(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2017-509988
(P2017-509988A)
(43)公表日　平成29年4月6日(2017.4.6)

(51)Int.Cl.		F I			テーマコード（参考）
G08B 25/04	(2006.01)	G08B	25/04	F	3E138
G08B 25/10	(2006.01)	G08B	25/04	G	5C087
G08B 27/00	(2006.01)	G08B	25/10	A	5K201
H04M 11/00	(2006.01)	G08B	27/00	B	
G07C 9/00	(2006.01)	H04M	11/00	301	

審査請求 未請求　予備審査請求 未請求　（全 17 頁）　最終頁に続く

(21)出願番号　特願2016-554636 (P2016-554636)
(86)(22)出願日　平成27年2月24日 (2015.2.24)
(85)翻訳文提出日　平成28年10月27日 (2016.10.27)
(86)国際出願番号　PCT/US2015/017221
(87)国際公開番号　WO2015/130641
(87)国際公開日　平成27年9月3日 (2015.9.3)
(31)優先権主張番号　61/946,054
(32)優先日　平成26年2月28日 (2014.2.28)
(33)優先権主張国　米国 (US)
(31)優先権主張番号　61/973,962
(32)優先日　平成26年4月2日 (2014.4.2)
(33)優先権主張国　米国 (US)
(31)優先権主張番号　14/463,733
(32)優先日　平成26年8月20日 (2014.8.20)
(33)優先権主張国　米国 (US)

(71)出願人　513206533
タイコ・ファイヤー・アンド・セキュリティ・ゲーエムベーハー
Ｔｙｃｏ　Ｆｉｒｅ　＆　Ｓｅｃｕｒｉｔｙ　ＧｍｂＨ
スイス　８２１２　ノイハウゼン・アム・ラインファル、ヴィクトーア・フォン・ブルンス通り　２１
Ｖｉｃｔｏｒ　ｖｏｎ　Ｂｒｕｎｓ－Ｓｔｒａｓｓｅ　２１，　８２１２　Ｎｅｕｈａｕｓｅｎ　ａｍ　Ｒｈｅｉｎｆａｌｌ，　ＳＷＩＴＺＥＲＬＡＮＤ
(74)代理人　100071010
弁理士　山崎　行造

最終頁に続く

(54)【発明の名称】無線センサ・ネットワークにおけるコンテクスト特定管理

(57)【要約】
物理的侵入検出／警報を管理するためのネットワーク化されたシステムは、サーバ・デバイスの上段を含んでおり、プロセッサ・デバイスと、このプロセッサ・デバイスと通信するメモリと、上段サーバと通信するゲートウェイ・デバイスの中段と、完全機能性ノード及び制限付きノードからなるデバイスの下方レベル段とを備える。ネットワーク化は、認証情報若しくはバッジから感覚的入力を受信するように構成されたデバイスを有すると共に、受信した認証データに関連した個々人の仮想グループを判定し、及び規則をグルーピング情報へ適用して、仮想グループ内の個々人を追跡及び検出する。
【選択図】図２

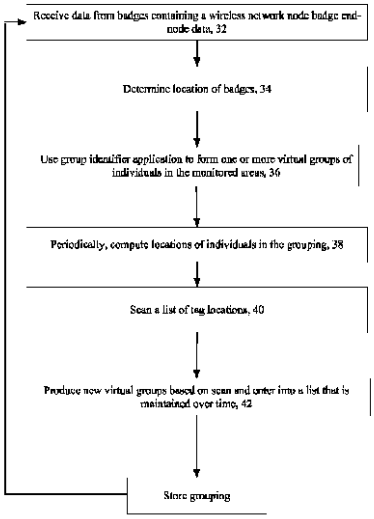

FIG. 2

【特許請求の範囲】
【請求項１】
物理的侵入検出／警報監視ネットワーク化されたシステムであって、
一つ以上のコンピュータ・デバイスであり、プロセッサ・デバイスと、このプロセッサ・デバイスと通信する及びメモリとを含むと共に、前記一つ以上のコンピュータ・デバイスは、
監視施設内の認証情報又はバッジからの検知入力を受信し、
期間に亘って個々人の相互の近接に関する受信入力から判定することにより、前記受信された認証情報に関連した個々人の仮想グループを判定し、
各々の仮想グループについてのタグ位置のリストを仮想グループ構成員が変化するにつれて変化させることにより、仮想グルーピングの設定可能な持続のオーバー・タイム・フレームを変更し、及び、
規則セットをグルーピング情報に適用し、仮想グループ内の個々人を追跡して検出するように構成されているネットワーク化されたシステム。
【請求項２】
請求項１のネットワーク化されたシステムにおいて、個々人の位置が、複数の認証情報読み取りデバイス及び／又はTX出力レベル掃引からの認証情報データの三角測量により測定されるネットワーク化されたシステム。
【請求項３】
請求項１のネットワーク化されたシステムにおいて、メッセージは、監視されている施設内の氏名バッジ・ノードと他のセンサ・ネットワーク・ノードとの間で交わされるネットワーク化されたシステム。
【請求項４】
請求項１のネットワーク化されたシステムにおいて、或る期間の後に、ネットワーク・ゲートウェイにおいて実行されるアプリケーションが個々人の各々の位置を計算すると共に、グループ識別子アプリケーションがタグ位置のリストを走査するネットワーク化されたシステム。
【請求項５】
請求項１のネットワーク化されたシステムにおいて、前記グルーピングはそれらが形成、導解、及びさもなければ新たな情報としてのリアルタイムにおける変化が個々人の現在の位置に関して利用可能となるに際し動的であるネットワーク化されたシステム。
【請求項６】
請求項１のネットワーク化されたシステムにおいて、前記グルーピングは、所定の個人が過去の経験から導かれた確実性／不確実性の程度によりグループへ割り当て得るという点で「ファジー」であるネットワーク化されたシステム。
【請求項７】
請求項１のネットワーク化されたシステムにおいて、前記一つ以上のコンピュータ・デバイスが更に、
仮想グループ構成員についての試験を規定する規則を適用するように構成されているネットワーク化されたシステム。
【請求項８】
請求項１のネットワーク化されたシステムにおいて、前記一つ以上のコンピュータ・デバイスが前記ネットワーク化されたシステムにおける単独のデバイスであるネットワーク化されたシステム。
【請求項９】
請求項１のネットワーク化されたシステムにおいて、前記一つ以上のコンピュータ・デバイスは、エンドノードのセット及びネットワーク・ノードとホストとの組み合わせの複数の分散されたデバイスであるネットワーク化されたシステム。
【請求項１０】
請求項１のネットワーク化されたシステムにおいて、前記コンテクスト特定規則又は規

則のセットは前記デバイスへロードされたアプリケーション・コード・モジュールであり、これはリアルタイム・コード再配置及び実行を使用して時間と共に変化するネットワーク化されたシステム。

【請求項１１】

監視領域内の物理的侵入の検出の方法であって、

一つ以上のコンピュータ・デバイスによりでの監視施設内の認証情報若しくはバッジから検知的入力を受信し、

前記一つ以上のコンピュータ・デバイスにより、期間に亘る個々人の近接に関する受信した入力から判定することによって、前記受信した認証情報データに関連した個々人の仮想グループを判定し、

前記一つ以上のコンピュータ・デバイスにより、前記個々人の判定された仮想グループをタグ位置のリストへ記憶させ、

前記一つ以上のコンピュータ・デバイスにより、仮想グループ構成員が変化するにつれて各々の仮想グループの前記タグ位置のリストを変化させることによって、前記仮想グループの変更可能な持続の時間フレームに亘って修正し、

前記一つ以上のコンピュータ・デバイスにより、規則セットを前記グルーピング情報へ適用して、前記仮想グループ内の個々人を追跡及び検出することを含む方法。

【請求項１２】

請求項１１の方法において、

前記一つ以上のコンピュータ・デバイスにより、前記規則の変更を受信し、

前記ネットワークにおけるセンサを前記規則になされた前記変更に従って更新することを更に含む方法。

【発明の詳細な説明】

【発明の概要】

【０００１】

優先権の主張

本出願はアメリカ合衆国法典第３５巻特許法第１１９(e)の下に、米国仮特許出願第６１／９７３,９６２号として、２０１４年４月２日に出願した発明の名称”Wireless Sensor Network”、及び米国仮特許出願第６１／９４６,０５４号として、２０１４年２月２８日に出願した発明の名称”Wireless Sensor Network”、並びに米国実用特許出願第１４／４６３,７３３号として、２０１４年８月２０日に出願した表題”Context Specific Management in Wireless Sensor Network”に基づく優先権を主張しており、それらの内容の全てが参照により本明細書に組み込まれている。

背景

【０００２】

この説明は、特定の侵入システムで保安システムの作動に関する。

【０００３】

企業や住宅所有者は、その者らの敷地における警報状況を検出するため及びその状況を監視ステーション若しくはその保安システムの認可ユーザへ信号を送るための保安システムを持つことが一般的である。保安システムはしばしば侵入検出パネルを含んでおり、これは様々なセンサへ電気的に又は無線で接続されている。これらのセンサ形式は一般的には動作検出器、カメラ、及び近接センサ（ドア又は窓が開放されたか否かを判定するのに用いられる）を含む。一般的に、このようなシステムは、監視される特定の状況が変化したか又は安全ではなくなったことを示す非常に単純な信号（電気的に開閉）をそれらのセンサの一つ以上から受信する。

【０００４】

政府機関、会社、学術機関等は、認証情報を従業員、契約者、学生等に交付して、建物及び施設、屋内及び屋外への出入りを管理する。故意に又は意図せずにの何れかで保安システムを回避して出入りを得ようとする個々人は、特定して突き止めることが困難である。アプリケーションは、建物内の個々人（人々）の位置及び傾向又は様々な目的のための

他の形式の設定情報に関連したデータ及び情報を使用することができる。
概要
【０００５】
アプリケーションの例における無線センサ・ネットワークは、領域アクセス制御（ドア・ロックなど）、侵入検出（ドア・ロック、窓ロック、近接検知）、防火性（煙探知器）その他を含む。無線ネットワークは、建物内の又は現地における人々の位置を様々な三角測量及び測距方法を用いて追跡することにも用いられる。開示されたものは高水準情報の干渉が、無線センサ・ネットワークにおけるノードからの生データ・センサ出力及び報告から有益な情報を得るための技術を提供することにより、データが監視領域内の個々人の位置に関するので、低レベルのセンサ・データから判定することができる技術である。
【０００６】
一つの態様によれば、物理的侵入検出／警報監視のためのシステムは、監視された施設内で認証情報又はバッジから検知入力を受信するように構成された一つ以上のコンピュータ・デバイスを含み、期間に亘って互いに対する個々人の近接に関する受信された入力からの判定により受信された認証情報データに関連した個々人の仮想グループを判定し、この判定された個々人の仮想グループをタグ位置のリストへ記憶し、仮想グループ構成員が変化するにつれて各々の仮想グループのためのタグ位置のリストを変化させることにより、仮想グループの設定変更持続時間のフレームを時間と共に変更し、及び規則セットをグルーピング情報へ適用して仮想グループ内の個々人を追跡及び検出する。
【０００７】
更なる態様によれば、監視領域内の物理的侵入の検出の方法は、一つ以上のコンピュータ・デバイスにより、監視施設内の認証情報若しくはバッジからの感知入力を受信し、一つ以上のコンピュータ・デバイスにより、その受信された認証情報に関連した個々人の仮想情報を、個々人の近接に関する受信された入力から判定することにより判定し、一つ以上のコンピュータ・デバイスにより、個々人の判定された仮想グループをタグ位置のリストへ記憶させ、一つ以上のコンピュータ・デバイスにより、仮想グループ構成員が変化するにつれて各々の仮想グループについてのタグ位置のリストを変化させることにより仮想グループグルーピングの設定可能持続時間のフレームを時間と共に変更し、及び一つ以上のコンピュータ・デバイスにより、規則セットをグループグルーピング情報へ適用し、仮想グループ内の個々人を追跡及び検出する。
【０００８】
以下の利点の一つ以上は、上述の態様の一つ以上により提供し得る。
【０００９】
このアプローチは、個々人を設定可能持続時間の比較的に短時間のフレームに亘って仮想グループにグルーピングする。そのグルーピング情報の使用により、この技術はグループにおける個々人のステータスを機能的に判定する。そのグルーピングは、そのグルーピング形式において動的であり、疑いなく、また、さもなければ、新たな情報が個々人の現在位置に関して利用可能になるにつれてリアルタイムで変化する。このグループは、所定の個人が過去の経験から導かれた確実性／不確実性の特定の程度によりグループに割り当てられるかもしれないという点で、「ファジー」である。個々人のグループの管理は、低レベル・アプリケーションに値を与える。このアプローチは、単独のデバイス又は多くのデバイスに亘って分布されている（即ち、エンドノードのセットのアプリケーション層ソフトウェア又はネットワーク・ノード若しくはホストの他の組み合わせ）かの何れかに常駐する複数の規則若しくは規則のセット（複合規則）を用い、仮想グループ構成員のための検査を含むもののみを規定する。これらの規則は、様々なデバイスへロードされて時間と共に変化するアプリケーション・コード・モジュールを用いて実行することができ、リアルタイム再配置及び実行（動的プログラミング）を用いる。
【００１０】
本発明の一つ以上の実施形態の詳細は、添付の図面及び下記の説明に記載される。本発明の他の特徴、目的、及び利点は、説明及び図面から、並びに特許請求の範囲から明らか

である。
【図面の簡単な説明】
【００１１】
【図１】図１は例示的なネットワーク化された保安システムの概略図である。
【図２】図２はコンテクスト特定管理処理を表すフローチャートである。
【図３】図３はコンテクスト特定管理処理の特定の使用を表すフローチャートである。
【図４】図４はコンテクスト特定管理処理のためのデータ受信を表すフローチャートである。
【図５】図５はコンテクスト特定管理処理を実行するデバイスのブロック図である。
【図６】図６は例示的ネットワーク化された保安システムの構成要素のブロック図である。
【発明を実施するための形態】
【００１２】
ここに記載するのは、保安／侵入及び警報システムを含むが、これに限定されるものではなく、様々な状況で用いられネットワーク機能の例である。例示的な保安システムは、侵入検出パネルを含むことがあり、これは様々なセンサへ電気的に又は無線で接続されている。これらのセンサ形式は、動作検出器、カメラ、及び近接センサ（例えば、ドア又は窓が開放されたか否かを判定するために用いられる）を含み得る。一般的に、そのようなシステムは、監視される特定の状況が変化したか若しくは安全ではなくなったことを示す比較的に単純な信号（電気的に開放又は閉止）をこれらのセンサの一つ以上から受信する。
【００１３】
例えば、例示的侵入システムは、建物内の入口ドアを監視するように設定することができる。ドアが閉止しているとき、近接センサは磁気接触を検知して、電気的閉止回路を生成する。ドアが開放されたとき、近接センサは回路を開放し、警報状況が発生した（例えば、入口ドアが開放された）ことを示す信号をパネルへ送る。
【００１４】
データ収集システムは、幾つかのアプリケーション、例えば家庭用安全監視においてより一般的になっている。データ収集システムは無線センサ・ネットワーク及び無線デバイスを採用し、かつ、遠隔サーバに基づく監視及び報告作成を含み得る。以下に詳細に説明するように、無線センサ・ネットワークは、一般的に、コンピュータ・デバイス同士の間の有線及び無線リンクの組み合わせを用いており、無線リンクは通常は最低レベルでの（例えば、エンド・ノード・デバイスからハブ／ゲートウェイへの）接続のために用いられている。例示的なネットワークでは、ネットワークのエッジ（無線接続された）段は、特定の機能でリソース制約されたデバイスからなる。これらデバイスは、小から中程度の処理能力及びメモリを有することがあり、バッテリで駆動されることがあるので、多くの時間をスリープ・モードに費やすことにより、それらのエネルギを節約する必要がある。一般的なモデルは、エンドノードがハブ及びスポーク形式アーキテクチュアでペアレント・ノードと直接に通信する単一の無線ネットワークを各エッジ・デバイスが形成するようなものとなる。ペアレント・ノードは、例えば、アクセス・ポイント又は他のサブコーディネータに接続されるゲートウェイ上のアクセス・ポイント又はサブコーディネータとすることができる。
【００１５】
ここで図１を参照すると、無線センサ・ネットワーク（Wireless Sensor Network：WSN）のための例示的な（グローバル）分散ネットワーク１０トポロジーが示されている。図１において、分散ネットワーク１０は一組の段又は階層的なレベル１２ａ－１２ｃへ論理的に分割されている。ネットワークの上段又は階層的なレベル１２ａは、配置サーバ及び／又は仮想サーバ１４であり、インターネット・プロトコルのような充分に確立されたネットワーキング技術を用いて一緒にネットワーク化された「クラウド・コンピューティング」パラダイムを実行させているか、又はインターネットを全く使わないか又は一部を用

いるプライベート・ネットワークとすることができる。それらのサーバ１４５で作動するアプリケーションは、様々なプロトコル、例えばウェブ・インターネット・ネットワークXML/SOAP、RESTfulウェブ・サービスと、他のアプリケーション層技術、例えばHTTP及びATOMを用いて通信する。

【００１６】

分散ネットワーク１０には第２の論理的分割段又は階層的レベル１２ｂを含み、ここでは中段を称し、これは個々の建築物又は構造物の内側の都合の良い位置に位置したゲートウェイ１６に関係している。これらゲートウェイ１６は上段におけるサーバ１４と通信し、これは、これらのサーバが独立型専用サーバ及び／又はウェブ・プログラミング技法を用いるクラウド・アプリケーションを実行しているクラウド・ベースのサーバであるか否かに関わらない。中央段ゲートウェイ１６はローカル・アリア・ネットワーク１７ａ（例えば、イーサネット（登録商標）又は８０２.１１）及びセルラー・ネットワーク・インターフェース１７ｂと共に示されている。

【００１７】

分散型ネットワーク・トポロジーは複数のデバイスの下段（エッジ層）１２ｃセットも含み、これは完全に機能的なセンサ・ノード１８（例えば、センサ・ノードであり、これは無線デバイスを含み、例えば受信機又は少なくとも送信機であり、これは図１においては、「Ｆ」で示されている）及び制限された無線センサ・ノード又はセンサ・エンドノード２０（図１には「Ｃ」で示されている）を含む。幾かの実施形態において、有線センサ（図示せず）は、分散ネットワーク１０の態様に含めることができる。

【００１８】

ここで用いられる制限付きコンピュータ２０は、実質的に少ない持続性及び揮発性メモリを有するデバイス、他のコンピュータ・デバイス、検出システムにおけるセンサである。制限付きデバイスの現在の例は、およそ１メガバイト未満のフラッシュ／持続的メモリ、及び１０－２０キロバイト未満のＲＡＭ／揮発性メモリを有するものである。これらの制限付きデバイス２０は、このように構成されており、一般にコスト／物理的構成の考慮事項に起因している。

【００１９】

一般的にネットワークにおいては、ネットワークのエッジ（無線接続されている）段は、特定の機能を有する非常にリソース制限付きデバイスからなる。これらのデバイスには小から中程度の処理力及びメモリを有し、しばしばバッテリで駆動されることがあり、従って、多くの時間をスリープ・モードに費やすことによって、それらがエネルギ節約をする必要がある。

【００２０】

一般的なモデルであるものは、一般的に、エンド・ノードがハブ及びスポーク形式アーキテクチュアでペアレント・ノードと直接に通信する単一の無線ネットワークを各エッジ・デバイスが単独の無線ネットワークを形成するようなものとなる。ペアレント・ノードは、例えば、ゲートウェイ上のアクセス・ポイント又はサブコーディネータとすることができ、そのゲートウェイは同様にアクセス・ポイント又は他のサブコーディネータに接続されている。

【００２１】

各々のゲートウェイは、アクセス・ポイント（完全な機能的ノード又は「F」ノード）を備えており、これはそのアクセス・ポイントに取り付けられており、無線ネットワークにおける他のノードに対する無線接続ポイントを与える。図１に示されたリンク（線で描かれており、番号付けされていない）は、複数のデバイスの間の直接（単独のホップ・ネットワーク層）接続を示す。形式ネットワーキング層（図１に示される３段の各々において機能する）は、一連のこれら直接リンクと一緒にルーティング・デバイスを用い、メッセージ（断片又は非断片）を一つのデバイスから他のデバイスへネットワーク上で送信する。

【００２２】

WSN１０は、アプリケーション層への状態マシン・アプローチを実行して、下段デバイス１８及び２０において実行される。このようなアプローチの特定の実行の例を以下に説明する。状態マシンにおける状態は、調整中に実行される機能のセットからなり、これらの機能は、マネージャー・プログラムによって特定の下段デバイスの状態マシンにおいて状態を変えることにより、個別に削除されるか、又は置き換えられるか、加えることができる。

【００２３】

WSN状態機能ベースのアプリケーション層は、エッジ・デバイス操作システム（図示しないが、例えば上述の仮出願に開示されている）を用い、これはデバイスを再起動させることなく（所謂「動的プログラミング」）、個々の機能のローディング及び実行のために（デバイスの起動の後に）可能とさせる。他の実施例において、エッジ・デバイスは、他のオペレーティングシステムを用い、このようなシステムは、好ましくはエッジ・デバイスの再起動をすることなく、個々の機能のローディング及び実行させることを可能にする。

【００２４】

ここで図２を参照すると、コンテクスト特定管理は、設定可能な持続の比較的に短い時間フレームに亘って個々人の仮想グループへのグルーピングと、個々人を、例えば、許可されていない領域等における資格を有さない個々人又は資格を有する個々人を追跡及び検出するグルーピング情報の使用に関する。コンテクスト特定管理は、上術のようにセンサから得られた情報を用いることができる。グルーピングの実行は固定することができ、予め選択されているか、ユーザが選択可能である。

【００２５】

コンテクスト特定管理処理は、図１において述べたシステム又は均等なシステムの何れかで実行する実行することができる。

【００２６】

コンテクスト特定管理は以下のように説明することができる。３人の個人は建物の廊下を歩いて下がっており、個人のそれぞれは氏名タグ又はバッジを装着しており、これは無線ネットワーク・ノードを包含しており、これはタグ読み取りセンサにより読み込まれたとき、バッジ又はタグが割り当てられた個人を特定するデータを有するメッセージを生成する。この読み込みデータは、バッジ（WSNエンドーノード）を装着する各個人が廊下を移動して下降して建物を通るにつれて、一つ以上のタグ読み取りセンサからサーバ又はゲートウェイにより受信される３２。バッジがネットワーク（図１）内のセンサ・ノードにより読み取られるにつれて、正確なバッジの位置が様々な技術、例えば三角測量、TXパワー・レベル掃引、及び／又は建築物廊下におけるがバッジの位置を或る規定された精度で正確に指摘する他の方法の組合せによって判定される。（精度の程度は、個別のセンサ・ノードの数、間隔、正確さ、並びにこのようなノードの範囲と受信可能範囲に原理的に関係しており、従って、実施が明白である。）

【００２７】

メッセージはモバイル・ノード（名前バッジ・ノード）により生成されて、上述の無線ネットワークにおいて他のセンサー・ネットワーク・ノードへ渡される。図１のネットワークの実施形態においては、ネットワークにおけるノード（例えば、固定された下位コーディネーター・ノード、位置参照点としての働きをしている固定された位置における他のエンドノードその他）は、より高い段、例えば、第１及び第２の段において、システムの継続的な関係を伴うことなく、これらのメッセージを処理する。しかしながら、時間内の点において、生メッセージ及び／又はノードからのメッセージの処理から提供される結果は、ネットワーク内の一つ以上のネットワーク・ゲートウェイへ送られる。例えば、サーバにおいては、サーバはグループ識別子アプリケーションを実行する。他のネットワークによれば、異なる構成が可能である。

【００２８】

従って、時間周期（おそらく３０乃至６０秒）の後、ノードからの入力は、サーバによ

り受信されて、かつ、このサーバにおいて動作するグループ識別子アプリケーション３６は、三人の個人の各々の位置を何度も計算及び再計算する３８。このグループ識別子アプリケーションは、複数のノードの中及びノードとゲートウェイとの間を通過したメッセージから構築されるタグ位置のリスト「タグ位置リスト」を連続的に走査し４０、３つのバッジ・ノードに関連した相関関係を判定し、即ち、３人の個人は全て、一連の異なる位置及び／又は時間について全体的システム（即ち、同一の一般的領域において）の位置解像度の限界の範囲内若しくは近似的に範囲内に存しており、及びその現在の閾値及び論理によれば、グループ識別子アプリケーションは３人の個人から成る仮想グループ４２を生成する。

【００２９】

この仮想分離は、コンピュータ記憶装置、例えばデータベース等に記憶された記録又は他の構造（以下に表として示される）であり、これはグループに関連したタグと、各々のタグが読まれた「タグ位置」及びタグ「時間」読み取りの時間を含み、これをグループ識別子アプリケーションが長い時間をかけて維持されるタグ位置リストへ入力する。タグ位置リストは、多くの異なる形態を採ることができる。例えば、タグ位置リストは、以下のようなリストから成ることができる。

【００３０】

【表１】

タグ場所リスト		
タグ	タグ場所	時間
タグ__1		
* * *	* * *	* * *
タグ__n		

仮想グループはタグ情報を調べることによって生成され、そのようなグループは以下の表におけるように追跡することができる。

【００３１】

【表２】

仮想グループ		
仮想グループ Id	タグ	時間
仮想グループ Id__1	タグ__2; タグ__3; タグ__9	
* * *	* * *	* * *
仮想グループ Id__n		

タグは関連した情報を有し、これは、タグの割り当てられたユーザ若しくは所有者、例えば、部局情報その他を含む。

【００３２】

【表３】

タグ＿1		
ユーザ名	部局	****

これらの仮想グループは継続的に更新されて、追加された新たな仮想グループにより変更されて、古い仮想グルーピングは、受信されたデータ及びこのデータに適用された仕様／規則によって削除される。

【００３３】

これらのグルーピングはそれらの形態、解除において動的であり、さもなければ、新たな情報が、関係する様々な個人の現在の位置に関して利用可能となるにつれて、リアルタイムで変化する。このグルーピングはまた、所定の個人が過去の経験から派生した確実性／不確実性の特定の程度によりグループに割り当てられ得るという点で、「ファジー」（応用人工知能からの用語を借用）である。

【００３４】

規則は、仮想グループを決定するために確立することができる。例えば、非常に短い時間（位置が建物内の全ての人々について、例えば１５秒ごとに再計算され、他の個人に近接して観察されるのであれば、１つの位置計算期間の間）について他の個人に近接して観察される１人の個人は、実際のグループ内にある比較的に僅かな可能性がある（即ち、同じ２人の個人が次の位置計算期間に同じ位置にいるという僅かな可能性がある）。２人の個人が二つの連続する計算期間について同じ位置において特定されるならば、２人の個人は第３の計算期間において一緒に観察されるという若干大きな可能性がある（即ち、２期間一緒であることは、１期間一緒であることが２回目の期間に一緒であることが推論されるよりも、３回目に大きな成功を有することが推論される）。この相対的な可能性又はN乃至N＋１相関関係は、グループ識別子アプリ又は他の計算モジュールによる履歴データ及び回帰法を用いて計算することができる。

【００３５】

一つの実施例の例においては、ユーザはアプリケーション構成の間、閾値を供給することができ、例えば、２人の個人が次の位置計算期間に一緒に観察されるという９０％の可能性があるならば、その２人の個人は当然に共通の仮想グループの構成員となる。

【００３６】

コンテクスト特定管理は、単独のデバイス又は分散された多くのデバイス（即ち、一組のエンドノードのアプリケーション層ソフトウェア又はネットワーク・ノードとホストとの他の組合せ）の何れかに駐在する規則又は規則のセット（合成規則）の使用も含み、仮想グループの構成員であることのための検査から成るものであることを単に規定する。

【００３７】

これらの規則は、様々なデバイスにロードされたアプリケーション・コード・モジュールを用いて実施することができ、リアルタイムコード再配置及び実行（動的プログラミング）を用いて、時間と共に変化する。

【００３８】

更に詳しくは、一つの固定された基盤ノードが時刻１において二つのモバイル・ノードを一緒に特定するならば、第２の固定された基盤ノードが時刻２において同一の二つのモバイル・ノードを一緒に特定し、グループ識別子アプリケーションが同じ二つのモバイル・ノードが二つの連続する位置計算期間の間に一緒に観察されたものと認識することができる前に、データは統合されるか又は比較される。これは、固定ノード１へ固定ノード２によりメッセージが送信された後に、固定ノード１においてなすことができるか、又は固定ノード２へ固定ノード１によりメッセージが送信された後に、固定ノード２においてなすことができるか、又は何らかの他のノード（例えば、共通下位コーディネータのような親ノード）へ固定ノード１と固定ノード２との両方によりメッセージが送信された後に、

何らかの他のノードにおいてなすことができる。

【００３９】

仮想グループを規定する処理は、同様になすことができるが、モバイル・ノードが位置における重要な変化をなしたときはいつでも、ブロードキャスト・モードにおけるネットワーク報告における各固定ノードによるより複雑な方式でなすことができる。ブロードキャスト・メッセージの収集は全てのノードのセットにより監視することができ、かつ、各々のノードは、何れのモバイル・タグのノードがメッセージをそのノードへ送信したかにより実行される処理に基づいて、それ自身の仮想グループのセットを維持することができ、そのセットにおける何れのノードが、そのセットにおけるそのノード及び何れのノードが、そのノード・セットによる連続的位置計算期間の特定の回数についてモバイル・タグを監視したかということを知らせる。（これらのリストは必ずしも各々の固定されたノードについて同一ではなく、というのは或る固定ノードは、範囲限定に起因して他の固定ノードに連絡を持つ必要はなく、又はメッセージが通信インターフェースへ届かないためなどである。）他の方式は、時間を通じて個々のモバイル・ノード位置の全ての発表された報告を監視する中央アプリケーションのためのものであり、また、マトリックス計算を用いて、二つ以上のモバイル・ノードの位置の相関関係を判定する。

【００４０】

コンテクスト特定管理のためのアプリケーション論理は、結合表現に基づいて関連性を実行し、これは、或る期間に亘って人１が人２と共に移動し、かつ、或る期間に亘って人２が人３と共に移動するならば（同じ時間である必要はない）、人１は人３に関連していることができる。これは更に、人１が頻繁に人２と共に、かつ、人２が人３と共に観察されるのであれば、人１は人３を知っていると推測することができる（人１が人３と共に直接にという必要性を通じてではない）。

【００４１】

ここで図３を参照すると、或る点において、緊急状況、例えば建物火災及び待避命令（例えば、建築火と避難命令（如何なる状況も存在することができ、これは単に説明的なだけである）に関連した警報事象がある。建物の外側で、消防署長とその部下は、全ての者が建物を出たか否かを判断しようと試みる。

【００４２】

単純な段階においては、消防士により使用されているコンピュータ・タブレット上で実行されるアプリケーションは、タグ位置リストにアクセス５２し、火災の時刻において建物の内部でどのバッジが有効であったか否か（及び可能な限りどのバッジが建物の内部で依然として有効か）を判定する。更に、タブレット上で実行されるアプリケーションは、グループ識別子アプリを調べて、警報の時刻においてどの仮想グループ５６が存在しているかを判定すると共に、個々人を調べて各々の仮想グループの構成員の全てが建物を退去していることが認められるか、又はその後に屋外で見られたか（又はおそらく単に重要なこととして、仮想グループの承認／共同構成員の証言として、構成員らの最後に知られた位置が建物内であるか）否か及び他の仮想グルーピングからのデータを判定する。このように、このデータは建物内の人々の安全な避難に関するそれらの質問５８への入力として用いられる。

【００４３】

図４を参照すると、位置データの全ては単独の物理的デバイスに駐在する必要はない。例として、一つの固定された基盤ノードは或る人々（モバイル・エンドノード）６２についてのデータを有することがあり、他方の固定基盤ノード６４は一回において他のモバイル・ノードについてのデータを有することがあり、又は同一のモバイル・ノードは幾つかの異なる時間にある。グループ識別子アプリケーションは、これら及び他の固定基盤ノードからのメッセージを用いて仮想グループ及び可能性グループにおける情報を共有し、これは一つのグループが指定された信頼性閾値内に存在するか否かを判定するためである。

【００４４】

幾つかの実施例では、カメラにより捕らえられたビデオ情報をタグリスト情報と共に用

いて、個々人のコンテクスト特定位置を相関させて、更に管理することができる。

【００４５】

ノードは、任意の適宜な形式のコンピュータ・デバイス、例えば、メインフレーム・ワークステーション、パーソナル・コンピュータ、サーバ、携帯型コンピュータ・デバイス、又は指令を実行して、ネットワークに接続して、ネットワークを通じてデータパケットを転送することができる任意の他の形式のインテリジェント・デバイスを用いることにより実施し得る。これらのノードは任意の適宜なコンピュータ・プログラムを実行することができ、ネットワークにおける使用のためにデータパケットを生成し、受信し、及び送信する。

【００４６】

図５を参照すると、コンテクスト特定管理処理７５を実行するデバイス７０のための例示的な回路が示されている。このデバイス７０は、プロセッサ７４、メモリ７６、及び記憶装置７８と共に、これらがバス７３又は類似の内部接続を介して接続されたネットワーク・インターフェース８０及び他のインターフェース８２を含む。デバイス７０は、コンテクスト特定管理処理の実行のための上述のノードの何れかを表すことができる。更に、グループ識別子アプリケーションにアクセスするデバイス及びコンテクスト特定処理により生成為れたデータの使用のためのタグリストは類似の回路であるが、図３及び図４において説明したものに対応する処理と共に構成される。

【００４７】

図６は、図１乃至図５に関して説明したWSNの特徴を有すると共に、ここに説明した様々な機能を有する保安システムの例を示す。図６に示すように、相関関係処理は特定の制限付きノードから入力を受け取る（しかし、これらは完全に機能的なノードとすることもできる）。これらの入力は認証情報及びビデオ情報を含むことがあり、相関関係処理は、相関関係結果を生成することがあり、これはネットワーク上に送信される。コンテクスト管理処理は特定の制限付きノードから入力を受け取り（しかし、これらは完全に機能的なノードとすることもできる）、これは例えば、認証情報、ビデオ及びグルーピング情報であり、コンテクスト処理を実行して結果をネットワーク上に送る。ネットワークは、非常口指標、非常用カメラのみならず、分散規則処理及び規則エンジン／メッセージ発信処理の操作を支持する。レンジ・エクステンダは、例えばゲートウェイと共に使用され、かつ、リアルタイム位置システムは図示のように様々なセンサ（例えば、制限付き形式）から入力を受け取る。サーバはクラウド・コンピューティング構成を介してWSNとインターフェースし、或るネットワークの部分はサブネットとして実行することができる。

【００４８】

センサは、センサの範囲内の領域で何かが検出されたことに加えて、詳細な付加的情報を与え、これは特定のセンサに対する入力の広範囲な解析を実行する必要がある侵入検出パネルを伴うことなく、その指標が何であるかを評価するのに用いることができる。

【００４９】

例えば、動作検出器は室内を動き回る暖かい物体の熱的特徴を分析して、それが人間かペットのそれであるか否かを判判するように構成することができる。その分析の結果は、検出された体に関する情報を伝達するメッセージ又はデータである。様々なセンサは、このように音、動作、振動、圧力、熱、画像その他を検知して、侵入発見パネルにおいて真実又は確認された警報状況を検出するのに適切な組み合わせとして用いられる。

【００５０】

認識ソフトウェアは、人間である対象物と動物である対象物とを区別するために用いることができ、更に顔認識ソフトウェアはビデオ・カメラに組み込むことができ、周辺への侵入が、認識され認可された個人によるものであるか否かを確認するために用いられる。そのようなビデオ・カメラは、プロセッサ及びメモリ、並びに認識ソフトウェアからなり、その認識ソフトウェアはカメラによる入力（撮像画像）を処理して、メタデータを生成し、ビデオ・カメラにより撮像された個人の認識又は認識の欠如に関する情報を伝達する。この処理は、これに代えて又はこれに加えて、ビデオ・カメラにより撮像／監視される

領域における個人の特徴に関する情報を含むこともできる。従って、状況に依存して、この情報は、周辺侵入の特徴を与えるセンサへの入力における向上された分析を実行する向上された動作検出器及びビデオ・カメラから受信したメタデータ、又は対象物の認識を確立するために非常に複雑な処理から得られたメタデータの何れかとなろう。

【００５１】

センサ・デバイスは、より複雑な出力を生成するために複数のセンサを統合することができ、それにより侵入検出パネルはその処理能力を利用して、建物仮想イメージ又は環境の特徴により環境を分析するアルゴリズムを実行し、違反の有効性についての理にかなった判断をなす。

【００５２】

メモリは、侵入検出パネルのプロセッサにより使用されるプログラム指令及びデータを記憶する。このメモリは、ランダム・アクセス・メモリとリード・オンリー・メモリとの適切な組合せとしてもよく、プログラム指令（例えばファームウェア又はオペレーティング・ソフトウェア）並びに構成及びオペレーティング・データに適するホストとしてもよく、また、ファイル・システム又はその他のものとして組織化してもよい。記憶されたプログラム指令は、一人以上のユーザを認証するための一つ以上の認証方法を含み得る。パネルのメモリ内に記憶されたプログラムは、更にソフトウェア構成要素を記憶することがあり、これはネットワーク通信とデータ・ネットワークへの接続の確立とを可能にする。ソフトウェア構成要素は、例えば、インターネット・プロトコル（IP）スタック、並びにインターフェース及びキーパッドを含む様々なインターフェースのためのドライバー構成要素を含み得る。ネットワークに亘る接続及び通信を確立するために適する他のソフトウェア構成要素は、当業者には明らかであろう。

【００５３】

構成データと共にメモリ内に記憶されているプログラム指令は、パネルの全体的な操作を制御し得る。

【００５４】

監視サーバは、一つ以上の処理デバイス（例えば、マイクロプロセッサ）、ネットワーク・インターフェース及びメモリ（全て図示しない）を含む。この監視サーバはラック搭載のカードの形態を物理的に採ることがあり、一つ以上のオペレータ・ターミナル（図示せず）と通信し得る。監視サーバの例は、SURGARD（登録商標） SG-System III Virtual、又は類似のシステムである。

【００５５】

各々の監視サーバのプロセッサは、各々の監視サーバのためのコントローラとして働き、各々のサーバと通信し、各々のサーバの全体的な操作を制御する。

【００５６】

プロセッサは、上述のメモリを含むか若しくはこのメモリと通信することがあり、このメモリは、監視サーバの全体的な操作を制御するプロセッサ実行可能指令を記憶する。適宜なソフトウェアは、各々の監視サーバにアラームを受信させて、適切な行為を起こさせることを可能とする。ソフトウェアは、適宜なインターネット・プロトコル（ＩＰ）スタック及びアプリケーション／クライアントを含み得る。

【００５７】

中央監視ステーションの各々の監視サーバは、IPアドレス及び単数又は複数のポートと関係することがあり、それにより、各々の監視サーバはコントロールパネル及び／又はユーザ・デバイスと通信し、警報イベント等を取り扱う。監視サーバ・アドレスは静的であり、ひいては監視サーバの特定の一つを侵入検出パネルへ常に特定し得る。これに代えて、動的アドレスを用いることができ、静的ドメイン名に関係して、ドメインネーム・サービスを通じて決定される。

【００５８】

ネットワーク・インターフェイス・カードはネットワークにインターフェースして、到来する信号を受信し、例えば、イーサネット・ネットワーク・インターフェイス・カード

（NIC）の形態を採り得る。サーバは、コンピュータ、シンクライアント、又はその種の他のものとすることができ、これには警報イベントを表す受信データが人間オペレータによる取扱いのために通過される。監視ステーションは、加入者データベースを更に含むか若しくはこれにアクセスすることがあり、その加入者データベースは、データベースエンジンの制御下のデータベースを含む。データベースは、監視ステーションによりサービスされる上述のパネルのようなパネルへの様々な加入者デバイス／処理に対応するデータ入力を包含することがある。

【００５９】

ここに説明した処理の全て又は部分及びそれらの様々な変更例（以下、「処理」として称する）は、少なくとも部分的には、コンピュータ・プログラム製品、即ち、一つ以上の有形の物理的ハードウェア記憶デバイスに有形に具象化されたコンピュータ・プログラムを介して実施することができ、そのハードウェア記憶デバイスは、データ処理装置（例えば、プログラマブル・プロセッサ、コンピュータ、又は複数のコンピュータ）により実行するため、又はそれらの操作を制御するためのコンピュータ及び／又は機械可読記憶デバイスである。コンピュータ・プログラムは任意の形態のプログラミング言語で書くことができ、これはコンパイル型又はインタープリタ型言語を含み、かつ、スタンド・アローン・プログラムとして、又はモジュール、構成要素、サブルーチン、又は計算環境における使用のために適する他のユニットとしてのものを含む任意の形態に展開することができる。コンピュータ・プログラムは、一つのコンピュータ又は複数のコンピュータであって、一つの位置又は複数の位置に亘って分散されてネットワークにより相互接続されてコンピュータにおいて実行されるように展開することができる。

【００６０】

処理を実行することに関連した行為は、較正処理の機能を実行する一つ以上のコンピュータ・プログラムを実行する一つ以上のプログラマブル・プロセッサにより実行することができる。処理の全て又は一部は、専用用途論理回路、例えば、FPGA（フィールド・プログラム可能ゲート・アレイ）及び／又はASIC（特定用途向け集積回路）として実施することができる。

【００６１】

コンピュータ・プログラムの実行のために適するプロセッサは、例として、一般的で専用用途マイクロプロセッサ、及び任意の種類のデジタル・コンピュータの任意の一つ以上のプロセッサを含む。一般に、プロセッサは、指令及びデータを読出し専用記憶領域域又はランダム・アクセス記憶領域又はその両方から受信する。コンピュータ（サーバを含む）の要素は、指令を実行するための一つ以上のプロセッサと、指令及びデータを記憶するための一つ以上の記憶領域デバイスとを含む。一般に、コンピュータはまた、一つ以上の機械可読記憶媒体、例えばデータを記憶するための大容量記憶デバイス（例えば、磁気、光磁気ディスク、又は光学ディスク）からデータを受信するように、又はそれにデータを転送するように、又は両方のために、上述の一つ以上の機械可読記憶媒体を含むか、それに作動的に結合されている。

【００６２】

コンピュータ・プログラム指令及びデータを実施するために適する有形の物理的ハードウェア記憶デバイスは、不揮発性ストレージの全ての形態を含み、例として、半導体記憶領域デバイス、例えば、EPROM、EEPROM、及びフラッシュ記憶領域デバイス；磁気ディスク、例えば、内蔵ハードディスク又はリムーバブル・ディスク；光磁気ディスク；　及びCD-ROM及びDVD-ROMディスクと不揮発性コンピュータ・メモリ、例えば、スタティック及びダイナミックRAMなどのRAM、並びに消去可能なメモリ、例えば、フラッシュメモリを含む。

【００６３】

更に、図面に描かれた論理フローは、望ましい結果を達成するために、図示された特定の順序、又は連続的順序を必要としない。更に、他の行為を設けてもよく、又は説明されたフローから行為を削除してもよく、また、説明されたシステムに対して他の構成要素を

追加してもよく、又は取り除いてもよい。同様に、図面に描かれた行為は、異なる実体によって実行されてもよく、又は統合されてもよい。

【００６４】

ここに説明した異なる実施形態の要素は、特に上述していない他の実施形態を形成するために組み合わせ得る。要素は、本明細書に説明した処理、コンピュータ・プログラム、ウェブ・ページ等から、それらの操作に悪影響を与えることなく、省略してもよい。更に、様々な個別の要素は、一つ以上の個々の要素に組み合わせて、本明細書に説明した機能を実行するようにしてもよい。

【００６５】

特にここに説明していない他の実施例も以下の請求項の範囲内にある。

【図１】

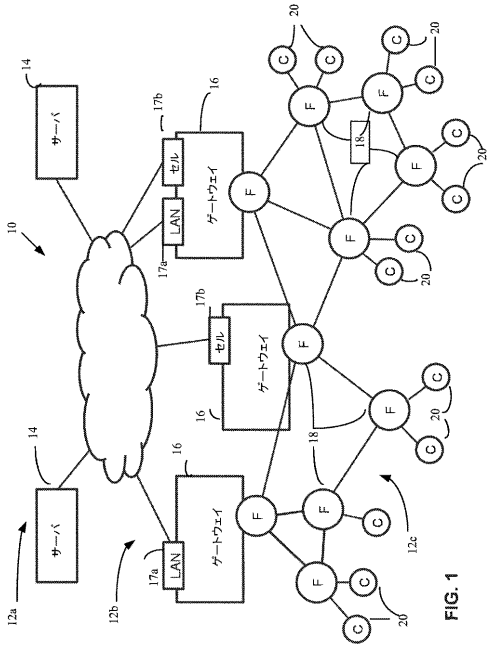

FIG. 1

【図２】

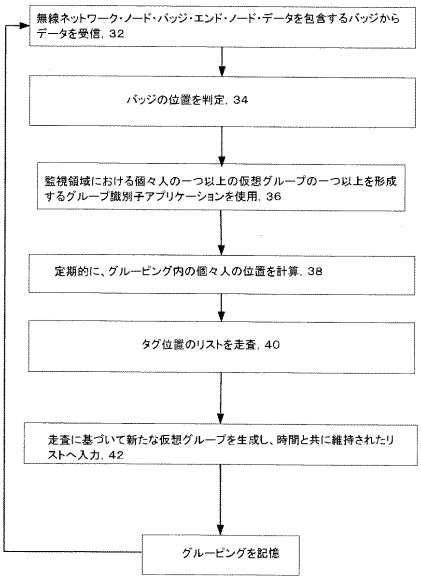

FIG. 2

【図３】

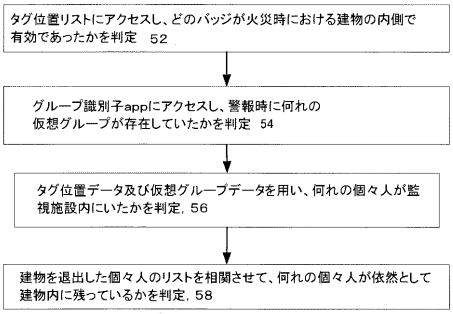

FIG. 3

【図４】

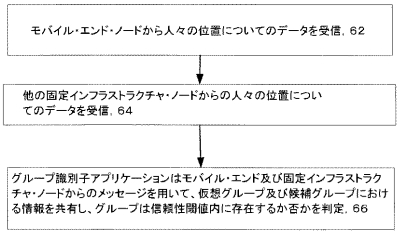

FIG. 4

【図５】

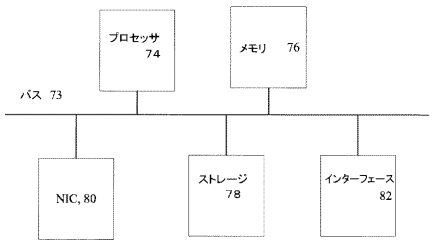

FIG. 5

【図６】

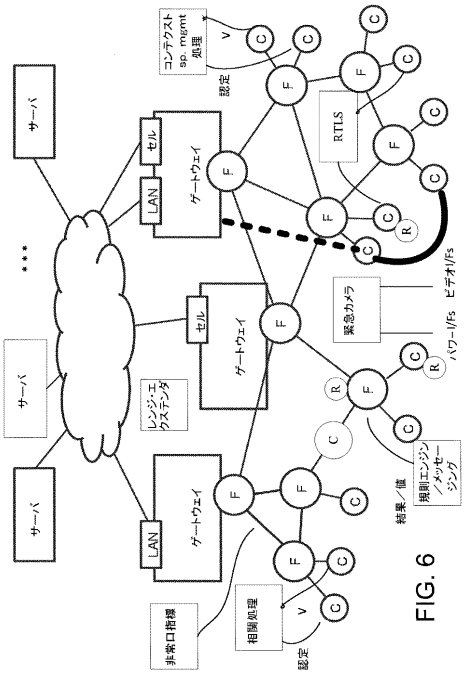

FIG. 6

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2015/017221

A. CLASSIFICATION OF SUBJECT MATTER
IPC(8) - H04L 9/32 (2015.01)
CPC - H04L 9/32 (2015.01)
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)
IPC(8) - G06F 3/01, 12/14, 15/16, 15/173, 21/00; H04L 9/00, 9/32, 12/24; H04Q 7/20; H04W 4/02 (2015.01)
USPC - 455/456.1, 456.3; 709/204, 206, 223; 713/168; 715/752; 726/4, 22

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
CPC - G06F 21/55; H04L 9/0866, 9/32, 12/1895, 43/028 (2015.01) (keyword delimited)

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
Orbit, Google Patents, Google Scholar.
Search terms used: alarm monitoring, intrusion detection, sensory input, credential, badge, monitored premises, virtual grouping, tag location, dynamic grouping, fuzzy grouping

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2007/0186106 A1 (TING et al.) 09 August 2007 (09.08.2007) entire document	1-12
Y	US 2012/0197986 A1 (CHEN et al.) 02 August 2012 (02.08.2012) entire document	1-12
A	US 2003/0216144 A1 (ROESE et al.) 20 November 2003 (20.11.2003) entire document	1-12
A	US 2006/0059557 A1 (MARKHAM et al.) 16 March 2006 (16.03.2006) entire document	1-12
A	US 2007/0106775 A1 (WONG) 10 May 2007 (10.05.2007) entire document	1-12
A	US 2012/0159579 A1 (PINEAU et al.) 21 June 2012 (21.06.2012) entire document	1-12

☐ Further documents are listed in the continuation of Box C. ☐

* 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
27 April 2015	26 MAY 2015
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-8300	Authorized officer: Blaine R. Copenheaver PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774

Form PCT/ISA/210 (second sheet) (July 2009)

フロントページの続き

(51)Int.Cl.	F I	テーマコード（参考）
	G07C 9/00 Z	

(81)指定国 AP(BW,GH,GM,KE,LR,LS,MW,MZ,NA,RW,SD,SL,ST,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,IR,IS,JP,KE,KG,KN,KP,KR,KZ,LA,LC,LK,LR,LS,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

(74)代理人 100118647
弁理士 赤松 利昭
(74)代理人 100138438
弁理士 尾首 亘聰
(74)代理人 100138519
弁理士 奥谷 雅子
(74)代理人 100123892
弁理士 内藤 忠雄
(74)代理人 100169993
弁理士 今井 千裕
(74)代理人 100185535
弁理士 逢坂 敦
(72)発明者 ラスバンド、ポール・ビー
アメリカ合衆国、フロリダ州 ３３４６２、ランタナ、ウィンドスウェプト・ドライブ ２９８１

Ｆターム(参考) 3E138 AA01 CB03 DA03 EA02 FA03 GA02 JA01 JB03 JC01 JD05
5C087 AA03 AA09 AA19 BB20 BB74 DD04 DD06 DD20 EE14 FF01
FF02 FF04 GG02 GG10 GG22 GG68 GG82
5K201 AA09 BA02 CB08 CB13 CC01 CC04 CC10 DC02 DC04 EA08
EB06 EC01 EC06 ED04 ED05 ED09 EE05 EE12 EF04 FA06