(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6824140号
(P6824140)
(45)発行日　令和3年2月3日(2021.2.3)　(24)登録日　令和3年1月14日(2021.1.14)

(51)Int.Cl.　F I
G06F 21/62 (2013.01)　G06F 21/62 363

請求項の数 19　外国語出願　(全 23 頁)

(21)出願番号　特願2017-211626(P2017-211626)
(22)出願日　平成29年11月1日(2017.11.1)
(65)公開番号　特開2018-109949(P2018-109949A)
(43)公開日　平成30年7月12日(2018.7.12)
審査請求日　令和2年8月17日(2020.8.17)
(31)優先権主張番号　15/394,929
(32)優先日　平成28年12月30日(2016.12.30)
(33)優先権主張国・地域又は機関
米国(US)

早期審査対象出願

(73)特許権者　000006013
三菱電機株式会社
東京都千代田区丸の内二丁目７番３号
(74)代理人　100110423
弁理士　曾我　道治
(74)代理人　100111648
弁理士　梶並　順
(74)代理人　100122437
弁理士　大宅　一宏
(74)代理人　100147566
弁理士　上田　俊一
(74)代理人　100161171
弁理士　吉田　潤一郎

最終頁に続く

(54)【発明の名称】プライバシー保護分析を集約データに用いるシステムおよびそのための方法及び記憶媒体

(57)【特許請求の範囲】
【請求項１】
集約データの分析的有用性を維持しながら該集約データのプライバシーが保護されるように該集約データを第三者に送信するシステムであって、
機密デバイス及び非機密デバイスの或る時間帯にわたって収集された時系列データを含む、複数のセンサーから生成された前記集約データを受信する送受信機であって、前記各センサーは、前記時間帯内の一組の時点においてデータを検知するものと、
前記送受信機と通信するプロセッサと、
前記プロセッサに結合され、実施するために前記プロセッサによって実行可能なプログラム命令を記憶するメモリと、
前記プロセッサが、
オフラインイントレーニングステージを、
前記集約データを生成した前記機密デバイスと同じデバイスタイプの機密デバイスから生成されたデータから、記憶された履歴統計寄与度データを入手すること、によって実行し、前記各機密デバイスの前記記憶された履歴統計寄与度は、前記時間帯内の前記各時点における前記機密デバイスの状態に応じた前記集約データに対応し、
リアルタイムステージを、
前記時間帯内の前記各時点において前記集約データに寄与する前記機密デバイスの状態を求めることと、
前記各時点における前記機密デバイスの前記求められた状態に基づいて、前記各時

点における前記集約データに対する前記機密デバイスの対応する記憶された履歴統計寄与度を前記メモリから選択し、対応する記憶された前記履歴統計寄与度は、前記機密デバイスの寄与度の平均及び分散を含み、前記各機密デバイスは、ユーザーによって求められた最大分散を含むようになっている、ことと、

或る時点について選択された、前記記憶された履歴統計寄与度を、該対応する時点における前記集約データの値から減算し、スケーリングされた雑音を加算して、変更された集約データを生成し、変更された集約データの分析的有用性を維持することと、

によって実行するように構成され、

前記変更された集約データを、通信チャネルを介して前記第三者に送信する送信機と、

を備える、システム。

【請求項２】

前記時点について選択された、前記記憶された履歴統計寄与度を、前記対応する時点における前記集約データの前記値から減算することは、前記変更された集約データの分析的有用性を維持しながら前記集約データのプライバシーが保護されるように、前記集約データを変更して、前記変更された集約データを生成する、請求項１に記載のシステム。

【請求項３】

前記減算することは、

前記時点における前記集約データの前記値から前記平均を減算し、前記機密デバイスの前記最大分散と前記時点における前記機密デバイスの前記分散との間の差の関数としてスケーリングされた雑音を加算して、前記変更された集約データを生成することを含む、請求項１に記載のシステム。

【請求項４】

前記プロセッサが、

前記時点における前記集約データの値から前記平均を減算して、前記変更された集約データを生成すること、を更に行うように構成されている、請求項１に記載のシステム。

【請求項５】

前記集約データは、ユーザーによる少なくとも１つのエネルギー消費体の使用量を含み、前記少なくとも１つエネルギー消費体は、構造体、該構造体の一部分、電子デバイス、エネルギー消費デバイス若しくは電力消費デバイス、又はそれらの或る組み合わせを含むようになっている、請求項１に記載のシステム。

【請求項６】

集約データの分析的有用性を維持しながら該集約データのプライバシーが保護されるように該集約データを第三者に送信する方法であって、

機密デバイス及び非機密デバイスの或る時間帯にわたって収集された時系列データを含む、複数のセンサーから生成された前記集約データを、送受信機を用いて受信することであって、前記各センサーは、前記時間帯内の一組の時点においてデータを検知することと、

前記送受信機及びメモリと通信するプロセッサを用い、実施するために前記プロセッサによって実行可能なプログラム命令を記憶することと、

オフライントレーニングステージを、

前記集約データを生成した前記機密デバイスと同じデバイスタイプの機密デバイスを含むデバイスから生成されたデータから、記憶された履歴デバイスデータ及び履歴データ統計寄与度データを入手すること、

によって実行することであって、前記各機密デバイスの前記記憶された履歴統計寄与度は、前記時間帯内の前記各時点における前記機密デバイスの状態に応じた前記集約データに対応することと、

リアルタイムステージを、

前記時間帯内の前記各時点において前記集約データに寄与する前記機密デバイスの状態を求めることと、

前記各時点における前記機密デバイスの前記求められた状態に基づいて、前記各時点

における前記集約データに対する前記機密デバイスの対応する記憶された履歴統計寄与度を前記メモリから選択し、対応する記憶された前記履歴統計寄与度は、前記機密デバイスの寄与度の平均及び分散を含み、前記各機密デバイスは、ユーザーによって求められた最大分散を含むようになっている、ことと、

或る時点について選択された、前記記憶された履歴統計寄与度を、該対応する時点における前記集約データの値から減算し、スケーリングされた雑音を加算して、変更された集約データを生成し、変更された集約データの分析的有用性を維持することと、

によって実行することと、

送信機を用いて、前記変更された集約データを、通信チャネルを介して前記第三者に送信することと、

を含む、方法。

【請求項７】

前記時点における前記集約データの値から前記平均を減算して、前記変更された集約データを生成すること、を更に含む、請求項６に記載の方法。

【請求項８】

前記各機密デバイスは、ユーザーによって求められた最大分散を含み、

前記時点における前記集約データの値から前記平均を減算し、前記機密デバイスの前記最大分散と前記時点における前記機密デバイスの前記分散との間の差の関数としてスケーリングされた雑音を加算して、前記変更された集約データを生成する、請求項６に記載の方法。

【請求項９】

前記集約データは、ユーザーが発信源であり、計測デバイスの消費者側に配置された該計測デバイスを用いて収集されたユーザーエネルギーデータである、請求項６に記載の方法。

【請求項１０】

前記記憶された履歴デバイスデータ及び履歴データ統計寄与度データは、デバイスマニュアル又はデバイス製品仕様から取得されたデータと、前記集約データを処理して前記変更された集約データを取得する前に、前記デバイスからの前記複数のセンサーから生成されたデータとを含む、請求項６に記載の方法。

【請求項１１】

少なくとも１つのユーザー入力インターフェースの表面上に提供されて前記プロセッサによって受信されるユーザー入力によって、前記送受信機によって受信される前記集約データの送信を開始すること、

を更に含む、請求項６に記載の方法。

【請求項１２】

少なくとも１つのユーザー入力インターフェースの表面上に提供されて前記プロセッサによって受信されるユーザー入力を用いることを更に含み、該ユーザー入力は、高められたプライバシーレベルとより低い歪みレベルとの間のトレードオフを行うために分散等化のレベルを選択する前記リアルタイムステージへの入力としてのトレードオフパラメーターに関係する、請求項６に記載の方法。

【請求項１３】

方法を実行するコンピューターによって実行可能なプログラムが具現化された非一時的コンピューター可読記憶媒体であって、前記方法は、集約データの分析的有用性を維持しながら該集約データのプライバシーが保護されるように該集約データを第三者に送信するものであり、前記方法は、

機密デバイス及び非機密デバイスの或る時間帯にわたって収集された時系列データを含む、複数のセンサーから生成された前記集約データを取得することであって、前記各センサーは、前記時間帯内の一組の時点においてデータを検知し、前記集約データは、第三者計測デバイスのユーザー側に配置されたユーザー計測デバイス又はユーザー測定デバイスを含む複数のセンサーを用いてユーザーによって収集されたユーザーエネルギーが発信源

であるものと、
プロセッサを用いて、オフライントレーニングステージを、
前記集約データを生成した前記機密デバイスと同じデバイスタイプの機密デバイスから生成されたデータから、記憶された履歴統計寄与度データを入手すること、によって実行することであって、前記各機密デバイスの前記記憶された履歴統計寄与度は、前記時間帯内の前記各時点における前記機密デバイスの状態に応じた前記集約データに対応することと、
前記プロセッサを用いて、リアルタイムステージを、
前記時間帯内の前記各時点において前記集約データに寄与する前記機密デバイスの状態を求めることと、
前記各時点における前記機密デバイスの前記求められた状態に基づいて、前記各時点における前記集約データに対する前記機密デバイスの対応する記憶された履歴統計寄与度を該非一時的コンピューター可読記憶媒体から選択し、対応する記憶された前記履歴統計寄与度は、前記機密デバイスの寄与度の平均及び分散を含み、前記各機密デバイスは、ユーザーによって求められた最大分散を含むようになっている、ことと、
或る時点について選択された、前記記憶された履歴統計寄与度を、該対応する時点における前記集約データの値から減算し、スケーリングされた雑音を加算して、変更された集約データを生成し、変更された集約データの分析的有用性を維持することと、
によって実行することと、
ユーザーがユーザー送信機を用いて、前記変更された集約データを、通信チャネルを介して前記第三者に送信することと、
を含む、非一時的コンピューター可読記憶媒体。
【請求項１４】
前記減算することは、
前記時点における前記集約データの前記値から前記平均を減算し、前記機密デバイスの前記最大分散と前記時点における前記機密デバイスの前記分散との間の差の関数としてスケーリングされた雑音を加算して、前記変更された集約データを生成することを含む、請求項１３に記載の非一時的コンピューター可読記憶媒体。
【請求項１５】
前記方法は、
前記時点における前記集約データの値から前記平均を減算して、前記変更された集約データを生成すること、
を更に含む、請求項１３に記載の非一時的コンピューター可読記憶媒体。
【請求項１６】
前記方法は、少なくとも１つのユーザー入力インターフェースの表面上に提供されて前記プロセッサによって受信されるユーザー入力を用いることを更に含み、該ユーザー入力は、高められたプライバシーレベルとより低い歪みレベルとの間のトレードオフを行うために分散等化のレベルを選択する前記リアルタイムステージへの入力としてのトレードオフパラメーターに関係する、請求項１３に記載の非一時的コンピューター可読記憶媒体。
【請求項１７】
前記時点について選択された、前記記憶された履歴統計寄与度を、前記対応する時点における前記集約データの前記値から減算することは、前記変更された集約データの分析的有用性を維持しながら前記集約データのプライバシーが保護されるように、前記集約データを変更して、前記変更された集約データを生成する、請求項１３に記載の非一時的コンピューター可読記憶媒体。
【請求項１８】
集約データの分析的有用性を維持しながら該集約データのプライバシーが保護されるように該集約データを第三者に送信するシステムであって、
機密デバイス及び非機密デバイスの或る時間帯にわたって収集された時系列データを含む、複数のセンサーから生成された前記集約データを受信する送受信機であって、前記各

センサーは、前記時間帯内の一組の時点においてデータを検知するものと、
前記送受信機と通信するプロセッサと、
前記プロセッサに結合され、実施するために前記プロセッサによって実行可能なプログラム命令を記憶するメモリと、
前記プロセッサが、
オフライントレーニングステージを、
前記集約データを生成した前記機密デバイスと同じデバイスタイプの機密デバイスから生成されたデータから、記憶された履歴統計寄与度データを入手すること、によって実行し、前記各機密デバイスの前記記憶された履歴統計寄与度は、前記時間帯内の前記各時点における前記機密デバイスの状態に応じた前記集約データに対応し、
リアルタイムステージを、
前記時間帯内の前記各時点において前記集約データに寄与する前記機密デバイスの状態を求めることと、
前記各時点における前記機密デバイスの前記求められた状態に基づいて、前記各時点における前記集約データに対する前記機密デバイスの対応する記憶された履歴統計寄与度を前記メモリから選択し、対応する記憶された前記履歴統計寄与度は、前記各時点における前記集約データに対する前記機密デバイスの寄与度の平均及び分散を含み、前記各機密デバイスは、ユーザーによって求められた最大分散を含むようになっている、ことと、
対応する時点における前記集約データの値から前記平均を減算し、前記機密デバイスの最大分散と前記時点における前記機密デバイスの分散との間の関数としてスケーリングされた雑音を加算して、変更された集約データを生成し、変更された集約データの分析的有用性を維持することと、
によって実行するように構成され、
前記変更された集約データを、通信チャネルを介して前記第三者に送信する送信機と、
を備える、システム。
【請求項１９】
集約データの分析的有用性を維持しながら該集約データのプライバシーが保護されるように該集約データを第三者に送信し、前記集約データは少なくとも１つのエネルギー消費デバイスの予防保守に基づく少なくとも１つのエネルギー消費デバイスの動作の制御を援助するシステムであって、
機密デバイス及び非機密デバイスの或る時間帯にわたって収集された時系列データを含む、複数のセンサーから生成された前記集約データを受信する送受信機であって、前記各センサーは、前記時間帯内の一組の時点においてデータを検知するものと、
前記送受信機と通信するプロセッサと、
前記プロセッサに結合され、実施するために前記プロセッサによって実行可能なプログラム命令を記憶するメモリと、
前記プロセッサが、
オフライントレーニングステージを、
前記集約データを生成した前記機密デバイスと同じデバイスタイプの機密デバイスから生成されたデータから、記憶された履歴統計寄与度データを入手すること、によって実行し、前記各機密デバイスの前記記憶された履歴統計寄与度は、前記時間帯内の前記各時点における前記機密デバイスの状態に応じた前記集約データに対応し、
リアルタイムステージを、
前記時間帯内の前記各時点において前記集約データに寄与する前記機密デバイスの状態を求めることと、
前記各時点における前記機密デバイスの前記求められた状態に基づいて、前記各時点における前記集約データに対する前記機密デバイスの対応する記憶された履歴統計寄与度を前記メモリから選択し、対応する記憶された前記履歴統計寄与度は、前記機密デバイスの寄与度の平均及び分散を含み、前記各機密デバイスは、ユーザーによって求められた最大分散を含み、

対応する時点における前記集約データの値から前記平均を減算し、前記機密デバイスの最大分散と前記時点における前記機密デバイスの分散との間の関数としてスケーリングされた雑音を加算して、変更された集約データを生成し、変更された集約データの分析的有用性を維持することと、
によって実行するように構成され、
前記変更された集約データを、通信チャネルを介して前記第三者に送信する送信機であって、前記変更された集約データに基づいて、前記第三者は前記少なくとも１つのエネルギー消費デバイスの予防保守により、前記少なくとも１つのエネルギー消費デバイスの動作の制御を援助するものと、
を備える、システム。

【発明の詳細な説明】
【技術分野】
【０００１】
本開示は、集合体データストリームからユーザー機密情報の部分を除去する方法及びシステムに関し、より詳細には、集約データの分析的有用性を維持しながら第三者への送信前のユーザー集約データのプライバシーを保護することに関する。
【背景技術】
【０００２】
多くの消費者にとって、ユーザーデータの収集は、プライバシーの問題を提起する。なぜならば、そのようなデータは、ユーザーが機密であるとみなすことがある情報及び内密にしておきたいと思う情報に特に関連付けられているからである。消費者にとっての問題は、消費者サービスプロバイダーが、個人の行動及びライフスタイル（器具の使用、食事及び睡眠のパターン、居住パターン、家族の活動パターン等）、健康状態、家族構成、移動パターン等を含む消費者のプライベート情報にアクセスすることができるということである。消費者サービスプロバイダーによるデータの収集は、ユーザーの同意なしに行われる可能性もあれば、場合によっては、ユーザーにオプトアウトする機会を与えることなく行われる可能性もある。ユーザーのデータを収集する消費者サービスプロバイダーは、ユーザーが知ることなく、及び／又は、ユーザーが自身の個人のプライバシーに関する収集データの範囲を知ることなく、このデータを第三者に利用可能にする可能性がある。通常、消費者は、データを収集する自身の消費者サービスプロバイダーを信頼しているが、この消費者サービスプロバイダーが消費者の収集データを共有し得る第三者を信頼していない。
【０００３】
具体的には、消費者／ユーザーのプライバシーデータを保護するこの問題は、消費者／ユーザーの個人データへのサービスプロバイダー及び第三者のアクセス、特に、消費者に内密と考えられる個人情報の公開を制御することに向かう。
【０００４】
消費者の個人データを保護する幾つかの従来の解決策は、消費者のデータを第三者に公開する前に消費者のプライバシーデータを変更することを含む。そのような方法は、一般に、データの分析的有用性を維持しながら消費者のプライバシーデータを保護することを目的としたデータ匿名化方法と呼ばれる。
【０００５】
例えば、幾つかの方法は、エネルギーデータの分析的有用性を維持しながらエネルギーデータのプライバシーを保護するように、非侵入型器具負荷監視を用いて集合体エネルギーデータを変更する。しかしながら、そのような方法は、エネルギーを消費している電力消費デバイスの実際の状態を必要とする。具体的には、そのような方法は、デバイスの実際の状態、すなわち、エネルギーデータが収集される特定の時点において、デバイスがＯＮにされているのか又はＯＦＦにされているのかを必要とする。デバイスの実際の状態を必要とするこれらの従来の方法は、多くの問題を提起する。なぜならば、各クライアント用に、エネルギーを消費する各消費デバイスにセンサーを接続する必要があるからであり

、これは、経済的に実現不可能であるか又はプライバシー制約の観点から禁止されることさえあるからである。

【発明の概要】

【発明が解決しようとする課題】

【０００６】

したがって、データを生成するデバイスの実際の状態の使用を最小化又は回避することができるデータ匿名化方法が必要とされている。

【課題を解決するための手段】

【０００７】

本開示の実施の形態によれば、集約データの分析的有用性を維持しながら集約データのプライバシーが保護されるように、集約データを第三者に送信するシステム及び方法が提供される。

【０００８】

本開示の実施の形態は、集合体データストリームのプライバシーを維持することを提供し、この集合体データストリームは、幾つかの構成要素データストリームの全体である時系列信号である。集合体データストリームはユーザー／クライアントに関係し、このユーザー／クライアントから収集され、集合体データは、通常、分析のために１つ以上のサービスプロバイダーに公開されるので、プライバシーの問題が発生する。集合体データは、ユーザーによる電力消費体の使用量を含み、電力消費体は、構造体、構造体の一部分、電子デバイス、電力消費デバイス、又はそれらの或る組み合わせを含む。さらに、計測デバイスの消費者側に配置された当該計測デバイスを用いてユーザーエネルギーデータを収集することができる。

【０００９】

さらに、世帯から収集された集合体エネルギー消費データストリームを考えると、この世帯の居住者は、自身の器具のエネルギー消費パターンから機密であるライフスタイル及び行動の詳細が暴露されることを心配する場合がある。別の例は、工場から収集されたデータを含む場合があり、事業者／所有者は、とりわけ、それらの事業者／所有者の機械／プロセスのエネルギー消費パターンに関連し得るプロセスの詳細又は他のトレードシークレットがリークすることを心配する場合がある。ユーザー／クライアント及び／又はプロバイダー（複数の場合もある）の利益のために有用な分析を実行することができる場合、１つ以上のサービスプロバイダーによる分析のためのユーザー／クライアントのデータの収集は望ましい場合もある。

【００１０】

集約データの分析的有用性を維持しながら集約データのプライバシーを保護することに対処するために、本開示の幾つかの実施の形態は、機密デバイス及び非機密デバイスの或る時間帯にわたって収集された時系列データを含む複数のセンサーから生成された集約データを受信するステップを含み、各センサーは、上記時間帯内の一組の時点においてデータを検知する。集約データを生成した機密デバイスと同じデバイスタイプの機密デバイスを含むデバイスから生成されたデータから、記憶された履歴デバイスデータ及び履歴統計寄与度データを入手することによってプロセッサを介してオフラインレーニングステージを実行する。各機密デバイスの記憶された履歴統計寄与度は、時間帯内の各時点における機密デバイスの状態に応じた集約データに対応する。時間帯内の各時点において集約データに寄与する機密デバイスの状態を求めることと、各時点における機密デバイスの求められた状態に基づいて、各時点における集約データに対する機密デバイスの対応する記憶された履歴統計寄与度をメモリから選択することと、或る時点について選択された、記憶された履歴統計寄与度を、対応する時点における集約データの値から減算して、変更された集約データを生成することとによってリアルタイムステージを実行する。最後に、送信機を用いて、変更された集約データを、通信チャネルを介して第三者に送信する。

【００１１】

本発明者らは、上記概念の形成を通じて、機密情報を隠蔽し又は歪ませる代わりに、集

約データから機密情報を除去すべきであると認識した。この形成の間、本発明者らは、幾つかの特定の情報が未知であることを知った。例えば、第１に、本発明者らは、集約データに対する機密情報の寄与の量を知らなかった。第２に、本発明者らは、集約データに対する寄与度の関数がどのようなものであるかを知らなかった。

【００１２】

これらの２つの未知のものを有することをどのように克服するのかに対処している際に、本発明者らは、幾つかの用途では、機密器具及び他の器具のエネルギー使用を介した加法的組み合わせとしての寄与度の関数は、総エネルギー使用信号、すなわち集合体データに組み合わせることができることを発見した。それらの用途の場合、本発明者らは、ガウス階乗隠れマルコフモデル（ＦＨＭＭ）を適用してデータ、例えば機密器具の使用データをモデル化することができることを発見又は認識した。その結果、データ、すなわち集合体データを統計的に分析することができ、したがって、本発明者らは、種々の状態にあるデバイスの平均及び分散が判明するので、統計学を用いて機密データの寄与の量を求めるという第１の未知の質問に対する回答を見つけることができる。

【００１３】

第２の未知のものに関して、本発明者らは、センサーの基礎となる状態にわたって平均及び分散を等化することによって機密構成要素を統計的に抑制することができることを認識した。この場合、本発明者らは、集合体データの機密構成要素の基礎となる状態を、ビタビアルゴリズムを介して推定することができた。さらに、本発明者らは、推定された状態の平均を集合体データから減算することによって、等化された平均を実施することができた。最後に、本発明者らは、等化された分散は、最大分散と推定された状態の分散との間の差に等しい分散を有するガウス白色雑音を加えることによって対処することができることを発見した。

【００１４】

したがって、本発明者らは、２つの未知のものを有することを克服するとともに、集合体データストリームのプライバシーを保護する問題を解決することができる。特に、本発明者らは、集合体データの全体を構成する個々の構成要素、すなわち、機密構成要素を、幾つかの基礎となる状態によって決まる平均及び分散を有する独立したガウスプロセスとして合理的に統計モデル化することができる状況に対処することができる。具体的には、本開示の方法及びシステムは、集合体データストリームの機密構成要素の基礎となる状態の検出可能性を抑制する。

【００１５】

本開示の幾つかの利点は、本開示が、機密構成要素の基礎となる状態の平均及び分散を等化するプライバシーメカニズムを適用するようにして、機密構成要素の基礎となる状態の検出可能性を低減することを含むことができる。もう１つの利益は、多くの利益の中でもとりわけ、より良好なプライバシーとより少ない歪みとの間のトレードオフを行うために、トレードオフパラメーターをこのプライバシー保護メカニズムへの入力として用いて、分散等化（variance equalization）のレベルを選択することができるということである。本開示の更に別の態様は、プライバシー保護メカニズムの出力を、機密構成要素の基礎となる状態の低減された検出可能性を有する変更された集合体データストリームとすることができるということである。さらに、本開示は、集合体データ、及び機密構成要素の基礎となる状態のシーケンスとしてプライバシー保護メカニズムへの入力を用いる。

【００１６】

本開示の別の態様は、入力が機密構成要素の基礎となる状態のシーケンスを含む必要がなく、したがって、集合体データストリームのみからなる一変形形態を含むことができる。この場合、機密構成要素の基礎となる状態のシーケンスが、集合体データから最初に推定される。さらに、本開示の別の変形形態では、複数の機密構成要素を考慮することができ、上記手順を数回、場合によっては並列に適用することによって複数の機密構成要素に対処して、各機密構成要素の検出可能性を低減することができる。

【００１７】

本開示は、非限定的な例として、複数のセンサーから生成された集約データを受信するステップから開始することによって実施することができる。集約データは、機密デバイス及び非機密デバイスの或る時間帯にわたって収集された時系列データを含み、各センサーは、この時間帯内の一組の時点においてデータを検知する。次に、プロセッサを介してオフラインレーニングステージを実行するステップが続く。オフラインレーニングステージは、集約データを生成した機密デバイスと同じデバイスタイプの機密デバイスを含むデバイスから生成されたデータから、記憶された履歴デバイスデータ及び履歴統計寄与度データを入手することを含む。具体的には、各機密デバイスの記憶された履歴統計寄与度は、時間帯内の各時点における機密デバイスの状態に応じた集約データに対応する。

【００１８】

次のステップは、リアルタイムステージを実行することを含む。リアルタイムステージは、時間帯内の各時点において集約データに寄与する機密デバイスの状態を求めることを含む。次に、各時点における機密デバイスの求められた状態に基づいて、各時点における集約データに対する機密デバイスの対応する記憶された履歴統計寄与度をメモリから選択することが続く。続いて、或る時点について選択された、記憶された履歴統計寄与度を、対応する時点における集約データの値から減算して、変更された集約データが生成される。

【００１９】

最後に、送信機を用いて、変更された集約データを、通信チャネルを介して第三者に送信するステップが実行される。

【００２０】

本開示の一実施の形態によれば、集約データの分析的有用性を維持しながら集約データのプライバシーが保護されるように集約データを第三者に送信するシステムが提供される。このシステムは、機密デバイス及び非機密デバイスの或る時間帯にわたって収集された時系列データを含む、複数のセンサーから生成された集約データを受信する送受信機を備え、各センサーは、時間帯内の一組の時点においてデータを検知する。システムは、送受信機と通信するプロセッサを備える。システムは、プロセッサに結合され、実施するためにプロセッサによって実行可能なプログラム命令を記憶するメモリを備える。プロセッサは、オフラインレーニングステージを実行するように構成されている。オフラインレーニングステージは、集約データを生成した機密デバイスと同じデバイスタイプの機密デバイスから生成されたデータから、記憶された履歴統計寄与度データを入手することを含む。各機密デバイスの記憶された履歴統計寄与度は、時間帯内の各時点における機密デバイスの状態に応じた集約データに対応する。プロセッサは、リアルタイムステージを実行するように構成されている。このリアルタイムステージは、時間帯内の各時点において集約データに寄与する機密デバイスの状態を求めることを含む。このリアルタイムステージは、各時点における機密デバイスの求められた状態に基づいて、各時点における集約データに対する機密デバイスの対応する記憶された履歴統計寄与度をメモリから選択することを含む。さらに、このリアルタイムステージは、或る時点について選択された、記憶された履歴統計寄与度を、対応する時点における集約データの値から減算して、変更された集約データを生成することを含む。最後に、変更された集約データを、通信チャネルを介して第三者に送信するために送信機を用いることができる。

【００２１】

本開示の別の実施の形態によれば、集約データの分析的有用性を維持しながら集約データのプライバシーが保護されるように集約データを第三者に送信する方法が提供される。この方法は、機密デバイス及び非機密デバイスの或る時間帯にわたって収集された時系列データを含む、複数のセンサーから生成された集約データを、送受信機を用いて受信することを含み、各センサーは、時間帯内の一組の時点においてデータを検知する。この方法は、送受信機及びメモリと通信するプロセッサを用い、実施するためにプロセッサによって実行可能なプログラム命令を記憶することを含む。この方法は、集約データを生成した機密デバイスと同じデバイスタイプの機密デバイスを含むデバイスから生成されたデータ

から、記憶された履歴デバイスデータ及び履歴データ統計寄与度データを入手することを含むオフライントレーニングステージを実行することを含み、各機密デバイスの記憶された履歴統計寄与度は、時間帯内の各時点における機密デバイスの状態に応じた集約データに対応する。この方法は、時間帯内の各時点において集約データに寄与する機密デバイスの状態を求めることと、各時点における機密デバイスの求められた状態に基づいて、各時点における集約データに対する機密デバイスの対応する記憶された履歴統計寄与度をメモリから選択することと、次に、或る時点について選択された、記憶された履歴統計寄与度を、対応する時点における集約データの値から減算して、変更された集約データを生成することとを含むリアルタイムステージを実行することを含む。最後に、この方法は、送信機を用いて、変更された集約データを、通信チャネルを介して第三者に送信することを含む。

【００２２】

本開示の別の実施の形態によれば、方法を実行するコンピューターによって実行可能なプログラムが具現化された非一時的コンピューター可読記憶媒体が提供される。この方法は、集約データの分析的有用性を維持しながら集約データのプライバシーが保護されるように集約データを第三者に送信するものである。この方法は、機密デバイス及び非機密デバイスの或る時間帯にわたって収集された時系列データを含む、複数のセンサーから生成された集約データを取得することを含み、各センサーは、時間帯内の一組の時点においてデータを検知する。この方法は、プロセッサを用いて、オフライントレーニングステージを実行することを含む。このオフライントレーニングステージは、集約データを生成した機密デバイスと同じデバイスタイプの機密デバイスから生成されたデータから、記憶された履歴統計寄与度データを入手することを含む。各機密デバイスの記憶された履歴統計寄与度は、時間帯内の各時点における機密デバイスの状態に応じた集約データに対応する。この方法は、プロセッサを用いて、リアルタイムステージを実行することを含む。このリアルタイムステージは、時間帯内の各時点において集約データに寄与する機密デバイスの状態を求めることを含む。このリアルタイムステージは、各時点における機密デバイスの求められた状態に基づいて、各時点における集約データに対する機密デバイスの対応する記憶された履歴統計寄与度を非一時的コンピューター可読記憶媒体から選択することを含む。このリアルタイムステージは、或る時点について選択された、記憶された履歴統計寄与度を、対応する時点における集約データの値から減算して、変更された集約データを生成することを含む。最後に、この方法は、送信機を用いて、変更された集約データを、通信チャネルを介して第三者に送信することを含む。

【００２３】

更なる特徴及び利点は、以下の詳細な説明を添付図面とともに取り入れると、この詳細な説明からより容易に明らかになる。

【００２４】

ここに開示されている実施の形態は、添付図面を参照して更に説明される。示されている図面は、必ずしも一律の縮尺というわけではなく、その代わり、一般的に、ここに開示されている実施の形態の原理を示すことに強調が置かれている。

【図面の簡単な説明】

【００２５】

【図１Ａ】本開示の実施の形態による、集約データのプライバシーが保護されるように集約データを第三者に送信する方法のブロック図である。

【図１Ｂ】本開示の実施の形態による、集約データのプライバシーが保護されるように、集約データを、図１Ａの方法の構成要素を備える第三者に送信する、当該方法の概略図である。

【図１Ｃ】本開示の実施の形態による、図１Ａの方法の代替の適用態様又は実施態様を示す図１Ａの方法の概略図である。

【図２】本開示の実施の形態による、集合体データストリームを歪ませるために、変更された集合体データに雑音が加えられるガウス階乗隠れマルコフモデルＦＨＭＭ仮定を示す

別の方法のブロック図である。
【図３】本開示の実施の形態による、代替の適用態様又は実施態様を示す別の方法の概略図である。
【図４】本開示の実施の形態による、代替のコンピューター又はプロセッサを用いて実施することができる図１Ａの方法を示すブロック図である。
【発明を実施するための形態】
【００２６】
上記で明らかにされた図面は、ここに開示されている実施の形態を記載しているが、この論述において言及されるように、他の実施の形態も意図されている。この開示は、限定ではなく代表例として例示の実施の形態を提示している。ここに開示されている実施の形態の原理の範囲及び趣旨に含まれる非常に多くの他の変更及び実施の形態を当業者は考案することができる。
【００２７】
以下の説明は、例示的な実施の形態のみを提供し、本開示の範囲も、適用範囲も、構成も限定することを意図していない。そうではなく、例示的な実施の形態の以下の説明は１つ以上の例示的な実施の形態を実施することを可能にする説明を当業者に提供する。添付の特許請求の範囲に明記されているような開示された主題の趣旨及び範囲から逸脱することなく要素の機能及び配置に行うことができる様々な変更が意図されている。以下の説明では、実施の形態の十分な理解を提供するために、具体的な詳細が与えられる。しかしながら、当業者は、これらの具体的な詳細がなくても実施の形態を実施することができることを理解することができる。例えば、開示された主題におけるシステム、プロセス、及び他の要素は、実施の形態を不必要な詳細で不明瞭にしないように、ブロック図形式の構成要素として示される場合がある。それ以外の場合において、よく知られたプロセス、構造、及び技法は、実施の形態を不明瞭にしないように不必要な詳細なしで示される場合がある。さらに、様々な図面における同様の参照符号及び名称は、同様の要素を示す。
【００２８】
また、個々の実施の形態は、フローチャート、フロー図、データフロー図、構造図、又はブロック図として描かれるプロセスとして説明される場合がある。フローチャートは、動作を逐次的なプロセスとして説明することができるが、これらの動作の多くは、並列又は同時に実行することができる。加えて、これらの動作の順序は、再配列することができる。プロセスは、その動作が完了したときに終了することができるが、論述されない又は図に含まれない追加のステップを有する場合がある。さらに、特に説明される任意のプロセスにおける全ての動作が全ての実施の形態において行われ得るとは限らない。プロセスは、方法、関数、手順、サブルーチン、サブプログラム等に対応することができる。プロセスが関数に対応するとき、その関数の終了は、呼び出し側関数又はメイン関数へのその機能の復帰に対応することができる。
【００２９】
さらに、開示された主題の実施の形態は、少なくとも一部は手動又は自動のいずれかで実施することができる。手動実施又は自動実施は、マシン、ハードウェア、ソフトウェア、ファームウェア、ミドルウェア、マイクロコード、ハードウェア記述言語、又はそれらの任意の組み合わせを用いて実行することもできるし、少なくとも援助することができる。ソフトウェア、ファームウェア、ミドルウェア又はマイクロコードで実施されるとき、必要なタスクを実行するプログラムコード又はプログラムコードセグメントは、マシン可読媒体に記憶することができる。プロセッサ（複数の場合もある）が、それらの必要なタスクを実行することができる。
【００３０】
用語の定義
本開示に関する用語の定義によれば、分析的有用性という用語は、提供されたデータの各構成要素を検査するために分析的及び論理的な推論を用いてデータを評価するプロセスとして理解することができる。この分析形態は、データの研究分析を行うときに完了する

ことができる多くのステップのうちの１つのみとすることができる。様々なソースからのデータを収集し、検査し、その後、分析して、或る種の発見又は結論に達することができる。例えば、クライアントからの収集されたエネルギーデータに関するものは、クライアント及び／又はプロバイダー（複数の場合もある）の利益のための分析を含むことができる。対象となる特定の分析目的は、クライアントが受ける他のサービス及び／又はプロバイダーが実行する他のサービスを支援し得ること等の、クライアント及び／又はプロバイダーに有益な情報（例えば、予防保守／監視サービスを支援するか又はマーケティング情報を提供する器具動作情報）を提供することができる特定のエネルギー消費デバイス（複数の場合もある）（例えば、世帯内の器具（複数の場合もある））の使用パターンを求めることとすることができる。一方、事前には求められていない一般的な分析作業を後に可能にするために、エネルギー消費データの正確な表現をプロバイダー（複数の場合もある）に公開することも望ましい場合がある。

【００３１】

概観

図１Ａは、本開示の実施の形態による、集約データのプライバシーが保護されるように集約データを第三者に送信する方法のブロック図である。本開示のシステム及び方法は、プロセッサ及びメモリを有するコンピューター１１２を介して複数のセンサーから生成された集約データを受信するステップ１１０を含むことができる。集約データ１１０ＢＢは、機密デバイス及び非機密デバイスから或る時間帯にわたって収集された時系列データを含み、各センサーが、その時間帯内の一組の時点においてデータを検知するようになっている。集合体データは、送受信機と通信するデバイスへの無線又は有線で受信することができ、コンピューター可読メモリに記憶することができることが意図されている。集約データは最大でセグメント時間長の遅延までのリアルタイムデータを介して、プロセッサを介して収集することもできる。集合体データは、プロセッサに接続された検知装置を介して収集することができることが可能である。例えば、世帯エネルギー監視アプリケーションの場合、これは、或る時間にわたる総世帯エネルギー使用を記録するスマートメーターであってもよいし、或る他のタイプの測定デバイスであってもよい。

【００３２】

ステップ１１５は、集約データ１１０ＢＢを生成した機密デバイスと同じデバイスタイプの機密デバイスを含むデバイスから生成されたデータから、記憶された履歴デバイスデータ及び履歴統計寄与度データを入手することによって実行されるオフラインイントレーニングステージを含む。各機密デバイスの記憶された履歴統計寄与度は、時間帯内の各時点における機密デバイスの状態に応じた集約データ１１０ＢＢに対応する。

【００３３】

次にステップ１２０が続き、リアルタイムステージが、時間帯内の各時点において集約データに寄与する機密デバイスの状態を求めるサブステップ１２０Ａによって実行される。ここでは、デバイス状態と集合体エネルギーデータとの間の統計関係を記述するために、統計モデルが用いられる。集合体データは、特定の用途に応じて前処理されてもよい。

【００３４】

サブステップ１２０Ｂは、各時点における機密デバイスの求められた状態に基づいて、各時点における集約データに対する、機密デバイスの対応する記憶された履歴統計寄与度をメモリから選択する。次に、サブステップ１２０Ｃは、或る時点について選択された、記憶された履歴統計寄与度を、対応する時点における集約データの値から減算し、変更された集約データ１２０ＢＢを生成する。任意選択で、ステップ１２５は、数ある利益の中でもとりわけ、より良好なプライバシーとより少ない歪みとの間のトレードオフを行うために、分散等化のレベルを選択する、リアルタイムステージ１２０への入力として用いられるトレードオフパラメーター、すなわち、プライバシー保護メカニズムを含んでもよい。

【００３５】

最後に、ステップ１３０は、送信機を用いて、変更された集約データを、通信チャネル

を介して第三者に送信する。

【００３６】

本開示の実施の形態をよりよく理解するには、最初に、集合体データストリームが何であるのかの重要性を認識する必要がある。集合体データは、幾つかの構成要素データストリームの全体である時系列信号であり、ユーザー／クライアントから収集され、集合体データは、通常、１つ以上のサービスプロバイダー、すなわち第三者に分析のために公開されるので、プライバシーの問題が生じる。例えば、幾つかのエネルギー消費デバイスにわたるエネルギー消費の全体である集合体エネルギー消費データストリームを考える。非限定的な例として、このエネルギー消費データが世帯から収集される場合、この世帯の居住者は、とりわけ、それらの居住者の器具のエネルギー消費パターンから、機密であるライフスタイル及び行動の詳細が暴露されることを心配する場合がある。別の例は、工場から収集されたデータを含む場合があり、事業者／所有者は、とりわけ、工場におけるそれらの事業者／所有者の機械／プロセスのエネルギー消費パターンに関連し得る製造プロセスの詳細又は潜在的なトレードシークレットがリークすることを心配する場合がある。しかしながら、１つ以上のサービスプロバイダーによる分析のためのユーザー／クライアントのデータの収集は望ましい場合があり、ユーザー／クライアントの利益のために、もちろん第三者のプロバイダー（複数の場合もある）の利益のために、有用な分析を実行することができる。

【００３７】

集合体データストリームの重要性は、例えば、分析目的を含むことができる。分析目的は、特定のエネルギー消費デバイス（複数の場合もある）（例えば、世帯内の器具（複数の場合もある）又は工場内の機械）の使用パターンを決定するエネルギー消費データについてのものであり得る。これらの使用パターンは、クライアントが受ける他のサービス及び／又はプロバイダーが行う他のサービスを支援することができるような有益な情報（例えば、予防保守／監視サービスを支援するデバイス動作情報又はマーケティング情報）をクライアント及び／又はプロバイダーに提供することができる。さらに、エネルギー消費デバイス（複数の場合もある）の使用パターンは、まだ事前には求められていない一般的な分析を後に可能にするために、エネルギー消費データの正確な表現をプロバイダー（複数の場合もある）に公開するためにも望ましい場合がある。例えば、プロバイダーのタイプは、住宅／事業所（residential/entities）等の消費者サービスプロバイダー、エネルギー／電力プロバイダー及び電話／通信プロバイダーを含むことができる。他のタイプの消費者サービスプロバイダーは、健康関連プロバイダー、すなわちヘルスモニタリングデバイス、又はセンサーを住宅、オフィス、自動車、ハンドヘルドデバイス等に提供する或るタイプの監視サービスプロバイダーを含むことができる。消費者サービスプロバイダーのユーザー又はクライアントは、個人及び団体のうちの一方であってもよいし、組み合わせであってもよい。

【００３８】

分析目的に加えて、プロバイダー（複数の場合もある）に公開されるデータによって暴露される機密情報を制限することによってプライバシーの問題に対処する必要がある。複数のプロバイダーが関与しているとき、各プロバイダーに関する異なるレベルのプライバシーが、クライアントによって所望される場合がある。これらのプライバシーの問題を形式的に特徴付けること、どれだけの情報が暴露されるのかを定量化すること、又は機密情報とみなされるものを判断することさえも、特定の用途の状況においてクライアントの固有の個人プライバシーの問題の理解を必要とする困難な作業となり得る。しかしながら、本開示の実施の形態は、具体的には、１つ以上の特定の構成要素データストリームに相関し得るクライアントの機密情報の秘匿としてプライバシーに対処する。例えば、居住者による機密性を有する行動と高く相関する世帯内の或る特定の器具（複数の場合もある）の使用、又は機密性を有する製造プロセスと高く相関した工場内の或る特定の機械（複数の場合もある）の動作である。全体的な問題は、機密情報、すなわち、或る他の機密デバイス（複数の場合もある）の使用パターンをプロバイダー（複数の場合もある）から秘匿す

るとともに、有用な分析、すなわち、或る特定のデバイス（複数の場合もある）の使用パターンの回復をプロバイダー（複数の場合もある）が行うことができるように、集合体データストリームをクライアント及びプロバイダー（複数の場合もある）がどのように取り扱い、処理し、分析するべきであるのかとして提起することができる。

【００３９】

本開示は、機密情報を隠蔽したり、歪ませたりするのではなく、集約データから機密情報を除去するべきであるとの認識に基づいている。しかしながら、本発明者らは、実施した実験を通じて、この認識は、結局、機密情報を歪ませる既知の方法よりも困難であることを発見した。本発明者らは、幾つかの特定の情報が未知であることを知った。例えば、第１に、本発明者らは、集約データに対する機密情報の寄与の量を知らなかった。第２に、本発明者らは、集約データに対する寄与度の関数がどのようなものであるかを知らなかった。

【００４０】

上記の未知の情報を克服する際に、本発明者らは、幾つかの用途では、機密器具及び他の器具のエネルギー使用を介した加法的組み合わせとしての寄与度の関数は、総エネルギー使用信号、すなわち集合体データに組み合わされることを知った。それらの用途の場合、本発明者らは、ガウス階乗隠れマルコフモデル（ＦＨＭＭ）を適用してデータ、例えば機密器具の使用データをモデル化することができることを理解した。その結果、種々の状態にあるデバイス平均及び分散が判明するので、このデータ、すなわち集合体データを統計的に分析することができ、したがって、本発明者らは、統計学を用いて機密データの寄与の量を求めるという第１の質問に対する回答を見つけることができる。

【００４１】

本発明者らは、センサーの基礎となる状態にわたって平均及び分散を等化することによって機密構成要素を統計的に抑制することができることを更に認識した。したがって、本発明者らは、上記認識の組み合わせに基づいて、集合体データの機密構成要素の基礎となる状態を、非限定的な例としてビタビアルゴリズムを介して推定することができた。さらに、本発明者らは、推定された状態の平均を集合体データから減算することによって、等化された平均を実施することができた。このため、本開示のシステム及び方法は、集約データのエネルギー信号内の精細な時間的特徴を測定するのに高いサンプリング周波数を必要としない。また、本開示のシステム及び方法は、プライバシーの問題によって機密と考えられる器具の真の状態の入力も必要としない。最後に、本発明者らは、等化された分散は、最大分散と推定された状態の分散との間の差に等しい分散を有するガウス白色雑音を加えることによって対処することができることを発見した。

【００４２】

上記認識及び実験に基づいて、本発明者らは、集合体データストリームのプライバシーを保護する問題を解決することができる。特に、本発明者らは、集合体データの全体を構成する個々の構成要素、すなわち、機密構成要素を、幾つかの基礎となる状態によって決まる平均及び分散を有する独立したガウスプロセスとして合理的に統計モデル化することができる状況に対処することができる。具体的には、本開示の方法及びシステムは、集合体データストリームの機密構成要素の基礎となる状態の検出可能性を抑制する。換言すれば、本開示のシステム及び方法は、現在の時間ステップ及び以前の時間ステップの双方のエネルギーデータ及び機密器具状態を、各時間ステップにおいて必要とせず、また、要求もしない。

【００４３】

本開示の幾つかの利点は、本開示が、機密構成要素の基礎となる状態の平均及び分散を等化するプライバシーメカニズムを適用するようにして、機密構成要素の基礎となる状態の検出可能性を低減することを含むことができる。もう１つの利益は、多くの利益の中でも、より良好なプライバシーとより少ない歪みとの間のトレードオフを行うために、トレードオフパラメーターをこのプライバシー保護メカニズムへの入力として用いて、分散等化のレベルを選択することができるということである。本開示の更に別の態様は、プライ

バシー保護メカニズムの出力を、機密構成要素の基礎となる状態の低減された検出可能性を有する変更された集合体データストリームとすることができるということである。さらに、本開示は、集合体データ、及び機密構成要素の基礎となる状態のシーケンスとしてプライバシー保護メカニズムへの入力を用いる。

【００４４】

図１Ｂは、本開示の実施の形態による、集約データのプライバシーが保護されるようにして、集約データを第三者に送信する図１Ａの方法１００を示す概略図である。図１Ｂは、数ある構成要素の中でもとりわけ、プロセッサ、メモリ及び送受信機を備えることができるコンピューターシステム１１２を示している。コンピューター１１２の送受信機は、ソースコンピューター１１０から集約データ１１０ＢＢを受信し、集約データ１１０ＢＢをコンピューターシステム１１２のメモリに記憶する。ここでは、コンピューターシステム１１２は、集約データ１１０ＢＢを、変更された集約データ１２０ＢＢに変換し、この変更された集約データ１２０ＢＢを第三者１２７の第三者コンピューター１２６に送信する。

【００４５】

図１Ｃは、本開示の実施の形態による、図１Ａの方法の代替の適用態様又は実施態様を示す図１Ａの方法の概略図である。図１Ｃは、ソース１１１を示し、このソースは、住宅等の、少なくとも１つの電力消費体１０５を有するクライアント１０４にエネルギー１０９を提供するエネルギーサービスプロバイダー（ＥＳＰ）とすることができる。ＥＳＰ１１１は、或る時間帯にわたってクライアントの住宅１０５からクライアント１０４のエネルギー使用を収集し、クライアントの集合体データ１１１ＢＢを系統的に表現し（formulates）、このデータはＥＳＰコンピューター１１４に記憶される。ここでは、ＥＳＰコンピューター１１４は、集約データ１１１ＢＢを、変更された集約データ１１４ＢＢに変換し、この変更された集約データ１１４ＢＢを第三者１２７の第三者コンピューター１２６に送信する。

【００４６】

図２は、本開示の実施の形態による、集合体データストリームを歪ませるために、変更された集合体データに雑音が加えられるガウス階乗隠れマルコフモデルＦＨＭＭ仮定を示す別の方法のブロック図である。

【００４７】

ステップ２１０は、複数のセンサーから生成された集約データを、プロセッサ及びメモリを有するコンピューター２１２を介して受信する。集約データ２１０ＢＢは、各センサーが或る時間帯内の一組の時点においてデータを検知するようにして、機密デバイス及び非機密デバイスからこの時間帯にわたって収集された時系列データを含む。

【００４８】

集約データ２１０ＢＢは、オフライントレーニングステージステップ２１５によって受信される。オフライントレーニングステージ２１５は、集約データ２１０ＢＢを生成した機密デバイスと同じデバイスタイプの機密デバイスを含むデバイスから生成されたデータから、記憶された履歴デバイスデータ及び履歴統計寄与度データを入手することによって実行される。各機密デバイスの記憶された履歴統計寄与度は、時間帯内の各時点における機密デバイスの状態に応じた集約データ２１０ＢＢに対応する。

【００４９】

ステップ２２０は、時間帯内の各時点において集約データに寄与する機密デバイスの状態を求めるサブステップ１２０Ａを含むリアルタイムステージを実行する。サブステップ１２０Ｂは、各時点における機密デバイスの求められた状態に基づいて、各時点における集約データに対する機密デバイスの対応する記憶された履歴統計寄与度をメモリから選択する。次に、サブステップ１２０Ｃは、或る時点について選択された、記憶された履歴統計寄与度を、対応する時点における集約データの値から減算して、変更された集約データ１２０ＢＢを生成する。

【００５０】

ステップ２２０の次は、ステップ２６０である。このステップは、対応する時点における集約データの値からの時点から選択された、記憶された履歴統計寄与度２１５を利用することによってリアルタイムステージを継続する。これは測定雑音を示す。その結果、ステップ２６０は、機密構成要素の分散を等化するガウス雑音を生成する。

【００５１】

例えば、クライアントの集合体データストリームは、Y_1，Y_2，…，Y_Tによって示すことができる。ここで、Ｔは、（サンプリングされた時間ステップの数に関する）シーケンスの長さである。個々の構成要素の数をＭで示すことにする。これらの構成要素は、｛１，２，…，Ｍ｝としてラベル付けされる。各ｔ∈｛１，２，…，Ｔ｝及び各ｍ∈｛１，…，Ｍ｝について、時刻ｔにおける構成要素ｍの値を$X_{m,t}$で示し、基礎となる状態を$S_{m,t}$で示すことにする。各構成要素ｍの基礎となる状態は、S_mによって示される状態の有限集合に属する。時刻ｔにおける集合体データストリームは、以下の和としてモデル化される。

【００５２】

【数１】

$$Y_t = N_t + \sum_{m=1}^{M} X_{m,t},$$

【００５３】

ここで、N_tは測定雑音を示す。ガウスＦＨＭＭの適用は、各構成要素の基礎となる状態シーケンスが相互に独立していることと、各構成要素の値$X_{m,t}$が状態$S_{m,t}$にのみ依存することと、$S_{m,t}$が与えられたときの$X_{m,t}$の条件付き分布が、状態$S_{m,t}$に依存する平均及び分散を有するガウス分布であることとを前提とする。各構成要素ｍ及び各状態ｓ∈S_mについて、$S_{m,t}$＝ｓである場合に、$X_{m,t}$の平均を$\mu_{m,s}$で示し、$X_{m,t}$の分散を$\sigma^2_{m,s}$で示すことにする。構成要素ｍの最大分散を、

【００５４】

【数２】

$$\sigma^2_{m,*} := \max_{s \in S_m} \sigma^2_{m,s}$$

【００５５】

で示すことにする。これは、ユーザーによって計算される。特定の用途に応じて、これらの平均及び分散は、トレーニングデータから知ることもできるし、場合によっては、デバイス仕様を調べることによって知ることもできる。特定の用途では、ガウスＦＨＭＭの適用は、近似した前提にすぎない場合があるが、それでも合理的に正確である場合があり、プライバシーを損なうことを試みているときにそのようなモデルを同様に前提としている敵対者に対しては特に適している場合がある。

【００５６】

任意選択で、ステップ２６５は、機密構成要素の集合体データストリーム（Y_1，Y_2，…，Y_T）及び基礎となる状態（$S_{k,1}$，$S_{k,2}$，…，$S_{k,T}$）の双方を入力として取るプライバシーメカニズムを含む。ここで、ｋは、機密構成要素のインデックスを示すものとする。加えて、ステップ２７０において、トレードオフパラメーターλ∈［０，１］を、分散等化のレベルを選択するプライバシーメカニズムへの入力とすることができる。プライバシーメカニズムの出力は、変更された集合体データストリームであり、以下の式に従って生成される（Z_1，Z_2，…，Z_T）によって示される。

【００５７】

【数３】

$$Z_t = Y_t - \mu_{k,S_{k,t}} + \lambda W_t,$$

【００５８】

ここで、W_tは、

【００５９】

【数４】

$$(\sigma^2_{k,*} - \sigma^2_{k,S_{k,t}})$$

【００６０】

に等しい分散を有する独立ゼロ平均ガウス雑音である。この分散は、すなわち、機密構成要素の最大分散と、現在の状態Ｓ$_{k,t}$を所与とする機密構成要素の分散との間の差である。各時間ステップにおける

【００６１】

【数５】

$$\mu_{k,S_{k,t}}$$

【００６２】

（すなわち、基礎となる状態がＳ$_{k,t}$である場合の時刻ｔにおける機密構成要素の平均）の減算は、全体の信号の平均に対する機密構成要素の寄与度を０に等化するという効果を有し、したがって、機密構成要素の基礎となる状態の検出可能性を、１次統計を介して低減する。この手順は、状態（Ｓ$_{k,1}$，Ｓ$_{k,2}$，…，Ｓ$_{k,T}$）から作成された機密構成要素の値（Ｘ$_{k,1}$，Ｘ$_{k,2}$，…，Ｘ$_{k,T}$）の最小平均二乗誤差推定値を減算除去するので、集合体データストリーム（Ｙ$_1$，Ｙ$_2$，…，Ｙ$_T$）の他の非機密構成要素を検出する能力も改善することができる。λが１に等しい場合、Ｗ$_t$の加算は、全体の信号の分散に対する機密構成要素の寄与度を、機密構成要素の最大分散に更に等化し、したがって、ガウスＦＨＭＭの前提が特定の用途について有効である場合に、変更された集合体データストリームからの機密構成要素の基礎となる状態の検出可能性を完全に低減する。一方、ステップ２８０は、集合体データストリームを歪ませる雑音を導入するＷ$_t$の加算を可能にし、したがって、パラメーターλは、システム事業者が、雑音を加える（２８０）ことによって機密構成要素の基礎となる状態を完全に検出不可能にするための（λ＝１における）完全分散等化と、加えられる雑音を有しない平均等化によってのみ低減される検出可能性を得るための（λ＝０における）分散等化なしとの間でトレードオフパラメーター２７０を選択することを可能にするのに用いられる。ここでは、加えられた雑音２８０ＢＢを有する変更された集約データをステップ２９０において第三者に公開することができる。

【００６３】

本開示の別の実施の形態では、機密構成要素の基礎となる状態を入力として必要としないようにプライバシーメカニズムを変更することができる。この場合、集合体データストリーム（Ｙ$_1$，Ｙ$_2$，…，Ｙ$_T$）のみを（トレードオフパラメーターとともに）プライバシーメカニズムへの主要な入力として用いて、機密構成要素の基礎となる状態が、集合体データストリームから最初に推定される。この推定は、よく知られたビタビアルゴリズムを適用することによって行うこともできるし、幾つかの他のアルゴリズムを介して行うこともでき、場合によっては、或る用途固有の領域知識を利用することもできる。

【００６４】

【数６】

$$(\hat{S}_{k,1}, \hat{S}_{k,2}, \ldots, \hat{S}_{k,T})$$

【００６５】

によって示されるこれらの推定された状態は、その後、基本的な実施の形態について説明される手順において、実際の状態（Ｓ$_{k,1}$，Ｓ$_{k,2}$，…，Ｓ$_{k,T}$）の代わりに用いられる。したがって、本発明のこの変形形態の場合、プライバシーメカニズムの出力は、以下の式に従って生成された、変更された集合体データストリーム（Ｚ$_1$，Ｚ$_2$，…，Ｚ$_T$）である。

【００６６】

【数７】

$$Z_t = Y_t - \mu_{k,\hat{S}_{k,t}} + \lambda W_t,$$

【００６７】

ここで、Ｗ$_t$は、

【００６８】

【数８】

$$\left(\sigma^2_{k,*} - \sigma^2_{k,\hat{S}_{k,t}}\right).$$

【００６９】

に等しい分散を有する独立ゼロ平均ガウス雑音である。

【００７０】

本開示の別の実施の形態では、２つ以上の機密構成要素を考慮に入れ、これらに対処することができる。一般性を失うことなく、機密構成要素を１～ｋによってインデックス付けすることにする。この場合の手順は、以下の式に従って、変更された集合体データストリーム（Ｚ$_1$，Ｚ$_2$，…，Ｚ$_T$）を生成するために、基本的には、各機密構成要素について平均及び分散の等化を適用することである。

【００７１】

【数９】

$$Z_t = Y_t + \sum_{j=1}^{k}\left[\lambda_j W_{j,t} - \mu_{j,S_{j,t}}\right],$$

【００７２】

ここで、各Ｗ$_{j,t}$は、

【００７３】

【数１０】

$$\left(\sigma^2_{j,*} - \sigma^2_{j,S_{j,t}}\right)$$

【００７４】

に等しい分散を有する独立ゼロ平均ガウス雑音であり、トレードオフパラメーターλ$_1$，…，λ$_T$∈［０，１］は同一とすることもできるし、異なるものとすることもできる。この手順は、機密構成要素間で容易に並列化することができる。従前の実施の形態と同様に、機密構成要素の基礎となる状態は、プライバシーメカニズムへの入力として直接利用可能でない場合に、集合体データストリームから作成された推定値に置き換えることができる。

【００７５】

換言すれば、本開示は、或る有限時間間隔（１，２，…，Ｔ）にわたって収集された集合体データストリームに適用することができるが、一方で、大きさが不定の（indefinite）データのストリーム（Ｙ$_1$，Ｙ$_2$，…）に容易に適用される。時刻ｔにおける変更された集合体データストリームＺ$_t$内の各値は、時刻ｔにおける集合体データストリームＹ$_t$内の１つの対応する値及び状態Ｓ$_{k,t}$にのみ依存し、これによって、大きさが不定のストリームに対する適用が容易になることに留意されたい。

【００７６】

図３は、本開示の実施の形態による、図１Ａ、図１Ｂ及び図１Ｃと同様に、集約データを第三者に送信する別の方法の概略図である。ここでは、ソース３１０は、クライアントコンピューター３０７を有するクライアント３０５であってもよく、クライアントコンピューター３０７は、このＥＳＰコンピューター３１４と通信し、第三者３２７の第三者コンピューター３２６と更に通信する。クライアントの住宅３０５は、クライアント３０４のエネルギー使用を或る時間長にわたって収集し、クライアントの集合体データ３０５Ｂ

Ｂを系統的に表現する。この集合体データは、クライアントのコンピューター３０７に記憶される。このコンピューター３０７において、集合体データ３０５ＢＢは、変更された集約データ３０７ＢＢに変換され、ＥＳＰのコンピューター３１４に送信され、ＥＳＰのコンピューター３１４は、この変更された集約データ３０７ＢＢを第三者３２７の第三者コンピューター３２６に送信する。

【００７７】

例えば、集合体データは、ユーザーが、ユーザー送信機を用いて、変換された集約データを、ユーザー通信チャネルを介して第三者に送信するようにして、第三者計測デバイスのユーザー側に配置されたユーザー計測デバイス又はユーザー測定デバイスを用いてユーザーによって収集されたエネルギーデータとしてユーザーから発信することができる。この方法のステップは、ユーザー送信機と作動接続されたプロセッサによって実行される。

【００７８】

図４は、本開示の実施の形態による、代替のコンピューター又はプロセッサを用いて実施することができる図１Ａの方法を示すブロック図である。特に、この方法は、集約データの分析的有用性を維持しながら、集合体データを変更して集約データのプライバシーを保護するように構成されている。コンピューター４１１は、プロセッサ４４０と、コンピューター可読メモリ４１２と、記憶デバイス４５８と、ディスプレイ４５２及びキーボード４５１とのユーザーインターフェース４４９とを備え、これらは、バス４５６を通じて接続されている。例えば、プロセッサ４４０及びコンピューター可読メモリ４１２と通信するユーザーインターフェース４４９は、ユーザーによるユーザーインターフェース４５７の表面、キーボード表面からの入力を受け取ると、集約データを入手し、コンピューター可読メモリ４１２に記憶する。

【００７９】

メモリ４１２は、プロセッサによって実行可能な命令と、履歴データと、本開示の方法及びシステムが利用することができる任意のデータとを記憶することができることが意図されている。プロセッサ４４０は、シングルコアプロセッサ、マルチコアプロセッサ、コンピューティングクラスター、又は任意の数の他の構成体とすることができる。プロセッサ４４０は、バス４５６を通じて１つ以上の入力デバイス及び出力デバイスに接続することができる。メモリ４１２は、ランダムアクセスメモリ（ＲＡＭ）、リードオンリーメモリ（ＲＯＭ）、フラッシュメモリ、又は他の任意の適したメモリシステムを含むことができる。

【００８０】

図４を更に参照すると、記憶デバイス４５８は、プロセッサによって用いられる補助データ及び／又はソフトウェアモジュールを記憶するように構成することができる。例えば、記憶デバイス４５８は、履歴デバイスデータと、デバイスのマニュアル等の他の関連したデバイスデータとを記憶することができる。加えて又は代替的に、記憶デバイス４５８は、集合体データと同様の履歴データを記憶することができる。記憶デバイス４５８は、ハードドライブ、光ドライブ、サムドライブ、ドライブのアレイ、又はそれらの任意の組み合わせを含むことができる。

【００８１】

システムは、任意選択で、バス４５６を通じて、システムをディスプレイデバイスに接続するように構成されたディスプレイインターフェースにリンクすることができ、ディスプレイデバイスは、とりわけ、コンピューターモニター、カメラ、テレビ、プロジェクター、又はモバイルデバイスを含むことができる。

【００８２】

コンピューター４１１は、用途に応じて、電力源４５４を備えることができ、電力源４５４は、任意選択でコンピューター４１１の外部に配置されてもよい。バス４５６を通じて、ディスプレイデバイス４４８に接続するように構成されたユーザー入力インターフェース４５７をリンクすることができ、ディスプレイデバイス４４８は、とりわけ、コンピューターモニター、カメラ、テレビ、プロジェクター、又はモバイルデバイスを含むこと

ができる。プリンターインターフェース４５９も、バス４５６を通じて接続することができ、印刷デバイス４３２に接続するように構成することができる。印刷デバイス４３２は、とりわけ、液体インクジェットプリンター、固体インクプリンター、大規模商用プリンター、感熱式プリンター、ＵＶプリンター、又は昇華型プリンターを含むことができる。ネットワークインターフェースコントローラー（ＮＩＣ）４３４は、バス４５６を通じてネットワーク４３６に接続するように構成され、とりわけ、変更された集合体データ又は他のデータは、コンピューター４１１の外部の第三者ディスプレイデバイス、第三者画像デバイス、及び／又は第三者印刷デバイス上にレンダリングすることができる。

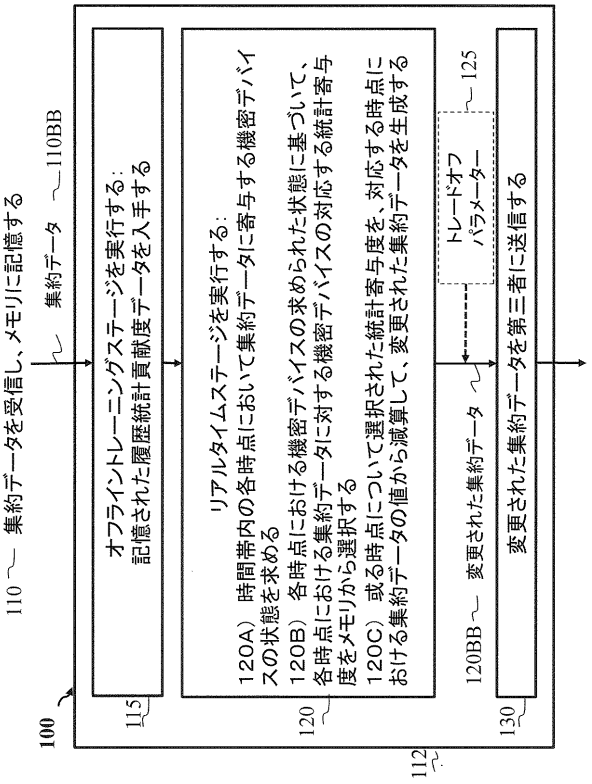
【００８３】

図４を更に参照すると、とりわけ、集約データ、変更された集合体データ又は他のデータは、記憶及び／又は更なる処理のために、ネットワーク４３６の通信チャネルを介して送信することができ及び／又は記憶デバイス４５８内に記憶することができる。さらに、集約データ、変更された集合体データ又は他のデータは、受信機４４６（又は外部受信機４３８）から無線又は配線接続で受信することもできるし、送信機４４７（又は外部送信機４３９）を介して無線又は配線接続で送信することもでき、受信機４４６及び送信機４４７はともに、バス４５６を通じて接続されている。コンピューター４１１は、入力インターフェース４０８を介して外部検知デバイス４４４及び外部入力／出力デバイス４４１に接続することができる。コンピューター４１１は、他の外部コンピューター４４２に接続することができる。出力インターフェース４０９は、プロセッサ４４０からの処理されたデータを出力するのに用いることができる。

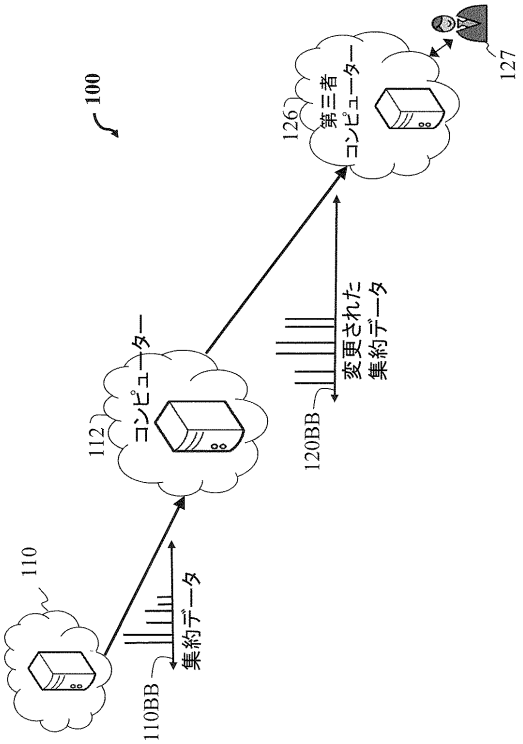
【００８４】

本開示の上述した実施の形態は、多数の方法のうちの任意のもので実施することができる。例えば、上記実施の形態は、ハードウェア、ソフトウェア、又はそれらの組み合わせを用いて実施することができる。請求項の要素を修飾する、特許請求の範囲における「第１」、「第２」等の序数の使用は、それ自体で、１つの請求項の要素の別の請求項の要素に対する優先順位も、優位性も、順序も暗示するものでもなければ、方法の動作が実行される時間的な順序も暗示するものでもなく、請求項の要素を区別するために、単に、或る特定の名称を有する１つの請求項の要素を、同じ（序数の用語の使用を除く）名称を有する別の要素と区別するラベルとして用いられているにすぎない。

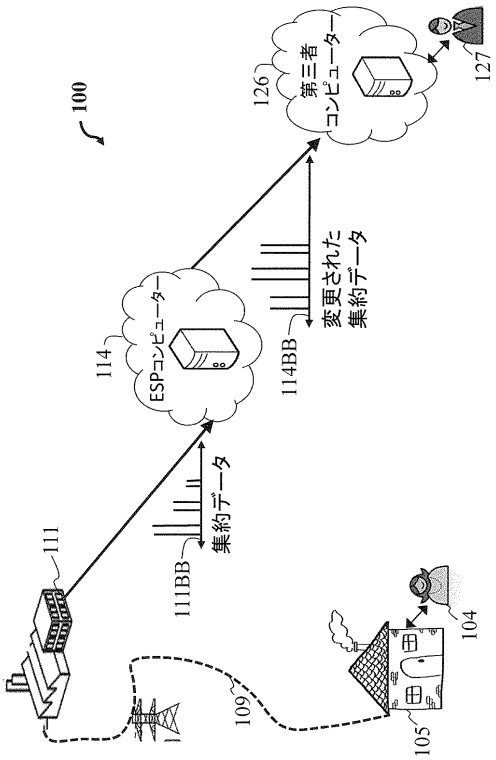
【図１Ａ】



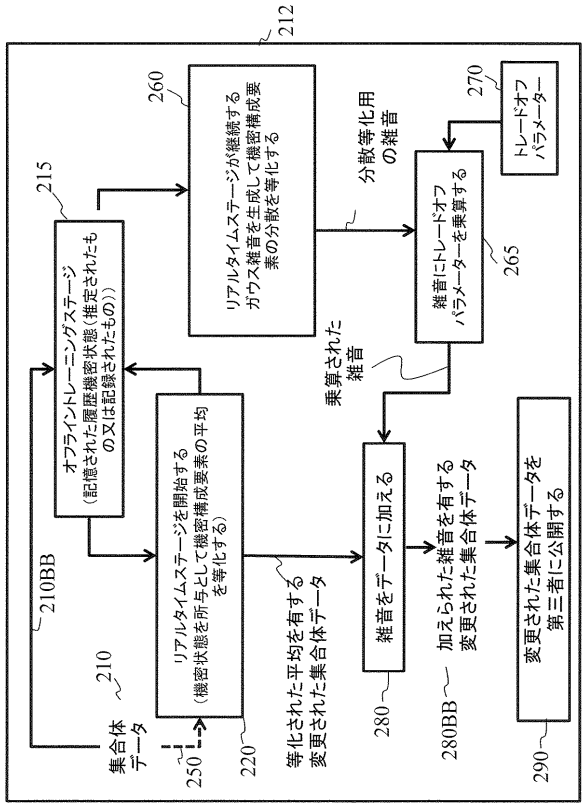
【図１Ｂ】



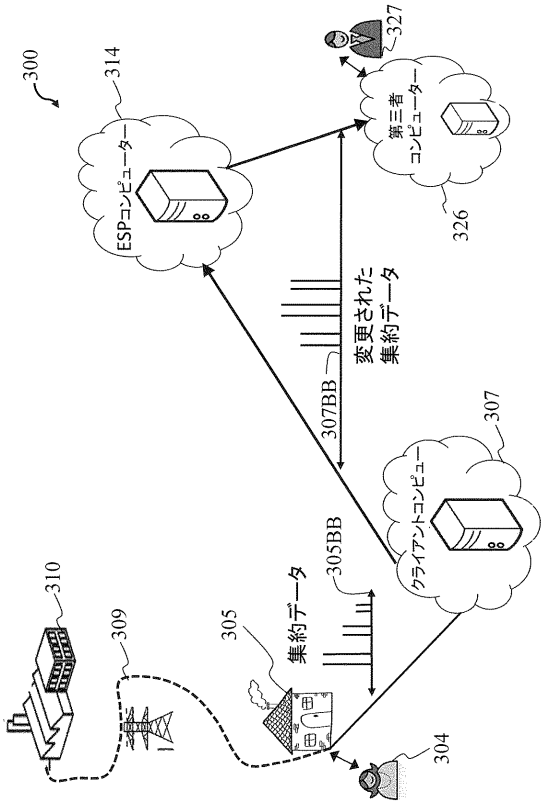
【図１Ｃ】



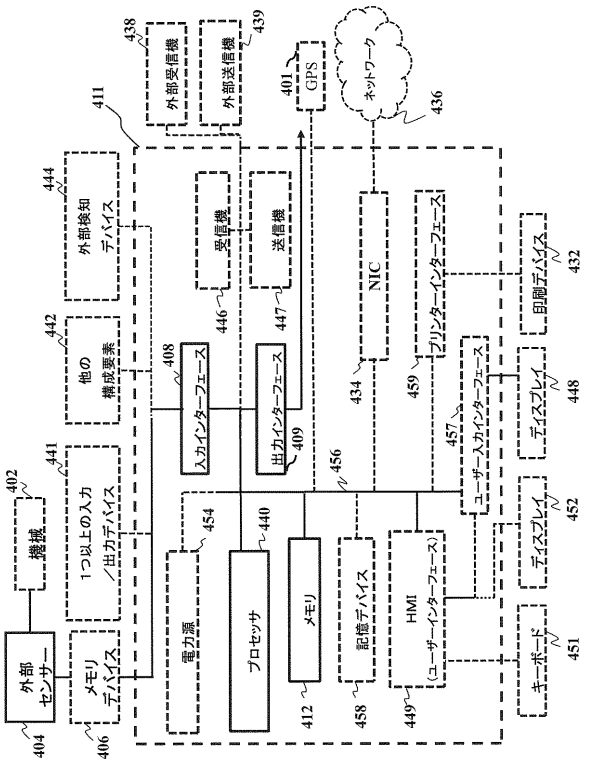
【図２】



【図３】


300
314
ESPコンピューター
327
第三者
コンピューター
326
変更された
集約データ
307BB
307
クライアントコンピュー
305BB
集約データ
310
309
305
304

【図４】


438
外部受信機
439
外部送信機
401
GPS
ネットワーク
436
411
444
外部検知
デバイス
442
他の
構成要素
408
入力インターフェース
446
受信機
447
送信機
出力インターフェース
409
456
NIC
434
プリンターインターフェース
459
457
ユーザー入力インターフェース
印刷デバイス
432
ディスプレイ
448
ディスプレイ
452
キーボード
451
HMI
ユーザーインターフェース
449
402
機械
外部
センサー
404
441
1つ以上の入力
/出力デバイス
メモリ
デバイス
406
454
電力源
440
プロセッサ
412
メモリ
458
記憶デバイス

フロントページの続き

(72)発明者　イェ・ワン
アメリカ合衆国、マサチューセッツ州、ケンブリッジ、ブロードウエイ　２０１、ケアオブ・ミツビシ・エレクトリック・リサーチ・ラボラトリーズ・インコーポレイテッド
(72)発明者　ニサルグ・ジャグディシュバイ・ラバル
アメリカ合衆国、マサチューセッツ州、ケンブリッジ、ブロードウエイ　２０１、ケアオブ・ミツビシ・エレクトリック・リサーチ・ラボラトリーズ・インコーポレイテッド
(72)発明者　プラカシュ・イシュワー
アメリカ合衆国、マサチューセッツ州、ケンブリッジ、ブロードウエイ　２０１、ケアオブ・ミツビシ・エレクトリック・リサーチ・ラボラトリーズ・インコーポレイテッド

審査官　平井　誠

(56)参考文献　特開２０１６－１６７８０４（ＪＰ，Ａ）
特開２０１２－０５８９９８（ＪＰ，Ａ）
特表２０１６－５３１５１３（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／６０－６４