(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6441917号
(P6441917)
(45)発行日　平成30年12月19日(2018.12.19)　(24)登録日　平成30年11月30日(2018.11.30)

(51)Int.Cl.　F I
G06F 13/00 (2006.01)　G06F 13/00 358F

請求項の数 13 (全 20 頁)

(21)出願番号	特願2016-524203 (P2016-524203)
(86)(22)出願日	平成26年6月26日 (2014.6.26)
(65)公表番号	特表2016-525246 (P2016-525246A)
(43)公表日	平成28年8月22日 (2016.8.22)
(86)国際出願番号	PCT/US2014/044371
(87)国際公開番号	WO2014/210330
(87)国際公開日	平成26年12月31日 (2014.12.31)
審査請求日	平成29年6月12日 (2017.6.12)
(31)優先権主張番号	61/839,815
(32)優先日	平成25年6月26日 (2013.6.26)
(33)優先権主張国	米国 (US)
(31)優先権主張番号	14/314,498
(32)優先日	平成26年6月25日 (2014.6.25)
(33)優先権主張国	米国 (US)

(73)特許権者　507364838
クアルコム，インコーポレイテッド
アメリカ合衆国　カリフォルニア　９２１
２１　サン　ディエゴ　モアハウス　ドライブ　５７７５
(74)代理人　100108453
弁理士　村山　靖彦
(74)代理人　100163522
弁理士　黒田　晋平
(72)発明者　ビニタ・グプタ
アメリカ合衆国・カリフォルニア・９２１２１・サン・ディエゴ・モアハウス・ドライヴ・５７７５

審査官　佐々木　洋

最終頁に続く

(54)【発明の名称】モノのインターネット（ＩｏＴ）デバイスとのリモート通信のユーザ存在に基づく制御

(57)【特許請求の範囲】
【請求項１】
1つまたは複数のモノのインターネット(IoT)デバイスを含んだIoT近接ネットワークとのリモート通信を制御する方法であって、
前記IoT近接ネットワーク内にIoTユーザデバイスが存在するか否かを検出するステップと、
前記IoT近接ネットワーク内の前記1つまたは複数のIoTデバイスとのリモート通信を無効にするための1つまたは複数のリモート通信基準が満たされるかどうかを判定するステップと、
前記IoT近接ネットワークに前記IoTユーザデバイスが存在している場合、および前記リモート通信を無効にするための前記リモート通信基準が満たされる場合、前記リモート通信を無効にするステップと
を含み、
前記IoTユーザデバイスは、前記IoT近接ネットワーク内の登録された優先度レベルに関連付けられ、
前記リモート通信を無効にするステップが、前記IoT近接ネットワークに、所定の優先度レベルを有する前記IoTユーザデバイスが存在する場合に、前記1つまたは複数のIoTデバイスの第1のセットに対するリモート通信を無効にするステップを含む、方法。
【請求項２】
前記IoT近接ネットワーク内の前記IoTユーザデバイスの前記存在を検出するステップが

、前記IoTユーザデバイスの存在または不在をIoTスーパーエージェント/ゲートウェイに伝えるための制御アプリケーションに基づき、前記IoTスーパーエージェント/ゲートウェイが前記IoT近接ネットワーク内のリモート通信を制御するためのものであり、前記制御アプリケーションが、前記IoTユーザデバイス上で実行される、請求項1に記載の方法。

【請求項３】

前記IoT近接ネットワーク内の前記IoTユーザデバイスの前記存在を検出するステップが、IoTスーパーエージェント/ゲートウェイへの前記IoTユーザデバイスの登録の定期的な更新に基づき、前記IoTスーパーエージェント/ゲートウェイが前記IoT近接ネットワーク内のリモート通信を制御するためのものである、請求項1に記載の方法。

【請求項４】

前記IoT近接ネットワークへのリモート通信を無効にするための前記1つまたは複数のリモート通信基準が、1つもしくは複数のイベント、または1つもしくは複数の時間インスタンスの少なくとも1つを含む、請求項1に記載の方法。

【請求項５】

前記リモート通信を無効にするステップが、前記1つまたは複数のIoTユーザデバイスの選択された機能に関してリモート通信能力を選択的に無効にするステップを含む、請求項1に記載の方法。

【請求項６】

前記IoT近接ネットワーク内の1つまたは複数の追加のIoTユーザデバイスの存在を検出するステップと、前記IoT近接ネットワーク内の前記IoTユーザデバイスの1つまたは複数のサブセットの存在、および前記IoT近接ネットワーク内に存在している前記1つまたは複数のIoTデバイスの前記サブセットのそれぞれに関するリモート通信基準に基づいて、前記リモート通信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７】

1つまたは複数のモノのインターネット(IoT)デバイスを含んだIoT近接ネットワークとのリモート通信を制御する方法であって、

前記IoT近接ネットワーク内にIoTユーザデバイスが不在であるか否かを検出するステップと、

前記IoT近接ネットワーク内の前記1つまたは複数のIoTデバイスとのリモート通信を有効にするための1つまたは複数のリモート通信基準が満たされるかどうかを判定するステップと、

前記IoT近接ネットワークに前記IoTユーザデバイスが不在である場合、および前記リモート通信を有効にするための前記リモート通信基準が満たされる場合、前記リモート通信を有効にするステップと

を含み、

前記IoTユーザデバイスは、前記IoT近接ネットワーク内の登録された優先度レベルに関連付けられ、

前記リモート通信を有効にするステップが、前記IoT近接ネットワークに、所定の優先度レベルを有する前記IoTユーザデバイスが不在である場合に、前記1つまたは複数のIoTデバイスの第1のセットに対するリモート通信を有効にするステップを含む、方法。

【請求項８】

前記リモート通信が、前記IoTユーザデバイスまたはクラウドサービスによる前記IoT近接ネットワーク内の前記IoTデバイスの1つまたは複数のリモートアクセスを含む、請求項1または7に記載の方法。

【請求項９】

前記リモート通信が、前記IoT近接ネットワーク内の前記1つまたは複数の前記IoTデバイスから前記IoTユーザデバイスへメッセージまたはイベントの通知をリモーティングすることを含む、請求項1または7に記載の方法。

【請求項１０】

前記リモート通信基準が、前記リモート通信の方向に基づいている、請求項1または7に

記載の方法。
【請求項１１】
1つまたは複数のモノのインターネット(IoT)デバイスを含んだIoT近接ネットワークとのリモート通信を制御するための手段と、
前記IoT近接ネットワークにIoTユーザデバイスが存在しているかどうかを検出するための手段と、
前記IoT近接ネットワーク内の前記1つまたは複数のIoTデバイスとのリモート通信を無効にするための1つまたは複数のリモート通信基準が満たされるかどうかを判定するための手段と、
前記IoT近接ネットワークに前記IoTユーザデバイスが存在している場合、および前記リモート通信を無効にするための前記リモート通信基準が満たされる場合、前記リモート通信を無効にするための手段と
を含み、
前記IoTユーザデバイスは、前記IoT近接ネットワーク内の登録された優先度レベルに関連付けられ、
前記リモート通信を無効にするための手段が、前記IoT近接ネットワークに、所定の優先度レベルを有する前記IoTユーザデバイスが存在する場合に、前記1つまたは複数のIoTデバイスの第1のセットに対するリモート通信を無効にするための手段を含む、通信システム。
【請求項１２】
前記IoT近接ネットワークに前記IoTユーザデバイスが存在していない場合、および前記リモート通信を有効にするための前記リモート通信基準が満たされる場合、前記リモート通信を有効にするための手段
をさらに含む、請求項11に記載の通信システム。
【請求項１３】
前記リモート通信が、
前記IoTユーザデバイスまたはクラウドサービスによる前記IoT近接ネットワーク内の前記IoTデバイスの1つまたは複数のリモートアクセスと、
前記IoT近接ネットワーク内の前記1つまたは複数の前記IoTデバイスから前記IoTユーザデバイスへメッセージまたはイベントの通知をリモーティングすることと
を含む、請求項11に記載の通信システム。
【発明の詳細な説明】
【技術分野】
【０００１】
米国特許法第119条に基づく優先権の主張
本特許出願は、本出願の譲受人に譲渡され、その全体が参照により本明細書に明確に組み込まれる、2013年6月26日に出願された、係属中の「USER PRESENCE BASED CONTROL OF REMOTE ACCESS TO INTERNET OF THINGS (IoT) DEVICES」という名称の仮特許出願第61/839,815号に基づく利益を主張する。
【０００２】
この開示の実施形態は、IoTデバイスへのリモートアクセスおよび/またはIoTデバイスからリモート通知を受信することに関する。より詳細には、例示的実施形態は、IoTデバイスへリモートアクセスすること/IoTデバイスから通知をリモーティングすることを含むリモート通信を、IoTデバイスの指定された近接ネットワーク内の他のリモート通信基準間の1人または複数のユーザの存在または不在を含むリモート通信基準に基づいて無効または有効にするためのシステムおよび方法を対象とする。
【背景技術】
【０００３】
インターネットは、標準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))を使用して互いに通信する、相互接続

されたコンピュータならびにコンピュータネットワークのグローバルシステムである。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、日常の物が、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り得るという発想に基づく。

【０００４】

たとえば住宅改善に関連する市場動向は、サービスプロバイダが「N」プレイ(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)を販売し、ホームネットワークを拡大することによる強化を含む、新しい「スマート」サービスのための開発を推進している。IoTのいくつかのアプリケーションは、自宅またはオフィス内の事実上いかなるデバイスまたは電化製品も集中制御することができるスマートホームおよびビルディングを含む。

【０００５】

したがって、近い将来には、増大するIoT技術の開発により、自宅で、車中で、職場で、およびその他の多くの場所で、数多くのIoTデバイスがユーザを取り囲むことになるであろう。たとえば、そこでのホーム設定では、指定された近傍内に、ホームWi-Fiネットワークに接続された数多くのIoTデバイスが存在している可能性がある。このようなネットワークは、リモートネットワークと対照的に「近接ネットワーク」と呼ばれてよく、ユーザはリモートネットワークを通じて近接ネットワーク上のIoTデバイスにリモートでアクセスすることができる。より詳細には、電化製品、TV、照明器具、エアコン、音楽システム、車庫のドア、ホームセキュリティシステム、ファン、スプリンクラーシステム、電子レンジ、オーブン、食洗機、洗濯機および乾燥機など、何百ものIoTデバイスが、近接ホームIoTネットワークに接続され得る。ユーザが、ホームIoTネットワークの外から、たとえば、ユーザのオフィスから、リモートでこれらのデバイスの1つまたは複数にアクセスし、制御することを望むことがある。したがって、ホームIoTネットワークへのリモートアクセス能力を提供することが望ましい。

【０００６】

しかしながら、このようなリモートアクセスを許可することは、セキュリティの問題を引き起こす。たとえば、ユーザのホームIoTネットワークへのリモートアクセス/制御を有効にすると、ネットワークセキュリティ脅威に対する脆弱性が生じ、ホームIoTネットワークは無許可のユーザまたは悪意のあるエージェントからの攻撃に対して開放されたままとなる。IoTデバイスは、ステータス更新および重要なイベント通知をユーザに提供するように構成されることもある。しかしながら、ユーザが遠隔地にいるとき、リモート通信が可能であるネットワークを通じて、これらの通知がユーザに提供される場合、無許可のユーザがこれらのリモート通知にアクセスするおそれがあり、これもまた、許可されたユーザへのセキュリティおよびプライバシー脅威に繋がる可能性がある。

【発明の概要】

【発明が解決しようとする課題】

【０００７】

よって、IoTデバイスとのリモート通信を許可することから発生する可能性のある攻撃の危険を減らす必要がある。

【課題を解決するための手段】

【０００８】

例示的実施形態は、1つまたは複数のモノのインターネット(IoT)デバイスを含んだIoT近接ネットワークとのリモート通信を制御するためのモノのインターネット(IoT)スーパーエージェント/ゲートウェイに関連するシステムおよび方法を含む。IoT近接ネットワーク内のIoTユーザデバイスの存在が検出される。IoT近接ネットワークにIoTユーザデバイスが存在している場合、およびリモート通信を無効にするためのリモート通信基準が満たされる場合、リモート通信は無効にされる。IoT近接ネットワークにIoTユーザデバイスが存在しない場合、およびリモート通信を有効にするためのリモート通信基準が満たされる

場合、リモート通信は有効にされる。リモート通信は、IoTユーザデバイスによるIoTデバイスの1つまたは複数のリモートアクセス、ならびに1つまたは複数のIoTデバイスからIoTユーザデバイスへ、メッセージまたはイベントの通知をリモーティングすることを含む。

【０００９】

たとえば、例示的実施形態は、1つまたは複数のモノのインターネット(IoT)デバイスを含んだIoT近接ネットワークとのリモート通信を制御するための方法に関し、この方法は、IoT近接ネットワーク内のIoTユーザデバイスの存在を検出するステップと、IoT近接ネットワーク内の1つまたは複数のIoTデバイスとのリモート通信を無効にするための1つまたは複数のリモート通信基準が満たされるかどうかを判定するステップとを含む。IoT近接ネットワークにIoTユーザデバイスが存在している場合、およびリモート通信を無効にするためのリモート通信基準が満たされる場合、リモート通信は無効にされる。

【００１０】

別の例示的実施形態は、1つまたは複数のモノのインターネット(IoT)デバイスを含んだIoT近接ネットワークとのリモート通信を制御するための方法を対象とし、この方法は、IoT近接ネットワーク内のIoTユーザデバイスの不在を検出するステップと、IoT近接ネットワーク内の1つまたは複数のIoTデバイスとのリモート通信を有効にするための1つまたは複数のリモート通信基準が満たされるかどうかを判定するステップとを含む。IoT近接ネットワークにIoTユーザデバイスが不在である場合、およびリモート通信を有効にするためのリモート通信基準が満たされる場合、リモート通信は有効にされる。

【００１１】

さらに別の例示的実施形態は、1つまたは複数のモノのインターネット(IoT)デバイスを含んだIoT近接ネットワークとのリモート通信を制御するように構成されたIoTスーパーエージェント/ゲートウェイと、IoT近接ネットワークにIoTユーザデバイスが存在しているかどうかを検出するように構成された存在検出ブロックと、IoT近接ネットワーク内の1つまたは複数のIoTデバイスとのリモート通信を有効にするまたは無効にするための1つまたは複数のリモート通信基準が満たされるかどうかを判定するように構成されたリモートアクセス/リモーティング制御ルールブロックとを含んだ装置を対象とする。この装置は、IoT近接ネットワークにIoTユーザデバイスが存在している場合、およびリモート通信を無効にするためのリモート通信基準が満たされる場合、リモート通信を無効にするように構成された、リモートアクセス/リモーティング有効/無効ブロックをさらに含む。

【００１２】

さらに別の例示的実施形態は、1つまたは複数のモノのインターネット(IoT)デバイスを含んだIoT近接ネットワークとのリモート通信を制御するための手段と、IoT近接ネットワークにIoTユーザデバイスが存在しているかどうかを検出するための手段と、IoT近接ネットワーク内の1つまたは複数のIoTデバイスとのリモート通信を有効または無効にするための1つまたは複数のリモート通信基準が満たされるかどうかを判定するための手段と、IoT近接ネットワークにIoTユーザデバイスが存在している場合、およびリモート通信を無効にするためのリモート通信基準が満たされる場合、リモート通信を無効にするための手段とを含む、通信システムを対象とする。

【００１３】

本開示の諸態様およびその付随する利点の多くは、単に本開示の説明のために、本開示の限定のためにではなく提示される添付の図面と関連付けて検討されると、次の詳細な説明を参照することによってよりよく理解されるようになるので、本開示の諸態様およびその付随する利点の多くのさらに完全な理解が容易に得られるであろう。

【図面の簡単な説明】

【００１４】

【図１】本発明の一態様によるワイヤレス通信システムのハイレベルシステムアーキテクチャを示す図である。

【図２】この開示の諸態様により近接ネットワークでIoTデバイスとのリモート通信を行うことができるIoT近接ネットワークを含んだ例示的ワイヤレス通信システムを示す図で

ある。
【図３】例示的リモート通信基準に基づいてIoT近接ネットワーク内のIoTデバイスとのリモート通信を制御することに関するこの開示の態様を示す図である。
【図４】例示的リモート通信基準に基づいてIoT近接ネットワークのIoTデバイスとのリモート通信を制御する例示的方法を示す図である。
【図５】例示的リモート通信基準に基づいてIoT近接ネットワークのIoTデバイスとのリモート通信を制御する例示的方法を示す図である。
【発明を実施するための形態】
【００１５】
モノのインターネット(IoT)デバイス間の近接検出の例示的実施形態に関する特定の例を示すために、次の説明および関連する図面で様々な態様が開示される。代替的実施形態は、この開示を読むと当業者には明らかであり、本開示の範囲または趣旨を逸脱することなく構築され、実践され得る。加えて、本明細書で開示される態様および実施形態の関連する詳細を不明瞭にしないように、よく知られている要素は詳細には説明されず、または省略され得る。
【００１６】
「例示的」という用語は、本明細書では「例、事例、または実例として役に立つこと」を意味するように使用される。「例示的」として本明細書で説明するいかなる実施形態も、他の実施形態よりも好ましいまたは有利であると必ずしも解釈されるべきではない。同様に、「実施形態」という用語は、すべての実施形態が、論じられている特徴、利点、または動作モードを含むことを必要としない。
【００１７】
本明細書で使用される用語は、特定の実施形態を説明するだけであり、本明細書で開示される任意の実施形態を制限すると解釈されるべきである。本明細書で使用される単数形「a」、「an」、および「the」は、文脈が別段に明確に示さない限り、複数形をも含むものとする。さらに、「含む(comprises)」、「含んでいる(comprising)」、「含む(includes)」、および/または「含んでいる(including)」という用語は、本明細書で使用されると、述べられた特徴、整数、ステップ、動作、要素、および/または構成要素の存在を規定するが、1つまたは複数の他の特徴、整数、ステップ、動作、要素、構成要素、および/またはそれらのグループの存在または追加を排除しないことが理解されるだろう。
【００１８】
さらに、多くの態様が、たとえばコンピュータデバイスの要素によって実行される一連のアクションの観点から説明される。本明細書に記載する様々なアクションは、特定の回路(たとえば、特定用途向け集積回路(ASIC))によって、1つまたは複数のプロセッサによって実行されているプログラム命令によって、または両方の組合せによって行われることが可能であることは認識されよう。さらに、本明細書に記載するこれらの一連のアクションは、実行されると関連するプロセッサに本明細書に記載する機能を行わせる、対応するコンピュータ命令のセットを記憶した任意の形態のコンピュータ可読記憶媒体内で完全に具体化されるとみなすことができる。このように、本開示の様々な態様は、いくつかの異なる形態で具体化されることが可能であり、そのすべてが請求される主題の範囲内であると考えられている。また、本明細書に記載する態様のそれぞれについては、このようないかなる態様の対応する形態も、本明細書ではたとえば、記載するアクションを行う「ように構成された論理」として記載されることがある。
【００１９】
本明細書で使用する「モノのインターネットデバイス」(すなわち「IoTデバイス」)という用語は、アドレス指定可能なインターフェース(たとえば、インターネットプロトコル(IP)アドレス、Bluetooth(登録商標)識別子(ID)、近距離無線通信(NFC: near-field communication)IDなど)を有し、有線またはワイヤレス接続を通じて1つまたは複数の他のデバイスに情報を送信することができる任意の物(たとえば、電化製品、センサーなど)を指すことができる。IoTデバイスは、クイックレスポンス(QR)コード、無線周波数識別(RFID

)タグ、NFCタグなどの受動通信インターフェース、または、モデム、送受信機、送信機-受信機などの能動通信インターフェースを有し得る。IoTデバイスは、中央処理装置(CPU)、マイクロプロセッサ、ASICなどの中に組み込まれること、ならびに/あるいは、それらによって制御/監視されることが可能であり、ローカルアドホックネットワークまた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た特定の属性セット(たとえば、IoTデバイスがオンであるか、もしくはオフであるか、開いているか、もしくは閉じているか、アイドルであるか、もしくはアクティブであるか、タスク実行のために利用可能であるか、もしくはビジーであるかなど、冷房機能であるか、もしくは暖房機能であるか、環境監視機能であるか、もしくは環境記録機能であるか、発光機能であるか、音響放射機能であるかなど、デバイスの状態またはステータス)を有し得る。

【００２０】

例示的実施形態は、リモートでアクセスされ得るIoTデバイスに関することがある。リモートアクセスは、ユーザの自宅内にある、またはより一般的には任意の「近接ネットワーク」内にあるIoTデバイスに利用可能であってもよく、このIoTデバイスは、あらかじめ定義された地理的境界内のデバイスまたはホームネットワークに直接接続されたデバイスを指すことができる。たとえば、ユーザが、遠隔地から、またはユーザが近接ホームネットワークから離れているとき、セキュリティカメラを監視する、暖房、冷却、空調(AC)システムを操作する、家の玄関ドアを操作する、車庫のドアを開ける、その他を行うことができることがある。さらに、IoTデバイスは、ユーザに(たとえば、裏庭のドアの鍵がかかっていないという)メッセージまたはイベントの通知を送信することができることもある。このような通知は、ユーザが遠隔地にいる、または家もしくはあらかじめ定義された近接位置から離れているとき、提供されることも可能である。このような通知をIoTデバイスによって遠隔地のユーザに送信することは、本明細書では、通知を「リモーティングする」、または通知が「リモーティングされる」と呼ばれ、通知は、メッセージまたはイベントの通知を含む。より一般的には、本明細書で述べる「リモート通信」は、リモートネットワークまたは通信媒体を介したIoT近接ネットワーク中のIoTデバイスの1つまたは複数のリモートアクセス、ならびに、リモートネットワークまたは通信媒体を介して送信またはブロードキャストされたIoT近接ネットワーク内の1つまたは複数のIoTデバイスによる通知のリモーティングを含む。このようなリモート通信は、脆弱である、またはリモート通信を有効にするリモートネットワークもしくは通信媒体を通じてセキュリティ脅威にさらされる可能性がある。

【００２１】

したがって、例示的態様は、IoTデバイスの指定された近接ネットワークに対するリモートアクセスおよび/またはリモーティング機能の安全性を向上させること、およびIoTデバイスをセキュリティの脅威にさらすことを減らすことを対象とする。いくつかの態様では、脅威にさらすことは、継続時間を減らすこと、および/または近接ネットワーク内のIoTデバイスへの/IoTデバイスからのリモート通信が許可される状況を制御することによって減らされる。たとえば、リモートアクセスおよびリモーティングは、ユーザが自宅または近接ネットワークから離れているときだけ許可されることが可能である。ユーザが近接ネットワーク内にいるとき、ユーザはローカルまたはホームネットワークを介してIoTデバイスにアクセスすることができる可能性があるので、ユーザがリモート接続を介してIoTデバイスにアクセスする必要はない可能性がある。したがって、リモートアクセスが必要とされないときに、リモートアクセスを完全に遮断することによって、ユーザが家にいるとき、リモート接続を介して外部の脅威にさらされることは、最小限にされ得る。同様に、リモーティングは、ユーザがホームネットワーク内にいるとき、オフにされることも可能である。たとえば、ユーザの家の裏庭のドアの鍵がかかっていないというIoTデバイスからの通知、またはユーザの家の窓が壊れているというIoTデバイスからの通知は、ユーザが家にいるとき、リモートネットワークに送信されないようにする、またはリモーティングされないようにすることができる。

【００２２】

したがって、実施形態は、近接ネットワーク内の1人または複数のユーザの存在または不在を検出または認識する、ならびにリモートアクセスおよびリモーティングの無効化または有効化をこの検出または認識に基づかせるように構成される。このように、ホームネットワークまたは任意の他の指定された近接ネットワーク内のIoTデバイスは、少なくともリモートアクセスおよび/またはリモーティングが無効であるとき、その時間の間は外部の攻撃から安全にされ得る。よって、いくつかの事例では、近接ネットワークの近傍または近くの1人または複数の主要なユーザの存在は、リモートアクセスおよび/またはリモーティングを有効または無効にするために利用され得る。いくつかの他の追加的または代替的基準および/またはイベントが、この開示において、リモートアクセスおよび/またはリモーティングに制限を加えるために使用され得る例示的要因として提供される。次に諸実施形態による例示的システムおよび方法について、図を参照して説明する。

【００２３】

図1を参照すると、この開示の態様に従ったワイヤレス通信システム100のシステムアーキテクチャのハイレベル図が示されている。ワイヤレス通信システム100は、複数のIoTデバイスを含み、この複数のIoTデバイスが、図のように、テレビ110と、エアコン(AC)ユニット112と、サーモスタット114と、冷蔵庫116と、洗濯機および乾燥機118とを含む。IoTデバイス110～118は、エアインターフェース108および/または直接有線接続109を通じ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。エアインターフェース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)に準拠することができる。インターネット175は、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(便宜上図1には示さず)を含み、標準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)を使用して異なるデバイス/ネットワークの間で通信する、相互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グローバルシステムである。例示的実施形態では、リモートアクセスおよび/またはリモーティングは、以下にさらに説明するように、たとえば、インターネット175を介して可能であることがある。

【００２４】

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が、(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ベースのネットワークを通じて)直接インターネット175に接続して示されている。コンピュータ120は、代替的に、または追加的に、インターネット175への有線接続を有することができ、またはコンピュータ120は、アクセスポイント125に直接接続されることができる。デスクトップコンピュータとして例示されているが、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り得る。コンピュータ120は、IoTデバイスである、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機能を含んでいることがある。

【００２５】

IoTサーバ170は、オプションとすることができ、複数の構造的に別個のサーバとして実装されてもよいし、あるいは単一サーバに対応してもよい。IoTデバイス110～120のグループは、ピアツーピア(P2P)ネットワークであってもよく、エアインターフェース108および/または有線接続109を通じて互いに直接通信することができる。代替的に、または追加的に、IoTデバイス110～120の一部または全部は、エアインターフェース108および有線接続109から独立した通信インターフェースで構成されてもよい。たとえば、エアインターフェース108がWi-Fiインターフェースに対応する場合、IoTデバイス110～120のいくつかは、互いにまたは他の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ことがある。

【００２６】

さらに、ワイヤレス通信システム100は、コントローラデバイス130を含むことができ、これは代替的にはIoTスーパーバイザまたはマネージャと呼ばれることもある。コントローラデバイス130がスタンドアロンデバイスまたはユニットとして図示されているが、い

くつかの実施において、コントローラデバイス130は、コンピュータ120など、IoTデバイスデバイス110～120の1つに統合されることがある。たとえば、コントローラデバイス130は、スマートフォンとして実装されたコンピュータ120に統合されることがある。いくつかの態様では、コントローラデバイス130は、物理デバイス、または物理デバイスで動作するソフトウェアアプリケーションであってよい。1つの実施形態では、コントローラデバイス130は、一般的に、ワイヤレス通信システム100の他の様々な構成要素を観察する、監視する、制御する、または別の方法で管理することがある。たとえば、コントローラデバイス130は、IoTデバイスと対話するために、エアインターフェース108および/または直接有線接続109を通じてアクセスネットワーク(たとえば、アクセスポイント125)と通信することができ、このような対話は、ワイヤレス通信システム100の様々なIoTデバイス110～120と関連する属性、活動、または他の状態を監視すること、または管理することを含むことができる。対話は、様々なIoTデバイス110～120からイベントまたはステータス更新の通知を受信することを含むこともでき、これはいくつかの事例では、リモーティングされることがある。例示的実施形態では、エアインターフェース108および/または直接有線接続109を含むアクセスネットワークは、IoTデバイス110～120を含んだ近接ネットワークの一部であり得る。コントローラデバイス130は、前述のように、スマートフォンもしくは携帯デバイスである、またはこれに備わっていることがあり、これを介してユーザは、近接ネットワークを通じてIoTデバイス110～120と対話することができる。コントローラデバイス130の諸態様は、ユーザインターフェースを含むことができる、スマートフォン「アプリ(App)」などの、ソフトウェアアプリケーションを使用して実装されることもある。

【００２７】

コントローラデバイス130は、インターネット175への、およびオプションとしてIoTサーバ170への(点線として示す)、有線またはワイヤレス接続を有することもできる。コントローラデバイス130は、インターネット175および/またはIoTサーバ170から情報を取得することができ、これを使用して、様々なIoTデバイス110～120と関連する属性、活動、または他の状態をさらに監視する、または管理することができる。例示的実施形態では、コントローラデバイス130は、たとえば、IoTデバイス110～120と対話するために、近接ネットワークから空間的に離れた遠隔地からインターネット175に接続することができる。これは、IoTデバイス110～120のリモートアクセス、ならびにIoTデバイス110～120からのリモーティングを含むことができ、これについては図2を参照してさらに説明する。

【００２８】

ワイヤレス通信システム100は、ゲートウェイまたはIoTスーパーエージェント/ゲートウェイ145を含むこともあり、これについては以下の章でさらに詳細に説明する。簡潔には、IoTスーパーエージェント/ゲートウェイ145は、近接ネットワークのIoTデバイス110～120と通信して、これらを監視および制御する、ならびにIoTデバイス110～120から通知を受信することができ、このような通知は、イベント検出またはステータス変化に基づいてデバイス自体によって開始されることが可能であり、したがって、IoTデバイス110～120からの通知は、たとえば、スーパーエージェント145からの問い合わせにだけ基づく必要はない。ゲートウェイまたはIoTスーパーエージェント/ゲートウェイ145は、ユーザがリモートでIoTデバイス110～120にアクセスするためのおよび/またはユーザにIoTデバイス110～120による通知をリモーティングするためのインターフェースを提供することができる。

【００２９】

図2を参照すると、ワイヤレス通信システム200を含む例示的実施形態が示されている。一般に、ワイヤレス通信システム200は、図1のワイヤレス通信システム100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むことができ、説明を簡潔および容易にするために、ワイヤレス通信システム200のいくつか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ワイヤレス通信システム100に関してすでに提供されている限りにおいて、ここでは省略されることがある。ワイヤレス通信システム200は、ローカルに接

続されたIoTデバイス110～118のグループを含んだIoT近接ネットワーク160を示す。コントローラデバイス130とIoTデバイス110～118との間に概略的通信リンク(有線またはワイヤレスであることがある)が示されているが、当技術分野で知られているように、IoTデバイス110～118間の他の様々なピアツーピア通信、ならびにコントローラデバイス130が可能であるが、簡潔にするためにここでは説明を省略する。

【００３０】

近接ネットワーク160は、いくつかの例ではユーザのホームネットワークであり得る。IoTデバイス110～118は、インターネット175に接続されたIoTスーパーエージェント/ゲートウェイ145を介して互いに接続されるおよび/または通信することが可能である。IoTスーパーエージェント/ゲートウェイ145は、近接ネットワーク160内のIoTデバイス110～118を管理および制御する機能を提供することができる。IoTスーパーエージェント/ゲートウェイ145は、近接ネットワーク160内のIoTデバイス110～118から通知を受信するための機能を提供することができ、いくつかの事例では、IoTスーパーエージェント/ゲートウェイ145は、インターネット175を通じてユーザにこれらの通知をリモーティングすることができる。いくつかの態様では、コントローラデバイス130が、近接ネットワーク160の外に位置している可能性があり(図2には示していないが、図3に示している)、IoTスーパーエージェント/ゲートウェイ145が、リモートでIoTデバイス110～118にアクセスし、これを制御するための、ならびに、たとえばコントローラデバイス130を介した、IoTデバイス110～118からの通知をリモーティングするための、インターフェースを提供することもできる。本明細書では詳細に説明しない態様では、IoTスーパーエージェント/ゲートウェイ145が、近接ネットワークの外の1つまたは複数のIoTデバイス(またはいくつかの事例では、IoTデバイスの1つもしくは複数のグループ)と通信し、これを管理することができることもある。ハイレベルでは、コントローラデバイス130が、IoTスーパーエージェント/ゲートウェイ145を介してIoTデバイス110～118と、近接ネットワーク160の外から通信することができる。IoTスーパーエージェント/ゲートウェイ145が、アクセスポイント125の機能に対応する、またはこれを含むことができる。あるいは、IoTスーパーエージェント/ゲートウェイ145が、IoTサーバ170などのIoTサーバの機能に対応する、またはこれを含むことができる。一般に、IoTスーパーエージェント/ゲートウェイ145が、ゲートウェイ機能145をカプセル化することができ、これについては実施形態に関してさらに詳細に説明する。

【００３１】

図3を参照すると、本開示のいくつかの主要な態様を強調するために、ワイヤレス通信システム300の簡略図が示されている。多くの態様では、ワイヤレス通信システム300は、図1および図2のワイヤレス通信システム100およびワイヤレス通信システム200と同様であり、よって、簡潔にするために、ここでは共通の特徴の詳細な説明を省略する。図3では、コントローラデバイス130が、2つの別個の位置に描かれた、すなわちIoT近接ネットワーク160の近傍に1度、および遠隔地に1度描かれた、ユーザ電話として示されている。IoTデバイス301～303は、図1～図2のIoTデバイス110～118などの、例示的IoTデバイスの一般的描写である。IoTデバイス301～303は、IoT近接ネットワーク160内に位置している。IoTデバイス301～303は、互いに通信することができ(点線で示す)、IoTスーパーエージェント/ゲートウェイ145と、ならびに、ユーザ電話130がIoT近接ネットワーク160内にある間はコントローラデバイス/ユーザ電話130と、直接通信することもできる。いくつかの態様では、IoTデバイス301～303などの物体は、これらが物理的にあらかじめ定義された地理的境界または同様の物理的範囲内に位置している場合、IoT近接ネットワーク160に属していると定義され得る。いくつかの態様では、IoT近接ネットワーク160内のデバイスは、IoT近接ネットワーク160の外のデバイス/物体からアクセス可能および/または制御可能である必要があることがある。たとえば、ユーザは、ユーザのオフィスなどの遠隔地にいるときに、近接ネットワーク160のIoTデバイス110～118からの通知を制御および/または受信したいと思うことがある。いくつかの態様では、リモートアクセスは、ユーザまたはユーザの電話130によって開始されるのではなく、クラウドサービス(インターネット175の一部として示される)によって開始されることもある。ユーザまたはクラウドサービスによ

るこのようなアクセスをサポートするために、IoTスーパーエージェント/ゲートウェイ145が、IoT近接ネットワーク160へのゲートウェイとして機能し、リモートでIoTデバイス110～118にアクセスするための、および/またはIoTデバイス110～118からの通知をリモーティングするためのインターフェースを提供することができる。しかしながら、インターネット175を通じたインターネットベースの攻撃などの攻撃からIoT近接ネットワーク160を保護するために、IoTスーパーエージェント/ゲートウェイ145が、ルールのセットを実施する、または満たされるべき一定の基準を課すことができ、これに基づいてリモートアクセスおよび/またはリモーティングが有効または無効にされ得る。

【００３２】

1つの態様では、基準は、IoT近接ネットワーク160内のユーザ電話130の存在または不在に関することがある。たとえば、イベントまたは時間に基づくことが可能である、様々な他のリモートアクセスおよびリモーティングルールまたは基準もまた考えられる。本明細書で説明する、ユーザによる近接ネットワーク内のIoTデバイスのリモート「アクセス」は、実質的に、ユーザによって開始される第1の通信の方向を(たとえこの通信がIoTデバイスとユーザとの間にいくつかの往復の対話を含んでいることがあるとしても)指すことができる。さらに、第1の方向は、クラウドサービスによって開始され得る通信もまた含むことに留意されたい。しかしながら、説明を容易にするために、この開示は、ユーザによって開始される通信に焦点を合わせることにするが、このような通信はまた、クラウドサービスによって開始され得ることは理解されよう。一方、近接ネットワーク内のIoTデバイスからユーザへの「リモーティング」は、IoTデバイスによって開始される反対の、第2の通信の方向を指すことができる。集合的に、これらの2つの通信の方向は、「リモート通信」と呼ばれることがあり、これは場合によって、リモートアクセスならびにリモーティングを含むことができる。それに応じて、リモート通信(リモートアクセスおよび/またはリモーティング)を有効または無効にするために使用される基準は、リモート通信基準と呼ばれることがある。リモートユーザと近接ネットワーク内のIoTデバイスとの通信という状況における様々なリモート通信基準について、本明細書では特定の例およびシナリオを参照して説明する。しかしながら、これらの例およびシナリオは、説明のために提供されるにすぎず、限定として解釈されてはならないことは理解されよう。したがって、これらのリモート通信基準は、1人または複数のユーザと近接ネットワークのIoTデバイスとのリモート通信を、近接ネットワーク内のユーザの存在または不在に基づいて有効または無効にするために使用され得る任意の他のルールまたは基準を含むことができる。

【００３３】

よって、リモートアクセスルールがユーザの存在に基づくことが可能である態様では、リモートアクセスルールは、ユーザ電話130が遠隔地にあるとき、ユーザ電話130がIoTスーパーエージェント/ゲートウェイ145を介して、インターネット175を通じて(パス306、308を通じて)IoTデバイス301～303と通信または対話することができるように、実施され得る。先に示したように、インターネット175がクラウドサービスを含むこともでき、クラウドサービスが開示する態様によりリモート通信を開始することができてもよい。ユーザ電話130は、IoTデバイス301～303をリモートで制御する、ならびにIoTデバイス301～303からのリモート通知を受信するために使用され得る、制御アプリケーションなどのモバイルアプリケーションを含むことができる。先に述べたように、このようなリモートアクセスおよび/またはリモーティングを許可すると、IoT近接ネットワーク160を、IoT近接ネットワーク160の外の悪意のあるエージェントまたは無許可のユーザからのセキュリティ脅威にさらすおそれがある。これらの攻撃は、インターネット175を通じて(たとえば、パス308を介して)IoT近接ネットワーク160にアクセスすることによって、および/または、インターネット175を通じてリモーティングされるIoTデバイス301～303からの通知に許可なくアクセスすることでユーザプライバシー/セキュリティを攻撃することによって、行われるおそれがある。よって、IoTスーパーエージェント/ゲートウェイ145は、ユーザがリモートアクセスを要求しない可能性があるとき、たとえば、ユーザがIoT近接ネットワーク160内にいて、したがってIoTデバイス301～303にアクセスすることができ、このような

アクセスのためにインターネット175に依存することがないとき、このような影響を受けやすい(susceptible)パスを通じたリモート通信、たとえばリモートアクセスおよび/またはリモーティングを拒否するように構成され得る。完全を期すために、この事例においてリモート通信を拒否することは、ある場合はクラウドサービスもまたリモート通信を拒否されるということを意味することにも留意されたい。

【００３４】

関連する態様では、IoTスーパーエージェント/ゲートウェイ145が、まずユーザ電話130を、許可されたまたは登録されたユーザとしてユーザ登録ブロック310に登録することができる。いくつかの事例では、これは、ユーザ電話130がIoT近接ネットワーク160内にあるとき、ローカル登録によって(たとえば、ユーザ電話130の電話番号または他の識別情報を使用して)行われることが可能である。前述の制御アプリケーションは、登録を行うためにユーザの識別情報の代わりに、またはユーザの識別情報と組み合わせて使用され得る。登録は、当業者には認識される追加の認証プロセス(たとえば、ユーザにホームWi-Fiネットワークに接続するよう要求することおよび/またはパスワード認証をクリアすること)を含むことができる。登録されると、ユーザ電話130は、認識された許可ユーザとしてIoTスーパーエージェント/ゲートウェイ145に、たとえば、プライマリユーザとして記憶されることになる。この事例では、ユーザ電話130はプライマリユーザであると仮定する。

【００３５】

複数のユーザについて詳細に示していないが、1つまたは複数のユーザデバイスが同様のフィールドの下に登録され得ることは理解されよう。たとえば、住宅内の居住者または居住者のサブセットの携帯電話が、許可ユーザとして登録され得る。いくつかの事例では、ユーザは、階層に分けられることがあり、その階層に基づいてユーザごとに異なるルールが適用され、たとえば、従来の家庭では、1人または複数の親の携帯電話が、プライマリユーザとして登録されることがあり、子供または未成年の携帯電話が、下の階層のセカンダリユーザとして登録されることがあり、リモート通信を有効/無効にすることは、ユーザの指定と関連するあらかじめ定義されたルールに基づくことができるようにする。言い換えれば、IoT近接ネットワーク内のIoTユーザデバイスの登録に基づいて、IoT近接ネットワーク160へのリモート通信を有効または無効にするための1つまたは複数のリモート通信基準は、IoT近接ネットワーク160内のIoTデバイスと通信することができる1つまたは複数のIoTデバイスのセットの間の各IoTユーザデバイスの指定または優先レベルを含むことができる。IoTユーザデバイスのセットは、その登録に基づいて階層に分けられることが可能である。プライマリユーザまたは高優先度IoTユーザデバイスの存在が、IoT近接ネットワーク160で検出されるとき、1つまたは複数のIoTデバイス(たとえば、温水器、玄関ドア入口(main door entry)、オーブンなど、明示せず)の第1のセットに対するリモートアクセス/リモーティングが無効にされるように、リモート通信基準が定義され得る。しかしながら、リモートアクセス/リモーティングを含むリモート通信は、セカンダリユーザなどの他の階層のユーザについては、IoTデバイス(たとえば、寝室の照明など、明示せず)の第2のセットに対して依然として有効とすることができる。

【００３６】

さらに、いくつかの事例では、リモート通信を無効にすることは、1つまたは複数のIoTユーザデバイスの選択された機能に関してリモート通信能力を選択的に無効にすることに関連することがある。たとえば、オーブンを含んだIoTデバイスに関して、1人または複数のプライマリユーザがIoT近接ネットワーク160にいることが検出されるとき、オーブンのオン/オフ機能を無効にすることが可能であってもよい。しかしながら、1人または複数のプライマリユーザがいるとき、オン/オフ機能がセカンダリユーザに対して無効にされ得るが、オーブンの機能のサブセットは、それでもなお利用可能であってもよい。このサブセットまたは選択された機能は、たとえばセカンダリユーザに利用可能にされてもよい。したがって、セカンダリユーザは、1人または複数のプライマリユーザがIoT近接ネットワーク160内にいるときでさえ、オーブンがオンであるかどうか、およびオーブンの中で何を作っているかを監視することができてもよい。

【００３７】
リモートアクセス制御ルールならびにリモーティングがいつ許可され得るかに関するルールは、カスタマイズ可能であり、前もって定義され、IoTスーパーエージェント/ゲートウェイ145でリモートアクセス/リモーティング制御ルール314として示されるブロックに記憶されることが可能である。このブロック、リモートアクセス/リモーティング有効/無効312は、IoTスーパーエージェント/ゲートウェイ145の説明図にも示しているが、ブロック314で判定されるリモートアクセス/リモーティング制御ルールによりリモートアクセスまたはリモーティングを有効または無効にするように構成され得る。
【００３８】
存在検出ブロック316は、IoTスーパーエージェント/ゲートウェイ145の外に、少なくともリモートアクセス/リモーティング有効/無効ブロック312と通信して示されている。存在検出ブロック316が物理的にIoTスーパーエージェント/ゲートウェイ145の外に位置している必要はなく、いくつかの態様では、存在検出ブロック316の機能は、IoTスーパーエージェント/ゲートウェイ145内で実施され得る、さらにより詳細にはブロック310～314のいずれか1つまたは複数とマージされ得ることは理解されよう。本質的に、存在検出ブロック316は、IoT近接ネットワーク160内の登録された(1人または複数の)ユーザまたはユーザ電話130の存在または不在を検出するように構成され得る。存在検出ブロック316は、ユーザ電話130の地理的位置に基づいて(たとえば、全地球測位システム(GPS)に基づいて)IoT近接ネットワーク160内でのみ利用できるローカルネットワークへのユーザ電話130の接続を検出することなど、ただしこれに限らず、任意の知られている発見機構を使用して、および/またはユーザ電話130に制御アプリケーションを発見することによって、ユーザ電話130の存在/不在を検出することができる。いくつかの事例では、存在検出ブロック316は、たとえば、ユーザ電話130の登録が現在のものであるかどうかを定期的にチェックすることによって、ユーザ電話130の登録に基づいて存在/不在を検出することができる。ユーザ電話130は、ユーザ登録ブロック310で定期的登録を生成することができ、これが、IoT近接ネットワーク160内のユーザ電話130の存在の存在検出ブロック316を更新するために使用され得る。あるいは、存在検出ブロック316は、たとえばホームネットワークを通じて、ユーザ電話130への定期的リクエストまたはpingを生成し、pingへの応答もしくは確認を求める、または登録の定期的な更新(refreshment)を求めることができる。閾値数のこのようなpingに応答がない、または閾値数の登録が失敗する(missed)場合、存在検出ブロック316は、ユーザ電話130はIoT近接ネットワーク160の構内または近傍を離れたと結論づけることができる。存在検出ブロック316は、ユーザの存在を検出するために間接的手段を使用することもできる。たとえば、IoTデバイス301～303の1つがユーザの車であることがあり、ユーザの車の存在または不在は、ユーザの存在または不在と関連付けられ得る。このように、他のIoTデバイスからのイベント/ステータス更新もまた、ユーザの存在を検出するために使用され得る。追加の態様では、ユーザ電話130上の制御アプリケーションは、IoT近接ネットワーク160内のユーザ電話130の存在もしくは不在(またはいくつかの事例では、対応するエントリもしくは離脱)に関する存在検出ブロックを知らせるために、存在検出ブロック316と通信することができる。存在検出ブロック316は、1つまたは複数の登録されたユーザまたはユーザ電話130の存在/不在を検出するために、他のプラットフォームまたは発見機構を利用することもできる。
【００３９】
たとえば存在検出ブロック316によって検出されるように、ユーザ電話130がIoT近接ネットワーク160にあるかないかに基づいて、リモートアクセス/リモーティングの制御ルールが、ブロック314で更新されることが可能であり、リモートアクセス/リモーティングは、それに応じてブロック312で有効または無効にされ得る。やはり、ブロック314でリモートアクセス/リモーティングを更新することは、ブロック310によって提供される、ユーザの登録(たとえば、ユーザ電話130の特定のユーザは、その存在/不在がリモート通信の有効/無効決定を判定するプライマリユーザであるかどうか)にさらに基づくことができる。いくつかの態様では、IoTデバイスへのリモートアクセスに、ならびにIoTデバイスからの

通知のリモーティングに、同じまたは共通の制御ルールのセットが定義され得る。別の実施形態では、リモートアクセスおよびリモーティング特性に、別個の制御ルールのセットが定義され得る。

【００４０】

より詳細には、リモートアクセス/リモーティング制御ルールブロック314は、ユーザの登録に基づいて、リモートアクセス/リモーティングが許可されるかどうかを判定することになる。1つの事例では、リモートアクセス/リモーティングは、存在検出ブロック316から判定されるように、ユーザ電話130がプライマリユーザとして指定され、ユーザ電話130がIoT近接ネットワーク160の外に位置しているときだけ有効にされ得る。同様に、リモートアクセス/リモーティングは、存在検出ブロック316によって判定されるように、ユーザ電話130がプライマリユーザとして指定され、ユーザ電話130がIoT近接ネットワーク160内にあるとき、無効にされ得る。やはり、これらのルール更新は、プライマリユーザがたとえばユーザの自宅内にいるとき、IoTデバイス301～303へのリモートアクセスおよび/またはIoTデバイス301～303からのリモーティングは不要であり、したがってIoTスーパーエージェント/ゲートウェイ145はリモートアクセスおよびリモーティング用のパスを閉鎖することができるという仮定に基づくことができる。

【００４１】

2人以上のプライマリユーザが存在しているいくつかの事例では、ブロック314におけるリモートアクセス/リモーティング制御ルールは、いくつかの方法でカスタマイズされ得る。たとえば、IoT近接ネットワーク160に1つまたは複数の追加のIoTユーザデバイス(ユーザ電話130など、ただし明示せず)がある場合、リモート通信を有効/無効にすることは、IoT近接ネットワーク160内の複数のIoTユーザデバイスのサブセットまたはいずれか1つの存在/不在検出に基づくことができる。1つまたは複数のIoTユーザデバイスのそれぞれに関するリモート通信基準が、個々に構成され得る。リモート通信を無効/有効にすることは、特定のIoTユーザデバイスおよび対応するリモート通信基準を含んだ様々な組合せに基づくことができる。

【００４２】

たとえば、リモートアクセス/リモーティングは、プライマリユーザとして指定されたIoTユーザデバイスのすべてがIoT近接ネットワーク160内にあるときだけ無効にされ得る(たとえば、家庭の両親が自宅にいるとき、リモートアクセス/リモーティングは必要とされない可能性があり、したがって無効にされ得る)。あるいは、リモートアクセス/リモーティングは、プライマリユーザの任意の1人または任意のあらかじめ定義されたサブセットがIoT近接ネットワーク160内にいるとき、無効にされ得る(たとえば、一方の親が自宅にいるとき、リモートアクセス/リモーティングは他方の親に対して無効にされ得る)。さらに別の代替形態では、リモートアクセス/リモーティングは、プライマリユーザのいずれかがIoT近接ネットワーク160の外にいることが検出されるとき、有効にされ得る(たとえば、両親のいずれか一方が自宅を出たことが検出されるとき、リモートアクセス/リモーティングが有効にされ得る)。上記の行に従った様々な他の代替形態およびカスタマイゼーションは、実施形態の範囲内である。一般に、近接ネットワーク内の1つまたは複数のコントローラデバイスの存在または不在は、近接ネットワークにおいてIoTデバイスへのリモートアクセス/IoTデバイスからのリモーティングを無効にするか、または有効にするかを判定する際に基準として使用され得る。

【００４３】

ブロック314のリモートアクセス/リモーティング制御ルールが、上記のようにユーザ電話130の存在または不在に関連することがあるが、追加的に、または代替的に、リモートアクセス/リモーティング制御ルールは、イベントまたは時間関数に関連することもある。リモートアクセス/リモーティングを有効/無効にするための決定に影響を与えるように使用され得るイベントの例として、IoT近接ネットワーク160内の1つまたは複数のIoTデバイス301～303が、緊急事態または障害などの、更新をトリガすることがあり、これは、他のリモートアクセス/リモーティング制御ルールと併せて使用され得る。特定の説明図で

は、温水器などのIoTデバイスの故障または機能不全は、IoTスーパーエージェント145への緊急通知をトリガすることができる。この事例では、IoTスーパーエージェント145が、プライマリユーザ(たとえば、このような緊急状況でリモートアクセスを必要とするとあらかじめ指定された第1のプライマリユーザ)はIoT近接ネットワーク160内にいないと認識する場合、(たとえば、存在検出ブロック316からの入力に基づいて)たとえ第2のプライマリユーザがIoT近接ネットワーク160内にいるとしても、リモートアクセス/リモーティング有効/無効ブロック312に第1のプライマリユーザのためにリモートアクセス/リモーティングを承諾するよう指示するために、ブロック314においてリモートアクセス/リモーティング制御ルールが更新され得る。このリモートアクセス/リモート制御ルール更新は、(たとえば、すべてのプライマリユーザがいないときだけ、リモートアクセス/リモーティングを可能にするための)あらかじめ構成された制御ルールに優先することができる。他の様々なこのようなカスタマイゼーションが、本開示の範囲を逸脱することなく、イベントに基づいて可能である。

【００４４】

ブロック314のリモートアクセス/リモーティング制御ルールは、時刻または週に基づくこともできる。たとえば、指定されたユーザがIoT近接ネットワーク160にいるかどうかにかかわらず、ブロック314のリモートアクセス/リモーティング制御ルールは、ある期間の間、リモートアクセス/リモーティングが無効にされるように設定され得る。たとえば、リモートアクセス/リモーティングは、午後10時から午前6時まで切ることができる。オフィス設定の場合、リモートアクセス/リモーティングは、特定の選好およびセキュリティ要件に応じて、週の間の業務時間の間は切られ、業務時間後もしくは週末の間だけ有効にされ得る、または逆もまた同様である。ブロック314のリモートアクセス/リモーティング制御ルールは、ユーザの存在/不在および時刻の組合せに基づいて定義されることも可能である。たとえば、家庭の所与のプライマリユーザ(たとえば、妻)がIoT近接ネットワーク160内にいる場合、リモートアクセス/リモーティング制御ルールは、この家庭の別のプライマリユーザ(たとえば、夫)が、金曜の夜の食事を準備するためにオーブンを操作する可能性が高いとき、金曜の夜を除いて午後5時から午後8時の間、オーブン(明示せず)などのIoTデバイスへのリモートアクセスを無効にすることに関係することがある。

【００４５】

よって、実施形態は、ユーザ存在、時刻/週に基づいて、および/または一般的に上述の基準の1つまたは複数の任意の他の組合せに基づいて、リモートアクセス/リモーティングの有効または無効を制御することに関連し得る。リモートアクセス/リモーティングを有効にすることの関連する態様もまた同様に、ユーザの存在/不在、およびオプションとして追加のリモートアクセス基準に基づくことができる。たとえば、許可ユーザ(たとえば、プライマリユーザ)がIoT近接ネットワーク160にいないことが検出される(または不在であると判定される)場合、リモートアクセス/リモーティングを有効にする前に、ある追加の基準がオプションとして、リモートアクセス/リモーティング制御ルールブロック314でチェックされ得る。これらの追加の基準もまた満たされる場合、ブロック312においてリモートアクセス/リモーティングが有効にされ得る。いくつかの事例では、追加の基準は存在しないことがあり、ユーザが不在であることが検出される場合、リモートアクセス/リモーティングは有効にされ得る。

【００４６】

いくつかの態様では、ブロック314のリモートアクセス/リモーティング制御ルールは、IoTデバイスを操作している1人または複数のプライマリユーザに基づいてIoTデバイスによって様々にリモート通信基準を定義するように構成されることも可能である。たとえば、リモートアクセス/リモーティング制御ルールは、第1のプライマリユーザ(たとえば、夫)がIoT近接ネットワーク160に不在であると判定された場合、温水器、HVACシステム、およびホームシアターシステム(これらのデバイスは明示していない)などのIoTデバイスに対してリモートアクセス/リモーティングを有効にするように構成され得る。さらに、リモートアクセス/リモーティング制御ルールは、第1のプライマリユーザがIoT近接ネッ

トワーク160に存在していると判定されるとき、これらのIoTデバイスに対してリモートアクセス/リモーティングを無効にするように構成され得る。別の関連する例では、リモートアクセス/リモーティング制御ルールは、第2のプライマリユーザ(たとえば、妻)がIoT近接ネットワーク160に不在であると判定されるとき、洗濯機/乾燥機、およびオーブン(明示せず)などのIoTデバイスに対してリモートアクセス/リモーティングを有効にするように構成され得る。さらに、リモートアクセス/リモーティング制御ルールは、第2のプライマリユーザがIoT近接ネットワーク160に存在していると判定されるとき、これらのIoTデバイスに対してリモートアクセス/リモーティングを無効にするように構成され得る。よって、リモートアクセス/リモーティング制御ルールは、選択された1つまたは複数のIoTデバイスが特定の1人または複数のプライマリユーザと関連付けられるように構成されることが可能であり、これらの選択された1つまたは複数のIoTデバイスに対するリモートアクセス/リモーティングは、関連付けられたプライマリユーザがIoT近接ネットワークに不在であると判定されるとき、有効にされ、それらの対応するリモートアクセス/リモーティングは、関連付けられたプライマリユーザがIoT近接ネットワークに存在していると判定されるとき、無効にされる。

【００４７】

実施形態は、本明細書に開示するプロセス、機能、および/またはアルゴリズムを実行するための様々な方法を含むことは理解されよう。たとえば、図4に示すように、実施形態は、1つまたは複数のモノのインターネット(IoT)デバイス(たとえば、IoTデバイス301～303)を含んだIoT近接ネットワーク(たとえば、図3のIoT近接ネットワーク160)へのリモートアクセスを制御する方法を含むことができ、この方法は、IoT近接ネットワークにおいて(たとえば、ユーザ電話130の存在/不在を検出するための存在検出ブロック316を使用して)IoTユーザデバイスの存在を検出するステップ-ブロック402と、IoT近接ネットワーク内の1つまたは複数のIoTデバイスとのリモート通信を無効にするための1つまたは複数のリモート通信基準(たとえば、ブロック314のリモートアクセス/リモーティング制御ルール)が満たされるかどうかを判定するステップ-ブロック404と、IoTユーザデバイスがIoT近接ネットワークに存在している場合、およびリモート通信を無効にするためのリモート通信基準が満たされる場合、(たとえば、IoTスーパーエージェント/ゲートウェイ145のリモートアクセス/リモーティング有効/無効ブロック312によって)リモート通信を無効にするステップ-ブロック406とを含む。

【００４８】

同様に、別の実施形態は、1つまたは複数のモノのインターネット(IoT)デバイス(たとえば、IoTデバイス301～303)を含んだIoT近接ネットワーク(たとえば、図3のIoT近接ネットワーク160)とのリモート通信を制御する方法を含むことができ、この方法は、IoT近接ネットワークにおいて(たとえば、ユーザ電話130の存在/不在を検出するための存在検出ブロック316を使用して)IoTユーザデバイスの不在を検出するステップ-ブロック502と、IoT近接ネットワーク内の1つまたは複数のIoTデバイスとの(たとえば、ブロック314のリモートアクセス/リモーティング制御ルールによる)リモート通信を有効にするための1つまたは複数のリモート通信基準が満たされるかどうかを判定するステップ-ブロック504と、IoTユーザデバイスがIoT近接ネットワークに不在である場合、およびリモート通信を有効にするためのリモート通信基準が満たされる場合、リモート通信を有効にするステップ-ブロック506とを含む。

【００４９】

一般に、明示的に別段の記載がない限り、この開示を通して使用される「ように構成された論理」という語句は、少なくとも部分的にハードウェアで実施される態様を思い起こすことを意図されており、ハードウェアから独立したソフトウェアのみの実施にマップすることを意図されていない。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、一般に、(ハードウェアまたはハードウェアとソフトウェアの組合せのいずれかにより)本明細書に記載する機能を行う能力を指すことは理解されよう。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、「論理」という語を共有しているにもかかわらず、必ずしも論理ゲートまたは論理要素として実施されない。様々なブロック中の論理間の他の相互作用または連携が、より詳細に以下に述べる態様の説明から当業者には明らかとなるであろう。

【００５０】

情報および信号が多種多様な異なる技術および技法のいずれかを使用して表すことができることを、当業者は理解されよう。たとえば、上記の説明全体にわたって参照することができるデータ、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、磁界もしくは磁性粒子、光場もしくは光粒子、またはその組合せによって表すことができる。

【００５１】

さらに、本明細書で開示した態様と関連して説明し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ステップは、電子ハードウェア、コンピュータソフトウェア、または両方の組合せとして実装され得ることを、当業者には理解されよう。ハードウェアとソフトウェアのこのような互換性をわかりやすく説明するために、様々な例示的な構成要素、ブロック、モジュール、回路、およびステップを、概してその機能に関して上述した。このような機能がハードウェアとして実装されるか、ソフトウェアとして実装されるかは、特定の応用およびシステム全体に課される設計の制約によって決まる。当業者は、説明される機能を具体的な応用形態ごとに様々な方法で実現することができるが、そのような実現の決定は、本開示の範囲からの逸脱を生じるものと解釈されるべきではない。

【００５２】

本明細書に開示する態様と関連して説明する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)、特定用途用集積回路(ASIC)、フィールドプログラマブルゲートアレイ(FPGA)もしくは他のプログラマブルロジックデバイス、個別のゲートもしくはトランジスタロジック、個別のハードウェア部品、または本明細書に記載した機能を行うように設計されたこれらの任意の組合せを用いて、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とすることができるが、代替的にプロセッサは、任意の従来のプロセッサ、コントローラ、マイクロコントローラ、または状態機械とすることができる。プロセッサはまた、コンピューティングデバイスの組合せ(たとえば、DSPおよび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、または任意の他のそのような構成)として実装され得る。

【００５３】

本明細書に開示する態様と関連して説明する方法、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、またはこの2つの組合せで、具体化され得る。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、リムーバブルディスク、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記憶媒体に、常駐することができる。例示的記憶媒体がプロセッサに結合され、プロセッサが記憶媒体から情報を読み取ること、および記憶媒体に情報を書き込むことができるようにする。代替として、記憶媒体はプロセッサと一体化され得る。プロセッサおよび記憶媒体はASIC内に存在し得る。ASICはIoTデバイス内に存在し得る。代替として、プロセッサおよび記憶媒体は、ユーザ端末内に個別の構成要素として存在し得る。

【００５４】

1つまたは複数の例示的な態様では、記載された機能は、ハードウェア、ソフトウェア、ファームウェア、またはそれらの任意の組合せに実装することができる。ソフトウェアに実装される場合、機能は、コンピュータ可読媒体上の1つもしくは複数の命令またはコードとしてこれに記憶され得る、またはこれを通じて伝送され得る。コンピュータ可読媒体は、ある場所から別の場所へのコンピュータプログラムの転送を容易にする任意の媒体

を含む、コンピュータ記憶媒体と通信媒体の両方を含む。記憶媒体は、コンピュータによってアクセスされ得る任意の利用可能な媒体であってもよい。一例として、限定ではないが、このようなコンピュータ可読媒体は、RAM、ROM、EEPROM、CD-ROMもしくは他の光ディスク記憶装置、磁気ディスク記憶装置もしくは他の磁気記憶装置、または所望のプログラムコードを命令もしくはデータ構造の形態で搬送するもしくは記憶するために使用することができ、コンピュータがアクセスすることができる任意の他の媒体を含むことができる。また、いかなる接続もコンピュータ可読媒体と適切に呼ばれる。たとえば、同軸ケーブル、光ファイバケーブル、ツイストペア、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、または他のリモートソースからソフトウェアが送信される場合、同軸ケーブル、光ファイバケーブル、ツイストペア、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。本明細書で使用するディスク(disk)およびディスク(disc)は、CD、レーザーディスク(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)は通常データを磁気的におよび/またはレーザーを用いて光学的に再生する。上記の組合せもコンピュータ可読媒体の範囲内に含まれるべきである。

【００５５】

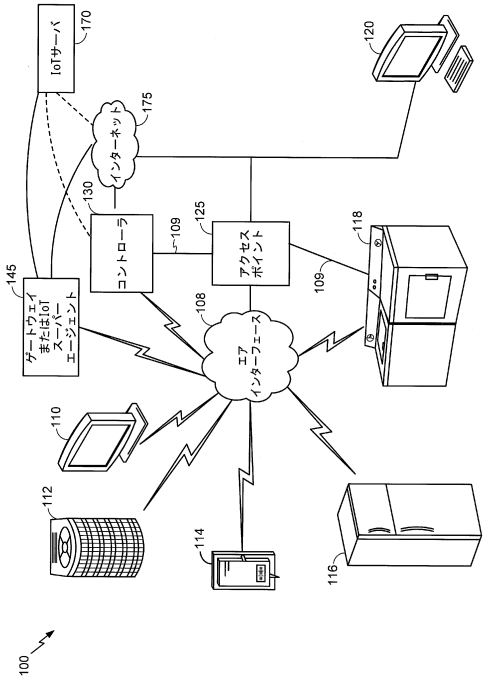
上述の開示は、本開示の例示的な態様を示すが、様々な変形形態および変更形態が、添付の特許請求の範囲によって定義される本開示の範囲から逸脱することなく本明細書において作成可能であることに留意すべきである。本明細書に記載した本開示の態様に従った方法の請求項の機能、ステップ、および/またはアクションは、特定の順序で行われる必要はない。さらに、本開示の要素は、単数で記載または請求される場合があるが、単数に限定することが明示的に表明されていない場合、複数が検討される。

【符号の説明】

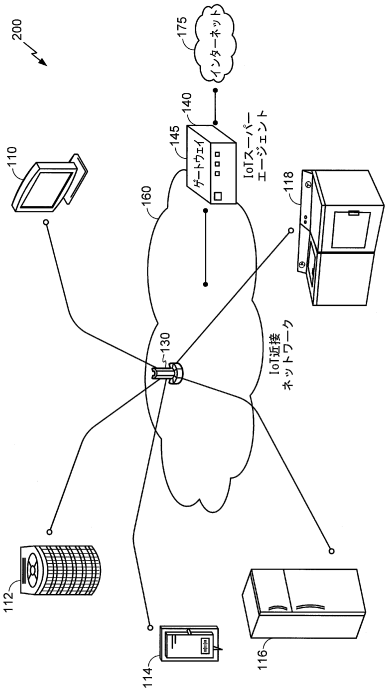
【００５６】

100 ワイヤレス通信システム
108 エアインターフェース
109 直接有線接続
110 IoTデバイス
112 IoTデバイス
114 IoTデバイス
116 IoTデバイス
118 IoTデバイス
120 IoTデバイス
125 アクセスポイント
130 コントローラ/ユーザ電話(リモートアクセス/制御アプリ)
145 IoTスーパーエージェント/ゲートウェイ
160 IoT近接ネットワーク
170 IoTサーバ
175 インターネット/クラウド
200 ワイヤレス通信システム
300 ワイヤレス通信システム
301 IoTデバイス
302 IoTデバイス
303 IoTデバイス
304 ローカル登録
310 ユーザ登録
312 リモートアクセス/リモーティング有効/無効
314 リモートアクセス/リモーティング制御ルール
316 存在検出

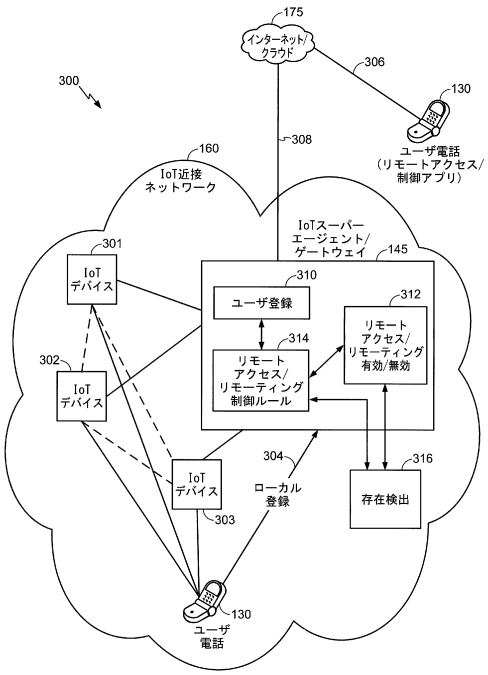
【図１】


IoTサーバ
170
120
175
インターネット
130
コントローラ
109
125
アクセスポイント
118
145
ゲートウェイまたはIoTスーパーエージェント
108
エアインターフェース
110
112
114
116
100

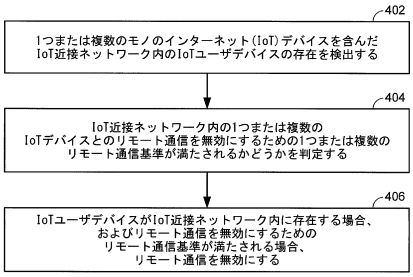
【図２】


200
175
インターネット
140
145
ゲートウェイ
IoTスーパーエージェント
110
160
118
130
IoT近接ネットワーク
112
114
116

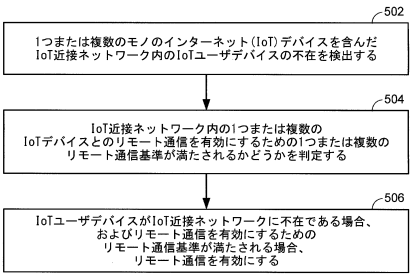
【図３】


300
175
インターネット/クラウド
306
130
ユーザ電話（リモートアクセス/制御アプリ）
308
160
IoT近接ネットワーク
IoTスーパーエージェント/ゲートウェイ
145
301
IoTデバイス
310
ユーザ登録
312
リモートアクセス/リモーティング有効/無効
314
リモートアクセス/リモーティング制御ルール
302
IoTデバイス
304
ローカル登録
316
存在検出
IoTデバイス
303
130
ユーザ電話

【図４】


402
1つまたは複数のモノのインターネット（IoT）デバイスを含むIoT近接ネットワーク内のIoTユーザデバイスの存在を検出する
404
IoT近接ネットワーク内の1つまたは複数のIoTデバイスとのリモート通信を無効にするための1つまたは複数のリモート通信基準が満たされるかどうかを判定する
406
IoTユーザデバイスがIoT近接ネットワーク内に存在する場合、およびリモート通信を無効にするためのリモート通信基準が満たされる場合、リモート通信を無効にする

【図５】


502
1つまたは複数のモノのインターネット（IoT）デバイスを含むIoT近接ネットワーク内のIoTユーザデバイスの不在を検出する
504
IoT近接ネットワーク内の1つまたは複数のIoTデバイスとのリモート通信を有効にするための1つまたは複数のリモート通信基準が満たされるかどうかを判定する
506
IoTユーザデバイスがIoT近接ネットワークに不在である場合、およびリモート通信を有効にするためのリモート通信基準が満たされる場合、リモート通信を有効にする

フロントページの続き

(56)参考文献 国際公開第０３／０９８９０９（WO，Ａ１）
特開２００１－２５１３１２（ＪＰ，Ａ）
特開２００８－０６７１９９（ＪＰ，Ａ）
国際公開第２０１４／１２２９４３（WO，Ａ１）
特開２０１３－１９２０１６（ＪＰ，Ａ）
特開２００６－１２８８２４（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　１３／００