

(19) 日本国特許庁 (JP)

(12) 特 許 公 報 (B2)

(11) 特許番号
特許第5990201号
(P5990201)

(45) 発行日 平成28年9月7日 (2016.9.7)

(24) 登録日 平成28年8月19日 (2016.8.19)

(51) Int. Cl.

F I

HO 4 W 12/08 (2009.01)

HO 4 W 4/04 (2009.01)

HO 4 W 84/18 (2009.01)

HO 4 W 12/08

HO 4 W 4/04 1 9 0

HO 4 W 84/18

請求項の数 27 (全 18 頁)

(21) 出願番号	特願2013-554472 (P2013-554472)	(73) 特許権者	513210390
(86) (22) 出願日	平成24年2月3日 (2012.2.3)		フェデックス コーポレート サービスズ
(65) 公表番号	特表2014-510465 (P2014-510465A)		, インコーポレイティド
(43) 公表日	平成26年4月24日 (2014.4.24)		アメリカ合衆国, テネシー 38017,
(86) 国際出願番号	PCT/US2012/023732		コリアービル, パーティカル, フェデック
(87) 国際公開番号	W02012/115761		ス パークウェイ 30, ファースト フ
(87) 国際公開日	平成24年8月30日 (2012.8.30)		ロア
審査請求日	平成27年1月29日 (2015.1.29)	(74) 代理人	100099759
(31) 優先権主張番号	61/445, 267		弁理士 青木 篤
(32) 優先日	平成23年2月22日 (2011.2.22)	(74) 代理人	100092624
(33) 優先権主張国	米国 (US)		弁理士 鶴田 準一
(31) 優先権主張番号	13/351, 861	(74) 代理人	100114018
(32) 優先日	平成24年1月17日 (2012.1.17)		弁理士 南山 知広
(33) 優先権主張国	米国 (US)	(74) 代理人	100165191
			弁理士 河合 章

最終頁に続く

(54) 【発明の名称】 センサーウェブネットワークにおいて機器を認証するためのシステム及び方法

(57) 【特許請求の範囲】

【請求項 1】

センサー機器に関連するセンサーデータを配信するための方法であって、
要求元機器が、第 1 センサー収集可能データにアクセスすることを認証され、前記第 1 センサー収集可能データへのアクセス要求は、ルーティング情報を含み、且つ前記ルーティング情報は前記要求元機器とは異なるセンサーデータホストを示す場合に、少なくとも一つの荷物に関連付けられた第 1 センサー収集可能データへの前記アクセス要求を前記要求元機器から受信するステップと、

前記第 1 センサー収集可能データへのアクセスの禁止に関連付けられた位置を示す第 2 センサー収集可能データに少なくとも部分的に基づいた前記第 1 センサー収集可能データへの前記アクセス要求を拒否するか否か判定するステップと、

を含み、

前記位置は前記センサーデータホストに関連するものである、方法。

【請求項 2】

前記要求元機器がセンサーを含む、請求項 1 に記載の方法。

【請求項 3】

前記第 2 センサー収集可能データが、前記要求元機器の前記センサーにより収集される、請求項 2 に記載の方法。

【請求項 4】

前記第 1 センサー収集可能データのアクセスを禁止している管轄区域に前記要求元機器

が位置していることに基づいて、前記アクセス要求を拒否するステップをさらに含む、請求項 1 に記載の方法。

【請求項 5】

前記少なくとも一つの荷物の近接にある前記センサー機器にて前記第 1 センサー収集可能データを収集するステップと、

前記センサー機器にて前記第 2 センサー収集可能データを収集するステップと、

をさらに含む方法である、請求項 1 に記載の方法。

【請求項 6】

前記第 1 センサー収集可能データに対する前記要求元機器を認証するために、ネットワークを介して、認証ホストにアクセスするステップをさらに含む、請求項 1 に記載の方法。

10

【請求項 7】

前記第 1 センサー収集可能データに対して前記要求元機器を認証するために、ローカルに予め設定されたリストにアクセスするステップをさらに含む、請求項 1 に記載の方法。

【請求項 8】

前記アクセス要求が許可される場合に、前記方法が、

前記第 1 センサー収集可能データを、前記ルーティング情報に従って、前記センサーデータホストに送信するステップをさらに含む、請求項 1 に記載の方法。

【請求項 9】

前記第 1 センサー収集可能データが、前記少なくとも一つの荷物の環境条件を記述する、請求項 1 に記載の方法。

20

【請求項 10】

センサー機器内のプロセッサにより実行されるときに、前記プロセッサにセンサーデータを配信するための方法を実行させるプログラムであって、前記方法が、

要求元機器が第 1 センサー収集可能データにアクセスすることを認証され、前記第 1 センサー収集可能データへのアクセス要求は、ルーティング情報を含み、且つ前記ルーティング情報は前記要求元機器とは異なるセンサーデータホストを示す場合に、少なくとも一つの荷物に関連付けられた前記第 1 センサー収集可能データへの前記アクセス要求を前記要求元機器から受信するステップと、

前記第 1 センサー収集可能データへのアクセスの禁止に関連付けられた位置を示す第 2 センサー収集可能データに少なくとも部分的に基づいた前記第 1 センサー収集可能データへの前記アクセス要求を拒否するか否か判定するステップと、

30

を含み、前記位置は前記センサーデータホストに関連するものである、方法である、プログラム。

【請求項 11】

前記要求元機器がセンサーを含む、請求項 10 に記載のプログラム。

【請求項 12】

前記第 2 センサー収集可能データが前記要求元機器の前記センサーによって収集される、請求項 11 に記載のプログラム。

【請求項 13】

40

前記方法が、

前記第 1 センサー収集可能データのアクセスを禁止する管轄区域に前記要求元機器が位置していることに基づいて、前記アクセス要求を拒否するステップをさらに含む、請求項 10 に記載のプログラム。

【請求項 14】

前記方法が、

前記少なくとも一つの荷物の近接にある前記センサー機器にて前記第 1 センサー収集可能データを収集するステップと、

前記センサー機器にて前記第 2 センサー収集可能データを収集するステップと、

をさらに含む、請求項 10 に記載のプログラム。

50

【請求項 15】

前記方法が、

前記第1センサー収集可能データに対して前記要求元機器を認証するために、ネットワークを介して、認証ホストにアクセスするステップをさらに含む、請求項10に記載のプログラム。

【請求項 16】

前記方法が

前記第1センサー収集可能データに対して前記要求元機器を認証するために、ローカルに予め設定されたリストにアクセスするステップをさらに含む、請求項10に記載のプログラム。

10

【請求項 17】

前記アクセス要求が許可される場合に、前記方法が、

前記ルーティング情報に従って、前記第1センサー収集可能データを前記センサーデータホストに送信するステップをさらに含む、請求項10に記載のプログラム。

【請求項 18】

前記第1センサー収集可能データが前記少なくとも一つの荷物の環境条件を記述する、請求項10に記載のプログラム。

【請求項 19】

センサーデータを配信するための機器であって、

要求元機器が第1センサー収集可能データにアクセスする認証を受け、前記第1センサー収集可能データへのアクセス要求は、ルーティング情報を含み、且つ前記ルーティング情報は前記要求元機器とは異なるセンサーデータホストを示す場合に、少なくとも一つの荷物に関連付けられた前記第1センサー収集可能データへの前記アクセス要求を前記要求元機器から受信するように構成された入出力部と、

20

前記第1センサー収集可能データへのアクセスの禁止に関連付けられた位置を示す第2センサー収集可能データに少なくとも部分的に基づいた前記第1センサー収集可能データへの前記アクセス要求を拒否するか否か判定するように構成されたプロセッサと、

を備え、前記位置は前記センサーデータホストに関連するものである、機器。

【請求項 20】

前記要求元機器がセンサーを含む、請求項19に記載の機器。

30

【請求項 21】

前記第2センサー収集可能データが前記要求元機器の前記センサーにより収集される、請求項20に記載の機器。

【請求項 22】

前記プロセッサが、

前記要求元機器が、前記第1センサー収集可能データへのアクセスを禁止する管轄区域に位置していることに基づいて、前記アクセス要求を拒否するようにさらに構成された、請求項19に記載の機器。

【請求項 23】

前記少なくとも一つの荷物の近接にあるセンサー機器にて前記第1センサー収集可能データを収集し、

40

前記センサー機器にて前記第2センサー収集可能データを収集するように構成された検出部をさらに備える、請求項19に記載の機器。

【請求項 24】

前記入出力部が、

前記第1センサー収集可能データに対して、前記要求元機器を認証するために、ネットワークを介して、認証ホストにアクセスするようにさらに構成された、請求項19に記載の機器。

【請求項 25】

前記プロセッサが、

50

前記第 1 センサー収集可能データに対して、前記要求元機器を認証するためにローカルに予め設定されたリストにアクセスするようにさらに構成された、請求項 19 に記載の機器。

【請求項 26】

前記アクセス要求が許可される場合、前記プロセッサが

前記ルーティング情報に従って、前記第 1 センサー収集可能データを前記センサーデータホストに前記入出力部から送信するようにさらに構成された、請求項 19 に記載の機器。

【請求項 27】

前記第 1 センサー収集可能データが前記少なくとも一つの荷物の環境条件を記述する、請求項 19 に記載の機器。

【発明の詳細な説明】

【技術分野】

【0001】

本開示は、一般に、コンピュータシステムの分野に関する。より具体的には、本開示は、無線メッシュネットワーク等のセンサーウェブネットワークにおいて機器を認証するためのコンピュータシステム及び方法に関する。

【0002】

関連出願の相互参照

本出願は、その全内容を参照により本明細書に組み込む、2011年2月22日出願の米国仮特許出願第 61 / 445, 267 号の優先権を主張する。

【背景技術】

【0003】

無線メッシュネットワークは、メッシュ形に編成された無線ノードで構成される通信ネットワークである。無線メッシュネットワークは、しばしば、メッシュクライアント (mesh client)、メッシュルーター (mesh router) 及びゲートウェイから成る。メッシュクライアントは無線機器であってもよく、ゲートウェイはインターネット等の外部のネットワークへのアクセスを許可し得る。その間、メッシュルーターはメッシュクライアントとゲートウェイとの間のトラフィックを転送できる。単一のネットワークとして動作する無線ノードのサービスエリアはメッシュクラウド (mesh cloud) と呼ばれることもある。メッシュクラウドへのアクセスは、無線ネットワークを作成するために互いに協働して動作する無線ノードに依存し得る。

【0004】

メッシュネットワークは信頼性を備え、冗長性を提供することもあり得る。一つのノードが動作できなくなっても、残りのノードは直接的に又は一つ以上の中間ノードを介して、依然として互いに通信が可能であり得る。無線メッシュネットワークは、802.11、802.16、セルラー技術又は複数の種類の組合せを含む、様々な無線技術を使って実現され得る。

【発明の概要】

【発明が解決しようとする課題】

【0005】

無線メッシュネットワークは、特殊な種類の無線アドホックネットワークとして見ることができる。メッシュルーターは高移動性 (highly mobile) を有することもあり、メッシュクライアント等の、ネットワーク中の他のノードと比較して、より多くのリソースを有し得る。したがって、メッシュルーターはよりリソース集約的な機能の実行に使用できる。このような点で、無線メッシュネットワークはノードがリソースによってしばしば制約されるアドホックネットワークとは異なる。

【0006】

場合によっては、ネットワーク中のノードは、センサー等のデータ収集機器及び記憶装置である。センサーは収集したデータを共有することが可能であり得るため、データのセ

10

20

30

40

50

セキュリティが問題となり得る。したがって、センサーが収集可能なデータを防護するためのシステム及び方法を実現することが必要となり得る。

【課題を解決するための手段】

【0007】

本発明に従って、センサーデータを配信するための方法が提供され、その方法は、要求元機器から、少なくとも一つの荷物に関連付けられた第1センサー収集可能データへのアクセスを求める要求を受信するステップと、要求元機器が第1センサー収集可能データにアクセスすることを認証されるステップと、及び第2センサー収集可能データが所定値に関連付けられているときに、アクセス要求を拒否するステップとを含む。

【0008】

本発明に従って、プロセッサによって実行されたときに、プロセッサにセンサーデータを配信するための方法を実行させるプログラム命令を格納するコンピュータ読み取り可能な媒体も提供され、その方法は、要求元機器から、少なくとも一つの荷物に関連付けられた第1センサー収集可能データにアクセスする要求を受信するステップと、その要求元機器が第1センサー収集可能データにアクセスすることを認証されるステップと、第2センサー収集可能データが所定値に関連付けられているときに、アクセス要求を拒否するステップとを含む。

【0009】

本発明に従って、さらにセンサーデータの配信のための機器も提供され、その機器は、要求元機器から、少なくとも一つの荷物に関連付けられた第1センサー収集可能データのアクセス要求を受信し、要求元機器が第1センサー収集可能データにアクセスすることを認証されるように構成された入出力部及び第2センサー収集可能データが所定値に関連付けられているときに、アクセス要求を拒否するように構成されたプロセッサを含む。

【0010】

本発明のさらなる態様は、ある程度は、以下に続く記述で説明され、ある程度は、その記述から明白になり、或いは本発明の実践により学習され得る。本発明の態様は、付属の特許請求の範囲で具体的に指摘される要素及び組合せを通じて実現及び達成される。

【0011】

上記の一般的な記述及び以下の詳細な記述のどちらも例示及び説明の目的のためのみのものであり、請求される本発明を限定するものでないことを理解されるべきである。

【図面の簡単な説明】

【0012】

添付された図面は、本明細書に組み込まれ、本明細書の一部を構成するものであり、本発明の一つ（又は複数）の実施形態を示し、記述と共に、本発明の原理を説明する役目を果たす。

【0013】

【図1】 荷物の環境に関するデータを収集するための例示的なシステムを示す図である。

【図2】 開示された実施形態で用いられる例示的な機器及びホストを説明するブロック図である。

【図3】 センサー収集可能データをセンサー機器から要求元機器に送信するための例示的な方法の操作のフローチャートである。

【図4】 要求元機器を認証するための表を示している。

【図5】 要求元機器が複数の種類のセンサー収集可能データを要求するときに、センサー収集可能データをセンサー機器から要求元機器に送信する例示的な方法の操作のフローチャートである。

【図6】 要求元機器により提供されるルーティング情報に従って、センサー機器から目的地にセンサー収集可能データを送信するための例示的な方法の操作のフローチャートである。

【図7】 特定のセンサー収集可能データが特定の値又は範囲に関連付けられている場合に、センサー機器から要求元機器にセンサー収集可能データを送信するための例示的な方法

10

20

30

40

50

の操作のフローチャートである。

【発明を実施するための形態】

【0014】

本開示は、一般に、配達網における荷物に関連付けられた一つ以上のセンサーから収集される情報の収集及び配信に関する。センサーは荷物に関連付けられた情報を収集する目的に使用され得る。収集する情報は、要求元機器に提供され得る。

【0015】

本開示の目的では、容器又は荷物は箱、封筒又は一つの地点から別の地点へと文書又は製品を出荷する目的に使用される任意の他の媒体とすることができる。商品は、典型的には、容器に保管されて荷物を形成する。したがって、荷物は、例えば傷みやすい物質又は規制物質も含めて、発生源から目的地までの通過プロセスの一部又は全部の間、特定の状態を必要とする一種以上の商品を含み得る。荷物の特定の形状又は寸法はこの記述には特に重要ではない。この配達網は種々多様な形状及び寸法の荷物を配達できる。

【0016】

一つの例における配達網は、航空機、列車、トラック、及びその他、任意の種類の品物を輸送するための手段等の輸送媒体のネットワークを含む。配達網は荷物を発生源（例えば、発信人）から収集し、その荷物を目的地（例えば、受取り人）に配達する目的に使用され得る。

【0017】

一つの例においては、一つ以上のセンサーが荷物に関連付けられることがあり得る。言い換えれば、一つ以上のセンサーが荷物内に配置される、荷物に取り付けられる、又は荷物の付近に配置できる。センサーは荷物及び／又はその内容物に関係する特定の種類の情報を収集するように構成され得る。荷物又は荷物の内容物に対するセンサーの配置は、センサーが収集するように設定された情報の種類に基づいていてもよい。例えば、このセンサー収集可能情報には、任意の所定時刻における荷物又はその内容物に関連付けられた地理的位置並びに／又は荷物の外部及び／若しくは内部温度、荷物内若しくは荷物周囲の湿度、荷物内若しくは荷物周囲の水分レベル、荷物の高度、及びセンサーが収集可能な任意のその他の状態を含む、その他の状態を含むことができる。

【0018】

センサーは通信無線等の送受信機を有し得る。一つの例では、送受信機は、荷物の輸送中に、荷物に関連付けられたセンサーと他の機器との効率的な通信を可能にする携帯電話の選択された要素（component）を有する。他の同様の無線及び／又は有線送信構成が、本開示と関連させて使用されることもあり得る。

【0019】

開示された実施形態は、センサー又は他の機器を複数備え、その一部又は全部が協働的なエコシステムにおいて情報を共有する、メッシュネットワーク等のネットワークを含み得る。例えば、センサーは断熱された荷物の内部に配置されて、荷物の内部温度を監視し得る。しかしながら、センサーは荷物の外側からも温度情報を必要とするかもしれない。したがって、センサーはそのセンサーが接続することが可能で、通信することが可能な他の近接のセンサーを識別するかもしれない。一部の実施形態においては、センサーは、外部温度情報を取得するために、荷物の外側に位置するセンサーに接続することも可能であり得る。機器は他の数多くの種類の収集された情報を共有することが可能であるため、これは一つの例にすぎない。

【0020】

他の実施形態において、センサーではない機器、例えばメッシュルーター等が、センサーからのセンサー収集可能データを要求して、収集データを集約及び解析することもあり得る。例えば、配達トラックの中のメッシュルーターは、トラックの至るところに置かれた個々の荷物に関連付けられたセンサーから温度情報を収集し、例えば、トラックの前部と後部での温度差も含め、トラックの温度トポロジーを求めるように構成されることもあり得る。

10

20

30

40

50

【 0 0 2 1 】

これらの様々な機器及びセンサーは情報を共有できるため、本開示は、収集済みの情報を求める任意の要求元機器が、許可を得ているものとして適正に認証されるように保証するためのデータアクセスプロトコルを説明する。例えば、開示された実施形態は、データアクセスのための認証のサーバー側モデルを採用してもよい。これは、さらに、要求元機器のポイント・ツー・ポイント識別（近接ノードのpingのようなスイープ（sweep））を実行する場合もある）を容易にすることもできる。近接ノードは応答する場合、要求元ノードのMACアドレス等の一意な識別子を識別し得る。応答側ノードは、部分的には、その一意な識別子に基づいて、要求元機器を認証できる。さらに、応答側ノードは、要求元ノードの認証において、他の要因、例えば他の収集したセンサー情報等も考慮に入れることもできる。

10

【 0 0 2 2 】

このポイント・ツー・ポイント・システムは、例えば、メッシュネットワークで、各通信機器が、収集した情報を中継する必要のある追加機器のオーバーヘッドを伴わずに、それぞれのデータ密度を増加することを可能にする。このシステムは、さらに、複数のメーカー製の機器が情報を共有することを可能にするために必要とされる集積化も容易にし得る。もちろん、これらの例は本発明の範囲を限定するものではなく、当業者であれば、本発明の範囲には、無数の実施形態が含まれることを理解されるであろう。

【 0 0 2 3 】

これから、添付された図面に示される例示的な実施形態に詳しく言及していく。可能な箇所では、同一又は同様の部品を参照するのに、図面全体を通して同一の参照番号が用いられる。

20

【 0 0 2 4 】

図1は、荷物の環境についてのデータを収集するための例示的なシステム100を示している。システム100は、メッシュネットワーク102を含み得る。メッシュネットワーク102は、センサー機器104、要求元機器106、及びセカンダリー機器108（secondary device）等の相互接続された複数の機器、並びに示されていない他の機器も含み得る。他の実施形態は、メッシュネットワーク102以外の異なる種類のネットワーク、例えばローカルエリア・ネットワーク（LAN）、広域ネットワーク（WAN）、無線及び/又は有線ネットワーク等を使用することもあり得る。

30

【 0 0 2 5 】

システム100は、また、認証ホスト110及び/又はセンサーデータホスト112を含み得、それはネットワーク114を介してメッシュネットワーク102に接続されてもよい。ネットワーク114は、メッシュネットワーク102、認証ホスト110、及び/又はセンサーデータホスト112の間等での通信を容易にするように構成される。加えて、メッシュネットワーク102、認証ホスト110及び/又はセンサーデータホスト112は、ネットワーク114を介して、システム100には示されていない、他のシステム又は他のエンティティにアクセスしてもよい。ネットワーク114は共有、パブリック又はプライベート・ネットワークであってよく、広域又はローカルエリアを含み得、有線及び/又は無線通信ネットワークの任意の適切な組合せを通じて実現され得る。さらに、ネットワーク114は、ローカルエリア・ネットワーク（LAN）、広域ネットワーク（WAN）、イントラネット又はインターネットを含んでもよい。一部の実施形態において、メッシュネットワーク102、認証ホスト110及び/又はセンサーデータホスト112は、ネットワーク114を通じて接続される代わりに、全体的又は部分的に、直接接続されてもよい。

40

【 0 0 2 6 】

メッシュネットワーク100は、荷物の配達に用いられる機器を含み得る。機器は、輸送中、一つ以上の荷物の環境での条件を追跡又は解析する目的に使用され得る。例えば、センサー機器104は、荷物の内部又は近くに配置されてもよく、温度、光源レベル、動作、圧力、湿度、ガス濃度、気流、振動、放射線、時刻、音声、動画、方向、位置、又は

50

その他のセンサー収集可能データ等、環境条件に関するデータを収集し得る。

【0027】

要求元機器106は、また、荷物の周囲の環境条件に関するデータも収集するように構成される。代わりに又は追加的に、要求元機器106は、センサー収集可能データを解析して、レポートを作成するか、又はセンサー収集可能データに基づいて動作又は警告をすることもある。一部の実施形態において、要求元機器106は、センサー機器104によって収集されるデータを要求できる。そして、一部の実施形態においては、要求元機器106はセンサーを含まないこと又はデータを収集しないこともあり得る。

【0028】

一つの例において、要求元機器106は、部分的に絶縁された荷物の中に配置されてもよい。荷物の内容物は、温度に依存する可能性があり、温度が一定の値を超えると、損傷を受ける可能性もある。要求元機器106、又はその他の一部の機器は、荷物内の温度が閾値を超えるか、又は閾値を超える危険にあると、警告をすることが可能であり得る。輸送中、荷物は倉庫でトラックからトラックへと移されることもあり、屋外に置かれることや冷蔵保存されていない容器に入れられることもあり得る。したがって、要求元機器106は、荷物の外部の温度情報を求めるために、近接のセンサーにpingを送ることもあり得る。この例では、センサー機器104は、荷物の外部の温度情報を収集でき、要求元機器106は、その外部温度情報を要求できる。荷物外部の温度が非常に高い場合は、要求元センサー106は、荷物が閾値温度を超える危険があると判断し、警告を発することもできる。

【0029】

要求元機器106又は任意の他の機器は、状態を解析するときに、履歴情報に依存することもできる。例えば、荷物が特定の時間に屋外に置かれている場合、要求元機器106は、温度が上昇又は低下することが予想できるか否か、及びどれだけの時間、屋外で待つことができるかを知る必要があるかもしれない。要求元機器106は、センサーデータホスト112等のホストから、直接的に又は別の機器若しくはホストを介して、この履歴情報を入手し得る。例えば、要求元機器106は、センサー機器104を通じて、この履歴情報を受信し得る。

【0030】

センサー収集可能データが非常に容易に共有される環境では、センサー収集可能データが外部の第三者に共有されることが不可能にするために認証技法を実現する必要があるかもしれない。実際、一部のセンサー収集可能データは、機密又は妥当性であり得る。したがって、一部の実施形態において、要求元機器106は、センサー収集可能データを受信する前に、何らかの方法でセンサー機器104に対して自己を認証することが要求されるかもしれない。

【0031】

さらに、メッシュネットワーク100内の他の機器は、センサー104からのデータを収集するように構成され得る。例えば、セカンダリー機器108は、そのようなデータを活用し得るが、センサー機器104から直接ではなく、要求元機器106からデータを取得することもできる。一部の実施形態では、要求元機器106は、セカンダリー機器108のプロキシとしての役割を務めることもあり得る。

【0032】

要求元機器106がセンサー104からのセンサーデータを要求すると、センサー104は、要求元機器106を認証して、センサーデータへのアクセスを確実に許可できる。センサー機器104は、この認証をローカルで実行することも、又は認証ホスト110に認証を実行するように要求することもできる。すると、認証ホスト110は要求元機器106を認証すべきか否かを判断し、この判定をセンサー機器104に送信できる。

【0033】

要求元機器106は、センサーデータホスト112の位置をセンサー機器104に提供できる。したがって、センサー機器104は要求元機器106を認証した後、処理、格納

10

20

30

40

50

及び／又は解析のために要求されたセンサー収集可能データをセンサーデータホスト 1 1 2 に送信できる。

【 0 0 3 4 】

システム 1 0 0 は一つの例示的な構成であり、示される様々なエンティティ (e n t i t i e s) の数及び分布は、具体的に実施形態に応じて異なる可能性がある。一部の実施形態において、認証ホスト 1 1 0 及び／又はセンサーデータホスト 1 1 2 は、他の分散システム、センサー、コンピュータ、携帯用コンピュータ、携帯電話、タブレットコンピュータ又はその他のコンピューティングプラットフォームを含む、複数のエンティティにまたがって分散され得る。したがって、システム 1 0 0 に記述された構成は一つの例にすぎず、限定することを意図していない。

10

【 0 0 3 5 】

図 2 は一部の例示的なシステム構成で活用される機器及びホストの非限定的な例を示すブロック図 2 0 0 である。ブロック図 2 0 0 は、機器 2 0 2 及びホスト 2 0 4 を含む。機器 2 0 2 はセンサー機器 1 0 4、要求元機器 1 0 6 及び／又はセカンダリー機器 1 0 8 に対応してもよい。そして、ホスト 2 0 4 は認証ホスト 1 1 0 及び／又はセンサーデータホスト 1 1 2 に対応してもよい。

【 0 0 3 6 】

機器 2 0 2 は検出部 2 0 6 を含むことができ、検出部 2 0 6 は、荷物の環境に関するデータを収集するためのソフトウェア及び／又はハードウェア構成要素を一つ以上含み得る。言い換えれば、検出部 2 0 6 はある種のセンサーとすることができる。例えば、検出部 2 0 6 は、荷物に関する位置情報を収集できる。一部の実施形態では、位置情報は全地球測位システム (G P S) の使用を含むこともできる。G P S が使用される場合、検出部 1 0 4 は、G P S 技術で活用される c o a r s e a c q u i s i t i o n c o d e (C / A コード) を使用することもできる。

20

【 0 0 3 7 】

位置情報は、また、セルラー三角測量、無線ネットワーク関連付け、固定位置スキンのキャプチャ (c a p t u r e)、又は移動位置スキンのキャプチャを通じても求めることができる。固定位置及び移動位置のスキンは、一次元又は二次元のバーコード、又は無線 I C タグ (R F I D) を使用することもできる。例えば、機器 2 0 2 は所定位置に対応するバーコードをスキャンするか、又は所定位置に対応する R F I D タグを読み取ることができる。機器 2 0 2 は、バーコード又は R F I D に対応する値を使ったスキャン後、所定位置を検索することも可能であってよい。

30

【 0 0 3 8 】

国際的な位置において、複数の全地球航行衛星システムが利用可能である場合もある。複数のセルラーネットワーク間での切り換えと同様、接続の切り換えを活用することにより、向上したサービスが提供され得る。例えば、N a v i S t a r (米国)、G L O N A S S (ロシア) 及びその他の衛星システムが利用可能であり得る。したがって、検出部 2 0 6 は、位置情報を求める際に異なる複数の G P S プロバイダ間で切り換えることも可能である。さらに、衛星をベースとする補強システムによるタイミング補正又は異なる G P S を追加することにより、ビルの谷間でのシステムの性能を向上し、精度を 1 メートル未満の単位まで向上できる。

40

【 0 0 3 9 】

位置情報に加えて、又は位置情報の代わりに、検出部 2 0 6 は、荷物及び／又はその内容物に関する他のデータ、例えば、任意の時点又は選択した時点での環境条件を収集できる。例えば、検出部 2 0 6 は、温度、光源レベル、動作、圧力、湿度、ガス濃度、気流、振動、放射線、時刻、音声、動画又はその他の環境条件に関するデータを収集できる。輸送中、いくつかの荷物の環境は一定のパラメータの範囲内、例えば、一定の温度範囲、圧力範囲又は湿度範囲内等である必要があるかもしれない。時刻、音声又は動画のようなその他の情報は、荷物の配達の状態を判定するのに関係していることもあり得る。

【 0 0 4 0 】

50

例えば、検出部 206 は、配達時、又は処理センターのような中継目的地への到着時に、荷物を受け取っている人の静止画像又は動画を記録するように構成されたカメラを含むこともできる。検出部 206 は、また、音声録音機を使って音声を録音すること又は内部クロックを使って時刻を求めることもできる。したがって、開示された実施形態は、異なる種類の環境データを収集するように構成された異なる種類のセンサーを使うこともできる。一部の実施形態においては、機器 202 は、数多くの検出部 206 を含むこともでき、その各々は異なる種類の環境データを収集するように構成される。一部の実施形態においては、単一の検出部 206 は、異なる種類の環境データを収集することが可能であり得る。

【0041】

機器 202 は、また、収集した環境データ等のデータを処理するために、中央演算処理装置 (CPU) 208 及びメモリ 210 を含むこともできる。CPU 208 は様々なプロセス及び方法を実行するために、コンピュータプログラム命令を実行するように構成された一つ以上のプロセッサを含むことができる。CPU 208 は、コンピュータプログラム命令をメモリ 210 から又は任意のコンピュータ読み取り可能な媒体から読み取ることができる。メモリ 210 は、情報及びコンピュータプログラム命令にアクセスし、格納するように構成されたランダムアクセスメモリ (RAM) 及び / 又は読み取り専用メモリ (ROM) を含むこともできる。メモリ 210 は、また、収集した環境データ等のデータ及び情報を格納するための追加メモリ、並びに / 又は表、リスト又はその他のデータ構造を格納するための一つ以上の内部データベースを含むこともできる。

【0042】

機器 202 内の入出力部 212 は、収集した環境データの処理及び / 又は格納のために別の機器に送信できる。入出力部 212 は、収集したデータをメッシュネットワーク 102 及び / 又はネットワーク 114 等の、ある種のネットワークを通じて送ることができる。

【0043】

ホスト 204 は、CPU 214、メモリ 216、データベース 218 及び入出力部 220 を含むことができる。データベース 218 は、大量のデータを格納でき、磁気、半導体、テープ、光又はその他の種類の記憶装置を含むことができる。

【0044】

ホスト 204 の CPU 214、メモリ 216 及び入出力部 220 は、機器 202 の CPU 208、メモリ 210 及び入出力部 212 と同様であってもよい。一部の実施形態においては、ホスト 204 からの CPU 214、メモリ 216 及び入出力部 220 は、より堅牢であり得、機器 202 からの CPU 208、メモリ 210 及び入出力部 212 よりも多くの機能を有し得る。実際、ホスト 204 をより大型で、より機能の高いコンピュータとし、機器 202 を小型で携帯可能とすることもできる。

【0045】

ブロック図 200 は、一つの例示的な構成であり、示される様々なエンティティの数及び構成要素は、具体的な実施形態によって異なる可能性がある。例えば、一部の実施形態においては、機器 202 は、CPU 208 及び / 又はメモリ 210 を含まないこともあり得る。他の実施形態においては、ホスト 204 は、他の分散システム、センサー、コンピュータ、携帯用コンピュータ、携帯電話、タブレットコンピュータ又はその他のコンピューティングプラットフォームを含む、複数のエンティティにまたがって分散され得る。機器 202 は、同様に、任意のコンピューティングプラットフォームを介して実現又は分散され得る。したがって、ブロック図 200 で記述した構成は一つの例にすぎず、限定することを意図していない。

【0046】

図 3 はセンサー収集可能データをセンサー機器 104 から要求元機器 106 に送信するための例示的な方法 300 の操作のフローチャートである。方法 300 は、センサー機器 104 上の様々な構成要素により実行され得る。方法 300 は、また、他の機器によって

10

20

30

40

50

、又は、システム 100 若しくはブロック図 200 に表示されていない機器も含め、任意の他の機器との組合せによって実行されてもよい。一部の構成では、方法 300 のステップのいくつかは省略可能であるか、又は並べ替えが可能である。さらに、追加のステップを方法 300 に追加することも可能である。

【0047】

センサー機器 104 は、検出部 206 を使って、第 1 センサー収集可能データを収集できる（ステップ 302）。第 1 センサー収集可能データは、任意の環境条件、例えば、荷物内の温度データに関するものであってよい。次に、センサー機器 104 は、CPU 208 を使って、第 1 センサー収集可能データにアクセスするための外部要求を受信したか否かを判定できる（ステップ 304）。外部要求は、要求元機器 106 から発生することもある。

10

【0048】

センサー機器 104 はこのような要求を受信しない場合、要求を受信するまでループし続ける。或いは、センサー機器はこのような要求を受信しない場合、要求元機器 106 が第 1 センサー収集可能データを受信する認証を受けているか否かを判定する（ステップ 306）。センサー機器 104 は、ローカルに格納されたリスト又は例えばメモリ 210 に格納されたその他のデータ構造を調べることにより、この判定ができる。

【0049】

この代わり又はこれに追加して、センサー 104 は、認証ホスト 110 に要求を送信して、要求元機器 106 が第 1 センサー収集可能データにアクセスするための認証を受けているか否かを判定する。認証ホスト 110 の方が処理パワーと記憶装置が大きい可能性があるため、要求元機器 106 の認証に用いると有利であるかもしれない。これは要求元機器 106 の認証に追加パラメータを使用することを可能にし得る。また、要求元機器 106 を認証するために用いるデータを認証ホスト 110 を使って更新するか、又はそうするために、第三者からの異なる種類のデータを追加する方がより容易になるかもしれない。

20

【0050】

要求元機器 106 が第 1 センサー収集可能データを受信するための認証を受けていない場合、センサー機器 104 は要求元機器 106 による第 1 センサー収集可能データへのアクセスを禁止でき（ステップ 308）、その後、例示的な方法 300 が終了できる。或いは要求元機器が第 1 センサー収集可能データを受信する認証を受けていた場合は、センサー機器 104 は、入出力部 212 を使って、第 1 センサー収集可能データを要求元機器 106 に送信でき（ステップ 310）、その後、例示的な方法 300 は終了できる。

30

【0051】

図 4 は、要求元機器 106 を認証するために使われる表 400 の例である。表 400 はセンサー機器 104 のメモリ 210 に格納され得る。或いは、表 400 は特定の実施形態又はその他の場所において認証ホスト 110 に格納され得る。

【0052】

一つの例示的な構成において、表 400 は列 402 及び 404 を含む。列 402 は、要求元機器と関連付けられた既知の要求元機器又はその他の識別子を一覧表示する。例えば、列 402 は、要求元機器がその機器自身を認証する目的に使用することのできるキーのリストを含んでもよい。代わりに、列 402 は要求元機器の MAC アドレスを一覧表示することもできる。列 402 はまた、範囲、機器の種類又はその他のより汎用的な識別子を一覧表示してもよい。当業者は、様々な静的識別子又は動的識別子が要求元機器の認証の目的に使用され得ることを理解するであろう。

40

【0053】

表 400 の列 404 は、特定の機器が認証される対象となる異なるセンサー収集可能データのリストを含む。例えば、行 406 は、機器 A が温度、湿度、音声、動画及び動作に関するデータを受信することを許可されることを述べている。したがって、要求元機器 106 は、一つ以上のこれらの種類のセンサー収集可能データをセンサー機器 104 から要求するとき、要求元機器 106 はそれらを受信することを認証される。同様に、行 408

50

は、機器Bが温度及び動画に関するデータを受信することを許可されることを述べている。しかしながら、行410は、機器Cがいかなる種類のセンサー収集可能データも受信することを許可されていないと述べている。当業者は、表400が、要求元機器106がどのように認証され得るかの例に過ぎず、限定するものでないことを理解するであろう。代わりに、要求元機器106はアルゴリズム又は異なるデータ構造に基づいて認証されてもよい。

【0054】

図5は、要求元機器106が複数の種類のセンサー収集可能データを要求するときに、センサー収集可能データをセンサー機器104から要求元機器106に送信するための例示的な方法500の操作のフローチャートである。方法500はセンサー機器104上の様々な構成要素によって実行され得る。方法500は、また、任意の他の機器によっても、又はシステム100又はブロック図200に示されていない機器も含め、任意の他の機器との組合せによって実行されてもよい。一部の構成においては、方法500のステップのいくつかは省略可能であるか、又は並べ替えが可能である。さらに、追加のステップを方法500に追加することも可能である。

10

【0055】

センサー機器104は、入出力部212を使って、複数の種類のセンサー収集可能データへのアクセス要求を受信し得る(ステップ502)。例えば、センサー機器104は、要求元機器106が温度、音声、動画及び湿度データを要求したことを判定できる。センサー機器104は、次に、CPU208を使って、要求元機器106が要求されたデータのどれに対しても認証されないのかを判定できる(ステップ504)。一部の実施形態においては、センサー機器は表400を参照して、この判定ができる。

20

【0056】

センサー機器104は、要求元機器106が要求されたセンサー収集可能データのどれに対しても認証されないと判定した場合、センサー機器104は、CPU208を使って、要求されたセンサー収集可能データへのアクセスを禁止できる(ステップ506)。例えば、センサー機器104は、要求元機器106が要求された温度、音声、動画及び湿度のデータにアクセスすることを禁止できる。

【0057】

代わりに、センサー機器104は、要求元機器106が要求されたセンサー収集可能データの少なくともいくつかに対して認証されると判定した場合、センサー機器104は、CPU208を使って、要求元機器106が要求されたデータのすべてに対して認証されるのかを判定できる(ステップ508)。要求元センサー106が要求されたデータのすべてに対して認証される場合、センサー機器104は、要求されたすべてのデータを要求元機器106に送信でき(ステップ510)、その後、方法500は終了する。例えば、センサー機器104は、要求された温度、音声、動画及び湿度のデータを要求元機器106に送信できる。

30

【0058】

代わりに、センサー機器104が要求元機器106は要求されたデータのすべてに対しては認証されないと判定した場合、これは要求元機器106が要求されたセンサー収集可能データのサブセット(subset)のみに対して認証されることを意味し得る。例えば、要求元機器106は、温度と動画データを受信することは認証されるが、音声と湿度データを受信することは認証されないこともあり得る。このシナリオでは、センサー機器104は、CPU208を使って、要求元機器106が要求されたデータのサブセットのみを受け付けるか否かを判定できる(ステップ516)。例えば、センサー機器104は、要求元機器106が、その要求の部分的な充足を受け付けるか否か、即ち、要求した温度と動画データは受信できるが、要求した音声と湿度データは受信できないことを判定できる。要求元機器106は、部分的な充足を受け付けるか否かの一般的なポリシーを備えている可能性があり、それをセンサー機器104が認識している場合もあり得る。代わりに、要求元機器106は、その要求の特定の部分的な充足を受け付けるか否かについて、

40

50

ケースバイケースで判定することもできる。

【 0 0 5 9 】

一部の実施形態においては、要求元機器 1 0 6 が要求したデータの部分的な充足を受け付けるか否かを判定する代わりに、センサー機器 1 0 4 は、条件付きで、その要求を拒否できる。例えば、センサー機器 1 0 4 は、要求されたデータの一部が要求元機器 1 0 6 に対して認証されないため、要求元機器 1 0 6 に、その要求は完全に拒否されたことを通知することもできる。このようにすると、要求元機器 1 0 6 は、恐らくは必要とするより優先度の高いデータに対して、追加の要求を出すこともあり得る。代わりに、要求元機器 1 0 6 は、そのアクセスを拒否する条件が変更された場合に備え、再びチェックすることもできる。

10

【 0 0 6 0 】

センサー機器 1 0 4 は、要求元機器 1 0 6 がその要求のサブセットのみを受け付けるか否かを判定する場合、センサー機器 1 0 4 は、入出力部 2 1 2 を使って、要求元機器 1 0 6 に対して認証される要求されたデータのみを送信する（ステップ 5 1 4）。例えば、センサー機器 1 0 4 は、要求元機器に対し、要求された温度と動画データは送信するが、要求された音声と湿度データは送信しないようにできる。代わりに、センサー機器 1 0 4 は、要求元機器 1 0 6 がその要求のサブセットのみでは受け付けないと判定した場合は、センサー機器 1 0 4 は、要求されたセンサー収集可能データのすべてに対するアクセスを拒否し（ステップ 5 1 6）、その後、方法 5 0 0 は終了する。

【 0 0 6 1 】

20

図 6 は、要求元機器 1 0 6 により提供されたルーティング情報に従って、センサー機器 1 0 4 から目的地にセンサー収集可能データを送信するための例示的な方法 6 0 0 の操作のフローチャートである。方法 6 0 0 は、センサー機器 1 0 4 内の様々な構成要素によって実行され得る。方法 6 0 0 は、また、任意の他の機器によっても、又はシステム 1 0 0 又はブロック図 2 0 0 に示されていない機器も含め、任意の他の機器との組合せによって実行されてもよい。一部の構成においては、方法 6 0 0 のステップのいくつかは省略可能であるか、又は並べ替えが可能である。さらに、追加のステップを方法 6 0 0 に追加することも可能である。

【 0 0 6 2 】

センサー機器 1 0 4 は、検出装置 2 0 6 を使って、第 1 センサー収集可能データを収集できる（ステップ 6 0 2）。続いて、センサー機器 1 0 4 は、第 1 センサー収集可能データへのアクセス要求を、入出力部 2 1 2 を介して、要求元機器 1 0 6 から受信することがあり得る（ステップ 6 0 4）。要求はルーティング情報を含み得る。ルーティング情報は、センサーデータホスト 1 1 2 等の第 1 センサー収集可能データの目的地を表すことができる。一部の実施形態においては、要求元機器 1 0 6 は、第 1 センサー収集可能データの格納及び／又は処理を許可しない位置にあってもよい。例えば、要求元機器 1 0 6 は、特定の種類の音声及び／又は動画情報の格納を禁止する国に存在し得る。したがって、要求元機器 1 0 6 は、センサー機器 1 0 4 に第 1 センサー収集可能データを、センサーデータホスト 1 1 2 等の別の位置に提供するように指示してもよい。センサーデータホスト 1 1 2 は、第 1 センサー収集可能データの格納及び／又は処理に制約のない位置に存在し得る。

30

40

【 0 0 6 3 】

一部の実施形態においては、ルーティング情報は、ネットワーク内の混雑を克服する役目を果たせる。例えば、要求元機器 1 0 6 は、ネットワークの特定部分が混雑していることを認識して、センサー機器 1 0 4 に、第 1 センサー収集可能データを、ネットワーク内の異なるルートを経由して送信するように指示できる。このような指示は、要求元機器 1 0 6 がセンサー機器 1 0 4 に送信することのできるルーティング情報の中にあってもよい。

【 0 0 6 4 】

要求を受信した後、センサー機器 1 0 4 は、要求元機器 1 0 6 が第 1 センサー収集可能データを受信、要求又はアクセスするための認証を受けているか否かを判定できる（ステ

50

ップ606)。代わりに又は追加的に、センサー機器104は、センサーデータホスト112が第1センサー収集可能データを受信、要求又はアクセスする認証を受けているか否かを判定できる。要求元機器106及び/又はセンサーデータホスト112が認証されない場合、センサー機器104は、第1センサー収集可能データへのアクセスを禁止でき(ステップ608)、その後、方法600は終了できる。

【0065】

代わりに、要求元機器106及び/又はセンサーデータホスト112が認証される場合、センサー機器104は、入出力部212を使って、ルーティング情報に従って、第1センサー収集可能データを送信でき(ステップ610)、その後、方法600は終了できる。例えば、センサー機器104は、第1センサー収集可能データをセンサーデータホスト112にルーティングしてもよい。そして、一部の実施形態においては、センサー機器104は、ネットワークの混雑を避けるために、第1センサー収集可能データをルーティングできる。

【0066】

図7は、特定のセンサー収集可能データが特定の値又は特定の範囲に関連付けられている場合に、センサー収集可能データをセンサー機器104から要求元機器106に送信するための例示的な方法700の操作のフローチャートである。方法700は、センサー機器104上の様々な構成要素によって実行され得る。方法700は、また、他の機器によって、又は、システム100若しくはブロック図200に表示されていない機器も含め、任意の他の機器との組合せによって実行されてもよい。一部の構成では、方法700のステップのいくつかは省略可能であるか、又は並べ替えが可能である。さらに、追加のステップを方法700に追加することも可能である。

【0067】

開示された実施形態は、第2センサー収集可能データの値に応じて、第1センサー収集可能データへのアクセスを禁止することに関係し得る。例えば、要求元機器106は、センサー機器104からの第1センサー収集可能データ、例えば、温度データを要求することもあり得る。要求元機器106は、温度データを受信する認証を受けているかもしれない。しかしながら、要求元機器106は、その独自の第2センサー収集可能データ、例えばGPS位置情報等を収集することを可能にする検出部206を含んでいることもあり得る。センサー機器104は、この第2センサー収集可能データ(例えば、位置情報)を解析して、要求元機器106が温度情報の格納又はアクセスを行うことを禁止するルールを持つ管轄区域に位置している可能性があることを判断できる。したがって要求元機器106は第1センサー収集可能データ(例えば、温度)にアクセスすることを認証されるかもしれないが、センサー機器104は、第2センサー収集可能データ(例えば、要求元機器106の位置)が所定値(例えば、温度データの収集を禁止する管轄区域)に関連付けられているという理由で、アクセスを禁止できる。

【0068】

一部の実施形態においては、第2センサー収集可能データは、また、センサー機器102で収集されることもあり得る。例えば、第2センサー収集可能データは、センサー機器102で収集された第1センサー収集可能データと同様又は同一である。一部の実施形態においては、特定の当事者は第1センサー収集可能データが特定の範囲を超える場合、第1センサー収集可能データを共有することを望まないかもしれない。例えば運送会社は、温度データが危険範囲にある場合を除き、温度データの報告を必要としないかもしれない。したがって、要求元機器106が、第1センサー収集可能データ(例えば、温度データ)にアクセスすることを認証されていても、センサー機器104は、それが所定範囲にないことを理由にこのデータをアクセス可能にしないこともあり得る。

【0069】

代わりに、第2センサー収集可能データがセンサー機器102によって収集されることもあり得るが、第1センサー収集可能データとは異なる可能性がある。例えば、運送会社は、湿度レベルが一定の範囲内にある場合を除き、温度の公表又は報告を必要としないか

10

20

30

40

50

もしれない。この例では、湿度レベルも一定の範囲内にある場合を除き、温度データは意味がないか、又は重要でないかもしれない。このような状況では、要求元機器 106 は、第 1 センサー収集可能データ（例えば、温度）を受信することを認証されているが、センサー機器 104 は、第 2 センサー収集可能データ（例えば、湿度）が所定範囲にないことを理由にこのデータをアクセス可能にしないこともあり得る。

【0070】

再び図 7 を参照すると、センサー機器 104 は、検出装置 206 を使って、第 1 センサー収集可能データを収集できる（ステップ 702）。次に、センサー機器 104 は、要求元機器 106 から、第 1 センサー収集可能データにアクセスする要求を受信することもある（ステップ 704）。センサー装置はこのような要求を受信しなかった場合、このような要求を受信するまでチェックを続けることができる。代わりに、センサー機器 104 はこの要求を受信した場合は、CPU 208 を使って、要求元機器が第 1 センサー収集可能データを受信する認証を受けているか否かを判定できる（ステップ 706）。10

【0071】

要求元機器 106 が認証を受けていない場合、センサー機器 104 は、CPU 208 を使って、要求元機器 106 による第 1 センサー収集可能データへのアクセスを禁止でき（ステップ 710）、その後、方法 700 は終了できる。代わりに、要求元機器 106 が認証された場合、センサー機器 104 は、第 2 センサー収集可能データが所定値又は所定範囲に等しいか又はそうでなければ関連付けられているかを CPU 208 を使って判定できる（ステップ 708）。第 2 センサー収集可能データが、所定値 / 所定範囲と関連付けられている場合、センサー機器 104 は、要求元センサー 106 による第 1 センサー収集可能データへのアクセスを、CPU 208 を使って禁止でき（ステップ 710）、その後、方法 700 は終了できる。20

【0072】

代わりに、第 2 センサー収集可能データが所定値又は所定範囲と関連付けられていない場合、センサー機器 104 は、要求元機器 106 に第 1 センサー収集可能データへのアクセスを、入出力部 212 を使って許可でき（ステップ 712）、その後、方法 700 は終了できる。例えば、センサー機器 104 は、第 2 センサー収集可能データを要求元機器 106 に送信できる。30

【0073】

本発明の一定の特徴及び実施形態を記述してきたが、本発明の他の実施形態も、本明細書で開示された実施形態の明細書及び実践を考慮することから、本発明の他の実施形態も当業者には明白になるであろう。さらに、本発明の実施形態の態様を、メモリ及びその他の記憶媒体に格納したソフトウェア、コンピュータ実行可能命令、及び / 又はその他のデータとして、部分的には記述してきたが、当業者は、これらの態様が他の種類の有形の持続性のコンピュータ読み取り可能な媒体、例えば、ハードディスク、フロッピー（登録商標）ディスク若しくは CD-ROM、又はその他の形態の RAM 若しくは ROM のようなセカンダリー記憶装置等に記憶又はそれらから読み取ることも可能であることを理解するであろう。さらに、開示した方法のステップは、ステップの並べ替え及び / 又はステップの挿入又は削除を含め、様々な方法で、本発明の原理から逸脱することなく、改変することができ得る。40

【0074】

本明細書及び例は、例示の目的のみであるとみなされることを目的としており、本発明の真の範囲及び精神は以下の特許請求の範囲によって示される。

【図 1】

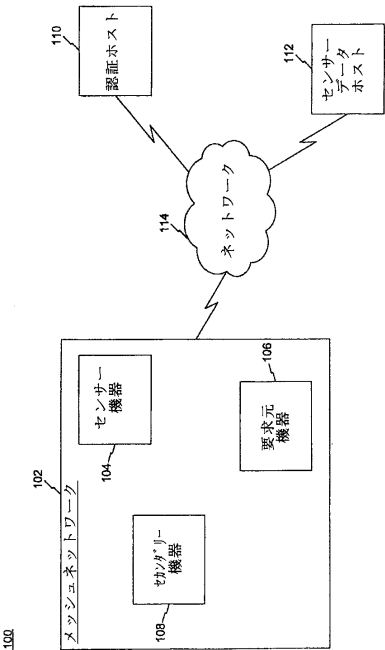


図 1

【図 2】

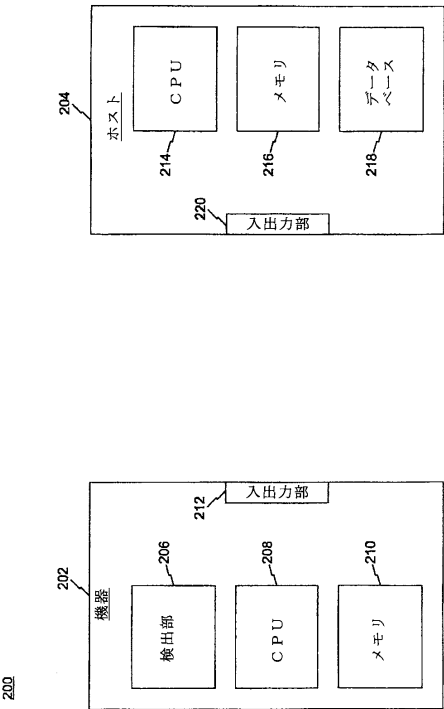


図 2

【図 3】

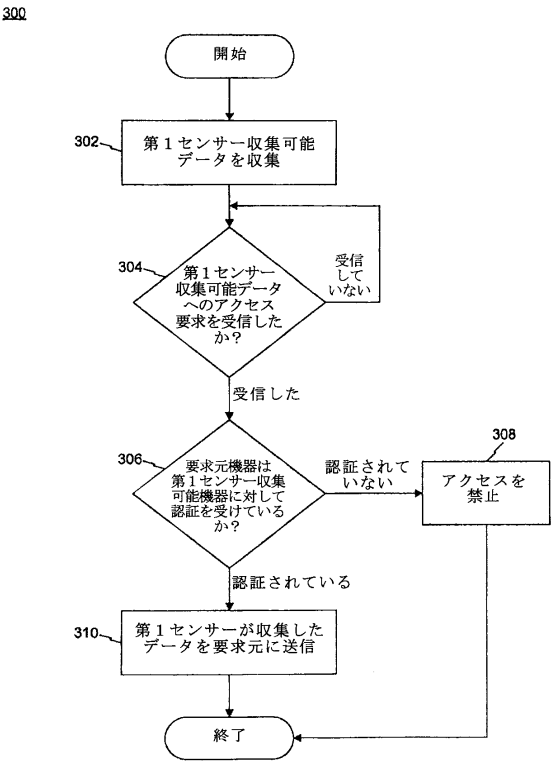


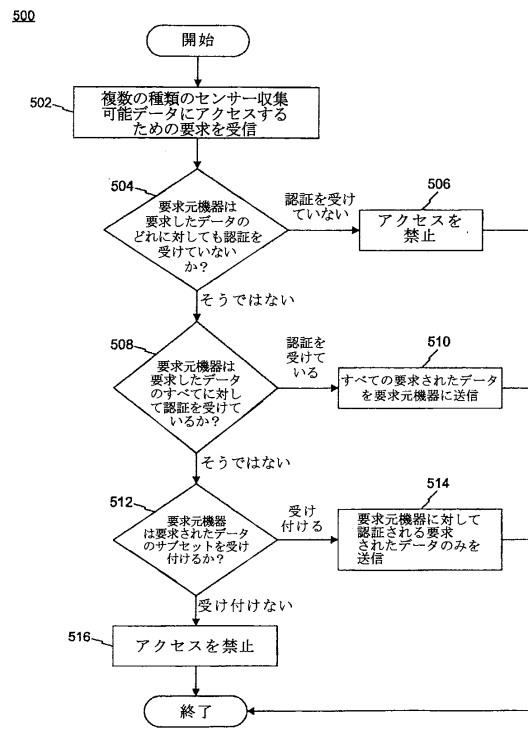
図 3

【図 4】

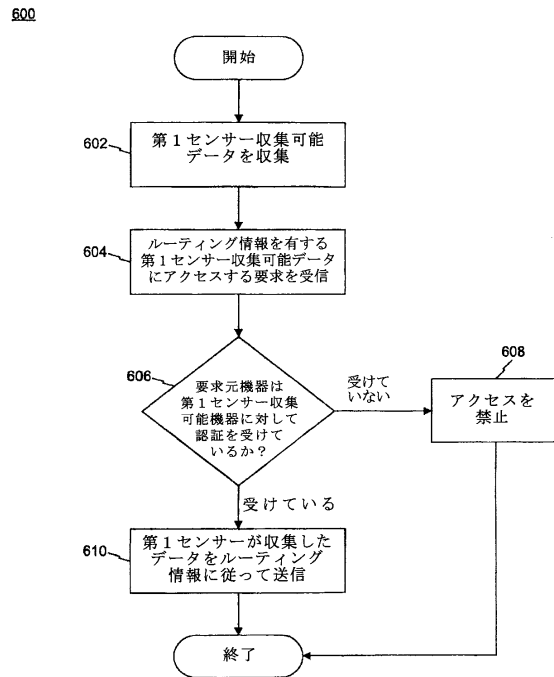
400	
機器	認証されたセンサー情報
406 機器 A	温度、湿度、音声、動画、動作
408 機器 B	温度、動画
410 機器 C	なし
⋮	⋮

図 4

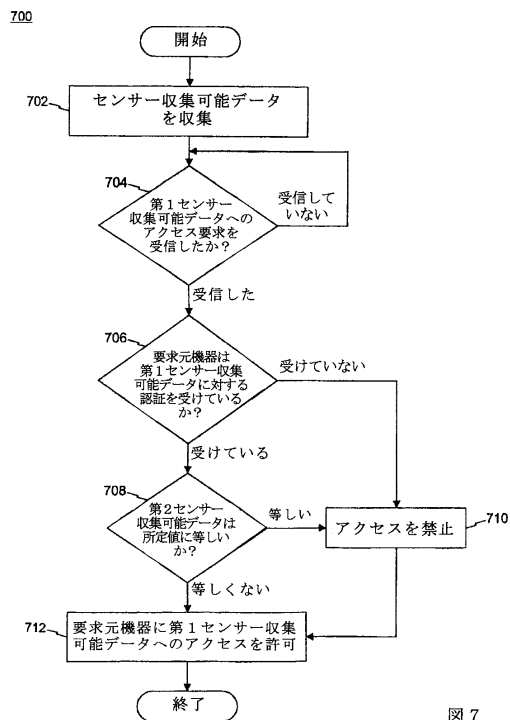
【図 5】



【図 6】



【図 7】



フロントページの続き

(74)代理人 100151459

弁理士 中村 健一

(74)代理人 100190632

弁理士 山 崎 誠也

(72)発明者 オレ - ペーター スカークスルド

アメリカ合衆国, テネシー 38002, レイクランド, イースト ファー ヒル ドライブ 4
114

(72)発明者 マイリー エインズワース

アメリカ合衆国, ミシシッピ 38632, ヘルナンド, タラ ドライブ 1814

審査官 望月 章俊

(56)参考文献 特開2007-323391(JP, A)

特開2006-157635(JP, A)

特表2005-539409(JP, A)

国際公開第2006/071501(WO, A2)

米国特許出願公開第2008/0083022(US, A1)

(58)調査した分野(Int.Cl., DB名)

H04W4/00 - H04W99/00

H04B7/24 - H04B7/26