(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2019-536144
(P2019-536144A)
(43)公表日　令和1年12月12日(2019.12.12)

(51)Int.Cl.		F I		テーマコード（参考）
G06F 21/57	(2013.01)	G06F	21/57	370
G06F 21/55	(2013.01)	G06F	21/55	

審査請求 未請求　予備審査請求 未請求　（全 21 頁）

(21)出願番号　特願2019-522908 (P2019-522908)
(86)(22)出願日　平成29年10月30日 (2017.10.30)
(85)翻訳文提出日　令和1年6月13日 (2019.6.13)
(86)国際出願番号　PCT/US2017/058926
(87)国際公開番号　WO2018/085166
(87)国際公開日　平成30年5月11日 (2018.5.11)
(31)優先権主張番号　15/344,461
(32)優先日　平成28年11月4日 (2016.11.4)
(33)優先権主張国・地域又は機関
米国 (US)

(71)出願人　314015767
マイクロソフト　テクノロジー　ライセンシング，エルエルシー
アメリカ合衆国　ワシントン州　９８０５２　レッドモンド　ワン　マイクロソフト　ウェイ
(74)代理人　100140109
弁理士　小野　新次郎
(74)代理人　100118902
弁理士　山本　修
(74)代理人　100106208
弁理士　宮前　徹
(74)代理人　100120112
弁理士　中西　基晴

最終頁に続く

(54)【発明の名称】ＩＯＴセキュリティーサービス

(57)【要約】
開示される本技術は、一般的には、ＩｏＴ環境においてのデバイスセキュリティーに向けられるものである。例えば、そのような技術は、ＩｏＴセキュリティーにおいて使用可能である。本技術の１つの例において、少なくとも１つのＩｏＴデバイスの予期される条件と関連付けられるセキュリティー規則のセットが格納される。少なくとも１つのＩｏＴデバイスと関連付けられるＩｏＴデータが受信される。ＩｏＴデータは、少なくとも２つの異なるタイプのデータを含む集約されたデータであり得る。ＩｏＴデータに基づいて、セキュリティー規則のセットが違反されているかどうかに関して決定が行われる。決定に基づいて、警告が選択的に送られる。

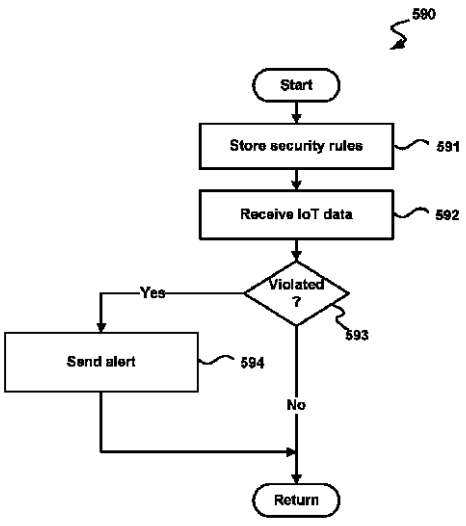

FIG. 5

【特許請求の範囲】
【請求項１】
モノのインターネット（ＩｏＴ）セキュリティーのための装置であって、
１つ又は複数のデバイスを含むＩｏＴハブを備え、前記デバイスは、前記デバイスに対するランタイムデータを格納するように適応される少なくとも１つのメモリーと、実行に応答して前記ＩｏＴハブが
少なくとも１つのＩｏＴデバイスの予期される条件と関連付けられるセキュリティー規則のセットを格納するステップと、
前記少なくとも１つのＩｏＴデバイスと関連付けられるＩｏＴデータを受信するステップであって、前記ＩｏＴデータは、少なくとも２つの異なるタイプのデータを含む集約されたデータである、受信するステップと、
前記ＩｏＴデータに基づいて、セキュリティー規則の前記セットが違反されているかどうかに関して決定を行うステップと、
前記決定に基づいて警告を選択的に送るステップと
を含むアクションを実施することを可能にするプロセッサー実行可能コードを実行するように適応される少なくとも１つのプロセッサーとを含む、装置。
【請求項２】
前記アクションは、
構成要求を受信するステップと、
セキュリティー規則の前記セットを前記構成要求に基づいて調整するステップと
をさらに含む、請求項１に記載の装置。
【請求項３】
前記少なくとも１つのＩｏＴデバイスは、複数のＩｏＴデバイスを含み、前記ＩｏＴデータは、前記複数のＩｏＴデバイス上に展開されるデータ収集エージェントから受信される、請求項１に記載の装置。
【請求項４】
セキュリティー規則の前記セットは、プロセスのホワイトリスト、及び、プロセスのブラックリストのうちの少なくとも１つを含む、請求項１に記載の装置。
【請求項５】
前記ＩｏＴデータは、前記少なくとも１つのＩｏＴデバイスを含む複数個のＩｏＴデバイスから集約される、請求項１に記載の装置。
【請求項６】
モノのインターネット（ＩｏＴ）セキュリティーのための方法であって、
構成可能なＩｏＴデバイスモデルを生成するステップと、
少なくとも１つのＩｏＴデバイスから、集約されたＩｏＴデバイスデータを受信するステップであって、前記集約されたデータＩｏＴデバイスデータは、少なくとも２つの異なるタイプのデータを含む、ステップと、
少なくとも１つのプロセッサーを用いて、前記集約されたＩｏＴデバイスデータを、前記構成可能なＩｏＴデバイスモデルと比較するステップと、
前記比較に基づいて警告を選択的に送るステップと
を含む、方法。
【請求項７】
前記少なくとも１つのＩｏＴデバイスは、複数のＩｏＴデバイスを含み、前記集約されたＩｏＴデバイスデータは、前記複数のＩｏＴデバイス上に展開されるデータ収集エージェントから受信される、請求項６に記載の方法。
【請求項８】
構成要求を受信するステップと、
前記構成可能なＩｏＴデバイスモデルを、前記構成要求に基づいて調整するステップと
をさらに含む、請求項６に記載の方法。
【請求項９】

モノのインターネット（ＩｏＴ）セキュリティーのための方法であって、
少なくとも１つのプロセッサーを用いて、構成要求を生成するステップであって、前記構成要求は、セキュリティー規則のセットを、セキュリティー規則の調整されたセットに変更するようにとの要求であり、セキュリティー規則の前記調整されたセットは、少なくとも１つのＩｏＴデバイスの予期される条件と関連付けられ、セキュリティー規則の前記調整されたセットは、前記少なくとも１つのＩｏＴデバイスと関連付けられるＩｏＴデータの評価に基づき、前記ＩｏＴデータは、少なくとも２つの異なるタイプのデータを含む集約されたデータである、ステップと、
ＩｏＴハブに前記構成要求を送るステップと、
セキュリティー規則の前記調整されたセットが違反されていると前記ＩｏＴハブが決定すると、前記ＩｏＴハブから警告を受信するステップと
を含む、方法。
【請求項１０】
セキュリティー規則の前記調整されたセットは、前記少なくとも１つのＩｏＴデバイスが複数のＩｏＴデバイスであるような、前記少なくとも１つのＩｏＴデバイスと関連付けられるＩｏＴデータの評価に基づく、請求項９に記載の方法。
【請求項１１】
前記ＩｏＴデータは、前記少なくとも１つのＩｏＴデバイス上の改ざんスイッチの状態を含む、請求項１に記載の装置。
【請求項１２】
前記ＩｏＴデータの前記集約されたデータは、環境データ及び内部データを含む、請求項９に記載の方法。
【請求項１３】
前記環境データは、温度、湿度、検知される場所、又は地理位置情報のうちの少なくとも１つを含み、前記内部データは、オペレーティングシステムバージョン、アクティブプロセスの現在の状態、オープンポート、又は、前記少なくとも１つのＩｏＴデバイスに接続されるデバイスと関連付けられる情報のうちの少なくとも１つを含む、請求項１２に記載の方法。
【請求項１４】
前記ＩｏＴデータの前記集約されたデータは、環境データ及び内部状態データを含む、請求項１に記載の装置。
【請求項１５】
前記内部データは、オペレーティングシステムバージョン、アクティブプロセスの現在の状態、オープンポート、又は、前記少なくとも１つのＩｏＴデバイスに接続されるデバイスと関連付けられる情報のうちの少なくとも１つを含む、請求項１４に記載の装置。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、ＩＯＴセキュリティーサービスに関する。
【背景技術】
【０００２】
[0001]モノのインターネット（「ＩｏＴ」）は、一般的には、ネットワークによって通信する能力のあるデバイスのシステムを指す。デバイスは、トースター、コーヒーメーカー、サーモスタットシステム、洗濯機、乾燥機、ランプ、自動車、及び同類のものなどの日常品を含み得る。ネットワーク通信は、デバイスオートメーション、データキャプチャー、警告の提供、設定のパーソナル化、及び、数多くの他の用途に対して使用され得る。
【発明の概要】
【発明が解決しようとする課題】
【０００３】
ＩＯＴセキュリティーサービスを提供する。

【課題を解決するための手段】
【０００４】
[0002]この概要は、発明を実施するための形態において下記でさらに説明される選択された概念について単純化された形式で紹介するために提供されるものである。この概要は、請求される主題の、主要な機能、又は、本質的な機能を識別することを意図されず、この概要は、請求される主題の範囲を制限するために使用されることもまた意図されない。
【０００５】
[0003]手短に説述すると、開示される本技術は、一般的には、ＩｏＴ環境においてのデバイスセキュリティーに向けられるものである。例えば、そのような技術は、ＩｏＴセキュリティーにおいて使用可能である。本技術の１つの例において、少なくとも１つのＩｏＴデバイスの予期される条件と関連付けられるセキュリティー規則のセットが格納される。少なくとも１つのＩｏＴデバイスと関連付けられるＩｏＴデータが受信される。ＩｏＴデータは、少なくとも２つの異なるタイプのデータを含む集約されたデータであり得る。ＩｏＴデータに基づいて、セキュリティー規則のセットが違反されているかどうかに関して決定が行われる。決定に基づいて、警告が選択的に送られる。
【０００６】
[0004]本開示の一部の例は、ＩｏＴデバイスセキュリティー状態に関するテレメトリーを使用して、及び、他のＩｏＴデバイスからの他の環境データを使用して、ＩｏＴデバイスに対するセキュリティー上の脅威を監視する、検出する、及び軽減するためのシステムを含む。一部の例において、環境内の複数個のＩｏＴデバイスからのテレメトリーデータが使用され、環境のモデルが形成される。一部の例において、結果的なモデルは、侵入及び改ざん（ｔａｍｐｅｒｉｎｇ）などのセキュリティー上の脅威を検出するために使用される。
【０００７】
[0005]開示される本技術の他の態様、及び、開示される本技術に対する用途は、添付される図及び説明を読み理解することで、察知されるであろう。
[0006]本開示の非制限的及び非網羅的な例が、後に続く図面を参照して説明される。図面において、同類の参照番号は、別段に指定されない限り、様々な図の全体を通して、同類の部分を指す。これらの図面は、必ずしも一定の縮尺で描かれない。
【０００８】
[0007]本開示のより良好な理解のために、付随する図面と関連して読まれることになる、後に続く、発明を実施するための形態を参照する。
【図面の簡単な説明】
【０００９】
【図１】[0008]本技術の態様が用いられ得る、適した環境の１つの例を例示するブロック線図である。
【図２】[0009]開示される本技術の態様による、適したコンピューティングデバイスの１つの例を例示するブロック線図である。
【図３】[0010]ＩｏＴセキュリティーのためのシステムの例を例示するブロック線図である。
【図４】[0011]ＩｏＴセキュリティーのためのプロセスに対する例データフローを例示する線図である。
【図５】[0012]本開示の態様による、ＩｏＴセキュリティーのためのプロセスの例を例示する論理フロー線図である。
【発明を実施するための形態】
【００１０】
[0013]後に続く説明は、本技術の様々な例の徹底的な理解、及び、本技術の様々な例に対する説明を可能にすることのために、具体的な詳細を提供する。当業者は、本技術が、これらの詳細の多くがなくとも実践され得るということを理解するであろう。一部の実例において、よく知られている構造及び機能は、本技術の例の説明を不必要に分かりにくく

することを回避するために、詳細には示され、又は説明されていない。本開示において使用される専門用語は、それが、本技術の所定の例の詳細な説明と連関して使用されているとしても、その専門用語の最も広範な合理的な様式で解釈されるということが意図される。所定の用語が下記で強調されることがあるが、何らかの限定される様式で解釈されることを意図される何らかの専門用語は、そのようなものとして、この、発明を実施するための形態セクションにおいて、明白に、及び具体的に定義されることになる。本明細書及び特許請求の範囲の全体を通して、後に続く用語は、文脈が別段に定めない限り、少なくとも、本明細書において明示的に関連付けられる意味をとる。下記で識別される意味は、必ずしも用語を制限するのではなく、単に用語に対する例示的な例を提供するものである。例えば、用語「に基づく」及び「を基にする」の各々は、排他的ではなく、用語「に少なくとも部分的に基づく」と同等であり、一部が本明細書において説明されないことがある追加の要因に基づくことのオプションを含む。別の例として、用語「を介する」は、排他的ではなく、用語「を少なくとも部分的に介する」と同等であり、一部が本明細書において説明されないことがある追加の要因を介することのオプションを含む。「内」の意味は、「内」及び「上」を含む。語句「１つの実施形態において」又は「１つの例において」は、本明細書において使用される際、必ずしも同じ実施形態又は例を指すものではないが、そうであることもある。特定の本文の数値指定子の使用は、より少ない値の数値指定子の存在を暗黙に示すものではない。例えば、「第３のフーと第４のバーとからなる群から選択される何とか部品」と詳述することは、それ自体は、少なくとも３つのフー要素が存するということも、少なくとも４つのバー要素が存するということも暗黙に示さないことになる。単数形での参照は、単に読むことの明瞭性のために行われるものであり、複数形参照が具体的に排除されない限りは複数形参照を含む。用語「又は」は、別段に具体的に指示されない限り、包含的「ｏｒ」演算子である。例えば、語句「Ａ又はＢ」は、「Ａ、Ｂ、又は、Ａ及びＢ」を意味する。本明細書において使用される際、用語「コンポーネント」及び「システム」は、ハードウェアー、ソフトウェアー、又は、ハードウェアー及びソフトウェアーの様々な組み合わせを包含することを意図される。つまり、例えば、システム又はコンポーネントは、プロセス、コンピューティングデバイス上で実行するプロセス、コンピューティングデバイス、又は、それらの一部分であり得る。用語「ＩｏＴハブ」は、１つの特定のタイプのＩｏＴサービスに制限されるのではなく、ＩｏＴデバイスが、プロビジョニングの後、任意のタイプの少なくとも１つのＩｏＴソリューション又はＩｏＴサービスのために通信するデバイスを指す。すなわち、用語「ＩｏＴハブ」は、本明細書及び特許請求の範囲の全体を通して使用される際、任意のＩｏＴソリューションに対して総称的である。

【００１１】

[0014]手短に説述すると、開示される本技術は、一般的には、ＩｏＴ環境においてのデバイスセキュリティーに向けられるものである。例えば、そのような技術は、ＩｏＴセキュリティーにおいて使用可能である。本技術の１つの例において、少なくとも１つのＩｏＴデバイスの予期される条件と関連付けられるセキュリティー規則のセットが格納される。少なくとも１つのＩｏＴデバイスと関連付けられるＩｏＴデータが受信される。ＩｏＴデータは、少なくとも２つの異なるタイプのデータを含む集約されたデータであり得る。ＩｏＴデータに基づいて、セキュリティー規則のセットが違反されているかどうかに関して決定が行われる。警告が、決定に基づいて選択的に送られる。

【００１２】

[0015]一部の用途において、ＩｏＴデバイスは、リモートで、潜在的可能性として、不利な環境において展開される傾向にある。頻繁に、そのようなデバイスは、デバイスに対するオペレーター又は所有者に、物理的にアクセス可能でないことがある。そのようなデバイスは、さらには「野外に」あることがあり、そのことによって、それらのデバイスは、物理的監視、物理的監督、又は物理的セキュリティーを伴わずに、無人であり、パブリックに物理的に利用可能であり、つまり、人々は、デバイスを物理的に改ざんすることができることがある。誰かが、マルウェアーをそのようなデバイスに転送すること、証明書

をそのようなデバイスから盗むこと、又は同類のことを行うことが可能であり得る。本開示の例は、デバイスのセキュリティーを監視し、デバイスに対する侵入及び／もしくは脅威を検出し、並びに／又は、そのような侵入及び／もしくは脅威を、リモートパーティー、例えば、侵入及び／もしくは脅威を軽減することができることがあるシステムもしくはオペレーターに伝達する。

【００１３】

[0016]本開示の一部の例は、ＩｏＴデバイスセキュリティー状態に関するテレメトリー情報を使用して、テレメトリーデータを使用して、及び、他のＩｏＴデバイスからの他の環境データを使用して、ＩｏＴデバイスに対するセキュリティー上の脅威を監視する、検出する、及び／又は軽減するためのシステムを含む。一部の例において、データ収集エージェントが、ＩｏＴデバイス上に展開され、そのようなＩｏＴデバイスにより生成されるセンサーデータが、ＩｏＴデバイスに対するセキュリティー上の脅威をモデル作成及び検出するために使用される。これらのデータ収集エージェントは、構成データを使用してリモートで構成され得る。

【００１４】

[0017]一部の例において、様々なＩｏＴデバイス上の複数個のエージェントが、様々なタイプのデータを収集するために使用され得るものであり、そのデータは、次いで、デバイス動作、及び侵入の、より全体論的なモデルを形成するために連結して使用され得る。一部の例において、ＩｏＴデバイスからのエージェントデータは、それ自体が、ＩｏＴデバイスのセキュリティー状態を報告するために使用される。一部の例において、デバイスの集合体からのエージェントデータは、動作環境のモデルを形成するために使用される。一部の例において、環境内の複数個のＩｏＴデバイスからのテレメトリーデータが使用され、環境のモデルが形成される。

【００１５】

[0018]一部の例において、結果的なモデルは、侵入及び／又は改ざんなどのセキュリティー上の脅威を検出するために使用される。

【００１６】

例示的なデバイス／動作環境

[0019]図１は、本技術の態様が実践され得る環境１００の線図である。示されるように、環境１００は、ネットワーク１３０を介して接続される、コンピューティングデバイス１１０と、ネットワークノード１２０とを含む。環境１００の特定のコンポーネントが図１において示されるとしても、他の例において、環境１００は、さらには、追加の、及び／又は異なるコンポーネントを含み得る。例えば、所定の例において、環境１００は、さらには、ネットワークストレージデバイス、メンテナンスマネージャー、及び／又は、他の適したコンポーネント（示されない）を含み得る。図１において示されるコンピューティングデバイス１１０は、オンプレミス、クラウド内、又は同類のことを含めて、様々な場所にあり得る。例えば、コンピューターデバイス１１０は、クライアント側にあり、サーバー側にあり、又は同類のことであり得る。

【００１７】

[0020]図１において示されるように、ネットワーク１３０は、１つ又は複数のネットワークノード１２０を含み得るものであり、それらのネットワークノード１２０は、複数個のコンピューティングデバイス１１０を相互接続し、コンピューティングデバイス１１０を外部ネットワーク１４０、例えばインターネット又はイントラネットに接続する。例えば、ネットワークノード１２０は、スイッチ、ルーター、ハブ、ネットワークコントローラー、又は、他のネットワーク要素を含み得る。所定の例において、コンピューティングデバイス１１０は、ラック、アクションゾーン（ａｃｔｉｏｎ　ｚｏｎｅ）、グループ、セット、又は、他の適した区分へと組織化され得る。例えば、例示される例において、コンピューティングデバイス１１０は、個々に第１の、第２の、及び第３のホストセット１１２ａ～１１２ｃと識別される３つのホストセットへとグループ化される。例示される例において、ホストセット１１２ａ～１１２ｃの各々は、それぞれ、「トップオブラック」

又は「ＴＯＲ」ネットワークノードと共通に呼称される、対応するネットワークノード１２０ａ～１２０ｃに動作可能に結合される。ＴＯＲネットワークノード１２０ａ～１２０ｃは、次いで、コンピューティングデバイス１１０と外部ネットワーク１４０との間の通信を許可する、階層、フラット、メッシュ、又は、他の適したタイプのトポロジーでのコンピューターネットワークを形成するために、追加のネットワークノード１２０に動作可能に結合され得る。他の例において、複数個のホストセット１１２ａ～１１２ｃは、単一のネットワークノード１２０を共有してもよい。コンピューティングデバイス１１０は、事実上任意のタイプの汎用又は特定目的コンピューティングデバイスであり得る。例えば、これらのコンピューティングデバイスは、デスクトップコンピューター、ラップトップコンピューター、タブレットコンピューター、ディスプレイデバイス、カメラ、プリンター、又はスマートフォンなどのユーザーデバイスであり得る。しかしながら、データセンター環境において、これらのコンピューティングデバイスは、アプリケーションサーバーコンピューター、仮想コンピューティングホストコンピューター、又はファイルサーバーコンピューターなどのサーバーデバイスであり得る。その上、コンピューティングデバイス１１０は、個々に、コンピューティング、ストレージ、及び／又は、他の適したコンピューティングサービスを提供するように構成され得る。

【００１８】

[0021]一部の例において、コンピューティングデバイス１１０のうちの１つ又は複数は、下記でより詳細に論考されるように、ＩｏＴデバイス、ゲートウェイデバイス、ＩｏＴハブの一部もしくはすべてを備えるデバイス、デバイスポータルサービスの一部もしくはすべてを備えるデバイス、又は同類のものである。

【００１９】

例示的なコンピューティングデバイス

[0022]図２は、本技術の態様が実践され得るコンピューティングデバイス２００の１つの例を例示する線図である。コンピューティングデバイス２００は、事実上任意のタイプの汎用又は特定目的コンピューティングデバイスであり得る。例えば、コンピューティングデバイス２００は、デスクトップコンピューター、ラップトップコンピューター、タブレットコンピューター、ディスプレイデバイス、カメラ、プリンター、又はスマートフォンなどのユーザーデバイスであり得る。同様に、コンピューティングデバイス２００は、さらには、アプリケーションサーバーコンピューター、仮想コンピューティングホストコンピューター、又はファイルサーバーコンピューターなどのサーバーデバイスであり得るものであり、例えば、コンピューティングデバイス２００は、図１のコンピューティングデバイス１１０又はネットワークノード１２０の例であり得る。コンピューティングデバイス２００は、さらには、ネットワークに接続してＩｏＴサービスを受けるＩｏＴデバイスであり得る。同様に、コンピューターデバイス２００は、下記でより詳細に論考されるように、図３～５において例示される、又は、図３～５において参照されるデバイスの、例の任意のものであり得る。図２において例示されるように、コンピューティングデバイス２００は、処理回路２１０と、動作メモリー２２０と、メモリーコントローラー２３０と、データストレージメモリー２５０と、入力インターフェイス２６０と、出力インターフェイス２７０と、ネットワークアダプター２８０とを含む。コンピューティングデバイス２００の、これらの、前に列挙されたコンポーネントの各々は、少なくとも１つのハードウェアー要素を含む。

【００２０】

[0023]コンピューティングデバイス２００は、本明細書において説明されるワークロード、プロセス、又は技術を実装するための命令などの命令を実行するように構成される、少なくとも１つの処理回路２１０を含む。処理回路２１０は、マイクロプロセッサー、マイクロコントローラー、グラフィックプロセッサー、コプロセッサー、フィールドプログラマブルゲートアレイ、プログラマブル論理デバイス、シグナルプロセッサー、又は、データを処理するのに適した任意の他の回路を含み得る。前に述べられた命令は、他のデータ（例えば、データセット、メタデータ、オペレーティングシステム命令、その他）とと

もに、動作メモリー２２０内に、コンピューティングデバイス２００のランタイムの間格納され得る。動作メモリー２２０は、さらには、揮発性メモリー、半揮発性メモリー、ランダムアクセスメモリー、スタティックメモリー、キャッシュ、バッファー、又は、ランタイム情報を格納するために使用される他のメディアなどの、各種のデータストレージデバイス／コンポーネントの任意のものを含み得る。１つの例において、動作メモリー２２０は、コンピューティングデバイス２００が電源をオフにされるときは情報を保持しない。むしろ、コンピューティングデバイス２００は、起動又は他の読み込みプロセスの一部として、非揮発性データストレージコンポーネント（例えば、データストレージコンポーネント２５０）から動作メモリー２２０に命令を転送するように構成され得る。

【００２１】

[0024]動作メモリー２２０は、第４世代ダブルデータレート（ＤＤＲ４）メモリー、第３世代ダブルデータレート（ＤＤＲ３）メモリー、他のダイナミックランダムアクセスメモリー（ＤＲＡＭ）、高帯域幅メモリー（ＨＢＭ）、ハイブリッドメモリーキューブメモリー、３Ｄ積層メモリー、スタティックランダムアクセスメモリー（ＳＲＡＭ）、又は他のメモリーを含み得るものであり、そのようなメモリーは、ＤＩＭＭ、ＳＩＭＭ、ＳＯＤＩＭＭ、又は他のパッケージ上に統合される、１つ又は複数のメモリー回路を備え得る。そのような動作メモリーモジュール又はデバイスは、チャネル、ランク、及びバンクによって組織化され得る。例えば、動作メモリーデバイスは、処理回路２１０に、メモリーコントローラー２３０を介して、チャネルにおいて結合され得る。コンピューティングデバイス２００の１つの例は、チャネルあたり１つ又は２つのランクを伴う、チャネルあたり１つ又は２つのＤＩＭＭを含み得る。ランクの中の動作メモリーは、共有クロック、及び共有アドレス、及びコマンドバスによって動作し得る。さらには、動作メモリーデバイスは、いくつかのバンクへと組織化され得るものであり、バンクは、行及び列によりアドレス指定されるアレイと考えられ得る。動作メモリーのそのような組織化に基づいて、動作メモリーの中の物理アドレスは、チャネル、ランク、バンク、行、及び列のタプルにより参照され得る。

【００２２】

[0025]上記の論考にもかかわらず、動作メモリー２２０は、それ自体は、通信メディアを、何らの通信メディアも、又は、何らのシグナルも、具体的に含まない、又は包含しない。

【００２３】

[0026]メモリーコントローラー２３０は、処理回路２１０を動作メモリー２２０にインターフェイスで接続するように構成される。例えば、メモリーコントローラー２３０は、コマンド、アドレス、及びデータを、動作メモリー２２０と処理回路２１０との間で、インターフェイスで接続するように構成され得る。メモリーコントローラー２３０は、さらには、処理回路２１０からの、又は、処理回路２１０に対するメモリー管理の所定のアスペクトを、抽出する、又は、他の形で管理するように構成され得る。メモリーコントローラー２３０は、処理回路２１０とは別々の単一のメモリーコントローラーとして例示されるが、他の例において、複数個のメモリーコントローラーが用いられることがあり、メモリーコントローラーは動作メモリー２２０と統合されることがあり、又は同類のことがある。さらに、メモリーコントローラーは、処理回路２１０内に統合され得る。これら及び他の変形形態が可能である。

【００２４】

[0027]コンピューティングデバイス２００において、データストレージメモリー２５０、入力インターフェイス２６０、出力インターフェイス２７０、及びネットワークアダプター２８０は、バス２４０により処理回路２１０にインターフェイスで接続される。図２はバス２４０を単一のパッシブバスとして例示するが、バスの集合体、ポイントツーポイントリンクの集合体、入出力コントローラー、ブリッジ、他のインターフェイス回路網、又は、それらの任意の集合体などの他の構成が、さらには、データストレージメモリー２５０、入力インターフェイス２６０、出力インターフェイス２７０、又はネットワークア

ダプター２８０を処理回路２１０にインターフェイスで接続するために、適して用いられ得る。

【００２５】

[0028]コンピューティングデバイス２００において、データストレージメモリー２５０は、長期非揮発性データストレージのために用いられる。データストレージメモリー２５０は、非揮発性メモリー、ディスク、ディスクドライブ、ハードドライブ、ソリッドステートドライブ、又は、情報の非揮発性ストレージのために使用され得る任意の他のメディアなどの、各種の非揮発性データストレージデバイス／コンポーネントの任意のものを含み得る。しかしながら、データストレージメモリー２５０は、それ自体は、通信メディアを、何らの通信メディアも、又は、何らのシグナルも、具体的に含まない、又は包含しない。動作メモリー２２０と対照的に、データストレージメモリー２５０は、ランタイムデータストレージのための代わりに、非揮発性長期データストレージのために、コンピューティングデバイス２００により用いられる。

【００２６】

[0029]さらには、コンピューティングデバイス２００は、プロセッサー読み取り可能ストレージメディア（例えば、動作メモリー２２０及びデータストレージメモリー２５０）及び通信メディア（例えば、通信シグナル及び無線波）などの、任意のタイプのプロセッサー読み取り可能メディアを含む、又は、そのプロセッサー読み取り可能メディアに結合されることがある。用語、プロセッサー読み取り可能ストレージメディアは、動作メモリー２２０及びデータストレージメモリー２５０を含むが、用語「プロセッサー読み取り可能ストレージメディア」は、本明細書及び特許請求の範囲の全体を通して、単数形で使用されようと複数形で使用されようと、本明細書において、用語「プロセッサー読み取り可能ストレージメディア」が、それ自体は、通信メディアを、何らの通信メディアも、又は、何らのシグナルも、具体的に排除し、包含しないように定義される。しかしながら、用語「プロセッサー読み取り可能ストレージメディア」は、プロセッサーキャッシュ、ランダムアクセスメモリー（ＲＡＭ）、レジスターメモリー、及び／又は同類のものをまさに包含する。

【００２７】

[0030]コンピューティングデバイス２００は、さらには、コンピューティングデバイス２００が、ユーザーから、又は他のデバイスから入力を受信することを可能にするように構成され得る入力インターフェイス２６０を含む。加えて、コンピューティングデバイス２００は、コンピューティングデバイス２００から出力を提供するように構成され得る出力インターフェイス２７０を含む。１つの例において、出力インターフェイス２７０は、フレームバッファー、グラフィックプロセッサー、グラフィックプロセッサー又はアクセラレーターを含み、別々の視覚ディスプレイデバイス（モニター、プロジェクター、仮想コンピューティングクライアントコンピューター、その他など）上の提示のために表示物をレンダリングするように構成される。別の例において、出力インターフェイス２７０は、視覚ディスプレイデバイスを含み、観覧のために表示物をレンダリング及び提示するように構成される。

【００２８】

[0031]例示される例において、コンピューティングデバイス２００は、ネットワークアダプター２８０を介して、他のコンピューティングデバイス又はエンティティーと通信するように構成される。ネットワークアダプター２８０は、ワイヤードネットワークアダプター、例えば、Ｅｔｈｅｒｎｅｔアダプター、トークンリングアダプター、又はデジタル加入者線（ＤＳＬ）アダプターを含み得る。ネットワークアダプター２８０は、さらには、ワイヤーレスネットワークアダプター、例えば、Ｗｉ－Ｆｉアダプター、Ｂｌｕｅｔｏｏｔｈ（登録商標）アダプター、ＺｉｇＢｅｅアダプター、ロングタームエボリューション（ＬＴＥ）アダプター、又は５Ｇアダプターを含み得る。

【００２９】

[0032]コンピューティングデバイス２００は、特定の配置で構成される所定のコンポー

ネントを伴って例示されるが、これらのコンポーネント及び配置は、単に、本技術が用いられ得るコンピューティングデバイスの１つの例である。他の例において、データストレージメモリー２５０、入力インターフェイス２６０、出力インターフェイス２７０、又はネットワークアダプター２８０は、処理回路２１０に直接結合される、又は、入出力コントローラー、ブリッジ、もしくは他のインターフェイス回路網を介して処理回路２１０に結合されることがある。本技術の他の変形形態が可能である。

【００３０】

[0033]コンピューティングデバイス２００の一部の例は、ランタイムデータを格納するように適応される少なくとも１つのメモリー（例えば、動作メモリー２２０）と、実行に応答して、コンピューティングデバイス２００がアクションを実施することを可能にする、プロセッサー実行可能コードを実行するようにそれぞれ適応される少なくとも１つのプロセッサー（例えば、処理ユニット２１０）とを含む。一部の例において、コンピューティングデバイス２００は、下記の図４もしくは図５のプロセスにおいてのアクション、又は、下記の図３においてのコンピューティングデバイスのうちの１つもしくは複数により実施されるプロセスにおいてのアクションなどのアクションを実施することを可能にされる。

【００３１】

例示的なシステム

[0034]図３は、ＩｏＴ通信のためのシステム（３００）の例を例示するブロック線図である。システム３００は、ネットワーク３３０と、すべてがネットワーク３３０に接続する、ＩｏＴハブ３５１と、ＩｏＴデバイス３４１～３４３と、ゲートウェイデバイス３１１及び３１２と、デバイスポータルサービス３１３とを含み得る。以前に論考されたように、用語「ＩｏＴハブ」は、１つの特定のタイプのＩｏＴサービスに制限されるのではなく、ＩｏＴデバイスが、プロビジョニングの後、任意のタイプの少なくとも１つのＩｏＴソリューション又はＩｏＴサービスのために通信するデバイスを指す。すなわち、用語「ＩｏＴハブ」は、本明細書及び特許請求の範囲の全体を通して使用される際、任意のＩｏＴソリューションに対して総称的である。用語「ＩｏＴデバイス」は、ＩｏＴサービスを使う、又は、使うことを意図されるデバイスを指す。ＩｏＴデバイスは、テレメトリー収集又は任意の他の目的のためということを含めて、クラウドに接続してＩｏＴサービスを使用する、事実上任意のデバイスを含み得る。デバイスポータルサービス３１３は、デバイスポータルを提供する１つ又は複数のデバイスを含む。用語「ＩｏＴハブ」は、ＩｏＴデバイスがＩｏＴサービスのためにネットワークを介して接続する、デバイス、又は、分散システムなどの複数個のデバイスを指す。

【００３２】

[0035]ＩｏＴデバイス３４１～３４３、ゲートウェイデバイス３１１及び３１２、並びに／又は、ＩｏＴハブ３５１を備えるデバイス、並びに／又は、デバイスポータルサービス３１３の各々は、図２のコンピューティングデバイス２００の例を含み得る。図３、及び、本明細書においての図３の対応する説明は、本開示の範囲を制限しない例示的な目的のための例システムを例示する。

【００３３】

[0036]ネットワーク３３０は、各々のネットワークが、例えば、ワイヤーレスネットワーク、ローカルエリアネットワーク（ＬＡＮ）、ワイドエリアネットワーク（ＷＡＮ）、及び／又は、インターネットなどのグローバルネットワークであり得る、ワイヤード及び／又はワイヤーレスネットワークを含む、１つ又は複数のコンピューターネットワークを含み得る。異なるアーキテクチャー及びプロトコルに基づくものを含む、ＬＡＮの相互接続されるセットについて、ルーターは、ＬＡＮの間のリンクとして働き、メッセージが１つのものから別のものに送られることを可能にする。さらには、ＬＡＮの中の通信リンクは、通常、ツイストワイヤーペアー又は同軸ケーブルを含み、一方で、ネットワークの間の通信リンクは、アナログ電話回線、Ｔ１、Ｔ２、Ｔ３、及びＴ４を含むフルもしくはフラクショナル専用デジタル回線、総合デジタル通信網（ＩＳＤＮ）、デジタル加入者線（

ＤＳＬ）、衛星リンクを含むワイヤーレスリンク、又は、当業者に知られている他の通信リンクを利用し得る。さらにまた、リモートコンピューター及び他の関係付けられる電子デバイスが、モデム及び一時的電話リンクを介して、ＬＡＮ又はＷＡＮのいずれかにリモート接続され得る。本質的に、ネットワーク３３０は、任意の通信方法であって、それにより、情報が、ＩｏＴハブ３５１、ＩｏＴデバイス３４１～３４３、ゲートウェイデバイス３１１～３１２、及びデバイスポータルサービス３１３の間で進行し得る、任意の通信方法を含む。

【００３４】

[0037]１つの例として、ＩｏＴデバイス３４１～３４３は、ＩｏＴハブ３５１などの１つ又は複数のＩｏＴハブにより提供されるＩｏＴサービスを使うことを意図されるデバイスである。デバイスポータルサービス３１３は、デバイスポータルをＩｏＴデバイスのユーザーに提供することにおいてアクションを実施する、１つ又は複数個のデバイスを含む。

【００３５】

[0038]オプションのゲートウェイデバイス３１１及び３１２は、ＩｏＴハブ３５１にアクセスするためにＩｏＴデバイス３４１～３４３の一部により使用され得るデバイスである。一部の例において、プロビジョニングの後、ＩｏＴデバイス３４１～３４３の一部又はすべては、仲介者を使用することなくＩｏＴハブ３５１と通信する。他の例において、ＩｏＴデバイス３４１～３４３の一部又はすべては、ゲートウェイデバイス３１１及び３１２のうちの１つ又は複数などの仲介デバイスを使用してＩｏＴハブ３５１と通信する。デバイスポータルサービス３１３は、ＩｏＴデバイス３４１～３４３を含むＩｏＴデバイスに対するＩｏＴサービスを管理するために、ＩｏＴデバイスのユーザーにより使用され得るサービスである。

【００３６】

[0039]システム３００は、例のみとして示される、図３において例示されるより多い、又は少ないデバイスを含み得る。

【００３７】

例示的なプロセス

[0040]明瞭性のために、本明細書において説明されるプロセスは、システムの特定のデバイス又はコンポーネントにより、特定のシーケンスで実施される動作の見地で説明される。しかしながら、他のプロセスは、説述されるシーケンス、デバイス、又はコンポーネントに制限されないということが特記される。例えば、所定の行為は、異なるシーケンスで、並列で実施される、省略されることが、又は、追加の行為もしくは機能により補足されることが、そのようなシーケンス、並列処理、行為、又は機能が本明細書において説明されるか否かを問わずにある。同様に、本開示において説明される技術の任意のものは、その技術がプロセスと連関して具体的に説明されるか否かを問わず、説明されるプロセス又は他のプロセス内に組み込まれ得る。開示されるプロセスは、さらには、他のデバイス、コンポーネント、もしくはシステム上で、又は、他のデバイス、コンポーネント、もしくはシステムにより実施されることが、そのようなデバイス、コンポーネント、又はシステムが本明細書において説明されるか否かを問わずにある。これらのプロセスは、さらには、各種の手立てで具現化され得る。例えば、それらのプロセスは、例えば、プロセッサー読み取り可能ストレージメディア内に格納されるプロセッサー読み取り可能命令として、製造品で具現化される、又は、コンピューター実装プロセスとして実施されることがある。代替の例として、これらのプロセスは、プロセッサー実行可能命令としてエンコードされ、通信メディアを介して送信され得る。

【００３８】

[0041]図４は、ＩｏＴ認証のためのプロセス（４２０）に対する例データフローを例示する線図である。図４、及び、本明細書においての図４の対応する説明は、本開示の範囲を制限しない例示的な目的のための例プロセスを例示する。

【００３９】

[0042]例示される例において、最初にステップ４２１が発生する。ステップ４２１で、ＩｏＴハブ４５１は、少なくとも１つのＩｏＴデバイス（例えば、ＩｏＴデバイス４４１）の予期される条件と関連付けられるセキュリティー規則のセットを格納する。一部の例において、セキュリティー規則のセットは、少なくとも１つのＩｏＴデバイス（例えば、ＩｏＴデバイス４４１）と関連付けられるＩｏＴデータの評価に基づく。格納されるセキュリティー規則のセットは、例えば、ＩｏＴデバイスのタイプに基づいて、特定の展開コンテキスト、及び他の要因に基づき、異なることがある。セキュリティー規則のセットは、下記で（下記のステップ４２４で収集されるＩｏＴデータの論考の後に）より詳細に論考される。

【００４０】

[0043]示されるように、ステップ４２２が、次に、一部の例において発生する。ステップ４２２において、構成要求が、デバイスポータルサービス４１３により生成され得るものであり、次いで、構成要求は、デバイスポータルサービス４１３からＩｏＴハブ４５１に伝達され得る。構成要求は、ＩｏＴハブ４５１内に格納されるセキュリティー規則のセットを調整することと関連付けられ得る。一部の例において、構成要求は、セキュリティー規則のセットを、セキュリティー規則の調整されたセットに変更するようにとの要求である。構成要求は、異なる例において、異なる手立てで作成され得る。一部の例において、セキュリティー規則の既定セットが使用される基本モードが存し、さらには、ユーザーが構成要求を作成してセキュリティー規則の既定セットを変更することができる詳細設定が存する。示されるように、ステップ４２３が、次に、一部の例において発生する。ステップ４２３で、ＩｏＴハブ４５１は、ＩｏＴハブ４５１内に格納されるセキュリティー規則のセットを、ステップ４２２でデバイスポータルサービス４１３から受信される構成要求に基づいて調整することができる。

【００４１】

[0044]示されるように、ステップ４２４が、次に、一部の例において発生する。ステップ４２４で、ＩｏＴデバイス４４１は、環境、例えば、ＩｏＴデバイス４４１の付近においての環境から、環境データを受信及び収集し、ＩｏＴデバイス４４１の内部セキュリティー状態に関するデータを収集する。環境データは、テレメトリーデータ、ＩｏＴデバイス４４１が物理的に改ざんされたか否かを指示するデータ、及び／又は同類のものを含み得る。テレメトリーデータは、温度、湿度、ＩｏＴデバイスと関連付けられる場所の占有、地理位置情報、及び／又は同類のものを含み得る。ＩｏＴデバイス４４１の内部セキュリティー状態に関するデータは、オペレーティングシステム（ＯＳ）バージョン、アクティブプロセスの現在の状態、オープンポート、接続されるデバイスのインターネットプロトコル（ＩＰ）アドレス、及び／又は同類のものを含み得る。データは、ソフトウェアー入力、ハードウェアー入力、又は両方を介して収集され得る。

【００４２】

[0045]ステップ４２４で収集されるテレメトリーデータは、一部の例において、ＩｏＴデバイスがすでに収集しているテレメトリーを含み得る。例えば、温度センサーであるＩｏＴデバイスは、すでに、温度データを収集するように構成されていることがある。

【００４３】

[0046]ＩｏＴデバイス４４１は、物理的改ざんを検出する１つ又は複数の改ざんスイッチを有し得る。１つの例において、改ざんスイッチは、ＩｏＴデバイス４４１が物理的に改ざんされていないならばオフであり、改ざんスイッチは、ＩｏＴデバイス４４１が物理的に改ざんされたならばオンである。環境データは、改ざんスイッチがオンであるか、それともオフであるかに関しての指示を含み得る。実例として、一部の例において、ＩｏＴデバイス４４１は、２つの改ざんスイッチに接続されるカバーを有する。カバーが開かれるならば、両方の改ざんスイッチはオンに変わる。

【００４４】

[0047]一部の例において、ＩｏＴデバイス４４１は、環境データと、ＩｏＴデバイス４４１の内部セキュリティーに関するデータとを収集するソフトウェアーエージェントを含

み得る。一部の例において、ＩｏＴデバイス４４１は、環境及び／又は内部状態データを収集するためにＩｏＴデバイス４４１上に展開されるソフトウェアーデータ収集エージェントを有する。一部の例において、ＩｏＴデバイスの一部又はすべては、ＩｏＴデバイスから環境及び／又は内部状態データを収集するためにＩｏＴデバイス上に展開されるソフトウェアーデータ収集エージェントを有する。

【００４５】

[0048]ＩｏＴハブ４５１内に格納されるセキュリティー規則のセットは、ＩｏＴデバイス（例えば、４４１、及び／又は、図３の３４１～４３４）の標準のビヘイビアーのモデルに基づく。このモデルは、ＩｏＴデバイスの、これらのデバイスが標準の条件のもとで作動している間の状態を表し得る。一部の例において、セキュリティー規則のセットは、構成可能なＩｏＴデバイスモデルとして働く。規則のセットは、攻撃もしくは他のセキュリティー侵入、又はセキュリティー上の脅威が発生するならば、規則のセットが違反されるように定義され得る。

【００４６】

[0049]例えば、ＩｏＴデバイスは、２つのカテゴリー：サイバー攻撃及び物理的攻撃に分類され得る、様々なタイプのセキュリティー攻撃を被りやすいことがある。サイバー攻撃は、オペレーティングシステム、ネットワークインフラストラクチャー、接続、及びデータについてなど、デバイスのサイバープロパティーについての攻撃を含む。物理的攻撃は、デバイスの物理的改ざん、デバイスのデータ生成要素の操作、再配置、及び同類のものなどの攻撃を含む。一部の例において、セキュリティー規則のセットは、セキュリティー規則のセットの違反が、１つ又は複数のＩｏＴデバイスについての攻撃（例えば、物理的攻撃又はサイバー攻撃）の少なくとも可能性を指示するように、生成又は調整される。よって、これらの攻撃のいずれかが発生すると、規則のセットの違反が、１つの例において発生するはずであり、なぜならば、デバイスから収集されるデータは、次いで、モデルに反することになるからである。モデルは、テレメトリーデータに対する１つ又は複数のパターンを含み得る。

【００４７】

[0050]よって、セキュリティー規則のセットは、満たされないならばセキュリティー上の脅威の可能性を指示し得る、標準の動作条件を定義し得る。例えば、セキュリティー規則のセットは、データ要素のうちの１つ又は複数が、予期される範囲の外側であるならば違反され得る。例えば、セキュリティー規則のセットは、温度が所定の範囲内にあるということ、改ざんスイッチがオフであるということ、所定の、ブラックリストに載っているプロセスが走っていないということ、及び／又は同類のことを必要とし得る。予期される範囲、又は、予期される離散値は、時刻及び他の要因に左右され得る。一部の例において、温度又は同類のものなどの各々のタイプのデータを、予期される範囲（又は、予期される離散値）と個々に、単純に比較するのではなく、セキュリティー規則のセットは、モデルに基づいて一体で考慮される、複数個のタイプのデータに基づく。実例として、一部の例において、予期される範囲より上の環境内の温度は、さらには環境内の占有が存しない限り、セキュリティー規則の違反を結果的に生じさせないことがある。

【００４８】

[0051]一部の例において、セキュリティー規則のセットは、ＩｏＴデバイスにより収集される、環境及び内部セキュリティーデータのモデルに基づき、その場合、モデルは、予期されるデータの「ゴールデン」イメージを効果的に提供する。ゴールデンイメージは、何らの侵入又はセキュリティー上の脅威もない標準の動作条件においてのＩｏＴデバイスの標準のビヘイビアーを反映し得る。受信されるＩｏＴデータに基づいて、一部のアスペクトがゴールデンイメージと異なるならば、規則のセットは、他のデータに依存して、違反されるとみなされ得る。実例として、適宜、モール内の特定のルームの占有センサーに対するゴールデンイメージに対して、占有センサーは、誰もモール内に存在することが予期されない所定の時間の間は占有を示さないはずである。しかしながら、規則は、例えば、モールのゲートが開いており、警備員が依然としてモール内に存在するならば、予期さ

れない時間での占有は、セキュリティー規則のセットの違反をトリガーしないということを指定することができる。一部の例において、複数個のＩｏＴデバイスからのデータが、モデル、及び、セキュリティー規則のセットに関与させられることが、規則のセットが違反されているか否かを決定するために行われ得る。複数個のＩｏＴデバイスからのデータを使用することにより、モデルが１つのＩｏＴデバイスを基にする場合より全体論的な、デバイス動作、及び動作環境、及び侵入のモデルが使用され得る。

【００４９】

[0052]一部の例において、セキュリティー規則のセットは、プロセスのホワイトリスト、及び、プロセスのブラックリストの、１つ又は両方を含む。プロセスのホワイトリスト及びブラックリストは、ＩｏＴデバイスがマルウェアーにより感染されているか否かを決定することにおいて有用であり得る。プロセスの「ホワイトリスト」は、承認済みのプロセスのリストを指し、プロセスの「ブラックリスト」は、禁止されているプロセスのリストを指す。

【００５０】

[0053]一部の例において、収集されるテレメトリーデータを含む、収集されるＩｏＴデータは、セキュリティー規則のセットを作成又は調整するために、モデルを構築することをアシストするために使用され得る。

【００５１】

[0054]示されるように、ステップ４２５が、次に、一部の例において発生する。ステップ４２５で、ＩｏＴデバイス４４１は、ＩｏＴハブ４５１にデータを送るべきか否かに関して決定を行い得る。一部の例において、ステップ４２５で、ＩｏＴデバイス４４１は、単純に、ＩｏＴハブ４５１にデータのすべてを常に送ると決定する。一部の例において、データは、データのタイプのより多くのもののうちの１つに基づくしきい値が超えられていることを基に、送られるのみである。

【００５２】

[0055]実例として、一部の例において、ＩｏＴデバイス４４１は、検出される温度が１８．３３～２３．８９℃（華氏６５～７５度）などの前もって決定された範囲の外側である場合にのみ、温度データを送ると決定する。一部の例において、温度が１８．３３～２３．８９℃（華氏６５～７５度）の範囲の外側であるという事実は、それ自体としては、セキュリティー規則の違反ではなく、ＩｏＴデバイス４４１は、この例において、セキュリティー規則のセットが違反されるか否かに関して決定を行うのではなく、温度が特定の範囲の外側であることを基に温度データを送るのみであり、そのことに対して、それゆえに、他の要因に依存する、セキュリティー規則のセットの違反が存することがある。

【００５３】

[0056]示されるように、ステップ４２６が、次に、一部の例において、ステップ４２５での決定が肯定的であるときに発生する。ステップ４２６で、ＩｏＴデータが、ＩｏＴデバイス４４１からＩｏＴハブ４５１に伝達され得る。対照的に、ステップ４２６での決定が否定的であるならば、他の処理が再開される。

【００５４】

[0057]示されるように、ステップ４２７が、次に、ステップ４２６の後に、一部の例において発生する。ステップ４２７で、ＩｏＴハブ４５１は、ステップ４２６で受信されたＩｏＴデータに基づいて、ＩｏＴハブ４５１内に格納されるセキュリティー規則のセットが違反されているかどうかに関して決定を行う。一部の例において、ステップ４２７での決定は、構成可能なＩｏＴデバイスモデルとの、集約されたＩｏＴデバイスデータの比較である。

【００５５】

[0058]示されるように、ステップ４２８が、次に、一部の例において発生する。ステップ４２８で、ＩｏＴハブ４５１は、警告をデバイスポータルサービス４１３に、ステップ４２７での決定に基づいて選択的に送る。ステップ４２７で、規則のセットが違反されたということが決定されたならば、ＩｏＴハブ４５１は、警告をデバイスポータルサービス

４１３に伝達する。代わりにステップ４２７で、規則のセットが違反されなかったということが決定されたならば、ＩｏＴハブ４５１は、警告を送り出さない。

【００５６】

[0059]ＩｏＴデバイス４４１がクラウドから切断された様態となるならば、データはＩｏＴデバイス４４１から収集され得ないが、ＩｏＴデバイス４４１がクラウドから切断されるという事実は、それ自体が情報の一形態であり、一部の例において、警告が、ＩｏＴデバイス４４１がクラウドから切断されていることから結果的に生じることがある。

【００５７】

[0060]一部の例において、セキュリティー規則のセットは、時間の経過に伴ってさらに調整されることが、誤検知を減らすため、及び、そうでなければ検出されないことがある攻撃を首尾よく検出するための両方で行われ得る。一部の例において、ＩｏＴハブ４５１は、異常から学習し、セキュリティー規則のセットを時間の経過に伴って変更すること、及び、時間の経過に伴って学習することにより適応する、学習層を含む。

【００５８】

[0061]一部の例において、直接ＩｏＴハブ４５１にＩｏＴデータを送るのではなく、ＩｏＴデバイス４４１は、ゲートウェイデバイス（例えば、図３のゲートウェイデバイス３１１又は３１２）にデータを送る。一部の例において、ＩｏＴデバイス４４１ではなくゲートウェイデバイスが、ＩｏＴハブ４５１にＩｏＴデータを送るべきか否かに関して決定を行う。一部の例において、複数個の異なるＩｏＴデバイス（例えば、図３の３４１～３４３）は、１つのゲートウェイデバイスにＩｏＴデータを送り、そのゲートウェイデバイスは、ＩｏＴハブ４５１に転送すべきかどうか、及び、どのＩｏＴデータを転送すべきかを決定する前に、データを集約する。

【００５９】

[0062]一部の例において、ステップ４２８で、警告を単純に送り出すのではなく、決定され得る限りの、例えば、攻撃又は脅威の性質に関する情報を含む、他の詳細が、さらには、警告とともに、ＩｏＴハブ４５１からデバイスポータルサービス４１３に伝達される。例えば、ＩｏＴハブ４５１が、ＧＰＳによって、デバイスが動かされたということを、及び、他のＩｏＴデータから、マルウェアーがインストールされたということを両方決定するならば、この攻撃の性質が、ＩｏＴハブ４５１からデバイスポータルサービス４１３に伝達され得るものであり、そのことは、潜在的可能性として、これらの２つのイベントのうちの１つのみが発生した場合とは異なるシナリオである。複数個のＩｏＴデバイスからの集約データは、さらには、適用可能なときに、ＩｏＴハブ４５１からデバイスポータルサービス４１３への通信において、セキュリティー上の脅威の性質をさらに説明するために使用され得る。

【００６０】

[0063]図５は、ＩｏＴ認証のためのプロセス（５９０）の例を例示する論理フロー線図である。１つの例において、プロセス５９０は、図１のＩｏＴハブ３５１などのＩｏＴハブにより実施される。開始ブロックの後、プロセスはブロック５９１に進む。ブロック５９１で、少なくとも１つのＩｏＴデバイスの予期される条件と関連付けられるセキュリティー規則のセットが格納される。プロセスは、次いで、ブロック５９２に移る。ブロック５９２で、少なくとも１つのＩｏＴデバイスと関連付けられるＩｏＴデータが受信される。ＩｏＴデータは、少なくとも２つの異なるタイプのデータを含む集約されたデータであり得る。プロセスは、次いで、判断ブロック５９３に進む。

【００６１】

[0064]判断ブロック５９３で、決定が、ＩｏＴデータに基づいて、セキュリティー規則のセットが違反されているかどうかに関して行われる。判断ブロック５９３での決定が否定的であるならば、プロセスはリターンブロックに進み、そこで、他の処理が再開される。代わりに、判断ブロック５９３での決定が肯定的であるならば、プロセスはブロック５９４に前進し、そこで、警告が送られる。実例として、一部の例において、警告はデバイスポータルサービスに送られる。プロセスは、次いで、リターンブロックに進み、そこで

、他の処理が再開される。この手立てにおいて、警告は、判断ブロック５９３での決定に基づいて選択的に送られる。

【００６２】

結論

[0065]上記の、発明を実施するための形態は、本技術の所定の例を説明し、思索される最良の形態を説明しているが、たとえどのように詳細に上記のものが本文に出ていても、本技術は、多くの手立てで実践され得る。詳細は、実装形態において変動し得るが、一方で、それでもなお、本明細書において説明される本技術により包含される。上記で特記されたように、本技術の所定の機能又は態様を説明するときに使用される特定の専門用語は、その専門用語が関連付けられる何らかの具体的な特性、機能、又は態様に限定されるように、その専門用語が本明細書において再定義されているということを暗黙に示すと受け止められるべきではない。一般的には、後に続く特許請求の範囲において使用される用語は、発明を実施するための形態が、そのような用語を明示的に定義しない限り、本明細書において開示される具体的な例に本技術を制限すると解されるべきではない。よって、本技術の実際の範囲は、開示される例のみではなく、さらには、本技術を実践又は実装するすべての等価の手立てを包含する。

【図１】

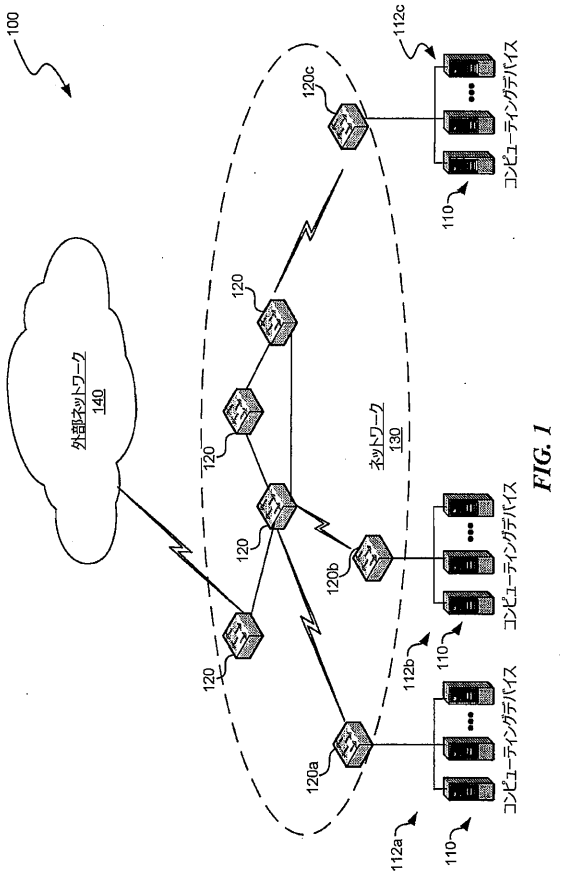

FIG. 1

【図２】

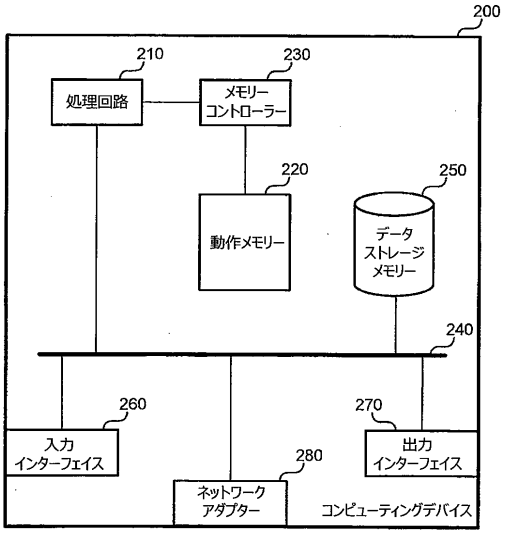

FIG. 2

【図３】

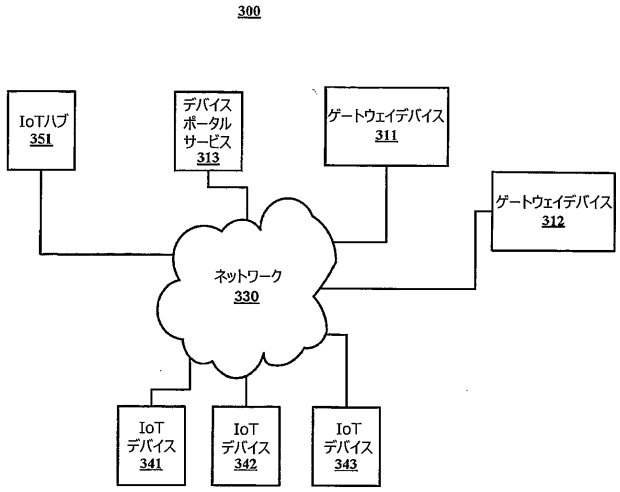

FIG. 3

【図４】

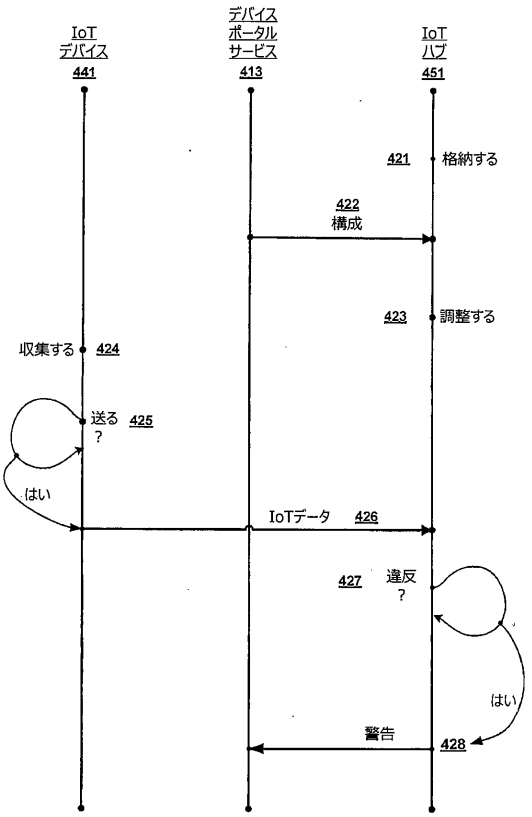

FIG. 4

【図５】

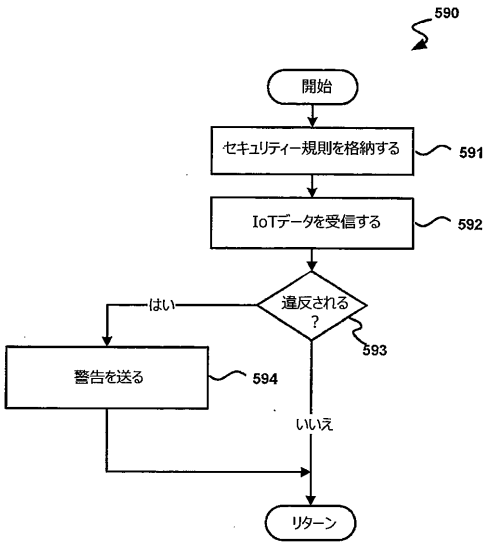

FIG. 5

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2017/058926

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/06 G06F21/55 H04W4/00
ADD. H04L12/26

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 H04W G06F

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, WPI Data, COMPENDEX, INSPEC, IBM-TDB

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2016/140912 A1 (QUALCOMM INC [US]) 9 September 2016 (2016-09-09) abstract; figures 9, 11, 12, 14-17; tables 1-3 paragraphs [0008], [0009] paragraphs [0098] - [0101] paragraphs [0111] - [0115] paragraphs [0120] - [0126] paragraphs [0128] - [0130] ----- -/--	1-15

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
11 December 2017	18/12/2017

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Schossmaier, Klaus

1

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2017/058926

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2015/271033 A1 (SRIVASTAVA ASHOK N [US] ET AL) 24 September 2015 (2015-09-24) abstract; figures 1, 4, 5A, 5B, 6, 7A, 7B, 7G paragraphs [0001], [0011], [0012] paragraphs [0041] - [0043] paragraphs [0046], [0049], [0053] paragraphs [0058] - [0061] paragraphs [0066], [0071], [0081] -----	1-15
X	US 2015/150124 A1 (ZHANG TAO [US] ET AL) 28 May 2015 (2015-05-28) abstract; figures 1, 4-8 paragraphs [0025] - [0027] paragraphs [0061], [0062], [0065] paragraphs [0084] - [0094] -----	1-15

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2017/058926

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2016140912 A1	09-09-2016	CN 107409073 A	28-11-2017
		US 2016261465 A1	08-09-2016
		WO 2016140912 A1	09-09-2016
US 2015271033 A1	24-09-2015	NONE	
US 2015150124 A1	28-05-2015	CN 105765940 A	13-07-2016
		EP 3075130 A1	05-10-2016
		US 2015150124 A1	28-05-2015
		WO 2015081034 A1	04-06-2015

Form PCT/ISA/210 (patent family annex) (April 2005)

フロントページの続き

(81)指定国・地域　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,DJ,DK,DM,DO,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,GT,HN,HR,HU,ID,IL,IN,IR,IS,JO,JP,KE,KG,KH,KN,KP,KR,KW,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

（特許庁注：以下のものは登録商標）
１．ＺＩＧＢＥＥ

(74)代理人　100147991
弁理士　鳥居　健一
(72)発明者　サミュエル，アルジマンド
アメリカ合衆国　ワシントン州　９８０５２－６３９９　レッドモンド　ワン　マイクロソフト　ウェイ，マイクロソフト　テクノロジー　ライセンシング，エルエルシー