(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2018年7月26日(26.07.2018)

WIPO | PCT

(10) 国際公開番号
WO 2018/134937 A1

(51) 国際特許分類:
H04L 9/32 (2006.01) *G06F 21/44* (2013.01)

(21) 国際出願番号： PCT/JP2017/001673

(22) 国際出願日： 2017年1月19日(19.01.2017)

(25) 国際出願の言語： 日本語

(26) 国際公開の言語： 日本語

(71) 出願人: 株式会社セゾン情報システムズ(SAISON INFORMATION SYSTEMS CO., LTD.) [JP/JP]; 〒1706021 東京都豊島区東池袋三丁目１番１号 Tokyo (JP). 株式会社アプレッソ(APPRESSO K.K.) [JP/JP]; 〒1120014 東京都文京区関口一丁目２０番１０号 住友不動産江戸川橋駅前ビル２F Tokyo (JP).

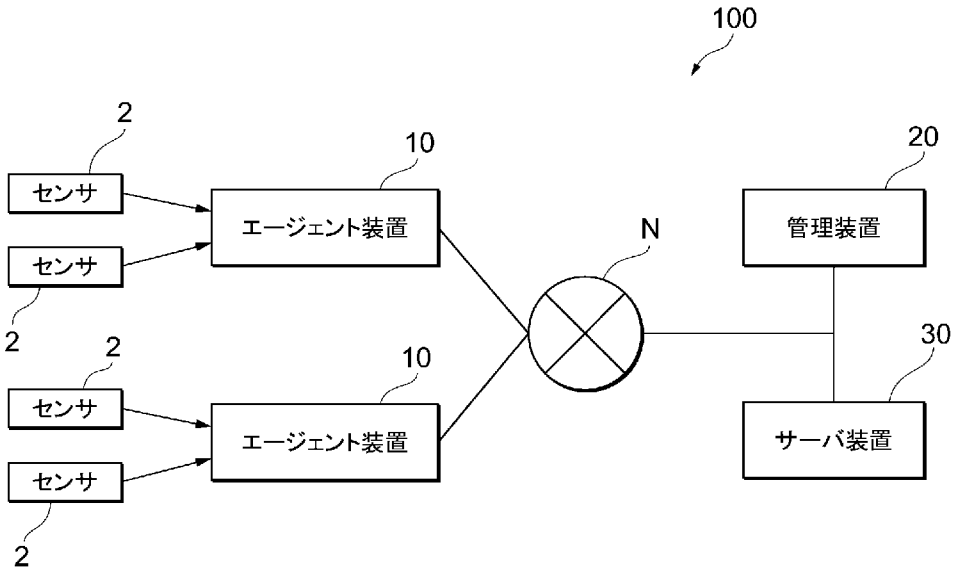
(72) 発明者: 樋口 義久 (HIGUCHI, Yoshihisa); 〒1706021 東京都豊島区東池袋三丁目１番１号 Tokyo (JP). 野原 和也(NOHARA, Kazuya); 〒1706021 東京都豊島区東池袋三丁目１番１号 Tokyo (JP). 大竹 純(OTAKE, Jun); 〒1706021 東京都豊島区東池袋三丁目１番１号 Tokyo (JP). 原田 智弘(HARADA, Tomohiro); 〒1706021 東京都豊島区東池袋三丁目１番１号 Tokyo (JP). 田中 健一(TANAKA, Kenichi); 〒1120014 東京都文京区関口一丁目２０番１０号 住友不動産江戸川橋駅前ビル２F Tokyo (JP).

(74) 代理人: 稲葉 良幸, 外(INABA, Yoshiyuki et al.); 〒1066123 東京都港区六本木６－１０－

WO 2018/134937 A1

(54) **Title:** IoT DATA COLLECTION SYSTEM, IoT DATA COLLECTION METHOD, MANAGEMENT DEVICE, MANAGEMENT PROGRAM, AGENT DEVICE, AND AGENT PROGRAM

(54) 発明の名称： ＩｏＴデータ収集システム、ＩｏＴデータ収集方法、管理装置、管理プログラム、エージェント装置及びエージェントプログラム



(57) **Abstract:** An IoT data collection system 100 includes: agent devices 10 for acquiring IoT data; a management device 20 for managing the agent devices 10; and a server device 30 for receiving the IoT data from the agent devices 10. Each agent device 10 is provided with a first transmission unit for transmitting an authentication activation key to the

［続葉有］

１ 六本木ヒルズ森タワー２３階 ＴＭＩ総合法律事務所 Tokyo (JP).

(81) 指定国(表示のない限り、全ての種類の国内保護が可能): 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, 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, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) 指定国(表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, RU, TJ, TM), ヨーロッパ (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), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

添付公開書類：

— 国際調査報告（条約第21条(3)）

— 補正された請求の範囲及び説明書（条約第19条(1)）

management device 20 at the time of startup. The management device 20 is provided with: a verification unit for verifying a registration activation key and the authentication activation key; and a transmission unit for transmitting an authentication agent ID to each agent device 10 when a verification result is correct. The agent device 10 is further provided with a second transmission unit for transmitting IoT data and the authentication agent ID to the server device 30. The server device 30 is provided with: a verification unit for verifying a registration agent ID and the authentication agent ID; and a reception unit for receiving the IoT data from each agent device 10 when a verification result is correct.

(57) 要約：ＩｏＴデータを取得するエージェント装置１０、エージェント装置１０を管理する管理装置２０及びエージェント装置１０からＩｏＴデータを受信するサーバ装置３０を含むＩｏＴデータ収集システム１００であって、エージェント装置１０は、起動時に管理装置２０に認証アクティベーションキーを送信する第１送信部を備え、管理装置２０は、登録アクティベーションキーと認証アクティベーションキーを照合する照合部と、照合結果が正しい場合に、エージェント装置１０に対し、認証エージェントＩＤを送信する送信部と、を備え、エージェント装置１０は、ＩｏＴデータ及び認証エージェントＩＤを、サーバ装置３０に送信する第２送信部をさらに備え、サーバ装置３０は、登録エージェントＩＤと認証エージェントＩＤを照合する照合部と、照合結果が正しい場合に、エージェント装置１０から、ＩｏＴデータを受信する受信部と、を備えるＩｏＴデータ収集システム１００。

明　細　書

発明の名称 ：

ＩｏＴデータ収集システム、ＩｏＴデータ収集方法、管理装置、管理プログラム、エージェント装置及びエージェントプログラム

技術分野

[0001] 本発明は、ＩｏＴデータ収集システム、ＩｏＴデータ収集方法、管理装置、管理プログラム、エージェント装置及びエージェントプログラムに関する。

背景技術

[0002] 近年、ＩｏＴ（Ｉｎｔｅｒｎｅｔ　ｏｆ　Ｔｈｉｎｇｓ）と呼ばれる技術が研究されている。ＩｏＴは、コンピュータに限られない様々な物をインターネット等の通信ネットワークに接続することによって、物に関する自動測定、自動認識及び自動制御等を行う技術である。

[0003] ＩｏＴに関し、特許文献１には、ＩＯＴデータベース内でデバイスコンフィギュレーションをシミュレーションし、デバイスコンフィギュレーションが使用可能であるか否かを判定して、使用可能でない場合、代替的なＩＯＴデバイスを含むようにデバイスコンフィギュレーションを再構成するＩＯＴデバイスコンフィギュレーションのための方法が記載されている。

先行技術文献

特許文献

[0004] 特許文献1：特開２０１６－４５９６４号公報

発明の概要

発明が解決しようとする課題

[0005] ＩｏＴデータをサーバ装置に収集するために、ＩｏＴデータを取得するエージェント装置が設置され、エージェント装置からサーバ装置へＩｏＴデータが転送される場合がある。エージェント装置とサーバ装置はインターネッ

トを介して接続され、サーバ装置が認証されたエージェント装置からのみデータ転送を受け付けることで、ＩｏＴデータの転送における安全性を確保する場合がある。

[0006] しかしながら、仮に複数のエージェント装置それぞれに異なる認証キーを割り当てると、設置されるエージェント装置の数が増えるほど、エージェント装置の管理が煩雑となる。また、仮に複数のエージェント装置それぞれに同一の認証キーを割り当てると、当該認証キーが漏洩した場合に、全てのエージェント装置によるデータ転送の安全性が損なわれるおそれがある。

[0007] そこで、本発明は、エージェント装置の容易な管理とデータ転送の安全性を両立したＩｏＴデータ収集システム、ＩｏＴデータ収集方法、管理装置、管理プログラム、エージェント装置及びエージェントプログラムを提供することを目的とする。

課題を解決するための手段

[0008] 本発明の一態様に係るＩｏＴデータ収集システムは、ＩｏＴデータを取得するエージェント装置、エージェント装置を管理する管理装置及びエージェント装置からＩｏＴデータを受信するサーバ装置を含むＩｏＴデータ収集システムであって、エージェント装置は、起動時に管理装置に認証アクティベーションキーを送信する第１送信部を備え、管理装置は、予め登録された登録アクティベーションキーと認証アクティベーションキーを照合する照合部と、登録アクティベーションキーと認証アクティベーションキーの照合結果が正しい場合に、エージェント装置に対し、登録アクティベーションキーと異なる認証エージェントＩＤを送信する送信部と、を備え、エージェント装置は、ＩｏＴデータ及び認証エージェントＩＤを、サーバ装置に送信する第２送信部をさらに備え、サーバ装置は、予め登録された登録エージェントＩＤと認証エージェントＩＤを照合する照合部と、登録エージェントＩＤと認証エージェントＩＤの照合結果が正しい場合に、エージェント装置から、ＩｏＴデータを受信する受信部と、を備える。

[0009] この態様によれば、エージェント装置の起動時に、認証アクティベーショ

ンキーと登録アクティベーションキーの照合が行われ、照合が確認された場合にエージェント装置に対して自動的に認証エージェントＩＤが付与される。これにより、違法にアクティベーションを試みたエージェント装置の起動と認証エージェントＩＤの漏洩が防止されるとともに、エージェント装置のＩＤ管理が容易に行われる。エージェント装置からサーバ装置へＩｏＴデータを転送する際には、認証エージェントＩＤと登録エージェントＩＤが照合され、転送の安全性が確保される。仮に認証エージェントＩＤが漏洩した場合であっても、認証アクティベーションキーを有さないため、エージェント装置のアクティベーションができず、ＩｏＴデータの転送の安全性が確保される。

[0010] 上記態様において、エージェント装置は、少なくともＩｏＴデータを取得する前又は定期的に、管理装置に対して、第２送信部の最新の動作設定を特定する情報の要求を送信する第３送信部をさらに備え、管理装置は、最新の動作設定を特定する情報の要求を受信した場合に、最新の動作設定を特定する情報をエージェント装置に送信する動作設定送信部をさらに備え、エージェント装置は、最新の動作設定を特定する情報と、第２送信部の現在の動作設定を特定する情報とを比較して、最新の動作設定に基づいて、第２送信部の動作設定を行う必要があるか否かを判断する判断部をさらに備え、第３送信部は、判断部により、最新の動作設定に基づいて、第２送信部の動作設定を行う必要があると判断された場合に、管理装置に対して、第２送信部の最新の動作設定の要求を送信し、動作設定送信部は、最新の動作設定の要求を受信した場合に、最新の動作設定をエージェント装置に送信し、エージェント装置は、最新の動作設定に基づいて、第２送信部の動作設定を行う設定部をさらに備えてもよい。

[0011] この態様によれば、エージェント装置自身が、エージェント装置からサーバ装置へＩｏＴデータを転送する等の高負荷処理を実行している間を避けたタイミングに安定的な稼働環境下で最新の動作設定に更新することができ、最新の動作設定に基づいてＩｏＴデータを取得し、サーバ装置へ転送するこ

とができる。また、エージェント装置の第２送信部の動作設定を行う必要があるか否かの判断について、エージェント装置での分散処理が可能となり、エージェント装置の数が増えた場合であっても、管理装置への当該処理の負荷が集中することを防ぎ、ＩｏＴデータ収集システム全体の可用性を維持・向上させる事ができる。また、エージェント装置と管理装置が自律分散協調的に動作設定の更新処理を実行するようになるため、エージェント装置の数が増えた場合であっても、管理者の管理工数が低く抑えられる。

[0012] 上記態様において、設定部は、最新の動作設定に基づいて、ＩｏＴデータをサーバ装置に送信する条件を示す転送条件を設定してもよい。

[0013] この態様によれば、エージェント装置からサーバ装置へＩｏＴデータを転送する条件を適宜変更することができ、ＩｏＴデータの特性に応じた効率の良い転送を行うことができる。

[0014] 上記態様において、管理装置は、エージェント装置に対して、エージェント装置がＩｏＴデータを受信する前又は後に実行する所定の動作に関する動作指令を送信する送信部をさらに備え、エージェント装置は、動作指令に基づいて、ＩｏＴデータを受信する前又は後に所定の動作を実行する動作実行部をさらに備えてもよい。

[0015] この態様によれば、ＩｏＴデータをサーバ装置に転送する前又は後に、エージェント装置が行う動作を規定することができ、より多様なデータ処理を実現することができる。

[0016] 本発明の一態様に係るＩｏＴデータ収集方法は、ＩｏＴデータを取得するエージェント装置、エージェント装置を管理する管理装置及びエージェント装置からＩｏＴデータを受信するサーバ装置を用い、エージェント装置の起動時に、エージェント装置から管理装置に認証アクティベーションキーを送信するステップと、管理装置により、予め登録された登録アクティベーションキーと認証アクティベーションキーを照合するステップと、管理装置による登録アクティベーションキーと認証アクティベーションキーの照合結果が正しい場合に、管理装置からエージェント装置に対し、登録アクティベーシ

ョンキーと異なる認証エージェントＩＤを送信するステップと、ＩｏＴデータ及び認証エージェントＩＤを、エージェント装置からサーバ装置に送信するステップと、サーバ装置により、予め登録された登録エージェントＩＤと認証エージェントＩＤを照合するステップと、サーバ装置による登録エージェントＩＤと認証エージェントＩＤの照合結果が正しい場合に、サーバ装置がエージェント装置から、ＩｏＴデータを受信するステップと、を含む。

[0017] この態様によれば、エージェント装置の起動時に、認証アクティベーションキーと登録アクティベーションキーの照合が行われ、照合が確認された場合にエージェント装置に対して自動的に認証エージェントＩＤが付与される。これにより、違法にアクティベーションを試みたエージェント装置の起動と認証エージェントＩＤの漏洩が防止されるとともに、エージェント装置のＩＤ管理が容易に行われる。エージェント装置からサーバ装置へＩｏＴデータを転送する際には、認証エージェントＩＤと登録エージェントＩＤが照合され、転送の安全性が確保される。仮に認証エージェントＩＤが漏洩した場合であっても、認証アクティベーションキーを有さないため、エージェント装置のアクティベーションができず、ＩｏＴデータの転送の安全性が確保される。

[0018] 本発明の一態様に係る管理装置は、ＩｏＴデータを取得するエージェント装置を管理する管理装置であって、予め登録された登録アクティベーションキーと、エージェント装置の起動時にエージェント装置から管理装置に送信される認証アクティベーションキーとを照合する照合部と、登録アクティベーションキーと認証アクティベーションキーの照合結果が正しい場合に、エージェント装置に対し、登録アクティベーションキーと異なる認証エージェントＩＤを送信する送信部と、を備える。

[0019] この態様によれば、エージェント装置の起動時に、認証アクティベーションキーと登録アクティベーションキーの照合が行われ、照合が確認された場合にエージェント装置に対して自動的に認証エージェントＩＤが付与される。これにより、違法にアクティベーションを試みたエージェント装置の起動

と認証エージェントＩＤの漏洩が防止されるとともに、エージェント装置のＩＤ管理が容易に行われる。

[0020] 本発明の一態様に係る管理プログラムは、ＩｏＴデータを取得するエージェント装置を管理する管理装置に備えられたコンピュータを、予め登録された登録アクティベーションキーと、エージェント装置の起動時にエージェント装置から管理装置に送信される認証アクティベーションキーとを照合する照合部と、登録アクティベーションキーと認証アクティベーションキーの照合結果が正しい場合に、エージェント装置に対し、登録アクティベーションキーと異なる認証エージェントＩＤを送信する送信部、として機能させる。

[0021] この態様によれば、エージェント装置の起動時に、認証アクティベーションキーと登録アクティベーションキーの照合が行われ、照合が確認された場合にエージェント装置に対して自動的に認証エージェントＩＤが付与される。これにより、違法にアクティベーションを試みたエージェント装置の起動と認証エージェントＩＤの漏洩が防止されるとともに、エージェント装置のＩＤ管理が容易に行われる。

[0022] 本発明の一態様に係るエージェント装置は、ＩｏＴデータを取得するエージェント装置であって、起動時に、エージェント装置を管理する管理装置に認証アクティベーションキーを送信する第１送信部と、管理装置に予め登録された登録アクティベーションキーと認証アクティベーションキーを管理装置が照合し、登録アクティベーションキーと認証アクティベーションキーの照合結果が正しい場合に、管理装置からエージェント装置に対して送信される、登録アクティベーションキーと異なる認証エージェントＩＤと、ＩｏＴデータとを、サーバ装置に送信する第２送信部と、を備える。

[0023] この態様によれば、エージェント装置の起動時に、認証アクティベーションキーと登録アクティベーションキーの照合が行われ、照合が確認された場合にエージェント装置に対して自動的に認証エージェントＩＤが付与される。これにより、違法にアクティベーションを試みたエージェント装置の起動と認証エージェントＩＤの漏洩が防止されるとともに、エージェント装置の

ＩＤ管理が容易に行われる。エージェント装置からサーバ装置へＩｏＴデータを転送する際には、認証エージェントＩＤと登録エージェントＩＤが照合され、転送の安全性が確保される。

[0024] 本発明の一態様に係るエージェントプログラムは、ＩｏＴデータを取得するエージェント装置に備えられたコンピュータを、起動時に、エージェント装置を管理する管理装置に認証アクティベーションキーを送信する第１送信部と、管理装置に予め登録された登録アクティベーションキーと認証アクティベーションキーを管理装置が照合し、登録アクティベーションキーと認証アクティベーションキーの照合結果が正しい場合に、管理装置からエージェント装置に対して送信される、登録アクティベーションキーと異なる認証エージェントＩＤと、ＩｏＴデータとを、サーバ装置に送信する第２送信部、として機能させる。

[0025] この態様によれば、エージェント装置の起動時に、認証アクティベーションキーと登録アクティベーションキーの照合が行われ、照合が確認された場合にエージェント装置に対して自動的に認証エージェントＩＤが付与される。これにより、違法にアクティベーションを試みたエージェント装置の起動と認証エージェントＩＤの漏洩が防止されるとともに、エージェント装置のＩＤ管理が容易に行われる。エージェント装置からサーバ装置へＩｏＴデータを転送する際には、認証エージェントＩＤと登録エージェントＩＤが照合され、転送の安全性が確保される。

発明の効果

[0026] 本発明によれば、エージェント装置の容易な管理とデータ転送の安全性を両立したＩｏＴデータ収集システム、ＩｏＴデータ収集方法、管理装置、管理プログラム、エージェント装置及びエージェントプログラムを提供することができる。

図面の簡単な説明

[0027] [図1]本発明の実施形態に係るＩｏＴデータ収集システムの概要を示す図である。

[図2]本発明の実施形態に係るエージェント装置、管理装置及びサーバ装置の機能ブロック図である。

[図3]本発明の実施形態に係るエージェント装置及び管理装置により行われるアクティベーション処理及び動作設定処理を示すフローチャートである。

[図4]本発明の実施形態に係るエージェント装置及びサーバ装置により行われる転送処理を示すフローチャートである。

[図5]本発明の実施形態に係る管理装置及びエージェント装置により行われる動作指令の設定処理を示すフローチャートである。

[図6]本発明の実施形態に係る管理装置に格納される動作設定の内容の一例を示す図である。

発明を実施するための形態

[0028] 添付図面を参照して、本発明の実施形態について説明する。なお、各図において、同一の符号を付したものは、同一又は同様の構成を有する。

[0029] 図１は、本発明の実施形態に係るＩｏＴデータ収集システム１００の概要を示す図である。ＩｏＴデータ収集システム１００は、ＩｏＴデータを取得するエージェント装置１０、エージェント装置１０を管理する管理装置２０及びエージェント装置１０からＩｏＴデータを受信するサーバ装置３０を含む。エージェント装置１０、管理装置２０及びサーバ装置３０は、それぞれ通信ネットワークＮを介して接続され、ＩｏＴデータや認証データを送受信する。通信ネットワークＮは、インターネットやＬＡＮ（Local Area Network）等の通信網であってよい。

[0030] エージェント装置１０は、１又は複数のセンサ２と通信ネットワークＮに接続され、センサ２からＩｏＴデータを取得する。本実施形態に係るエージェント装置１０は、センサ２と通信ネットワークＮを接続するゲートウェイ装置である。本明細書において、ＩｏＴデータとは、物に関する自動測定、自動認識及び自動制御等を行うためのデータであり、本実施形態に係るＩｏＴデータ収集システム１００の場合、センサ２から出力されるセンシングデータである。ＩｏＴデータは、センシングデータ以外に、機械の動作ログデ

ータ及びＰＯＳ（Ｐｏｉｎｔ　Ｏｆ　Ｓａｌｅｓ）データ等の統計データを含んでよい。また、ＩｏＴデータは、サーバ装置３０に動作を指示するための指示データであってもよい。

[0031] 管理装置２０は、エージェント装置１０のアクティベーションや動作設定を管理する。アクティベーションとは、エージェント装置１０の起動時に、エージェント装置１０を利用可能な状態にすることである。管理装置２０は、複数のエージェント装置１０に対して１台備えられればよく、複数のエージェント装置１０を一括して管理するものであってよい。サーバ装置３０は、エージェント装置１０からＩｏＴデータを受信し、格納する。サーバ装置３０は、ＩｏＴデータを格納するデータベースを備えてもよいし、通信ネットワークＮを介してデータベースに接続されるものであってもよい。

[0032] 図２は、本発明の実施形態に係るエージェント装置１０、管理装置２０及びサーバ装置３０の機能ブロック図である。エージェント装置１０は、記憶部１１と、送信部１２と、受信部１３と、設定部１４と、判断部１５と、動作実行部１６と、を備える。管理装置２０は、認証アクティベーションキー受信部２１と、アクティベーションキー照合部２２と、認証エージェントＩＤ発行部２３と、認証エージェントＩＤ送信部２４と、動作設定受信部２５と、動作設定送信部２６と、動作指令編集部２７と、動作指令送信部２８と、登録アクティベーションキーデータベースＤＢ１と、動作設定データベースＤＢ２と、動作指令データベースＤＢ３と、を備える。なお、登録アクティベーションキーデータベースＤＢ１、動作設定データベースＤＢ２及び動作指令データベースＤＢ３は、管理装置２０と別体に設けられるものであってもよい。サーバ装置３０は、認証エージェントＩＤ受信部３１と、エージェントＩＤ照合部３２と、ＩｏＴデータ受信部３３と、登録エージェントＩＤデータベースＤＢ４と、ＩｏＴデータベースＤＢ５と、を備える。なお、登録エージェントＩＤデータベースＤＢ４及びＩｏＴデータベースＤＢ５は、サーバ装置３０と別体に設けられるものであってもよい。なお、管理装置２０及びサーバ装置３０は、それぞれ汎用の記憶部を備え、種々のデータを

格納してよい。

[0033] エージェント装置１０の記憶部１１は、センサ２から取得したＩｏＴデータを一時的に格納する。送信部１２は、アクティベーションが完了していない状態で起動された時に管理装置２０に認証アクティベーションキーを送信する第１送信部１２ａと、ＩｏＴデータ及び認証エージェントＩＤを、サーバ装置３０に送信する第２送信部１２ｂと、少なくともＩｏＴデータを取得する前又は定期的に、管理装置２０に対して、第２送信部１２ｂの最新の動作設定を特定する情報の要求を送信する第３送信部１２ｃと、を含む。ここで、認証アクティベーションキーは、エージェント装置１０の記憶部１１に予め格納され、第１送信部１２ａは、記憶部１１に格納された認証アクティベーションキーを管理装置２０に対して送信する。受信部１３は、管理装置２０から認証エージェントＩＤを受信する認証エージェントＩＤ受信部１３ａと、管理装置２０から第２送信部１２ｂの最新の動作設定を特定する情報及び最新の動作設定を受信する動作設定受信部１３ｂと、を含む。認証エージェントＩＤ受信部１３ａにより受信された認証エージェントＩＤは、エージェント装置１０の記憶部１１に格納される。そして、第２送信部１２ｂは、記憶部１１に格納された認証エージェントＩＤをサーバ装置３０に対して送信する。また、第３送信部１２ｃが送信した最新の動作設定を特定する情報の要求に対して、管理装置２０が最新の動作設定を特定する情報を返信した場合に、動作設定受信部１３ｂは、最新の動作設定を特定する情報を受信し、判断部１５は、第２送信部１２ｂの最新の動作設定を特定する情報と、第２送信部１２ｂの現在の動作設定を特定する情報とを比較して、最新の動作設定に基づいて、第２送信部１２ｂの動作設定を行う必要があるか否かを判断する。判断部１５によって第２送信部１２ｂの動作設定を行う必要があると判断された場合、第３送信部１２ｃは、管理装置２０に対して最新の動作設定の要求を送信し、動作設定受信部１３ｂは、管理装置２０から返信された最新の動作設定を受信して記憶部１１に格納する。そして、設定部１４は、記憶部１１に格納された最新の動作設定に基づいて、第２送信部１２ｂ

の動作設定を行う。また、動作実行部１６は、エージェント装置１０の記憶部１１に格納された動作指令に基づいて、ＩｏＴデータを送信する前又は後に所定の動作を実行する。

[0034] 管理装置２０の認証アクティベーションキー受信部２１は、エージェント装置１０の第１送信部１２ａから送信された認証アクティベーションキーを受信する。アクティベーションキー照合部２２は、登録アクティベーションキーデータベースＤＢ１に予め登録された登録アクティベーションキーと認証アクティベーションキーを照合する。認証エージェントＩＤ発行部２３は、認証アクティベーションキーと登録アクティベーションキーの照合結果が正しい場合に、エージェント装置１０に紐付けられた認証エージェントＩＤを発行する。なお、認証エージェントＩＤは、登録アクティベーションキーとは異なる情報であってよい。認証エージェントＩＤ送信部２４は、エージェント装置１０に対し、認証エージェントＩＤを送信する。認証エージェントＩＤは、例えば、管理装置２０が備える不揮発性の記憶領域に記憶される。ここで、認証エージェントＩＤは、エージェント装置１０を特定する情報（例えばエージェントＩＤのシリアル番号やＩＰアドレス等）と紐付けられて記憶される。管理装置２０は、例えば、認証エージェントＩＤが記憶されているかどうかによって、アクティベーションが完了しているかどうかを判断することができる。なお、アクティベーションの状態の判断手法はこれに限られず、例えば、アクティベーションの状態を表すフラグを不揮発性の記憶領域に記憶する等、任意の手法を採用することができる。なお、認証アクティベーションキーと登録アクティベーションキーは、必ずしも同一のキーでなくてもよい。認証アクティベーションキーと登録アクティベーションキーは、アクティベーションキー照合部２２によって照合が確認できる態様のものであれば、互いに異なるキーであってもよい。また、認証アクティベーションキーは、複数台のエージェント装置１０について共通のキーであってよく、認証エージェントＩＤは、複数台のエージェント装置１０それぞれに固有のＩＤであってよい。

[0035] 管理装置２０の動作設定受信部２５は、エージェント装置１０の第３送信部１２ｃから送信されたエージェント装置１０の第２送信部１２ｂの最新の動作設定を特定する情報の要求を受信する。管理装置２０は、エージェント装置１０に紐付けられた第２送信部１２ｂの最新の動作設定を特定する情報を、動作設定データベースＤＢ２から検索する。ここで、動作設定を特定する情報は、動作設定のバージョン情報であってよい。動作設定データベースＤＢ２に格納される第２送信部１２ｂの動作設定の内容は、管理装置２０のユーザ（ＩｏＴデータ収集システム１００の管理者等）によって編集され、バージョン情報によって最新版が判別可能に管理される。動作設定送信部２６は、エージェント装置１０から最新の動作設定を特定する情報の要求を受信した場合に、検索された最新の動作設定を特定する情報をエージェント装置１０に送信する。また、動作設定受信部２５は、エージェント装置１０から、第２送信部１２ｂの最新の動作設定の要求を受信する。動作設定送信部２６は、動作設定受信部２５によって最新の動作設定の要求を受信した場合に、エージェント装置１０に紐付けられた第２送信部１２ｂの最新の動作設定を動作設定データベースＤＢ２から検索し、エージェント装置１０に送信する。動作設定は、例えば、エージェント装置１０からサーバ装置３０へのＩｏＴデータの転送に関する情報を含む。なお、本明細書において、動作設定に関する情報を単に動作設定と称する。

[0036] 管理装置２０の動作指令編集部２７は、エージェント装置１０がＩｏＴデータを送信する前又は後に実行する所定の動作に関する動作指令を編集し、動作指令データベースＤＢ３に格納する。動作指令送信部２８は、エージェント装置１０に対して、エージェント装置１０がＩｏＴデータを送信する前又は後に実行する所定の動作に関する動作指令を送信する。動作指令データベースＤＢ３に格納される動作指令の内容は、管理装置２０のユーザ（ＩｏＴデータ収集システム１００の管理者等）によって編集される。なお、図２では、動作設定データベースＤＢ２と動作指令データベースＤＢ３を別体のものとして図示しているが、動作設定データベースＤＢ２と動作指令データ

ベースＤＢ３は単一のデータベースによって構成されてもよい。

[0037] サーバ装置３０の認証エージェントＩＤ受信部３１は、エージェント装置１０の第２送信部１２ｂから認証エージェントＩＤを受信する。エージェントＩＤ照合部３２は、登録エージェントＩＤデータベースＤＢ４に予め登録された登録エージェントＩＤと認証エージェントＩＤを照合する。ＩｏＴデータ受信部３３は、登録エージェントＩＤと認証エージェントＩＤの照合結果が正しい場合に、エージェント装置１０から、ＩｏＴデータを受信し、ＩｏＴデータベースＤＢ５に格納する。なお、認証エージェントＩＤと登録エージェントＩＤは、必ずしも同一のＩＤでなくてもよい。認証エージェントＩＤと登録エージェントＩＤは、エージェントＩＤ照合部３２によって照合が確認できる態様のものであれば、互いに異なるＩＤであってもよい。

[0038] 図３は、本発明の実施形態に係るエージェント装置１０及び管理装置２０により行われるアクティベーション処理及び動作設定処理を示すフローチャートである。アクティベーション処理は、少なくともエージェント装置１０が初めて起動されるときに行われる処理であり、エージェント装置１０がＩｏＴデータ収集システム１００に含まれる正規の装置であることを確認する処理である。アクティベーション処理が行われるタイミングは、必ずしもエージェント装置１０の初回起動時に限られない。管理装置２０は、認証エージェントＩＤ生成の有無やフラグの有無によってエージェント装置１０が既にアクティベーションされているか否かを判断し、アクティベーションが未だされていない場合にアクティベーション処理を行うこととしてもよい。

[0039] 管理装置２０は、予め登録アクティベーションキーを発行し、登録アクティベーションキーデータベースＤＢ１に格納する（Ｓ１０）。登録アクティベーションキーは、ランダムな文字列や数列であってよく、秘密に管理される。エージェント装置１０には、ユーザが変更不可能な形式で、登録アクティベーションキーに対応する認証アクティベーションキーが割り当てられる。エージェント装置１０には、例えば製造段階や出荷段階等において認証アクティベーションキーが割り当てられる。

[0040] エージェント装置１０は、少なくとも初回の起動時に、自機に割り当てられた認証アクティベーションキーを管理装置２０に送信する（Ｓ１１）。管理装置２０は、アクティベーションキー照合部２２により認証アクティベーションキーと登録アクティベーションキーの照合を行う（Ｓ１２）。照合結果が正しくない場合（Ｓ１３：Ｎｏ）、アクティベーション処理は終了する。ただし、管理装置２０は、照合結果が正しくない場合、エージェント装置１０又は管理装置２０に対してアクティベーション失敗を表す通知を行ってもよい。管理装置２０に対してアクティベーション失敗を表す通知を行うことで、エージェント装置１０を不正にアクティベートしようとした者にアクティベーション失敗を認識させることなく、対策を講じることが可能となる。

[0041] 認証アクティベーションキーと登録アクティベーションキーの照合結果が正しい場合（Ｓ１３：Ｙｅｓ）、管理装置２０は、エージェント装置１０に対して認証エージェントＩＤを送信する（Ｓ１４）。認証エージェントＩＤは、認証アクティベーションキーと登録アクティベーションキーの照合結果が正しい場合にのみ発行され、アクティベーション処理が成功したエージェント装置１０を管理するためのＩＤである。以上により、本実施形態に係るエージェント装置１０及び管理装置２０により行われるアクティベーション処理が終了する。

[0042] 本実施形態に係るＩｏＴデータ収集システム１００によれば、エージェント装置１０の起動時に、認証アクティベーションキーと登録アクティベーションキーの照合が行われ、照合が確認された場合にエージェント装置１０に対して自動的に認証エージェントＩＤが付与される。これにより、正当な認証アクティベーションキーを有さずに違法にアクティベーションを試みたエージェント装置１０の起動と認証エージェントＩＤの漏洩が防止されるとともに、エージェント装置１０のＩＤ管理が容易に行われる。また、エージェント装置１０と管理装置２０が自律分散協調的にアクティベーションを実行するようになるため、管理者がエージェント装置１０毎にアクティベーショ

ンを行う必要が無くなり、エージェント装置１０の数が増えた場合であっても、管理者の管理工数が低く抑えられる。

[0043] 管理装置２０は、定期的に新しい登録アクティベーションキーの発行を行って、エージェント装置１０に対して、出荷時期に応じた認証アクティベーションキーを割り当ててもよい。例えば、管理装置２０は、新しい登録アクティベーションキーの発行を毎月行い、エージェント装置１０に対して、出荷される月に対応した認証アクティベーションキーを割り当ててもよい。このように、定期的に新しい登録アクティベーションキーの発行を行うことで、仮に以前発行した認証アクティベーションキーが漏洩した場合であっても、漏洩した認証アクティベーションキーを用いた違法なアクティベーションが継続的に行われることが防止される。そのため、エージェント装置１０の違法な起動と認証エージェントＩＤの漏洩が防止され、ＩｏＴデータの転送の安全性が確保される。

[0044] 管理装置２０から、エージェント装置１０に対して認証エージェントＩＤが送信された後（Ｓ１４）、エージェント装置１０は、少なくともＩｏＴデータを取得する前又は定期的に、管理装置２０に対して、第２送信部１２ｂの最新の動作設定のバージョン情報（最新の動作設定を特定する情報）の要求を送信する（Ｓ５０）。なお、動作設定の具体的内容については、図６を用いて詳細に説明する。管理装置２０は、最新の動作設定のバージョン情報の要求を受信した場合、最新の動作設定のバージョン情報をエージェント装置１０に送信する（Ｓ５１）。エージェント装置１０の判断部１５は、最新の動作設定のバージョン情報と、現在の動作設定のバージョン情報とを比較して、最新の動作設定に基づいて、第２送信部１２ｂの動作設定を行う必要があるか否かを判断する（Ｓ５２）。判断部１５は、最新の動作設定のバージョン情報が、現在の動作設定のバージョン情報と異なる場合（最新の動作設定のバージョン情報の数値が、現在の動作設定のバージョン情報の数値より大きい場合）、最新の動作設定に基づいて、第２送信部１２ｂの動作設定を行う必要があると判断し、最新の動作設定のバージョン情報が、現在の動

作設定のバージョン情報と同一である場合（最新の動作設定のバージョン情報の数値が、現在の動作設定のバージョン情報の数値が等しい場合）、最新の動作設定に基づいて、第２送信部１２ｂの動作設定を行う必要が無いと判断する。エージェント装置１０の最新の動作設定のバージョン情報と現在の動作設定のバージョン情報に相違が無いか又は特段の事情により動作設定の更新の必要が無いと判断された場合（Ｓ５２：Ｎｏ）、動作設定処理は終了する。

[0045] エージェント装置１０の最新の動作設定のバージョン情報と現在の動作設定のバージョン情報に相違が有り、動作設定を更新する必要があると判断された場合（Ｓ５２：Ｙｅｓ）、エージェント装置１０は、管理装置２０に対して最新の動作設定の要求を送信する（Ｓ５３）。管理装置２０は、最新の動作設定をエージェント装置１０に送信する（Ｓ５４）。エージェント装置１０は、設定部１４により、最新の動作設定に基づいて、第２送信部１２ｂの動作設定を行う（Ｓ５５）。

[0046] 本実施形態に係るＩｏＴデータ収集システム１００によれば、エージェント装置１０自身が、エージェント装置１０からサーバ装置３０へＩｏＴデータを転送する等の高負荷処理を実行している間を避けたタイミングに安定的な稼働環境下で最新の動作設定に更新することができ、エージェント装置１０が最新の動作設定に基づいてＩｏＴデータを取得し、サーバ装置３０へＩｏＴデータを転送することができる。

[0047] エージェント装置１０の設定部１４は、最新の動作設定に基づいて、ＩｏＴデータをサーバ装置３０に送信する条件を示す転送条件を設定する。例えば、エージェント装置１０の設定部１４は、最新の動作設定に基づいて、記憶部１１に格納されたＩｏＴデータの容量に関する条件を設定したり、記憶部１１に格納されたＩｏＴデータの容量を確認する時間間隔に関する条件を設定したりできる。本実施形態に係るＩｏＴデータ収集システム１００によれば、エージェント装置１０からサーバ装置３０へＩｏＴデータを転送する条件を適宜変更することができ、ＩｏＴデータの特性に応じた効率の良い転

送を行うことができる。また、エージェント装置１０の第２送信部１２ｂの動作設定を行う必要があるか否かの判断について、エージェント装置１０での分散処理が可能となり、エージェント装置１０の数が増えた場合であっても、管理装置２０への当該処理の負荷が集中することを防ぎ、ＩｏＴデータ収集システム１００全体の可用性を維持・向上させる事ができる。また、エージェント装置１０と管理装置２０が自律分散協調的に動作設定の更新処理を実行するようになるため、管理者がエージェント装置１０毎に動作設定を行う必要が無くなり、エージェント装置１０の数が増えた場合であっても、管理者の管理工数が低く抑えられる。

[0048] 図４は、本発明の実施形態に係るエージェント装置１０及びサーバ装置３０により行われる転送処理を示すフローチャートである。転送処理は、図３を用いて説明したアクティベーション処理が行われ、第２送信部１２ｂの動作設定が行われた後に実行される。

[0049] エージェント装置１０は、センサ２からＩｏＴデータを取得し、記憶部１１に格納する（Ｓ２０）。エージェント装置１０は、ＩｏＴデータの転送条件が満足されたか否かを定期的に判断する（Ｓ２１）。ここで、ＩｏＴデータの転送条件は、管理装置２０から送信される動作設定に基づいて定められるものであり、例えば記憶部１１に格納されたＩｏＴデータの容量が所定値以上であるか否かという条件であってよい。また、ＩｏＴデータの転送条件が満足されたか否かを判断する間隔は、管理装置２０から送信される動作設定に基づいて定められるものであり、例えば１分間隔である。

[0050] ＩｏＴデータの転送条件が満足された場合（Ｓ２１：Ｙｅｓ）、エージェント装置１０は、記憶部１１に格納された動作指令を確認し、ＩｏＴデータを送信する前に実行する所定の動作があるか否かを判断する（Ｓ２２）。ＩｏＴデータを送信する前に実行する所定の動作がある場合（Ｓ２２：Ｙｅｓ）、エージェント装置１０は、動作指令に基づいて、所定の動作を実行する（Ｓ２３）。ここで、ＩｏＴデータを送信する前に実行する所定の動作は、例えば、ＩｏＴデータのフォーマット統一、レイアウト変換、クレンジング

（不正データの排除）等であってよい。所定の動作を実行した後又はＩｏＴデータを送信する前に実行する所定の動作が無い場合（Ｓ２２：Ｎｏ）、エージェント装置１０は、自機に割り当てられた認証エージェントＩＤをサーバ装置３０に送信する（Ｓ２４）。サーバ装置３０は、エージェントＩＤ照合部３２により、認証エージェントＩＤと登録エージェントＩＤの照合を行う（Ｓ２５）。認証エージェントＩＤと登録エージェントＩＤの照合結果が正しくない場合（Ｓ２６：Ｎｏ）、ＩｏＴデータの転送を受け付けることなく転送処理は終了する。ただし、サーバ装置３０は、照合結果が正しくない場合、エージェント装置１０又は管理装置２０に対して照合失敗を表す通知を行ってもよい。管理装置２０に対して照合失敗を表す通知を行うことで、エージェント装置１０から不正にＩｏＴデータを転送しようとした者に照合失敗を認識させることなく、対策を講じることが可能となる。

[0051] 認証エージェントＩＤと登録エージェントＩＤの照合結果が正しい場合（Ｓ２６：Ｙｅｓ）、サーバ装置３０は、ＩｏＴデータの転送を許可することを表す転送許可通知をエージェント装置１０に送信する（Ｓ２７）。エージェント装置１０は、転送許可通知を受けて、サーバ装置３０に対してＩｏＴデータの転送を行う（Ｓ２８）。サーバ装置３０は、ＩｏＴデータをＩｏＴデータベースＤＢ５に保存する（Ｓ２９）。サーバ装置３０は、ＩｏＴデータを送信したエージェント装置１０の登録エージェントＩＤと紐付けて、ＩｏＴデータを保存してもよい。

[0052]（エージェントＩＤ照合の効果、漏洩防止について）

本実施形態に係るＩｏＴデータ収集システム１００によれば、エージェント装置１０からサーバ装置３０へＩｏＴデータを転送する際に、認証エージェントＩＤと登録エージェントＩＤが照合され、転送の安全性が確保される。また、仮に認証エージェントＩＤが漏洩した場合であっても、認証アクティベーションキーを有さないため、エージェント装置１０のアクティベーションができず、ＩｏＴデータの転送の安全性が確保される。

[0053] エージェント装置１０は、ＩｏＴデータを転送した後、記憶部１１に格納

された動作指令を確認し、ＩｏＴデータを送信した後に実行する所定の動作があるか否かを判断する（Ｓ３０）。ＩｏＴデータを送信した後に実行する所定の動作がある場合（Ｓ３０：Ｙｅｓ）、エージェント装置１０は、動作指令に基づいて、所定の動作を実行する（Ｓ３１）。ここで、ＩｏＴデータを送信した後に実行する所定の動作は、例えば、他のシステムやアプリケーションとの連携等であってよい。以上により、本実施形態に係るエージェント装置１０及びサーバ装置３０により行われる転送処理が終了する。

[0054] 図５は、本発明の実施形態に係る管理装置２０及びエージェント装置１０により行われる動作指令の設定処理を示すフローチャートである。動作指令の設定処理は、エージェント装置１０によりサーバ装置３０に対してＩｏＴデータが送信される前に行われる。管理装置２０は、エージェント装置１０がＩｏＴデータを送信する前又は後に実行する所定の動作に関する動作指令を、動作指令編集部２７によって編集する（Ｓ４０）。編集された動作指令は、動作指令データベースＤＢ３に格納される。編集された動作指令は、動作指令送信部２８によって、エージェント装置１０に送信される（Ｓ４１）。エージェント装置１０は、動作指令を受信し、記憶部１１に格納する（Ｓ４２）。

[0055] 本実施形態に係るＩｏＴデータ収集システム１００によれば、エージェント装置１０がＩｏＴデータをサーバ装置３０に転送する前後に、エージェント装置１０が行う動作を規定することができ、より多様なデータ処理を実現することができる。

[0056] 図６は、本発明の実施形態に係る管理装置２０に格納される動作設定ＳＤの内容の一例を示す図である。動作設定ＳＤは、配信先ＳＤ１と、監視ＳＤ２と、動作指令ＳＤ３と、暗号化ＳＤ４と、圧縮ＳＤ５と、を含む。動作設定ＳＤは、管理装置２０の表示部に表示され、編集することができる。

[0057] 配信先ＳＤ１は、エージェント装置１０からサーバ装置３０へのＩｏＴデータの転送に関する設定データである。配信先ＳＤ１は、ファイルＩＤ、転送タイプ及び転送コードセットの項目を含む。ファイルＩＤは、転送された

ＩｏＴデータに対してサーバ装置３０において与えられるＩＤであり、本例の場合、「ＴＥＳＴ」である。転送タイプ及び転送コードセットは、エージェント装置１０からサーバ装置３０へＩｏＴデータを転送する際の転送プロトコルを表し、本例の場合、転送タイプは「バイナリ転送」であり、転送コードセットは「ＵＴＦ－８」である。ユーザは、配信先ＳＤ１に含まれる選択タブによって、転送タイプ及び転送コードセットをそれぞれ変更することができる。

[0058] 監視ＳＤ２は、監視ファイル名、監視モード、監視サイズ、監視間隔及び転送完了後動作を含む。監視ファイル名は、記憶部１１に格納されるファイルのうち、転送対象となるファイル名を示し、本例の場合「／ｔｅｓｔｄａｔａ／ｔｅｓｔ．ｔｘｔ」である。監視モードは、監視対象を示しており、本例の場合「ファイルサイズ」すなわちデータ容量である。監視サイズは、監視モードで示される対象がどのようなサイズとなった場合に転送を開始するかという条件を示しており、本例の場合「１００［ＭＢ］」である。監視間隔は、監視対象が監視サイズで示される条件を満たしているか否かを判断する時間間隔を示しており、本例の場合「１［分］」である。転送完了後動作は、エージェント装置１０からサーバ装置３０へＩｏＴデータを転送した後、エージェント装置１０の記憶部１１に格納されたＩｏＴデータをどのように処理するかを示しており、本例の場合「ファイルを削除する」こととなっている。ユーザは、監視ＳＤ２に含まれる選択タブによって、監視モード及び転送完了後動作をそれぞれ変更することができる。なお、監視ファイル名の指定にはワイルドカード「＊」の使用が可能であり、例えば「／ｔｅｓｔｄａｔａ／＊．ｔｘｔ」と指定することで、ｔｅｓｔｄａｔａフォルダに含まれる全てのテキストファイルを監視対象として指定することとができる。

[0059] 動作指令ＳＤ３は、転送前ジョブ及び転送後ジョブを含む。転送前ジョブは、エージェント装置１０がＩｏＴデータを転送する前に行う所定の動作を表す。本例の場合、転送前ジョブは、「フォーマット統一」であり、ＩｏＴ

データのフォーマットを統一する処理を行うことが示されている。また、転送後ジョブは、エージェント装置１０がＩｏＴデータを転送した後に行う所定の動作を表す。本例の場合、転送後ジョブは「他アプリケーションと連携」であり、他のアプリケーションと連携した動作を行うことが示されている。ユーザは、管理装置２０によって、動作指令を編集することができる。

[0060] 暗号化ＳＤ４は、ＩｏＴデータを転送する際の暗号化処理について規定する。圧縮ＳＤ５は、ＩｏＴデータを転送する際の圧縮処理について規定する。暗号化ＳＤ４及び圧縮ＳＤ５は、それぞれ展開タブを押下することで、詳細を設定することができる。

[0061] ＩｏＴデータ収集システム１００の実施形態は、以上説明したものに限られない。例えば、エージェント装置１０は、少なくともＩｏＴデータを取得する前又は定期的に現在の動作設定を特定する情報（バージョン情報）を管理装置２０に送信し、管理装置２０が判断部を備えて、管理装置２０の判断部によって、現在の動作設定を特定する情報と最新の動作設定を特定する情報を比較して動作設定の更新の要否を判断し、動作設定の更新が必要であると判断された場合に、管理装置２０からエージェント装置１０に対して、最新の動作設定を送信することとしてもよい。

[0062] なお、エージェント装置１０の第２送信部１２ｂの現在の動作設定を特定する情報は、バージョン情報に限られず、例えば、動作設定の内容に変更が生じたことを表すフラグの情報とする等、任意の形式を採用することができる。また、エージェント装置１０の第２送信部１２ｂの動作設定の更新が必要であると判断された場合に、管理装置２０からエージェント装置１０に送信される最新の動作設定は、動作設定データベースＤＢ２に格納されるエージェント装置１０の第２送信部１２ｂの動作設定の内容を管理装置２０のユーザ（ＩｏＴデータ収集システム１００の管理者等）が編集した変更履歴に基づく動作設定の差分情報であってもよく、エージェント装置１０の設定部１４は、その動作設定の差分情報に基づき、第２送信部１２ｂの動作設定の差分部分を更新してもよい。

[0063] なお、エージェント装置１０の第２送信部１２ｂの動作設定を編集し、変更履歴を保存・管理する装置は、管理装置２０と別体に設けることもできる。また、エージェント装置１０がサーバ装置３０へＩｏＴデータを送信する条件を示す転送条件は、例えばエージェント装置１０に搭載されたタイマーの時刻が所定の日時を過ぎたか否かという条件又はエージェント装置１０の記憶部１１に格納されたＩｏＴデータがセンサ２から収集されてからの経過時間が所定時間以上であるか否かという条件等又は定期的であってよい。また、管理装置２０及びエージェント装置１０により行われる動作指令の設定処理は、エージェント装置１０がＩｏＴデータを送信する前又は後に実行する所定の動作に関する動作指令を、管理装置２０の動作指令編集部２７によって編集し、動作指令データベースＤＢ３に格納した後、動作指令送信部２８によって、エージェント装置１０に送信される形式に限られず、例えば、エージェント装置１０の第２送信部１２ｂの動作設定の更新処理と同様に、管理装置２０及びエージェント装置１０の間で自律分散協調的に行われる形式を採用することができる。

[0064] また、サーバ装置３０は、ＩｏＴデータを受信した後に実行する所定の動作に関する動作指令に基づいて、所定の動作を実行する動作実行部を備えてもよい。この場合、管理装置２０は、サーバ装置３０の動作指令を動作指令編集部２７によって編集し、動作指令送信部２８によってサーバ装置３０に送信する。サーバ装置３０は、動作指令に基づいて、例えば、ＩｏＴデータを受信した後に、当該ＩｏＴデータを他のデータベース等に転送する動作を動作指令実行部により実行してもよい。また、動作指令は、管理装置２０で編集された後、エージェント装置１０に送信され、エージェント装置１０からサーバ装置３０に認証エージェントＩＤが送信される際に、認証エージェントＩＤと併せて送信されてもよい。

[0065] 以上説明した実施形態は、本発明の理解を容易にするためのものであり、本発明を限定して解釈するためのものではない。実施形態が備える各要素並びにその配置、材料、条件、形状及びサイズ等は、例示したものに限定され

るわけではなく適宜変更することができる。また、異なる実施形態で示した構成同士を部分的に置換し又は組み合わせることが可能である。

請求の範囲

[請求項1] ＩｏＴデータを取得するエージェント装置、前記エージェント装置を管理する管理装置及び前記エージェント装置から前記ＩｏＴデータを受信するサーバ装置を含むＩｏＴデータ収集システムであって、

前記エージェント装置は、起動時に前記管理装置に認証アクティベーションキーを送信する第１送信部を備え、

前記管理装置は、

予め登録された登録アクティベーションキーと前記認証アクティベーションキーを照合する照合部と、

前記登録アクティベーションキーと前記認証アクティベーションキーの照合結果が正しい場合に、前記エージェント装置に対し、前記登録アクティベーションキーと異なる認証エージェントＩＤを送信する送信部と、を備え、

前記エージェント装置は、前記ＩｏＴデータ及び前記認証エージェントＩＤを、前記サーバ装置に送信する第２送信部をさらに備え、

前記サーバ装置は、

予め登録された登録エージェントＩＤと前記認証エージェントＩＤを照合する照合部と、

前記登録エージェントＩＤと前記認証エージェントＩＤの照合結果が正しい場合に、前記エージェント装置から、前記ＩｏＴデータを受信する受信部と、を備える、

ＩｏＴデータ収集システム。

[請求項2] 前記エージェント装置は、少なくとも前記ＩｏＴデータを取得する前又は定期的に、前記管理装置に対して、前記第２送信部の最新の動作設定を特定する情報の要求を送信する第３送信部をさらに備え、

前記管理装置は、前記最新の動作設定を特定する情報の要求を受信した場合に、前記最新の動作設定を特定する情報を前記エージェント装置に送信する動作設定送信部をさらに備え、

前記エージェント装置は、前記最新の動作設定を特定する情報と、前記第２送信部の現在の動作設定を特定する情報とを比較して、前記最新の動作設定に基づいて、前記第２送信部の動作設定を行う必要があるか否かを判断する判断部をさらに備え、

前記第３送信部は、前記判断部により前記第２送信部の動作設定を行う必要があると判断された場合に、前記管理装置に対して、前記第２送信部の最新の動作設定の要求を送信し、

前記動作設定送信部は、前記最新の動作設定の要求を受信した場合に、前記最新の動作設定を前記エージェント装置に送信し、

前記エージェント装置は、前記最新の動作設定に基づいて、前記第２送信部の動作設定を行う設定部をさらに備える、

請求項１に記載のＩｏＴデータ収集システム。

[請求項3] 前記設定部は、前記最新の動作設定に基づいて、前記ＩｏＴデータを前記サーバ装置に送信する条件を示す転送条件を設定する、

請求項２に記載のＩｏＴデータ収集システム。

[請求項4] 前記管理装置は、前記エージェント装置に対して、前記エージェント装置が前記ＩｏＴデータを送信する前又は後に実行する所定の動作に関する動作指令を送信する送信部をさらに備え、

前記エージェント装置は、前記動作指令に基づいて、前記ＩｏＴデータを送信する前又は後に前記所定の動作を実行する動作実行部をさらに備える、

請求項２又は３に記載のＩｏＴデータ収集システム。

[請求項5] ＩｏＴデータを取得するエージェント装置、前記エージェント装置を管理する管理装置及び前記エージェント装置から前記ＩｏＴデータを受信するサーバ装置を用い、

前記エージェント装置の起動時に、前記エージェント装置から前記管理装置に認証アクティベーションキーを送信するステップと、

前記管理装置により、予め登録された登録アクティベーションキー

と前記認証アクティベーションキーを照合するステップと、

前記管理装置による前記登録アクティベーションキーと前記認証アクティベーションキーの照合結果が正しい場合に、前記管理装置から前記エージェント装置に対し、前記登録アクティベーションキーと異なる認証エージェントＩＤを送信するステップと、

前記ＩｏＴデータ及び前記認証エージェントＩＤを、前記エージェント装置から前記サーバ装置に送信するステップと、

前記サーバ装置により、予め登録された登録エージェントＩＤと前記認証エージェントＩＤを照合するステップと、

前記サーバ装置による前記登録エージェントＩＤと前記認証エージェントＩＤの照合結果が正しい場合に、前記サーバ装置が前記エージェント装置から、前記ＩｏＴデータを受信するステップと、

を含むＩｏＴデータ収集方法。

[請求項6] ＩｏＴデータを取得するエージェント装置を管理する管理装置であって、

予め登録された登録アクティベーションキーと、前記エージェント装置の起動時に前記エージェント装置から前記管理装置に送信される認証アクティベーションキーとを照合する照合部と、

前記登録アクティベーションキーと前記認証アクティベーションキーの照合結果が正しい場合に、前記エージェント装置に対し、前記登録アクティベーションキーと異なる認証エージェントＩＤを送信する送信部と、を備える、

管理装置。

[請求項7] ＩｏＴデータを取得するエージェント装置を管理する管理装置に備えられたコンピュータを、

予め登録された登録アクティベーションキーと、前記エージェント装置の起動時に前記エージェント装置から前記管理装置に送信される認証アクティベーションキーとを照合する照合部と、

前記登録アクティベーションキーと前記認証アクティベーションキーの照合結果が正しい場合に、前記エージェント装置に対し、前記登録アクティベーションキーと異なる認証エージェントＩＤを送信する送信部、

として機能させる管理プログラム。

[請求項8] ＩｏＴデータを取得するエージェント装置であって、

起動時に、前記エージェント装置を管理する管理装置に認証アクティベーションキーを送信する第１送信部と、

前記管理装置に予め登録された登録アクティベーションキーと前記認証アクティベーションキーを前記管理装置が照合し、前記登録アクティベーションキーと前記認証アクティベーションキーの照合結果が正しい場合に、前記管理装置から前記エージェント装置に対して送信される、前記登録アクティベーションキーと異なる認証エージェントＩＤと、前記ＩｏＴデータとを、サーバ装置に送信する第２送信部と、を備える、

エージェント装置。

[請求項9] ＩｏＴデータを取得するエージェント装置に備えられたコンピュータを、

起動時に、前記エージェント装置を管理する管理装置に認証アクティベーションキーを送信する第１送信部と、

前記管理装置に予め登録された登録アクティベーションキーと前記認証アクティベーションキーを前記管理装置が照合し、前記登録アクティベーションキーと前記認証アクティベーションキーの照合結果が正しい場合に、前記管理装置から前記エージェント装置に対して送信される、前記登録アクティベーションキーと異なる認証エージェントＩＤと、前記ＩｏＴデータとを、サーバ装置に送信する第２送信部、

として機能させるエージェントプログラム。

補正された請求の範囲
[2017年12月13日 (13.12.2017) 国際事務局受理]

[請求項１] （補正後） ＩｏＴデータを取得するエージェント装置、前記エージェント装置を管理する管理装置及び前記エージェント装置から前記ＩｏＴデータを受信するサーバ装置を含むＩｏＴデータ収集システムであって、

前記エージェント装置は、起動時に前記管理装置に認証アクティベーションキーを送信する第１送信部を備え、

前記管理装置は、

予め登録された登録アクティベーションキーと前記認証アクティベーションキーを照合する照合部と、

前記登録アクティベーションキーと前記認証アクティベーションキーの照合結果が正しい場合に、前記エージェント装置に対し、前記登録アクティベーションキーと異なる認証エージェントＩＤを送信する送信部と、を備え、

前記エージェント装置は、前記ＩｏＴデータ及び前記認証エージェントＩＤを、前記サーバ装置に自動的に送信する第２送信部をさらに備え、

前記サーバ装置は、

予め登録された登録エージェントＩＤと前記認証エージェントＩＤを照合する照合部と、

前記登録エージェントＩＤと前記認証エージェントＩＤの照合結果が正しい場合に、前記エージェント装置から、前記ＩｏＴデータを受信する受信部と、を備え、

前記認証アクティベーションキーは、複数台の前記エージェント装置について共通し、

前記認証エージェントＩＤは、複数台の前記エージェント装置それぞれに固有のＩＤである、

ＩｏＴデータ収集システム。

[請求項２] 前記エージェント装置は、少なくとも前記ＩｏＴデータを取得する前又は定期的に、前記管理装置に対して、前記第２送信部の最新の動作設定を特定する情報の要求を送信する第３送信部をさらに備え、

前記管理装置は、前記最新の動作設定を特定する情報の要求を受信した場合に、前記最新の動作設定を特定する情報を前記エージェント装置に送信する動作設定送信部をさらに備え、

前記エージェント装置は、前記最新の動作設定を特定する情報と、前記第２送信部の現在の動作設定を特定する情報とを比較して、前記最新の動作設定に基づいて、前記第２送信部の動作設定を行う必要が

あるか否かを判断する判断部をさらに備え、

前記第３送信部は、前記判断部により前記第２送信部の動作設定を行う必要があると判断された場合に、前記管理装置に対して、前記第２送信部の最新の動作設定の要求を送信し、

前記動作設定送信部は、前記最新の動作設定の要求を受信した場合に、前記最新の動作設定を前記エージェント装置に送信し、

前記エージェント装置は、前記最新の動作設定に基づいて、前記第２送信部の動作設定を行う設定部をさらに備える、

請求項１に記載のＩｏＴデータ収集システム。

［請求項３］ 前記設定部は、前記最新の動作設定に基づいて、前記ＩｏＴデータを前記サーバ装置に送信する条件を示す転送条件を設定する、

請求項２に記載のＩｏＴデータ収集システム。

［請求項４］ 前記管理装置は、前記エージェント装置に対して、前記エージェント装置が前記ＩｏＴデータを送信する前又は後に実行する所定の動作に関する動作指令を送信する送信部をさらに備え、

前記エージェント装置は、前記動作指令に基づいて、前記ＩｏＴデータを送信する前又は後に前記所定の動作を実行する動作実行部をさらに備える、

請求項２又は３に記載のＩｏＴデータ収集システム。

［請求項５］ （補正後） ＩｏＴデータを取得するエージェント装置、前記エージェント装置を管理する管理装置及び前記エージェント装置から前記ＩｏＴデータを受信するサーバ装置を用い、

前記エージェント装置の起動時に、前記エージェント装置から前記管理装置に認証アクティベーションキーを送信するステップと、

前記管理装置により、予め登録された登録アクティベーションキーと前記認証アクティベーションキーを照合するステップと、

前記管理装置による前記登録アクティベーションキーと前記認証アクティベーションキーの照合結果が正しい場合に、前記管理装置から前記エージェント装置に対し、前記登録アクティベーションキーと異なる認証エージェントＩＤを送信するステップと、

前記ＩｏＴデータ及び前記認証エージェントＩＤを、前記エージェント装置から前記サーバ装置に自動的に送信するステップと、

前記サーバ装置により、予め登録された登録エージェントＩＤと前記認証エージェントＩＤを照合するステップと、

前記サーバ装置による前記登録エージェントＩＤと前記認証エージ

ェントＩＤの照合結果が正しい場合に、前記サーバ装置が前記エージェント装置から、前記ＩｏＴデータを受信するステップと、
を含み、
前記認証アクティベーションキーは、複数台の前記エージェント装置について共通し、
前記認証エージェントＩＤは、複数台の前記エージェント装置それぞれに固有のＩＤである、
ＩｏＴデータ収集方法。

［請求項６］ （補正後） ＩｏＴデータを取得するエージェント装置を管理する管理装置であって、
予め登録された登録アクティベーションキーと、前記エージェント装置の起動時に前記エージェント装置から前記管理装置に送信される認証アクティベーションキーとを照合する照合部と、
前記登録アクティベーションキーと前記認証アクティベーションキーの照合結果が正しい場合に、前記エージェント装置に対し、前記登録アクティベーションキーと異なる認証エージェントＩＤを送信する送信部と、を備え、
前記認証アクティベーションキーは、複数台の前記エージェント装置について共通し、
前記認証エージェントＩＤは、複数台の前記エージェント装置それぞれに固有のＩＤである、
管理装置。

［請求項７］ （補正後） ＩｏＴデータを取得するエージェント装置を管理する管理装置に備えられたコンピュータを、
予め登録された登録アクティベーションキーと、前記エージェント装置の起動時に前記エージェント装置から前記管理装置に送信される認証アクティベーションキーとを照合する照合部と、
前記登録アクティベーションキーと前記認証アクティベーションキーの照合結果が正しい場合に、前記エージェント装置に対し、前記登録アクティベーションキーと異なる認証エージェントＩＤを送信する送信部、として機能させ、
前記認証アクティベーションキーは、複数台の前記エージェント装置について共通し、
前記認証エージェントＩＤは、複数台の前記エージェント装置それぞれに固有のＩＤである、
管理プログラム。

［請求項８］ （補正後） ＩｏＴデータを取得するエージェント装置であって、
起動時に、前記エージェント装置を管理する管理装置に認証アクティベーションキーを送信する第１送信部と、
前記管理装置に予め登録された登録アクティベーションキーと前記認証アクティベーションキーを前記管理装置が照合し、前記登録アクティベーションキーと前記認証アクティベーションキーの照合結果が正しい場合に、前記管理装置から前記エージェント装置に対して送信される、前記登録アクティベーションキーと異なる認証エージェントＩＤと、前記ＩｏＴデータとを、サーバ装置に自動的に送信する第２送信部と、を備え、
前記認証アクティベーションキーは、複数台の前記エージェント装置について共通し、
前記認証エージェントＩＤは、複数台の前記エージェント装置それぞれに固有のＩＤである、
エージェント装置。

［請求項９］ （補正後） ＩｏＴデータを取得するエージェント装置に備えられたコンピュータを、
起動時に、前記エージェント装置を管理する管理装置に認証アクティベーションキーを送信する第１送信部と、
前記管理装置に予め登録された登録アクティベーションキーと前記認証アクティベーションキーを前記管理装置が照合し、前記登録アクティベーションキーと前記認証アクティベーションキーの照合結果が正しい場合に、前記管理装置から前記エージェント装置に対して送信される、前記登録アクティベーションキーと異なる認証エージェントＩＤと、前記ＩｏＴデータとを、サーバ装置に自動的に送信する第２送信部、
として機能させ、
前記認証アクティベーションキーは、複数台の前記エージェント装置について共通し、
前記認証エージェントＩＤは、複数台の前記エージェント装置それぞれに固有のＩＤである、
エージェントプログラム。

条約第１９条（１）に基づく説明書

明細書の段落０００９及び００３４等に基づき、請求の範囲第１項は、「前記エージェント装置は、前記ＩｏＴデータ及び前記認証エージェントＩＤを、前記サーバ装置に 自動的に 送信する第２送信部をさらに備え」、「前記認証アクティベーションキーは、複数台の前記エージェント装置について共通し、前記認証エージェントＩＤは、複数台の前記エージェント装置それぞれに固有のＩＤである 」、ＩｏＴデータ収集システムであることを明確にした。

文献１の「固定の認証ＩＤ及び固定のパスワード」並びに文献２の「ユーザＩＤとパスワード」は、それぞれ端末に固有のＩＤ、パスワードでなければならない。

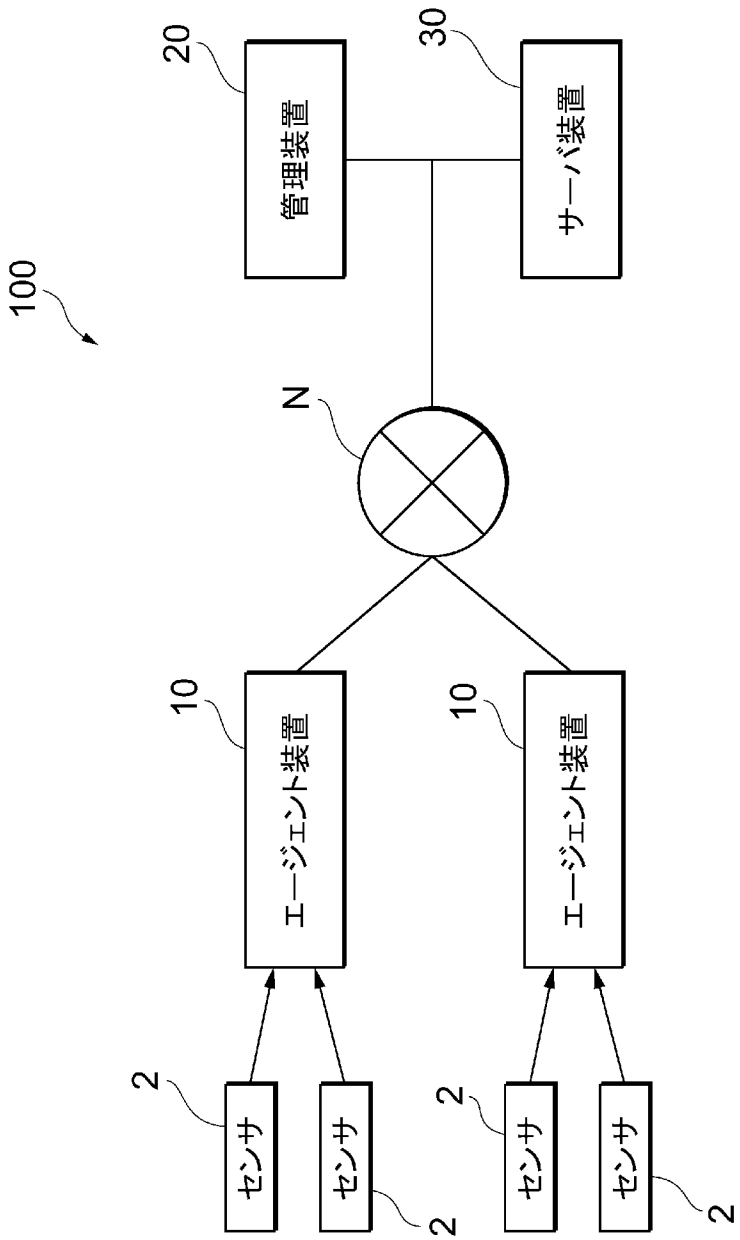
本発明は、「前記認証アクティベーションキーは、複数台の前記エージェント装置について共通し、前記認証エージェントＩＤは、複数台の前記エージェント装置それぞれに固有のＩＤである 」ことで、「仮に複数のエージェント装置それぞれに異なる認証キーを割り当てると、設置されるエージェント装置の数が増えるほど、エージェント装置の管理が煩雑となる。また、仮に複数のエージェント装置それぞれに同一の認証キーを割り当てると、当該認証キーが漏洩した場合に、全てのエージェント装置によるデータ転送の安全性が損なわれるおそれがある。」（本願明細書の段落０００６）という課題を解決し、エージェント装置の容易な管理とデータ転送の安全性を両立するという効果を奏する。

また、文献１の「固定の認証ＩＤ及び固定のパスワード」並びに「使い捨てＩＤ及び使い捨てパスワード」、文献２の「ユーザＩＤとパスワード」及び「ワンタイムパスワード」は、いずれも人に通知され、人が入力する。

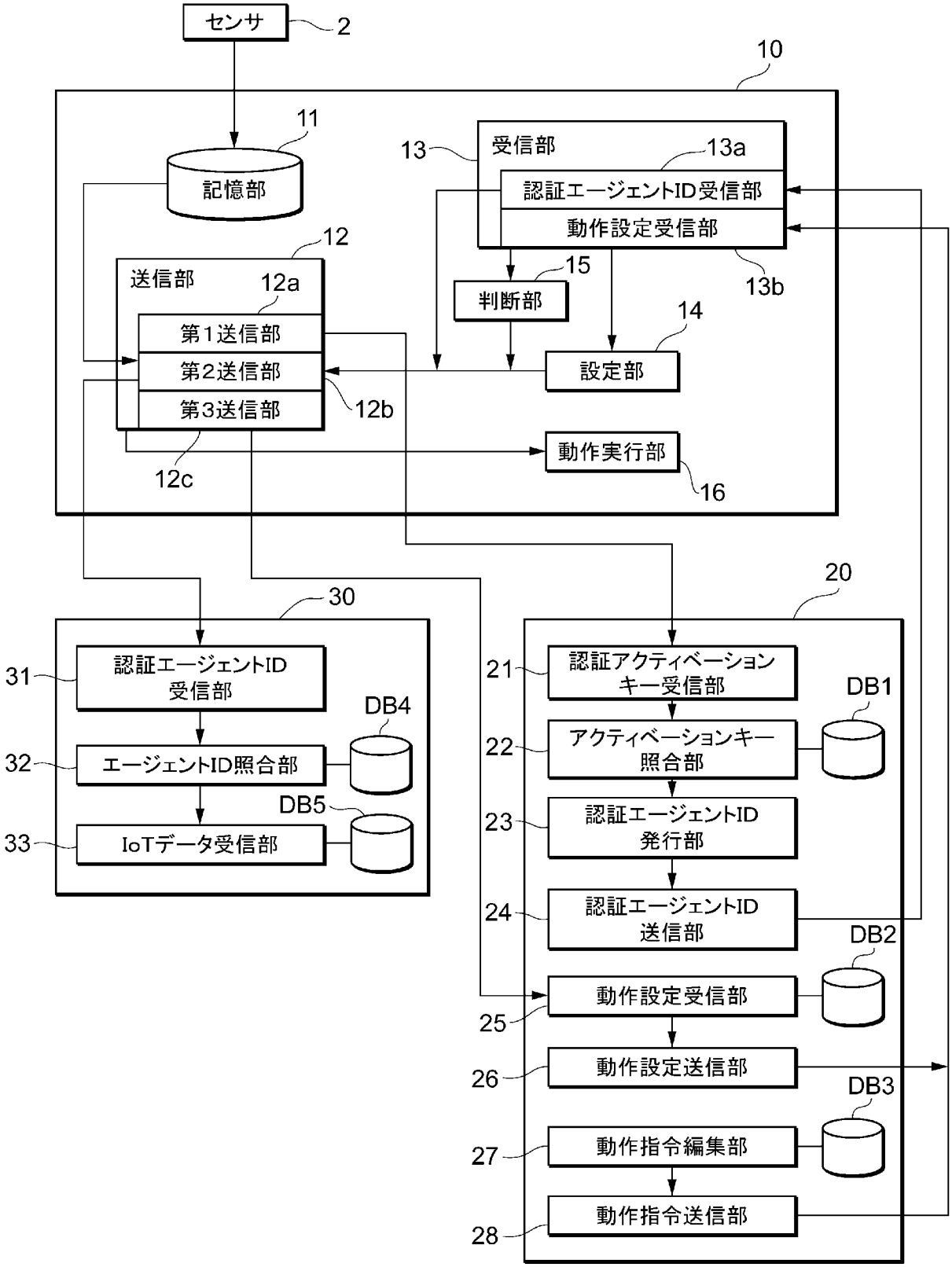
本発明は、「前記エージェント装置は、前記ＩｏＴデータ及び前記認証エージェントＩＤを、前記サーバ装置に 自動的に 送信する」ことで、エージェント装置の容易な管理とデータ転送の安全性を両立するという効果を奏する。

請求の範囲第５項から第９項についても、第１項と同様の補正を行った。

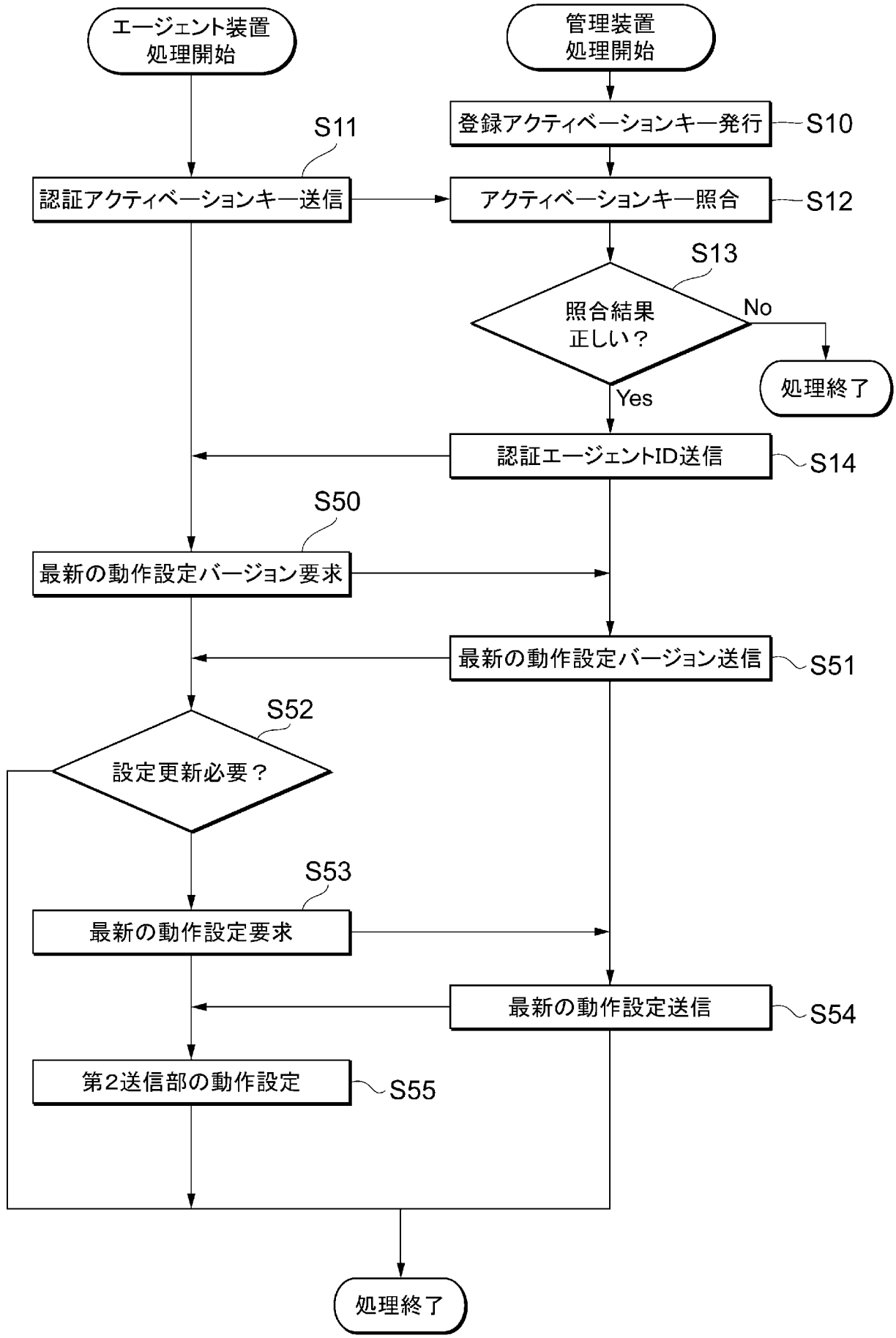
[図1]


100
20
管理装置
30
サーバ装置
N
10
エージェント装置
10
エージェント装置
2
センサ
2
センサ
2
センサ
2
センサ

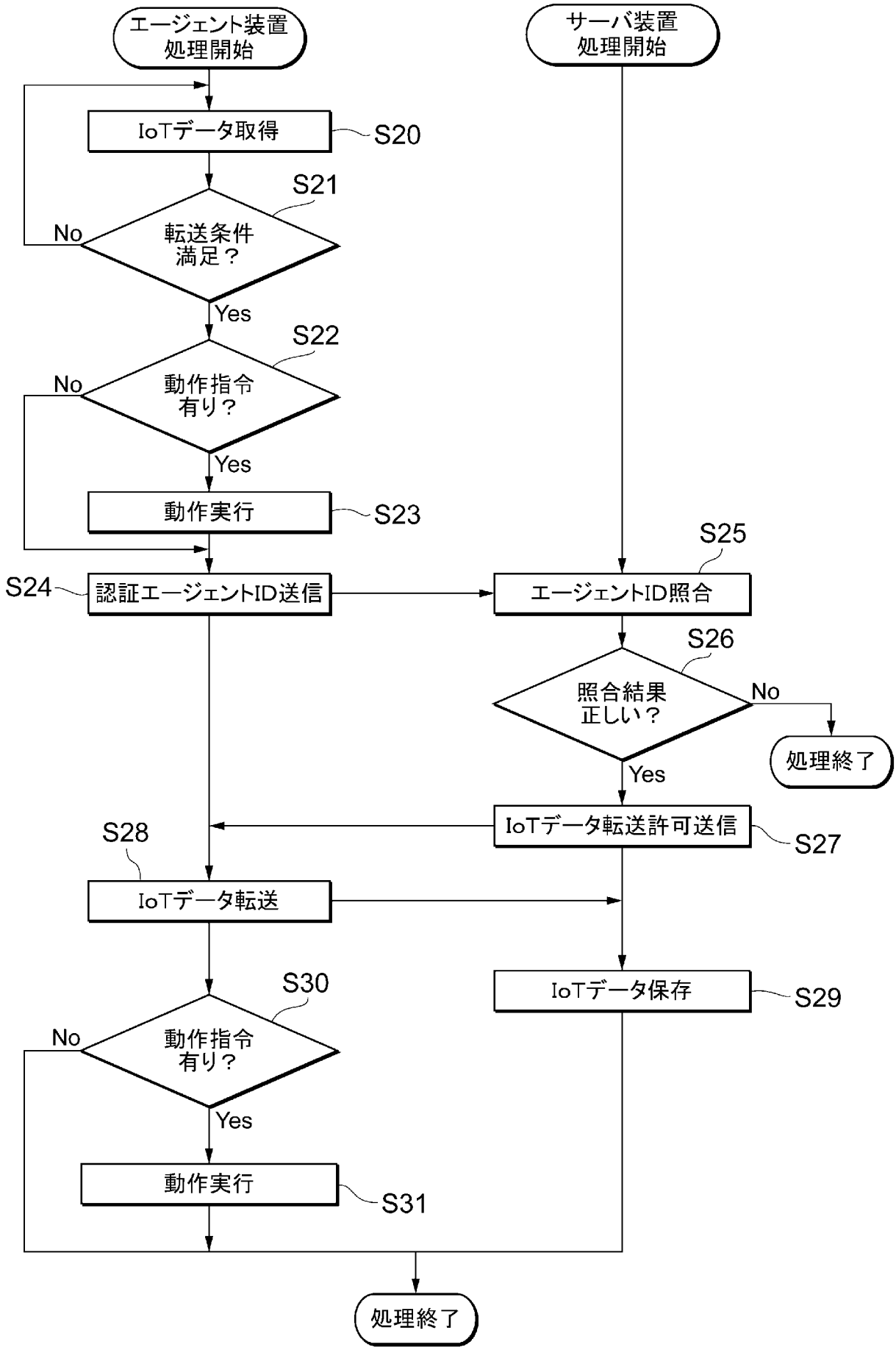
[図2]


センサ
2
10
11
記憶部
13
受信部
13a
認証エージェントID受信部
動作設定受信部
13b
15
判断部
12
送信部
12a
第1送信部
第2送信部
第3送信部
12b
12c
14
設定部
動作実行部
16
30
31
認証エージェントID
受信部
DB4
32
エージェントID照合部
DB5
33
IoTデータ受信部
20
21
認証アクティベーション
キー受信部
DB1
22
アクティベーションキー
照合部
23
認証エージェントID
発行部
24
認証エージェントID
送信部
DB2
動作設定受信部
25
26
動作設定送信部
DB3
27
動作指令編集部
28
動作指令送信部

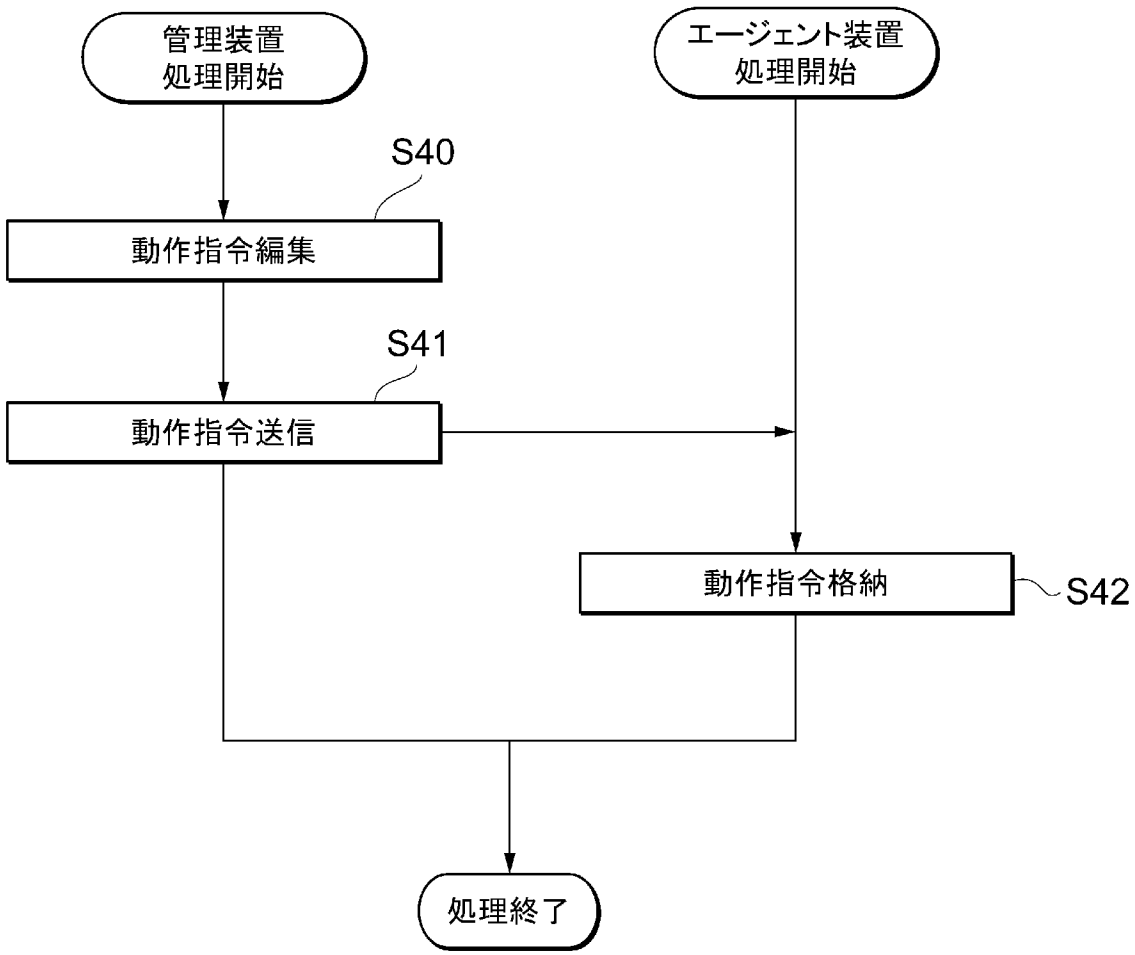
[図3]


エージェント装置
処理開始
管理装置
処理開始
登録アクティベーションキー発行
S10
S11
認証アクティベーションキー送信
アクティベーションキー照合
S12
S13
照合結果
正しい？
No
処理終了
Yes
認証エージェントID送信
S14
S50
最新の動作設定バージョン要求
最新の動作設定バージョン送信
S51
S52
設定更新必要？
S53
最新の動作設定要求
最新の動作設定送信
S54
第2送信部の動作設定
S55
処理終了

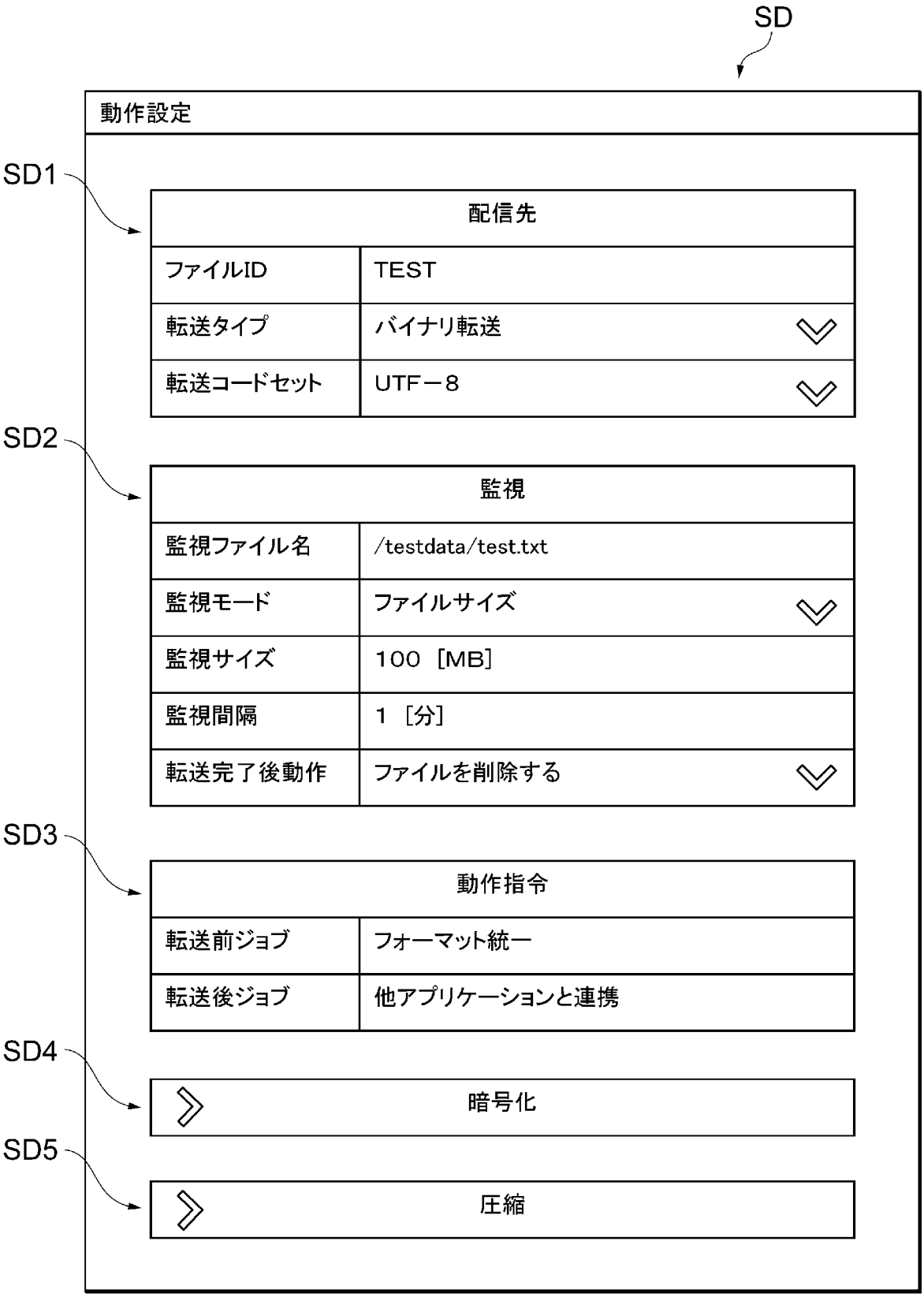
[図4]


エージェント装置
処理開始
サーバ装置
処理開始
IoTデータ取得
S20
S21
No
転送条件
満足？
Yes
S22
No
動作指令
有り？
Yes
動作実行
S23
S24
認証エージェントID送信
S25
エージェントID照合
S26
照合結果
正しい？
No
処理終了
Yes
IoTデータ転送許可送信
S27
S28
IoTデータ転送
IoTデータ保存
S29
S30
No
動作指令
有り？
Yes
動作実行
S31
処理終了

[図5]


管理装置
処理開始
エージェント装置
処理開始
S40
動作指令編集
S41
動作指令送信
動作指令格納
S42
処理終了

[図6]


SD
動作設定
SD1
配信先
ファイルID
TEST
転送タイプ
バイナリ転送
転送コードセット
UTF－8
SD2
監視
監視ファイル名
/testdata/test.txt
監視モード
ファイルサイズ
監視サイズ
100 [MB]
監視間隔
1 [分]
転送完了後動作
ファイルを削除する
SD3
動作指令
転送前ジョブ
フォーマット統一
転送後ジョブ
他アプリケーションと連携
SD4
暗号化
SD5
圧縮

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2017/001673

A. CLASSIFICATION OF SUBJECT MATTER
H04L9/32(2006.01)i, *G06F21/44*(2013.01)i

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)
H04L9/32, G06F21/44

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2017
Kokai Jitsuyo Shinan Koho	1971-2017	Toroku Jitsuyo Shinan Koho	1994-2017

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y A	JP 2011-248709 A (Funai Electric Co., Ltd.), 08 December 2011 (08.12.2011), paragraphs [0025] to [0055], [0077]; fig. 2 & US 2011/0295715 A1 paragraphs [0044] to [0079], [0101]; fig. 2 & EP 2390828 A1	1,5-9 2-4
Y A	JP 2003-296279 A (Digital Electronics Corp.), 17 October 2003 (17.10.2003), paragraphs [0029], [0033] (Family: none)	1,5-9 2-4
A	JP 2015-70573 A (Oki Electric Industry Co., Ltd.), 13 April 2015 (13.04.2015), paragraphs [0024] to [0049] (Family: none)	1-9

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
12 April 2017 (12.04.17)	25 April 2017 (25.04.17)

Name and mailing address of the ISA/	Authorized officer
Japan Patent Office 3-4-3,Kasumigaseki,Chiyoda-ku, Tokyo 100-8915,Japan	Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2017/001673

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2013-172179 A (KDDI Corp.), 02 September 2013 (02.09.2013), paragraphs [0032] to [0082] (Family: none)	1-9
A	JP 2015-106349 A (Nippon Telegraph and Telephone Corp.), 08 June 2015 (08.06.2015), paragraphs [0019] to [0046] (Family: none)	1-9
A	WO 2015/025830 A1 (Ricoh Co., Ltd.), 26 February 2015 (26.02.2015), paragraphs [0126] to [0135] & US 2016/0173496 A1 paragraphs [0178] to [0187]	2-4

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２０１７／００１６７３

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　H04L9/32(2006.01)i, G06F21/44(2013.01)i

Ｂ．　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Int.Cl.　H04L9/32, G06F21/44

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２０１７年
日本国実用新案登録公報	１９９６－２０１７年
日本国登録実用新案公報	１９９４－２０１７年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

Ｃ．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求項の番号
Y A	JP 2011-248709 A (船井電機株式会社) 2011.12.08, 段落 [0025] － [0055], [0077], 図２ & US 2011/0295715 A1, 段落 [0044] － [0079], [0101], 図２ & EP 2390828 A1	1, 5-9 2-4
Y A	JP 2003-296279 A (株式会社デジタル) 2003.10.17, 段落 [0029], [0033] (ファミリーなし)	1, 5-9 2-4

☑　Ｃ欄の続きにも文献が列挙されている。　　☐　パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの
「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「Ｏ」口頭による開示、使用、展示等に言及する文献
「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「＆」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
１２．０４．２０１７	２５．０４．２０１７

国際調査機関の名称及びあて先
日本国特許庁（ＩＳＡ／ＪＰ）
郵便番号１００－８９１５
東京都千代田区霞が関三丁目４番３号

特許庁審査官（権限のある職員）　５Ｓ　６３０４
青木　重徳
電話番号　０３－３５８１－１１０１　内線　３５４６

C（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求項の番号
A	JP 2015-70573 A (沖電気工業株式会社) 2015.04.13, 段落［0024］－［0049］ (ファミリーなし)	1-9
A	JP 2013-172179 A (ＫＤＤＩ株式会社) 2013.09.02, 段落［0032］－［0082］ (ファミリーなし)	1-9
A	JP 2015-106349 A (日本電信電話株式会社) 2015.06.08, 段落［0019］－［0046］ (ファミリーなし)	1-9
A	WO 2015/025830 A1 (株式会社リコー) 2015.02.26, 段落［0126］－［0135］ & US 2016/0173496 A1, 段落［0178］－［0187］	2-4