

(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2016-514399
(P2016-514399A)

(43) 公表日 平成28年5月19日(2016.5.19)

(51) Int.Cl.	F 1	HO 4 L	9/00	601 B	テーマコード (参考)
HO4L 9/08	(2006.01)	HO4L	9/00	601 B	5C087
HO4M 11/04	(2006.01)	HO4M	11/04		5J104
HO4W 4/22	(2009.01)	HO4W	4/22		5K067
HO4W 12/04	(2009.01)	HO4W	12/04		5K201
G08B 25/04	(2006.01)	G08B	25/04	G	

審査請求 未請求 予備審査請求 有 (全 31 頁)

(21) 出願番号	特願2015-559267 (P2015-559267)	(71) 出願人	507364838 クアルコム、インコーポレイテッド
(86) (22) 出願日	平成26年2月25日 (2014. 2. 25)		アメリカ合衆国 カリフォルニア 921 21 サン デイエゴ モアハウス ドラ イブ 5775
(85) 翻訳文提出日	平成27年8月20日 (2015. 8. 20)	(74) 代理人	100108453 弁理士 村山 靖彦
(86) 國際出願番号	PCT/US2014/018313	(74) 代理人	100163522 弁理士 黒田 晋平
(87) 國際公開番号	W02014/131009	(72) 発明者	アミット・ゴエル アメリカ合衆国・カリフォルニア・921 21-1714・サン・ディエゴ・モアハ ウス・ドライブ・5775
(87) 國際公開日	平成26年8月28日 (2014. 8. 28)		
(31) 優先権主張番号	61/769,115		
(32) 優先日	平成25年2月25日 (2013. 2. 25)		
(33) 優先権主張国	米国 (US)		
(31) 優先権主張番号	14/187,978		
(32) 優先日	平成26年2月24日 (2014. 2. 24)		
(33) 優先権主張国	米国 (US)		

最終頁に続く

(54) 【発明の名称】 IoTデバイスのための緊急モード

(57) 【要約】

信頼された機関のソースからの緊急メッセージに基づいて緊急命令を実施するための方法および装置。方法は、モノのインターネット(IoT)デバイスにおいて、信頼された機関のソースから緊急秘密鍵を受信するステップを含む。方法は、IoTデバイスにおいて、信頼された機関のソースから緊急メッセージを受信し、IoTデバイスにおいて、緊急秘密鍵を使用して信頼された機関のソースからの緊急メッセージを復号して緊急メッセージ内の値を判定する。方法は、IoTデバイスにおいて、判定された値に基づいて結果を計算する。方法は、IoTデバイスにおいて、結果が所定の閾値を超える場合に緊急命令を実施する。

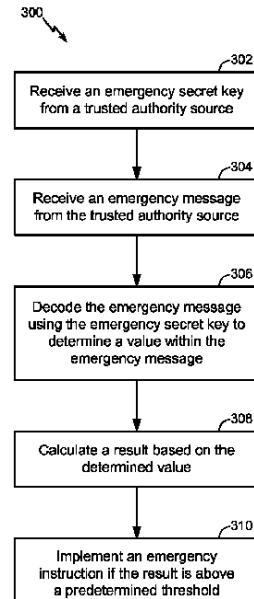


FIG. 3

【特許請求の範囲】**【請求項 1】**

信頼された機関のソースからの緊急メッセージに基づいて緊急命令を実施するための方法であって、

モノのインターネット(IoT)デバイスにおいて、信頼された機関のソースからIoT秘密鍵を受信するステップと、

IoTデバイスにおいて、前記信頼された機関のソースからの緊急メッセージを受信するステップであって、前記緊急メッセージが、緊急秘密鍵を含む、ステップと、

IoTデバイスにおいて、前記IoT秘密鍵を使用して前記信頼された機関のソースからの前記緊急メッセージを復号して前記緊急メッセージ内の値を判定するステップと、

IoTデバイスにおいて、前記判定された値に基づいて結果を計算するステップと、

IoTデバイスにおいて、前記結果が所定の閾値を超える場合に緊急命令を実施するステップと

を含む、方法。

【請求項 2】

異なるIoT秘密鍵が、前記IoTデバイスに周期的に送信される請求項1に記載の方法。

【請求項 3】

前記IoT秘密鍵が、第2の信頼された機関のソースから確認される請求項1に記載の方法。

【請求項 4】

IoTデバイスにおいて、

次の物、すなわち、前記IoTデバイス、同じLAN上の別のIoTデバイス、および前記同じLAN上の非IoTデバイスのうちの少なくとも1つからのデータを確かめるステップと、

確かめられたデータと一緒に前記値を変数として式に組み込むステップと

をさらに含む請求項1に記載の方法。

【請求項 5】

前記緊急命令が、以下の物、すなわち、停止命令、始動命令、出力増加命令、出力削減命令、および警報命令のうちの少なくとも1つを含む請求項1に記載の方法。

【請求項 6】

前記緊急メッセージが、2つ以上のIoTデバイスへのブロードキャスト/マルチキャスト/ユニキャストメッセージである請求項1に記載の方法。

【請求項 7】

前記緊急メッセージが、ネットワークに固有である請求項6に記載の方法。

【請求項 8】

前記緊急命令が、少なくとも1つの非IoTデバイスに送信される請求項1に記載の方法。

【請求項 9】

前記緊急秘密鍵が、前記IoT秘密鍵で暗号化される請求項1に記載の方法。

【請求項 10】

IoTデバイスにおいて、グローバルなIoTの語彙を使用して前記緊急メッセージを解釈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 11】

IoTデバイスにおいて、外部ソースからオーバーライド命令を受信するステップと、

IoTデバイスにおいて、前記オーバーライド命令に基づいて前記緊急命令を無効にするステップと

をさらに含む請求項1に記載の方法。

【請求項 12】

前記オーバーライド命令が、前記信頼された機関のソースからのものである請求項11に記載の方法。

【請求項 13】

日常的なデバイスが、前記緊急命令を実施しながら緊急モードで動作する請求項1に記

10

20

30

40

50

載の方法。

【請求項 1 4】

命令が実施される度合いが、前記判定された値に基づく請求項1に記載の方法。

【請求項 1 5】

前記緊急メッセージが、次の物、すなわち、緊急事態のレベル、前記緊急メッセージを発する機関のレベル、前記緊急事態の予想される継続時間、実行すべき推薦される全般的な行為、肯定応答の要求、ユーザの認可の要求、および応答の要求のうちの少なくとも1つを含み得る請求項1に記載の方法。

【請求項 1 6】

前記IoTデバイスが、前記信頼された機関のソースに応答メッセージを送信する請求項1に記載の方法。 10

【請求項 1 7】

前記IoTデバイスが前記信頼された機関のソースに提供する情報が、リソースを実装することを助ける請求項16に記載の方法。

【請求項 1 8】

前記緊急メッセージが、前記IoTデバイスへの前記緊急メッセージの優先ルーティングを可能にするためのサービス品質パラメータを含む請求項1に記載の方法。

【請求項 1 9】

信頼された機関のソースからの緊急メッセージに基づいて緊急命令を実施するように構成されたプロセッサと、 20

信頼された機関のソースからIoT秘密鍵を受信するように構成された論理手段と、

前記信頼された機関のソースからの緊急メッセージを受信するように構成された論理手段であって、前記緊急メッセージが、緊急秘密鍵を含む、論理手段と、

前記IoT秘密鍵を使用して前記信頼された機関のソースからの前記緊急メッセージを復号して前記緊急メッセージ内の値を判定するように構成された論理手段と、

前記判定された値に基づいて結果を計算するための論理手段と、

前記結果が所定の閾値を超える場合に緊急命令を実施するための論理手段とを含む装置。

【請求項 2 0】

異なるIoT秘密鍵が、前記IoTデバイスに周期的に送信される請求項19に記載の装置。 30

【請求項 2 1】

前記IoT秘密鍵が、第2の信頼された機関のソースから確認される請求項19に記載の装置。 。

【請求項 2 2】

次の物、すなわち、前記IoTデバイス、同じLAN上の別のIoTデバイス、および前記同じLAN上の非IoTデバイスのうちの少なくとも1つからのデータを確かめるように構成された論理手段と、

確かめられたデータと一緒に前記値を変数として式に組み込むように構成された論理手段と

をさらに含む請求項19に記載の装置。 40

【請求項 2 3】

前記緊急命令が、少なくとも1つの非IoTデバイスに送信される請求項19に記載の装置。

【請求項 2 4】

前記緊急秘密鍵が、前記IoTデバイスの秘密鍵で暗号化される請求項19に記載の装置。

【請求項 2 5】

外部ソースからオーバーライド命令を受信するように構成された論理手段と、前記オーバーライド命令に基づいて前記緊急命令を無効にするように構成された論理手段と

をさらに含む請求項19の装置。

【請求項 2 6】

50

前記外部ソースが、前記信頼された機関のソースである請求項25に記載の装置。

【請求項 27】

命令が実施される度合いが、前記判定された値に基づく請求項19に記載の装置。

【請求項 28】

前記緊急メッセージが、次の物、すなわち、緊急事態のレベル、前記緊急メッセージを発する機関のレベル、前記緊急事態の予想される継続時間、実行すべき推薦される全般的な行為、肯定応答の要求、ユーザの認可の要求、および応答の要求のうちの少なくとも1つを含み得る請求項19に記載の装置。

【請求項 29】

信頼された機関のソースが緊急メッセージを送信するための方法であって、

IoT秘密鍵を外部ソースから受信するステップと、

前記信頼された機関のソースから少なくとも1つのIoTデバイスに前記IoT秘密鍵を送信するステップと、

前記外部ソースから緊急秘密鍵を受信するステップであって、前記緊急メッセージが、緊急秘密鍵を含む、ステップと、

前記信頼された機関のソースから前記少なくとも1つのIoTデバイスのサブセットに緊急メッセージを送信するステップであって、前記緊急メッセージが、前記秘密鍵を含む、ステップと

を含む、方法。

【請求項 30】

IoTデバイスに緊急メッセージを送信するように構成されたプロセッサと、

IoT秘密鍵を受信するように構成された論理手段と、

少なくとも1つのIoTデバイスに前記IoT秘密鍵を送信するように構成された論理手段と

、緊急メッセージを受信するように構成された論理手段であって、前記緊急メッセージが、緊急秘密鍵を含む、論理手段と、

前記少なくとも1つのIoTデバイスのサブセットに前記緊急メッセージを送信するように構成された論理手段と

を含む装置。

【発明の詳細な説明】

【技術分野】

【0001】

本出願は、本出願の譲受人に譲渡され、参照によりその全体が本明細書に明示的に組み込まれている、2013年2月25日に出願した「EMERGENCY MODE FOR IOE DEVICES」と題した米国仮出願第61/769,115号の利益を主張するものである。

【0002】

本開示は、信頼された機関のソース(trusted authority source)からの緊急メッセージに基づいて緊急命令を実施することを対象とする。

【背景技術】

【0003】

インターネットは、互いに通信するために標準的なインターネットプロトコルスイート(たとえば、伝送制御プロトコル(TCP)およびインターネットプロトコル(IP))を用いる相互に接続されたコンピュータおよびコンピュータネットワークの全世界的システムである。モノのインターネット(IoT)は、コンピュータおよびコンピュータネットワークだけでなく日常的な物体(everyday object)がIoT通信ネットワーク(たとえば、アドホックシステムまたはインターネット)を介して読み取り可能、認識可能、位置特定可能、アドレス指定可能、および制御可能であるという考えに基づく。

【0004】

いくつかの市場の流れが、IoTデバイスの開発を促している。たとえば、上昇しているエネルギーコストが、スマートグリッド、ならびに電気自動車および公共の充電ステーション

10

20

30

40

50

ヨンなどの未来の消費のサポートへの政府の戦略的投資を促している。上昇している健康管理のコストおよび高齢化が、遠隔/ネットワーク接続型健康管理およびフィットネスサービスの開発を促している。家庭向けの技術革新が、サービスプロバイダが「N」プレイ('N' play)(たとえば、データ、音声、映像、セキュリティ、エネルギー管理など)を売り出し、ホームネットワークを拡大することによる整理統合を含む新しい「スマート」デバイスの開発を促している。建物は、企業の設備の運用コストを削減するための手段としてよりスマートでより便利になりつつある。

【0005】

IoTに関するいくつかの重要な応用がある。たとえば、スマートグリッドおよびエネルギー管理の領域では、公益事業会社が、家庭および企業へのエネルギーの送達を最適化することができる一方、顧客が、エネルギーの使用をより適切に管理することができる。家および建物のオートメーションの領域では、スマートホームおよびビルディングが、家庭または事業所で、電化製品からプラグイン電気自動車(PEV)のセキュリティシステムまで実質的に任意のデバイスまたはシステムを集中的に制御することができる。資産追跡(asset tracking)の分野では、企業、病院、工場、およびその他の大きな組織が、価値の高い機器、患者、車両などの位置を性格に追跡することができる。健康およびウェルネスの領域では、医者が、患者の健康を遠隔で監視することができる一方、人が、フィットネスルーチンの経過を追跡することができる。

10

【発明の概要】

【課題を解決するための手段】

20

【0006】

本開示は、信頼された機関のソースからの緊急メッセージに基づいて緊急命令を実施することを対象とする。

【0007】

たとえば、例示的な実施形態は、信頼された機関のソースからの緊急メッセージに基づいて緊急命令を実施するための方法であって、モノのインターネット(IoT)デバイスにおいて、信頼された機関のソースからIoT秘密鍵(IoT secret key)を受信するステップと、IoTデバイスにおいて、信頼された機関のソースからの緊急メッセージを受信するステップであって、緊急メッセージが、緊急秘密鍵(emergency secret key)を含む、ステップと、IoTデバイスにおいて、IoT秘密鍵を使用して信頼された機関のソースからの緊急メッセージを復号して緊急メッセージ内の値を判定するステップと、IoTデバイスにおいて、判定された値に基づいて結果を計算するステップと、IoTデバイスにおいて、結果が所定の閾値を超える場合に緊急命令を実施するステップとを含む、方法を対象とする。

30

【0008】

別の例示的な実施形態は、信頼された機関のソースからの緊急メッセージに基づいて緊急命令を実施するように構成されたプロセッサと、信頼された機関のソースからIoT秘密鍵を受信するように構成された論理と、信頼された機関のソースからの緊急メッセージを受信するように構成された論理であって、緊急メッセージが、緊急秘密鍵を含む、論理と、IoT秘密鍵を使用して信頼された機関のソースからの緊急メッセージを復号して緊急メッセージ内の値を判定するように構成された論理と、判定された値に基づいて結果を計算するための論理と、結果が所定の閾値を超える場合に緊急命令を実施するための論理とを含む装置を対象とする。

40

【0009】

さらに別の例示的な実施形態は、信頼された機関のソースが緊急メッセージを送信するための方法であって、IoT秘密鍵を外部ソースから受信するステップと、信頼された機関のソースから少なくとも1つのIoTデバイスにIoT秘密鍵を送信するステップと、外部ソースから緊急秘密鍵を受信するステップであって、緊急メッセージが、緊急秘密鍵を含む、ステップと、信頼された機関のソースから少なくとも1つのIoTデバイスのサブセットに緊急メッセージを送信するステップであって、緊急メッセージが、秘密鍵を含む、ステップとを含む、方法を対象とする。

50

【0010】

さらに別の例示的な実施形態は、IoTデバイスに緊急メッセージを送信するように構成されたプロセッサと、IoT秘密鍵を受信するように構成された論理と、少なくとも1つのIoTデバイスにIoT秘密鍵を送信するように構成された論理と、緊急メッセージを受信するように構成された論理であって、緊急メッセージが、緊急秘密鍵を含む、論理と、少なくとも1つのIoTデバイスのサブセットに緊急メッセージを送信するように構成された論理とを含む装置を対象とする。

【0011】

本開示のいくつかの利点は、公共の安全を保証し、被害を最小化するために、信頼された機関(たとえば、消防署、警察署、ガス会社)とIoTデバイスとの間の通信のシステムを提供することである可能性がある。通信は、自然のものと人為的なものとの両方の地震、火災、洪水、暴動、およびその他の災害を含む緊急事態の際に有益である可能性がある。

10

【0012】

本開示の態様およびそれに付随する利点のより完全な理解は、本開示の限定ではなく例示のためにだけに示される添付の図面に関連して考慮されるときに以下の詳細な説明を参照することによって本開示の態様およびそれに付随する利点がより深く理解されるようになるときに容易に得られるであろう。

【図面の簡単な説明】**【0013】**

【図1A】本開示の一態様によるワイヤレス通信システムの高レベルのシステムアーキテクチャを示す図である。

20

【図1B】本開示の一態様によるワイヤレス通信システムの高レベルのシステムアーキテクチャを示す図である。

【図1C】本開示の一態様によるワイヤレス通信システムの高レベルのシステムアーキテクチャを示す図である。

【図1D】本開示の一態様によるワイヤレス通信システムの高レベルのシステムアーキテクチャを示す図である。

【図1E】本開示の一態様によるワイヤレス通信システムの高レベルのシステムアーキテクチャを示す図である。

【図2A】本開示の態様による例示的なモノのインターネット(IoT)デバイスを示す図である。

30

【図2B】本開示の態様による例示的な受動的IoTデバイスを示す図である。

【図3】信頼された機関のソースからの緊急メッセージに基づいて緊急命令を実施するための方法の動作フローを示す図である。

【図4】信頼された機関のソースからの緊急メッセージに基づいて緊急命令を実施するように構成された論理を含む通信デバイスを示す図である。

40

【図5】IoTデバイスに緊急命令を送信するための例示的なサーバを示す図である。

【図6】IoTデバイスに緊急命令を送信するための方法の動作フローを示す図である。

【図7】デバイスに関する信頼された機関のソースからの緊急メッセージの情報を示す通信デバイスの表示を示す図である。

【発明を実施するための形態】**【0014】**

様々な態様が、以下の説明および関連する図面で開示される。代替的な態様が、本開示の範囲を逸脱することなく案出され得る。加えて、本開示のよく知られている要素は、本開示の重要な詳細を曖昧にしないように詳細に示されないかまたは省略される。

【0015】

語「例示的な」および/または「例」は、本明細書においては「例、具体例、または事例としての役割を果たす」ことを表すために使用される。本明細書で「例示的」および/または「例」と記載されたいずれの態様も、必ずしも他の態様よりも好ましいかまたは有利であると解釈されるべきでない。同様に、用語「本開示の態様」は、本開示のすべての

50

態様が検討される特徴、利点、または動作のモードを含むことを必要としない。

【0016】

さらに、多くの態様が、たとえば、コンピューティングデバイスの要素によって実行される一連の行為によって説明される。本明細書において説明される様々な行為が特定の回路(たとえば、特定用途向け集積回路(ASIC))、1つもしくは複数のプロセッサによって実行されるプログラム命令、またはこれら両方の組合せによって実行され得ることは、認められるであろう。加えて、本明細書において説明されるこれらの一連の行為は、実行されると関連するプロセッサに本明細書において説明される機能を実行させるコンピュータ命令の対応する組を記憶する任意の形態のコンピュータ可読ストレージ媒体内に完全に具現化されると考えられ得る。したがって、本開示の様々な態様は、いくつかの異なる形態で具現化される可能性があり、それらの異なる形態のすべては、特許請求の対象の範囲内にあると考えられた。さらに、本明細書において説明される態様のそれぞれに関して、対応する形態の任意のそのような態様は、たとえば、説明される行為を実行する「ように構成された論理」として本明細書において説明される可能性がある。

10

【0017】

本明細書において使用されるとき、用語「モノのインターネット(IoT)デバイス」は、中央演算処理装置(CPU)、マイクロプロセッサ、特定用途向け集積回路(ASIC)などに埋め込まれるおよび/または中央演算処理装置(CPU)、マイクロプロセッサ、特定用途向け集積回路(ASIC)などによって制御/監視され、ローカルアドホックネットワークもしくはインターネットなどのIoTネットワークに接続するように構成され得る特定の1組のデバイスの属性(たとえば、冷やすまたは暖める機能、環境を監視または記録する機能、光を発する機能、音を発する機能など)を有する電子デバイスを指すために使用される。たとえば、IoTデバイスは、デバイスがIoTネットワークと通信するための通信インターフェースを備えている限り、冷蔵庫、トースター、オーブン、電子レンジ、冷凍庫、食洗機、洗濯機、衣類乾燥機、炉、エアコン、サーモスタット、テレビ、照明設備、掃除機、電気メータ、ガスマーティなどを含み得るがこれらに限定されない。IoTデバイスは、セル電話、デスクトップコンピュータ、ラップトップコンピュータ、タブレットコンピュータ、携帯情報端末(PDA)なども含み得る。したがって、IoTネットワークは、通常、インターネット接続性を持たないデバイス(たとえば、食洗機など)に加えて「レガシーの」インターネットに接続可能なデバイス(たとえば、ラップトップまたはデスクトップコンピュータ、セル電話など)の組合せからなる可能性がある。

20

【0018】

「信頼された機関のソース」は、IoTデバイスに関するデータのソースである。たとえば、信頼された機関のソースは、サーバである可能性がある。個人または主体が、信頼された機関のソースに独占的にアクセスすることができる可能性がある。たとえば、個人は、市長、知事、会社の最高情報責任者、警察長、または消防長である可能性がある。主体は、地域の消防署、地域の警察署、エネルギー供給業者(たとえば、ガスまたは電力事業者)、森林局(Forest Service)、FEMA、国立気象局(National Weather Service)、国防総省、または国土安全保障省である可能性がある。

30

【0019】

これらの個人および主体は、それぞれが「外部ソース」として働く可能性がある。外部ソースは、安全なウェブインターフェースを通じて信頼された機関のソースに送信する可能性もある。一実施形態においては、個人が、信頼された機関のソースのデータを提供する可能性がある。個人は、IoTトークンを含むコマンドを手動で入力する可能性がある。個人は、データを提供するために、外付けメモリデバイス(たとえば、メモリスティック、外付けドライブ)を使用するか、または音声コマンドもしくはスキャンされる視覚的な物(たとえば、画像、網膜スキャン、バーコード、QRコード(登録商標))などの別のソースを提供する可能性がある。

40

【0020】

外部ソースからのこのデータは、「IoT秘密鍵」である。信頼された機関のソースは、I

50

IoTデバイスがメモリに記憶することができる緊急秘密鍵を送信し得る。緊急秘密鍵は、安全な送信、およびIoT秘密鍵が共有された信頼された機関(trusted authority)からその緊急秘密鍵が生じていることの証明のために上記のIoT秘密鍵を使用して暗号化される。それから、信頼された機関のソースは、緊急秘密鍵を含む緊急メッセージをIoTデバイスに送信することができる。IoTデバイスは、信頼されたソースから送信された緊急メッセージをそのIoTデバイスの記憶された緊急秘密鍵を使用して復号することができる。一部の実施形態において、信頼された機関のソースは、緊急メッセージをブロードキャスト/マルチキャスト/ユニキャストメッセージで複数のIoTデバイスに送信する可能性がある。たとえば、信頼された機関のソースは、天然ガスで動くデバイスなどの特定の種類のIoTデバイスのみに緊急メッセージを送信する可能性がある。信頼された機関のソースは、特定の都市のブロックなどの指定された領域内のIoTデバイスに緊急メッセージを送信する可能性もある。

10

【0021】

IoTデバイスは、緊急メッセージを復号すると、緊急メッセージに基づいて緊急命令を実施すべきかどうかを判定することができる。緊急命令は、停止命令または始動命令のような命令を含み得る。たとえば、オープンは、リヒタースケールで8.0以上のマグニチュードの地震が起きた場合、ガスを遮断する。一部の実施形態において、緊急命令は、出力を増やすまたは減らすことである可能性がある。たとえば、電力使用制限(rolling brown out)緊急メッセージに応答するために、緊急命令は、デバイスが70 °Fではなく80 °F未満の温度を保つように空調デバイスの出力を下げることがある可能性がある。緊急命令は、温度がその晩に下がるためにパイプが破裂することを防止するために熱が高められるべきであることの可聴警報をサーモスタッフがユーザに発するための命令などの警報命令を含む可能性がある。

20

【0022】

図1Aは、本開示の一態様によるワイヤレス通信システム100Aの高レベルのシステムアーキテクチャを示す。ワイヤレス通信システム100Aは、テレビ110、空調室外機112、サーモスタッフ114、冷蔵庫116、ならびに洗濯機および乾燥機118を含む複数のIoTデバイスを含む。

【0023】

図1Aを参照すると、IoTデバイス110～118は、図1Aにおいては無線インターフェース108および直接有線接続109として示される物理的な通信インターフェースまたはレイヤを介してアクセスネットワーク(たとえば、アクセスポイント125)と通信するように構成される。無線インターフェース108は、IEEE 802.11などのワイヤレスインターネットプロトコル(IP)に準拠する可能性がある。図1AはIoTデバイス110～118が無線インターフェース108を介して通信し、IoTデバイス118が有線接続109を介して通信するところを示すが、各IoTデバイスは、有線もしくは無線接続、またはこれら両方を介して通信する可能性がある。

30

【0024】

インターネット175は、(図1Aには便宜上示されていない)いくつかのルーティングエージェントおよび処理エージェントを含む。インターネット175は、異なるデバイス/ネットワーク間で通信するために標準的なインターネットプロトコルスイート(たとえば、伝送制御プロトコル(TCP)およびIP)を用いる相互に接続されたコンピュータおよびコンピュータネットワークの全世界的システムである。TCP/IPは、データがどのようにフォーマットされ、アドレス指定され、送信され、ルーティングされ、送信先で受信されるべきかを規定するエンドツーエンドの接続性を提供する。

40

【0025】

図1Aにおいて、デスクトップまたはパーソナルコンピュータ(PC)などのコンピュータ120は、(たとえば、イーサネット(登録商標)接続またはWi-Fiもしくは802.11に基づくネットワークを介して)インターネット175に直接接続するものとして示される。コンピュータ120は、モ뎀またはルータへの直接接続などのインターネット175への有線接続を有する可能性があり、モ뎀またはルータは、一例において、(たとえば、有線接続性とワイヤ

50

レス接続性との両方を有するWi-Fiルータの)アクセスポイント125自体に相当する可能性がある。代替的に、有線接続を介してアクセスポイント125およびインターネット175に接続されるのではなく、コンピュータ120は、無線インターフェース108または別のワイヤレスインターフェースを介してアクセスポイント125に接続され、無線インターフェースを介してインターネット175にアクセスする可能性がある。デスクトップコンピュータとして示されているが、コンピュータ120は、ラップトップコンピュータ、タブレットコンピュータ、PDA、スマートフォンなどである可能性がある。コンピュータ120は、IoTデバイスであり、および/またはIoTデバイス110～118のネットワーク/グループなどのIoTネットワーク/グループを管理するための機能を含む可能性がある。

【0026】

アクセスポイント125は、たとえば、FiOSなどの光通信システム、ケーブルモデム、デジタル加入者線(DSL)モデムなどを介してインターネット175に接続される可能性がある。アクセスポイント125は、標準的なインターネットプロトコル(たとえば、TCP/IP)を使用してIoTデバイス110～118/120およびインターネット175と通信し得る。

【0027】

図1Aを参照すると、IoTサーバ170は、インターネット175に接続されるものとして示される。IoTサーバ170は、複数の構造的に別々のサーバとして実装される可能性があり、または代替的に、単一のサーバに相当する可能性がある。一態様において、IoTサーバ170は、(破線によって示されるように)任意であり、IoTデバイス110～118/120のグループは、ピアツーピア(P2P)ネットワークである可能性がある。その場合、IoTデバイス110～118/120は、無線インターフェース108および/または有線接続109を介して互いに直接通信し得る。代替的にまたは追加的に、IoTデバイス110～118/120の一部またはすべては、無線インターフェース108および有線接続109とは独立した通信インターフェースを使用して構成される可能性がある。たとえば、無線インターフェース108がWiFiインターフェースに相当する場合、IoTデバイス110～118/120のうちの特定のものは、互いにまたはその他のBluetooth(登録商標)もしくはNFC対応デバイスと直接通信するためのBluetooth(登録商標)またはNFCインターフェースを有する可能性がある。

【0028】

ピアツーピアネットワークにおいては、サービス発見方式が、ノードの存在、それらのノードの能力、およびグループの加入者資格をマルチキャストする可能性がある。ピアツーピアデバイスは、この情報に基づいて関連付けおよびその後のインタラクションを確立し得る。

【0029】

本開示の態様によれば、図1Bは、複数のIoTデバイスを含む別のワイヤレス通信システム100Bの高レベルのアーキテクチャを示す。概して、図1Bに示されるワイヤレス通信システム100Bは、上でより詳細に説明された図1Aに示されたワイヤレス通信システム100Aと同じおよび/または実質的に同様である様々な構成要素(たとえば、無線インターフェース108および/または直接有線接続109を介してアクセスポイント125と通信するように構成されるテレビジョン110、空調室外機112、サーモスタット114、冷蔵庫116、ならびに洗濯機および乾燥機118、インターネット175に直接接続し、および/またはアクセスポイント125を介してインターネットに接続するコンピュータ120、ならびにインターネット175を介してアクセス可能なIoTサーバ170などを含む様々なIoTデバイス)を含み得る。したがって、説明を簡潔および簡単にするために、図1Bに示されるワイヤレス通信システム100Bの特定の構成要素に関連する様々な詳細は、同じまたは同様の詳細が図1Aに示されたワイヤレス通信システム100Aに関連して上で既に与えられている限り、本明細書において省略される可能性がある。

【0030】

図1Bを参照すると、ワイヤレス通信システム100Bは、ワイヤレス通信システム100Bの様々なその他の構成要素を観測、監視、制御、またはその他の方法で管理するために使用され得るスーパーバイザデバイス130を含む可能性がある。たとえば、スーパーバイザデバ

10

20

30

40

50

イス130は、無線インターフェース108および/または直接有線接続109を介してアクセスネットワーク(たとえば、アクセスポイント125)と通信して、ワイヤレス通信システム100B内の様々なIoTデバイス110～118/120に関連する属性、活動、またはその他の状態を監視または管理することができる。スーパーバイザデバイス130は、インターネット175および任意で(破線として示される)IoTサーバ170への有線またはワイヤレス接続を有する可能性がある。スーパーバイザデバイス130は、様々なIoTデバイス110～118/120に関連する属性、活動、またはその他の状態をさらに監視または管理するために使用され得る情報をインターネット175および/またはIoTサーバ170から取得し得る。スーパーバイザデバイス130は、スタンドアロンのデバイス、またはコンピュータ120などのIoTデバイス110～118/120のうちの1つである可能性がある。スーパーバイザデバイス130は、物理的なデバイス、または物理的なデバイスで実行されるソフトウェアアプリケーションである可能性がある。スーパーバイザデバイス130は、IoTデバイス110～118/120に関連する監視された属性、活動、またはその他の状態に関連する情報を出力し、IoTデバイス110～118/120に関連する属性、活動、またはその他の状態を制御またはそうでなければ管理するための入力された情報を受信することができるユーザインターフェースを含み得る。したがって、スーパーバイザデバイス130は、概して、ワイヤレス通信システム100B内の様々な構成要素を観測、監視、制御、またはそうでなければ管理するために様々な構成要素を含み、様々な有線およびワイヤレス通信インターフェースをサポートする可能性がある。

10

【0031】

図1Bに示されるワイヤレス通信システム100Bは、ワイヤレス通信システム100Bに結合されるか、またはそうでなければワイヤレス通信システム100Bの一部にされる可能性がある(能動的なIoTデバイス110～118/120とは対照的な)1つまたは複数の受動的IoTデバイス105を含む可能性がある。概して、受動的IoTデバイス105は、バーコード付きデバイス、Bluetooth(登録商標)デバイス、無線周波数(RF)デバイス、RFIDタグ付きデバイス、赤外線(IR)デバイス、NFCタグ付きデバイス、または近距離インターフェースを介して問い合わせるときにそのデバイスの識別子および属性を別のデバイスに提供することができる任意の他の好適なデバイスを含み得る。能動的なIoTデバイスは、受動的IoTデバイスの属性の変化を検出する可能性、伝達する可能性、そのような変化に基づき動作する可能性などがある。

20

【0032】

たとえば、受動的IoTデバイス105は、それぞれがRFIDタグまたはバーコードを有するコーヒーカップおよびオレンジジュースの容器を含む可能性がある。棚IoTデバイスおよび冷蔵庫IoTデバイス116は、それぞれ、コーヒーカップおよび/またはオレンジジュースの容器の受動的IoTデバイス105が追加されたかまたは取り除かれたときを検出するためにRFIDタグまたはバーコードを読み取ることができる適切なスキャナまたはリーダを有する可能性がある。棚IoTデバイスがコーヒーカップの受動的IoTデバイス105が取り除かれたことを検出すること、および冷蔵庫IoTデバイス116がオレンジジュースの容器の受動的IoTデバイスが取り除かれたことを検出することに応じて、スーパーバイザデバイス130は、棚IoTデバイスおよび冷蔵庫IoTデバイス116で検出された活動に関する1つまたは複数の信号を受信し得る。そのとき、スーパーバイザデバイス130は、ユーザがコーヒーカップからオレンジジュースを飲んでいる、および/またはコーヒーカップからオレンジジュースを飲むのが好きであると推測する可能性がある。

30

【0033】

以上は受動的IoTデバイス105を何らかの形態のRFまたはバーコード通信インターフェースを有するものとして説明するが、受動的IoTデバイス105は、そのような通信能力を持たない1つまたは複数のデバイスまたは他の物理的な物体(object)を含む可能性がある。たとえば、特定のIoTデバイスは、受動的IoTデバイス105を特定するために受動的IoTデバイス105に関連する形、大きさ、色、および/または他の観測可能な特徴を検出することができる適切なスキャナまたはリーダメカニズムを有する可能性がある。このようにして、任意の好適な物理的な物体は、その物体の識別情報および属性を伝達し、ワイヤレ

40

50

ス通信システム100Bの一部になり、スーパーバイザデバイス130により観測、監視、制御、またはそうでなければ管理され得る。さらに、受動的IoTデバイス105は、図1Aに示されたワイヤレス通信システム100Aに結合されるか、またはそうでなければ図1Aに示されたワイヤレス通信システム100Aの一部にされ、実質的に同様の方法で観測、監視、制御、またはそうでなければ管理され得る。

【0034】

本開示の別の態様によれば、図1Cは、複数のIoTデバイスを含む別のワイヤレス通信システム100Cの高レベルのアーキテクチャを示す。概して、図1Cに示されるワイヤレス通信システム100Cは、上でより詳細に説明された図1Aおよび図1Bにそれぞれ示されたワイヤレス通信システム100Aおよび100Bと同じおよび/または実質的に同様である様々な構成要素を含み得る。したがって、説明を簡潔および簡単にするために、図1Cに示されるワイヤレス通信システム100Cの特定の構成要素に関連する様々な詳細は、同じまたは同様の詳細が図1Aおよび図1Bにそれぞれ示されたワイヤレス通信システム100Aおよび100Bに関連して上で既に与えられている限り、本明細書において省略される可能性がある。

10

【0035】

図1Cに示される通信システム100Cは、IoTデバイス110～118とスーパーバイザデバイス130との間の例示的なピアツーピア通信を示す。図1Cに示されるように、スーパーバイザデバイス130は、IoTスーパーバイザインターフェースを介してIoTデバイス110～118のそれぞれと通信する。さらに、IoTデバイス110および114、IoTデバイス112、114、および116、ならびにIoTデバイス116および118は、互いに直接通信する。

20

【0036】

IoTデバイス110～118は、近隣IoTグループ160を構成する。近隣IoTグループは、ユーザのホームネットワークに接続されたIoTデバイスなどのローカルに接続されたIoTデバイスのグループである。示されていないが、複数の近隣IoTグループが、インターネット175に接続されたIoT SuperAgent 140を介して互いに接続されるおよび/または通信する可能性がある。高いレベルで、スーパーバイザデバイス130がグループ内通信を管理し、一方、IoT SuperAgent 140はグループ間通信を管理することができる。別々のデバイスとして示されているが、スーパーバイザ130およびIoT SuperAgent 140は、同じデバイスであるか、または同じデバイスに存在する可能性がある。これは、スタンドアロンのデバイス、または図1Aのコンピュータ120などのIoTデバイスである可能性がある。代替的に、IoT SuperAgent 140は、アクセスポイント125に相当するか、またはアクセスポイント125の機能を含む可能性がある。さらに別の代替として、IoT SuperAgent 140は、IoTサーバ170などのIoTサーバに相当するか、またはIoTサーバの機能を含む可能性がある。IoT SuperAgent 140は、ゲートウェイ機能145を包含する可能性がある。

30

【0037】

それぞれのIoTデバイス110～118は、スーパーバイザデバイス130をピアとして扱い、スーパーバイザデバイス130に属性/スキーマの更新を送信する可能性がある。IoTデバイスは、別のIoTデバイスと通信する必要があるとき、スーパーバイザデバイス130にそのIoTデバイスへのポインタを要求し、それから、ピアとして目標のIoTデバイスと通信することができる。IoTデバイス110～118は、共通メッセージングプロトコル(CMP: common messaging protocol)を使用してピアツーピア通信ネットワークを介して互いに通信する。2つのIoTデバイスは、CMPに対応しており、共通通信トランスポート(common communication transport)を介して接続される限り、互いに通信し得る。プロトコルスタックにおいて、CMPレイヤ154は、アプリケーションレイヤ152の下、ならびにトランスポートレイヤ156および物理レイヤ158の上にある。

40

【0038】

本開示の別の態様によれば、図1Dは、複数のIoTデバイスを含む別のワイヤレス通信システム100Dの高レベルのアーキテクチャを示す。概して、図1Dに示されるワイヤレス通信システム100Dは、上でより詳細に説明された図1A～図1Cにそれぞれ示されたワイヤレス通信システム100A～Cと同じおよび/または実質的に同様である様々な構成要素を含み得る。

50

したがって、説明を簡潔および簡単にするために、図1Dに示されるワイヤレス通信システム100Dの特定の構成要素に関連する様々な詳細は、同じまたは同様の詳細が図1A～図1Cにそれぞれ示されたワイヤレス通信システム100A～Cに関連して上で既に与えられている限り、本明細書において省略される可能性がある。

【0039】

インターネットは、IoTの概念を使用して規制され得る「リソース」である。しかし、インターネットは、規制されるリソース單なる一例であり、任意のリソースが、IoTの概念を使用して規制され得る。規制され得るその他のリソースは、電気、ガス、ストレージ、セキュリティなどを含むがこれらに限定されない。IoTデバイスは、リソースに接続され、それによってリソースを規制する可能性があり、リソースは、インターネットを介して規制される可能性がある。図1Dは、インターネット175に加えて規制され得る、またはインターネット175を介して規制され得る天然ガス、ガソリン、温水、および電気などのいくつかのリソース180を示す。

【0040】

IoTデバイスは、それらのIoTデバイスのリソースの使用を規制するために互いに通信し得る。たとえば、トースター、コンピュータ、およびヘアドライヤーなどのIoTデバイスが、それらのIoTデバイスの電気(リソース)の使用を規制するためにBluetooth(登録商標)通信インターフェースを介して互いに通信する可能性がある。別の例として、デスクトップコンピュータ、電話、およびタブレットコンピュータなどのIoTデバイスが、インターネット(リソース)へのそれらのIoTデバイスのアクセスを規制するためにWiFi通信インターフェースを介して通信する可能性がある。さらに別の例として、ストーブ、衣類乾燥機、および給湯器などのIoTデバイスが、それらのIoTデバイスのガスの使用を規制するためにWiFi通信インターフェースを介して通信する可能性がある。代替的にまたは追加的に、それぞれのIoTデバイスは、IoTデバイスから受信された情報に基づいてそれらのIoTデバイスのリソースの使用を規制するための論理を有するIoTサーバ170などのIoTサーバに接続される可能性がある。

【0041】

本開示の別の態様によれば、図1Eは、複数のIoTデバイスを含む別のワイヤレス通信システム100Eの高レベルのアーキテクチャを示す。概して、図1Eに示されるワイヤレス通信システム100Eは、上でより詳細に説明された図1A～図1Dにそれぞれ示されたワイヤレス通信システム100A～Dと同じおよび/または実質的に同様である様々な構成要素を含み得る。したがって、説明を簡潔および簡単にするために、図1Eに示されるワイヤレス通信システム100Eの特定の構成要素に関連する様々な詳細は、同じまたは同様の詳細が図1A～図1Dにそれぞれ示されたワイヤレス通信システム100A～Dに関連して上で既に与えられている限り、本明細書において省略される可能性がある。

【0042】

通信システム100Eは、2つの近隣IoTグループ160Aおよび160Bを含む。複数の近隣IoTグループが、インターネット175に接続されたIoT SuperAgentを介して互いに接続されるおよび/または通信する可能性がある。高いレベルで、IoT SuperAgentが、グループ間通信を管理する。図1Eにおいて、近隣IoTグループ160Aは、IoTデバイス116A、122A、および124A、ならびにIoT SuperAgent 140Aを含む。近隣IoTグループ160Bは、IoTデバイス116B、122B、および124B、ならびにIoT SuperAgent 140Bを含む。IoT SuperAgent 140Aおよび140Bは、インターネット175に接続され、インターネット175を介してまたは直接互いに通信する可能性がある。IoT SuperAgent 140Aおよび140Bは、近隣IoTグループ160Aと近隣IoTグループ160Bとの間の通信を容易にする。図1EはIoT SuperAgent 140Aおよび140Bを介して互いに通信する2つの近隣IoTグループを示すが、任意の数の近隣IoTグループが、IoT SuperAgentを使用して互いに通信する可能性がある。

【0043】

図2Aは、本開示の態様によるIoTデバイス200Aの高レベルの例を示す。外観および/または内部の構成要素がIoTデバイスの間で大きく異なる可能性があるが、ほとんどのIoTデバ

10

20

30

40

50

イスは、ディスプレイおよびユーザ入力のための手段を含み得るある種のユーザインターフェースを有する。ユーザインターフェースのないIoTデバイスは、図1A～図Bおよび図Dの無線インターフェース108などの有線またはワイヤレスネットワークを介して遠隔で通信され得る。

【0044】

図2Aに示されるように、IoTデバイス200Aに関する例示的な構成において、IoTデバイス200Aの外部ケーシングは、当技術分野で知られているように、コンポーネントの中でもとりわけ、ディスプレイ226、電源ボタン222、ならびに2つの制御ボタン224Aおよび224Bを使用して構成される可能性がある。ディスプレイ226は、タッチスクリーンディスプレイである可能性があり、その場合、制御ボタン224Aおよび224Bは、必要でない可能性がある。IoTデバイス200Aの一部として明示的に示されていないが、IoTデバイス200Aは、Wi-Fiアンテナ、セルラーアンテナ、衛星測位システム(SPS)アンテナ(たとえば、全地球測位システム(GPS)アンテナ)などを含むがこれらに限定されない1つもしくは複数の外部アンテナおよび/または外部ケーシングに組み込まれた1つもしくは複数の組込みアンテナを含む可能性がある。

10

【0045】

IoTデバイス200AなどのIoTデバイスの内部の構成要素は、異なるハードウェア構成で具現化される可能性があるが、内部のハードウェア構成要素に関する基本的な高レベルの構成は、図2Aにおいてプラットフォーム202として示される。プラットフォーム202は、図1A～図1Bおよび図1Dの無線インターフェース108および/または有線インターフェースなどのネットワークインターフェースを介して送信されたソフトウェアアプリケーション、データ、および/またはコマンドを受信し、実行し得る。また、プラットフォーム202は、ローカルに記憶されたアプリケーションを独立して実行し得る。プラットフォーム202は、概してプロセッサ208として呼ばれるマイクロコントローラ、マイクロプロセッサ、特定用途向け集積回路、デジタル信号プロセッサ(DSP)、プログラミング可能な論理回路、またはその他のデータ処理デバイスなどの1つまたは複数のプロセッサ208に動作可能なように結合された有線および/またはワイヤレス通信のために構成された1つまたは複数のトランシーバ206(たとえば、Wi-Fiトランシーバ、Bluetooth(登録商標)トランシーバ、セルラートランシーバ、衛星トランシーバ、GPSもしくはSPS受信機など)を含み得る。プロセッサ208は、IoTデバイスのメモリ212内のアプリケーションプログラミング命令を実行し得る。メモリ212は、読み取り専用メモリ(ROM)、ランダムアクセスメモリ(RAM)、電気的消去可能プログラマブルROM(EEPROM)、フラッシュカード、またはコンピュータプラットフォームによくある任意のメモリのうちの1つまたは複数を含み得る。1つまたは複数の入力/出力(I/O)インターフェース214は、示されたディスプレイ226、電源ボタン222、制御ボタン224Aおよび224Bなどの様々なI/Oデバイス、ならびにIoTデバイス200Aに関連するセンサー、アクチュエータ、中継機、バルブ、スイッチなどの任意のその他のデバイスとプロセッサ208が通信することと、それらのデバイスからの制御とを可能にするように構成され得る。

20

【0046】

したがって、本開示の態様は、本明細書において説明される機能を実行する能力を含むIoTデバイス(たとえば、IoTデバイス200A)を含み得る。当業者によって理解されるであろうように、様々な論理要素は、ディスクリート要素(discrete element)、プロセッサ(たとえば、プロセッサ208)で実行されるソフトウェアモジュール、または本明細書において開示される機能を実現するためのソフトウェアとハードウェアとの任意の組合せで具現化され得る。たとえば、トランシーバ206、プロセッサ208、メモリ212、およびI/Oインターフェース214が、本明細書で開示される様々な機能を協力してロードし、記憶し、実行するためにすべて使用される可能性があり、したがって、これらの機能を実行するための論理が、様々な要素に分散される可能性がある。代替的に、機能は、1つのディスクリート構成要素(discrete component)に組み込まれる可能性がある。したがって、図2AのIoTデバイス200Aの特徴は、例示的であるに過ぎないと見なされるべきであり、本開示は、示さ

30

40

50

れる特徴または構成に限定されない。

【0047】

図2Bは、本開示の態様による受動的IoTデバイス200Bの高レベルの例を示す。概して、図2Bに示される受動的IoTデバイス200Bは、上でより詳細に説明された図2Aに示されたIoTデバイス200Aと同じおよび/または実質的に同様である様々な構成要素を含み得る。したがって、説明を簡潔および簡単にするために、図2Bに示される受動的IoTデバイス200Bの特定の構成要素に関する様々な詳細は、同じまたは同様の詳細が図2Aに示されたIoTデバイス200Aに関連して上で既に与えられている限り、本明細書において省略される可能性がある。

【0048】

概して、図2Bに示される受動的IoTデバイス200Bは、受動的IoTデバイス200Bがプロセッサ、内部メモリ、または特定のその他の構成要素を持たない可能性があるという点で、図2Aに示されたIoTデバイス200Aとは異なる可能性がある。その代わりに、一実施形態において、受動的IoTデバイス200Aは、I/Oインターフェース214、または受動的IoTデバイス200Bが制御されるIoTネットワーク内で観測されるか、監視されるか、制御されるか、管理されるか、もしくはそうでなければ知られることを可能にするその他の好適なメカニズムのみを含み得る。たとえば、一実施形態において、受動的IoTデバイス200Bに関連するI/Oインターフェース214は、バーコード、Bluetooth(登録商標)インターフェース、無線周波数(RF)インターフェース、RFIDタグ、IRインターフェース、NFCインターフェース、または近距離インターフェースを介して問い合わせされるとときに受動的IoTデバイス200Bに関連する識別子および属性を別のデバイス(たとえば、受動的IoTデバイス200Bに関連する属性に関する情報を検出するか、記憶するか、伝達するか、そのような情報に基づき動作するか、もしくはそうでなければそのような情報を処理することができるIoTデバイス200Aなどの能動的IoTデバイス)に提供することができる任意のその他の好適なI/Oインターフェースを含み得る。

【0049】

以上は受動的IoTデバイス200Bをある形態のRF、バーコード、またはその他のI/Oインターフェース214を有するものとして示すが、受動的IoTデバイス200Bは、そのようなI/Oインターフェース214を持たないデバイスまたはその他の物理的な物体を含む可能性がある。たとえば、特定のIoTデバイスは、受動的IoTデバイス200Bを特定するために受動的IoTデバイス200Bに関連する形、大きさ、色、および/またはその他の観測可能な特徴を検出することができる適切なスキャナまたはリーダメカニズムを有する可能性がある。このようにして、任意の好適な物理的な物体は、その物体の識別情報および属性を伝達し、制御されるIoTネットワーク内で観測、監視、制御、またはそうでなければ管理され得る。図3は、機能を実行するように構成された論理を含む通信デバイス300を示す。通信デバイス300は、IoTデバイス110～118/120、IoTデバイス200Aおよび200B、インターネット175に結合された任意の構成要素(たとえば、IoTサーバ170)などを含むがこれらに限定されない上述の通信デバイスのいずれかに相当する可能性がある。したがって、通信デバイス300は、図1A～図1Bおよび図1Dのワイヤレス通信システム100A～BおよびEを介して1つまたは複数のその他のエンティティと通信する(またはそれらのその他のエンティティとの通信を容易にする)ように構成される任意の電子デバイスに相当する可能性がある。

【0050】

図3に示されるように、実施形態は、信頼された機関のソースからの緊急メッセージに基づいて緊急命令を実施するための方法であって、信頼された機関のソースから(たとえば、消防署のサーバから)IoT秘密鍵を受信するステップ-ブロック302と、信頼された機関のソースから緊急秘密鍵を含む緊急メッセージを受信するステップ(たとえば、消防署のサーバからの緊急メッセージでガス漏れの場所を受信するステップであって、緊急秘密鍵がIoTデバイスの秘密鍵で暗号化される、ステップ)-ブロック304と、IoT秘密鍵を使用して緊急メッセージを復号して(たとえば、IoT秘密鍵を使用してガス漏れの場所を復号して)緊急メッセージ内の値を判定するステップ-ブロック306と、判定された値に基づいて結

10

20

30

40

50

果を計算する(たとえば、そのガス漏れがデバイスが使用する同じガス本管の一部であるか否かを判定する)ステップ-ブロック308と、結果が所定の閾値を超える場合に緊急命令を実施する(たとえば、ガス漏れがデバイスと同じガス本管系内である場合にガス吸気弁を遮断する)ステップ-ブロック310とを含む、方法を含み得る。

【0051】

一部の実施形態において、IoTデバイスは、結果を計算するためのその他のソースからのデータを受信する可能性がある。たとえば、IoTデバイスは、サーモスタットであり、結果の計算の一部として現在の室温を用いる可能性がある。IoTデバイスと見なされない物体が、結果を計算するためのデータを提供する可能性もある。たとえば、屋外の温度計が、たとえそれが日常的なデバイスではないとしても、サーモスタットにデータを提供する可能性がある。データは、別の日常的なデバイス、信頼された機関のソース、または別の信頼された機関のソースから提供される可能性もある。

10

【0052】

一部の実施形態においては、値が、緊急命令を実施すべきかどうかを判定するための式の変数として使用される可能性がある。たとえば、日常的なデバイスがサーモスタットであり、緊急メッセージが吹雪に関するデータを提供する場合、サーモスタットは、屋外の温度計、室温を判定するためのそれ自体の温度計からのデータ、および緊急メッセージからのデータを使用して緊急命令を計算する可能性がある。サーモスタットは、午前10:00にオフになり、午後4:00に低レベルでオンになり、午後5:00に中間のレベルでオンになるように設定される可能性がある。緊急モードでは、サーモスタットは、提供されたすべてのデータに基づいて、常に加熱を続けることなくパイプが凍結しないことを保証するために、そのサーモスタットが加熱を午後2:00に低いレベルでオンにし、午後4:00に中間のレベルでオンにし、午後5:00に高いレベルでオンにすべきであると判定する可能性がある。

20

【0053】

一部の実施形態においては、異なるIoT秘密鍵が、IoTデバイスに周期的に送信される。たとえば、新しい鍵が毎日送信されるが、日々、異なる信頼された機関のソースから更新される。IoT秘密鍵は、鍵を確認するために複数の信頼された機関のソースから送信される可能性がある。

【0054】

図4は、機能を実行するように構成された論理を含む通信デバイス400を示す。通信デバイス400は、IoTデバイス110～118/120、IoTデバイス200A、インターネット175に結合された任意の構成要素(たとえば、IoTサーバ170)などを含むがこれらに限定されない上述の通信デバイスのいずれかに相当する可能性がある。したがって、通信デバイス400は、図1A～図1Eのワイヤレス通信システム100A～Eを介して1つまたは複数のその他のエンティティと通信する(またはそれらのその他のエンティティとの通信を容易にする)ように構成される任意の電子デバイスに相当する可能性がある。

30

【0055】

図4を参照すると、通信デバイス400は、情報を受信および/または送信するように構成された論理405を含む。一例においては、通信デバイス400がワイヤレス通信デバイス(たとえば、IoTデバイス200Aおよび/または受動的IoTデバイス200B)に相当する場合、情報を受信および/または送信するように構成された論理405は、ワイヤレストランシーバなどのワイヤレス通信インターフェース(たとえば、Bluetooth(登録商標)、Wi-Fi、Wi-Fi Direct、ロングタームエボリューション(LTE) Directなど)ならびに関連するハードウェア(たとえば、RFアンテナ、モデム、変調器および/または復調器など)を含み得る。別の例において、情報を受信および/または送信するように構成された論理405は、有線通信インターフェース(たとえば、シリアル接続、USBまたはFirewire接続、インターネット175がアクセスされ得るイーサネット(登録商標)接続など)に対応する可能性がある。したがって、通信デバイス400がある種のネットワークに基づくサーバ(たとえば、IoTサーバ170)に対応する場合、情報を受信および/または送信するように構成された論理405は、一例においては、ネットワークに基づくサーバをイーサネット(登録商標)プロトコルによってその他

40

50

の通信エンティティに接続するイーサネット(登録商標)カードに相当する可能性がある。さらなる例において、情報を受信および/または送信するように構成された論理405は、通信デバイス400がその通信デバイス400のローカルの環境を監視することができる感知または測定ハードウェア(たとえば、加速度計、温度センサー、光センサー、ローカルのRF信号を監視するためのアンテナなど)を含む可能性がある。情報を受信および/または送信するように構成された論理405は、実行されるときに、情報を受信および/または送信するように構成された論理405の関連するハードウェアがその論理の受信および/もしくは送信機能を実行することを可能にするソフトウェアを含む可能性もある。しかし、情報を受信および/または送信するように構成された論理405は、ソフトウェアのみに相当せず、情報を受信および/または送信するように構成された論理405は、その論理の機能を実現するために少なくとも部分的にハードウェアに依拠する。

10

20

30

40

【0056】

図4を参照すると、通信デバイス400は、情報を処理するように構成された論理410をさらに含む。一例において、情報を処理するように構成された論理410は、少なくともプロセッサを含み得る。情報を処理するように構成された論理410によって実行され得る処理の種類の例示的な実装は、判定を行うこと、接続を確立すること、異なる情報の選択肢の間で選択を行うこと、データに関連する評価を行うこと、通信デバイス400に結合されたセンサーとインタラクションして測定動作を実行すること、情報をある形式から別の形式に(たとえば、.wmvから.aviへなど異なるプロトコルの間で)変換することなどを含むがこれらに限定されない。たとえば、情報を処理するように構成された論理410に含まれるプロセッサは、汎用プロセッサ、DSP、ASIC、フィールドプログラマブルゲートアレイ(FPGA)もしくはその他のプログラマブルロジックデバイス、ディスクリートゲート(discrete gate)もしくはトランジスタ論理、ディスクリートハードウェア構成要素(discrete hardware component)、または本明細書で説明される機能を実行するように設計されたこれらの任意の組合せに相当する可能性がある。汎用プロセッサはマイクロプロセッサである可能性があるが、別法として、プロセッサは、任意の通常のプロセッサ、コントローラ、マイクロコントローラ、または状態機械である可能性がある。また、プロセッサは、コンピューティングデバイスの組合せ(たとえば、DSPとマイクロプロセッサの組合せ、複数のマイクロプロセッサ、DSPコアと連携する1つもしくは複数のマイクロプロセッサ、または任意のその他のそのような構成)として実装され得る。情報を処理するように構成された論理410は、実行されるときに、情報を処理するように構成された論理410の関連するハードウェアがその論理の処理機能を実行することを可能にするソフトウェアを含む可能性もある。しかし、情報を処理するように構成された論理410は、ソフトウェアのみに相当せず、情報を処理するように構成された論理410は、その論理の機能を実現するために少なくとも部分的にハードウェアに依拠する。

【0057】

図4を参照すると、通信デバイス400は、情報を記憶するように構成された論理415をさらに含む。一例において、情報を記憶するように構成された論理415は、少なくとも非一時的メモリおよび関連するハードウェア(たとえば、メモリコントローラなど)を含み得る。たとえば、情報を記憶するように構成された論理415に含まれる非一時的メモリは、RAM、フラッシュメモリ、ROM、消去可能プログラマブルROM(EPROM)、EEPROM、レジスタ、ハードディスク、取り外し可能なディスク、CD-ROM、または当技術分野で知られている任意のその他の形態のストレージ媒体に相当する可能性がある。情報を記憶するように構成された論理415は、実行されるときに、情報を記憶するように構成された論理415の関連するハードウェアがその論理の記憶機能を実行することを可能にするソフトウェアを含む可能性もある。しかし、情報を記憶するように構成された論理415は、ソフトウェアのみに相当せず、情報を記憶するように構成された論理415は、その論理の機能を実現するために少なくとも部分的にハードウェアに依拠する。

【0058】

図4を参照すると、通信デバイス400は、任意で、情報を提示するように構成された論理

50

420をさらに含む。一例において、情報を提示するように構成された論理420は、少なくとも出力デバイスおよび関連するハードウェアを含み得る。たとえば、出力デバイスは、映像出力デバイス(たとえば、ディスプレイスクリーン、USB、HDMI(登録商標)などの映像情報を運ぶことができるポート)、音声出力デバイス(たとえば、スピーカ、マイクロホンジャック、USB、HDMI(登録商標)などの音声情報を運ぶことができるポート)、振動デバイス、および/または情報が出力のためにフォーマットされ、もしくは通信デバイス400のユーザもしくはオペレータによって実際に出力され得る任意のその他のデバイスを含む可能性がある。たとえば、通信デバイス400が図2Aに示されたIoTデバイス200Aおよび/または図2Bに示された受動的IoTデバイス200Bに相当する場合、情報を提供するように構成された論理420は、ディスプレイ226を含み得る。さらなる例において、情報を提示するように構成された論理420は、ローカルユーザのいないネットワーク通信デバイス(たとえば、ネットワークスイッチまたはルータ、遠隔のサーバなど)などの特定の通信デバイスに関しては省略される可能性がある。情報を提示するように構成された論理420は、実行されるときに、情報を提示するように構成された論理420の関連するハードウェアがその論理の提示機能を実行することを可能にするソフトウェアを含む可能性もある。しかし、情報を提示するように構成された論理420は、ソフトウェアのみに相当せず、情報を提示するように構成された論理420は、その論理の機能を実現するために少なくとも部分的にハードウェアに依拠する。

【0059】

図4を参照すると、通信デバイス400は、任意で、ローカルユーザ入力を受信するように構成された論理425をさらに含む。一例において、ローカルユーザ入力を受信するように構成された論理425は、少なくともユーザ入力デバイスおよび関連するハードウェアを含み得る。たとえば、ユーザ入力デバイスは、ボタン、タッチスクリーンディスプレイ、キーボード、カメラ、音声入力デバイス(たとえば、マイクロホン、もしくはマイクロホンジャックなどの音声情報を運ぶことができるポート)、および/または情報が通信デバイス400のユーザもしくはオペレータから受信され得る任意のその他のデバイスを含む可能性がある。たとえば、通信デバイス400が図2Aに示されたIoTデバイス200Aおよび/または図2Bに示された受動的IoTデバイス200Bに相当する場合、ローカルユーザ入力を受信するように構成された論理425は、ボタン222、224A、および224B、ディスプレイ226(タッチスクリーンの場合)などを含み得る。さらなる例において、ローカルユーザ入力を受信するように構成された論理425は、ローカルユーザのいないネットワーク通信デバイス(たとえば、ネットワークスイッチまたはルータ、遠隔のサーバなど)などの特定の通信デバイスに関しては省略される可能性がある。ローカルユーザ入力を受信するように構成された論理425は、実行されるときに、ローカルユーザ入力を受信するように構成された論理425の関連するハードウェアがその論理の入力受信機能を実行することを可能にするソフトウェアを含む可能性もある。しかし、ローカルユーザ入力を受信するように構成された論理425は、ソフトウェアのみに相当せず、ローカルユーザ入力を受信するように構成された論理425は、その論理の機能を実現するために少なくとも部分的にハードウェアに依拠する。

【0060】

図4を参照すると、405から425までの構成された論理が図4の別々のまたは異なるブロックとして示されているが、それぞれの構成された論理がその論理の機能を実行するハードウェアおよび/またはソフトウェアは、部分的に重なる可能性があることが理解されるであろう。たとえば、405から425までの構成された論理の機能を助けるために使用される任意のソフトウェアは、405から425までの構成された論理が情報を記憶するように構成された論理415によって記憶されたソフトウェアの動作に基づいてその論理の機能(つまり、この場合、ソフトウェアの実行)をそれぞれ実行するように、情報を記憶するように構成された論理415に関連する非一時的メモリに記憶される可能性がある。同様に、構成された論理のうちの1つに直接関連付けられるハードウェアが、他の構成された論理によって時折借用または使用され得る。たとえば、情報を処理するように構成された論理410のプロセッサは、情報を受信および/または送信するように構成された論理405が情

10

20

30

40

50

報を処理するように構成された論理410に関連するハードウェア(すなわち、プロセッサ)の動作に部分的に基づいてその論理の機能(つまり、この場合、データの送信)を実行するよう、情報を受信および/または送信するように構成された論理405によって送信される前にデータを適切な形式にフォーマットする可能性がある。

【0061】

概して、別途明示的に示されない限り、本開示の全体を通じて使用される語句「～ように構成された論理」は、少なくとも部分的にハードウェアで実装される態様をもたらすように意図されており、ハードウェアとは独立したソフトウェアのみの実装に当てはまるように意図されていない。また、様々なブロックの構成された論理または「～ように構成された論理」は、特定の論理ゲートまたは要素に限定されず、概して、(ハードウェアかまたはハードウェアとソフトウェアとの組合せかのどちらかによって)本明細書において説明される機能を実行する能力を指すことが理解されるであろう。したがって、様々なブロックに示される構成された論理または「～ように構成された論理」は、語「論理」を共有するにもかかわらず、必ずしも論理ゲートまたは論理要素として実装されない。様々なブロックの論理の間のその他のインタラクションまたは協力が、以下でより詳細に説明される態様を考察することにより当業者に明らかになるであろう。

10

【0062】

様々な実施形態が、図5に示されるサーバ500などの様々な市販のサーバデバイスのいずれかで実装され得る。一例において、サーバ500は、上述のIoTサーバ170の1つの例示的な構成に相当する可能性がある。図5において、サーバ500は、不揮発性メモリ502およびディスクドライブ503などの大容量不揮発性メモリに結合されたプロセッサ500を含む。サーバ500は、プロセッサ501に結合されたフロッピー(登録商標)ディスクドライブ、コンパクトディスク(CD)またはDVDディスクドライブ506も含む可能性がある。サーバ500は、その他のブロードキャストシステムのコンピュータおよびサーバまたはインターネットに結合されたローカルエリアネットワークなどのネットワーク507とのデータ接続を確立するためにプロセッサ501に結合されたネットワークアクセスポート504も含む可能性がある。図4に関連して、図5のサーバ500は、通信デバイス400の1つの例示的な実装を示し、それによって、情報を送信および/または受信するように構成された論理405は、ネットワーク507と通信するためにサーバ500によって使用されるネットワークアクセスポイント504に相当し、情報を処理するように構成された論理410は、プロセッサ501に相当し、情報を記憶するための論理の構成415は、揮発性メモリ502、ディスクドライブ503、および/またはディスクドライブ506の任意の組合せに相当することが理解されるであろう。情報を提示するように構成された任意の論理420およびローカルユーザ入力を受信するように構成された任意の論理425は、図5に明示的に示されておらず、サーバ500に含まれる可能性があり、または含まれない可能性がある。したがって、図5は、図2AのようなIoTデバイスの実装に加えて、通信デバイス400がサーバとして実装され得ることを示すのに役立つ。

20

【0063】

図6に示されるように、実施形態は、IoTデバイスに緊急命令を送信するための方法であって、外部ソースからIoT秘密鍵を受信するステップ(たとえば、電力事業者からIoT秘密鍵を受信するステップ)-ブロック602と、少なくとも1つのIoTデバイスにIoT秘密鍵を送信するステップ(たとえば、すべての空調ユニットに鍵を送信するステップ)-ブロック604と、緊急秘密鍵を含む緊急メッセージを少なくとも1つのIoTデバイスのサブセットに送信するステップ(たとえば、電力使用制限の時間の変化、および電力使用制限の時間を減らすために消費を減らすために必要とされるユニットの数を含む電力使用制限メッセージを指定された数のACユニットに送信するステップ)であって、緊急秘密鍵がIoTデバイスの秘密鍵で暗号化される、ステップ)-ブロック606とを含む、方法を含み得る。一部の実施形態において、緊急メッセージは、ブロードキャスト/マルチキャスト/ユニキャストされる緊急メッセージである可能性がある。IoTデバイスへのこの緊急メッセージのルーティングは、ネットワークに固有である可能性がある。一部の実施形態において、緊急メッセージは、各IoTデバイスへの緊急メッセージの優先ルーティングを可能にするためのサービス

30

40

50

品質パラメータを含み得る。

【0064】

図7は、デバイスに関する信頼された機関のソースからの緊急メッセージの情報の少なくとも一部を示す通信デバイスの表示を示す。示されるように、図2のデバイスのディスプレイ226が、6つのセクションを提供する。各セクションは、緊急メッセージからユーザに情報を提供する。ディスプレイ226はテキストに基づくが、実施形態は、色、音、アニメーション、およびその他の手段を使用してユーザに緊急情報を提供し得る。

【0065】

図7において、セクション702は、ここでは「緊急レベル3」として示される緊急事態のレベルを表示する。セクション704は、緊急メッセージを発する機関のレベル、本明細書においては「電力事業者」を示す。機関のレベルは、信頼された機関のソース、または信頼された機関のソースへの情報提供者と同じである可能性がある。

10

【0066】

緊急事態の予測される継続時間が図7のセクション706に示される可能性があり、セクション706はIoTデバイスが緊急モードの動作に留まるべきである提案される時間を示す。IoTデバイスが実行すべき推薦される全般的な行為が、セクション708に「ACユニットの設定を10度下げる」と示される。ディスプレイ226は、セクション710で、肯定応答が必要とされるまたはリクエストされるかどうかをユーザに知らせる可能性もある。

20

【0067】

緊急メッセージは、ユーザの応答が所与の継続時間内にIoTデバイスによって受信されない場合のIoTデバイスの提案される行為を含み得る。セクション712に示されているが、ユーザにとって、そのユーザの承認が緊急命令で考慮に入れられなくなるまで残り42秒である。ユーザの承認が必要とされる場合、緊急命令は実施されない可能性がある。ユーザの承認が必要とされない場合、緊急命令は実施される可能性がある。

20

【0068】

IoTデバイスは、信頼された機関のソースに応答メッセージを送信する可能性がある。応答は、ユーザおよびIoTデバイスからの応答の詳細を含む可能性がある。たとえば、緊急メッセージに肯定応答し、提案される行為を承認するユーザの応答が、信頼された機関のソースに送信される可能性がある。IoTデバイスが信頼された機関のソースに提供し得る情報は、リソースを実装することを助ける可能性がある。たとえば、消防署のシステムは、緊急メッセージが送信されたどのIoTデバイスがガスの遮断などの必要とされる行為を行うことができなかったかを示すレポートを生成する可能性がある。そのレポートにも基づいて、消防署は、手動による介入のためのリソースを割り振る可能性がある。

30

【0069】

一部の実装においては、日常的なデバイスの緊急モードを無効にすることが望ましい可能性がある。緊急モードが開始されると、緊急モードは、オーバーライド命令を使用して無効にされる可能性がある。たとえば、信頼された機関のソースは、機関が緊急事態が終わっていると判定するとオーバーライド命令を与える外部ソースである可能性がある。また、ユーザは、緊急モードを実施することを望まないと決定した場合、オーバーライド信号を与える可能性がある。日常的なデバイスは、別のパラメータが決定される場合に緊急モードを無効にする可能性がある。たとえば、日常的なデバイスは、潜在的な電力使用制限のために電力を節約するために停止したが、低い電力使用および空調をさらに弱くすることがユーザ定義のパラメータを満たすと判定する冷蔵庫である可能性がある。これらのパラメータを使用して、冷蔵庫は、緊急モードを無効にし、電力消費の同じ所望の削減を引き続き達成し得る。

40

【0070】

一部の実装において、IoTデバイスは、緊急メッセージに基づいて日常的でないデバイスに緊急命令を送信する可能性がある。IoTデバイスは、家の照明も制御するコンピュータである可能性がある。照明のスイッチは、IoTデバイスではない可能性がある。つまり、照明は、インターネットと通信せず、IoT秘密鍵を受信することもできない。しかし、

50

コンピュータは、緊急メッセージを受信する場合、所定の時間にオンになるのではなく、激しい雷雨の間、オフのままであるように照明にメッセージを送信する可能性がある。

【0071】

当業者は、情報および信号が様々な異なる技術および技法のうちのいずれかを使用して表され得ることを理解するであろう。たとえば、上の説明を通して言及される可能性があるデータ、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、磁界もしくは磁気的粒子、光場もしくは光学的粒子、またはこれらの任意の組合せによって表され得る。

【0072】

さらに、当業者は、本明細書において開示された態様に関連して説明された様々な例示的な論理ブロック、モジュール、回路、およびアルゴリズムのステップが、電子的なハードウェア、コンピュータソフトウェア、またはそれら両方の組合せとして実装される可能性があることを理解するであろう。ハードウェアとソフトウェアとのこの互換性を明確に示すために、様々な例示的な構成要素、ブロック、モジュール、回路、およびステップが、概してそれらの機能の観点で上で説明された。そのような機能がハードウェアとして実装されるかまたはソフトウェアとして実装されるかは、システム全体に課された特定の用途および設計の制約による。当業者は、説明された機能をそれぞれの特定の用途のために様々な方法で実装し得るが、そのような実装の判断は、本開示の範囲からの逸脱をもたらすものと解釈されるべきでない。

【0073】

本明細書において開示された態様に関連して説明された様々な例示的な論理ブロック、モジュール、および回路は、汎用プロセッサ、デジタル信号プロセッサ(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)もしくはその他のプログラマブルロジックデバイス、ディスクリートゲートもしくはトランジスタ論理、ディスクリートハードウェア構成要素、または本明細書において説明された機能を実行するように設計されたこれらの任意の組合せを使用して実装または実行され得る。汎用プロセッサはマイクロプロセッサである可能性があるが、別法として、プロセッサは、任意の通常のプロセッサ、コントローラ、マイクロコントローラ、または状態機械である可能性がある。また、プロセッサは、コンピューティングデバイスの組合せ、たとえば、DSPとマイクロプロセッサとの組合せ、複数のマイクロプロセッサ、DSPコアと連携する1つもしくは複数のマイクロプロセッサ、または任意のその他のそのような構成として実装され得る。

【0074】

本明細書において開示された態様と関連して説明された方法、シーケンス、および/またはアルゴリズムは、直接ハードウェアで、プロセッサによって実行されるソフトウェアモジュールで、またはこれら2つの組合せで具現化される可能性がある。ソフトウェアモジュールは、RAM、フラッシュメモリ、ROM、EPROM、EEPROM、レジスタ、ハードディスク、取り外し可能なディスク、CD-ROM、または当技術分野で知られている任意の他の形態のストレージ媒体に存在する可能性がある。例示的なストレージ媒体は、プロセッサがストレージ媒体から情報を読むことができ、ストレージ媒体に情報を書き込むことができるようプロセッサに結合される。別法として、ストレージ媒体は、プロセッサに一体化される可能性がある。プロセッサおよびストレージ媒体は、ASIC内に存在する可能性がある。ASICは、電子オブジェクトに存在する可能性がある。別法として、プロセッサおよびストレージ媒体は、ユーザ端末内の別個の構成要素として存在する可能性がある。

【0075】

1つまたは複数の例示的な態様において、説明された機能は、ハードウェア、ソフトウェア、ファームウェア、またはこれらの任意の組合せで実装され得る。ソフトウェアで実装される場合、機能は、コンピュータ可読媒体上の1つまたは複数の命令またはコードとして記憶または送信され得る。コンピュータ可読媒体は、ある場所から別の場所へとコンピュータプログラムを転送することを容易にする任意の媒体を含むコンピュータストレージ媒体と通信媒体との両方を含む。ストレージ媒体は、コンピュータによってアクセスさ

10

20

30

40

50

れ得る任意の利用可能な媒体である可能性がある。限定ではなく例として、そのようなコンピュータ可読媒体は、RAM、ROM、EEPROM、CD-ROMもしくはその他の光ディスクストレージ、磁気ディスクストレージもしくはその他の磁気ストレージデバイス、または命令もしくはデータ構造の形態で所望のプログラムコードを運ぶかもしくは記憶するために使用可能であり、コンピュータによってアクセス可能である任意のその他の媒体を含み得る。また、当然、任意の接続がコンピュータ可読媒体と呼ばれる。たとえば、ソフトウェアが、同軸ケーブル、光ファイバケーブル、ツイストペアケーブル、DSL、または赤外線、無線、およびマイクロ波などのワイヤレス技術を使用してウェブサイト、サーバ、またはその他の遠隔のソースから送信される場合、同軸ケーブル、光ファイバケーブル、ツイストペアケーブル、DSL、または赤外線、無線、およびマイクロ波などのワイヤレス技術は、媒体の定義に含まれる。本明細書において使用されるとき、ディスク(disk)およびディスク(disc)は、CD、レーザディスク(登録商標)(laser disc)、光ディスク(optical disc)、DVD、フロッピー(登録商標)ディスク(floppy disk)、およびブルーレイディスク(Blu-ray(登録商標)disc)を含み、ディスク(disk)が、通常、磁気的にデータを再生する一方、ディスク(disc)は、レーザを使用して光学的にデータを再生する。上記のものの組合せも、コンピュータ可読媒体の範囲に含まれるべきである。

10

20

30

40

50

【0076】

上述の開示は本開示の説明的な態様を示すが、添付の特許請求の範囲で定義された本開示の範囲を逸脱することなしに本明細書において種々の変更および修正がなされ得ることに留意されたい。本明細書において説明された本開示の態様による方法の請求項の機能、ステップ、および/または行為は、必ずしもいずれかの特定の順序で実行されない。さらに、本開示の要素が単数形で説明されるか、または特許請求の範囲に記載される可能性があるが、単数への限定が明示的に述べられない限り、複数も想定される。

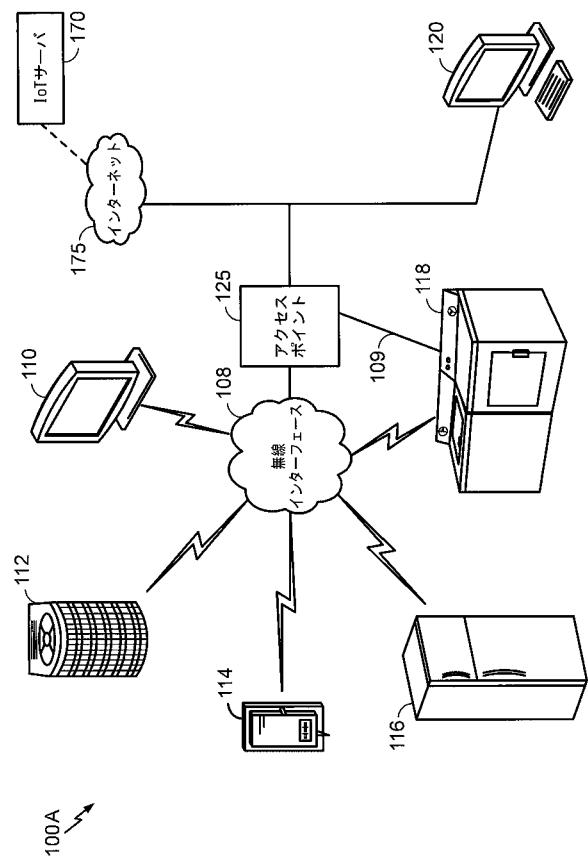
【符号の説明】

【0077】

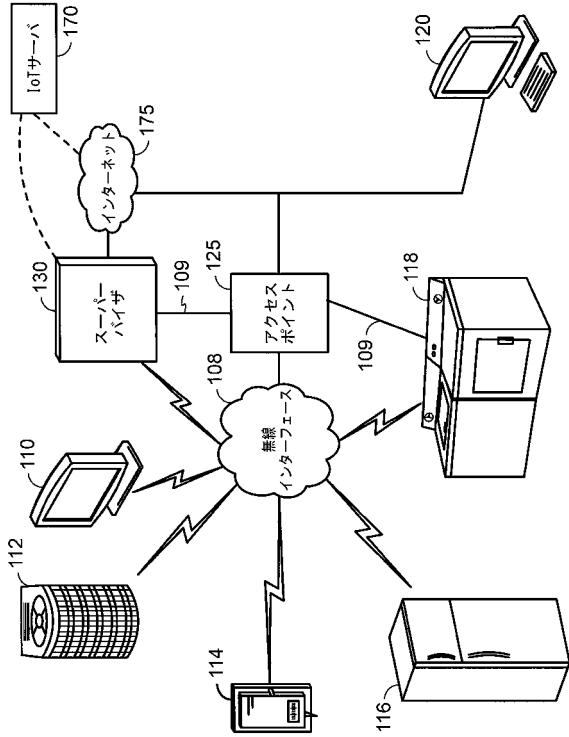
- 100A ワイヤレス通信システム
- 100B ワイヤレス通信システム
- 100C ワイヤレス通信システム
- 100D ワイヤレス通信システム
- 100E ワイヤレス通信システム
- 105 IoTデバイス
- 108 無線インターフェース
- 109 直接有線接続
- 110 テレビ、IoTデバイス
- 112 空調室外機、IoTデバイス
- 114 サーモスタット、IoTデバイス
- 116 冷蔵庫、IoTデバイス
- 116A IoTデバイス
- 116B IoTデバイス
- 118 洗濯機および乾燥機、IoTデバイス
- 120 コンピュータ、IoTデバイス
- 122A IoTデバイス
- 122B IoTデバイス
- 124A IoTデバイス
- 124B IoTデバイス
- 125 アクセスポイント
- 130 スーパーバイザデバイス
- 140 IoT SuperAgent
- 140A IoT SuperAgent
- 140B IoT SuperAgent

145	ゲートウェイ機能	
152	アプリケーションレイヤ	
154	CMPレイヤ	
156	トランスポートレイヤ	
158	物理レイヤ	
160	近隣IoTグループ	
160A	近隣IoTグループ	
160B	近隣IoTグループ	
170	IoTサーバ	10
175	インターネット	
200A	IoTデバイス	
200B	IoTデバイス	
202	プラットフォーム	
206	トランシーバ	
208	プロセッサ	
212	メモリ	
214	入力/出力(I/O)インターフェース	
222	電源ボタン	
224A	制御ボタン	20
224B	制御ボタン	
226	ディスプレイ	
300	通信デバイス	
400	通信デバイス	
405	論理	
410	論理	
415	論理	
420	論理	
425	論理	
702	セクション	
704	セクション	30
706	セクション	
708	セクション	
710	セクション	
712	セクション	

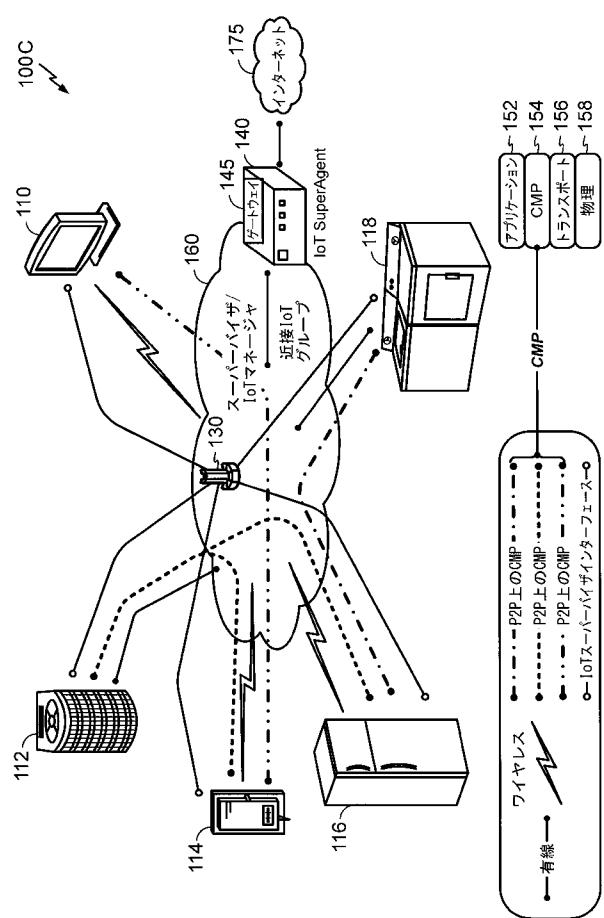
【図1A】



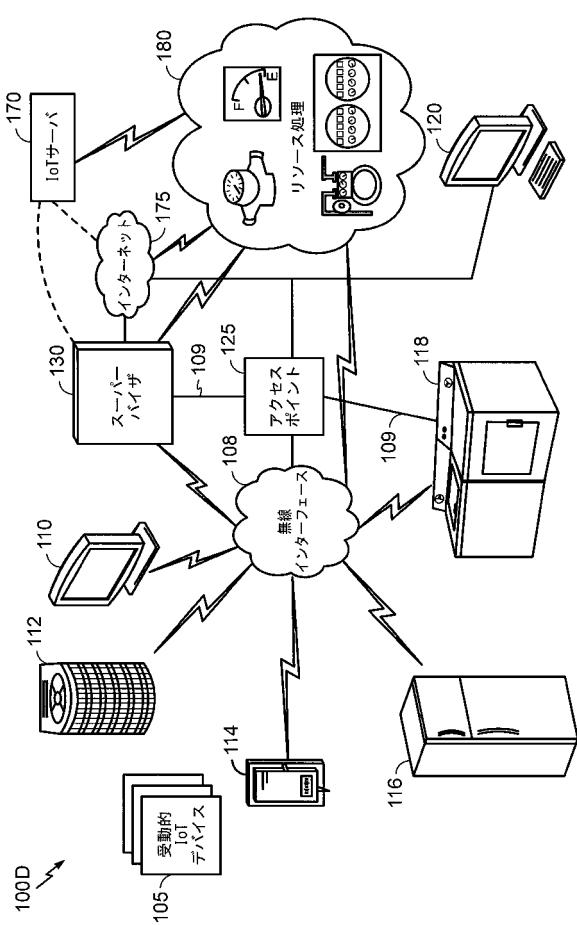
【図1B】



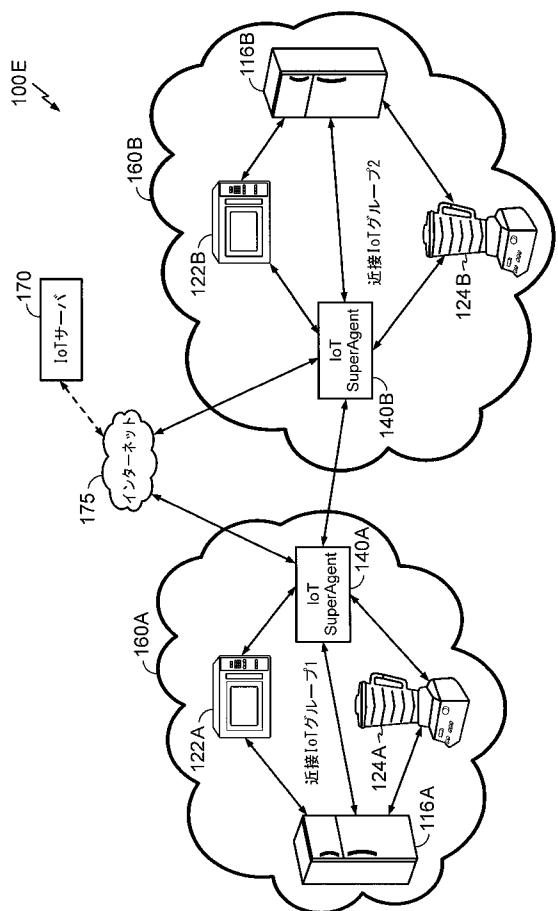
【図1C】



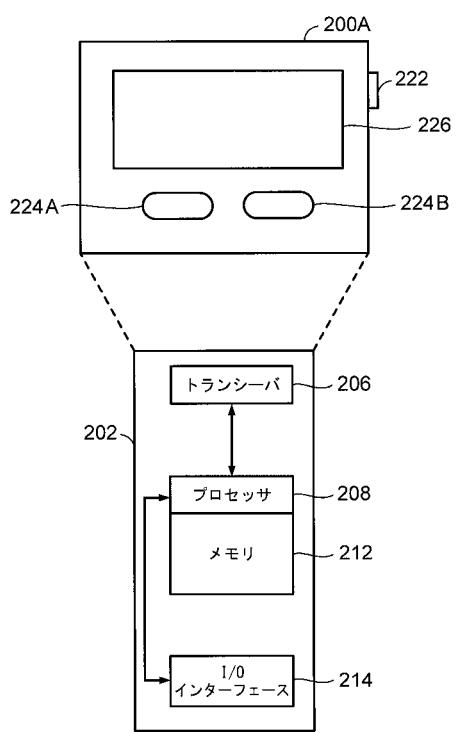
【図1D】



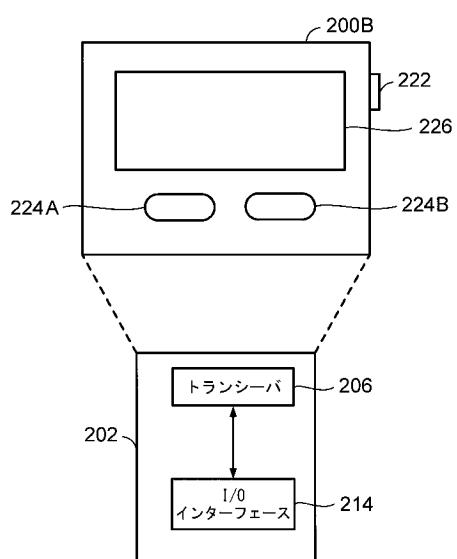
【図 1 E】



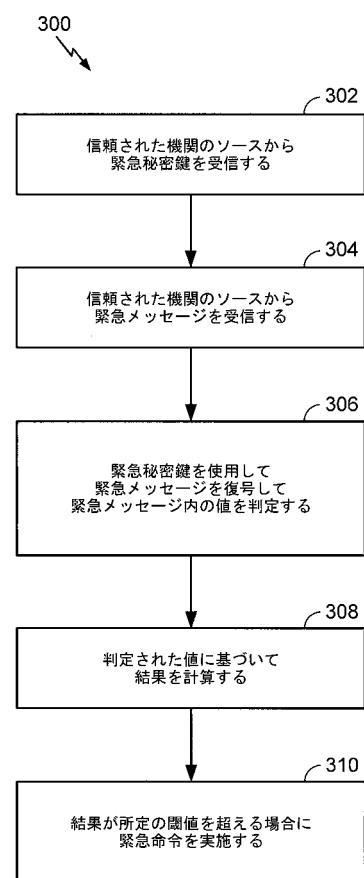
【図 2 A】



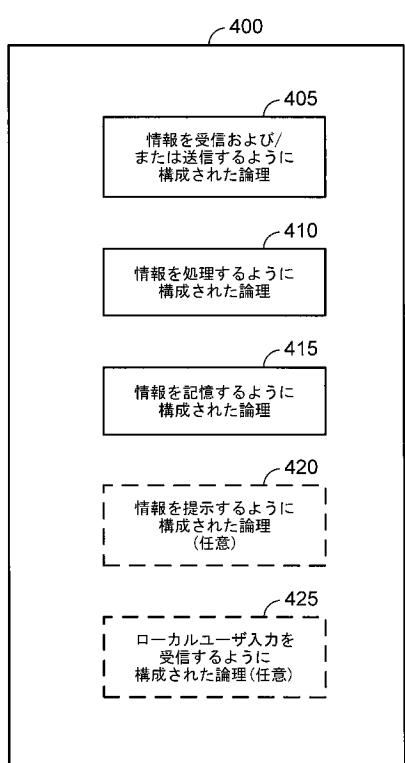
【図 2 B】



【図 3】



【図4】



【図5】

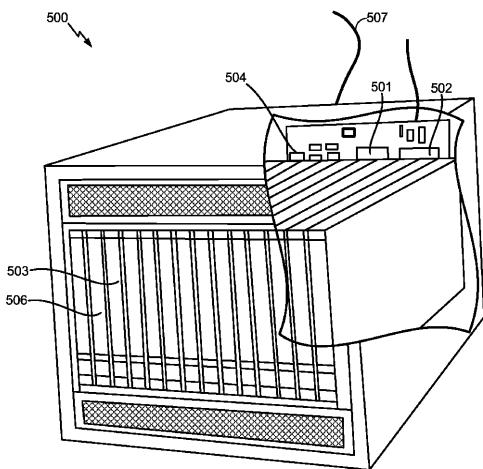
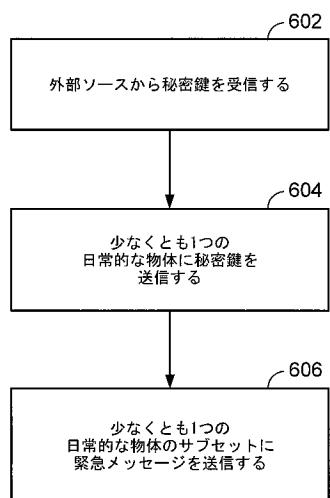
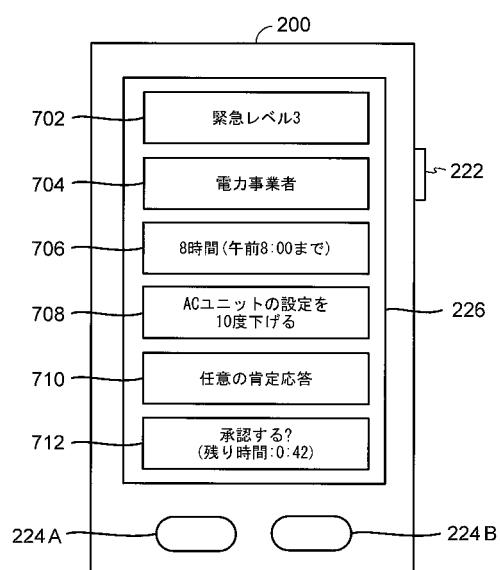


FIG. 5

【図6】



【図7】



【手続補正書】

【提出日】平成27年4月3日(2015.4.3)

【手続補正1】

【補正対象書類名】特許請求の範囲

【補正対象項目名】全文

【補正方法】変更

【補正の内容】

【特許請求の範囲】

【請求項1】

信頼された機関のソースからの緊急メッセージに基づいて緊急命令を実施するための方法であって、

モノのインターネット(IoT)デバイスにおいて、信頼された機関のソースからの緊急メッセージを受信するステップであって、前記緊急メッセージが、IoT秘密鍵を使用して暗号化された緊急秘密鍵を含む、ステップと、

前記IoTデバイスにおいて、前記緊急秘密鍵を使用して前記信頼された機関のソースからの前記緊急メッセージを復号して前記緊急メッセージ内の値を判定するステップと、

前記IoTデバイスにおいて、前記判定された値に基づいて結果を計算するステップと、

前記IoTデバイスにおいて、前記結果が所定の閾値を超えることに基づいて緊急命令を実施するステップと

を含む、方法。

【請求項2】

異なる緊急秘密鍵が、前記IoTデバイスに周期的に送信される請求項1に記載の方法。

【請求項3】

前記緊急秘密鍵が、第2の信頼された機関のソースから確認される請求項1に記載の方法。

。

【請求項4】

前記IoTデバイスにおいて、

次の物、すなわち、前記IoTデバイス、同じLAN上の別のIoTデバイス、および前記同じLAN上の非IoTデバイスのうちの少なくとも1つからのデータを確かめるステップと、

確かめられたデータと一緒に前記値を変数として式に組み込むステップと

をさらに含む請求項1に記載の方法。

【請求項5】

前記緊急命令が、以下の物、すなわち、停止命令、始動命令、出力増加命令、出力削減命令、および警報命令のうちの少なくとも1つを含む請求項1に記載の方法。

【請求項6】

前記緊急メッセージが、2つ以上のIoTデバイスへのブロードキャスト/マルチキャスト/ユニキャストメッセージである請求項1に記載の方法。

【請求項7】

前記緊急メッセージが、ネットワークに固有である請求項6に記載の方法。

【請求項8】

前記緊急命令が、少なくとも1つの非IoTデバイスに送信される請求項1に記載の方法。

【請求項9】

前記緊急秘密鍵が、前記IoT秘密鍵で暗号化される請求項1に記載の方法。

【請求項10】

前記IoTデバイスにおいて、グローバルなIoTの語彙を使用して前記緊急メッセージを解釈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11】

前記IoTデバイスにおいて、外部ソースからオーバーライド命令を受信するステップと

、前記IoTデバイスにおいて、前記オーバーライド命令に基づいて前記緊急命令を無効に

するステップと

をさらに含む請求項1に記載の方法。

【請求項 1 2】

前記オーバーライド命令が、前記信頼された機関のソースからのものである請求項11に記載の方法。

【請求項 1 3】

前記IoTデバイスが、前記緊急命令を実施しながら緊急モードで動作する請求項1に記載の方法。

【請求項 1 4】

命令が実施される度合いが、前記判定された値に基づく請求項1に記載の方法。

【請求項 1 5】

前記緊急メッセージが、次の物、すなわち、緊急事態のレベル、前記緊急メッセージを発する機関のレベル、前記緊急事態の予想される継続時間、実行すべき推薦される全般的な行為、肯定応答の要求、ユーザの認可の要求、および応答の要求のうちの少なくとも1つを含み得る請求項1に記載の方法。

【請求項 1 6】

前記IoTデバイスが、前記信頼された機関のソースに応答メッセージを送信する請求項1に記載の方法。

【請求項 1 7】

前記IoTデバイスが前記信頼された機関のソースに提供する情報が、リソースを実装することを助ける請求項16に記載の方法。

【請求項 1 8】

前記緊急メッセージが、前記IoTデバイスへの前記緊急メッセージの優先ルーティングを可能にするためのサービス品質パラメータを含む請求項1に記載の方法。

【請求項 1 9】

信頼された機関のソースからの緊急メッセージに基づいて緊急命令を実施するように構成されたプロセッサと、

信頼された機関のソースからの緊急メッセージを受信するように構成された論理手段であって、前記緊急メッセージが、モノのインターネット(IoT)秘密鍵を使用して暗号化された緊急秘密鍵を含む、論理手段と、

前記緊急秘密鍵を使用して前記信頼された機関のソースからの前記緊急メッセージを復号して前記緊急メッセージ内の値を判定するように構成された論理手段と、

前記判定された値に基づいて結果を計算するように構成された論理手段と、

前記結果が所定の閾値を超えることに基づいて緊急命令を実施するように構成された論理手段と

を含む装置。

【請求項 2 0】

異なる緊急秘密鍵が、前記装置に周期的に送信される請求項19に記載の装置。

【請求項 2 1】

前記緊急秘密鍵が、第2の信頼された機関のソースから確認される請求項19に記載の装置。

【請求項 2 2】

次の物、すなわち、前記装置、同じLAN上の別のIoTデバイス、および前記同じLAN上の非IoTデバイスのうちの少なくとも1つからのデータを確かめるように構成された論理手段と、

確かめられたデータと一緒に前記値を変数として式に組み込むように構成された論理手段と

をさらに含む請求項19に記載の装置。

【請求項 2 3】

前記緊急命令が、少なくとも1つの非IoTデバイスに送信される請求項19に記載の装置。

【請求項 2 4】

前記緊急秘密鍵が、前記IoT秘密鍵で暗号化される請求項19に記載の装置。

【請求項 2 5】

外部ソースからオーバーライド命令を受信するように構成された論理手段と、

前記オーバーライド命令に基づいて前記緊急命令を無効にするように構成された論理手段と

をさらに含む請求項19の装置。

【請求項 2 6】

前記外部ソースが、前記信頼された機関のソースである請求項25に記載の装置。

【請求項 2 7】

命令が実施される度合いが、前記判定された値に基づく請求項19に記載の装置。

【請求項 2 8】

前記緊急メッセージが、次の物、すなわち、緊急事態のレベル、前記緊急メッセージを発する機関のレベル、前記緊急事態の予想される継続時間、実行すべき推薦される全般的な行為、肯定応答の要求、ユーザの認可の要求、および応答の要求のうちの少なくとも1つを含み得る請求項19に記載の装置。

【請求項 2 9】

信頼された機関のソースが緊急メッセージを少なくとも1つのモノのインターネット(IoT)デバイスに送信するための方法であって、

IoT秘密鍵を外部ソースから受信するステップと、

前記外部ソースから1つまたは複数の緊急命令を受信するステップと、

前記緊急メッセージの前記1つまたは複数の緊急命令を符号化するステップであって、前記緊急メッセージが、前記IoT秘密鍵を使用して暗号化された緊急秘密鍵を含む、ステップと、

前記信頼された機関のソースから前記少なくとも1つのIoTデバイスのサブセットに前記緊急メッセージを送信するステップと

を含む、方法。

【請求項 3 0】

少なくとも1つのモノのインターネット(IoT)デバイスに緊急メッセージを送信するように構成されたプロセッサと、

外部ソースからIoT秘密鍵を受信するように構成された論理手段と、

前記外部ソースから1つまたは複数の緊急命令を受信するように構成された論理手段と、

前記緊急メッセージの前記1つまたは複数の緊急命令を符号化するように構成された論理手段であって、前記緊急メッセージが、前記IoT秘密鍵を使用して暗号化された緊急秘密鍵を含む、論理手段と、

前記少なくとも1つのIoTデバイスのサブセットに前記緊急メッセージを送信するように構成された論理手段と

を含む装置。

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2014/018313

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04W12/08
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

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, INSPEC, 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	EP 2 482 488 A1 (ZTE CORP [CN]) 1 August 2012 (2012-08-01) paragraph [0023] - paragraph [0030]; figure 2 paragraph [0031] - paragraph [0034]; figure 3 -----	1-30



Further documents are listed in the continuation of Box C.



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

13 June 2014

24/06/2014

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

Raposo Pires, João

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2014/018313

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 2482488	A1 01-08-2012	CN 102142974 A EP 2482488 A1 WO 2011091728 A1	03-08-2011 01-08-2012 04-08-2011

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,R,S,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,H,R,HU,ID,IL,IN,IR,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

(特許庁注：以下のものは登録商標)

1. FIREWIRE

(72)発明者 モハメド・アタウル・ラフマーン・シューマン

アメリカ合衆国・カリフォルニア・92121-1714・サン・ディエゴ・モアハウス・ドライブ・5775

(72)発明者 ビニタ・グプラ

アメリカ合衆国・カリフォルニア・92121-1714・サン・ディエゴ・モアハウス・ドライブ・5775

(72)発明者 アシュトーシュ・アガルワル

アメリカ合衆国・カリフォルニア・92121-1714・サン・ディエゴ・モアハウス・ドライブ・5775

(72)発明者 サンディープ・シャルマ

アメリカ合衆国・カリフォルニア・92121-1714・サン・ディエゴ・モアハウス・ドライブ・5775

F ターム(参考) 5C087 AA02 AA03 BB20 BB74 BB75 DD02 DD03 FF01 FF02 FF04
FF23 GG10 GG59
5J104 AA16 EA17 NA02 NA37 PA07
5K067 AA21 BB21 CC08 DD11 DD24 DD28 DD51 EE02 EE10 EE16
FF02 FF18 FF20 FF23 HH22 HH23 HH24 HH36
5K201 AA08 BA03 BC27 BD06 CC01 CC08 DA02 DC02 EA05 EB01
EB06 EC06 EC08 ED04 ED07 ED08 EE04 EF01 EF09