(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2020-5282
(P2020-5282A)
(43)公開日　令和2年1月9日(2020.1.9)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 9/16	(2006.01)	H04L	9/00	643	5K067
H04L 9/32	(2006.01)	H04L	9/00	673C	
H04W 12/12	(2009.01)	H04W	12/12		

審査請求 有　請求項の数 10　OL　（全 13 頁）

(21)出願番号　特願2019-152075 (P2019-152075)
(22)出願日　令和1年8月22日 (2019.8.22)
(62)分割の表示　特願2016-557119 (P2016-557119)の分割
原出願日　平成27年3月30日 (2015.3.30)
(31)優先権主張番号　201410136738.0
(32)優先日　平成26年4月4日 (2014.4.4)
(33)優先権主張国・地域又は機関
中国 (CN)

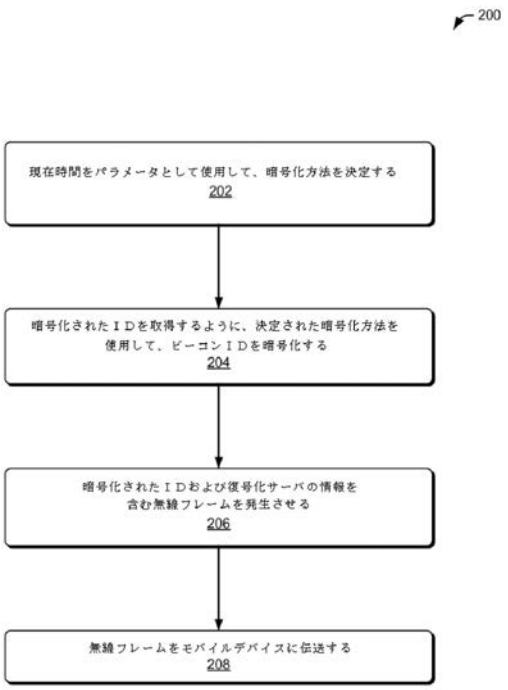
（特許庁注：以下のものは登録商標）
1．ＺＩＧＢＥＥ

(71)出願人　510330264
アリババ・グループ・ホールディング・リミテッド
ＡＬＩＢＡＢＡ　ＧＲＯＵＰ　ＨＯＬＤＩＮＧ　ＬＩＭＩＴＥＤ
英国領，ケイマン諸島，グランド・ケイマン，ジョージ・タウン，ワン・キャピタル・プレイス，フォース・フロア，ピー．オー．ボックス　８４７
(74)代理人　110001243
特許業務法人　谷・阿部特許事務所

最終頁に続く

(54)【発明の名称】ビーコンメッセージの伝送

(57)【要約】　（修正有）
【課題】ビーコンメッセージを伝送する方法及びシステムを提供する。
【解決手段】コンピューティングデバイスにより、所定のアルゴリズムに基づいて、現在時間をパラメータとして使用して、暗号化方法を決定する方法であって、暗号化されたビーコンメッセージを取得するように、決定された暗号化方法を使用してビーコンメッセージを暗号化し、暗号化されたビーコンメッセージ及び復号化コンピューティングデバイスと関連した情報を含む無線フレームを発生させ、当該無線フレームをモバイルデバイスに伝送する。ユーザの機密情報の漏洩が防止され、それゆえ、ユーザのプライバシーが保護され、また、ビーコン伝送の安全な使用が向上する。
【選択図】図２



【特許請求の範囲】
【請求項１】
現在時間に少なくとも部分的に基づいて、複数の異なる種類の暗号化方法の中から暗号化方法を決定することと、
前記決定された暗号化方法を使用して、ビーコンの識別子を暗号化し、前記ビーコンの暗号化された識別子を少なくとも含むビーコンメッセージを取得することと、
前記ビーコンメッセージを含む無線フレームを発生させることと、
前記無線フレームをモバイルデバイスに送信することと
を備える方法。
【請求項２】
前記モバイルデバイスのために前記ビーコンの前記暗号化された識別子を復号するように構成されたサーバの情報を検索することと、
前記サーバの前記情報を前記無線フレームにパッケージすることと
をさらに備える、請求項１の方法。
【請求項３】
前記サーバの前記情報は、前記モバイルデバイスが、復号のために前記ビーコンの前記暗号化された識別子を送信する前記サーバを識別し、および検索できるようにする、請求項２の方法。
【請求項４】
前記決定された暗号化方法を、相互参照を使用して、サーバによって使用される復号方法と同期することをさらに備える、請求項１の方法。
【請求項５】
前記相互参照は、前記現在時間を含む、請求項４の方法。
【請求項６】
前記決定された暗号化方法は、前記現在時間を使用して決定された暗号鍵を持つ暗号化アルゴリズムを含む、請求項１の方法。
【請求項７】
実行可能命令を格納する１つまたは複数のコンピュータ可読媒体であって、前記実行可能命令は、サーバの１つまたは複数のプロセッサによって実行される場合、前記１つまたは複数のプロセッサに、
現在時間に少なくとも部分的に基づいて、複数の異なる種類の復号方法の中から復号方法を決定することと、
ビーコンの暗号化された識別子を含む暗号化されたメッセージをモバイルデバイスから受信することと、
前記復号方法を使用して前記ビーコンの前記暗号化された識別子を復号し、前記ビーコンの復号された識別子を取得することと
を備える動作を実行させる、１つまたは複数のコンピュータ可読媒体。
【請求項８】
前記動作は、
前記ビーコンの前記復号された識別子に対応するサービスの情報を決定することと、
前記情報を前記モバイルデバイスに送信することと
をさらに備える、請求項７の１つまたは複数のコンピュータ可読媒体。
【請求項９】
前記動作は、前記決定された復号方法を、相互参照を使用して、前記ビーコンによって使用される暗号化方法と同期することをさらに備える、請求項７の１つまたは複数のコンピュータ可読媒体。
【請求項１０】
前記相互参照は、前記現在時間を含む、請求項９の１つまたは複数のコンピュータ可読媒体。
【発明の詳細な説明】

【技術分野】
【０００１】
関連出願の相互参照
本出願は、2014年4月4日に出願された、「ビーコンベースのサービスのためのビーコンメッセージの伝送方法及びデバイス」という表題の中国特許出願第201410136738.0号の優先権を主張するものであり、その全体が参照により本明細書に組み込まれる。
【０００２】
本開示は、通信ネットワーク技術に関し、より詳細には、ビーコンデータ伝送に関する。
【背景技術】
【０００３】
スマートフォン技術の人気と共に、モバイルデバイスは、人々の生活に深く定着してきている。例えば、モバイル測位技術を使用して、モバイルデバイスは個別的及び局所的サービスをユーザに提供する。
【０００４】
ＧＰＳ（全地球測位システム）は、現在、広く利用される測位技術である。しかし、ＧＰＳ受信機が室内で動作している場合、部屋が信号を減衰させ、ＧＰＳの精度を低下させる。最近、ＷｉＦｉ（Wireless Fidelity）、ＺｉｇＢｅｅ、Ｂｌｕｅｔｏｏｔｈ（登録商標）、及び、超広域ワイヤレスネットワークなどの屋内測位技術が開発されている。
【０００５】
ビーコンは、屋内測位技術を実施し、建物内部の測位に有望な解決策を提供する。ビーコンは、無線フレームを発生させて、一定のビーコン信号領域におけるモバイルデバイスに伝送する。しかし、モバイルデバイスに常駐するアプリケーションが、ビーコンとモバイルデバイスとの通信中にユーザの機密情報を検索することがあるので、セキュリティがビーコン技術の商用化にとって問題となっている。
【発明の概要】
【０００６】
本概要は、詳細に以下でさらに説明される選択された概念を簡易化した形で紹介するために提供される。本概要は、請求される主題のすべての重要な特徴または不可欠な特徴を特定することを意図するものでなく、また、請求される主題の範囲を決定する助けとしてのみ使用されることを意図するものでもない。「技法」という用語は、例えば、上記の文脈により、及び、本開示全体を通して認められるような、装置、システム、方法、及び／または、コンピュータにより実行可能な命令を指してよい。
【０００７】
本開示の実施態様は、ビーコンメッセージを伝送するための方法に関する。実施態様は所定のアルゴリズムに基づいたビーコンの１つまたは複数のプロセッサにより、現在時間をパラメータとして使用して、暗号化方法を決定することを含んでよい。ビーコンは、ビーコンの暗号化されたＩＤを含むビーコンメッセージを取得するように、決定された暗号化方法を使用して、ビーコンの識別子（ＩＤ）を暗号化してよい。ビーコンは、ビーコンメッセージ及び復号化コンピューティングデバイスと関連した情報を含む無線フレームを発生させてよく、当該無線フレームをモバイルデバイスに伝送してよい。
【０００８】
本開示の実施態様はさらに、コンピュータにより実行可能な命令を記憶する１つまたは複数のコンピュータ可読媒体に関し、当該命令は、１つまたは複数のプロセッサにより実行される場合、１つまたは複数のプロセッサに動作を実行するように命令する。動作は、所定のアルゴリズムに基づいたコンピューティングデバイスにより、現在時間をパラメータとして使用して、復号化方法を決定することを含んでよい。コンピューティングデバイスは、ビーコンの暗号化されたＩＤを含む暗号化されたビーコンメッセージをモバイルデバイスから受信してよい。コンピューティングデバイスは、ビーコンのＩＤを取得するように、決定された復号化方法を使用して、暗号化されたＩＤを復号化してよく、ビーコン

のＩＤに対応するタスクをモバイルデバイスに提供してよい。
【０００９】
本開示の実施態様はさらに、１つまたは複数のプロセッサと、１つまたは複数のプロセッサにより実行可能な複数の構成要素を保持するメモリとを含むシステムに関する。複数の構成要素は、暗号化決定モジュール、暗号化モジュール、及び、伝送モジュールを含んでよい。暗号化決定モジュールは、所定のアルゴリズムに基づいて、現在時間をパラメータとして使用して、暗号化方法を決定するように構成される。暗号化モジュールは、ビーコンの暗号化されたＩＤを含むビーコンメッセージを取得するように、当該決定された暗号化を使用して、ビーコンのＩＤを暗号化するように構成される。伝送モジュールは、ビーコンメッセージ及び復号化コンピューティングデバイスと関連した情報を含む無線フレームを発生させるように、及び、当該無線フレームをモバイルデバイスに伝送するように構成される。
【００１０】
本開示の実施態様はさらに、１つまたは複数のプロセッサと、１つまたは複数のプロセッサにより実行可能な複数の構成要素を保持するメモリとを含む別のシステムに関する。複数の構成要素は、復号化決定モジュール、暗号化メッセージ受信モジュール、暗号化メッセージ受信モジュール、復号化モジュール、及び、タスク提供モジュールを含んでよい。復号化決定モジュールは、所定のアルゴリズムに基づいて、現在時間をパラメータとして使用して、復号化方法を決定するように構成される。暗号化メッセージ受信モジュールは、ビーコンの暗号化されたＩＤを含むビーコンメッセージをモバイルデバイスから受信するように構成される。復号化モジュールは、ビーコンのＩＤを取得するように、決定された復号化方法を使用して、暗号化されたＩＤを復号化するように構成される。タスク提供モジュールは、ビーコンのＩＤに対応するタスクをモバイルデバイスに提供するように構成される。
【００１１】
本開示の実施態様は、許可されていないマルウェアがビーコンの真正且つ安定したＩＤを取得することができないように、ビーコンＩＤと関連した経時変化する暗号化を発生させてよい。それゆえ、ユーザの機密情報を含むことがある、サービスに対応するビーコンＩＤを偽造するのは困難である。これにより、ユーザの利益が保護され、また、ビーコンネットワークの安全性が改善される。
【００１２】
発明を実施するための形態が、添付の図面を参照して説明される。異なる図面における同じ参照番号の使用は、類似または同一の項目を示す。
【図面の簡単な説明】
【００１３】
【図１】ビーコンメッセージの伝送を可能にする説明的なコンピューティング環境の概略図である。
【図２】ビーコンメッセージを伝送するための説明的なプロセスのフローチャートである。
【図３】ビーコンベースのサービスを提供するための説明的なプロセスのフローチャートである。
【図４】ビーコンメッセージの伝送を可能にする説明的なコンピューティングアーキテクチャの概略図である。
【図５】ビーコンメッセージの伝送を可能にする説明的なコンピューティングアーキテクチャの概略図である。
【発明を実施するための形態】
【００１４】
従来の技法では、ビーコンの識別子（ＩＤ）は、暗号化されていないメッセージを介して伝送される。モバイルデバイス上のアプリケーションは、当該ＩＤを取得できる。これはマルウェアの機会を提供する。ビーコンＩＤが、悪質なソフトウェア設計者によって取

得された後、こうした設計者は、顧客をフィッシングサーバに導くことがあり、また、顧客の金融情報を取得するために虚偽の注文／支払いページを使用することがある。

【００１５】

本開示の実施態様は、従来の技法の問題に対処するために、ビーコンデータ伝送の新たな方法に関する。図１は、ビーコンメッセージの伝送を可能にする説明的なコンピューティング環境１００の概略図である。当該環境は、ビーコン信号１０４を発生させてよいビーコン１０２、及び、一定の距離内でビーコン信号１０４を受信してよいモバイルデバイス１０６を含んでよい。いくつかの実施態様において、ビーコン信号１０４は、ビーコン１０２と関連した暗号化された情報１１２、及び／または、ビーコン１０２と関連したサービスを含んでよい。モバイルデバイス１０６及びビーコン１０２は、データ伝送用の様々なサポートされるワイヤレスプロトコルを使用してよい。モバイルデバイス１０６は、ネットワーク１１０を介してサーバ１０８とさらに通信してよい。いくつかの実施態様において、ビーコン１０２は、モバイル通信ネットワーク、ネットワーク管理サーバ、及び／または、データ交換用の他のデバイスに接続されてよい。コンピューティング環境１００において使用されるワイヤレス通信のモバイルデバイス、プロトコル、またはネットワーク構造の種類は、本開示の実施態様によって限定されない。

【００１６】

本開示の実施態様は、ビーコン１０２の暗号化されたＩＤなどの暗号化情報を含むビーコンメッセージを発生させるように、ビーコン１０２のＩＤを暗号化してよい。ビーコンメッセージは、経時的に修正されてよい暗号化方法を使用して暗号化されてよい。いくつかの実施形態において、ビーコンメッセージを受信した後、モバイルデバイス１０６は、ビーコンメッセージをサーバ１０８に送信してよい。サーバ１０８は、ビーコンメッセージを復号化してよく、モバイルデバイス１０６と関連した顧客に、対応するサービスを提供してよい。

【００１７】

図２は、ビーコンメッセージを伝送するための説明的なプロセスのフローチャートである。２０２で、ビーコン１０２は、所定のアルゴリズムに基づいて、現在時間をパラメータとして使用して、暗号化方法を決定してよい。いくつかの実施態様において、ビーコン１０２は、現在時間を使用して暗号化アルゴリズムを決定してよい。いくつかの実施態様において、ビーコン１０２は、現在時間を使用してプライベート鍵を決定するように所定の暗号化アルゴリズムを実施してよい。あるいは、ビーコン１０２は、現在時間を使用して暗号化アルゴリズム及びプライベート鍵を決定してよい。すなわち、暗号化方法は、暗号化アルゴリズム及び／またはプライベート鍵を含んでよい。これらの例において、サーバ１０８は、復号化のために、対応する復号化方法を使用してよい。

【００１８】

いくつかの実施態様において、ビーコン１０２は、一定の位置にインストールされてよく、また、当該インストール後に初期構成が実行されてよい。初期構成の後、ビーコン１０２は、初期構成に基づいて無線フレームを発生させてよく、モバイルデバイス１０６などのコンピューティングデバイスに当該無線フレームを伝送してよい。いくつかの実施態様において、ビーコン１０２の暗号化はビーコン１０２によって実行されてよく、復号化はサーバ１０８によって実行されてよい。いくつかの実施態様において、サーバ１０８及びビーコン１０２は、ほとんど通信しなくてもよい。これらの例において、暗号化及び復号化は、それぞれ暗号化方法及び復号化方法を同期及び／または修正するように、相互参照を使用して実施されてよい。例えば、相互参照には現在時間が含まれてよい。

【００１９】

ビーコン１０２及びサーバ１０８は、所定の時間期間の間、それぞれ暗号化方法及び復号化方法を修正してよい。いくつかの実施態様において、修正周波数が、様々な条件に基づいて決定されてよい。例えば、暗号化方法及び復号化方法は、固定及び／または可変の時間間隔の後に修正されてよい。暗号化方法及び復号化方法は、ビーコン１０２により暗号化されたメッセージが、サーバ１０８により復号化されてもよいように、対応するやり

方で同時に修正されてよい。
【００２０】
例えば、ビーコン１０２及びサーバ１０８は、所定の対称暗号化アルゴリズムを（例えば、同一の復号化及びプライベート鍵を使用して）実施してよい。暗号化及びプライベート鍵は、アルゴリズムに基づいて、現在時間の整数（例えば９：４５に対して９）を入力パラメータとして使用して決定されてよい。従って、ビーコン１０２及びサーバ１０８は、それぞれ毎時に暗号化方法及び復号化方法を修正してよい。
【００２１】
いくつかの実施態様において、ビーコン１０２は、Ｎ種類の暗号化方法をプリセットしてよい。Ｎは、１よりも大きい自然数である。ビーコン１０２は、所定のマッピングアルゴリズムを使用して、現在時間をＭにマッピングしてよく、Ｍに対応する暗号化方法を、決定された暗号化方法として指定してよい。Ｍは１よりも大きいか、または１と等しく、且つ、Ｎよりも小さい自然数である。いくつかの実施態様において、サーバ１０８は、Ｎ種類の暗号化方法に対応するＮ種類の復号化方法をプリセットしてよい。同じマッピングアルゴリズムに従って、サーバ１０８は、決定された復号化方法として実施されてよいＭ番の復号化方法を取得してよい。従って、ビーコン１０２及びサーバ１０８は、それぞれ対応する暗号化及び復号化方法を有してよい。
【００２２】
２０４で、ビーコン１０２は、ビーコン１０２の暗号化されたＩＤを含むビーコンメッセージを取得するように、決定された暗号化方法を使用してビーコンのＩＤを暗号化してよい。いくつかの実施態様において、ビーコン１０２によって発生及び／または伝送される無線フレームは、ビーコンメッセージを含んでよい。これらの例において、無線フレームは、ビーコン１０２の一意的なＩＤ、ならびに、ビーコン１０２の位置コード及びビーコン１０２の機器情報などの他のビーコン情報を含んでよい。ビーコン１０２は、ＩＤ、及び／または、サーバ１０８が暗号化された情報を正確に復号化し得る限り、ビーコン１０２と関連した他のビーコン情報を暗号化してよい。
【００２３】
例えば、ビーコン１０２の無線フレームは、以下の種類の情報、すなわち、ＵＵＩＤ、Ｍａｊｏｒ（例えば、ビーコン１０２の主要な特徴）、Ｍｉｎｏｒ（例えば、ビーコン１０２の副次的な特徴）、Ｍｅａｓｕｒｅｄ　Ｐｏｗｅｒ（例えば、強さの測定）を含んでよい。ＵＵＩＤは、ビーコン１０２、すなわちビーコンＩＤを一意的に特定するのに使用される１２８ビットのＩＤであってよい。Ｍａｊｏｒ及びＭｉｎｏｒは、１６ビットのＩＤであってよく、ビーコン１０２の追加のＩＤ情報を伝えるようにビーコンオペレータによって設定される。例えば、或る店舗は、Ｍａｊｏｒに位置情報を含んでよく、また、当該店舗と関連した参照番号及び／またはＩＤを含んでよい。例えば、ビーコン１０２が或る機器にインストールされる場合、製品モデルがＭａｊｏｒに含まれてよく、エラーの種類に対応する参照番号がＭｉｎｏｒに含まれてよい。
【００２４】
Ｍｅａｓｕｒｅｄ　Ｐｏｗｅｒは、ビーコンの伝送モジュールと受信機（例えば、モバイルデバイス１０６）との間の距離がおおよそ所定の距離（例えば、１メートル）である場合、ビーコン１０２により発生される信号強度を示す強度基準を表してよい。受信機は、強度基準及び現在受信される信号強度に基づいて距離を判定してよい。暗号化の間、ビーコン１０２は、ビーコン１０２と関連したＵＵＩＤ、Ｍａｊｏｒ、または、Ｍｉｎｏｒのうちの少なくとも１つを暗号化してよい。
【００２５】
２０６で、ビーコン１０２は、暗号化されたＩＤと、復号化コンピューティングデバイス（例えば、サーバ１０８）と関連した情報とを含む、無線フレームを発生させてよい。
【００２６】
いくつかの実施態様において、モバイルデバイス１０６は、無線フレームを受信してよく、ビーコン１０２の暗号化されていないＩＤを無線フレームから検索してよく、当該暗

号化されていないＩＤに対応する一定の動作を実行してよい。いくつかの実施態様において、こうした一定の動作は、対応するサーバのアドレスの探索及びこれとの接続を含んでよい。例えば、モバイルデバイス１０６は、サーバ１０８の対応するサーバアドレスを特定してよく、また、サーバ１０８への接続を開始してよい。他の実施態様において、ビーコン１０２のＩＤは暗号化されて得、モバイルデバイス１０６は、暗号化されたＩＤを復号化できないかもしれない。これらの例において、サーバ１０８が、暗号化されたＩＤを復号化するように構成されてよい。それゆえ、モバイルデバイス１０６が、対応する復号化方法を有する適切なサーバ（例えば、サーバ１０８）へ暗号化されたＩＤを伝送できるように、サーバ１０８の情報及び暗号化されたＩＤが、無線フレームに含まれてもよい。

【００２７】

ビーコン１０２は、サーバ１０８の情報を検索してよく、当該情報を無線フレームにまとめてよい。いくつかの実施態様において、ビーコン１０２は、モバイルデバイス１０６に常駐され、且つ、無線フレームを分析するアプリケーションを使用して、情報を検索してよい。例えば、情報は、モバイルデバイス１０６がそれに応じてサーバ１０８を特定及び／または探索できるように、アプリケーションにより認識されるサーバ１０８のＩＰ（インターネットプロトコル）アドレス、ＵＲＬ（ユニフォームリソースロケータ）アドレス、または、番号を含んでよい。

【００２８】

２０８で、ビーコン１０２は、サーバ１０８を特定し、且つ、復号化の要求をサーバ１０８に伝送するモバイルデバイス１０６に、無線フレームを伝送してよい。

【００２９】

図３は、ビーコンベースのサービスを提供するための説明的なプロセスのフローチャートである。３０２で、サーバ１０８は、所定のアルゴリズムに基づいて、現在時間をパラメータとして使用して、復号化方法を決定してよい。いくつかの実施態様において、復号化方法は、復号化アルゴリズム及び／またはプライベート鍵を含んでよい。

【００３０】

いくつかの実施態様において、サーバ１０８は、Ｎ種類の復号化方法をプリセットしてよい。Ｎは、１よりも大きい自然数である。サーバ１０８は、所定のマッピングアルゴリズムを使用して、現在時間をＭにマッピングしてよく、Ｍに対応する復号化方法を、決定された暗号化方法として指定してよい。Ｍは、１よりも大きいか、または１と等しく、且つ、Ｎよりも小さい自然数である。サーバ１０８と関連した復号化方法が、ビーコン１０２と関連した暗号化方法に対応するので、サーバ１０８は、ビーコン１０２により決定及び／または指定された暗号化方法に基づいて、復号化方法を決定してよい。

【００３１】

３０４で、サーバ１０８は、ビーコン１０２の暗号化されたＩＤを含む暗号化されたメッセージを受信してよい。例えば、モバイルデバイス１０６は、無線フレームを受信してよく、サーバ１０８の情報及び暗号化されたメッセージを無線フレームから検索してよい。モバイルデバイス１０６は、ビーコン１０２の暗号化されたＩＤを含む暗号化されたメッセージをサーバ１０８に伝送してよい。

【００３２】

３０６で、サーバ１０８は、ビーコン１０２の暗号化されたＩＤに対応する復号化方法に基づいて、ビーコン１０２のＩＤを取得してよい。ビーコン１０２のＩＤに加えて、サーバ１０８は、ビーコン１０２の位置コード及びビーコン１０２の機器情報などの他のビーコン情報を復号化してよい。

【００３３】

３０８で、サーバ１０８は、ビーコン１０２のＩＤに対応するタスクの情報（例えば、サービス）を判定してよく、当該情報をモバイルデバイス１０６に伝送してよい。いくつかの実施態様において、サーバ１０８は、ビーコン１０２のＩＤに対応するタスクを特定及び／または位置ずけてよく、タスクの情報をモバイルデバイス１０６に伝送してよい。例えば、サーバ１０８は、ビーコン１０２と関連した店舗の情報を記憶してよい。当該情

報は、店舗により顧客に提供されるサービスを含んでよい。サーバ１０８は、ビーコン１０２のＩＤを取得してよく、ビーコン１０２と関連した店舗を特定及び／または位置ずけてよく、店舗と関連したサービスの情報を顧客に提供してよい。

【００３４】

モバイルデバイス１０６が、ビーコン１０２のＩＤ及び追加の情報をサーバ１０８に伝送できるので、サーバ１０８は、サービスの詳細且つ正確な情報をモバイルデバイス１０６へ提供できる。いくつかの実施態様において、サーバ１０８は、モバイルデバイス１０６からサーバ１０８へ伝送される追加の情報に基づいて、サービスをさらに促進してよい。追加の情報は、ビーコン１０２の位置、ビーコン１０２の機器情報、ビーコン１０２と関連した環境情報（例えば、天候及び交通）、または、モバイルデバイス１０６と関連したデバイス情報のうちの少なくとも１つを含んでよい。

【００３５】

ビーコン１０２がＢｌｕｅｔｏｏｔｈビーコン（例えばｉＢｅａｃｏｎ（登録商標））であると想定されたい。非対称暗号化及び復号化アルゴリズム（例えば、ＲＳＡ）が、ビーコン１０２のＵＵＩＤに対して実行されてよい。これらのアルゴリズムが、それぞれビーコン１０２及びサーバ１０８に対して実行されてよい。いくつかの例において、サーバ１０８及びビーコン１０２の暗号化方法は、それぞれプライベート鍵及び公開鍵であってよい。プライベート鍵及び公開鍵は、現在日時に基づいて決定されてよい。いくつかの実施態様において、ビーコン１０２は、Ｋ個の公開鍵をプリセットしてよく、サーバ１０８は、Ｋ個のプライベート鍵をプリセットしてよい。これらの例において、Ｋ個の公開鍵はＫ個のプライベート鍵に対応する。個別の公開鍵及び対応するプライベート鍵が、それぞれビーコン１０２及びサーバ１０８によって採用されてよい。ビーコン１０２及びサーバ１０８は、それぞれ個別の公開鍵及び対応する個別のプライベート鍵をさらに修正してよい。

【００３６】

いくつかの実施態様において、Ｋ個の公開鍵及び現在時間が、ビーコン１０２に記憶されてよい。ビーコン１０２は、現在時間及び所定のアルゴリズムに基づいてプライベート鍵を決定及び／または設定してよい。ビーコン１０２はさらにＵＵＩＤを暗号化してよく、暗号化されたメッセージ及びサーバ１０８と関連した情報を含む情報をモバイルデバイス１０６へ伝送してよい。

【００３７】

ビーコン１０２が固定周波数で無線フレームを伝送できるので、ビーコン１０２は、ビーコン１０２が一定の時間で送信する無線フレームの数を決定してよい。それゆえ、ビーコン１０２は、プライベート鍵が修正される必要があるかどうかを判定してよい。いくつかの実施態様において、無線フレームの数が、１日あたりに伝送されることが認められた無線フレームの総数と等しいという判定に応答して、ビーコン１０２はプライベート鍵を修正してよい。ビーコン１０２は、暗号化方法を修正してよく、無線フレームの数を再集計してよい。無線フレームの数が、翌日のゼロクロックで１日あたりに伝送されることが認められた無線フレームの総数に到達できるように、初日に、初期数が、現在時間及び無線フレームの伝送周波数に基づいて決定されてよい。

【００３８】

初期設定の後、ビーコン１０２は自動モードに入ってよい。いくつかの実施態様において、ビーコン１０２は、所定の周波数で無線フレームを伝送してよい。無線フレーム伝送の数が、１日あたりに伝送されることが認められた無線フレーム伝送の総数と等しいという判定に応答して、ビーコン１０２は、現在のプライベート鍵に次いで新たなプライベート鍵を採用してよい。ビーコンは、新たな暗号化されたメッセージを取得するように、新たなプライベート鍵を使用してＵＵＩＤ及び他のパラメータを暗号化してよい。ビーコン１０２は、新たな配信日に入ってよい。モバイルデバイス１０６がビーコン１０２から無線フレームを受信する場合、モバイルデバイス１０６は、復号化サーバ（例えば、サーバ１０８）の情報ならびにＵＵＩＤ及び他のパラメータを含む暗号化されたメッセージを検

索してよい。モバイルデバイス１０６は、その後、暗号化されたメッセージをサーバ１０８へ伝送してよい。

【００３９】

サーバ１０８が暗号化されたメッセージを受信した後、暗号化されたメッセージを復号化して、ＵＵＩＤ及びビーコン１０２と関連した他のパラメータを取得するように、サーバ１０８は、現在日時及び所定のアルゴリズムに基づいて、対応するプライベート鍵を決定及び／または位置ずけてよい。サーバ１０８は、ＵＵＩＤに対応するタスクを決定してよく、タスクの情報をモバイルデバイス１０６に伝送してよい。

【００４０】

本開示の実施態様は、ビーコン１０２のＩＤを暗号化してよく、経時的に修正されてもよい暗号化されたメッセージを発生させてよい。第三者が暗号化されたメッセージを取得できたとしても、暗号化されたメッセージが経時的に変化するので、第三者がビーコン１０２と関連した情報を取得することは困難であろう。さらに、第三者は、モバイルデバイス１０６から機密情報を盗用することはできないであろう。同様に、モバイルデバイス１０６上の許可されていないアプリケーションが、暗号化されたメッセージを単に取得するだけで、暗号化されたメッセージにおいて暗号化された情報が、許可されていないアプリケーションによって取得されることはない。

【００４１】

図４及び図５は、ビーコンメッセージの伝送を可能にする説明的なコンピューティングアーキテクチャの概略図である。図４は、コンピューティングデバイス４００（例えば、ビーコン１０２）の図である。コンピューティングデバイス４００は、多数の位置ログイン制御に対応したユーザデバイスまたはサーバであってよい。１つの例示的な構成において、コンピューティングデバイス４００は、１つまたは複数のプロセッサ４０２、入力／出力インターフェース４０４、ネットワークインターフェース４０６、及び、メモリ４０８を含む。

【００４２】

メモリ４０８は、ランダムアクセスメモリ（ＲＡＭ）などの揮発性メモリ、及び／または、リードオンリメモリ（ＲＯＭ）若しくはフラッシュＲＡＭなどの不揮発性メモリの形をとるコンピュータ可読媒体を含んでよい。メモリ４０８は、コンピュータ可読媒体の実施例である。

【００４３】

コンピュータ可読媒体は、コンピュータ可読命令、データ構造、プログラムモジュール、または他のデータなどの、情報の記憶のための任意の方法または技術で実施される、揮発性及び不揮発性、取り外し可能及び取外しできない媒体を含む。コンピュータ記憶媒体の実施例は、これに限定されるのではないが、相変化メモリ（ＰＲＡＭ）、スタティックランダムアクセスメモリ（ＳＲＡＭ）、ダイナミックランダムアクセスメモリ（ＤＲＡＭ）、他の種類のランダムアクセスメモリ（ＲＡＭ）、リードオンリメモリ（ＲＯＭ）、電気的消去可能プログラマブルリードオンリメモリ（ＥＥＰＲＯＭ）、フラッシュメモリまたは他のメモリ技術、コンパクトディスクリードオンリメモリ（ＣＤ‐ＲＯＭ）、デジタル多用途ディスク（ＤＶＤ）または他の光学記憶装置、磁気カセット、磁気テープ、磁気ディスク記憶装置または他の磁気記憶デバイス、または、コンピューティングデバイスによるアクセス用の情報を記憶するのに使用されてよい任意の他の非伝達媒体を含む。本明細書において規定されるように、コンピュータ可読媒体は、変調されたデータ信号及び搬送波などの一時的な媒体を含まない。

【００４４】

メモリ４０８にさらに詳細に目を向けると、メモリ４０８は、暗号化決定モジュール４１０、暗号化モジュール４１２、及び、伝送モジュール４１４を含んでよい。暗号化決定モジュール４１０は、所定のアルゴリズムに基づいて、現在時間をパラメータとして使用して、暗号化方法を決定するように構成される。暗号化モジュール４１２は、ビーコンの暗号化されたＩＤを取得するように、決定された暗号化を使用してビーコンのＩＤを暗号

化するように構成される。伝送モジュール４１４は、暗号化されたＩＤ及び復号化コンピューティングデバイス（例えば、サーバ１０８）と関連した情報を含む無線フレームを発生させ、且つ、当該無線フレームをモバイルデバイス１０６に伝送するように構成される。

【００４５】

いくつかの実施態様において、暗号化決定モジュール４１０は、暗号化プリセッティングモジュール、暗号化マッピングモジュール、及び暗号化選択モジュールを含んでよい。暗号化プリセッティングモジュールは、Ｎ種類の暗号化方法をプリセットするように構成される。Ｎは、１よりも大きい自然数である。暗号化マッピングモジュールは、所定のマッピングアルゴリズムを使用して現在時間をＭにマッピングするように構成される。Ｍは、１よりも大きいか、または１と等しく、且つ、Ｎよりも小さい自然数である。暗号化選択モジュールは、Ｍに対応する暗号化方法を、決定された暗号化方法として指定するように構成される。

【００４６】

いくつかの実施態様において、暗号化方法は公開鍵であり、現在時間は現在日時である。いくつかの例において、暗号化決定モジュール４１０は、合計集計モジュール、集計モジュール、及び、暗号化修正モジュールを含んでよい。合計集計モジュールは、無線伝送周波数に基づいて１日の無線フレームの伝送回数の総数を決定するように構成される。集計モジュールは、現在時間及び無線伝送周波数に基づいて、無線フレームの伝送回数の数を集計するように構成される。暗号化修正モジュールは、伝送回数の数が伝送回数の総数と等しいという判定に応答して、所定のアルゴリズムに基づいて暗号化方法を修正するように、及び、伝送回数の数を再集計するように構成される。いくつかの実施態様において、暗号化方法は、プライベート鍵及び／または暗号化アルゴリズムを含んでよい。

【００４７】

図５は、コンピューティングデバイス５００（例えば、サーバ１０８）の図である。コンピューティングデバイス５００は、多数の位置ログイン制御に対応したユーザデバイスまたはサーバであってよい。１つの例示的な構成において、コンピューティングデバイス５００は、１つまたは複数のプロセッサ５０２、入力／出力インターフェース５０４、ネットワークインターフェース５０６、及び、メモリ５０８を含む。

【００４８】

メモリ５０８は、ランダムアクセスメモリ（ＲＡＭ）などの揮発性メモリ、及び／または、リードオンリメモリ（ＲＯＭ）若しくはフラッシュＲＡＭなどの不揮発性メモリの形をとるコンピュータ可読媒体を含んでよい。メモリ５０８はコンピュータ可読媒体の実施例である。

【００４９】

コンピュータ可読媒体は、コンピュータ可読命令、データ構造、プログラムモジュール、または他のデータなどの、情報の記憶のための任意の方法または技術で実施される、揮発性及び不揮発性、取り外し可能及び取外しできない媒体を含む。コンピュータ記憶媒体の実施例は、これに限定されるのではないが、相変化メモリ（ＰＲＡＭ）、スタティックランダムアクセスメモリ（ＳＲＡＭ）、ダイナミックランダムアクセスメモリ（ＤＲＡＭ）、他の種類のランダムアクセスメモリ（ＲＡＭ）、リードオンリメモリ（ＲＯＭ）、電気的消去可能プログラマブルリードオンリメモリ（ＥＥＰＲＯＭ）、フラッシュメモリまたは他のメモリ技術、コンパクトディスクリードオンリメモリ（ＣＤ‐ＲＯＭ）、デジタル多用途ディスク（ＤＶＤ）または他の光学記憶装置、磁気カセット、磁気テープ、磁気ディスク記憶装置または他の磁気記憶デバイス、または、コンピューティングデバイスによるアクセス用の情報を記憶するのに使用されてよい任意の他の非伝達媒体を含む。本明細書において規定されるように、コンピュータ可読媒体は、変調されたデータ信号及び搬送波などの一時的な媒体を含まない。

【００５０】

メモリ５０８にさらに詳細に目を向けると、メモリ５０８は、復号化決定モジュール５

１０、暗号化メッセージ受信モジュール５１２、復号化モジュール５１４、及びタスク提供モジュール５１６を含んでよい。復号化決定モジュール５１０は、所定のアルゴリズムに基づいて、現在時間をパラメータとして使用して復号化方法を決定するように構成される。暗号化メッセージ受信モジュール５１２は、ビーコンの暗号化されたＩＤをモバイルデバイスから受信するように構成される。復号化モジュール５１４は、ビーコンのＩＤを取得するように、決定された復号化方法を使用して、暗号化されたＩＤを復号化するように構成される。タスク提供モジュール５１６は、当該ＩＤに対応するタスクをモバイルデバイスに提供するように構成される。

【００５１】

いくつかの実施態様において、サーバ１０８は、Ｎ種類の復号化方法をプリセットしてよい。Ｎは、１よりも大きい自然数である。サーバ１０８は、所定のマッピングアルゴリズムを使用して現在時間をＭにマッピングしてよく、Ｍに対応する復号化方法を、決定された復号化方法として指定してよい。Ｍは、１よりも大きいか、または１と等しく、且つ、Ｎよりも小さい自然数である。

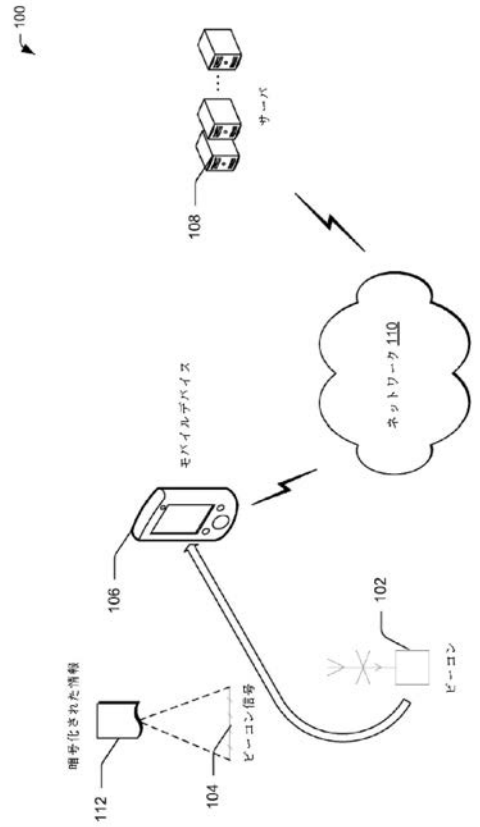
【００５２】

従来の技法では、ビーコンは暗号化なしで無線フレームを伝送する。本開示の実施態様は、ビーコン１０２のＩＤを暗号化でき、経時的に暗号化方法を修正できる。従って、ビーコン１０２により許可されていないアプリケーションは、ビーコン１０２の安定したＩＤを取得できず、すなわち、許可されていないサービスが、ビーコン１０２を介して提供されることがない。これにより、顧客の機密情報の開示だけでなく、ビーコンメッセージの盗用も防止される。

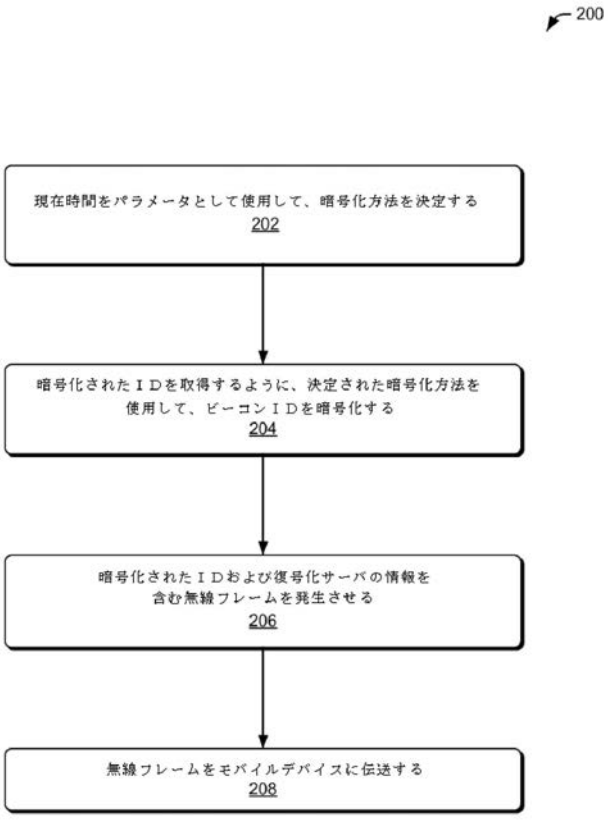
【００５３】

実施態様は、本開示を説明するためだけのものであり、本開示の範囲を限定することを意図しない。一定の修正及び改良が、本開示の原則から逸脱せずになされてよく、また、本開示の保護の下にあると解釈されるべきであることを当業者は理解すべきである。

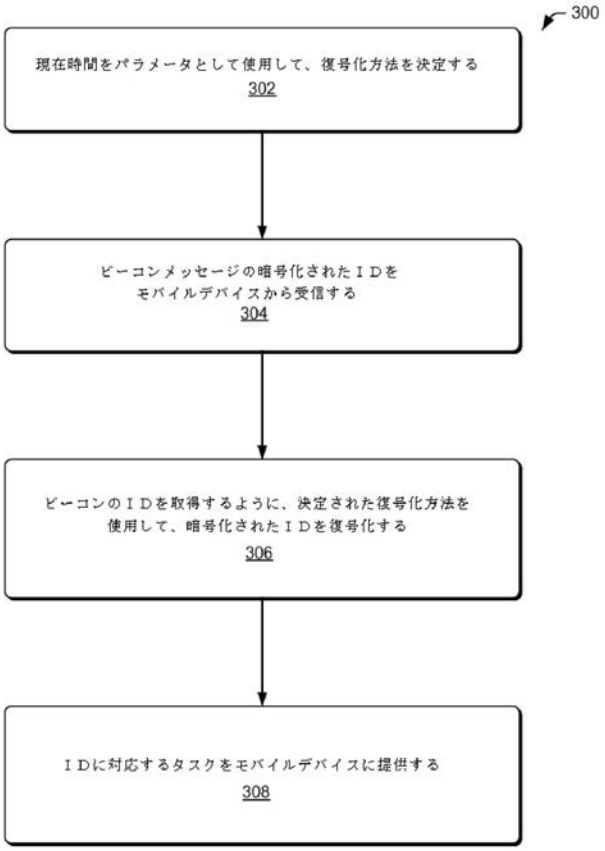
【図１】



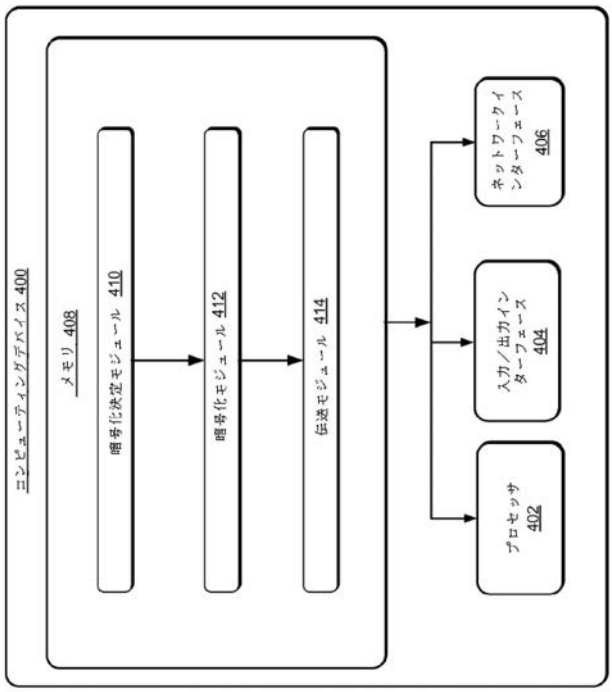
【図２】



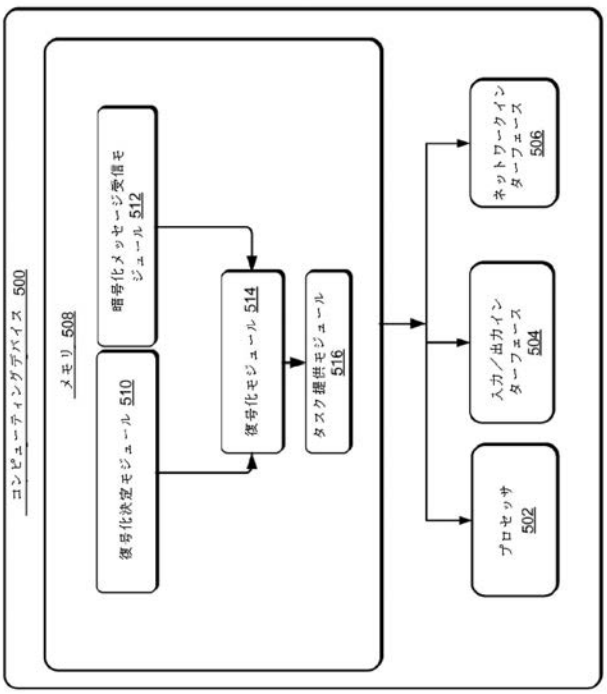
【図３】


300
現在時間をパラメータとして使用して、復号化方法を決定する
302
ビーコンメッセージの暗号化されたＩＤを
モバイルデバイスから受信する
304
ビーコンのＩＤを取得するように、決定された復号化方法を
使用して、暗号化されたＩＤを復号化する
306
ＩＤに対応するタスクをモバイルデバイスに提供する
308

【図４】


コンピューティングデバイス 400
メモリ 408
暗号化決定モジュール 410
暗号化モジュール 412
伝送モジュール 414
ネットワークインターフェース 406
入力／出力インターフェース 404
プロセッサ 402

【図５】


コンピューティングデバイス 500
メモリ 508
暗号化メッセージ受信モジュール 512
復号化決定モジュール 510
復号化モジュール 514
タスク提供モジュール 516
ネットワークインターフェース 506
入力／出力インターフェース 504
プロセッサ 502

フロントページの続き

(72)発明者　ジエン　チン
中華人民共和国　３１１１２１　ハンチョウ　ユー　ハン　ディストリクト　ウェスト　ウェン　イー　ロード　ナンバー　９６９　ビルディング　３　５／エフ　アリババ　グループ　リーガル　デパートメント内

Ｆターム(参考) 5K067 AA30　AA32　DD11　EE02　EE10　EE16　HH36