(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
2021年4月22日(22.04.2021)

WIPO | PCT

(10) 国際公開番号
WO 2021/075475 A1

(51) 国際特許分類:
H01L 21/02 (2006.01)

(21) 国際出願番号： PCT/JP2020/038838

(22) 国際出願日： 2020年10月14日(14.10.2020)

(25) 国際出願の言語： 日本語

(26) 国際公開の言語： 日本語

(30) 優先権データ：
特願 2019-189021 2019年10月15日(15.10.2019) JP

(71) 出願人: 株式会社ウフル (**UHURU CORPORATION**) [JP/JP]; 〒1050001 東京都港区虎ノ門４－３－１３ ヒューリック神谷町ビル４Ｆ Tokyo (JP).

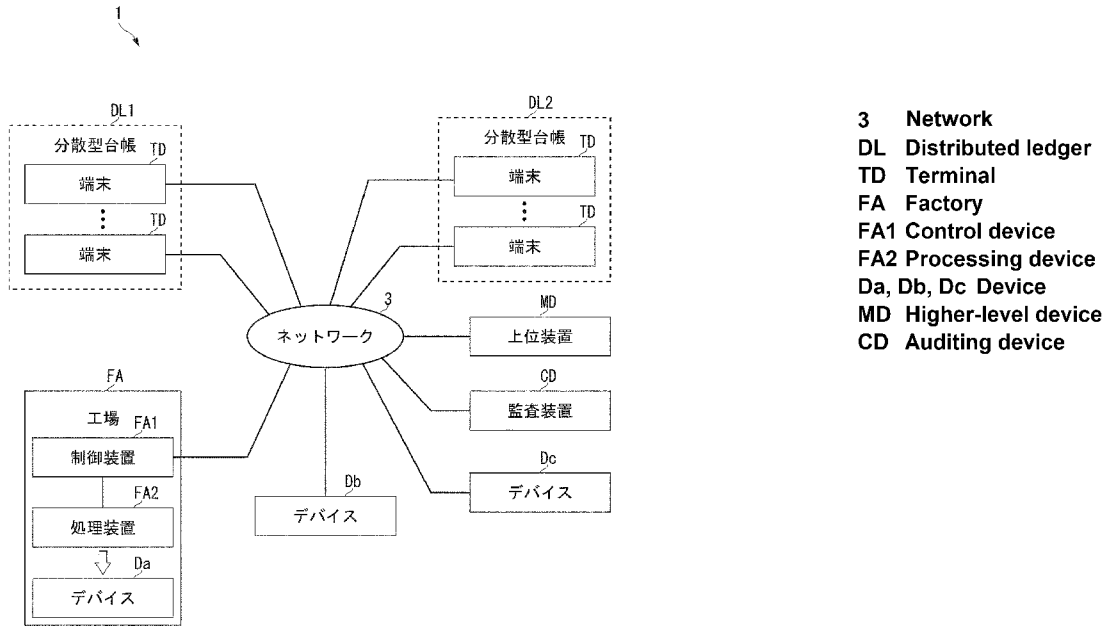
(72) 発明者: 古城 篤 (**KOJO, Atsushi**); 〒1050001 東京都港区虎ノ門４－３－１３ ヒューリック神谷町ビル４Ｆ 株式会社ウフル内 Tokyo (JP). 竹之下 航洋 (**TAKENOSHITA, Koyo**); 〒1050001 東京都港区虎ノ門４－３－１３ ヒューリック神谷町ビル４Ｆ 株式会社ウフル内 Tokyo (JP).

(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, IT, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT,

(54) **Title:** DEVICE MANAGEMENT SYSTEM

(54) 発明の名称： デバイス管理システム

[図1]



3 Network
DL Distributed ledger
TD Terminal
FA Factory
FA1 Control device
FA2 Processing device
Da, Db, Dc Device
MD Higher-level device
CD Auditing device

(57) **Abstract:** This device management system is provided with: a first information processing device which causes a storage unit to store at least one information item among manufacturing information which relates to a step of manufacturing a device having a storage area for holding identifying information and includes identifying information, start-up information which relates to a step of starting up a device and includes identifying information, and updating information which relates to a step of updating a device and includes identifying information; and a second information processing

WO 2021/075475 A1

[続葉有]

QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, 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:

一 国際調査報告 (条約第21条(3))

device which reads, from among the manufacturing information, the start-up information, and the updating information stored in the storage unit, at least one information item including the identifying information read from the storage area of an object being managed, and which uses the information that has been read to determine the reliability of a device being managed.

(57) 要約:デバイス管理システムは、識別情報を保持する記憶域が設けられるデバイスの製造工程に係る情報であって識別情報を含む製造時情報と、デバイスの起動工程に係る情報であって識別情報を含む起動時情報と、デバイスの更新工程に係る情報であって識別情報を含む更新時情報との少なくとも1つの情報を記憶部に記憶させる第1の情報処理装置と、記憶部に記憶された製造時情報と起動時情報と更新時情報との少なくとも1つの情報のうち、管理対象の記憶域から読み出される識別情報を含む少なくとも1つの情報を読み出し、読み出した情報を用いて管理対象のデバイスの信頼性を判定する第2の情報処理装置と、を備える。

明　細　書

発明の名称 ： デバイス管理システム

技術分野

[0001]　本発明は、デバイス管理システムに関する。

背景技術

[0002]　下記の特許文献１には、半導体チップ等に微小な識別情報を設けることによって、半導体デバイスの管理を容易に実現することが記載されている。通信を介して接続される各種デバイスを利用する技術分野において、デバイスが信頼できるか否かを精度よく判別できることが望まれる。

先行技術文献

特許文献

[0003] 特許文献1：特開２０１４－１４６７２２号公報

発明の概要

[0004]　本発明の態様に従えば、識別情報を保持する記憶域が設けられるデバイスの製造工程に係る情報であって識別情報を含む製造時情報と、デバイスの起動工程に係る情報であって識別情報を含む起動時情報と、デバイスの更新工程に係る情報であって識別情報を含む更新時情報との少なくとも１つの情報を記憶部に記憶させる第１の情報処理装置と、記憶部に記憶された製造時情報と起動時情報と更新時情報との少なくとも１つの情報のうち、管理対象の記憶域から読み出される識別情報を含む少なくとも１つの情報を読み出し、読み出した情報を用いて管理対象のデバイスの信頼性を判定する第２の情報処理装置と、を備えるデバイス管理システムが提供される。

図面の簡単な説明

[0005] [図1]実施形態に係るデバイス管理システムを示す図である。

[図2]製造時のトラスト情報を記憶する処理を示す図である。

[図3]起動時または更新時のトラスト情報を記憶する処理を示す図である。

[図4]監査時のトラスト情報を記憶する処理を示す図である。

[図5]システムにデバイスを組み込む処理を示す図である。

[図6]実施形態に係るデバイス管理システムを示す図である。

[図7]デバイス管理システムが管理するデバイスを示す図である。

[図8]情報処理装置を示す図である。

[図9]デバイス管理システムが管理するデバイスを示す図である。

[図10]記憶部の一例である分散型台帳を示す図である。

[図11]分散型台帳の一例であるタングルを示す図である。

[図12]デバイスの製造時情報を記憶するデバイス管理システムを示す図である。

[図13]デバイスの製造時情報を記憶する処理を示す図である。

[図14]デバイスの起動時情報を記憶するデバイス管理システムを示す図である。

[図15]デバイスの起動時情報を記憶する処理を示す図である。

[図16]デバイスの更新時情報を記憶するデバイス管理システムを示す図である。

[図17]デバイスの起動時情報を記憶する処理を示す図である。

[図18]デバイスの更新時情報を所定時間ごとに記憶する処理を示す図である。

[図19]複数のトラスト情報を参照するデバイス管理システムを示す図である。

[図20]複数のトラスト情報を参照する処理を示す図である。

[図21]実施形態に係るデバイス管理システムを適用した実施例を示す図である。

[図22]実施形態に係るデバイス管理システムの適用した実施例を示す図である。

発明を実施するための形態

[0006] 図１は、実施形態に係るデバイス管理システムを示す図である。図１において、符号Ｄａ、Ｄｂ、及びＤｃは、それぞれ、管理対象のデバイスである

。デバイス管理システム１は、管理対象のデバイスの信頼性を評価することに利用される情報（適宜、トラスト情報という）を、記憶部ＤＬ１に記憶する。トラスト情報は、管理対象のデバイスの製造時情報、起動時情報、及び更新時情報の少なくとも１つを含む。デバイス管理システム１は、記憶部ＤＬ１、記憶部ＤＬ１と接続されるネットワーク３、ネットワーク３を介してトラスト情報を記憶部ＤＬ１に記憶させる情報処理装置（後述する）とを備える。

[0007] 管理対象のデバイスはデバイスごとに識別情報を有し、製造時情報、起動時情報、及び更新時情報は、それぞれ、デバイスの識別情報と関連付けられている。以下の説明において適宜、識別情報をＩＤと記載する。管理対象の第１のデバイスに対応する製造時情報は、第１のデバイスのＩＤを含み、第１のデバイスと異なる第２のデバイスに対応する製造時情報と区別できる。管理対象の第１のデバイスに対応する起動時情報は、第１のデバイスのＩＤを含み、第１のデバイスと異なる第２のデバイスに対応する起動時情報と区別できる。管理対象の第１のデバイスに対応する更新時情報は、第１のデバイスのＩＤを含み、第１のデバイスと異なる第２のデバイスに対応する更新時情報と区別できる。

[0008] 記憶部ＤＬ１は、例えば分散型台帳であるが、分散型台帳以外の形態の記憶部（例えば、集中型ストレージ）でもよい。以下の説明において適宜、記憶部ＤＬ１を分散型台帳ＤＬ１という。図１において、符号ＴＤは、分散型台帳を構成する端末である。端末ＴＤは、例えばコンピュータである。端末ＴＤは、例えば、CPUなどの処理部（プロセッサ）、RAMなどの揮発性メモリ、HDDあるいはSSDなどの不揮発性記憶装置、及びLAN等の所定の通信規格に準拠した通信部を備える。端末ＴＤは、ネットワーク３と接続される。

[0009] デバイス管理システム１は、トラスト情報を記憶部（例えば、分散型台帳ＤＬ１）から読み出す。デバイス管理システム１は、読み出したトラスト情報を用いて、管理対象のデバイスの信頼性を評価する。以下の説明において適宜、デバイスの信頼性を評価する処理を監査という。以下の説明において

適宜、信頼できると監査によって評価されたデバイスを「信頼できるデバイス」あるいは「トラステッドデバイス」という。デバイス管理システム１は、例えば、信頼できないと監査によって評価されたデバイスの利用を制限することによって、セキュアなシステムを提供する。

[0010] 図１において、符号ＦＡは、デバイスＤａを製造する工場である。デバイスＤａは、例えば複数の部品を含むコンピュータなどである。デバイスＤａは、例えば、単独で動作するデバイスである。デバイスＤａは、単独で動作するデバイスを構成する部品でもよい。デバイスＤａは、製造途中の未完成のデバイスでもよい。デバイスＤａは、完成品であって検査が予定されるデバイスでもよい。

[0011] 工場ＦＡは、制御装置ＦＡ１と、処理装置ＦＡ２とを備える。処理装置ＦＡ２は、デバイスＤａに処理を施すデバイスである。処理装置ＦＡ２は、例えば、製造過程のデバイスＤａに部品を実装するロボットを含む。処理装置ＦＡ２は、完成後のデバイスＤａを検査する検査装置を含んでもよい。工場ＦＡは、複数の処理装置を備えてもよい。図１には、１つの処理装置ＦＡ２が代表的に図示されている。

[0012] 制御装置ＦＡ１は、工場ＦＡの各部を制御する。制御装置ＦＡ１は、処理装置ＦＡ２を制御し、デバイスＤａに対する所定の処理を処理装置ＦＡ２に実行させる。制御装置ＦＡ１は、製造時情報を分散型台帳ＤＬ１に記憶させる情報処理装置の一例である。制御装置ＦＡ１は、処理装置ＦＡ２による処理対象のデバイスＤａのＩＤを特定する。例えば、デバイスＤａは、書き換え不能な記憶域を有し、この記憶域は、デバイスＤａのＩＤを記憶する。デバイスＤａのＩＤは、処理装置ＦＡ２によって、記憶域に書き込まれてもよい。

[0013] 制御装置ＦＡ１は、デバイスＤａに対して処理装置ＦＡ２による処理が完了した後、デバイスＤａの製造時情報を生成する。製造時情報は、例えば、デバイスの出荷前に生成される情報であり、デバイスの出荷後に更新されない情報である。出荷後のデバイスの状態を示す情報は、例えば、起動時情報

または更新時情報に含まれる。デバイスＤａの製造時情報は、例えば、デバイスＤａのＩＤと、デバイスＤａの製造に関係するデバイスの情報とを含む。デバイスＤａの製造に関係するデバイスは、例えば、デバイスＤａの部品、デバイスＤａに処理を施した処理装置ＦＡ２、及びデバイスＤａに対する処理を実行させた制御装置ＦＡ１を含む。デバイスＤａの製造に関係するデバイスの情報は、例えば、デバイスＤａの部品のＩＤ、処理装置ＦＡ２のＩＤ、及び制御装置ＦＡ１のＩＤを含む。制御装置ＦＡ１は、ネットワーク３を介して、分散型台帳ＤＬ１を構成する端末ＴＤと通信可能に接続される。制御装置ＦＡ１は、デバイスＤａの製造時情報を送信する。分散型台帳ＤＬ１を構成する端末ＴＤは、制御装置ＦＡ１が送信した製造時情報を記憶する。このように、第１の情報処理装置は、デバイスの製造に使用される製造装置、又は製造装置と通信可能に接続される装置を含み、デバイスの出荷前に生成される製造時情報を記憶部に記憶させてもよい。

[0014] ここで、図１のデバイス管理システム１の構成に基づき、製造時のトラスト情報である製造時情報を記憶する処理について説明する。図２は、製造時のトラスト情報を記憶する処理の例を示す図である。デバイス管理システム１の各部については、適宜、図１を参照する。ステップＳ１１において、工場ＦＡの制御装置ＦＡ１は、デバイスＤａに識別情報を割り付ける。ステップＳ１２において、処理装置ＦＡ２は、制御装置ＦＡ１に制御され、ステップＳ１１において割り付けた識別情報をデバイスＤａの記憶域に書き込む。ステップＳ１３において、制御装置ＦＡ１は、デバイスＤａに実装する部品の識別情報を取得する。ステップＳ１４において、処理装置ＦＡ２は、制御装置ＦＡ１に制御され、デバイスＤａに部品を実装する。ステップＳ１５において、制御装置ＦＡ１は、デバイスＤａの製造時情報を生成する。例えば、制御装置ＦＡ１は、ステップＳ１１で割り付けたデバイスＤａの識別情報と、ステップＳ１３で取得した部品の識別情報と、デバイスＤａの製造に関係するデバイス（例、制御装置ＦＡ１、処理装置ＦＡ２）の識別情報と、を一組にして製造時情報を生成する。ステップＳ１６において、制御装置ＦＡ

１は、製造時のトラスト情報である製造時情報を、記憶部ＤＬ１に記憶させる。このように、制御装置ＦＡ１は、例えば、デバイスの製造に関係する情報が発生した場合（例、部品が実装された場合）、この情報（例、実装された部品のＩＤ、部品を実装した処理装置のＩＤ、部品を実装した製造ラインのＩＤ）を、このデバイスのＩＤと関連付けて製造時情報を生成する。制御装置ＦＡ１は、例えば、デバイスの製造に関係する情報の発生を検知した場合、製造時情報を生成する。例えば、制御装置ＦＡ１は、検査を含む製造過程において、デバイスに対して変更（例、部品の実装、データの書き込み）を加える処理が実行された場合、デバイスの製造に関係する情報が発生したと検知（例、判定）する。制御装置ＦＡ１は、例えば、デバイスを製造または検査する処理を、予め定められた手順で処理装置に実行させ、この処理を実行させたことをトリガーとして、製造時情報を生成する。

[0015] 図１の説明に戻り、デバイスＤｂは、上位装置ＭＤによって制御されるデバイスである。デバイスＤｂは、例えばＩｏＴシステムにおけるエッジデバイスである。デバイスＤｂは、例えば、センサ、アクチュエータ、及びプロセッサの少なくとも１つを含む。デバイスＤｂは、ネットワーク３を介して、上位装置ＭＤと通信可能に接続される。上位装置ＭＤは、ネットワーク３を介してデバイスＤｂへ指令を送信する。デバイスＤｂは、上位装置ＭＤから送信された指令に規定された動作を実行する。デバイスＤｂは、連続的に動作するデバイスでもよいし、断続的に動作するデバイスでもよい。

[0016] ここでは、デバイスＤｂが断続的に動作するものとして説明する。デバイスＤｂは、所定の動作を行う第１モードと、第２モードよりも省電力な第２モードとを有する。デバイスＤｂは、第２モードで待機し、所定のトリガーによって第１モードに遷移する。第２モードから第１モードへの遷移は、例えばデバイスの起動に相当する。第１モードから第２モードへの遷移は、例えばデバイスのシャットダウンに相当する。

[0017] デバイスＤｂは、起動時情報を分散型台帳ＤＬ１に記憶させる情報処理装置の一例である。例えば、デバイスＤｂは、書き換え不能な記憶域と、処理

部とを備える。この記憶域は、処理部に所定の処理を実行させるプログラムを記憶する。デバイスＤｂの処理部は、記憶域に記憶されたプログラムに従って、デバイスＤｂの起動時にデバイスＤｂのデバイス構成をスキャンする。デバイス構成は、ハードウェア構成とソフトウェア構成との一方または双方を含む。デバイスＤｂは、例えば、今回のスキャン結果を前回のスキャン結果と比較し、今回のスキャン結果が前回のスキャン結果と異なる場合、起動時情報を生成する。例えば、デバイスＤｂの処理部は、書き換え不能な記憶域に記憶されたプログラムに従って、起動時情報を生成する処理を実行する。起動時情報は、例えば、ハードウェア構成に変更があった場合、追加または削除された部品のＩＤを含む。起動時情報は、例えば、ソフトウェア構成に変更があった場合、変更に使われたファイルを特定する情報（例、ハッシュ値）を含む。

[0018] デバイスＤｂは、生成した起動時情報を、ネットワークを介して送信する。例えば、デバイスＤｂの処理部は、書き換え不能な記憶域に記憶されたプログラムに従って、起動時情報を送信する。分散型台帳ＤＬ１を構成する端末ＴＤは、デバイスＤｂが送信した起動時情報を記憶する。デバイスＤｂは、起動時情報を端末ＴＤへ送信してもよいし、起動時情報を上位装置ＭＤへ送信してもよい。上位装置ＭＤは、デバイスＤｂが送信した起動時情報を受信し、この起動時情報を端末ＴＤに記憶させてもよい。このように、第１の情報処理装置は、管理対象のデバイスを含み、自装置を起動する際に起動時情報を生成し、生成した起動時情報を記憶部に記憶させてもよい。なお、デバイスＤｂは、起動時情報を生成しなくてもよい。例えば、上位装置ＭＤは、デバイスＤｂにデバイス構成のスキャンを実行させ、スキャン結果に基づいてデバイスＤｂの起動時情報を生成してもよい。例えば、上位装置ＭＤは、書き換え不能な記憶域を備え、この記憶域に記憶されたプログラムに従って、起動時情報を生成する。例えば、上位装置ＭＤは、書き換え不能な記憶域に記憶されたプログラムに従って、起動時情報を外部の記憶部（例、分散型台帳のノードの端末における記憶部）に記憶させる。

[0019] 上位装置ＭＤは、更新時情報を分散型台帳ＤＬ１に記憶させる情報処理装置の一例である。例えば、上位装置ＭＤは、制御対象であるデバイスＤｂが記憶するプログラム（例えば、ファームウェア）を更新する。例えば、上位装置ＭＤは、デバイスＤｂにプログラムの更新を実行させる更新プログラムを含むファイルを送信する。デバイスＤｂは、受信した更新プログラムに従って、更新処理を実行する。デバイスＤｂは、更新処理が完了した後に、上位装置ＭＤに対して更新処理の完了を通知する。上位装置ＭＤは、更新処理の完了の通知を受けて、更新時情報を生成する。更新時情報は、例えば、デバイスＤｂのＩＤと、更新に使われたファイルと特定する情報（例、ハッシュ値）を含む。例えば、上位装置ＭＤは、書き換え不能な記憶域を備え、この記憶域に記憶されたプログラムに従って、更新時情報を生成する。なお、上位装置ＭＤは、デバイスＤｂにおいて更新処理が実行される前に、又は更新処理と並行して、更新時情報を生成してもよい。例えば、上位装置ＭＤは、デバイスＤｂに更新処理を実行させるスケジュールが登録された段階で、更新プログラムを含むファイルを特定する情報とデバイスＤｂのＩＤとを含む更新時情報を生成してもよい。上位装置ＭＤは、生成した更新時情報を、ネットワーク３を介して送信する。分散型台帳ＤＬ１を構成する端末ＴＤは、上位装置ＭＤが送信した更新時情報を記憶する。例えば、上位装置ＭＤは、書き換え不能な記憶域に記憶されたプログラムに従って、更新時情報を外部の記憶部（例、分散型台帳のノードの端末における記憶部）に記憶させる。このように、第１の情報処理装置は、管理対象のデバイスを制御する上位装置を含み、管理対象のデバイスから取得される情報に基づいて、起動時情報と更新時情報との一方又は双方を記憶部に記憶させてもよい。

[0020] なお、更新時情報は、デバイスＤｂによって生成されてもよい。例えば、デバイスＤｂの処理部は、書き換え不能な記憶域に記憶されたプログラムに従って、更新時情報を生成してもよい。デバイスＤｂの処理部は、更新処理を実行する前に、更新時情報を生成してもよい。例えば、デバイスＤｂは、更新プログラムを含むファイルを受信した後、更新処理の開始前に、このフ

ァイル特定する情報とデバイスＤｂのＩＤとを含む更新時情報を生成してもよい。更新プログラムの送信元は、上位装置ＭＤでもよいし、上位装置ＭＤと異なる装置でもよい。デバイスＤｂは、更新時情報を生成した場合、生成した更新時情報を端末ＴＤに記憶させてもよい。例えば、デバイスＤｂの処理部は、書き換え不能な記憶域に記憶されたプログラムに従って、更新時情報を端末ＴＤに記憶させてもよい。デバイスＤｂの処理部は、例えば、更新処理を開始する前に、更新時情報を端末ＴＤに記憶させてもよい。このように、第１の情報処理装置は、管理対象のデバイスを含み、自装置を更新する際に更新時情報を生成し、生成した更新時情報を記憶部に記憶させてもよい。また、デバイスＤｂは、生成した更新時情報を上位装置ＭＤへ送信し、上位装置ＭＤは、受信した更新時情報を端末ＴＤに記憶させてもよい。例えば、デバイスＤｂの処理部は、書き換え不能な記憶域に記憶されたプログラムに従って、更新時情報を送信してもよい。デバイスＤｂの処理部は、例えば、更新処理を開始する前に、更新時情報を送信してもよい。上述の各プログラムは、書き換え可能な記憶域に記憶されてもよい。デバイスのＩＤは、書き換え可能な記憶域に記憶されてもよい。デバイスは、処理部を含むデバイス本体と、デバイス本体に外付けされる記憶域とを備えてもよい。この記憶域は、例えば、外部から電磁波を受けて電磁誘電により発電し、その電力によって電気信号を出力（例、送信）する回路（例、ＲＦタグ、ＮＦＣタグ）の一部でもよい。例えば、デバイス本体の外部にＲＦタグが接合され、このＲＦタグは、デバイスのＩＤを含む電気信号を送信してもよい。ＲＦタグとデバイス本体とを接合する力は、上記回路が破壊する力よりも強くてもよい。例えば、悪意があるユーザが、デバイス本体からＲＦタグを外そうとした場合、その力によって上記回路が破壊されてデバイスのＩＤが利用不能になり、デバイスのＩＤが悪用されることが回避される。ここで、ＲＦタグが設けられたデバイスが部品であるとする。この部品が実装されたデバイスは、例えば、ＲＦリーダを備え、部品から送信されるＩＤをＲＦリーダにより取得することで、自装置のハードウェア構成の少なくとも一部を検出してもよ

い。このデバイスが動作する際に電力を供給する電源は、上記ＲＦリーダに電力を供給してもよい。上記ＲＦリーダを含むデバイスは、外部装置（例、上位装置ＭＤ）に対して、部品から取得したＩＤを送信してもよい。

[0021] ここで、図１のデバイス管理システム１の構成に基づき、起動時のトラスト情報である起動時情報、又は更新時のトラスト情報である更新時情報を記憶する処理の例について説明する。図３は、起動時または更新時のトラスト情報を記憶する処理を示す図である。デバイス管理システム１の各部については、適宜、図１を参照する。ステップＳ２１において、デバイスＤｂの処理部は、デバイスＤｂのデバイス構成をスキャンする。ステップＳ２２において、デバイスＤｂの処理部は、構成の変更があるか否かを判定する。デバイスＤｂの処理部は、例えば、今回のスキャン結果が前回のスキャン結果と異なる場合、構成の変更があると判定する（ステップＳ２２；Ｙｅｓ）。デバイスＤｂの処理部は、構成の変更があると判定した場合（ステップＳ２２；Ｙｅｓ）、ステップＳ２３においてトラスト情報を生成する。ステップＳ２１の処理がデバイスＤｂの起動時に実行された場合、デバイスＤｂの処理部は、ステップＳ２３において、トラスト情報として起動時情報を生成する。ステップＳ２１の処理がデバイスＤｂの更新時に実行された場合、デバイスＤｂの処理部は、ステップＳ２３において、トラスト情報として更新時情報を生成する。デバイスＤｂの処理部は、例えば、デバイスＤｂのＩＤと、変更により追加または削除されたハードウェア要素（例、部品）がある場合にそのＩＤと、ソフトフェア構成が変更された場合に変更に使用されたファイルを特定する情報と、を一組にして、トラスト情報を生成する。デバイスＤｂの処理部は、ステップＳ２３で生成したトラスト情報を、ステップＳ２４において記憶部ＤＬ１に記憶させる。なお、ステップＳ２１からステップＳ２４の処理の少なくとも一部は、デバイスＤｂと異なるデバイス（例、上位装置ＭＤ）によって実行されてもよい。

[0022] 図１の説明に戻り、本実施形態において、デバイス管理システム１は、監査装置ＣＤと、記憶部ＤＬ２とを備える。監査装置ＣＤは、トラスト情報を

記憶部に記憶させる情報処理装置の一例である。監査装置ＣＤは、分散型台帳ＤＬ１に記憶されたトラスト情報を用いて監査を実行し、監査結果を示すトラスト情報を生成する。以下の説明において適宜、監査結果を示すトラスト情報を監査時のトラスト情報という。監査時のトラスト情報は、例えば、管理対象のデバイスが信頼できるか否かを示す情報（例、フラグ）と、デバイスのＩＤとを関連付けた情報（例、ホワイトリスト）である。監査装置ＣＤは、生成したトラスト情報を、分散型台帳ＤＬ１と異なる記憶部ＤＬ２に記憶させる。記憶部ＤＬ２は、例えば分散型台帳であるが、分散型台帳以外の形態の記憶部（例えば、集中型ストレージ）でもよい。以下の説明において適宜、記憶部ＤＬ２を分散型台帳ＤＬ２という。なお、監査時のトラスト情報の記憶先は、製造時情報、起動時情報、及び更新時情報の少なくとも一部の記憶先と同じでもよい。

[0023] ここで、図１のデバイス管理システム１の構成に基づき、監査時のトラスト情報を記憶する処理について説明する。図４は、監査時のトラスト情報を記憶する処理を示す図である。デバイス管理システム１の各部については、適宜、図１を参照する。

[0024] ステップＳ３１において、監査装置ＣＤは、監査対象のデイバスのＩＤを特定する。ここでは、監査対象のデバイスは、工場ＦＡで製造されたデバイスＤａであるとする。監査装置ＣＤは、例えば、監査対象のデバイスＤａの記憶域から読み取られたＩＤをデバイスＤａから取得することによって、デバイスＤａのＩＤを特定する。監査装置ＣＤは、その他の手法で、デバイスＤａのＩＤを特定してもよい。例えば、監査装置ＣＤは、デバイスＤａと接続されたデバイスからデバイスＤａのＩＤを指定されることによって、デバイスＤａのＩＤを特定してもよい。

[0025] ステップＳ３２において、監査装置ＣＤは、監査対象のデバイスのトラスト情報を取得する。例えば、監査装置ＣＤは、ステップＳ３１で特定したＩＤを含むトラスト情報を、分散型台帳ＤＬ１に記憶されたトラスト情報において検索することで、デバイスＤａのトラスト情報を取得する。監査装置Ｃ

Ｄは、デバイスＤａのトラスト情報として、デバイスＤａの製造時情報を取得する。

[0026] ステップＳ３３において、監査装置ＣＤは、監査対象のデバイスＤａに関係するデバイス（適宜、関係デバイスという）の識別情報を特定する。例えば、ステップＳ３２においてデバイスＤａの製造時情報が取得された場合、製造時情報にはデバイスＤａに関係デバイスのＩＤとして、工場ＦＡの制御装置ＦＡ１のＩＤ、処理装置ＦＡ２のＩＤ、デバイスＤａの部品であるデバイスのＩＤが含まれる。監査装置ＣＤは、製造時情報を参照することによって、関係デバイスのＩＤを特定する。

[0027] ステップＳ３３において、監査装置ＣＤは、ステップＳ３４において、関係デバイスのトラスト情報を取得する。ここでは、関係デバイスは、工場ＦＡの制御装置ＦＡ１、処理装置ＦＡ２、デバイスＤａの部品であるものとし、監査装置ＣＤは、これらデバイスについて監査済であるものとする。ステップＳ３４において、監査装置ＣＤは、ステップＳ３３で特定した制御装置ＦＡ１のＩＤを用いて、分散型台帳ＤＬ２から制御装置ＦＡ１の監査時のトラスト情報を取得する。

[0028] ステップＳ３５において、監査装置ＣＤは、関係デバイスとして、ステップＳ３３においてＩＤを特定したデバイスの１つ（例、制御装置ＦＡ１）を選択し、このデバイスが信頼できるか否かを判定する。例えば、監査装置ＣＤは、ステップＳ３４で取得した制御装置ＦＡ１の監査時のトラスト情報を参照して、制御装置ＦＡ１が信頼できるか否かを判定する。監査装置ＣＤは、監査時のトラスト情報において制御装置ＦＡ１が信頼できるデバイスである旨の情報が含まれる場合、又は監査時のトラスト情報において制御装置ＦＡ１が信頼できないデバイスである旨の情報が含まれない場合、このデバイスは信頼できると判定する（ステップＳ３５；Ｙｅｓ）。監査装置ＣＤは、関係デバイスについてのトラスト情報が存在しない場合、監査時のトラスト情報において制御装置ＦＡ１が信頼できないデバイスである旨の情報が含まれる場合、又は監査時のトラスト情報において制御装置ＦＡ１が信頼できる

デバイスである旨の情報が含まれない場合、このデバイスは信頼できないと判定する（ステップＳ３５；Ｎｏ）。

[0029] 監査装置ＣＤは、関係デバイス（例、制御装置ＦＡ１）が信頼できると判定した場合（ステップＳ３５；Ｙｅｓ）、ステップＳ３６において、関係デバイスが他にあるか否かを判定する。監査装置ＣＤは、ステップＳ３３においてＩＤを特定したデバイスの少なくとも１つについて、ステップＳ３５の処理を実行していない場合、関係デバイスが他にあると判定する（ステップＳ３６；Ｙｅｓ）。監査装置ＣＤは、関係デバイスが他にあると判定した場合（ステップＳ３６；Ｙｅｓ）、ステップＳ３４に戻り、ステップＳ３３においてＩＤを特定した次のデバイス（例、処理装置ＦＡ２）を選択し、このデバイスが信頼できるか否かを判定する。

[0030] 監査装置ＣＤは、関係デバイスのそれぞれについて信頼できると判定し、かつ関係デバイスが他にないと判定した場合（ステップＳ３６；Ｎｏ）、ステップＳ３７において、監査時のトラスト情報として監査対象のデバイスＤａが信頼できることを記憶させる。例えば、監査装置ＣＤは、監査対象のデバイスＤａのＩＤと、デバイスＤａが信頼できることを示す情報（例、フラグ）とを一組にすることで、監査時のトラスト情報を生成する。監査装置ＣＤは、生成した監査時のトラスト情報を、分散型台帳ＤＬ２に記憶させる。

[0031] 監査装置ＣＤは、関係デバイスの少なくとも１つについて、関係デバイスが信頼できないと判定した場合（ステップＳ３５；Ｎｏ）、監査対象のデバイスＤａが信頼できる旨の情報を記憶させることなく、一連の処理を終了する。なお、監査装置ＣＤは、関係デバイスの少なくとも１つについて、関係デバイスが信頼できないと判定した場合（ステップＳ３５；Ｎｏ）、監査対象のデバイスＤａが信頼できない旨の情報（例、ブラックリスト）を生成し、この情報を記憶部（例、分散型台帳ＤＬ２）に記憶させてもよい。

[0032] 次に、監査対象のデバイスについて、起動時情報または更新時情報が存在する場合の監査について説明する。ここでは、監査対象のデバイスがデバイスＤｂであり、上位装置ＭＤによってデバイスＤｂが更新されて更新時情報

が存在するものとする。ステップＳ３１において、監査装置ＣＤは、監査対象のデバイスＤｂのＩＤを特定する。監査装置ＣＤは、デバイスＤｂの記憶域からＩＤを読み取ってもよいし、デバイスＤｂを制御する上位装置ＭＤからデバイスＤｂのＩＤを取得してもよい。ステップＳ３２において、監査装置ＣＤは、監査対象のデバイスＤｂのトラスト情報として、更新時情報を取得する。ステップＳ３３において、監査装置ＣＤは、監査対象のデバイスＤｂに関係する関係デバイスの識別情報を特定する。更新時情報には、関係デバイスのＩＤとして、デバイスＤｂの更新に関係する上位装置ＭＤのＩＤが含まれる。また、監査対象のデバイスＤｂは、関係デバイスの一つである。

[0033] ステップＳ３４において、監査装置ＣＤは、関係デバイスのトラスト情報を取得する。例えば、監査装置ＣＤは、関係デバイスの１つとしてデバイスＤｂを選択し、デバイスＤｂに対して今回の更新前であって、デバイスＤｂに対して前回の更新がなされた場合にそれ以降のデバイスＤｂのトラスト情報を取得する。ここでは、デバイスＤｂに対して前回の更新がなされており、その後に監査装置ＣＤがデバイスＤｂに対して監査済であるとする。監査装置Ｓ３４は、ステップＳ３１で特定したデバイスＤｂのＩＤを用いて、分散型台帳ＤＬ２からデバイスＤｂの前回の監査時のトラスト情報を検索し、デバイスＤｂの前回の監査時のトラスト情報を取得する。

[0034] ステップＳ３５において、監査装置ＣＤは、デバイスＤｂの前回の監査時のトラスト情報を用いて、関係デバイス（例、今回の更新前のデバイスＤｂ）が信頼できるか否かを判定する。監査装置ＣＤは、今回の更新前のデバイスＤｂが信頼できると判定した場合（ステップＳ３５；Ｙｅｓ）、ステップＳ３６において関係デバイスが他にあるか否かを判定する。ここでは、関係デバイスとしてデバイスＤｂの他に上位装置ＭＤが存在するため、監査装置ＣＤは、関係デバイスが他にあると判定する（ステップＳ３６；Ｙｅｓ）。監査装置ＣＤは、関係デバイスが他にあると判定した場合（ステップＳ３６；Ｙｅｓ）、ステップＳ３４に戻り、次の関係デバイスとして上位装置ＭＤのトラスト情報を取得する。監査装置ＣＤは、ステップＳ３５において、関

係デバイス（例、上位装置ＭＤ）が信頼できるか否かを判定する。監査装置ＣＤは、関係デバイスの全てが信頼できると判定し、かつ監査対象のデバイスＤｂの更新に使われたファイルが信頼できると判定した場合、更新後のデバイスＤｂが信頼できると判定する。そして、監査装置ＣＤは、更新後のデバイスＤｂについて、今回の監査時のトラスト情報として監査対象のデバイスＤｂが信頼できることを示す情報を記憶部（例、分散型台帳ＤＬ２）に記憶させる。

[0035] なお、監査装置ＣＤは、第１の監査対象のデバイスと、関係デバイスとの少なくとも１つについて前回の監査時のトラスト情報が存在しない場合、前回の監査時のトラスト情報が存在しないデバイスを第２の監査対象のデバイスに設定する。そして、監査装置ＣＤは、第２の監査対象のデバイスの関係デバイスの各々について、製造時情報と起動時情報と更新時情報とのうち存在する情報に基づいて、関係デバイスが信頼できるか否かを判定する。そして、監査装置ＣＤは、関係デバイスの全てが信頼できると判定した場合、第２の監査対象のデバイスが信頼できる判定する。監査装置ＣＤは、このような処理を繰り返すことによって監査時のトラスト情報を補完し、第１の監査対象のデバイスに対する監査を実行する。

[0036] 図１の説明に戻り、デバイスＤｃは、上位装置ＭＤを含むシステム（例、ＩｏＴシステム）に組み込みが予定されたデバイスである。上位装置ＭＤは、例えば、デバイスＤｃの信頼性を確認した上で、デバイスＤｃをシステムに組み込む処理を実行する。ここで、図１のデバイス管理システム１の構成に基づき、システムにデバイスを組み込む処理について説明する。図５は、システムにデバイスを組み込む処理を示す図である。デバイス管理システム１の各部については、適宜、図１を参照する。

[0037] ステップＳ４１において、上位装置ＭＤは、システムに組込対象のデバイスＤｃのＩＤを特定する。例えば、上位装置ＭＤは、デバイスＤｃの記憶域からＩＤを読み取ることによって、デバイスＤｃのＩＤを特定する。ステップＳ４２において、上位装置ＭＤは、組込対象のデバイスＤｃのトラスト情

報を取得する。上位装置ＭＤは、ステップＳ４１で特定したＩＤを用いて、分散型台帳ＤＬ２においてデバイスＤｃの監査時のトラスト情報を検索する。デバイスＤｃの監査時のトラスト情報が分散型台帳ＤＬ２に記憶されている場合、上位装置ＭＤは、デバイスＤｃの監査時のトラスト情報を分散型台帳ＤＬ２から取得する。また、デバイスＤｃの監査時のトラスト情報が分散型台帳ＤＬ２に記憶されていない場合、上位装置ＭＤは、ステップＳ４１で特定したＩＤを用いて、デバイスＤｃの製造時情報と起動時情報と更新時情報とのうち分散型台帳ＤＬ１に記憶されているトラスト情報を検索する。デバイスＤｃのトラスト情報が分散型台帳ＤＬ１に記憶されている場合、上位装置ＭＤは、デバイスＤｃのトラスト情報を分散型台帳ＤＬ１から取得する。

[0038] 上位装置ＭＤは、ステップＳ４３において、ステップＳ４２で取得したトラスト情報を用いて、組込対象のデバイスＤｃが信頼できるか否かを判定する。例えば、上位装置ＭＤは、ステップＳ４２において監査時のトラスト情報を取得した場合、監査時のトラスト情報に基づいてデバイスＤｃが信頼できるか否かを判定する。上位装置ＭＤは、監査時のトラスト情報にデバイスＤｃが信頼できる旨の情報が含まれる場合、または監査時のトラスト情報にデバイスＤｃが信頼できない旨の情報が含まれない場合、デバイスＤｃが信頼できると判定する（ステップＳ４３；Ｙｅｓ）。上位装置ＭＤは、ステップＳ４２においてトラスト情報として製造時情報、起動時情報、及び更新時情報のうち存在する情報を取得した場合、図４で説明した監査装置ＣＤと同様の処理によって、デバイスＤｃついて監査を実行する。なお、デバイスＤｃの監査時のトラスト情報が存在しない場合、上位装置ＭＤは、監査装置ＣＤに対してデバイスＤｃについての監査の実行を要求し、その監査結果を用いて、ステップＳ４３の処理を実行してもよい。

[0039] 上位装置ＭＤは、組込対象のデバイスＤｃが信頼できると判定した場合（ステップＳ４３；Ｙｅｓ）、ステップＳ４４において、デイバスＤｃをシステムに組み込む処理を実行する。上位装置ＭＤは、組込対象のデバイスＤｃ

が信頼できないと判定した場合（ステップＳ４３；Ｎｏ）、デイバスＤｃをシステムに組み込む処理を実行せずに、一連の処理を終了する。このように、実施形態に係るデバイス管理システムは、複数のデバイスを含むシステムを管理する管理装置（例、上位装置）を備え、管理装置は、管理対象のデバイスが信頼できるか否かを第２の情報処理装置が判定した結果に基づいて、管理対象のデバイスをシステムに組み込むか否かを判定してもよい。

[0040] 本実施形態のデバイス管理システム１は、例えば、第１のデバイスに関係する第２のデバイスの信頼性を示す情報を記憶部に記憶する。したがって、デバイス管理システム１は、第２のデバイスの信頼性に基づいて、第１のデバイスの信頼性を評価できる。例えば、デバイス管理システム１は、第１のデバイスの変更に関係する全ての関係デバイスが信頼できると判定した場合、第１のデバイスも信頼できると判定する。この場合、デバイス管理システム１は、複数のデバイスの信頼性を連鎖的に評価することができる。デバイス管理システム１は、信頼性が評価されたデバイスの数が増えることにより、例えばセキュアなシステムを容易に構築することに寄与する。

[0041] 本実施形態に係るデバイス管理システム１は、トラスト情報を記憶させる第１の情報処理装置と、トラスト情報を読み出してデバイスの信頼性を判定する第２の情報処理装置との一方または双方を含む。デバイス管理システム１は、上記第１の情報処理装置または上記第２の情報処理装置を含まなくてもよい。例えば、デバイス管理システム１は、トラスト情報を記憶させる第１の情報処理装置を含み、トラスト情報を読み出してデバイスの信頼性を判定する第２の情報処理装置は、デバイス管理システム１の外部の装置であって、デバイス管理システム１が提供する情報を利用する装置であってもよい。また、デバイス管理システム１は、トラスト情報を読み出してデバイスの信頼性を判定する第２の情報処理装置を含み、トラスト情報を記憶させる第１の情報処理装置は、デバイス管理システム１の外部の装置であって、デバイス管理システム１へ情報を提供する装置であってもよい。

[0042] また、デバイス管理システム１は、上記第１の情報処理装置と、上記第２

の情報処理装置とのいずれとも異なる装置を含まなくてもよい。例えば、デバイス管理システム１は、記憶部ＤＬ１と記憶部ＤＬ２との一方または双方を備えなくてもよい。記憶部ＤＬ１と記憶部ＤＬ２との一方または双方は、デバイス管理システム１の外部の装置であって、デバイス管理システム１へ情報を提供する装置であってもよい。

[0043] また、デバイス管理システム１は、監査装置ＣＤを含まなくてもよい。例えば、デバイス管理システム１は、監査時のトラスト情報を生成しなくてもよく、この場合、記憶部ＤＬ２が設けられなくてもよい。デバイス管理システム１は、監査装置ＣＤを含まない場合であっても、製造時情報と起動時情報と更新時情報とのうち存在するトラスト情報を用いて、デバイスが信頼できるか否かを判定することができる。例えば、デバイス管理システム１は、製造時情報と起動時情報と更新時情報とのうち所定の情報が不足する場合、デバイスが信頼できないと判定し、その他の場合にデバイスが信頼できると判定してもよい。ここで、製造時情報は、管理対象のデバイスの部品の情報を含むとする。第２の情報処理装置は、製造時情報を用いて管理対象のデバイスの信頼性を確認（例、評価、判定）する場合、例えば、管理対象のデバイスについての製造時情報を記憶部から取得し、製造時情報に含まれる部品の情報を用いて、各部品が信頼できるか否かを判定する。例えば、第２の情報処理装置は、部品のＩＤが所定の条件を満たす場合、この部品が信頼できると判定する。所定の条件は、例えば、信頼できる部品のＩＤを登録したデータベースに、管理対象の部品のＩＤが含まれることを含む。上記データベースは、例えば、デバイスが所定の規格を満たすか否かを検査する検査機関が、規格を満たすデバイスのＩＤを登録するデータベース等でもよい。第２の情報処理装置は、例えば、製造時情報に含まれる部品のＩＤの全てが所定の条件を満たす場合、管理対象のデバイスが信頼できると判定する。第２の情報処理装置は、製造時情報に含まれる部品のＩＤのうち少なくとも１つが所定の条件を満たさない場合、管理対象のデバイスが信頼できないと判定してもよい。第２の情報処理装置は、製造時情報に含まれる部品のＩＤのうち

少なくとも１つが所定の条件を満たさない場合、所定の条件を満たさないＩＤに対応する部品について、信頼できるか否かを外部に問い合わせてもよい。例えば、第２の処理装置は、所定の条件を満たさないＩＤに対応する部品について、管理対象のデバイスの所有者または利用者から、この部品が信頼できるか否かを示す入力を受け付けてもよい。第２の情報処理装置は、所定の条件を満たさないＩＤに対応する部品について、信頼できることを示す入力が管理対象のデバイスの所有者または利用者からあった場合、管理対象のデバイスを信頼できると判定してもよい。

[0044] また、上位装置ＭＤは、起動時情報と更新時情報との一方または双方に基づいて、デバイスＤｂが信頼できるか否かを判定してもよい。例えば、上位装置ＭＤは、デバイスＤｂのソフトウェアを更新する処理をデバイスＤｂに実行させ、デバイスＤｂは、起動時情報と更新時情報との一方または双方を生成するものとする。上位装置ＭＤは、デバイスＤｂがソフトウェアを更新する際にデバイスＤｂに提供するソフトウェアから想定されるハッシュ値と、デバイスＤｂが生成した起動時情報あるいは更新時情報に含まれるハッシュ値とを比較する。上位装置ＭＤは、デバイスＤｂが生成した起動時情報あるいは更新時情報に含まれるハッシュ値が想定値と異なる場合、デバイスＤｂが信頼できないと判定してもよい。上位装置ＭＤは、信頼できないと判定したデバイスＤｂの機能を制限してもよい。例えば、上位装置ＭＤは、デバイスＤｂが出力する情報を利用しない、デバイスＤｂの少なくとも一部の機能を停止させる、デバイスＤｂをネットワークから遮断する等の処理の少なくとも１つを実行してもよい。このように、実施形態に係るデバイス管理システムは、第２の情報処理装置が管理対象のデバイスの信頼性を判定した結果を用いて、管理対象のデバイスを制御する制御部（例、上位装置）を備えてもよい。ここで、更新時情報は、デバイスの更新処理に使われる更新プログラムのファイルを特定する情報と、このファイルのハッシュ値とを含むとする。正規の更新プログラムのファイルを特定する情報と、このファイルのハッシュ値とが関連付けられた情報は、データベースに予め登録されてもよ

い。正規の更新プログラムは、例えば、公的機関によって認証された提供者から提供されるプログラムである。第２の情報処理装置は、管理対象のデバイスについての更新時情報に含まれ、更新処理に使われる更新プログラムのファイルを特定する情報と、このファイルのハッシュ値とを関連付けられた情報が上記データベースに登録されている場合、管理対象のデバイスで実行された更新処理が正規の処理であると判定してもよい。第２の情報処理装置は、更新処理前の管理対象のデバイスが信頼できると判定され、かつこの更新処理が正規の処理であると判定された場合、更新処理後の管理対象のデバイスが信頼できると判定してもよい。

[0045] 上述の実施形態において、上記第１の情報処理装置は、例えばコンピュータシステムを含む。第１の情報処理装置は、記憶部と処理部とを備え、記憶部に記憶されているプログラムを読み出し、このプログラムに従って処理部が各種の処理を実行する。また、上記第２の情報処理装置は、例えばコンピュータシステムを含む。第２の情報処理装置は、記憶部と処理部とを備え、記憶部に記憶されているプログラムを読み出し、このプログラムに従って処理部が各種の処理を実行する。

[0046] 図６は、実施形態に係るデバイス管理システムを示す図である。デバイス管理システム１は、複数の情報処理装置２と、ネットワーク３とを備える。複数の情報処理装置２は、それぞれ、複数の情報処理装置２のうち自装置以外の情報処理装置２と、ネットワーク３を介して接続される。ネットワーク３は、例えばＰ２Ｐ（ピア・ツー・ピア）型ネットワークである。ネットワーク３は、有線のネットワークであってもよいし、無線のネットワークであってもよい。ネットワーク３は、例えばインターネット網である。デバイス管理システム１は、分散型台帳技術（Ｄｉｓｔｒｉｂｕｔｅｄ Ｌｅｄｇｅｒ Ｔｅｃｈｎｏｌｏｇｙ）を利用する。複数の情報処理装置２のそれぞれは、分散型台帳技術におけるノードを構成する。本実施形態のデバイス管理システム１は、ＩＯＴＡ（アイオータ）のＴａｎｇｌｅ（タングル）を分散型台帳として用いるが、他の分散型台帳を用いてもよい。例えば、分散型台

帳として、Ｅｔｈｅｒｅｕｍ（イーサリアム（登録商標））のブロックチェーンを用いてもよい。

[0047] 図７は、デバイス管理システムが管理するデバイスを示す図である。デバイス管理システム１はＩｏＴデバイス５の管理を行う。ＩｏＴデバイス５は、ネットワーク４によって情報処理装置２と接続される。情報処理装置２は、ＩｏＴデバイス５の動作制御を行う。ネットワーク４は、有線のネットワークであってもよいし、無線のネットワークであってもよい。ネットワーク４は、例えばインターネット網である。ＩｏＴデバイス５は、温度、湿度、圧力、光量、音量などの自然現象や、物体の向きや位置の移動速度及びその加速度などの、既知の変動量を検出する如何なるセンサーであってもよい。また、ＩｏＴデバイス５は、周囲を撮影可能なカメラであってもよい。また、ＩｏＴデバイス５は、エアコンなどの家電製品、自動車、ロボットなど如何なる製品であってもよい。本実施形態のデバイス管理システム１は、管理するデバイスがＩｏＴデバイスであるとするが、ネットワークで接続されないデバイスを管理するものであってもよい。ＩｏＴデバイス５は、分散型台帳技術におけるノードを構成するデバイスであってもよい。

[0048] 図８は、情報処理装置を示す図である。情報処理装置２は、一般にパソコンと呼ばれる装置であってもよく、ワークステーション、メインフレーム、或いはスーパーコンピュータと呼ばれる装置であってもよい。また、情報処理装置２は、スマートフォンやタブレットと呼ばれる装置であってもよい。また、情報処理装置２は、コンピュータの機能のほかに、センサー機能やカメラ機能といったそのデバイス特有の機能を有する各種デバイスであってもよい。ここでは、情報処理装置２の一例としての端末装置１１の構成について説明する。端末装置１１は、各種の処理を行う処理部１２と、操作者に対する入出力を行う入出力部１３と、処理部１２で動作するプログラムや各種のデータを記憶する記憶部１４と、ネットワーク３及びネットワーク４を介した通信を行う通信部１５と、を有して構成される。なお、端末装置１１は、本実施形態のデバイス管理システム１で管理されるデバイスであってもよ

い。インターネットに接続可能なすべての装置は、本実施形態のデバイス管理システム１による管理対象のＩｏＴデバイスである。

[0049] 処理部１２は、ＣＰＵやＭＰＵと呼ばれる演算装置である。処理部１２は、記憶部１４に記憶されたプログラムを実行する。入出力部１３は、キーボード、マウス、ディスプレイといった入出力装置である。記憶部１４は、ＲＡＭやＲＯＭ、ハードディスク、さらに磁気的記憶装置、光学的記憶装置など、既知のいかなる記憶装置であってもよい。複数の情報処理装置２のそれぞれは、すべて同じ構成であってもよいし、装置ごとに、他の装置と異なる構成を有するものであってもよい。

[0050] 図９は、デバイス管理システムが管理するデバイスを示す図である。デバイス１６は、各種の処理を行う処理部１７と、そのデバイス特有の機能を実行するデバイス機能実行部１８と、処理部１７で動作するプログラムや各種のデータを記憶する記憶部１９と、ネットワーク４を介した通信を行う通信部２０と、を有して構成される。処理部１７は、ＣＰＵやＭＰＵと呼ばれる演算装置である。処理部１７は、記憶部１９に記憶されたプログラムを実行する。記憶部１４は、ＲＡＭやＲＯＭ、ハードディスク、さらに磁気的記憶装置、光学的記憶装置など、既知のいかなる記憶装置であってもよい。複数の情報処理装置２のそれぞれは、すべて同じ構成であってもよいし、装置ごとに、他の装置と異なる構成を有するものであってもよい。

[0051] デバイス機能実行部１８は、そのデバイス特有の機能を実行する構成である。デバイス１６がセンサーである場合には、デバイス機能実行部１８は、対象の検知を行う検知素子、及び検知素子を制御する制御部などを有する。デバイス１６がカメラである場合には、デバイス機能実行部１８は、周囲を撮像する撮像素子、撮像素子で得た撮像画像に対して画像処理を施す画像処理部、及び撮像素子や画像処理部を制御する制御部などを有する。デバイス１６がエアコンである場合には、デバイス機能実行部１８は、冷凍サイクルに係る各構成を駆動する駆動部、温度や湿度を検知する検知部、及び駆動部や検知部を制御する制御部などを有する。デバイス１６が自動車である場合

には、デバイス機能実行部１８は、自動車の走行に係る各構成を駆動する駆動部、車外の安全性に関する状況や車内の快適性に関する状況などを検知する検知部、及び駆動部や検知部を制御する制御部などを有する。デバイス１６がロボットである場合には、デバイス機能実行部１８は、ロボットを駆動する駆動部、ロボットの周囲状況を検知する検知部、及び駆動部や検知部を制御する制御部などを有する。デバイス１６がロボットである場合は、このロボットによって、本実施形態のデバイス管理システム１による管理対象のＩｏＴデバイスを製造してもよい。このようにすることによって、より信頼性の高いＩｏＴデバイスを製造することができる。

[0052] 図１０は、記憶部の一例である分散型台帳を示す図である。本実施形態のデバイス管理システム１では、ノードとして、分散型台帳の一例であるタングルを有するフルノードと、タングルを有しないライトウォレットと、を有する。フルノードは自身が有するタングルと、他のフルノードが有するタングルとを同期させる。ライトウォレットは、ライトノードとも呼ばれる。ここでは、ライトウォレットをライトノードと呼ぶ。ライトノードは、自身でタングルを有しない分、タングルの管理などが不要なので動作上の負担が小さくて済むが、フルノードから情報を得て動作する場合にはわずかながら通信時間による処理の遅延が生じるおそれがある。フルノードでは、自身でタングルを管理する負担があるが、自身が有するタングルを用いることで通信の必要がなく、他の装置に依存せず動作可能である。なお、デバイス管理システム１においては、各装置間又は各装置内で生じる情報の授受に対して課金するようにしてもよい。わずかな情報の授受では課金額もわずかであるが、仮想通貨であるＩＯＴＡで課金額の支払いをすることで、マイクロペイメントに適したシステムを構築することができる。情報処理装置２、ＩｏＴデバイス５、端末装置１１、デバイス１６は、フルノードであってもよいし、ライトノードであってもよい。

[0053] 図１１は、分散型台帳の一例であるタングルを示す図である。タングルは、ＤＡＧ（有向非巡回グラフ）を用いている。図１１に示したデバイス管理

システム１において、分散型台帳に情報を記帳するということは、タングルにトランザクション（ＴＸ）を記録することになる。新たなトランザクションを記録する際には、プルーフオブワーク（ＰｏＷ）が実行される。ＩＯＴＡのタングルを分散型台帳として用いることで、分散型台帳への記帳速度を速くすることができる。

[0054] 図１２は、デバイスの製造時情報を記憶するデバイス管理システムを示す図である。デバイス製造時用分散型台帳１０１は、デバイス管理システム１が管理するデバイス（以下、「管理対象デバイス」という）の製造工程に係る情報である製造時情報を記帳する分散型台帳である。デバイス製造時用分散型台帳１０１は、デバイス管理システム１を構成するフルノードが有するタングルである。端末装置１１は、製造時情報１６ａをデバイス製造時用分散型台帳１０１に記帳する。

[0055] 端末装置１１は、デバイスを製造する設備（例、図１の工場ＦＡ、製造ライン）に配置される装置、またはデバイスを製造する設備に配置される装置と通信可能に接続される装置である。端末装置１１は、例えば、図１の制御装置ＦＡ１に相当する。端末装置１１は、書き換え不能な記憶域（例えば、TrustZone（登録商標））を有する。この記憶域は、製造時情報を生成する処理を端末装置１１の処理部に実行させるプログラムを記憶する。端末装置１１の処理部は、上記プログラムに従って、製造過程のデバイスに部品が組み込まれたことを検出し、この部品のＩＤと、部品を組み込む製造ラインの情報とを、製造対象のデバイスのＩＤと関連付けることで、製造時情報を生成する。製造ラインの情報は、例えば、処理を実行する処理装置（例えば、図１の処理装置ＦＡ２）の情報（例えば、ＩＤ）を含む。端末装置１１の記憶域に記憶されたプログラムは、生成した製造時情報を分散型台帳に記帳する処理を、端末装置１１の処理部に実行させる。

[0056] 製造時情報１６ａは、デバイス製造時用分散型台帳１０１におけるトランザクションである。製造時情報１６ａは、管理対象デバイスを製造する際の情報である。製造時情報１６ａは、管理対象デバイスの製造工程において、

管理対象デバイスを構成する部品が選択され、組付けられる都度、発生する。例えば、管理対象デバイスの製造工程において、管理対象デバイスを構成する部品である回路基板Ａが選択され、回路基板Ａに電子部品Ｂ（ＣＰＵ、メモリ等）が実装された場合、その管理対象デバイスに対し、回路基板Ａについての製造時情報１６ａが発生するとともに、電子部品Ｂについての製造時情報１６ａが発生する。

[0057] 製造時情報１６ａは、管理対象デバイスを特定可能なデバイスＩＤと、管理対象デバイスを構成する部品を特定可能な部品ＩＤと、部品ＩＤが示す部品を管理対象デバイスに組み入れた製造ラインを特定可能な製造ラインＩＤと、部品ＩＤが示す部品を管理対象デバイスに組み入れた時刻を示す製造時刻情報とを含む。また、製造時情報１６ａは、部品ＩＤ、製造ラインＩＤ及び製造時刻情報を、デバイスＩＤに紐付けた情報である。製造ラインＩＤは、作業者または製造装置を特定するため、作業者担当者ＩＤまたは製造装置（ロボット）ＩＤを含んでもよい。

[0058] 図１３は、デバイスの製造時情報を記憶する処理を示す図である。図１３は、端末装置１１が実行する処理を示す。まず、端末装置１１の処理部１２は、新たに発生した製造時情報１６ａがあるか否かを検出する（ステップＳ８０１）。製造時情報１６ａは、製造担当者が端末装置１１の入出力部１３を操作して端末装置１１に入力してもよい。また、ロボットが管理対象デバイスを製造する場合には、そのロボットが端末装置１１の通信部１５を介して端末装置１１に製造時情報１６ａを入力してもよい。

[0059] ステップＳ８０１において、新たに発生した製造時情報１６ａがある場合には、処理部１２は、デバイス製造時用分散型台帳１０１に今回の製造時情報１６ａを記帳し（ステップＳ８０２）、処理を終了する。ステップＳ８０１において、新たに発生した製造時情報１６ａがない場合には、処理部１２は、そのまま処理を終了する。なお、デバイス製造時用分散型台帳１０１に記帳する端末装置１１は、情報処理装置２、ＩｏＴデバイス５又はデバイス１６のいずれかであってもよいし、管理対象デバイス自身であってもよい。

一般に、デバイス製造工程は、部品の実装、組み立て、検査など複数の工程に分かれる。製造時情報１６ａは、工程ごとに記録してもよいし、最終の組み立て・検査工程で少なくとも一回記録してもよい。

[0060] 図１４は、デバイスの起動時情報を記憶するデバイス管理システムを示す図である。デバイス変更履歴用分散型台帳１０２は、管理対象デバイスの起動工程に係る情報である起動時情報１６ｂを記帳する分散型台帳である。デバイス変更履歴用分散型台帳１０２は、デバイス管理システム１を構成するフルノードが有するタングルである。デバイス変更履歴用分散型台帳１０２は、デバイス製造時用分散型台帳１０１と同じ分散型台帳であってもよい。端末装置１１は、起動時情報１６ｂをデバイス変更履歴用分散型台帳１０２に記帳する。端末装置１１は、例えば、管理対象のデバイス（例、図１のデバイスＤｂ）、又は管理対象のデバイスを制御するデバイス（例、図１の上位装置ＭＤ）である。

[0061] 起動時情報１６ｂは、デバイス変更履歴用分散型台帳１０２におけるトランザクションである。起動時情報１６ｂは、管理対象デバイスを起動する際の情報である。製造工程において製造された管理対象デバイスは、起動時に起動工程を実施する。この起動工程では、管理対象デバイスを初期化して起動する。本実施形態では、管理対象デバイスは、プログラムを記憶したＲＯＭ、ＲＯＭに記憶したプログラムを実行するＣＰＵおよびセキュアエレメントを有する。セキュアエレメントは耐タンパー性を有するＴＰＭ（Ｔｒｕｓｔｅｄ Ｐｌａｔｆｏｒｍ Ｍｏｄｕｌｅ）、ＳＩＭ（Ｓｕｂｓｃｒｉｂｅｒ Ｉｄｅｎｔｉｔｙ Ｍｏｄｕｌｅ）、ＳＡＭ（Ｓｅｃｕｒｅ Ａｐｐｌｉｃａｔｉｏｎ Ｍｏｄｕｌｅ）であってもよいし、既知の他の如何なる構成を設けてもよい。セキュアエレメントは、デジタル署名の検証鍵を保存できる機能を有していれば、必ずしも耐タンパー性を備えている必要は無く、例えばＣＰＵ内に通常のメモリとは別に存在するＴｒｕｓｔＺｏｎｅと呼ばれる仕組みを使ってもよい。管理対象デバイスの起動工程が実施されると、起動時情報１６ｂが発生する。

[0062] 例えば、上記セキュアエレメントには、端末装置１１の処理部１２に、起動時情報を生成する処理を実行させるプログラムが格納されている。処理部１２は、デバイスを起動するタイミングで、起動時の処理を定義するソースコードが記述されたファイルのハッシュ値および起動ログを生成する。処理部１２は、生成したハッシュ値および起動ログの少なくとも一部と、デバイスのＩＤとを含む起動時情報を生成する。また、上記セキュアエレメントには、端末装置１１の処理部１２に、起動時情報を分散型台帳に記帳する処理を実行させるプログラムが格納されている。処理部１２は、このプログラムに従って、生成した起動時情報を分散型台帳へ記帳する。

[0063] 起動時情報１６ｂは、管理対象デバイスを特定可能なデバイスＩＤと、管理対象デバイスの起動工程を実施した時刻を示す検証時刻情報と、管理対象デバイスの起動工程に用いたプログラムやデータのファイルのハッシュ値と、管理対象デバイスによるデジタル署名と、を含む。また、起動時情報１６ｂは、検証時刻情報、ハッシュ値及びデジタル署名を、デバイスＩＤに紐付けた情報である。

[0064] 図１５は、デバイスの起動時情報を記憶する処理を示す図である。図１５は、端末装置１１が実行する処理を示す。まず、端末装置１１の処理部１２は、新たに発生した起動時情報１６ｂがあるか否かを検出する（ステップＳ１００１）。管理対象デバイスは、端末装置１１の通信部１５を介して、起動時情報１６ｂを端末装置１１に入力してもよい。なお、管理対象デバイス自身が、起動時情報１６ｂをデバイス変更履歴用分散型台帳１０２に記帳してもよい。

[0065] ステップＳ１００１において、新たに発生した起動時情報１６ｂがある場合には、処理部１２は、デバイス変更履歴用分散型台帳１０２に今回の起動時情報１６ｂを記帳し（ステップＳ１００２）、処理を終了する。ステップＳ１００１において、新たに発生した起動時情報１６ｂがない場合には、処理部１２は、そのまま処理を終了する。なお、デバイス変更履歴用分散型台帳１０２に記帳する端末装置１１は、情報処理装置２、ＩｏＴデバイス５又

はデバイス１６のいずれかであってもよいし、管理対象デバイス自身であってもよい。

[0066] 図１６は、デバイスの更新時情報を記憶するデバイス管理システムを示す図である。デバイス変更履歴用分散型台帳１０２は、起動時情報１６ｂに加えて、管理対象デバイスの更新工程に係る情報である更新時情報１６ｃを記帳する分散型台帳である。デバイス変更履歴用分散型台帳１０２は、デバイス管理システム１を構成するフルノードが有するタングルである。端末装置１１は、更新時情報１６ｃをデバイス変更履歴用分散型台帳１０２に記帳する。端末装置１１は、例えば、管理対象のデバイス（例、図１のデバイスＤｂ）、又は管理対象のデバイスを制御するデバイス（例、図１の上位装置ＭＤ）である。

[0067] 更新時情報１６ｃは、デバイス変更履歴用分散型台帳１０２におけるトランザクションである。更新時情報１６ｃは、管理対象デバイスを更新する際の情報である。起動工程において起動された管理対象デバイスは、動作中に、プログラムの更新を行う更新工程を実施する。例えば、管理対象デバイスは、ファームウェアのパッチ、管理対象デバイス特有の機能において新機能を追加するプログラム、バグを修正するプログラム、及び各種データ等をインターネット経由で受信し、受信したプログラム等で、管理対象デバイスで実行するプログラムを更新する。本実施形態では、管理対象デバイスは、管理対象デバイスで実行するファームウェア（ＦＷ）、及び管理対象デバイスで実行するプログラムや実行に際して利用するデータのファイル（Ｆｉｌｅ）を有する。なお、ファームウェアもプログラムの一種である。管理対象デバイスの更新工程が実施されると、更新時情報１６ｃが発生する。管理対象デバイスの更新工程は、例えば端末装置１１により管理対象デバイスのファームウェアやコンフィグファイルのアップデートを含んでもよい。この場合、端末装置１１は、アップデートに関する更新時情報１６ｃをデバイス変更履歴用分散型台帳１０２に記帳する。

[0068] 例えば、上記セキュアエレメントには、端末装置１１の処理部１２に、更

新時情報を生成する処理を実行させるプログラムが格納されている。処理部１２は、デバイスを更新するタイミングで、更新時の処理を定義するソースコードが記述されたファイルのハッシュ値および更新ログを生成する。処理部１２は、生成したハッシュ値および更新ログの少なくとも一部と、デバイスのＩＤとを含む起動時情報を生成する。また、上記セキュアエレメントには、端末装置１１の処理部１２に、更新時情報を分散型台帳に記帳する処理を実行させるプログラムが格納されている。処理部１２は、このプログラムに従って、生成した更新時情報を分散型台帳へ記帳する。

[0069] 更新時情報１６ｃは、管理対象デバイスを特定可能なデバイスＩＤと、管理対象デバイスの更新工程を実施した時刻を示す検証時刻情報と、管理対象デバイスの更新工程に用いたプログラムやデータのファイルのハッシュ値と、管理対象デバイスによるデジタル署名と、を含む。また、更新時情報１６ｃは、検証時刻情報、ハッシュ値及びデジタル署名を、デバイスＩＤに紐付けた情報である。

[0070] 図１７は、デバイスの起動時情報を記憶する処理を示す図である。図１７は、端末装置１１が実行する処理を示す。まず、端末装置１１の処理部１２は、新たに発生した更新時情報１６ｃがあるか否かを検出する（ステップＳ１２０１）。管理対象デバイスは、端末装置１１の通信部１５を介して、更新時情報１６ｃを端末装置１１に入力してもよい。なお、管理対象デバイス自身が、更新時情報１６ｃをデバイス変更履歴用分散型台帳１０２に記帳してもよい。

[0071] ステップＳ１２０１において、新たに発生した更新時情報１６ｃがある場合には、処理部１２は、デバイス変更履歴用分散型台帳１０２に今回の更新時情報１６ｃを記帳し（ステップＳ１２０２）、処理を終了する。ステップＳ１２０１において、新たに発生した更新時情報１６ｃがない場合には、処理部１２は、そのまま処理を終了する。なお、デバイス変更履歴用分散型台帳１０２に記帳する端末装置１１は、情報処理装置２、ＩｏＴデバイス５又はデバイス１６のいずれかであってもよいし、管理対象デバイス自身であっ

てもよい。

[0072] なお、端末装置１１は、新たな更新時情報１６ｃがある場合（更新がされたとき）だけではなく、更新がされていなくても所定時間ごとに、現在の管理対象デバイスの状態を示す更新時情報１６ｃをデバイス変更履歴用分散型台帳１０２に記帳するようにしてもよい。現在の管理対象デバイスの状態を示す更新時情報１６ｃは、管理対象デバイスを特定可能なデバイスＩＤと、現在の時刻を示す検証時刻情報と、管理対象デバイスで現在実行されているプログラムやデータのファイルのハッシュ値と、管理対象デバイスによるデジタル署名と、を含む。また、更新時情報１６ｃは、検証時刻情報、ハッシュ値及びデジタル署名を、デバイスＩＤに紐付けた情報である。

[0073] 図１８は、デバイスの更新時情報を所定時間ごとに記憶する処理を示す図である。図１８は、端末装置１１が実行する処理を示す。まず、端末装置１１の処理部１２は、前回の更新時情報１６ｃの記帳から所定時間経過したかを確認する（ステップＳ１３０１）。なお、ステップＳ１３０１で判定する所定時間は、管理対象デバイスが改竄されるおそれがある頻度に応じて定めるようにしてもよい。また、所定時間は一定の時間にしてもよいし、変動させてもよい。管理対象デバイスは、端末装置１１の通信部１５を介して、更新時情報１６ｃを端末装置１１に入力してもよい。なお、管理対象デバイス自身が、更新時情報１６ｃをデバイス変更履歴用分散型台帳１０２に記帳してもよい。

[0074] ステップＳ１３０１において、所定時間経過した場合には、処理部１２は、デバイス変更履歴用分散型台帳１０２に今回の起動時情報１６ｂを記帳し（ステップＳ１３０２）、処理を終了する。ステップＳ１３０１において、所定時間経過しない場合には、処理部１２は、そのまま処理を終了する。なお、デバイス変更履歴用分散型台帳１０２に記帳する端末装置１１は、情報処理装置２、ＩｏＴデバイス５又はデバイス１６のいずれかであってもよいし、管理対象デバイス自身であってもよい。図１８に示した処理によれば、管理対象デバイスが更新されているにもかかわらず、更新されていない状態

を装う改竄に対しても対応することができ、管理対象デバイスの現在の状況が正しくデバイス変更履歴用分散型台帳１０２に反映される。

[0075] 図１９は、複数のトラスト情報を参照するデバイス管理システムを示す図である。デバイス管理システム１において、例えば端末装置１１は、デバイス製造時用分散型台帳１０１に記帳された製造時情報１６ａ、デバイス変更履歴用分散型台帳１０２に記帳された起動時情報１６ｂ、及びデバイス変更履歴用分散型台帳１０２に記帳された更新時情報１６ｃを参照する。

[0076] 図２０は、複数のトラスト情報を参照する処理を示す図である。図２０は、端末装置１１が実行する処理を示す。まず、端末装置１１は、管理対象デバイスの信頼性を確認する処理が発生したかを判定する（ステップＳ１５０１）。管理対象デバイスの信頼性を確認する処理とは、例えば、ある管理対象デバイスの動作に何らかの不審な動きがあったときに、その管理対象デバイスの状態を確認する処理を含む。管理対象デバイスの信頼性を確認する処理とは、例えば、ある管理対象デバイスからのデータを利用する際に、その管理対象デバイスの信頼性を確認する処理を含む。管理対象デバイスの信頼性を確認する処理とは、例えば、ある管理対象デバイスを駆動制御する際に、その管理対象デバイスの信頼性を確認する処理を含む。管理対象デバイスの信頼性を確認する処理とは、例えば、ある管理対象デバイスの監査などが必要になったときに、その管理対象デバイスの状態を確認する処理を含む。

[0077] ステップＳ１５０１において、管理対象デバイスの信頼性を確認する処理が発生していない場合には、端末装置１１は、そのまま処理を終了する。ステップＳ１５０１において、管理対象デバイスの信頼性を確認する処理が発生した場合には、ステップＳ１５０２において、端末装置１１は、今回信頼性を確認する管理対象デバイスがどのデバイスなのかを特定するデバイスＩＤを取得する。このデバイスＩＤの取得は、入出力部１３から入力されることで取得してもよいし、通信部１５を介して外部から受信することで取得してもよいし、記憶部１４から読み出してくることで取得してもよい。さらに、ステップＳ１５０２において、端末装置１１は、取得したデバイスＩＤに

ついての製造時情報１６ａをデバイス製造時用分散型台帳１０１から読み出し、取得したデバイスＩＤについての起動時情報１６ｂをデバイス変更履歴用分散型台帳１０２から読み出し、取得したデバイスＩＤについての更新時情報１６ｃをデバイス変更履歴用分散型台帳１０２から読み出す。

[0078] 続いて、端末装置１１は、ステップＳ１５０１で読み出した製造時情報１６ａ、起動時情報１６ｂ及び更新時情報１６ｃを判定し、管理対象デバイスの現在の信頼性を確認する（ステップＳ１５０３）。ステップＳ１５０４では、ステップＳ１５０３の判定結果である、管理対象デバイスの現在の信頼性に基づいた制御を行った後、処理を終了する。例えば、デバイス製造時用分散型台帳１０１から読み出した製造時情報１６ａに、当初予定した部品以外の部品についての情報が含まれていた場合には、その管理対象デバイスを利用しない制御を行うことができる。また、例えば、デバイス変更履歴用分散型台帳１０２から読み出した更新時情報１６ｃに、非正規のアップデートについての情報が含まれていた場合には、その管理対象デバイスを利用しない制御を行うことができる。また、例えば、製造時情報１６ａ、起動時情報１６ｂ及び更新時情報１６ｃに何ら不審な点が無ければ、その管理対象デバイスが信頼できるデバイスであるとして利用する制御を行うことができる。なお、図２０の処理を実行する端末装置１１は、情報処理装置２、ＩｏＴデバイス５又はデバイス１６のいずれかであってもよいし、管理対象デバイス自身であってもよい。このように本実施形態によれば、管理対象デバイスに対してトレーサビリティな環境を提供することができる。また、本実施形態によれば、第三者に対して、管理対象デバイスが正当なデバイスであることを主張する根拠を提供することができる。

実施例 1

[0079] 図２１は、実施形態に係るデバイス管理システムを適用した実施例を示す図である。本実施例は、実施形態に係るデバイス管理システムを、人物の足跡を追う人物追跡システムに適用した例である。人物追跡システム１６００は、管理対象デバイスである監視カメラ１６０６、１６０７及び１６０８を

有する。監視カメラ１６０６、１６０７及び１６０８の製造時、起動時及び更新時の情報は、随時分散型台帳１６０２に記帳される。監視カメラ１６０６、１６０７及び１６０８の信頼性は分散型台帳１６０２によって保証される。分散型台帳１６０２は、信頼できるデバイス足る根拠となるエビデンスが記帳された分散型台帳１６０１を参照する。

[0080] 人物１６０５の顔画像は分散型台帳１６０４に記帳されている。監視カメラ１６０６、１６０７及び１６０８は、分散型台帳１６０４に記帳された顔画像と、自身が撮影した人物の顔画像とを突合することで、人物１６０５が監視カメラ１６０６、１６０７及び１６０８の設置位置を通過したという行動履歴を取得する。この行動履歴は分散型台帳１６０３に記帳される。この行動履歴の記帳の際には、分散型台帳１６０２が参照され、監視カメラ１６０６、１６０７及び１６０８の撮影結果の信頼性が保証される。店舗１６０９では、分散型台帳１６０３を参照し、人物１６０５の行動パターンや購入傾向などを分析し、商品仕入れや商品開発に利用することができる。

実施例 2

[0081] 図２２は、実施形態に係るデバイス管理システムを適用した実施例を示す図である。本実施例は、実施形態に係るデバイス管理システムを、危険運転車を判別する危険車判別システムに適用した例である。危険車判別システム１７００は、管理対象デバイスである監視カメラ１７０５及び１７０６を有する。監視カメラ１７０５及び１７０６は、車両１７０４に搭載される。監視カメラ１７０５は車両１７０４の前方を撮影し、先行車１７０７の運転状況を撮影する。監視カメラ１７０６は車両１７０４の後方を撮影し、後続車１７０８の運転状況を撮影する。監視カメラ１７０５及び１７０６の製造時、起動時及び更新時の情報は、随時分散型台帳１７０２に記帳される。監視カメラ１７０５及び１７０６の信頼性は分散型台帳１７０２によって保証される。分散型台帳１７０２は、信頼できるデバイス足る根拠となるエビデンスが記帳された分散型台帳１７０１を参照する。

[0082] 監視カメラ１７０５及び１７０６で撮影された、先行車や後続車の運転状

況や車両ナンバーは分散型台帳１７０３に記帳される。また、監視カメラ１７０５及び１７０６は、分散型台帳１７０３に過去に記帳された内容を参照することで、過去に危険運転をした車両の車両ナンバーを取得することができる。監視カメラ１７０５及び１７０６は、現在撮影している先行車や後続車の車両ナンバーと、分散型台帳１７０３から取得した過去に危険運転をした車両の車両ナンバーとを突合することで、先行車や後続車が危険運転をするおそれについて、車両１７０４を運転する運転者のスマートフォン１７１０に通知したり、車両１７０４に搭載されたナビゲーションシステム１７０９に通知したりすることができる。

[0083] デバイス管理システムの１つの形態は、分散型台帳（デバイス製造時用分散型台帳１０１、デバイス変更履歴用分散型台帳１０２）と、デバイスの製造工程に係る情報である製造時情報、前記デバイスの起動工程に係る情報である起動時情報、及び前記デバイスの更新工程に係る情報である更新時情報のうちの少なくとも一つの情報を前記分散型台帳に記帳する記帳手段（Ｓ８０２、Ｓ１００２、Ｓ１２０２、Ｓ１３０２）と、前記分散型台帳に記帳された情報を読み出す情報読出手段（Ｓ１５０２）と、を有する。これにより、デバイスの信頼性を向上可能なデバイス管理システムを提供する。また、デバイスに関する情報を分散型台帳に記帳することにより、情報が改竄されにくくすることができる。また、パブリックな分散型台帳に記帳するようにすれば、デバイスに関する情報を誰でもが参照可能なシステムを提供することができ、デバイスの信頼性を誰でもが確認することができる。

[0084] デバイス管理システムの１つの形態において、前記分散型台帳がタングル（図６参照）である。これにより、分散型台帳への記帳をリアルタイムで行うことができる。また、記帳の際に手数料が必要となる他の分散型台帳と異なり、分散型台帳への記帳を無料で行うことができる。また、スケーラビリティのあるシステムを提供することができる。また、仮想通貨ＩＯＴＡを利用したマイクロペイメントとの親和性が高いシステムを提供することができる。

[0085] デバイス管理システムの１つの形態において、前記製造時情報は、前記デバイスを特定可能なデバイスＩＤと、前記デバイスを構成する部品を特定可能な部品ＩＤと、前記部品ＩＤが示す部品を前記デバイスに組み入れた製造ラインを特定可能な製造ラインＩＤと、前記部品ＩＤが示す部品を前記デバイスに組み入れた時刻を示す製造時刻情報と、を含み、各情報を前記デバイスＩＤに紐付けた情報である。これにより、デバイスの製造時についての信頼性を高めたシステムを提供することができる。

[0086] デバイス管理システムの１つの形態において、前記起動時情報は、前記デバイスを特定可能なデバイスＩＤと、前記デバイスの起動工程を実施した時刻を示す検証時刻情報と、前記デバイスの起動工程に用いたファイルのハッシュ値と、前記デバイスによるデジタル署名と、を含み、各情報を前記デバイスＩＤに紐付けた情報である。これにより、デバイスの起動時についての信頼性を高めたシステムを提供することができる。

[0087] デバイス管理システムの１つの形態において、前記更新時情報は、前記デバイスを特定可能なデバイスＩＤと、前記デバイスの更新工程を実施した時刻を示す検証時刻情報と、前記デバイスの更新工程に用いたファイルのハッシュ値と、前記デバイスによるデジタル署名と、を含み、各情報を前記デバイスＩＤに紐付けた情報である。これにより、デバイスの更新時についての信頼性を高めたシステムを提供することができる。

[0088] デバイス管理システムの１つの形態において、前記デジタル署名は、前記ファイルのハッシュ値を秘密鍵で暗号化して得られたデジタル署名である。これにより、また、分散型台帳に記帳したデバイスに関する情報を、より改竄されにくくすることができる。

[0089] デバイス管理システムの１つの形態において、前記デバイスは、ＩｏＴデバイスである。これにより、インターネット接続されることでマルウェア等の攻撃を受ける可能性があるＩｏＴデバイスに対し、その信頼性を高めることができる。また、この形態によれば、例えばマルウェアによって、ＩｏＴデバイスを制御するプログラムが書き換えられたとしても、その書き換えら

れたことが分散型台帳に記帳されるので、そのＩｏＴデバイスの現況について知ることができ、操作者は、そのＩｏＴデバイスを活用するか否かを判断する際の判断材料を得ることができる。

[0090] デバイス管理方法の１つの形態は、コンピュータを用いてデバイスの管理を行うデバイス管理方法であって、デバイスの製造工程に係る情報である製造時情報、前記デバイスの起動工程に係る情報である起動時情報、及び前記デバイスの更新工程に係る情報である更新時情報のうちの少なくとも一つの情報を分散型台帳に記帳する記帳工程と、前記分散型台帳に記帳された情報を読み出す情報読出工程と、を有する。これにより、デバイスの信頼性を向上可能なデバイス管理方法を提供する。また、デバイスに関する情報を分散型台帳に記帳することにより、情報が改竄されにくくすることができる。また、パブリックな分散型台帳に記帳するようにすれば、デバイスに関する情報を誰でもが参照可能な方法を提供することができ、デバイスの信頼性を誰でもが確認することができる。

[0091] デバイス管理方法の１つの形態において、情報処理装置は、デバイスの製造工程に係る情報である製造時情報、前記デバイスの起動工程に係る情報である起動時情報、及び前記デバイスの更新工程に係る情報である更新時情報のうちの少なくとも一つの情報を分散型台帳に記帳する記帳手段を有する。これにより、情報処理装置がデバイスに関する情報を分散型台帳に記帳することで、デバイスに関する情報を改竄されにくくすることができ、信頼性の高い情報を提供することができる。

[0092] デバイス管理方法の１つの形態において、ＩｏＴデバイスは、デバイスの製造工程に係る情報である製造時情報、前記デバイスの起動工程に係る情報である起動時情報、及び前記デバイスの更新工程に係る情報である更新時情報のうちの少なくとも一つの情報を分散型台帳に記帳する記帳手段を有する。これにより、ＩｏＴデバイスがデバイスに関する情報を分散型台帳に記帳することで、デバイスに関する情報を改竄されにくくすることができ、信頼性の高い情報を提供することができる。

[0093] プログラムの１つの形態は、デバイスの製造工程に係る情報である製造時情報、前記デバイスの起動工程に係る情報である起動時情報、及び前記デバイスの更新工程に係る情報である更新時情報のうちの少なくとも一つの情報を分散型台帳に記帳する記帳手段として、コンピュータを機能させる。これにより、デバイスの信頼性を向上可能なプログラムを提供する。また、デバイスに関する情報を分散型台帳に記帳することにより、情報が改竄されにくくすることができる。また、パブリックな分散型台帳に記帳するようにすれば、デバイスに関する情報を誰でもが参照可能なプログラムを提供することができ、デバイスの信頼性を誰でもが確認することができる。

[0094] プログラムの１つの形態において、前記分散型台帳がタングルである。これにより、分散型台帳への記帳をリアルタイムで行うことができる。また、記帳の際に手数料が必要となる他の分散型台帳と異なり、分散型台帳への記帳を無料で行うことができる。また、スケーラビリティのあるプログラムを提供することができる。また、仮想通貨ＩＯＴＡを利用したマイクロペイメントとの親和性が高いプログラムを提供することができる。

[0095] プログラムの１つの形態において、前記製造時情報は、前記デバイスを特定可能なデバイスＩＤと、前記デバイスを構成する部品を特定可能な部品ＩＤと、前記部品ＩＤが示す部品を前記デバイスに組み入れた製造ラインを特定可能な製造ラインＩＤと、前記部品ＩＤが示す部品を前記デバイスに組み入れた時刻を示す製造時刻情報と、を含み、各情報を前記デバイスＩＤに紐付けた情報である。これにより、デバイスの製造時についての信頼性を高めたプログラムを提供することができる。

[0096] プログラムの１つの形態において、前記起動時情報は、前記デバイスを特定可能なデバイスＩＤと、前記デバイスの起動工程を実施した時刻を示す検証時刻情報と、前記デバイスの起動工程に用いたファイルのハッシュ値と、前記デバイスによるデジタル署名と、を含み、各情報を前記デバイスＩＤに紐付けた情報である。これにより、デバイスの起動時についての信頼性を高めたプログラムを提供することができる。

[0097] プログラムの１つの形態において、前記更新時情報は、前記デバイスを特定可能なデバイスＩＤと、前記デバイスの更新工程を実施した時刻を示す検証時刻情報と、前記デバイスの更新工程に用いたファイルのハッシュ値と、前記デバイスによるデジタル署名と、を含み、各情報を前記デバイスＩＤに紐付けた情報である。これにより、デバイスの更新時についての信頼性を高めたプログラムを提供することができる。

[0098] プログラムの１つの形態において、前記記帳手段は、前記製造工程によって前記デバイスが製造された場合に、前記製造時情報を前記分散型台帳に記帳する。これにより、デバイスの製造時についての信頼性を高めたプログラムを提供することができる。

[0099] プログラムの１つの形態において、前記記帳手段は、前記起動工程によって前記デバイスが起動された場合に、前記起動時情報を前記分散型台帳に記帳する。これにより、デバイスの起動時についての信頼性を高めたプログラムを提供することができる。

[0100] プログラムの１つの形態において、前記記帳手段は、前記更新工程によって前記デバイスが更新された場合に、前記更新時情報を前記分散型台帳に記帳する。これにより、デバイスの更新時についての信頼性を高めたプログラムを提供することができる。

[0101] プログラムの１つの形態において、前記記帳手段は、所定時間ごとに、前記更新時情報を前記分散型台帳に記帳する。これにより、所定時間ごとのデバイスの状況を確認することができ、デバイスの信頼性を高めたプログラムを提供することができる。

[0102] なお、本発明の技術範囲は、上述の実施形態などで説明した態様に限定されない。上述の実施形態などで説明した要件の１つ以上は、省略されることがある。また、上述の実施形態などで説明した要件は、適宜組み合わせることができる。この出願は、２０１９年１０月１５日に出願された日本国特願２０１９－１８９０２１を基礎とする優先権主張による出願であり、基礎出願の開示の全てを援用して本文の記載の一部とする。また、法令で許容され

る限りにおいて、上述の実施形態などで引用した全ての文献の開示を援用して本文の記載の一部とする。

符号の説明

[0103] １　デバイス管理システム

２　情報処理装置

３　ネットワーク

４　ネットワーク

５　ＩｏＴデバイス

１１　端末装置

１２　処理部

１３　入出力部

１４　記憶部

１５　通信部

１６　デバイス

１７　処理部

１８　デバイス機能実行部

１９　記憶部

２０　通信部

１０１　デバイス製造時用分散型台帳

１０２　デバイス変更履歴用分散型台帳

１６ａ　製造時情報

１６ｂ　起動時情報

１６ｃ　更新時情報

請求の範囲

[請求項1] 識別情報を保持する記憶域が設けられるデバイスの製造工程に係る情報であって前記識別情報を含む製造時情報と、前記デバイスの起動工程に係る情報であって前記識別情報を含む起動時情報と、前記デバイスの更新工程に係る情報であって前記識別情報を含む更新時情報との少なくとも１つの情報を記憶部に記憶させる第１の情報処理装置と、

前記記憶部に記憶された前記製造時情報と前記起動時情報と前記更新時情報との少なくとも１つの情報のうち、管理対象の前記記憶域から読み出される前記識別情報を含む少なくとも１つの情報を読み出し、読み出した情報を用いて前記管理対象のデバイスの信頼性を判定する第２の情報処理装置と、を備えるデバイス管理システム。

[請求項2] 前記第２の情報処理装置が前記管理対象のデバイスの信頼性を判定した結果を用いて、前記管理対象のデバイスを制御する制御部を備える、

請求項１に記載のデバイス管理システム。

[請求項3] 前記制御部は、前記管理対象のデバイスが信頼できないと前記第２の情報処理装置が判定した場合、前記管理対象のデバイスの少なくとも一部の機能を停止させる、

請求項２に記載のデバイス管理システム。

[請求項4] 前記制御部は、前記管理対象のデバイスが信頼できないと前記第２の情報処理装置が判定した場合、前記管理対象のデバイスをネットワークから遮断する、

請求項２または請求項３に記載のデバイス管理システム。

[請求項5] 前記管理対象のデバイスが信頼できるか否かを前記第２の情報処理装置が判定した結果と、前記管理対象のデバイスの識別情報とを関連付けたトラスト情報を記憶する第２の記憶部を備え、

前記制御部は、前記第２の記憶部に記憶された前記トラスト情報を

用いて、前記管理対象のデバイスを制御する、

請求項２から請求項４のいずれか一項に記載のデバイス管理システム。

[請求項6] 複数のデバイスを含むシステムを管理する管理装置を備え、

前記管理装置は、前記管理対象のデバイスが信頼できるか否かを前記第２の情報処理装置が判定した結果に基づいて、前記管理対象のデバイスを前記システムに組み込むか否かを判定する、

請求項１から請求項５のいずれか一項に記載のデバイス管理システム。

[請求項7] 前記第１の情報処理装置は、前記デバイスの製造に使用される製造装置、又は前記製造装置と通信可能に接続される装置を含み、前記デバイスの出荷前に生成される前記製造時情報を前記記憶部に記憶させる、

請求項１から請求項６のいずれか一項に記載のデバイス管理システム。

[請求項8] 前記第１の情報処理装置は、前記管理対象のデバイスを制御する上位装置を含み、前記管理対象のデバイスから取得される情報に基づいて、前記起動時情報と前記更新時情報との一方又は双方を前記記憶部に記憶させる、

請求項１から請求項６のいずれか一項に記載のデバイス管理システム。

[請求項9] 前記第１の情報処理装置は、前記管理対象のデバイスを含み、自装置を起動する際に前記起動時情報を生成し、生成した前記起動時情報を前記記憶部に記憶させる、

請求項１から請求項６のいずれか一項に記載のデバイス管理システム。

[請求項10] 前記第１の情報処理装置は、前記管理対象のデバイスを含み、自装置を更新する際に前記更新時情報を生成し、生成した前記更新時情報

を前記記憶部に記憶させる、

請求項１から請求項６、請求項９のいずれか一項に記載のデバイス管理システム。

[請求項11] 前記記憶域は、前記デバイスの処理部を含むデバイス本体に内蔵される、

請求項１から請求項１０のいずれか一項に記載のデバイス管理システム。

[請求項12] 前記記憶域は書き換え不能な記憶域である、

請求項１１に記載のデバイス管理システム。

[請求項13] 前記記憶域は、前記デバイスの処理部を含むデバイス本体に外付けされたＲＦタグを含む、

請求項１から請求項１０のいずれか一項に記載のデバイス管理システム。

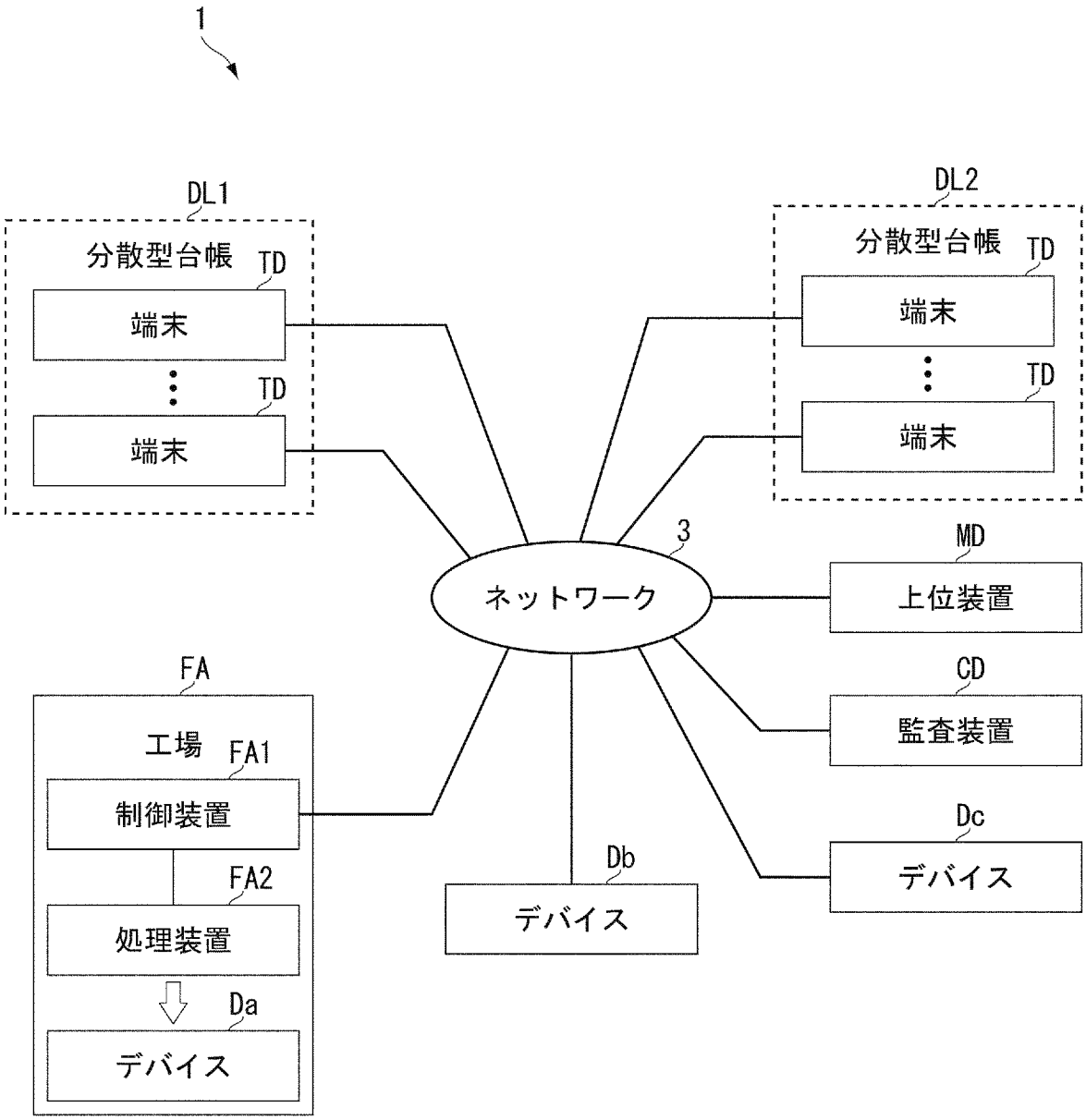
[請求項14] 前記ＲＦタグと前記デバイス本体とを接合する力は、前記回路が壊れる力よりも強い、

請求項１３に記載のデバイス管理システム。

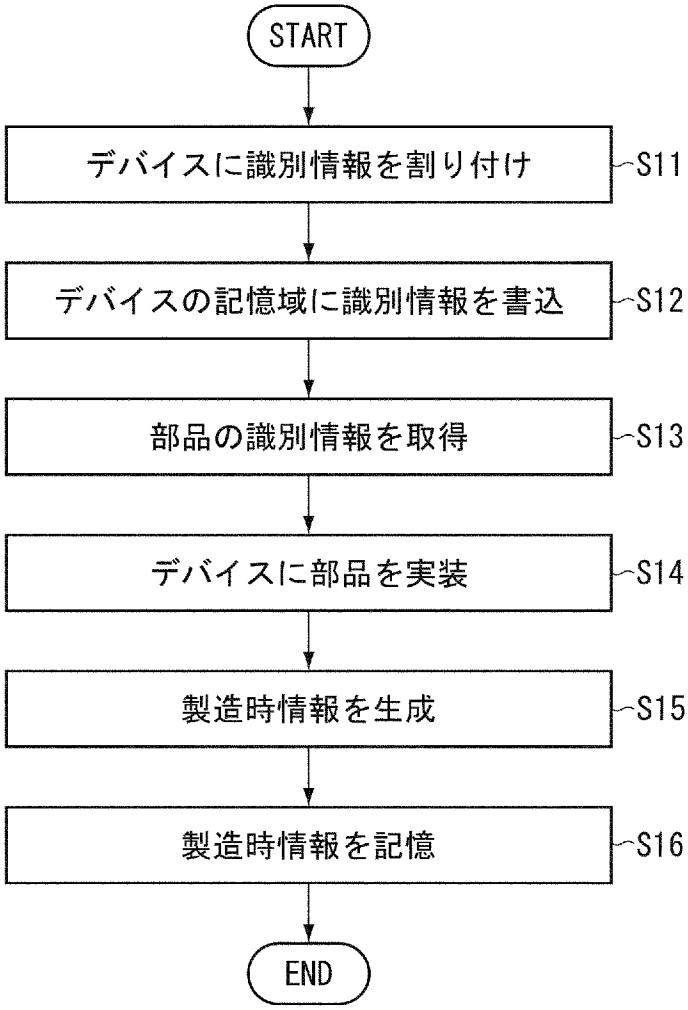
[請求項15] 前記記憶部は、分散型台帳を含む、

請求項１から請求項１４のいずれか一項に記載のデバイス管理システム。

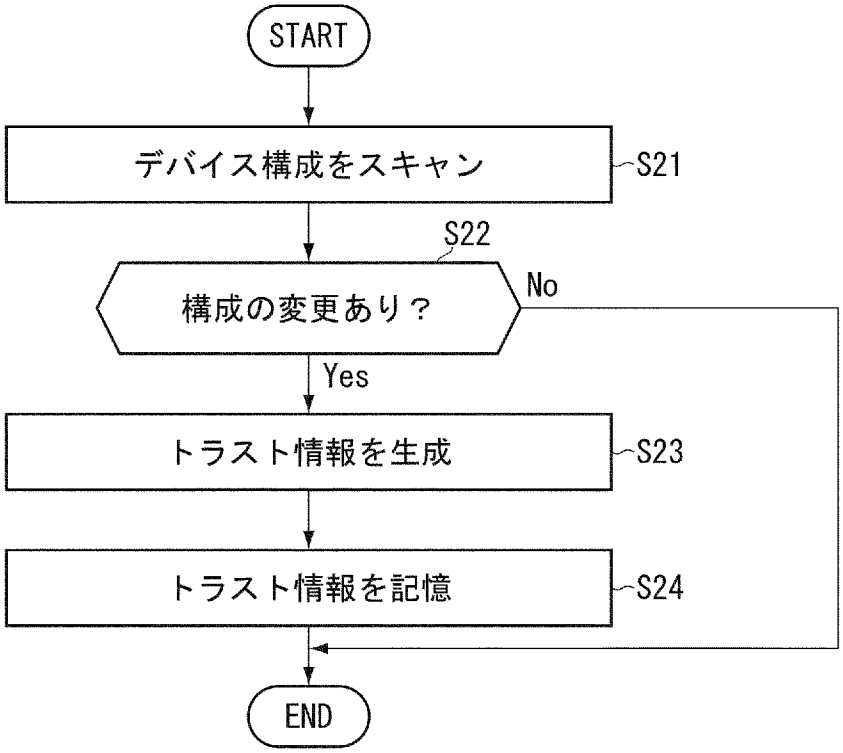
[図1]


1
DL1
分散型台帳
TD
端末
TD
端末
DL2
分散型台帳
TD
端末
TD
端末
3
ネットワーク
MD
上位装置
CD
監査装置
Dc
デバイス
Db
デバイス
FA
工場
FA1
制御装置
FA2
処理装置
Da
デバイス

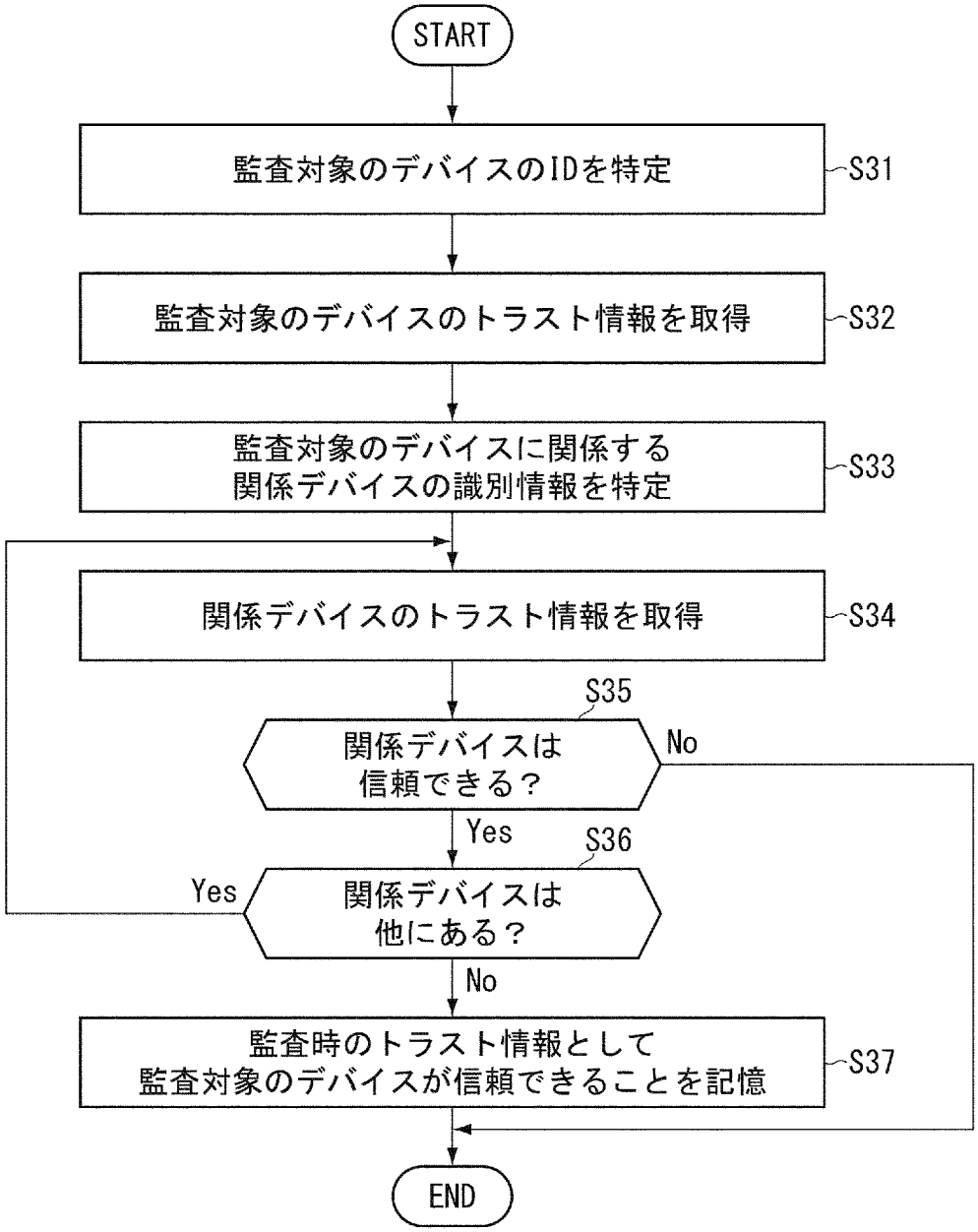
[図2]


START
デバイスに識別情報を割り付け
S11
デバイスの記憶域に識別情報を書込
S12
部品の識別情報を取得
S13
デバイスに部品を実装
S14
製造時情報を生成
S15
製造時情報を記憶
S16
END

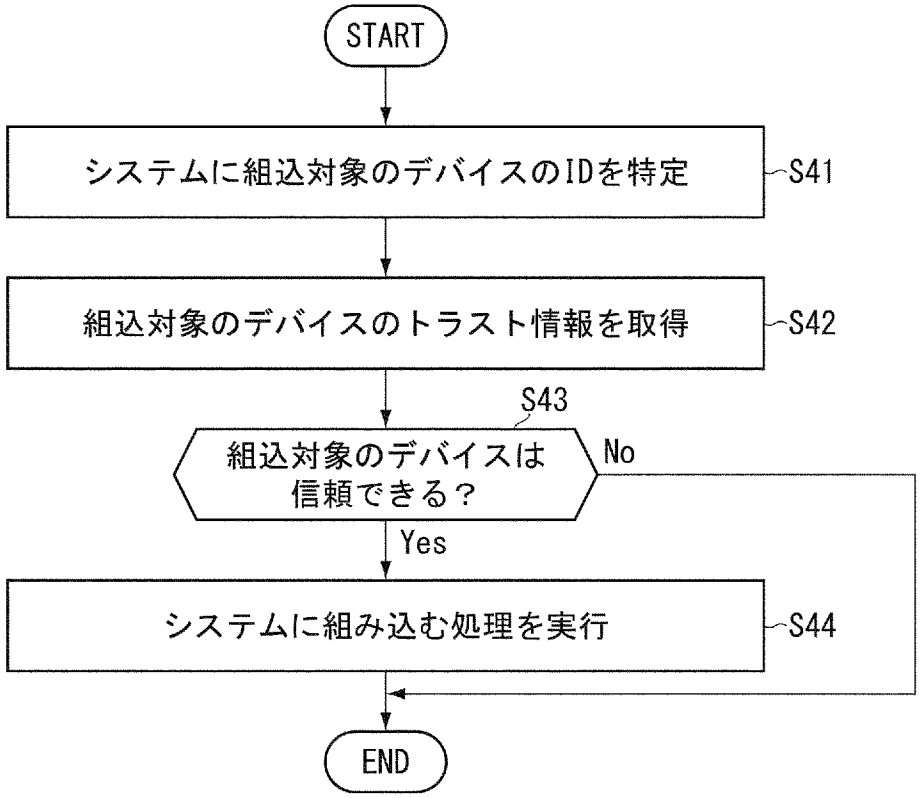
[図3]


START
デバイス構成をスキャン
S21
S22
構成の変更あり？
No
Yes
トラスト情報を生成
S23
トラスト情報を記憶
S24
END

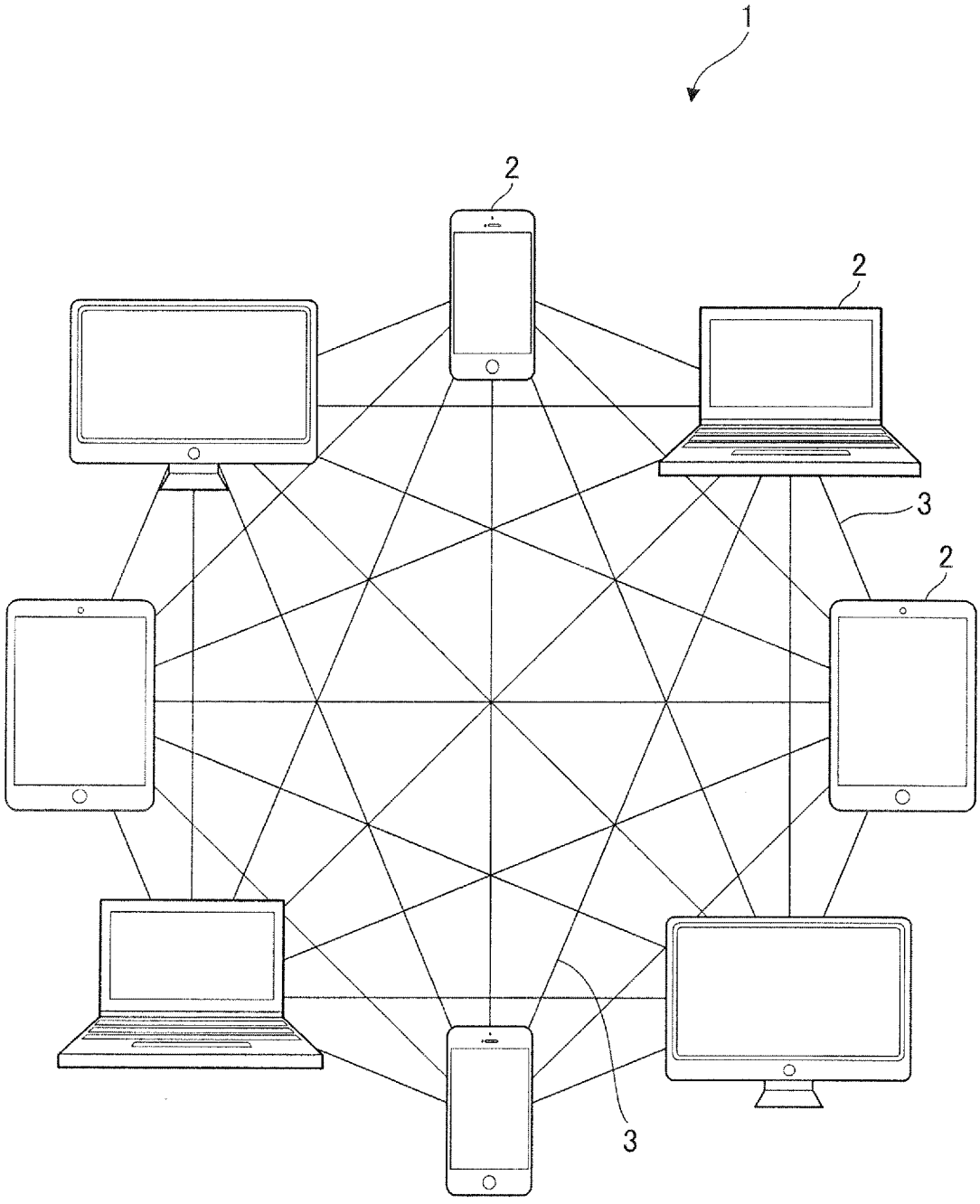
[図4]


START
監査対象のデバイスのIDを特定
S31
監査対象のデバイスのトラスト情報を取得
S32
監査対象のデバイスに関係する
関係デバイスの識別情報を特定
S33
関係デバイスのトラスト情報を取得
S34
S35
関係デバイスは
信頼できる？
No
Yes
S36
Yes
関係デバイスは
他にある？
No
監査時のトラスト情報として
監査対象のデバイスが信頼できることを記憶
S37
END

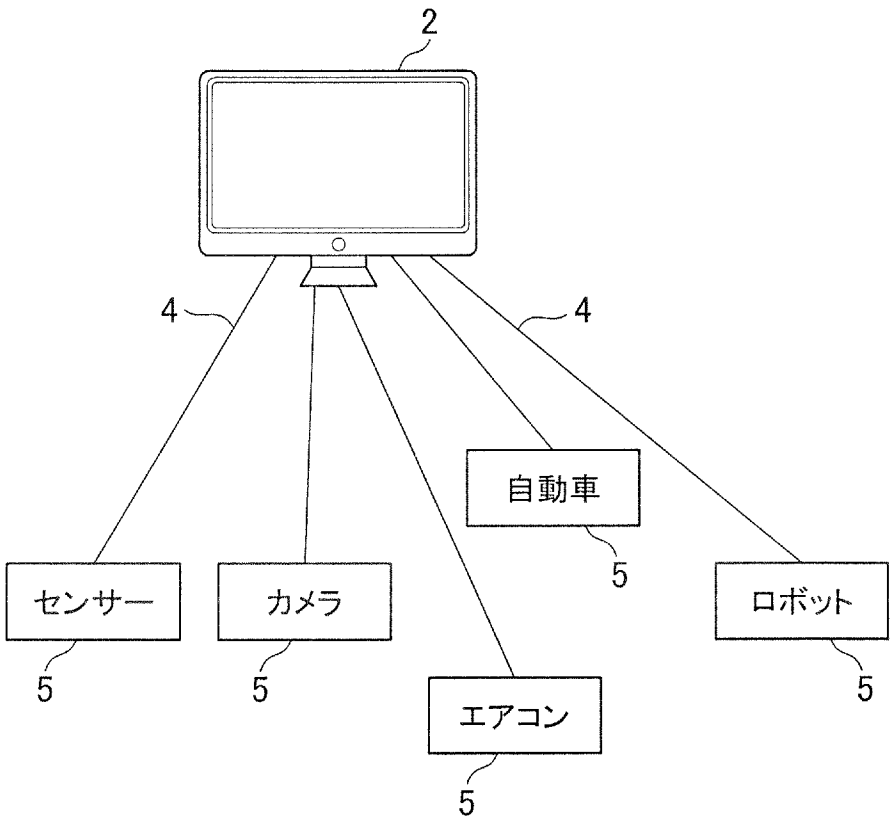
[図5]


START
システムに組込対象のデバイスのIDを特定
S41
組込対象のデバイスのトラスト情報を取得
S42
S43
組込対象のデバイスは
信頼できる？
No
Yes
システムに組み込む処理を実行
S44
END

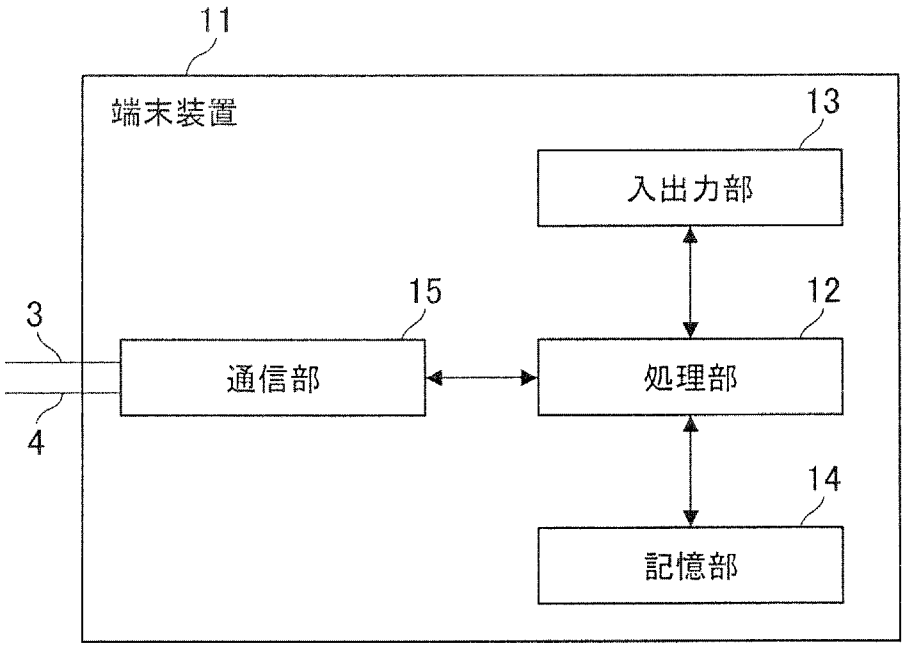
[図6]



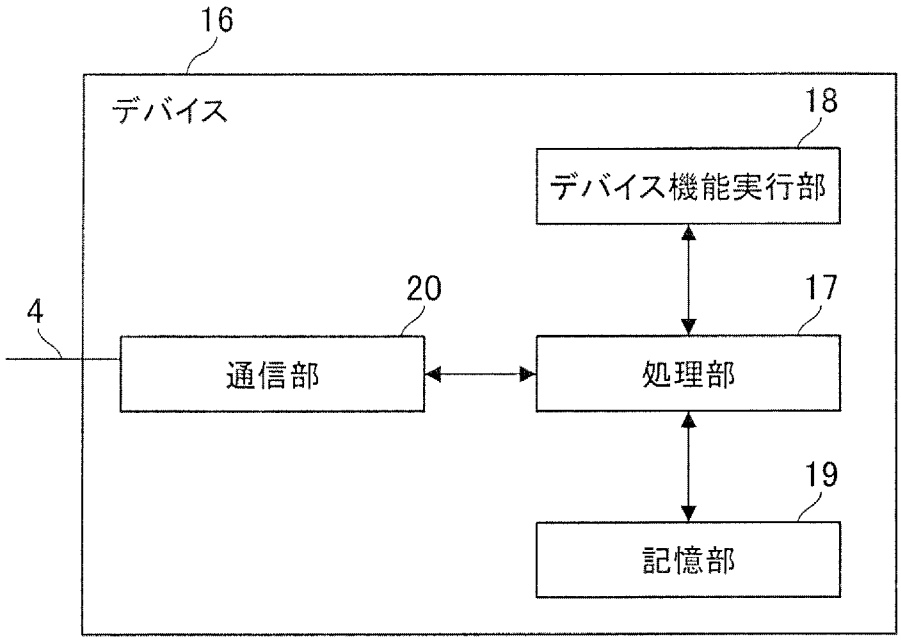
[図7]



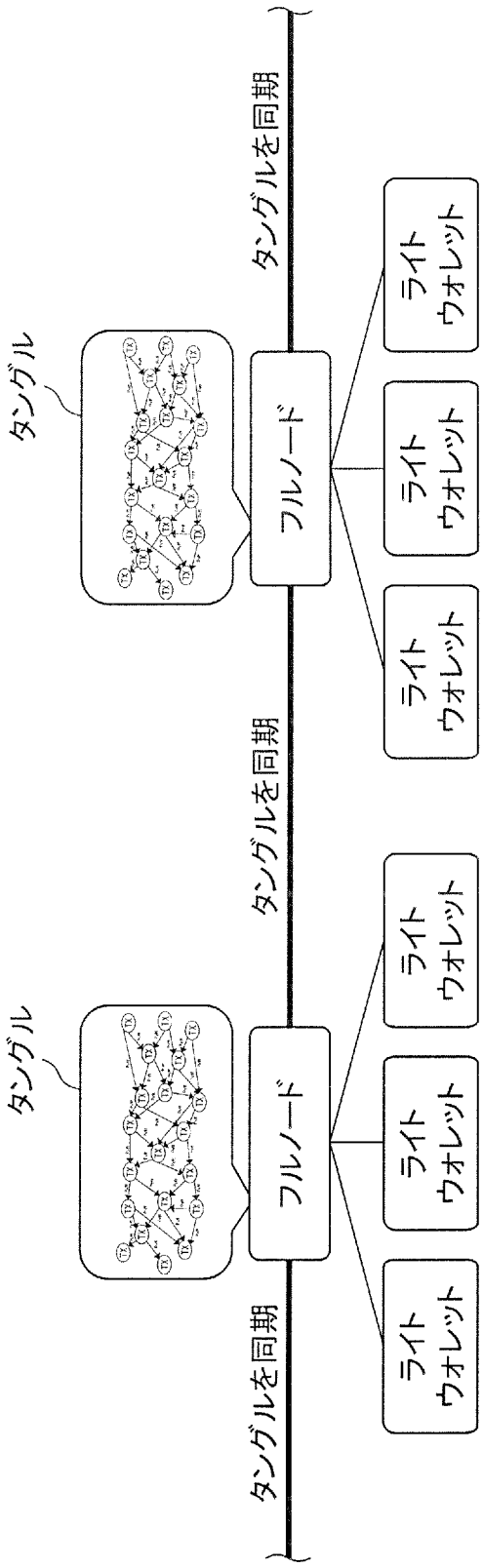
[図8]


11
端末装置
13
入出力部
15
12
3
通信部
処理部
4
14
記憶部

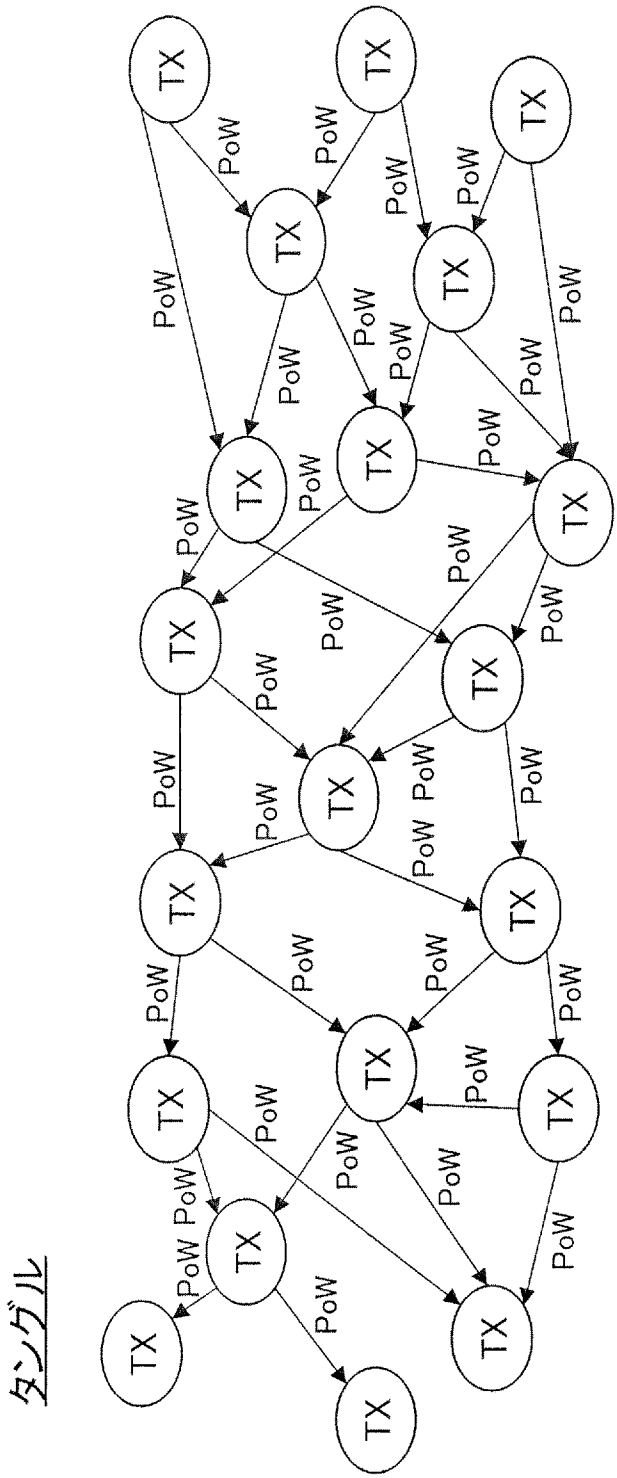
[図9]


16
デバイス
18
デバイス機能実行部
20
17
4
通信部
処理部
19
記憶部

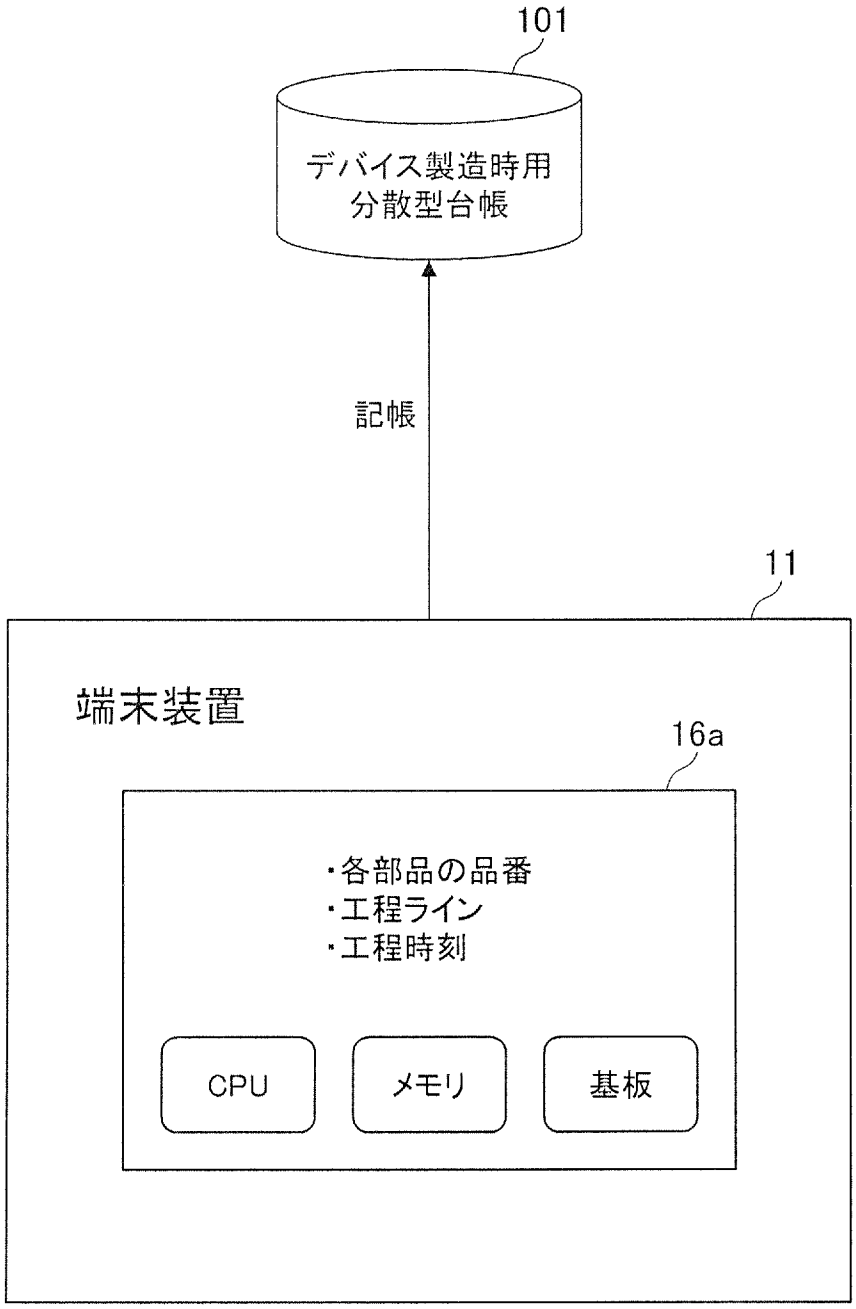
[図10]


タングル
タングル
フルノード
フルノード
ライト
ウォレット
ライト
ウォレット
ライト
ウォレット
ライト
ウォレット
ライト
ウォレット
ライト
ウォレット
タングルを同期
タングルを同期
タングルを同期

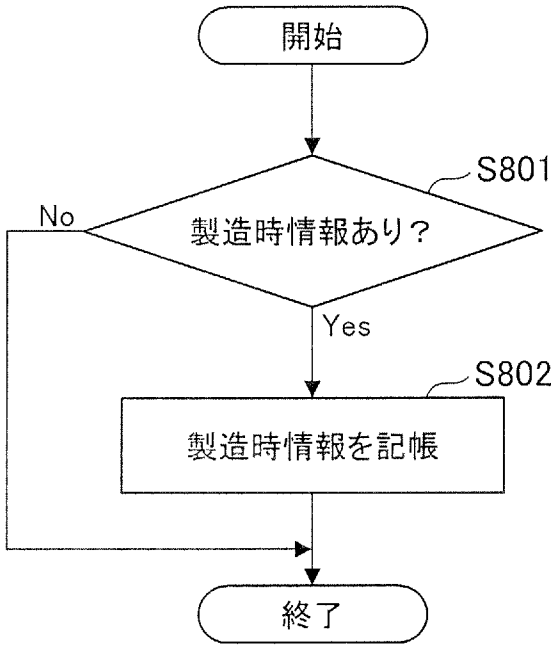
[図11]



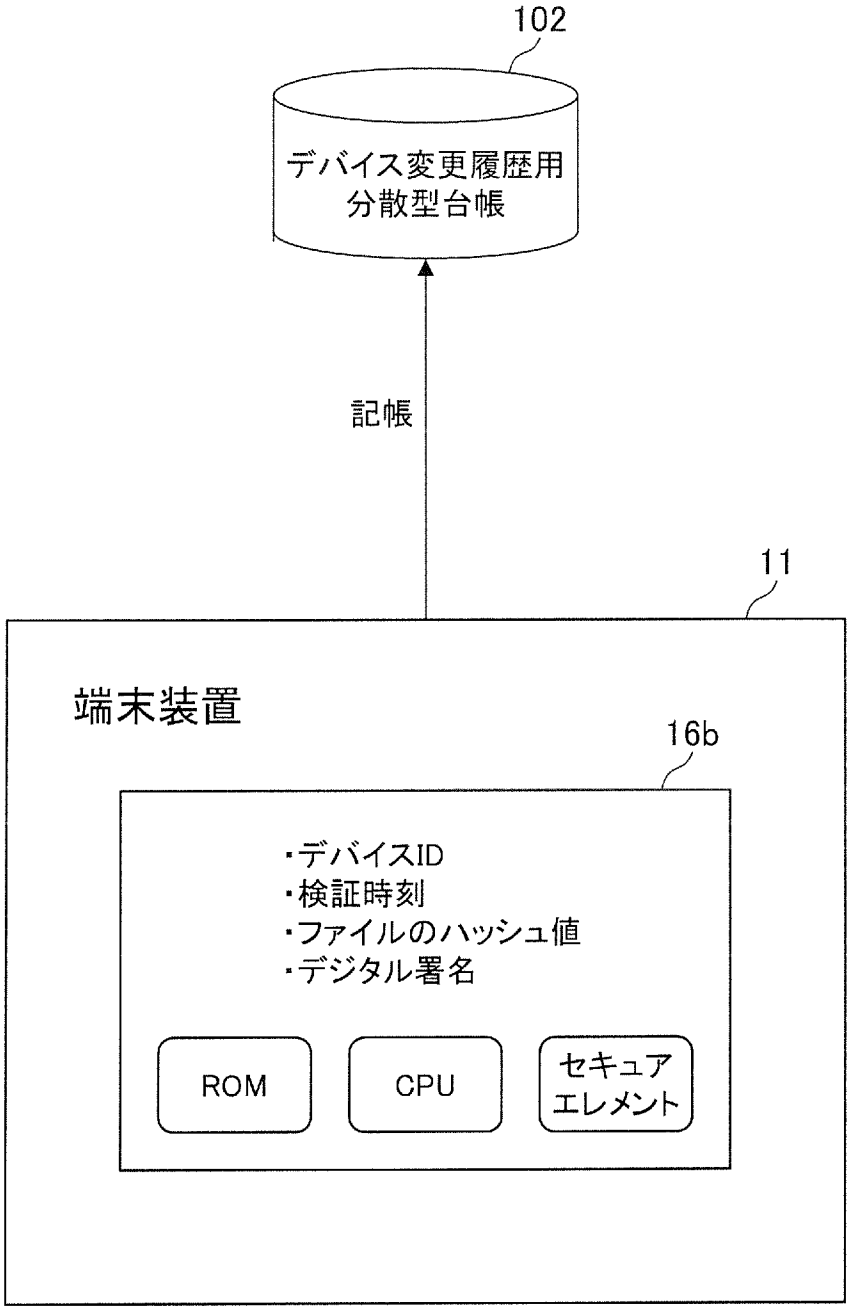
[図12]


101
デバイス製造時用
分散型台帳
記帳
11
端末装置
16a
・各部品の品番
・工程ライン
・工程時刻
CPU
メモリ
基板

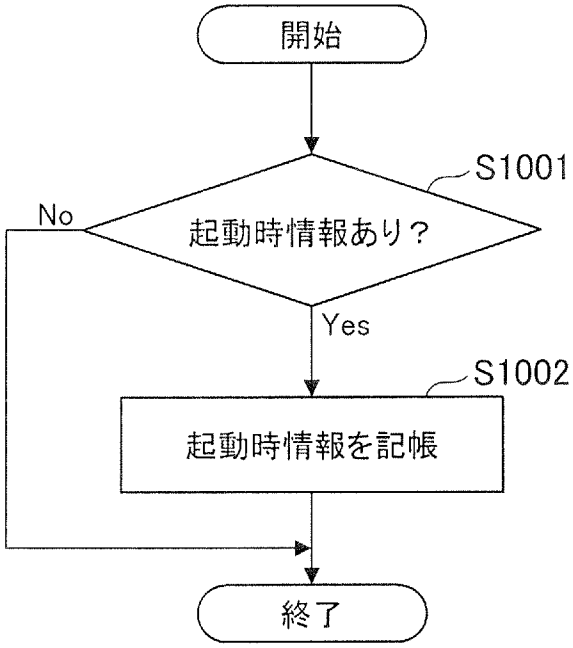
[図13]



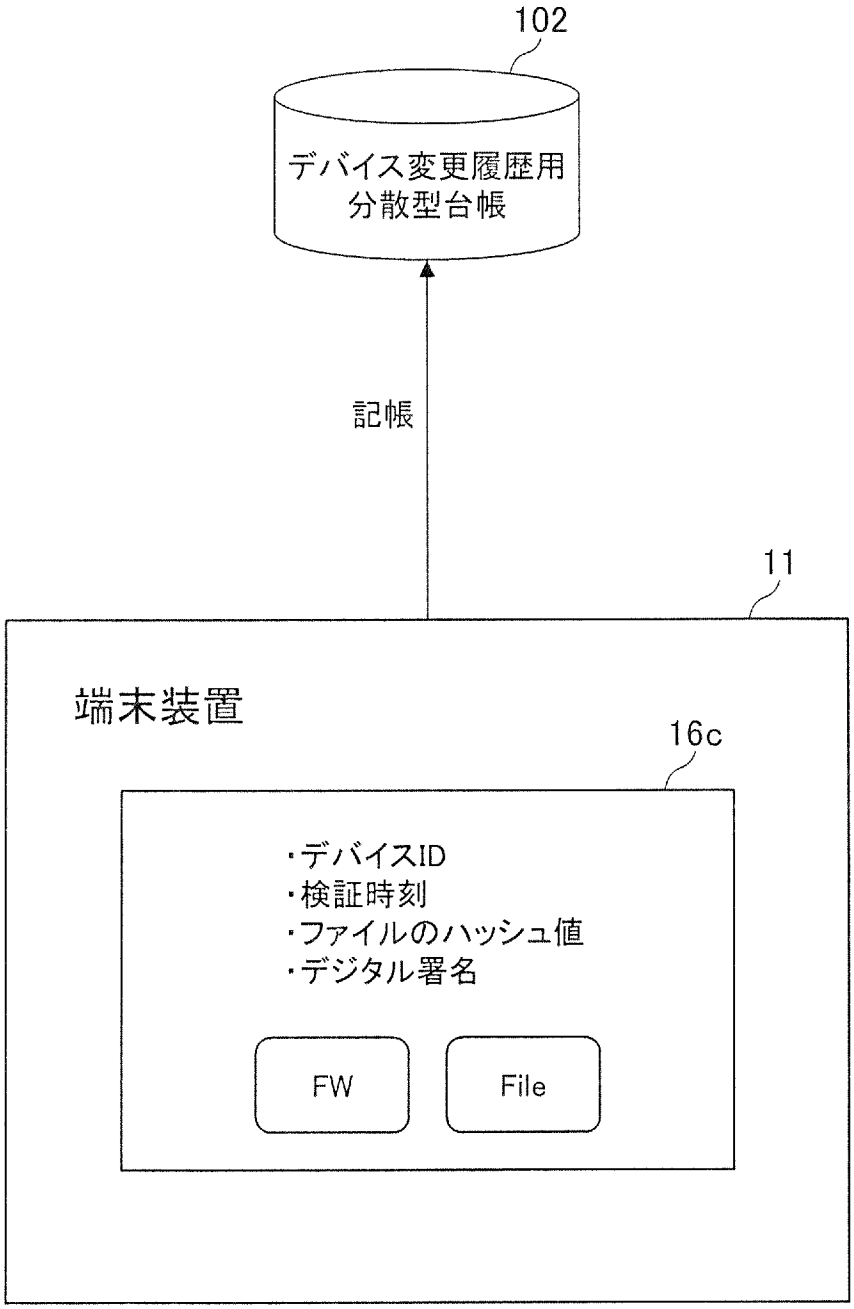
[図14]


102
デバイス変更履歴用
分散型台帳
記帳
11
端末装置
16b
・デバイスID
・検証時刻
・ファイルのハッシュ値
・デジタル署名
ROM
CPU
セキュア
エレメント

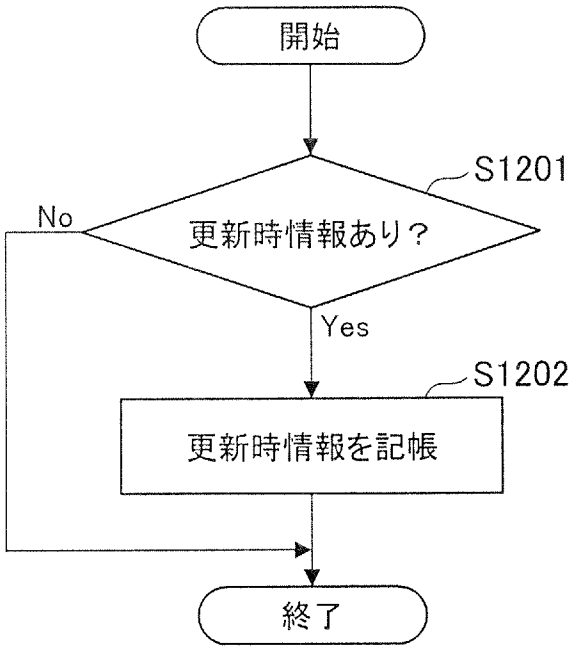
[図15]



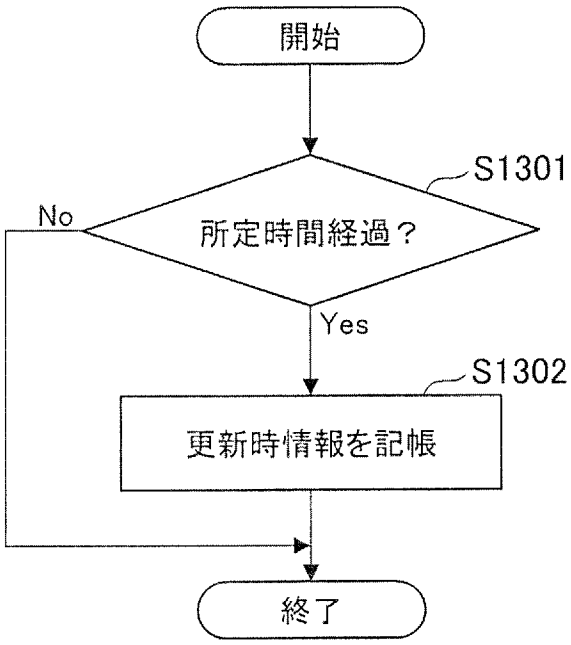
[図16]


102
デバイス変更履歴用
分散型台帳
記帳
11
端末装置
16c
・デバイスID
・検証時刻
・ファイルのハッシュ値
・デジタル署名
FW
File

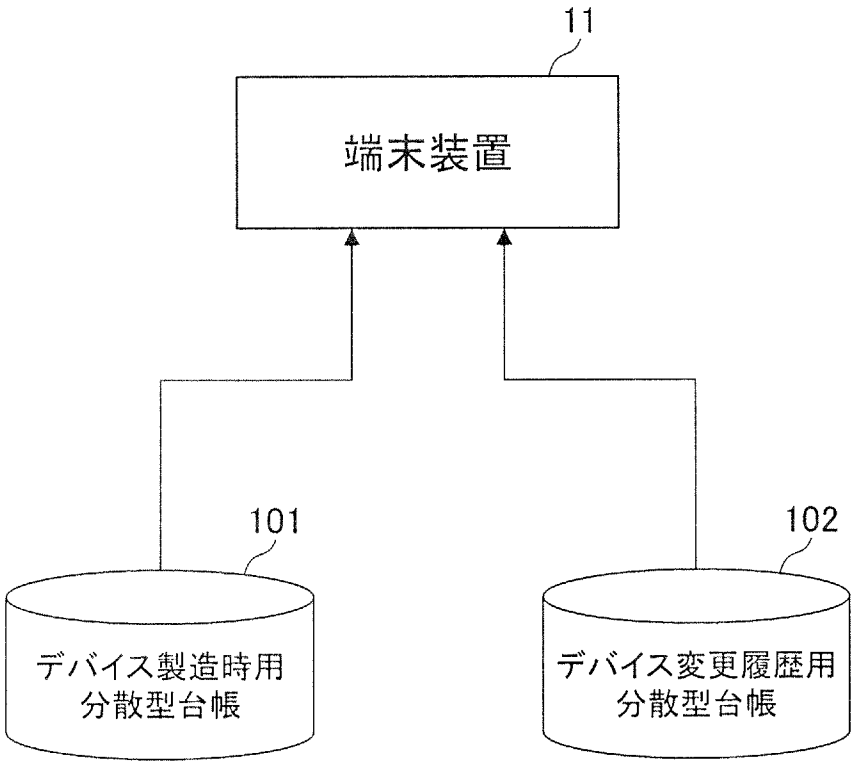
[図17]


開始
S1201
No
更新時情報あり？
Yes
S1202
更新時情報を記帳
終了

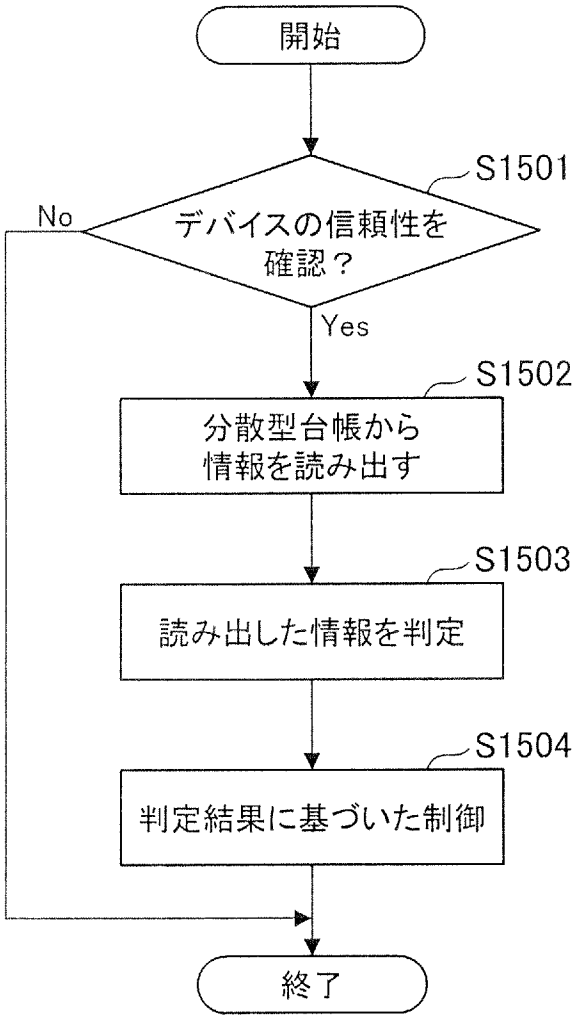
[図18]


開始
S1301
No
所定時間経過？
Yes
S1302
更新時情報を記帳
終了

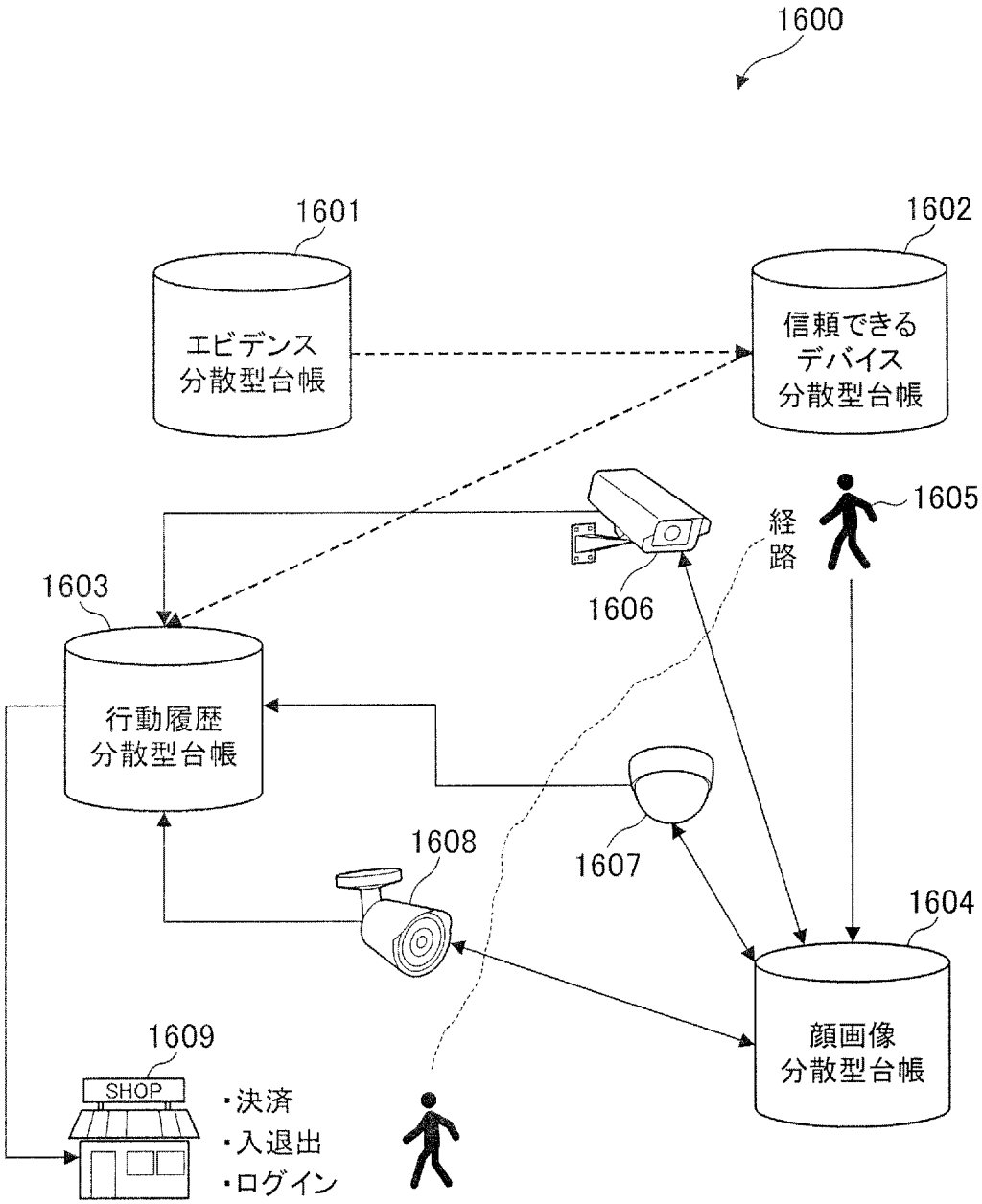
[図19]



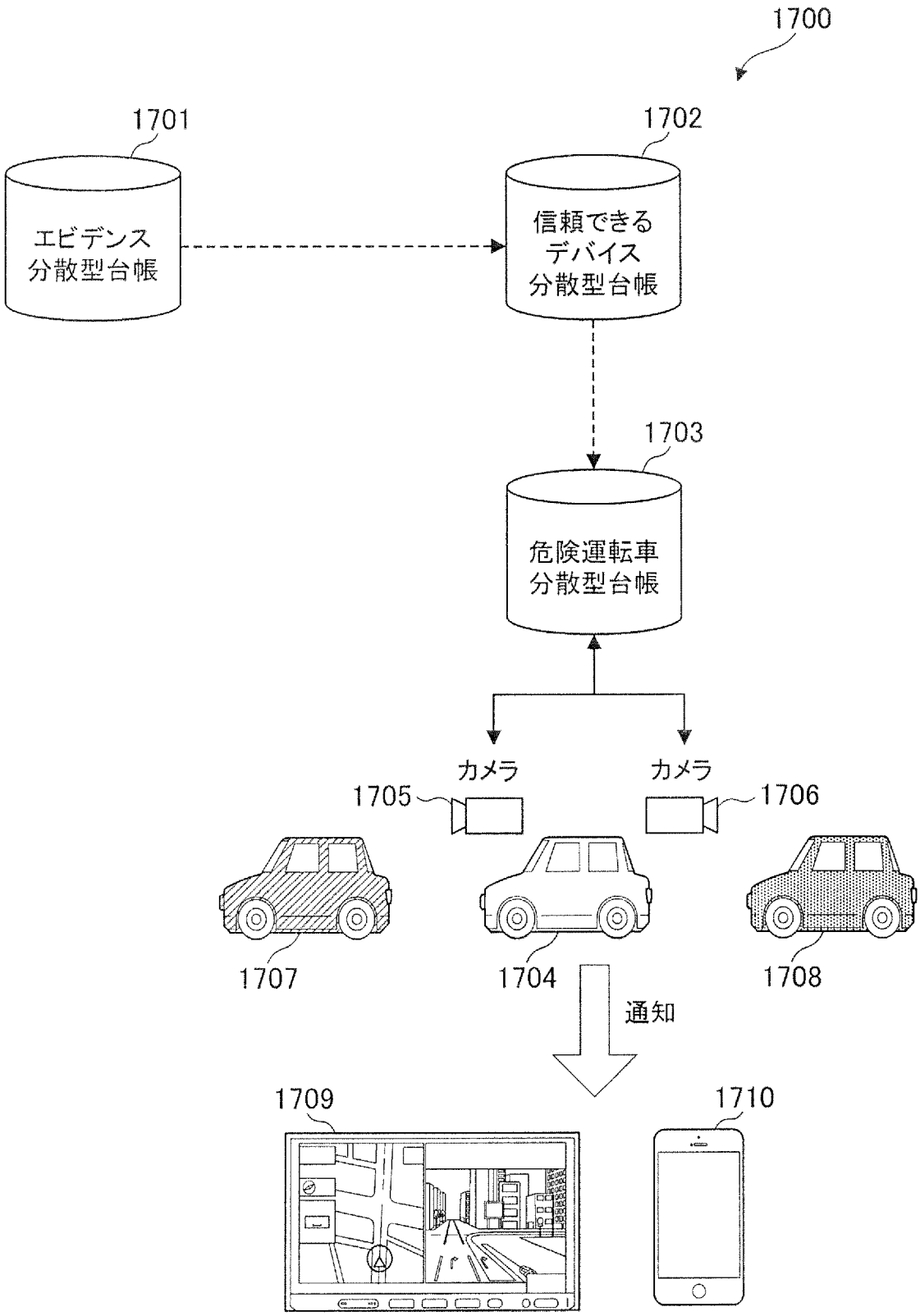
[図20]


開始
S1501
デバイスの信頼性を確認？
No
Yes
S1502
分散型台帳から情報を読み出す
S1503
読み出した情報を判定
S1504
判定結果に基づいた制御
終了

[図21]


1600
1601
エビデンス
分散型台帳
1602
信頼できる
デバイス
分散型台帳
1605
経路
1606
1603
行動履歴
分散型台帳
1607
1608
1604
顔画像
分散型台帳
1609
SHOP
・決済
・入退出
・ログイン

[図22]


1700
1701
エビデンス
分散型台帳
1702
信頼できる
デバイス
分散型台帳
1703
危険運転車
分散型台帳
カメラ
カメラ
1705
1706
1707
1704
1708
通知
1709
1710

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2020/038838

A. CLASSIFICATION OF SUBJECT MATTER
H01L 21/02(2006.01)i
FI: H01L21/02 Z

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)
H01L21/02

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

Published examined utility model applications of Japan	1922-1996
Published unexamined utility model applications of Japan	1971-2020
Registered utility model specifications of Japan	1996-2020
Published registered utility model applications of Japan	1994-2020

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.
X	JP 2012-532466 A (CERTICOM CORP.) 13 December 2012 (2012-12-13) paragraphs [0014]-[0020], [0040]-[0041], [0092]-[0093], [0127]-[0130], [0160]-[0167], [0395]-[0400]	1-12, 15
Y	paragraphs [0014]-[0020], [0040]-[0041], [0092]-[0093], [0127]-[0130], [0160]-[0167], [0395]-[0400]	13-14
Y	JP 2011-108225 A (INTEL CORPORATION) 02 June 2011 (2011-06-02) paragraphs [0005]-[0011], [0032]-[0059]	13-14

☐ 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
23 December 2020 (23.12.2020)	12 January 2021 (12.01.2021)

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
Information on patent family members

International application No.
PCT/JP2020/038838

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
JP 2012-532466 A	13 Dec. 2012	US 2011/0063093 A1 paragraphs [0084]-[0090], [0110]-[0111], [0160]-[0161], [0195]-[0198], [0228]-[0233], [0454]-[0459] WO 2011/003201 A1 CN 102696045 A	
JP 2011-108225 A	02 Jun. 2011	US 2011/0121065 A1 paragraphs [0012]-[0018], [0039], [0071] CN 102073897 A	

国際調査報告

国際出願番号
PCT/JP2020/038838

A. 発明の属する分野の分類（国際特許分類（ＩＰＣ））

H01L 21/02(2006.01)i
FI: H01L21/02 Z

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））

H01L21/02

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	１９７１－２０２０年
日本国実用新案登録公報	１９９６－２０２０年
日本国登録実用新案公報	１９９４－２０２０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
X	JP 2012-532466 A (サーティコム コーポレーション) 13.12.2012 (2012-12-13) 段落[0014]-[0020], [0040]-[0041], [0092]-[0093], [0127]-[0130], [0160]-[0167], [0395]-[0400]	1-12, 15
Y	段落[0014]-[0020], [0040]-[0041], [0092]-[0093], [0127]-[0130], [0160]-[0167], [0395]-[0400]	13-14
Y	JP 2011-108225 A (インテル・コーポレーション) 02.06.2011 (2011-06-02) 段落[0005]-[0011], [0032]-[0059]	13-14

☐ 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抵触するものではなく、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
23.12.2020	12.01.2021

名称及びあて先
日本国特許庁(ISA/JP)
〒100-8915
日本国
東京都千代田区霞が関三丁目４番３号

権限のある職員（特許庁審査官）
平野　崇 5F 3657
電話番号 03-3581-1101 内線 3516

国際調査報告
パテントファミリーに関する情報

国際出願番号
PCT/JP2020/038838

引用文献	公表日	パテントファミリー文献	公表日
JP 2012-532466 A	13.12.2012	US 2011/0063093 A1 段落[0084]-[0090], [0110]-[0111], [0160]-[0161], [0195]-[0198], [0228]-[0233], [0454]-[0459] WO 2011/003201 A1 CN 102696045 A	
JP 2011-108225 A	02.06.2011	US 2011/0121065 A1 段落[0012]-[0018], [0039]-[0071] CN 102073897 A	