

(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2018-513457

(P2018-513457A)

(43) 公表日 平成30年5月24日(2018.5.24)

(51) Int.Cl.	F I	テーマコード (参考)
G06F 13/00 (2006.01)	G06F 13/00 358A	5K030
H04L 12/70 (2013.01)	G06F 13/00 ZJG	
G06F 17/30 (2006.01)	H04L 12/70 100Z	
	G06F 17/30 210D	
	G06F 17/30 170Z	
審査請求 未請求 予備審査請求 有 (全 63 頁) 最終頁に続く		

(21) 出願番号 特願2017-545750 (P2017-545750)
 (86) (22) 出願日 平成28年2月29日 (2016.2.29)
 (85) 翻訳文提出日 平成29年8月30日 (2017.8.30)
 (86) 国際出願番号 PCT/US2016/020072
 (87) 国際公開番号 W02016/140912
 (87) 国際公開日 平成28年9月9日 (2016.9.9)
 (31) 優先権主張番号 14/638,602
 (32) 優先日 平成27年3月4日 (2015.3.4)
 (33) 優先権主張国 米国 (US)

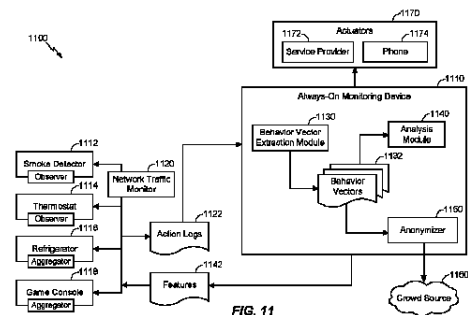
(71) 出願人 507364838
 クアルコム、インコーポレイテッド
 アメリカ合衆国 カリフォルニア 921
 21 サン ディエゴ モアハウス ドラ
 イブ 5775
 (74) 代理人 100108453
 弁理士 村山 靖彦
 (74) 代理人 100163522
 弁理士 黒田 晋平
 (72) 発明者 ラジャルシ・グプタ
 アメリカ合衆国・カリフォルニア・921
 21-1714・サン・ディエゴ・モアハ
 ウス・ドライブ・5775

最終頁に続く

(54) 【発明の名称】モノのインターネットデバイスの健全性の直接的および間接的ローカル監視を自動化するための挙動分析

(57) 【要約】

本開示は概して、モノのインターネット(IoT)デバイスの健全性を直接的および/または間接的に監視することを自動化するための挙動分析に関する。詳細には、ローカルIoTネットワーク内のIoTデバイスに関連する正常挙動をモデル化してもよく、それによって、IoTデバイスにおいて観測された挙動をモデル化された正常挙動と比較して、IoTデバイスにおいて観測された挙動が正常であるかそれとも異常であるかを判定してもよい。したがって、分散型IoT環境において、より高性能の「アナライザ」デバイスが、他の(たとえば、より単純な)「オブザーバ」デバイスにおいてローカルに観測された挙動を収集し、分散型IoT環境全体にわたって挙動分析を行い、悪意のある攻撃、誤動作、あるいは顧客サービスおよび/またはさらなる注意を必要とする他の問題を潜在的に示す異常を検出することができる。さらに、十分な機能を有するデバイスが、(ローカル)オンデバイス挙動分析を行って、ローカルに観測された挙動を別のアグリゲータデバイスおよび/またはアナライザデバイスに送ることなく異常条件を検出してもよい。



【特許請求の範囲】**【請求項 1】**

モノのインターネット(IoT)デバイスの健全性を監視するための方法であって、ローカルIoTネットワーク内のIoTデバイスに関連する正常挙動をモデル化するステップと、

前記IoTデバイスにおいて観測された挙動情報を分析するステップと、

前記分析された挙動情報を前記IoTデバイスに関連する前記モデル化された正常挙動と比較して、前記IoTデバイスにおいて観測された前記挙動情報が正常挙動を示すかそれとも異常挙動を示すかを判定するステップとを含む方法。

【請求項 2】

前記IoTデバイスにおいて観測された前記挙動情報を分析する前記ステップは、

前記観測された挙動情報から1つまたは複数の挙動ベクトルを抽出するステップであって、前記観測された挙動情報が、 n 個の挙動特性を表し、前記1つまたは複数の挙動ベクトルが前記 n 個の挙動特性を n 次元空間にマップする、ステップをさらに含む、請求項1に記載の方法。

【請求項 3】

前記IoTデバイスを含む前記ローカルIoTネットワークをモデル化するステップと、

前記分析された挙動情報を前記モデル化されたローカルIoTネットワークと比較して、前記ローカルIoTネットワークに関連する現在の状態を判定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 4】

前記ローカルIoTネットワークをモデル化する前記ステップは、

前記ローカルIoTネットワーク内の各IoTデバイスに関連する属性をモデル化するステップと、

前記ローカルIoTネットワークに関連するトポロジを構築するステップと、

前記ローカルIoTネットワーク内の各IoTデバイスに関連する挙動モデルを、各IoTデバイスに関連する製造業者あるいは前記挙動モデルを記憶するように構成された1つまたは複数のリポジトリから取得するステップと、

前記ローカルIoTネットワーク内の各IoTデバイスに関連する前記集約された属性、前記ローカルIoTネットワークに関連する前記トポロジ、および前記ローカルIoTネットワークをモデル化するように前記ローカルIoTネットワーク内の各IoTデバイスに関連付けられた前記挙動モデルを組み合わせるステップとを含む、請求項3に記載の方法。

【請求項 5】

前記IoTデバイスにおいて観測された前記挙動情報が異常挙動を示すと判定したことに応答して、前記IoTデバイスにおいて観測された前記挙動情報を顧客サービスエンティティに報告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 6】

前記異常挙動は、前記IoTデバイスまたは前記IoTデバイスを含む前記ローカルIoTネットワークに対する潜在的な悪意のある攻撃を含む、請求項5に記載の方法。

【請求項 7】

前記異常挙動は、前記IoTデバイスにおける潜在的な誤動作または異常動作条件を含む、請求項5に記載の方法。

【請求項 8】

前記IoTデバイスは、前記挙動情報を観測するように装備された第1の構成要素と、前記観測された挙動情報を分析し、前記IoTデバイスに関連する前記モデル化された正常挙動と比較するように構成された第2の構成要素とを少なくとも備える、請求項1に記載の方法。

【請求項 9】

前記IoTデバイスは、前記挙動情報を観測するように装備された1つまたは複数の構成要素と、前記観測された挙動情報を分析し、前記IoTデバイスに関連する前記モデル化され

10

20

30

40

50

た正常挙動と比較するように構成された外部ノードに、前記観測された挙動情報を表す1つまたは複数の挙動特性を送るように構成されたトランスミッタとを備える、請求項1に記載の方法。

【請求項10】

前記IoTデバイスを含む前記ローカルIoTネットワークは、前記IoTデバイスが前記ローカルIoTネットワークを介して送信するメッセージを監視し、前記ローカルIoTネットワークを介して送信される前記監視されたメッセージに従って前記IoTデバイスにおける前記挙動情報を観測するように構成された1つまたは複数のノードをさらに含む、請求項1に記載の方法。

【請求項11】

モノのインターネット(IoT)デバイスの健全性を監視するための装置であって、
ローカルIoTネットワーク内の少なくとも1つのIoTデバイスに関連する正常挙動をモデル化する情報を記憶するように構成された少なくとも1つの記憶デバイスと、
1つまたは複数のプロセッサとを備え、前記1つまたは複数のプロセッサは、
前記IoTデバイスにおいて観測された挙動情報を分析することと、
前記分析された挙動情報を前記IoTデバイスに関連する前記モデル化された正常挙動と比較して、前記IoTデバイスにおいて観測された前記挙動情報が正常挙動を示すかそれとも異常挙動を示すかを判定することを行うように構成される装置。

【請求項12】

前記1つまたは複数のプロセッサは、前記観測された挙動情報から1つまたは複数の挙動ベクトルを抽出するようにさらに構成され、前記観測された挙動情報は、 n 個の挙動特性を表し、前記1つまたは複数の挙動ベクトルは、前記 n 個の挙動特性を n 次元空間にマップする、請求項11に記載の装置。

【請求項13】

前記少なくとも1つの記憶デバイスは、前記IoTデバイスを含む前記ローカルIoTネットワークをモデル化する情報を記憶するようにさらに構成され、
前記1つまたは複数のプロセッサは、前記分析された挙動情報を前記モデル化されたローカルIoTネットワークと比較して、前記ローカルIoTネットワークに関連する現在の状態を判定するようにさらに構成される、請求項11に記載の装置。

【請求項14】

前記1つまたは複数のプロセッサは、
前記ローカルIoTネットワーク内の各IoTデバイスに関連する属性を集約することと、
前記ローカルIoTネットワークに関連するトポロジを構築することと、
前記ローカルIoTネットワーク内の各IoTデバイスに関連する挙動モデルを、各IoTデバイスに関連する製造業者あるいは前記挙動モデルを記憶するように構成された1つまたは複数のリポジトリから取得することと、
前記ローカルIoTネットワーク内の各IoTデバイスに関連する前記集約された属性、前記ローカルIoTネットワークに関連する前記トポロジ、および前記ローカルIoTネットワークをモデル化するように前記ローカルIoTネットワーク内の各IoTデバイスに関連付けられた前記挙動モデルを組み合わせることを行うようにさらに構成される、請求項13に記載の装置。

【請求項15】

前記1つまたは複数のプロセッサは、前記IoTデバイスにおいて観測された前記挙動情報が異常挙動を示していることに応答して、前記IoTデバイスにおいて観測された前記挙動情報を顧客サービスエンティティに報告するようにさらに構成される、請求項11に記載の装置。

【請求項16】

前記異常挙動は、前記IoTデバイスまたは前記IoTデバイスを含む前記ローカルIoTネットワークに対する潜在的な悪意のある攻撃あるいは前記IoTデバイスにおける潜在的な誤動作または異常動作条件のうちの1つまたは複数を含む、請求項15に記載の装置。

10

20

30

40

50

【請求項 17】

オンデバイス健全性監視プラットフォームをさらに備え、前記オンデバイス健全性監視プラットフォームは、

前記挙動情報を観測するように装備された観測モジュールと、

前記観測された挙動情報から1つまたは複数の挙動ベクトルを抽出するように構成された挙動ベクトル抽出モジュールと、

前記1つまたは複数の挙動ベクトル内に表された前記観測された挙動情報を、前記IoTデバイスに関連する前記モデル化された正常挙動と比較して、前記IoTデバイスにおいて観測された前記挙動情報が正常挙動を示すかそれとも異常挙動を示すかを判定するように構成された分析モジュールとをさらに備える、請求項11に記載の装置。

10

【請求項 18】

前記挙動情報を観測するように装備された1つまたは複数の構成要素と、

前記観測された挙動情報を分析し、前記IoTデバイスに関連する前記モデル化された正常挙動と比較するように構成された外部ノードに、前記観測された挙動情報を表す1つまたは複数の挙動特性を送るように構成されたトランスミッタとをさらに備える、請求項11に記載の装置。

【請求項 19】

前記ローカルIoTネットワークを介して伝送された1つまたは複数のメッセージを受信するように構成されたレシーバであって、前記1つまたは複数のメッセージが、前記観測された挙動情報を含むレシーバと、

20

健全性監視プラットフォームであって、

前記観測された挙動情報から1つまたは複数の挙動ベクトルを抽出するように構成された挙動ベクトル抽出モジュールと、

前記1つまたは複数の挙動ベクトル内に表された前記観測された挙動情報を、前記IoTデバイスに関連する前記モデル化された正常挙動と比較して、前記IoTデバイスにおいて観測された前記挙動情報が正常挙動を示すかそれとも異常挙動を示すかを判定するように構成された分析モジュールとを備える健全性監視プラットフォームとをさらに備える、請求項11に記載の装置。

【請求項 20】

前記観測された挙動情報を含む前記1つまたは複数のメッセージは、前記IoTデバイス、あるいは前記IoTデバイスが前記ローカルIoTネットワークを介して送信するメッセージを監視し、前記IoTデバイスが前記ローカルIoTネットワークを介して送信する前記監視されたメッセージに従って前記観測された挙動情報を含む前記1つまたは複数のメッセージを伝送するように構成された1つまたは複数のネットワークトラフィック監視ノードのうちの1つまたは複数から受信される、請求項11に記載の装置。

30

【請求項 21】

モノのインターネット(IoT)デバイスの健全性を監視するための装置であって、

ローカルIoTネットワーク内のIoTデバイスに関連する正常挙動をモデル化するための手段と、

前記IoTデバイスにおいて観測された挙動情報を分析するための手段と、

40

前記分析された挙動情報を前記IoTデバイスに関連する前記モデル化された正常挙動と比較して、前記IoTデバイスにおいて観測された前記挙動情報が正常挙動を示すかそれとも異常挙動を示すかを判定するための手段とを備える装置。

【請求項 22】

前記観測された挙動情報から1つまたは複数の挙動ベクトルを抽出するための手段をさらに備え、前記観測された挙動情報は、 n 個の挙動特性を表し、前記1つまたは複数の挙動ベクトルは、前記 n 個の挙動特性を n 次元空間にマップする、請求項21に記載の装置。

【請求項 23】

前記IoTデバイスを含む前記ローカルIoTネットワークをモデル化するための手段と、

前記分析された挙動情報を前記モデル化されたローカルIoTネットワークと比較して、

50

前記ローカルIoTネットワークに関連する現在の状態を判定するための手段とをさらに備える、請求項21に記載の装置。

【請求項 2 4】

前記ローカルIoTネットワーク内の各IoTデバイスに関連する属性を集約するための手段と、

前記ローカルIoTネットワークに関連するトポロジを構築するための手段と、

前記ローカルIoTネットワーク内の各IoTデバイスに関連する挙動モデルを、各IoTデバイスに関連する製造業者あるいは前記挙動モデルを記憶するように構成された1つまたは複数のリポジトリから取得するための手段と、

前記ローカルIoTネットワーク内の各IoTデバイスに関連する前記集約された属性、前記ローカルIoTネットワークに関連する前記トポロジ、および前記ローカルIoTネットワークをモデル化するように前記ローカルIoTネットワーク内の各IoTデバイスに関連付けられた前記挙動モデルを組み合わせるための手段とをさらに備える、請求項23に記載の装置。

【請求項 2 5】

前記IoTデバイスにおいて観測された前記挙動情報が異常挙動を示していることに応答して、前記IoTデバイスにおいて観測された前記挙動情報を顧客サービスエンティティに報告するための手段をさらに備える、請求項21に記載の装置。

【請求項 2 6】

前記異常挙動は、前記IoTデバイスまたは前記IoTデバイスを含む前記ローカルIoTネットワークに対する潜在的な悪意のある攻撃を含む、請求項25に記載の装置。

【請求項 2 7】

前記異常挙動は、前記IoTデバイスにおける潜在的な誤動作または異常動作条件を含む、請求項25に記載の装置。

【請求項 2 8】

前記観測された挙動情報を分析し、前記IoTデバイスに関連する前記モデル化された正常挙動と比較するように構成された外部ノードに、前記観測された挙動情報を表す1つまたは複数の挙動特性を送信するための手段をさらに備える、請求項21に記載の装置。

【請求項 2 9】

前記IoTデバイス、あるいは前記IoTデバイスが前記ローカルIoTネットワークを介して送信するメッセージを監視し、前記IoTデバイスが前記ローカルIoTネットワークを介して送信する前記監視されたメッセージに従って前記観測された挙動情報を含む前記1つまたは複数のメッセージを伝送するように構成された1つまたは複数のネットワークトラフィック監視ノードのうちの1つまたは複数から、前記観測された挙動情報を表す1つまたは複数の挙動特性を受信するための手段をさらに備える、請求項21に記載の装置。

【請求項 3 0】

コンピュータ実行可能命令を記録したコンピュータ可読記憶媒体であって、1つまたは複数のプロセッサ上で前記コンピュータ実行可能命令を実行することが、前記1つまたは複数のプロセッサに、

ローカルIoTネットワーク内のモノのインターネット(IoT)デバイスに関連する正常挙動をモデル化することと、

前記IoTデバイスにおいて観測された挙動情報を分析することと、

前記分析された挙動情報を前記IoTデバイスに関連する前記モデル化された正常挙動と比較して、前記IoTデバイスにおいて観測された前記挙動情報が正常挙動を示すかそれとも異常挙動を示すかを判定することとを行わせるコンピュータ可読記憶媒体。

【発明の詳細な説明】

【技術分野】

【0 0 0 1】

本明細書において説明する様々な態様および実施形態は、概してモノのインターネット(IoT)に関し、より詳細には、IoTデバイスの健全性の直接的および/または間接的な監視を自動化するための挙動分析に関する。

10

20

30

40

50

【背景技術】

【0002】

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。

【0003】

10

いくつかの市場動向がIoTデバイスの開発を推進している。たとえば、増大するエネルギーコストは、政府によるスマートグリッドに対する戦略投資、ならびに電気自動車および公共充電ステーションなど、将来の消費に対するサポートを推進している。増大する医療費および高齢人口は、遠隔/コネクテッドヘルスケア(connected health care)およびフィットネスサービスの開発を推進している。住居内の技術革命は、「N」プレイ(たとえば、データ、音声、ビデオ、セキュリティ、エネルギー管理など)をマーケティングして、ホームネットワークを拡張するサービスプロバイダによる統合を含めて、新しい「スマート」サービスの開発を推進している。企業設備の運転費を削減するための手段として、建造物はよりスマートかつより便利になっている。

【0004】

20

IoT用のいくつかの重要なアプリケーションが存在する。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、公益事業会社は住居および事業に対するエネルギーの配給を最適化することができるのに対して、カスタマはエネルギー使用をより良好に管理することができる。住居およびビルディングオートメーションの領域では、スマートホームおよびスマート建造物は、住居もしくは事務所内の、電化製品からプラグイン電気自動車(PEV)セキュリティシステムまで、事実上、どのようなデバイスまたはシステムに対しても集中制御し得る。資産管理の分野では、企業、病院、工場、および他の大型組織は、価値が高い設備、患者、車両などの位置を正確に追跡することができる。ヘルスおよびウェルネスの領域では、医師は患者の健康を遠隔で監視することができるのに対して、人々はフィットネスルーチンの進捗を追跡することができる。

30

【0005】

したがって、IoT技術がますます発展しているので、近い将来IoTデバイスが激増し、それによって、家庭、車両内、職場、および他の多くの場所においてユーザの周りに多数のIoTデバイスが存在することになることが予想されている。IoT技術空間における1つの問題は、IoTデバイスに関する顧客サービスを製造業者と顧客の両方に対して自動化し、より安価に、より容易に、かつより高速に実行することに関する。たとえば、あるデバイスの問題を把握し、次いでこの問題に対処する人を見つけるか、あるいは時間を割いてサービス要員にこの問題について説明し理解させるのは、面倒で、コストと時間がかかるプロセスである。さらに、特定の接続されたデバイス(たとえば、コンピュータ)がリモートトラブルシューティングをサポートする場合があるが、多くのデバイスは、リモートログインおよびロギングをサポートする機能を有さないことがあり、リモートログイン機能を有する接続されたデバイス上でもシステムの問題を理解し解決することは単純な問題ではない。IoTに関する別の問題は、多くのIoTデバイスは、セキュリティを考慮せずに製造されることが多い単純なデバイス(たとえば、トースター、サーモスタット、洗濯機、テレビジョン、照明器具、およびその他の日常的な対象物)であることに少なくとも部分的に起因して悪意のある攻撃を受けやすいことである。同時に、デバイスが単純であることは、特定のIoTデバイスの可能な挙動が比較的限られており、顧客サービス問題とセキュリティ問題の両方に対処する機会を与える可能性があることを意味する。その理由は、どちらの問題も少なくともある程度挙動の異常さを伴うからである(たとえば、ネットワークトラフィックの突然のスパイクは、コンピュータに対するサービス拒否(DoS)攻撃を示す場

40

50

合があり、長期間の電力ドロワーは機器の故障を示す場合がある)。

【0006】

したがって、コンピュータ化された接続された家庭およびその他の接続されたIoT環境では、大部分の機器およびその他のIoTデバイスは、互いに接続され、ローカルに生じる挙動を少なくとも監視する機能を有する可能性がある。とはいえ、特定の挙動特性を監視する能力を有するにもかかわらず、多くのIoTデバイスは、異常挙動を検出し是正するのに必要な挙動分析を行うのに十分なリソースを有さないと考えることができる。さらに、多数のIoTデバイスを有する接続された環境では、潜在的なセキュリティ違反または誤動作を示す特定の異常は、環境全体の状態を検討した後にのみ明らかになる場合があり、このことは、限られた機能を有する多数の単純なIoTデバイスを含む環境では困難である場合がある。

10

【発明の概要】

【課題を解決するための手段】

【0007】

以下に、本明細書で開示する1つまたは複数の態様および/または実施形態に関する簡略化された概要を示す。したがって、以下の概要は、すべての考えられる態様および/または実施形態に関連する包括的な概説と見なされるべきではなく、また、以下の概要は、すべての考えられる態様および/または実施形態に関連する重要な、または決定的な要素を特定するか、任意の特定の態様および/または実施形態に関連付けられる範囲を定めると見なされるべきでもない。したがって、以下の概要は、以下に提示される詳細な説明に先立って、本明細書において開示される機構に関連する1つまたは複数の態様および/または実施形態に関連する特定の概念を簡略化された形で提示することが唯一の目的である。

20

【0008】

様々な態様によれば、IoT環境が一般に、それぞれに異なる機能を有する様々な異種デバイスを含むと考えられることを利用して、直接的および間接的な挙動分析を行ってIoT環境における1つまたは複数のデバイスに対する潜在的に悪意のある攻撃を検出し、デバイスの健全性を監視し、誤動作およびその他の異常を検出することができ、それによって、IoT環境における顧客サービスを製造業者の視点と顧客の視点の両方から自動化し、より安価に、より容易に、かつより高速に実行することができる。たとえば、多くの異常は、いくつかの基本的な観測値(たとえば、特定の期間にわたる電力ドロワー、局所温度および/または周囲温度を示すセンサー測定値、水位、煙レベル、一酸化炭素および/または二酸化炭素レベル、可視性レベル、慣性測定ユニット(IMU)によって測定された振動など)に基づいて検出し分析することができる。したがって、多くのIoTデバイスが比較的限られた挙動を有する単純なデバイス(たとえば、トースター、サーモスタット、洗濯機、テレビジョン、照明器具、およびその他の日常的な対象物)であることを考えて、IoT環境における(すべてではないとしても)大部分のデバイスが特定のローカル挙動(たとえば、電力消費量、センサー出力など)を観測する機能を少なくとも有すると仮定することができる。さらに、特定のIoT環境におけるすべてのデバイスが、挙動分析を行うのに十分な処理リソース、記憶リソース、および/または他の機能を有するわけではないにもかかわらず、コンピュータ化された接続されたIoT環境における(すべてではないとしても)大部分の機器およびその他のデバイスは、ネットワークを介して通信する機能を有し、したがって、ローカルに観測された挙動をより高性能のデバイスに送る機能を有すると考えることができる。したがって、分散型アーキテクチャを有するIoT環境では、IoT環境におけるより高性能の1つまたは複数のデバイス(たとえば、スマートフォン、「常時接続」ワイヤレスルータなど)が、他の(より単純な)デバイスがローカルに観測する挙動を集約し、ならびに/あるいは分散型IoT環境全体にわたって挙動分析を行い、顧客サービスを必要とする悪意のある攻撃または誤動作を潜在的に示す異常を検出することができる。さらに、IoT環境におけるより高性能のデバイスは、オンデバイス(ローカル)挙動分析を行って、ローカルに観測された挙動を別のアグリゲータおよび/またはアナライザデバイスに送る必要なしに異常条件を検出してもよい。

30

40

50

【0009】

たとえば、様々な態様によれば、モノのインターネット(IoT)デバイスの健全性を監視するための方法は、ローカルIoTネットワーク内のIoTデバイスに関連する正常挙動をモデル化するステップと、IoTデバイスにおいて観測された挙動情報を分析するステップと、分析された挙動情報をIoTデバイスに関連するモデル化された正常挙動と比較して、IoTデバイスにおいて観測された挙動情報が正常挙動を示すかそれとも異常挙動を示すかを判定するステップとを含んでもよい。様々な実施形態では、IoTデバイスにおいて観測される挙動情報を分析するステップは、観測された挙動情報から1つまたは複数の挙動ベクトルを抽出するステップであって、観測された挙動情報が、 n 個の挙動特性を表し、1つまたは複数の挙動ベクトルが n 個の挙動特性を n 次元空間にマップする、ステップを含んでもよい。さらに、様々な実施形態では、IoTデバイスを含むローカルIoTネットワークはモデル化されてもよく、分析された挙動情報をモデル化されたローカルIoTネットワークと比較してローカルIoTネットワークに関連する現在の状態を判定してもよい。たとえば、ローカルIoTネットワークをモデル化するステップは、ローカルIoTネットワーク内の各IoTデバイスに関連する属性を集約するステップと、ローカルIoTネットワークに関連するトポロジを構成するステップと、各IoTデバイスに関連する製造業者あるいは挙動モデルを記憶するように構成された1つまたは複数のリポジトリからローカルIoTネットワーク内の各IoTデバイスに関連する挙動モデルを取得するステップと、ローカルIoTネットワーク内の各IoTデバイスに関連する集約された属性、ローカルIoTネットワークに関連するトポロジー、およびローカルIoTネットワーク内の各IoTデバイスに関連する挙動モデルを組み合わせるステップとを含んでもよい。したがって、IoTデバイスにおいて観測された挙動情報は、IoTデバイスにおいて観測された挙動情報が異常挙動を示すと判定したことに応答して顧客サービスエンティティに報告されてもよく、異常挙動は、IoTデバイスまたはIoTデバイスを含むローカルIoTネットワークに対する潜在的な悪意のある攻撃、IoTデバイスにおける潜在的な誤動作または異常動作条件、あるいは注意および/または是正を必要とする場合がある別の問題を含んでもよい。さらに、様々な実施形態では、IoTデバイスは、挙動情報を観測するように装備された第1の構成要素と、観測された挙動情報を分析し、(たとえば、スタンドアロン「オンデバイス」アーキテクチャにおける)IoTデバイスに関連するモデル化された正常挙動と比較するように構成された第2の構成要素とを少なくとも備えてもよく、あるいはIoTデバイスは、挙動情報を観測するように装備された1つまたは複数の構成要素と、観測された挙動情報を表す1つまたは複数の挙動特性を、観測された挙動情報を分析して(たとえば、分散型アーキテクチャにおける)IoTデバイスに関連するモデル化された正常挙動と比較するように構成された外部ノードに送るように構成されたトランスミッタとを備えてもよい。さらに、様々な実施形態では、ローカルIoTネットワークは、IoTデバイスがローカルIoTネットワークを介して送信するメッセージを監視し、ローカルIoTネットワークを介して送信される監視されたメッセージに従ってIoTデバイスにおける挙動情報を観測するように構成された1つまたは複数のノードをさらに含んでもよい。

【0010】

様々な態様によれば、IoTデバイスの健全性を監視するための装置は、ローカルIoTネットワーク内の少なくとも1つのIoTデバイスに関連する正常挙動をモデル化する情報を記憶するように構成された少なくとも1つの記憶デバイスと、IoTデバイスにおいて観測された挙動情報を分析し、分析された挙動情報をIoTデバイスに関連するモデル化された正常挙動と比較して、IoTデバイスにおいて観測された挙動情報が正常挙動を示すかそれとも異常挙動を示すかを判定するように構成された1つまたは複数のプロセッサとを備えてもよい。

【0011】

様々な態様によれば、IoTデバイスの健全性を監視するための装置は、ローカルIoTネットワーク内のIoTデバイスに関連する正常挙動をモデル化するための手段と、IoTデバイスにおいて観測された挙動情報を分析するための手段と、分析された挙動情報をIoTデバイ

10

20

30

40

50

スに関連するモデル化された正常挙動と比較して、IoTデバイスにおいて観測された挙動情報が正常挙動を示すかそれとも異常挙動を示すかを判定するための手段とを備えてもよい。

【0012】

様々な態様によれば、コンピュータ可読記憶媒体は、コンピュータ実行可能な命令が記憶されてもよく、1つまたは複数のプロセッサ上でコンピュータ実行可能な命令を実行することによって、1つまたは複数のプロセッサに、ローカルIoTネットワーク内のIoTデバイスに関連する正常挙動をモデル化することと、IoTデバイスにおいて観測された挙動情報を分析することと、分析された挙動情報をIoTデバイスに関連するモデル化された正常挙動と比較して、IoTデバイスにおいて観測された挙動情報が正常挙動を示すかそれとも異常挙動を示すかを判定することとを行わせてもよい。

10

【0013】

本明細書において開示される態様および実施形態に関連付けられる他の目的および利点は、添付の図面および詳細な説明に基づいて、当業者に明らかになるであろう。

【0014】

以下の詳細な説明を参照し、限定のためではなく、単に説明のために提示される添付の図面とともに検討することによって本明細書に記載される様々な態様および実施形態、ならびにそれらに付随する多くの利点がよりよく理解されるようになるので、それらの様々な態様および実施形態ならびにそれに付随する多くの利点についてのより完全な理解は容易に実現される。

20

【図面の簡単な説明】

【0015】

【図1A】様々な態様によるワイヤレス通信システムの例示的なハイレベルシステムアーキテクチャを示す図である。

【図1B】様々な態様によるワイヤレス通信システムの例示的なハイレベルシステムアーキテクチャを示す図である。

【図1C】様々な態様によるワイヤレス通信システムの例示的なハイレベルシステムアーキテクチャを示す図である。

【図1D】様々な態様によるワイヤレス通信システムの例示的なハイレベルシステムアーキテクチャを示す図である。

30

【図1E】様々な態様によるワイヤレス通信システムの例示的なハイレベルシステムアーキテクチャを示す図である。

【図2A】様々な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。

【図2B】様々な態様による例示的な受動IoTデバイスを示す図である。

【図3】様々な態様による、機能を実現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。

【図4】様々な態様による例示的なサーバを示す図である。

【図5】様々な態様による、直接D2D通信を有効化することができる発見可能なデバイス間(D2D)(またはピアツーピア(P2P))サービスをサポートする場合があるワイヤレス通信ネットワークを示す図である。

40

【図6】様々な態様による、様々なデバイスがD2D技術を使用して通信するのに利用することができる近接度ベースの分散バスを確立するために発見可能なD2Dサービスを使用し得る例示的な環境を示す図である。

【図7】様々な態様による、様々なデバイスがD2D技術を使用して通信するのに利用することができる近接度ベースの分散バスを確立するために発見可能なD2Dサービスを使用し得る例示的なシグナリングフローを示す図である。

【図8A】一態様による、2つのホストデバイス間のD2D通信をサポートするためにホストデバイス間に形成される場合がある近接度ベースの例示的な分散バスを示す図である。

【図8B】一態様による、1つまたは複数の埋込みデバイスが近接度ベースの分散バスに

50

接続するためにホストデバイスに接続する場合がある近接度ベースの例示的な分散バスを示す図である。

【図 9】様々な態様による、ローカルデバイス健全性監視を自動化するために挙動分析をサポートする場合がある例示的なオンデバイスアーキテクチャを示す図である。

【図 10】様々な態様による、様々なノードが、ローカルIoT環境における直接的および/または間接的な挙動分析ならびに自動化されたデバイス健全性監視をサポートするために通信する場合がある例示的なローカルIoT環境を示す図である。

【図 11】様々な態様による、様々なノードが、ローカルIoT環境における直接的および/または間接的な挙動分析ならびに自動化されたデバイス健全性監視をサポートするために通信する場合がある例示的な分散型アーキテクチャを示す図である。

【図 12】様々な態様による、自動化されたデバイス健全性監視をサポートすることができる挙動分析を行う例示的な方法を示す図である。

【図 13】様々な態様による、自動化されたデバイス健全性監視をサポートするために行うことができる挙動分析を初期設定する例示的な方法を示す図である。

【図 14】様々な態様による、ローカルIoT環境において行われる直接的および/または間接的な挙動分析を使用して異常挙動を検出し是正することができる例示的な分散型アーキテクチャを示す図である。

【図 15】様々な態様による、ローカルIoT環境における直接的および/または間接的な挙動分析を行って顧客サービスおよびセキュリティインシデント応答を自動化して異常挙動を是正するための例示的な方法を示す図である。

【図 16】様々な態様による、冷蔵庫IoTデバイスに関連する健全性を監視するために直接的および/または間接的な挙動分析が行われる場合がある例示的な顧客サービス使用事例に対応する方法を示す図である。

【図 17】様々な態様による、煙感知器IoTデバイスに関連する健全性を監視するために直接的および/または間接的な挙動分析が行われる場合がある例示的な顧客サービス使用事例に対応する方法を示す図である。

【図 18】様々な態様による、IoTデバイス挙動の観測、集約、および/または分析を行うように構成されてもよい例示的な通信デバイスを示す図である。

【発明を実施するための形態】

【0016】

様々な態様および実施形態が、例示的な態様および実施形態に関する特定の例を示すために以下の説明および関連する図面において開示される。代替的態様および代替的实施形態は、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、本明細書で開示す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。

【0017】

「例示的」という言葉は、本明細書では「例、事例、または例示として機能すること」を意味するために使用される。本明細書で「例示的」として説明するいかなる実施形態も、必ずしも他の実施形態よりも好ましいか、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、論じられた特徴、利点または動作モードを含むことを要求しない。

【0018】

本明細書で使用される用語は、特定の実施形態のみを説明しており、本明細書で開示されるいずれかの実施形態を限定すると解釈されるべきではない。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すのでなければ、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、本明細書で使用すると、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明示するが、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、

10

20

30

40

50

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よう。

【0019】

さらに、多くの態様について、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施されるべき、動作のシーケンスに関して説明する。本明細書で説明する様々な動作は、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るプログラム命令によって、あるいは両方の組合せによって実施され得ることは認識されよう。さらに、本明細書で説明されるこれらの一連の動作は、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ことになる対応する1組のコンピュータ命令を記憶した、任意の形のコンピュータ可読記憶媒体内で完全に具現されるものと見なされ得る。したがって、本明細書において説明する様々な態様は、特許請求される主題の範囲内にすべて入ることが企図されているいくつかの異なる形で具現され得る。さらに、本明細書で説明される実施形態ごとに、任意のそのような実施形態の対応する形は、本明細書において、たとえば、説明される動作を実行する「ように構成された論理」として説明される場合がある。

【0020】

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、トランシーバ、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、および/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。たとえば、IoTデバイスは、これらのデバイスがIoTネットワークと通信するためのアドレス指定可能通信インターフェースを備える限り、冷蔵庫、トースター、オーブン、電子レンジ、冷凍庫、皿洗い機、パラボラアンテナ(dishes)、手工具、洗濯機、衣類乾燥機、加熱炉、空調機、温度自動調整器、テレビジョン、照明設備、掃除機、スプリンクラー、電気メータ、ガスメータなどを含み得るが、これらに限定されない。IoTデバイスはまた、セルフォン、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)などを含み得る。したがって、IoTネットワークは、通常はインターネット接続性を有しないデバイス(たとえば、皿洗い機など)に加えて、「レガシー」インターネットアクセス可能デバイス(たとえば、ラップトップコンピュータまたはデスクトップコンピュータ、セルフォンなど)の組合せから構成され得る。

【0021】

図1Aは、様々な態様によるワイヤレス通信システム100Aのハイレベル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、テレビジョン110と、屋外空調機112と、温度自動調整器114と、冷蔵庫116と、洗濯機および乾燥機118とを含む、複数のIoTデバイスを含む。

【0022】

図1Aを参照すると、IoTデバイス110~118は、図1Aにエアインターフェース108および直接有線接続109として示す物理通信インターフェースまたは物理通信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。エア

インターフェース108は、IEEE 802.11など、ワイヤレスインターネットプロトコル(IP)に準拠し得る。図1Aは、エアインターフェース108を介して通信するIoTデバイス110~118と、直接有線接続109を介して通信するIoTデバイス118とを示すが、各IoTデバイスは、有線接続もしくはワイヤレス接続、または両方を介して通信することができる。

【0023】

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1Aには示されていない)を含む。インターネット175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IP)を使用して、異種のデバイス/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。TCP/IPは、データが、宛先において、どのようにフォーマッティング、アドレス指定、送信、経路指定、および受信されるべきかを指定するエンドツーエンド接続性を提供する。

10

【0024】

図1Aでは、デスクトップコンピュータ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、Ethernet(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介して)インターネット175と直接接続するとして示される。コンピュータ120は、(たとえば、有線接続性とワイヤレス接続性の両方を有するWiFiルータ用の)アクセスポイント125自体などに相当してよいモデムまたはルータとの直接接続など、インターネット175との有線接続を有し得る。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、エアインターフェース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に接続されてよく、エアインターフェース108を介してインターネット175にアクセスしてよい。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デバイスであり得、かつ/またはIoTデバイス110~118のネットワーク/グループなど、IoTネットワーク/グループを管理するための機能を含み得る。

20

【0025】

アクセスポイント125は、たとえば、FiOS、ケーブルモデム、デジタル加入者線(DSL)モデムなど、光通信システムを介して、インターネット175に接続され得る。アクセスポイント125は、標準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110~120およびインターネット175と通信することができる。

30

【0026】

図1Aを参照すると、IoTサーバ170は、インターネット175に接続されるように示されている。IoTサーバ170は、複数の構造的に別々の複数のサーバとして実装され得るか、または代替的には、単一のサーバに対応し得る。様々な実施形態では、IoTサーバ170は、(点線によって示されるように)オプションであり、IoTデバイス110~120のグループは、ピアツーピア(P2P)ネットワークであり得る。そのような場合、IoTデバイス110~120は、適切なデバイス間(D2D)通信技術を使用してエアインターフェース108および/または直接有線接続109を介して互いに直接通信することができる。代替的に、または追加として、IoTデバイス110~120の一部またはすべては、エアインターフェース108および直接有線接続109に依存しない通信インターフェースで構成され得る。たとえば、エアインターフェース108がWiFiインターフェースに対応する場合、IoTデバイス110~120のうちの1つもしくは複数は、互いに、または他のBluetooth(登録商標)対応デバイスもしくはNFC対応デバイスと直接通信するためのBluetooth(登録商標)インターフェースあるいはNFCインターフェースを有し得る。

40

【0027】

ピアツーピアネットワークでは、サービス発見方式は、ノードの存在、その能力、およびグループメンバーシップをマルチキャストすることができる。ピアツーピアデバイスは、この情報に基づいて、関連性および後続の相互作用を確立することができる。

【0028】

50

様々な態様によれば、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のハイレベルアーキテクチャを示す。一般に、図1Bに示すワイヤレス通信システム100Bは、上でより詳細に説明した、図1Aに示すワイヤレス通信システム100Aと同じ、ならびに/または実質的に同様の様々な構成要素(たとえば、エアインターフェース108および/もしくは直接有線接続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た、テレビジョン110と、屋外空調機112と、温度自動調整器114と、冷蔵庫116と、洗濯機および乾燥機118とを含む様々なIoTデバイス、インターネット175に直接接続する、かつ/あるいはアクセスポイント125を通してインターネット175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)を含み得る。したがって、説明を簡潔かつ簡単にするために、同じまたは同様の詳細が図1Aに示したワイヤレス通信システム100Aに関して上ですでに提供されている限り、図1Bに示すワイヤレス通信システム100B内のいくつかの構成要素に関する様々な詳細は本明細書で省略される場合がある。

10

【0029】

図1Bを参照すると、ワイヤレス通信システム100Bは、代替的に、IoTマネージャ130またはIoTマネージャデバイス130と呼ばれる場合もあるスーパーバイザデバイス130を含み得る。したがって、以下の説明が「スーパーバイザデバイス」130という用語を使用する場合、IoTマネージャ、グループ所有者、または同様の用語に対するいずれの参照もスーパーバイザデバイス130、あるいは同じもしくは実質的に同様の機能を提供する別の物理的構成要素または論理的構成要素を指す場合があることを当業者は諒解されよう。

【0030】

様々な実施形態では、スーパーバイザデバイス130は、一般に、ワイヤレス通信システム100B内の様々な他の構成要素を観測、監視、制御、あるいは管理することができる。たとえば、スーパーバイザデバイス130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110~120に関連付けられた属性、活動、もしくは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に対して、および、オプションで、(点線として示される)IoTサーバ170に対して、有線接続またはワイヤレス接続を有し得る。スーパーバイザデバイス130は、様々なIoTデバイス110~120に関連付けられた属性、活動、もしくは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/あるいはIoTサーバ170から取得することができる。スーパーバイザデバイス130は、独立型デバイスであってよく、または、コンピュータ120など、IoTデバイス110~120のうちの1つであってよい。スーパーバイザデバイス130は、物理デバイスであってよく、または物理デバイス上で実行するソフトウェアアプリケーションであってよい。スーパーバイザデバイス130は、IoTデバイス110~120に関連付けられた、監視される属性、活動、または他の状態に関する情報を出力して、それらに関連付けられた属性、活動、または他の状態を制御あるいは管理するための入力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、一般に、様々な構成要素を含むことが可能であり、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、あるいは管理するために様々な有線通信インターフェースおよびワイヤレス通信インターフェースをサポートし得る。

20

30

40

【0031】

図1Bに示す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に結合され得るか、あるいはワイヤレス通信システム100Bの一部であり得る(能動IoTデバイス110~120と対照的な)1つまたは複数の受動IoTデバイス105を含み得る。一般に、受動IoTデバイス105は、短距離インターフェースを介して問い合わせられたとき、その識別子と属性とを別のデバイスに提供することができる、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、または任意の他の適切なデバイスを含み得る。能動IoTデバイスは、受動IoTデバイスの属性の変化を検出すること、記憶すること、通信すること、それらの変化に

50

作用することなどが可能である。

【0032】

たとえば、受動IoTデバイス105は、各々、RFIDタグまたはバーコードを有するコーヒーカップとオレンジジュースの容器とを含み得る。キャビネットIoTデバイスおよび冷蔵庫IoTデバイス116は、各々、RFIDタグもしくはバーコードを読み取って、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IoTデバイス105がいつ追加あるいは除去されたかを検出することができる適切なスキャナまたはリーダーを有し得る。キャビネットIoTデバイスがコーヒーカップの受動IoTデバイス105の除去を検出し、冷蔵庫IoTデバイス116がオレンジジュースの容器の受動IoTデバイスの除去を検出すると、スーパーバイザデバイス130は、キャビネットIoTデバイスおよび冷蔵庫IoTデバイス116において検出された活動に関する1つまたは複数の信号を受信することができる。スーパーバイザデバイス130は、次いで、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みたいことを推定することができる。

10

【0033】

上記は何らかの形のRFIDタグ通信インターフェースまたはバーコード通信インターフェースを有するとして受動IoTデバイス105を説明しているが、受動IoTデバイス105は、そのような通信能力を有しない、1つもしくは複数のデバイスまたは他の物理的対象物を含み得る。たとえば、あるIoTデバイスは、受動IoTデバイス105を識別するために、受動IoTデバイス105に関連付けられた形状、サイズ、色、および/もしく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機構またはリーダー機構を有し得る。このようにして、任意の適切な物理的対象物はその識別情報および属性を通信して、ワイヤレス通信システム100Bの一部になることができ、スーパーバイザデバイス130を用いて観測、監視、制御、あるいは管理され得る。さらに、受動IoTデバイス105は、図1Aのワイヤレス通信システム100Aに結合され得るか、あるいはその一部であり得、実質的に同様の形で、観測、監視、制御、または管理され得る。

20

【0034】

様々な態様によれば、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のハイレベルアーキテクチャを示す。一般に、図1Cに示すワイヤレス通信システム100Cは、上でより詳細に説明した、図1Aおよび図1Bにそれぞれ示したワイヤレス通信システム100Aならびに100Bと同じ、かつ/または実質的に同様の様々な構成要素を含み得る。したがって、説明を簡潔かつ簡単にするために、同じまたは類似の詳細が、それぞれ、図1Aおよび図1Bに示したワイヤレス通信システム100Aならびに100Bに関して上ですでに提供されている限り、図1Cに示すワイヤレス通信システム100C内のいくつかの構成要素に関する様々な詳細は本明細書で省略される場合がある。

30

【0035】

図1Cに示す通信システム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に示すように、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の各々と通信する。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。

40

【0036】

IoTデバイス110~118はIoTグループ160を構成する。IoTデバイスグループ160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、ローカルに接続されたIoTデバイスのグループである。示さないが、複数のIoTデバイスグループは、インターネット175に接続されたIoT SuperAgent140を介して互いに接続されること、および/または通信することが可能である。ハイレベルで、スーパーバイザデバイス130はグループ内通信を管理するのに対して、IoT SuperAgent140はグループ間通信を管理することができる。別個のデバイスとして示すが、スーパーバイザデバイス130およびIoT SuperAgent140は、同じデバイス(たとえば、図1Aのコンピュータ120など、独立型デバイスもしくはIoTデバイス)であり得るか、またはその中に存在し得る。代替的に、IoT SuperAgent140は、アクセスボイ

50

ント125の機能に対応し得るか、またはその機能を含み得る。さらに別の代替として、IoT SuperAgent140は、IoTサーバ170などのIoTサーバの機能に対応し得るか、またはその機能を含み得る。IoT SuperAgent140は、ゲートウェイ機能145をカプセル化することができる。

【0037】

各IoTデバイス110～118は、スーパーバイザデバイス130をピアとして扱って、属性/スキーマ更新をスーパーバイザデバイス130に送信することができる。IoTデバイスが別のIoTデバイスと通信する必要があるとき、IoTデバイスは、スーパーバイザデバイス130にそのIoTデバイスに対するポイントを要求し、次いで、ピアとしてターゲット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)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デバイスがCMP対応であり、共通通信トランスポートを介して接続される限り、それらのIoTデバイスは互いに通信することができる。プロトコルスタック内で、CMPレイヤ154は、アプリケーションレイヤ152の下にあり、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。

10

【0038】

様々な態様によれば、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のハイレベルアーキテクチャを示す。一般に、図1Dに示すワイヤレス通信システム100Dは、それぞれ、上でより詳細に説明した、図1A～図1Cに示したワイヤレス通信システム100A～100Cと同じ、かつ/または実質的に類似した様々構成要素を含み得る。したがって、説明を簡潔かつ簡単にするために、同じまたは類似の詳細がそれぞれ図1A～図1Cに示したワイヤレス通信システム100A～100Cに関して上ですでに提供されている限り、図1Dに示すワイヤレス通信システム100D内のいくつかの構成要素に関する様々な詳細は本明細書で省略される場合がある。

20

【0039】

インターネット175は、IoTの概念を使用して調整され得る「リソース」である。しかしながら、インターネット175は、調整されるリソースのほんの一例であり、任意のリソースがIoTの概念を使用して調整され得る。調整され得る他のリソースは、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得、それによって、リソースを調整するか、またはリソースはインターネット175を介して調整され得る。図1Dは、天然ガス、ガソリン、湯、および電気など、いくつかのリソース180を示し、リソース180は、インターネット175に加えて調整され得るか、またはインターネット175を介して調整され得る。

30

【0040】

IoTデバイスは、互いに通信して、リソース180の使用を調整することができる。たとえば、トースター、コンピュータ、およびヘアドライヤなどのIoTデバイスは、Bluetooth(登録商標)通信インターフェースを介して互いに通信して、その電気(リソース180)使用を調整することができる。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デバイスは、Wi-Fi通信インターフェースを介して通信して、インターネット175(リソース180)に対するそのアクセスを調整することができる。さらに別の例として、ストーブ、衣類乾燥機、および湯沸かし器などのIoTデバイスは、Wi-Fi通信インターフェースを介して通信して、そのガス使用を調整することができる。代替的に、または追加として、各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、そのリソース180の使用を調整するための論理を有する、IoTサーバ170などのIoTサーバに接続され得る。

40

【0041】

様々な態様によれば、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のハイレベルアーキテクチャを示す。一般に、図1Eに示すワイヤレス通信システム100Eは、上でより詳細に説明した、それぞれ、図1A～図1Dに示したワイヤレス通信システム100A～100Dと同じ、かつ/または実質的に類似した様々構成要素を含み得る。したがって、

50

説明を簡潔かつ簡単にするために、同じまたは類似の詳細がそれぞれ図1A～図1Dに示したワイヤレス通信システム100A～100Dに関して上ですでに提供されている限り、図1Eに示すワイヤレス通信システム100E内のいくつかの構成要素に関する様々な詳細は本明細書で省略される場合がある。

【0042】

通信システム100Eは、2つのIoTデバイスグループ160Aおよび160Bを含む。複数のIoTデバイスグループは、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こと、および/または互いに通信することが可能である。ハイレベルで、IoT SuperAgentは、IoTデバイスグループ内のグループ間通信を管理することができる。たとえば、図1Eで、IoTデバイスグループ160Aは、IoTデバイス116A、122A、および124Aと、IoT SuperAgent140Aとを含むのに対して、IoTデバイスグループ160Bは、IoTデバイス116B、122B、および124Bと、IoT SuperAgent140Bとを含む。したがって、IoT SuperAgent140Aおよび140Bは、インターネット175と接続して、インターネット175を介して互いと通信すること、ならびに/またはIoTデバイスグループ160Aおよび160B間の通信を促すために互いと直接通信することができる。さらに、図1Eは、IoT SuperAgent140Aおよび140Bを介して互いと通信する2つのIoTデバイスグループ160Aおよび160Bを示すが、任意の数のIoTデバイスグループが、IoT SuperAgentを使用して互いと好適に通信することができることを当業者は諒解されよう。

【0043】

図2Aは、様々な態様によるIoTデバイス200Aのハイレベルな例を示す。外観および/または内部構成要素はIoTデバイス間でかなり異なる場合があるが、大部分のIoTデバイスは、ディスプレイとユーザ入力のための手段とを含み得る、ある種のユーザインターフェースを有することになる。ユーザインターフェースがないIoTデバイスは、図1A～図1Bにおけるエアインターフェース108など、有線ネットワークまたはワイヤレスネットワークを介してリモートで通信され得る。

【0044】

図2Aに示すように、IoTデバイス200Aに関する例示的な構成では、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、構成要素の中でも、ディスプレイ226と、電源ボタン222と、2つの制御ボタン224Aおよび224Bとで構成され得る。ディスプレイ226は、タッチスクリーンディスプレイであり得、その場合、制御ボタン224Aおよび224Bは必要でない場合がある。IoTデバイス200Aの一部として明示的に示されてはいないが、IoTデバイス200Aは、限定はしないが、Wi-Fiアンテナ、セルラーアンテナ、衛星位置システム(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、1つまたは複数の外部アンテナおよび/または外部ケーシングに内蔵される1つのまたは複数の内蔵アンテナを含むことができる。

【0045】

IoTデバイス200AなどのIoTデバイスの内部構成要素は異なるハードウェア構成によって具体化され得るが、内部ハードウェア構成要素のための基本的なハイレベル構成は図2Aにプラットフォーム202として示されている。プラットフォーム202は、図1A～図1Bのエアインターフェース108ならびに/または有線インターフェースなど、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ならびに実行することができる。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てもよい。プラットフォーム202は、一般に、プロセッサ208と呼ばれることになる、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)、プログラマブル論理回路、または他のデータ処理デバイスなど、1つもしくは複数のプロセッサ208に動作可能に結合された有線通信および/あるいはワイヤレス通信のために構成された1つもしく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受信機またはSPS受信機など)を含み得る。プロセッサ208は、IoTデバイス内のメモリ212内でアプリケーションプログラミング命令を実行するこ

とができる。メモリ212は、読取り専用メモリ(ROM)、ランダムアクセスメモリ(RAM)、電気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共通の任意のメモリのうちの1つもしくは複数を含み得る。1つもしくは複数の入出力(I/O)インターフェース214は、プロセッサ208が、示すようなディスプレイ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に関連付けられたセンサー、アクチュエータ、リレー、バルブ、スイッチなどの任意の他のデバイスと通信すること、ならびにそれらから制御することを可能にするように構成され得る。

【0046】

したがって、様々な態様は、本明細書に記載された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)を含むことができる。当業者によって諒解されるように、様々な論理要素は、本明細書で開示する機能を実現するように個別の要素、プロセッサ(たとえば、プロセッサ208)上で実行されるソフトウェアモジュール、またはソフトウェアとハードウェアとの任意の組合せにおいて具現されてもよい。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をすべて協調的に使用して、本明細書で開示する様々な機能をロードし、記憶し、実行してもよく、したがって、これらの機能を実行するための論理は様々な要素に分散されてもよい。代替的には、機能は1つの個別の構成要素に組み込むことができる。したがって、図2AにおけるIoTデバイス200Aの特徴は、単に例示にすぎないものと見なされ、IoTデバイス200Aは、図2Aに示す、示された特徴または構成に限定されない。

【0047】

図2Bは、様々な態様による受動IoTデバイス200Bのハイレベルな例を示す。一般に、図2Bに示す受動IoTデバイス200Bは、上でより詳細に説明した、図2Aに示したIoTデバイス200Aと同じ、かつ/または実質的に類似した様々な構成要素を含み得る。したがって、説明を簡潔かつ簡単にするために、同じまたは類似の詳細が図2Aに示したIoTデバイス200Aに関して上ですでに提供されている限り、図2Bに示す受動IoTデバイス200B内のいくつかの構成要素に関する様々な詳細は本明細書で省略される場合がある。

【0048】

図2Bに示す受動IoTデバイス200Bは、プロセッサ、内部メモリ、またはある種の他の構成要素を有しない場合があるという点で、一般に、図2Aに示すIoTデバイス200Aとは異なる場合がある。代わりに、様々な実施形態では、受動IoTデバイス200Bは、受動IoTデバイス200Bが、制御されたIoTネットワーク内で観測されること、監視されること、制御されること、管理されること、あるいは知られることを可能にする、I/Oインターフェース214または他の適切な機構だけを含み得る。たとえば、様々な実施形態では、受動IoTデバイス200Bに関連付けられたI/Oインターフェース214は、短距離インターフェースを介して問い合わせられたとき、受動IoTデバイス200Bに関連付けられた識別子および属性を別のデバイス(たとえば、受動IoTデバイス200Bに関連付けられた属性に関する情報を検出すること、記憶すること、通信すること、その情報に作用すること、あるいはその情報を処理することができる、IoTデバイス200Aなどの能動IoTデバイス)に提供することができる、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、または任意の他の適切なI/Oインターフェースを含み得る。

【0049】

上記は何らかの形のRF、バーコード、または他のI/Oインターフェース214を有するとして受動IoTデバイス200Bを説明しているが、受動IoTデバイス200Bは、そのようなI/Oインターフェース214を有しないデバイスまたは他の物理的対象物を含み得る。たとえば、あるIoTデバイスは、受動IoTデバイス200Bを識別するために、受動IoTデバイス200Bに関連付けられた形状、サイズ、色、および/もしく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機構またはリーダー機構を有し得る。このようにして、任意の適切な物理的対象物は、その識別および属性を通信することができ、制御されたIoTネットワー

ク内で観測、監視、制御、あるいは管理され得る。

【0050】

図3は、機能を実行するように構成される論理を含む通信デバイス300を示す。通信デバイス300は、限定はしないが、IoTデバイス110~120、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)を含む、上記の通信デバイスのうちのいずれかに対応し得る。したがって、通信デバイス300は、図1A~図1Bのワイヤレス通信システム100A~100Bを介して1つもしくは複数の他のエンティティと通信する(または通信を容易にする)ように構成された任意の電子デバイスに対応し得る。

【0051】

図3を参照すると、通信デバイス300は、情報を受信および/または送信するように構成される論理305を含む。一例では、通信デバイス300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IoTデバイス200B)に対応する場合には、情報を受信および/または送信するように構成される論理305は、ワイヤレストランシーバおよび関連ハードウェア(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)のような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、Long-Term Evolution (LTE) Directなど)を含むことができる。別の例では、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305は、有線通信インターフェース(たとえば、インターネット175にアクセスする手段となり得るシリアル接続、USBまたはFirewire接続、Ethernet(登録商標)接続など)に対応することができる。したがって、通信デバイス300が、何らかのタイプのネットワークベースのサーバ(たとえば、アプリケーション170)に対応する場合には、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305は、一例では、Ethernet(登録商標)プロトコルによってネットワークベースのサーバを他の通信エンティティに接続するEthernet(登録商標)カードに対応し得る。さらなる例では、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305は、通信デバイス300がそのローカル環境を監視する手段となり得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RF信号を監視するためのアンテナなど)を含むことができる。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305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305の関連ハードウェアがその受信機能および/または送信機能を実行できるようにするソフトウェアも含むことができる。しかしながら、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305は、ソフトウェアだけに対応するのではなく、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305は、その機能性を達成するためのハードウェアに少なくとも部分的に依拠する。

【0052】

図3を参照すると、通信デバイス300は、情報を処理するように構成される論理310をさらに含む。一例では、情報を処理するように構成される論理310は、少なくともプロセッサを含むことができる。情報を処理するように構成された論理310によって実施され得るタイプの処理の例示的な実装形態は、判断を行うこと、接続を確立すること、異なる情報オプション間で選択を行うこと、データに関係する評価を実施すること、測定動作を実施するために通信デバイス300に結合されたセンサーと対話すること、情報をあるフォーマットから別のフォーマットに(たとえば、.wmvから.aviへなど、異なるプロトコル間で)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310中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)もしくは他のプログラマブル論理デバイス、個別ゲートもしくはトランジスタ論理、個別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る機能を実行するように設計されたそれらの任意の組合せに対応し得る。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、代替として、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)として実現され得る。情報を処理するように構成された論理310は、実行されるとき、情報を処理するように構成された論理310の関連ハードウェアがその処理機能を実行できるようにするソフトウェアも含むことができる。しかしながら、情報を処理するように構成された論理310は、ソフトウェアだけに対応するのではなく、情報を処理するように構成された論理310は、その機能を達成するためにハードウェアに少なくとも部分的に依拠する。

【0053】

図3を参照すると、通信デバイス300は、情報を記憶するように構成される論理315をさらに含む。一例では、情報を記憶するように構成される論理315は、少なくとも非一時的メモリおよび関連ハードウェア(たとえば、メモリコントローラなど)を含むことができる。たとえば、情報を記憶するように構成される論理315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、リムーバブルディスク、CD-ROM、または当該技術分野において知られている任意の他の形の記憶媒体に対応することができる。情報を記憶するように構成される論理315は、実行されるときに、情報を記憶するように構成される論理315の関連ハードウェアがその記憶機能を実行できるようにするソフトウェアも含むことができる。しかしながら、情報を記憶するように構成される論理315は、ソフトウェアだけに対応するのではなく、情報を記憶するように構成される論理315は、その機能を達成するためにハードウェアに少なくとも部分的に依拠する。

【0054】

図3を参照すると、通信デバイス300は、情報を提示するように構成された論理320をさらにオプションで含む。一例では、情報を提示するように構成される論理320は、少なくとも出力デバイスおよび関連ハードウェアを含むことができる。たとえば、出力デバイスは、ビデオ出力デバイス(たとえば、ディスプレイスクリーン、USB、HDMI(登録商標)のようなビデオ情報を搬送することができるポートなど)、オーディオ出力デバイス(たとえば、スピーカ、マイクロフォンジャック、USB、HDMI(登録商標)のようなオーディオ情報を搬送することができるポートなど)、振動デバイス、および/または、情報がそれによって出力のためにフォーマットされ得る、または通信デバイス300のユーザもしくは操作者によって実際に出力され得る任意の他のデバイスを含むことができる。たとえば、通信デバイス300が、図2Aに示したIoTデバイス200Aおよび/または図2Bに示した受動IoTデバイス200Bに対応する場合、情報を提示するように構成された論理320は、ディスプレイ226を含み得る。さらなる一例では、情報を提示するように構成される論理320は、ローカルユーザを有し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、リモートサーバなど)のようないくつかの通信デバイスでは省くことができる。情報を提示するように構成された論理320は、実行されるとき、情報を提示するように構成された論理320の関連ハードウェアがその提示機能を実施できるようにするソフトウェアも含むことができる。しかしながら、情報を提示するように構成された論理320は、ソフトウェアだけに対応するのではなく、情報を提示するように構成された論理320は、その機能性を達成するためにハードウェアに少なくとも部分的に依拠する。

【0055】

図3を参照すると、通信デバイス300は、ローカルユーザ入力を受信するように構成された論理325をさらにオプションで含む。一例では、ローカルユーザ入力を受信するように構成される論理325は、少なくともユーザ入力デバイスおよび関連ハードウェアを含むことができる。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、オーディオ入力デバイス(たとえば、マイクロフォン、もしくはマイクロフォンジャックなど、オーディオ情報を搬送することができるポートなど)、および/または情報がそれによって通信デバイス300のユーザもしくはオペレータから受信され得る任意の他のデバイスを含み得る。たとえば、通信デバイス300が図2Aに示すようなIoTデバイス200Aおよび/または図2Bに示すような受動IoTデバイス200Bに対応する場合、ローカルユーザ入力を受信するように構成された論理325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。さらなる例では、ローカルユーザ入力を受信するように構成された論理325は、(たとえば、ネットワークスイッチまたはルータ、リモートサーバなど)ローカルユーザを有さないネットワーク通信デバイスのようにいくつかの通信デバイスでは省略されることがある。ローカルユーザ入力を受信するように構成された論理325は、実行されるとき、ローカルユーザ入力を受信するように構成された論理325の関連ハードウェアがその入力受信機能を実施できるようにするソフトウェアも含むことができる。しかしながら、ローカルユーザ入力を受信するように構成された論理325は、ソフトウェアだけに対応するのではなく、ローカルユーザ入力を受信するように構成された論理325は、その機能性を達成するためにハードウェアに少なくとも部分的に依拠する。

10

【0056】

図3を参照すると、305~325の構成された論理は、図3では別個のまたは相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機能を実行するためのハードウェアおよび/またはソフトウェアは、部分的に重複できることは理解されよう。たとえば、305~325の構成された論理の機能を容易にするために使用される任意のソフトウェアを、情報を記憶するように構成された論理315に関連する非一時的メモリに記憶することができ、それにより、305~325の構成された論理は各々、その機能(すなわち、この場合、ソフトウェア実行)を、情報を記憶するように構成された論理315によって記憶されたソフトウェアの動作に部分的に基づいて実行する。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は、時々、他の構成された論理によって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310のプロセッサは、データを、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305によって送信される前に、適切な形式にフォーマットすることができ、それにより、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305は、その機能(すなわち、この場合、データの送信)を、情報を処理するように構成された論理310に関連付けられたハードウェア(すなわち、プロセッサ)の動作に部分的に基づいて実行する。

20

【0057】

概して、別段に明示的に記載されていない限り、本明細書において使用される「ように構成された論理」という句は、ハードウェアにより少なくとも部分的に実施される論理を指すものとし、ハードウェアから独立したソフトウェアだけの実施形態に位置づけるものではない。様々なブロックにおける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論理要素に限定されるのではなく、概して、本明細書に記載した機能性を、(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を介して)実施するための能力を指すことが諒解されよう。したがって、様々なブロックに示す構成された論理または「ように構成された論理」は、「論理」という言葉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とは限らない。様々なブロックの論理間の他のやりとりまたは協働が、以下でより詳細に説明する態様の検討から、当業者には明らかになるであろう。

30

【0058】

様々な実施形態は、図4に示すサーバ400などの、様々な市販のサーバデバイスのいずれにおいても実装され得る。一例では、サーバ400は、上記で説明したIoTサーバ170の1つの例示的な構成に対応し得る。図4では、サーバ400は、揮発性メモリ402と、ディスクドライブ403などの大容量の不揮発性メモリとに結合されたプロセッサ401を含む。サーバ400は、プロセッサ401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)ドライブまたはDVDディスクドライブ406を含むことも可能である。サーバ400は、他のブロードキャストシステムコンピュータおよびサーバに、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407とのデータ接続を確立するための、プロセッサ401に結合されたネットワークアクセスポート404を含むことも可能である。図3の文脈において、図4のサーバ400は、通信デバイス300の1つの例示的な実装形態を示すが、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305は、ネッ

40

50

トワーク407と通信するためにサーバ400によって使用されるネットワークアクセスポート404に相当し、情報を処理するように構成された論理310は、プロセッサ401に相当し、情報を記憶するように構成された論理315は、揮発性メモリ402、ディスク(disk)ドライブ403、および/またはディスク(disk)ドライブ406のうちの任意の組合せに相当することが諒解されよう。情報を提示するように構成されたオブションの論理320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オブションの論理325は、図4には明示的に示さず、その中に含まれる場合もあれば、含まれない場合もある。したがって、図4は、通信デバイス300が、図2Aに示すようなIoTデバイスの実装形態に加えてサーバとして実装され得ることを説明するのを助ける。

【0059】

概して、上述のように、IPベースの技法およびサービスが成熟し、コストを削減しIPの可用性を向上させており、それによって、インターフェース接続性をますます多くの種類の日常の電子対象物に付加することが可能になっている。したがって、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、日常の電子的対象物が、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。概して、IoTが開発され普及することによって、それぞれに異なる種類を有しそれぞれに異なる活動を実行する多数の近位異種IoTデバイスおよびその他の対象物(たとえば、ライト、プリンタ、冷蔵庫、空調装置など)は、多くの異なる方法で相互作用し、多くの異なる方法で使用される場合がある。したがって、制御されたIoTネットワーク内で使用される場合がある場合によっては多数の異種IoTデバイスおよびその他の対象物に起因して、概して、特に、様々な異種IoTデバイスが適切に構成され、管理され、かつ互いに通信して情報を交換することが可能になるように、明確な信頼できる通信インターフェースを様々な異種IoTデバイスに接続する必要がある。したがって、図5～図8に関する以下の説明では、概して、本明細書で開示するように分散型プログラミング環境における異種デバイス間の直接D2D通信を可能にすることができる発見可能なデバイス間(D2D)またはピアツーピア(P2P)サービスをサポートする場合がある例示的な通信フレームワークについて概略的に説明する。

【0060】

概して、ユーザ機器(UE)(たとえば、電話、タブレットコンピュータ、ラップトップコンピュータおよびデスクトップコンピュータ、車両など)は、互いに(たとえば、Bluetooth(登録商標)、ローカルWi-Fiなどによって)ローカルに接続するように構成されても、あるいは(たとえば、セルラーネットワーク、インターネットなどを介して)リモートに接続するように構成されても、あるいはそれらの適切な組合せに従って構成されてもよい。さらに、いくつかのUEは、1対1の接続をサポートするかまたは互いに直接通信するいくつかのデバイスを含むグループに同時に接続するのをサポートする特定のワイヤレスネットワーク技法(たとえば、Wi-Fi、Bluetooth(登録商標)、Wi-Fi Directなど)を使用する近接度ベースのD2D通信をサポートしてもよい。そのために、図5は、直接D2D通信を可能にすることができる発見可能なD2Dサービスをサポートする場合がある例示的なワイヤレス通信ネットワークまたはWAN500を示し、ワイヤレス通信ネットワーク500は、様々な基地局510と他のネットワークエンティティとを含むLTEネットワークまたは別の適切なWANを備えてもよい。簡単のために、図5には、3つの基地局510a、510bおよび510c、1つのネットワークコントローラ530、ならびに1つのダイナミックホストコンフィギュレーションプロトコル(DHCP)サーバ540のみを示す。基地局510は、デバイス520と通信するエンティティであってもよく、Node B、evolved Node B(eNB)、アクセスポイントなどとも呼ばれることがある。各基地局510は、特定の地理的エリアに対して通信カバレッジを実現し得、カバレッジエリア内に位置するデバイス520のための通信をサポートし得る。ネットワーク容量を向上させるために、基地局510の全体的なカバレッジエリアが複数の(たとえば、3つの)より小さいエリアに区分されてもよく、各々のより小さいエリアがそれぞれの基地局510によってサービスされてもよい。3GPPでは、「セル」という用語は、この用語が使用される状況に応じて、このカバレッジエリアにサービスしている基地局510および/また

10

20

30

40

50

は基地局サブシステム510のカバレッジエリアを指し得る。3GPP2では、「セクタ」または「セルセクタ」という用語は、このカバレッジエリアにサービスしている基地局510および/または基地局サブシステム510のカバレッジエリアを指し得る。明確にするために、本明細書の説明では3GPPの「セル」の概念が使用されることがある。

【0061】

基地局510は、マクロセル、ピコセル、フェムトセル、および/または他のセルタイプの通信カバレッジを可能にすることができる。マクロセルは、比較的大きい地理的エリア(たとえば、半径数キロメートル)をカバーすることができ、サービスに加入しているデバイス520による無制限アクセスを可能にし得る。ピコセルは、比較的小さい地理的エリアをカバーすることができ、サービスに加入しているデバイス520による無制限アクセスを可能にし得る。フェムトセルは、比較的小さい地理的エリア(たとえば、家庭)をカバーすることができ、フェムトセルとの関連付けを有するデバイス520(たとえば、限定加入者グループ(CSG)中のデバイス)による限定アクセスを可能にし得る。図5に示す例では、ワイヤレスネットワーク500は、マクロセルのためのマクロ基地局510a、510b、および510cを含む。ワイヤレスネットワーク500は、ピコセルのためのピコ基地局510および/またはフェムトセルのためのホーム基地局510(図5には示されていない)も含み得る。

10

【0062】

ネットワークコントローラ530は、基地局510のセットに結合することができ、これらの基地局510の調整および制御を行うことができる。ネットワークコントローラ530は、バックホールを介して基地局と通信することができる単一のネットワークエンティティまたはネットワークエンティティの集合であってもよい。また、基地局は、(たとえば、直接またはワイヤレスバックホールまたはワイヤラインバックホールを介して間接的に)互いに通信し得る。DHCPサーバ540は、以下に説明するように、D2D通信をサポートすることができる。DHCPサーバ540は、ワイヤレスネットワーク500の一部であっても、またはインターネット接続共有(ICS)を介して実行されるワイヤレスネットワーク500の外部のサーバであっても、またはそれらの任意の適切な組合せであってもよい。DHCPサーバ540は、(図5に示されるように)別個のエンティティであってもよく、または、基地局510、ネットワークコントローラ530、もしくは他の何らかのエンティティの一部であってもよい。いずれの場合も、DHCPサーバ540は、ピアツーピアの通信を望むデバイス520によって到達可能であり得る。

20

30

【0063】

デバイス520はワイヤレスネットワーク500全体にわたって分散され得、各デバイス520は固定されてもまたは移動可能であってもよい。デバイス520はまた、ノード、ユーザ機器(UE)、局、移動局、端末、アクセス端末、加入者ユニットなどと呼ばれ得る。デバイス520は、セルラー電話、携帯情報端末(PDA)、ワイヤレスモデム、ワイヤレス通信デバイス、ハンドヘルドデバイス、ラップトップコンピュータ、コードレス電話、ワイヤレスローカルループ(WLL)局、スマートフォン、ネットブック、スマートブック、タブレットなどであってもよい。デバイス520は、ワイヤレスネットワーク500内の基地局510と通信してもよく、さらに他のデバイス520とピアツーピア通信してもよい。たとえば、図5に示すように、デバイス520aとデバイス520bがピアツーピア通信してもよく、デバイス520cとデバイス520dがピアツーピア通信してもよく、デバイス520eとデバイス520fがピアツーピア通信してもよく、デバイス520gとデバイス520hとデバイス520iがピアツーピア通信し、一方、残りのデバイス520が基地局510と通信してもよい。さらに図5に示すように、デバイス520a、520d、520f、および520hは、(たとえば、D2D通信を行っていないときに、または場合によってはD2D通信と同時に)基地局510と通信してもよい。

40

【0064】

本明細書の説明では、WAN通信は、(たとえば別のデバイス520などのリモートエンティティと通話するための)ワイヤレスネットワーク500におけるデバイス520と基地局510との間の通信を指し得る。WANデバイスは、WAN通信に関心を持っているか、WAN通信に参与しているデバイス520である。概して、本明細書において使用される「ピアツーピア」また

50

は「P2P」通信および「デバイス間」または「D2D」通信という用語は、基地局510を介さない2つ以上のデバイス520間の直接的な通信を指す。説明を簡単にするために、本明細書における説明では、そのような直接的な通信を指すために「デバイス間」または「D2D」という用語を使用する。ただし、本明細書において説明する様々な態様および実施形態では「ピアツーピア」、「P2P」、「デバイス間」、および「D2D」という用語が交換可能であってもよいことを当業者は諒解されよう。

【0065】

様々な実施形態によれば、D2Dデバイスは、D2D通信に関心を持っているかまたはD2D通信に関与しているデバイス520(たとえば、D2Dデバイスの近傍内の別のデバイス520に関するトラフィックデータを有するデバイス520)である。2つのデバイスは、たとえば、各デバイス520が他のデバイス520を検出できる場合、互いに近傍に位置すると見なされてもよい。概して、デバイス520は、別のデバイス520と、D2D通信の場合は直接通信してもよく、WAN通信の場合は少なくとも1つの基地局510を介して通信してもよい。

10

【0066】

様々な実施形態では、D2Dデバイス520間の直接通信はD2Dグループとして構成されてもよい。より詳細には、D2Dグループは概して、D2D通信に関心を持っているか、またはD2D通信に関与している2つ以上のデバイス520のグループを指し、D2Dリンクは、D2Dグループ用の通信リンクを指す。さらに、様々な実施形態では、D2Dグループは、D2Dグループオーナー(またはD2Dサーバ)と指定される1つのデバイス520と、D2DグループオーナーによってサービスされるD2Dクライアントと指定される1つまたは複数のデバイス520とを含んでもよい。D2Dグループオーナーは、WANとのシグナリングの交換、D2DグループオーナーとD2Dクライアントとの間のデータ送信の調整などのような、いくつかの管理機能を実行することができる。たとえば、図5に示すように、第1のD2Dグループは、基地局510aの対象となるデバイス520aおよび520bを含み、第2のD2Dグループは、基地局510bの対象となるデバイス520cおよび520dを含み、第3のD2Dグループは、異なる基地局510bおよび510cの対象となるデバイス520eおよび520fを含み、第4のD2Dグループは、基地局510cの対象となるデバイス520g、520h、および520iを含む。デバイス520a、520d、520f、および520hは、そのそれぞれのD2DグループにおけるD2Dグループオーナーであってもよく、デバイス520b、520c、520e、520g、および520iは、そのそれぞれのD2DグループにおけるD2Dクライアントであってもよい。図5の他のデバイス520は、WAN通信に関与していてもよい。

20

30

【0067】

様々な実施形態では、D2D通信は、D2Dグループ内でのみ行われ、かつ、D2Dグループに関連するD2DグループオーナーとD2Dクライアントとの間でのみ行われる。たとえば、同じD2Dグループ内の2つのD2Dクライアント(たとえば、デバイス520gおよび520i)が情報を交換することを望む場合、D2Dクライアントの一方がD2Dグループオーナー(たとえば、デバイス520h)に情報を送ってもよく、次いでD2Dグループオーナーが送信を他のD2Dクライアントに中継してもよい。様々な実施形態では、特定のデバイス520は、複数のD2Dグループに属してもよく、各D2Dグループ内でD2DグループオーナーまたはD2Dクライアントのいずれかとして振る舞ってもよい。さらに、様々な実施形態では、特定のD2Dクライアントは、1つのD2Dグループのみに属するかまたは複数のD2Dグループに属し、任意の特定の瞬間に複数のD2DグループのいずれかにおけるD2Dデバイス520と通信してもよい。概して、通信は、ダウンリンクおよびアップリンク上での送信を通じて促進され得る。WAN通信では、ダウンリンク(または順方向リンク)は基地局510からデバイス520への通信リンクを指し、アップリンク(または逆方向リンク)はデバイス520から基地局510への通信リンクを指す。D2D通信では、D2DダウンリンクはD2DグループオーナーからD2Dクライアントへの通信リンクを指し、D2DアップリンクはD2DクライアントからD2Dグループオーナーへの通信リンクを指す。様々な実施形態では、2つ以上のデバイスが、WAN技法を使用してD2D通信するのではなく、Wi-Fi、Bluetooth(登録商標)、またはWi-Fi Directなどの技法を使用してより小さいD2Dグループを形成してワイヤレスローカルエリアネットワーク(WLAN)上でD2D通信してもよい。たとえば、Wi-Fi、Bluetooth(登録商標)、Wi-Fi Direct、またはその他の

40

50

WLAN技法を使用するD2D通信では、2つ以上のモバイルフォン、ゲームコンソール、ラップトップコンピュータ、またはその他の適切な通信エンティティ間のD2D通信を可能にすることができる。

【0068】

図6は、様々な態様による、様々なデバイス610、620、630がD2D技術を使用して通信するのに利用することができる近接度ベースの分散バス640を確立するために発見可能なD2Dサービスを使用し得る例示的な環境600を示す。たとえば、様々な実施形態では、ネットワーク化コンピューティング環境におけるアプリケーション間通信を有効化するのに使用されるソフトウェアパスを含んでもよい分散バス640を介したプロセス間通信プロトコル(IPC)フレームワークを使用して単一のプラットフォーム上でのアプリケーション同士などの間の通信を容易にすることができ、この場合、ネットワーク化コンピューティング環境におけるアプリケーション間通信では、各アプリケーションが分散バス640に登録して他のアプリケーションにサービスを提供し、他のアプリケーションに登録されているアプリケーションに関する情報を分散バス640に問い合わせる。そのようなプロトコルは、信号メッセージ(たとえば、通知)がポイントツーポイントメッセージであってもまたはブロードキャストメッセージであってもよく、メソッド呼出しメッセージ(たとえば、RPC)が同期メッセージであってもまたは非同期メッセージであってもよく、分散バス640が(たとえば、1つまたは複数のパスルータまたは「デーモン」あるいは分散バス640との接続を可能にする場合がある他の適切なプロセスを介して)様々なデバイス610、620、630間のメッセージルーティングに対処する場合がある、非同期通知およびリモートプロシージャ呼出し(RPC)を可能にしてもよい。

【0069】

様々な実施形態では、分散バス640は、様々なトランスポートプロトコル(たとえば、Bluetooth(登録商標)、TCP/IP、Wi-Fi、CDMA、GPRS、UMTSなど)によってサポートされてもよい。たとえば、様々な態様によれば、第1のデバイス610は、分散バスノード612と1つまたは複数のローカルエンドポイント614とを含んでもよく、分散バスノード612は、第1のデバイス610に関連するローカルエンドポイント614と第2のデバイス620および第3のデバイス630に関連するローカルエンドポイント624および634との間の、分散バス640を通じた(たとえば、第2のデバイス620および第3のデバイス630上の分散バスノード622および632を介した)通信を容易にすることができる。図7を参照しながら以下にさらに詳細に説明するように、分散バス640は、対称的マルチデバイスネットワークトポロジをサポートしてもよく、デバイスドロップアウトの存在下でロバストな動作を可能にしてもよい。したがって、仮想分散バス640は、概して任意の下位トランスポートプロトコル(たとえば、Bluetooth(登録商標)、TCP/IP、Wi-Fiなど)とは無関係であってもよく、非セキュア(たとえば、オープン)からセキュア(たとえば、認証または暗号化)まで様々なセキュリティオプションを実現することができ、セキュリティオプションは、第1のデバイス610、第2のデバイス620、および第3のデバイス630間の自発的な接続を容易にしつつ、様々なデバイス610、620、630が互いの範囲に入るかまたは互いに近接したときに介入せずに使用され得る。

【0070】

図7は、様々な態様による、第1のデバイス(「デバイスA」)710および第2のデバイス(「デバイスB」)720がD2D技術を使用して通信するのに利用することができる近接度ベースの分散バスを確立するために発見可能なD2Dサービスを使用し得る例示的なシグナリングフロー700を示す。たとえば、図7に示すシグナリングフロー700において、デバイスA 710は、デバイスB 720との通信を要求してもよく、デバイスA 710は、そのような通信を容易にする助けになる場合があるバスノード712に加えて、通信を要求する場合があるローカルエンドポイント714(たとえば、ローカルアプリケーション、サービスなど)を含んでもよい。さらに、デバイスB 720は、ローカルエンドポイント714が、デバイスA 710上のローカルエンドポイント714とデバイスB 720上のローカルエンドポイント724との間の通信を容易にするのを助けることができるバスノード722に加えて通信を試み得るローカルエン

ドポイント724を含んでもよい。

【0071】

様々な実施形態では、754において、バスノード712および722は適切な発見機構を実行してもよい。たとえば、Bluetooth(登録商標)、TCP/IP、UNIX(登録商標)などによってサポートされる接続を発見するための機構が使用されてもよい。756において、デバイスA 710上のローカルエンドポイント714は、バスノード712を通じて利用可能なエンティティ、サービス、エンドポイントなどに接続することを要求してもよい。様々な実施形態では、この要求は、ローカルエンドポイント714とバスノード712との間の要求応答プロセスを含んでもよい。758において、分散メッセージバスが、バスノード712をバスノード722に接続し、それによってデバイスA 710とデバイスB 720との間のD2D接続を確立するように形成されてもよい。様々な実施形態では、バスノード712とバスノード722との間に分散バスを形成するための通信は、近接度ベースのD2Dプロトコル(たとえば、接続された製品間の相互運用性を実現するように設計されたAllJoyn(登録商標)ソフトウェアフレームワークおよび近位ネットワークを動的に作成し近位D2D通信を容易にするための様々な製造業者によるソフトウェアアプリケーション)を使用して容易にされてもよい。代替として、様々な実施形態では、サーバ(図示せず)はバスノード712とバスノード722との間の接続を容易にしてもよい。さらに、様々な実施形態では、バスノード712とバスノード722との間に接続を形成する前に適切な認証機構が使用されてもよい(たとえば、クライアントが認証コマンドを送って認証対話を開始することができるSASL認証)。さらに、758において、バスノード712および722は、利用可能な他のエンドポイント(たとえば、図6のデバイスC 630上のローカルエンドポイント634)に関する情報を交換してもよい。そのような実施形態では、バスノードが維持する各ローカルエンドポイントが他のバスノードに通知されてもよく、この通知は、一意のエンドポイント名、トランスポートタイプ、接続パラメータ、または他の適切な情報を含んでもよい。

【0072】

様々な実施形態では、760において、バスノード712およびバスノード722は、それぞれローカルエンドポイント724および714に関連する得られた情報を使用して、様々なバスノードを通じて利用可能な得られた実エンドポイントを表すことのできる仮想エンドポイントを作成してもよい。様々な実施形態では、バスノード712上のメッセージルーティングでは、実エンドポイントおよび仮想エンドポイントを使用してメッセージを送信してもよい。さらに、リモートデバイス(たとえば、デバイスA 710)上に存在するあらゆるエンドポイントに1つのローカル仮想エンドポイントがあってもよい。さらに、そのような仮想エンドポイントは、分散バス(たとえば、バスノード712とバスノード722との間の接続)を介して送られたメッセージを多重化しならびに/あるいは多重化解除してもよい。様々な実施形態では、仮想エンドポイントは、実エンドポイントと同様にローカルバスノード712または722からメッセージを受信してもよく、分散バスを介してメッセージを転送してもよい。したがって、仮想エンドポイントは、エンドポイント多重化分散バス接続からローカルバスノード712および722へメッセージを転送してもよい。さらに、様々な実施形態では、リモートデバイス上の仮想エンドポイントに対応する仮想エンドポイントは、任意の時点で特定のトランスポートタイプの所望のトポロジーに対処するように再接続されてもよい。そのような実施形態では、UNIX(登録商標)ベースの仮想エンドポイントは、ローカルと見なされることがあり、したがって、再接続の候補とは見なされないことがある。さらに、TCPベースの仮想エンドポイントは、1つのホップルーティングに関して最適化されてもよい(たとえば、各バスノード712および722は互いに直接接続されてもよい)。さらに、Bluetooth(登録商標)ベースの仮想エンドポイントは、Bluetooth(登録商標)ベースのマスタがローカルマスタノードと同じバスノードであってもよい単一ピコネット(たとえば、1つのマスタおよびn個のスレーブ)に関して最適化されてもよい。

【0073】

様々な実施形態では、バスノード712とバスノード722は、762においてバス状態情報を交換してバスインスタンス同士をマージし、分散バスを介した通信を可能にしてもよい。

たとえば、様々な実施形態では、バス状態情報は、周知の一意のエンドポイント名マッピング、整合規則、ルーティンググループ、または他の適切な情報を含んでもよい。様々な実施形態では、状態情報は、分散バスベースのローカル名と通信するローカルエンドポイント714および724とのインターフェースを使用してバスノード712インスタンスとバスノード722インスタンスとの間で伝達されてもよい。別の態様では、バスノード712およびバスノード722の各々は、分散バスへのフィードバックを可能にする役割を果たすローカルバスコントローラを維持してもよく、バスコントローラは、グローバルメソッド、引数、信号、およびその他の情報を分散バスに関連する規格に変換してもよい。バスノード712およびバスノード722は、764において上述のようなバスノードノード接続の間に導入されるあらゆる変化に関してそれぞれのローカルエンドポイント714および724に通知する信号を伝達(たとえば、ブロードキャスト)してもよい。様々な実施形態では、新しいおよび/または削除されたグローバル名および/または変換後の名前が、名前オーナー変更後信号によって示されてもよい。さらに、(たとえば、名前衝突に起因して)ローカルに失われることがあるグローバル名が名前喪失信号によって示されてもよい。さらに、名前衝突に起因して転送されるグローバル名が名前オーナー変更後信号によって示されてもよく、バスノード712およびバスノード722が切り離された場合および/またはときに消える一意の名前が名前オーナー変更後信号によって示されてもよい。

10

【0074】

上記に使用されたように、周知の名前を使用してローカルエンドポイント714および724を一意に記述してもよい。様々な実施形態では、デバイスA 710とデバイスB 720との間で通信が行われるとき、異なる周知の名前タイプが使用されてもよい。たとえば、バスノード712が直接接続されるデバイスA 710に関連するバスノード712上にのみデバイスローカル名が存在してもよい。別の例では、すべての既知のバスノード712および722上にグローバル名が存在してもよく、すべてのバスセグメント上に存在してもよい名前のオーナーは1人だけである。言い換えれば、バスノード712とバスノード722が連結され、衝突が起これば、オーナーのうちの1人がグローバル名を失うことがある。さらに別の例では、クライアントが仮想バスに関連する他のバスノードに接続されるときに変換後の名前が使用されてもよい。そのような実施形態では、変換後の名前はアペンデッドエンドを含んでもよい(たとえば、グローバルに一意の識別子「1234」を有する分散バスに接続された周知の名前「org.foo」を有するローカルエンドポイント714は「G1234.org.foo」と見なされてもよい)。

20

30

【0075】

様々な実施形態では、バスノード712およびバスノード722は、766においてエンドポイントバスポロジの変更について他のバスノードに通知するための信号を伝達(たとえば、ブロードキャスト)してもよい。その後、ローカルエンドポイント714からのトラフィックは、仮想エンドポイントを通過してデバイスB 720上の意図されるローカルエンドポイント724に達してもよい。さらに、動作中に、ローカルエンドポイント714とローカルエンドポイント724との間の通信はルーティンググループを使用してもよい。様々な実施形態では、ルーティンググループは、エンドポイントが信号、メソッド呼出し、またはエンドポイントのサブセットからの他の適切な情報を受信するのを可能にしてもよい。したがって、ルーティング名は、バスノード712または722に接続されたアプリケーションによって決定されてもよい。たとえば、D2Dアプリケーションは、アプリケーションに組み込まれた一意で周知のルーティンググループ名を使用してもよい。さらに、バスノード712および722は、ローカルエンドポイント714および724のルーティンググループへの登録および/または登録解除をサポートしてもよい。様々な実施形態では、ルーティンググループは、現在のバスインスタンスよりも後のインスタンスまで持続しなくてもよい。別の態様では、アプリケーションは、分散バスに接続するたびにアプリケーションの好ましいルーティンググループの登録をしてもよい。さらに、グループはオープンであっても(たとえば、任意のエンドポイントが参加してよい)またはクローズドであっても(たとえば、グループの作成者がグループを修正してもよい)よい。さらに、バスノード712または722は、

40

50

他のリモートバスノードにルーティンググループエンドポイントの追加、削除、またはその他の変更を通知するための信号を送ってもよい。そのような実施形態では、バスノード712または722は、グループにメンバーが追加されならびに/あるいはグループからメンバーが削除されたときはいつでも他のグループメンバーにルーティンググループ変更信号を送ってもよい。さらに、バスノード712または722は、最初にルーティンググループから削除されることなく分散バスから切り離されるエンドポイントにルーティンググループ変更信号を送ってもよい。

【0076】

様々な態様によれば、図8Aは、第1のホストデバイス810と第2のホストデバイス830との間のD2D通信を可能にするために第1のホストデバイス810と第2のホストデバイス830との間に形成される場合がある近接度ベースの例示的な分散バスを示す。より詳細には、図6に関して上記に説明したように、近接度ベースの分散バスの基本構造は、別個の物理的ホストデバイス上に存在する複数のバスセグメントを備えてもよい。したがって、図8Aでは、近接度ベースの分散バスの各セグメントがホストデバイス810、830のうちの1つのホストデバイス上に配置されてもよく、ホストデバイス810、830の各々は、それぞれのホストデバイス810、830上に配置されたバスセグメントを実施する場合があるローカルバスルータ(または「デモン」)を実行する。たとえば、図8Aでは、各ホストデバイス810、830は、それぞれのホストデバイス810、830上に配置されたバスセグメントを実施するバスルータを表すために丸で囲まれた「D」を含む。さらに、ホストデバイス810、830のうちの1つまたは複数はいくつかのバスアタッチメントを有してもよく、各バスアタッチメントはローカルバスルータに接続する。たとえば、図8Aでは、ホストデバイス810および830上のバスアタッチメントは、各々がサービス(S)またはサービスを要求する場合があるクライアント(C)に対応する六角形として示されている。

【0077】

しかし、場合によっては、埋込みデバイスにはローカルバスルータを実行するのに十分なリソースがない場合がある。したがって、図8Bは、1つまたは複数の埋込みデバイス820、825が近接度ベースの分散バスに接続するためにホストデバイス(たとえば、ホストデバイス830)に接続し、それによって、(たとえば、ホストデバイス830あるいはホストデバイス830を介して近接度ベースの分散バスにアタッチされた他のホストデバイス810および/または埋込みデバイス825との)D2D通信に関与することができる例示的な近接度ベースの分散バスを示す。したがって、埋込みデバイス820、825は概して、ホストデバイス830上で実行されているバスルータを「借用して」もよく、図8Bは、埋込みデバイス820、825が、埋込みデバイス820、825が存在する分散バスセグメントを管理する借用されたバスルータを実行するホストデバイス830から物理的に分離される構成を示す。概して、埋込みデバイス820、825とホストデバイス830との間の接続は、伝送制御プロトコル(TCP)に従って行われてもよく、埋込みデバイス820、825とホストデバイス830との間を流れるネットワークトラフィックは、上記に図6および図7に関してさらに詳細に説明したのと同様にそれぞれのセッションを介して流れるバスメソッド、バス信号、および特性を実現するメッセージを含んでもよい。

【0078】

より詳細には、埋込みデバイス820、825は、クライアントとサービスとの間の発見および接続プロセスと概念的に同様であってもよい発見および接続プロセスに従ってホストデバイス830に接続してもよく、ホストデバイス830は、埋込みデバイス820、825をホストする能力または意志をシグナリングする周知の名前を通知してもよい(たとえば、「org.alljoyn.BusNode」)。一使用事例では、埋込みデバイス820、825は、単に、周知の名前を通知する「第1の」ホストデバイスに接続してもよい。しかし、埋込みデバイス820、825は、単に、周知の名前を通知する第1のホストデバイスに接続する場合、そのホストデバイスに関連する種類に関する知識(たとえば、ホストデバイス830がモバイルデバイスであるか、セットトップボックスであるか、アクセスポイントであるか、など)を有さない場合があり、またホストデバイスに関するロードステータスに関する知識を有さない可能性が

ある。したがって、他の使用事例では、埋込みデバイス820、825は、ホストデバイス810、830が、他のデバイス(たとえば、埋込みデバイス820、825)をホストする能力または意志を通知するときに提供する情報に基づいてホストデバイス830に適応的に接続してもよく、それによって、他のデバイスは、ホストデバイス810、830に関連する特性(たとえば、種類、ロードステータスなど)および/または埋込みデバイス820、825に関連する要件(たとえば、同じ製造業者から得られる、ホストデバイスに接続するための優先権を表すランキングテーブル)に従って近接度ベースの分散バスに参加してもよい。

【0079】

様々な態様によれば、IoT環境が一般に、それぞれに異なる機能を有する様々な異種デバイスを含むと考えられることを利用して、直接的および間接的な挙動分析を行ってIoT環境における1つまたは複数のデバイスに対する潜在的に悪意のある攻撃を検出し、デバイスの健全性を監視し、誤動作およびその他の異常を検出することができ、それによって、IoT環境における顧客サービスを製造業者の視点と顧客の視点の両方から自動化し、より安価に、より容易に、かつより高速に実行することができる。たとえば、多くの異常は、いくつかの基本的な観測値(たとえば、特定の期間にわたる電力ドロワー、局所温度および/または周囲温度を示すセンサー測定値、水位、煙レベル、一酸化炭素および/または二酸化炭素レベル、可視性レベル、慣性測定ユニット(IMU)によって測定された振動など)に基づいて検出し分析することができる。

【0080】

したがって、多くのIoTデバイスが比較的限られた挙動を有する単純なデバイス(たとえば、トースター、サーモスタット、洗濯機、テレビジョン、照明器具、およびその他の日常的な対象物)であることを考えて、IoT環境における(すべてではないとしても)大部分のデバイスが特定のローカル挙動(たとえば、電力消費量、センサー出力など)を観測する機能を少なくとも有すると仮定することができる。さらに、特定のIoT環境におけるすべてのデバイスが、挙動分析を行うのに十分な処理リソース、記憶リソース、および/または他の機能を有するわけではないにもかかわらず、コンピュータ化された接続されたIoT環境における(すべてではないとしても)大部分の機器およびその他のデバイスは、ネットワークを介して通信する機能を有し、したがって、(たとえば、分散型プログラミング環境における異種デバイス間の直接D2D通信を可能にする場合がある、図5～図8に関して上記において説明した通信フレームワークによる)ローカルに観測された挙動をより高性能のデバイスに送る機能を有すると考えることができる。したがって、分散型アーキテクチャを有するIoT環境では、IoT環境におけるより高性能の1つまたは複数のデバイス(たとえば、スマートフォン、「常時接続」ワイヤレスルータなど)が、他の(より単純な)デバイスがローカルに観測する挙動を集約し、ならびに/あるいは分散型IoT環境全体にわたって挙動分析を行い、顧客サービスを必要とする悪意のある攻撃または誤動作を潜在的に示す異常を検出することができる。さらに、IoT環境におけるより高性能のデバイスは、オンデバイス(ローカル)挙動分析を行って、ローカルに観測された挙動を別のアグリゲータおよび/またはアナライザデバイスに送る必要なしに異常条件を検出してよい。

【0081】

したがって、図9は、オンデバイス挙動分析を行い、それによってローカルな視点から異常条件を検出するうえで適切な記憶リソース、処理リソース、および/またはその他の機能を有する例示的なIoTデバイス900を示す。しかし、当業者には、図9に示すIoTデバイス900が、(たとえば、このIoTデバイスが、デバイス900においてローカルに観測されならびに/あるいは分析された挙動を分散型IoT環境における1つまたは複数の他のデバイスに関してならびに/あるいは分散型IoT環境全体に関してより広いコンテキストにおいて検討できるように分散型IoT環境に関連付けられる場合に)代替としてならびに/あるいは追加として、様々な環境においてローカルに観測されならびに/あるいは分析された挙動を1つまたは複数のアグリゲータデバイスおよび/またはアナライザデバイスに送ってもよいことが諒解されよう。さらに、IoTデバイス900は図9におけるスマートフォンの外観を有するが、当業者には、図9に示すIoTデバイス900が、オンデバイス挙動分析を行うのに十分

10

20

30

40

50

な記憶リソース、処理リソース、および/または他の機能を有する任意の適切なデバイス(たとえば、実質的な記憶リソースおよび処理リソースを有するタブレット、ワイヤレスゲートウェイ、デスクトップコンピュータ、機器など)を備えてもよいことが諒解されよう。

【0082】

様々な実施形態において、IoTデバイス900は、オンデバイス挙動分析を有効化するために、少なくとも観測モジュール920と、挙動ベクトル抽出モジュール930と、分析モジュール940とを含むオンデバイス健全性監視プラットフォーム910を備えてもよい。より詳細には、IoTデバイス900は、1つまたは複数のセンサー、測定ハードウェア、またはIoTデバイス900が関連付けられたローカル環境を監視するのを可能にする他の適切な構成要素(たとえば、加速度および傾斜を測定することができる加速度計、内部温度および/または周囲温度を測定することができる温度センサー、光を検出することができる光検出器、ローカルワイヤレス信号を監視することができるアンテナ、プロセッサ活動、ネットワーク活動などを検出することができる計器)を備えると仮定することができる。したがって、様々な実施形態では、観測モジュール920は、モバイルスタックにおける1つまたは複数のレベルにおける1つまたは複数のアプリケーションプログラムインターフェース(API)呼出しおよび最低限の計器によってIoTデバイス900に関するローカル挙動情報を監視するか場合によっては収集するように構成されてもよい。したがって、観測モジュール920は、高速で効率的なメモリ内処理を利用して、IoTデバイス900に関連する挙動情報(たとえば、ハートビート、センサー測定値、電力消費量、試験結果など)を監視、測定、または場合によ

10

20

【0083】

様々な実施形態において、観測モジュール920は次いで、観測された挙動情報を表す特性を含む1つまたは複数のアクションログ922を挙動ベクトル抽出モジュール930に渡してもよく、挙動ベクトル抽出モジュール930は次いで、アクションログ922に含まれる特性をn次元空間内にマップして、IoTデバイス900上の観測された挙動を表す1つまたは複数の挙動ベクトル932を抽出してもよい。したがって、挙動ベクトル932の各々はサイズnを有してもよく、挙動ベクトル932における各数字は、1つの特性(または観測された挙動)に関連する値を表す。たとえば、IoTデバイス900がスマートフォンを備え、アクションログ922に含まれる特性が、(たとえば、バッテリーにおいて消費されるミリアンペア(mA)数による)電力消費量、内部温度、(たとえば、パーセンテージによる)プロセッサ使用率、および特定の観測期間におけるネットワーク接続性を表すと仮定すると、挙動ベクトル抽出モジュール930が生成する例示的な挙動ベクトル932は以下の形式を有してもよく、図示の例におけるnは4に等しい。

30

【0084】

【表1】

特性	power_consumption	temperature_internal	cpu_usage	internet_connectivity
値	0.25	78	30	1

40

Table 1 :: 例示的なオンデバイス挙動ベクトル

【0085】

様々な実施形態において、挙動ベクトル抽出モジュール930において生成された1つまたは複数の挙動ベクトル932は次いで、分析モジュール940に供給され、この場合、1つまた

50

は複数の挙動ベクトル932は、それぞれに異なる観測粒度によるそれぞれに異なる特性セットを含んでもよい。たとえば、上記に示した例示的な挙動ベクトル932では、power_consumption特性、temperature_internal特性、およびcpu_usage特性は厳密な値を有し、一方、internet_connectivityはバイナリ値を有し、それによって、power_consumption特性、temperature_internal特性、およびcpu_usage特性は、internet_connectivity特性よりも細かい粒度を有する。したがって、分析モジュール940は、それぞれに異なる観測粒度を示すことができる1つまたは複数の特性セットを含む挙動ベクトルを集約してもよく、分析モジュール940は、集約された挙動ベクトル932を分析して、IoTデバイス900に対する潜在的な悪意のある攻撃、IoTデバイス900における誤動作もしくはバーンアウト、またはさらなる調査、顧客サービス、もしくは他の是正を必要とする場合がある他の異常944を示す可能性がある1つまたは複数の挙動異常944を検出してもよい。たとえば、様々な実施形態において、分析モジュール940は、IoTデバイス900に関連する型式、バージョンなどに固有のモデルとの比較に応じて挙動ベクトル抽出モジュール930において生成された集約された挙動ベクトル932を分析してもよく、集約された挙動ベクトル932と比較して使用されるモデルは、IoTデバイス900に関連する製造業者またはその他の適切なりポジトリ(たとえば、IoTデバイス900と同一であるかまたはIoTデバイス900と同様の他のIoTデバイスに関連する1つまたは複数のモデルを含むローカルIoTネットワーク上のリポジトリ)から取得されてもよい。代替として(または追加として)、比較において使用されるモデルは、ローカルIoTネットワークに関連する全体的な状態モデルを備えてもよい(たとえば、「internet_connectivity」特性が、観測間隔の間ネットワーク接続性が存在しなかったことを示すゼロ値を有する場合、ネットワーク接続性が存在しなかったことは、ローカルIoTネットワークに関連する全体的な状態モデルが、ローカルIoTネットワーク内のすべてのデバイスがネットワーク接続性の問題を有することが予想されるようにホームゲートウェイにおける誤動作を示す場合に挙動異常944を反映しないことがある。)

10

20

30

40

50

【0086】

したがって、分析モジュール940は必ずしも、挙動ベクトル932内の任意の1つの特性に基づいて挙動異常944を検出するわけではない。その代わりに、分析モジュール940は、機械学習を使用して、組み合わせられた挙動ベクトル932における特性を評価することによって挙動異常944を検出してもよい。さらに、様々な実施形態において、分析モジュール940は、IoTデバイス900に関連する正常挙動を表すモデルを経時的に構築してもよく、IoTデバイス900に関連する正常挙動を表すモデルは、IoTデバイス900に関連する製造業者から取得されるモデル、オンデバイス健全性監視プラットフォーム910において生成された挙動ベクトル932、ローカルIoTネットワーク内の他のデバイスに対応する挙動ベクトルおよび/またはモデル、ローカルIoTネットワークに関連する1人または複数のユーザからの入力および対話に対応する挙動ベクトルおよび/またはモデル、ローカルIoTネットワークに関連する全体的な状態モデル、ならびに/あるいはIoTデバイス900上の正常挙動と異常挙動の関係を評価するための関連性を有する場合がある他の任意の適切な情報に基づいて経時的に構築されてもよい。

【0087】

さらに、様々な実施形態において、分析モジュール940は、分析された挙動ベクトル932から1つまたは複数の挙動異常944を検出したことに応答してオンライントラブルシューティング、オンデバイス診断、または他の是正技術呼び出ししてもよい。たとえば、一実施形態では、分析モジュール940は、より多くの情報を収集できるように要求/応答システムを呼び出してIoTデバイス900と顧客サービスとの間の往復メッセージングを有効化してもよい(たとえば、分析モジュール940は、IoTデバイス900と顧客サービスとの間のルータとして働いてもよい)。別の例では、分析モジュール940は、ローカルIoTネットワークにおける別のアグリゲータおよび/またはアナライザノードに通知して、(たとえば、IoTデバイス900が是正をローカルに実行できないほど挙動異常944が深刻である場合に)挙動異常944を是正するための支援を要求し、ならびに/あるいはローカルIoTネットワークに関連する全体的な状態の構築を支援してもよい。上述の使用事例では、分析モジュール

ル940は、挙動異常944が検出された関連する挙動ベクトル932(またはそれに含まれる特性)をさらに生成してもよい。さらに、分析モジュール940は、分析された挙動ベクトル932に基づいて、観測モジュール940を構成するための観測フィードバックおよび調整942を生成してもよい。たとえば、観測フィードバックおよび調整942は、IoTデバイス900に関する挙動情報を観測すること、観測すべき(または観測しない)1つまたは複数の特性または挙動を指定することなどのために観測モジュール920が使用する頻度、間隔持続時間などを調整してもよい。その場合、観測モジュール920は、周期的にならびに/あるいは特定のトリガリング基準に応答してアクションログ922を生成してもよく、アクションログ922および挙動ベクトル932は同様に、それぞれ挙動ベクトル抽出モジュール930および分析モジュール940において周期的に集約され分析されてもよい。

10

【0088】

図10は、様々な態様による、様々なノードが、例示的なローカルIoTネットワーク1000における直接的および/または間接的な挙動分析ならびに自動化されたデバイス健全性監視をサポートするために通信する場合がある分散型アーキテクチャを有するローカルIoTネットワーク1000を示す図である。より詳細には、図9に示すオンデバイス健全性監視プラットフォーム910は、オンデバイス挙動分析を行ううえで適切な記憶リソース、処理リソース、および/またはその他の機能を有するIoTデバイス上で利用されてもよいが、図10に示す分散型IoTネットワーク1000は、ローカル挙動を観測し、ネットワークを介して通信してより高性能のデバイスにローカルに観測された挙動を送る機能を有する場合があります。得る様々なより単純なデバイスを備えてもよく、より高性能のデバイスは次いで、分散型IoTネットワーク1000全体にわたって観測された挙動に基づいて挙動分析を行う。概して、分散型IoTネットワーク1000内の様々なノード間の通信は、図5～図8に関して上記にさらに詳しく説明したように、異種デバイス間の直接デバイス間(D2D)通信を有効化することができる通信フレームワークに従って行われてもよい。

20

【0089】

したがって、様々な実施形態では、分散型IoTネットワーク1000内の様々なデバイスは、1つまたは複数のレガシーデバイス(たとえば、電球)、限られた機能を有する1つまたは複数のIoTデバイス(たとえば、新型の冷蔵庫)、および分散型IoTネットワーク1000全体にわたって挙動分析を行うのに十分な記憶機能および処理機能を有する1つまたは複数のIoTデバイスを含んでもよい。したがって、分散型IoTネットワーク1000内のデバイスは概して、各クラスに分割されてもよく、関連付けられたそれぞれのクラスに対応する指定された役割に応じて動作してもよい。より詳細には、分散型IoTネットワーク1000内のデバイスが分割されるクラスは、(1)ローカル挙動を観測し、観測されたローカル挙動をIoTネットワーク1000全体にわたって送ることができ、「オブザーバ」の役割に従って動作する場合があります。レガシーデバイス、(2)限られた機能(すなわち、レガシーデバイスよりも多いが挙動分析を行うには不十分な機能)を有し、「アグリゲータ」の役割に従って動作する場合があります。IoTデバイス、および(3)分散型IoTネットワーク1000全体にわたって挙動分析を行うのに十分な記憶機能および処理機能を有し、「アナライザ」の役割において動作する場合があります。IoTデバイスを少なくとも含んでもよい。

30

【0090】

さらに、特定の実施形態において、分散型IoTネットワーク1000内の1つまたは複数のデバイスは、限られたピアツーピア通信機能を有してもよく、デバイスが観測されたローカル挙動をIoTネットワーク1000全体にわたって送ることができないような限られたレンジを有する、Bluetooth(登録商標)を介した通信、近距離通信、低電力無線周波数、またはその他のプロトコルのみをサポートするデバイスを含んでもよい。したがって、分散型IoTネットワーク1000が、そのような限られた通信機能を有する1つまたは複数のデバイスを含む場合、オブザーバ、アグリゲータ、および/またはアナライザの役割において動作するように構成されたデバイスは、上記のデバイスが関連付けられた限られた通信レンジ内を通過する際にそのようなデバイスから任意の関連する挙動情報を収集してもよい(これには、たとえば、そのようなデバイスから収集される挙動情報が必ずしもリアルタイム

40

50

アクションを必要としないという効率上の目的がある)。さらに、様々な実施形態において、IoTネットワーク1000は、IoTネットワーク1000内のデバイスがネットワークを介して送信するメッセージによってそれらのデバイスに関連する挙動を(たとえば、ネットワークスヌーピングまたはパケットスニффingを介して)観測することができる1つまたは複数のネットワーク監視デバイスを備えてもよい。

【0091】

したがって、図10に示す分散型IoTネットワーク1000では、オブザーバの役割において動作するように構成されたデバイスは、本明細書ではまとめてオブザーバノード1012~1036と呼ぶ、屋外スピーカ1012、1014と、屋内スピーカ1016、1018と、サーモスタット1020と、洗濯機1022と、時計1024と、コーヒーメーカー1026と、リビングルームフロアスピーカ1028と、本棚オーディオシステム1030と、ホームシアタースピーカ1032、1034と、ドアノブ1036とを備える。さらに、アグリゲータの役割において動作するように構成されたデバイスは、本明細書ではまとめてアグリゲータノード1050~1052と呼ぶ冷蔵庫1050およびテレビジョン1052を含み、アナライザの役割において動作するように構成されたデバイスは、本明細書ではまとめてアナライザノード1070~1072と呼ぶスマートフォン1070およびワイヤレスルータまたはホームゲートウェイ1072を含む。様々な実施形態において、図9に示すオンデバイス健全性監視プラットフォーム910に関連するコンテキストでは、オブザーバノード1012~1036は概して、オブザーバモジュール920と同様の機能を実行し、それによって、オブザーバノード1012~1036は、ローカル挙動情報を監視するかまたは場合によっては収集し、観測された挙動を表す1つまたは複数の特性を含む1つまたは複数のアクションログを生成してもよい。さらに、アグリゲータノード1050~1052およびアナライザノード1070~1072は同様に、ローカル挙動を観測し、観測された挙動を表す特性を含む1つまたは複数のアクションログを生成してもよい。たとえば、トースター、煙感知器、冷蔵庫、およびテレビジョンにおいて生成されたアクションログに含まれる場合がある例示的な特性を以下の表に示す。

【0092】

10

20

【表 2】

IoT デバイス	例示的な特性
トースター	toaster_on temperature power_consumption settings item_weight weight_zero_when_toaster_ON temperature_above_threshold toaster_ON_temperature_change_zero
煙感知器	smoke_sensor battery_level test_signal
冷蔵庫	power_consumption load_level temperature settings
テレビジョン	power_consumption temperature internet_connectivity settings_resolution settings_brightness input_devices content_type parental_control (ON/OFF)

10

20

30

Table 2 :: 例示的な IoT デバイス特性

【 0 0 9 3 】

様々な実施形態において、オブザーバノード1012～1036は次いで、ローカルに生成されたアクションログを最も近いアグリゲータノード1050～1052に送信するか、あるいは代替として、最も近いアナライザノード1070～1072にアクションログを送信してもよい(この目的は、たとえば、アグリゲータノード1050～1052のオーバーローディングを防止することであり、この場合、オブザーバノード1012～1036はアグリゲータノード1050～1052よりもアナライザノード1070～1072に近い)。さらに、アグリゲータノード1050～1052は、オブザーバノード1012～1036から受信されたアクションログを最も近いアナライザノード1070～1072に周期的に中継してもよく、アナライザノード1070～1072は次いで、アクションログに基づいてIoTネットワーク1000全体にわたって挙動分析を実行してもよい。その場合、アナライザノード1070～1072は、図9に示す挙動ベクトル抽出モジュール930および分析モジュール940と同様の機能を実行してもよく、アナライザノード1070～1072は、アグリゲータノード1050～1052(および/またはアクションログが受信された任意のオブザーバ

40

50

ノード1012～1036)から受信されたアクションログに含まれる特性をn次元空間内にマップしてIoTネットワーク1000において観測された挙動から挙動ベクトルを抽出してもよい。したがって、挙動ベクトルは、IoTネットワーク1000において観測された特性(または挙動)を組み合わせてもよく、この場合、挙動ベクトルにおける各値は、1つの観測された特性(または挙動)に関連する値を表す。たとえば、挙動ベクトルは、ルータまたは他の適切なアナライザノード1070～1072において生成され、トースター(TS)およびスマート電源プラグ(SP)において観測された特性を組み合わせる例示的な挙動ベクトルは以下の形成を有してもよい。

【0094】

【表3】

10

特性	TS_ON	TS_temp	TS_weight	TS_max_temp	SP_ON	SP_power_drawn
値	1	78	0.1	90	1	0.7

Table 3 :: 例示的な挙動ベクトル

20

【0095】

したがって、様々な実施形態において、アナライザノード1070～1072において抽出された挙動ベクトルは、それぞれに異なる観測粒度を示すそれぞれに異なる特性セットを含んでもよく、アナライザノード1070～1072は、集約および分析を行い、IoTネットワーク1000またはIoTネットワーク1000内のデバイスに対する潜在的な悪意のある攻撃、IoTネットワーク1000内の1つまたは複数のデバイスにおける誤動作またはバーンアウト、あるいはさらなる調査、顧客サービス、および/または是正を必要とする場合があるその他の異常を示す可能性がある1つまたは複数の挙動異常を検出してもよい。たとえば、様々な実施形態において、アナライザノード1070～1072は、IoTネットワーク1000内のすべてのデバイスからの挙動ベクトルおよびIoTネットワーク1000に固有のモデルならびに/あるいはIoTネットワーク1000に関連するユーザからの入力および対話などに基づいて、製造業者または他の適切なリポジトリから取得される場合がある、観測された挙動に対応するデバイスに関連する型式、バージョンなどに固有のモデルとの比較に従って集約された挙動ベクトルを分析してもよい。したがって、アナライザノード1070～1072は、任意の1つの特性のみに基づいて挙動異常を検出するのではなく、機械学習を使用して、正常挙動、全体的な環境の状態などを示すように経時的に構築されたモデルに対して組み合わせられた挙動ベクトルを評価することによって挙動異常を検出してもよい。

30

【0096】

したがって、様々な実施形態において、IoTネットワーク1000は、ネットワークに含まれる様々なデバイスに関連する機能に応じて直接的および間接的な挙動分析をサポートするためのそれぞれに異なる構成を有してもよい。たとえば、ある仮説的なシナリオでは、IoTネットワーク1000におけるすべてのデバイスが、(たとえば、図9のように)オンデバイス挙動分析を行うのに十分な機能を有してもよく、その場合、各デバイスは、アナライザの役割において動作し、単に、異常挙動を検出するのに使用されるモデルを構築し維持するのに適切な所望の情報を報告してもよい。別のシナリオでは、IoTネットワーク1000は、オンデバイス挙動分析を行うのに十分な機能を有するいくつかのデバイスと、(たとえば、アグリゲータノード1050～1052および/またはオブザーバノード1012～1036とのD2D通信、監視されるネットワークメッセージなどによって)他のデバイスからできるだけ多くの情報を収集することができず(その場合、オンデバイス挙動分析を行うのに十分な機能を有する各デバイスはアナライザの役割において動作してもよい)、かつアナライザの役

40

50

割において動作する隣接するデバイスから任意の他の余分な情報を収集することができない他のデバイスを含んでもよい。さらに別のシナリオでは、IoTネットワーク1000が、オンデバイス挙動分析を行うのに十分な機能を有する1つのデバイス(たとえば、スマートフォン1070)のみを含む場合、そのデバイスは、オブザーバノード1012~1036、アグリゲータノード1050~1052、任意のネットワーク監視エージェントなどとのワイヤレス通信によって任意の利用可能な情報を収集し、(たとえば、デバイスライブラリネスを監視するために)その情報に基づいて挙動分析を行ってもよい。たとえば、スマートフォン1070、ホームゲートウェイ1072、またはアナライザの役割において動作することができる別の単一のデバイスは、IoTネットワーク1000に関する任意の利用可能な情報(たとえば、温度、光、移動量など)を収集し、収集できる利用可能な情報に基づいてIoTネットワーク1000を監視し、ローカル環境に関して取得される測定値をオブザーバノード1012~1036、アグリゲータノード1050~1052、ネットワーク監視エージェントなどとのワイヤレス通信を介して収集することのできる任意の情報と一致させることができる適切なハードウェアおよびソフトウェアを備えてもよい。

10

20

30

40

50

【0097】

様々な態様によれば、図11を参照すると、別の例示的な分散型アーキテクチャ1100が図示されており、図11に示す分散型アーキテクチャ1100は、様々なノードが直接的および/または間接的な挙動分析ならびに自動化されたデバイス健全性監視をサポートするために互いに通信する場合があるローカルIoT環境を備えてもよい。概して、図11に示す分散型アーキテクチャ1100は、図10に示す分散型IoTネットワーク1000と同じでありならびに/あるいは実質的に同様である様々な構成要素および機能を含んでもよく、したがって、説明を簡潔にかつ容易にするために、分散型アーキテクチャ1100における特定の構成要素に関する様々な詳細は、関連する詳細が上記においてすでに提示されている限りここでは省略されてもよい。たとえば、図11において、分散型アーキテクチャ1100は、上述のオブザーバの役割において動作する場合がある煙感知器1112およびサーモスタット1114と、上述のアグリゲータの役割において動作する場合がある冷蔵庫1116およびゲームコンソール1118と、上述のアナライザの役割において動作する場合がある常時接続監視デバイス1110と、煙感知器1112、サーモスタット1114、冷蔵庫1116、ゲームコンソール1118、および1つまたは複数の他のデバイスに関連する挙動を各デバイスがネットワークを介して送信するメッセージによって(たとえば、ネットワークスヌーピングまたはパケットスニффイングを介して)観測する場合があるネットワークトラフィックモニタ1120とを含んでもよい。

【0098】

したがって、図11に示す分散型アーキテクチャ1100では、常時接続監視デバイス1110は、オブザーバデバイス1112、1114、アグリゲータデバイス1116、1118、およびネットワークトラフィックモニタ1120から1つまたは複数のアクションログ1122を受信してもよく、常時接続監視デバイス1110は、アクションログ1122に含まれる特性をn次元空間内にマップして観測された挙動を表す1つまたは複数の挙動ベクトル1132を抽出するように構成された挙動ベクトル抽出モジュール1130を備えてもよい。挙動ベクトル抽出モジュール1130において生成された挙動ベクトル1132は次いで、分析モジュール1140に供給されてもよく、分析モジュール1140は、監視されたデバイスにおける潜在的な悪意のある攻撃、誤動作、またはバーンアウト、あるいはその他の異常を示す可能性がある1つまたは複数の挙動異常を検出するために挙動ベクトル1132を集約してもよい。たとえば、様々な実施形態において、分析モジュール1140は、上述のように、IoTネットワーク1100内のすべてのデバイスからの挙動ベクトルおよびIoTネットワーク1100に固有のモデルならびに/あるいはIoTネットワーク1100に関連するユーザからの入力および対話に基づいて、製造業者または他の適切なリポジトリから取得される場合がある、観測された挙動に対応するデバイスに関連する型式、バージョンなどに固有のモデルとの比較に従って集約された挙動ベクトル1132を分析してもよい。さらに、様々な実施形態において、挙動ベクトル1132はアノニマイザ1150に供給されてもよく、アノニマイザ1150は、挙動ベクトル1132をクラウドソース1160に供給する前に1つまたは複数の匿名アルゴリズムを適用して挙動ベクトル1132から

個人情報または機密情報を除去してもよい。その場合、クラウドソース1160は、正常挙動と匿名挙動との関係を判定するのに使用されるモデルを、他のIoT環境において行われる場合がある挙動分析に基づいてさらに経時的に構築するかまたは場合によっては開発するのを可能にしてもよく、経時的に開発され分散型ネットワーク1100における異常を検出するのに使用されるモデルを向上させるために、クラウドソース1150との対話によって学習された任意の情報が分析モジュール1140に供給されてもよい。

【0099】

さらに、様々な実施形態において、分析モジュール1140は、1つまたは複数のアクチュエータ1170を呼び出して、分析された挙動ベクトル1132において検出された1つまたは複数の挙動異常を是正してもよい。たとえば、アクチュエータは、1つまたは複数のサービスプロバイダ1172、オンラインサポートと通信するのに使用される電話1174、オンライントラブルシューティング、オンデバイス診断または家庭内診断、あるいは分析された挙動ベクトル1132から検出された1つまたは複数の挙動異常を是正する助けになる他の技法を実行することのできる他のアクチュエータ1170を含んでもよい。たとえば、一実施形態では、分析モジュール1140は、より多くの情報を収集することができるよう、要求/応答システムを呼び出してアクチュエータ1170との往復メッセージングを有効化してもよい(たとえば、分析モジュール1140は、ローカル分散型アーキテクチャ1100と外部アクチュエータ1170との間のルータとして働いてもよい)。さらに、分析モジュール1140は、分析された挙動ベクトル1132に基づいて、オブザーバデバイス1112、1114、アグリゲータデバイス1116、1118、およびネットワークトラフィックモニタ1120を構成するための観測フィードバックおよび調整特性1142を生成してもよい。たとえば、観測フィードバックおよび調整特性1142は、オブザーバデバイス1112、1114、アグリゲータデバイス1116、1118、およびネットワークトラフィックモニタ1120が挙動情報を観測すること、観測すべき(または観測しない)特定の特性または挙動を指定することなどを行うのに使用する頻度、間隔持続期間などを調整してもよい。その場合、オブザーバデバイス1112、1114、アグリゲータデバイス1116、1118、およびネットワークトラフィックモニタ1120は、周期的にならびに/あるいはフィードバック特性1142による特定のトリガリング基準にตอบสนองしてアクションログ1122を生成してもよく、アクションログ1122は同様に、常時接続監視デバイス1110において周期的に集約され分析されてもよい。

【0100】

図12は、様々な態様による、自動化されたデバイス健全性監視をサポートすることができる挙動分析を行う例示的な方法1200を示す。詳細には、ブロック1210において様々な監視パラメータを初期設定してもよく、この初期設定は、挙動を観測するための1つまたは複数の頻度の確立および/または調整、観測すべき特定の特性の定義などを含んでもよい。さらに、分散型アーキテクチャでは、監視パラメータを初期設定することは、分散型アーキテクチャ全体にわたって行われる場合がある挙動分析の助けとして特定の機能を実行するように構成された1つまたは複数のオブザーバノード、アグリゲータノード、およびアナライザノードを指定することを含んでもよい。様々な実施形態では、ブロック1220において、観測された挙動および/または環境挙動を表す1つまたは複数の特性を含む1つまたは複数のアクションログを、ローカル(オンデバイス)健全性監視を実行するIoTデバイスにおいて取得しても、あるいは分散型アーキテクチャにおける1つまたは複数のオブザーバノードおよび/またはアグリゲータノードから取得してもよい。たとえば、分散型アーキテクチャでは、オブザーバノードは次いで、ローカルに生成されたアクションログを最も近いアグリゲータノードに送信してもよく、あるいは代替として、アクションログを最も近いアナライザノードに送信してもよい。さらに、アグリゲータノードは、任意のオブザーバノードから受信されたアクションログを周期的に最も近いアナライザノードに中継してもよい。したがって、ブロック1230において、アクションログに含まれる特性をn次元空間にマップし、IoTネットワーク内の観測された挙動および/または環境変数から1つまたは複数の挙動ベクトルを抽出してもよい。次いでブロック1240において、挙動ベクトルを特定のデバイス型式、バージョンなどに固有のモデルと比較してもよく、これらの

モデルは、IoTネットワーク内のすべてのデバイスからの挙動ベクトルおよびIoTネットワークに固有のモデル、IoTネットワークに関連するユーザからの入力および対話などに基づいて、製造業者または他の適切なリポジトリから取得されてもよい。

【0101】

様々な実施形態では、ブロック1250において、挙動ベクトルと正常デバイスモデルおよび/または正常環境モデルとの比較結果を評価して、1つまたは複数の異常が検出されたかどうかを判定してもよい。挙動ベクトルが1つまたは複数の異常を表すと判定したことに応答して、ブロック1260において適切な是正措置がトリガされてもよい。たとえば、様々な実施形態において、ブロック1260においてトリガされる是正措置は、1つまたは複数のアクチュエータを呼び出して、分析された挙動ベクトルにおいて検出された任意の挙動異常を是正してもよく、アクチュエータは、1つまたは複数のサービスプロバイダ、オンラインサポートと通信するのに使用される電話、あるいはオンライントラブルシューティング、オンデバイス診断もしくは家庭内診断、または分析された挙動ベクトルから検出された1つもしくは複数の挙動異常の是正の助けとなる他の技法を実行することができる他のアクチュエータ(たとえば、より多くの情報を収集することができるように、要求/応答システムを呼び出してアクチュエータとの往復メッセージングを有効化してもよい)を含んでもよい。

10

【0102】

様々な実施形態では、ブロック1270において、機械学習を適用して、挙動分析を行うのに使用されるデバイスモデルおよび/または環境モデルを更新してもよい。たとえば、様々な実施形態では、ブロック1270は、特定のデバイス型式、バージョンなどに固有のモデルを更新すること、全体的なIoTネットワークに関連するモデルを更新すること、IoTネットワークに関連するユーザからの入力および対話に応じて適切なモデルを更新すること、挙動ベクトルをクラウドソースに供給して、正常挙動と匿名挙動との関係を判定するのに使用されるモデルを、他のIoT環境において行われる場合がある挙動分析に基づいてさらに経時的に構築するかまたは場合によっては開発するのを可能にすることなどを含んでもよい。したがって、ブロック1270において適用される機械学習によって、任意の1つの特性のみに基づいて挙動異常を検出するのではなく、挙動異常を検出するのに使用されるモデルが、正常挙動、全体的な環境状態などを示すように経時的に構築されたコンテキストにおいて関連する情報を含むようになる場合がある。

20

30

【0103】

さらに、ブロック1280において、以後の監視パラメータおよび観測パラメータを構成するための観測フィードバックおよび調整特性を生成してもよい。たとえば、この監視フィードバックおよび観測パラメータ調整は、挙動情報を観測し収集するのに使用される頻度、間隔持続時間などを調整すること、観測すべき(または観測しない)特定の特性または挙動を指定することなどを可能にする。その場合、監視フィードバックおよび観測パラメータ調整によって、周期的にならびに/あるいはフィードバック特性による特定のトリガリング基準に応答してアクションログが生成されてもよく、アクションログが、監視フィードバックおよび調整された観測パラメータに従って周期的に集約され分析されてもよい。

【0104】

40

様々な態様によれば、図13は、自動化されたデバイス健全性監視をサポートするために行うことのできる挙動分析を初期設定するための例示的な方法1300を示し、図13に示す方法1300は概して、(たとえば、図10および図11のように)分散型健全性監視アーキテクチャに適用されてもよい。しかし、当業者には、同様の初期設定方法を(たとえば、図9のように)スタンドアロン(オンデバイス)健全性監視コンテキストにおいて実行してもよいことが諒解されよう。ただし、そのような実装形態では、特定の特性が省略されなれば/あるいは適切に修正されてもよい。たとえば、スタンドアロン(オンデバイス)健全性監視コンテキストでは、必ずしも、接続されたIoTデバイスから属性および機能を取得しアグリゲータおよびアナライザの役割を指定する必要はなく、それによって、後述のそのような初期設定ステップは省略されてもよい。

50

【0105】

様々な実施形態では、ブロック1310において、自動化されたデバイス健全性監視をサポートするために行うことのできる挙動分析を初期設定することは、接続されたIoTデバイスから属性および機能(たとえば、ネットワーク化、電力、プロセッサ、機能などに関する属性および機能)を取得することを含んでもよい。様々な実施形態では、ブロック1320において、アグリゲータノードを指定してもよく、ハンドシェイクプロトコルを実行して指定された役割を示し確認応答してもよい。たとえば、アグリゲータの役割を果たす能力は、ブロック1310において取得された属性および機能に基づいて判定されてもよい十分なネットワーク機能(たとえば、サポートされるネットワークタイプ、帯域幅、レンジなど)、電力、および処理機能を有する指定されたデバイスによって決まる場合がある。様々な実施形態では、ブロック1330において、環境トポロジを構築してもよく、関連するトポロジ情報を接続されたIoTデバイスと共有してもよく、接続されたIoTデバイスに関連する挙動モデルは、ブロック1340においてそれらのモデルに関連する製造業者および/または他の適切なリポジトリから取得されてもよい。様々な実施形態では、ブロック1350において、アグリゲータノードにおいてデータ収集をスケジュールしてもよく、アグリゲータノードからデータをプルすることをスケジュールしてもよく、その時点で、システムは上述のように挙動分析を行う準備が完了してもよい。

【0106】

図14は、様々な態様による、ローカルIoT環境において行われる直接的および/または間接的な挙動分析を使用して異常挙動を検出し是正することができる例示的な分散型アーキテクチャ1400を示す。概して、図14に示す分散型アーキテクチャ1400は、それぞれ図10および図11に示す分散型IoTネットワーク1000、1100と同じでありならびに/あるいは実質的に同様である様々な構成要素および機能を含んでもよく、したがって、説明を簡潔にかつ容易にするために、分散型アーキテクチャ1400における特定の構成要素に関する様々な詳細は、関連する詳細が上記においてすでに提示されている限りここでは省略されてもよい。たとえば、図14では、分散型アーキテクチャ1400は、観測された電力挙動、センサー情報などを表すための特性を含む1つまたは複数のアクションログを顧客サービスプラットフォーム1410に供給する場合がある第1のオブザーバIoTデバイス1412を、観測された電力挙動、センサー情報などに加えて1つまたは複数の試験信号を表すための特性を含む1つまたは複数のアクションログを顧客サービスプラットフォーム1410に供給する場合がある第2のオブザーバIoTデバイス1414の他に含んでもよい。さらに、図14では、分散型アーキテクチャ1400は、概して、他のローカルコンテキスト情報および/または環境情報(たとえば、ロケーション情報、天候、エネルギー単位当たりコストなど)を顧客サービスプラットフォーム1410に供給する場合がある情報IoTデバイス1416、1418、1420を備える場合がある他のローカルIoTデバイスを含んでもよい。

【0107】

したがって、図14に示す分散型アーキテクチャ1400では、顧客サービスプラットフォーム1410は、情報IoTデバイス1416、1418、1420からの関連するローカルコンテキストおよび/または環境情報に加えてオブザーバIoTデバイス1412、1414からの1つまたは複数のアクションログを受信してもよく、アクションログならびに関連するローカルコンテキストおよび/または環境情報は、アクションログならびに関連するローカルコンテキストおよび/または環境情報に含まれる特性をn次元空間にマップして1つまたは複数の挙動ベクトルを抽出するように構成された挙動ベクトル抽出モジュール1430(またはアグリゲータノード)において組み合わされてもよい。挙動ベクトルは次いで、1つまたは複数の異常は正サポートパートナー1470および分析モジュール1440に供給されてもよく、分析モジュール1440は、監視されたデバイスにおける潜在的な悪意のある攻撃、誤動作、またはパニアウト、あるいはその他の異常を示す可能性がある1つまたは複数の挙動異常を検出するために挙動ベクトルを集約してもよい。たとえば、様々な実施形態において、分析モジュール1440は、上述のように、IoTネットワーク1400内のすべてのデバイスからの挙動ベクトルおよびIoTネットワーク1400に固有のモデルならびに/あるいはIoTネットワーク1400に

関連するユーザからの入力および対話などに基づいて、製造業者1472または他の適切なリポジトリから取得される場合がある、観測された挙動に対応するデバイスに関連する型式、バージョンなどに固有のモデルとの比較に従って集約された挙動ベクトルを分析してもよい。

【0108】

さらに、図14に示す顧客サービス使用事例では、挙動ベクトルを1つまたは複数のしきい値または他の適切なパラメータと比較して異常を検出してもよい。その場合、異常を検出するのに使用されるしきい値またはその他のパラメータは、異常検出しきい値またはその他の異常検出パラメータが正常条件または異常条件をそれぞれに異なるシナリオに反映することができるのでコンテキストに依存する場合がある。したがって、ロケーション情報、天候情報、および情報IoTデバイス1416、1418、1420からのその他の関連するローカルコンテキストおよび/または環境情報を有すると、異常を検出するのに使用されるしきい値またはその他のパラメータを判定するうえで有用である。さらに、様々な実施形態では、異常検出しきい値または異常検出パラメータを経時的に学習し、特定のユーザ要件または使用パターンに対してデバイス固有にカスタマイズすることができ、それによって、モデルをまったく使用せずにすべての異常が検出されるようになり、それによって、フォールスポジティブ率および/またはフォールスネガティブ率が潜在的に高くなる場合がある。たとえば、食料品およびその他の品目が自動的に家庭環境に配達される使用事例を考える。家庭環境における冷蔵庫は、内部に貯蔵されている品目をスキャンし、食料品がなくなったときに自動的に注文する機能を有する場合がある。一般に、ユーザは、特定の(比較的一定の)期間の間持つと考えられる標準的な食料品を購入し(たとえば、2ガロンのミルク、2ダースの卵など)、光熱費における一成分として、スラブ単位で表されるタリフがあり、非線形的に増大する。したがって、現在の単位当たりエネルギーコスト、電子メールのスキャンによって何人の客が予測されるかなどを考慮して、購入する必要がある食料品に関してユーザに推奨することができるよう情報の取得および/または推定を行うことができる。

【0109】

さらに、様々な実施形態において、分析モジュール1440は、異常是正サポートパートナー1470に1つまたは複数の検出された異常を報告して、環境1400において検出された1つまたは複数の挙動異常の是正の助けを要求してもよい。たとえば、異常是正サポートパートナー1470は、デバイス製造業者1472、顧客サービス1474、セキュリティインシデント応答システム1476、または環境1400内で検出された挙動異常の是正の助けとすることができる他の適切なエンティティを備えてもよい。たとえば、分析モジュール1440は、より多くの情報を収集できるように、要求/応答システムを呼び出して、適切な異常是正サポートパートナー1470との往復メッセージングを有効化してもよく、それによって、分析モジュール1440は、ローカル環境1400と外部異常是正サポートパートナー1470との間のルータとして働いてもよい。

【0110】

図15は、様々な態様による、ローカルIoT環境における直接的および/または間接的な挙動分析を行って顧客サービスおよびセキュリティインシデント応答を自動化して異常挙動を是正するための例示的な方法を示す図である。より詳細には、ブロック1510において、IoT環境内の1つまたは複数のデバイスにおいて観測される挙動を表す1つまたは複数のアクションログをローカルコンテキスト情報、環境情報、および/またはローカルIoT環境に関連する全体的な状態のモデル化に関連する場合がある他の適切な情報とともに集約してもよく、ブロック1510において集約されたローカルコンテキスト情報、環境情報などは、1つまたは複数の情報IoTデバイス(たとえば、天候センサー、積算電力計など)から受信されてもよい。さらに、当業者には、デバイス挙動観測およびローカルコンテキスト情報、環境情報などが、IoT環境全体にわたって挙動分析を行うアナライザノードとして動作するように指定された特定のIoTデバイス上に存在する場合がある(たとえば、図14に示すような)顧客サービスプラットフォームにおいて集約されてもよく、あるいはオンデバイス

顧客サービスプラットフォームを使用して、ローカルに観測された挙動を情報IoTデバイスから集約されたローカルコンテキスト情報、環境情報などと組み合わせて使用してローカルレベルにおいて顧客サービス挙動分析を行う場合がある特定のIoTデバイスにおいて集約されてもよいことが諒解されよう。したがって、図15に示す、本明細書において説明する方法1500は概して、分散型アーキテクチャにおいて(たとえば、ローカルIoT環境全体にわたって)実行され、スタンドアロンアーキテクチャまたは集中型アーキテクチャにおいて(たとえば、オンデバイス顧客サービス/健全性監視プラットフォームを使用して挙動分析を行うのに十分な処理機能を有する特定のIoTデバイスにおいて)実行され、ならびに/あるいはそれらの様々な組合せにおいて実行されてもよい。

【0111】

様々な実施形態では、ブロック1520において、1つまたは複数の異常検出パラメータを判定してもよく、1つまたは複数の異常検出パラメータは、(たとえば、図15および図16に関して以下にさらに詳しく説明するように)コンテキストに応じて使用事例ごとに異なる場合がある。たとえば、様々な実施形態では、ブロック1520において判定された異常検出パラメータは、正常条件、異常条件、または他の適切な条件をそれぞれに異なるシナリオおよび/またはコンテキストに反映してもよい。したがって、様々な実施形態において、ブロック1510において集約されたローカルコンテキスト情報および/または環境情報を他の関連する情報と組み合わせて使用して、異常検出パラメータを判定してもよい(たとえば、他の関連する情報には、異常検出パラメータがそのIoTデバイスで観測された現在の挙動と比較される使用事例において特定のIoTデバイスで観測された前の挙動を含めてもよい)。さらに、様々な実施形態において、ブロック1520において判定された異常検出パラメータを経時的に学習し、特定のユーザ要件または使用パターンに対してデバイス固有にカスタマイズすることができ、それによって、モデルをまったく使用せずにすべての異常が検出されるので、フォールスポジティブ率および/またはフォールスネガティブ率が低下する場合がある。

【0112】

様々な実施形態では、ブロック1530において、集約されたデバイス挙動観測値を異常パラメータと比較して、集約されたデバイス挙動観測値が1つまたは複数の潜在的な異常を示すかどうかを判定してもよい。たとえば、様々な実施形態において、集約されたデバイス挙動観測値および他の任意の関連するコンテキスト情報をn次元空間にマップして1つまたは複数の挙動ベクトルを抽出してもよく、これらの挙動ベクトルを異常検出パラメータと比較して、挙動観測値が、監視されるデバイスにおける悪意のある攻撃、誤動作、バーンアウト、または別の異常を潜在的に反映するかどうかを判定してもよい。したがって、ブロック1540において、挙動観測値が1つまたは複数の潜在的な異常を示していると判定したことに応答して、ブロック1550において異常是正要求および応答システムを呼び出してもよい。たとえば、異常是正要求および応答システムを呼び出して、ブロック1540において検出された挙動異常の是正に関して助けとなることのできる1つまたは複数のサポートパートナーにブロック1540において検出された異常を報告してもよい。したがって、より多くの情報を収集することができ、かつ適切なトラブルシューティング手順によって異常挙動を診断し解消することができるように、ブロック1550において要求および応答システムを呼び出して、適切なサポートパートナーとの往復メッセージングを有効化してもよい。

【0113】

様々な実施形態では、ブロック1560において、機械学習を適用して、自動化された顧客サービスおよびセキュリティインシデント応答方法を実行するのに使用される1つまたは複数のデバイスモデル、環境モデル、異常パラメータなどを更新してもよい。たとえば、様々な実施形態において、ブロック1560は、特定のデバイス型式、バージョンなどに固有のモデルを更新すること、全体的なIoT環境に関連するモデルを更新すること、IoTネットワークに関連するユーザからの入力および対話に従って適切なモデルを更新すること、挙動観測値をクラウドソースに供給して、他のIoT環境において行われる挙動分析に基づい

10

20

30

40

50

てモデルをさらに構築するかまたは場合によっては開発すること、異常パラメータを更新して経時的に観測された挙動パターンを反映することなどを含んでもよい。したがって、ブロック1560において適用される機械学習によって、任意の1つの特性(または挙動)のみに基づいて挙動異常を検出するのではなく、挙動異常を検出するのに使用されるモデルが、正常挙動、全体的な環境状態などを示すように経時的に構築されたコンテキストにおいて関連する情報を含むようになる場合がある。

【0114】

図16は、様々な態様による、冷蔵庫IoTデバイスに関連する健全性を監視するために直接および/または間接的な挙動分析が行われる場合がある例示的な顧客サービス使用事例に対応する方法1600を示す図である。より詳細には、様々な実施形態において、冷蔵庫IoTデバイスは、ローカル挙動を観測し、冷蔵庫IoTデバイスにおいて観測された挙動を表す1つまたは複数のアクションログを生成してもよく、冷蔵庫IoTデバイスに関連する観測された挙動を表すアクションログは、ブロック1610において顧客サービスプラットフォームにおいて受信されてもよい。たとえば、様々な実施形態において、顧客サービスプラットフォームは、十分な機能(たとえば、記憶リソース、プロセッサリソース、ネットワークリソースなど)を有する冷蔵庫IoTデバイス上に存在することができ、あるいは代替として、挙動分析を行うのに十分な処理機能を有するスマートフォン、常時接続ルータ、または別の適切なデバイスなどのリモートデバイス上に存在することができる。いずれの場合も、次いで、ブロック1620において、冷蔵庫IoTデバイスに関連する正常挙動を表し、異常挙動を検出するのに使用することができる1つまたは複数の正常しきい値および/または異常しきい値を定義する1つまたは複数のモデルと、冷蔵庫IoTデバイスにおいて観測された挙動を比較してもよい。たとえば、様々な実施形態において、1つまたは複数のモデルは、冷蔵庫IoTデバイスに関連する正常(または異常)電力消費量、周囲温度、負荷、および/または他の適切な状態を示す情報を含んでもよい。したがって、異常を検出するために監視されるしきい値は、コンテキストに応じて正常になる場合も異常になる場合もあるので、ブロック1620において実行される比較では、ロケーション固有の情報(たとえば、地元の天気)をさらに使用して、しきい値を冷蔵庫IoTデバイスにおいて観測された挙動と、そのようなコンテキスト情報が利用可能である限り比較して判定してもよい。

【0115】

したがって、図16に示す冷蔵庫IoTデバイス使用事例では、ブロック1620は、冷蔵庫IoTデバイスに関連する正常(または異常)電力消費量値、周囲温度値、および負荷値を示す1つまたは複数のモデルと冷蔵庫IoTデバイスにおいて観測された挙動を比較することを含んでもよい。したがって、ブロック1630において、冷蔵庫IoTデバイスにおいて観測された現在の挙動を表すアクションログが、しきい値(たとえば、超えると冷蔵庫の故障、回路の過負荷などが生じる場合がある電力消費量レベル)を超えない値を有する電力消費量挙動特性を含むと判定したことに応答して、ブロック1660において冷蔵庫の健全性を正常であると見なししてもよい。代替として、ブロック1630において、電力消費量挙動特性に関連する値がしきい値を超えていると判定したことに応答して、1つまたは複数のさらなる挙動特性を検査して、顧客サービスを必要とする場合がある潜在的な異常を示すかそれともこのような状況下での正常状態を示すかを判定してもよい。たとえば、ブロック1640において、冷蔵庫IoTデバイスにおいて観測された周囲温度を正常周囲温度と比較してもよく、その場合、冷蔵庫の健全性は、ブロック1660において、観測された周囲温度が正常周囲温度を超えていることに応答して正常であると見なされてもよい(この理由は、たとえば、冷蔵庫が、周囲環境が通常よりも暑いときに同じ内部温度レベルを維持するためにより多くの電力を引き込むと考えることができるからである)。同様に、観測された周囲温度が正常周囲温度を超えていない場合、ブロック1650は、冷蔵庫IoTデバイスにおける観測された負荷(たとえば、重量、容積などによって表された冷蔵庫に貯蔵された食品の量)を正常(または一般的な)負荷と比較することを含んでもよく、その場合、冷蔵庫の健全性は、ブロック1660において、観測された負荷が正常負荷/一般的な負荷を超えていることに応答して正常と見なされてもよい(この理由は、たとえば、冷蔵庫は、周囲温度が正常

10

20

30

40

50

値以下である場合でも大量の食品を冷却するにはより多くの電力を引き込むと考えることができるからである)。

【0116】

しかし、ブロック1630、1640、1650のそれぞれにおいて、観測された電力消費量がしきい値を超えており、観測された周囲温度が正常値以下であり、観測された負荷が正常値以下であると判定されたことに応答して、ブロック1670において異常条件を検出して報告してもよく、報告することは、観測された挙動パラメータ(たとえば、観測された電力消費量、観測された周囲温度、および観測された負荷)を顧客サービスに送信することを含んでもよく、場合によってはさらに、(たとえば、潜在的なフォールスポジティブを検出するために適切なしきい値が使用されたことを確認するために)しきい値を観測された挙動パラメータと比較してもよい。さらに、ブロック1650において、より多くの情報を収集することができ、かつ適切なトラブルシューティング手順によって異常挙動を診断し解消することができるように、異常是正要求および応答システムを呼び出して適切なサポートパートナーとの往復メッセージングを有効化してもよい。

10

20

30

40

50

【0117】

図17は、様々な態様による、煙感知器IoTデバイスに関連する健全性を監視するために直接および/または間接的な挙動分析が行われる場合がある例示的な顧客サービス使用事例に対応する方法1700を示す。より詳細には、様々な実施形態において、煙感知器IoTデバイスは、ローカル挙動を観測し、ローカルに観測された挙動を表す1つまたは複数のアクションログを生成してもよく、ブロック1710は、観測された挙動を表すアクションログを顧客サービスプラットフォームにおいて受信することを含んでもよい。たとえば、様々な実施形態において、顧客サービスプラットフォームは、煙感知器IoTデバイスが十分な処理機能を有する場合に煙感知器IoTデバイス上に存在することができ、あるいは挙動分析を行うのに十分な処理機能を有するスマートフォン、常時接続ルータ、または別の適切なデバイスなどのリモートデバイス上に存在することができる。様々な実施形態では、ブロック1720において、観測された挙動を煙感知器IoTデバイスに関連する正常挙動を表す1つまたは複数のモデルと比較してもよく、これらのモデルは、正常条件および/または異常条件を示し、異常挙動を検出するのに使用することができる1つまたは複数のパラメータをさらに定義してもよい。

【0118】

したがって、図17に示す煙感知器使用事例において、ブロック1730は、煙感知器IoTデバイスにおいて収集された観測値が、ハートビートが存在することを示すかどうかを判定することを含んでもよく、この場合、ハートビートは、機能している煙感知器の最も基本的なパラメータを表すので、ハートビートが存在しないことは、潜在的に異常な挙動を示す場合がある。したがって、ブロック1730においてハートビートが存在しないと判定されたことに応答して、ブロック1750においてさらなる検査を行い、バッテリー電力が利用可能であるかどうかを判定してもよく、その場合、ユーザは、ブロック1780においてバッテリーを交換するよう警告を受ける場合がある(この理由は、たとえば、ハートビートが存在しないのは、誤動作またはその他の異常条件に起因するのではなく単にバッテリーが枯渇したことが原因であるからである)。しかし、ブロック1750においてバッテリー電力が利用可能である(たとえば、ハートビートが存在しないのはバッテリーの枯渇に起因するものではない)と判定されたことに応答するか、あるいは代替として、ブロック1730においてハートビートが検出されたと判定されたことに応答して、ブロック1740において、試験機能と呼び出してさらなる検査を実行し、煙感知器IoTデバイスが試験機能に合格したことを現在の観測された挙動が示すかどうかを判定してもよい。判定が肯定である場合、ブロック1760において煙感知器の健全性は正常であると見なされてもよい。代替として、ブロック1740において、煙感知器IoTデバイスが試験機能に合格しなかったと判定されたことに応答して、ブロック1770において異常状態を検出し報告してもよく、報告することは、観測された挙動パラメータ(たとえば、ハートビート検査による結果、試験機能結果、観測された一酸化炭素レベルなど)を顧客サービスに送信することを含んでもよい。さ

らに、ブロック1770において、より多くの情報を収集することができ、かつ適切なトラブルシューティング手順によって異常挙動を診断し解消することができるように、異常是正要求および応答システムを呼び出して適切なサポートパートナーとの往復メッセージングを有効化してもよい。

【0119】

図18は、様々な態様による、本明細書で開示する様々な態様および実施形態による、発見可能なD2Dサービスを使用した近接度ベースの分散バスを介した通信によってIoTデバイス挙動の観測、集約、および/または分析を行うように構成される場合がある例示的な通信デバイス1800を示す図である。詳細には、図18に示すように、通信デバイス1800は、たとえば、受信アンテナ(図示せず)から信号を受信し、受信信号に対して典型的なアクション(たとえばフィルタ処理、増幅、ダウンコンバートなど)を実行し、条件付きの信号をデジタル化してサンプルを取得するレシーバ1802を備えてもよい。レシーバ1802は、受信されたシンボルを復調し、復調されたシンボルをチャネル推定のためにプロセッサ1806に提供することができる復調器1804を備えてもよい。プロセッサ1806については、レシーバ1802によって受信された情報の分析および/またはトランスミッタ1820によって送信される情報の生成専用を使用すること、通信デバイス1800の1つまたは複数の構成要素を制御すること、ならびに/あるいはそれらの任意の適切な組合せが可能であってもよい。

【0120】

様々な実施形態では、通信デバイス1800は、プロセッサ1806に動作可能に結合されたメモリ1808をさらに備えることができ、メモリ1808は、受信されたデータ、送信すべきデータ、利用可能なチャネルに関連する情報、分析された信号および/または干渉強度に関連するデータ、割り当てられたチャネル、電力、レートなどに関連する情報、およびチャネルを推定し、チャネルを介して通信するための任意の他の適切な情報を記憶することができる。様々な実施形態では、メモリ1808は、1つまたは複数のローカルエンドポイントアプリケーション1810を含むことができ、ローカルエンドポイントアプリケーション1810は、分散バスモジュール1830を通じた通信デバイス1800および/または他の通信デバイス(図示せず)上のエンドポイントアプリケーション、サービスなどとの通信を求めてもよい。メモリ1808は、(たとえば、性能ベース、容量ベースなど)チャネルの推定および/またはチャネルの使用に関連付けられたプロトコルおよび/またはアルゴリズムをさらに記憶することができる。

【0121】

当業者には、本明細書で説明するメモリ1808が、揮発性メモリもしくは不揮発性メモリであることが可能であり、または揮発性と不揮発性の両方のメモリを含むことが可能であることが諒解されよう。限定ではなく例として、不揮発性メモリは、読取り専用メモリ(ROM)、プログラマブルROM(PROM)、電気的プログラマブルROM(EPROM)、電気的消去可能PROM(EEPROM)、またはフラッシュメモリを含むことができる。揮発性メモリは、外部キャッシュメモリとして働くランダムアクセスメモリ(RAM)を含むことができる。限定ではなく例として、RAMは、同期RAM(SRAM)、ダイナミックRAM(DRAM)、同期DRAM(SDRAM)、ダブルデータレートSDRAM(DDR SDRAM)、拡張SDRAM(ESDRAM)、シンクリンクDRAM(SLDRAM)、およびダイレクトRambus RAM(DRRAM(登録商標))などの多くの形で使用可能である。対象のシステムおよび方法におけるメモリ1808は、それだけに限定されないが、これらの種類のメモリおよび任意の他の適切な種類のメモリを備えてもよい。

【0122】

様々な実施形態では、通信デバイス1800に関連する分散バスモジュール1830は、他のデバイスとの接続を確立するのをさらに容易にすることができる。分散バスモジュール1830は、分散バスモジュール1830が複数のデバイス間の通信を管理するのを助けるためのバスノードモジュール1832をさらに備えてもよい。様々な実施形態では、バスノードモジュール1832は、バスノードモジュール1832が他のデバイスに関連するエンドポイントアプリケーションと通信するのを助けるためのオブジェクト命名モジュール1834をさらに含んでもよい。さらに、分散バスモジュール1830は、ローカルエンドポイントアプリケーション18

10が確立された分散バスを通じて他のローカルエンドポイントおよび/または他のデバイス上のアクセス可能なエンドポイントアプリケーションと通信するのを助けるためのエンドポイントモジュール1836を含んでもよい。別の態様では、分散バスモジュール1830は、複数の利用可能なトランスポート(たとえば、Bluetooth(登録商標)、Unixドメインソケット、TCP/IP、Wi-Fiなど)を介したデバイス間通信および/またはデバイス内通信を容易にしてもよい。したがって、様々な実施形態では、分散バスモジュール1830およびエンドポイントアプリケーション1810を使用して、通信デバイス1800が直接デバイス間(D2D)通信を使用して通信デバイス1800に近接する他の通信デバイスと通信することができる近接度ベースの分散バスを確立しならびに/あるいはそのような近接度ベースの分散バスに参加してもよい。

10

【0123】

さらに、様々な実施形態では、通信デバイス1800は、ユーザインターフェース1840を含んでもよく、ユーザインターフェース1840は、通信デバイス1800への入力を生成するための1つまたは複数の入力機構1842と、通信デバイス1800のユーザによって消費される情報を生成するための1つまたは複数の出力機構1844とを含んでもよい。たとえば、入力機構1842は、キーまたはキーボード、マウス、タッチスクリーンディスプレイ、マイクロフォンなどの機構を含んでもよい。さらに、たとえば、出力機構1844は、ディスプレイ、オーディオスピーカ、触覚フィードバック機構、パーソナルエリアネットワーク(PAN)送受信機などを含んでもよい。図示した態様では、出力機構1844は、メディアコンテンツをオーディオ形式にレンダリングするように動作可能なオーディオスピーカ、メディアコンテンツの画像フォーマットもしくはビデオフォーマットへのレンダリングおよび/または時限メタデータのテキスト形式または視覚形式へのレンダリングを行うように動作可能なディスプレイ、あるいは他の適切な出力機構を含んでもよい。しかし、様々な実施形態では、ヘッドレス通信デバイス1800は、一般にモニタ、キーボード、および/またはマウスなしで動作するように構成されたコンピュータシステムまたはデバイスを指すので、いくつかの入力機構1842および/または出力機構1844を含まなくてもよい。

20

【0124】

さらに、様々な実施形態では、通信デバイス1800は、通信デバイス1800に関連するローカル環境に関係する様々な測定値を取得することができる1つまたは複数のセンサー1850を含んでもよい。たとえば、様々な実施形態では、センサー1850は、加速度計、ジャイロスコプ、または通信デバイス1800に加えられる動きに関係する測定値を取得することができる他の適切なセンサーを含んでもよい。別の例では、センサー1850は、内部温度および/または周囲温度、電力消費量、ローカル無線信号、照明、ならびに/あるいは他のローカル環境変数および/または周囲環境変数に関係する測定値を取得することのできる適切なハードウェア、回路、または他の適切なデバイスを含んでもよい。

30

【0125】

したがって、ローカルIoT環境におけるデバイス健全性監視を自動化するのに使用することができる直接的および/または間接的な挙動分析に関する上述の様々な態様および実施形態では、図18に示す通信デバイス1800は、図9に示すIoTデバイス900に対応してもよく、その場合、ローカルエンドポイントアプリケーション1810は、オンデバイス健全性監視プラットフォーム910と、それに関連する様々なモジュールおよび/またはその他の構成要素とを備えてもよい。追加(または代替)として、通信デバイス1800は、オブザーバモード、アグリゲータモード、またはアナライザモードにおいて動作するように構成されるかまたは場合によっては指定された、図10に示すデバイスのうちの任意の1つまたは複数に相当してもよい。たとえば、通信デバイス1800がオブザーバモードにおいて動作するように構成されたデバイスに相当する実装形態では、通信デバイス1800に関連する様々な構成要素を使用して、通信デバイス1800に関連する挙動を観測するかまたは場合によっては監視し、アグリゲータモードおよび/またはアナライザモードにおいて動作するように構成された別のデバイスに(たとえば、分散バスモジュール1830を介して)観測された挙動を伝送してもよい。同様に、通信デバイス1800がアグリゲータモードにおいて動作するように

40

50

構成されたデバイスに相当する実装形態では、通信デバイス1800は、オブザーバモードにおいて動作するように構成された1つまたは複数のデバイスから挙動観測値を受信し、分散バスモジュール1830を使用して、アナライザモードにおいて動作するように構成された別のデバイスに挙動観測値を中継してもよい。さらに、通信デバイス1800は、アナライザモードにおいて動作するのに十分な機能を有し、通信デバイス1800は、オブザーバモードおよび/またはアグリゲータモードにおいて動作するように構成された1つまたは複数のデバイスから、分散バスモジュール1830を介して、集約された挙動観測値を受信してもよく、それによって、通信デバイス1800は、図11に示す常時接続監視デバイス1110に相当してもよく、ローカルエンドポイントアプリケーション1810は、環境内の他のデバイスにおいてならびに/あるいは環境自体内において挙動ベクトルを導出し異常挙動を検出するのに使用される挙動ベクトル抽出モジュールと分析モジュールとを備えてもよい。

10

【0126】

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。たとえば上記説明全体を通して参照することができるデータ、命令、指令、情報、信号、ビット、記号およびチップは、電圧、電流、電磁波、磁界または粒子、光学場または粒子、あるいはそれらの任意の組合せによって表すことができる。

【0127】

さらに、本明細書で開示する態様に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は理解されよう。ハードウェアおよびソフトウェア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、およびステップは、一般的にそれらの機能性に関してこれまで説明されてきた。そのような機能性がハードウェアとして実現されるか、またはソフトウェアとして実現されるかは、具体的な適用例および全体的なシステムに課される設計制約によって決まる。当業者は、記載された機能を特定の適用例ごとに様々な方法で実装することができるが、そのような実装の決定は、本明細書に記載された態様および/または実施形態の範囲から逸脱するものと解釈されるべきではない。

20

【0128】

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。汎用プロセッサを、マイクロプロセッサとすることができるが、代替案では、プロセッサを、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。

30

40

【0129】

本明細書において開示する態様に関連して説明した方法、シーケンス、および/またはアルゴリズムは、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、またはその2つの組合せで直接具現され得る。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内に存在し得る。例示的な記憶媒体は、プロセッサが記憶媒体から情報を読み取り、そこに情報を書込みできるようにプロセッサに結合される。代替案では、記憶媒体は、プロセッサに一体とされ得る。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

50

て存在し得る。

【0130】

1つまたは複数の例示的な態様では、述べられる機能は、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で、実施され得る。ソフトウェアに実装される場合、機能は、1つまたは複数の命令またはコードとして、コンピュータ可読媒体上に記憶されるか、または、コンピュータ可読媒体を介して送信される場合がある。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可能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できるすべての使用可能な媒体とすることができる。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もしくは他の光ディスク(disc)ストレージ、磁気ディスク(disk)ストレージもしくは他の磁気ストレージデバイス、あるいは命令もしくはデータ構造の形で所望のプログラムコードを担持しまたは記憶するのに使用でき、コンピュータによってアクセスできる任意の他の媒体を含むことができる。また、任意の接続は、適切にコンピュータ可読媒体と呼ばれる。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、レーザディスク(disc)、光ディスク(disc)、DVD、フロッピーディスク(disk)およびBlu-ray(登録商標)ディスク(disc)を含み、ディスク(disk)は、通常、データを磁氣的に再生し、ディスク(disc)は、データをレーザで光学的に再生する。前述の組合せも、コンピュータ可読媒体の範囲内に含まれるべきである。

10

20

【0131】

上記の開示は、例示的な態様および実施形態を示しているが、添付の特許請求の範囲によって定義されるような本開示の範囲から逸脱することなく、本明細書において様々な変更および修正を施すことが可能であることが、当業者には諒解されよう。本明細書で説明した態様および実施形態による方法クレームの機能、ステップおよび/または動作は、特定の順序で実施される必要はない。さらに、要素は、単数形で上に記載または特許請求されている場合があるが、単数形に限定することが明示的に述べられていない限り、複数形が考えられる。

30

【符号の説明】

【0132】

- 100A、100B、100C ワイヤレス通信システム
- 105 受動IoTデバイス
- 108 エアインターフェース
- 109 直接有線接続
- 110 テレビジョン、IoTデバイス
- 112 屋外空調機、IoTデバイス
- 114 温度自動調整器、IoTデバイス
- 116 冷蔵庫、IoTデバイス
- 116A、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
- 122A、122B IoTデバイス
- 124A、124B IoTデバイス
- 125 アクセスポイント
- 130 IoTマネージャ、スーパーバイザデバイス
- 140、140A、140B IoT SuperAgent
- 145 ゲートウェイ機能

40

50

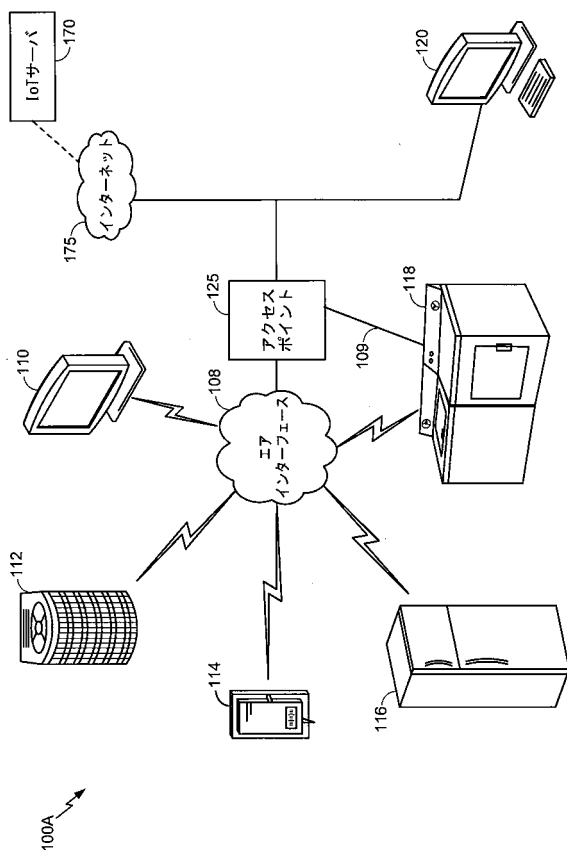
152	アプリケーションレイヤ	
154	CMPレイヤ	
156	トランスポートレイヤ	
158	物理レイヤ	
160	IoTグループ、IoTデバイスグループ	
160A、160B	IoTデバイス	
170	IoTサーバ	
175	インターネット	
180	リソース	
200A	IoTデバイス	10
202	プラットフォーム	
206	トランシーバ	
208	プロセッサ	
210	カメラ	
212	メモリ	
214	入出力(I/O)インターフェース	
222、224A、224B	ボタン	
226	ディスプレイ	
300	通信デバイス	
305	論理	20
310	論理	
315	論理	
320	論理	
325	論理	
400	サーバ	
401	プロセッサ	
402	揮発性メモリ	
403	ディスクドライブ	
404	ネットワークアクセスポート	
406	ディスクドライブ	30
407	ネットワーク	
500	ワイヤレス通信ネットワーク、WAN、ワイヤレスネットワーク	
510、510a、510b、510c	基地局	
520	デバイス	
530	ネットワークコントローラ	
540	DHCPサーバ	
600	例示的な環境	
610	第1のデバイス	
612	分散バスノード	
614	ローカルエンドポイント	40
620	第2のデバイス	
622	分散バスノード	
624	ローカルエンドポイント	
630	第3のデバイス	
632	分散バスノード	
634	ローカルエンドポイント	
640	分散バス、仮想分散バス	
700	例示的なメッセージシーケンス	
710	第1のデバイス、デバイスA	
712	バスノード	50

714	ローカルエンドポイント	
720	第2のデバイス、デバイスB	
722	バスノード	
724	ローカルエンドポイント	
810	ホストデバイス	
820	埋込みデバイス	
830	第2のホストデバイス	
900	IoTデバイス	
910	オンデバイス健全性監視プラットフォーム	
920	観測モジュール	10
922	アクションログ	
930	拳動ベクトル抽出モジュール	
932	拳動ベクトル	
940	分析モジュール	
944	拳動異常	
1000	ローカルIoTネットワーク	
1012	屋外スピーカ	
1020	サーモスタット	
1024	時計	
1026	コーヒーメーカー	20
1028	リビングルームフロアスピーカ	
1030	本棚オーディオシステム	
1036	ドアノブ	
1050	冷蔵庫	
1052	テレビジョン	
1070	スマートフォン	
1072	ホームゲートウェイ	
1100	分散型アーキテクチャ	
1110	常時接続監視デバイス	
1112	煙感知器	30
1114	サーモスタット	
1116	冷蔵庫	
1118	ゲームコンソール	
1120	ネットワークトラフィックモニタ	
1122	アクションログ	
1130	拳動ベクトル抽出モジュール	
1132	拳動ベクトル	
1140	分析モジュール	
1142	観測フィードバックおよび調整特性	
1150	アノニマイザ	40
1160	クラウドソース	
1170	アクチュエータ	
1172	サービスプロバイダ	
1174	電話	
1400	環境	
1410	顧客サービスプラットフォーム	
1412	第1のオブザーバIoTデバイス	
1414	第2のオブザーバIoTデバイス	
1416	情報IoTデバイス	
1430	拳動ベクトル抽出モジュール	50

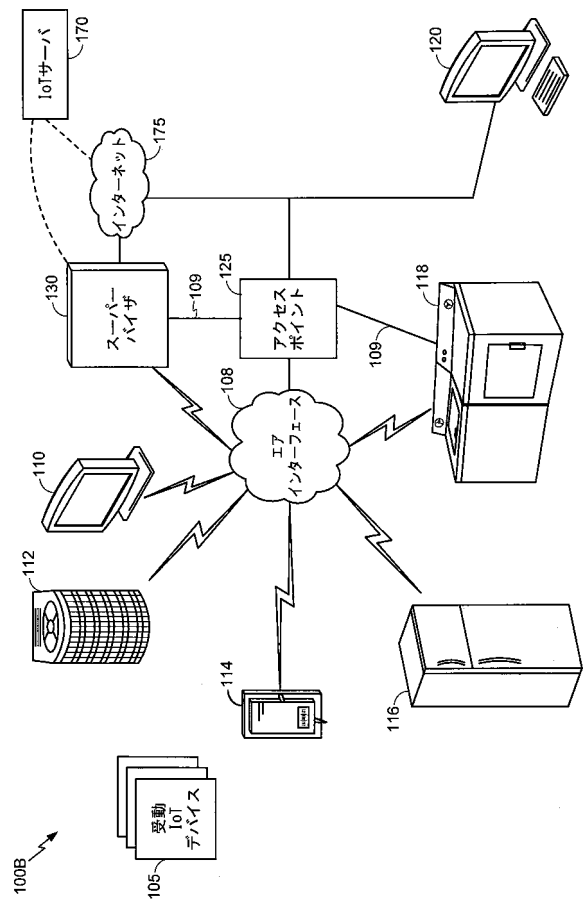
- 1440 分析モジュール
- 1470 異常是正サポートパートナー
- 1472 デバイス製造業者
- 1474 顧客サービス
- 1476 セキュリティインシデント応答システム
- 1800 通信デバイス
- 1802 レシーバ
- 1804 変調器
- 1806 プロセッサ
- 1808 メモリ
- 1810 ローカルエンドポイントアプリケーション
- 1820 トランスミッタ
- 1830 分散バスモジュール
- 1832 バスノードモジュール
- 1834 オブジェクト命名モジュール
- 1836 ローカルエンドポイントモジュール
- 1840 ユーザインターフェース
- 1842 入力機構
- 1844 出力機構

10

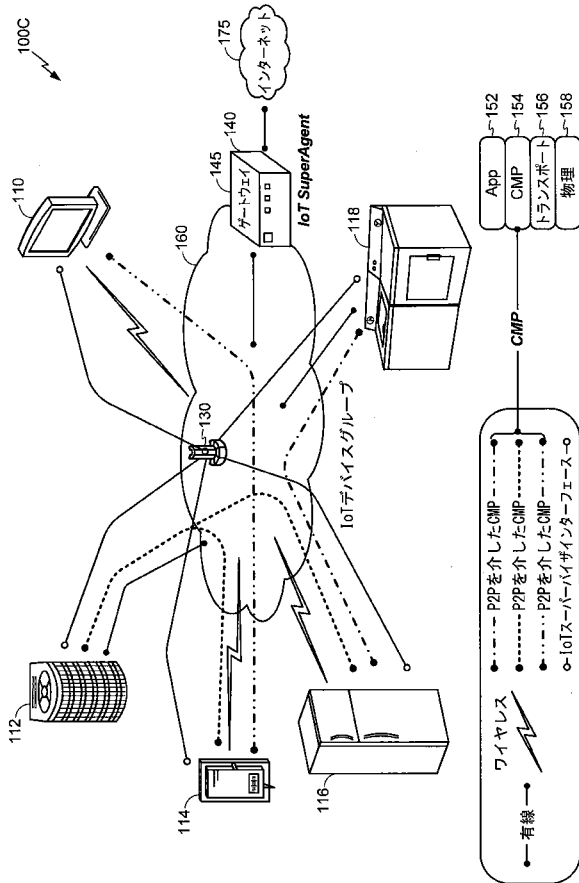
【図 1 A】



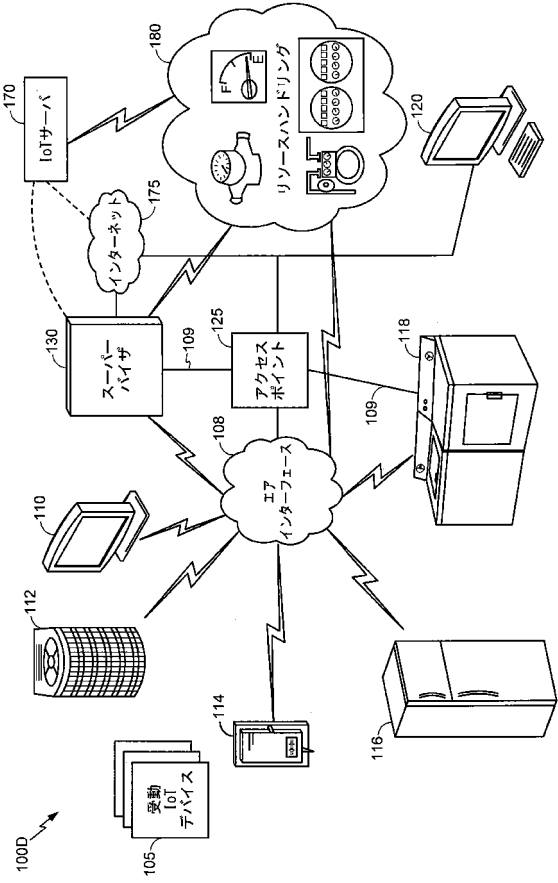
【図 1 B】



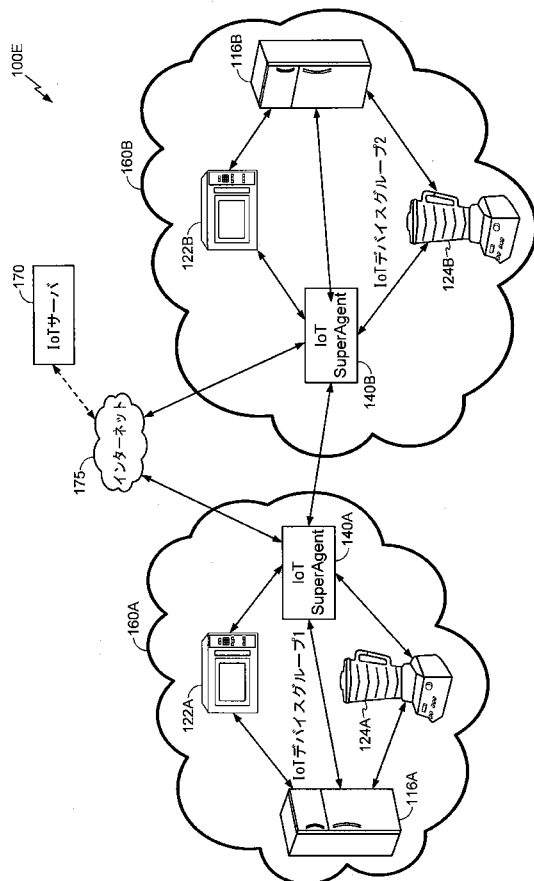
【図 1 C】



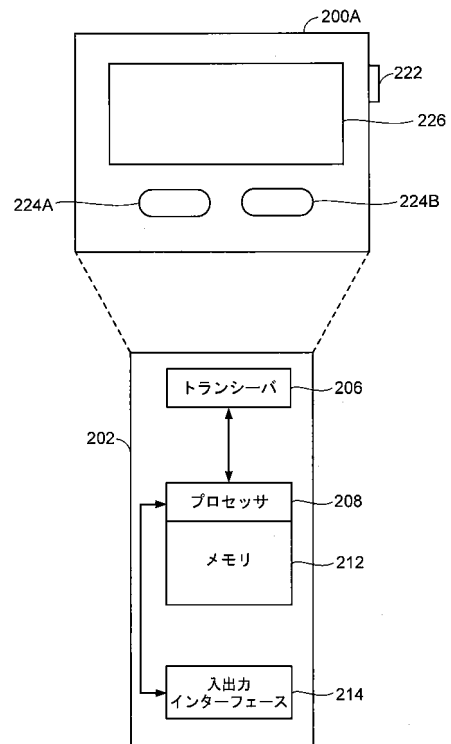
【図 1 D】



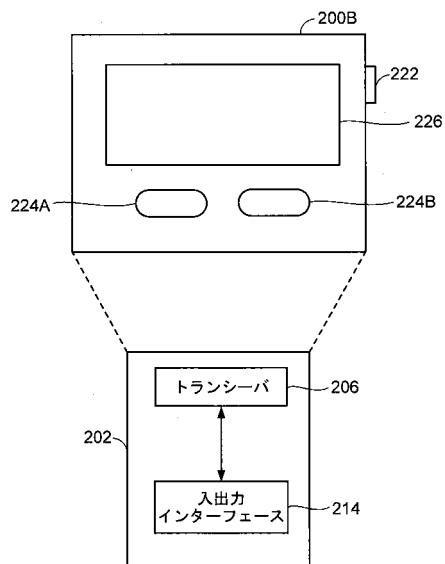
【図 1 E】



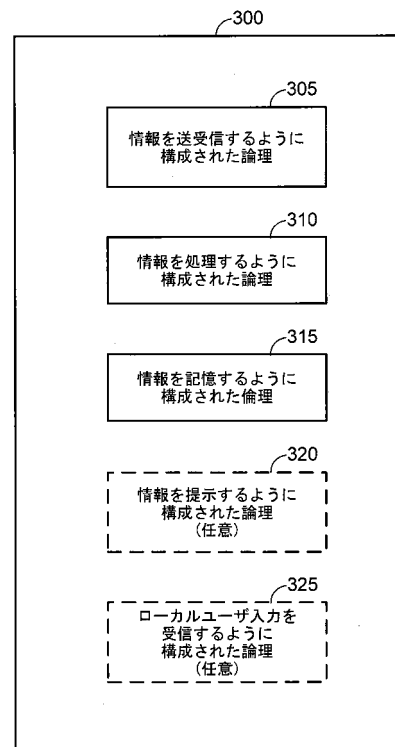
【図 2 A】



【図 2 B】



【図 3】



【図 4】

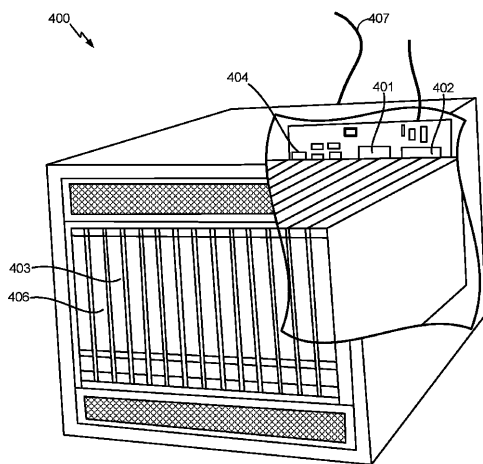
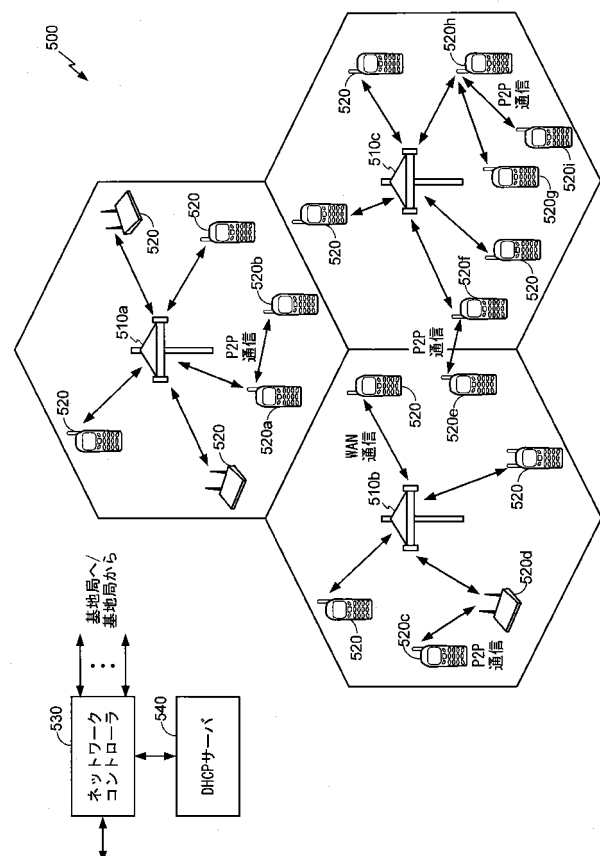
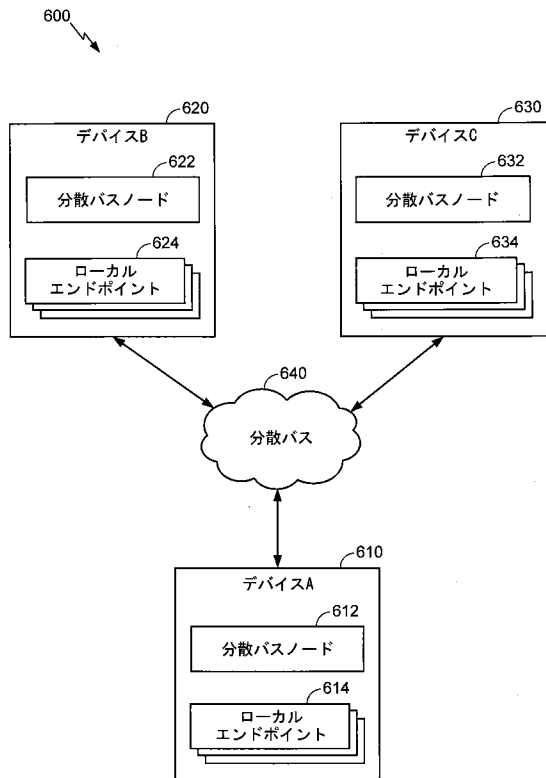


FIG. 4

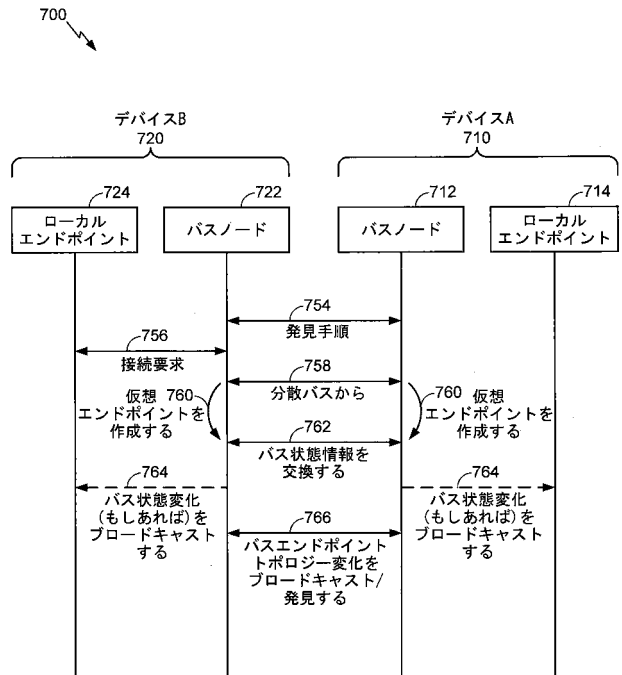
【図 5】



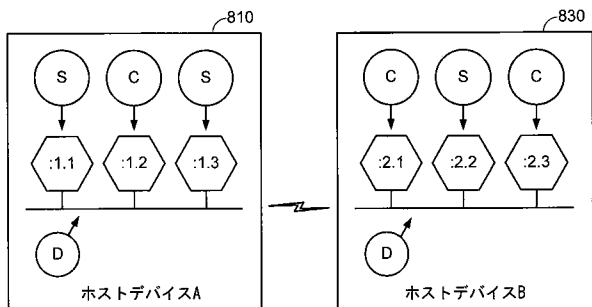
【図 6】



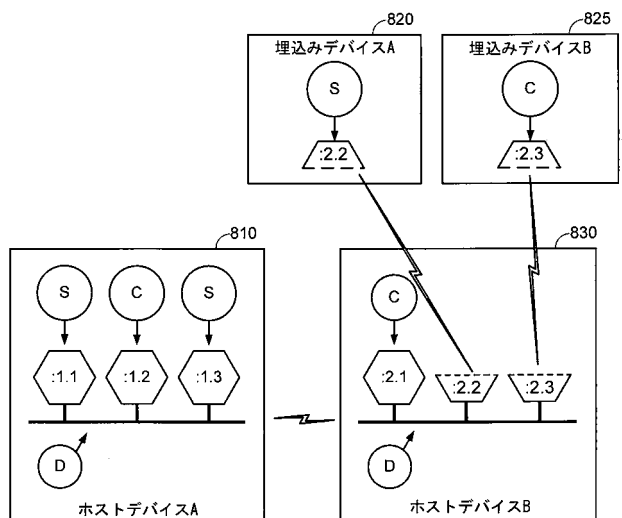
【図 7】



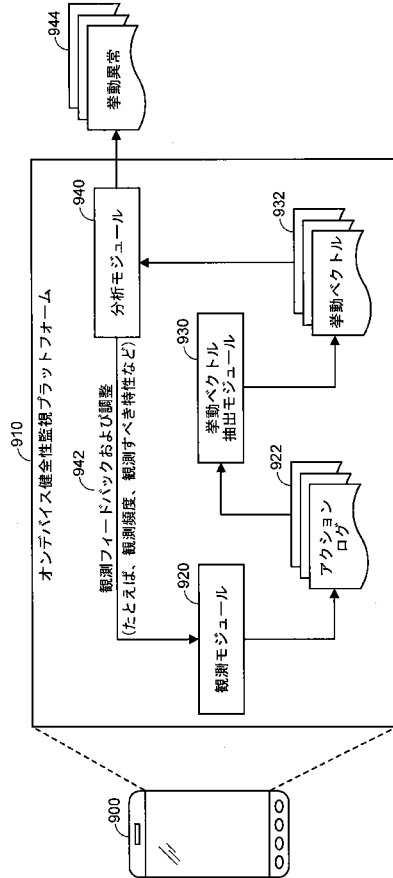
【図 8 A】



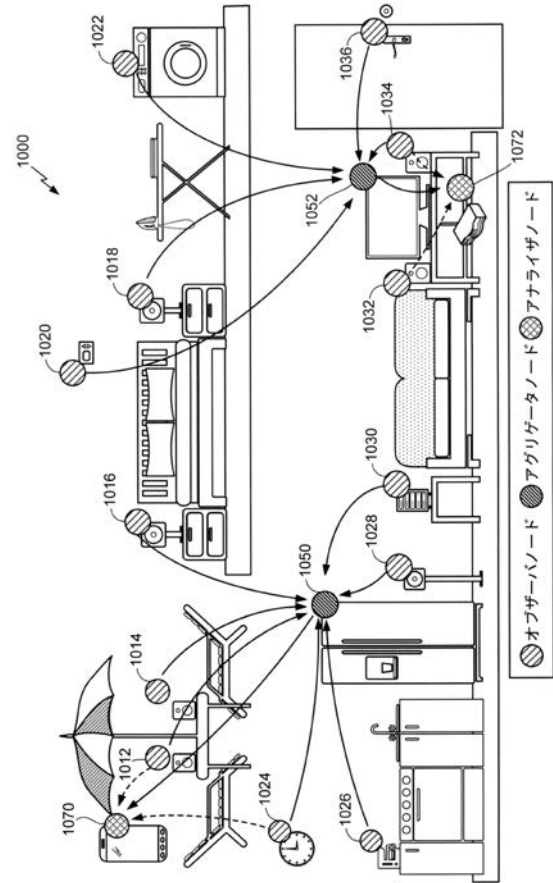
【図 8 B】



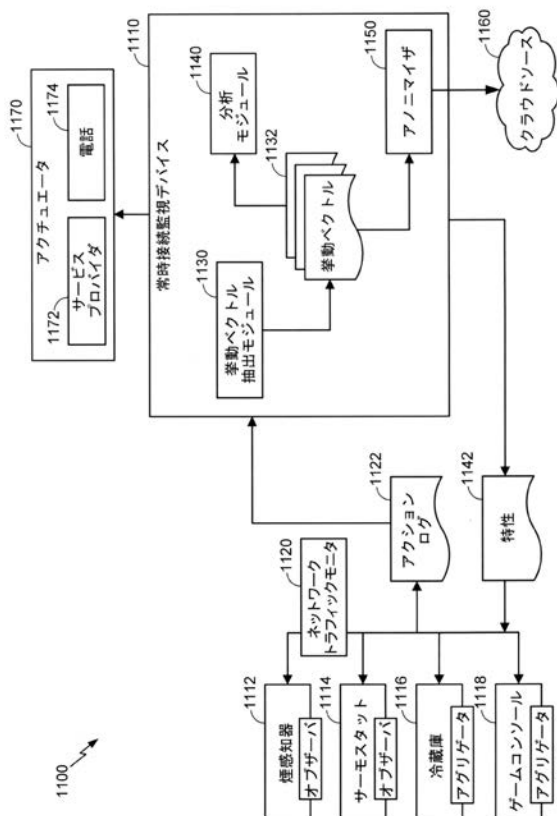
【図 9】



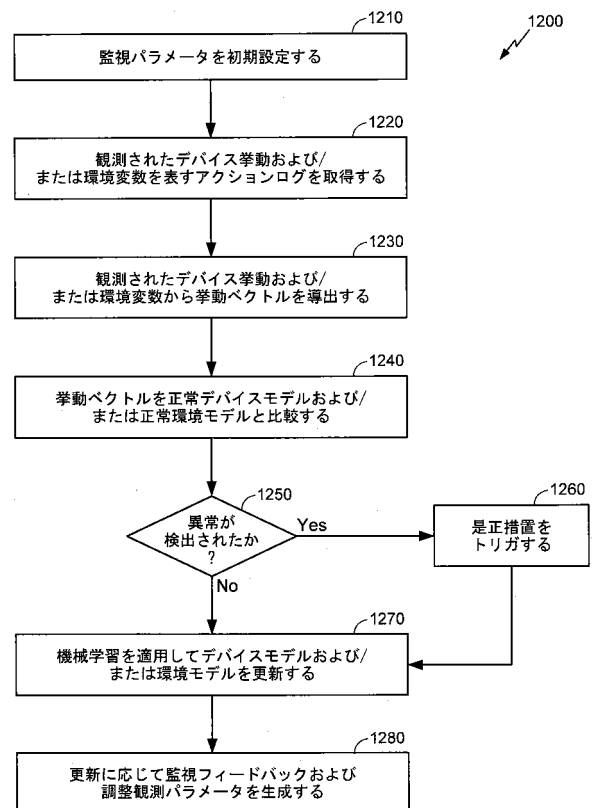
【図 10】



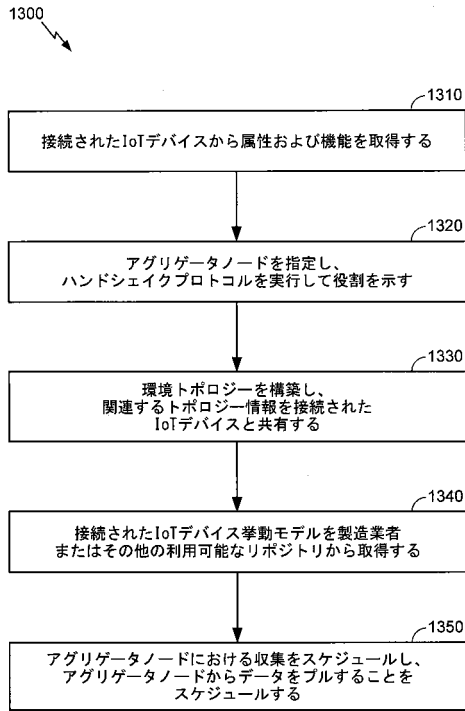
【図 11】



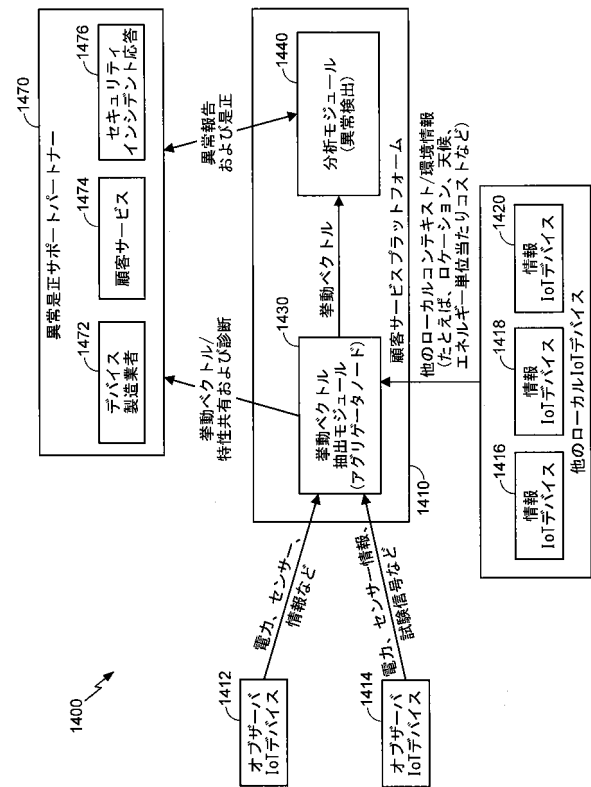
【図 12】



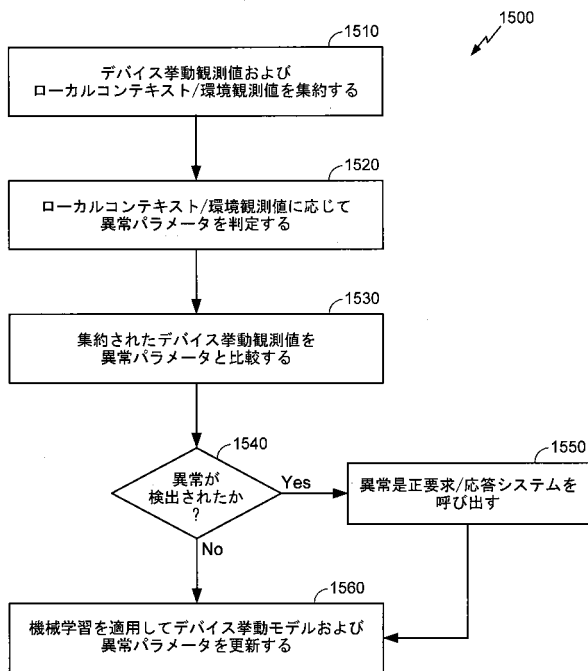
【図 13】



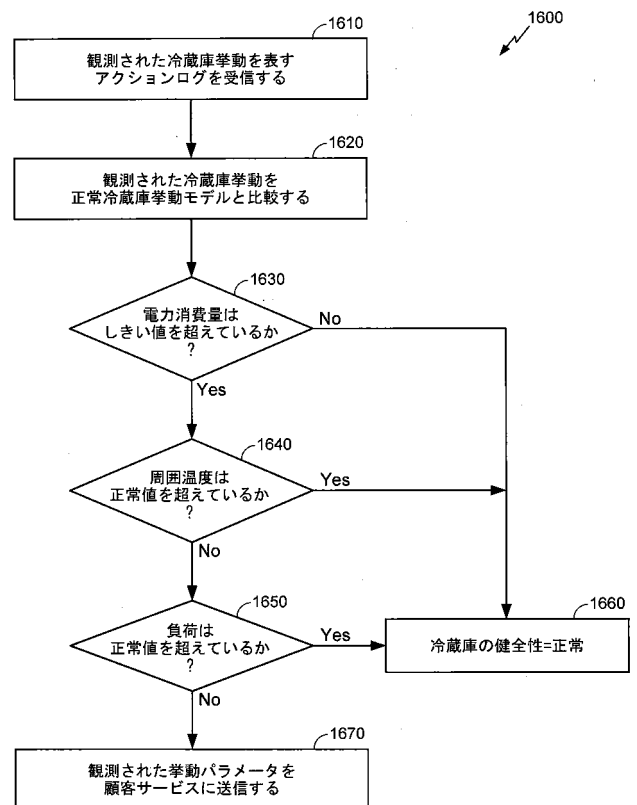
【図 14】



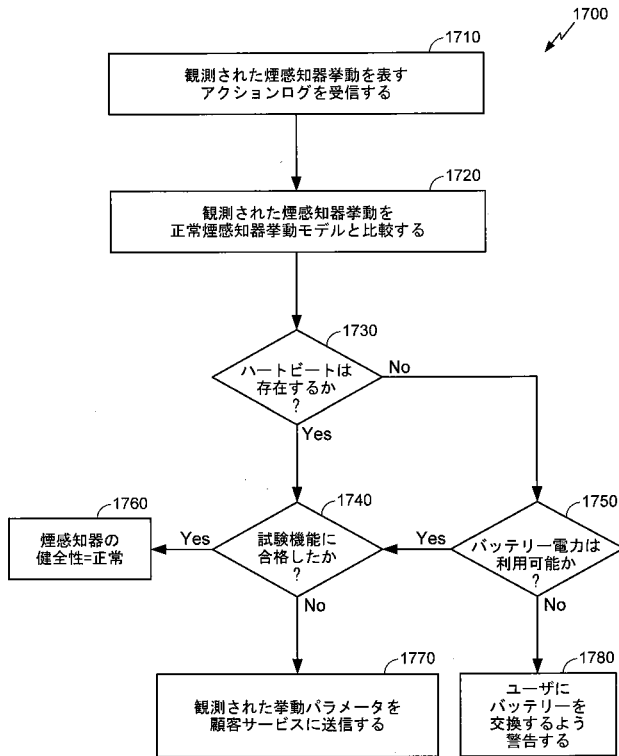
【図 15】



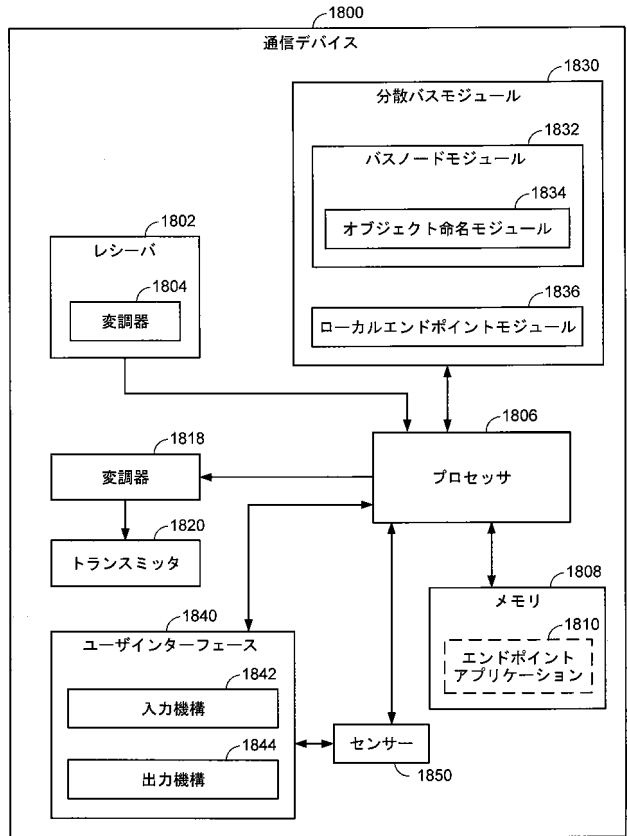
【図 16】



【図 17】



【図 18】



【手続補正書】

【提出日】平成29年9月5日(2017.9.5)

【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】

モノのインターネット(IoT)デバイスの健全性を監視するための方法であって、
ローカルIoTネットワーク内のアナライザノードにおいて、前記ローカルIoTネットワーク内のIoTデバイスに関連する正常挙動をモデル化するステップと、
前記ローカルIoTネットワーク上の前記アナライザノードにおいて、前記IoTデバイスにおいて観測された1つまたは複数の挙動に関する挙動情報を受信するステップと、
前記アナライザノードにおいて、前記IoTデバイスにおいて観測された前記1つまたは複数の挙動に関する前記挙動情報を分析するステップと、
前記アナライザノードにおいて、前記分析された挙動情報を前記IoTデバイスに関連する前記モデル化された正常挙動と比較して、前記IoTデバイスにおいて観測された前記1つまたは複数の挙動が正常であるかそれとも異常であるかを判定するステップとを含む方法。

【請求項 2】

前記IoTデバイスにおいて観測された前記1つまたは複数の挙動に関する前記挙動情報を分析する前記ステップは、

前記挙動情報から1つまたは複数の挙動ベクトルを抽出するステップであって、前記挙動情報が、n個の挙動特性を表し、前記1つまたは複数の挙動ベクトルが前記n個の挙動特

性をn次元空間にマップする、ステップをさらに含む、請求項1に記載の方法。

【請求項3】

前記IoTデバイスを含む前記ローカルIoTネットワークをモデル化するステップと、
前記分析された挙動情報を前記モデル化されたローカルIoTネットワークと比較して、
前記ローカルIoTネットワークに関連する現在の状態を判定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4】

前記ローカルIoTネットワークをモデル化する前記ステップは、
前記ローカルIoTネットワーク内の各IoTデバイスに関連する属性をモデル化するステップと、
前記ローカルIoTネットワークに関連するトポロジを構築するステップと、
前記ローカルIoTネットワーク内の各IoTデバイスに関連する挙動モデルを、各IoTデバイスに関連する製造業者あるいは前記挙動モデルを記憶するように構成された1つまたは複数のリポジトリから取得するステップと、
前記ローカルIoTネットワーク内の各IoTデバイスに関連する集約された属性、前記ローカルIoTネットワークに関連する前記トポロジ、および前記ローカルIoTネットワークをモデル化するように前記ローカルIoTネットワーク内の各IoTデバイスに関連付けられた前記挙動モデルを組み合わせるステップとを含む、請求項3に記載の方法。

【請求項5】

前記IoTデバイスにおいて観測された前記1つまたは複数の挙動が異常であると判定したことに応答して、前記IoTデバイスにおいて観測された前記1つまたは複数の挙動を顧客サービスエンティティに報告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6】

前記1つまたは複数の異常挙動は、前記IoTデバイスまたは前記IoTデバイスを含む前記ローカルIoTネットワークに対する潜在的な悪意のある攻撃を示す、請求項5に記載の方法。

【請求項7】

前記1つまたは複数の異常挙動は、前記IoTデバイスにおける潜在的な誤動作または異常動作条件を示す、請求項5に記載の方法。

【請求項8】

前記IoTデバイスは、前記1つまたは複数の挙動を観測するように装備された1つまたは複数の構成要素を備える、請求項1に記載の方法。

【請求項9】

前記IoTデバイスは、前記アナライザノード、あるいは前記IoTデバイスから前記1つまたは複数の挙動特性を受信し、前記1つまたは複数の挙動特性を前記アナライザノードに中継するように構成されたアグリゲータノードのうちの1つまたは複数に、前記1つまたは複数の観測された挙動を表す1つまたは複数の挙動特性を送るように構成されたトランスミッタをさらに備える、請求項8に記載の方法。

【請求項10】

前記IoTデバイスを含む前記ローカルIoTネットワークは、前記IoTデバイスが前記ローカルIoTネットワークを介して送信するメッセージを監視し、前記ローカルIoTネットワークを介して送信される前記監視されたメッセージに従って前記IoTデバイスにおける前記挙動情報を観測するように構成された1つまたは複数のノードをさらに含む、請求項1に記載の方法。

【請求項11】

モノのインターネット(IoT)デバイスの健全性を監視するための装置であって、
ローカルIoTネットワーク内のIoTデバイスに関連する正常挙動をモデル化する情報を記憶するように構成された少なくとも1つの記憶デバイスと、
前記IoTデバイスにおいて観測された1つまたは複数の挙動に関する挙動情報を前記ローカルIoTネットワークを介して受信するように構成されたトランシーバと、

1つまたは複数のプロセッサとを備え、前記1つまたは複数のプロセッサは、

前記IoTデバイスにおいて観測された前記1つまたは複数の挙動に関する前記挙動情報を分析することと、

前記分析された挙動情報を前記IoTデバイスに関連する前記モデル化された正常挙動と比較して、前記IoTデバイスにおいて観測された前記1つまたは複数の挙動が正常挙動を示すかそれとも異常挙動を示すかを判定することを行うように構成される装置。

【請求項12】

前記1つまたは複数のプロセッサは、前記挙動情報から1つまたは複数の挙動ベクトルを抽出するようにさらに構成され、前記挙動情報は、n個の挙動特性を表し、前記1つまたは複数の挙動ベクトルは、前記n個の挙動特性をn次元空間にマップする、請求項11に記載の装置。

【請求項13】

前記少なくとも1つの記憶デバイスは、前記IoTデバイスを含む前記ローカルIoTネットワークをモデル化する情報を記憶するようにさらに構成され、

前記1つまたは複数のプロセッサは、前記分析された挙動情報を前記モデル化されたローカルIoTネットワークと比較して、前記ローカルIoTネットワークに関連する現在の状態を判定するようにさらに構成される、請求項11に記載の装置。

【請求項14】

前記1つまたは複数のプロセッサは、

前記ローカルIoTネットワーク内の各IoTデバイスに関連する属性を集約することと、

前記ローカルIoTネットワークに関連するトポロジを構築することと、

前記ローカルIoTネットワーク内の各IoTデバイスに関連する挙動モデルを、各IoTデバイスに関連する製造業者あるいは前記挙動モデルを記憶するように構成された1つまたは複数のリポジトリから取得することと、

前記ローカルIoTネットワーク内の各IoTデバイスに関連する前記集約された属性、前記ローカルIoTネットワークに関連する前記トポロジ、および前記ローカルIoTネットワークをモデル化するように前記ローカルIoTネットワーク内の各IoTデバイスに関連付けられた前記挙動モデルを組み合わせることを行うようにさらに構成される、請求項13に記載の装置。

【請求項15】

前記1つまたは複数のプロセッサは、前記IoTデバイスにおいて観測された前記1つまたは複数の挙動が異常挙動を示していることに応答して、前記IoTデバイスにおいて観測された前記1つまたは複数の挙動を顧客サービスエンティティに報告するようにさらに構成される、請求項11に記載の装置。

【請求項16】

前記異常挙動は、前記IoTデバイスまたは前記IoTデバイスを含む前記ローカルIoTネットワークに対する潜在的な悪意のある攻撃あるいは前記IoTデバイスにおける潜在的な誤動作または異常動作条件のうちの1つまたは複数を含む、請求項15に記載の装置。

【請求項17】

オンデバイス健全性監視プラットフォームをさらに備え、前記オンデバイス健全性監視プラットフォームは、

前記IoTデバイスにおいて観測された前記1つまたは複数の挙動に関する前記挙動情報から1つまたは複数の挙動ベクトルを抽出するように構成された挙動ベクトル抽出モジュールと、

前記挙動情報から抽出された前記1つまたは複数の挙動ベクトルを、前記IoTデバイスに関連する前記モデル化された正常挙動と比較して、前記IoTデバイスにおいて観測された前記1つまたは複数の挙動が正常挙動を示すかそれとも異常挙動を示すかを判定するように構成された分析モジュールとを少なくとも備える、請求項11に記載の装置。

【請求項18】

前記挙動情報は、前記IoTデバイスまたは前記IoTデバイスから前記挙動情報を受信し、

前記挙動情報を前記装置に中継するように構成されたアグリゲータノードのうちの1つまたは複数から受信される、請求項17に記載の装置。

【請求項19】

前記オンデバイス健全性監視プラットフォームは、
前記装置におけるローカル挙動を観測するように装備された1つまたは複数の構成要素であって、前記IoTデバイスに関連する前記正常挙動をモデル化する前記情報が、前記装置において観測された前記ローカル挙動に少なくとも部分的に基づく1つまたは複数の構成要素をさらに備える、請求項17に記載の装置。

【請求項20】

前記挙動情報は、前記IoTデバイスが前記ローカルIoTネットワークを介して送信するメッセージを監視し、前記IoTデバイスが前記ローカルIoTネットワークを介して送信する前記監視されたメッセージに従って前記挙動情報を前記装置に伝送するように構成された1つまたは複数のネットワークトラフィック監視ノードから受信される、請求項11に記載の装置。

【請求項21】

モノのインターネット(IoT)デバイスの健全性を監視するための装置であって、
ローカルIoTネットワーク内のIoTデバイスに関連する正常挙動をモデル化するための手段と、

前記ローカルIoTネットワークを介して、前記IoTデバイスにおいて観測された1つまたは複数の挙動に関する挙動情報を受信するための手段と、

前記IoTデバイスにおいて観測された前記1つまたは複数の挙動に関する前記挙動情報を分析するための手段と、

前記分析された挙動情報を前記IoTデバイスに関連する前記モデル化された正常挙動と比較して、前記IoTデバイスにおいて観測された前記1つまたは複数の挙動が正常であるかそれとも異常であるかを判定するための手段とを備える装置。

【請求項22】

前記挙動情報から1つまたは複数の挙動ベクトルを抽出するための手段をさらに備え、
前記挙動情報は、n個の挙動特性を表し、前記1つまたは複数の挙動ベクトルは、前記n個の挙動特性をn次元空間にマップする、請求項21に記載の装置。

【請求項23】

前記IoTデバイスを含む前記ローカルIoTネットワークをモデル化するための手段と、
前記分析された挙動情報を前記モデル化されたローカルIoTネットワークと比較して、
前記ローカルIoTネットワークに関連する現在の状態を判定するための手段とをさらに備える、請求項21に記載の装置。

【請求項24】

前記ローカルIoTネットワーク内の各IoTデバイスに関連する属性を集約するための手段と、

前記ローカルIoTネットワークに関連するトポロジを構築するための手段と、

前記ローカルIoTネットワーク内の各IoTデバイスに関連する挙動モデルを、各IoTデバイスに関連する製造業者あるいは前記挙動モデルを記憶するように構成された1つまたは複数のリポジトリから取得するための手段と、

前記ローカルIoTネットワーク内の各IoTデバイスに関連する前記集約された属性、前記ローカルIoTネットワークに関連する前記トポロジ、および前記ローカルIoTネットワークをモデル化するように前記ローカルIoTネットワーク内の各IoTデバイスに関連付けられた前記挙動モデルを組み合わせるための手段とをさらに備える、請求項23に記載の装置。

【請求項25】

前記IoTデバイスにおいて観測された前記1つまたは複数の挙動が異常挙動を示していることに応答して、前記IoTデバイスにおいて観測された前記1つまたは複数の挙動を顧客サービスエンティティに報告するための手段をさらに備える、請求項21に記載の装置。

【請求項26】

前記異常挙動は、前記IoTデバイスまたは前記IoTデバイスを含む前記ローカルIoTネットワークに対する潜在的な悪意のある攻撃を含む、請求項25に記載の装置。

【請求項27】

前記異常挙動は、前記IoTデバイスにおける潜在的な誤動作または異常動作条件を含む、請求項25に記載の装置。

【請求項28】

前記挙動情報は、前記IoTデバイスまたは前記IoTデバイスから前記挙動情報を受信し、前記挙動情報を前記装置に中継するように構成されたアグリゲータノードのうちの1つまたは複数から受信される、請求項21に記載の装置。

【請求項29】

前記挙動情報は、前記IoTデバイスが前記ローカルIoTネットワークを介して送信するメッセージを監視し、前記IoTデバイスが前記ローカルIoTネットワークを介して送信する前記監視されたメッセージに従って前記挙動情報を前記装置に伝送するように構成された1つまたは複数のネットワークトラフィック監視ノードから受信される、請求項21に記載の装置。

【請求項30】

コンピュータ実行可能命令を記録したコンピュータ可読記憶媒体であって、1つまたは複数のプロセッサ上で前記コンピュータ実行可能命令を実行することが、前記1つまたは複数のプロセッサに、

ローカルIoTネットワーク内のモノのインターネット(IoT)デバイスに関連する正常挙動をモデル化することと、

前記ローカルIoTネットワークを介して、前記IoTデバイスにおいて観測された1つまたは複数の挙動に関する挙動情報を受信することと、

前記IoTデバイスにおいて観測された前記1つまたは複数の挙動に関する前記挙動情報を分析することと、

前記分析された挙動情報を前記IoTデバイスに関連する前記モデル化された正常挙動と比較して、前記IoTデバイスにおいて観測された前記1つまたは複数の挙動が正常であるかそれとも異常であるかを判定することとを行わせるコンピュータ可読記憶媒体。

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2016/020072

A. CLASSIFICATION OF SUBJECT MATTER

INV. H04L12/28 H04L12/24
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)
H04L

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2014/053261 A1 (GUPTA RAJARSHI [US] ET AL) 20 February 2014 (2014-02-20) the whole document	1-30
X	----- L Chekina ET AL: "Detection of deviations in mobile applications network behavior", arXiv:1208.0564v2 [cs.CR], 5 August 2012 (2012-08-05), XP055107301, Retrieved from the Internet: URL:http://arxiv.org/abs/1208.0564v2 [retrieved on 2014-03-12]	1-3, 11-13, 21-23,30
A	the whole document ----- -/--	4-10, 14-20, 24-29

☒ 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

"Z" document member of the same patent family

Date of the actual completion of the international search

25 April 2016

Date of mailing of the international search report

03/05/2016

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

Le Bras, Patrick

INTERNATIONAL SEARCH REPORT

International application No

PCT/US2016/020072

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X A	US 2009/199296 A1 (XIE LIANG [US] ET AL) 6 August 2009 (2009-08-06) the whole document	1,11,21, 30 2-10, 12-20, 22-29
X,P	----- WO 2015/157108 A1 (QUALCOMM INC [US]) 15 October 2015 (2015-10-15) the whole document -----	1-30

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/US2016/020072

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2014053261 A1	20-02-2014	NONE	
US 2009199296 A1	06-08-2009	NONE	
WO 2015157108 A1	15-10-2015	US 2015286820 A1 WO 2015157108 A1	08-10-2015 15-10-2015

フロントページの続き

(51)Int.Cl.

F I

テーマコード(参考)

G 0 6 F 17/30 1 1 0 G

(81)指定国 AP(BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), EA(AM, AZ, BY, KG, KZ, RU, TJ, TM), EP(AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OA(BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG), AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US

(特許庁注: 以下のものは登録商標)

1 . F I R E W I R E

(72)発明者 マストウーレ・サラジェゲ

アメリカ合衆国・カリフォルニア・9 2 1 2 1 - 1 7 1 4・サン・ディエゴ・モアハウス・ドライブ・5 7 7 5

(72)発明者 ミハイ・クリストオドレスク

アメリカ合衆国・カリフォルニア・9 2 1 2 1 - 1 7 1 4・サン・ディエゴ・モアハウス・ドライブ・5 7 7 5

(72)発明者 ヴィナイ・シュリダラ

アメリカ合衆国・カリフォルニア・9 2 1 2 1 - 1 7 1 4・サン・ディエゴ・モアハウス・ドライブ・5 7 7 5

(72)発明者 ゴヴィンダラジャン・クリシュナマーティ

アメリカ合衆国・カリフォルニア・9 2 1 2 1 - 1 7 1 4・サン・ディエゴ・モアハウス・ドライブ・5 7 7 5

Fターム(参考) 5K030 GA14 HB06 HD03 JA10 MA06 MB01 MC07 MC09