(19)日本国特許庁(JP)　(12)特　許　公　報(B1)　(11)特許番号
特許第6830285号
(P6830285)
(45)発行日　令和3年2月17日(2021.2.17)　(24)登録日　令和3年1月28日(2021.1.28)

(51)Int.Cl.　F I
H04M 3/42 (2006.01)　H04M 3/42 Z
H04M 11/00 (2006.01)　H04M 11/00 301

請求項の数 13　(全 33 頁)

(21)出願番号　特願2020-88305(P2020-88305)
(22)出願日　令和2年5月20日(2020.5.20)
審査請求日　令和2年5月21日(2020.5.21)
(31)優先権主張番号　特願2020-71397(P2020-71397)
(32)優先日　令和2年4月13日(2020.4.13)
(33)優先権主張国・地域又は機関
日本国(JP)

(73)特許権者　519234291
ｉｏＴ－ＥＸ株式会社
東京都千代田区神田富山町５番１
(74)代理人　100185971
弁理士　高梨　玲子
(72)発明者　松村　淳
東京都千代田区神田富山町５番１　ｉｏＴ－ＥＸ株式会社内

審査官　山岸　登

最終頁に続く

(54)【発明の名称】情報処理システム、情報処理方法およびコンピュータプログラム

(57)【特許請求の範囲】
【請求項１】
信号を発信する機能を有する第一の情報処理装置と、
前記信号を受信する機能を有する第二の情報処理装置であって、特定の場所に設置される第二の情報処理装置と、
前記第二の情報処理装置とインターネットを介して接続可能なサーバ装置と
を備える情報処理システムであって、
前記第一の情報処理装置は、
当該第一の情報処理装置の第一識別情報を含む信号を発信し、
前記第二の情報処理装置は、
前記第一の情報処理装置から発信された前記信号を受信し、当該信号を受信した時刻に関する時刻情報、前記信号の受信強度に基づく強度情報および前記第一識別情報を、前記第二の情報処理装置の第二識別情報とともに前記サーバ装置に送信し、
前記サーバ装置は、
前記第二の情報処理装置から受信した前記時刻情報、前記強度情報、前記第一識別情報および前記第二識別情報を互いに関連付けて記憶し、
特定の第一の情報処理装置の特定の第一識別情報の指定を受け付けた場合に、前記特定の第一識別情報に関連付けて記憶された特定の第二識別情報に基づいて、当該特定の第二識別情報に関連付けて記憶された１以上の他の第一識別情報を抽出する情報処理システム。

【請求項２】
前記サーバ装置は、
前記特定の第一識別情報の指定を受け付けた場合に、当該特定の第一識別情報に関連付けて記憶された特定の第二識別情報および当該特定の第一識別情報を含む信号を受信した特定の時刻に関する特定時刻情報に基づいて、当該特定時刻情報に関連する時刻情報に関連付けて記憶された１以上の他の第一識別情報を抽出することを特徴とする請求項１に記載の情報処理システム。
【請求項３】
前記サーバ装置は、
前記特定の第一識別情報の指定を受け付けた場合に、抽出された１以上の第一識別情報を有する第一の情報処理装置に対して、特定の情報を通知することを特徴とする請求項１または２に記載の情報処理システム。
【請求項４】
前記第二の情報処理装置は、
前記サーバ装置にインターネットを介して接続され、
設置場所の環境情報を所定のセンサから取得し、当該環境情報を受信した時刻に関する時刻情報を、前記環境情報とともにサーバ装置に送信し、
前記サーバ装置は、
前記第二の情報処理装置から受信した環境情報および時刻情報を、前記第二識別情報に関連付けて記憶することを特徴とする請求項１、２または３に記載の情報処理システム。
【請求項５】
前記サーバ装置は、
前記第二の情報処理装置から受信した環境情報が特定の条件を満たす場合に、前記第二識別情報に関連付けて記憶された１以上の第一識別情報を抽出することを特徴とする請求項４に記載の情報処理システム。
【請求項６】
前記サーバ装置は、
前記特定の条件を満たす場合に抽出された１以上の第一識別情報を有する第一の情報処理装置の少なくとも一つに対して、注意情報を通知することを特徴とする請求項５に記載の情報処理システム。
【請求項７】
前記第二の情報処理装置は、
クラウド上で実現されるＩｏＴハブ、および、ローカルにありＩｏＴハブと接続されるＩｏＴルータを備えるＩｏＴ接続システムにおけるＩｏＴルータであって、
前記ＩｏＴハブは、第一のデバイスが接続可能なプライベートクラウドと当該ＩｏＴハブとを接続するための第一のドライバ、または、第二のデバイスと当該ＩｏＴハブとを接続するための第二のドライバの少なくとも一方を有し、
前記ＩｏＴルータは、第三のデバイスと当該ＩｏＴルータとを接続するための第三のドライバを有することを特徴とする請求項１から６のいずれか一項に記載の情報処理システム。
【請求項８】
前記サーバ装置は、
前記第二の情報処理装置から受け付けた第一識別情報に対応する第一の情報処理装置に対してのみ、特定の電子錠を解除可能な解除キーに関する情報を送信することを特徴とする請求項１から７のいずれか一項に記載の情報処理システム。
【請求項９】
前記第一の情報処理装置は、スマートフォンおよび／またはビーコンタグを含むことを特徴とする請求項１から８のいずれか一項に記載の情報処理システム。
【請求項１０】
前記情報処理システムは、さらに、第三識別情報が記録された二次元コードが表された

媒体を備え、
前記第二の情報処理装置は、
前記媒体から前記第三識別情報を読み取り、当該第三識別情報を読み取った時刻に関する時刻情報および前記第三識別情報を、前記第二の情報処理装置の第二識別情報とともに前記サーバ装置に送信することを特徴とする請求項１から９のいずれか一項に記載の情報処理システム。
【請求項１１】
前記サーバ装置は、
前記第一の情報処理装置の信号を発信する機能と前記第二の情報処理装置の前記信号を受信する機能とを切り替え可能であることを特徴とする請求項１から１０のいずれか一項に記載の情報処理システム。
【請求項１２】
信号を発信する機能を有する第一の情報処理装置と、
前記信号を受信する機能を有する第二の情報処理装置であって、特定の場所に設置される第二の情報処理装置と、
前記第二の情報処理装置とインターネットを介して接続可能なサーバ装置と
を備える情報処理システムにおいて実行される情報処理方法であって、
前記第一の情報処理装置に、
当該第一の情報処理装置の第一識別情報を含む信号を発信するステップを実行させ、
前記第二の情報処理装置に、
前記第一の情報処理装置から発信された信号を受信するステップと、
前記信号を受信した時刻に関する時刻情報、前記信号の受信強度に基づく強度情報および前記第一識別情報を、前記第二の情報処理装置の第二識別情報とともに前記サーバ装置に送信するステップと
を実行させ、
前記サーバ装置に、
前記第二の情報処理装置から受信した前記時刻情報、前記強度情報、前記第一識別情報および前記第二識別情報を互いに関連付けて記憶するステップと、
特定の第一の情報処理装置の特定の第一識別情報の指定を受け付けるステップと、
前記指定を受け付けた場合に、前記特定の第一識別情報に関連付けて記憶された特定の第二識別情報に基づいて、当該特定の第二識別情報に関連付けて記憶された１以上の他の第一識別情報を抽出するステップと
を実行させる、情報処理方法。
【請求項１３】
信号を発信する機能を有する第一の情報処理装置と、
前記信号を受信する機能を有する第二の情報処理装置であって、特定の場所に設置される第二の情報処理装置と、
前記第二の情報処理装置とインターネットを介して接続可能なサーバ装置と
を備える情報処理システムの前記サーバ装置において実行されるコンピュータプログラムであって、
前記第二の情報処理装置は、
前記第一の情報処理装置から発信された前記第一の情報処理装置の第一識別情報を含む信号を受信し、
前記信号を受信した時刻に関する時刻情報、前記信号の受信強度に基づく強度情報および前記第一識別情報を、前記第二の情報処理装置の第二識別情報とともに前記サーバ装置に送信し、
前記サーバ装置に、
前記第二の情報処理装置から受信した前記時刻情報、前記強度情報、前記第一識別情報および前記第二識別情報を互いに関連付けて記憶する機能と、
特定の第一の情報処理装置の特定の第一識別情報の指定を受け付けた場合に、前記特定

の第一識別情報に関連付けて記憶された特定の第二識別情報に基づいて、当該特定の第二識別情報に関連付けて記憶された１以上の他の第一識別情報を抽出する機能と
を実現させる、コンピュータプログラム。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、情報処理システム、情報処理方法およびコンピュータプログラムに関する。
【背景技術】
【０００２】
新型コロナウイルス（ＣＯＶＩＤ－１９）等の感染症に罹患した者（以下、「感染者」という。）が特定された場合に、かかる感染者に基づく感染性の高い他の者（以下、「濃厚接触者」という。）を特定するためには、感染者の行動履歴を知る必要がある。
【０００３】
ここでいう濃厚接触者は、一般的に、手で触れること又は対面で会話することが可能な距離で、必要な感染予防策なしで、「患者（確定例）」と接触があった者とされている。
【０００４】
現状、かかる行動履歴は、感染者に聞き取り調査を行うことにより得るのが一般的であり、不確実なものであった。
【０００５】
最近では、互いのスマートフォンの近距離無線通信機能を利用して近くにいる他人の情報を自身のスマートフォンに記録しておくことで、自身が感染者となった場合に当該情報に基づいて濃厚接触者を特定するというアプリケーションが開発されている。
【先行技術文献】
【特許文献】
【０００６】
【非特許文献１】“シンガポール、コロナ感染をアプリで追跡、政府開発”、日本経済新聞電子版、令和２年４月２日検索＜URL:https://www.nikkei.com/article/DGXMZO57056430Q0A320C2FF8000/＞
【発明の概要】
【発明が解決しようとする課題】
【０００７】
しかしながら、かかる技術によれば、他人の情報は個々のスマートフォンに記録されているため、行動履歴の追跡チームによる管理が容易ではないという問題がある。
【０００８】
したがって、本開示の目的は、感染者の行動履歴の特定および濃厚接触者の抽出を容易に確実に行うことが可能な情報処理システム、情報処理方法およびコンピュータプログラムを提供することにある。
【課題を解決するための手段】
【０００９】
本開示の実施形態における情報処理システムは、信号を発信する機能を有する第一の情報処理装置と、信号を受信する機能を有する第二の情報処理装置と、第二の情報処理装置とインターネットを介して接続可能なサーバ装置とを備える情報処理システムであって、第一の情報処理装置は、当該第一の情報処理装置の第一識別情報を含む信号を発信し、第二の情報処理装置は、第一の情報処理装置から発信された信号を受信し、当該信号を受信した時刻に関する時刻情報、信号の受信強度に基づく強度情報および第一識別情報を、第二の情報処理装置の第二識別情報とともにサーバ装置に送信し、サーバ装置は、第二の情報処理装置から受信した時刻情報、強度情報、第一識別情報および第二識別情報を互いに関連付けて記憶し、特定の第一の情報処理装置の特定の第一識別情報の指定を受け付けた場合に、特定の第一識別情報に関連付けて記憶された特定の第二識別情報に基づいて、当

該特定の第二識別情報に関連付けて記憶された１以上の他の第一識別情報を抽出することを特徴とする。

【００１０】

サーバ装置は、特定の第一識別情報の指定を受け付けた場合に、特定の第一識別情報に関連付けて記憶された特定の第二識別情報および当該特定の第一識別情報を含む信号を受信した特定の時刻に関する時刻情報に基づいて、当該特定時刻情報に関連付けて記憶された１以上の他の第一識別情報を抽出することができる。

【００１１】

サーバ装置は、特定の第一識別情報の指定を受け付けた場合に、抽出された１以上の第一識別情報を有する第一の情報処理装置に対して、特定の情報を通知することができる。

【００１２】

第二の情報処理装置は、サーバ装置にインターネットを介して接続され、設置場所の環境情報を所定のセンサから取得し、当該環境情報を受信した時刻に関する時刻情報を、環境情報とともにサーバ装置に送信し、サーバ装置は、第二の情報処理装置から受信した環境情報および時刻情報を、第二識別情報に関連付けて記憶することができる。

【００１３】

サーバ装置は、第二の情報処理装置から受信した環境情報が特定の条件を満たす場合に、第二識別情報に関連付けて記憶された１以上の第一識別情報を抽出することができる。

【００１４】

サーバ装置は、特定の条件を満たす場合に抽出された１以上の第一識別情報を有する第一の情報処理装置の少なくとも一つに対して、注意情報を通知するができる。

【００１５】

第二の情報処理装置は、クラウド上で実現されるＩｏＴハブ、および、ローカルにありＩｏＴハブと接続されるＩｏＴルータを備えるＩｏＴ接続システムにおけるＩｏＴルータであって、ＩｏＴハブは、第一のデバイスが接続可能なプライベートクラウドと当該ＩｏＴハブとを接続するための第一のドライバ、または、第二のデバイスと当該ＩｏＴハブとを接続するための第二のドライバの少なくとも一方を有し、ＩｏＴルータは、第三のデバイスと当該ＩｏＴルータとを接続するための第三のドライバを有することができる。

【００１６】

サーバ装置は、第二の情報処理装置から受け付けた第一識別情報に対応する第一の情報処理装置に対してのみ、特定の電子錠を解除可能な解除キーに関する情報を送信することができる。

【００１７】

本開示の実施形態における情報処理方法は、信号を発信する機能を有する第一の情報処理装置と、信号を受信する機能を有する第二の情報処理装置と、第二の情報処理装置とインターネットを介して接続可能なサーバ装置とを備える情報処理システムにおいて実行される情報処理方法であって、第一の情報処理装置に、当該第一の情報処理装置の第一識別情報を含む信号を発信するステップを実行させ、第二の情報処理装置に、第一の情報処理装置から発信された信号を受信するステップと、信号を受信した時刻に関する時刻情報、信号の受信強度に基づく強度情報および第一識別情報を、第二の情報処理装置の第二識別情報とともにサーバ装置に送信するステップとを実行させ、サーバ装置に、第二の情報処理装置から受信した時刻情報、強度情報、第一識別情報および第二識別情報を互いに関連付けて記憶するステップと、特定の第一の情報処理装置の特定の第一識別情報の指定を受け付けた場合に、特定の第一識別情報に関連付けて記憶された特定の第二識別情報に基づいて、当該特定の第二識別情報に関連付けて記憶された１以上の他の第一識別情報を抽出するステップとを実行させることを特徴とする。

【００１８】

本開示の実施形態におけるコンピュータプログラムは、信号を発信する機能を有する第一の情報処理装置と、信号を受信する機能を有する第二の情報処理装置と、第二の情報処理装置とインターネットを介して接続可能なサーバ装置とを備える情報処理システムにお

いて実行されるコンピュータプログラムであって、第二の情報処理装置に、第一の情報処理装置から発信された第一の情報処理装置の第一識別情報を含む信号を受信する機能と、信号を受信した時刻に関する時刻情報、信号の受信強度に基づく強度情報および第一識別情報を、第二の情報処理装置の第二識別情報とともにサーバ装置に送信する機能とを実現させ、サーバ装置は、第二の情報処理装置から受信した時刻情報、強度情報、第一識別情報および第二識別情報を互いに関連付けて記憶し、特定の第一の情報処理装置の特定の第一識別情報の指定を受け付けた場合に、特定の第一識別情報に関連付けて記憶された特定の第二識別情報に基づいて、当該特定の第二識別情報に関連付けて記憶された１以上の他の第一識別情報を抽出することを特徴とする。

【発明の効果】

【００１９】

本開示によれば、感染者の行動履歴の特定および濃厚接触者の抽出を容易に確実に行うことが可能な情報処理システム、情報処理方法およびコンピュータプログラムを提供することができる。

【図面の簡単な説明】

【００２０】

【図１】本開示の実施形態に係る情報処理システムの構成の一例を示したシステム構成図である。

【図２】本開示の実施形態にかかる第一の情報処理装置のハードウェア構成を示すハードウェア構成図である。

【図３】本開示の実施形態にかかる第一の情報処理装置の機能構成を示す機能構成図である。

【図４】本開示の実施形態にかかる第二の情報処理装置の機能構成を示す機能構成図である。

【図５】本開示の実施形態にかかるサーバ装置の機能構成を示す機能構成図である。

【図６】本開示の実施形態にかかるサーバ装置の記憶部に記憶されるデータテーブルの一例を示したイメージ図である。

【図７】本開示の実施形態にかかるサーバ装置の記憶部に記憶されるデータテーブルの一例を示したイメージ図である。

【図８】本開示の実施形態にかかるサーバ装置の機能構成の他の例を示す機能構成図である。

【図９】本開示の実施形態にかかる第二の情報処理装置の機能構成の他の例を示す機能構成図である。

【図１０】本開示の実施形態に係るＩｏＴ接続システムの構成の一例を示したシステム構成図である。

【図１１】本開示の実施形態に係るＩｏＴ接続システムの複数のプライベートクラウドの一例を示したイメージ図である。

【図１２】本開示の実施形態に係るＩｏＴ接続システムのプライベートクラウドに接続される複数の第一のデバイスの一例を示したイメージ図である。

【図１３】本開示の実施形態に係るＩｏＴ接続システムで提供されるサービスの流れの一例を示したイメージ図である。

【図１４】本開示の実施形態にかかるＩｏＴルータのハードウェア構成を示すハードウェア構成図である。

【図１５】本開示の実施形態に係るＩｏＴ接続システムで提供されるサービスの流れの一例を示したイメージ図である。

【図１６】本開示の実施形態に係るＩｏＴ接続システムの接続界面を説明するためのイメージ図である。

【図１７】本開示の実施形態に係るＩｏＴ接続システムで提供されるサービスの流れの他の例を示したイメージ図である。

【図１８】本開示の実施形態に係るＩｏＴ接続システムで提供される仮想ドライバ機能の

流れの一例を示したイメージ図である。
【図１９】本開示の実施形態に係るＩｏＴ接続システムで提供される仮想ドライバ機能の流れの他の例を示したイメージ図である。
【図２０】本開示の実施形態に係る情報処理方法のフローの一例を示したフロー図である。
【図２１】本開示の実施形態に係る情報処理システムの構成の他の例を示した概念図である。
【発明を実施するための形態】
【００２１】
本開示の情報処理システムの実施形態について、図面を参照しながら説明する。
【００２２】
図１に一例として示されるように、本開示の情報処理システム１０００は、第一の情報処理装置１００と、第二の情報処理装置２００と、サーバ装置３００とを備えるものである。
【００２３】
第一の情報処理装置１００は、信号を発信する機能を有する装置である。
【００２４】
信号を発する機能とは、例えば、Ｂｌｕｅｔｏｏｔｈ（登録商標） Ｌｏｗ Ｅｎｅｒｇｙ（ＢＬＥ）やＷｉ－Ｆｉ等の無線技術を使い、当該信号を受信可能な装置に対して情報を発信することができる機能である。
【００２５】
第一の情報処理装置１００は、上記信号を発する機能を有する装置であれば特に限定されないが、一例としてスマートフォンやタブレット等の情報処理装置とすることができる。
【００２６】
そして、上記信号を発する機能は、専用のアプリケーションをインストールすることにより第一の情報処理装置１００により実現されることができる。
【００２７】
第二の情報処理装置２００は、上記信号を受信する機能を有する装置である。
【００２８】
第二の情報処理装置２００は、上記信号を受信する機能を有する装置であれば特に限定されないが、一例としてスマートフォンやタブレット等の情報処理装置とすることができる。また、第二の情報処理装置２００として後述するＩｏＴルータを用いてもよい。
【００２９】
そして、上記信号を受信する機能は、専用のアプリケーションをインストールすることにより第二の情報処理装置２００により実現されることができる。
【００３０】
サーバ装置３００は、第二の情報処理装置２００とインターネットを介して接続可能な装置である。
【００３１】
ここで、図２を用いて、第一の情報処理装置１００のハードウェア構成について説明する。第一の情報処理装置１００は、プロセッサ１０１と、メモリ１０２と、ストレージ１０３と、入出力インターフェース（入出力Ｉ／Ｆ）１０４と、通信インターフェース（通信Ｉ／Ｆ）１０５とを含むことができる。各構成要素は、バスＢを介して相互に接続される。
【００３２】
第一の情報処理装置１００は、プロセッサ１０１と、メモリ１０２と、ストレージ１０３と、入出力Ｉ／Ｆ１０４と、通信Ｉ／Ｆ１０５との協働により、本実施形態に記載される機能、方法を実現することができる。
【００３３】

プロセッサ１０１は、ストレージ１０３に記憶されるプログラムに含まれるコード又は命令によって実現する機能、及び／又は、方法を実行する。プロセッサ２０１は、例えば、中央処理装置（ＣＰＵ）、ＭＰＵ（Micro Processing Unit）、ＧＰＵ（Graphics Processing Unit）、マイクロプロセッサ（microprocessor）、プロセッサコア（processor core）、マルチプロセッサ（multiprocessor）、ＡＳＩＣ（Application-Specific Integrated Circuit）、ＦＰＧＡ（Field Programmable Gate Array）等を含み、集積回路（ＩＣ（Integrated Circuit）チップ、ＬＳＩ（Large Scale Integration））等に形成された論理回路（ハードウェア）や専用回路によって各実施形態に開示される各処理を実現してもよい。また、これらの回路は、１又は複数の集積回路により実現されてよく、各実施形態に示す複数の処理を１つの集積回路により実現されることとしてもよい。また、ＬＳＩは、集積度の違いにより、ＶＬＳＩ、スーパーＬＳＩ、ウルトラＬＳＩ等と呼称されることもある。

【００３４】

メモリ１０２は、ストレージ１０３からロードしたプログラムを一時的に記憶し、プロセッサ１０１に対して作業領域を提供する。メモリ１０２には、プロセッサ１０１がプログラムを実行している間に生成される各種データも一時的に格納される。メモリ１０２は、例えば、ＲＡＭ（Random Access Memory）、ＲＯＭ（Read Only Memory）等を含む。

【００３５】

ストレージ１０３は、プログラムを記憶する。ストレージ１０３は、例えば、ＨＤＤ（Hard Disk Drive）、ＳＳＤ（Solid State Drive）、フラッシュメモリ等を含む。

【００３６】

通信Ｉ／Ｆ１０５は、ネットワークアダプタ等のハードウェアや通信用ソフトウェア、及びこれらの組み合わせとして実装され、ネットワークを介して各種データの送受信を行う。当該通信は、有線、無線のいずれで実行されてもよく、互いの通信が実行できるのであれば、どのような通信プロトコルを用いてもよい。通信Ｉ／Ｆ１０５は、ネットワークを介して、他の情報処理装置との通信を実行する。通信Ｉ／Ｆ１０５は、各種データをプロセッサ１０１からの指示に従って、他の情報処理装置に送信する。また、通信Ｉ／Ｆ１０５は、他の情報処理装置から送信された各種データを受信し、プロセッサ１０１に伝達する。

【００３７】

入出力Ｉ／Ｆ１０４は、第一の情報処理装置１００に対する各種操作を入力する入力装置、及び、第一の情報処理装置１００で処理された処理結果を出力する出力装置を含む。入出力Ｉ／Ｆ１０４は、入力装置と出力装置が一体化していてもよいし、入力装置と出力装置とに分離していてもよい。

【００３８】

入力装置は、ユーザからの入力を受け付けて、当該入力に係る情報をプロセッサ１０１に伝達できる全ての種類の装置のいずれか、又は、その組み合わせにより実現される。入力装置は、例えば、タッチパネル、タッチディスプレイ、キーボード等のハードウェアキーや、マウス等のポインティングデバイス、カメラ（画像を介した操作入力）、マイク（音声による操作入力）を含む。

【００３９】

出力装置は、プロセッサ１０１で処理された処理結果を出力する。出力装置は、例えば、タッチパネル、スピーカ等を含む。

【００４０】

上記第二の情報処理装置２００およびサーバ装置３００についても、上記第一の情報処理装置１００と同様のハードウェア構成とすることができる。

【００４１】

そして、本開示における第一の情報処理装置１００は、図３に示されるように、発信部１１０を有する。

【００４２】

発信部１１０は、第一の情報処理装置１００の第一識別情報を含む信号を発信するものである。

【００４３】

第一識別情報は、第一の情報処理装置１００を特定可能な識別情報であれば特に限定されるものではない。第一識別情報の例として、ＵＤＩＤ（Unique Device IDentifier）やＵＵＩＤ（Universally Unique IDentifier）等を用いることができるが、プライバシー・セキュリティー上の観点からＵＵＩＤを第一識別情報とするのが好ましい。

【００４４】

第二の情報処理装置２００は、図４に示されるように、受信部２１０と、送信部２２０とを有する。

【００４５】

受信部２１０は、第一の情報処理装置１００から発信された信号を受信するものである。

【００４６】

送信部２２０は、時刻情報、強度情報および第一識別情報を、第二の情報処理装置２００の第二識別情報とともにサーバ装置３００に送信するものである。

【００４７】

時刻情報は、上記信号を受信した時刻に関する情報である。かかる時刻情報は日付および時刻を含み、時刻は時分秒を含むものとすることができる。

【００４８】

強度情報は、信号の受信強度に基づく情報である。かかる受信強度に関する情報は受信した電波の強度を示す電波強度に加え、基準強度を含むことができる。そして、これらから第一の情報処理装置１００と第二の情報処理装置２００との推定距離を算出しておくことも可能であり、この推定距離を受信強度に基づく情報としてもよい。かかる推定距離の算出については、第二の情報処理装置２００で行うものとしてもよいし、サーバ装置３００で行うものとしてもよい。

【００４９】

第二識別情報は、第二の情報処理装置２００を特定可能な識別情報であれば特に限定されるものではない。第二識別情報の例として、第一識別情報と同様に、ＵＤＩＤ（Unique Device IDentifier）やＵＵＩＤ（Universally Unique IDentifier）等を用いることができるが、プライバシー・セキュリティー上の観点からＵＵＩＤを第二識別情報とするのが好ましい。このＵＵＩＤは、上述した専用のアプリケーションにより発行される数値であって、個人情報を含まないものとすることができる。

【００５０】

そして、サーバ装置３００は、図５に示されるように、記憶部３１０と、受付部３２０と、抽出部３３０とを有する。

【００５１】

記憶部３１０は、第二の情報処理装置２００から受信した時刻情報、強度情報、第一識別情報および第二識別情報を互いに関連付けて記憶するものである。

【００５２】

図６は、記憶部３１０が記憶されるデータテーブルの一例を示したものである。図６に示されるように、第二の情報処理装置２００が、受信した信号を発信した第一の情報処理装置１００とその受信時刻、電波強度とともに記憶される。

【００５３】

なお、図６では時刻情報が各第一識別情報に１つのみ示しているが、信号を最初に受信した時刻から受信しなくなった時刻まで所定の間隔で記憶されることができる。

【００５４】

受付部３２０は、特定の第一の情報処理装置１００の特定の第一識別情報の指定を受け付けるものである。

【００５５】

上記指定は、本開示における情報処理システムを利用するユーザにより所定の情報処理端末を介して行われるものとする。

【００５６】

そして、特定の第一の情報処理装置１００は、感染者の所有するスマートフォン等の携帯端末とすることができる。

【００５７】

この場合、上記指定を行うユーザの例としては、感染者の行動履歴を追跡する者、例えば、保健所の担当者や医療従事者などであるが、これらの者に限定されるものではない。

【００５８】

例えば、感染者自身が、第一の情報処理装置１００から感染症に感染した旨の情報をサーバ装置３００に送信し、自分の特定の第一の情報処理装置１００Ａの特定の第一識別情報を指定することもできる。

【００５９】

抽出部３３０は、受付部３２０が特定の第一の情報処理装置１００の特定の第一識別情報の指定を受け付けた場合に、特定の第一識別情報に関連付けて記憶された特定の第二識別情報に基づいて、当該特定の第二識別情報に関連付けて記憶された１以上の他の第一識別情報を抽出することを特徴とする。

【００６０】

特定の第一の情報処理装置１００Ａの特定の第一識別情報が図６における「１００００２」であった場合に抽出される他の第一識別情報のイメージを示した例を図７に示す。

【００６１】

なお、抽出部３３０は、時刻情報および／または強度情報に基づくフィルタ条件に基づいて、他の第二識別情報を抽出してもよい。詳細については後述する。

【００６２】

以上のように、本開示における情報処理システムによれば、特定の第一の情報処理装置を有する者が、いつ何処にいたかという行動履歴を容易に確実に取得することができ、かつ、上記者と同じ場所にいた者を容易に確実に特定することができるようになる。すなわち、本開示における情報処理システムは、感染者のトレーサビリティを可能にする。

【００６３】

例えば、会社内の部屋に第二の情報処理装置２００を設置しておけば、感染者が生じた場合に、感染者がどの部屋にどのくらいの時間滞在したか、濃厚接触者は誰かなどの情報を迅速に抽出することができる。

【００６４】

濃厚接触者を迅速に特定することで、会社内に出入りした者全員ではなく、濃厚接触者のみを自宅待機させるなどの効果的な対応を迅速にとることができる。その結果、事務所の全閉鎖といった事態を避けることができ、ＢＣＰ（事業継続性）対策にもなる。

【００６５】

抽出部３３０は、特定の第一識別情報の指定を受け付けた場合に、特定の第一識別情報に関連付けて記憶された特定の第二識別情報および当該特定の第一識別情報を含む信号を受信した特定の時刻に関する特定時刻情報に基づいて、当該特定時刻情報に関連付けて記憶された１以上の他の第一識別情報を抽出することができる。

【００６６】

すなわち、抽出部３３０は、時刻情報に基づくフィルタ条件に基づいて、他の第二識別情報を抽出することができる。

【００６７】

特定の時刻に関する特定時刻情報は、一例として、特定の第一の情報処理装置が信号を最初に受信した時刻から受信しなくなった時刻まで所定の間隔で記憶される時刻のすべてとすることができる。

【００６８】

あるいは、特定の時刻に関する特定時刻情報は、他の例として、特定の第一の情報処理

装置が信号を最初に受信した時刻、および、当該最初に受信した時刻から受信しなくなった時刻までの時間に基づいて算出される滞在時間を含むことができる。

【００６９】

そして、特定時刻情報に関連する時刻情報とは、上記特定時刻情報に基づいて設定された、感染者と濃厚接触の可能性が高い時刻とすることができる。

【００７０】

具体的には、感染者と同じ場所・時間にいた者に加えて、感染者と同じ場所に、感染者がいなくなった後、予め設定された所定の時間が経過するまでの間にいた者も濃厚接触者として抽出することができる。

【００７１】

さらに、抽出部３３０は、強度情報に基づくフィルタ条件に基づいて、他の第二識別情報を抽出してもよい。

【００７２】

すなわち、感染者が第二の情報処理装置２００が設置されたある部屋にいると推定される場合に、強度情報に基づいて当該部屋の外にいると推定される者については、濃厚接触者として抽出しなくともよい。

【００７３】

サーバ装置３００は、図８に示すように、さらに、通知部３４０を有することができる。

【００７４】

通知部３４０は、特定の第一識別情報の指定を受け付けた場合に抽出された１以上の第一識別情報を有する第一の情報処理装置１００に対して、特定の情報を通知する。

【００７５】

特定の情報とは、一例として、第二の情報処理装置２００の近くにいたことを知らせる内容の情報とすることができる。かかる情報には、さらに、感染症に対応が可能な近くの施設の情報、相談窓口の電話番号などの情報を含めてもよい。

【００７６】

通知は、プッシュ通知の技術を利用して強制的に行うのが好ましい。

【００７７】

第二の情報処理装置２００は、図９に示されるように、取得部２３０と、環境情報送信部２４０とをさらに有することができる。

【００７８】

取得部２３０は、設置場所の環境情報を所定のセンサから取得する。

【００７９】

所定のセンサは設置場所の環境情報を測定可能な物であれば特に限定されるものではないが、一例として、室温センサ、湿度センサ、照度センサ、気圧センサ、騒音センサ、各種ガス濃度センサ、不快指数センサ、熱中症警戒度センサの少なくとも一つとすることができる。

【００８０】

ガスセンサが測定可能なガスの例としてはCO_2、揮発性有機溶媒量線などとすることができる。

【００８１】

環境情報送信部２４０は、当該環境情報を受信した時刻に関する時刻情報を、環境情報とともにサーバ装置３００に送信する。

【００８２】

そして、サーバ装置３００の記憶部３１０は、第二の情報処理装置２００から受信した環境情報および時刻情報を、第二識別情報に関連付けて記憶することができる。

【００８３】

そして、サーバ装置３００の抽出部３３０は、第二の情報処理装置２００から受信した環境情報が特定の条件を満たす場合に、第二識別情報に関連付けて記憶された１以上の第

一識別情報を抽出してもよい。
【００８４】
特定の条件とは、いわゆる三密（密閉・密集・密接）の条件を満たす条件とすることができる。具体的な数値については予め適切に設定されることができる。
【００８５】
また、
上述した通知部３４０は、特定の条件を満たす場合に抽出された１以上の第一識別情報を有する第一の情報処理装置１００の少なくとも一つに対して、注意情報を通知することができる。
【００８６】
すなわち、部屋が三密の条件を満たしてしまっている場合に、会議の開催者などに対して換気などを促す等の注意情報を通知することができる。
【００８７】
あるいは、環境情報が特定の条件を満たす場合に、室内のＩｏＴデバイス（エアコン、空気清浄機、加湿器等）を自動制御することにより三密を解消させるようにしてもよい。ＩｏＴデバイスの自動制御については、後述するように第二の情報処理装置２００がＩｏＴルータである場合に適用することができる。
【００８８】
そして、本開示における第二の情報処理装置２００は、ＩｏＴルータとすることができる。
【００８９】
ＩｏＴルータは、図１０に示されるように、クラウド上で実現されるＩｏＴハブ１２００、および、ローカルにありＩｏＴハブ１２００と接続されるＩｏＴルータ１３００を備えるＩｏＴ接続システム２０００におけるＩｏＴルータ１３００である。
【００９０】
ここで、本開示の実施形態におけるＩｏＴ接続システム２０００の実施形態について、図面を参照しながら説明する。
【００９１】
図１０に示すように、本開示の実施形態におけるＩｏＴ接続システム２０００は、ＩｏＴハブ１２００およびＩｏＴルータ１３００を備えるものとする。
【００９２】
ＩｏＴハブ１２００は、クラウド上で実現されるものとする。具体的には、ＩｏＴハブ１２００は、クラウド内でホストされているマネージドサービスであり、ＩｏＴアプリケーション（以下「ＩｏＴアプリ」という。）とＩｏＴデバイスとの間の双方向通信に対する中継器として機能する。
【００９３】
ＩｏＴルータ１３００は、ローカルにあり、ＩｏＴハブ１２００とＷＡＮ（Wide Area Network）により接続されるものとする。
【００９４】
具体的には、ＩｏＴルータ１３００は、宅内ネットワークなどインターネットに接続されていないＩｏＴデバイスがＩｏＴハブ１２００に接続することを実現するものである。
【００９５】
そして、ＩｏＴハブ１２００は、第一のドライバ１２１０または第二のドライバ１２２０の少なくとも一方を有する。
【００９６】
第一のドライバ１２１０および第二のドライバ１２２０は、各ＩｏＴデバイスのメーカごとの仕様の違いを吸収するものである。
【００９７】
第一のドライバ１２１０は、第一のデバイス１４１０が接続可能なプライベートクラウド１４００と当該ＩｏＴハブ１２００とを接続するためのものである。

【００９８】
一例として、第一のデバイス１４１０とプライベートクラウド１４００とはＬＡＮ（Local Area Network）またはＷＡＮによる接続とし、プライベートクラウド１４００と第一のドライバ１２１０もＬＡＮまたはＷＡＮによる接続とするのが好ましい。
【００９９】
プライベートクラウド１４００は、第一のデバイス１４１０の事業者により提供されるものである。図１０ではプライベートクラウド１４００が一つである場合が示されているが、この数は一つに限られるものではなく、複数のプライベートクラウド１４００がＩｏＴハブ１２００に接続されることができる。また、ＩｏＴハブ１２００は、複数の第一のドライバ１２１０を有してもよい。
【０１００】
図１１、異なる事業者Ａ，Ｂにより提供される２つのプライベートクラウド１４００Ａ，１４００Ｂの詳細を示したものである。図１１に示されるように、プライベートクラウド１４００Ａは、事業者Ａが提供するアプリケーションＡ（以下、「アプリＡ」とする。）と接続され、第一のデバイス１４１０に対してアプリＡによるサービスを提供するものである。
【０１０１】
同様に、プライベートクラウド１４００Ｂは、事業者Ｂが提供するアプリケーションＢ（以下、「アプリＢ」とする。）と接続され、第一のデバイス１４１０に対してアプリＢによるサービスを提供するものである。
【０１０２】
なお、図１０、１１ではプライベートクラウド１４００に第一のデバイス１４１０が一つだけ接続されている例が示されているが、図１２に示すように、一つのプライベートクラウド１４００に複数の第一のデバイス１４１０が接続されてもよい。
【０１０３】
第一のデバイス１４１０は、事業者がプライベートクラウドを提供しているデバイスとすることができる。一例として、リモートロック機能を有する電子錠、ＡＩスピーカ、リモート操作が可能な介護ベッドなどが挙げられるが、特にこれらに限定されるものではない。
【０１０４】
図１０に戻り、第二のドライバ１２２０は、第二のデバイス１５１０とＩｏＴハブ１２００とを直接接続するためのものである。
【０１０５】
第二のデバイス１５１０は、インターネット上にあるＩｏＴハブ１２００とＷＡＮにより接続されることができる（ＬＡＮ経由でもよい）。
【０１０６】
なお、図１０では第二のドライバ１２２０に第二のデバイス１５１０が一つだけ接続されている例が示されているが、一つの第二のドライバ１２２０に複数の第二のデバイス１５１０が接続されてもよい。また、ＩｏＴハブ１２００は複数の第二のドライバ１２２０を有してもよい。
【０１０７】
第二のデバイス１５１０は、事業者がプライベートクラウドを提供していないデバイスとすることができる。一例として、扇風機、エアコン、窓、カーテン、照明などとすることができるが、特にこれらに限定されるものではない。
【０１０８】
そして、ＩｏＴルータ１３００は、第三のドライバ１３１０を有する。また、ＩｏＴルータ１３００は、複数の第三のドライバ１３１０を有してもよい。
【０１０９】
第三のドライバ１３１０は、第三のデバイス１６１０と当該ＩｏＴルータ１３００とを接続するためのものである。

【０１１０】
一例として、第三のデバイス１６１０と第三のドライバ１３１０とはＬＡＮによる接続とし、ＩｏＴルータ１３００とＩｏＴハブ１２００とはＷＡＮによる接続とするのが好ましい。
【０１１１】
第三のデバイス１６１０は、上述したとおり、宅内ネットワークなどインターネットに接続されていないＩｏＴデバイスとすることができる。また、第三のデバイス６１０は、セキュリティ、プライバシーおよびセーフティ上の観点で、直接ＩｏＴハブ１２００と接続すべきでないデバイスとすることができる。一例として、ガスコンロ、顔認証デバイス、センサ情報収集用データロガーなどとすることができるが、特にこれに限定されるものではない。ただし、後述する災害時のリスク低減の観点から、どのようなデバイスであっても第三のデバイス１６１０としてＩｏＴルータ１３００へ接続させるようにしてもよい。
【０１１２】
このように、本発明のＩｏＴ接続システム２０００は、すべてのデバイスをクラウド上のＩｏＴハブ１２００に直接的に接続させるものではなく、一部のデバイスをローカル上のＩｏＴルータ１３００に接続させるハイブリッドタイプのＩｏＴ接続システムである。
【０１１３】
以上によれば、直接接続されたＩｏＴデバイス同士のみならず、従来のプライベートクラウドに接続されたＩｏＴデバイス同士も、容易に相互接続させることが可能となる。
【０１１４】
これにより、決まったメーカのＩｏＴデバイス同士しか繋がっていなかった従来とは異なり、様々なメーカのＩｏＴデバイスを容易に相互接続させることができる。また、様々なメーカのＩｏＴデバイスを相互接続させることにより、従来にはなかったユニークなサービスを創造することができるようになる。
【０１１５】
例えば、本発明のＩｏＴ接続システム２０００によれば、図１３に示すように、外部のサーバからの緊急地震速報を受信したら、ガスコンロに消火信号を送り、玄関ドアのカギを解錠するといったサービスを実現することも容易に可能である。
【０１１６】
ここで、図１４を用いて、情報処理端末（ＩｏＴハブ）１２００のハードウェア構成について説明する。情報処理端末１２００は、プロセッサ１２０１と、メモリ１２０２と、ストレージ１２０３と、入出力インターフェース（入出力Ｉ／Ｆ）１２０４と、通信インターフェース（通信Ｉ／Ｆ）１２０５とを含むことができる。各構成要素は、バスＢを介して相互に接続される。
【０１１７】
情報処理端末１２００は、プロセッサ１２０１と、メモリ１２０２と、ストレージ１２０３と、入出力Ｉ／Ｆ１２０４と、通信Ｉ／Ｆ１２０５との協働により、本実施形態に記載される機能、方法を実現することができる。
【０１１８】
プロセッサ１２０１は、ストレージ１２０３に記憶されるプログラムに含まれるコード又は命令によって実現する機能、及び／又は、方法を実行する。プロセッサ１２０１は、例えば、中央処理装置（ＣＰＵ）、ＭＰＵ（Micro Processing Unit）、ＧＰＵ（Graphics Processing Unit）、マイクロプロセッサ（microprocessor）、プロセッサコア（processor core）、マルチプロセッサ（multiprocessor）、ＡＳＩＣ（Application-Specific Integrated Circuit）、ＦＰＧＡ（Field Programmable Gate Array）等を含み、集積回路（ＩＣ（Integrated Circuit）チップ、ＬＳＩ（Large Scale Integration））等に形成された論理回路（ハードウェア）や専用回路によって各実施形態に開示される各処理を実現してもよい。また、これらの回路は、１又は複数の集積回路により実現されてよく、各実施形態に示す複数の処理を１つの集積回路により実現されることとしてもよい。また

、ＬＳＩは、集積度の違いにより、ＶＬＳＩ、スーパーＬＳＩ、ウルトラＬＳＩ等と呼称されることもある。

【０１１９】

メモリ１２０２は、ストレージ１２０３からロードしたプログラムを一時的に記憶し、プロセッサ１２０１に対して作業領域を提供する。メモリ１２０２には、プロセッサ１２０１がプログラムを実行している間に生成される各種データも一時的に格納される。メモリ１２０２は、例えば、ＲＡＭ（Random Access Memory）、ＲＯＭ（Read Only Memory）等を含む。

【０１２０】

ストレージ１２０３は、プログラムを記憶する。ストレージ１２０３は、例えば、ＨＤＤ（Hard Disk Drive）、ＳＳＤ（Solid State Drive）、フラッシュメモリ等を含む。

【０１２１】

通信Ｉ／Ｆ１２０５は、ネットワークアダプタ等のハードウェアや通信用ソフトウェア、及びこれらの組み合わせとして実装され、ネットワークを介して各種データの送受信を行う。当該通信は、有線、無線のいずれで実行されてもよく、互いの通信が実行できるのであれば、どのような通信プロトコルを用いてもよい。通信Ｉ／Ｆ１２０５は、ネットワークを介して、他の情報処理装置との通信を実行する。通信Ｉ／Ｆ１２０５は、各種データをプロセッサ１２０１からの指示に従って、他の情報処理装置に送信する。また、通信Ｉ／Ｆ１２０５は、他の情報処理装置から送信された各種データを受信し、プロセッサ１２０１に伝達する。

【０１２２】

入出力Ｉ／Ｆ１２０４は、情報処理端末１２００に対する各種操作を入力する入力装置、及び、情報処理端末１２００で処理された処理結果を出力する出力装置を含む。入出力Ｉ／Ｆ１３０４は、入力装置と出力装置が一体化していてもよいし、入力装置と出力装置とに分離していてもよい。

【０１２３】

入力装置は、ユーザからの入力を受け付けて、当該入力に係る情報をプロセッサ１２０１に伝達できる全ての種類の装置のいずれか、又は、その組み合わせにより実現される。入力装置は、例えば、タッチパネル、タッチディスプレイ、キーボード等のハードウェアキーや、マウス等のポインティングデバイス、カメラ（画像を介した操作入力）、マイク（音声による操作入力）を含む。

【０１２４】

出力装置は、プロセッサ１２０１で処理された処理結果を出力する。出力装置は、例えば、タッチパネル、スピーカ等を含む。

【０１２５】

上記ＩｏＴルータ１３００についても、上記ＩｏＴハブ１２００と同様のハードウェア構成とすることができる。

【０１２６】

また、ＩｏＴルータ１３００は、所定の基地局と通信可能な情報処理端末とするのが好ましい。

【０１２７】

所定の基地局と通信可能な情報処理端末は、一例として、スマートフォンやタブレット端末などのＳＩＭカードを挿入して用いる情報処理端末である。ＩｏＴルータ１３００とＩｏＴハブ１２００との間の通信容量はひと月に１００Ｍバイト以下の低容量であることから、ＩｏＴルータ１３００には通信容量が少ない低額なＳＩＭカードを挿入すれば足りる。一例として、一つの会議室の周辺に平均１０ビーコン（人）が存在し、５分単位で情報をサーバに送信した場合には必要な通信容量は１７．３Ｍ／会議室（月）である。

【０１２８】

また、ＩｏＴルータ１３００は、バッテリを含むものとする。かかるバッテリは、充電することにより電力を蓄えることができるものである。ＩｏＴルータ１３００は、満充電

から３日程度は、電源に接続せずに本開示における機能を実現することができる。平常時（後述する特定の状況下に無い場合）には、ＩｏＴルータ１３００は、電源に接続して使用されるものとする。

【０１２９】

そして、第三のデバイス１６１０は、特定の状況下において、ＩｏＴルータ１３００が備えるテザリング機能を介してＩｏＴハブ１２００に接続されることができる。

【０１３０】

特定の状況は、第三のデバイス１６１０と所定の無線／有線ＬＡＮとの接続が途絶えた状況、ＩｏＴルータ１３００と所定の無線／有線ＬＡＮとの接続が途絶えた状況などとすることができるが、これに限られるものではない。

【０１３１】

この特定の状況に陥る原因としては、停電が挙げられるが、これに限られるものではなく、Ｗｉ－Ｆｉ（登録商標）ルータの故障や接続不良等などが原因である場合もある。

【０１３２】

また、テザリング機能としては公知の技術を用いることができ、Ｗｉ－Ｆｉテザリング、Ｂｌｕｅｔｏｏｔｈ（登録商標）テザリング、ＵＳＢテザリングなどの手法を用いることができる。

【０１３３】

以上の構成によれば、プライベートクラウドごとにサイロ化状態になっている暮らしのＩｏＴを、インターネットを介して自由に相互接続して魅力的なサービスを提供することができる。

【０１３４】

具体的には、本開示によれば、直接接続されたＩｏＴデバイス同士のみならず、従来のプライベートクラウドに接続されたＩｏＴデバイス同士も、容易に相互接続させることが可能となる。

【０１３５】

また、以上の構成によれば、第三のデバイス１６１０が、特定の状況下において、ＩｏＴルータ１３００が備えるテザリング機能によりＩｏＴハブ１２００に接続されることで、災害等においてＩｏＴデバイスがネットワークに接続できない状態であっても、サービスを継続して利用することができるようになる。

【０１３６】

また、ＩｏＴルータ１３００は、管理者装置によりＲｅｍｏｔｅ　Ｃｏｎｔｒｏｌ（遠隔操作）が可能なものとするのが好ましい。かかる構成によれば、ＩｏＴルータの一つ一つをフルサポートすることができるようになる。

【０１３７】

なお、上記遠隔操作は、管理者装置およびＩｏＴルータ１３００の双方に専用のアプリケーションをインストールしておくことで実現される。なお、遠隔操作のサポートのし易さを考慮して、ＩｏＴルータ１３００としての情報処理端末は、Ａｎｄｒｏｉｄ端末を用いるのが好ましい。

【０１３８】

また、ＩｏＴルータ１３００は、管理者装置によりＣＤＭ（Connected Device Management：多様なデバイス管理）されるものとするのが好ましい。かかるＣＤＭは、既知のＭＤＭ（Mobile Device Management）の手法を用いて実現されることができる。かかる構成によれば、膨大数の世帯に設置されるＩｏＴルータを即時に一元管理し、遠隔監視・更新することができるようになる。また、ＣＤＭにより、デバイスの設定やアプリの配布、更新を遠隔監視制御することができるようになる。これにより、コスト削減と業務効率化を実現することができる。

【０１３９】

また、ＩｏＴハブ１２００へは認証されたアプリやデバイスしか接続できないが、ＩｏＴルータ１３００は、ＩｏＴハブ１２００をローカル（宅内等）に延長し、ローカルでな

ければ実現できないリアルタイム性、セキュリティやプライバシーの確保、通信量の削減などに対応させることができる。

【０１４０】

また、ＩｏＴルータ１３００を情報処理端末とすることで、顧客のスマートフォンや家庭内のインターネット回線を使用する必要がなくなり、想定外のトラブルが発生するリスクを低減させることができる。

【０１４１】

また、本発明のＩｏＴ接続システム２０００は、第一のドライバ１２１０、第二のドライバ１２２０および第三のドライバ１３１０を作成するのにユーザが記述すべき情報は、デバイス定義およびコマンド定義に関する情報に限られてもよい。

【０１４２】

ここで、第一のドライバ１２１０、第二のドライバ１２２０および第三のドライバ１３１０を作成する方法について説明を行う。なお、作成者は、ＩｏＴデバイスの製造開発に関するユーザ、あるいは、本発明のＩｏＴ接続システムの提供に関するユーザとすることができる。

【０１４３】

なお、第一のドライバ１２１０および第二のドライバ１２２０と、第三のドライバ１３１０とは、同内容の情報が記述されればよく、プログラミング言語が異なるものであってもよい。

【０１４４】

初めに、作成者は、デバイス定義として、利用機器一覧を定義する。一例として、利用機器として「気象センサ」、「屋内センサ」、「屋外センサ」、「不審者センサ」、「承認センサ」、「電力センサ」を定義する場合には、これらの名称およびそのＩＤとなる「weather」、「inhouse」、「outdoor」、「security」、「approve」、「power」を記述する。

【０１４５】

続いて、作成者は、コマンド定義として、利用可能コマンドを定義する。一例として、「屋外センサ」の利用可能コマンドを定義する場合には、センサ値の観測コマンドを記述する。観測コマンドは、一例として、「観測」，「ゲット」，「屋外を観測します」などとすることができる。

【０１４６】

以上のデバイス定義およびコマンド定義に関する情報を、作成者が穴埋め形式でプログラムに埋めていくことにより、第一のドライバ１２１０、第二のドライバ１２２０、第三のドライバ１３１０を完成させることができる。その他の部分については、ＳＤＫとして提供者から提供されることができる。

【０１４７】

ＳＤＫ部分は、受信したコマンドでのデバイス操作処理に関する部分、収集したセンサデータ／操作結果データの前処理に関する部分、ＩｏＴハブへのデータ送信処理に関する部分を含むものとする。

【０１４８】

以上の構成によれば、様々な形態のＩｏＴデバイスに対するドライバを簡易に完成させることができるため、ＩｏＴデバイスを柔軟にかつ容易に接続可能なＩｏＴ接続システムを実現することが可能となる。

【０１４９】

通常、デバイスの開発に係るエンジニアは、Ｗｅｂ開発のエンジニアとは取得している技術の分野が異なり、デバイスをＩｏＴハブに繋ぐことができる技術レベルを有していない者も多い。

【０１５０】

そのため、本開示のように、どのドライバ用プログラムに対しても共通の穴埋め形式の

簡易な手法で作成が可能であることは、非常に有益である。これにより、ＩｏＴデバイスのＩｏＴハブへの接続に係る開発コストや開発期間を従来よりも抑えることができる。

【０１５１】

また、開発コストの低減により、扇風機とエアコンのように掛けられるコストの許容値に差がある場合であっても、平等にＩｏＴハブへの接続を実現することができる。

【０１５２】

続いて、本開示におけるＩｏＴ接続システム２０００に係るＩｏＴハブ１２００とＩｏＴアプリとの接続について説明する。

【０１５３】

図１０に示されているように、ＩｏＴハブ１２００は、ＩｏＴアプリ１７００を利用するためのＷｅｂＡＰＩ１２３０を有することができる。なお、図１０に示すように、ＩｏＴアプリ１７００はサービスの数だけ接続されることができ、それぞれがＷｅｂＡＰＩ１２３０を使用して接続されることができる。

【０１５４】

ＩｏＴアプリ１７００は、アプリ内にＩｏＴデバイス（センサ）からのデータ取得ロジックおよび／またはＩｏＴデバイスの操作ロジックを記述することで作成される。

【０１５５】

データ取得ロジックは、取得したセンサデータの前処理を行う部分と、ＩｏＴハブ１２００のＡＰＩへの送信を行う部分とで構成される。必要な情報は、ＩｏＴ接続システム２０００の運営者から提供される接続先ＵＲＬ、運営者から提供されるＡＰＩキー、デバイス情報および実行コマンドである。

【０１５６】

デバイスの操作ロジックは、操作したいデバイスコマンドの前処理を行う部分と、ＩｏＴハブ１２００のＡＰＩへの送信を行う部分とで構成される。必要な情報は、ＩｏＴ接続システム２０００の運営者から提供される接続先ＵＲＬ、運営者から提供されるＡＰＩキー、デバイス情報および実行コマンドである。

【０１５７】

図１５は、ＩｏＴサービス利用者（エンドユーザ）が、ＩｏＴデバイス事業者により提供されたＩｏＴデバイスを用いて、ＩｏＴサービス提供事業者からＩｏＴサービスの提供を受けるフローを示した図である。図１５に示すように、初めに第一のデバイス１４１０からイベントの通知があると、プライベートクラウド１４００、第一のドライバ１２１０、ＷｅｂＡＰＩ１２３０、ＩｏＴアプリ１７００を介してエンドユーザにイベントが通知される。

【０１５８】

続いて、エンドユーザがアクションを決定すると、ＩｏＴアプリ１７００、ＷｅｂＡＰＩ１２３０、第二のドライバ１２２０を介して第二のデバイス５１０にアクションの実行が指示される。

【０１５９】

ＩｏＴデバイスの連携は、「～がこうなったら○○する」といったイベント駆動型のプログラムで表現することができる。そして、この処理をマイクロサービスとして部品化し、共通化して使えるようにしたうえで、ＦａａＳ（Function as a Service）の関数として実装することができる。

【０１６０】

ところで、上述したＩｏＴデバイスである第一のデバイス～第三のデバイスは、近年のＩｏＴ分野の発展により様々なメーカにより開発・製造されることとなった。しかしながら、デバイスまたはＩｏＴアプリとの常時接続は、Ｇｏｏｇｌｅ社またはＡｐｐｌｅ社等の大手ベンダーが提供するプッシュ通知用サービスのためのサーバに接続可能なデバイスに限られるという問題があった。

【０１６１】

本開示におけるＩｏＴハブ１２００は、すべてのＩｏＴデバイスの連携を目的として、

常時接続機能と、ディレクトリ機能とを実現することを特徴とする。

【０１６２】

常時接続機能は、第一のデバイス１４１０、第二のデバイス１５１０および第三のデバイス１６１０ならびにＩｏＴハブ１２００を介して利用可能なＩｏＴサービス（ＩｏＴアプリ１７００）を相互に常時接続させるものである。

【０１６３】

ただし、ＩｏＴハブに接続されるＩｏＴデバイスには、常時接続が必須でないものと、必須なものの２種類がある。前者には、定期的または不定期的に情報を発信するセンサ系のデバイスが含まれる。後者には、リモコン操作を行う必要がある制御可能装置のようなデバイスが含まれる。よって、本開示における上記常時接続機能は、後者の常時接続が必須のＩｏＴデバイスに対しては常時接続を、前者の常時接続が必須でないＩｏＴデバイスに対しては求められた時に限定した接続を実現すればよい。

【０１６４】

常時接続機能は、本開示におけるＩｏＴハブ１２００と第一のデバイス１４１０、第二のデバイス１５１０および第三のデバイス１６１０ならびにＩｏＴサービス１７００とを、ＩｏＴ向けのＭＱＴＴ（Message Queue Telemetry Transport）等の通信プロトコルを用いることで実現することができる。

【０１６５】

また、ディレクトリ機能は、第一のデバイス１４１０、第二のデバイス１５１０および第三のデバイス１６１０ならびにＩｏＴサービスを相互に連携させる。

【０１６６】

すなわち、ディレクトリ機能は、あるモノ（デバイス）からあるサービスへ、あるサービスからあるモノへ、あるモノからあるモノへ、モノまたはサービスを特定し、モノまたはサービスへ指示する機能を実現するものである。

【０１６７】

そして、ディレクトリ機能は、連携元のデバイスにより指定された連携先のデバイスを、デバイスの識別情報、ドライバの識別情報および接続界面の識別情報に基づいて特定することができる。

【０１６８】

デバイスの識別情報は、ＩｏＴデバイスのＵＵＩＤである。ドライバの識別情報は、ドライバのＩＤである。接続界面の識別情報は、ドライバとＩｏＴハブ１２００との界面であるＲ界面を特定するための情報である。

【０１６９】

また、ディレクトリ機能は、さらに、連携先のデバイスを、ＩｏＴハブ１２００の識別情報に基づいて特定することができる。

【０１７０】

なお、デバイスの識別情報、ドライバの識別情報および接続界面の識別情報は、所定の記憶装置に記憶され、当該記憶装置は、さらに、接続を許可しない接続元デバイスの識別情報および／またはデバイスの機能をホワイトリストとして記憶することができる。かかるリストについては、後述するサポート方法のメニュー票を利用することができる。

【０１７１】

図１６は、本開示におけるＩｏＴ接続システムにおける相互接続インフラの構造を示した概念図である。図１６に示すように、アプリケーションとして示されるＩｏＴアプリとＩｏＴハブとの接続面はＰ界面であるが、ＷｅｂＡＰＩ（α、β、γ）を使用して接続することで標準化されたＱ界面持つことができる。

【０１７２】

同様に、ＩｏＴデバイスとＩｏＴハブとの接続面はＳ界面であるが、ドライバ（Ａ～Ｚ）を使用して接続することで標準化されたＲ界面を持つことができる。

【０１７３】

従来、ＩｏＴアプリはＩｏＴデバイスの組み込みアプリと情報の授受を行うために、Ｉ

ｏＴアプリ側で宛先となるＩｏＴデバイスを指定する必要があるとともに、ＩｏＴデバイス側でもＩｏＴアプリから指定が可能な識別情報を持つ必要があった。

【０１７４】

一方、本開示のＩｏＴ接続システムにおいて、上記宛先の指定はＩｏＴハブにより実現されるディレクトリ機能により行われる。

【０１７５】

例えば、ＩｏＴデバイスの追加や交換は、ＩｏＴハブにドライバを追加して接続先を追加または切り替えることのみで対応可能となり、ＩｏＴアプリ自体を修正する必要がない。

【０１７６】

すなわち、ＩｏＴアプリにおいて必要であったＩｏＴデバイスを指定する宛先部分、および、ＩｏＴデバイスにおいて必要であったＩｏＴアプリから指定が可能な識別情報部分は、いずれのＩｏＴハブに集約されることができる。

【０１７７】

そのため、ＩｏＴデバイスの追加や交換は、アプリ開発者の工数を増やすことはなく、コストの低減につながる。

【０１７８】

このように、本開示におけるＩｏＴ接続システムによれば、ＩｏＴデバイスの製造メーカや機種が異なっても、ＩｏＴハブに接続されることでプロトコルフリーな相互接続を実現することが可能となる。

【０１７９】

また、図１７に示すように、本発明のＩｏＴハブ１２００は、関所エンジン１８００と接続されることができる。この関所エンジン１８００は、ＩｏＴハブ１２００がデバイスに指示する内容をチェックし、不適切なアクションが実行されることを防ぐためのものである。

【０１８０】

例えば、“外気が爽やかなら、エアコンを止めて窓を開ける”、といったＩｏＴサービスを提供する場合、直後にゲリラ豪雨に見舞われると室内が濡れてしまうおそれがあるが、上記関所エンジン１８００は、このようなＩｏＴ由来の脅威を未然に防ぐためのものである。

【０１８１】

また、本発明の第一のドライバ１２１０、第二のドライバ１２２０および第三のドライバ１３１０の少なくとも一つは、仮想デバイス機能を実現することができる。

【０１８２】

この仮想デバイス機能は、第一のデバイス１４１０、第二のデバイス１５１０または第三のデバイス１６１０を仮想的に再現するものである。

【０１８３】

図１８は、本発明の第二のドライバ１２２０が仮想デバイス機能を実現する例を示したものである。図１８に示すように、第二のドライバ１２２０に、第二のデバイス１５１０のコマンドの送受信を再現可能な仮想デバイス１９００を設けることにより、仮に第二のデバイス１５１０が接続されていなくても、第二のデバイス１５１０を用いるＩｏＴアプリの開発が可能となる。また、動作不良があった場合、現地に赴かずとも第二のデバイス１５１０とＩｏＴハブ１２００のどちらが故障しているのか故障切り分けを容易に行うことができる。

【０１８４】

また、本発明では、図１９に示すように、ドライバではなくＩｏＴハブ１２００に仮想デバイス機能を実現させてもよい。これは、ローカルに存在するＩｏＴルータ１３００に接続される第三のデバイス１６１０の故障切り分けに有効な手段である。

【０１８５】

上述したとおり、本開示におけるＩｏＴハブは、異なる通信プロトコルを使用するクラ

ウド間であっても、ドライバと呼ばれるインターフェースによって、それらの相互接続を可能とするプロトコルフリーのインフラである。また、ディレクトリ機能によって、複数のアプリやＩｏＴデバイスを複雑に組み合わせて接続をすることも可能である。

【０１８６】

また、本発明のＩｏＴ接続システム２０００において、第一のデバイス１４１０、第二のデバイス１５１０または第三のデバイス１６１０から取得される情報は、ＩｏＴハブ１２００では保存されないものとすることができる。

【０１８７】

本発明のＩｏＴ接続システム２０００は、電気通信事業者により運営されることを想定している。電気通信事業者は、通信の秘密を遵守する義務が課せられるため、各種デバイスから取得される情報を、他の利活用を目的として保存することはしない。

【０１８８】

これら情報は有益な情報であるため、各社のプライベートクラウドではかかる情報を独占的に取得すべく、ＩｏＴデバイスの囲い込みを行うのが通常である。

【０１８９】

一方で、本発明のＩｏＴ接続システム２０００は、運営を電気通信事業者が行うことにより、各ＩｏＴデバイスおよびＩｏＴアプリを中立の立場で相互接続させ、ＩｏＴビジネスを促進させることができる。

【０１９０】

また、ＩｏＴ相互接続サービスの継続性は利用する企業のＩｏＴサービスの継続性に影響するため、利用企業が共同で相互接続インフラを共有するのが好ましい。

【０１９１】

また、本発明のＩｏＴ接続システム２０００において、ＩｏＴハブ１２００に接続できるのはＡＰＩキーと認証スキームにより許可されたデバイスやＩｏＴアプリのみとすることができる。すなわち、本発明のＩｏＴ接続システム２０００は、インターネット上にＩｏＴ通信専用の閉域網を構築することができる。また、通信経路も暗号化され、ＭＤＭ（Mobile Device Management）の手法を用いてＩｏＴルータも管理するため、新たな攻撃方法やＯＳやアプリの脆弱性対応も可能とする。

【０１９２】

また、ＩｏＴ化されていないデバイスをＩｏＴハブ１２００に接続するには、ＢａａＳ（Backend as a service）やＳＤＫを活用することで、短期間での開発を行うことができる。

【０１９３】

以上の構成によれば、上述した従来技術の問題の少なくとも一部を解決又は緩和する技術的な改善を提供することができる。また、以上の構成によれば、複数のデバイスの機能を組み合わせた新たなサービスの創造を効率的に行うことができるようになる。

【０１９４】

サーバ装置３００は、図８に示すように、さらに、送信部３５０を有することができる。

【０１９５】

送信部３５０は、第二の情報処理装置２００から受け付けた第一識別情報に対応する第一の情報処理装置１００に対してのみ、特定の電子錠を解除可能な解除キーに関する情報を送信する。

【０１９６】

すなわち、自身のスマートフォンにアプリを入れている人だけ会議室への入出を許可するなどすることができる。

【０１９７】

以上、上記の実施形態において、第二の情報処理装置２００が信号を受信する機能を有する装置であって会社内の会議室等に設置されるもので、第一の情報処理装置１００が信号を発信する機能を有するスマートフォン等の装置であってユーザが所持するものである

ことを想定して説明を行ったが、これらの発信受信機能は逆であってもよい。すなわち、第一の情報処理装置１００が信号を受信する機能を有し、第二の情報処理装置２００が信号を発信する機能を有するものであってもよい。

【０１９８】
また、第一の情報処理装置１００および第二の情報処理装置２００のいずれもが発信機能および受信機能の両方の機能を有するものとしてもよい。この場合、どちらの装置がどちらの機能を実現するのかはサーバ装置３００からの指示に基づいて遠隔で自動的に切り替えられるものとすることができる。
【０１９９】
また、発信機能を実現する装置（上記の実施形態では第一の情報処理装置１００）としては、上述したスマートフォン等の情報処理装置に限られず、タグ型の発信機（所謂「ビーコンタグ」）を用いることも可能である。
【０２００】
これによれば、スマートフォンを所持しない／することができない子供や高齢者、持ち歩けない医療・介護従事者の行動履歴を容易に確実に取得することができ、かつ、上記者と同じ場所にいた者を容易に確実に特定することができるようになる。
【０２０１】
以下に、本開示における情報処理システム、情報処理方法およびコンピュータプログラムにより実現されるサービスの実施形態について説明する。
【０２０２】
＜概要＞
本開示における情報処理システム、情報処理方法およびコンピュータプログラムにより実現されるサービスによれば、会議室等にＩｏＴセンサを設置し、当該会議室に一定時間入室した社員をその所有するスマートフォンにより特定することができる。
【０２０３】
社員の中で新型コロナウイルス等の感染者が見つかった時に、その情報を利用して濃厚接触者を特定できる。このことにより、ビル内に出入りした社員全員では無く、濃厚接触者のみを自宅待機させたりするなどの感染拡大の防止手段が取りやすくなる。
【０２０４】
合わせて、ＩｏＴセンサとして室内環境センサ等の様々なセンサを組み込むことにより、室内環境の継続的なモニターを行い、適切な換気等により室内での感染拡大をできるだけ防止するというような措置も採ることが可能となる。
【０２０５】
＜提供方法＞
本サービスを提供するにあたり、ＩｏＴセンサとそのセンサがインターネットと通信するためのゲートウェイ（ＩｏＴルータ）を提供する。なお、ＩｏＴセンサの中でもＢＬＥビーコンをブロードキャストして入室する社員を特定するための機能はＩｏＴルータに内蔵される。
【０２０６】
また、社員がＢＬＥビーコンを受けて入室したことを特定するためには、社有ないしは私用スマホに本開示におけるアプリケーションを事前にインストールして登録する必要がある。
【０２０７】
この仕組みによって収集された入室情報および室内の環境情報は、以下に詳説する「ＩｏＴ　Ｅｘｃｈａｎｇｅ」を通して「Ｃｏｒｏｎａ　Ｔｒａｃｅｒ」サービス内に蓄積され、各企業の担当者が自由に引き出すことができる。
【０２０８】
なお、情報の取り出しとその情報に基づいたアクションについては、ＲＰＡ（ロボティック・プロセス・オートメーション）などの自動化ツールを使っても良い。

【０２０９】
＜サービスの構成要素とその機能＞
「ＩｏＴ　Ｅｘｃｈａｎｇｅ」は、センサ等を制御するための命令やセンサから上がってくる情報を送受信する。
【０２１０】
「ＩｏＴルータ」は、環境センサとの接続を担って、環境データを「ＩｏＴ　Ｅｘｃｈａｎｇｅ」に送信するだけで無く、内蔵するＢＬＥチップがＢＬＥ送受信機としての役割を果たし、スマートフォンから送出されるＢＬＥビーコンを受信したり、自らＢＬＥビーコンを送出したりすることができる。
【０２１１】
「環境センサ」は、会議室等の環境データ（室温、湿度、騒音、CO_2量、揮発性有機溶媒量等）を測定して、ＩｏＴルータ経由で「Ｃｏｒｏｎａ　Ｔｒａｃｅｒ」サービスに送付する。
【０２１２】
「Ｃｏｒｏｎａ　Ｔｒａｃｅｒ　Ａｐｐ」は、ｉＯＳおよびＡｎｄｒｏｉｄに対応し、社員の持つスマートフォン（社給ないしは個人所有）にインストールされ、ＢＬＥビーコンを送信する。また、ＢＬＥビーコンが常に送信されているかの確認情報を「Ｃｏｒｏｎａ　Ｔｒａｃｅｒ」サービスに対して送出する。また、ＢＬＥビーコンを受信してその情報（タイムスタンプ、会社ＩＤ、社員ＩＤ、ビーコンＩＤ、ビーコン強度）を「Ｃｏｒｏｎａ　Ｔｒａｃｅｒ」サービスに送付するものであってもよい。
【０２１３】
「Ｃｏｒｏｎａ　Ｔｒａｃｅｒ」サービスは、環境センサ、ＩｏＴルータおよび「Ｃｏｒｏｎａ　Ｔｒａｃｅｒ　Ａｐｐ」からの情報を収集して保存する。また、本サービスはＩｏＴルータの設定を遠隔で行うことができる。また、ＩｏＴルータをＢＬＥ発信機として利用する場合には、ＢＬＥの早出間隔や送信強度を変更することができる。本サービスは更に、社員の会議室への入退出情報についてレポートを生成してｃｓｖファイルに保存することができる。
【０２１４】
「ＲＰＡ」または、連携を希望する他システムは、「Ｃｏｒｏｎａ　Ｔｒａｃｅｒ」サービスにアクセスし、社員の会議室入退出情報を取得し、その情報に基づいてレポートを生成したり、アラートを送出したりする。
【０２１５】
＜サービス提供の準備＞
本サービスの提供にあたっては、会議室へのデバイスの設置と社員によるアプリのインストールおよびＲＰＡまたは、連携を希望する他システムへの種々の登録が必要である。会議室に設置されるデバイスは、ＩｏＴルータ、環境センサ及びＡＣアダプタである。電源が室内に無い場合には、モバイルバッテリーも必要である。ＩｏＴルータはＡｎｄｒｏｉｄスマホであるが、アクティベーション、アプリのインストレーション等のキッティングは本サービス提供者にて行う。よって、設置業者は本デバイス一式を会議室に置いていくだけで良い。
【０２１６】
社員のスマホにインストールされるアプリは、Ｇｏｏｇｌｅ　Ｐｌａｙ　Ｓｔｏｒｅないしは Ａｐｐｌｅ　Ａｐｐ　Ｓｔｏｒｅからそれぞれの社員がダウンロードし、インストールすることとする。また、インストール後は、会社ＩＤと社員ＩＤを登録する必要がある。
【０２１７】
先行技術文献として挙げたアプリケーションは、双方がスマホにアプリを入れていることが前提であるが、本開示における発明によれば、片方はタグなどでも動作可能である。これにより、スマートフォンを持っていない子供や高齢者、持ち歩けない医療・介護従事者にも対応可能である。

【０２１８】
また、先行技術文献として挙げたアプリケーションは、スマートフォンに保存する方式のみであるが、本開示における発明によれば、スマートフォンおよびクラウドの双方に保存する方法を選択可能である。また、双方の相対距離情報と本人を特定できる情報を全く別システムとして分離し、連携システム経由でのアクセスしかできないよう制限されている。これにより、端末側の情報、クラウド側の情報にアクセスできたとしても情報の入手は不可能である。
【０２１９】
また、先行技術文献として挙げたアプリケーションは、スマートフォン用アプリケーションであって親機・子機の概念がなくいずれの端末も対等であり位置情報を取得しないことが前提であるが、本開示における発明によれば、受信側を特定の場所に設置することができるため、集団感染場所の特定を容易に行うことができる。これにより、集団感染が発生した場所と日時を容易に特定できる。具体的には、会議室、トイレ、店舗、クラブ、教室、カラオケルームなどである。場所や日時が特定できれば、その場所にいた人間がスマートフォンやアプリ、タグ等を持たない人がいた場合でも、感染リスクを知らせることができる場合がある。また、本開示における発明によれば、子機が何台あっても、親機が受信する方式なので、データ蓄積・収集先を限定・一元化することができる。親機は、会社が会議室等に導入・設置して管理することで、親機の場所（位置情報を含む）を特定することができる、なお、親機は会社が遠隔から運用保守可能とするのが好ましい。
【０２２０】
また、先行技術文献として挙げたアプリケーションは、このアプリケーションが必ず必要で、これ以外の同様のアプリケーションやサービスと連携することが難しいが、本開示における発明によれば、特定の企業、団体、自治体等が個別に入れたシステムを簡単に相互接続することができ、契約が成立した相手と契約に基づいた情報だけを共有することができる。これにより、個人の同意や契約に基づかない情報の共有は行われないことが保証できる。
【０２２１】
また、先行技術文献として挙げたアプリケーションは、基本的に個人情報を極力特定しない方式の一般的な感染情報共有システムであるが、本開示における発明は、事業者の設置した場所の情報を追加できるので、どの場所が感染場所になったかを特定することができる。その結果、事業者が事業停止リスクを減少させ、かつ従業員の安全を確保することが可能になる。ここでいう事業者とは、会社（会議室、トイレ）、学校（教室、トイレ）、店舗（飲食、カラオケ、クラブ等）など、これまで個別に対策を取れなかった事業者全てである。
【０２２２】
また、本開示における発明は、第一の情報処理装置が備えるＧＰＳ（Ｇｌｏｂａｌ　Ｐｏｓｉｔｉｏｎｉｎｇ　Ｓｙｓｔｅｍ）機能と連動させて、帰国後自宅待機を命じられた人の周辺で感染者が発生した場合に、自分は自宅にずっと待機していたことを証明するために自分の位置情報を提出できるような仕組みを構築してもよい。
【０２２３】
最後に、本開示における情報処理方法およびコンピュータプログラムの実施形態について説明する。
【０２２４】
本開示における情報処理方法は、図１に示したように、信号を発信する機能を有する第一の情報処理装置１００と、信号を受信する機能を有する第二の情報処理装置２００と、第二の情報処理装置２００とインターネットを介して接続可能なサーバ装置３００とを備える情報処理システム１０００において実行される情報処理方法である。
【０２２５】
本開示における情報処理方法は、図２０に示されるように、第一の情報処理装置１００に、当該第一の情報処理装置１００の第一識別情報を含む信号を発信するステップＳ１０

を実行させる。
【０２２６】
そして、本開示における情報処理方法は、第二の情報処理装置２００に、第一の情報処理装置１００から発信された信号を受信するステップＳ２０と、信号を受信した時刻に関する時刻情報、信号の受信強度に基づく強度情報および第一識別情報を、第二の情報処理装置２００の第二識別情報とともにサーバ装置３００に送信するステップＳ３０とを実行させる。
【０２２７】
そして、本開示における情報処理方法は、サーバ装置３００に、第二の情報処理装置２００から受信した時刻情報、強度情報、第一識別情報および第二識別情報を互いに関連付けて記憶するステップＳ３０と、特定の第一の情報処理装置１００の特定の第一識別情報の指定を受け付けるステップＳ４０と、特定の第一の情報処理装置１００の特定の第一識別情報の指定を受け付けた場合に、特定の第一識別情報に関連付けて記憶された特定の第二識別情報に基づいて、当該特定の第二識別情報に関連付けて記憶された１以上の他の第一識別情報を抽出するステップＳ５０とを実行させる。
【０２２８】
以上のように、本開示における情報処理方法によれば、特定の第一の情報処理装置を有する者が、いつ何処にいたかという行動履歴を容易に確実に取得することができ、かつ、上記者と同じ場所にいた者を容易に確実に特定することができるようになる。すなわち、本開示における情報処理方法は、感染者のトレーサビリティを可能にする。
【０２２９】
本開示におけるコンピュータプログラムは、信号を発信する機能を有する第一の情報処理装置と、信号を受信する機能を有する第二の情報処理装置と、第二の情報処理装置とインターネットを介して接続可能なサーバ装置とを備える情報処理システムにおいて実行されるコンピュータプログラムである。
【０２３０】
本開示におけるコンピュータプログラムは、第二の情報処理装置に、第一の情報処理装置から発信された第一の情報処理装置の第一識別情報を含む信号を受信する機能と、信号を受信した時刻に関する時刻情報、信号の受信強度に基づく強度情報および第一識別情報を、第二の情報処理装置の第二識別情報とともにサーバ装置に送信する機能とを実現させる。
【０２３１】
そして、本開示におけるコンピュータプログラムは、サーバ装置に、第二の情報処理装置から受信した時刻情報、強度情報、第一識別情報および第二識別情報を互いに関連付けて記憶させる機能と、特定の第一の情報処理装置の特定の第一識別情報の指定を受け付ける機能と、指定を受け付けた場合に、特定の第一識別情報に関連付けて記憶された特定の第二識別情報に基づいて、当該特定の第二識別情報に関連付けて記憶された１以上の他の第一識別情報を抽出する機能とを実現させる。
【０２３２】
以上のように、本開示におけるコンピュータプログラムによれば、特定の第一の情報処理装置を有する者が、いつ何処にいたかという行動履歴を容易に確実に取得することができ、かつ、上記者と同じ場所にいた者を容易に確実に特定することができるようになる。すなわち、本開示におけるコンピュータプログラムは、感染者のトレーサビリティを可能にする。
【０２３３】
最後に、本開示における情報処理システムの他の適用例について説明する。
新型コロナウイルスは、主に感染者との飛沫接触等により伝染する事が報告されており、公衆衛生機関は、感染拡大を抑えるためには感染経路を断つこと、やむを得ず接触し感染した場合には速やかに濃厚接触者を特定するように求めている。
【０２３４】

そのため、政府や感染症研究機関は、感染者の利用等があった場所（店舗、事業所、等の施設）を公開し、ＧＰＳ等の位置情報を使って地図上で確認できるサービスを提供する会社や、非特許文献１のように、感染経路を追跡し、濃厚接触者に通知できるサービスも現れている。

【０２３５】

非特許文献１に記載されたサービスでは、該当のアプリをインストールしているスマートフォン同士が近づくと、端末ごとに割り振られたＩＤを近距離無線通信の「ブルートゥース」を使って交換し、記録する。感染した人がアプリ利用者の時は、保健省の職員が本人の同意を得た上でアプリ上の記録を手掛かりに感染者の近くに一定時間以上いたスマートフォン利用者を特定・連絡し、必要な措置を講ずる。

【０２３６】

このようなアプリの活用により、本人が気付かない濃厚接触者を追跡することができ、クラスター（感染者集団）の早期発見や感染の恐れがある人の早期隔離に効果がある。しかし、このアプリはスマートフォンの利用が前提であり、しかも大勢の人が利用しないと効果が高まらない。

【０２３７】

現在、新型コロナウイルスの感染拡大対策として緊急事態宣言が発令され、多くの企業が外出自粛の要請をされている。しかし、在宅では対応できない業務や、社会機能を維持するために必要な業種もあり、そうした業務に従事する人々は、引き続き出勤を継続せざるを得ない状況を強いられている。

【０２３８】

ところが、現在では国民生活・国民経済の安定確保に不可欠な業務を行う企業、店舗、病院等でも感染者が発見され、特定の業務だけでなく事業そのものを一時的に停止しなければならない事態が発生している。

【０２３９】

既に、すべての事業者にとって、濃厚接触者を速やかに特定し、仕分けを行うことが、事業継続性（ＢＣＰ）対策として必須になっている。

【０２４０】

そこで、本発明者は、企業のＢＣＰ対策を目的として、第二の情報処理装置２００として会議室等に設置した本開示におけるＩｏＴルータ１３００を活用して「濃厚接触者特定サービス」を開発した。

【０２４１】

まず、企業の会議室など「三密」になりやすい場所に、本開示におけるＩｏＴルータ（親機：第二の情報処理装置２００）を設置する。そこに、Ｂｅａｃｏｎアプリをインストールしたスマートフォン（子機：第一の情報処理装置１００）を持った社員が近づくと、社員の子機ＵＵＩＤと距離を検知し、時刻と共に記録する。

【０２４２】

そのため、総務部門等の管理者は、感染した社員名を指定するだけで、濃厚接触の可能性のある社員名を簡単に特定することができる。

【０２４３】

この「濃厚接触者特定サービス」は、「Ｂｅａｃｏｎデータ収集システム」と「濃厚接触者特定システム」という別々のシステムを、「ＩｏＴハブ」と「ＩｏＴルータ」を経由し、必要なデータを必要な時に必要な分だけ取得する仕組みになっており、管理者が誰かの行動を監視し続けることはできない仕組みになっている。

【０２４４】

すなわち、本開示における第一の情報処理装置１００および第二の情報処理装置２００を含むシステムが「Ｂｅａｃｏｎデータ収集システム」であり、サーバ装置３００を含むシステムが「濃厚接触者特定システム」であり、上述したＩｏＴハブ１２００がこれらを繋ぐハブとして機能する。

【０２４５】

そのため、高いプライバシー保護とセキュリティ確保を両立することが可能である。すなわち、収集するデータを個人情報に当たらないものだけに限定した「Ｂｅａｃｏｎデータ収集システム」と社員の氏名と連絡先といった個人情報を扱う「濃厚接触者特定システム」という二つのシステムを作り、これら二つのシステムを分けることによって、情報を遮断する。

【０２４６】

そして、これらのシステムを必要な時に限りＩｏＴハブを使って疎結合することで、社員の行動の常時監視を防止しつつ、濃厚接触者を特定できるようにする。

【０２４７】

かかるシステム構成は、ＩｏＴハブ１２００に様々な機能のシステムを接続することにより機能を拡張していくことが可能である。

【０２４８】

続いて、図２１を用いて感染者発生から濃厚接触者を特定するフローを説明する。

【０２４９】

具体的には、予め、図２１に示すＢｅａｃｏｎデータ収集システム３１００において、会議室に設置したＢｅａｃｏｎやスマートフォンアプリを利用して、会議室にいた人のデータ（ＵＵＩＤ、時刻、親機であるＩｏＴルータと子機であるスマートフォンの距離）を自動収集する。このＢｅａｃｏｎデータ収集システム３１００には、個人情報は一切含まれない。

【０２５０】

そして、管理者が感染者となった従業員から感染の報告を受けた際には、管理者は、管理画面から従業員の名前を入力する。そうすると、濃厚接触者特定システム３２００は感染者のＵＵＩＤをＢｅａｃｏｎデータ収集システム３１００に送付する。このＵＵＩＤを基にＢｅａｃｏｎデータ収集システム３１００は、濃厚接触の恐れがあるＵＵＩＤを特定し濃厚接触者特定システム３２００に送付する。そして、このシステム３２００はＵＵＩＤと氏名を紐づけ、濃厚接触候補者リストとして出力する。管理者である総務の担当者は、そのリストの情報から優先順位を付けて濃厚接触者候補に連絡し、自宅待機や検査の指示、継続的な報告などの指示を行う。

【０２５１】

なお、「Ｃｏｒｏｎａ　Ｔｒａｃｅｒ」では、ＢＬＥをＢｅａｃｏｎとして活用している。スマートフォン同士でＢｅａｃｏｎを活用し、濃厚接触を検知することも可能であるが、スマートフォンを持たない社員がいること、一部のスマートフォンはＢＬＥの双方向通信が可能でないことを考慮し、ＩｏＴルータを親機として活用し、ＢＬＥ双方向通信ができない社員にはＢｅａｃｏｎタグを持たせることで全ての社員がシステムを使うことができるようにしている。スマートフォン間のＢＬＥ活用で収集したデータは、距離精度の向上など補助的な用途に活用されている。

【０２５２】

なお、本システムの管理者はＩＤとパスワードをメールで社員に通知する。通知を受けた社員がアプリをインストールする際に送付されたＩＤとパスワードを入力するとスマートフォンの中で自動的にＵＵＩＤが生成され、氏名とともに濃厚接触者特定システムに登録される。Ｂｅａｃｏｎデータ収集システムには、このＵＵＩＤのみが送付され記録に使用されるので、ＵＵＩＤから個人の特定はできない。

【０２５３】

また、ＩｏＴハブを利用することにより、異なる会社のデータを契約に基づき限定的に情報共有することができる。この機能を活用すれば、同席した別の会社の社員にも感染リスクがあることを教えることが可能になる。

【０２５４】

また、導入企業が同意すれば、個人情報を伏せて、政府や自治体、または保険機関に情報を一括して提供することも可能である。これにより、感染者集団（クラスター）情報をいち早く提供することが可能になる。

【０２５５】
最後に、第一の情報処理装置１００に代えて、または、加えて、二次元コードを印刷した媒体を用いた例について付記する。
【０２５６】
上述した実施例では、第一の情報処理装置１００に専用のアプリケーションがインストールされた者を対象者であると想定して説明を行ったが、他の情報処理装置（専用のアプリケーションがインストールされていない情報処理端末）を有する者や、情報処理端末を有しない者などが会社に来訪する場合も多い。
【０２５７】
例えば、工事などを行う作業員や、会議などのために一時的に来訪する者などの来訪者などは、上述した専用のアプリケーションをインストールしたスマートフォンやビーコンタグを用いて管理するよりも、入館証にＱＲコード（登録商標）などの二次元コードを印刷し、この二次元コードに含まれる情報を管理する方が容易である。
【０２５８】
このＱＲコードには、来訪者の氏名および連絡先（メールアドレスおよび／または電話番号等）の情報を記録する。これらの情報は、来訪時に来訪者が所定の入力端末を介して入力するものであってもよいし、来訪者または迎え入れる側の者が事前に登録しておくものであってもよい。
【０２５９】
そして、来訪者は会議室に入室した際に、会議室に設置された親機である第二の情報処理装置２００に、自身の入館証に印刷された二次元コードを読み取らせる。これにより、来訪者の情報、および、読み取った時間等の情報はサーバ装置３００に記録される。
【０２６０】
なお、二次元コードを読み取るのは親機に限られず、子機である第一の情報処理装置１００が読み取り、親機に送信する形式としてもよい。
【０２６１】
そして、上述した実施形態と組み合わせ、来訪者に対して連絡する必要がある場合には、連絡先として記録されたメールアドレスや電話番号に対してＥメールまたはＳＭＳ（ショートメッセージサービス）を送信することにより行われるのが好ましい。
【０２６２】
さらに、上記二次元コードは、オンライン名刺として活用することも可能である。すなわち、実際の紙媒体を交換する従来の名刺交換に代えて、名刺の内容を二次元コードに記録してスマートフォン等の画面に表示することで、接触を避けて遠隔からでも名刺交換を行うことが可能になる。
【０２６３】
また、会議において参加者に共有される画面上にオンライン名刺を表示することで、参加者と一斉に名刺交換を行うことも可能である。
【０２６４】
本発明のいくつかの実施形態を説明したが、これらの実施形態は、例として提示したものであり、発明の範囲を限定することは意図していない。これら新規な実施形態は、その他の様々な形態で実施されることが可能であり、発明の要旨を逸脱しない範囲で、種々の省略、置き換え、変更を行うことができる。これら実施形態やその変形は、発明の範囲や要旨に含まれるとともに、特許請求の範囲に記載された発明とその均等の範囲に含まれる。
【０２６５】
また、実施形態に記載した手法は、計算機（コンピュータ）に実行させることができるプログラムとして、例えば磁気ディスク（フロッピー（登録商標）ディスク、ハードディスク等）、光ディスク（ＣＤ－ＲＯＭ、ＤＶＤ、ＭＯ等）、半導体メモリ（ＲＯＭ、ＲＡＭ、フラッシュメモリ等）等の記録媒体に格納し、また通信媒体により伝送して頒布することもできる。なお、媒体側に格納されるプログラムには、計算機に実行させるソフトウ

ェア手段（実行プログラムのみならずテーブルやデータ構造も含む）を計算機内に構成させる設定プログラムをも含む。本装置を実現する計算機は、記録媒体に記録されたプログラムを読み込み、また場合により設定プログラムによりソフトウェア手段を構築し、このソフトウェア手段によって動作が制御されることにより上述した処理を実行する。なお、本明細書でいう記録媒体は、頒布用に限らず、計算機内部あるいはネットワークを介して接続される機器に設けられた磁気ディスクや半導体メモリ等の記憶媒体を含むものである。記憶部は、例えば主記憶装置、補助記憶装置、又はキャッシュメモリとして機能してもよい。

【符号の説明】

【０２６６】

１０００　情報処理システム
　１００　第一の情報処理装置
　１１０　発信部
　１２０　取得部
　１３０　環境情報送信部
　２００　第二の情報処理装置
　２１０　受信部
　２２０　送信部
　３００　サーバ装置
　３１０　記憶部
　３２０　受付部
　３３０　抽出部
　３４０　通知部
　３５０　送信部

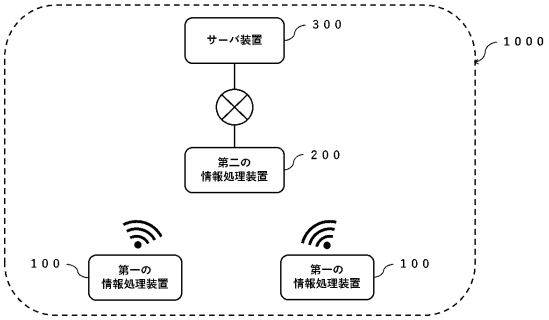
【要約】　（修正有）

【課題】感染者の行動履歴の特定および濃厚接触者の抽出を容易に確実に行うことが可能な情報処理システム、情報処理方法およびコンピュータプログラムを提供する。

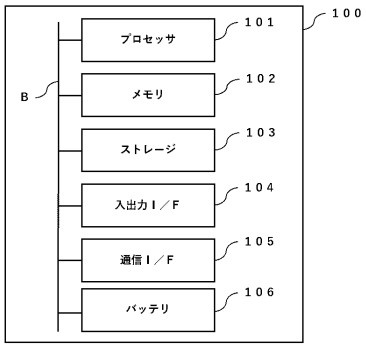
【解決手段】情報処理システム１０００は、信号を発信する機能を有する第一の情報処理装置と、信号を受信する機能を有する第二の情報処理装置と、第二の情報処理装置とインターネットを介して接続可能なサーバ装置とを備える情報処理システムであって、サーバ装置は、第二の情報処理装置から受信した時刻情報、強度情報、第一識別情報および第二識別情報を互いに関連付けて記憶し、特定の第一の情報処理装置の特定の第一識別情報の指定を受け付けた場合に、特定の第一識別情報に関連付けて記憶された特定の第二識別情報に基づいて、当該特定の第二識別情報に関連付けて記憶された１以上の他の第一識別情報を抽出することを特徴とする。

【選択図】図１

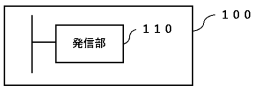
【図１】



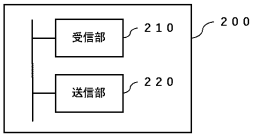
【図２】



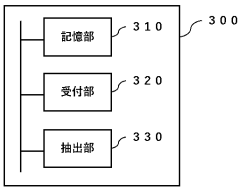
【図３】



【図４】



【図５】



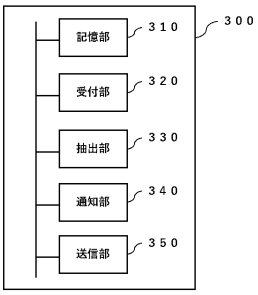
【図６】

第二の情報処理装置（識別ID）	第一の情報処理装置（識別ID）	時刻	電波強度（dB）	基準強度（dBm）	推定距離（m）
200001	100001	2020:03:31:15:02	-79	-76	1.41
	100002	2020:03:31:15:02	-80	-76	1.58
	100003	2020:03:31:15:30	-79	-76	1.41
	・・・	・・・	・・・	・・・	・・・
200002	100002	2020:04:01:10:00	-92	-94	0.79
	100004	2020:04:01:15:02	-93	-94	0.89
	100005	2020:04:02:10:00	-93	-94	0.89
	・・・	・・・	・・・	・・・	・・・
・・・	・・・	・・・	・・・	・・・	・・・

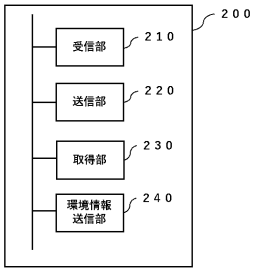
【図７】

特定の第一の情報処理装置（識別ID）	第二の情報処理装置（識別ID）	特定の時刻	他の第一の情報処理装置（識別ID）	時刻
100002	200001	2020:03:31:15:02	100001	2020:03:31:15:02
			100003	2020:03:31:15:30
			・・・	・・・
	200002	2020:04:01:10:00	100004	2020:04:01:15:02
			100005	2020:04:02:10:00
			・・・	・・・
	・・・	・・・	・・・	・・・

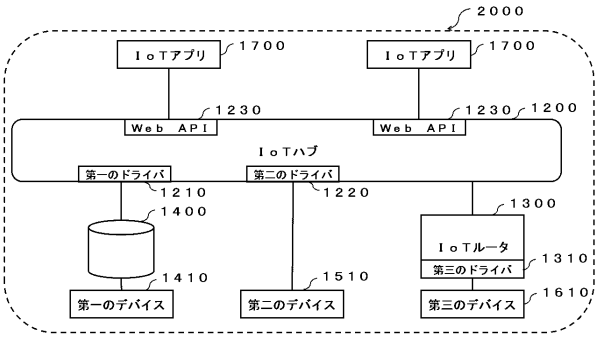
【図８】



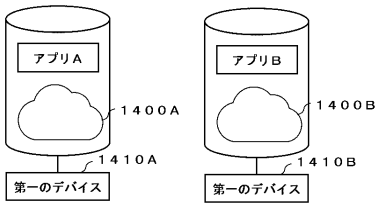
【図９】



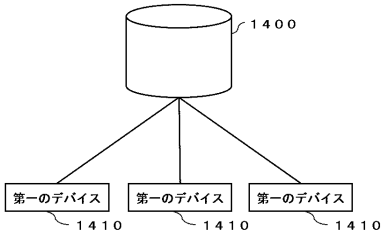
【図１０】



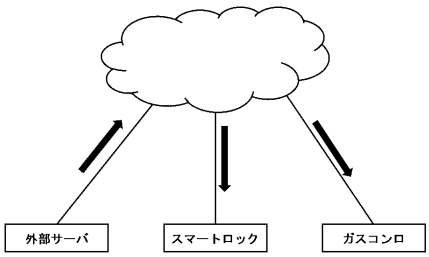
【図１１】



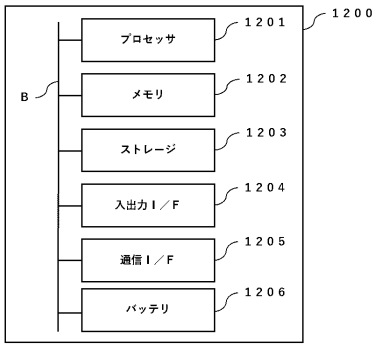
【図１２】



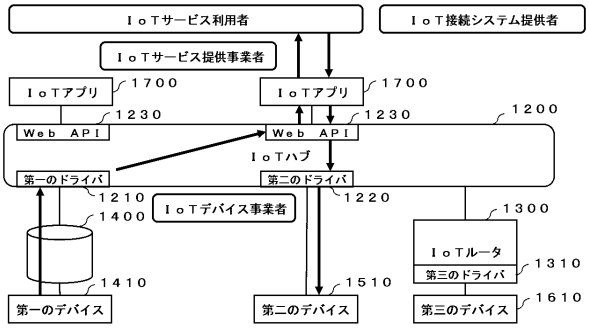
【図１３】



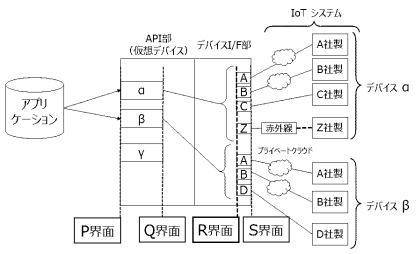
【図１４】



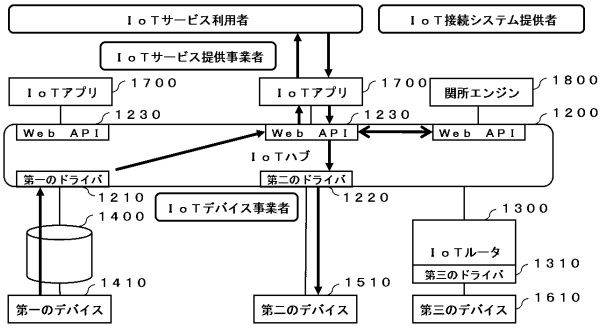
【図１５】



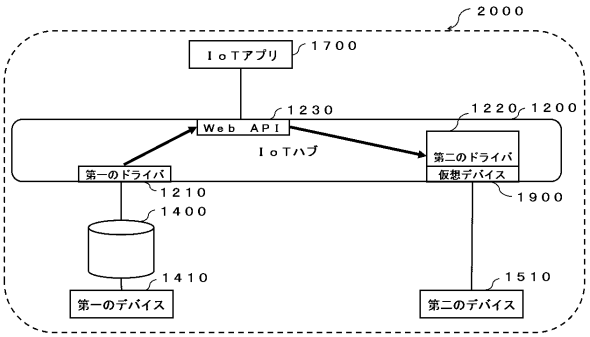
【図１６】



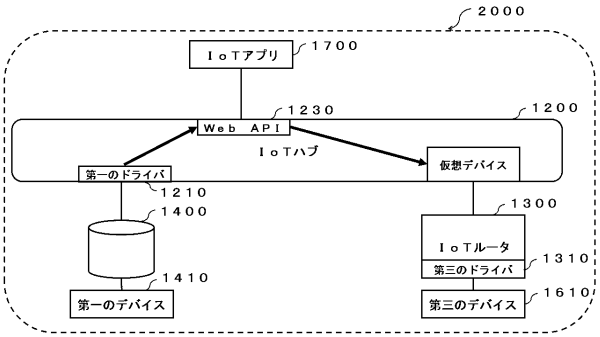
【図１７】



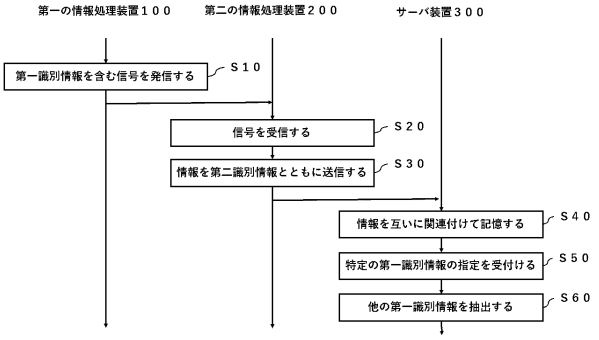
【図１８】



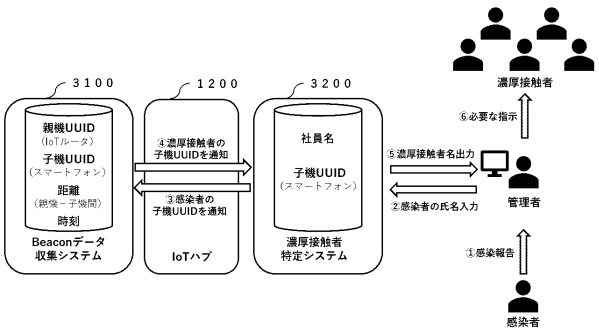
【図１９】



【図２０】



【図２１】



フロントページの続き

特許法第３０条第２項適用　・令和２年４月２０日　ｈｔｔｐｓ：／／ｗｗｗ．ｉｏｔ－ｅｘ．ｃｏ．ｊｐ／ｎｅｗｓ／ｎｅｗｓ＿２００４２０．ｈｔｍｌ　・令和２年４月２８日　ｈｔｔｐｓ：／／ｗｗｗ．ｉｏｔ－ｅｘ．ｃｏ．ｊｐ／ｎｅｗｓ／ｎｅｗｓ＿２００４２８．ｈｔｍｌ　・令和２年４月２８日　ｈｔｔｐｓ：／／ｓｍａｒｔｉｏｔ－ｆｏｒｕｍ．ｊｐ／ｉｏｔ－ｖａｌ－ｔｅａｍ／ｉｏｔ－ｃａｓｅ／ｃａｓｅ－ｉｏｔ－ｅｘ　・令和２年５月１５日　ｈｔｔｐｓ：／／ｓｍａｒｔｉｏｔ－ｆｏｒｕｍ．ｊｐ／ｉｏｔ－ｖａｌ－ｔｅａｍ／ｉｏｔ－ｃａｓｅ／ｍａｉｌｍａｇａｚｉｎｅ／ｍａｉｌｍａｇａ－０３９－２０２００５１４?ｍａｉｌｍａｇａ＝

早期審査対象出願

(56)参考文献　特開２０１０－２７７４５２（ＪＰ，Ａ）
特開２０１７－１１７４１６（ＪＰ，Ａ）
特開２０１１－１７２００７（ＪＰ，Ａ）
特開２０１７－１６２２１４（ＪＰ，Ａ）
特開２０１２－１９８７１７（ＪＰ，Ａ）
特開２０１２－１９４８０８（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｑ５０／２２
Ｇ１６Ｈ１０／００
Ｈ０４Ｍ１／００
１／２４－３／００
３／１６－３／２０
３／３８－３／５８
７／００－７／１６
１１／００－１１／１０
９９／００