチェックを通過させるステップを含む請求項 19 のコンピュータで実行される方法。

【請求項 35】

前記方法は、

複数の鍵のなかから前記第 1 の鍵を選択し、前記復号された位置信号のデータは、前記第 1 の鍵を用いて前記第 1 の組の暗号化された位置信号を復号する場合にのみ、予測される範囲の値と照合するステップを含む請求項 19 のコンピュータで実行される方法。

【請求項 36】

前記第 1 の組の暗号化された位置信号は複数の送信機からのパケットデータを含み、前記方法は、

10

複数の鍵のなかから前記第 1 の鍵を選択し、前記複数の送信機からの前記パケットデータは、前記第 1 の鍵を用いて前記第 1 の組の暗号化された位置信号を復号する場合にのみ、1 つ以上の整合性チェックを通過させるステップを含む請求項 19 のコンピュータで実行される方法。

【発明の詳細な説明】

【分野】

【0001】

本開示は、主に測位システムおよび方法に関する。より詳細には、本開示は、位置情報へのアクセスを管理するシステムおよび方法に関するものであるが、これに限らない。

20

【背景】

【0002】

位置情報を提供する数々のシステムが当該分野において公知である。例えば、LORAN、GPS、GLONASS などの無線ベースのシステムを用いて人、車両、装置などの位置情報を提供してきた。しかし、これらのシステムの場合、位置精度、送受信信号レベル、無線チャネル干渉、および / または、例えばマルチパス、装置電力消費などの伝送路問題などの諸要因に関連する制約があった。

【0003】

モバイル加入者の正確な位置を判別することは、極めて困難である場合がある。加入者が屋内にいたり障害物の多い都市部にいたりする場合、加入者のモバイルデバイスは、GPS 衛星から信号を受信できず、ネットワークは、精度の低いネットワークベースの三角測量 / マルチラレーション方式に依存せざるを得ない場合がある。さらに、加入者が高層建物内にいても、建物内であることは分かっているが何階にいるか分からない場合、(命の危険に関わり得る) 緊急支援の提供が遅れてしまうことがある。明らかに必要なのは、加入者のコンピューティングデバイス (例えば、モバイルコンピューティングデバイス) の位置判別処理の高速化に役立ち、より高精度 (高さ情報を含む) を提供し、都市部および建物内における位置判別問題の一部を解消することが可能なシステムである。

30

【0004】

さらに、GPS などのシステムにおいて送信される位置情報は、さまざまな装置にとって容易に利用可能であり、位置情報へアクセス可能な装置を規制するか、またはより具体的には、装置に搭載されて位置情報を利用可能なソフトウェアアプリケーションを規制するという選択肢は無い。このような規制ができないため、多数の装置上の多数のアプリケーションからネットワークを通してそれらのアプリケーションに関連するサードパーティサービスへ位置情報が送られると、ネットワーク管理者にとって帯域幅の負担となり得る。位置情報の利用を規制することができれば、ネットワーク管理者は、不要な帯域幅の利用を低減しつつ、顧客へのより良いサービスレベルを維持することができる。さらに、ネットワーク管理者による管理を拡大することができれば、ユーザ装置ごとの、またはユーザ装置の各ユーザごとのアプリケーションレベルもしくはサービスレベルで収益化が可能になる。よって、既存の測位システムおよび装置におけるこれらの問題および / または

40

50

他の問題に対処することが可能な、向上した測位システムが必要とされている。

【概要】

【0005】

説明するのは、いくつかのシステム、方法およびコンピュータプログラム製品であり、プログラム製品は、コンピュータ読取り可能なプログラムコードが内部で具現化されコンピュータで利用可能な媒体を含み、プログラムコードは、実行すると、コンピューティングデバイスの位置情報への条件付きアクセスを提供する方法を実現するように構成されている。例えば、本開示の特定の態様は、1つ以上のアプリケーションによる位置情報へのアクセスを管理するシステム、方法、コンピュータプログラム製品および手段に関する。これらのシステム、方法、コンピュータプログラム製品および手段は、地上波送信機のネットワークから受信した第1の組の暗号化された位置信号を第1の鍵を用いて復号することができる。本システム、方法、コンピュータプログラム製品および手段はさらに、第1の組の復号された位置信号から位置情報を判別し、第1の組の位置情報を識別することができる。第1の組の位置情報は、第1のアプリケーションに対応する第1のサービスレベルに基づいて識別される。本システム、方法、コンピュータプログラム製品および手段はさらに、第2の鍵を用いて第1の組の位置情報を暗号化し、暗号化された第1の組の位置情報を第1のアプリケーションへ提供することができる。他のさまざまな態様、特徴および機能について、以下に添付図面と共に述べる。

10

【図面の簡単な説明】

【0006】

20

以下、図面および詳細な説明に移る。

【図1】は、各実施形態を実現可能な地上波位置/測位システムの詳細を示す図である。

【図2】は、各実施形態を実現可能な地上波位置/測位システムの特定の詳細例を示す図である。

【図3】は、送信機/ビーコンを示す図である。

【図4A】は、受信機の一実施形態の詳細を示す図である。

【図4B】は、受信機/ユーザ装置の一実施形態および受信機/ユーザ装置外部の他の構成要素の詳細を示す図である。

【図4C】は、受信機/ユーザ装置の別の実施形態および受信機/ユーザ装置外部の他の構成要素の詳細を示す図である。

30

【図5A】は、ある受信機について位置情報を判別し、その受信機における当該位置情報へのアクセスを管理する処理を示す。

【図5B】は、E-911呼の位置情報を配信する処理を示す。

【図5C】は、未設定鍵についての処理を示す。

【図5D】は、事前設定された鍵の処理を示す。

【図6】は、位置情報への条件付きアクセスを提供する処理を示す。

【図7】は、条件付きアクセス証明書を設定する処理を示す。

【図8】は、位置情報を処理する処理を示す。

【図9】は、条件付きアクセス処理時において用いられるデータの種別を示す。

【図10A】は、パケット構造を示す。

40

【図10B】は、特定の態様で用いられるビット列を示す。

【図11】は、受信機/ユーザ装置における位置情報への条件付きアクセスを提供する処理を示す。

【詳細な説明】

【0007】

本開示の多様な態様について以下に述べる。本願の教示内容は、さまざまな形態で具現化可能であり、本願に開示される特定の構造、機能またはその両方は、どれもあくまで例示であることが明らかである。当業者であれば、本願の教示内容に基づいて、どの開示の態様も他のどの態様とは別個に実現可能であり、これらの態様のうち2つ以上をさまざまに組み合わせることが可能であることを理解する。例えば、本願に記載された各態様をい

50

くつか用いて、1つのシステムを実現することもできるし、あるいは1つの方法を実行することもできる。

【0008】

本願に用いられる「例示的」という用語は、一例、例示または説明用を意味する。本願において「例示的」なものとして記載された態様および／または実施形態はどれも、必ずしも他の態様および／または実施形態より好適または有利であると解釈すべきものとは限らない。

【概略】

【0009】

本開示は主に、位置判別用信号方式を提供し高精度の位置／測位情報を判別する測位システムおよび方法に関するものであり、これは、携帯電話または他の可搬型装置などの受信機（本願では、ユーザ装置、ユーザ端末／UEまたは類似の用語と同義にも用いる）と通信する広領域送信機配列を用いる。特定の態様に関連する測位信号サービスにおいて、暗号化された測位信号を送信するように構成されたブロードキャスト専用ビーコン／送信機が用いられることがある。相応のチップセットを有する受信機は、エアリンクアクセス認証技術に基づく測位信号を受信し利用することができ、これは、初期復号段階でエアリンクアクセス証明書（ALAC）の保存コピーを用いて位置信号を復号することで認証を行うことを含んでいる。初期復号段階においてALACにより復号すると、受信機は、受信機において動作するソフトウェアアプリケーションに対して別の復号段階に基づいて位置情報への条件付きアクセスを提供することができ、後者の復号段階は、当該特定のソフトウェアアプリケーションに対応して認証済サービスレベル証明書（ASLC）を用いるものである。

10

20

【0010】

受信機内のさまざまな構成要素を用いて、復号段階を実行することができる。例えば、ブロードキャスト信号の復号は、セキュアなハードウェア領域（例えば、GPSチップ内の）のファームウェアに設けられたALACに関連するGPSチップにて行ってもよい。これとは対照的に、ASLCを用いた位置情報の復号は、ファームウェアに設けられていないASLC（例えば、異なるレベルのソフトウェアを介してアクセス可能な）に関連する別のチップ（例えば、受信機の処理回路）にて行ってもよい。もちろん、当業者であれば、別の構成を想到しよう。

30

【0011】

復号されると、位置情報は処理回路（例えば、測位エンジン）によって処理されて、緯度、経度および高度などのさまざまな測位信号データ単位をさまざまな精度で算出することができる。高度計算の例については、「広領域測位システム」と題する2011年11月14日付出願の米国特許出願番号13/296,067号に記載があり、これを引用することにより本願に取り込む。

【0012】

受信機において位置情報の2段階復号を行うことにより、従来技術に比べていくつかの利点を得られる。例えば、2段階復号の各態様によれば、送信機および／または受信機は、認証済受信機および／または認証済ソフトウェアアプリケーション（本願では以下「アプリケーション」と呼ぶ）へ測位信号を提供する一方、未認証受信機および未認証アプリケーションへのアクセスを拒否することができる。同様に、位置情報へのアクセスは、アクセスを要求したユーザまたは他の種類の考慮事項に基づいても制御することができる。

40

【0013】

位置情報へのアクセスを認証に基づいて管理することにより、通信事業者およびアプリケーション開発者は、さまざまな事業契約に基づいて購入可能な階層レベルのサービスを提供することができる。階層レベルとは、精度レベル、カバー領域、有効期間、使用量、使用期間または他の考慮事項に関するものでよい

【0014】

受信機において位置情報の2段階復号を行うことにより、未認証ユーザ（例えば、ハッ

50

カ) が測位情報へのアクセスを得て使用する収益損失に繋がる可能性が低下する。

【 0 0 1 5 】

上記の利点の達成は、測位システムの性能条件に対してバランスをとる必要がある。特定の態様によれば、測位システムにおいて行われる暗号化段階および復号段階は、受信機位置の初期位置算出時間 (T T F F) や何らかの位置判別の精度などのシステム性能指標を損なわなくてよい。さらに、本願に記載のさまざまな条件付きアクセス方法に対応する処理は、特定の受信機の処理能力に起因して制限される場合もあり、その場合、処理集約的な暗号処理手順が排除される可能性がある。

【 0 0 1 6 】

他の態様によれば、条件付きアクセス機能は、さまざまな装置プラットフォームにおいて利用可能であり、本願に記載の使用例で示される配信モデルをサポートすることができる。他の態様では、本願に記載の条件付きアクセス方法をサポートする工場ベースまたは消費者ベースの受信機設定を (何らかの再設定の他に) 行うことができる。例えば、さまざまな設定方式の実施形態が本願に記載されている。重要なことは、本願に記載の条件付きアクセス処理はいずれかも、何らかの E - 9 1 1 機能要件に適合しなければならない。

【 0 0 1 7 】

さらなるさまざまな態様、特徴および機能について、添付図面と共に以下に述べる。本開示の実施形態は、細部が異なっても請求項に記載の開示の範囲内にあればよく、当業者であれば、ここに記載の図面は、発明の各態様の使用または機能性の範囲についてどんな限定も与えないことを理解する。図面およびその説明は、図示の構成要素のいずれか 1 つ、またはそれらの組合せに対して何らかの従属性または要件を課すものと解釈すべきでない。

【 0 0 1 8 】

以下の記載では、多数の特定の細部を提示するが、これは、記載したシステムおよび方法の深い理解および可能な説明を行うためである。しかし、当業者であれば、これらの実施形態は、特定の細部の 1 つ以上がなくても、または他の構成要素、システムなどと共に実施することが可能であることを認識する。他の場合において、周知の構造または動作を図示せず、また詳述もしないことで、開示の実施形態の諸態様の焦点がぼけないようにしている。

【システムとしての態様】

【 0 0 1 9 】

図 1 は、さまざまな実施形態を実現することが可能な例示的な位置 / 測位システム 1 0 0 の詳細を示す図である。測位システム 1 0 0 は、ここでは広領域測位システム (W A P S)、または簡潔に「システム」と称し、典型的には、地上波である同期ビーコン (ここでは「送信機」とも記す) のネットワークと、ユーザ装置 (ここでは「受信機ユニット」、または単に「受信機」とも記す) とを含み、ユーザ装置は、ビーコンおよび / または他の位置信号方式から提供される信号を取得し追跡するように構成され、他の位置信号方式とは、全地球測位システム (G P S) および / または他の衛星または地上波ベースの位置システムなどの衛星システムから提供されるものでよい。これらの受信機は、位置計算エンジンを任意選択的に含んでもよく、ビーコンおよび / または衛星システムから受信した信号から位置 / 測位情報を判別する。システム 1 0 0 はさらに、さまざまな他のシステムと通信するサーバシステムを含んでもよく、他のシステムとは、ビーコンなどの他に、インターネット、セルラネットワーク、広領域もしくはローカルエリアネットワーク、および / または他のネットワークなどのネットワーク・インフラストラクチャなどである。サーバシステムは、アンテナ塔識別情報、課金インタフェース、1 つ以上の専用暗号化アルゴリズムに基づくものでよい 1 つ以上の暗号化アルゴリズム処理部などのさまざまなシステム関連情報、位置計算エンジン、および / または他の処理要素を含んでもよく、システムの各ユーザの位置、動きおよび / または位置判別を促進する。

【 0 0 2 0 】

例示的システム 1 0 0 に示すように、ビーコンは、複数の送信機 1 1 0 の形態をとって

よく、受信機ユニットは、１つ以上のユーザ装置１２０の形態をとってよく、ユーザ装置は、送信機１１０から信号を受信するように構成されたさまざまな電子通信装置のうちのいずれかでよく、任意選択的には、ＧＰＳまたは他の衛星システム信号方式、セルラ信号方式、Ｗｉ－Ｆｉ信号方式、Ｗｉ－Ｍａｘ信号方式、Ｂｌｕｅｔｏｏｔｈ、Ｅｔｈｅｒｎｅｔ、および／または当該分野において公知であるか、または開発された他のデータまたは情報信号方式に対応するように構成してもよい。受信機ユニット１２０は、セルラ電話もしくはスマートフォン、タブレット装置、ＰＤＡ、ノートパソコンもしくは他のコンピュータシステム、デジタルカメラ、商品出所表示タグおよびアングルプレスレット、ならびに／または類似もしくは相当する装置の形態であってよい。いくつかの実施形態において、受信機ユニット１２０は、単独の位置／測位装置でよく、専らもしくは主に、送信機１１０から信号を受信して少なくとも部分的にこの受信信号に基づいて位置／測位判定を行うように構成されたものである。ここに記載のように、受信機ユニット１２０はここでは、「ユーザ装置」（ＵＥ）、ハンドセット、スマートフォン、タブレットおよび／または「受信機」とも称することがある。

10

【００２１】

送信機１１０（ここでは「アンテナ塔」と呼ぶこともある）は、送信機出力信号を複数の受信機ユニット１２０（図１では簡潔のため１台の受信機ユニット１２０を示すが、典型的なシステムは、画成したカバー領域内にある多数の受信機ユニットをサポートするように構成される）へ図示のように通信リンク１１３を介して送るように構成されている。送信機１１０は、通信リンク１３３を介してサーバシステム１３０へ接続してもよく、および／または、有線接続、セルラデータ接続、Ｗｉ－Ｆｉ、Ｗｉ－Ｍａｘもしくは他の無線接続等のネットワーク・インフラストラクチャ１７０への他の通信接続（図示せず）を有してもよい。

20

【００２２】

１台以上の受信機１２０は、複数の送信機１１０からの信号を、送信機１１０のそれぞれの対応する通信リンク１１３を介して受信することができる。加えて、図１に示すように、受信機１２０は、例えばセルラ基地局（ＮｏｄｅＢ、ｅＮＢ、または基地局としても公知）からの通信リンク１６３を介するセルラネットワーク信号、Ｗｉ－Ｆｉネットワーク信号、ページャネットワーク信号または他の有線もしくは無線接続信号、ならびにＧＰＳまたは他の衛星測位システムなどからの衛星通信リンク１５３を介する衛星信号などの他の信号を受信および／または送信するように構成してもよい。図１の例示的实施形態に示す衛星測位信号はＧＰＳシステム衛星１５０から提供される様子が図示されているが、他の実施形態では、信号は他の衛星システムから提供され、および／または、いくつかの実施形態では、地上波ベースの有線もしくは無線測位システムまたは他のデータ通信システムから提供するようにしてもよい。

30

【００２３】

例示的实施形態において、システム１００の送信機１１０は、専用免許または共用免許／免許不要の無線帯域で動作するように構成される。しかし、いくつかの実施形態は、免許不要の共用帯域にて信号を提供するように構成してもよい。送信機１１０は、本願中に後述するような新規な信号方式を用いてさまざまな無線帯域で信号を送ることができる。この信号方式は、位置およびナビゲーション目的に有利に規定されたフォーマットで特定のデータを提供するように構成された専用信号の形態をとってよい。例えば、本願中に後述するように、信号方式は、従来の衛星位置信号が反射やマルチパスなどによって減衰し、および／または影響されるような障害物環境で動作するのに特に有利なように構成してもよい。加えて、信号方式は、迅速な取得および位置判別時間を提供するように構成して、装置電源オンもしくは測位起動時の迅速な位置判別や電力消費低減を可能とし、および／または他の利点を供するようにしてもよい。

40

【００２４】

ＷＡＰＳのさまざまな実施形態は、他の測位システムと組み合わせて高度の位置および測位判別を行なってもよい。これに代わって、または追加して、ＷＡＰＳシステムを用い

50

て他の測位システムを補助してもよい。加えて、W A P S システムの受信機ユニット 1 2 0 の判別した情報は、セルラ、W i - F i、ページャなどの他の通信ネットワークリンク 1 6 3 を介して提供し、位置および位置情報をサーバシステム 1 3 0 ならびにネットワーク・インフラストラクチャ 1 7 0 にある既存の、またはこれに接続された他のネットワーク接続されたシステムへ報告するようにしてもよい。例えば、セルラネットワークでは、セルラバックホールリンク 1 6 5 を用いて受信機ユニット 1 2 0 から対応のセルラ通信事業者等（図示せず）へネットワーク・インフラストラクチャ 1 7 0 を介して情報を提供することができる。これを用いて緊急時に受信機 1 2 0 の位置を迅速かつ正確に特定することができるし、あるいは、これを用いて位置ベースのサービスまたは他の機能をセルラ通信事業者または他のネットワークユーザもしくはシステムから提供することができる。

10

【 0 0 2 5 】

本開示の文脈における測位システムは、緯度、経度および高度座標のうち 1 つ以上によって位置を特定するシステムであり、座標は、1 次元、2 次元または 3 次元座標系（例えば、x、y、z 座標、角度座標等）によって記述または図示してもよい点に留意されたい。加えて、「G P S」という用語を用いる場合、全地球測位航法衛星システム（G N S S）が G L O N A S S などの他の既存の衛星測位システムならびに G a l i l e o および C o m p a s s / B e i d o u などの将来の測位システムを含んでもよいという、より広範な意味の全地球測位航法衛星システム（G N S S）としてそのように用いる点に留意されたい。加えて、先に述べたように、いくつかの実施形態において、衛星ベースの測位システムに加えて、またはこれに代わって地上波ベースの測位システムなどの他の測位システムを用いることも可能である。

20

【 0 0 2 6 】

W A P S の実施形態を挙げると、図 1 に示すような複数の送信機 1 1 0 などのアンテナ塔または送信機が複数あり、これらは、W A P S データ測位情報および / または他のデータもしくは情報を送信機出力信号として受信機 1 2 0 へブロードキャストする。測位信号は、特定のシステムまたは地域的カバレッジ領域の全送信機にわたって同期するように調整され、G P S 基準クロック源を用いてタイミング同期を行うことができる。W A P S データ測位送信は、三辺測量に必要なデータや加入者 / 加入者群への通知の送信、メッセージのブロードキャストおよび / または W A P S ネットワークの全体動作を促進するための専用の通信チャネル資源（例えば、時間、符号および / または周波数）を含んでもよい。W A P S データ測位送信についての開示については、本願に取り込んだ出願に記載がある。

30

【 0 0 2 7 】

到着時間差を用いた測位システムすなわち三辺測量において、送信される測位情報は典型的には、高精度タイミングシーケンスおよび測位信号データのうち 1 つ以上を含み、測位信号データは、送信機の位置およびさまざまなタイミング修正値ならびに他の関連データまたは情報を含む。1 つの W A P S 実施形態において、データは、さらなるメッセージまたは情報、例えば、加入者群のための通知 / アクセス管理メッセージ、一般的ブロードキャストメッセージ、ならびに / またはシステム動作、ユーザ、他のネットワークとのインタフェースおよび他のシステム機能に関連する他のデータもしくは情報を含んでもよい。測位信号データは、複数の方法で提供してもよい。測位信号データは、例えば、符号化されたタイミングシーケンスへ変調したり、そのタイミングシーケンスに付加もしくはオーバーレイし、および / またはこのタイミングシーケンスで連鎖させたりしてもよい。

40

【 0 0 2 8 】

本願に記載のデータ送信方法および装置を用いて、W A P S の位置情報スループットを向上させることができる。詳細には、より高次の変調データを疑似雑音（P N）測距データとは別の情報として送信してもよい。これを用いると、C D M A 多重化、T D M A 多重化または C D M A / T D M A 多重化の組合せを用いたシステムにおける取得速度の向上が可能になる。本願での開示は、同期した測位信号が複数のアンテナ塔から、より詳細には地上波用のアンテナ塔を用いて U E へブロードキャストされる広領域測位システムについて説明している。しかし、実施形態はこれに限定されず、本開示の意図および範囲内で他

50

のシステムも実現可能である。

【 0 0 2 9 】

例示的实施形態において、W A P S は、送信機 1 1 0 などのアンテナ塔または送信機から送られた符号化変調（スペクトル拡散変調または疑似雑音（P N）変調と呼ばれる）を用いて広い帯域幅を達成することができる。受信機またはユーザ装置 1 2 0 などの対応する受信機ユニットは、例えば整合フィルタまたは一連の相関器などの逆拡散回路を用いてこのような信号を処理する 1 つ以上の構成要素を含む。このような受信機によって生成される波形は理想的には、より低レベルのエネルギーによって囲まれた高ピークを有する。ピークの到着時間は、送信された信号の U E における到着時間を示す。高い精度で位置が既知の多数のアンテナ塔からの多数の信号にこの動作を行うことにより、三辺測量を介して受信機位置を判別することができる。送信機 1 1 0 などの送信機における W A P S 信号生成についてのさまざまな他の詳細については、受信機 1 2 0 などの受信機における受信信号処理とともに、本願中で後述する。

10

【 0 0 3 0 】

一実施形態において、W A P S は、2 値符号化変調を拡散方式として用いてもよい。例示的实施形態の W A P S 信号は、特定の 2 種類の情報を含んでもよい。すなわち、（ 1 ）（他の信号に比べて高速に伝送され得る）高精度測距信号、および（ 2 ）送信機 I D および位置などの位置データ、時刻、健康、大気情報（例えば、気圧、気温、湿度、風向および風力、ならびに他の状態）などの環境状態である。W A P S は、G P S と同様に、高速度の 2 値疑似ランダム測距信号をより低速の情報源で変調することにより、位置情報を送信してもよい。本願に加えて、ここに取り込んだ各出願では、疑似ランダム測距信号および変調情報信号を使用する方法の実施形態が開示されている。両者はどちらも、4 値または 8 値変調などのより高次の変調を用いることができる。一実施形態において、測距信号は 2 値位相変調され、位置情報は、より高次の変調を用いて別個の信号として提供される。

20

【 0 0 3 1 】

従来のシステムにおいては、位置信号（例えば、時分割多重構成に用いられる）のフォーマットを用いるが、そのフォーマットでは、各スロット送信において、疑似ランダム測距信号の後にさまざまな種類の位置データが続く。これらの従来のシステムは、同期信号すなわち s y n c 信号も含み、この信号は、疑似ランダム測距信号を s y n c 信号として用いる場合は、なくてよい。しかし、他の従来のシステムの場合のように、これらの従来のシステムの位置データは 2 値であるため、スループットに限界がある。これらのシステムは、位置データが送信される時間間隔で多数の 2 値ビットも送信する。

30

【 0 0 3 2 】

これらの制限に対処するため、例示的实施形態において、2 値または 4 値の疑似ランダム信号を特定のスロット中に入れて送った後、非常に高次の変調データ信号がこれに続く。例えば、あるスロットにおいて、スロットごとに 4 ビットの情報を送るために、差分 1 6 位相変調を用いて 1 つ以上の位置情報シンボルを送信することができる。これは、2 値位相変調を疑似ランダム搬送波に加えたときに典型的に送信される 1 ビットに対してスループットが 4 倍に向上することを示している。1 6 Q A M などの他の種類の位置情報変調も利用可能である。加えて、トレリス符号の使用など、ある誤り制御変調方法をより高レベルの変調に用いてもよい。これらの変調方法は一般に、誤り率を低減する。

40

【 0 0 3 3 】

図 2 は、ここに記載した条件付きアクセス処理を実現するように構成された測位システム 2 4 0 の特定の態様を示す。図 2 に示すように、測位システム 2 4 0 は、さまざまな機能を行うことができる。例えば、測位システム 2 4 0 は、A L A C を生成し利用可能にすることができる。各 A L A C は、個々に生成され、製造業者 2 1 0 および / またはサービスプロバイダ 2 3 0 へ A L A C のブロックとして提供され、ユーザ装置 2 2 0 （例えば、G P S F W 画面）へ加えることができる。これらの A L A C は、装置識別子の使用を含む個々の装置に固有の方法、および A L A C 用のさらなる保護層を提供する装置固有のアル

50

ゴリズムで実現することができる。測位システム 240 はさらに、課金および監査システムを作動させて、測位システム 240 によって提供される測位機能の利用を追跡し課金することができる。

【0034】

測位システム 240 は、ASLC を生成し、製造業者 210、ユーザ装置 220、サービスプロバイダ 230 および / または外部エンティティ 250 (例えば、アプリケーション開発者またはプロバイダ) がこれを利用可能なようにすることができる。これらの ASLC は、IMEI、MAC アドレス等のような一意の装置識別子を含むように系統化してもよい。

【0035】

測位システム 240 は、ダウンロード可能なアプリケーションに位置情報を取り込もうとする外部エンティティ 250 について、開発者鍵、SDK および API を生成し管理することができる。各開発者鍵は、対応するアプリケーションのサービスレベルに基づいて、いくつかの対応する ASLC を有してもよい。各アプリケーション ASLC は、一意の識別子として開発者鍵を含んでもよく、他の一意の ID も含んでもよい。測位システム 240 は、フィールド内で (すなわち、ユーザ装置 220 上で) 展開されたアプリケーションからの要求を処理してユーザ装置 220 へ ASLC を動的に送信するサーバも保持するようにしてもよい。

【0036】

製造業者 210 は、1 つ以上の ALAC および ASLC (例えば、測位システム 240 から得たものか、または独立して生成し維持したもの) を必要なファームウェア (「FW」) およびソフトウェア (「SW」) と共に受信機に画像表示することができる。製造業者 210 は、ライブラリを画像としてロードしてもよい。製造業者 210 は、チップセット供給業者、装置 OEM、OS 供給元を含んでもよい。これとは対照的に、全送信機からの全送信に同じ ALAC を用いてもよい一方、各受信機の各アプリケーションごとに個々のユーザアカウントに基づいて異なる ASLC を用いてもよい。ASLC および ALAC の両方を暗号化してもよいし、あるいは、UE における未認証アクセスから保護してもよい。

【0037】

サービスプロバイダ 230 は、セルラサービスおよびウェブベースのサービスを含むさまざまなサービスをユーザ装置 220 へ提供することができる。さらなるサービスを挙げると、任意のコンテンツ (例えば、ビデオコンテンツ、音声コンテンツ、画像コンテンツ、テキストコンテンツ、他のコンテンツ) の無線または有線配信がある。サービスプロバイダ 230 は、ユーザ装置 220 へ提供するアプリケーションに対応する ASLC を保存してもよい。サービスプロバイダ 230 では、適用可能な場合、E-911 用の制御プレーン (c プレーン) メッセージ送信フローおよびネットワーク管理も可能である。サービスプロバイダ 230 はさらに、インハウス LBS のための SUPL メッセージ送信フローを介してユーザプレーン (u - プレーン) も可能にすることができる。

【0038】

外部エンティティ 250 は、さまざまな位置サービスをユーザの受信機を介してユーザへ提供するベンダを含んでもよい。例えば、外部エンティティ 250 は、PSAP、位置ベースのアドネットワーク、および LBS アプリケーション開発者 / 公開者などを含んでもよい。測位システム 240 およびサービスプロバイダ 230 は、位置案内、ASLC 検証および設定、付加価値サービス、課金サービスおよび監査サービスなどの一定範囲のサービスを外部エンティティ 250 に提供してもよい。

【0039】

ユーザ装置 220 としては、スマートフォン、タブレットおよび接続されたコンピューティングデバイスなどでよい。ユーザ装置 220 は、個々のアプリケーション (例えば、e-911、ネットワーク管理 (NW) または LBS) によって位置情報へのアクセスを管理するように構成してよい。アクセスの管理は、ユーザ装置 220 の製造後市場に投入

10

20

30

40

50

された後、ファームウェア上に画像表示されるか、またはダウンロードされる A S L C を用いて行ってもよい。図示のように、ドライバおよびライブラリ層は、装置上の複数のアプリケーションおよびユーザについて A S L C の管理、位置情報の復号、A S L C の示す許可に基づいたアプリケーションによる復号された位置情報の使用の制限に役立てる。例えば、ライブラリは、A S L C をそれに対応するアプリケーション（例えば、E 9 1 1、ネットワーク管理、L B S）へ関連付け、該当の位置情報をアプリケーションへ配信し、または調停することができる。

【 0 0 4 0 】

送信機および受信機を含むさまざまなシステム機能について上述してきた。以下に述べる図 3 および図 4 A、図 4 B および図 4 C は、送信機および受信機の実現例についてのさらなる詳細を示す。

10

【 0 0 4 1 】

図 3 は、ビーコン / 送信機システムの一実施形態 3 0 0 の特定の詳細を示す図である。このビーコン / 送信機システムから、本願中に後述するように位置 / 測位信号を送ることができる。送信機実施形態 3 0 0 は、図 1 に示すような送信機 1 1 0 に対応するとしてよい。送信機実施形態 3 0 0 は、関連する信号受信および / または処理を行うさまざまな構成要素を含むが、他の実施形態では、これらの構成要素は異なる様態で組み合わせたり、および / または編成したりして、類似のまたは同様の信号処理、信号生成および信号送信を行うことができる点に留意されたい。

【 0 0 4 2 】

20

図 3 では示していないが、送信機 / ビーコン実施形態 3 0 0 は、G P S 信号を受信する 1 つ以上の G P S 部を含んでもよく、これは、位置情報、および / もしくはタイミングデータ、精度希釈 (D O P) データなどの他のデータ、あるいは、G P S もしくは他の測位システムから得ることのあるような他のデータもしくは情報を処理部 (図示せず) へ出力するものである。図 3 では送信機 3 0 0 を G P S 部と共に示しているが、これに代わって、衛星または地上波信号を受信し、および類似または相当の出力信号、データもしくは他の情報を出力する他の構成要素をさまざまな実施形態において用いることが可能である点に留意されたい。G P S または他のタイミング信号を用いて送信機内部の高精度タイミング動作、および / または W A P S ネットワークにおけるタイミング修正を行うことができる。

30

【 0 0 4 3 】

送信機 3 0 0 は、本願中で後述するように送信機出力信号の生成および送信を行う 1 つ以上の送信機部 (例えば、R F 送信部 3 7 0) も含んでよい。送信機部も、送信アンテナへ出力信号を送る当該分野において既知であるか、または開発されたアナログまたはデジタル論理回路および電源回路、信号処理回路、同調回路、バッファおよび電力増幅器等のさまざまな要素を含んでよい。出力信号を生成する信号処理は、処理部 (図示せず) において行ってもよい。処理部は、いくつかの実施形態では、図 3 について説明する別の構成要素と一体化してもよいし、あるいは、他の実施形態では、複数の信号処理および / または他の動作機能を行う単独の処理部としてもよい。

【 0 0 4 4 】

40

1 つ以上のメモリ (図示せず) を処理部 (図示せず) と接続することにより、データの蓄積および索出を行い、ならびに / あるいは処理部で実行する命令の蓄積および索出を行ってもよい。例えば、命令は、本願中で後述するさまざまな処理方法および機能、例えば、その送信機に関連する局所的環境状態などの位置情報または他の情報の判別を行う命令、ならびに図 1 に示すようにユーザ装置 1 2 0 へ送るべき送信機出力信号を生成する命令でよい。

【 0 0 4 5 】

送信機 3 0 0 はさらに、その送信機に対する局所的気圧、気温、湿度、風または他の (まとめて、または個々に「大気」) 状態を検出または判別する 1 つ以上の環境検出器部 (図示せず) を含んでよい。例示的实施形態において、大気 (例えば、気圧) 情報は、環境

50

検出器部にて生成され、本願に後述するように送信機出力信号中の他のデータと一緒に処理部へ送ってもよい。１つ以上のサーバインタフェース部（図示せず）を送信機３００に設けることにより、送信機と図１に示すようなサーバシステム１３０などのサーバシステムとの間、および／または図１に示すようなネットワーク・インフラストラクチャ１７０などのネットワーク・インフラストラクチャに対してインタフェースを提供することができる。例えば、システム１３０は、位置システムおよび／またはユーザ装置に関連するデータまたは情報を送信機のインタフェース部を介して送信機３００へ送信してもよい。

【００４６】

各送信機３００は、物理層においてスロット当たりの調節可能な毎秒ビット数（例えば、スロット当たり毎秒９６ビット以上）で位置情報を含むデータを送信することができ、各送信機は、相互に独立してよい。送信機３００は、データの生成、暗号化、保護、変調および送信を行うさまざまな構成要素を含んでよい。例えば、送信機３００は、位置情報を生成するデータ生成部３１０、個々のエアリンクアクセス証明書（ＡＬＡＣ）に基づいて位置情報を暗号化する暗号化部３２０、ＡＬＡＣを蓄積するアクセス証明書蓄積部３３０、および他の構成要素、図示しないがとりわけ、例えば、パケットＩＤ／ＣＲＣ部３４０、符号化、消印およびインタリーピング部３５０、変調部３６０、およびＲＦ送信部３７０を含んでもよい。構成要素３４０および３５０は、前方誤り訂正（ＦＥＣ）方式およびＣＲＣ方式を他のデータフォーマット方式と共に提供し、フェーディング、経路損失および他の環境状態による影響を低減することができる。構成要素３６０は、データに変調を行う。

10

20

【００４７】

変調および信号構成は異なってもよいが、さまざまなフレーム当たりビット数を用いる場合、送信機３００からの送信にフレーム当たり１９０ビットが利用可能であることが分かる。例えば、符号化オーバーヘッド後に１０２データビットが利用可能となり、そのうち暗号化されないフレーミング情報用に７ビットが確保され、暗号化位置情報用には９５ビットが用意されている。低オーバーヘッドを維持するためには、暗号化を最小限にするのが好適である。例えば、暗号化速度の一例では、３秒ごとに約９５ビット／秒でよい。送信は、データ変化前の数サイクル（例えば、１０サイクルまたは３０秒）間、繰り返される。ペイロードは、緯度、経度、高度、気圧、気温、伝送補正および伝送品質を含むさまざまなものが考えられる。さらなるペイロードを挙げると、セキュリティ情報、サービスＩＤ、条件付きアクセスデータ（例えば、ＡＳＬＣ情報）がある。これらのさまざまなペイロードは、複数のスロットにわたってセグメント化することができる。当業者には、他のペイロード、他のビット数、およびさまざまなペイロードパッケージ方法も明らかであろう。

30

40

【００４８】

いくつかの場合、送信中のパケットの種別、いくつかのパケットにわたって送信される情報の種別、または同じ情報の互に関連するパケットの数を記述するには、 n ビットの表示子が必要である。パケット構造には、パケット内のどこかの位置にこの n ビット表示子を含んでよい。図１０Ａは、４桁のパケット種別表示ビットとその他のビットを示すパケット構造の一例を示す。図１０Ｂは、４ビットのパケット種別表示子を用いた一連のパケットの一例を示す。

【００４９】

図１０Ａおよび図１０Ｂに示すように、４ビットがパケット種別を示し、主パケットペイロードは９８ビットを含んでよい。４ビットは暗号化されず、「０」としてのパケット種別は暗号化されず、一方、「１」であるパケット種別は暗号化されている。パケット種別が「０」または「１」でない場合、一例であるが非限定的として、５ビット目は暗号ビットであり、このパケットが暗号化されているか否かを示すことができる。このビットは、暗号化しなくてよい。６ビット目はスタートビットでよく、これによって、新たなパケットの開始か（１）、または前のパケットの続きか（０）を示すことができる。このビットは、暗号化されていない。７ビット目はストップビットであり、これが最終パケットか

50

(1) 否か (0) を示すことができる。このビットは、暗号化されていない。次の 9 5 ビットは、主パケットペイロードを含み、これは、暗号ビットが 1 である場合は暗号化され、暗号ビットが 0 である場合は暗号化されていない。ペイロードは任意選択的に、現パケットのインデックス、および / または現に送信中の情報で予測される総パケット数を含んでもよい。

【 0 0 5 0 】

ここで受信機 4 0 0 の機能を示す図 4 A に戻り、送信機信号を受信および処理して、(例えば、E - 9 1 1 または L B S アプリケーション用に) 位置 / 測位情報を判別する。

【 0 0 5 1 】

受信機実施形態 4 0 0 は、図 1 に示すようなユーザ装置 1 2 0 に対応し、1 つ以上の G P S 部 4 8 0 を含んでよい。G P S 部は、G P S 信号を受信し、位置情報および / またはタイミングデータ、精度希釈 (D O P) データもしくは G P S もしくは他の測位システムから提供可能な他のデータもしくは情報などの他のデータを処理部 (図示せず) へ出力することができる。もちろん、他の全地球測位航法衛星システム (G N S S) もあり、G P S に関する開示はこれら他のシステムにも適用してよいことを理解すべきである。受信機 4 0 0 は、図 4 A では G P S 部を有するとして示されているが、これに代わって衛星もしくは地上波信号を受信し同様または同じ出力信号、データもしくは他の情報を出力する他の構成要素をさまざまな実施形態において用いてもよい点に留意されたい。もちろん、本願または取り込んだ各出願に記載の位置情報を受信し処理するように何らかの位置処理部を構成してもよい。

【 0 0 5 2 】

受信機 4 0 0 は、セルラまたは他のデータ通信システムを介してデータまたは情報を送受信する 1 つ以上のセルラ部 4 9 0 も含んでよい。これに代わって、または追加的に、受信機 4 0 0 は、W i - F i 、W i - M a x 、B l u e t o o t h 、U S B もしくは他のネットワークなどの他の有線または無線通信ネットワークを介してデータの送信および / または受信を行う通信構成要素 (図示せず) を含んでもよい。

【 0 0 5 3 】

受信機 4 0 0 は、点線 4 2 0 によって囲まれた 1 つ以上の構成要素 (「構成要素 4 2 0 」と呼ぶ) を含んでよい。これらの構成要素は、本願中に後述するように、図 1 に示すような送信機 1 1 0 などの地上波送信機から信号を受信し、信号を処理して位置 / 測位情報を判別するように構成されている。構成要素 4 2 0 は、アンテナ、R F 回路などの資源等と一体化してもよく、および / またはアンテナ、R F 回路などの資源を図 4 A に示す他の構成要素と共通にしてもよい。例えば、構成要素 4 2 0 および G P S 部 4 8 0 は、無線フロントエンド (R F E) 部および / または処理部をいくつか、または全て共有してもよい。処理部 (図示しないが、受信機 4 0 0 における処理機能を示すために概説する) は、構成要素 4 2 0 のうちいくつか、または全てと一体化してもよいし、あるいは、構成要素 4 2 0 および / または G P S 部 4 8 0 のうちいくつか、または全てと資源を共有して、本願に記載のような位置 / 測位情報を判別し、および / または他の処理機能を実行するようにしてもよい。同様に、セルラ部 4 9 0 は、R F 部 4 1 0 および / または構成要素 4 2 0 と R F 機能および / または処理機能を共有してもよい。ネットワーク部 4 6 0 も図示されているが、これは、何らかのタイプの有線通信路および無線通信路を用いたローカルエリアネットワーク、広域ネットワークまたは他のネットワークとすることができる。構成要素 4 1 0 、4 2 0 、4 6 0 、4 8 0 および 4 9 0 はそれぞれ、データを位置エンジン 4 4 0 へ送ることができ、位置エンジンは、このデータを用いて受信機 4 0 0 の推定位置を決める。位置エンジン 4 0 0 は、当該分野において公知のように、または後に開発されるように実現することができ、これは、推定位置を算出するように構成された処理装置を含むような実現形態を含むものである。

【 0 0 5 4 】

例えば、一実現形態において、構成要素 4 9 0 は、制御プレーンまたはユーザプレーンを通して測位データをセキュアに配信してもよいし、あるいは、このデータをインタネッ

トリックを通して直接入手してもよい。４９０とセルラモデムとの間のインタフェース上のデータは、受信機４００に固有のインタフェース暗号化／復号機能で保護してもよい。

【００５５】

１つ以上のメモリ４３０を処理部（図示せず）および他の構成要素と接続して、データの蓄積および索出を行い、ならびに／または処理部にて実行する命令の蓄積および索出を行うことができる。例えば、命令は、位置情報の復号および位置情報の判別などの本願に記載のさまざまな処理方法および機能を行うことができる。よって、構成要素４２０に含まれる特定の構成要素（例えば、構成要素４２１～４２４）は、本願に記載の位置情報、復号鍵および／または他の情報の処理を行うことができる。または、この処理の一部または全てを単独の処理装置（図示せず）で行ってもよい。

10

【００５６】

遠隔位置算出に用いる位置推定値または位置情報を含む位置データをこれらの遠隔構成要素へ送るには、制御プレーン信号方式もしくはユーザプレーン（ＳＵＰＬ）信号方式、もしくはインターネット／データプロトコル、またはこれらのいくつかの組合せなどの業界標準プロトコルを用いてもよい。

【００５７】

受信機４００はさらに、受信機４００の位置判別に用いられその受信機に関連する局所的気圧、気温、湿度または他の状態などの諸状態を検出し、または判別する１つ以上の環境検出器要素（図示せず）を含んでもよい。例示的实施形態では、気圧情報はこのような環境検出器要素で生成され、受信した送信機信号、ＧＰＳ信号、セルラ信号またはその他の信号に関連して位置／測位情報を判別するのに用いることができる。

20

【００５８】

受信機４００はさらに、ユーザ入力部（図示せず）などのさまざまな他のユーザインタフェース部を含んでもよい。このユーザインタフェース部は、キーボード、タッチスクリーンディスプレイ、マウスまたは他のユーザインタフェース要素の形態をとり得る。音声および／またはビデオデータもしくは情報は、当該分野において公知もしくは開発されるような１つ以上のスピーカもしくは他の音声変換器、タッチスクリーンなどの１つ以上の画像表示器、および／または他のユーザＩ／Ｏ要素などの形態の出力要素（図示せず）に出力することができる。例示的实施形態において、このような出力部を用いれば、受信した送信機信号に基づいて判別した位置／測位情報を可視表示することができる。判別した位置／測位情報は、セルラ部４９０から対応の通信事業者などへ送ってもよい。

30

【００５９】

受信機４００は、図５Ａ、図６、図７および図８に示す各処理を含む本開示のさまざまな機能を実行するように構成されたさまざまな他の構成要素を含んでもよい。例えば、構成要素４２０は、デジタル処理部４２１ａを含む信号処理部４２１を含んでもよい。デジタル処理部４２１ａは、ＲＦ部４１０からの受信ＲＦ信号を復調し、後に位置判別に用いる到着時間（ＴＯＡ）を推定するように構成されている。信号処理部４２１はさらに、疑似距離生成部４２１ｂおよびデータ処理部４２１ｃを含んでもよい。疑似距離生成部４２１ｂは、推定ＴＯＡから「生の」測位疑似距離データを生成して疑似距離データを精緻化し、この疑似距離データを位置エンジン４４０へ提供するように構成してもよい。位置エンジン４４０は、疑似距離データを用いて受信機４００の位置を判別する。データ処理部４２１ｃは、符号化された位置情報を復号し、暗号化されたパケットデータを符号化位置情報から抽出し、データに対して誤り訂正（例えば、ＣＲＣ）を行うように構成してもよい。データ処理部４２１ｃは、暗号化されたパケットデータを第１の暗号部４２２へ出力する。

40

【００６０】

第１の暗号部４２２は少なくとも、メモリ４３０に蓄積されたＡＬＡＣに基づいて位置情報を暗号化されたパケットデータから復号するように構成されている。受信機４００には複数のＡＬＡＣが蓄積され、同時にはそのうち１つのみを適用可能であるため、第１の暗号ブロック４２２は、使用すべき正しいＡＬＡＣ鍵を決定するさまざまな技術を用いることができる。データパケット自体、正しいＡＬＡＣ鍵が適用された場合のみチェックを

50

通すCRC / ダイジェストフィールドを持つことができる。パケットコンテンツの制約に起因してCRC / ダイジェストフィールドが無い場合、復号したパケットの個々のフィールドの予測値の範囲について、当該フィールドをチェックすることができる。加えて、受信機は受信機の近隣の複数の送信機からパケットデータを得ることができるため、複数の送信機からの位置情報は、正しいALAC鍵が選択された場合のみ、送信機間の距離、地域識別子その他など特定の整合性チェックを通すことになる。第1の暗号部422はまた、911緊急呼が生じたとの通知を受けると、復号した位置情報をE-911手順に関連する該当処理部へ出力する。

【0061】

図4A中の構成要素420はさらに、第2の暗号部423を含んでよく、これは、位置情報の一部または全てを、メモリ430に蓄積された該当するASLCに基づいて復号するように構成されている。ASLCは、位置情報を要求したアプリケーションすなわち位置判別に応じて決めてよい。例えば、ASLCは、受信機400のLBSアプリケーションまたはE-911アプリケーションに対応するものでよい。

【0062】

位置情報が第2の暗号部423によって復号されると、復号された位置情報はデータ単位出力部424へ出力され、データ単位出力部は、位置情報の離散的なデータ単位（例えば、緯度、経度、高度、気圧、気温、湿度、システム時間、タイミング修正値、および/または送信機ID）を判別する。そこで、位置情報の特定のデータ単位は、位置情報へのアクセスを要求したアプリケーションについてASLCの示すサービスレベルに基づいて、位置エンジン440へ送ることができる。

【0063】

位置エンジン440は、受信機400の位置を特定の限界（例えば、精度レベル）内で判別するために、位置情報（および、場合によってはGPSデータ、セルデータおよび/または他のネットワークデータ）を処理するように構成してもよい。判別後、位置情報はアプリケーション450へ提供することができる。当業者であれば分かるように、位置エンジン440は、位置情報を判別可能な任意の処理装置を意味し、GPS位置エンジンまたは他の位置エンジンを含んでよい。図4Aに示すさまざまな構成要素の位置は、受信機内の別のチップ場所であってよい。

【0064】

本願中の他の箇所に記載のように、また明確さのためにここで繰り返すが、受信機400上の各アプリケーションは、受信機400の位置判別のために、位置情報へのアクセス用に自身のASLCを必要とすることがある。いくつかの態様について、1つのASLCを複数のアプリケーションで用いてもよく、また複数のASLCを1つのアプリケーションで別々のユーザまたは別々の状況に用いてもよい。ASLCを用いて、特定の期間中、および特定のサービス領域において特定の位置情報の使用を制限することができる。

【0065】

E-911ネットワークサポートおよびLBSアプリケーション/サービスは、互に別個に取り扱うことができ、その場合、受信機400の製造後、それらの各ASLCを受信機400のファームウェアヘインストールするか、メモリへアップロードすることができる。各ASLCを用いて、各アプリケーション/サービスごとに自身で位置情報を与えることができる。別個の処理経路を用いて、これらのアプリケーション/サービスをさらに分けてもよい。

【0066】

受信機400は、位置判別専用のハードウェア/ソフトウェア機能が制限されている場合がある。ここに記載の条件付きアクセス機能に利用可能な総メモリ容量は、32キロバイトのオーダーでよい。他のメモリ容量もあり得る。

【0067】

位置情報は、GPS処理部、アプリケーション処理部または外部サーバにおいて処理してもよい。一態様によれば、本願に記載の機能は、受信機のGPS集積回路(IC)にお

10

20

30

40

50

いて、またはこれに従って実行することができる。例えば、受信機におけるホストプロセッサを用いて、双方向シリアルリンクを介してGPSICと通信してもよい。緯度および経度ならびに他の情報をこのシリアルリンクを用いて送信することができる。シリアルリンクをGPSICに対する証明書交換（例えば、ASLC）に用いることができる。GPSICは、送信機を（例えばPN系列との相関によって）検索する信号処理部を含み、送信機から受信した信号を復調して物理層ペイロードを取り出すことも考えられる。物理層ペイロードは暗号化された形でもよい（し、本願に記載の特定の実施形態によれば暗号化された形をとっている）。復号エンジンは、データを復号した後、このデータを次の処理層へ提供することができる。次の処理層とは、位置エンジンでよい。位置エンジンは、復号されたデータを用いて受信機位置を算出することができる。さまざまなエンジンをGPSICまたは他の受信機回路に配設することができる。

10

【0068】

ここで図4Bを参照すると、図4Bは、第1の位置における受信機400を示し、また受信機400の位置から遠隔位置にある他の位置に存在する構成要素も示す。受信機400とこれら他の構成要素は、送信機信号の処理に基づいて位置情報を集散的にまたは個々に判別することができる。図4Aの特定の態様を図4Bに示す。よって、図4Aに関するこれらの態様の説明は、図4Bにおけるそれらの態様にも、特定の実施形態で適用されるが、必ずしも全ての実施形態である必要はない。

【0069】

図4Bに示すように、受信機400は、保護のないインタフェース境界をデータが通るか、または保護のない通信路でデータ通信が行われる際にデータを保護するインタフェース（I/F）暗号化/復号（「スクランプリング/デスクランプリング」とも呼ぶ）部を含んでよい。いくつかの場合、これらのI/F部は、各受信機400ごとに別々に生成されたI/F鍵で動作することができる。

20

【0070】

図4Bは、第2の暗号部423aの前での受信機400における位置算出を示す。第2の暗号部423aは、受信機400内のアプリケーション450または受信機400にないアプリケーション499aへ位置算出結果を提供することができる。あるいは、位置算出は、受信機400から受け取った位置データを用いる遠隔構成要素（例えば、サーバの遠隔位置エンジン440b）が行ってもよく、これにより、遠隔位置算出の結果が受信機400へ返送されるか、または遠隔アプリケーション499bにて用いられる。

30

【0071】

図4Bに点線で示す構成要素間のデータ転送は、これらの構成要素間で直接行ってもよいし、あるいは中間構成要素（例えば、RF部410またはネットワーク部460）を介して行ってもよい。点線は、別の実施形態を示すことがある。例えば、アプリケーション管理部498aは、位置データを第2の暗号部423aから受信することができ、その後、アプリケーション管理部498aは、この位置データを（例えば、ネットワーク部460もしくはRF部410、または受信機400内の他の構成要素を介して）遠隔アプリケーションサービス499aへ転送することができる。そこで、遠隔アプリケーションサービス499aは、位置データ（例えば、位置推定値）を用いて、受信機400についてe911またはLBSサービスを提供することができる。

40

【0072】

別の例として、アプリケーション管理部498aは、データをデータ単位出力部424から直接、あるいは中間部（例えば、I/F暗号化部）を通して受信してもよい。その後、アプリケーション管理部498bは、この位置データを遠隔位置エンジン440bへ転送することができ、遠隔位置エンジンは、受信機400の推定位置（例えば、受信機400の緯度、経度、高度）を算出する。遠隔位置エンジン440bは、この位置推定を第2の暗号部423aへ（例えば、ネットワーク部460もしくはRF部410または受信機400内の他の構成要素を通して）、または第2の暗号部423bへ送信し、これらの構成要素におけるさらなる処理に供する。第2の暗号部423bは、例えば、1つ以上の遠

50

隔アプリケーションサービス 4 9 9 b または受信機 4 0 0 上で走行するアプリケーション 4 5 0 により、（例えば、ネットワーク部 4 6 0 もしくは R F 部 4 1 0 または受信機 4 0 0 中の他の構成要素を介する位置推定値の転送によって）位置推定値へのアクセスを管理するように動作することができる。そこで、遠隔アプリケーションサービス 4 9 9 b またはアプリケーション 4 5 0 は、位置推定値を用いて受信機 4 0 0 に対して e 9 1 1 または L B S サービスを提供することができる。遠隔構成要素はどれも、同じ位置でもよく、またさまざまな地理的位置に配置されてもよい。

【 0 0 7 3 】

図 4 B において、第 1 の暗号部 4 2 2 は、復号された位置情報をデータ単位出力部 4 2 4 へ出力し、データ単位出力部は、位置情報の離散的なデータ単位（例えば、緯度、経度、高度、気圧、気温、その他の大気情報または測定値、システム時間、タイミング修正値、および / または送信機 I D ）を判別する。そこで、これらのデータ単位は、位置エンジン 4 4 0 a または 4 4 0 b へ送信される。位置エンジン 4 4 0 a または 4 4 0 b は、ある限界（例えば、精度レベルおよび他の限界）内で受信機 4 0 0 の位置を判別するために、位置情報（および場合によっては G P S データ、セルデータ、および / または他のネットワークデータ）を処理するように構成してもよい。判別後、位置情報は、第 2 のレベル暗号部 4 2 3 a または 4 2 3 b （と、場合によっては他の中間部を通して）アプリケーション 4 5 0 、 4 9 9 a または 4 9 9 b へ提供することができる。当業者であれば、位置エンジン 4 4 0 a または 4 4 0 b は、G P S 位置エンジンまたは他の位置エンジンを含む位置情報を判別可能な任意の処理装置を意味し得ることを理解しよう。

【 0 0 7 4 】

第 2 の暗号部 4 2 3 a は、特定のサービスレベルの特定のアプリケーション用またはアプリケーション群用のセッション鍵を用いて特定のデータを暗号化するように構成してもよい。サービスレベルは、特定のアプリケーションのための特定のデータ単位サブセット（例えば、緯度、経度、高度、精度など）へのアクセスを認証することができる。

【 0 0 7 5 】

（例えばセッション鍵を用いて）データを暗号化した後、第 2 の暗号部 4 2 3 a は、暗号化されたデータをアプリケーション 4 5 0 へ利用可能にすることができる。セッション鍵は、受信機 4 0 0 において動的に生成してもよく、セキュリティ向上のために定期的に変更してもよい。単一のセッション鍵をアプリケーション群に用いる場合、各アプリケーションのうちのいずれかの A S L C の有効期間が切れた時に、セッション鍵を変更することができ、これにより、当該アプリケーション群は新たなセッション鍵を要求することになる。

【 0 0 7 6 】

一実施形態では、第 2 の暗号部 4 2 3 は、あるアプリケーションの A S L C を有効化した後、セッション鍵をそのアプリケーションと交換して、アプリケーションが当該アプリケーション用のデータを復号できるようにする。第 2 の暗号部 4 2 3 は、当初に A S L C をアプリケーションから受けるか、または、メモリ 4 3 0 もしくは他の箇所から A S L C を参照するよう指示されてもよい。こうして、当該アプリケーションには位置情報の特定の暗号化されたデータ単位がアクセス可能になる。

【 0 0 7 7 】

A S L C は、アプリケーションのサービスレベル認証を表示してもよい。特定のアプリケーションについて認証されたデータのみへのアクセスを管理するために、第 2 の暗号部 4 2 3 a は、セッション鍵をアプリケーションと交換して当該アプリケーションの A S L C に示された認証に応じて暗号化データを送ってもよい。

【 0 0 7 8 】

遠隔アプリケーション 4 9 9 a に対し、遠隔アプリケーション管理部 4 9 8 a は、A S L C およびセッション鍵を遠隔アプリケーションと第 2 の暗号部 4 2 3 a との間で送るための通信インタフェースを備えてもよい。

【 0 0 7 9 】

10

20

30

40

50

ここで図4Cを参照するが、図4Cは、受信機へのデータ送信または受信機からのデータ受信を行う受信機およびその他の構成要素に関する本開示のいくつかの態様を示す。図4Cに示すように、送信機から（例えば、PN系列との相関によって送信機を検索する信号処理を用いて）位置信号が得られる。この信号処理は、信号を復調して、各送信機ごとに物理層パイロードおよび生の到着時間（TOA）を取り出すことができる。これらの信号は、さまざまなハードウェア（HW）、ファームウェア（FW）、および/またはソフトウェア（SW）構成要素によって取得し追跡してもよい。例えば、GPSチップ上のFWおよび/またはHWは、信号送信のさまざまなサブフレームのうちのいずれか1つからパケットを復号し、CRCを確認するように動作してもよい。あるいは、ホストプロセッサがCRCを復号し確認することでもよい。

10

【0080】

追跡用HW/FW/SWは、生のTOAデータを生成し、生の暗号化データ（例えば、パケット）を復号部へ送るように動作することができる。いくつかの実現形態では、全てのパケット種別についてパケットIDが暗号化される訳ではない。生の暗号化されたデータの復号は、特定のHW/FW（例えば、WAPSに固有のHW/FW）内でALAC鍵を用いて行ってもよい。これらのALACは、各装置または装置クラスに固有の装置IDに基づいて暗号化するか、または秘密化してもよい。装置固有のIDは、その装置上のWAPS位置サービスの資格付与に用いてもよい。

【0081】

ALAC復号処理および/または復号を行うFW/HW/SWは、チップレベル、受信機/ハンドセットレベルまたは通信事業者レベルの各供給元で異なり得る。そこで、生の復号されたデータは、生のTOA測定値とともに（例えば、スクランプリングアルゴリズムおよび装置で生成された鍵を用いて）スクランブルしてもよく、スクランブルされたデータは、GPSチップ自体もしくはホストプロセッサまたはこれら両方で走行する位置ライブラリへ保護もしくは非保護データストリームに載せて送ってもよい。復号および位置ライブラリが同一HW/FW（例えば、GPSチップ）上において動作する場合は、スクランプリングがなくてもよい。

20

【0082】

そこで、位置ライブラリは、生データおよびTOA測定値をデスクランブルし、ライブラリ内でさらに利用することができる。例えば、デスクランブルされたデータを以下のようなデータ単位（DU）1～5に組み立てることができる。すなわち、DU1（送信機の緯度、経度、高度（LLA））；DU2（送信機における気圧/気温）；DU3（送信機のタイミング修正値）；DU4（送信側ネットワークの時間（WAPS時間））；およびDU5（送信機の識別子）。

30

【0083】

DU3からの生のタイミング修正値を用いて、精密なTOAを生成してもよい。測位エンジンは、精密なTOAおよび気圧センサ読取り値と共にさまざまなデータ単位（例えば、DU1、DU2、DU5）を用いて、受信機のLLAを算出することができる。DU4は、（例えば受信機が他の受信機と同期動作する場合に用いられる）タイミング信号を生成するように構成された測位エンジンによって用いることができる点に留意されたい。

40

【0084】

受信機のLLAまたはDU1～DU5のうちいずれかは、要求元アプリケーションまたは要求元アプリケーションの属するアプリケーション群のASLCによって指定されたパラメータに基づいて暗号化してもよい。暗号化は、ランダムもしくは所定のセッション鍵、ASLCによって規定された別の鍵、または当該分野において公知の他の暗号化方法などのさまざまな技術を用いて実行することができる。サービスレベル暗号化および復号がアプリケーションの単一のインスタンスまたは異なるアプリケーションの複数のインスタンスに影響を与えかねない実現形態など、さまざまな実現形態があり得る。

【0085】

一実現形態において、暗号化されたデータは、要求元アプリケーションのサービスレベ

50

ルによって指定された当該アプリケーションの利用可能なデータのみを含んでよい。例えば、ある精度レベル内における受信機の L L A の推定値を利用可能としてもよい（例えば、100メートル内の L L A 精度、10メートル内の L L A 精度）。このような実現形態において、受信機内の処理部が既知の L L A を x メートルの精度で分析した後、サービスレベル認証に応じた y メートルの精度で別の L L A を生成してもよい。このような実現形態は、さまざまな位置精度レベルに応じてサービスレベルの料金が異なる場合に有用なことがある。

【0086】

いずれかの測位エンジンは、複数の送信機のそれぞれの D U 2 について受信した気圧および気温読取り値を用いて、基準気圧の最良の推定値を生成してもよい。基準気圧は、暗号化された形でいずれかの測位エンジンへ送ってもよく、測位エンジンは、基準気圧および受信機の気圧センサ読取り値を用いて、前述の取り込んだ文献に記載のように高度を算出することができる。

【0087】

ある S W 技術によれば、測位エンジンは、W i - F i、G P S、W A P S、およびその他の送信機のうちいずれかからの信号を用いるハイブリッド実現形態において他のソースからのさらなる測定値を用いることができる。このようなハイブリッド測位エンジンは、暗号化された受信機 L L A または他の暗号化されたデータ（例えば、D U 1 ~ D U 5 のいずれか）のサービスレベル復号の後、ホストプロセッサと協働動作してもよい。あるいは、ハイブリッド測位エンジンは、サービスレベル暗号化の前に動作することもでき、そうすれば、得られたデータへのハイブリッド測位エンジンからのアクセスは、認証されたアプリケーションに限られる。

【0088】

図 4 C を参照した上記説明は、M S 補助 (M S - A)、M S ベース (M S - B) または単独のユーザプレーン呼フローに適用することができる。制御プレーン呼フロー（例えば、E - 9 1 1）の場合、データは、(M S A モードの) 生のまたは精密な T O A / 疑似距離および高度推定値の形でデータ、または (M S ベースのモードの) 受信機の L L A の形で位置判別エンティティ (P D E)、サービングモバイル位置センタ (S M L C)、または他の装置へ送られて、位置算出および P S A P への転送が行われる。このような送信は、セルラシステムの 1 つ以上の制御プレーンチャネルを通して行うことができる。

【0089】

好適ではないものの、測位補助データは、ウェブベースの経路、ローカルエリアネットワーク経路、広域ネットワーク経路、および R F 経路をまたがる他のネットワーク経路などの別の通信手段を用いて測位エンジンへ供給することができる点に留意されたい。このような送信は、受信側ネットワークと送信側ネットワークとの間の信号条件が低下していると、必要になることがある。測位補助データは、このような別の通信手段を用いて送信されると、その A L A C に対応する鍵を用いて、または通信手段に固有の別の鍵を用いて暗号化することができる。あるいは、A L A C も類似の鍵も用いず、サービスレベル暗号化および復号を用いてもよい。

【0090】

図 4 C は、さまざまな H W / F W / S W 内のさまざまな構成要素を示しているが、ある実施形態では、ホストプロセッサ、G P S チップまたはこれら両方などの 1 つ以上のハードウェア構成要素に図 4 C のさまざまな構成要素を組み込んでもよい。

【方法に関する態様】

【0091】

図 5 A は、特定の態様に従ってある受信機について位置情報を判別し、その受信機における位置情報へのアクセスを管理するネットワーク処理の詳細を示す図である。ここで、図 5 A に示す処理について述べる際、図 2 を参照することがある。当業者であれば、図 5 A に示す処理フローは例示であり、図 5 A に示す各段階の順序に本開示を限定するものではないことを理解しよう。よって、各段階を省いたり再配置したりしてもよく、また図示し

10

20

30

40

50

ていない別の段階を本開示の範囲および意図内において実行することが可能である。

【0092】

段階501において、測位システム240は、受信機による位置情報へのアクセスを管理する際に用いられる情報を生成および維持する。例えば、測位システム240は、エアリンクアクセス証明書(ALAC)、「システムレベル鍵/証明書」とも呼ばれる)および認証されたサービスレベル証明書(ASLC)を生成し、これらは、後にUE220で使用されてネットワーク(例えば、サービスプロバイダ230および/または測位システム240)から受信した位置情報を復号した後、この位置情報を要求した受信機上の特定のアプリケーションについてASLCで指定された制限事項に基づいてこの位置情報を用いる。段階502において、生成されたALACおよびASLCは製造業者210へ提供され、製造業者210は、段階503において(例えばファームウェアにこれらを画像化することにより)UE220にALAC/ASLCを設定する。

10

【0093】

段階504において(例えば、ユーザがUE220を購入した後)、UE220は、アプリケーションを起動するか、または緊急911呼を開始する。ステップ504に先立って、図に明示していないが、アプリケーションはUE220へダウンロードすることができる。アプリケーションに対応するASLCが製造業者によって設定されている場合、段階505は不要である。そうでない場合、UE220は、アプリケーションに対応する開発者鍵をネットワークへ送る。開発者鍵の経路は、サービスプロバイダ230、測位システム240、および/または外部エンティティ250としてのアプリケーションの開発者を通ることができる(経路は図示せず)。開発者鍵の受信および確認後、ネットワークは、当該アプリケーションのASLCをUE220へ送り、UE220はASLCを蓄積してもよい。

20

【0094】

段階506において、UE220は、ネットワークから位置情報を索出する。位置情報は、測位システム240から発したブロードキャスト信号から得てもよいし、かつ/またはサービスプロバイダ230を通して得てもよい。同様に、UE220は、位置情報を要求するか、または位置情報についてブロードキャストをモニタしてもよい。

【0095】

段階507~508において、UE220は位置情報を復号するが、その際、ALAC(例えば、位置情報をブロードキャストした送信機に対応するALAC)および位置情報を要求中の受信機のアプリケーションに対応するASLCを用いてもよい。

30

【0096】

段階509~510では、復号された位置情報を処理し、UE220の位置に関する位置情報を(例えば、位置エンジンにおいて)判別する。

【0097】

911呼の場合、段階511~512において、位置情報、測位情報、および/または位置(例えば、疑似距離および疑似距離を算出した送信機についての情報)の判別に用いる情報が、サービスプロバイダ230および/または外部エンティティ250として動作するPSAPへ送られる。そうでない場合、段階512において、LBSベースのアプリケーションについての位置情報は、UE220に残って位置ベースのサービスを実行し、および/または外部エンティティとして動作するLBSエンティティへ送られて当該LBSエンティティからの位置ベースのサービスの提供を補助することもできる。E911呼に代わる別の例として、暗号化したパケットを受信機が生ずるTOA情報と共にサーバへ送るものがある。暗号化されたパケットを復号して、サーバにおける位置分解能の計算に必要な情報を抽出する。

40

【0098】

図5Bは、ネットワークアプリケーションまたはE911処理について位置情報を配信する処理を示す。ASLCは、E911処理において用いても用いなくてもよい点に留意されたい。例えば、ASLCをE911呼において用いる場合、サービスレベルが最高で

50

有効期限のない緊急呼用に特殊な A S L C を設定してもよい。

【 0 0 9 9 】

図 6 は、受信機において特定の態様によって位置情報への条件付きアクセスを行う処理の詳細図である。ここで、図 6 に示す処理について述べる際、図 2 および図 4 A ~ 図 4 C を参照する。

【 0 1 0 0 】

上記したように、暗号化された測位信号データは、受信機（例えば、図 4 A ~ 図 C の受信機 4 0 0 ）へ送ることができる。測位信号データを暗号化は、認証済受信機へこれを配信して使用する際の保護に役立つ。しかし、受信機における帯域幅の制約および処理能力の制限によっては、ロバストな暗号化技術が有効でない場合がある。よって、データ/パケット空間の利用を最小限にしつつ、暗号化によって送信データを保護する必要があるが、その場合、一般にロバストな復号を短期間で行う処理能力がないような受信機では過大な復号を要さないようにする。

【 0 1 0 1 】

さまざまなパラメータ（例えば、アプリケーションに対応する課金の有効性、ユーザの現在位置、ユーザまたはアプリケーションによる位置要求が所定回数を超えたか、位置情報へアクセス可能な期間その他）に基づいて認証済アプリケーションおよびユーザによる位置情報の使用を保護するために、さらなる暗号化を行ってもよい。あるアプリケーションへの位置情報の配信を制御しながら他のアプリケーションによる当該位置情報へのアクセスを制限するようなこの第 2 の暗号化および復号層は、本願に記載のさまざまな実施形態の重要な特徴である。なぜならば、この層により、ネットワーク管理者、通信事業者、アプリケーション供給元/開発者または図 2 に示す他のエンティティが位置情報の配信を事業化することが可能になるからである。さらに、第 2 の暗号化および復号層は、未認証ユーザ（例えば、ハッカ）が未認証アプリケーションを使用して位置情報へのアクセスを得ようとするさまざまな試みの可能性を排斥する。

【 0 1 0 2 】

図 6 は、一態様による 2 段階の復号を示す。当業者であれば、図 6 における変形例が本開示の範囲および意図内にあることを理解しよう。段階 6 1 0 において、受信機は、（例えば、ある所定の条件やユーザ入力に自動的に応動して）第 1 のアプリケーションを起動する。次に、受信機は、第 1 のアプリケーションに対応する A S L C のコピーを受信機のメモリ（例えば、図 4 A ~ 図 4 C のメモリ 4 3 0 ）に蓄積されているかを判定する。コピーが存在する場合、受信機にその A S L C を「設定」し、段階 6 3 0 を実行する。そうでない場合は、受信機は「設定せず」に、段階 6 2 0 を実行する。

【 0 1 0 3 】

段階 6 2 0 において、受信機は、ネットワークから A S L C のコピーを得る。図 7 は、段階 6 2 0 のサブルーチンの詳細を示す。当業者であれば、図 6 に示す他の段階の後（例えば、段階 6 6 0 の前の任意の段階）に段階 6 2 0 を行ってもよいことを理解しよう。

【 0 1 0 4 】

段階 6 3 0 において、暗号化された測位信号は、ネットワークから受信機に到着する。測位信号は、送信機によってブロードキャストしてもよいし、あるいは、他の通信路（例えば、セルラ経路、ウェブベースの経路、ローカルエリアネットワーク経路）を介して到着してもよい。段階 6 4 0 において、受信機は、先ず測位信号を処理する。段階 6 4 0 に関するサブルーチンを図 8 に示す。

【 0 1 0 5 】

段階 6 5 0 において、測位信号は、第 1 の暗号部 4 2 2 に到着し、ここで、測位信号は、メモリ 4 3 0 に蓄積されている A L A C のコピーを用いて復号される。次に、段階 6 6 0 において、復号された測位信号からの位置データは、第 2 の暗号部 4 2 3 によって第 1 のアプリケーションに対応する A S L C を用いることでその一部または全部が復号される。A S L C は、（段階 6 2 0 および図 7 について述べたように）メモリ 4 3 0 から、またはネットワークから索出することができる。

【 0 1 0 6 】

最後に、段階 6 7 0 において、位置エンジン 4 4 0 は、復号された位置データを位置 T O A または疑似距離情報と共に受信して、第 1 のアプリケーション用に受信機の位置を算出する。この位置算出は、第 1 のアプリケーション用の A S L C によって示されるサービスレベルに基づいて決めてもよい。

【 0 1 0 7 】

図 7 は、受信機における特定の態様による条件付きアクセス証明書の設定処理および図 6 の段階 6 2 0 の詳細を示す。図 7 に示す処理について述べる際、図 2 を参照する。

【 0 1 0 8 】

段階 7 1 0 において、U E 2 2 0 は、あるアプリケーションに対応する開発者鍵を取り出す。開発者鍵は、アプリケーションが U E 2 2 0 ヘダウンロードされた後に U E 2 2 0 上に保存してもよい。開発者鍵と A S L C の対応関係は、ネットワーク（例えば、サービスプロバイダ 2 3 0、測位システム 2 4 0 または外部エンティティ 2 5 0）に保存してもよい。A S L C は、アプリケーションに対してだけでなく、U E 2 2 0 のアクセスレベルに対しても固有でよい。段階 7 2 0 において、開発者鍵は、処理を行うネットワーク（例えば、サービスプロバイダ 2 3 0、測位システム 2 4 0 および / または開発者もしくはアプリケーションプロバイダ 2 5 0）へ送られる。

【 0 1 0 9 】

段階 7 3 0 において、開発者鍵の送信に応答して、U E 2 2 0 / 受信機 4 0 0 は、開発者鍵 / アプリケーションに対応する A S L C をネットワークを介して受信する。段階 7 4 0 において、A S L C は、将来用いるために保存される。あるいは、A S L C は保存せずに、次回に（図 6 に示し本願の他の箇所で説明する 2 段階復号モデルにおいてそのアプリケーションに対応する A S L C を必要とする）アプリケーションが位置情報を要求したときに、段階 7 1 0 ~ 7 3 0 を繰り返してもよい。

【 0 1 1 0 】

図 8 は、特定の態様による測位信号データを処理する処理および図 6 の段階 6 4 0 の詳細を示す図である。図 8 に示す処理を述べる際、図 4 A ~ 図 4 C を参照する。例えば、段階 6 4 0 は、図 4 A ~ 図 4 C 中の信号処理部 4 2 1 によって行ってもよい。

【 0 1 1 1 】

段階 8 1 0 において、送信機から R F 部 4 1 0 を通して受信した測位信号を用いて、生の T O A を（例えば、デジタル処理部 4 2 1 a において）推定することができる。次に、生の T O A 推定値は、疑似距離生成部 4 2 1 b において生の測位疑似距離情報へ変換することができる。

【 0 1 1 2 】

段階 8 2 0 において、測位信号はデータ処理部 4 2 1 c において復号することができる。段階 8 3 0 において、データ処理部 4 2 1 c は、測位信号に対して誤り検出を行った後、これを復号対象として第 1 の暗号部 4 2 2 へ送ってもよい。

【 0 1 1 3 】

図 1 1 は、第 1 の復号段階、第 2 の暗号化段階、および第 3 の復号段階を示す。当業者であれば、図 1 1 の変形例が本開示の範囲および意図内であることを理解しよう。図 1 1 に示す特定の段階を他の実現例では再配置または省略することができる。以下の議論は、主に受信機に関する。しかし、この議論は、以下に具体的に述べる機能の一部または全てを実行する 1 つ以上の処理装置にも適用可能である。

【 0 1 1 4 】

段階 1 1 1 0 において、（例えば、自動的に、ある所定の条件やユーザ入力に応動し、または別の事象もしくは状況に応動して）第 1 のアプリケーションが起動される。このアプリケーションは、受信機、または他の装置のうちでも受信機から遠隔のサーバにおいて起動してもよい。受信機は、図 4 B ~ 図 C に示すものを含む多様な形態をとり得る。

【 0 1 1 5 】

段階 1 1 2 0 において、受信機は、第 1 のアプリケーションに対応する A S L C のコピ

10

20

30

40

50

ーを得る。受信機は、受信機におけるメモリ、第1のアプリケーションまたは外部源からA S L Cを入手し得る。A S L Cは、他の条件のなかでも、どんな情報が第1のアプリケーションへ提供可能か/第1のアプリケーションがアクセス可能かの他に、いつ、どのようにして第1のアプリケーションが情報を提供し/これにアクセス可能かを定めるパラメータを規定してもよい。A S L Cの使用に代わるもの、例えば、A S L C中のデータを証明書無しで使用するだけのこともあり得る。

【0116】

段階1130において、暗号化された測位信号は、送信機から受信機に到着する。測位信号はそれぞれ、各送信機からブロードキャストされ、他の通信路（例えば、セルラ経路、ウェブベースの経路、ローカルエリアネットワーク経路）または両方を介して到着することもある。

10

段階1140において、受信機は、先ず測位信号を処理する。

【0117】

段階1150において、測位信号は、受信機に蓄積された鍵（例えば、A L A Cによって指定されたもの）または受信機によってアクセス可能な外部源からの鍵を用いて復号される。

【0118】

段階1160において、受信機は、測位信号からの位置情報を識別または判別することができる。このような位置情報を挙げると、生の、および精密なT O A測定値、本願の他の箇所で述べたデータ単位（D U）、測位信号のデータに基づいて算出した受信機の推定位置座標、推定位置座標に基づいて算出した修正位置座標、または他のデータがある。修正された位置座標は、段階1120からのパラメータに基づいて決めてもよい。このようなパラメータは、推定位置座標の所定の精度レベル（例えば、距離）内で位置座標をアプリケーションが受信できることを示してもよい。この場合、処理装置は、その精度レベルに基づいて新規の位置座標を生成することができる（例えば、推定緯度からx個の測定単位の範囲内に収まるように緯度を変更し、高度を0に変更し、したがって2次元のみが得られる）。より低精度の位置情報を提供すれば、アプリケーションごとの、または使用の度ごとの加入サービスが可能になる。

20

【0119】

段階1120からのA S L Cもしくはそのデータによって指定され、またはそれらに基づいて生成された鍵を用いて、位置情報の一部または全てを段階1170において暗号化することができる。暗号化すべき位置情報の選択は、A S L Cで指定されたサービスレベル条件によって制御してもよい。このようなサービスレベル条件により、第1のアプリケーションがアクセス可能なデータを指定することができ、また本願の他の箇所で述べたデータ、例えば、図9について述べたデータの一部または全てから決定することができる。

30

【0120】

段階1180において、暗号化された位置情報は第1のアプリケーションによって復号されて使用される。第1のアプリケーションを実行する処理装置は、位置情報の暗号化に用いる鍵を知得し得る。この知得は、A S L Cへアクセスすることにより得る（例えば、A S L Cが鍵、または鍵を判別するアルゴリズムを指定する場合）か、または、鍵を受信する（例えば、セッション識別子を用いる場合）ことにより得てもよい。

40

【データに関する態様】

【0121】

図9は、条件付きアクセス処理時における特定の態様での使用データを示す。図示のように、データは次のようなものを識別し、または表すことができる。すなわち、アプリケーション種別（例えば、E - 911、L B S、ネットワーク管理、規則適用）、U E I DもしくはU E種別、サービス種別（例えば、利用精度、利用範囲、利用時間、利用可能なデータ単位）、サービスプロバイダ種別、製造業者種別、開発者種別、ユーザI Dもしくはユーザ種別、要求の種別、または、アプリケーションへ提供可能な位置情報を決めるアプリケーションのサービスレベル、その位置情報を提供する時期、その位置情報の提供の

50

仕方、およびその位置を提供できる場所を決めるなどのパラメータとして利用可能な他の情報種別である。GPSまたは他の時刻を送信して、時限に基づいて利用状況をモニタしてもよい。このデータの一部または全てを特定のアプリケーションおよび/またはUEのASLC内に組み込んで、後で処理部によってアクセスして、位置情報を識別することができる。この位置情報は、暗号化した後、受信機内部または受信機外部（すなわち、遠隔）のアプリケーションへ送ることができる。データはそれぞれ、受信機の処理装置にて特定の復号された位置情報のフィルタリングに用いられ、その後、この特定の位置情報がアプリケーション、装置またはユーザへ暗号化された形で送られる。換言すれば、このデータは、利用可能な位置情報と、当該情報が利用可能な時期と、当該情報が利用可能な期間とを指定するものである。ASLCは、暗号化鍵または暗号化鍵生成用アルゴリズム（例えば、リアルタイムデータもしくは保護された環境において配信されるか、そうでなければ暗号化段階および復号段階にて利用可能となる他のデータを用いて暗号化鍵を生成するアルゴリズム）も含んでよい。

10

20

30

40

50

【0122】

サービス種別は、3次元までの精度レベルに関するものでよく、高測距精度（例えば、3メートル）、中測距精度（25～50メートル）および低測距精度（400メートル）を含む。サービス種別はまた、サービスレベルに関するものでよく、とりわけ局所的、地域的、全国のおよび世界的なレベルを含む。サービス種別はさらに、有効期限レベルに関するものでよく、有効期間のなかでもとりわけ、アクセス特権の期限がワンタイム、月単位、年単位または生涯期間を含む。サービス種別は、従量制および無制限を含む使用量レベルにも関するものでもよい。多様なレベルの組合せが利用可能である。

【0123】

同様の復号は、非セルラ装置用の測位アプリケーションでも考えられる。例えば、VoIPアプリケーション（例えば、Skype（商標））、カメラ/ビデオカメラなどを介するE-911呼は、ファームウェア内に焼き込まれるか、そうでなければメモリへダウンロードされるASLCを有し得る。

【使用例に関する態様】

【0124】

さまざまな種類のコンピューティングデバイスとそれらの接続性状態が考えられ、これらには、セルラネットワーク、測位ネットワーク、ローカルエリアネットワークまたは他のネットワークへほぼ常時接続されるか、大部分接続されるか、または（接続されるにしろ）まれに接続される装置が含まれる。これらのコンピューティングデバイスそれぞれについて処理能力も併せて考慮する。

【0125】

接続性の種類を挙げると、セルラ（例えば、3G/4G、プリペイド）、Wi-Fi、有線（例えば、USB、Ethernet）およびその他の接続性がある。

【0126】

コンピューティングデバイスの種類を挙げると、スマートフォン、他の携帯電話、タブレット、ラップトップ、接続されたTV、VoIP電話、STB、DMA、電化製品、セキュリティシステム、PGD、PND、DSC、M2Mアプリケーション、資産のジオフェンシングなどがある。接続される受信機としては、アクティブなデータパイプ（例えば、セルラ、およびWi-Fi/有線Ethernet）を利用可能な携帯電話、タブレットおよびラップトップなどの装置がある。大部分接続される受信機は、Wi-Fi/有線Ethernetなどの非セルラ手段へのアクセスを有するタブレットおよびラップトップなどの装置である。非接続型受信機または限定接続型受信機を挙げると、インターネットへ（接続されるにしろ）まれに接続されるがセルラ接続性を持たない受信機がある。

【0127】

非接続型受信機は、受信機の耐用年数に合わせてプログラムされ事前認証された1組のALACおよびASLCを備えるように製造してもよいことが考えられる。この初期期間経過後の鍵更新は、ファームウェア更新によって装置へ（例えば、USB接続を用いて）

行うか、または装置をデータネットワークへ一時的に接続することにより行える。このような非接続型受信機は、暗号化された位置情報を受信する適切なRF受信機（例えば、GPSチップ）によって自身の位置を判別することができる。

【さらなる態様】

【0128】

1つ以上の態様は、1つ以上のアプリケーションによる位置情報へのアクセスを管理するシステム、方法、手段およびコンピュータプログラム製品に関するものでよい。システムは、方法を実現するように動作可能な処理部を含んでよい。コンピュータプログラム製品は、方法を実現するように構成されコンピュータ読取り可能なプログラムコードが内部に具現化された、コンピュータで利用可能な非一時的媒体を含んでよい。

10

【0129】

方法ステップにおいて、地上波送信機のネットワークから受信した第1の組の暗号化された位置信号を第1の鍵で復号し、第1の組の復号された位置信号から位置情報を判別し、第1の組の位置情報を識別するが、その場合、第1の組の位置情報は、第1のアプリケーションに対応する第1のサービスレベルに基づいて特定され、さらに、第1の組の位置情報を第2の鍵を用いて暗号化し、暗号化された第1の組の位置情報を第1のアプリケーションへ提供する。

【0130】

いくつかの態様によれば、第1の組の位置情報は、地上波送信機のネットワークからの1台以上の送信機の位置座標、タイミング修正値および大気測定値のうち少なくとも1つを含む。

20

【0131】

いくつかの態様によれば、方法ステップではさらに、復号された位置信号を用いて受信機の位置の推定座標を算出してもよく、第1の組の位置情報は、受信機の推定座標を含む。

【0132】

いくつかの態様によれば、復号された位置信号は、地上波送信機のそれぞれにおける大気測定値を指定するデータを含む。その場合、推定座標は、復号された位置信号および受信機における少なくとも1つの大気測定値を用いて算出される高度座標を含む。

【0133】

いくつかの態様によれば、方法ステップではさらに、復号された位置信号を用いて受信機の位置の推定座標を算出し、第1のアプリケーションに許可された精度レベルに基づいて推定座標に基づく修正座標を算出してもよく、修正された座標は、受信機の位置の指定が推定座標よりも低精度であり、第1の組の位置情報は修正された座標を含む。

30

【0134】

いくつかの態様によれば、方法ステップではさらに、第2の組の位置情報を識別し、第2の組の位置情報は、第2のアプリケーションに対応する第2のサービスレベルに基づいて識別され、第1の組に含まれる特定の位置情報は第2の組に含まれず、さらに、第2の組の位置情報を第3の鍵を用いて暗号化し、第2の組の位置情報を第2のアプリケーションへ提供するようにしてもよい。

40

【0135】

いくつかの態様によれば、方法ステップではさらに、地上波送信機のネットワークから受信した第2の組の暗号化された位置信号を第1の鍵または第3の鍵を用いて復号し、第1の組の暗号化された位置信号は受信機の第1の位置において受信され、第2の組の暗号化された位置信号は受信機の第2の位置における受信機であり、さらなる位置情報を第2の組の復号された位置信号から判別し、第2の組のさらなる位置情報を識別し、第2の組のさらなる位置情報は、第2のアプリケーションに対応する第2のサービスレベルに基づいて識別され、第2の組の位置情報を第4の鍵を用いて暗号化し、第2の組の位置情報を第2のアプリケーションへ提供するようにしてもよい。

【0136】

50

いくつかの態様によれば、方法ステップではさらに、第 1 の組の位置情報を識別する前に、第 1 のサービスレベルを指定する情報が受信機に蓄積されているかを判定し、第 1 のサービスレベルを指定する情報が受信機に蓄積されていないと判定すると、第 1 のアプリケーションに対応する第 1 の開発者鍵へアクセスし、第 1 の開発者鍵をサーバへ送り、第 1 の開発者鍵のサーバへの送信に呼応して第 1 のサービスレベルを指定する情報を受信するようにしてもよい。

【0137】

いくつかの態様によれば、第 1 のサービスレベルを指定する情報は、第 1 のアプリケーションに対応する第 1 の認証済サービスレベル証明書に含まれ、この証明書は開発者鍵に対応する。

10

【0138】

いくつかの態様によれば、第 1 のサービスレベルは、第 2 の鍵を用いて第 1 の組の位置情報および何らかの後続の位置情報の任意の後続する組を暗号化するのに使用可能な期間を指定する。

【0139】

いくつかの態様によれば、第 2 の鍵は、位置信号が復号された後に生成されるセッション鍵である。

【0140】

いくつかの態様によれば、第 1 のアプリケーションは遠隔サーバにて走行し、第 1 の組の位置情報は遠隔サーバへ提供される。

20

【0141】

いくつかの態様によれば、方法ステップではさらに、第 1 のアプリケーションに対応する第 1 の証明書にて指定されたパラメータに基づいて第 1 のサービスレベルを判別してもよい。

【0142】

いくつかの態様によれば、方法ステップではさらに、保護されていない通信路を通して位置情報を送る前に位置情報をスクランブルし、スクランブルされた位置情報をスクランブル解除してから第 1 の組を識別するようにしてもよい。

【0143】

いくつかの態様によれば、方法ステップではさらに、保護されていない通信路を通して推定座標を送る前に推定座標をスクランブルし、スクランブルされた推定座標をスクランブル解除してから第 1 の組を暗号化するようにしてもよい。

30

【0144】

いくつかの態様によれば、方法ステップではさらに、複数の鍵のなかから第 1 の鍵を選択し、暗号化された位置信号の CRC フィールドは、第 1 の鍵を使って第 1 の組の暗号化された位置信号を復号する場合にのみチェックを通過させるようにしてもよい。

【0145】

いくつかの態様によれば、方法ステップではさらに、複数の鍵のなかから第 1 の鍵を選択し、その場合、復号された位置信号のデータは、第 1 の鍵を使って第 1 の組の暗号化された位置信号を復号する場合にのみ予測値と照合するようにしてもよい。

40

【0146】

いくつかの態様によれば、方法ステップではさらに、複数の鍵のなかから第 1 の鍵を選択し、複数の送信機からのパケットデータは、第 1 の鍵を用いて第 1 の組の暗号化された位置信号を復号する場合にのみ、1 つ以上の整合性チェックを通過させ、その場合、第 1 の組の暗号化された位置信号は、複数の送信機からのパケットデータを含むようにしてもよい。

【他の態様】

【0147】

多様な開示の特徴についてのさらなる開示は、以下の本出願人に譲渡された特許出願に記載され、これら全体を参照することによって任意のあらゆる目的で本願に取り込む。す

50

なわち、「広領域測位システム」と題する2012年3月5日付特許出願の米国特許出願番号13/412,487号、「広領域測位システム」と題する2009年9月10日付特許出願の米国特許番号12/557,479号（現在では米国特許第8,130,141号）、「広領域測位システム」と題する2012年3月5日付特許出願の米国特許出願番号13/412,508号、「広領域測位システム」と題する2011年11月14日付特許出願の米国特許出願番号13/296,067号、「広領域測位システム」と題する2011年6月28日付特許出願の国際出願番号PCT/US12/44452号）、「広領域測位システムにおける符号化」と題する2012年6月28日付特許出願の米国特許出願番号13/536,051号、「広領域測位システム（WAPS）における符号化」と題する2012年6月28日付特許出願の米国特許出願番号13/565,614号、「広領域測位システム（WAPS）におけるセル構成および伝送方式」と題する2012年8月2日付特許出願の米国特許出願番号13/565,732号、「広領域測位システムにおけるセル構成および伝送方式」と題する2012年8月2日付特許出願の米国特許出願番号13/565,723号、「3次元空間における基準位置に対応するタイミングデータを使用して受信機位置を推定するように構成されたシステムおよび方法」と題する2013年3月14日付特許出願の米国特許出願番号13/831,740号、「ユーザ装置の測位システムおよび方法」と題する2013年6月4日付特許出願の米国特許出願番号13/909,977号、NEXN-009-201（「送信された情報への条件付きアクセスを提供するシステムおよび方法」と題する2013年8月26日付特許出願の米国特許出願番号14/010,437号、「広領域測位システム（WAPS）における疑似ランダム符号化方法および装置」と題する2013年8月27日付特許出願の米国特許出願番号14/011,277号である。上記の出願、公報および特許は、本願中において個々に、または全体として「取り込んだ文献」、「取り込んだ出願」、「取り込んだ公報」、「取り込んだ特許」または別の呼称で呼ぶことがある。本願に開示のさまざまな態様、詳細、装置、システムおよび方法は、取り込んだ文献のいずれの開示とも組み合わせ得る。

10

20

30

40

50

【0148】

本願に記載のシステムおよび方法は、位置コンピューティングデバイスまたは他の物を追跡して、位置情報およびナビゲーションをこのような装置や物に提供することができる。「GPS」という用語は、GLONASS、GalileoおよびCompass/Beidouなどの任意の全地球測位航法衛星システム（GNSS）を指し得る点に留意されたい。送信機は、ユーザ装置の受信した信号に測位データを入れて送信してもよい。測位データは、信号伝播時間（例えば、到着時間（TOA））を求めるのに使用可能な「タイミングデータ」を含んでもよい。信号伝播時間は、信号の伝播時間を信号速度で乗算することにより、ユーザ装置と送信機との間の距離（例えば、疑似距離）を推定するのに用いることができる。

【0149】

さまざまなアーキテクチャのGPS受信機が考えられる。例えば、GPS受信機の論理機能は（1）信号処理および（2）位置算出の2つの部分に分けることができる。信号処理機能は、ハードウェアで実現し、位置算出は、ファームウェア/ソフトウェアにて実現してもよい。これらの機能は、DSPハードウェアブロックと、DSPハードウェアを管理し位置を算出するARM処理サブシステムとを有するGPSSASIC「チップ」上に実現してもよい。このようなGPSチップは典型的には、NMEAメッセージの形で最終緯度、経度および高度を生成する。あるいは、位置算出をハンドセット内のアプリ処理装置で行って、さらなる位置情報を付加し、全体として測位方式を構築してもよい。本願での開示は、（他の信号処理および位置算出処理構成に加えて）両方の実現形態へ適用し得る。

【0150】

本願に記載のさまざまな例示的なシステム、方法、論理機能、ブロック、モジュール、構成要素、回路およびアルゴリズムステップは、当該分野において公知であるか、または開発される適切なハードウェア、もしくは処理回路（「処理装置」とも呼ばれ、また任意

の台数の処理装置も含む)によって実行されるソフトウェア、あるいはその両方によって実現され、実行され、またそうでなければ制御される。処理装置は、本願に開示のデータの分析、操作、変換もしくは生成、またはその他のデータ操作を含む処理/方法およびシステムに関するいずれの処理ステップ、計算ステップ、方法ステップまたは他のシステム機能も行うか、または行わせることができる。処理装置は、汎用処理装置、デジタル信号処理装置(DSP)、特定用途向け集積回路(ASIC)、フィールドプログラマブルゲートアレイ(FPGA)もしくは他のプログラマブル論理デバイス、個別素子ゲートもしくはトランジスタ論理回路、個別素子ハードウェア構成要素、サーバ、またはこれらの任意の組合せを含んでよい。処理装置は、従来の処理装置、マイクロプロセッサ、制御装置、マイクロコントローラまたは状態機械を含んでよい。処理装置はまたチップを指すことがあり、その場合、チップは、さまざまな構成要素(例えば、マイクロプロセッサ、およびその他の構成要素)を含む。「処理装置」という用語は、同じタイプまたは異なるタイプの1つ、2つまたはそれ以上の処理装置を指し得る。「コンピュータ」もしくは「コンピューティングデバイス」または「ユーザ装置」などの用語は、処理回路を有する装置を指す場合もあれば、処理装置そのものを指す場合もある。ソフトウェアは、RAMメモリ、フラッシュメモリ、ROMメモリ、EPROMメモリ、EEPROMメモリ、レジスタ、ハードディスク、リムーバブルディスク、CD-ROM、または任意の他の形態の記憶媒体に記憶することができる。「メモリ」を処理装置に接続することにより、処理回路はメモリから情報を読み出し、情報をメモリへ書き込むことができる。記憶媒体は、処理回路と一体でもよい。ソフトウェアは、コンピュータ読取り可能な媒体に蓄積され、または1つ以上の命令すなわちコードとしてこれに符号化することができる。コンピュータ読取り可能な媒体は、不揮発性媒体(例えば、光学的、磁氣的、半導体)、ならびにデータおよび命令を無線、光または有線の信号媒体を通しネットワーク転送プロトコルを用いたネットワークで転送する搬送波を含む任意の利用可能な記憶媒体でよい。本願に記載のシステムおよび方法の各態様は、多様な回路のいずれかにプログラムされた機能として実現することができる。各態様は、ソフトウェアベースの回路エミュレーション、個別素子論理回路、カスタムデバイス、神経論理回路、量子素子、PLD、FPGA、PAL、ASIC、MOSFET、CMOS、ECL、ポリマ技術、アナログ・デジタルの混合、およびそれらのハイブリッドを有する処理装置として具体化することができる。これまでの記載全体にわたって触れたことのあるデータ、命令、コマンド、情報、信号、ビット、シンボルおよびチップは、電圧、電流、電磁波、磁界もしくは粒子、光場もしくは粒子、またはこれらの任意の組合せによって表すことができる。コンピューティングネットワークを用いて各態様を実行することができ、コンピューティングネットワークは、ハードウェア構成要素(サーバ、モニタ、I/O、ネットワーク接続)を含んでよい。アプリケーションプログラムは、データの受信、変換、処理、蓄積、索出、転送および/またはエクスポートにより各態様を実行することができ、データは、階層構造データ源、ネットワークデータ源、リレーショナルデータ源、非リレーショナルデータ源、オブジェクト指向データ源または他のデータ源に蓄積してもよい。「データ」および「情報」は、互いに同義に用いられる。「含む」、「備える」、「有する」、「持つ」などの用語は、排他的な意味(すなわち、~のみからなる)ではなく、包含的(すなわち、非限定的)な意味として解釈されるべきである。単数形または複数形を用いた用語は、それぞれ複数形または単数形も含む。「または」または「および」という用語は、列挙した項目のうちの任意のもの、および全部をカバーする。「一部の」および「任意の」また「少なくとも1つの」とは、1つ以上を指す。「装置」という用語は、1つ以上の構成要素(例えば、処理装置、メモリ、画面)を含み得る。「モジュール」、「ブロック」、「特徴」または「構成要素」という用語は、これらのモジュール、ブロック、特徴または構成要素に対応する機能を実行するか、さもなくば達成するように構成されたハードウェアもしくはソフトウェア、またはハードウェアおよびソフトウェアの組合せを指し得る。同様に、システム図および装置図において矩形として描かれた機能部は、ハードウェアまたはソフトウェアを指すとしてよい。2つのこのような機能部を繋ぐ線は、これらの機能部間のデータ転送を示してもよい点

10

20

30

40

50

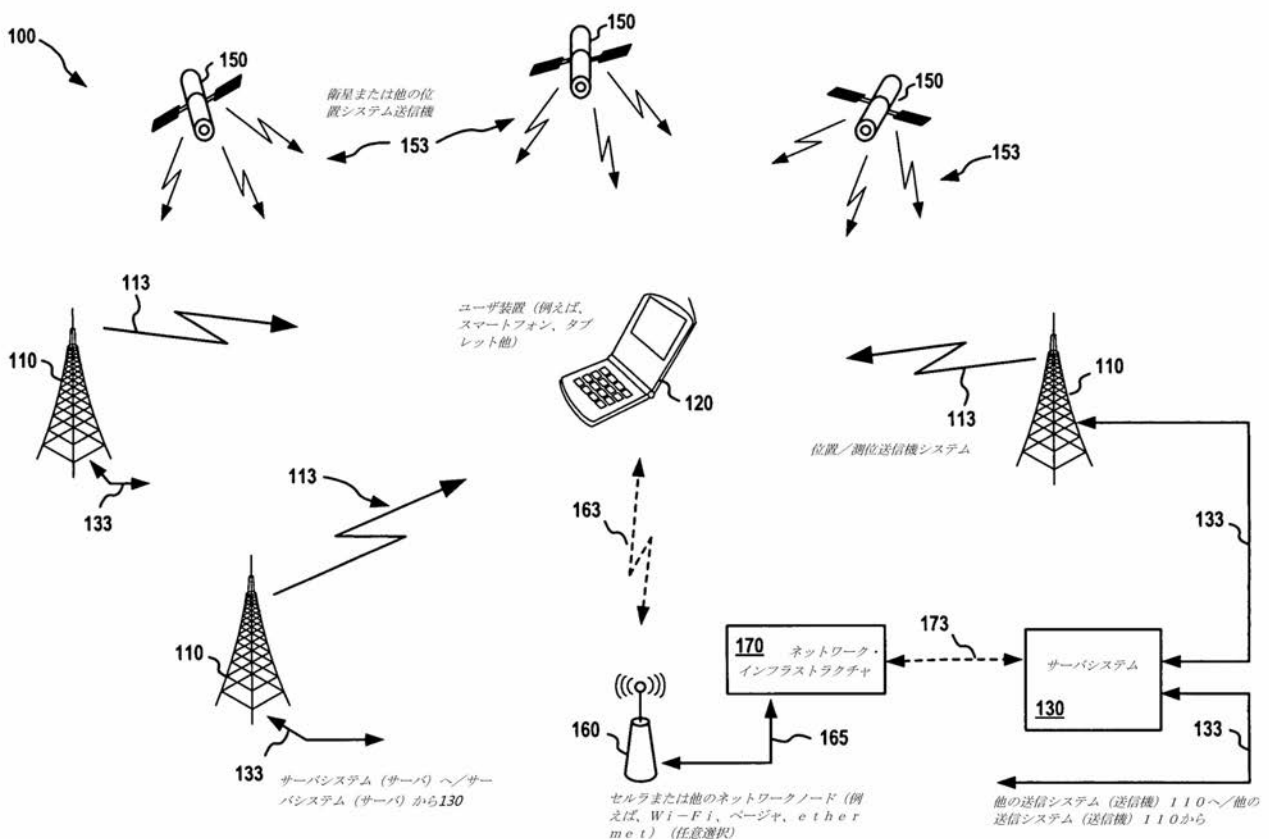
に留意されたい。このような転送は、これらの機能部間において直接行われる場合もあれば、図示しなくても中間的な機能部を通して行われる場合もある。2つの機能部を接続する線がない場合、他に明記しない限り、これらの機能部間のデータ転送があり得る。よって、これらの線は特定の態様を例示するために設けたのであって、制限的なものとして解釈されるべきではない。

【0151】

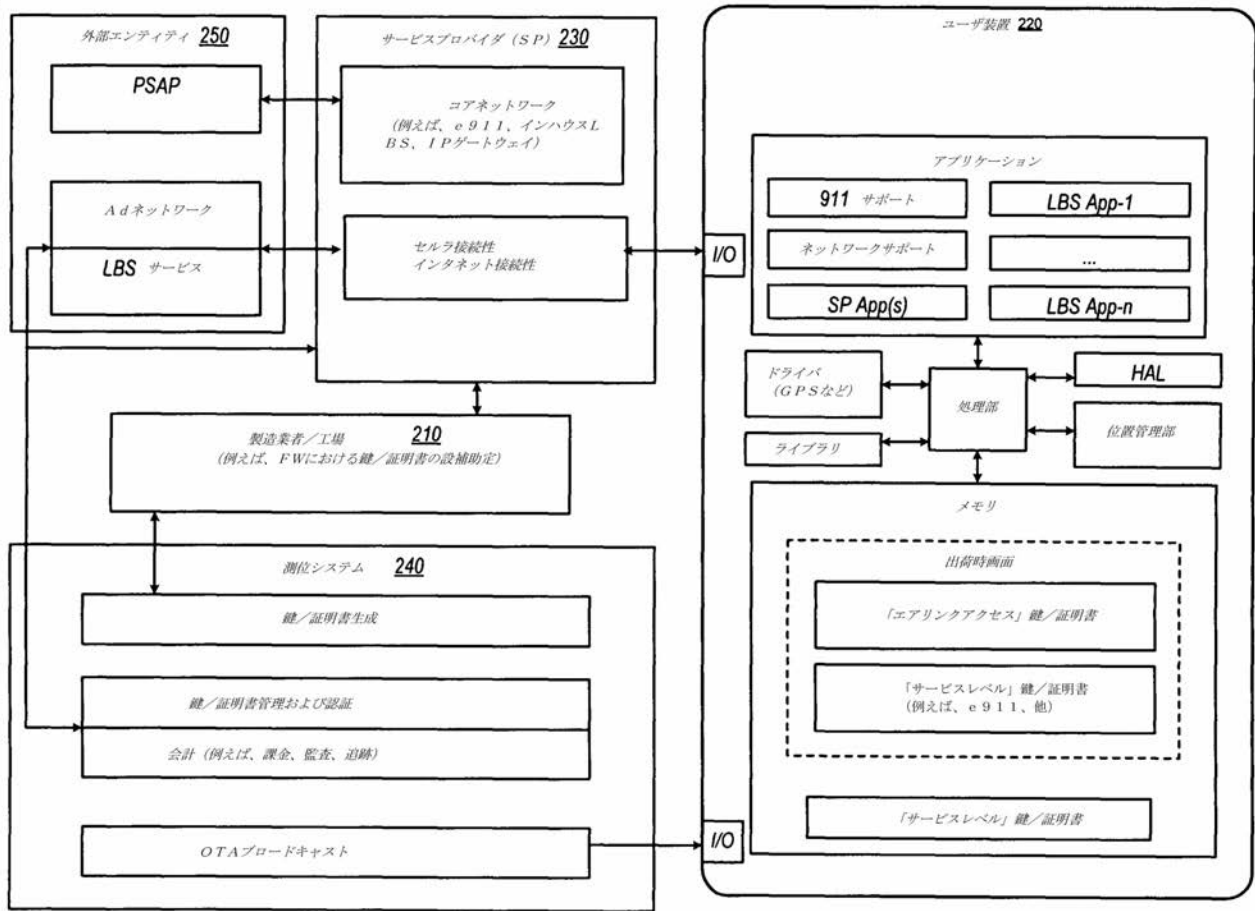
本開示は、本願に示す態様に限定するものとして解釈されるべきでなく、相当するシステムおよび方法を含む当業者の最も広い理解の範囲として解釈されるべきである。本発明によって提供される保護は、以下の特許請求の範囲のみに従って制限されるべきである。

10

【図1】



【図 2】



【図 3】

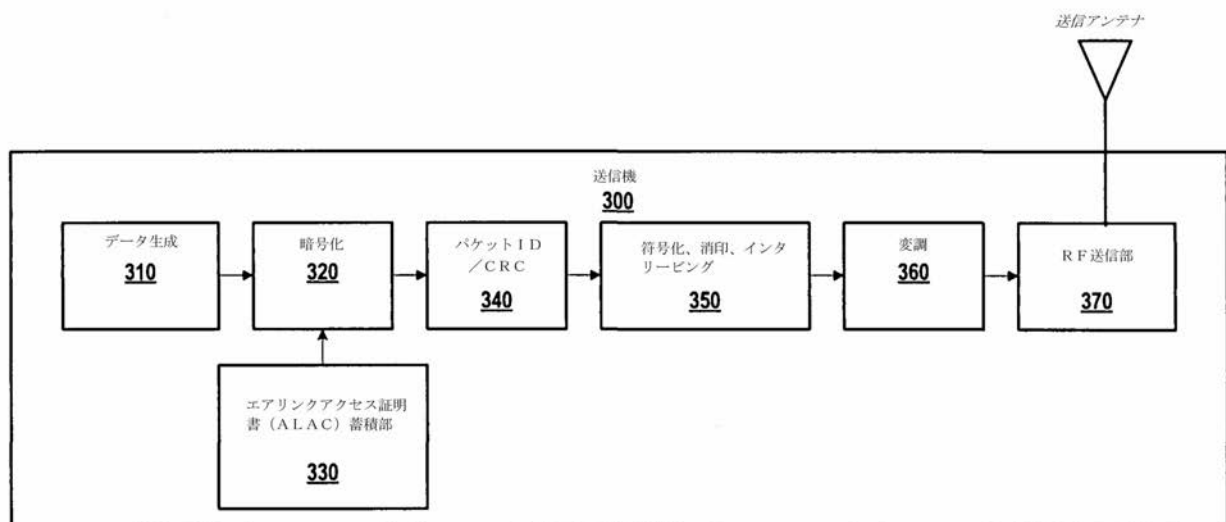
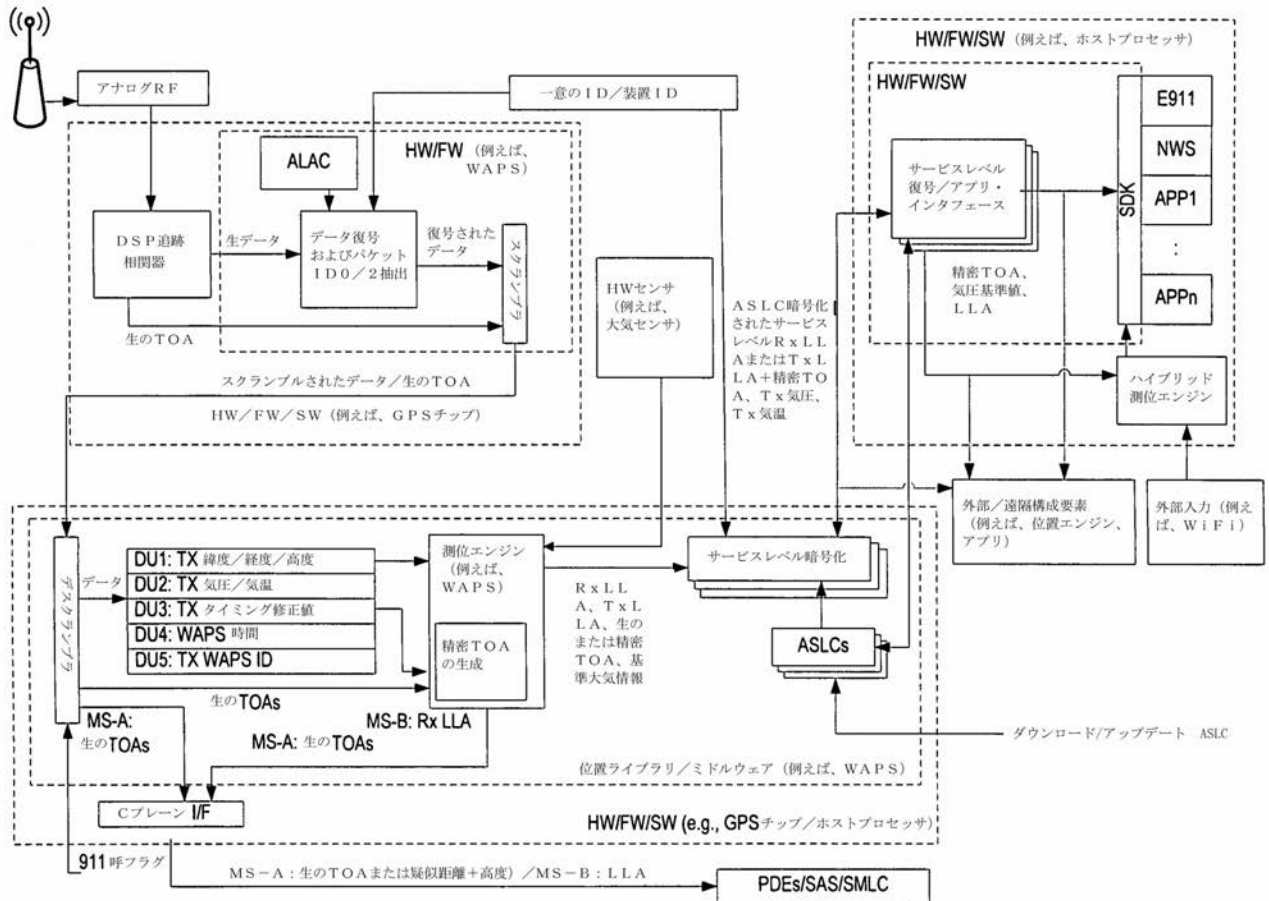


Figure 1 is a block diagram of a mobile station device. The diagram illustrates the internal components and data flow of the device. Key components include:

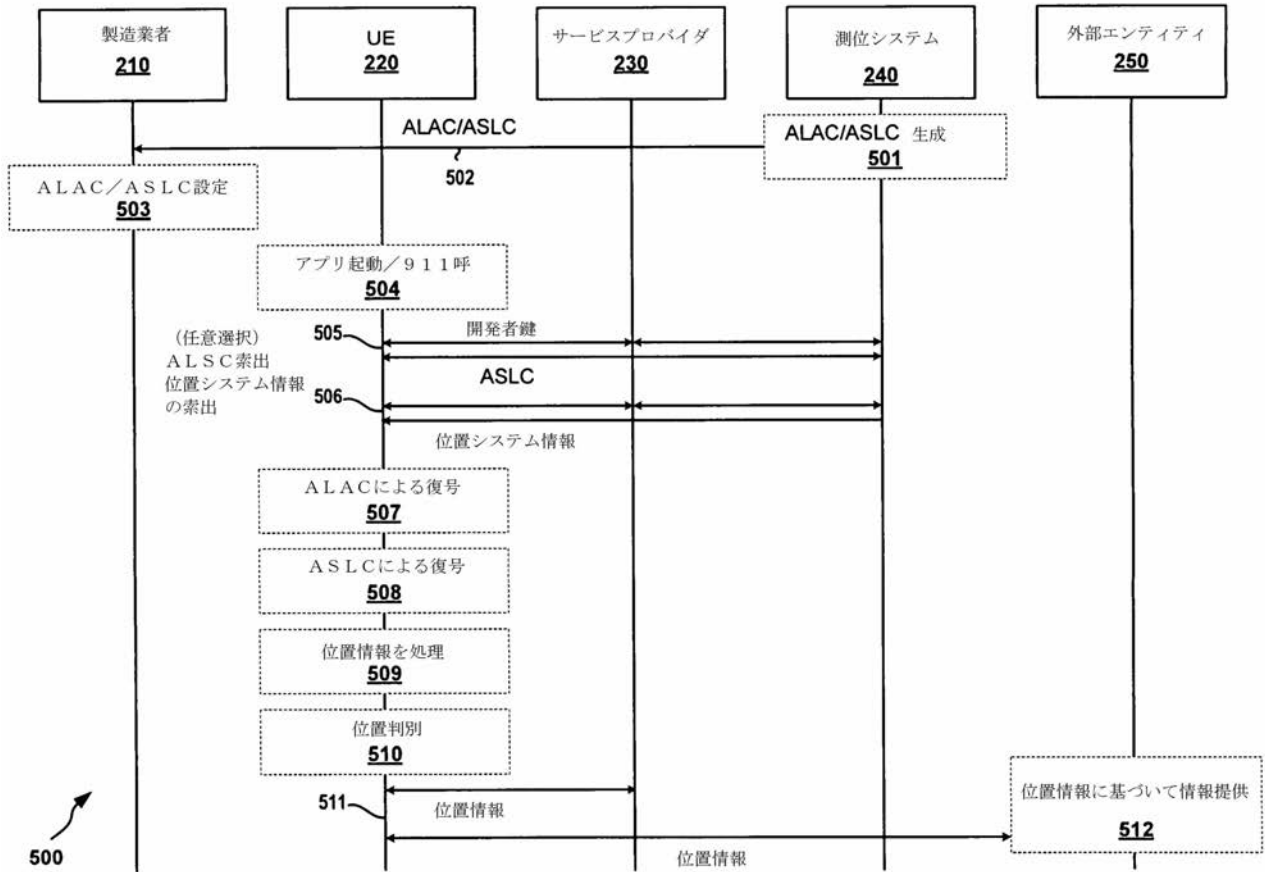
- Antenna (アンテナ)**: Connected to the **RF I/O 410** block.
- RF I/O 410**: Receives RF signals from other blocks or the antenna.
- Cellular Data (セルラ (n回目生成) 490)**: Provides **セルラデータ** (Cellular data) to the **位置エンジン 440** (Position engine).
- Satellite (衛星 480)**: Provides **GPSデータ; GPS疑似距離補助** (GPS data; GPS pseudo-range assistance) to the **位置エンジン 440**.
- Network Data (ネットワークデータ)**: Provides data to the **位置エンジン 440**.
- Position Engine (位置エンジン 440)**: Processes data from cellular, satellite, and network sources to generate **測位データ** (Positioning data).
- Application (アプリケーション (例えば、E-911 LBS) 450)**: Receives data from the position engine and provides output to other blocks.
- Signal Processing (信号処理 421)**: A sub-system containing:
 - Digital Processing (デジタル処理 (例えば、T-OA推定、復調) 421a)**: Receives RF signals and outputs to **データ処理 (復号、パケット抽出、CRC) 421c**.
 - Pseudo-range Generation (疑似距離生成 (例えば、TOAから) 421b)**: Receives timing correction and outputs pseudo-range data.
 - Data Processing (データ処理 (復号、パケット抽出、CRC) 421c)**: Outputs to **第1の暗号 422** and **第2の暗号 423**.
- Timing Correction (タイミング修正)**: Receives data from the position engine and outputs to the pseudo-range generation block.
- Pseudo-range (疑似距離)**: Receives data from the pseudo-range generation block and outputs to the position engine.
- Call Flag (911 呼フラグ)**: A flag used for emergency calls, outputting to the position engine.
- Data Output (データ出力 (例えば、緯度、経度、高度、気圧、気温、システム時間、タイミング修正値、送信機ID) 424)**: Receives data from the position engine and outputs to the application.
- Memory (メモリ 430)**: Stores data, including **開発者鍵 (Developer key)**, **ALAC**, **ASLC**, and **他のデータ (Other data)**.

[illegible]

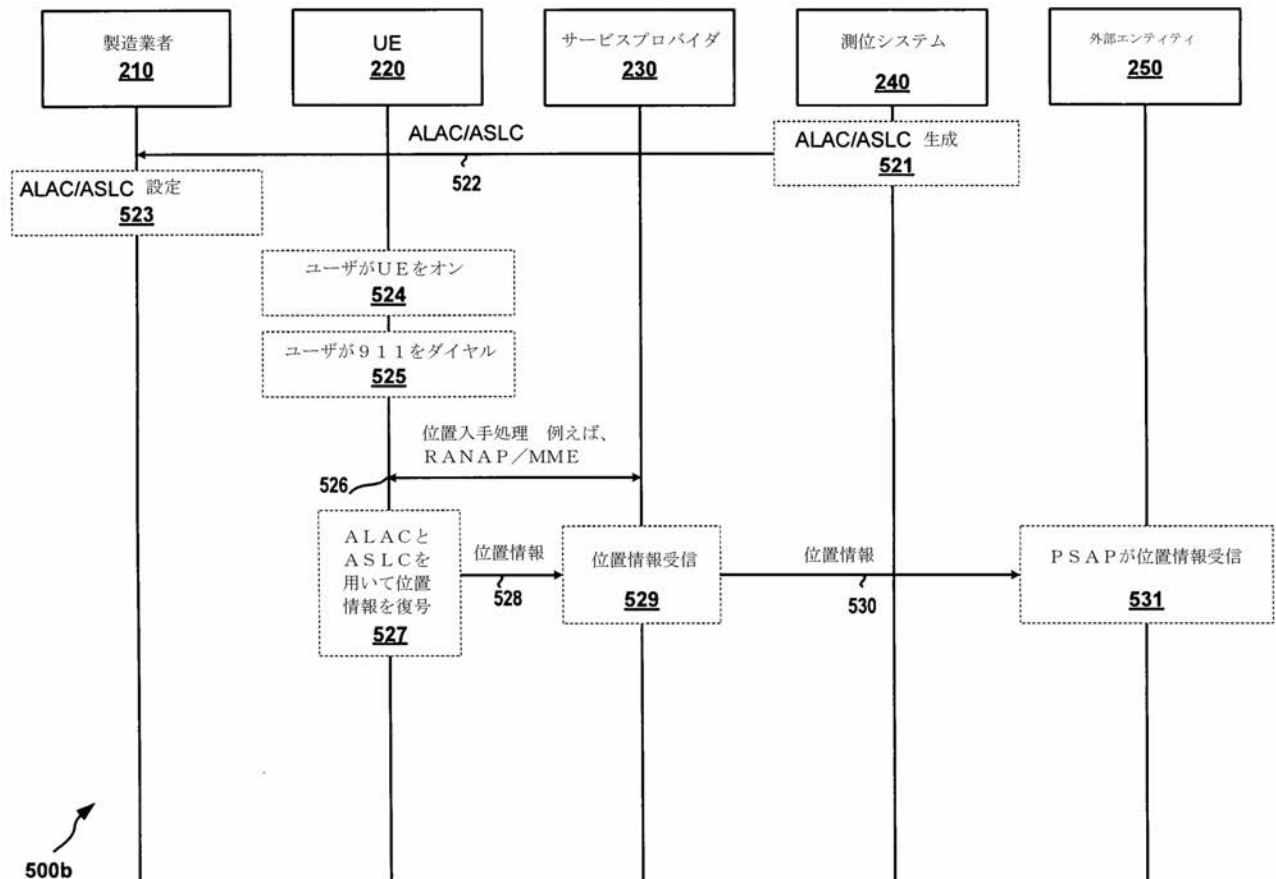
【図 4 C】



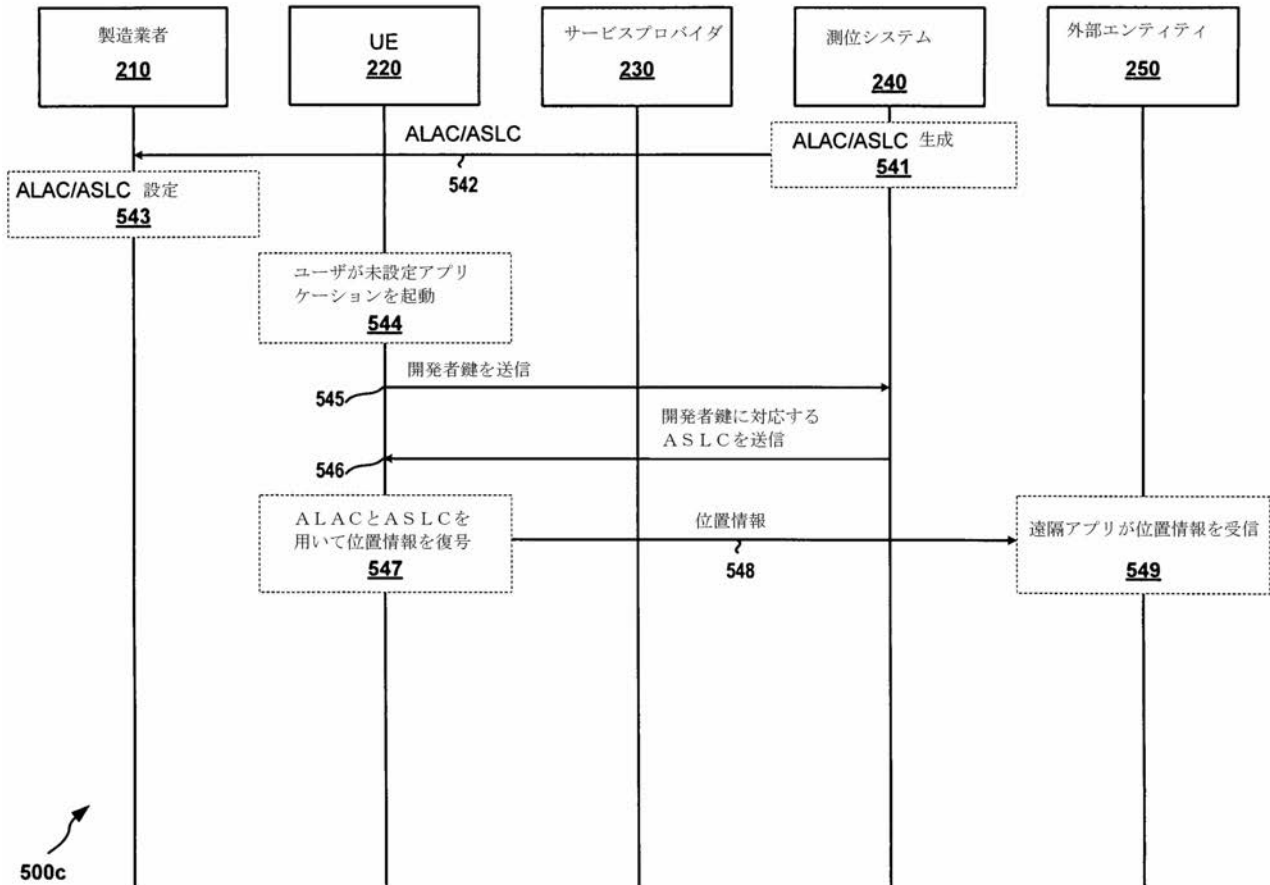
【図 5 A】



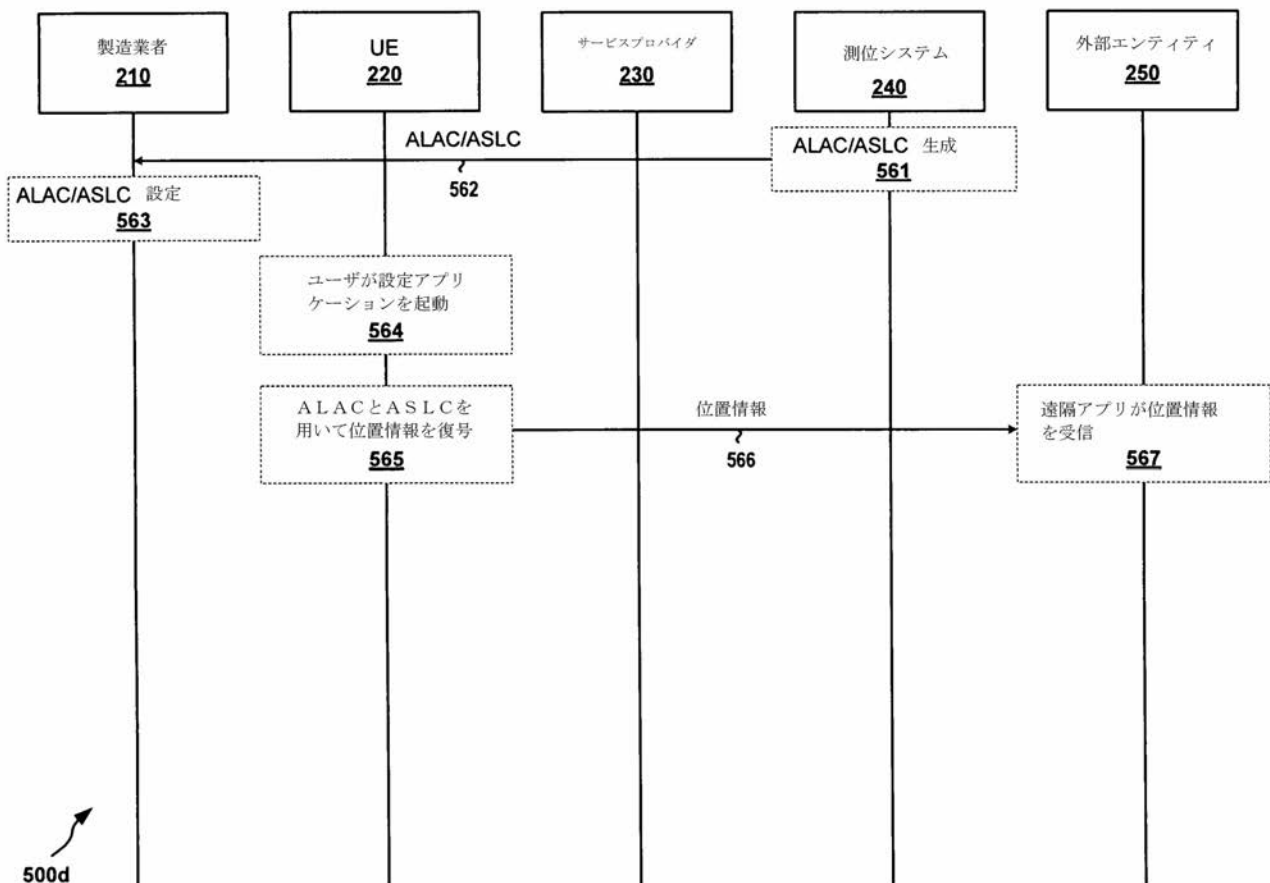
【図 5 B】



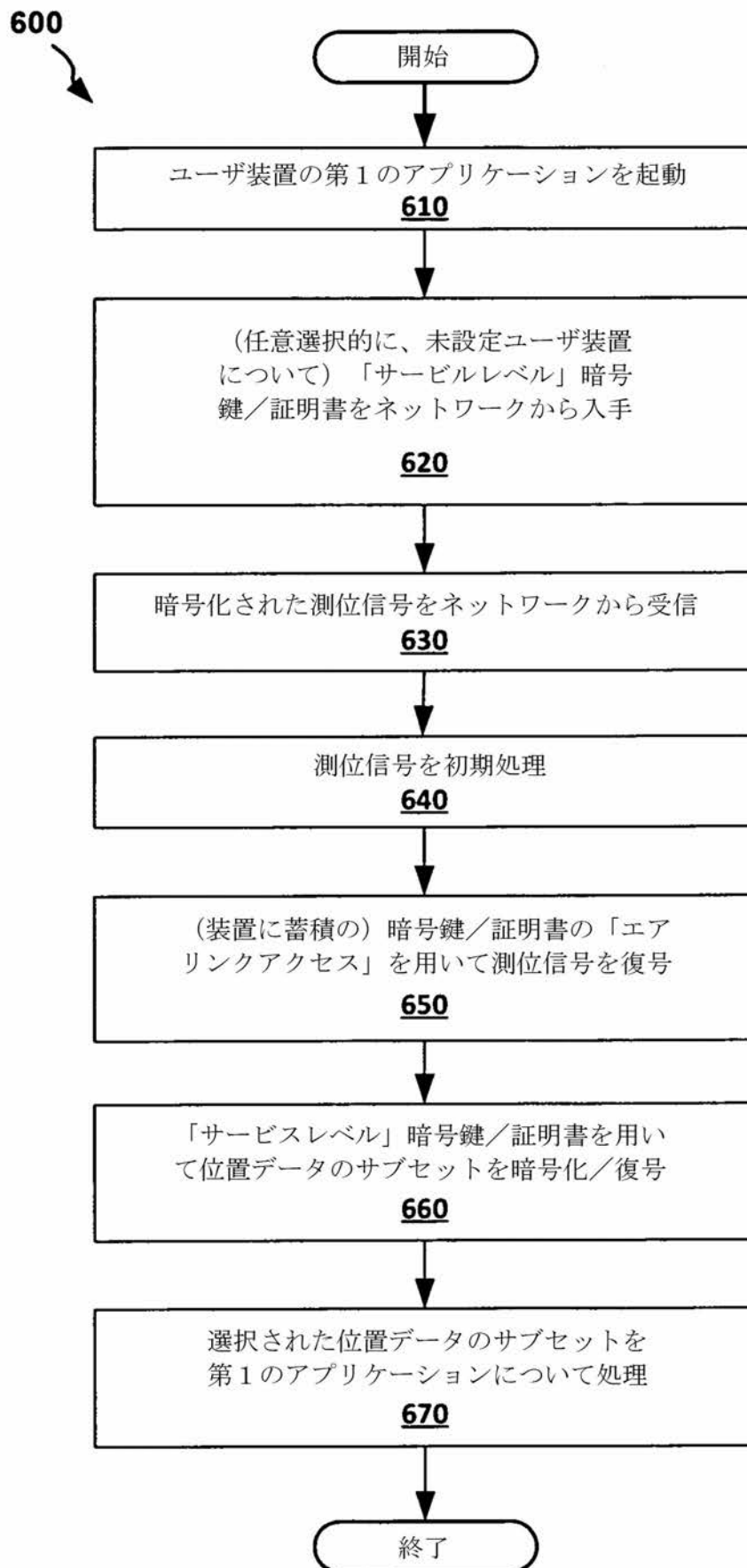
【図 5 C】



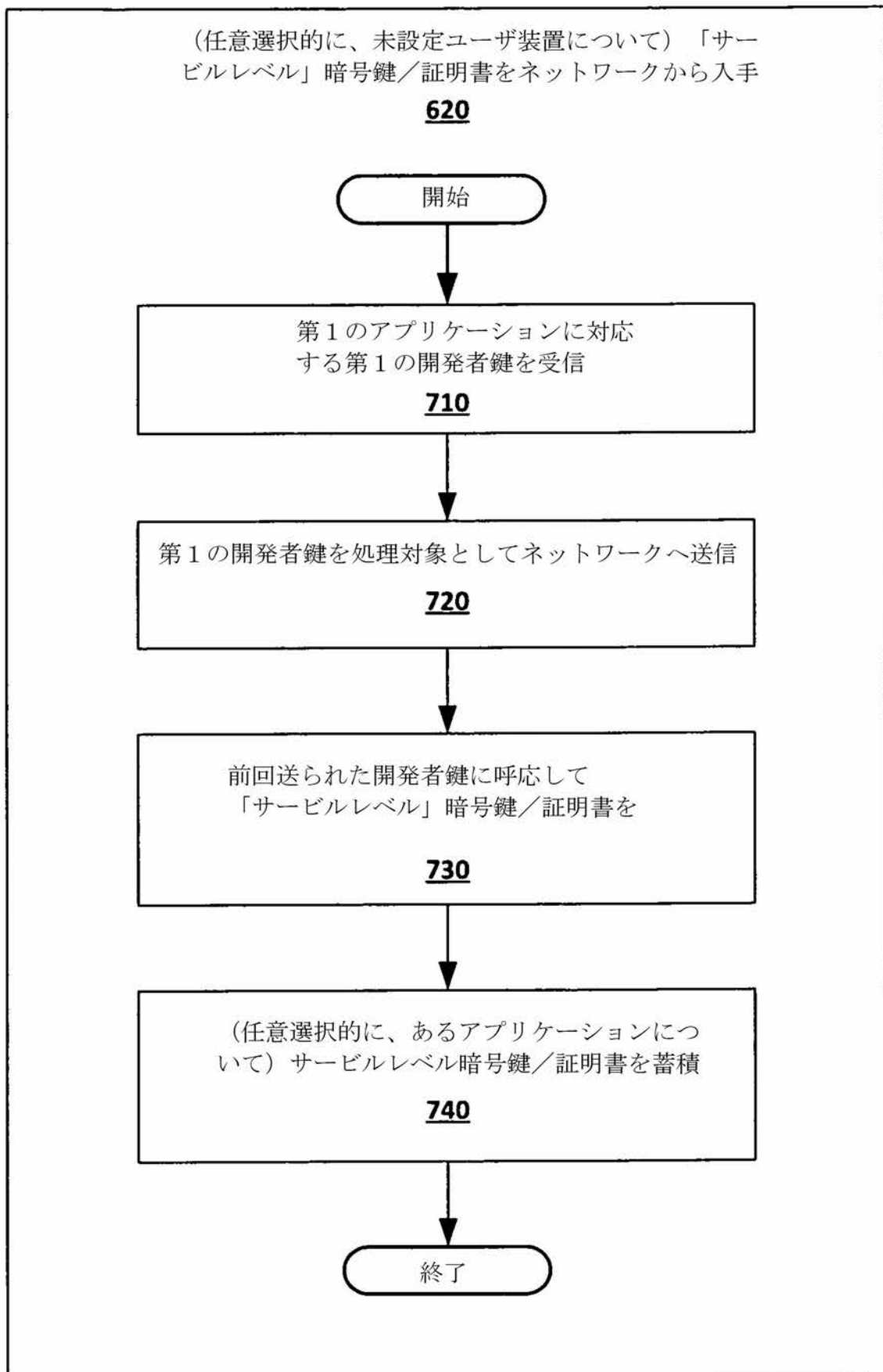
【図 5 D】



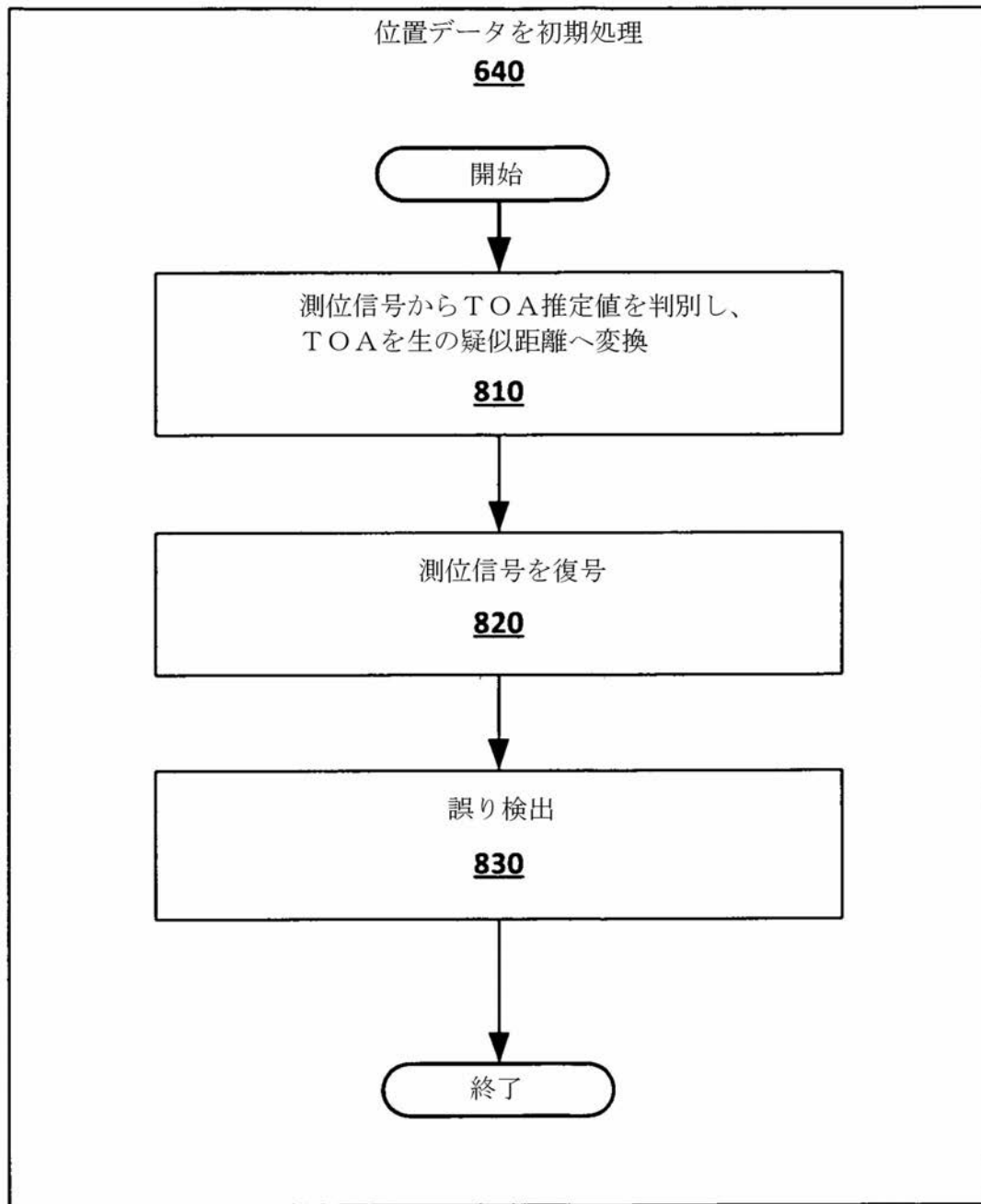
【図 6】



【図 7】



【図 8】



【図 9】

アプリケーション	UE (一意のID)	サービス	MNO	OEM	開発者	ユーザ (一意のID)	要求種別 (すな わち、サービス 要求を判別)	[他]
<ul style="list-style-type: none"> • E-911 • LBS • NW 		<ul style="list-style-type: none"> • 精度 • サービス • 時間 • DUs 	<ul style="list-style-type: none"> • ATT • Verizon • Sprint • 他 	<ul style="list-style-type: none"> • Apple • Samsung • MOT • 他 	<ul style="list-style-type: none"> • Apple • Google • マイクロソフト • 他 			

【図 10 A】

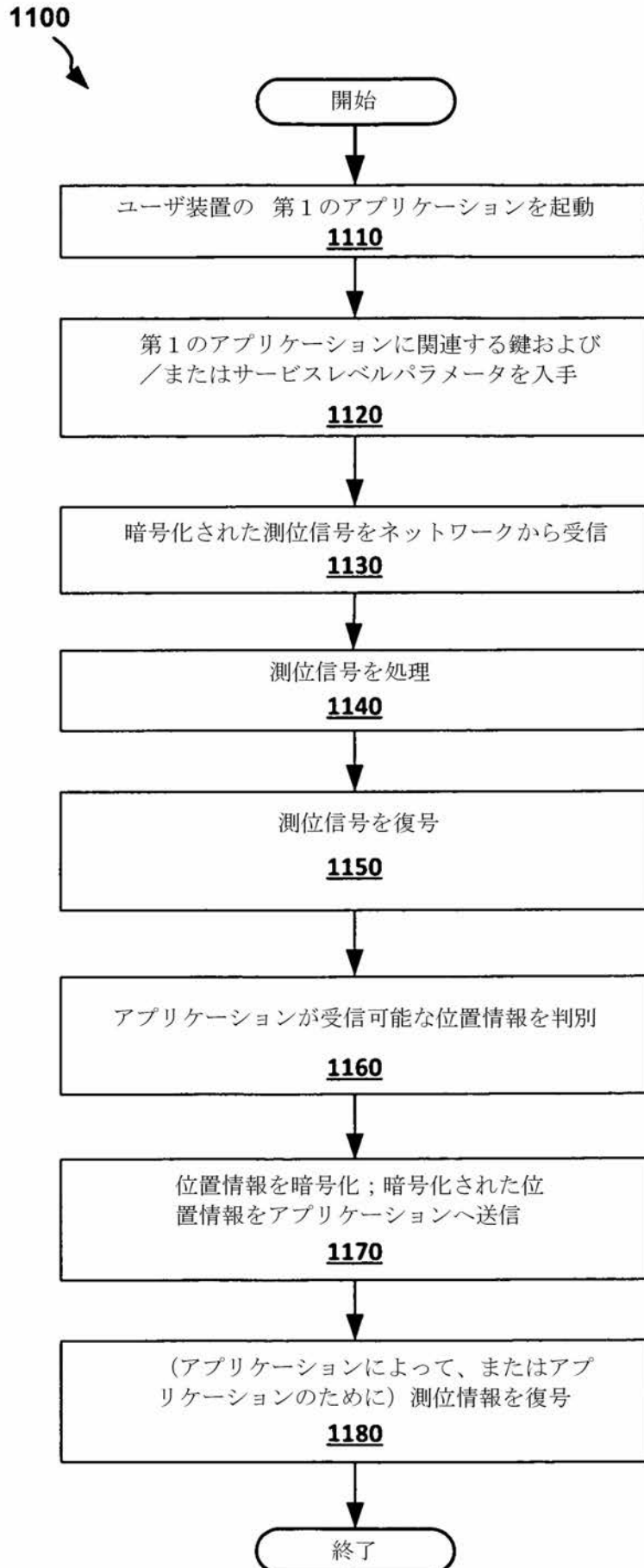
X	X	X	X	Y	Z	W	ペイロード (9 5
---	---	---	---	---	---	---	------------

XXXX : パケット種別
Y : 暗号ビット
Z : スタートビット
W : ストップビット

【図 10 B】

0	1	1	0	1	1	0	ペイロード (9 5ビット)	パケット種別 6 の暗号化された第 1 フレーム
0	1	1	0	1	0	0	ペイロード (9 5ビット)	パケットの続き
0	1	1	0	1	0	0	ペイロード (9 5ビット)	パケットの続き
...								
0	1	1	0	1	0	1	ペイロード (9 5ビット)	パケットの最終フレーム
1	1	0	0	0	1	0	ペイロード (9 5ビット)	パケット種別 1 2 の暗号化されていない第 1 フレーム、
1	1	1	0	0	0	1	ペイロード (9 5ビット)	パケットの最終スロット
1	0	0	1	1	1	1	ペイロード (9 5ビット)	パケット種別 9 の暗号化された第 1 フレームと最終フレーム

【図 11】



【国際調査報告】

A. CLASSIFICATION OF SUBJECT MATTER INV. H04L29/08 ADD.		
According to International Patent Classification (IPC) or to both national classification and IPC		
B. FIELDS SEARCHED Minimum documentation searched (classification system followed by classification symbols) H04W H04L		
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched		
Electronic data base consulted during the international search (name of data base and, where practicable, search terms used) EPO-Internal, WPI Data		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2001/055392 A1 (MCDONNELL JAMES THOMAS EDWARD [GB] ET AL) 27 December 2001 (2001-12-27) abstract paragraph [0029] paragraph [0051] - paragraph [0054] figure 7	1-36
A	US 2011/078376 A1 (DESHPANDE MANOJ M [US] ET AL) 31 March 2011 (2011-03-31) abstract paragraph [0023] - paragraph [0028] paragraph [0049] figure 5 claim 1	1-36
<input type="checkbox"/> Further documents are listed in the continuation of Box C. <input checked="" type="checkbox"/> See patent family annex.		
* Special categories of cited documents : "A" document defining the general state of the art which is not considered to be of particular relevance "E" earlier application or patent but published on or after the international filing date "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) "O" document referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art "&" document member of the same patent family		
Date of the actual completion of the international search		Date of mailing of the international search report
29 November 2013		06/12/2013
Name and mailing address of the ISA/ European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016		Authorized officer Canosa Aresté, C

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2001055392 A1	27-12-2001	DE 60131799 T2	05-06-2008
		EP 1139687 A2	04-10-2001
		JP 2001320760 A	16-11-2001
		US 2001055392 A1	27-12-2001

US 2011078376 A1	31-03-2011	CN 102550050 A	04-07-2012
		KR 20120079117 A	11-07-2012
		US 2011078376 A1	31-03-2011
		WO 2011041329 A1	07-04-2011

フロントページの続き

(81)指定国 AP(BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), EA(AM, AZ, BY, KG, KZ, RU, TJ, TM), EP(AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OA(BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG), AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ

(特許庁注：以下のものは登録商標)

1. B L U E T O O T H

2. E T H E R N E T

(72)発明者 ヴァージハラ, ヴアラブラサド
アメリカ合衆国, カリフォルニア州 9 4 5 8 2 サン ラモン, アスアーナ コート 2 3 5

(72)発明者 ジョセフ, ディーバック
アメリカ合衆国, ヴァージニア州 2 2 0 3 3 フェアファックス, インヴァ - ネス ロード
3 8 5 6

(72)発明者 メイヤッパン, サブラマニアン
アメリカ合衆国, カリフォルニア 9 5 1 3 1, サン ホゼ, フミア ドライブ 1 7 2 0

(72)発明者 ラグフパートシ, アルン
インド, バンガロール 5 6 0 0 6 6 ホワイトフィールド, アセート ガルデニア エンクラ
ヴェ ラマゴンダナハリー, ナンバー 1 4 イー

F ターム(参考) 5J104 AA01 AA12 AA16 EA15 JA00 NA02 NA03 NA37
5K067 DD19 DD20 EE02 EE10