(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
2007 年3 月1 日 (01.03.2007)

PCT

(10) 国際公開番号
WO 2007/023657 A1

(51) 国際特許分類:
G08G 1/00 (2006.01) *G06F 21/24* (2006.01)
G06F 3/06 (2006.01)

(21) 国際出願番号: PCT/JP2006/315427

(22) 国際出願日: 2006 年8 月3 日 (03.08.2006)

(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2005-246253 2005 年8 月26 日 (26.08.2005) JP

(71) 出願人 (米国を除く全ての指定国について): 三菱電機株式会社 (MITSUBISHI ELECTRIC CORPORATION) [JP/JP]; 〒1008310 東京都千代田区丸の内二丁目７番３号 Tokyo (JP).

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 泉 幸雄 (IZUMI, Yukio) [JP/JP]; 〒1008310 東京都千代田区丸の内二丁目７番３号 三菱電機株式会社内 Tokyo (JP). 山田 敬喜 (YAMADA, Keiki) [JP/JP]; 〒1008310 東京都千代田区丸の内二丁目７番３号 三菱電機株式会社内 Tokyo (JP).

(74) 代理人: 溝井 章司, 外(MIZOI, Shoji et al.); 〒2470056 神奈川県鎌倉市大船二丁目１７番１０号ＮＴＡ大船ビル３階 溝井国際特許事務所 Kanagawa (JP).

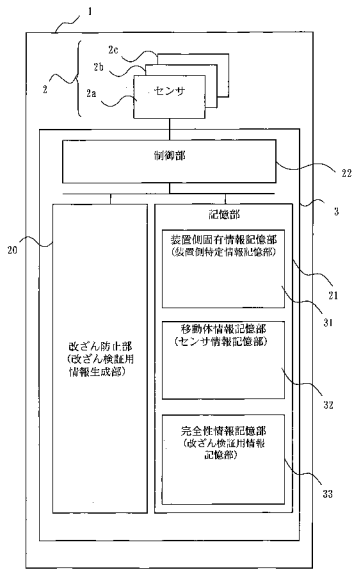
(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SY, 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, LS, MW, MZ, NA, SD,

/続葉有/

(54) **Title:** INFORMATION STORAGE DEVICE, INFORMATION STORAGE PROGRAM, VERIFICATION DEVICE AND INFORMATION STORAGE METHOD

(54) **発明の名称:** 情報記憶装置及び情報記憶プログラム及び検証装置及び情報記憶方法



1 MOBILE BODY
2a SENSOR
22 CONTROL SECTION
3 MOBILE BODY INFORMATION STORAGE DEVICE (INFORMATION STORAGE DEVICE)
21 STORAGE SECTION
20 FALSIFICATION PREVENTING SECTION (FALSIFICATION VERIFYING INFORMATION GENERATING SECTION)
31 UNIQUE INFORMATION STORAGE SECTION ON DEVICE SIDE (SPECIFYING INFORMATION STORAGE SECTION ON DEVICE SIDE)
32 MOBILE BODY INFORMATION STORAGE SECTION (SENSOR INFORMATION STORAGE SECTION)
33 INTEGRITY INFORMATION STORAGE SECTION (FALSIFICATION VERIFYING INFORMATION STORAGE SECTION)

(57) **Abstract:** Provided is an information storage device wherein highly reliable information can be recorded. The mobile body information storage device (3) is an information storage device equipped in a mobile body (1). The information storage device is provided with a mobile body information storage section (32) for storing mobile body information based on the information detected by a sensor which detects information relating to the mobile body (1); a falsification preventing section (20), which acquires specifying information for specifying the mobile body (1), and generates integrity information to be used for verifying whether at least either specifying information or the mobile information is falsified, based on the acquired specifying information and the mobile body information stored in the mobile body information storage section (32); and an integrity information storage section (33) for storing integrity information generated by the falsification preventing section (20).

(57) **要約:** 信頼性の高い情報を記録できる情報記憶装置を提供する。移動体情報記憶装置３は、移動体１に装備される情報記憶装置であり、移動体１に関する情報を検出するセンサが検出した情報に基づく移動体情報を記憶する移動体情報記憶部３２と、移動体１を特定可能な特定情報を取得し、取得した前記特定情報と前記移動体情報記憶部３２が記憶した前記移動体情報とに基づき、前記特定情報と移動体情報との少なくともいずれかに対する改ざんの有無を検証するために使用する完全性情報を生成する改ざん防止部２０と、改ざん防止部２０が生成した完全性情報を記憶する完全性情記憶部３３とを備えた。

WO 2007/023657 A1

SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書

２文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

明 細 書

情報記憶装置及び情報記憶プログラム及び検証装置及び情報記憶方法

技術分野

[0001] この発明は、センサが検出した情報を収集して記憶する報記憶装置、情報記憶プログラム、情報記憶方法及び前記情報の正当性を検証する検証装置に関する。

[0002] この発明は、例えば、移動体の移動状態に関わる移動体情報を収集して記憶する情報記憶装置に関する。

[0003] また、この発明は、例えば食料品(野菜、魚、ワインなど)、動物(競走馬や闘犬など)、割れ物、薬品、写真、芸術品、骨董品、公的書類(紙での書類や遺書など)、ゴミなどの物の運搬環境や保管環境に関わる情報、例えば温度、湿度、照度、時間、位置、ゆれ、重量、傾斜、圧力、音、風力、不純物度、扉や蓋の開閉などの環境情報を収集して記憶する環境情報記憶装置や、これらの情報を処理する環境情報保証システムに関する。

背景技術

[0004] (1)自動車税の税額は、従来、自動車の種類、用途、排気量などにより決められている。近年では、自動車税の税額は、排出ガスや燃費の性能に応じて変わる。これらは運転状況により決定されるものではなく、使用している自動車の仕様によって決定されていると言える。例えば、燃費性能が良い自動車であれば、急発進や急停止などの乱暴な運転をする運転者であっても税金は優遇されることになる。

(2)また、自動車保険も、自動車の種類や用途、運転者の年齢、過去の事故歴、走行距離などから決定される。この自動車保険も、乱暴な運転する者であっても、事故を起こしていない運転者であれば、保険料が安くなり、実際に運転者がどのような運転を行っているかという運転状況に見合った保険料の算出方法ではない。

[0005] これらを解決するために、いくつかの発明がある。

[0006] 特開2004－145489号公報(特許文献1)は、自動車保険料決定方法に関わるシステムを開示していいる。前記特許文献1が開示するシステムは、タイヤ空気圧等の管理をこまめに行っているような安全性が高い自動車及び所有者は事故を起こす可

能性が低いとみなし、保険料を減額する。すなわち、自動車のタイヤ空気圧に関する時系列的情報を取得する車輌状況解析部と、この車輌状況解析部が取得した情報を外部へ送信する通信装置とを備えた車載装置と、受信した情報に基づいて当該自動車のタイヤ空気圧管理状況を評価する車輌管理状態診断部と、この車輌管理状態診断部による評価結果に基づいて自動車保険の保険料及び／又は保険金を算出する保険料算出部とを備えた中央装置とからなるシステムである。これによって、タイヤ空気圧などの情報が、インタネットを介して保険事業者のサーバに送信され、受信した情報を基に車両管理状態を診断し、事故を起こす可能性が低い自動車の所有者に対して、保険料を減額するなど保険料が算出される。

[0007] また、特開2002－279298号公報（特許文献2）は、車両履歴情報に基づくビジネス手法として、車両の運転歴や維持管理履歴などの車両履歴情報を個人情報と共に車両に設けられた記憶媒体に記録し、車検・メンテナンス時や保険契約・更新時にこれらの情報を用いて料金を設定する手法を開示している。この中には、各種センサ情報を車載管理コンピュータによって処理された自動車の運転歴に対するユーザ側の改ざんを不能にするというデータ保護機能を有する記憶媒体を使用している例が記述されている。

[0008] また、特開2002－183456号公報（特許文献3）は、取得した自動車の走行状態情報やGPS（Global Positioning System）による位置情報、地図情報、交通規制情報を基に運転評価結果を演算して、演算結果を記録する運転評価装置において、保険会社以外の人間に記録内容を解読されるのを防ぐために、すなわち、記録内容の機密性を維持するために、暗号化もしくはパスワードによって保護している例を開示している。

[0009] しかし、従来のシステムでは、自動車の所有者が車載装置を改良し、偽の情報を保険事業者に送信することができる。すなわち、実際にはタイヤ空気圧等の管理をしていないにもかかわらず、こまめに行っているように見せかけたり、他の自動車の情報を送信したりして、安い保険料を得ることが可能であるという問題点があった。

[0010] さらに、通信中の情報が改ざんされる、すなわち情報の完全性を維持できない恐れがあり、保険会社などが実際に使用する情報を信頼できないという信頼性が欠けると

いう問題点があった。

[0011] また、通信中の情報が改ざんされた場合や、車載装置内に記録している情報が改ざんされた場合、保険会社などは受信した情報が改ざんされていることを検知することができないという問題があった。これは、情報を暗号化する・しないに問わず発生する問題である。すなわち、暗号化によって情報の機密性は維持できるが、改ざんされたことは検知できない、つまり完全性を維持できないからである。

[0012] (3)また、従来、物の運搬や保管を依頼した依頼者(以下、依頼者と記す)は、運搬や保管を実施する業者(以下、業者と記す)を信頼し、運搬や保管を依頼していた。例えば、魚市場から新鮮な魚を市場に運搬する場合、魚市場で運搬を依頼した依頼者は、運搬中の魚の環境、すなわち温度や湿度などが新鮮な状態に保たれているか知ることが出来なかった。また、魚を使用する料理店などの物を受け取る人(以下、使用者と記す)も運搬された魚の鮮度状態を確認することはできず、経験に基づく目視による確認によって、鮮度状態を把握していた。

また、貸し倉庫に物を保管する場合、使用者(依頼者と同じ場合もある)は、入・出庫する際の保管物の検量や状態等の比較することで、保管中の物の状態を推測していた。

[0013] さらに、保冷車の運行管理装置に関する特開平11－348647号公報では、保冷庫内の温度センサが検出した温度情報を車両から事務所に送信・管理することで、運転者の負荷を減らす発明が記述されており、温度センサの情報を車両に設けられたメモリカードに記録し、後で運転中の記録証明が可能であるとの記述がある。

[0014] 従来技術では、依頼者や使用者が、運搬中や保管中の環境に関しては、業者を信用するしか方法がなく、その運搬環境や保管環境を確認することは困難であった。また、メモリカードなど記録媒体に記録された環境の情報を業者が改ざんし、改ざんされた業者に都合の良い偽の情報を依頼者や使用者に提出し、問題なく見せかけることが可能であるという課題があった。

特許文献1:特開2004－145489号公報

特許文献2:特開2002－279298号公報

特許文献3:特開2002－183456号公報

特許文献4:特開2002－7718号公報

特許文献5:特開2002－373258号公報

特許文献6:特開2002－297910号公報

特許文献7:特開平11－348647号公報

発明の開示

発明が解決しようとする課題

[0015] この発明は、信頼性の高い移動体の移動体情報を記録できる移動体情報記憶装置を提供することを目的とする。また、保険、税金、交通違反などに関するサービスを利用者に提供するサービス提供者が、移動体情報記憶装置が記録した移動体情報を安心して利用でき、これらの移動体情報が改ざんされたことをサービス提供者が検知できる移動体情報検証装置、システムを提供することを目的とする。

[0016] さらに、この発明は、運搬中や保管中の物の環境に関する情報を記録でき、依頼者や利用者がその情報を確認できる信頼性の高い環境情報記憶装置や環境情報保証システ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

[0017] 本発明の情報記憶装置は、

移動体に装備され、前記移動体に関する情報を記憶する情報記憶装置において、

前記移動体に関する情報を検出するセンサが検出した情報に基づくセンサ情報を記憶するセンサ情報記憶部と、

前記移動体を特定可能な特定情報を取得し、取得した前記特定情報と前記センサ情報記憶部が記憶した前記センサ情報とに基づいて、前記特定情報と前記センサ情報との少なくともいずれかに対する改ざんの有無を検証するために使用する改ざん検証用情報を生成する改ざん検証用情報生成部と、

前記改ざん検証用情報生成部が生成した前記改ざん検証用情報を記憶する改ざん検証用情報記憶部と

を備えたことを特徴とする。

[0018] 前記情報記憶装置は、さらに、

前記特定情報を装置側特定情報として記憶する装置側特定情報記憶部を備え、

前記改ざん検証用情報生成部は、

前記装置側特定情報記憶部が記憶した前記装置側特定情報を取得することを特徴とする。

[0019] 前記移動体は、

前記特定情報を移動体側特定情報として記憶する移動体側特定情報記憶部を備え、

前記改ざん検証用情報生成部は、

前記移動体側特定情報記憶部が記憶した前記移動体側特定情報を取得することを特徴とする。

[0020] 前記情報記憶装置は、さらに、

自己と前記移動体とが分離しているかどうかを検出する分離検出部を備えたことを特徴とする。

[0021] 前記情報記憶装置は、さらに、

自己が装備された前記移動体である前記装備移動体が、予め装備されることが指定された指定移動体かどうかを判断する移動体判断部を備えたこと特徴とする。

[0022] 前記情報記憶装置は、さらに、

前記移動体判断部が前記装備移動体は前記指定移動体ではないと判断した場合に、前記センサ情報記憶部が記憶した前記センサ情報を消去する情報消去部を備えたことを特徴とする。

[0023] 前記装備移動体は、

移動体である自己を特定可能な移動体側特定情報を記憶する移動体側特定情報記憶部を備え、

前記情報記憶装置は、さらに、

前記指定移動体を特定可能な装置側特定情報を記憶する装置側特定情報記憶部を備え、

前記移動体判断部は、

前記装置側特定情報記憶部が記憶した前記装置側特定情報と前記移動体側特定情報記憶部が記憶した前記移動体側特定情報とを入力し、入力した前記装置側

特定情報と前記移動体側特定情報とに基づいて、前記装備移動体が前記指定移動体かどうかを判断することを特徴とする。

[0024] 前記改ざん検証用情報生成部は、

前記移動体判断部が前記装備移動体を前記指定移動体と判断した場合に、前記移動体判断部が入力した前記装置側特定情報と前記移動体側特定情報とのうちのいずれかを選択対象として選択して取得し、取得した前記選択対象と前記センサ情報記憶部が記憶した前記センサ情報とに基づいて、前記選択対象と前記センサ情報との少なくともいずれかに対する改ざんの有無を検証するために使用する改ざん検証用情報を生成することを特徴とする。

[0025] 前記装備移動体は、

通信により認証要求を受け付けて、予め設定された規則に基いて認証処理を実行する移動体側認証実行部を備え、

前記移動体判断部は、

前記移動体側認証実行部に前記認証要求を送信し、前記予め設定された規則に基いて前記移動体側認証実行部との間で認証処理を実行することにより、前記装備移動体が前記指定移動体かどうかを判断することを特徴とする。

[0026] 前記情報記憶装置は、さらに、

前記センサが正当かどうかを確認するセンサ確認部を備えたことを特徴とする。

[0027] この発明の情報記憶装置は、

移動体に装備され、前記移動体に関する情報を記憶する情報記憶装置において、

前記移動体に関する情報を検出する複数のセンサのそれぞれが検出したそれぞれの情報に基づくぞれぞれのセンサ情報を入力し、予め設定された条件に基づいて前記それぞれのセンサ情報のうちから少なくとも一つのセンサ情報を選択する選択部と、

前記選択部が選択したセンサ情報から構成されるグループを示す選択情報群を記憶する選択情報群記憶部と、

前記移動体を特定可能な特定情報を取得し、取得した前記特定情報と前記選択情報群記憶部が記憶した前記選択情報群とに基づいて、前記特定情報と前記選択

情報群に含まれる前記センサ情報との少なくともいずれかに対する改ざんの有無を検証するために使用する改ざん検証用情報を生成する改ざん検証用情報生成部と、

前記改ざん検証用情報生成部が生成した前記改ざん検証用情報を記憶する改ざん検証用情報記憶部と

を備えたことを特徴とする。

[0028] この発明の情報記憶装置は、

移動体に装備され、前記移動体に関する情報を記憶する情報記憶装置において、

前記移動体に関する情報を検出する複数のセンサのそれぞれが検出したそれぞれの情報に基づくそれぞれのセンサ情報を記憶するセンサ情報記憶部と、

予め設定された条件に基づいて、前記センサ情報記憶部が記憶した前記それぞれのセンサ情報のうちから少なくとも一つのセンサ情報を選択する選択部と、

前記移動体を特定可能な特定情報を取得し、取得した前記特定情報と前記選択部が選択したセンサ情報から構成されるグループを示す前記選択情報群とに基づいて、前記特定情報と前記選択情報群に含まれる前記センサ情報との少なくともいずれかに対する改ざんの有無を検証するために使用する改ざん検証用情報を生成する改ざん検証用情報生成部と、

前記改ざん検証用情報生成部が生成した前記改ざん検証用情報を記憶する改ざん検証用情報記憶部と

を備えたことを特徴とする。

[0029] 前記情報記憶装置は、さらに、

前記センサ情報を入力し、入力した前記センサ情報が予め設定された条件に合致するかどうかを判定し、前記条件に合致すると判定した場合に、入力した前記センサ情報を前記

センサ情報記憶に記憶させる条件判定部を備えたことを特徴とする。

[0030] 前記情報記憶装置は、さらに、

前記センサ情報記憶部が記憶した前記センサ情報と、前記改ざん検証用情報生成部が取得した前記特定情報と、前記改ざん検証用情報記憶部が記憶した前記改

ざん検証用情報とを出力する出力部を備えたことを特徴とする。

[0031] 前記出力部は、

前記センサ情報と前記特定情報と前記改ざん検証用情報とを出力する場合に、出力先が予め指定された指定装置かどうかを認証する出力先認証部を備えたことを特徴とする。

[0032] 前記出力部は、

情報を記憶可能であるとともに携帯が可能である携帯型記憶媒体に、前記センサ情報と前記特定情報と前記改ざん検証用情報とを出力することを特徴とする。

[0033] 前記出力部は、

予め設定された時間間隔で、前記センサ情報と前記特定情報と前記改ざん検証用情報とを出力することを特徴とする。

[0034] 前記情報記憶装置は、さらに、

操作者による操作を受け付け、受け付けた前記操作に基いて、前記出力部に対して出力を命じる命令部を備え、

前記出力部は、

前記命令部から出力を命じられた場合に、前記センサ情報と前記特定情報と前記改ざん検証用情報とを出力することを特徴とする。

[0035] 前記情報記憶装置は、さらに、

前記命令部が受け付けた前記操作者による前記操作に基づいて、前記操作者が正当であるかどうかを認証する操作者認証部を備え、

前記命令部は、

前記操作者認証部が前記操作者を正当と認証した場合に、前記出力部に対して出力を命じることを特徴とする。

[0036] この発明の情報記憶プログラムは、

移動体に装備され、前記移動体の情報を記憶するコンピュータである情報記憶装置に以下の処理を実行させることを特徴とする。

(1)前記移動体に関する情報を検出するセンサが検出した情報に基づくセンサ情報を記憶する処理

(2)前記移動体を特定可能な特定情報を取得し、取得した前記特定情報と記憶した前記センサ情報とに基づいて、前記特定情報と前記センサ情報との少なくともいずれかに対する改ざんの有無を検証するために使用する改ざん検証用情報を生成する処理

(3)生成した前記改ざん検証用情報を記憶する処理

[0037] この発明の情報記憶装置は、

情報を検出するセンサから前記センサが検出した情報を入力する情報入力部と、

前記情報入力部が前記センサから入力した情報に基づくセンサ情報を記憶するセンサ情報記憶部と、

前記センサ情報記憶部が記憶した前記センサ情報に基づいて、前記センサ情報に対する改ざんの有無を検証するために使用する改ざん検証用情報を生成する改ざん検証用情報生成部と、

前記改ざん検証用情報生成部が生成した前記改ざん検証用情報を記憶する改ざん検証用情報記憶部と

を備えたことを特徴とする。

[0038] 前記情報記憶装置は、さらに、

所定の情報を記憶する装置側特定情報記憶部を備え、

前記改ざん検証用情報生成部は、

前記センサ情報記憶部が記憶した前記センサ情報と前記装置側特定情報記憶部が記憶した前記所定の情報とに基づいて、前記所定の情報と前記センサ情報との少なくともいずれかに対する改ざんの有無を検証するために使用する改ざん検証用情報を生成することを特徴とする。

[0039] 前記センサは、

自己が配置されている環境に関する情報を検出し、

前記装置側特定情報記憶部は、

前記所定の情報として、前記センサが配置される前記環境と自己である前記環境情報記憶装置が配置される場所との少なくともいずれかを特定可能な特定情報を記憶することを特徴とする。

[0040] 前記情報記憶装置は、さらに、

前記センサが配置されている環境に所定の物が継続して置かれているかどうかを検出する存在検出部を備え、

前記改ざん検証用情報生成部は、

前記センサ情報記憶部が記憶した前記センサ情報と前記存在検出部が検出した検出結果とに基づいて、前記センサ情報と前記検出結果との少なくともいずれかに対する改ざんの有無を検証するために使用する改ざん検証用情報を生成することを特徴とする。

[0041] 前記情報記憶装置は、さらに、

前記センサ情報記憶部が記憶した前記センサ情報と、前記装置側特定情報記憶部が記憶した前記所定の情報と、前記改ざん検証用情報記憶部が記憶した前記改ざん検証用情報とを他の装置に出力する出力部を備えたことを特徴とする。

[0042] 前記出力部は、

前記センサ情報と前記所定の情報と前記改ざん検証用情報とを出力する場合に、前記他の装置を認証する出力先認証部を備えたことを特徴とする。

[0043] 前記情報記憶装置は、さらに、

前記センサが正当かどうかを確認するセンサ確認部を備えたことを特徴とする。

[0044] 前記情報記憶装置は、

所定の情報を格納する格納機器から前記所定の情報を入力する外部インタフェース部と、

前記外部インタフェース部が前記格納機器から前記所定の情報を入力する場合に前記格納機器との間で通信を行うことにより前記格納機器が正当であるかどうかを認証し、正当と判断した場合に、前記所定の情報を前記装置側特定情報記憶部に記憶する格納制御部と

を備えたことを特徴とする。

[0045] 前記情報記憶装置は、

所定の情報を格納する格納機器から前記所定の情報を入力する外部インタフェース部と、

前記外部インタフェース部が入力した前記所定の情報が正当であるかどうかを認証し、正当と判断した場合に、前記所定の情報を前記装置側特定情報記憶部に記憶する格納制御部と

を備えたことを特徴とする。

[0046] この発明の検証装置は、

情報を検出するセンサから前記センサが検出した情報を入力する情報入力部と、

前記情報入力部が前記センサから入力した情報に基づくセンサ情報を記憶するセンサ情報記憶部と、

前記センサ情報記憶部が記憶した前記センサ情報に基づいて、前記センサ情報に対する改ざんの有無を検証するために使用する改ざん検証用情報を生成する改ざん検証用情報生成部と、

前記改ざん検証用情報生成部が生成した前記改ざん検証用情報を記憶する改ざん検証用情報記憶部と、

前記センサ情報記憶部が記憶した前記センサ情報と、前記改ざん検証用情報記憶部が記憶した前記改ざん検証用情報とを出力する出力部とを備えた情報記憶装置から、

前記情報記憶装置が出力した前記センサ情報と前記改ざん検証用情報とを入力し、入力した前記センサ情報と前記改ざん検証用情報とを用いることにより前記センサ情報の正当性を検証する検証部を備えたことを特徴とする。

[0047] この発明の情報記憶方法は、

コンピュータである情報記憶装置が行なう情報記憶方法において、

情報入力部が、情報を検出するセンサから前記センサが検出した情報を入力し、

センサ情報記憶部が、前記情報入力部が前記センサから入力した情報に基づくセンサ情報を記憶し、

改ざん検証用情報生成部が、前記センサ情報記憶部が記憶した前記センサ情報に基づいて、前記センサ情報に対する改ざんの有無を検証するために使用する改ざん検証用情報を生成し、

改ざん検証用情報記憶部が、前記改ざん検証用情報生成部が生成した前記改ざ

ん検証用情報を記憶することを特徴とする。

[0048] この発明の情報記憶プログラムは、

以下の処理をコンピュータに実行させることを特徴とする。

(1)情報を検出するセンサから前記センサが検出した情報を入力する処理

(2)前記センサから入力した情報に基づくセンサ情報を記憶する処理

(3)記憶した前記センサ情報に基づいて、前記センサ情報に対する改ざんの有無を検証するために使用する改ざん検証用情報を生成する処理

(4)生成した前記改ざん検証用情報を記憶する処理

発明の効果

[0049] 本発明により、移動体との関連性が明確であり、かつ、改ざんに対して信頼性の高い移動体情報を記録できる移動体情報記憶装置を提供することができる。

発明を実施するための最良の形態

[0050] 実施の形態1.

図1～図4を参照して、実施の形態1を説明する。実施の形態1は、センサが検出した移動体に関する情報である移動体情報(センサ情報)を記憶する移動体情報記憶装置(情報記憶装置)に関する。ここで、「移動体情報」とは、自動車、バイク、船、飛行機、遊具(例えば、ジェットコースター(登録商標))などの移動体ついての、速度、距離、エンジン回転数、GPS(GPS位置)、ジャイロ、タイヤ空気圧、車間距離、ゆれ、ステアリング(舵角)、加速度、上昇度、アクセルの空ぶかし、蛇行運転の長さや時間、急ブレーキの回数、急発進の回数、運転者のいねむり状況、ブレーキ踏み圧、シートベルト装着などの移動状況や移動状態に関わる情報をいう。

[0051] 図1は、実施の形態1の移動体情報記憶装置3の使用状態の一例を示す図である。移動体情報記憶装置3は、例えば、自動車のような移動体に装備される。以下では、移動体情報記憶装置3が装備される移動体を「装備移動体」と呼ぶ場合がある。また、移動体情報記憶装置3は、あらかじめ、装備されるべき移動体が指定されている。移動体情報記憶装置3が、あらかじめ装備されることが指定された移動体を「指定移動体」と呼ぶ場合がある。

[0052] (1)移動体情報記憶装置3は、図1のように装備移動体である移動体1に装備されて

いる。

(2)移動体情報記憶装置3は、複数のセンサから構成されるセンサ群2の各センサが検出した各移動体情報を入力して記憶する。後述のようにセンサ群2はセンサ2a，センサ2b，センサ2c等から構成される。

(3)移動体情報記憶装置3は、記憶した移動体情報と後述の固有情報とに基づき、後述の「完全性情報」を生成し、「完全性情報」と「移動体情報」と「固有情報」とを、例えば公衆回線を介して、保険会社のサービスセンターに配置された移動体情報検証装置600に送信する。

(4)移動体情報検証装置600は、受信した「完全性情報」に基づき、「移動体情報」の正当性を検証する。

[0053] 図2は、実施の形態1の移動体情報記憶装置3の構成ブロック図である。図2は、移動体1に装備された状態を示している。移動体情報記憶装置3は、センサ2a～センサ2cから移動体情報を入力する。

[0054] 図2において、移動体1は、自動車、バイク、船、飛行機、遊具(例えば、ジェットコースター(登録商標)や観覧車)など、人が乗車可能である。

[0055] センサ2a等は、移動体1に設置されており、移動体1の速度、走行距離、エンジン回転数、GPSを利用した位置、ジャイロ、タイヤや客室の空気圧、車間距離、ゆれ、高度、傾き、ステアリング(舵角)、温度、湿度など、移動状況や移動状態を示す「移動体情報」を検出する。なお、後述する実施の形態20では、移動体情報記憶装置3がセンサを内蔵する例を示している。

[0056] 本実施の形態1では、センサ2a等は、自身が検出した情報を演算し、演算結果を移動体情報として移動体情報記憶装置3に出力するもので構わない。このような演算結果で得られる移動体情報には、例えば、加速度、上昇度、アクセルの空ぶかし、蛇行運転の長さや時間、急ブレーキの回数、急発進の回数、車内外の映像情報などがある。

[0057] なお、センサ2a等が、自身の検出した情報を演算せず、移動体情報記憶装置3で演算する場合を実施の形態2に示す。後述する本実施の形態2では、移動体情報記憶装置3の装置側演算部201による演算結果を「移動体情報」として記憶しているが

、前記のようにセンサ自身が検出した情報も「移動体情報」である。このように、本明細書において、「移動体情報」とは、センサ自身が検出した情報、及びセンサ自身が検出した情報を処理した結果（演算結果）とのいずれをも含むものである。すなわち、「移動体情報」（センサ情報）とは、移動体に関する情報を検出するセンサが検出した情報に基づく情報である。ここで「基づく」とは、前記のように、センサ自身が検出した情報と、この情報を演算した結果の情報の両者を含む意味である。

[0058] 移動体情報記憶装置3（情報記憶装置）は、移動体情報を記憶する記憶部21と、制御部22と、改ざん防止部20（改ざん検証用情報生成部）とを備える。また、記憶部21は、装置側固有情報記憶部31（装置側特定情報記憶部）と、移動体情報記憶部32（センサ情報記憶部）と、完全性情報記憶部33（改ざん検証用情報記憶部）とを備える。図2では記憶部21が装置側固有情報記憶部31等をそなえるが、装置側固有情報記憶部31、移動体情報記憶部32等は、それぞれ独立して存在しても構わない。記憶部21は、例えば、ハードディスク、あるいはEEPROM（Electronically Erasable and Programmable Read Only Memory）、RAMなどの半導体メモリである。

[0059] 装置側固有情報記憶部31は、後述の「装置側固有情報」（装置側特定情報）を記憶する。移動体情報記憶部32は、「移動体情報」を記憶する。完全性情報記憶部33は、後述の「完全性情報」を記憶する。

[0060] 改ざん防止部20は、装置側固有情報記憶部31に格納されている「装置側固有情報」と、移動体情報記憶部32に記録されている「移動体情報」とに基いて、これらの情報の完全性を証明する「完全性情報」を生成する。

[0061] 制御部22は、これらの動作を制御する。

[0062] 次に、図3を参照して、移動体情報記憶装置3の動作について説明する。図3は、移動体情報記憶装置3の動作を説明するフローチャートである。

[0063] （1）移動体情報記憶装置3は、必要なタイミングから、センサ2a等が検出（S101）した移動体情報の記録を開始する。このタイミングは、例えば自動車やバイクなどであればエンジン始動、ジェットコースター（登録商標）などの遊具であれば電源がオンになった場合が考えられる。これらはサービス提供者によって決定される。

(2)制御部22には、接続しているすべてのセンサ2a等が検出した移動体情報が入力される。制御部22は、移動体情報を移動体情報記憶部32に記憶する(S102)。

(3)そして、必要なタイミングで、制御部22の命令により、改ざん防止部20は、装置側固有情報記憶部31に記憶されている「装置側固有情報」と、移動体情報記憶部32に記憶されている「移動体情報」とに基づいて、「完全性情報」を生成する(S103)。ここで「装置側固有情報」とは、移動体情報記憶装置3が予め装備されることが指定されている移動体である「指定移動体」を特定可能な情報である。「装置側固有情報」とは、具体的には、「指定移動体」が自動車とすれば、ナンバープレート情報や車体番号、製造番号など指定移動体を一意に区別できる情報である。

(4)また、「完全性情報」(改ざん検証用情報)とは、「移動体情報」と「装置側固有情報」とが改ざんされていないことを確認するための情報を意味する。すなわち、「完全性情報」は、「装置側固有情報」と「移動体情報」との少なくともいずれかに対する改ざんの有無を検証するために使用する情報である。例えば、デジタル署名がある。「完全性情報」の生成の具体例は、移動体情報検証装置600を備えるシステムである実施の形態6で詳しく述べる。

(5)生成された「完全性情報」は、必要に応じて制御部22により、完全性情報記憶部33に記憶される。制御部22は、「完全性情報」を記録する際、「完全性情報」と、その生成の基になった「移動体情報」との対応関係を管理してもよい。この対応関係を管理することによって、「移動体情報」と「完全性情報」との対応関係が明確になる(S104)。

(6)図4は、「移動体情報」と「完全性情報」の対応関係の管理例を示す。図4において、「移動体情報a」は「完全性情報a」と対応し、「移動体情報b」は「完全性情報b」と対応する。「移動体情報c」については、対応する「完全性情報c」が、まだ生成されていない状態を表している。このような管理により、「完全性情報」とその生成の基になった「移動体情報」の対応関係が明確になる。

(7)「完全性情報」の生成のタイミングは、本実施の形態1の適用先に依存するが、例えば、エンジン始動時に「完全性情報」が生成されていない「移動体情報」が移動体情報記憶部32にあった時や、「移動体情報」を移動体情報記憶装置3の外部に出力

する時、「移動体情報」が移動体情報記憶装置3に入力された時、移動体1に事故や不具合が発生した時などがある。

[0064] 以上のように、移動体情報記憶装置3内部において、改ざん防止部20が、「移動体情報」と「装置側固有情報」との完全性を証明する「完全性情報」を生成するので、移動体1と「移動体情報」との対応が明確になり、信頼性の高い「移動体情報」を記憶する移動体情報記憶装置3をサービス提供者に提供することができる。

[0065] 実施の形態2.

次に図5を参照して実施の形態2を説明する。実施の形態2は、制御部22が、センサ群2が検出した信号を演算する装置側演算部201を備えた場合である。

[0066] 装置側演算部201は、接続されているセンサ群2が検出した情報を演算する機能を有する。このような構成において、センサ群2が検出した情報を制御部22の装置側演算部201で演算し、演算結果を「移動体情報」として記憶部21に記憶する。

[0067] このような演算結果で得られる情報には、例えば、加速度、上昇度、アクセルの空ぶかし、蛇行運転の長さや時間、急ブレーキの回数、急発進の回数、車内外の映像情報などがある。

[0068] 例えば、速度センサの信号を演算することにより加速度をえることができる。このため、加速度センサは不要となる。よって、センサ群2が検出した信号を演算することによりセンサに代替する場合は、センサを追加する必要がなくなるという効果がある。

[0069] 実施の形態3.

次に、図6～図10を参照して、実施の形態3を説明する。実施の形態3は、移動体情報記憶装置3が、装備されることが予め指定されている指定移動体である移動体1に装備された場合、移動体1から分離することを防ぐ分離防止手段を移動体情報記憶装置3に設けた実施形態である。

[0070] (1. 特殊ネジ)

分離防止手段の一例として、特殊ネジの使用が挙げられる。図6は、「特殊ネジ303」の一例を示す。このように、市販されている「プラスネジ」や「マイナスネジ」ではなく、特殊な形状をした「特殊ネジ303」を用いて、移動体情報記憶装置3を指定移動体である移動体1に固定する。これにより、移動体情報記憶装置3を外すためには、こ

の「特殊ネジ303」に対応した特殊なドライバーなどの工具が必要となり、容易に移動体情報記憶装置3をはずすことはできない。

[0071] (2. 分離防止シール)

他の分離防止手段を説明する。図7は、改ざん防止シールや封印シール等の「シール60」によって移動体情報記憶装置3を封印した場合の、移動体1への移動体情報記憶装置3の取り付け状態を示す。「シール60」は、一度貼り付けた後にはがすと、表面に「開封済」などの文字が現れる。移動体1に移動体情報記憶装置3を固定した後、「シール60」を、移動体1と移動体情報記憶装置3とをまたぐように貼る。これにより、移動体情報記憶装置3を移動体1から外した場合、「シール60」には上記「開封済」などの文字が現れる。このため、サービス提供者は、移動体情報記憶装置3を外したことを検出することができる。また、このようなシールを貼っているので、ユーザ等が、移動体情報記憶装置3を移動体1から外す試みを抑止することができる。

[0072] (3. 施錠)

図示はしていないが、他の分離防止手段として、移動体情報記憶装置3と移動体1を両方同時に物理錠により施錠することや物理錠により移動体情報記憶装置3を移動体1に固定することでも実現できる。

[0073] (4. 電気的分離防止)

また、他の分離防止手段として、電気的に実現した例を説明する。図8は、実施の形態3における移動体情報記憶装置3の構成ブロック図である。図8に示す移動体情報記憶装置3は、図2に示す実施の形態1の移動体情報記憶装置3に対して、分離防止部302(分離検出部の一例、移動体判断部の一例)を備える。分離防止部302は、指定移動体との分離を防止するとともに、装備移動体が指定移動体であるかどうかを判断する。

[0074] 移動体1は、移動体側固有情報処理部301(移動体側認証実行部の一例)を備える。移動体側固有情報処理部301は、移動体側固有情報記憶部311を備える。移動体側固有情報記憶部311は、移動体側固有情報(移動体側特定情報)を記憶する。「移動体側固有情報」とは、移動体1が保有する情報であって、移動体1を特定可能な情報である。「移動体側固有情報」とは、具体的には、移動体1が自動車とすれ

ば、ナンバープレート情報や車体番号、製造番号など、移動体1を一意に区別できる情報を意味する。

[0075] 移動体側固有情報処理部301は、分離防止部302との間で認証処理を行なう。図8では、移動体1の移動体側固有情報処理部301は、移動体情報記憶装置3の制御部22に接続されている。そして、分離防止部302は、制御部22を介して移動体側固有情報処理部301と通信する構成である。しかし、これに限定するものではなく、分離防止部302を直接に移動体側固有情報処理部301に接続し、通信する構成でもよい。

[0076] 次に動作について、図9を用いて説明する。図9は、移動体側固有情報処理部301と分離防止部302とのやりとりを示すシーケンス図である。図9では、分離防止部302は、装置側固有情報記憶部31が記憶した装置側固有情報と、移動体側固有情報記憶部311が記憶した移動体側固有情報とを入力し、入力した装置側固有情報と移動体側固有情報とに基づいて、移動体1が指定移動体かどうかを判断する。図9を参照して具体的に説明する。

[0077] (1)移動体側固有情報処理部301は、移動体1の「移動体側固有情報」を移動体側固有情報記憶部311に格納している。この「移動体側固有情報」は、移動体1が指定移動体であれば、移動体情報記憶装置3の装置側固有情報記憶部31に格納されている装置側固有情報と同一性があるべきものである。なお同一である必要はなく、それぞれから同一の移動体が特定できればよい。

(2)分離防止部302は、必要なタイミングで、移動体側固有情報処理部301と通信し、移動体1が保有する「移動体側固有情報」を取得する(S1)。

(3)そして、分離防止部302は、取得した「移動体側固有情報」と、装置側固有情報記憶部31に保管している「装置側固有情報」との比較を行う(S2)。

(3)比較結果が正しければ正常終了(S3)し、例えば、記憶部21に正常終了した内容を記録する。正しくなければ異常終了(S4)し、例えば、記憶部21に異常終了した旨を記録する。

[0078] なお、分離防止部302が移動体側固有情報処理部301と通信するタイミングは、エンジン始動時、「完全性情報」の生成時、一定もしくはランダムな時間毎などである。

これにより、移動体情報記憶装置3が移動体1から分離して異なる移動体に装着されたことを検出することができる。よって、本機能が移動体情報記憶装置3に搭載されていること

をユーザに知らせることにより、移動体情報記憶装置3を移動体から外す試みを抑止することができる。

[0079] 次に、図10参照して、移動体側固有情報処理部301と分離防止部302との間で認証処理を行う場合の例を説明する。図10は、移動体側固有情報処理部301と分離防止部302との間で行なわれる認証処理のフローチャートである。分離防止部302は、移動体側固有情報処理部301(移動体側認証実行部)に認証要求を送信する。そして、分離防止部302は、「予め設定された規則」に基いて、移動体側固有情報処理部301との間で認証処理を実行することにより、自己(移動体情報記憶装置3)が装備された装備移動体が指定移動体かどうかを判断する。以下に、さらに説明する。

[0080] 図10の場合は、「予め設定された規則」として、「乱数の暗号化、復号化」の場合を示している。移動体情報記憶装置3と移動体1の移動体側固有情報処理部301は暗号鍵(図示していない)を持っている。

[0081] (1)移動体情報記憶装置3の分離防止部302は、乱数(R)を生成し(S6)、移動体1の移動体側固有情報処理部301に送信する(認証要求の一例)(S7)。

(2)移動体側固有情報処理部301は乱数(R)を受信(S8)し、暗号化(e(R))した(S9)後、移動体情報記憶装置3に送信する(S10)。

(3)移動体情報記憶装置3の分離防止部302では、応答データ(e(R´))を受信し(S11)、それを復号し(S12)、先に生成した乱数と比較する(S13)。

(4)分離防止部302は、比較結果により、装備移動体である移動体1が指定移動体かどうかを判断する。分離防止部302は、比較結果が一致した場合、移動体1を指定移動体であると判断し、比較結果が一致しない場合は、移動体1を指定移動体ではないと判断する。

(5)比較結果が一致していた場合(S14)、正常終了し、一致していない場合(S15)、異常終了する。

[0082] (別の例1)

「予め設定された規則」として次の場合がある。図10の場合は、移動体情報記憶装置3にて、移動体側固有情報処理部301から受信した暗号化された乱数を復号し(S12)、その後に比較を行っている(S13)。しかし、生成した乱数を移動体情報記憶装置3の分離防止部302で暗号化し、その結果と移動体側固有情報処理部301から受信した暗号化された乱数を比較しても良い。

[0083] (別の例2)

「予め設定された規則」として次の場合がある。図10の場合は、移動体側固有情報処理部301で暗号化(S9)した乱数を、分離防止部302で確認している。しかし、移動体側固有情報処理部301が受信した乱数に対して、メッセージ認証子やデジタル署名を生成し、それらを分離防止部302が検証しても良い。

[0084] (別の例3)

さらに、「予め設定された規則」として、前述の図9で説明した固有情報を確認する方法と組み合わせて実現してもよい。すなわち、移動体側固有情報処理部301にて乱数を暗号化する際、乱数と移動体側固有情報の両方を暗号化し、分離防止部302にて復号した乱数、移動体側固有情報を、生成した乱数、保管している装置側固有情報と比較する方法でもよい。

[0085] 以上の前記で述べた「予め設定された規則」により、分離防止部302は、移動体情報記憶装置3が移動体1から分離され、異なる移動体に装着されたことを検出することがで

きる。また、暗号化を行っているので、前述の移動体側固有情報、装置側固有情報の確認よりも信頼性の高い移動体情報記憶装置3を実現できる。本機能が移動体情報記憶装置3に搭載されていることをユーザに知らせることにより、移動体情報記憶装置3を外す試みを抑止することができる。

[0086] 以上のように、移動体情報記憶装置3に分離防止部302を設けることによって、移動体情報記憶装置3と移動体1との対応関係が明確になり、移動体情報記憶装置3を他の移動体に装着し、偽の「移動体情報」を収集することを防ぐことが出来る。よって、信頼性の高い移動体情報記憶装置3をサービス提供者に提供することができる。また、移動体情報記憶装置3が保管している装置側固有情報、取得した他の移動体

の移動体側固有情報や、移動体情報記憶装置3が他の移動体へ装着されたという情報をサービス提供者に提供する構成にすることにより、サービス提供者が、それらの情報を基に利用者へ警告することが可能になる。

[0087] 実施の形態4.

次に、図11、図12を参照して、実施の形態4を説明する。実施の形態4は、図8の分離防止部302が、電力を供給するバッテリ401(電源)を備えた実施形態である。図11は、実施の形態4の移動体情報記憶装置3の構成を示すブロック図である。図11は、実施の形態3の図8に対して、分離防止部302がバッテリ401を備えている点が異なる。

[0088] 図11では、バッテリ401は、分離防止部302が内蔵しているが、これは一例である。バッテリ401は、移動体情報記憶装置3に備えられていればよい。すなわち、移動体情報記憶装置3が移動体1と分離した場合であっても、電源が供給される構成であればよい。

[0089] 図11の分離防止部302は、一定もしくはランダムな時間毎に実施の形態3の図9で示した移動体1の移動体側固有情報の取得や、あるいは図10で示した乱数による認証を行う。このような構成であるため、移動体情報記憶装置3が移動体1から分離された場合でも、分離防止部302は、バッテリ401を稼動電源として、必要なタイミングで、移動体側固有情報の取得や認証を実施することは可能である。しかし、移動体情報記憶装置3は移動体1と接続されていないため、分離防止部302は、移動体1からの応答を得ることができない。これにより、分離防止部302は、移動体1から分離していることを検出する。

[0090] すなわち、移動体情報記憶装置3は、電力を供給するバッテリ401(電源)を備えている。前記のように、バッテリ401は、分離防止部302が備えることに限定することはなく、移動体情報記憶装置3に備えられていれば構わない。分離防止部302は、分離された場合であってもバッテリ401(電源)から電力の供給を受けることにより、移動体の移動体側固有情報処理部301に、移動体側固有情報の送信を要求する「送信要求信号」を送信し応答を求め、あるいは、認証処理の開始要求する「認証処理開始要求信号」を送信し応答を求める。これら分離防止部302が送信する、「送信要求

信号」や「認証処理開始要求信号」は、分離防止部302が、移動体情報記憶装置3が移動体に装備されているかどうか、すなわち移動体から分離されているかどうかを確認する「分離確認信号」の機能を果たす。また、移動体の移動体側固有情報処理部301は、「分離確認信号」に対して応答する「応答部」の機能を果たす。このように、分離防止部302は、移動体側固有情報処理部301（応答部）に向けて、「分離確認信号」を送信することにより移動体側固有情報処理部301からの応答を求め、応答がない場合に、移動体と分離したと判断する。

[0091] 次に、図12を参照して、分離防止部302の別の例を説明する。図12は、移動体1において、分離防止部302の別の例を示すブロック図である。信号線402は、分離防止部302から移動体1を経て再び分離防止部302に入力される。移動体1と分離防止部302は、例えば図に示す様に、コネクタで接続される。このような構成において、次に動作を説明する。

[0092] 分離防止部302は、バッテリ401を電源として信号線402に電流を流す。移動体情報記憶装置3が移動体1に装着されている場合は、信号線402には電流が流れている。しかし、移動体情報記憶装置3が移動体1から分離した場合、信号線402は寸断される。よって、電流は流れなくなる。つまり、分離防止部302は、信号線402に流れる電流を観測することによって、移動体情報記憶装置3が移動体1から分離したことを検出することができる。

[0093] 以上のように、移動体情報記憶装置3にバッテリ401を備えることにより、移動体情報記憶装置3が移動体1から分離した事実を正確に検出することが出来る。このため、信頼性の高い移動体情報記憶装置3をサービス提供者に提供することができる。また、移動体情報記憶装置3が保管している装置側固有情報や、移動体から取得した移動体側固有情報や、移動体情報記憶装置3が移動体1から分離したという情報をサービス提供者に提供する構成にすることにより、サービス提供者が、それらの情報を基に利用者へ警告することが可能になる。

[0094] 実施の形態5.

次に、図13を参照して実施の形態5を説明する。実施の形態5は、分離防止部302が移動体との分離を検出した場合に、移動体情報記憶装置3の記憶している情報

を消去する分離防止部302を備えた場合の実施形態について説明する。

[0095] 図13に示す様に、分離防止部302は、情報消去部501を備える。情報消去部501は、分離防止部302が移動体1との分離を検出した場合に、記憶部21の情報を消去する。例えば、情報消去部501は、分離防止部302が自己(移動体情報記憶装置3)が装備される装備移動体は指定移動体ではないと判断した場合に、移動体情報記憶部32が記憶した移動体情報を消去する。

[0096] このような構成において、分離防止部302は、一定もしくはランダムな時間毎に実施の形態2や実施の形態3で示した図9の移動体1の移動体側固有情報の取得や、図10の乱数による認証などにより、分離したことを検出する。そして、移動体情報記憶装置3内の情報、例えば、前記のように移動体情報記憶部32に記憶されている「移動体情報」などを消去する。どの情報を消去するかは、設定することができる。

[0097] 以上のように、情報消去部501は、移動体情報記憶装置3が移動体と分離した場合に、記憶部21の情報を消去する。このため、サービス提供者は確実に分離したことを知ることができ、また、サービス提供者がその情報を基に利用者への警告が可能になる。従って、信頼性の高い移動体情報記憶装置3をサービス提供者に提供することができる。

[0098] 実施の形態6.

次に図14、図15を参照して、実施の形態6を説明する。実施の形態6は、移動体情報記憶装置3と移動体情報検証装置600とからなる移動体情報保証システムの実施形態である。本実施の形態6は、実施の形態1に対応し、実施の形態1に対して移動体情報検証装置600を備えることにより、システムとした実施形態である。

[0099] 移動体情報検証装置600は、検証部601を備える。図14は、実施の形態6の移動体情報保証システムの構成図である。図14の移動体情報記憶装置3は、図2の移動体情報記憶装置3と同様である。図14において、移動体情報検証装置600は、サービス提供者が保有する。検証部601は、入力された情報に対する改ざんの有無を検証する。なお、他の実施の形態と同様に、移動体情報記憶装置3には分離防止部302を設けても良い。

[0100] 次に、図15を参照して実施の形態6の移動体情報保証システムの動作について説

明する。

[0101] 移動体情報記憶装置3の動作は、実施の形態1の場合と同様である。すなわち、移動体情報記憶装置3は、「移動体情報」を保管し、「完全性情報」を生成する。そして、移動体情報検証装置600の検証部601は、「完全性情報」を用いて、「移動体情報」が改ざんされていないことを確認する。

[0102] なお、移動体情報記憶装置3と移動体情報検証装置600との間の情報のやり取りは、実施の形態8で後述する「通信」、あるいは実施の形態10で後述する「ICカード」を用いることを想定している。

[0103] 図15に、改ざん防止部20と検証部601とによる処理のフローを示す。図15は、デジタル署名を用いた場合を示している。このデジタル署名は、「完全性情報」を生成する場合の一例である。

(1)改ざん防止部20は、「移動体情報」と「装置側固有情報」とをハッシュ関数に入力してハッシュ値を求める(S40)。そして、そのハッシュ値を署名鍵で暗号化して「完全性情報」を生成する(S41)。署名鍵は、予め移動体情報記憶装置3の記憶部21に格納される。

(2)検証部601では、「移動体情報」と「装置側固有情報」とから、改ざん防止部20と同様にハッシュ値を求める(S42)。

(3)一方で「完全性情報」を検証鍵で復号し(S43)、前記ハッシュ値と復号結果のハッシュ値を比較する(S44)。

(4)検証部601は、比較した結果、前記ハッシュ値が同一と認めれば、「移動体情報」は正当な情報、すなわち改ざんされていないと判断する。前記ハッシュ値が異なっていた場合、検証部601は、「移動体情報」、あるいは「装置側移動体情報」の少なくともいずれかは、改ざんされていると判断する。

[0104] 図15は、改ざん防止部20が、「移動体情報」と「装置側固有情報」とに基づいて「完全性情報」を生成している。図15に示す改ざん防止部20の処理とは、別の例を説明する。改ざん防止部20は「装置側固有情報」を用いているが、移動体1が記憶する「移動体側固有情報」と「移動体情報」とから、「完全性情報」を生成することもできる。この場合、図8に示すように、移動体1は、移動体側固有情報記憶部311を備えてい

ることが前提である。

[0105] 図15は、改ざん防止部20が、「移動体情報」と「装置側固有情報」とに基づいて「完全性情報」を生成している。図15に示す改ざん防止部20の処理とは、別の例を説明する。まず、移動体情報記憶装置3では、分離防止部302が、図9に示す「装置側固有情報」と「移動体側固有情報」との比較検証処理を実施する。そして、分離防止部302による検証の結果、「装置側固有情報」と「移動体側固有情報」とが同一の移動体に関する情報と判明した場合に、改ざん防止部20が、「装置側固有特定情報」と「移動体側固有情報」とのうちのいずれかを選択対象として選択して取得する。そして、改ざん防止部20は、取得した選択対象と移動体情報記憶部32が記憶した移動体情報とに基づいて、完全性情報を生成する。この場合は、移動体が正当であることが判明した後に完全性情報
を生成するので、移動情報に対する信頼をより高めることができる。

[0106] 以上のように、「移動体情報」と「装置側固有情報」(あるいは移動体側固有情報)とが改ざんされていないことを検証できるので、信頼性の高い移動体情報検証装置600および移動体情報保証システムをサービス提供者に提供することができる。

[0107] なお、図15ではデジタル署名を用いた例を示したが、「完全性情報」は、「移動体情報」と「装置側固有情報」とが改ざんされていないことを確認することができればよく、デジタル署名に限らず、例えばメッセージ認証子や電子透かしやCRC(Cyclic Redundancy Check)を用いてもよい。

[0108] 実施の形態7.

次に図16を参照して実施の形態7を説明する。実施の形態7は、実施の形態6の移動体情報検証装置600が、さらに、処理部701を備えた構成である。図16は、実施の形態7の移動体情報保証システムの構成図である。図16は、図14に対して、移動体情報検証装置600が、さらに、処理部701を備えた点が異なる。

[0109] 図16において、処理部701は、検証部601による検証結果を基に「移動体情報」を処理する。なお、他の実施の形態と同様に、移動体情報記憶装置3には分離防止部302を設けても良い。

[0110] 次に動作について説明する。

(1)移動体情報記憶装置3の動作は、実施の形態1、あるいは実施の形態6と同様である。すなわち、移動体情報記憶装置3は、「移動体情報」を保管し、「完全性情報」を生成する。

(2)そして、例えば、実施の形態6で示した方法により、サービス提供者は、移動体情報検証装置の検証部601にて、「完全性情報」を用いて、「移動体情報」と「装置側固有情報」が改ざんされていないことを確認する。

(3)そして、これらの情報が改ざんされていない場合、処理部701にて「移動体情報」や「装置側固有情報」を処理する。この「処理」とは、「移動体情報」や「装置側固有情報」に基づいて、保険料を決定し、あるいは自動車税を決定し、あるいは警察において交通違反の検出を行うなどが考えられる。

[0111] 以上のように、移動体情報検証装置600が処理部701を備えるので、「移動体情報」と「装置側固有情報」(あるいは「移動体側固有情報」)が改ざんされていないことを検証した上で、その検証結果を反映してユーザに対するサービスを決定できる。このため、サービス提供者は信頼性の高い移動体情報保証システムを用いて、木目細かいサービスをユーザに提供することができる。

[0112] 実施の形態8.

次に図17、図18を参照して実施の形態8を説明する。実施の形態8は、移動体情報記憶装置3と移動体情報検証装置600とが通信を行なう実施形態である。図17は、実施の形態8の移動体情報保証システムの構成図である。図17は、実施の形態7の図16において、移動体情報記憶装置3が記憶側通信部801(出力部の一例)を備え、移動体情報検証装置600が、検証側通信部802を備えた構成である。記憶側通信部801は、「移動体情報」と、「装置側固有情報」と、「完全性情報」とを送信(出力)する。記憶側通信部801は、例えば、移動体情報検証装置600に送信する。ここで、記憶側通信部801は、無線・有線LAN、RS232C、Bluetooth(登録商標)、DSRC(専用狭帯域通信)、携帯電話、PHS(登録商標)などを利用して通信を行なう。検証側通信部802は、移動体情報記憶装置3の記憶側通信部801と通信する移動体情報検証装置600の通信部である。なお、他の実施の形態と同様に、移動体情報記憶装置3には、分離防止部302を設けても良い。

[0113] 次に図18を参照して実施の形態8の移動体情報保証システムの動作を説明する。図18は、実施形態6で示したデジタル署名を改ざん防止部20と検証部601に適用した場合のフロー例である。

[0114] (1)移動体情報検証装置600(サービス提供者)は、移動体情報記憶装置3に署名鍵を格納し、検証鍵を保管する(S30)。

(2)移動体情報記憶装置3の移動体情報記憶部32は、「移動体情報」を記録(S31)する。

(3)そして、移動体情報記憶装置3の改ざん防止部20は、必要なタイミングで、署名鍵を用いて「完全性情報」を生成する(S32)。

(4)そして、制御部22は、記憶側通信部801を介して、移動体情報検証装置600(サービス提供者)に「移動体情報」と、「装置側固有情報」と、「完全性情報」とを送信する(S33)。

(5)サービス提供者の移動体情報検証装置600は、検証側通信部802で「移動体情報」と、「装置側固有情報」と、「完全性情報」とを受信する(S34)。

(6)検証部601が検証鍵を用いて検証(S35)した後に、

(7)処理部701が「移動体情報」、「装置側固有情報」の処理を行う(S36)。

(8)なお、図18の例では、「完全性情報」を作成した後、「移動体情報」と、「装置側体固有情報」と、「完全性情報」とを送信しているが、図4のように、複数の「完全性情報」を作成した後、まとめて送信するようにしてもよい。

[0115] 以上のように、「移動体情報」、「移動体固有情報」、「完全性情報」を記憶側通信部801により移動体情報検証装置600に送信し、改ざんされていないことを検証した上でユーザに対するサービスを決定できるので、サービス提供者が信頼性の高い移動体情報保証システムを用いて、木目細かいサービスをユーザに提供することができる。

[0116] 実施の形態9.

次に図19を参照して実施の形態9を説明する。図19は、実施の形態9の移動体情報保証システムを示す構成図である。実施の形態9は、実施の形態8の図17に対して、移動体情報記憶装置3の記憶側通信部801が通信先(出力先)を認証する通信

先認証部901（出力先認証部）を備えた構成である。なお、他の実施の形態と同様に、移動体情報記憶装置3には、分離防止部302を設けても良い。

[0117] 通信先認証部901は、「移動体情報」、「装置側固有情報」、「完全性情報」を出力する場合に、送信先（出力先）を認証する。

[0118] 次に動作について説明する。移動体情報記憶装置3の動作は実施の形態1、あるいは実施の形態8と同様である。

（1）すなわち、移動体情報記憶装置3は、「移動体情報」を保管し、「完全性情報」を生成する。

（2）そして、通信先認証部901は、記憶側通信部801が移動体情報検証装置600（サービス提供者）に「移動体情報」、「装置側固有情報」、及び「完全性情報」を転送する前に、通信先である移動体情報検証装置600（検証側通信部802）を認証する。認証する方法は、図10に示したような乱数を使用する方法でもよい。

（3）そして、認証が成功した場合に、記憶側通信部801は、「移動体情報」、「装置側固有情報」、及び「完全性情報」を移動体情報検証装置600に送信する。

（4）認証が失敗した場合、「移動体情報」等の送信は行わない。例えば、制御部22は

、通信先認証部901による認証が失敗した情報を記憶部21に記録する。

（5）その後、移動体情報検証装置600は、検証側通信部802が受信した「移動体情報」、「装置側固有情報」、「完全性情報」を使用して、検証及び処理を行う。後の処理は実施の形態8と同様である。

[0119] 以上のように、移動体情報記憶装置3は、記憶側通信部801により通信先（出力先）を認証し、正しい通信先であることを確認した後、「移動体情報」、「装置側固有情報」、「完全性情報」を送信（出力）する。このため、通信データを解析するなどの不正行為を防ぐことができ、サービス提供者に信頼性の高い移動体情報記憶装置3、あるいは移動体情報保証システムを提供することができる。

[0120] 実施の形態10.

次に図20、図21を参照して実施の形態10を説明する。実施の形態10は、実施の形態8を元にし、実施の形態8を示す図17に対して、さらにICカード1001を備えた

システムである。実施の形態10では、記憶側通信部801はICカード1001と通信する。なお、ICカード101は、情報を記憶可能であるとともに携帯が可能である携帯型記憶媒体の一例である。例えば、携帯可能なメモリカードでもよい。あるいは、情報の記憶が可能な携帯電話でもよい。

[0121] 図20は、実施の形態10の移動体情報保証システムを示す構成図である。実施の形態10は、実施の形態8の図17に対しICカードを追加した点が異なる。

[0122] 記憶側通信部801は、ICカード1001と通信し、「移動体情報」、「装置側固有情報」、及び「完全性情報」をICカード1001に送信(出力)する。

[0123] 検証側通信部802は、ICカード1001と通信し、ICカード1001内の情報を読み出す。

[0124] ICカード1001は、交換型記憶媒体である。

[0125] 検証側通信部802は、ICカード1001がユーザの自宅のPC(Personal Computer)に接続された場合に、前記PCからインタネットや携帯電話を介して「移動体情報」等を受信する構成でもよい。

[0126] あるいは、検証側通信部802は、サービス提供者の事務所に設置された専用端末、また、ガソリンスタンド、コンビニエンスストア、カーディーラ、車両整備工場に設置されたサービス提供者の専用端末にICカード1001が接続された場合、前記専用端末からインタネットや携帯電話を介して「移動体情報」等を受信する構成でもよい。インタネットを使用する場合、安全な通信路を構成するためにSSL(Secure Socket Layer)やバーチャルプライベートネットワークなどを使用すればよい。

[0127] なお、他の実施の形態と同様に、移動体情報記憶装置3には、分離防止部302や通信先認証部901を設けても良い。この場合、通信先認証部901は、ICカード1001を認証する。

[0128] 次に動作について図21を用いて説明する。図21は、実施の形態6で示したデジタル署名を改ざん防止部20と検証部601に適用した場合のフロー例である。

(1)移動体情報検証装置600(サービス提供者)は、移動体情報記憶装置3に署名鍵を格納し、検証鍵を保管する。

(2)移動体情報記憶装置3の移動体情報記憶部32は、「移動体情報」を記録する。

(3)改ざん防止部20は、必要なタイミングで署名鍵を用いて「完全性情報」を生成する。

(4)そして、記憶側通信部801は、ICカード1001に「移動体情報」、「装置側固有情報」、及び「完全性情報」とを送信する(S33)。

(5)これらの情報がICカード1001に記録される(S40)。

(6)ICカード1001内の情報は、検証側通信部802によって読み出される(S34)。

(7)移動体情報検証装置600の検証部601が検証鍵を用いて検証した後に、処理部701が「移動体情報」や「装置側固有情報」の処理を行う。

[0129] 図21の例では、「完全性情報」を作成した後、「移動体情報」、「装置側固有情報」及び「完全性情報」を送信しているが、図4のように、複数の「完全性情報」を作成した後、まとめて送信するようにしてもよい。

[0130] 以上のように、ICカード1001を使用するので、システムを簡便に構築することができる。

[0131] 実施の形態11.

次に図22を参照して実施の形態11を説明する。システム構成は、図17の実施の形態8と同様である。なお、他の実施の形態と同様に、移動体情報記憶装置3には、分離防止部302や通信先認証部901を設けても良い。

[0132] 実施の形態11は、記憶側通信部801が、予め設定された時間間隔で、「移動体情報」、「装置側固有情報」、及び「完全性情報」を送信(出力)する実施形態である。

「予め設定された時間間隔」として、

まずは「移動体情報a」、「完全性情報a」、「装置側固有情報a」を送信し、

次に、「移動体情報b」、「完全性情報b」、「装置側固有情報a」を送信し、

次に、「移動体情報c」、「完全性情報c」、「装置側固有情報a」を送信というように、記憶側通信部801が、できる限り休み無く常時、送信するように「時間間隔」を設定しておく。ここで「装置側固有情報a」のみ変わらないが、「装置側固有情報a」は移動体を特定するための情報であり通常、変化はない。

[0133] 図22は、実施の形態6で示したデジタル署名を改ざん防止部20と検証部601に適用し、常時、「移動体情報」等を送信する場合のフロー例である。

(1)移動体情報検証装置600(サービス提供者)は、移動体情報記憶装置3に署名鍵を格納し、検証鍵を保管する(S30)。

(2)移動体情報記憶装置3の移動体情報記憶部32は、「移動体情報」を記録する(S31)。

(3)移動体情報記憶装置3の改ざん防止部20は、署名鍵を用いて「完全性情報」を生成する(S32)。

(4)そして、記憶側通信部801は移動体情報検証装置600(サービス提供者)に「移動体情報」、「装置側固有情報」と「完全性情報」を送信する(S33)。

(5)移動体情報記憶装置3は、この処理を繰り返す。移動体情報検証装置600は、検証側通信部802で「移動体情報」、「装置側固有情報」、「完全性情報」を受信(S34)する。

(6)検証部601は、検証鍵を用いて検証(S35)し、

(7)その後に、処理部701が「移動体情報」や「装置側固有情報」の処理を行う(S36)。

なお、通信先認証部901を備えた図19と同一の構成を用いても実現できることはいうまでもない。この場合、通信開始時や通信路が途切れて、再接続した場合に通信先を認証

するようにすればよい。

[0134] 以上のように、記憶側通信部801が、「移動体情報」、「装置側固有情報」、「完全性情報」を、移動体情報検証装置600(サービス提供者)に、常時、送信する時間間隔で送信しているので、記憶部21の記憶容量を少なくすることができる。

[0135] 実施の形態12.

次に図23を参照して実施の形態12を説明する。以上の実施の形態では、移動体情報記憶装置3から出力される情報の完全性を証明していたが、移動体1に設置されたセンサ2a等が改ざんされた場合には対抗できていない。そこで、実施の形態12では、センサ2a等が正当なものであることを確認する実施形態を示す。

[0136] 図23は、センサを認証する場合の移動体情報保証システムにおける移動体情報記憶装置3の構成図である。図23は、実施の形態1を示す図2に対して、センサ確認

部1201を追加した構成である。なお、他の実施の形態と同様に、移動体情報記憶装置3には、分離防止部302、記憶側通信部801、通信先認証部901等を設けても良い。

[0137] センサ確認部1201は、移動体情報記憶装置3に設けられ、移動体情報記憶装置3に接続されているセンサ2a等を確認する機能を有する。図23は、センサ確認部1201は、制御部22を介してセンサ2a等を確認する構成になっているが、センサ2a等と直接接続して確認する構成でもよい。

[0138] 次に動作について説明する。

(1)センサ確認部1201は、必要なタイミングで、移動体情報記憶装置3に接続されているセンサ2a，センサ2b，センサ2c等の確認を行う。確認する方法は、図9、あるいは図10に示したような移動体を確認する方法と同様の方法を採ることができる。すなわち、図9に示した方法と同様に、センサ2a等の有する「センサ固有情報」を用いた方法でもよし、あるいは、図10に示したような乱数を使用した方法でもよい。

(2)センサ確認部1201による確認の結果、センサ2a等が正当であれば、制御部22は、「移動体情報」を移動体情報記憶部32に記録する。以上の処理を移動体情報記憶装置3は、接続されているすべてのセンサに対して行う。

[0139] センサの確認を行うタイミングは、エンジン始動時、一定もしくはランダムな時間毎、「移動体情報」の取出し時などでよい。応答が無かった場合や確認の結果が不正なセンサである場合の処理は、サービス提供者に依存するが、「移動体情報」の記録を中止しても良い。あるいは応答が無かったことを記憶部21に記録し「装置側固有情報」とともに移動体情報検証装置600に送信してもよい。あるいは、不正なセンサであることを記憶部21に記録し、「装置側固有情報」とともに移動体情報検証装置600に送信してもよい。

[0140] 以上のように、移動体情報記憶装置3は、センサ確認部1201が接続されているセンサが正当であるかどうかを確認するので、センサに対する不正を防ぎ、さらに情報の信頼性を高めることができる。

[0141] 実施の形態13.

次に図24、図25を参照して実施の形態13を説明する。以上の実施の形態では、

移動体情報記憶装置3において、すべての「移動体情報」を移動体情報記憶部32に記録する例を示していた。すなわち、移動体情報が速度情報とすれば、いかなる速度でも記録していた。実施の形態13では、記憶するべき移動体情報について条件を設定しておき、設定済みの条件に合致する移動体情報のみを記録する実施形態である。

[0142] 図24は、実施の形態13の移動体情報記憶装置3の構成図である。図24は、実施の形態1の図2に対して範囲判定部1301（条件判定部）を備えた構成である。なお、他の実施の形態と同様に、移動体情報記憶装置移動体情報記憶装置3には、分離防止部302、記憶側通信部801、通信先認証部901、センサ確認部1201等を設けても良い。

[0143] 図において、範囲判定部1301は、「移動体情報」が、「予め設定された条件」に合致するかどうかを判定し、合致すると判定した場合に移動情報を移動体情報記憶部32に記憶させる。その例えば、範囲判定部1301は、「移動体情報」が設定された範囲を超えた場合に記録する。範囲判定部1301は、「予め設定された範囲」（条件の一例）にあるか否かを判定する。なお、本実施の形態13では、範囲判定部1301は制御部22に接続されているが、センサと制御部22の間に設置し、範囲外の場合（範囲を超える場合）に制御部22に「移動体情報」を出力し、範囲内の場合は出力しない構成にしてもよい。

[0144] 次に、図25を参照して動作を説明する。図25は、センサとして速度センサを例に、この速度センサが検出した速度情報を例とした「移動体情報」と時間経過との関係を示す。移動体情報記憶装置3に入力もしくは生成された「移動体情報」は、範囲判定部1301により設定された範囲外であるか判定される。範囲外の場合、移動体情報記憶部32に、該当する「移動体情報」（例えば前記速度情報）を記録する。図25中、点線までが設定された範囲とすると、実施の形態13では、点線を超える斜線の部分に相当する速度情報を記録する。

[0145] また、他の例では、急発進の回数が設定された規定回数以上になった場合に、その旨を「移動体情報」として記録することもできる。

[0146] 以上のように、実施の形態13の移動体情報記憶装置3では、範囲判定部が、あら

かじめ設定された範囲外の「移動体情報」を記録し、範囲内の「移動体情報」は記録しないので、移動体情報記憶部の記憶容量を少なくすることができる。

[0147] 実施の形態14.

次に、図26～図28を参照して実施の形態14を説明する。以上の実施の形態では、ユーザは、一つのサービスしか受けることができなかった。本実施の形態14は、複数のサービス受けることが可能な実施形態を示す。

[0148] 図26は、実施の形態14の移動体情報保証システムにおける移動体情報記憶装置3の構成図である。図26は、図2の移動体情報記憶装置3に対して、選択部1401を備えた構成である。なお、他の実施の形態と同様に、移動体情報記憶装置3には、分離防止部302、記憶側通信部801、通信先認証部901、センサ確認部1201、範囲判定部1301等を設けても良い。

[0149] 図26において、移動体情報記憶装置3内の選択部1401は、サービス提供者に対応する複数のサービス情報を管理し、それぞれに対応する「移動体情報」を作成する。

[0150] 図26において、選択部1401は、それぞれのセンサに基づくそれぞれの移動体情報を入力し、サービス情報として予め設定された条件に基づいて、それぞれの移動体情報のうちから少なくとも一つの移動体情報を選択する。移動体情報群記憶部34は、選択部1401が選択した一つあるいは複数の移動体情報から構成されるグループを移動体情報群として記憶する。改ざん防止部20は、移動体を特定可能な特定情報を取得し、取得した

特定情報と移動体情報群記憶部が記憶した移動体情報群とに基づいて、前記特定情報と前記移動体情報群に含まれる前記移動体情報との少なくともいずれかに対する改ざんの有無を検証するために使用する「完全性情報」を生成する。完全性情報記憶部33は、改ざん防止部20が生成した完全性情報情報を記憶する。

[0151] 次に図27を参照して移動体情報記憶装置3の具体的な動作を説明する。図27は、移動体情報記憶装置3と各移動体情報検証装置600A、600Bとのやり取り示すシーケンス図である。ここで各移動体情報検証装置600A、600Bは、例えば実施の形態6に示した移動体情報検証装置600と同様である。図27は、実施の形態6で示し

たデジタル署名を改ざん防止部20と検証部601に適用した場合のフロー例である。図27の例では、複数のサービス提供者として、サービス提供者Aとサービス提供者Bを示している。

[0152] (1)サービス提供者A(移動体情報検証装置600A)は、移動体情報記憶装置3に署名鍵Aと使用する「移動体情報」を示したサービス情報Aとを格納し、検証鍵Aを保管する(S50)。

(2)同様の処理をサービス提供者B(移動体情報検証装置600B)も行う(S51)。

(3)移動体情報記憶装置3の選択部1401は、格納された各サービス情報を基に、例えば図28に示すサービス管理テーブル1402を作成する。図28の例では、「1」は使用すること、「0」は使用しないことを示している。すなわち、サービスAでは「移動体情報X」と「移動体情報Y」を使用し、サービスBでは「移動体情報X」と「移動体情報Z」を使用する。また、選択部1401は、格納された署名鍵と対応するサービスの関係も管理する。

(4)そして、選択部1401は、各移動体情報とサービス管理テーブル1402とを用いて、各サービスに必要な「移動体情報」を選択して、「移動体情報群A」(選択情報群)と「移動体情報群B」(選択情報群)を作成する(S52)。

(5)選択された「各移動体情報群」は、記憶部21の移動体情報群記憶部34(選択情報群記憶部)に記録される。

(6)改ざん防止部20は、必要なタイミングで、それぞれに対応した署名鍵を用いて、「移動体情報群」と「装置側固有情報」とに基づき、「完全性情報」を生成する(S53)。この時、選択部1401は、格納された署名鍵と対応するサービスの関係も管理しているので、改ざん防止部20は、対応する署名鍵を用いて「完全性情報」を生成することができる。

(7)そして、移動体情報記憶装置3は、サービス提供者(移動体情報検証装置)に応じて、「移動体情報群」、「装置側固有情報」、「完全性情報」を出力する。

(8)図27では、「移動体情報群A」、「装置側固有情報」、「完全性情報A」を出力する(S54)。

(9)サービス提供者Aの移動体情報検証装置600Aは、「移動体情報群」、「装置側

固有情報」と「完全性情報」を取得し、検証・処理する。例えば、サービス提供者Aの移動体情報検証装置600Aは「移動体情報群A」、「装置側固有情報」と「完全性情報A」を取得(S55)し、検証(S56)・処理(S57)を行う。

[0153] なお、この例では、「完全性情報」を作成した後、「移動体情報」、「装置固有情報」と「完全性情報」を出力しているが、「完全性情報」を記憶部21の完全性情報記憶部33に記録される前に作成した後、まとめて出力する形態でもよいし、実施の形態11を示す図22のように、常時、「移動体情報群」と「完全性情報」とを出力する形態でもよい。

[0154] 以上のように、移動体情報記憶装置3では複数のサービスに対応した「移動体情報」を
管理・記録することができるので、1台の移動体情報記憶装置3で複数のサービスを受けることができ、また、サービスを追加することが出来る。

[0155] 実施の形態15.

実施の形態14の移動体情報記憶装置3では、サービスに対応して複数の「移動体情報」を記録していた。実施の形態15は、記録された「移動体情報」から選択して、複数のサービスに対応した「移動体情報群」を作成する実施形態を示す。
このような場合の移動体情報保証システムにおける移動体情報記憶装置3とセンサ群2は、実施の形態14の図26と同じ構成で実現できる。なお、他の実施の形態と同様に、移動体情報記憶装置3には、分離防止部302、記憶側通信部801、通信先認証部901、センサ確認部1201、範囲判定部1301、選択部1401を設けても良い。

[0156] 次に動作について説明する。

(1)移動体情報記憶装置3は、すべての「移動体情報」を記憶部21の移動体情報記憶部32に記録する。

(2)そして、「移動体情報」を移動体情報記憶装置3の外部に出力する際に、選択部1401が、サービス情報を参照し、移動体情報記憶部32から必要な種類の「移動体情報」を選択する。

(3)改ざん防止部20は、選択部1401により選択された移動体情報から構成される「移動体情報群」(選択情報群)と、「装置側固有情報」(特定情報)とから「完全性情報

」を作成する。

(4)この時、選択部1401は、格納された署名鍵と対応するサービスの関係も管理しているので、改ざん防止部20は、「完全性情報」の生成に際し、対応する署名鍵を用いることができる。

(5)その後、サービス提供者の移動体情報検証装置600は、選択された「移動体情報群」、「装置側固有情報」とその「完全性情報」を取得し、検証・処理を行う。

[0157] このように、実施の形態15の移動体情報記憶装置3は、選択部1401が、記録された「移動体情報」から必要な情報を選択して送信するので、複数のサービスに対応可能することができるとともに、少ない記憶容量で複数サービスに対応することができる。また、サービスを追加することが出来る。

[0158] 実施の形態16.

次に図29を参照して実施の形態16を説明する。以上の実施の形態では、ユーザの了解を得た上で移動体情報記憶装置3から「移動体情報」を出力することはできなかった。例えば、実施の形態8において、通信方式に携帯電話を用いた場合は、通信コストがかかる。よって、情報の送信時にユーザの同意を得ることは重要である。そこで、実施の形態16では、「移動体情報」を出力する際に、ユーザに同意を求める実施形態を示す。

[0159] 図29は、実施の形態16の移動体情報保証システムにおける移動体情報記憶装置3の構成図である。図29は、実施の形態1の図20の移動体情報記憶装置3に対してマンマシンインタフェース部1601(命令部の一例)を備えた構成である。なお、他の実施の形態と同様に、移動体情報記憶装置3には、分離防止部302、記憶側通信部801、通信先認証部901、センサ確認部1201等を設けても良い。

[0160] マンマシンインタフェース部1601は、ユーザに移動体情報記憶装置3の操作を提供し、処理結果等を応答する。マンマシンインタフェース部1601は、操作者による操作を受け付け、受け付けた操作に基いて、記憶側通信部801に対して送信(出力)を命じる。記憶側通信部801は、マンマシンインタフェース部1601からの命令に応答して、「移動体情報」、「装置側固有情報」、「完全性情報」とを出力する。

[0161] 具体的には、このような構成において、「移動体情報」を出力する必要がある場合に

、マンマシンインタフェース部1601は、ユーザから、所定の操作による出力命令を受け付ける。マンマシンインタフェース部1601は、ユーザからの出力命令を受け付けると、記憶側通信部801に出力を命じる。記憶側通信部801は、マンマシンインタフェース部1601から出力を命じられた場合、記録されている「移動体情報」、「装置固有情報」、「完全性情報」を出力する。

[0162] また、マンマシンインタフェース部1601が、ユーザから出力命令を入力された後に「移動体情報」と「装置側固有情報」とから「完全性情報」を生成し、これらを出力する構成でもよい。なお、「移動体情報」を出力するタイミングは、サービス提供者のユーザへの要求、記憶部21の残記憶容量から、移動体情報記憶装置3が判断してマンマシンインタフェース部1601を介してユーザに推奨してもよい。

[0163] このように、出力時にユーザの同意を得ることができるので、ユーザは自身が納得した通信コストによってサービス提供者は「移動体情報」を取得することができる。

[0164] 実施の形態17.

次に図30、図31を参照して実施の形態17を説明する。以上の実施の形態では、正当なユーザやサービス提供者以外の第三者によって移動体情報記憶装置3から「移動体情報」が出力されてしまう恐れがあった。例えば、実施の形態10では、第三者が保有する自身のICカードを利用して「移動体情報」を移動体情報記憶装置3から取り出し、正当なユーザがサービスを受けられなくなる恐れがある。また、実施の形態16において、第三者が勝手に「移動体情報」や「完全性情報」を転送してしまう恐れがある。そこで、実施の形態17では、「移動体情報」を出力する際に、正当なユーザやサービス提供者であることを認証する場合の実施形態を示す。

[0165] 図30は、このような場合の移動体情報保証システムにおける移動体情報記憶装置3の構成図である。図30は、実施の形態16の図29に対して、さらに操作者認証部1701を備えた構成である。操作者認証部1701は、「移動体情報」を出力する前に、マンマシンインタフェース部1601から入力された情報を認証する。すなわち、操作者認証部1701は、マンマシンインタフェース部1601が操作者から受け付けた操作に基づいて、前記操作者が正当であるかどうかを認証する。そして、マンマシンインタフェース部1601は、操作者認証部1701が操作者を正当と認証した場合に、記憶側

通信部801に対して出力を命じる。

[0166] 操作者は、正当なユーザもしくはサービス提供者である。なお、他の実施の形態と同様に、分離防止部302、記憶側通信部801、通信先認証部901、センサ確認部1201、範囲判定部1301、選択部1401を移動体情報記憶装置3に設けても良い。

[0167] このような構成において、「移動体情報」を出力する際に、移動体情報記憶装置3は、マンマシンインタフェース部1601により、操作者に認証するための情報の入力(操作)を要求する。例えば、マンマシンインタフェース部1601がタッチパネルを備える構成を図31に示す。図31は、認証のメカニズムに操作者のみが知っている暗証番号を用いた場合のタッチパネル操作画面の例を示している。タッチパネル62には、入力された暗証番号に対応してアスタリスクを表示する暗証番号応答画面61が表示される。操作者は、本タッチパネル62で暗証番号を入力(操作の一例)する。操作者認証部1701は、入力された暗証番号が、あらかじめ移動体情報記憶装置3に設定された暗証番号と一致すると判断した場合、正当な操作者であると認識(認証)する。マンマシンインタフェース部1601は、操作者認証部1701が、操作者を正当と認証した場合に、記憶側通信

部801に対して出力を命じる。記憶側通信部801は、この命令に応答して、「移動体情報」、「装置側固有情報」、「完全性情報」とを出力する。操作者認証部1701が、一致しない、すなわち操作者が正当ではないと判断した場合は、マンマシンインタフェース部1601は、出力を命じない。よって記憶側通信部801は、「移動体情報」、「装置側固有情報」、「完全性情報」を出力せずに、例えば、一致しない旨をタッチパネル62に表示し、入力(操作)した操作者に報告する。

[0168] このように、実施の形態17の移動体情報記憶装置3は、操作者認証部を備えるので、操作者を認証することで、正当な操作者のみによって「移動体情報」、「装置側固有情報」、「完全性情報」が移動体情報記憶装置3から出力ため、信頼性が高くなる。

[0169] 実施の形態18.

次に図32を参照して実施の形態18を説明する。以上の実施の形態では、「移動体情報」の完全性を維持するシステムであるが、機密性が維持されていない、すなわち第三者に盗聴される恐れがある。そこで、実施の形態18は、「移動体情報」の機密性

を維持するシステムの実施形態を示す。

[0170] 図32は、このような場合の移動体情報保証システムの構成図である。図32は、実施の形態7を示す図16に対して、移動体情報記憶装置3が暗号部1801を備え、移動体情報検証装置600が復号部1802を備えた構成である。

[0171] 暗号部1801は、「移動体情報」を暗号化する。復号部1802は、取得した情報を復号する。なお、他の実施の形態と同様に、移動体情報記憶装置3には、分離防止部302、記憶側通信部801、通信先認証部901、センサ確認部1201、範囲判定部1301、選択部1401、マンマシンインタフェース部1601などを設けても良い。

[0172] このような構成において、移動体情報記憶装置3は、「移動体情報」を出力する前に、他の実施の形態と同様に「完全性情報」を作成する。そして、「移動体情報」を暗号部1801により暗号化する。実施の形態18では、「移動体情報」を暗号対象としているが、「完全性情報」や「装置側固有情報」を含めて暗号化してもよい。「完全性情報」を暗号対象にする場合、図15で示したハッシュ値をそのまま「完全性情報」として使用することもできる。すなわち、「移動体情報」と合わせて暗号化しているので、署名鍵でハッシュ値を暗号化しなくてもよい。暗号化に使用する暗号鍵は、サービス提供者が予め移動体情報記憶装置3に格納しておく。そして、出力された暗号化された「移動体情報」は移動体情報検証装置600の復号部1802により復号され、他の実施の形態と同じように処理される。

[0173] このように、暗号化された「移動体情報」を出力しているので、例えば通信路で盗聴された場合でも、ICカード1001を紛失した場合でも、「移動体情報」というユーザに関わる個人情報の機密性を維持することができ、サービス提供者は安心してサービスを提供することができる。

[0174] 実施の形態19.

次に図33を参照して実施の形態19を説明する。以上の実施の形態では、「移動体情報」は、実施の形態6を示す図14や実施の形態7を示す図16のように、直接サービス提供者(移動体情報検証装置)に出力される。本実施の形態19では、仲介業者を介して出力するような場合の実施形態を示す。なお、他の実施形態と同様に、移動体情報記憶装置3には、分離防止部302、記憶側通信部801、通信先認証部901、

センサ確認部1201、範囲判定部1301、選択部1401、マンマシンインタフェース部1601を設けても良い。

[0175] 図33は、このような場合の移動体情報保証システム全体の構成を示すブロック図である。図33は、実施の形態7を示す図16において、移動体情報検証装置600の検証部601と処理部701を分割して、移動体情報検証装置600a，移動体情報検証装置600bとした構成である。検証部601を仲介業者の所有する移動体情報検証装置600aに設け、サービス提供者の所有する移動体情報検証装置600bには処理部701のみを設ける。

[0176] 以上の構成において、他の実施の形態と同様の手順にて、仲介業者は「移動体情報」、「装置側固有情報」、「完全性情報」を取得する。そして、検証部601にて「完全性情報」が検証され、改ざんされていないことが確認された「移動体情報」を保管する。サービス提供者は、仲介業者から「移動体情報」を受領して、処理部701で処理する。

[0177] 以上のように、仲介業者が「移動体情報」の完全性を証明し、サービス提供者はその証明された「移動体情報」を利用することができるので、サービス提供者は、サービスの提供にリソースを投入することができる。また、ユーザは、サービス提供者が変わった場合、例えば保険事業者Aから保険事業者Bに変更した場合でも、署名鍵を変更する必要がないので、移動体情報記憶装置3を変更することなく使用し続けることができる。さらに、異なる複数のサービス提供者のサービスを受ける場合、仲介業者は移動体情報記憶装置3からのすべての「移動体情報」を取得し、サービス提供者は必要な情報のみを仲介業者から入手することができるので、移動体情報記憶装置3に複数のサービスに対応した署名鍵や情報を格納する必要がなく、記憶部21の記憶容量を少なくすることができる。

[0178] 実施の形態20.

次に図34を参照して実施の形態20を説明する。実施の形態20は、移動体情報記憶装置3が少なくとも一つのセンサを備える構成である。実施の形態1～実施の形態19では、センサ群2は、移動体1側に装備されていた。図34に示すように、実施の形態20では、センサ群2は、移動体情報記憶装置3の内部に備えられている。

[0179] 実施の形態21.

次に図35、図36を用いて実施の形態21を説明する。実施の形態21は、実施の形態1の移動体情報記憶装置3の動作を、プログラム及びプログラムを記録した記録媒体により実施する実施形態である。

[0180] 前記の実施の形態1においては、移動体情報記憶装置3における「～部」として示した各構成要素の動作は互いに関連しており、動作の関連を考慮しながら、コンピュータに実施させる一連の処理(プログラム)に置き換えることができる。各構成要素の動作を一連の処理に置き換えることにより、情報記憶プログラムの実施形態とすることができる。また、この情報記憶プログラムを、コンピュータ読み取り可能な記録媒体に記録させることで、プログラムを記録したコンピュータ読み取り可能な記録媒体の実施の形態とすることができる。

[0181] 図35は、図2に示した移動体情報記憶装置3の

(1)移動体情報記憶部32の動作、

(2)改ざん防止部20の動作、

(3)完全性情報記憶部33の動作、

コンピュータに実施させるための一連の処理に置き換えて移動体情報記憶プログラムの実施形態としたフローチャートを示す。

[0182] S201は、センサが検出した情報に基づく「移動体情報」(センサ情報)を記憶する処理である。

[0183] S202は、移動体を特定可能な固有情報(特定情報)を取得し、取得した固有情報と記憶した「移動体情報」とに基づいて「完全性情報」(改ざん検証用情報)を生成する処理である。

[0184] プログラムの実施の形態及びプログラムを記録したコンピュータ読み取り可能な記録媒体の実施の形態は、すべてコンピュータで動作可能なプログラムにより構成することができる。

[0185] 図36は、移動体情報記憶装置3の動作を実行するコンピュータシステム805のハードウェア構成図である。図36において、コンピュータシステム805は、プログラムを実行するCPU(Central Processing Unit)810を備えている。CPU810は、バス

825を介してROM811、センサ812、通信ボード813及び磁気ディスク装置820と接続されている。

[0186] 磁気ディスク装置820には、オペレーティングシステム(OS)821、プログラム群823、ファイル群824が記憶されている。プログラム群823は、CPU810、OS821により実行される。

[0187] 上記プログラム群823には、実施の形態1の説明において「～部」として説明した機能を実行するプログラムが記憶されている。プログラムは、CPU810により読み出され実行される。

[0188] また、ファイル群824には実施の形態1で説明した「装置側固有情報」、「移動体情報」「完全性情報」などが記憶されている。

[0189] 図2において「～部」として説明したものは、ROM811に記憶されたファームウェアで実現されていても構わない。或いは、ソフトウェアのみ、或いは、ハードウェアのみ、或いは、ソフトウェアとハードウェアとの組み合わせ、さらには、ファームウェアとの組み合わせで実施されても構わない。

[0190] プログラムの実施の形態及びプログラムを記録したコンピュータ読み取り可能な記録媒体の実施の形態における各処理は、プログラムで実行されるが、このプログラムは、前述のようにプログラム群823に記録されている。そして、プログラム群823からCPU810に読み込まれ、CPU810によって、プログラムの各処理が実行される。また、ソフトウェア、あるいはプログラムは、ROM811に記憶されたファームウェアで実行されても構わない。あるいは、ソフトウェアとファームウェアとハードウェアの組み合わせでプログラムを実行しても構わない。

[0191] この実施の形態21のプログラムは、「移動体情報」と固有情報との完全性を証明する「完全性情報」を生成する処理をコンピュータである移動体情報記憶装置に実行させるので、移動体1と「移動体情報」との対応が明確になり、信頼性の高い「移動体情報」を記憶する移動体情報記憶装置をサービス提供者に提供することができる。

[0192] 以上の実施の形態では、移動状況や移動状態に関わる情報を検出する複数のセンサを有した、人が乗車可能な移動体において、前記センサの情報を記憶する記憶手段と、記憶している情報と移動体の固有情報の改ざんを防止する改ざん防止手段

と、これらの動作を制御する制御手段とを備えた移動体情報記憶装置を説明した。

[0193] 以上の実施の形態では、前記制御手段は、前記センサの情報を演算することを特徴とする移動体情報記憶装置を説明した。

[0194] 以上の実施の形態では、前記移動体情報記憶装置が移動体から分離することを防ぐ分離防止手段を備えたことを特徴とする移動体情報記憶装置を説明した。

[0195] 以上の実施の形態では、前記分離防止手段は、バッテリを備えたことを特徴とする移動体情報記憶装置を説明した。

[0196] 以上の実施の形態では、前記分離防止手段は、分離した場合に移動体情報記憶装置内の情報を消去することを特徴とする移動体情報記憶装置を説明した。

[0197] 以上の実施の形態では、前記移動体情報記憶装置で生成された情報に対する改ざんの有無を検証する検証部を備えたことを特徴とする移動体情報検証装置を説明した。

[0198] 以上の実施の形態では、移動状況や移動状態に関わる情報を検出する複数のセンサを有した、人が乗車可能な移動体において、前記センサの情報を記憶する記憶手段と、記録された情報の改ざんを防止する改ざん防止手段と、これらの動作を制御する制御手段とを備えた移動体情報記憶装置と、及び／または前記センサの情報を演算する演算手段と、及び／または前記移動体情報記憶装置が移動体から分離することを防ぐ分離防止手段と、入力された情報に対する改ざんの有無を検証する検証部とを備えたことを特徴とする移動体情報保証システムを説明した。

[0199] 以上の実施の形態では、移動状況や移動状態に関わる情報を検出する複数のセンサを有した、人が乗車可能な移動体において、前記センサの情報を記録する記録手段と、記録された情報の改ざんを防止する改ざん防止手段と、これらの動作を制御する制御手段とを備えた移動体情報記憶装置と、及び／または前記センサの情報を演算する演算手段と、及び／または前記移動体情報記憶装置が移動体から分離することを防ぐ分離防止手段と、入力された情報に対する改ざんの有無を検証する検証部と、前記検証部の出力を参照して処理を行う処理手段とを備えたことを特徴とする移動体情報保証システムを説明した。

[0200] 以上の実施の形態では、前記移動体情報記憶装置は、移動体外部の機器と通信

する通信手段を備えたことを特徴とする移動体情報記憶装置及び移動体情報保証システムを説明した。

[0201] 以上の実施の形態では、前記通信手段は、通信先を認証し、正しい通信先の場合にのみ通信することを特徴とする移動体情報記憶装置及び移動体情報保証システムを説明した。

[0202] 以上の実施の形態では、前記通信手段は、ICカードと通信し、装置に記憶している情報をICカードに送信することを特徴とする移動体情報記憶装置及び移動体情報保証システムを説明した。

[0203] 以上の実施の形態では、装置内の情報を移動体外部の機器に無線通信にて常時送信することを特徴とする移動体情報記憶装置及び移動体情報保証システムを説明した。

[0204] 以上の実施の形態では、前記移動体情報記憶装置は、前記センサの真正性を確認する手段を備えたことを特徴とする移動体情報記憶装置及び移動体情報保証システムを説明した。

[0205] 以上の実施の形態では、前記移動体情報記憶装置は、設定された範囲外の情報を記録す

ることを特徴とする移動体情報記憶装置及び移動体情報保証システムを説明した。

[0206] 以上の実施の形態では、前記移動体情報記憶装置は、複数のサービス提供者のサービス情報を記録し、前記サービス情報に基づき、複数のサービスに対応した複数の情報を記録することを特徴とする移動体情報記憶装置及び移動体情報保証システムを説明した。

[0207] 以上の実施の形態では、前記移動体情報記憶装置は、複数のサービス提供者のサービス情報を記録し、前記サービス情報に基づき、記録されたすべての移動体情報から選択して必要な情報を取り出すことを特徴とする移動体情報記憶装置及び移動体情報保証システムを説明した。

[0208] 以上の実施の形態では、前記移動体情報記憶装置は、ユーザの指示を受けるマンマシンインタフェース手段を備え、ユーザの指示によって移動体情報を出力することを特徴とする移動体情報記憶装置及び移動体情報保証システムを説明した。

[0209] 以上の実施の形態では、前記移動体情報記憶装置は、移動体情報を出力する際にユーザを認証することを特徴とする移動体情報記憶装置及び移動体情報保証システムを説明した。

[0210] 以上の実施の形態では、前記移動体情報記憶装置は、移動体情報を暗号化する手段を備えたことを特徴とする移動体情報記憶装置及び移動体情報保証システムを説明した。

[0211] 以上の実施の形態では、入力された情報に対する改ざんの有無を検証する検証部と、前記検証部の出力を参照して処理を行う処理手段とを異なるサーバで構成したことを特徴とする移動体情報保証システムを説明した。

[0212] 実施の形態22.

図37～図39を用いて実施の形態22を説明する。実施の形態22は、「環境情報」を収集し記憶する環境情報記憶装置に関する実施形態である。実施の形態22は、実施の形態1に対応する。ここで「環境情報」とは、物の運搬環境や保管環境などにかかわる情報であって、例えば、温度、湿度、照度、空気圧、日時、位置、ゆれ、重量、傾斜、圧力、音、風力、不純物度、扉の開閉などの情報である。

[0213] 図37は、この実施の形態22の環境情報記憶装置2003（情報記憶装置の一例）の構成を示すブロック図である。環境情報記憶装置2003は、複数のセンサ2002a～2002cからなるセンサ群2002の各センサから情報を入力する。具体的には、環境情報記憶装置2003は、車両や鉄道、航空機、船舶など物を運搬可能な交通手段における荷室や荷台、貨物室、コンテナ、あるいは倉庫などの運搬、保管のために物を置く場所に配置されたセンサ群2002の各センサから情報を入力する。

[0214] 図37において、

(1)物2001は、保管中や運搬中の何らかの物である。

(2)センサ群2002を構成する各センサ2002a等は、上記の「荷室や荷台、貨物室、コンテナ、倉庫」などの場所に設置される。各センサ2002a等は、物の運搬環境や保管環境に関わる環境情報を検出する。

(3)環境情報記憶装置2003は、接続されているセンサ2002a等が検出した環境情報を記憶する。

[0215] センサ2002a等は、自身が検出した情報を演算し、演算結果を環境情報として環境情報記憶装置2003に出力しても構わない。あるいは後述の実施の形態23のように、環境情報記憶装置2003は、各センサ2002a等から情報を入力して演算処理し、処理結果を環境情報として記憶する構成でも構わない。あるいは、環境情報記憶装置2003は、センサが検出した演算前の情報を入力し、入力した情報を演算処理することなく環境情報として記憶する構成でも構わない。センサによる演算結果、あるいは環境情報記憶装置2003による演算結果、あるいはセンサから入力した情報としての環境情報には、例えば、設定された範囲外に達した異常な温度や湿度、その回数、扉の開閉回数、運搬中や保管中の映像情報などがある。このように、本明細書において、「環境情報」とは、センサが検出した情報であって演算していない情報、センサ自身が検出であってセンサが演算処理した情報、及びセンサが検出した情報であって環境情報記憶装置2003が演算処理した情報(演算結果)とのいずれをも含むものである。すなわち、「環境情報」(センサ情報の一例)とは、センサから入力した情報に基づく情報である。ここで「基づく」とは、前記のように、センサが検出した情報であって演算処理していない情報と、センサが検出した情報であってセンサが演算処理した情報と、センサが検出した情報であって環境情報記憶装置2003が演算処理した情報とのいずれも含む意味である。

[0216] また、環境情報記憶装置2003は、センサと同じ場所に設置されてもよいし、センサとは別の場所に設置されても構わない。例えば倉庫の場合を例にとれば、センサと環境情報記憶装置2003とを倉庫内に設置してもよいし、環境情報記憶装置2003を倉庫外の事務所などに設置してもよい。

[0217] さらに、センサと環境情報記憶装置2003との間の接続は、有線による接続でも良いし、無線による接続でも構わない。

[0218] 図37を参照して環境情報記憶装置2003の構成を説明する。環境情報記憶装置2003は、環境情報や後述する特定情報、後述する完全性情報を記憶する記憶部2021と、記憶部2021に記録されている環境情報の完全性(改ざんされていないこと)を証明する完全性情報を生成する改ざん防止部2020(改ざん検証用情報生成部の一例)と、これらの動作を制御する制御部2022(情報入力部の一例)とを備える。記

憶部2021は、特定情報を記憶する装置側特定情報記憶部2031と、環境情報を記憶する環境情報記憶部2032(センサ情報記憶部の一例)と、完全性情報を記憶する完全性情報記憶部2033(改ざん検証用情報記憶部の一例)とを備える。記憶部2021は、ハードディスクやEEPROM、RAMなどの半導体メモリを用いて実現することができる。

[0219] 次に、図38を用いて動作を説明する。

(1)環境情報記憶装置2003の制御部2022は、「必要なタイミング」から、センサが検出(S2101)した環境情報の記録を開始する。この「必要なタイミング」は、一例として、交通手段であればエンジン始動時であり、倉庫や貨物室、コンテナであれば扉が閉まった時である。あるいは、この「必要なタイミング」は、環境情報記憶装置2003に別途設けられたスイッチ(図示していない)がオンされた時や、照度センサで明るさを検出し暗くなった時のように、一つあるいは複数のセンサが検出した環境情報が、予め設定された範囲内に入った時など、物の運搬や保管が開始されるタイミングでよい。

(2)制御部2022には、接続しているすべてのセンサが検出した環境情報が入力される。そして、制御部2022は、環境情報を記憶部2021の環境情報記憶部2032に記憶する(S2102)。

(3)装置側特定情報記憶部2031は、予め特定情報を記憶している。ここで「特定情報」とは、センサが配置される環境、あるいは環境情報記憶装置2003が予め装備されることが指定される場所を特定可能な情報であり、具体的には、「特定情報」とは、荷室が一つのトラックなどの運搬自動車であれば、そのナンバープレート情報や車体番号、製造番号などであり、荷室やコンテナを特定できる情報である。そして、改ざん防止部2020は、必要なタイミングに、制御部2022の命令により、記憶部2021の環境情報記憶部2032に記憶されている環境情報と、記憶部2021の装置側特定情報記憶部2031に記憶されているその環境を特定できる特定情報とを基に、完全性情報を生成する(S2103)。

(4)ここで「完全性情報」(改ざん検証用情報の一例)とは、環境情報などが改ざんされているかどうかを検証するために使用する情報である。本実施の形態22では、改

ざん防止部2020は、環境情報と特定情報とを基に完全性情報を生成する。この場合、完全性情報は、特定情報と環境情報との少なくともいずれかに対する改ざんの有無を検証するために使用される。また、実施の形態27の図49で後述するように、改ざん防止部2020は、環境情報を基に完全性情報を生成しても構わない。この場合、完全性情報は、環境情報に対する改ざんの有無を検証するために使用される。完全性情報を生成する方法としては、一例として、デジタル署名がある。改ざん防止部2020が生成する「完全性情報」の具体例は、実施の形態26で後述する。

(5)生成された完全性情報は、記憶部2021の完全性情報記憶部2033に記憶される。あるいは完全性情報記憶部2033に記憶された完全性情報は、環境情報記憶装置2003の外へ環境情報と共に出力される。これらは、環境情報記憶装置2003が適用されているシステムに依存する。環境情報記録装置20003の制御部2022は、改ざん防止部2020の生成した完全情報を完全性情報記憶部2033に記録する際、完全性情報と、その生成の基になった環境情報との対応関係を管理する。この管理により、完全性情報とその生成の基になった環境情報との対応関係が明確になる(S2104)。

(6)図39は、環境情報と完全性情報との対応関係の管理例を示す。図39において、「環境情報a」は「完全性情報a」に対応し、「環境情報b」は「完全性情報b」に対応する。「環境情報c」については、対応する完全性情報がまだ生成されていない状態を表している。このような管理により、完全性情報とその生成の基になった環境情報との対応関係が明確になる。

(7)完全性情報の生成タイミングは、本実施の形態22の環境情報記憶装置2003の適用先に依存するが、例えば、扉の開閉などのイベント発生時に完全性情報が生成されていない環境情報が記憶部2021にあった時や、環境情報を環境情報記憶装置2003外に出力する時、環境情報が環境情報記憶装置2003に入力された時、予め設定されたイベントが発生した時などがある。

[0220] 以上のように、環境情報記憶装置2003の内部にて、改ざん防止部2020が環境情報の完全性を証明する完全性情報を生成するので、環境情報を記憶する信頼性の高い環境情報記憶装置を実現することができる。

[0221] 実施の形態23.

次に、図40を用いて実施の形態23を説明する。実施の形態23は、環境情報記憶装置2003の制御部2022が、センサの検出した信号を処理する実施形態である。本実施の形態23は、実施の形態2に対応する。

[0222] 図40は、本実施の形態23の環境情報記憶装置2003の構成を示す。図40の環境情報記憶装置2003は、図37の環境情報記憶装置2003と同様の構成であるが、図40の場合、制御部2022が、接続されているセンサの検出した情報を処理する装置側演算部2201を備える点が異なる。このような構成において、制御部2022は、センサが検出した情報を装置側演算部2201により処理し、処理結果を環境情報として記憶部2021の環境情報記憶部2032に記憶する。このような処理結果で得られる情報には、例えば、環境情報が設定された範囲外に達した時の情報や、イベントが発生した時の環境情報やその回数、扉の開閉回数、運搬中や保管中の映像情報などがある。

[0223] 以上のように、制御部2022が、センサの検出した信号を演算処理する装置側演算部2201を備えたので、取得するべき情報によっては、センサを追加することなく多種多様の移動状況や移動状態を取得して記憶できる。また、環境情報記憶装置2003は、設定された範囲外の環境情報やイベントが発生した回数だけを環境情報記憶部2032に記録できるので、環境情報記憶装置2003のメモリ容量を減らすことができる。

[0224] なお、本実施の形態23では演算結果を環境情報として記憶しているが、センサが検出した情報も合わせて環境情報として記憶する構成でもよい。

[0225] また、以降の実施の形態における環境情報は、センサが検出した情報(演算処理していない情報、演算処理した情報)、及び制御部2022が演算した結果のいずれをも含むものとする。

[0226] 実施の形態24.

次に図41、図42を参照して実施の形態24を説明する。実施の形態22、実施の形態23では、環境情報記憶装置2003が、運搬中や保管中の物の環境情報を記憶する場合を説明した。しかし、実際に運搬中や保管中の物が、その環境に存在している

ことを確認していない。そこで、実施の形態24は、物と環境との対応関係を明確にする構成を説明する。

[0227] 図41は、運搬中や保管中の物を置いておく場所における、本実施の形態24の環境情報記憶装置2003の構成を示すブロック図である。図41の環境情報記憶装置2003は、図37に示した実施の形態22の環境情報記憶装置2003に対し、さらに、物2001の存在を検出する存在検出部2023を備える。

[0228] 存在検出部2023は、物2001の存在を検出した場合に存在情報を出力する。図41の構成において、環境情報記憶装置2003は、存在検出部2023が出力した存在情報を環境情報とともに記憶部2021の環境情報記憶部2032に記憶する。そして、改ざん防止部2020は、環境情報と、特定情報と存在情報とをまとめた情報に対して完全性情報を生成する。

即ち、実施の形態22では、改ざん防止部2020は、

「環境情報＋特定情報→完全性情報」

のように、環境情報と特定情報とから完全性情報を生成した。

これに対して実施の形態24では、改ざん防止部2020は、

「環境情報＋特定情報＋存在情報→完全性情報」

のように、環境情報と特定情報と存在情報とから完全性情報を生成する。環境情報と特定情報と存在情報とから生成される完全性情報は、環境情報と特定情報と存在情報とのうち、少なくともいずれかに対する改ざんの有無を検証するために使用する情報である。

[0229] さらに具体的な場合を説明する。図42は、運搬中や保管中の物を置いておく場所における、この実施の形態24の環境情報記憶装置2003とセンサとの構成を示すブロック図である。

(1)倉庫／コンテナ2040は、運搬中や保管中の物2001を置いておく倉庫あるいはコンテナを示す。

(2)扉／蓋2041は、倉庫やコンテナに設けられた扉や蓋を示す。

(3)開閉検知センサ2042は、扉や蓋の開閉を検知する。

(4)無線タグ2043は、物2001に搭載されるとともに、ユニークな識別情報を有する。

(5)無線タグリーダ2044は、無線タグ2043の識別情報を読み取る。

(6)識別情報比較部2045は、制御部2022に接続している。また、識別情報比較部2045は、無線タグリーダ2044から識別情報を入力し、前回入力した識別情報と今回入力した識別情報とを比較し、比較結果を存在情報として環境情報記憶部2032に出力する。図41の存在検出部2023は、無線タグ2043と、無線タグリーダ2044と、識別情報比較部2045とにより構成される。

(7)なお、実施の形態22で述べたように、環境情報記憶装置2003は、倉庫やコンテナの外に設置されてもよい。

[0230] 図42のような構成において、扉／蓋2041が開いて物2001が運び込まれると、環境情報記憶装置2003の制御部2022は、開閉検知センサ2042からの信号により、扉が開いたことを検知する。この検知に連動して、識別情報比較部2045は、無線タグリーダ2044を介して無線タグ2043の識別情報を読み取り、記録する。識別情報比較部2045は、物2001が複数ある場合には、無線タグリーダ2044を介して、それぞれの物に取り付けられたすべての無線タグの識別情報を読み取る。また、環境情報記憶装置2003の制御部2022は、環境情報の記録を開始する。

[0231] 運搬中や保管中、識別情報比較部2045は、無線タグリーダ2044を介して、必要なタイミングで、無線タグ2043の識別情報を読み取る。このタイミングは、常時読み取り続けてもよいし、一定時間毎でもよいし、また、扉や蓋が開閉した場合や、完全性情報を作成する場合でもよい。そして、環境情報記憶装置2003の識別情報比較部2045は、無線タグリーダ2044が最初に読み取った識別情報よりも後の識別情報、すなわち2回目以降に読み取った識別情報と最初に読み取った識別情報とを比較し、その比較結果を「存在情報」として出力する。また、改ざん防止部2020が完全性情報を作成する時に無線タグリーダ2044が識別情報を読み取る場合には、改ざん防止部2020は、無線タグリーダ2044が読み取った識別情報を存在情報として、この存在情報と環境情報とを基に完全性情報を作成してもよい。このように識別情報をそのまま存在情報として用いる場合には、識別情報比較部2045は、無線タグリーダ2044から入力した識別情報をそのまま記憶部2021の環境情報記憶部2032へ出力する。

[0232] 以上のように、環境情報記憶装置は存在検出部を備えたので、環境情報記憶装置の記録している環境に物が存在しているかどうかを検出することができる。このため、環境情報と物との対応関係を確実にすることができ、より信頼性の高い環境情報記憶装置を実現することができる。

[0233] 実施の形態25.

次に図43を用いて実施の形態25を説明する。実施の形態25は、環境情報記憶装置2003が複数のセンサ群の各センサから情報を入力する実施形態である。以上の実施の形態22～実施の形態24では、倉庫やコンテナに配置された一つのセンサ群に対して、一つの環境情報記憶装置を設置していた。これに対して、実施の形態25は、複数のセンサ群に対して、一つの環境情報記憶装置を設置する場合である。

[0234] 図43は、運搬中や保管中の物2001を置いておく場所における、本実施の形態25の環境情報記憶装置2003とセンサとの構成を示すブロック図である。図43に示すように、環境情報記憶装置2003は、倉庫／コンテナ2040a，倉庫／コンテナ2040bの外部に設置される。そして、倉庫あるいは、コンテナの内部に配置されたセンサ群2002－1及びセンサ群2002－2の各センサと環境情報記憶装置2003とを接続する。図43に示すように、センサ群2002－1は物2001aに対応し、センサ群2002－2は物2001bに対応する。なお、実施の形態24と同様に、存在検出部2023を倉庫やコンテナに設置して、一つの環境情報記憶装置2003に接続しても良い。

[0235] このような構成において、環境情報記憶装置2003は、倉庫やコンテナに設置されたセンサ群2002－1，センサ群2002－2の各センサから環境情報を取得し、記憶する。そして、環境情報記憶装置2003は、センサ群2002－1の各センサから取得した環境情報については、倉庫／コンテナ2040aを特定することができる特定情報を基に完全性情報を生成する。また、環境情報記憶装置2003は、センサ群2002－2の各センサから取得した環境情報については、倉庫／コンテナ2040bを特定することができる特定情報を基に完全性情報を生成する。

[0236] 以上のように、実施の形態25の環境情報記憶装置は、複数の倉庫やコンテナなどの互いに異なる環境に配置された複数のセンサ群から環境情報を取得して記録する。このため、環境情報記憶装置のコストを低減することができる。

[0237] 実施の形態26.

次に図44～図46を用いて実施の形態26を説明する。実施の形態26は、環境情報記憶装置2003と、環境情報記憶装置2003から環境情報、特定情報及び完全性情報を入力して環境情報及び特定情報の正当性を検証する端末装置2600(検証装置の一例)とを備えた環境情報保証システム2000に関する。この実施の形態26は、実施の形態6に対応する。

[0238] 以上の実施の形態22～実施の形態25は、環境情報記憶装置2003に関するものであった。この実施の形態26は、環境情報記憶装置2003と端末装置2600とを備えた環境情報保証システム2000において、端末装置2600が、環境情報及び特定情報の正当性を検証する検証部2601を備えた場合を説明する。

[0239] 図44は、本実施の形態26における環境情報保証システム2000の構成を示すブロック図である。図44において、端末装置2600は、環境情報が改ざんされていないことを検証する確認者が使用可能な端末装置である。端末装置2600は、例えば、携帯電話やPC(Personal Computer)である。確認者は、依頼者、使用者の他、公的に認められた第三者機関である。端末装置2600の検証部2601は、環境情報が改ざんされているかどうかを検証する。なお、他の実施の形態と同様に、環境情報記憶装置2003は、存在検出部2023を備えてもよい。

[0240] 次に動作を説明する。環境情報記憶装置2003の動作は、実施の形態22～実施の形態25と同様である。すなわち、環境情報記憶装置2003は、環境情報や特定情報を保管し、あるいは場合によっては実施の形態24で述べた存在情報を保管し、完全性情報を生成する。そして、端末装置2600は、検証部2601が完全性情報を用いて、環境情報や存在情報が改ざんされていないことを検証する。以下に図45を参照して検証の流れを説明する。

[0241] (検証の例)

図45は、改ざん防止部2020と検証部2601とのやり取りのフローである。図45は、デジタル署名を用いた例を示している。改ざん防止部2020による完全性情報の生成は、実施の形態22の場合に対応する。このデジタル署名は、完全性情報を生成する場合の一例である。

[0242] (環境情報記憶装置2003)

(1)改ざん防止部2020は、環境情報(存在情報を含んでもよい)と完全性情報とをハッシュ関数に入力してハッシュ値を求める(S2001)。本実施の形態26では、環境情報に存在情報を含まない場合を説明する。改ざん防止部2020は、そのハッシュ値を署名鍵で暗号化して完全性情報を生成する(S2002)。署名鍵は、端末装置2600が持つ検証鍵と対応したものが予め環境情報記憶装置2003の記憶部2021に格納されている。

[0243] (端末装置2600)

(2)端末装置2600は、環境情報、完全性情報及び完全性情報を取得する。取得方法は、記憶媒体を介して取得してもよいし、端末装置2600と環境情報記憶装置2003との通信によって取得してもよい。

(3)端末装置2600の検証部2601は、取得した環境情報と特定情報とから、改ざん防止部2020と同様にハッシュ値を求める(S2003)。

(4)一方で、検証部2601は、環境情報記憶装置2003から取得した完全性情報を予め格納している検証鍵で復号し(S2004)、前記ハッシュ値と復号結果のハッシュ値とを比較する(S2005)。

(5)検証部2601は、比較した結果、ハッシュ値どうしを同一と認めれば、環境情報は正当な情報、すなわち改ざんされていないと判断する。ハッシュ値どうしが異なっていた場合、検証部2601は、環境情報もしくは完全性情報とのうち少なくともいずれかは改ざんされていると判断する。

[0244] (検証の別の例)

また、図46は、検証の別の例を示す図である。図46は、環境情報と特定情報とのそれぞれから完全性情報を生成する場合における、改ざん防止部2020と検証部2601とのやり取りの別の例を示す。この例では、デジタル署名を用いた例を示している。

[0245] (環境情報記憶装置2003)

(1)改ざん防止部2020は、環境情報(存在情報を含んでもよい)をハッシュ関数に入力してハッシュ値aを求める(S2001a)。

(2)同様に、改ざん防止部2020は、特定情報のハッシュ値bを求める(S2001b)。

(3)そして、改ざん防止部2020は、環境情報のハッシュ値aと、特定情報のハッシュ値bとをそれぞれ署名鍵で暗号化し、環境情報に対応する「完全性情報a」と、特定情報に対応する「完全性情報b」とを生成する(S2002a、S2002b)。

[0246] (端末装置2600)

(4)端末装置2600は、環境情報、特定情報、完全性情報a、完全性情報bを取得する。取得方法は、記憶媒体を介してもよいし、端末装置2600と環境情報記憶装置2003との通信によってもよい。

(5)次に、端末装置2600の検証部2601は、改ざん防止部2020と同様に、環境情報から「ハッシュ値a」を求めるとともに、特定情報から「ハッシュ値b」を求める(S2003a、S2003b)。

(6)一方で検証部2601は、「完全性情報a」及び「完全性情報b」を検証鍵で復号し(S2004a、S2004b)、「ハッシュ値a」及び「ハッシュ値b」と、復号結果のハッシュ値とをそれぞれについて比較する(S2005a、S2005b)。

(7)検証部2601は、比較した結果、それぞれの対応するべきハッシュ値どうしが同一であると判断した場合、環境情報と特定情報とは正当な情報、すなわち改ざんされていないと判断する。検証部2601は、比較の結果、異なっていると判断した場合、異なっていると判断した情報は、改ざんされていると判断する。なお、この別の例は、環境情報に存在情報を含むことが可能な例を示しているが、環境情報に存在情報を含むことなく存在情報を基にする完全性情報を生成してもよい。

[0247] なお、本実施の形態26ではデジタル署名を用いた例を示したが、環境情報(存在情報を含んでも良い)、特定情報、あるいは存在情報が改ざんされていないことを確認する完全性情報を生成できればよく、他にも例えばメッセージ認証子や電子透かしやCRC(Cyclic Redundancy Check)を用いてもよい。

[0248] 以上のように、端末装置2600は、検証部2601を備えたので、業者ではない確認者が環境情報、存在情報、特定情報が改ざんされていないことを検証できる。このため、信頼性の高い環境情報保証システムが実現できる。

[0249] 実施の形態27.

次に図47～図50を用いて実施の形態27を説明する。実施の形態27は、実施の形態26の環境情報保証システム2000において、環境情報記憶装置2003と端末装置2600とが、通信する構成である。本実施の形態27は、実施の形態8に対応する。

[0250] 図47は、実施の形態27の環境情報保証システム2000の構成を示すブロック図である。本実施の形態27の環境情報記憶装置2003は、図37に示す実施の形態22の環境情報記憶装置2003に対して、さらに、端末装置2600と通信する記憶側通信部2801（出力部の一例）を備えた。また、本実施の形態27の端末装置2600は、図44に示す実施の形態26の端末装置2600に対して、さらに、環境情報記憶装置2003と通信を行なう検証側通信部2802と、環境情報などを処理する処理部2701とを備えた。

（1）記憶側通信部2801(出力部の一例)は、環境情報記憶装置2003に設けられた通信部であって、無線・有線LAN（Local Area Network）、RS232C、Blue tooth（登録商標）、DSRC（Dedicated Short Range Communication）、携帯電話などを利用して、環境情報記憶装置2003の外部機器と通信する。

（2）また、端末装置2600の検証側通信部2802は、記憶側通信部2801から送信された情報を受信する。図47では、検証側通信部2802が、記憶側通信部2801から送信された情報を直接に受信する。これは一例であり、検証側通信部2802は、通信経路上に設けられた中継器を介して記憶側通信部2801から情報を受信してもよい。

（3）処理部2701は、環境情報を処理する。例えば、処理部2701は、環境情報を基に運搬中や保管中の環境状態を表示し、あるいは環境情報の異常な場合を検索して表示する。

（4）なお、他の実施の形態と同様に、環境情報記憶装置2003は、存在検出部2023を備えても良い。

[0251] 次に、図48、図49を参照して動作を説明する。図48は、本実施の形態27の環境情報保証システムにおける環境情報記憶装置と確認者が使用可能な端末間のフローを示したものである。本実施の形態27の環境情報記憶装置2003は、図49に示すように環境情報に基づき完全性情報を生成する。

[0252] （環境情報記憶装置2003）

(1)環境情報記憶装置2003は、環境情報を記録する(S2010)。

(2)そして、改ざん防止部2020は、必要なタイミングで、図49のS2031とS2032に示すように、完全性情報を生成する(S2011)。改ざん防止部2020は、環境情報をハッシュする。

(3)記憶側通信部2801は、環境情報と完全性情報とを端末装置2600に送信する(S2012)。

[0253] (端末装置2600)

(4)確認者が使用可能な端末装置2600は、検証側通信部2802が環境情報と完全性情報とを受信する(S2013)。

(5)検証部2601は、図49のS2033～S2035に示すように、完全性情報の検証を行う(S2014)。

(6)その後、検証部2601による認証結果が正当である場合には、処理部2701が、環境情報を処理する(S2015)。

[0254] 上記(1)～(6)の例では、環境情報記憶装置2003は、完全性情報を作成した後、環境情報と完全性情報とを送信する(S2011, S2012)。しかし、図39に示したように、環境情報記憶装置2003は、複数の完全性情報を作成した後、複数の完全性情報とこれらに対応する環境情報とをまとめて送信してもよい。すなわち、環境情報記憶装置2003が完全性情報を作成するタイミングと、環境情報と完全性情報とを送信するタイミングとは、次の(a)～(e)のうちのいずれでも構わない。

(a)常時、(b)運搬や保管が終わった時、(c)予め設定されたイベント発生時、(d)一定時間毎、(e)通信可能時。

[0255] なお、図48では端末装置2600において検証された後に環境情報を処理するフローを示した(S2014、S2015)。しかし、端末装置2600は、受信した環境情報を処理し、必要に応じて環境情報を処理して検証するフローでも構わない。

[0256] 図50は、本実施の形態27における環境情報保証システム2000の他の構成を示すブロック図である。図50は、図47の端末装置2600を端末装置2600aと端末装置2600bとに分けた構成である。図50に示すように、第一の端末装置2600aは、検証側通信部2802と処理部2701とを備える。また、第二の端末装置2600bは、検証部

2601を備える。このような構成の場合、依頼者や使用者が第一の端末装置2600a(例えば携帯電話)を用いて環境情報から環境状態を確認する。そして、必要に応じて、公的に認められた第三者機関が、確認者として第二の端末装置2006b(検証装置)を用いて完全性情報を検証することにより環境情報の正当性を検証する。

[0257] 以上のように、実施の形態27の環境情報記憶装置2003は、環境情報と完全性情報とを記憶側通信部2801により外部の装置に送信する。外部の装置は、これらの情報を検証・処理できるので、利便性が高い環境情報保証システムを実現することができる。

[0258] 実施の形態28.

次に図51を参照して実施の形態28を説明する。実施の形態28は、環境情報保証システム2000において、環境情報記憶装置2003が、内部にセンサを備えた実施形態である。実施の形態28は、実施の形態20に相当する。

[0259] 図51は、本実施の形態28の環境情報保証システム2000の構成を示すブロック図である。図51において、環境情報を検出するセンサ2002a、センサ2002b、センサ2002c等は、環境情報記憶装置2003の内部に設けられている。環境情報記憶装置2003は、物が置かれている環境に設置されても良いし、物に取り付けられても良い。

[0260] 次に、本実施の形態28の環境情報記憶装置2003の動作を説明するが、環境情報記憶装置2003がセンサ2002a等を内部に備える他は、実施の形態22と同様である。

[0261] 環境情報記憶装置2003は、必要なタイミングから、センサ2002a等が検出した環境情報の記録を開始する。このタイミングは、交通手段であればエンジン始動時、倉庫や貨物室、コンテナの扉が閉まった時、環境情報記憶装置2003に別途設けられたスイッチをオンした時、照度センサで明るさを検出し暗くなった時のように、一つあるいは複数のセンサの環境情報が設定された範囲内に入った時など、運搬や保管が開始されるタイミングでよい。

[0262] 制御部2022には、接続しているすべてのセンサが検出した環境情報が入力される。そして、制御部2022は、環境情報を記憶部2021の装置側特定情報記憶部2031に記憶する。そして、必要なタイミングに、制御部2022の命令により、改ざん防止部

2020は、実施の形態27を示す図49に示したのS2031、S2032と同様に、装置側特定情報記憶部2031に記憶されている環境情報の完全性情報を生成する。そして、完全性情報と環境情報は、記憶側通信部2801を介して送信される。確認者が使用可能な端末装置2600は、検証側通信部2802が、環境情報と完全性情報とを受信する。そして、検証部2601が完全性情報の検証を行い、また処理部2701が環境情報の処理を行う。

[0263] 本実施の形態28では、完全性情報を作成した後、環境情報と完全性情報を送信しているが、複数の完全性情報を作成した後、まとめて送信するようにしてもよい。すなわち、完全性情報の作成するタイミングと、環境情報と完全性情報を送信するタイミングは以下の(a)～(e)のどのタイミングでも構わない。(a)常時、(b)運搬や保管が終わった時、(c)予め設定されたイベント発生時、(d)一定時間毎、(e)通信可能時。さらに、図50に示すように、検証側通信部2802と処理部2701とを有する第一の端末装置2600aと、検証部2601を有する別の第二の端末装置2600bとに分ける構成でもよい。

[0264] 以上のように、環境情報記憶装置2003がセンサを内部に持つにより、荷室や荷台、貨物室、コンテナ、倉庫などに新たにセンサを設置するなどの改修の必要ないので、低コストで信頼性の高い環境情報保証システムを実現することができる。

[0265] 実施の形態29.

次に図52、図53を用いて実施の形態29を説明する。以上の実施の形態27、実施の形態28では、環境情報記憶装置2003が、不正な端末装置2600に情報を送信する可能性があった。そこで、本実施の形態29では、環境情報記憶装置2003が、記憶側通信部2801に通信先認証部2901(出力先認証部の一例)を備えた構成を説明する。本実施の形態29は、実施の形態9に対応する。

[0266] 図52は、本実施の形態29の環境情報保証システム2000の構成を示すブロック図である。図52は、図51に対して、記憶側通信部2801が通信先認証部2901を備えた点が異なる。通信先認証部2901は、通信先を認証する。なお、他の実施の形態と同様に、環境情報記憶装置2003は、存在検出部2023を備えても良いし、内部にセンサを備えてもよい。

[0267] 次に動作を説明する。本実施の形態29の環境情報保証システム2000の動作は、他の実施の形態と同様である。すなわち、環境情報記憶装置2003は、環境情報を記録し、完全性情報を生成する。そして、環境情報記憶装置2003は、記憶側通信部2801を介して端末装置2600に環境情報と完全性情報とを転送する。本実施の形態29の特徴は、この転送前に、通信先認証部2901が通信先である端末装置2600を認証する点にある。

[0268] 図53は、通信先認証部2901による認証方法の一例を示す図である。図53において、環境情報記憶装置2003と端末装置2600とは、暗号鍵を持っているものとする。

(1)通信先認証部2901は、乱数(R)を生成し(S2020)、端末装置2600に送信する(S2021)。

(2)端末装置2600は、乱数(R)を受信(S2022)し、暗号化(e(R))した後(S2023)、環境情報記憶装置2003に送信する(S2024)。

(3)環境情報記憶装置2003の通信先認証部2901は、応答データ(e(R´))を受信し(S2025)、それを復号し(S2026)、先に生成した乱数(R)と比較する(S2027)。

(4)比較結果が一致していた場合(S2028)、正常終了し、一致していない場合(S2029)、異常終了する。

[0269] なお、本実施の形態29では、環境情報記憶装置2003の通信先認証部2901は、受信した暗号化された乱数を復号した後に、比較を行っている(S2027)。しかし、これは一例であり、通信先認証部2901は、自己の生成した乱数を暗号化し、その結果と端末装置2600から受信した暗号化された乱数とを比較しても良い。そして、認証が成功した場合、記憶側通信部2801は、環境情報と完全性情報とを端末装置2600に送信する。端末装置2600は、検証側通信部2802にて受信した環境情報と完全性情報とを使用して、検証及び処理を行う。認証が失敗した場合、記憶側通信部2801は端末装置2600と通信を行わなず、記憶部2021に認証失敗の情報を記録する。

[0270] 本実施の形態29では、端末装置で暗号化した乱数を通信先認証部2901で確認しているが(S2027)、端末装置は受信した乱数に対してメッセージ認証子やデジタル署名を生成して環境情報記憶装置2003に返信し、環境情報記憶装置2003の通

信先認証部2901が、それらを検証する方法でも良い。

[0271] 以上のように、記憶側通信部2801が、通信先を認証するとともに、正しい通信先であることを確認した後、環境情報と完全性情報とを通信先に送信するので、環境情報や完全性情報を解析するなどの不正行為を防ぐことができ、さらに信頼性の高い環境情報記憶装置や環境情報保証システムを実現できる。

[0272] 実施の形態30.

次に図54、図55を用いて実施の形態30を説明する。以上の実施の形態22～実施の形態29では、環境情報記憶装置2003から出力される情報の完全性(改ざんされていないこと)を証明していた。しかし、センサが改ざんされた場合には、センサの改ざんを検出できない。そこで、本実施の形態30は、センサが正当なものかどうかを確認する実施形態を示す。本実施の形態30は、実施の形態12に対応する。

[0273] 図54は、本実施の形態30の環境情報記憶装置2003の構成を示す。図54の環境情報記憶装置2003は、図37に示した実施の形態22の環境情報記憶装置2003と同様の構成であるが、制御部2022(センサ確認部の一例)が、それぞれのセンサが正当かどうかを確認する機能を有する点が異なる。なお、制御部2022が、センサの正当性を検出するが、他の構成要素がセンサの正当性を確認する構成でも構わない。また、他の実施の形態と同様に、環境情報記憶装置2003は、存在検出部2023や通信先認証部2901を備えてもよい。また、環境情報記憶装置2003は、内部にセンサを備えても良い。

[0274] 次に図55を用いて動作を説明する。制御部2022は、必要なタイミングで、接続されているセンサの確認を行う。図55は、確認方法の一例を示すフローチャートである。

[0275] (1)センサは、センサ固有の「固有情報」(以下、センサ側固有情報という)を保持しているものとする。環境情報記憶装置2003は、この「センサ側固有情報」に対応する「記憶装置側固有情報」を格納しているものとする。センサが改ざんされていない正規品であれば、「センサ側固有情報」と「記憶装置側固有情報」とは一致する。制御部2022は、必要なタイミングで、センサから「センサ側固有情報」を取得する(S2040)。(2)そして、制御部2022は、取得した「センサ側固有情報」と保管されている「記憶

装置側固有情報」との比較を行う(S2041)。

(3)制御部2022は、比較結果が一致した場合、正常と判断して正常終了(S2042)し、記憶部2021に正常終了した内容を記録する。制御部2022は、比較結果が一致しない場合や、「センサ側固有情報」を取得できない場合は、異常と判断して終了(S2043)し、記憶部2021に異常終了した旨を記録する。制御部2022は、以上の処理を接続されているすべてのセンサに対して行う。

[0276] 以上のように、環境情報記憶装置2003の制御部2022は、センサが正当であることを確認するので、センサに対する不正を防ぎ、さらに信頼性の高い環境情報記憶装置や環境情報保証システムを実現できる。

[0277] 実施の形態31.

次に図56を用いて実施の形態31を説明する。以上の実施の形態22～実施の形態30は、環境情報の完全性のみを維持するシステムであるが、機密性が維持されていない。すなわち、環境情報は、第三者に盗聴される恐れがある。そこで、本実施の形態31は、環境情報の機密性を維持する場合を示す。本実施の形態31は、実施の形態18に対応する。

[0278] 図56は、本実施の形態31の環境情報保証システム2000の構成を示すブロック図である。図56では、実施の形態26の図44に対して、環境情報記憶装置2003が暗号部3801を備えるとともに、端末装置2600が復号部3802を備えた構成である。暗号部3801は、環境情報を暗号化する。復号部3802は、取得した情報を復号する。なお、他の実施の形態と同様に、環境情報記憶装置2003は、存在検出部2023、通信先認証部2901、あるいはセンサを確認する機能を備えてもよい。また、環境情報記憶装置2003は、内部にセンサを備えてもよい。

[0279] 図56に示す構成において、環境情報記憶装置2003は、環境情報を出力する前や、完全性情報を作成した後に、暗号部3801により環境情報を暗号化する。本実施の形態31は、環境情報を暗号対象するが、特定情報や完全性情報などの他の情報を含めて暗号化してもよい。そして、暗号化され出力された環境情報は、端末装置2600の復号部3802により復号され、他の実施の形態と同じように検証される。

[0280] このように、本実施の形態31の環境情報記憶装置2003は、暗号部3801により暗

号化された環境情報を出力するので、通信経路で環境情報を盗聴された場合でも、環境情報の機密性を維持可能な環境情報記憶装置や環境情報保証システムを実現することができる。

[0281] 実施の形態32.

次に図57を参照して実施の形態32を説明する。本実施の形態32は、環境情報記憶装置2003が後述の格納情報を格納する実施形態である。

[0282] 以上の実施の形態22～実施の形態31では、環境を特定するための特定情報(実施の形態22)、認証に使用する鍵(実施の形態29)や暗号化で使用する暗号鍵(実施の形態31)などの情報は、事前に環境情報記憶装置2003に格納されているとして説明した。これら特定情報などのような事前に環境情報記憶装置に格納される「格納情報」は、システムを運用する組織や環境によって異なる。このため、それぞれの環境情報記憶装置2003は、通常、異なる値を持つ。また、一旦格納された格納情報は、格納後に変更が必要となるケースもある。従って、格納情報は、環境情報記憶装置の出荷後に記録・変更できなければならない。

[0283] 一方、格納情報は、環境情報の完全性を維持するシステムでは重要な情報である。このため、環境情報記憶装置2003への格納情報の格納は、正当な組織やそれに属する人、正当な端末、機器によって行われるべきである。もしくは、正しい格納情報だけが、格納情報として格納されなければならない。そこで、次に、格納情報を環境情報記憶装置2003に格納する実施形態を示す。

[0284] 図57は、本実施の形態32の環境情報記憶装置2003の構成を示すブロック図である。図57の環境情報記憶装置2003は、図37に示す実施の形態22の環境情報記憶装置2003に対して、さらに、外部インタフェース部2051と格納制御部2052とを備えている。

(1)格納機器2050は、接触式・非接触式ICカードやPC(Personal Computer)のような、外部インタフェース部2051と通信して格納情報を環境情報記憶装置2003に転送する機器である。

(2)外部インタフェース部2051は、接触式・非接触式ICカードインタフェース、無線・有線LANのインタフェース、RS232Cのインタフェース、Blue tooth(登録商標)の

インタフェースなど、格納情報を格納するために環境情報記憶装置2003に設けられたインタフェースである。

(3)格納制御部2052は、外部インタフェース部2051を介して格納機器の正当性及び／または転送された格納情報の正当性を確認する。

(4)なお、他の実施の形態と同様に、環境情報記憶装置2003は、存在検出部2023、通信先認証部2901、あるいはセンサを確認する機能を備えてもよい。また、環境情報記憶装置2003は、内部にセンサを備えてもよい。

[0285] (格納機器の認証)

このような図57の構成において、環境情報記憶装置2003は、格納機器2050から転送された格納情報を格納する前に、格納制御部2052が格納機器を認証する。格納制御部2052は、外部インタフェース部2051が格納機器2050から格納情報(所定の情報)を入力する場合に、格納機器2050との間で通信を行うことにより格納機器2050が正当であるかどうかを認証し、正当と判断した場合に、格納情報を装置側特定情報記憶部2031に記憶する。格納制御部2052は、格納情報を入力する前に格納機器2050を認証し、正当な場合にのみ格納機器2050から格納情報を入力する。あるいは、格納制御部2052は、格納制御部2052から格納情報を入力後に格納制御部2052を認証し、正当な場合にのみ格納情報を格納するようにしてもよい。格納機器2050の認証方法は、事前に環境情報記憶装置2003に格納された暗証番号による方法、実施の形態29の図53で示した認証方法などがある。この認証に使用する暗証番号や暗号化で使用する暗号鍵は、環境情報記憶装置2003の製造時に格納しておけばよい。格納制御部2052は、この認証により、正当な格納機器であれば、転送された格納情報を記憶部2021に格納する。

[0286] (格納情報の認証)

また、環境情報記憶装置2003は、格納機器から転送された格納情報を格納する前に、格納制御部2052が、これらの格納情報の正当性を確認してもよい。すなわち、格納制御部2052は、外部インタフェース部2051が入力した格納情報が正当であるかどうかを認証し、格納情報を正当と判断した場合に、格納情報を装置側特定情報記憶部2031に記憶する。この場合の認証方法は、実施の形態26の図45、図46

などで述べた完全性情報の完全性を維持する方法と同様の方法を利用すればよい。すなわち、格納情報の完全性(改ざんの有無)を確認する方法である。

[0287] なお、格納機器2050の認証や格納情報の確認は、それぞれどちらを実施してもよい。また両者の認証を組み合わせて使用してもよい。また、格納機器2050から転送される格納情報は、実施の形態31のように暗号化してもよい。

[0288] なお、図57では、格納制御部2052は、制御部2022、記憶部2021、改ざん防止部2020と接続している。しかしこれは一例であり、格納制御部2052は、記憶部2021にのみ接続するような構成でもよい。

[0289] このように、実施の形態32の環境情報記憶装置2003は格納制御部を備えたので、正当な組織やそれに属する人、正当な端末、機器による格納情報が格納され、あるいは正当な格納情報だけが格納される。このため、実施の形態32の環境情報記憶装置2003は、システムの利便性を向上すると共に、より安全な環境情報保証システムを実現できる。また、格納制御部2052が使用する暗証番号や暗号鍵などを変更する際にも、本手段を用いた手続きを経た上で変更可能な構成とすることで、環境情報記憶装置2003の信頼性・安全性を向上させると共に利便性も向上させることができる。

[0290] 実施の形態33.

次に、図58を参照して実施の形態33を説明する。実施の形態33は、環境情報記憶装置2003が日時に関する情報を生成する時計部2060を備えた実施形態である。

[0291] 図58は、実施の形態33の環境情報記憶装置2003の構成を示す図である。実施の形態33の環境情報記憶装置2003は、図37に示す実施の形態22の環境情報記憶装置2003に対して、さらに、時計部2060を備えた点が異なる。

[0292] 時計部2060は、制御部2022に接続されているとともに、日時に関する情報、例えば、日付と時刻とを生成する。なお、他の実施の形態と同様に、環境情報記憶装置2003は、存在検出部2023、通信先認証部2901、あるいはセンサを確認する機能を備えてもよい。また、環境情報記憶装置2003は、内部にセンサを備えてもよい。

[0293] このような図58の構成において、環境情報記憶装置2003では、制御部2022が記

憶部2021に環境情報を記録する際、時計部2060が生成した情報を使用する。例えば、制御部2022は、環境情報を取得した時刻や特定のイベントが発生している時間を算出する際に、時計部2060が提供する情報を使用し、取得した時刻や算出した時間を環境情報に付加する。

[0294] 以上のように、環境情報記憶装置2003は、内部に時計部2060を備えたので、環境情報記憶装置2003外部から日時の情報を取得することが不要になる。このため、日時情報を改ざんすることが困難になる。従って、信頼性の高い環境情報記憶装置を提供することができる。

[0295] なお、時計部2060が保持する日時情報の調整には、実施の形態32で述べた構成を用いることにより、時計部2060の日時も信頼性の高い情報になる。つまり、時計部2060が保持する日時情報を調整するために、実施の形態32に示したように、格納機器2050から情報を取得する。この場合、格納制御部2052が、格納機器2050を認証し、あるいは取得する情報を認証する構成とする。また、本実施の形態33では時計部2060を設けたが、時計部2060の機能を制御部2022に組み込んでもよい。

[0296] 実施の形態34.

次に、図59を参照して実施の形態34を説明する。実施の形態34では、環境情報記憶装置2003が、日時に関する情報を自動調整する自動調整部2061を備えた場合を説明する。

[0297] 図59は、実施の形態34の環境情報記憶装置2003の構成を示す図である。実施の形態34の環境情報記憶装置2003は、図58の環境情報記憶装置2003に対して、さらに、自動調整部2061を備えた点が異なる。自動調整部2061は、環境情報記憶装置2003の外部から標準時刻に関する情報を受信し、受信した情報に基づき時計部2060を調整する。なお、他の実施の形態と同様に、環境情報記憶装置2003は、存在検出部2023、通信先認証部2901、あるいはセンサを確認する機能を備えてもよい。また、環境情報記憶装置2003は、内部にセンサを備えてもよい。

[0298] このような図58の構成において、環境情報記憶装置2003は、自動調整部2061により修正された時計部2060が提供する日時の情報を使用する。例えば、環境情報

を取得した時刻や特定のイベントが発生している時間を算出する際には修正された時計部2060が提供する情報を使用する。

[0299] 以上のように、環境情報記憶装置2003は、内部に日時情報を自動的に調整する自動調整部2061を備えたので、日時情報を改ざんすることが困難になり、また、調整するための保守も不要になる。従って、環境情報記憶装置の信頼性と利便性を向上することができる。

[0300] 実施の形態35.

次に、図60、図61を参照して実施の形態35を説明する。実施の形態35は、実施の形態21に対応する。実施の形態35は、実施の形態22に示した環境情報記憶装置2003を環境情報記憶方法及び環境情報記憶プログラムとして把握した実施形態である。環境情報記憶装置2003はコンピュータである。コンピュータである環境情報記憶装置2003の制御部2022(情報入力部)、環境情報記憶部2032(センサ情報記憶部)、改ざん防止部2020(改ざん検証用情報生成部)、完全性情報記憶部2033(改ざん検証用情報記憶部)の一連の動作は互いに関連しており、これらの一連の動作を環境情報記憶方法として把握することができる。

[0301] 図60は、図37の環境情報記憶装置2003の制御部2022等の動作を環境情報記憶プログラムとして把握した場合のフローチャートを示す。

[0302] (1)S2201において、制御部2022が、情報を検出するセンサから前記センサが検出した情報を入力する。

(2)S2202において、環境情報記憶部2032が、制御部2022が前記センサから入力した情報に基づく環境情報(センサ情報)を記憶する。

(3)S2203において、改ざん防止部2020が、環境情報記憶部2032が記憶した環境情報に基づいて、環境情報に対する改ざんの有無を検証するために使用する完全性情報(改ざん検証用情報)を生成する。

(4)S2204において、完全性情報記憶部2033が、改ざん防止部2020が生成した完全性情報を記憶する。

[0303] また、図61は、コンピュータである図37の環境情報記憶装置2003に実行させる環境情報記憶プログラムのフローチャートを示す。

(1)S2301は、情報を検出するセンサから前記センサが検出した情報を入力する処理である。

(2)S2302は、前記センサから入力した情報に基づく環境情報(センサ情報)を記憶する処理である。

(3)S2303は、記憶した環境情報に基づいて、環境情報に対する改ざんの有無を検証するために使用する完全性情報を生成する処理である。

(4)S2304は、生成した完全性情報を記憶する処理である。

[0304] 以上のように、環境情報記憶方法、環境情報記憶プログラムは、環境情報の完全性を証明する完全性情報を生成するので、環境情報を記憶する信頼性の高い環境情報記憶装置を実現することができる。

[0305] 以上の実施の形態では、運搬中や保管中における物の環境に関わる情報を検出する複数のセンサを有し、物の状態・環境を監視するシステムにおいて、前記センサの情報と環境を特定可能な特定情報とを記憶する記憶部と、記憶している情報の改ざんを防止する改ざん防止部と、これらの動作を制御する制御部と
を備えた環境情報記憶装置を説明した。

[0306] 以上の実施の形態では、制御部はセンサの情報を演算し、記憶部は制御部の演算結果を記録する環境情報記憶装置を説明した。

[0307] 以上の実施の形態では、存在検出部は物がその環境に存在していることを検出し、記憶部は存在検出部の出力情報も記録する環境情報記憶装置を説明した。

[0308] 以上の実施の形態では、環境情報記憶装置と検証装置とを備えた環境情報保証システムにおいて、環境情報記憶装置は、センサの情報や制御部の演算結果や環境を特定可能な特定情報を記憶する記憶部と、記憶している情報の改ざんを防止する改ざん防止部と、これらの動作を制御し、センサの情報を演算する制御部と、物がその環境に存在していることを検出する存在検出部とを備え、検証装置は、入力された情報に対する改ざんの有無を検証する検証部を備えた環境情報保証システムを説明した。

[0309] 以上の実施の形態では、環境情報記憶装置と検証装置とを備えた環境情報保証システムにおいて、前記環境情報記憶装置は、センサの情報や制御部の演算結果

や環境を特定可能な特定情報を記憶する記憶部と、記憶している情報の改ざんを防止する改ざん防止部と、これらの動作を制御し、センサの情報を演算する制御部と、物がその環境に存在していることを検出する存在検出部と、外部の機器と通信する通信部とを備え、前記検証装置は、入力された情報に対する改ざんの有無を検証する検証部と、外部の機器から情報を受信する受信部と、検証部の出力を参照して処理を行う処理部とを備えた環境情報保証システムを説明した。

[0310] 以上の実施の形態では、運搬中や保管中における物の環境に関わる情報を検出する複数のセンサと、物がその環境に存在していることを検出する存在検出部と、センサと存在検出部が検出した情報や演算結果の改ざんを防止する改ざん防止部と、動作を制御し、センサの情報を演算する制御部と、外部の機器と通信する通信部と、センサと存在検出部が検出した情報や改ざん防止部の出力や環境を特定可能な特定情報を記憶する記憶部とを備えた環境情報記憶装置を説明した。

[0311] 以上の実施の形態では、環境情報記憶装置と検証装置とを備えた環境情報保証システムにおいて、前記環境情報記憶装置は、運搬中や保管中における物の環境に関わる情報を検出する複数のセンサと、物がその環境に存在していることを検出する存在検出部と、センサと存在検出部が検出した情報や演算結果の改ざんを防止する改ざん防止部と、動作を制御し、センサの情報を演算する制御部と、装置外部の機器と通信する通信部と、センサと存在検出部が検出した情報や改ざん防止部の出力環境を特定可能な特定情報を記憶する記憶部とを備え、前記検証装置は、入力された情報に対する改ざんの有無を検証する検証部と、前記環境情報記憶装置から情報を受信する受信部と、前記検証部の出力を参照して処理を行う処理部とを備えた環境情報保証システムを説明した。

[0312] 以上の実施の形態では、環境情報記憶装置は、通信先を認証する通信先認証部を備え、正しい通信先の場合にのみ通信する環境情報記憶装置を説明した。

[0313] 以上の実施の形態では、センサの真正性を確認する環境情報記憶装置を説明した。

[0314] 以上の実施の形態では、環境情報や、環境を特定可能な特定情報を暗号化する環境情報記憶装置を説明した。

[0315] 以上の実施の形態では、格納情報を格納する前に格納機器もしくは格納情報の正当性を確認する環境情報記憶装置を説明した。

[0316] 以上の実施の形態では、日時に関する情報を自己の内部で生成する環境情報記憶装置を説明した。

[0317] 以上の実施の形態では、日時に関する情報を自己の内部で自動的に調整可能な環境情報記憶装置を説明した。

図面の簡単な説明

[0318] [図1]実施の形態1における移動体情報記憶装置3の使用状態の一例を示す。

[図2]実施の形態1における移動体情報記憶装置3の構成図である。

[図3]実施の形態1における移動体情報記憶装置3の動作を示すフローチャートである。

[図4]実施の形態1における移動体情報と完全性情報との対応関係を示す。

[図5]実施の形態2における移動体情報記憶装置3の構成図である。

[図6]実施の形態3における特殊ネジの一例を示す。

[図7]実施の形態3におけるシールを示す。

[図8]実施の形態3における移動体情報記憶装置3の構成図である。

[図9]実施の形態3における移動体側固有情報処理部と分離防止部との固有情報の比較のシーケンスである。

[図10]実施の形態3における移動体側固有情報処理部と分離防止部との認証処理のシーケンスを示す。

[図11]実施の形態4における移動体情報記憶装置3の構成図である。

[図12]実施の形態4における別の例の移動体情報記憶装置3の構成図である。

[図13]実施の形態5における移動体情報記憶装置3の構成図である。

[図14]実施の形態6における移動体情報保証システムの構成図である。

[図15]実施の形態6における移動体情報記憶装置3と移動体情報検証装置とのやり取りを示す。

[図16]実施の形態7における移動体情報保証システムの構成図である。

[図17]実施の形態8における移動体情報保証システムの構成図である。

[図18]実施の形態8における移動体情報記憶装置3と移動体情報検証装置とのやり取りを示す。

[図19]実施の形態9における移動体情報保証システムの構成図である。

[図20]実施の形態10における移動体情報保証システムの構成図である。

[図21]実施の形態10における移動体情報記憶装置3とICカードと移動体情報検証装置とのやり取りを示す。

[図22]実施の形態11における移動体情報記憶装置3と移動体情報検証装置とのやり取りを示す。

[図23]実施の形態12における移動体情報保証システムの構成図である。

[図24]実施の形態13における移動体情報保証システムの構成図である。

[図25]実施の形態13における範囲判定部の動作を説明する図である。

[図26]実施の形態14における移動体情報保証システムの構成図である。

[図27]実施の形態14における移動体情報記憶装置3と各移動体情報検証装置とのやり取りを示す。

[図28]実施の形態14におけるサービス管理テーブルの一例を示す。

[図29]実施の形態16における移動体情報保証システムの構成図である。

[図30]実施の形態17における移動体情報保証システムの構成図である。

[図31]実施の形態17におけるタッチパネル表示の一例を示す。

[図32]実施の形態18における移動体情報保証システムの構成図である。

[図33]実施の形態19における移動体情報保証システムの構成図である。

[図34]実施の形態20における移動体情報保証システムの構成図である。

[図35]実施の形態21における情報記憶プログラムの処理を示すフローチャートである。

[図36]実施の形態21におけるコンピュータシステムのハードウェア構成を示す。

[図37]実施の形態22における環境情報記憶装置2003の構成図である。

[図38]実施の形態22における環境情報記憶装置2003の動作のフローチャートである。

[図39]実施の形態22における環境情報と完全性情報との対応関係を示す図である

。

[図40]実施の形態23における環境情報記憶装置2003の構成図である。

[図41]実施の形態24における環境情報記憶装置2003の構成図である。

[図42]実施の形態24における具体例を示す図である。

[図43]実施の形態25における複数のセンサ群と環境情報記憶装置2003との関係を示す図である。

[図44]実施の形態26における環境情報保障システム2000の構成図である。

[図45]実施の形態26における認証動作を示す図である。

[図46]実施の形態26における別の認証動作を示す図である。

[図47]実施の形態27における環境情報保障システム2000の構成図である。

[図48]実施の形態27における動作を示す図である。

[図49]実施の形態27における認証動作を示す図である。

[図50]実施の形態27における別のシステム構成を示す図である。

[図51]実施の形態28における環境情報保障システム2000の構成図である。

[図52]実施の形態29における環境情報保障システム2000の構成図である。

[図53]実施の形態29における認証動作を示す図である。

[図54]実施の形態30における環境情報記憶装置2003の構成図である。

[図55]実施の形態30における認証動作を示す図である。

[図56]実施の形態31における環境情報保障システム2000の構成図である。

[図57]実施の形態32における環境情報記憶装置2003の構成図である。

[図58]実施の形態33における環境情報記憶装置2003の構成図である。

[図59]実施の形態34における環境情報記憶装置2003の構成図である。

[図60]実施の形態35における環境情報記憶方法のフローチャートである。

[図61]実施の形態35における環境情報記憶プログラムのフローチャートである。

符号の説明

[0319] 1 移動体、2 センサ群、2a, 2b, 2c センサ、3 移動体情報記憶装置、20 改ざん防止部、21 記憶部、22 制御部、31 装置側固有情報記憶部、32 移動体情報記憶部、33 完全性情報記憶部、34 移動体情報群記憶部、60 シール、61

暗証番号応答画面、62 タッチパネル、201 装置側演算部、301 移動体側固有情報処理部、302 分離防止部、303 特殊ネジ、311 移動体側固有情報記憶部、401 バッテリ、402 信号線、501 情報消去部、600, 600a, 600b 移動体情報検証装置、601 検証部、701 処理部、801 記憶側通信部、802 検証側通信部、805 コンピュータシステム、810 CPU、811 ROM、812 センサ、813 通信ボード、820 磁気ディスク装置、821 OS、823 プログラム群、824 ファイル群、901 通信先認証部、1001 ICカード、1201 センサ確認部、1301 範囲判定部、1401 選択部、1402 サービス管理テーブル、1601 マンマシンインタフェース部、1701 操作者認証部、1801 暗号部、1802 復号部、 2000 環境情報保証システム、2001 物、2002 センサ群、2002－1, 2002－2 センサ群、2002a, 2002b,2002c センサ、2003 環境情報記憶装置、2020 改ざん防止部、2021 記憶部、2022 制御部、2023 存在検出部、2031 特定情報記憶部、2032 環境情報記憶部、2033 完全性情報記憶部、2040, 2040a, 2040b 倉庫／コンテナ、2041 扉／蓋、2042 開閉検知センサ、2043 無線タグ、2044 無線タグリーダ、2045 識別情報比較部、2050 格納機器、2051 外部インタフェース部、2052 格納制御部、2060 時計部、2061 自動調整部、2201 装置側演算部、2600, 2600a, 2600b 端末装置、2601 検証部、2701 処理部、2801 記憶側通信部、2802 検証側通信部、2901 通信先認証部、3201 センサ確認部、3801 暗号部、3802 復号部。

請求の範囲

[1] 移動体に装備され、前記移動体に関する情報を記憶する情報記憶装置において、

前記移動体に関する情報を検出するセンサが検出した情報に基づくセンサ情報を記憶するセンサ情報記憶部と、

前記移動体を特定可能な特定情報を取得し、取得した前記特定情報と前記センサ情報記憶部が記憶した前記センサ情報とに基づいて、前記特定情報と前記センサ情報との少なくともいずれかに対する改ざんの有無を検証するために使用する改ざん検証用情報を生成する改ざん検証用情報生成部と、

前記改ざん検証用情報生成部が生成した前記改ざん検証用情報を記憶する改ざん検証用情報記憶部と

を備えたことを特徴とする情報記憶装置。

[2] 前記情報記憶装置は、さらに、

前記特定情報を装置側特定情報として記憶する装置側特定情報記憶部を備え、

前記改ざん検証用情報生成部は、

前記装置側特定情報記憶部が記憶した前記装置側特定情報を取得することを特徴とする請求項1記載の情報記憶装置。

[3] 前記移動体は、

前記特定情報を移動体側特定情報として記憶する移動体側特定情報記憶部を備え、

前記改ざん検証用情報生成部は、

前記移動体側特定情報記憶部が記憶した前記移動体側特定情報を取得することを特徴とする請求項1記載の情報記憶装置。

[4] 前記情報記憶装置は、さらに、

自己と前記移動体とが分離しているかどうかを検出する分離検出部を備えたことを特徴とする請求項1記載の情報記憶装置。

[5] 前記情報記憶装置は、さらに、

自己が装備された前記移動体である前記装備移動体が、予め装備されることが指定された指定移動体かどうかを判断する移動体判断部を備えたこと特徴とする請求

項1記載の情報記憶装置。

[6] 前記情報記憶装置は、さらに、

前記移動体判断部が前記装備移動体は前記指定移動体ではないと判断した場合に、前記センサ情報記憶部が記憶した前記センサ情報を消去する情報消去部を備えたことを特徴とする請求項5記載の情報記憶装置。

[7] 前記装備移動体は、

移動体である自己を特定可能な移動体側特定情報を記憶する移動体側特定情報記憶部を備え、

前記情報記憶装置は、さらに、

前記指定移動体を特定可能な装置側特定情報を記憶する装置側特定情報記憶部を備え、

前記移動体判断部は、

前記装置側特定情報記憶部が記憶した前記装置側特定情報と前記移動体側特定情報記憶部が記憶した前記移動体側特定情報とを入力し、入力した前記装置側特定情報と前記移動体側特定情報とに基づいて、前記装備移動体が前記指定移動体かどうかを判断することを特徴とする請求項5記載の情報記憶装置。

[8] 前記改ざん検証用情報生成部は、

前記移動体判断部が前記装備移動体を前記指定移動体と判断した場合に、前記移動体判断部が入力した前記装置側特定情報と前記移動体側特定情報とのうちのいずれかを選択対象として選択して取得し、取得した前記選択対象と前記センサ情報記憶部が記憶した前記センサ情報とに基づいて、前記選択対象と前記センサ情報との少なくともいずれかに対する改ざんの有無を検証するために使用する改ざん検証用情報を生成することを特徴とする請求項7記載の情報記憶装置。

[9] 前記装備移動体は、

通信により認証要求を受け付けて、予め設定された規則に基いて認証処理を実行する移動体側認証実行部を備え、

前記移動体判断部は、

前記移動体側認証実行部に前記認証要求を送信し、前記予め設定された規則に

基いて前記移動体側認証実行部との間で認証処理を実行することにより、前記装備移動体が前記指定移動体かどうかを判断することを特徴とする請求項5記載の情報記憶装置。

[10] 前記情報記憶装置は、さらに、

前記センサが正当かどうかを確認するセンサ確認部を備えたことを特徴とする請求項1記載の情報記憶装置。

[11] 移動体に装備され、前記移動体に関する情報を記憶する情報記憶装置において、

前記移動体に関する情報を検出する複数のセンサのそれぞれが検出したそれぞれの情報に基づくそれぞれのセンサ情報を入力し、予め設定された条件に基づいて前記それぞれのセンサ情報のうちから少なくとも一つのセンサ情報を選択する選択部と、

前記選択部が選択したセンサ情報から構成されるグループを示す選択情報群を記憶する選択情報群記憶部と、

前記移動体を特定可能な特定情報を取得し、取得した前記特定情報と前記選択情報群記憶部が記憶した前記選択情報群とに基づいて、前記特定情報と前記選択情報群に含まれる前記センサ情報との少なくともいずれかに対する改ざんの有無を検証するために使用する改ざん検証用情報を生成する改ざん検証用情報生成部と、

前記改ざん検証用情報生成部が生成した前記改ざん検証用情報を記憶する改ざん検証用情報記憶部と

を備えたことを特徴とする情報記憶装置。

[12] 移動体に装備され、前記移動体に関する情報を記憶する情報記憶装置において、

前記移動体に関する情報を検出する複数のセンサのそれぞれが検出したそれぞれの情報に基づくそれぞれのセンサ情報を記憶するセンサ情報記憶部と、

予め設定された条件に基づいて、前記センサ情報記憶部が記憶した前記それぞれのセンサ情報のうちから少なくとも一つのセンサ情報を選択する選択部と、

前記移動体を特定可能な特定情報を取得し、取得した前記特定情報と前記選択部が選択したセンサ情報から構成されるグループを示す前記選択情報群とに基づい

て、前記特定情報と前記選択情報群に含まれる前記センサ情報との少なくともいずれかに対する改ざんの有無を検証するために使用する改ざん検証用情報を生成する改ざん検証用情報生成部と、

前記改ざん検証用情報生成部が生成した前記改ざん検証用情報を記憶する改ざん検証用情報記憶部と

を備えたことを特徴とする情報記憶装置。

[13] 前記情報記憶装置は、さらに、

前記センサ情報を入力し、入力した前記センサ情報が予め設定された条件に合致するかどうかを判定し、前記条件に合致すると判定した場合に、入力した前記センサ情報を前記

センサ情報記憶に記憶させる条件判定部を備えたことを特徴とする請求項1記載の情報記憶装置。

[14] 前記情報記憶装置は、さらに、

前記センサ情報記憶部が記憶した前記センサ情報と、前記改ざん検証用情報生成部が取得した前記特定情報と、前記改ざん検証用情報記憶部が記憶した前記改ざん検証用情報とを出力する出力部を備えたことを特徴とする請求項1記載の情報記憶装置。

[15] 前記出力部は、

前記センサ情報と前記特定情報と前記改ざん検証用情報とを出力する場合に、出力先が予め指定された指定装置かどうかを認証する出力先認証部を備えたことを特徴とする請求項14記載の情報記憶装置。

[16] 前記出力部は、

情報を記憶可能であるとともに携帯が可能である携帯型記憶媒体に、前記センサ情報と前記特定情報と前記改ざん検証用情報とを出力することを特徴とする請求項14記載の情報記憶装置。

[17] 前記出力部は、

予め設定された時間間隔で、前記センサ情報と前記特定情報と前記改ざん検証用情報とを出力することを特徴とする請求項14記載の情報記憶装置。

[18] 前記情報記憶装置は、さらに、

操作者による操作を受け付け、受け付けた前記操作に基いて、前記出力部に対して出力を命じる命令部を備え、

前記出力部は、

前記命令部から出力を命じられた場合に、前記センサ情報と前記特定情報と前記改ざん検証用情報とを出力することを特徴とする請求項14記載の情報記憶装置。

[19] 前記情報記憶装置は、さらに、

前記命令部が受け付けた前記操作者による前記操作に基づいて、前記操作者が正当であるかどうかを認証する操作者認証部を備え、

前記命令部は、

前記操作者認証部が前記操作者を正当と認証した場合に、前記出力部に対して出力を命じることを特徴とする請求項18記載の情報記憶装置。

[20] 移動体に装備され、前記移動体の情報を記憶するコンピュータである情報記憶装置に以下の処理を実行させる情報記憶プログラム

(1)前記移動体に関する情報を検出するセンサが検出した情報に基づくセンサ情報を記憶する処理

(2)前記移動体を特定可能な特定情報を取得し、取得した前記特定情報と記憶した前記センサ情報とに基づいて、前記特定情報と前記センサ情報との少なくともいずれかに対する改ざんの有無を検証するために使用する改ざん検証用情報を生成する処理

(3)生成した前記改ざん検証用情報を記憶する処理

[21] 情報を検出するセンサから前記センサが検出した情報を入力する情報入力部と、

前記情報入力部が前記センサから入力した情報に基づくセンサ情報を記憶するセンサ情報記憶部と、

前記センサ情報記憶部が記憶した前記センサ情報に基づいて、前記センサ情報に対する改ざんの有無を検証するために使用する改ざん検証用情報を生成する改ざん検証用情報生成部と、

前記改ざん検証用情報生成部が生成した前記改ざん検証用情報を記憶する改ざ

ん検証用情報記憶部と

を備えたことを特徴とする情報記憶装置。

[22] 前記情報記憶装置は、さらに、

所定の情報を記憶する装置側特定情報記憶部を備え、

前記改ざん検証用情報生成部は、

前記センサ情報記憶部が記憶した前記センサ情報と前記装置側特定情報記憶部が記憶した前記所定の情報とに基づいて、前記所定の情報と前記センサ情報との少なくともいずれかに対する改ざんの有無を検証するために使用する改ざん検証用情報を生成することを特徴とする請求項21の情報記憶装置。

[23] 前記センサは、

自己が配置されている環境に関する情報を検出し、

前記装置側特定情報記憶部は、

前記所定の情報として、前記センサが配置される前記環境と自己である前記環境情報記憶装置が配置される場所との少なくともいずれかを特定可能な特定情報を記憶することを特徴とする請求項22記載の情報記憶装置。

[24] 前記情報記憶装置は、さらに、

前記センサが配置されている環境に所定の物が継続して置かれているかどうかを検出する存在検出部を備え、

前記改ざん検証用情報生成部は、

前記センサ情報記憶部が記憶した前記センサ情報と前記存在検出部が検出した検出結果とに基づいて、前記センサ情報と前記検出結果との少なくともいずれかに対する改ざんの有無を検証するために使用する改ざん検証用情報を生成することを特徴とする請求項21記載の情報記憶装置。

[25] 前記情報記憶装置は、さらに、

前記センサ情報記憶部が記憶した前記センサ情報と、前記装置側特定情報記憶部が記憶した前記所定の情報と、前記改ざん検証用情報記憶部が記憶した前記改ざん検証用情報とを他の装置に出力する出力部を備えたことを特徴とする請求項22記載の情報記憶装置。

[26] 前記出力部は、

前記センサ情報と前記所定の情報と前記改ざん検証用情報とを出力する場合に、前記他の装置を認証する出力先認証部を備えたことを特徴とする請求項25記載の情報記憶装置。

[27] 前記情報記憶装置は、さらに、

前記センサが正当かどうかを確認するセンサ確認部を備えたことを特徴とする請求項21記載の情報記憶装置。

[28] 前記情報記憶装置は、

所定の情報を格納する格納機器から前記所定の情報を入力する外部インタフェース部と、

前記外部インタフェース部が前記格納機器から前記所定の情報を入力する場合に前記格納機器との間で通信を行うことにより前記格納機器が正当であるかどうかを認証し、正当と判断した場合に、前記所定の情報を前記装置側特定情報記憶部に記憶する格納制御部と

を備えたことを特徴とする請求項22記載の情報記憶装置。

[29] 前記情報記憶装置は、

所定の情報を格納する格納機器から前記所定の情報を入力する外部インタフェース部と、

前記外部インタフェース部が入力した前記所定の情報が正当であるかどうかを認証し、正当と判断した場合に、前記所定の情報を前記装置側特定情報記憶部に記憶する格納制御部と

を備えたことを特徴とする請求項22記載の情報記憶装置。

[30] 情報を検出するセンサから前記センサが検出した情報を入力する情報入力部と、

前記情報入力部が前記センサから入力した情報に基づくセンサ情報を記憶するセンサ情報記憶部と、

前記センサ情報記憶部が記憶した前記センサ情報に基づいて、前記センサ情報に対する改ざんの有無を検証するために使用する改ざん検証用情報を生成する改ざん検証用情報生成部と、

前記改ざん検証用情報生成部が生成した前記改ざん検証用情報を記憶する改ざん検証用情報記憶部と、

前記センサ情報記憶部が記憶した前記センサ情報と、前記改ざん検証用情報記憶部が記憶した前記改ざん検証用情報とを出力する出力部とを備えた情報記憶装置から、

前記情報記憶装置が出力した前記センサ情報と前記改ざん検証用情報とを入力し、入力した前記センサ情報と前記改ざん検証用情報とを用いることにより前記センサ情報の正当性を検証する検証部を備えたことを特徴とする検証装置。

[31] コンピュータである情報記憶装置が行なう情報記憶方法において、

情報入力部が、情報を検出するセンサから前記センサが検出した情報を入力し、

センサ情報記憶部が、前記情報入力部が前記センサから入力した情報に基づくセンサ情報を記憶し、

改ざん検証用情報生成部が、前記センサ情報記憶部が記憶した前記センサ情報に基づいて、前記センサ情報に対する改ざんの有無を検証するために使用する改ざん検証用情報を生成し、

改ざん検証用情報記憶部が、前記改ざん検証用情報生成部が生成した前記改ざん検証用情報を記憶することを特徴とする情報記憶方法。

[32] 以下の処理をコンピュータに実行させることを特徴とする情報記憶プログラム

(1)情報を検出するセンサから前記センサが検出した情報を入力する処理

(2)前記センサから入力した情報に基づくセンサ情報を記憶する処理

(3)記憶した前記センサ情報に基づいて、前記センサ情報に対する改ざんの有無を検証するために使用する改ざん検証用情報を生成する処理

(4)生成した前記改ざん検証用情報を記憶する処理

図 1

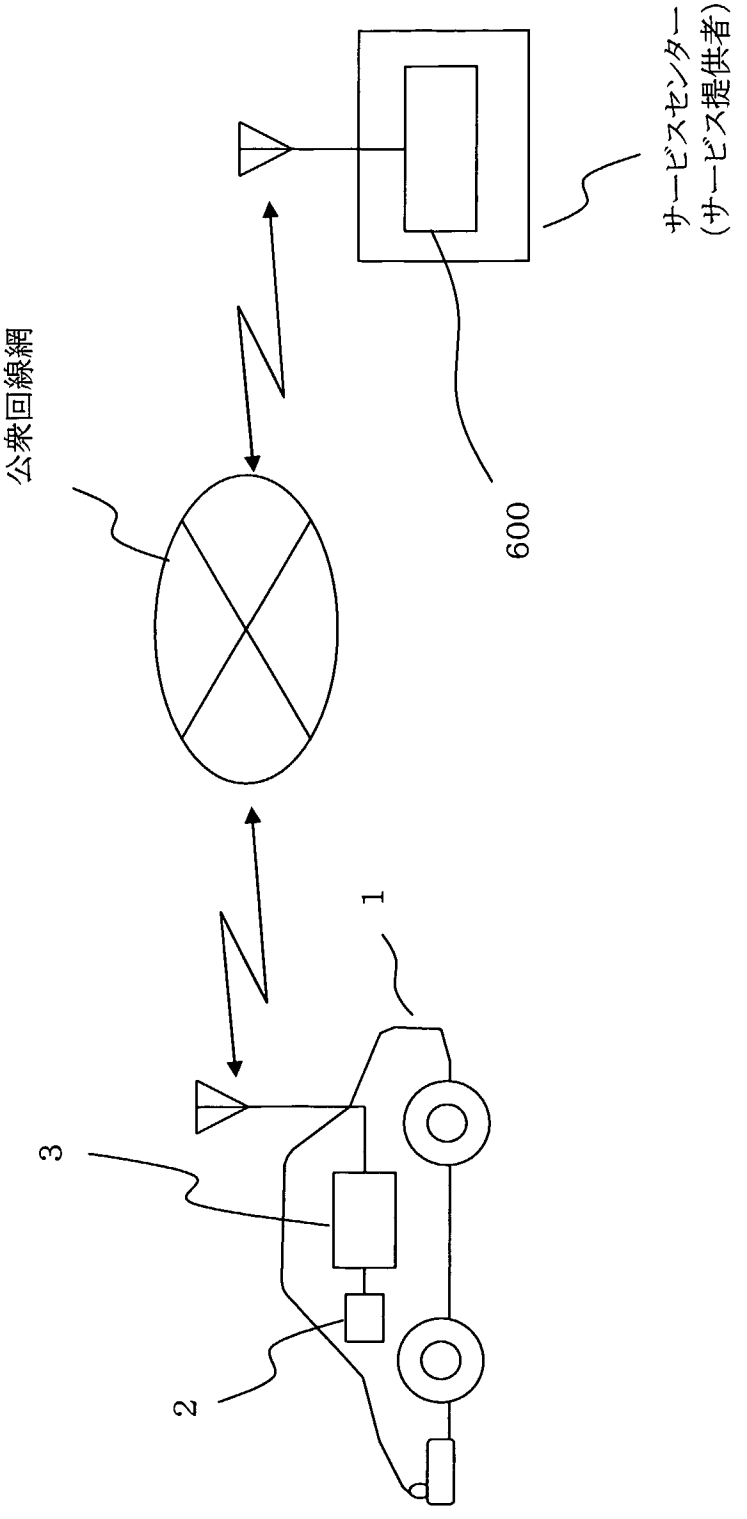
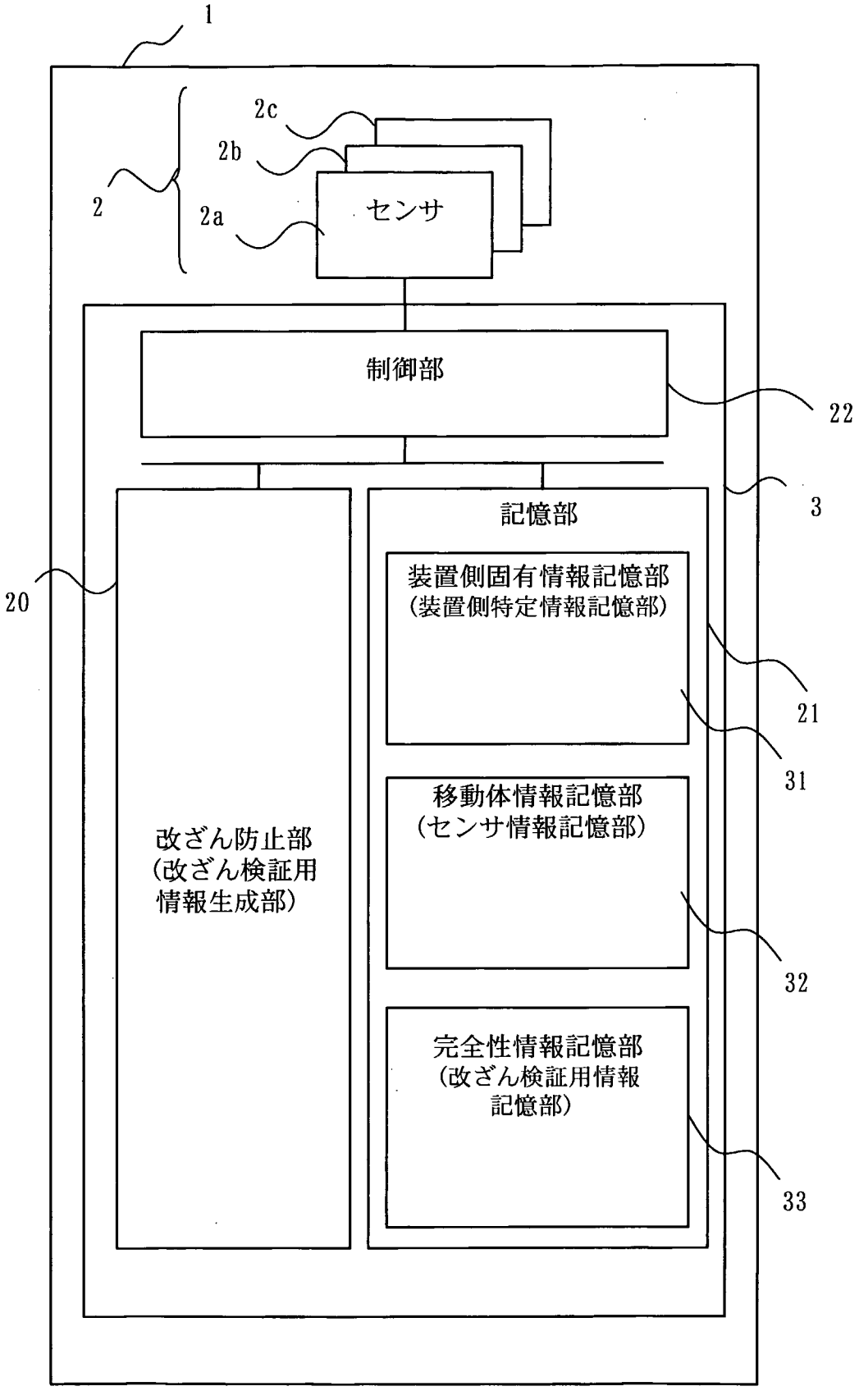
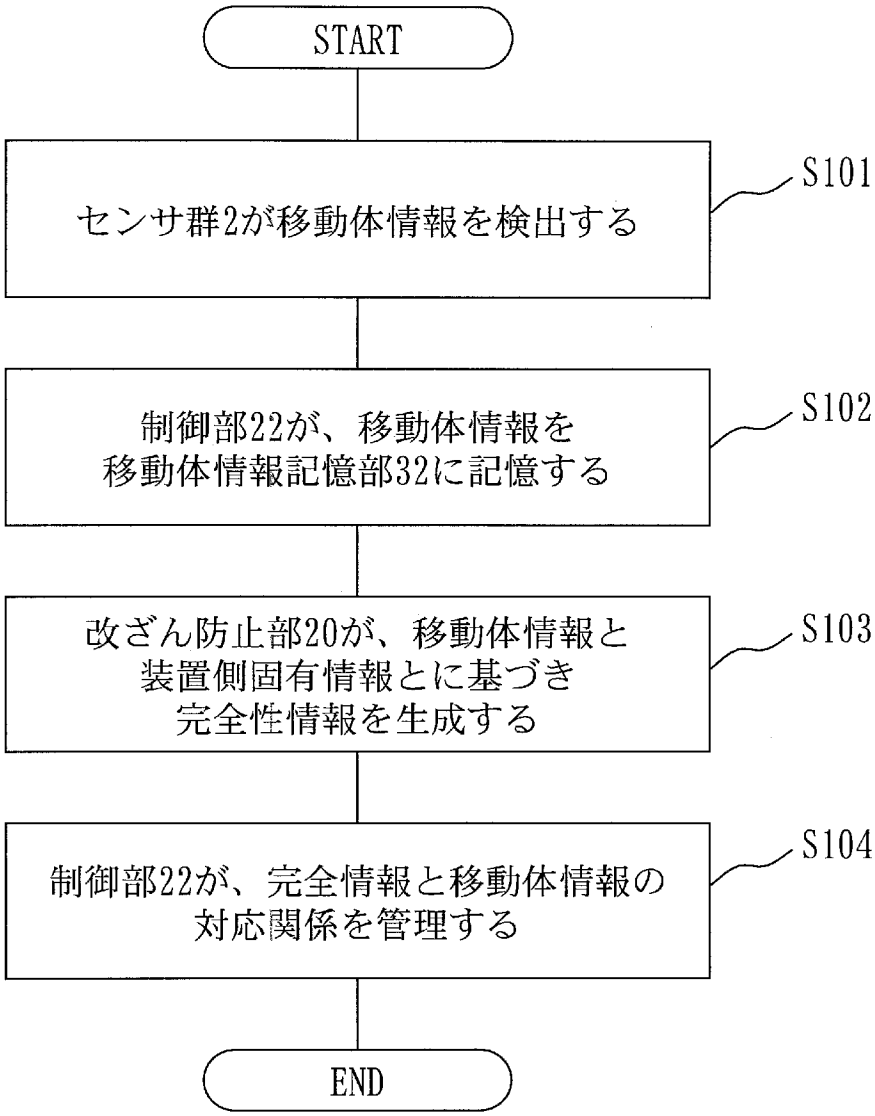


図 2


1
2c
2b
2
2a
センサ
制御部
22
3
記憶部
20
装置側固有情報記憶部
(装置側特定情報記憶部)
21
31
移動体情報記憶部
(センサ情報記憶部)
改ざん防止部
(改ざん検証用
情報生成部)
32
完全性情報記憶部
(改ざん検証用情報
記憶部)
33

[図3]


START
センサ群2が移動体情報を検出する
S101
制御部22が、移動体情報を
移動体情報記憶部32に記憶する
S102
改ざん防止部20が、移動体情報と
装置側固有情報とに基づき
完全性情報を生成する
S103
制御部22が、完全情報と移動体情報の
対応関係を管理する
S104
END

[図4]

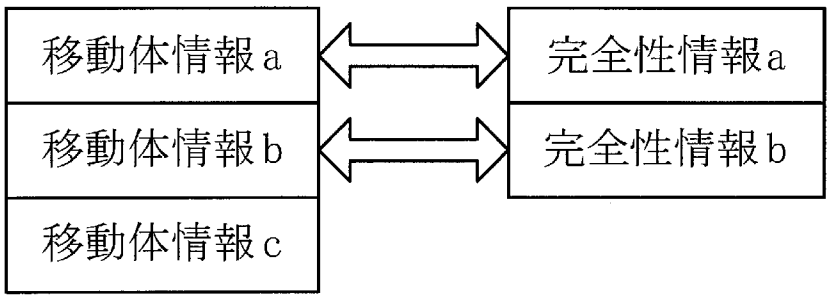
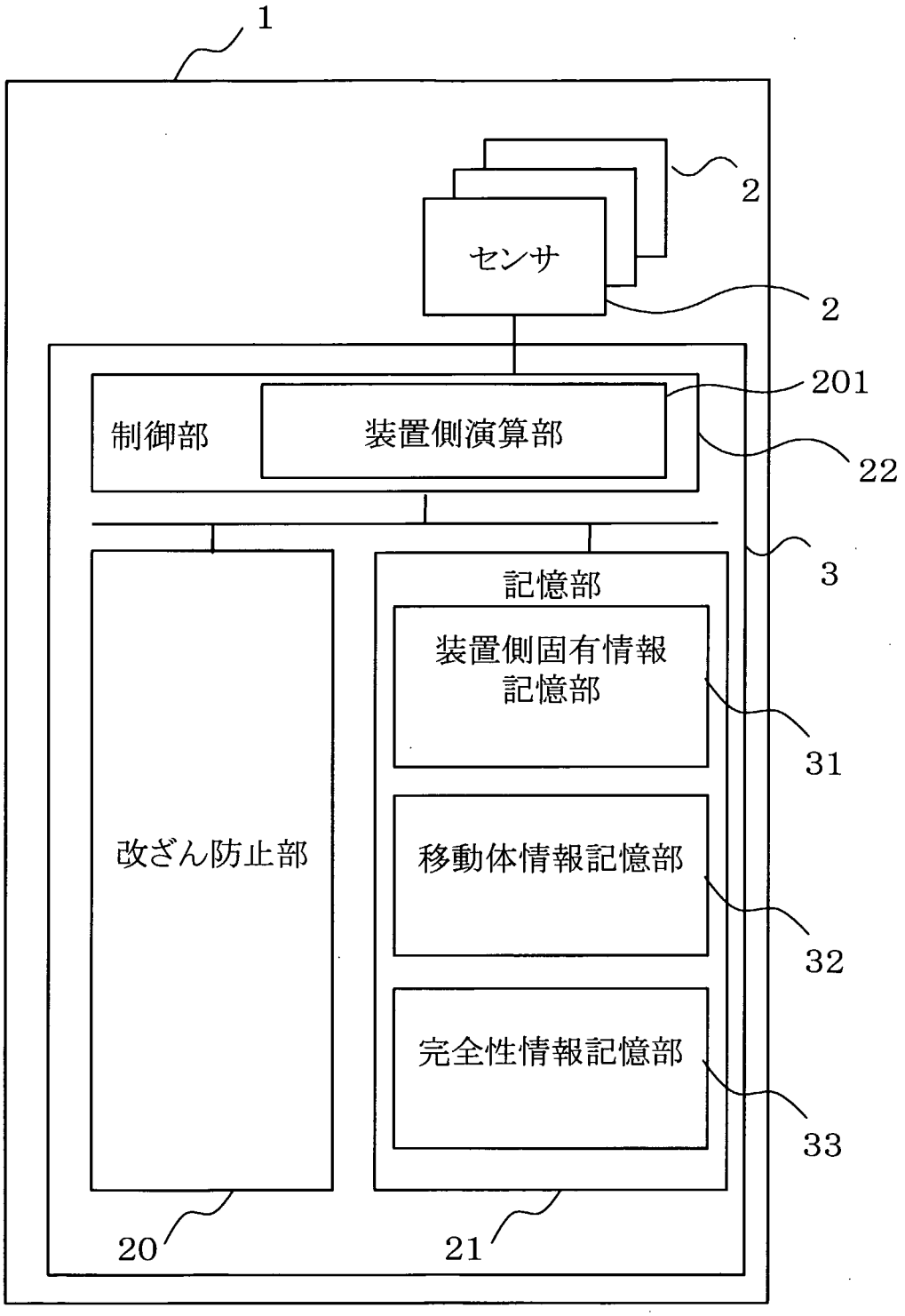

移動体情報a
移動体情報b
移動体情報c
完全性情報a
完全性情報b

図 5


1
2
センサ
2
201
制御部
装置側演算部
22
3
記憶部
装置側固有情報
記憶部
31
改ざん防止部
移動体情報記憶部
32
完全性情報記憶部
33
20
21

[図6]

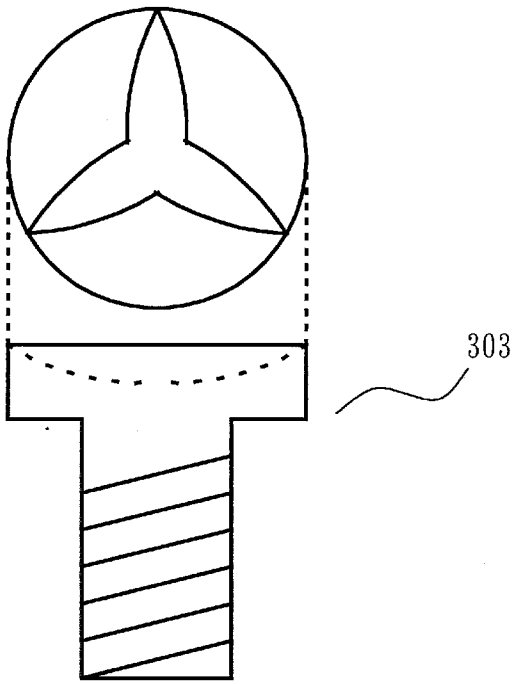


図 7

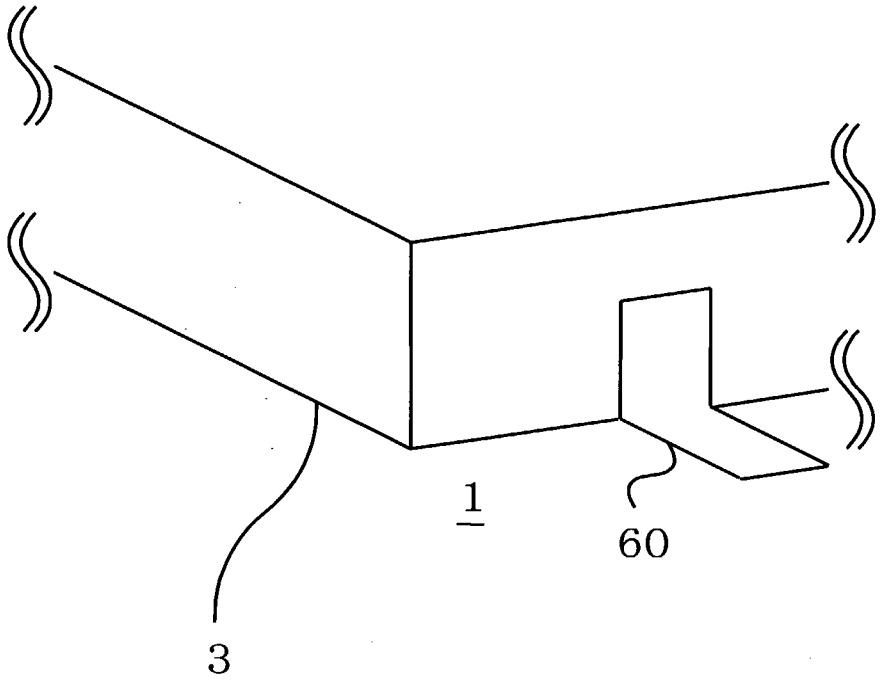
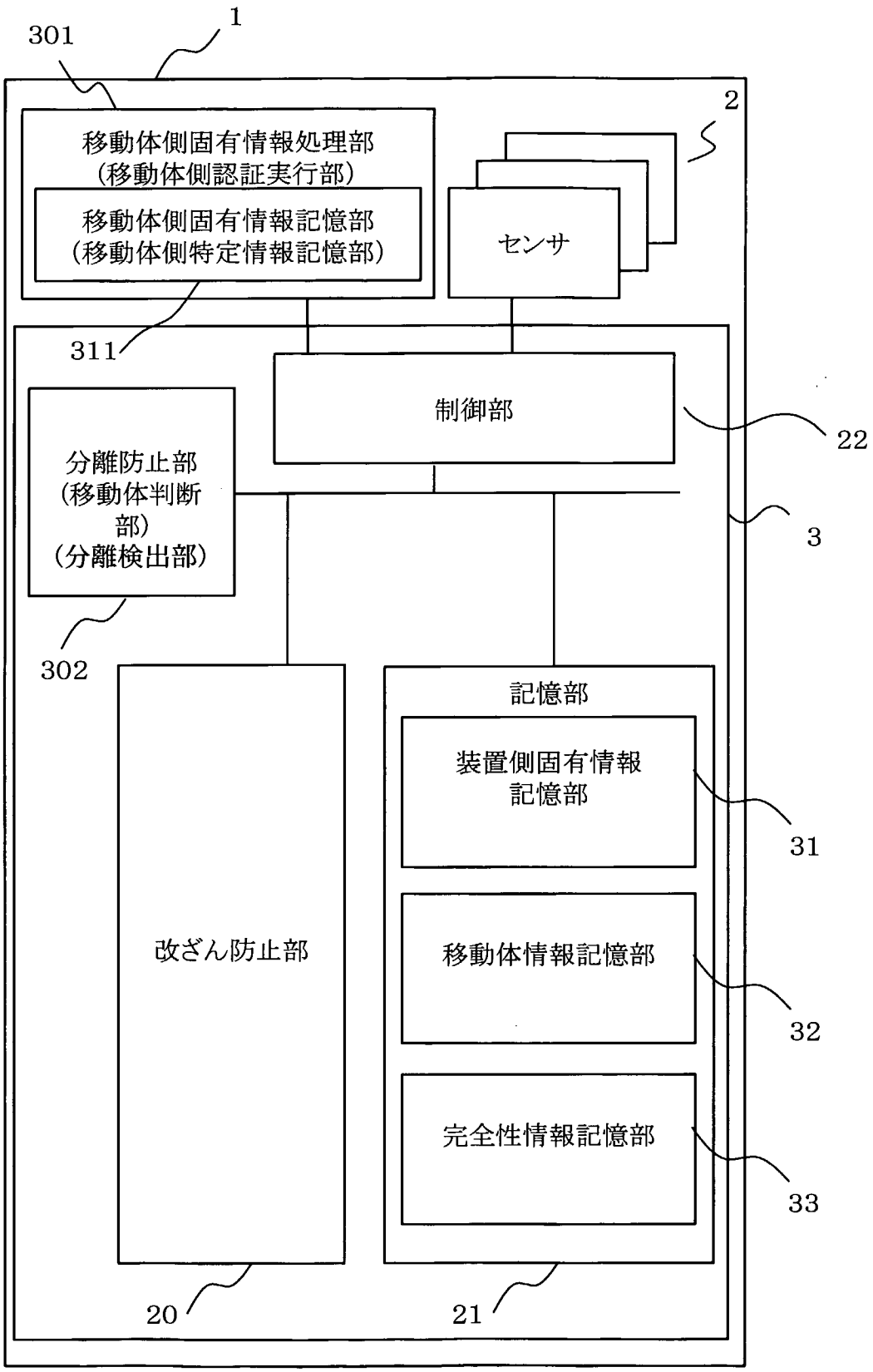
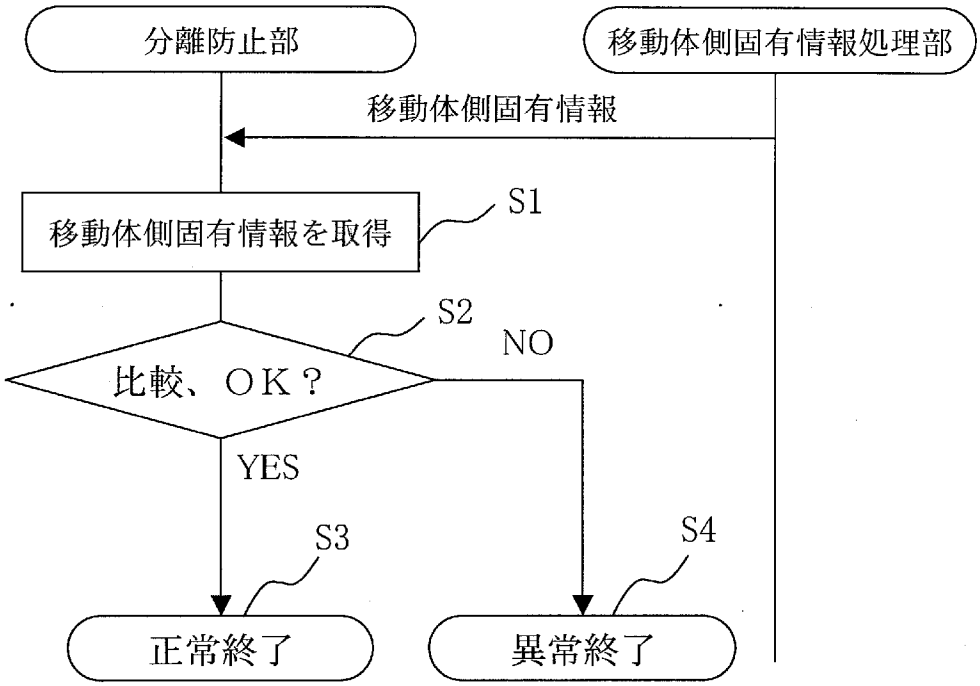


図 8


1
301
2
移動体側固有情報処理部
(移動体側認証実行部)
移動体側固有情報記憶部
(移動体側特定情報記憶部)
センサ
311
制御部
22
分離防止部
(移動体判断
部)
(分離検出部)
3
302
記憶部
装置側固有情報
記憶部
31
改ざん防止部
移動体情報記憶部
32
完全性情報記憶部
33
20
21

[図9]


分離防止部
移動体側固有情報処理部
移動体側固有情報
移動体側固有情報を取得
S1
S2
比較、ＯＫ？
NO
YES
S3
S4
正常終了
異常終了

[図10]

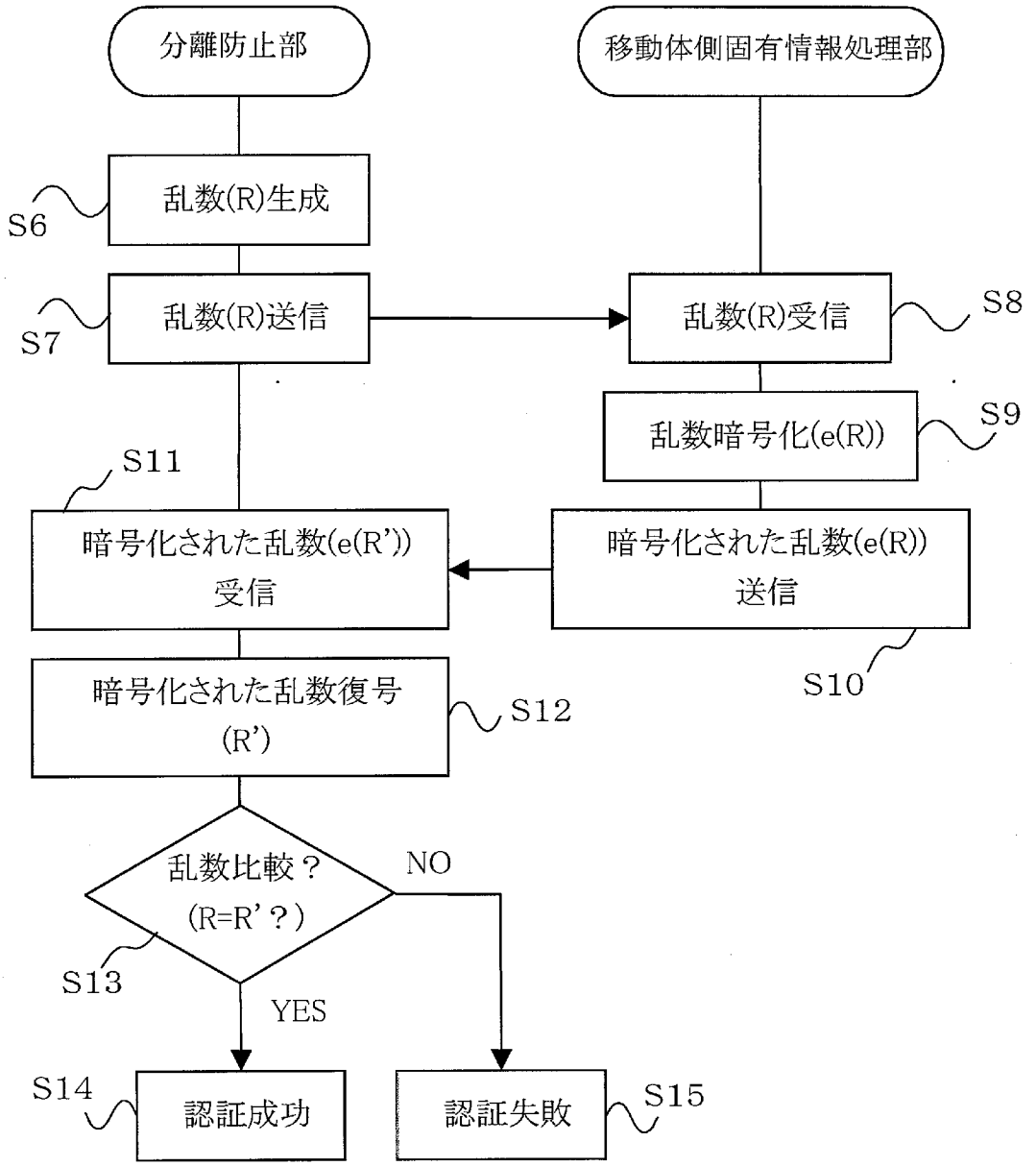

分離防止部
移動体側固有情報処理部
乱数(R)生成
S6
乱数(R)送信
S7
乱数(R)受信
S8
乱数暗号化(e(R))
S9
S11
暗号化された乱数(e(R'))
受信
暗号化された乱数(e(R))
送信
S10
暗号化された乱数復号
(R')
S12
乱数比較？
(R=R'？)
NO
S13
YES
S14
認証成功
認証失敗
S15

図11

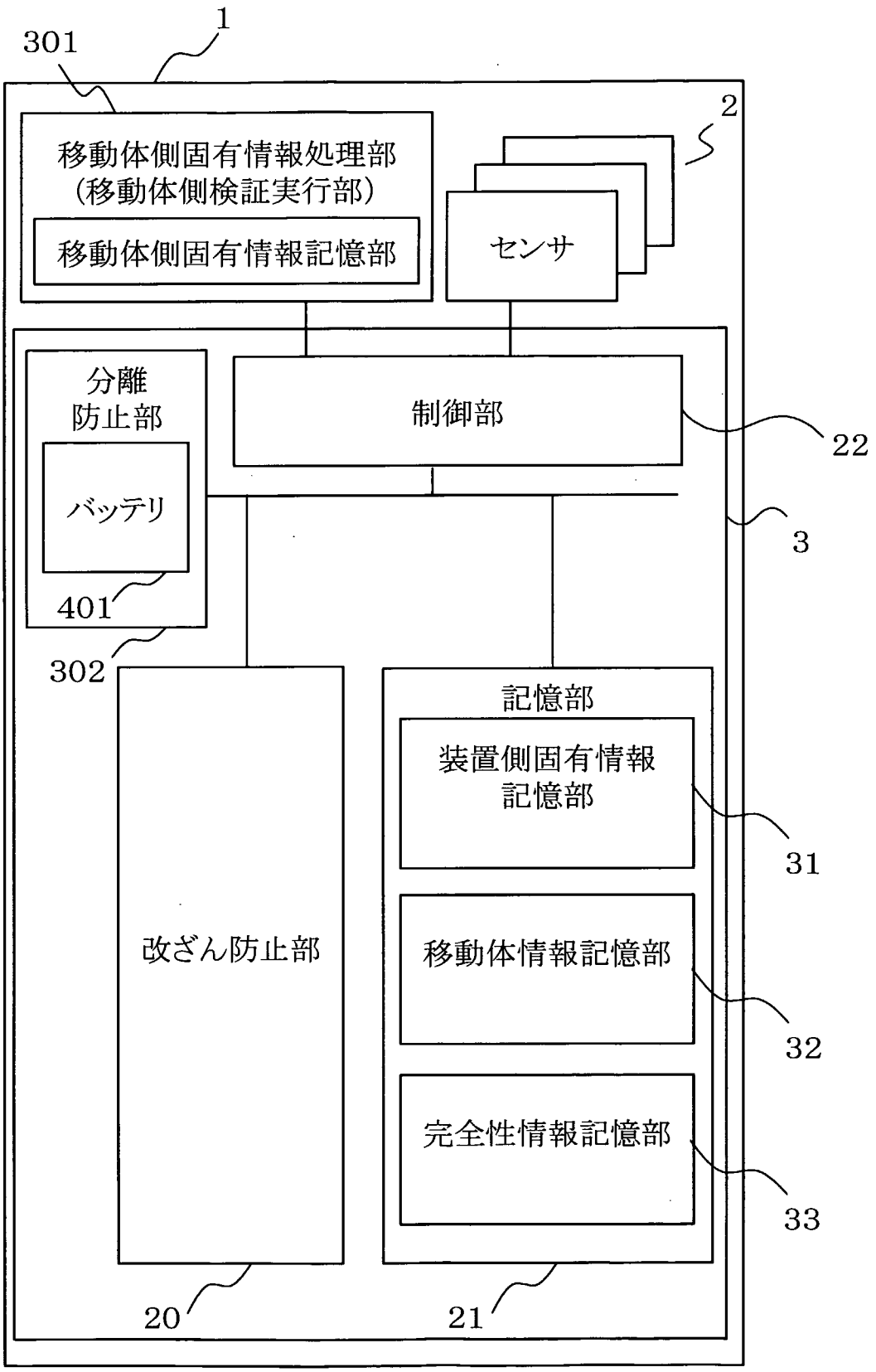

1
301
移動体側固有情報処理部
(移動体側検証実行部)
移動体側固有情報記憶部
2
センサ
分離
防止部
バッテリ
401
302
制御部
22
3
記憶部
装置側固有情報
記憶部
31
移動体情報記憶部
32
完全性情報記憶部
33
改ざん防止部
20
21

図12

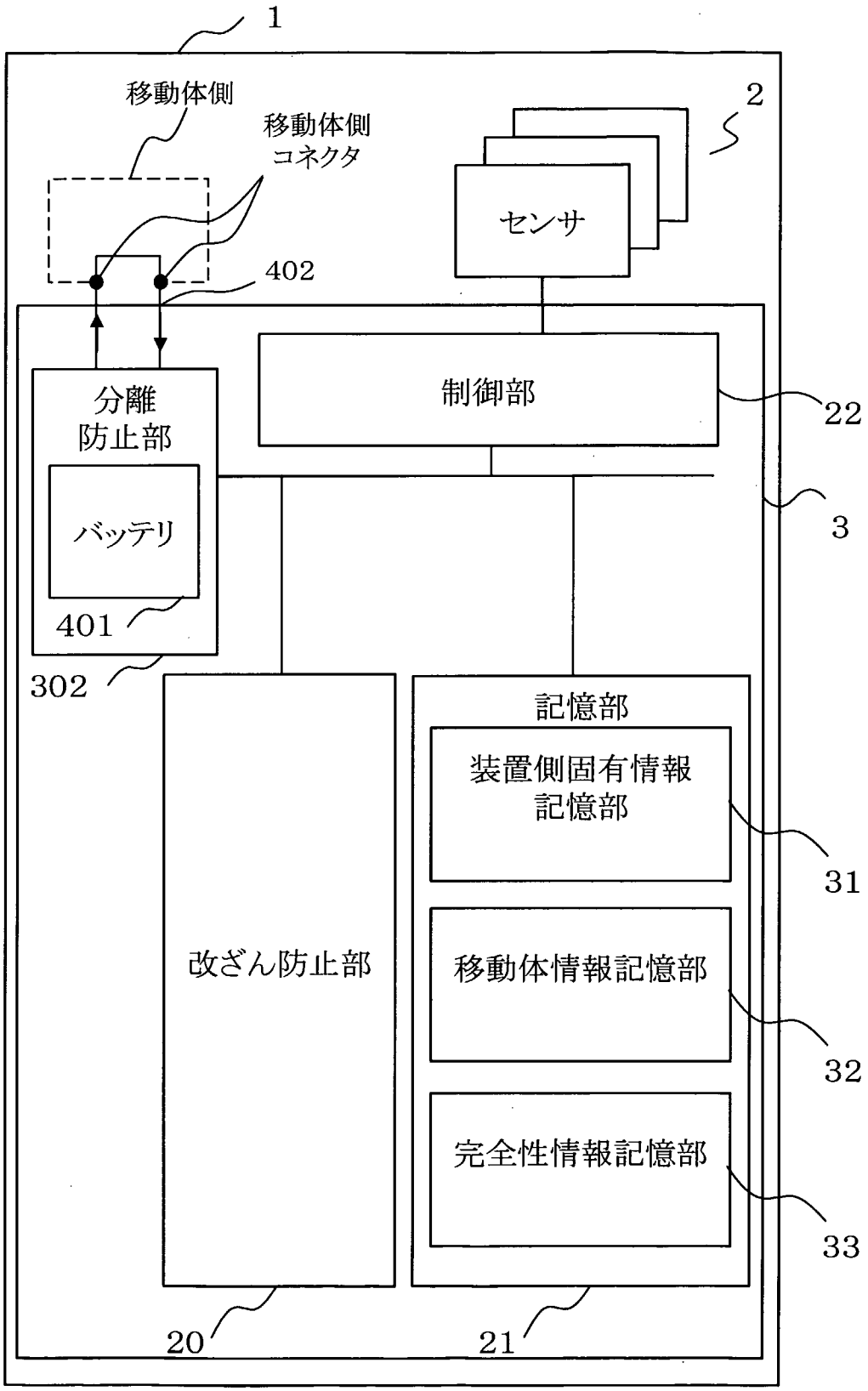

1
移動体側
移動体側
コネクタ
402
2
センサ
制御部
22
分離
防止部
バッテリ
401
302
3
記憶部
装置側固有情報
記憶部
31
改ざん防止部
移動体情報記憶部
32
完全性情報記憶部
33
20
21

図 13

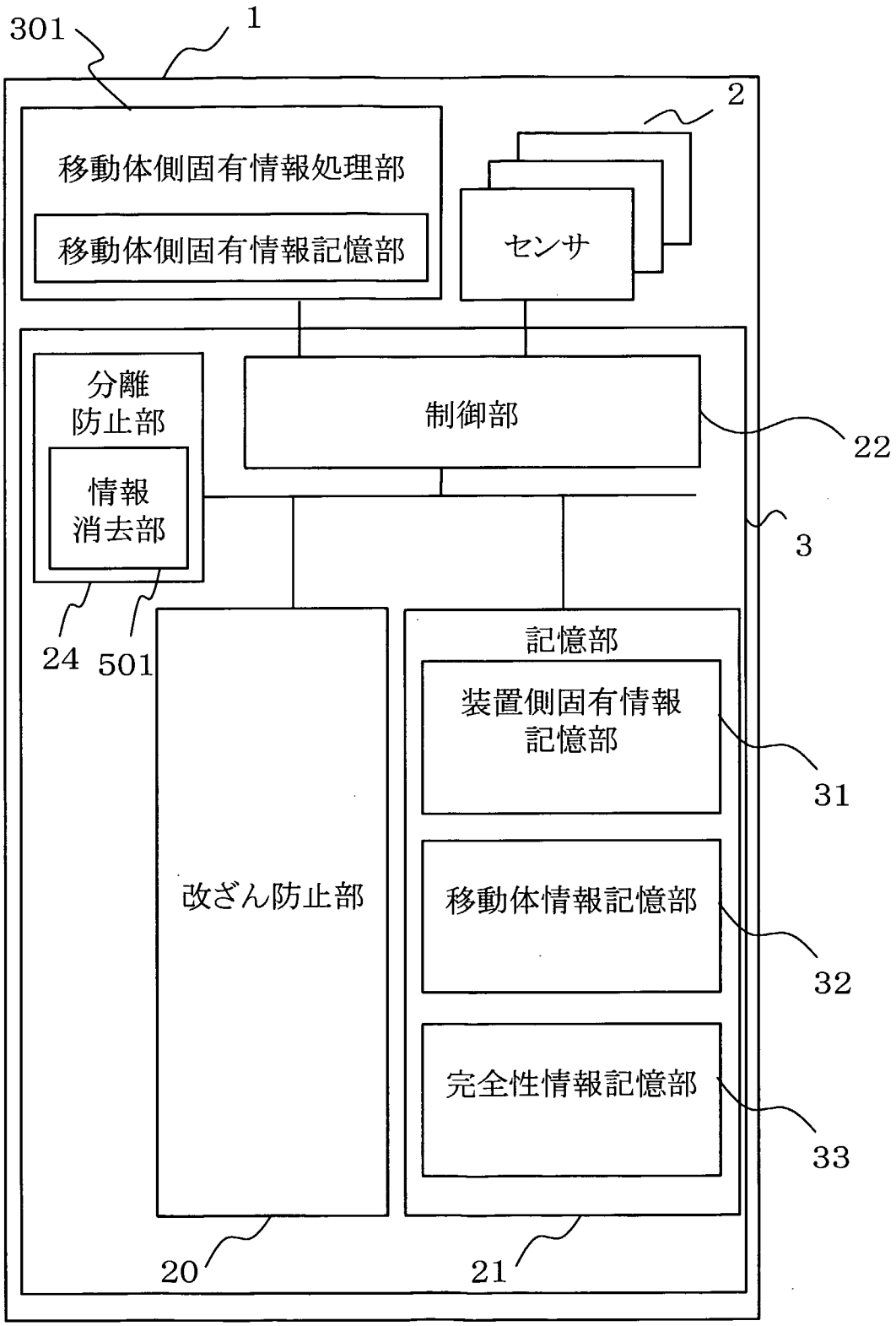
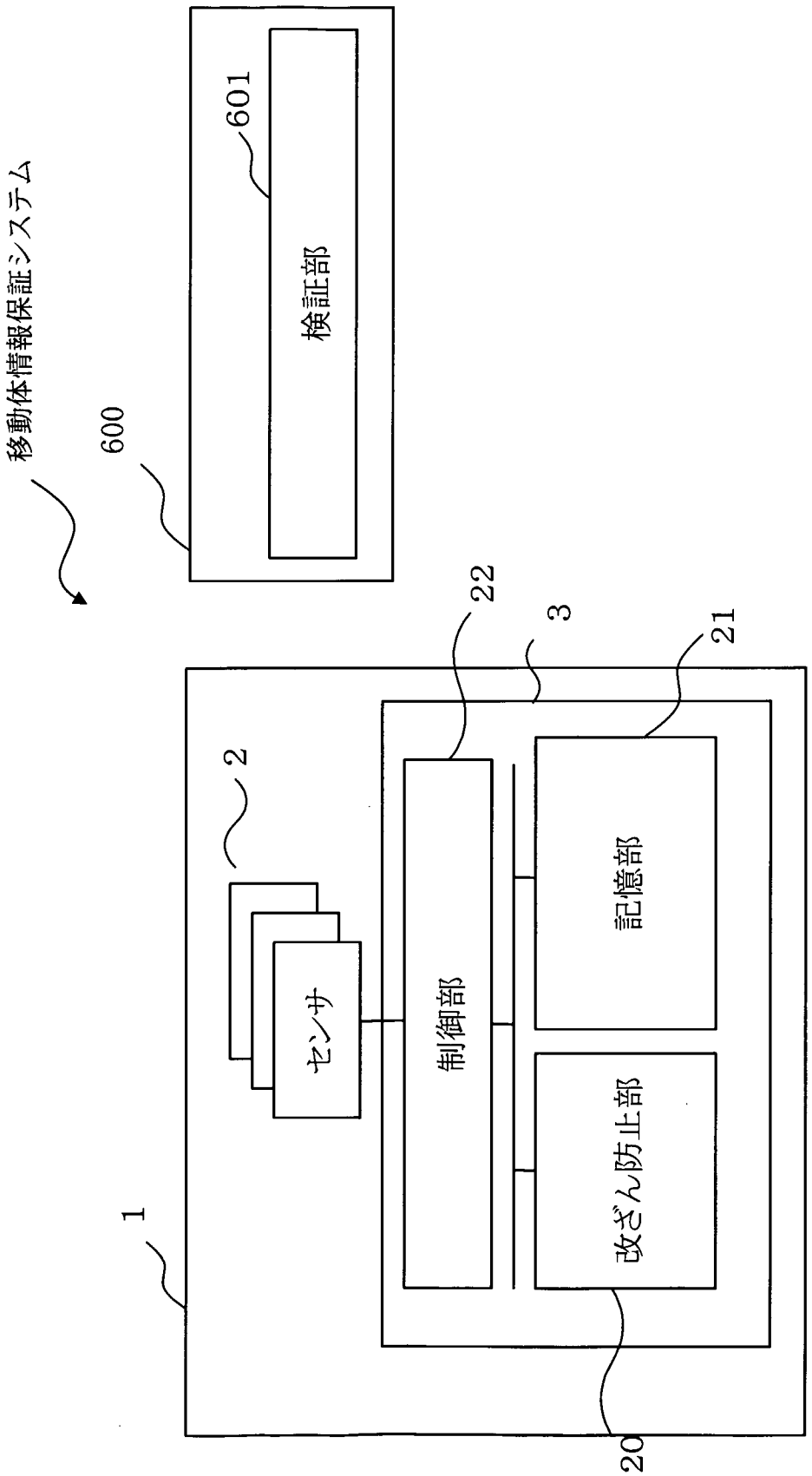

301
1
2
移動体側固有情報処理部
移動体側固有情報記憶部
センサ
分離
防止部
情報
消去部
制御部
22
3
24
501
記憶部
装置側固有情報
記憶部
31
改ざん防止部
移動体情報記憶部
32
完全性情報記憶部
33
20
21

図 14



[図15]

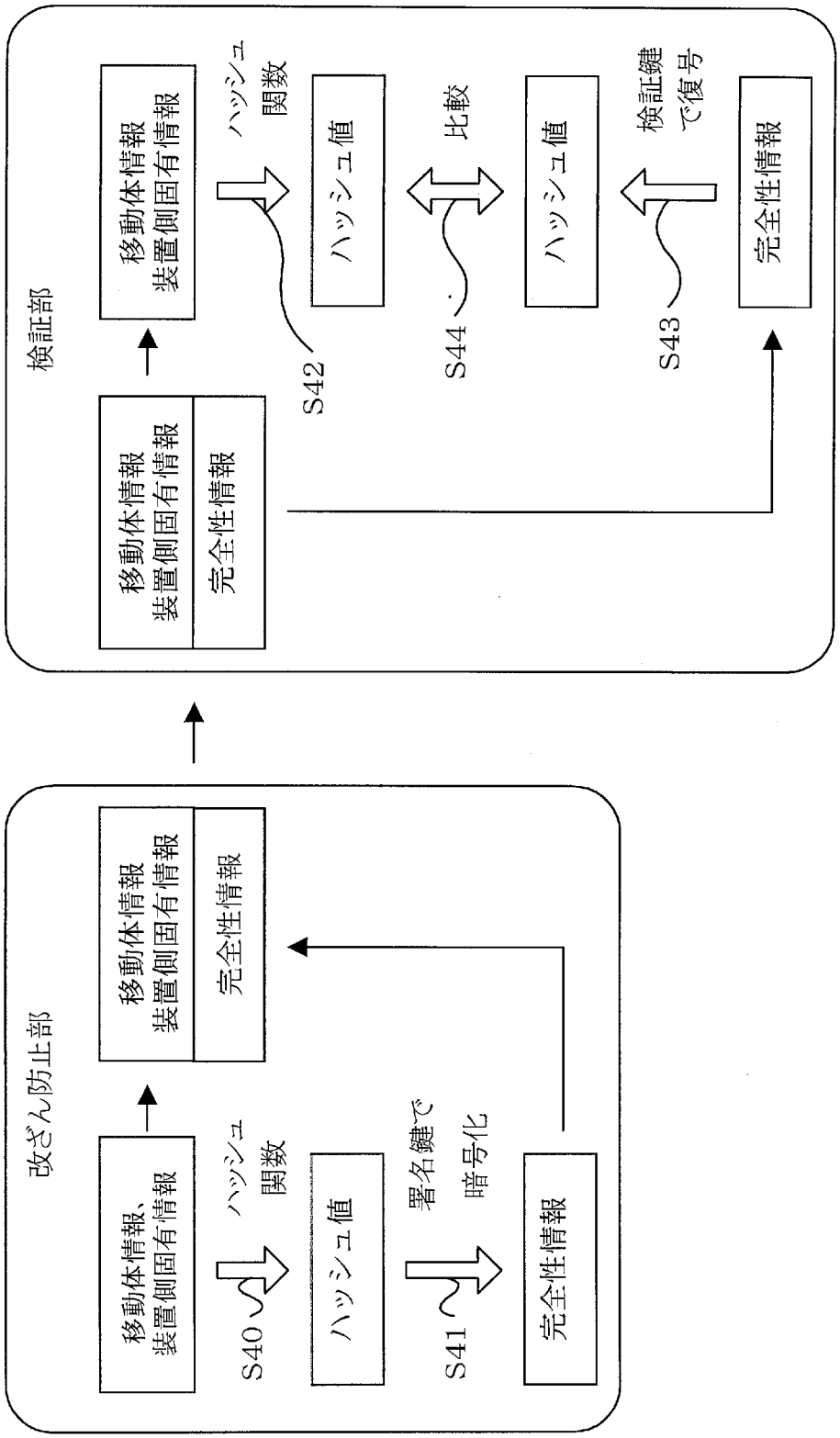

改ざん防止部
移動体情報、
装置側固有情報
S40
ハッシュ
関数
ハッシュ値
S41
署名鍵で
暗号化
完全性情報
移動体情報
装置側固有情報
完全性情報
検証部
移動体情報
装置側固有情報
S42
ハッシュ
関数
ハッシュ値
S44
比較
ハッシュ値
S43
検証鍵
で復号
完全性情報

図16

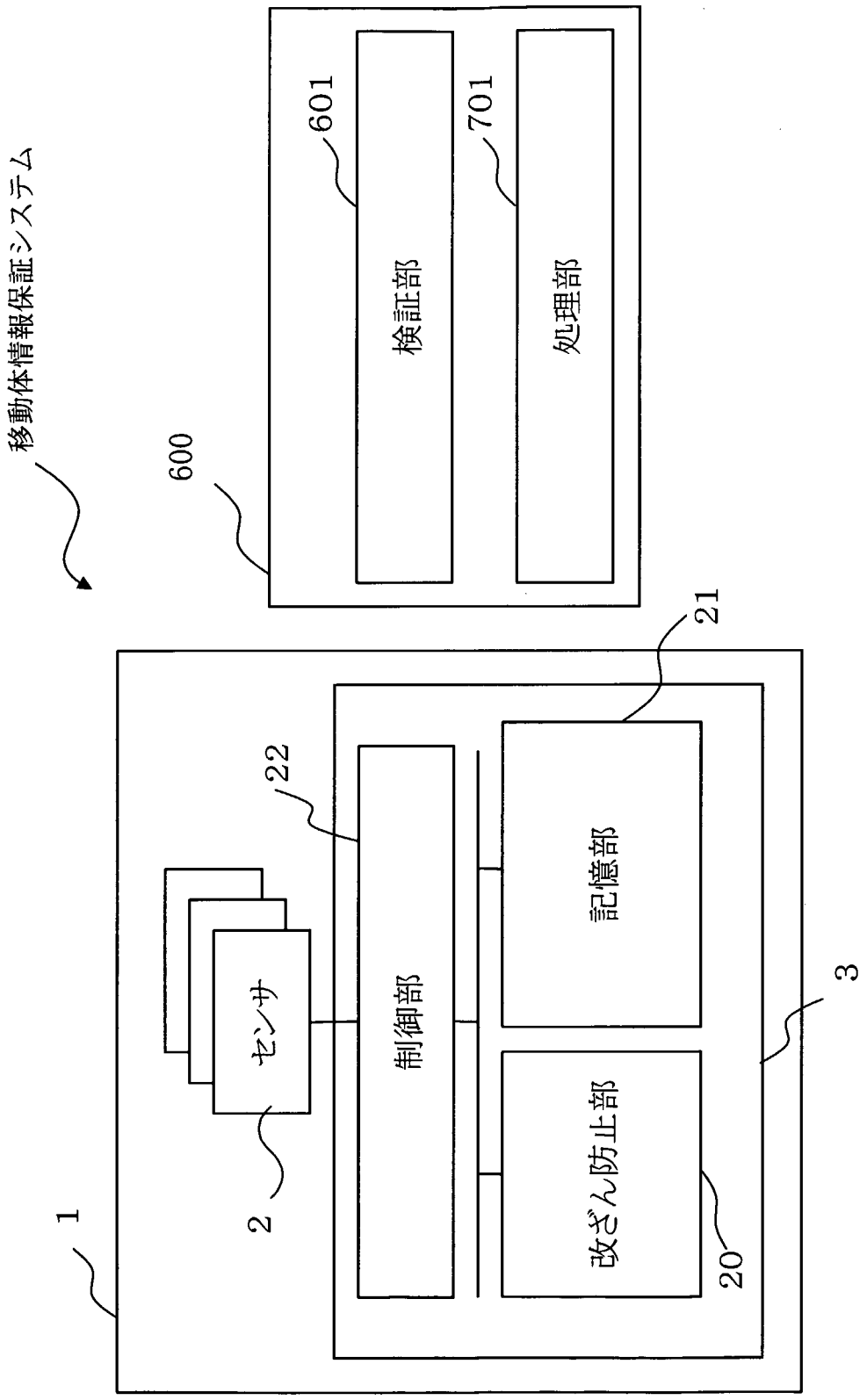
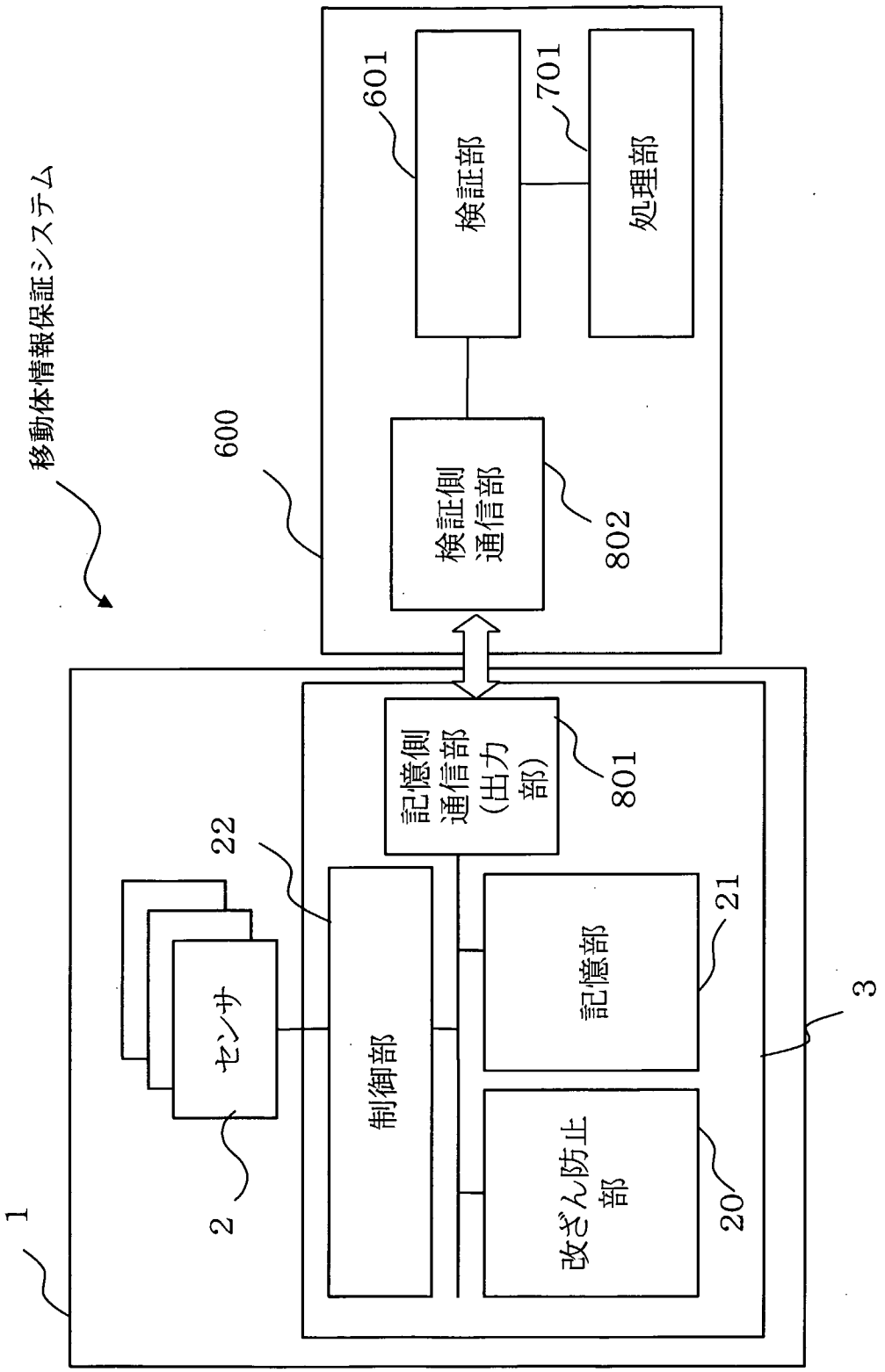

移動体情報保証システム
600
601
検証部
701
処理部
21
22
センサ
制御部
記憶部
改ざん防止部
1
2
3
20

図 17


移動体情報保証システム
600
601
検証部
701
処理部
検証側
通信部
802
記憶側
通信部
(出力
部)
801
22
センサ
制御部
記憶部
21
3
改ざん防止
部
20
2
1

[図18]

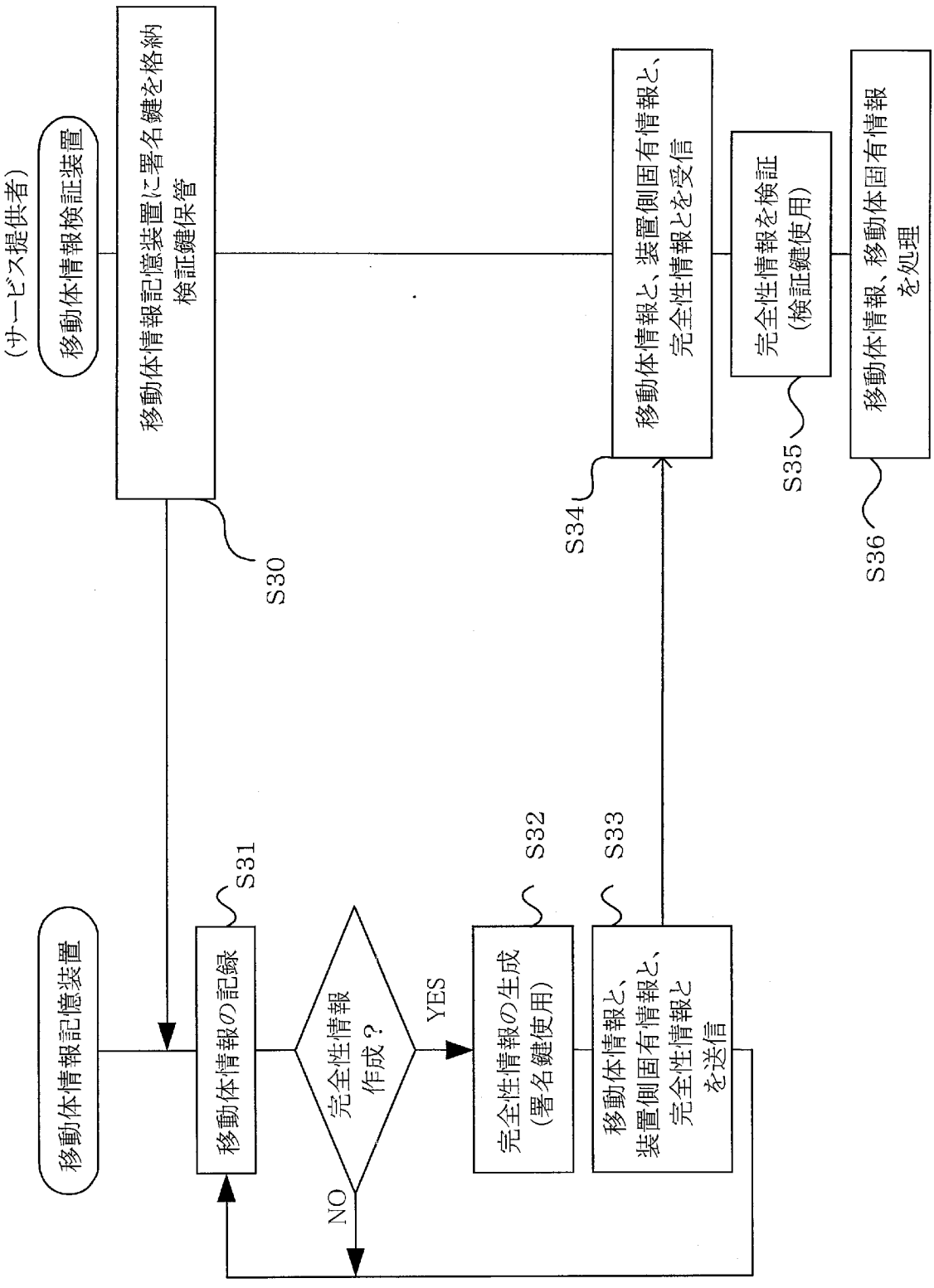

(サービス提供者)
移動体情報検証装置
移動体情報記憶装置に署名鍵を格納
検証鍵保管
S30
移動体情報記憶装置
移動体情報の記録
S31
完全性情報
作成？
YES
NO
完全性情報の生成
(署名鍵使用)
S32
移動体情報と、
装置側固有情報と、
完全性情報と
を送信
S33
移動体情報と、装置側固有情報と、
完全性情報とを受信
S34
完全性情報を検証
(検証鍵使用)
S35
移動体情報、移動体固有情報
を処理
S36

図 19

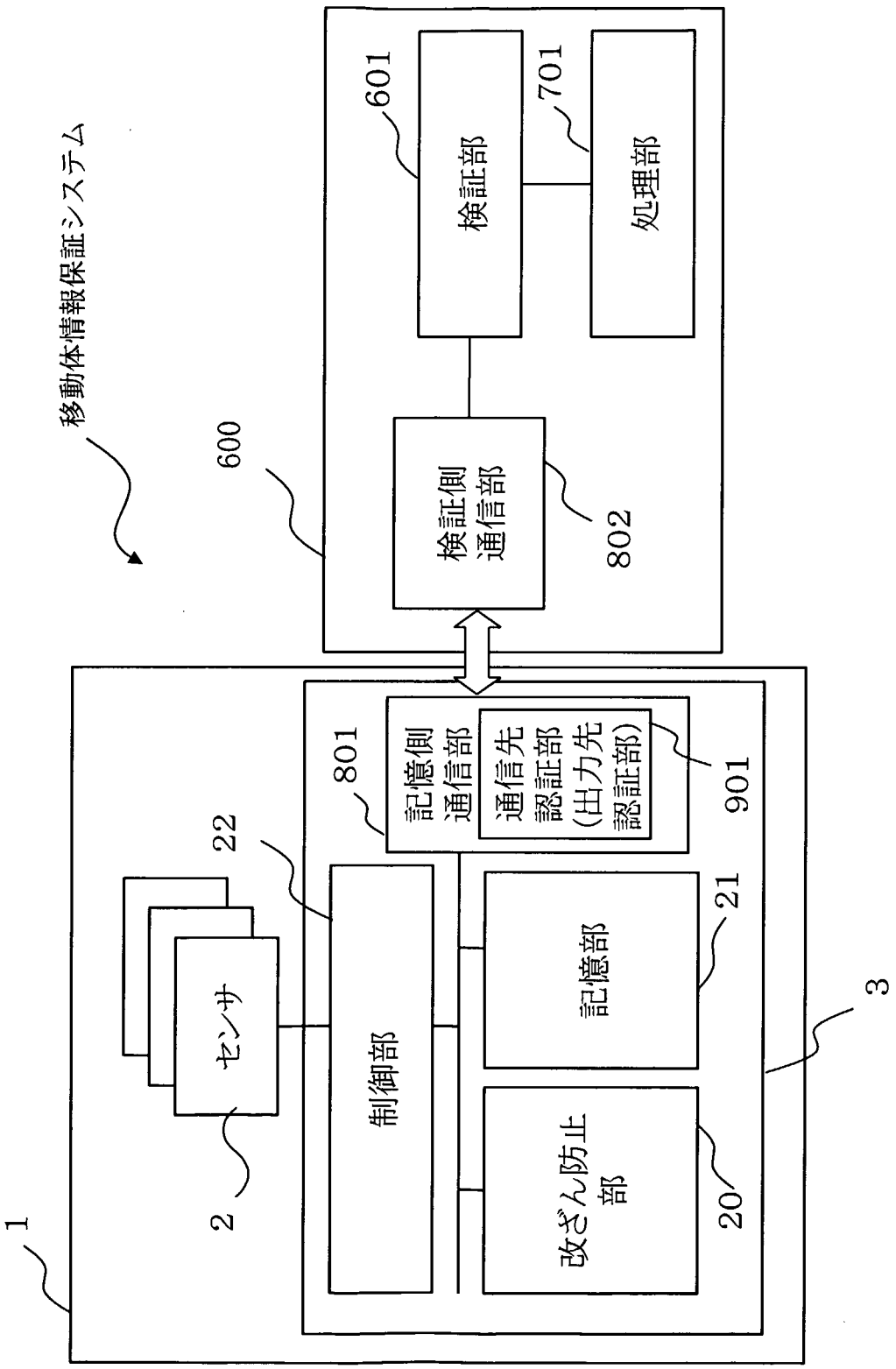
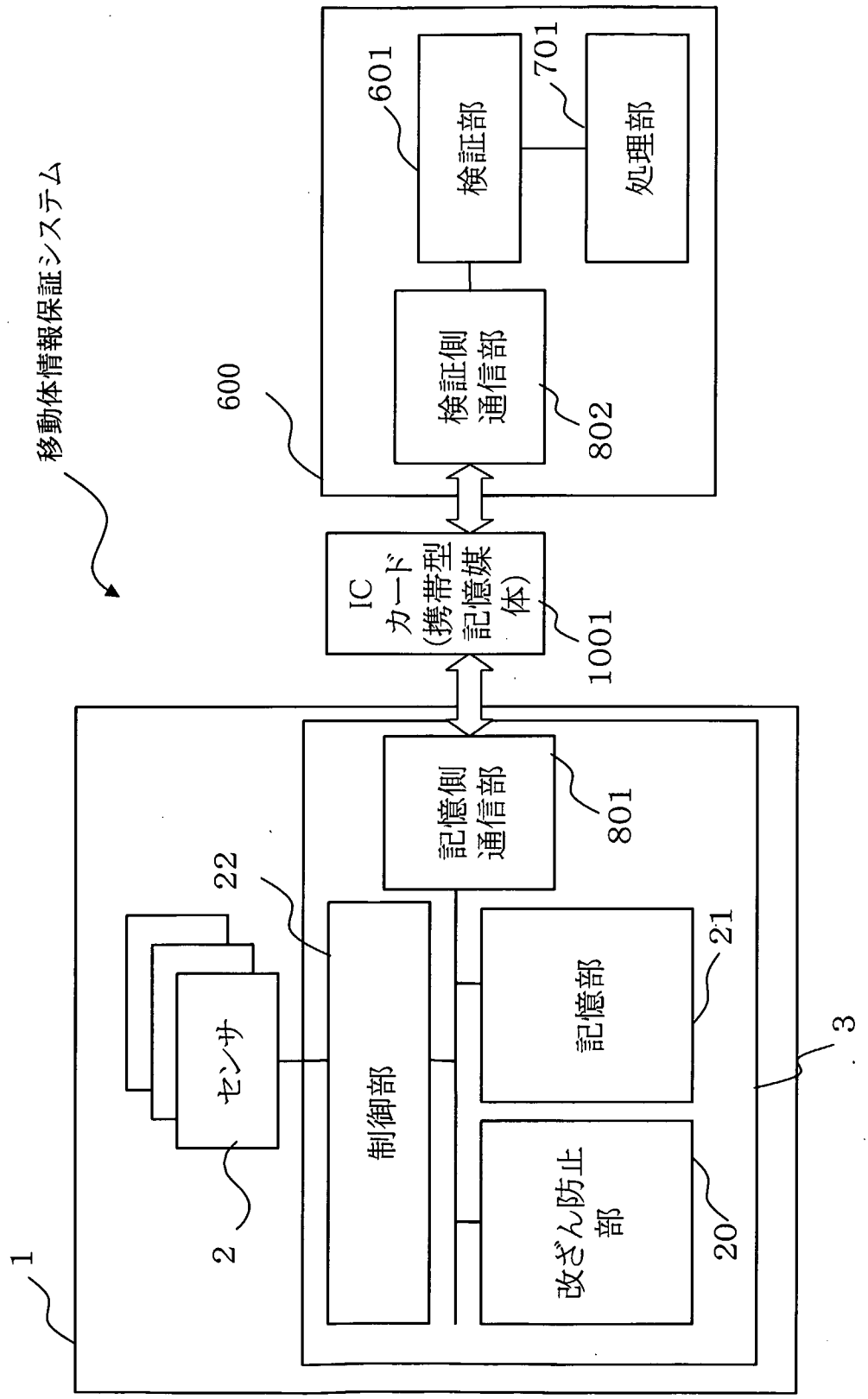
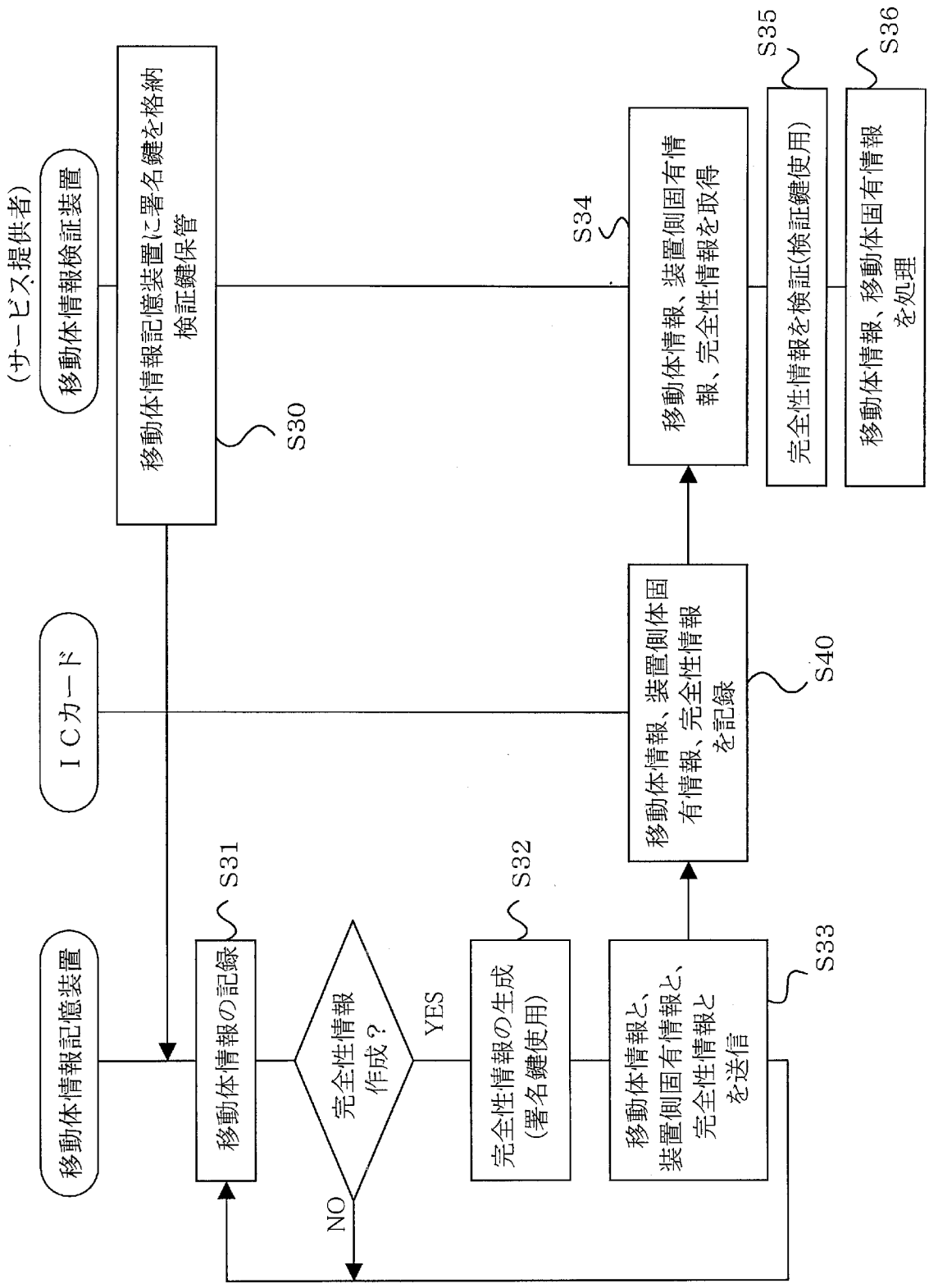

移動体情報保証システム
600
601
検証部
701
処理部
検証側
通信部
802
1
2
センサ
22
制御部
801
記憶側
通信部
通信先
認証部
(出力先
認証部)
901
記憶部
21
改ざん防止
部
20
3

図 20


移動体情報保証システム
600
601
検証部
701
処理部
検証側
通信部
802
IC
カード
(携帯型
記憶媒
体)
1001
記憶側
通信部
801
22
センサ
制御部
記憶部
21
3
改ざん防止
部
20
2
1

[図21]


(サービス提供者)
移動体情報検証装置
ICカード
移動体情報記憶装置
移動体情報記憶装置に署名鍵を格納
検証鍵保管
S30
移動体情報の記録
S31
完全性情報
作成？
YES
NO
完全性情報の生成
(署名鍵使用)
S32
移動体情報と、
装置側固有情報と、
完全性情報と
を送信
S33
移動体情報、装置側体固
有情報、完全性情報
を記録
S40
移動体情報、装置側固有情
報、完全性情報を取得
S34
完全性情報を検証(検証鍵使用)
S35
移動体情報、移動体固有情報
を処理
S36

[図22]

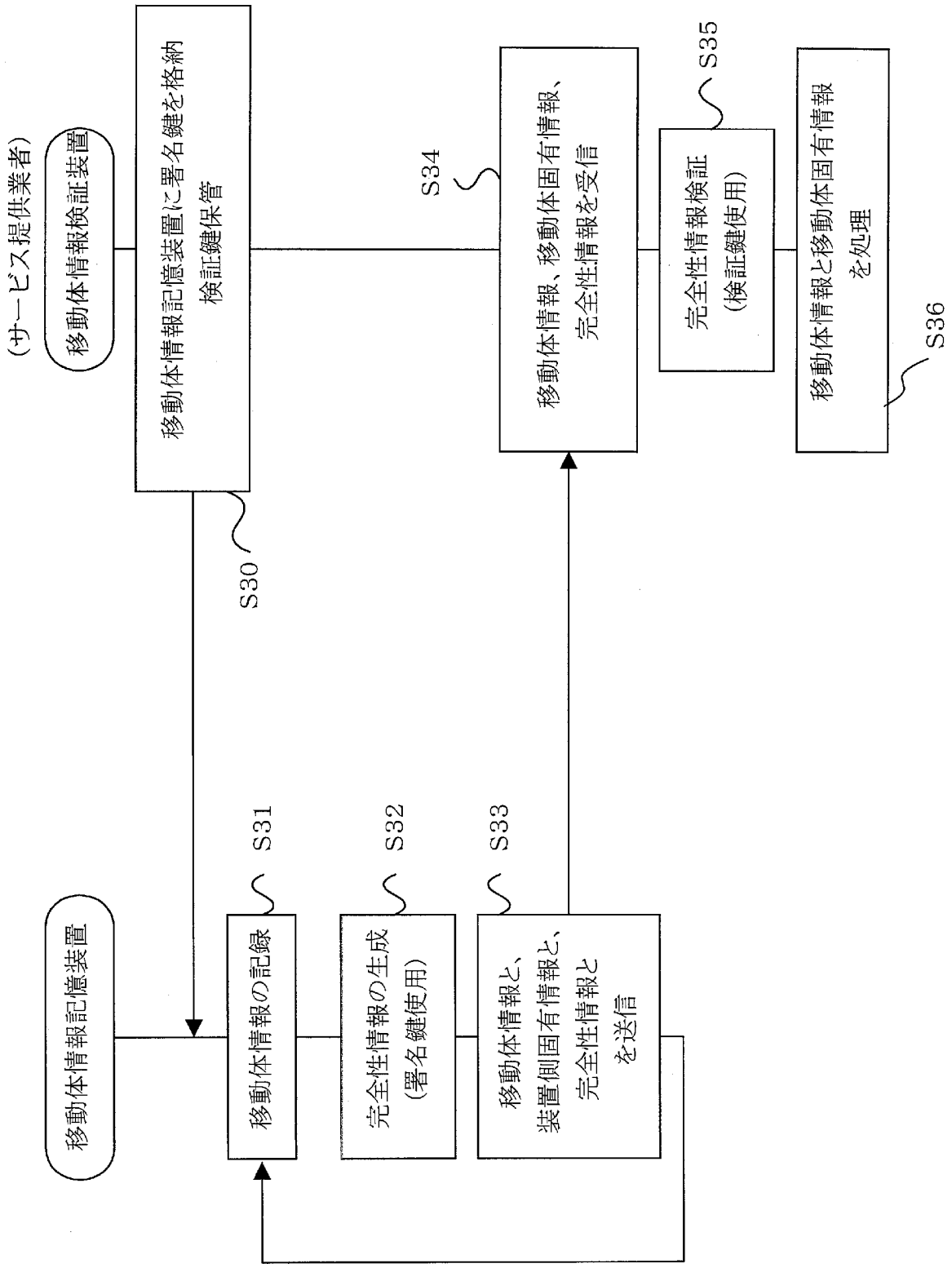

(サービス提供業者)
移動体情報検証装置
移動体情報記憶装置に署名鍵を格納
検証鍵保管
S30
S34
移動体情報、移動体固有情報、
完全性情報を受信
S35
完全性情報検証
(検証鍵使用)
移動体情報と移動体固有情報
を処理
S36
移動体情報記憶装置
S31
移動体情報の記録
S32
完全性情報の生成
(署名鍵使用)
S33
移動体情報と、
装置側固有情報と、
完全性情報と
を送信

図 23

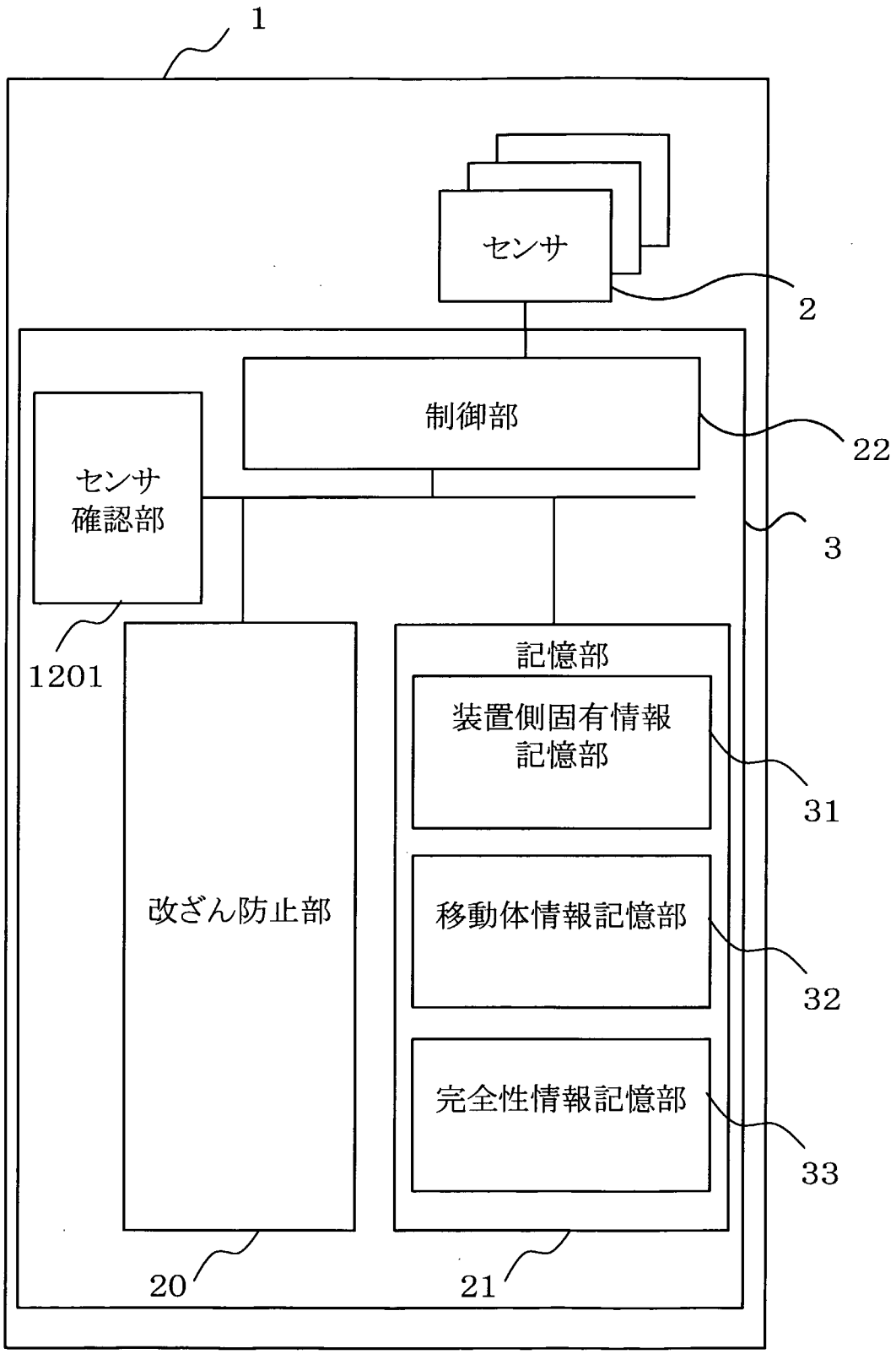
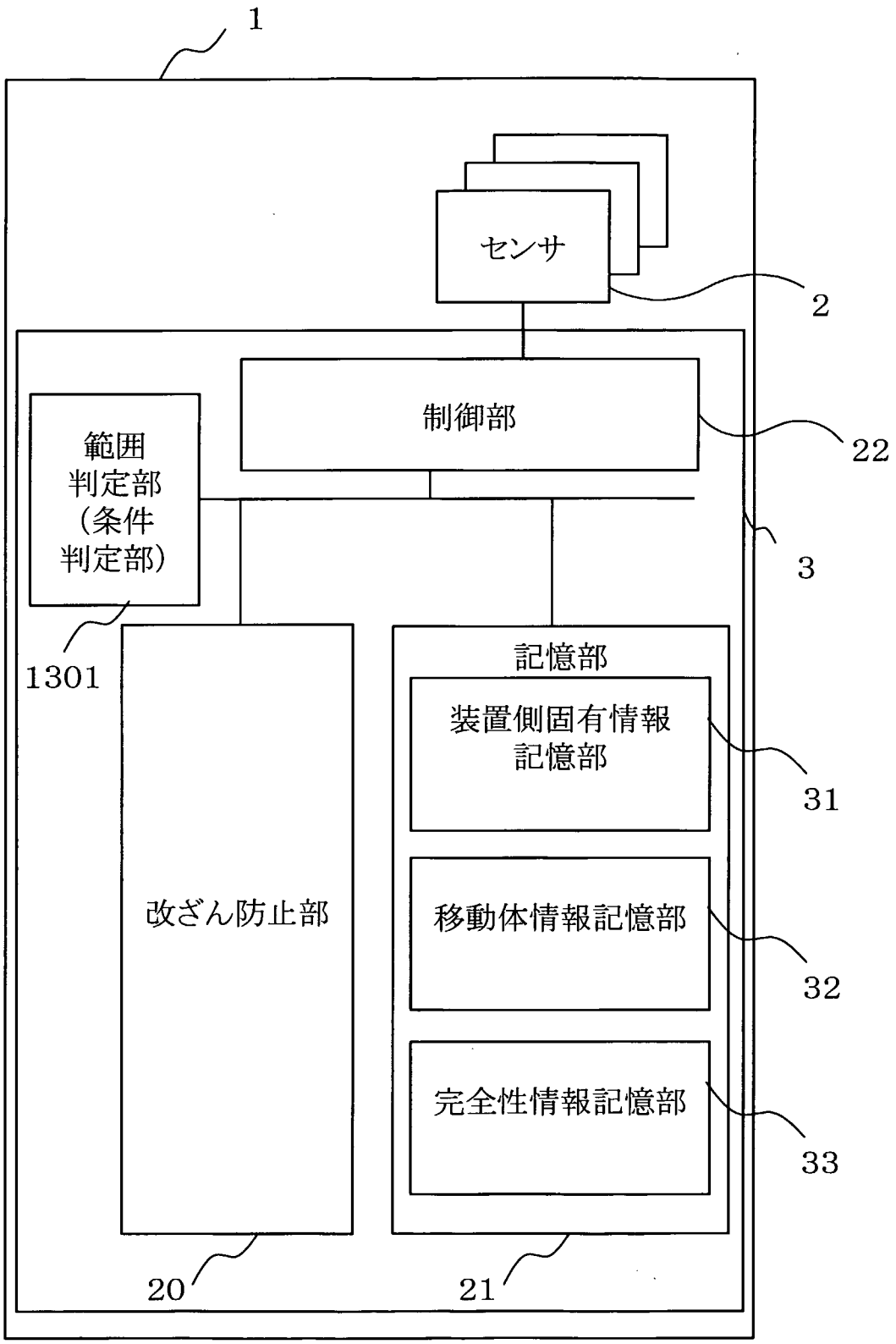

1
センサ
2
制御部
22
センサ
確認部
3
1201
記憶部
装置側固有情報
記憶部
31
改ざん防止部
移動体情報記憶部
32
完全性情報記憶部
33
20
21

図 24


1
センサ
2
制御部
22
範囲
判定部
(条件
判定部)
1301
3
記憶部
装置側固有情報
記憶部
31
改ざん防止部
移動体情報記憶部
32
完全性情報記憶部
33
20
21

[図25]

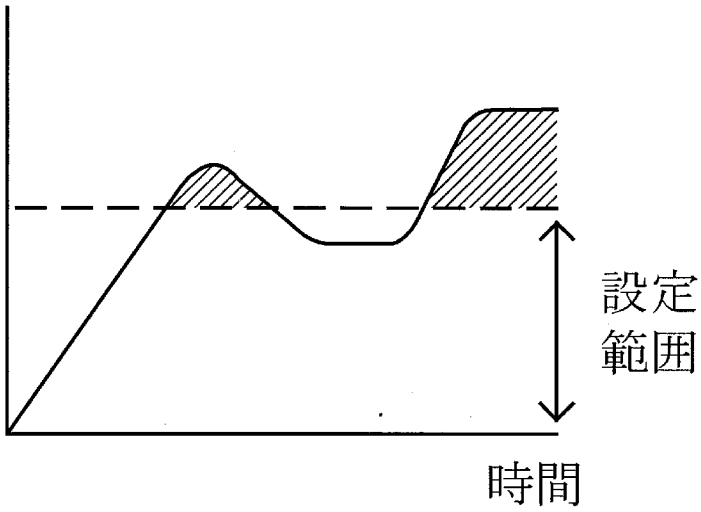
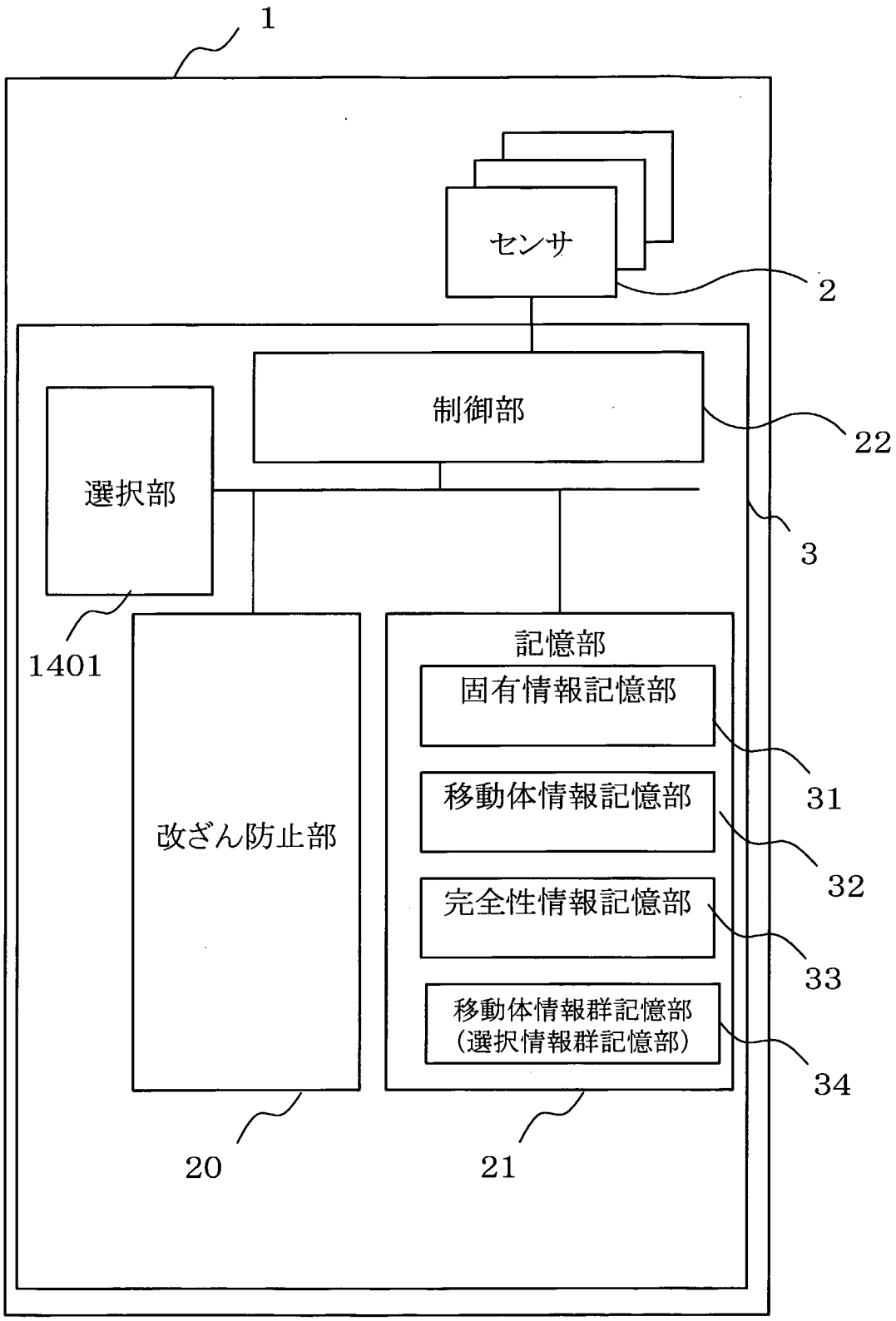


図 26


1
センサ
2
制御部
22
選択部
3
1401
記憶部
固有情報記憶部
31
移動体情報記憶部
32
完全性情報記憶部
33
移動体情報群記憶部
(選択情報群記憶部)
34
改ざん防止部
20
21

[図27]

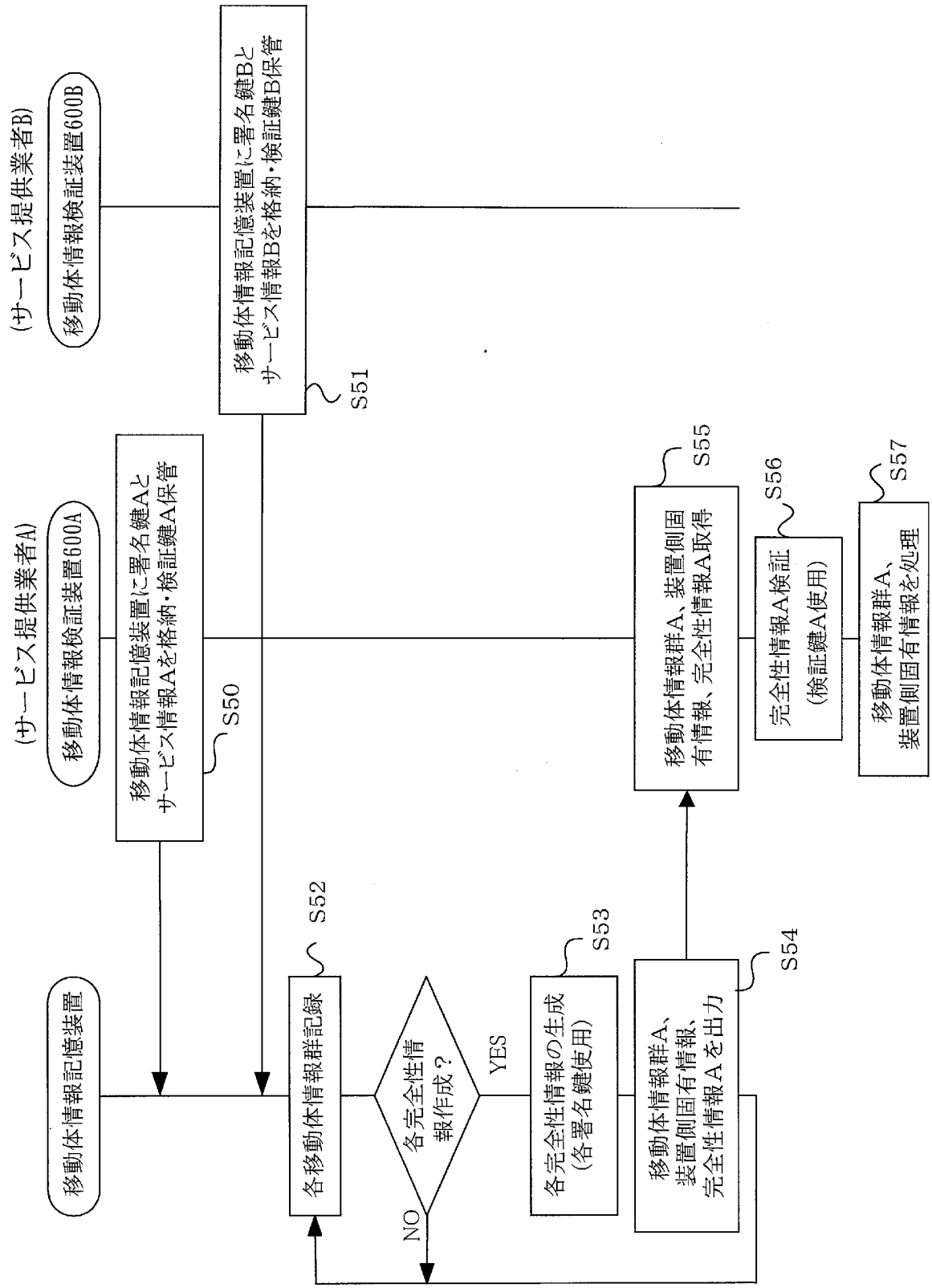

(サービス提供業者B)
移動体情報検証装置600B
移動体情報記憶装置に署名鍵Bとサービス情報Bを格納・検証鍵B保管
S51
(サービス提供業者A)
移動体情報検証装置600A
移動体情報記憶装置に署名鍵Aとサービス情報Aを格納・検証鍵A保管
S50
移動体情報記憶装置
各移動体情報群記録
S52
各完全性情報の生成
(各署名鍵使用)
S53
移動体情報群A、
装置側固有情報、
完全性情報Aを出力
S54
各完全性情報群完成？
YES
NO
移動体情報群A、装置側固有情報、完全性情報A取得
S55
完全性情報A検証
(検証鍵A使用)
S56
移動体情報群A、
装置側固有情報を処理
S57

図 28

1402

	移動体情報X (速度)	移動体情報Y (走行距離)	移動体情報Z (エンジン回転数)
サービスA	1	1	0
サービスB	1	0	1

図 29

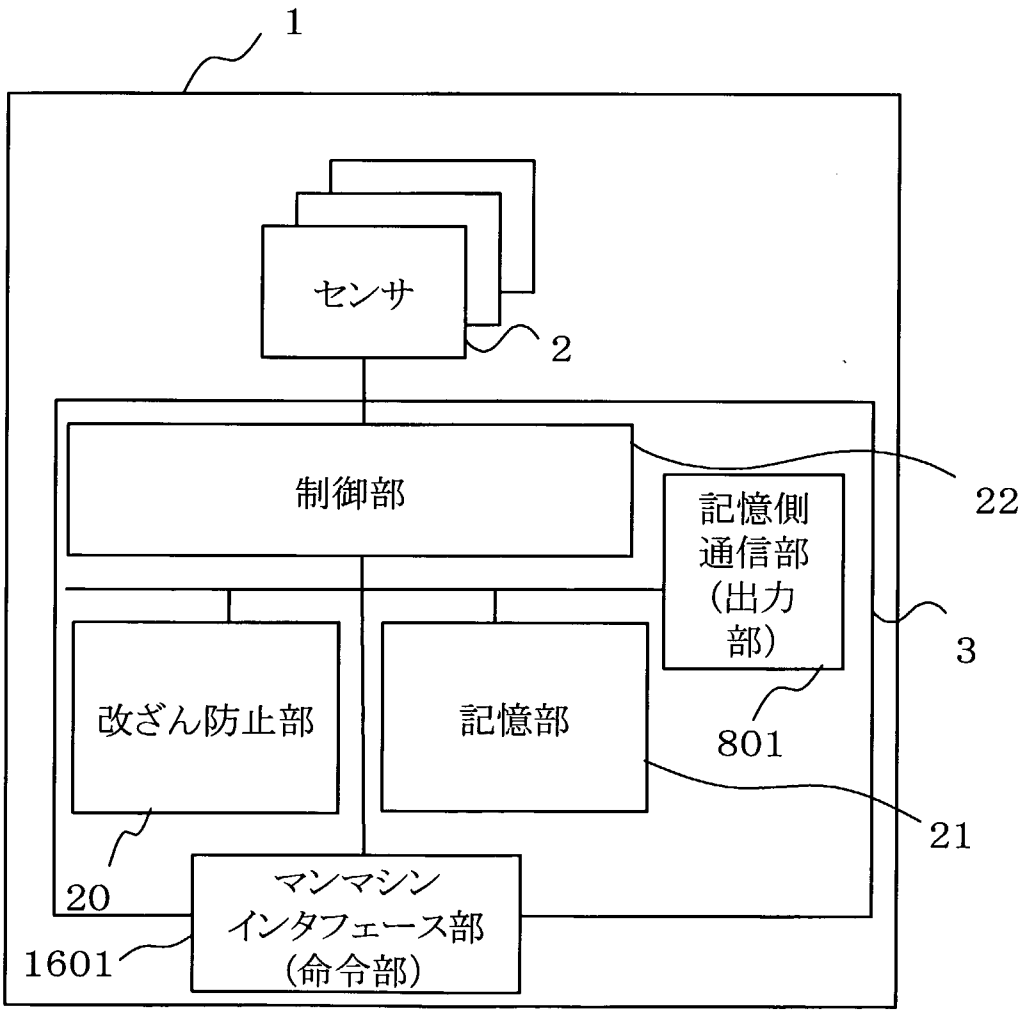
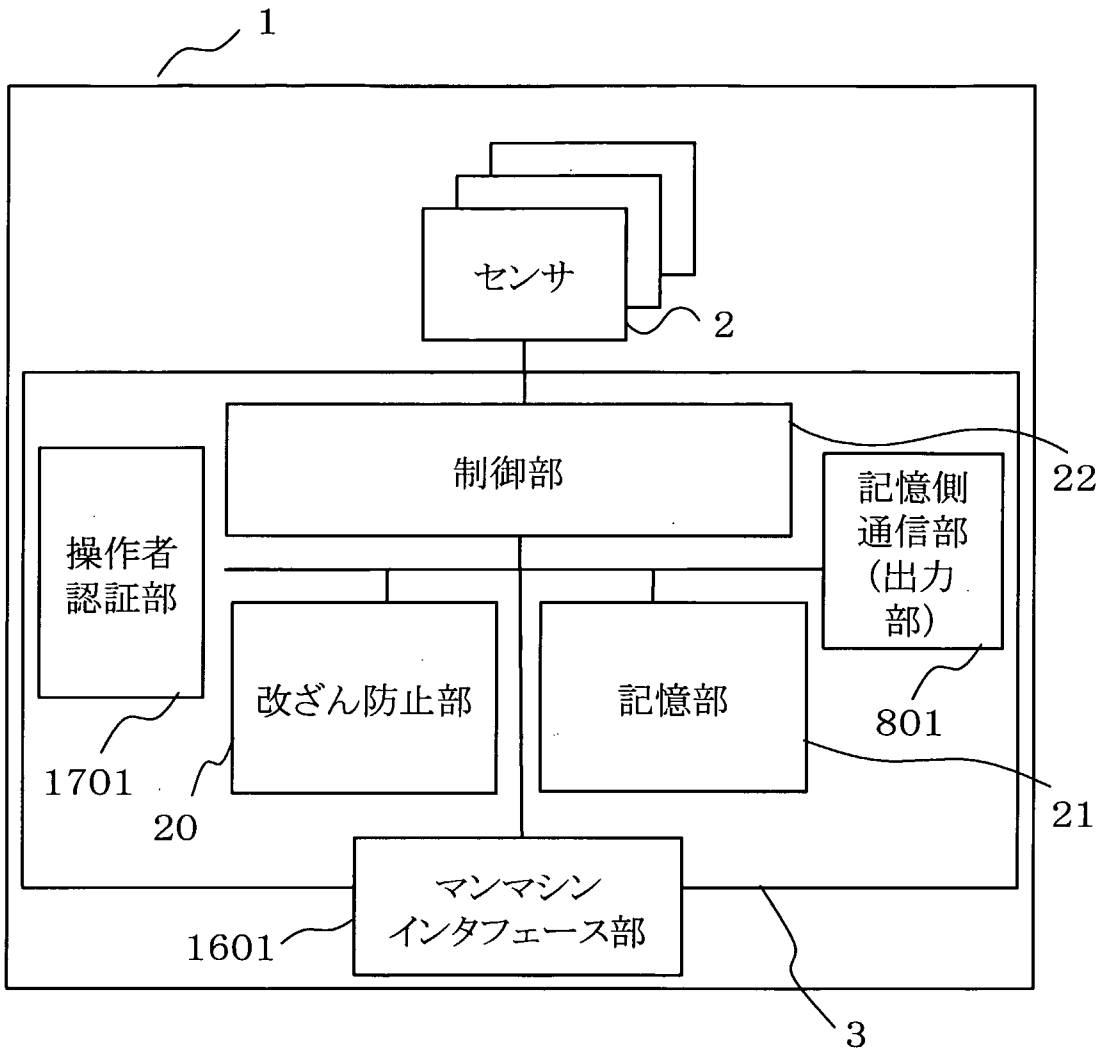


図 30


1
センサ
2
制御部
22
操作者
認証部
記憶側
通信部
(出力
部)
改ざん防止部
記憶部
801
1701
20
21
マンマシン
インタフェース部
1601
3

[図31]

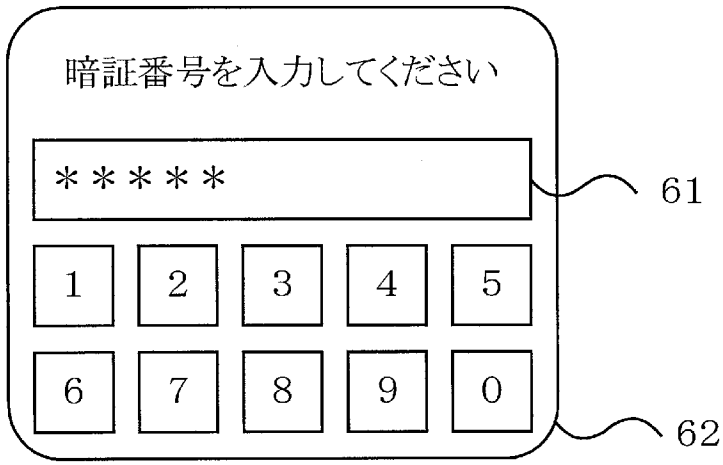


図 32

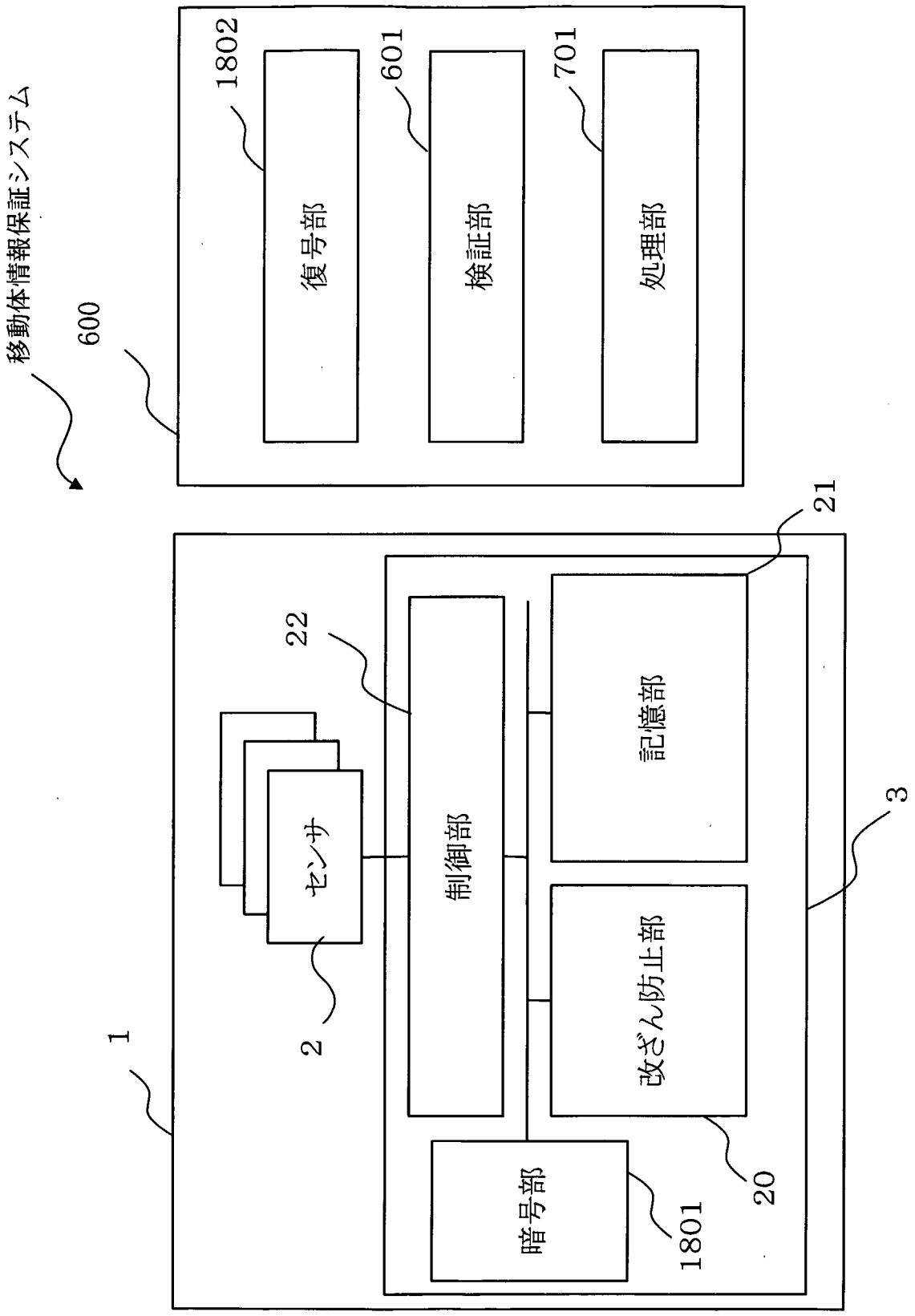

移動体情報保証システム
600
1802
復号部
601
検証部
701
処理部
1
2
センサ
22
制御部
21
記憶部
3
改ざん防止部
20
暗号部
1801

図 33

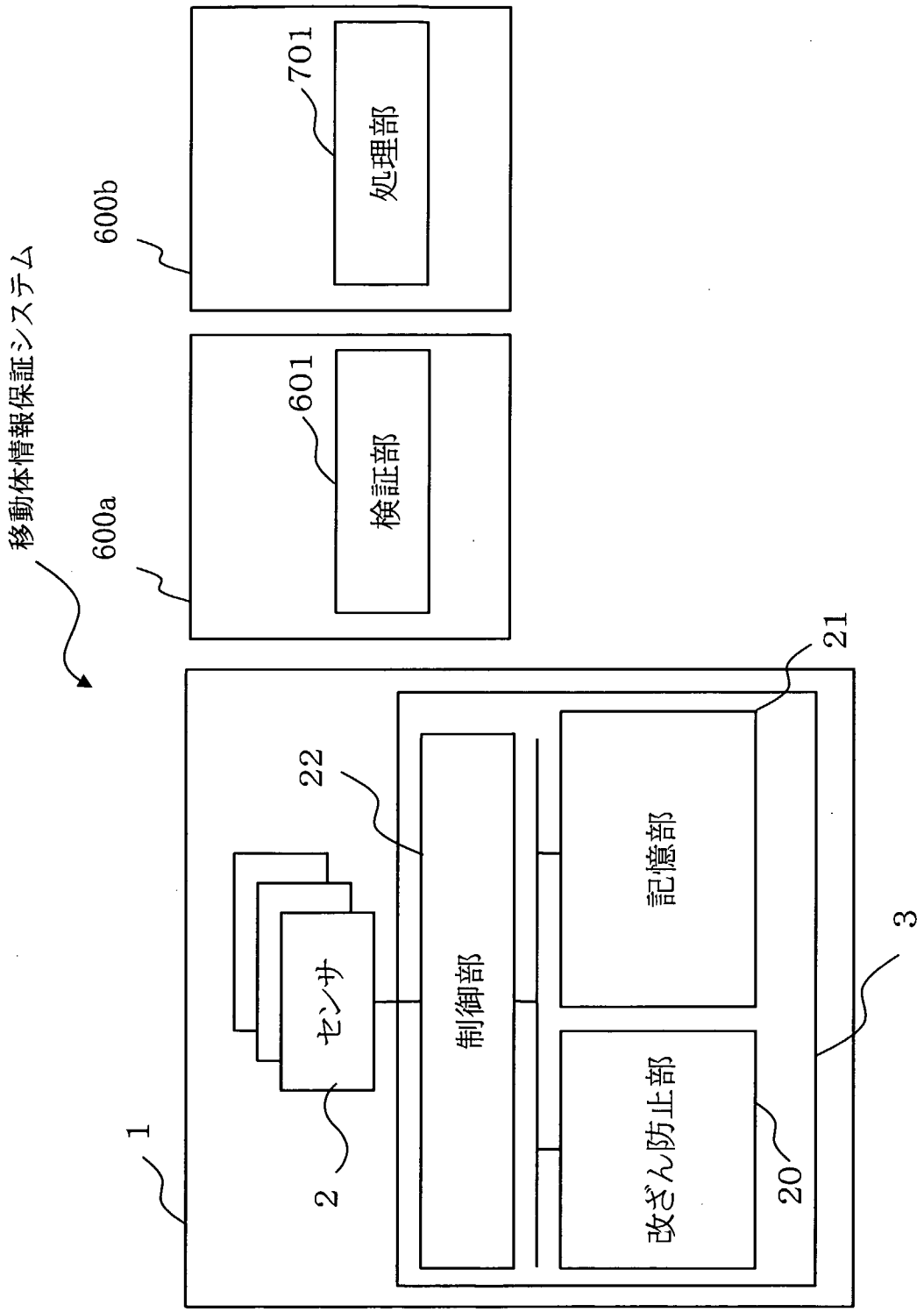
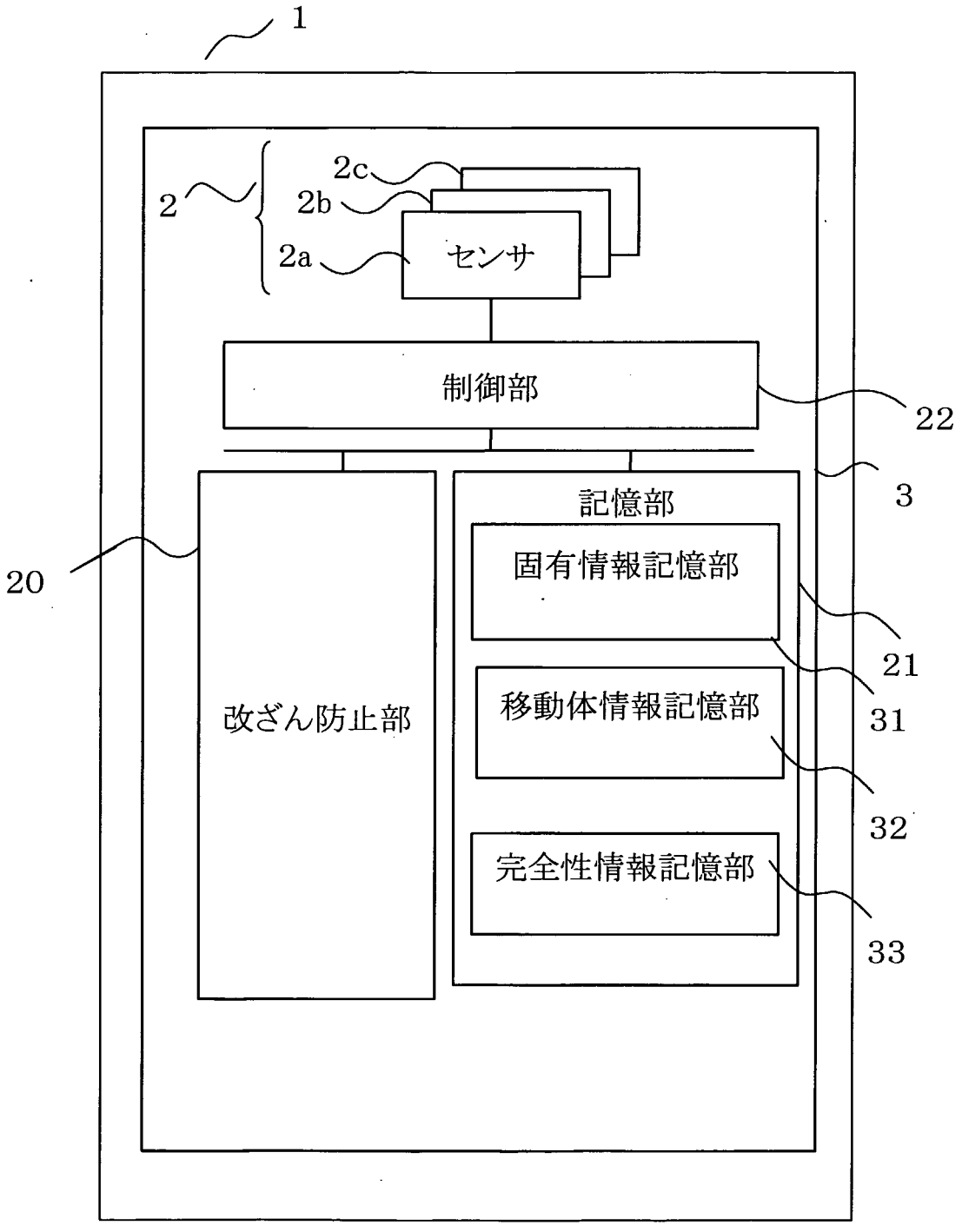
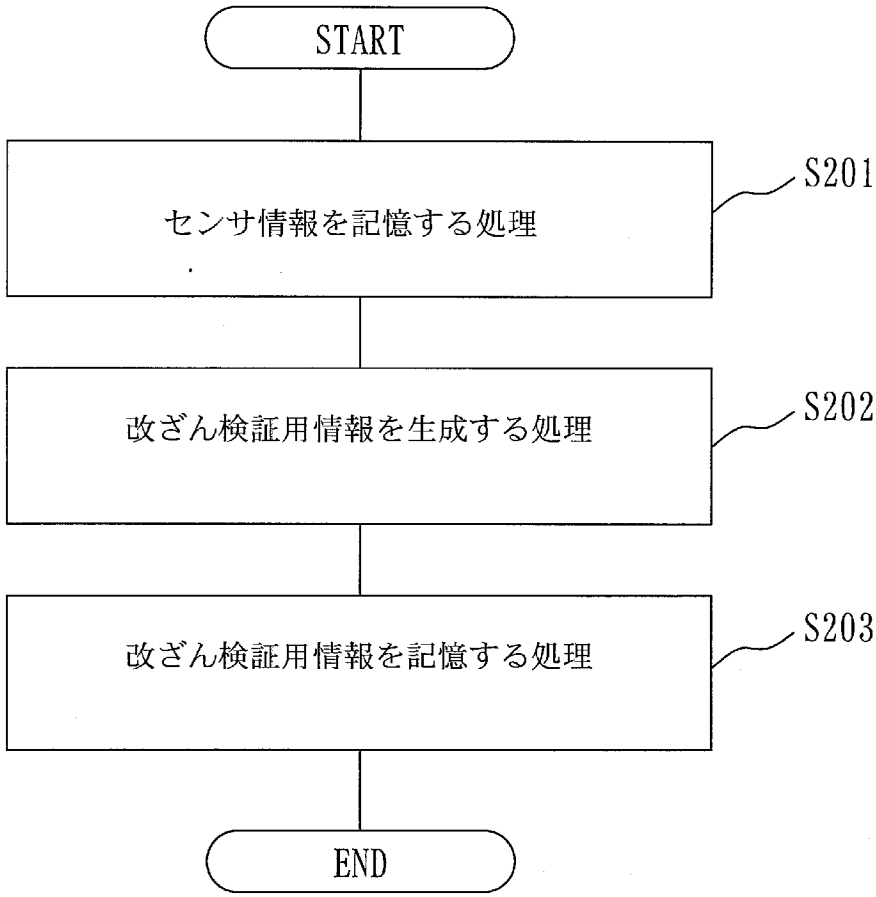

移動体情報保証システム
600a
600b
601
検証部
701
処理部
1
2
センサ
22
制御部
21
記憶部
20
改ざん防止部
3

図 34


1
2
2c
2b
2a
センサ
制御部
22
3
記憶部
固有情報記憶部
21
移動体情報記憶部
31
32
完全性情報記憶部
33
20
改ざん防止部

[図35]


START
センサ情報を記憶する処理
S201
改ざん検証用情報を生成する処理
S202
改ざん検証用情報を記憶する処理
S203
END

[図36]

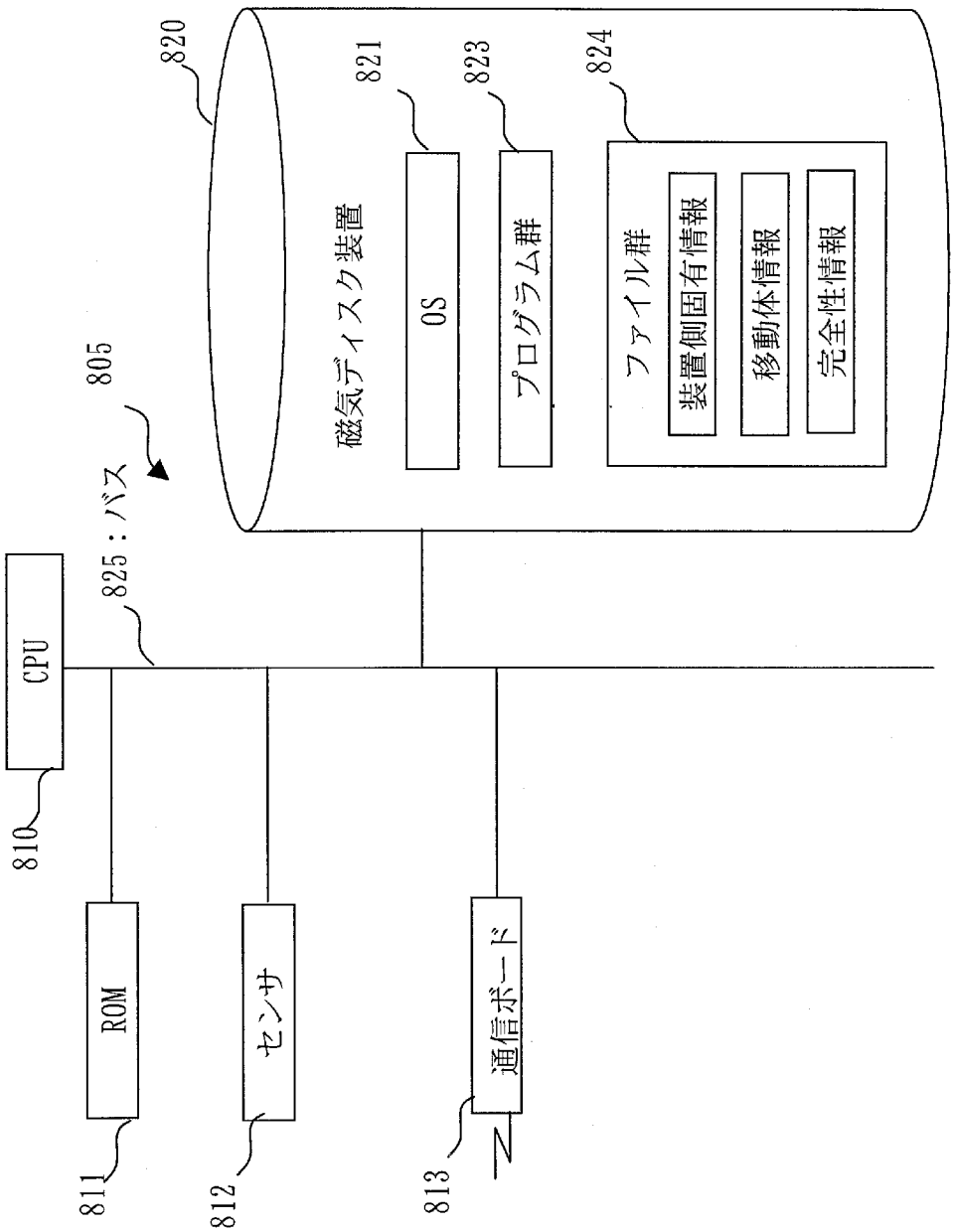
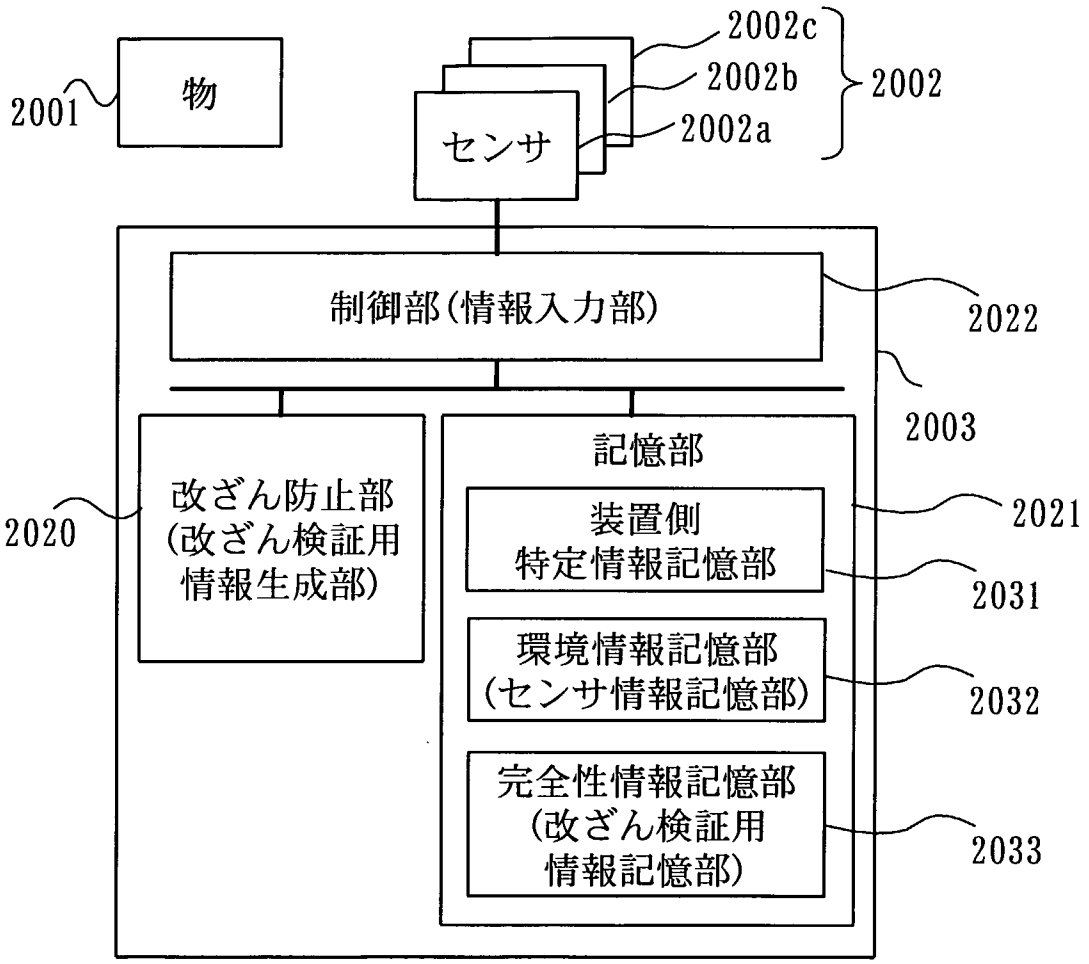
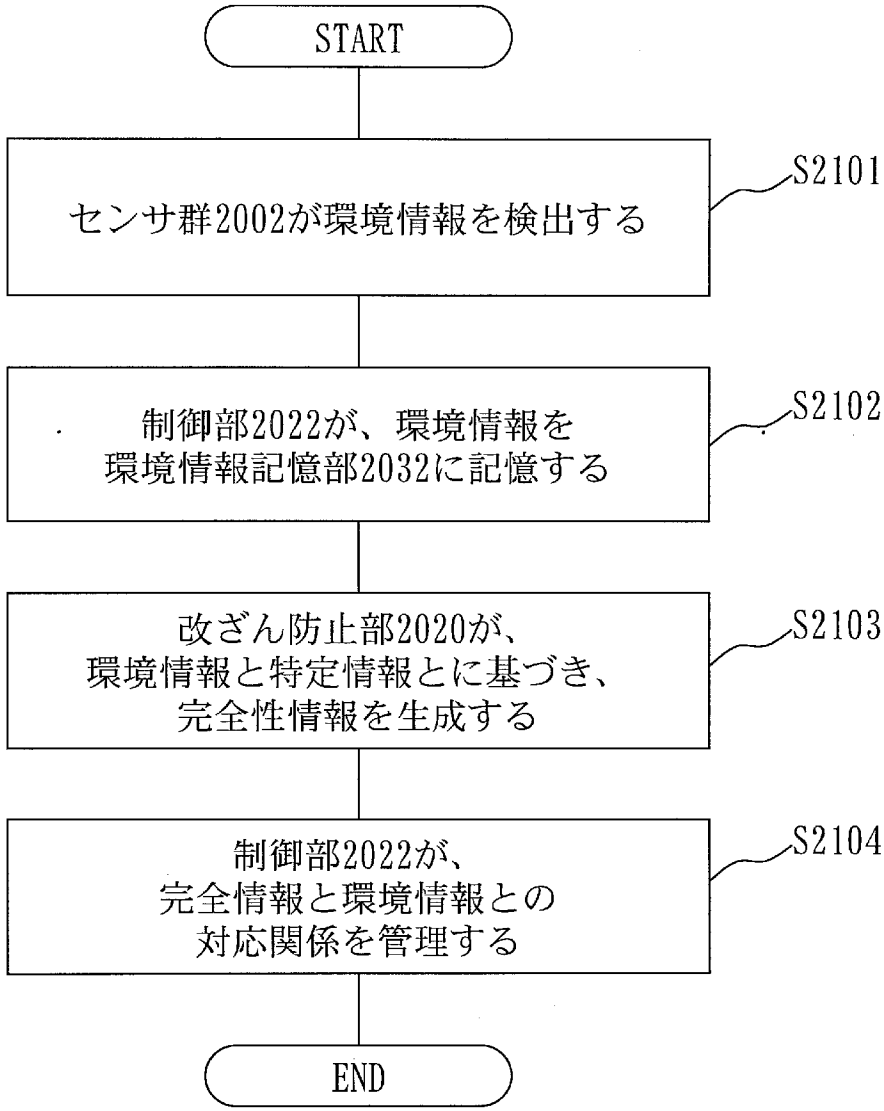

820
磁気ディスク装置
821
OS
823
プログラム群
824
ファイル群
装置側固有情報
移動体情報
完全性情報
805
825：バス
CPU
810
ROM
811
センサ
812
通信ボード
813

図 37


2001
物
センサ
2002c
2002b
2002a
2002
制御部(情報入力部)
2022
2003
記憶部
改ざん防止部
(改ざん検証用
情報生成部)
2020
装置側
特定情報記憶部
2021
2031
環境情報記憶部
(センサ情報記憶部)
2032
完全性情報記憶部
(改ざん検証用
情報記憶部)
2033

[図38]


START
センサ群2002が環境情報を検出する
S2101
制御部2022が、環境情報を
環境情報記憶部2032に記憶する
S2102
改ざん防止部2020が、
環境情報と特定情報とに基づき、
完全性情報を生成する
S2103
制御部2022が、
完全情報と環境情報との
対応関係を管理する
S2104
END

[図39]

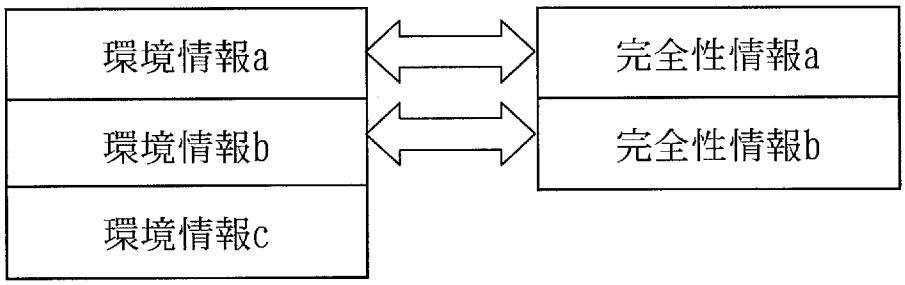

環境情報a
環境情報b
環境情報c
完全性情報a
完全性情報b

図 40

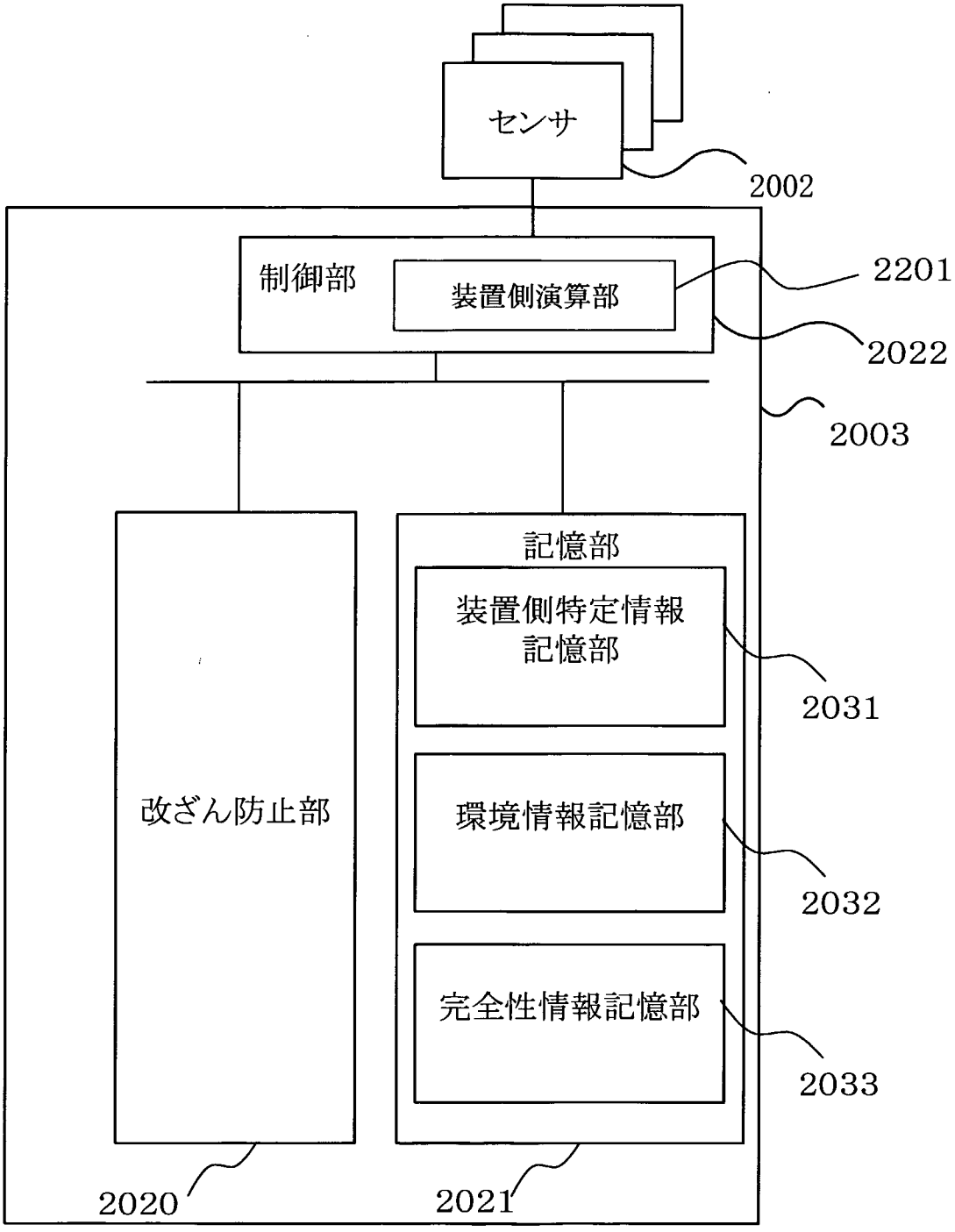

センサ
2002
制御部
装置側演算部
2201
2022
2003
記憶部
装置側特定情報記憶部
2031
改ざん防止部
環境情報記憶部
2032
完全性情報記憶部
2033
2020
2021

図 41

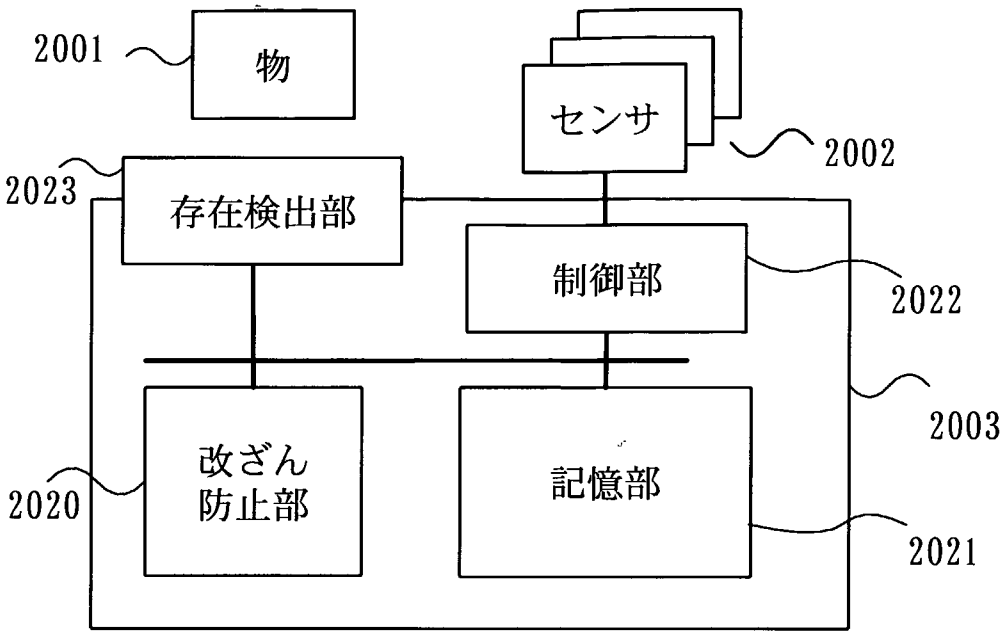

2001
物
センサ
2002
2023
存在検出部
制御部
2022
2003
改ざん
防止部
2020
記憶部
2021

図 42

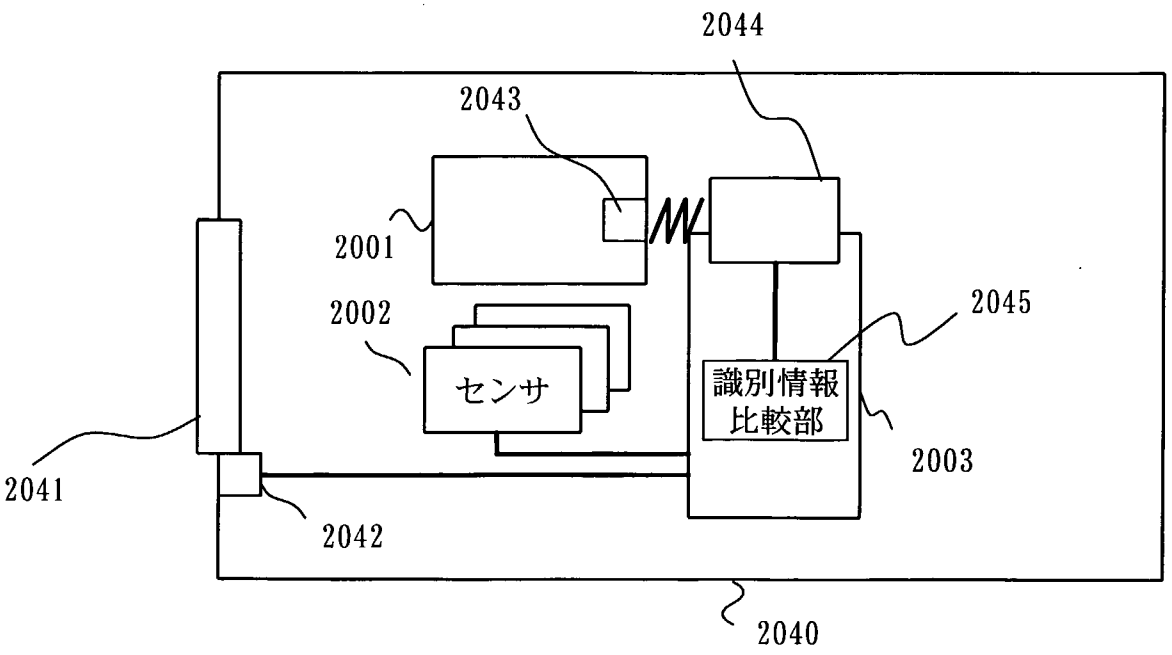

2044
2043
2001
2002
センサ
2045
識別情報
比較部
2003
2041
2042
2040

図 43

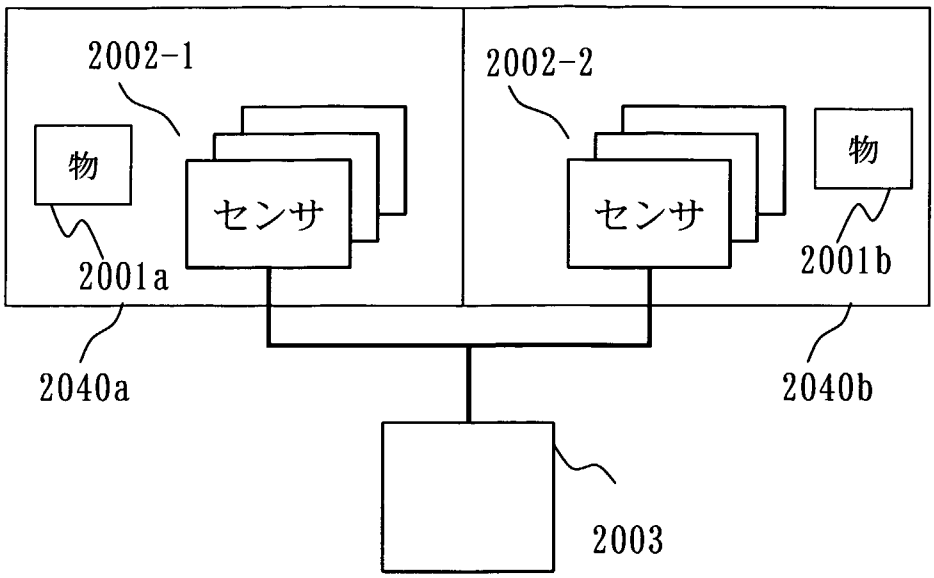
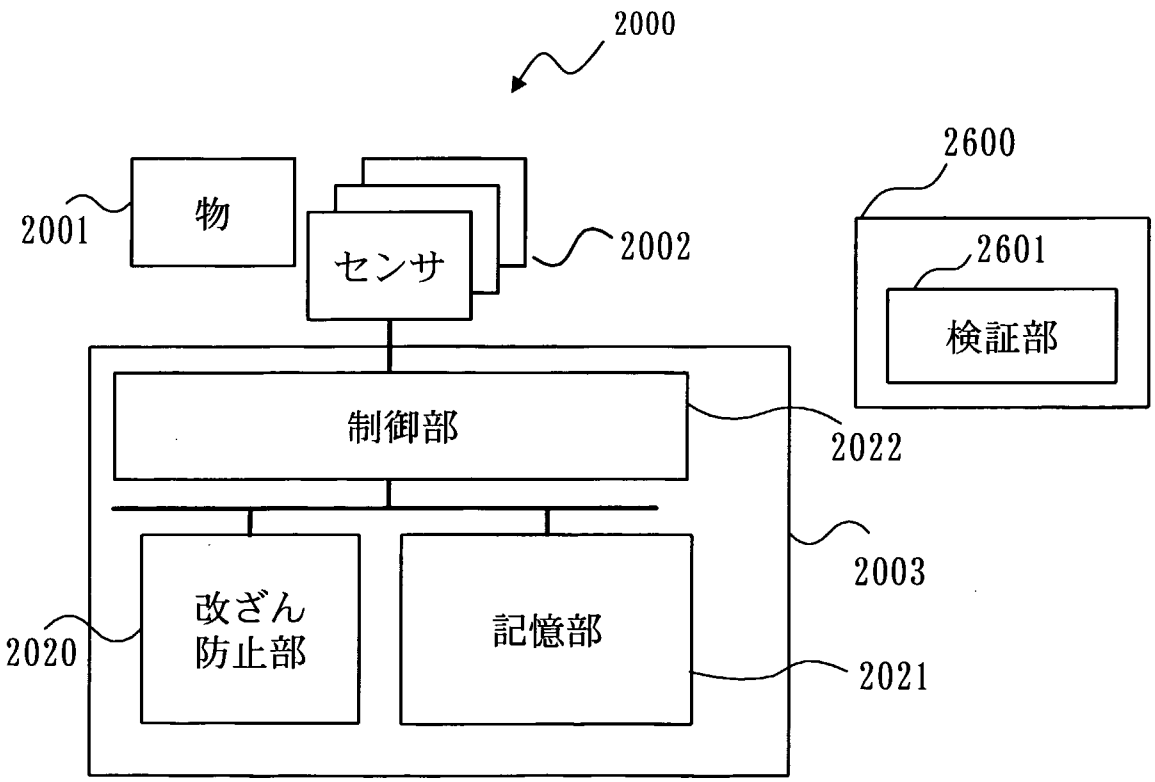
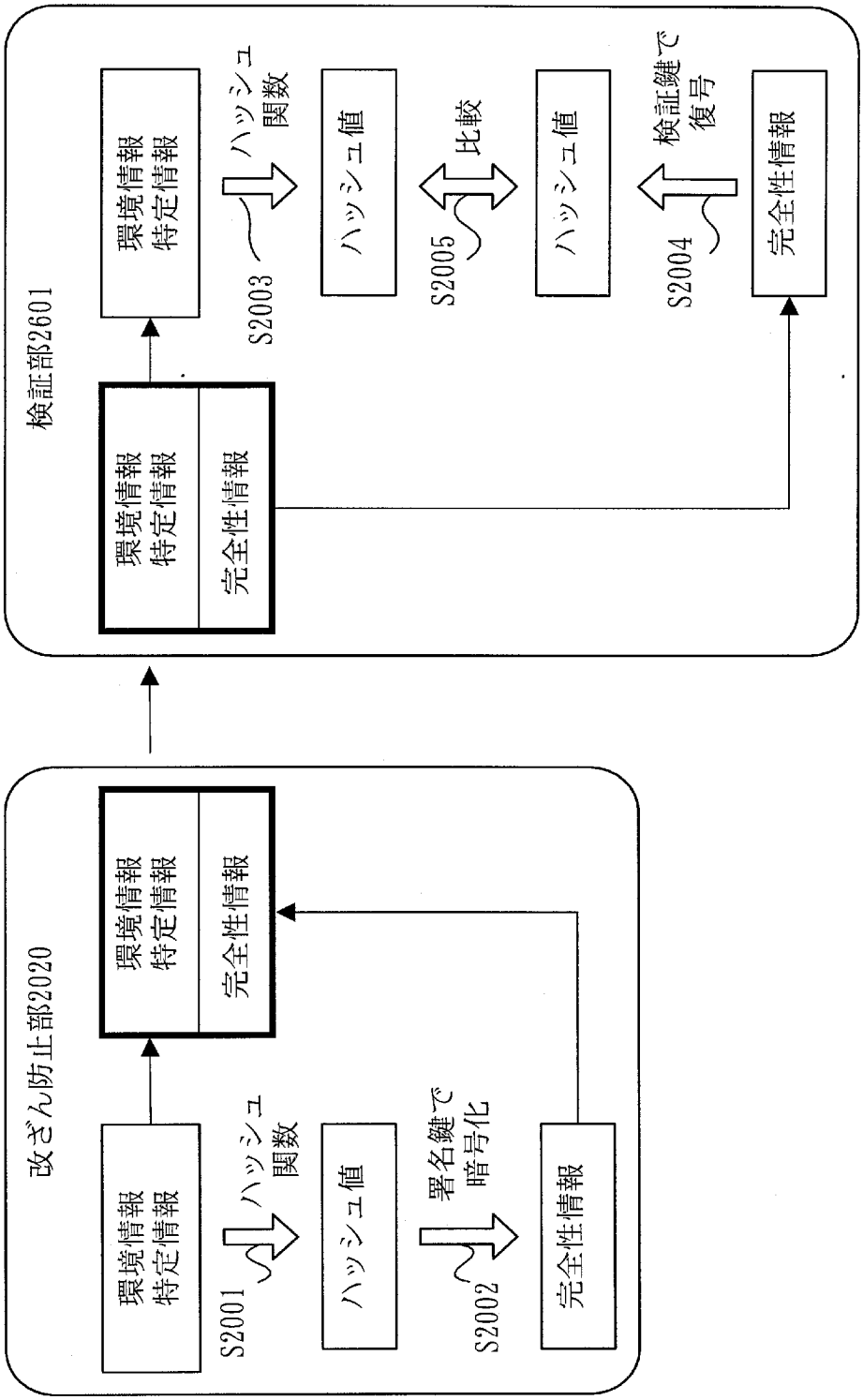

2002-1
2002-2
物
センサ
センサ
物
2001a
2001b
2040a
2040b
2003

図 44


2000
2600
2001
物
センサ
2002
2601
検証部
制御部
2022
2003
改ざん
防止部
2020
記憶部
2021

[図45]


改ざん防止部2020
環境情報
特定情報
ハッシュ
関数
S2001
ハッシュ値
署名鍵で
暗号化
S2002
完全性情報
環境情報
特定情報
完全性情報
検証部2601
環境情報
特定情報
ハッシュ
関数
S2003
ハッシュ値
S2005
比較
ハッシュ値
検証鍵で
復号
S2004
完全性情報

[図46]

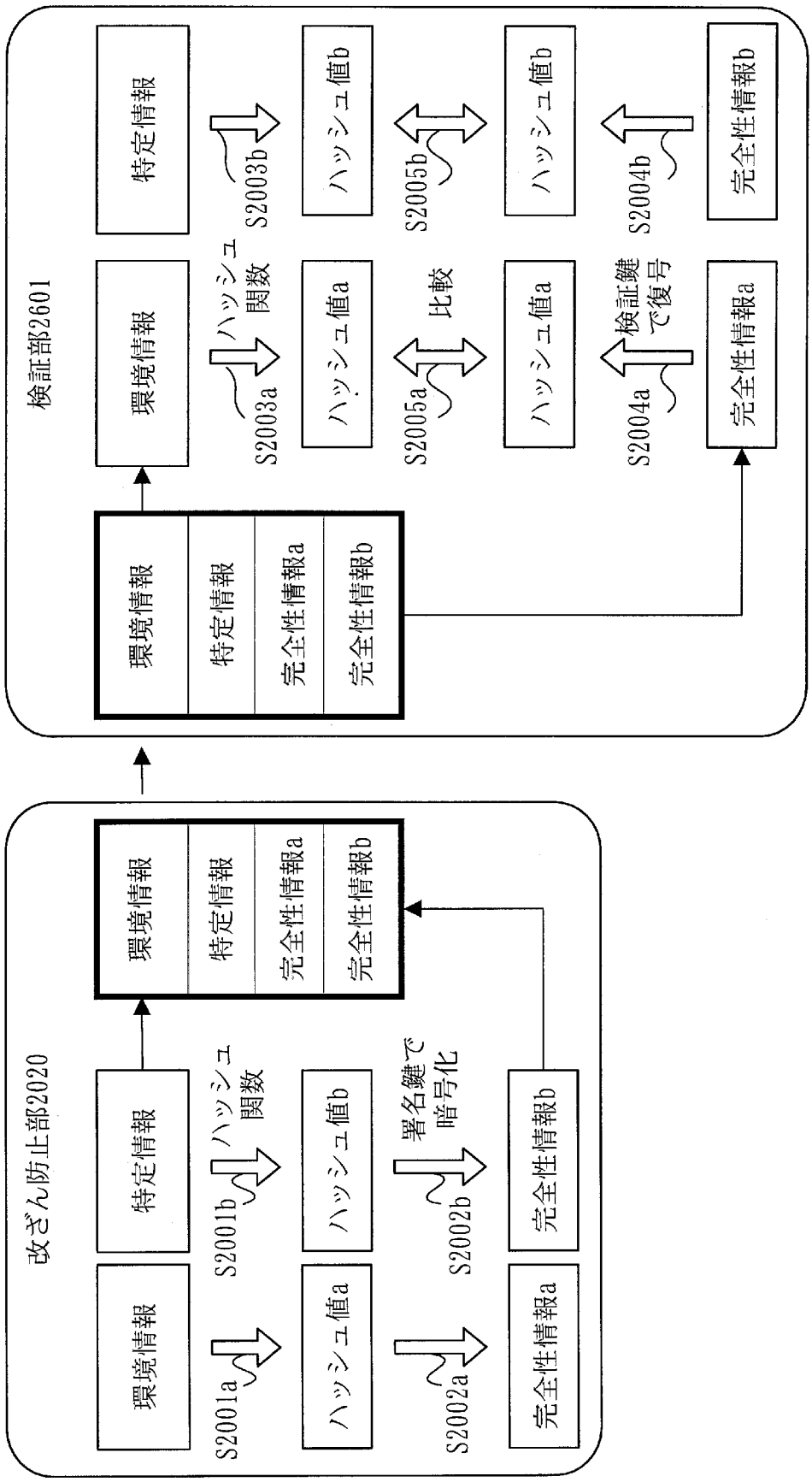
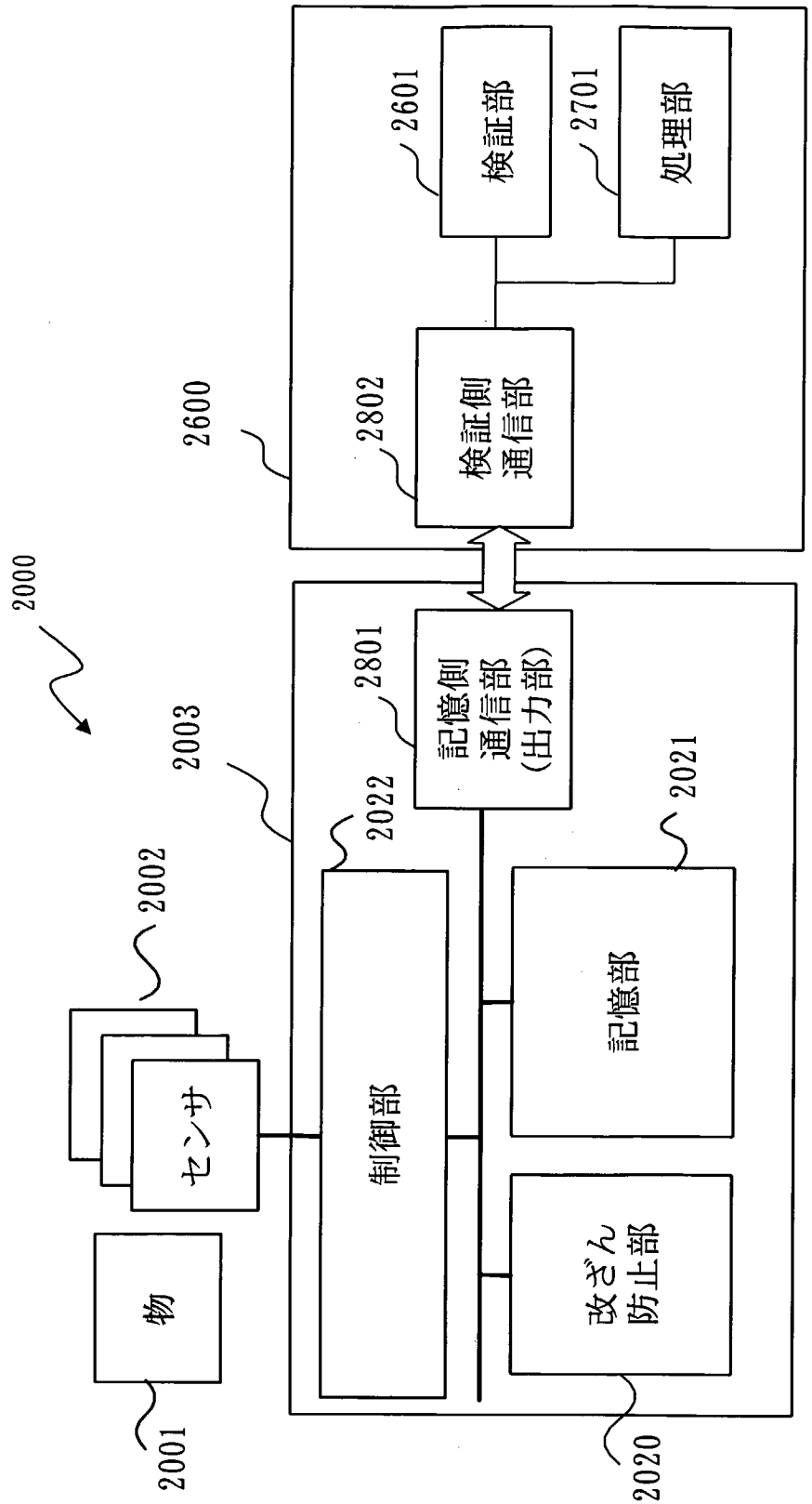
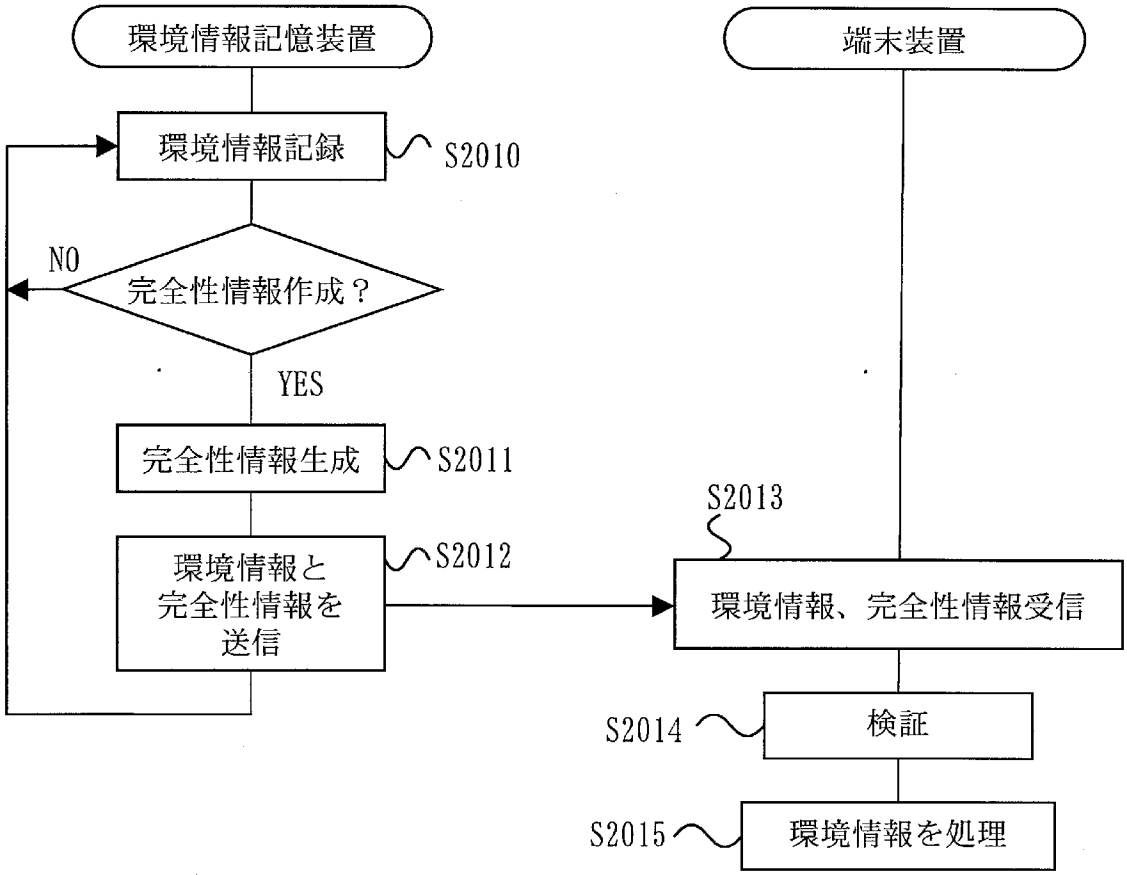

改ざん防止部2020
環境情報
特定情報
ハッシュ値a
ハッシュ値b
完全性情報a
完全性情報b
S2001a
S2001b
ハッシュ関数
S2002a
署名鍵で暗号化
S2002b
環境情報
特定情報
完全性情報a
完全性情報b
検証部2601
環境情報
特定情報
ハッシュ値a
ハッシュ値b
S2003a
ハッシュ関数
S2003b
S2004a
検証鍵で復号
S2004b
S2005a
比較
S2005b
完全性情報a
完全性情報b

図 47


2000
2001
物
2002
センサ
2003
制御部
2020
改ざん防止部
2021
記憶部
2022
2600
2601
検証部
2701
処理部
2801
記憶側通信部(出力部)
2802
検証側通信部

[図48]


環境情報記憶装置
端末装置
環境情報記録
S2010
NO
完全性情報作成？
YES
完全性情報生成
S2011
S2013
環境情報と
完全性情報を
送信
S2012
環境情報、完全性情報受信
S2014
検証
S2015
環境情報を処理

[図49]

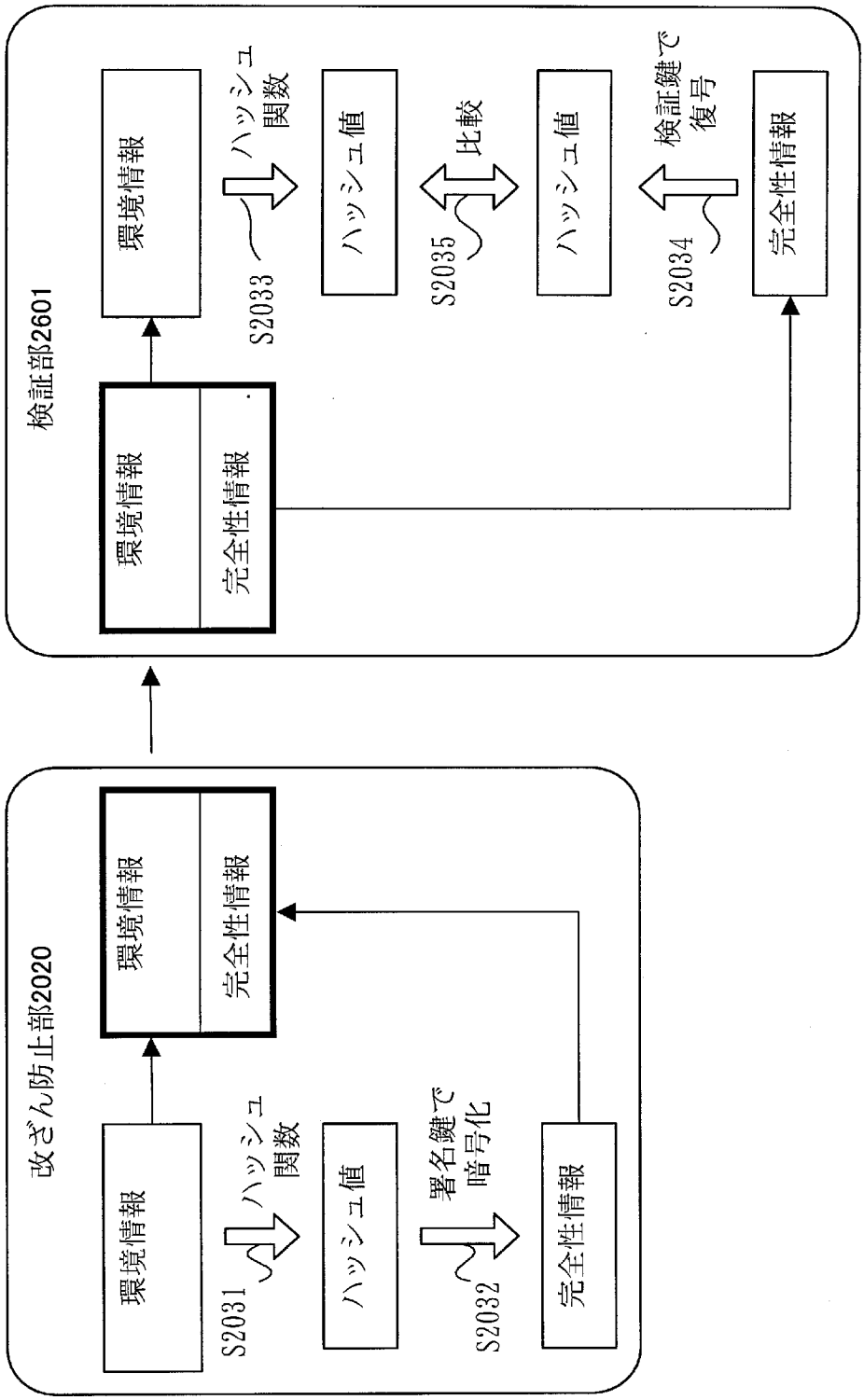

改ざん防止部2020
環境情報
S2031
ハッシュ関数
ハッシュ値
S2032
署名鍵で暗号化
完全性情報
環境情報
完全性情報
検証部2601
環境情報
S2033
ハッシュ関数
ハッシュ値
S2035
比較
ハッシュ値
S2034
検証鍵で復号
完全性情報
環境情報
完全性情報

図 50

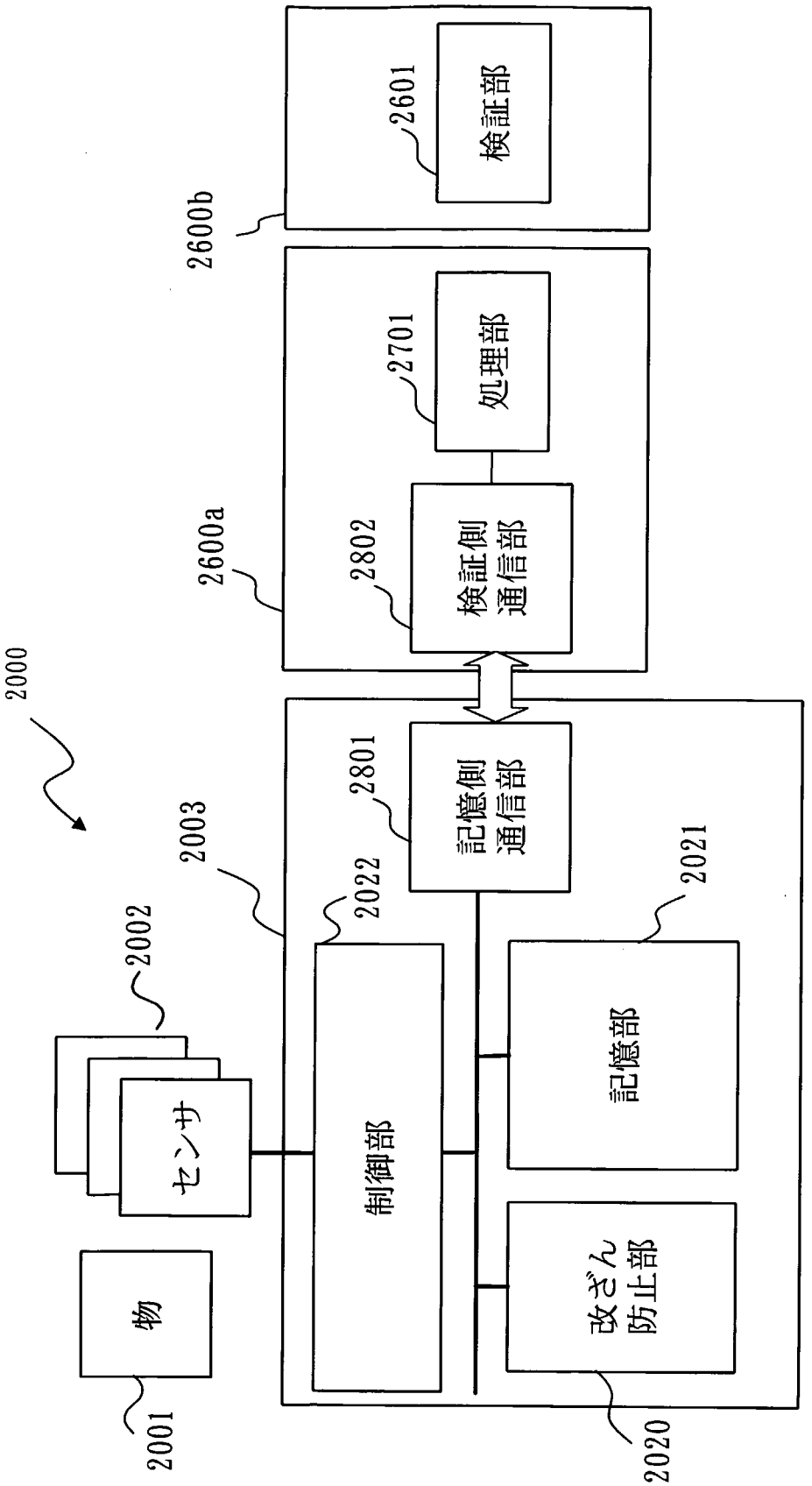

2000
2001
物
2002
センサ
2003
制御部
2020
改ざん防止部
2021
記憶部
2022
2801
記憶側通信部
2600a
2802
検証側通信部
2701
処理部
2600b
2601
検証部

図51

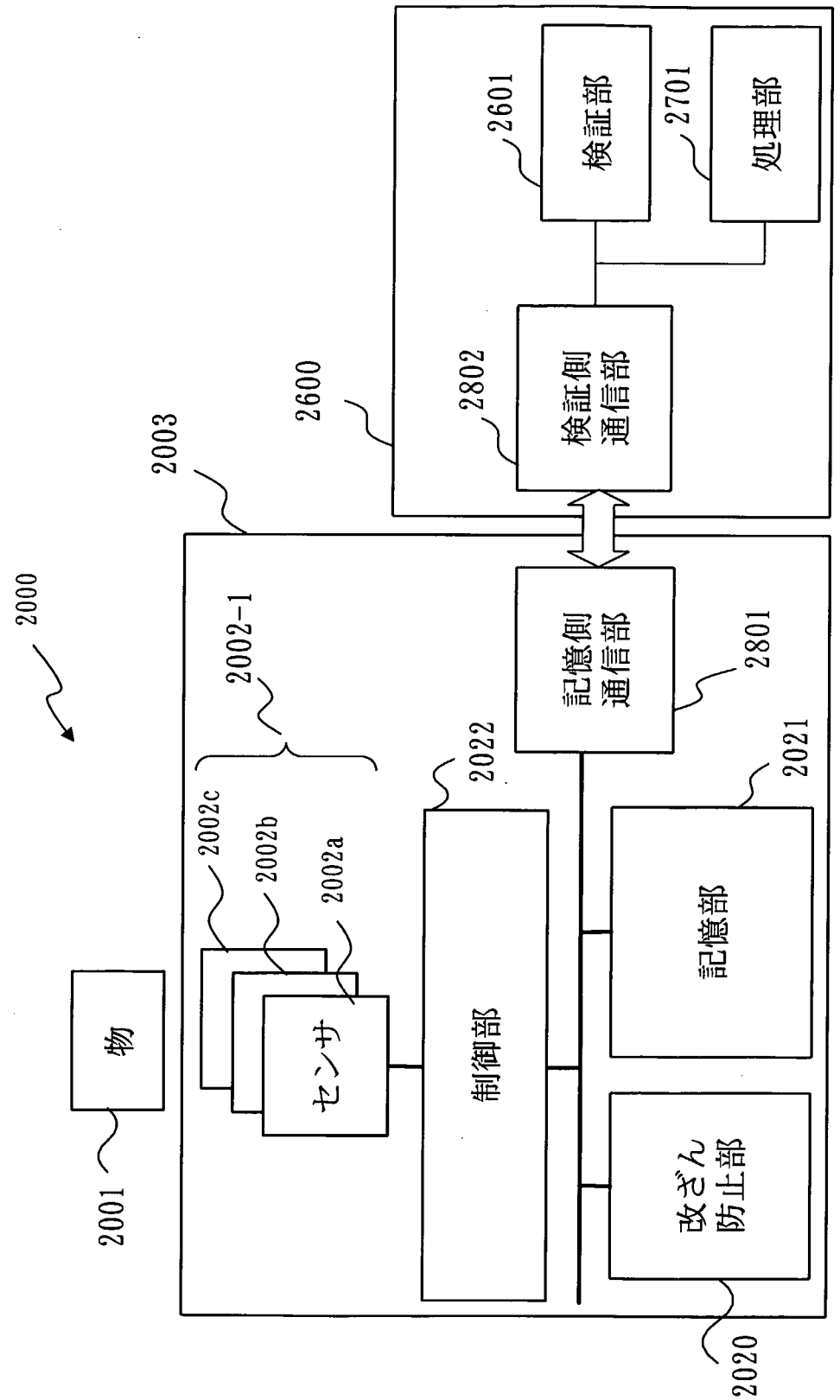
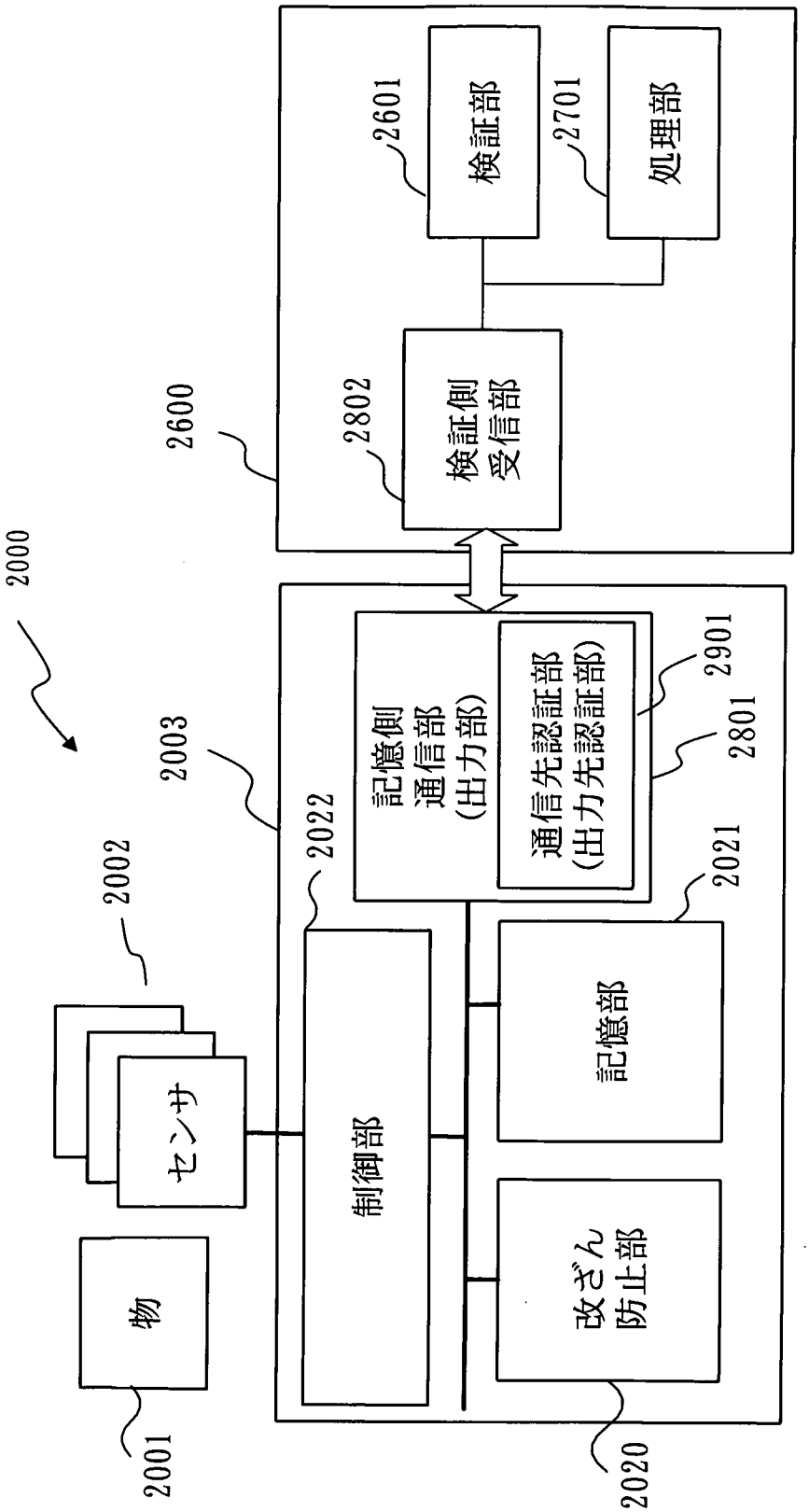

2000
2001
物
2002-1
2002a
2002b
2002c
センサ
2003
制御部
2020
改ざん防止部
2021
記憶部
2022
記憶側通信部
2801
2600
2601
検証部
2701
処理部
2802
検証側通信部

図 52


2000
2001
物
2002
センサ
2003
制御部
2020
改ざん防止部
2021
記憶部
2022
記憶側通信部(出力部)
通信先認証部(出力先認証部)
2801
2901
2600
2802
検証側受信部
2601
検証部
2701
処理部

[図53]

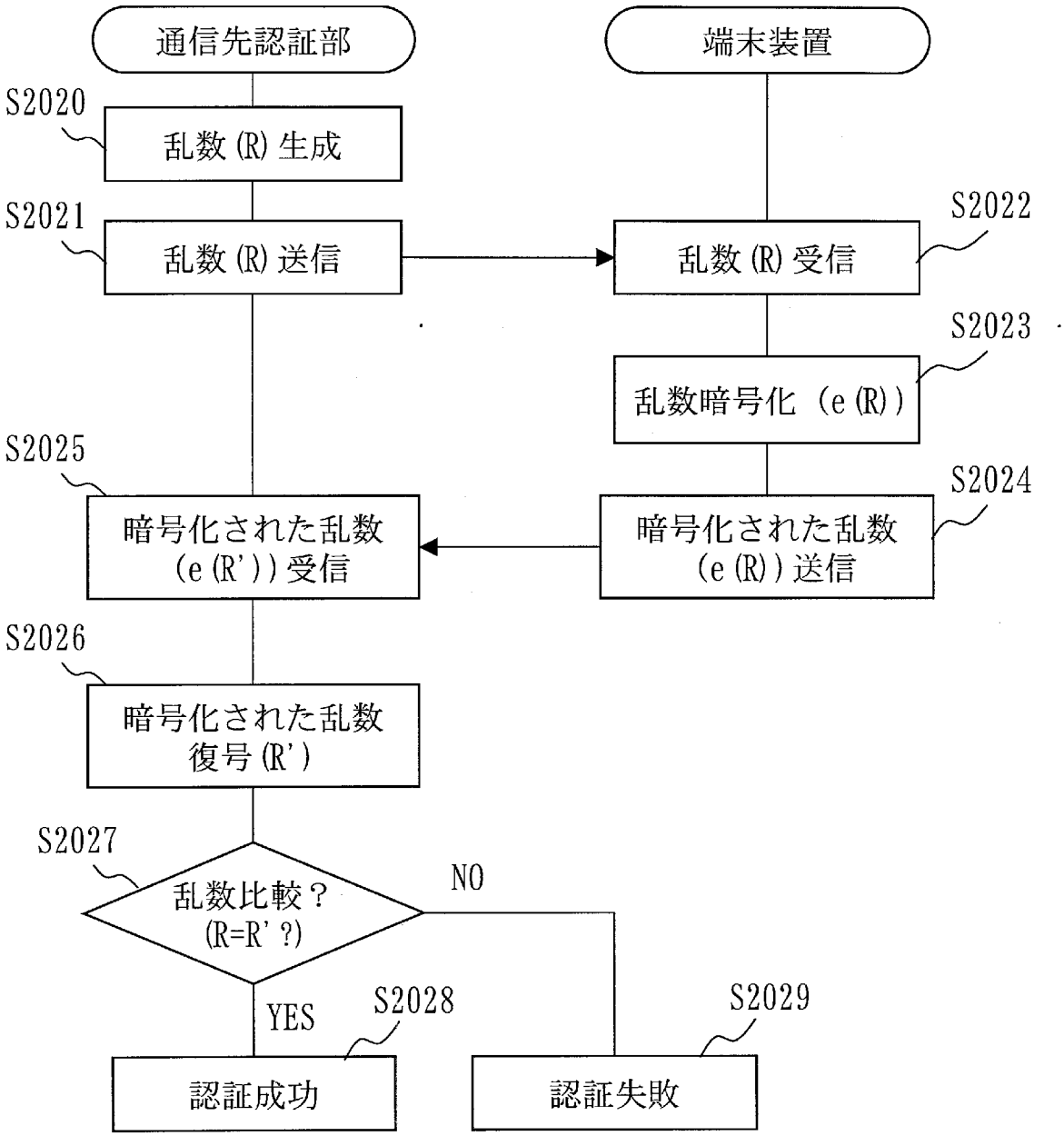
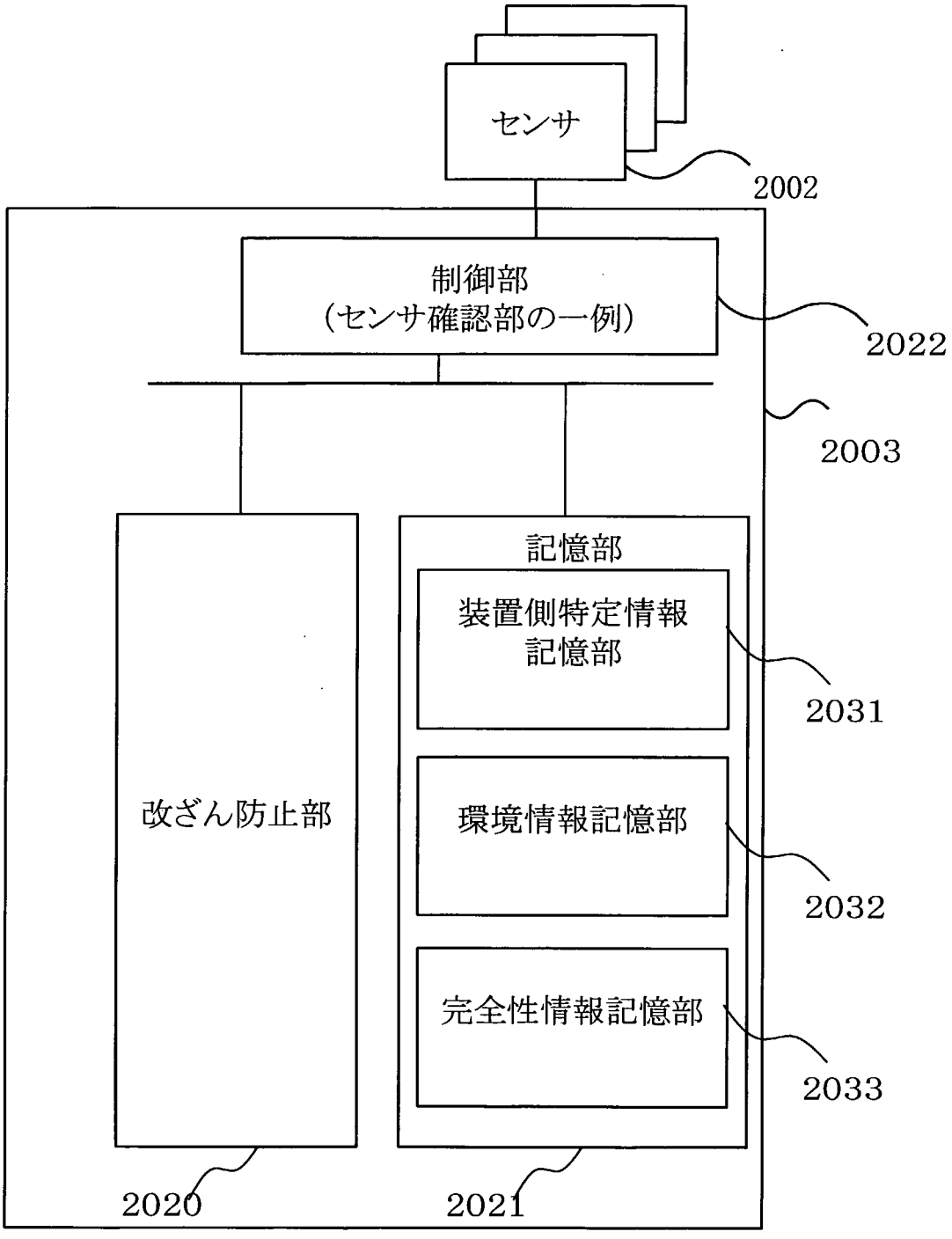

通信先認証部
端末装置
S2020
乱数(R)生成
S2021
乱数(R)送信
S2022
乱数(R)受信
S2023
乱数暗号化（e(R)）
S2024
暗号化された乱数
(e(R))送信
S2025
暗号化された乱数
(e(R'))受信
S2026
暗号化された乱数
復号(R')
S2027
乱数比較？
(R=R'?)
NO
YES
S2028
認証成功
S2029
認証失敗

図 54


センサ
2002
制御部
(センサ確認部の一例)
2022
2003
記憶部
装置側特定情報
記憶部
2031
改ざん防止部
環境情報記憶部
2032
完全性情報記憶部
2033
2020
2021

[図55]

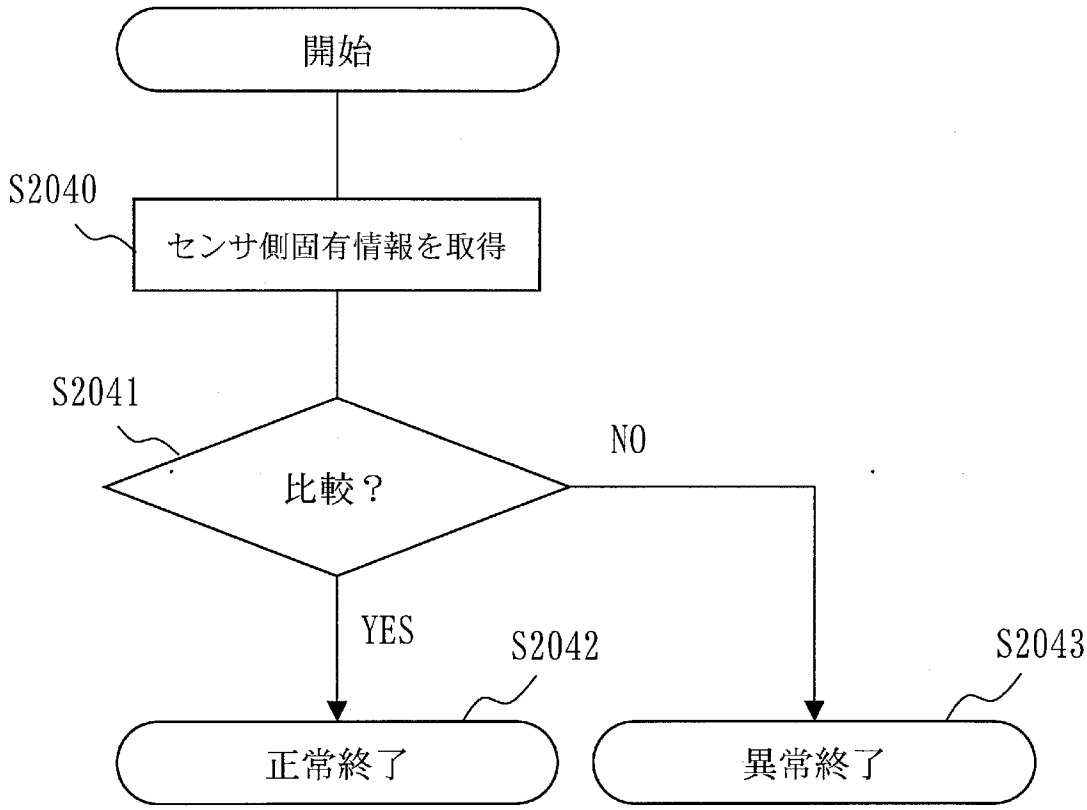


図56

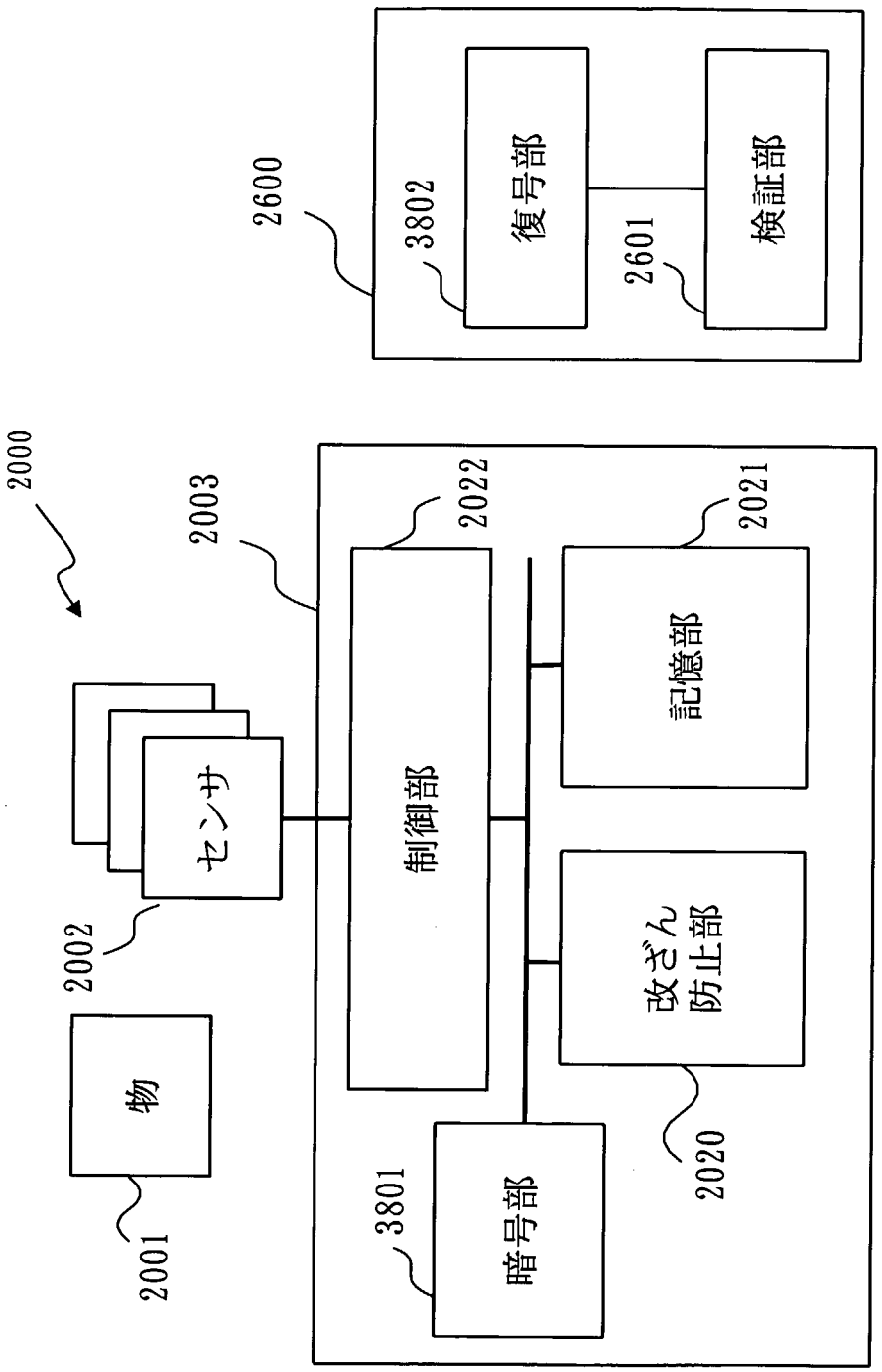

2600
3802
復号部
2601
検証部
2000
2003
2022
2021
制御部
記憶部
センサ
2002
改ざん防止部
物
2001
3801
暗号部
2020

図57

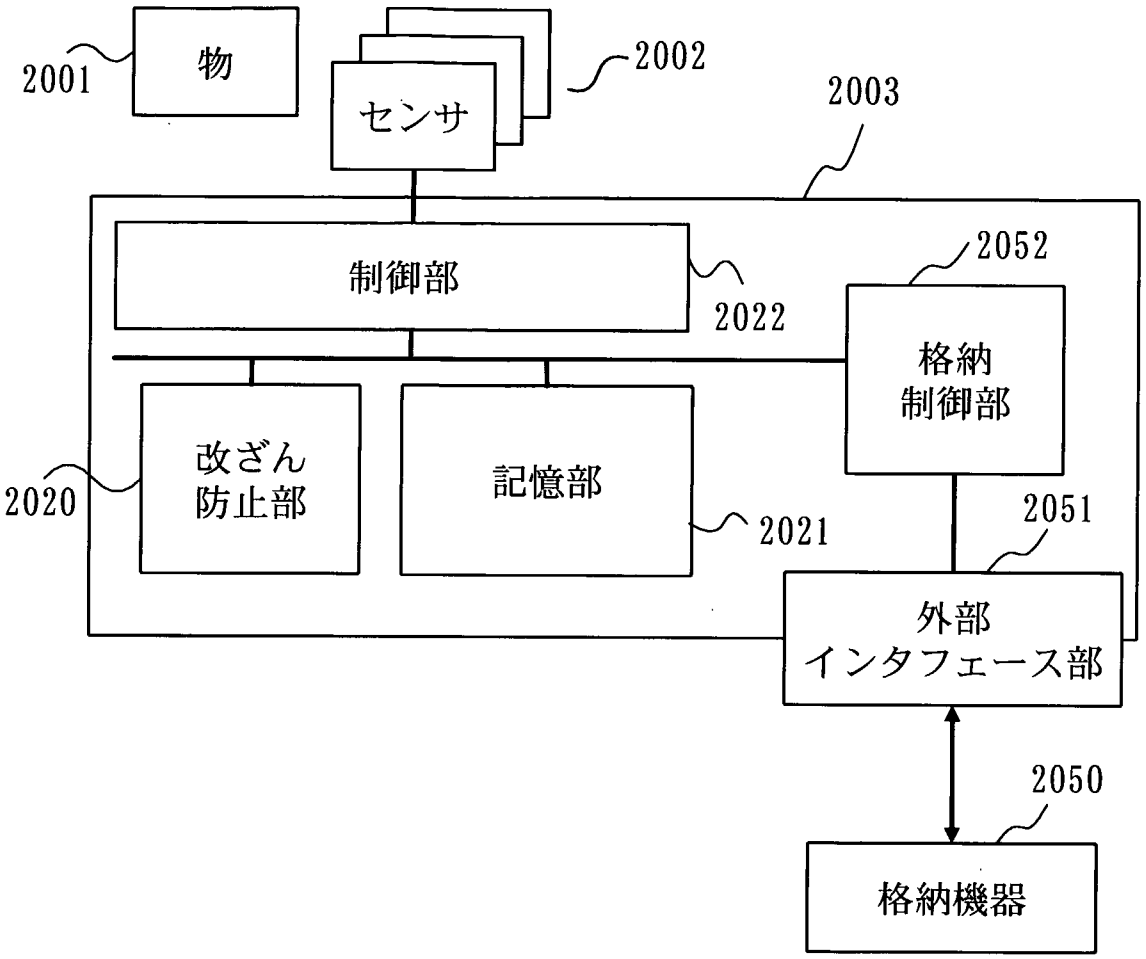

2001
物
センサ
2002
2003
制御部
2022
2052
格納
制御部
2020
改ざん
防止部
記憶部
2021
2051
外部
インタフェース部
2050
格納機器

図 58

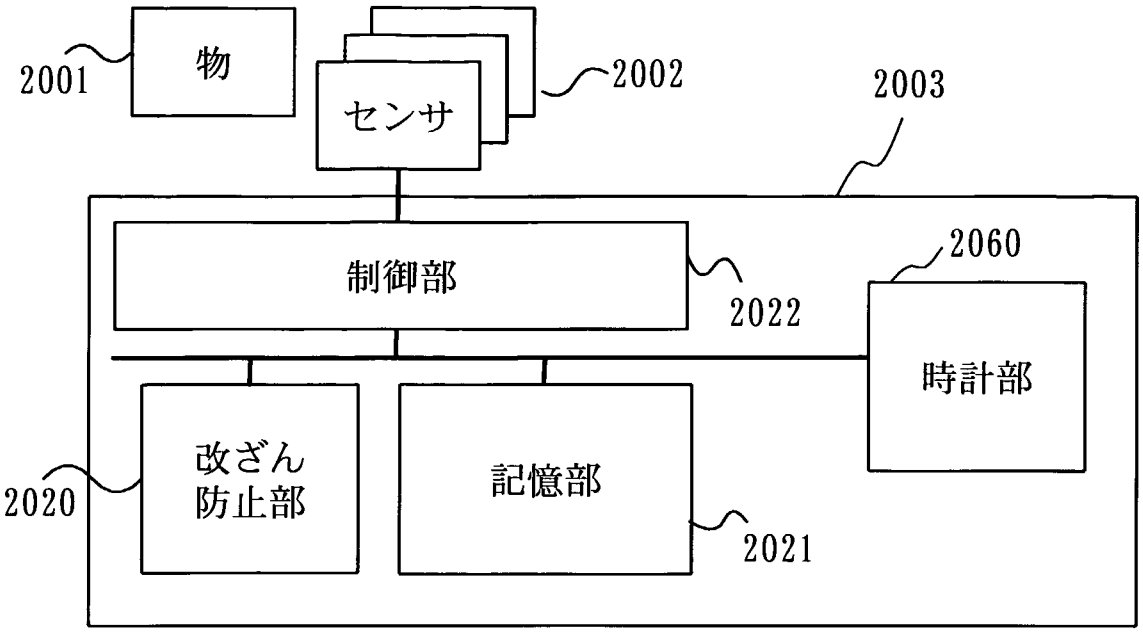
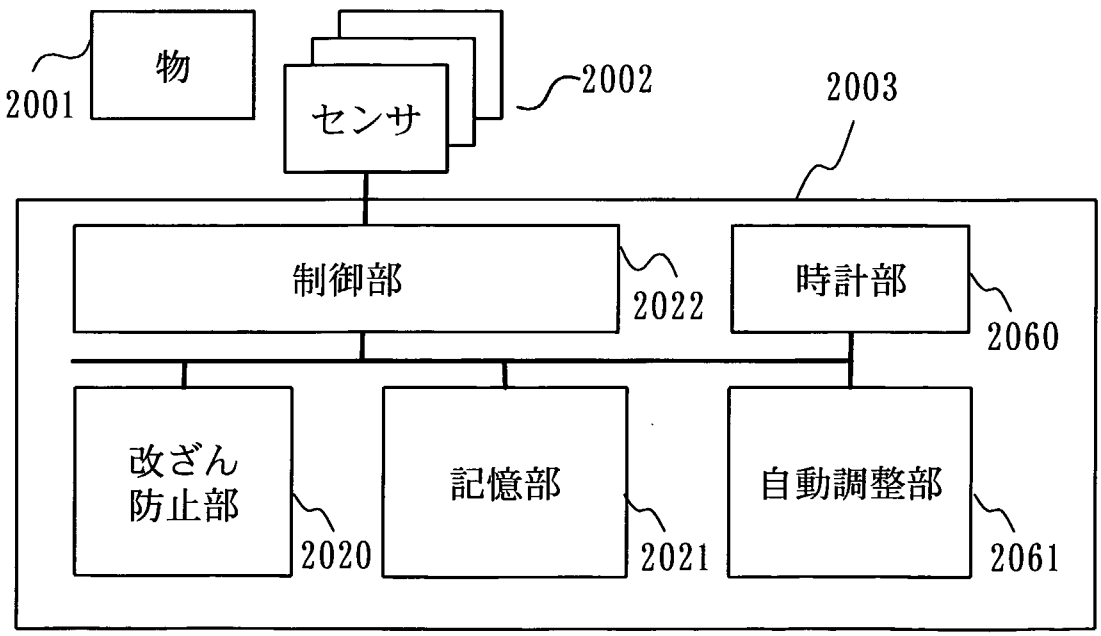
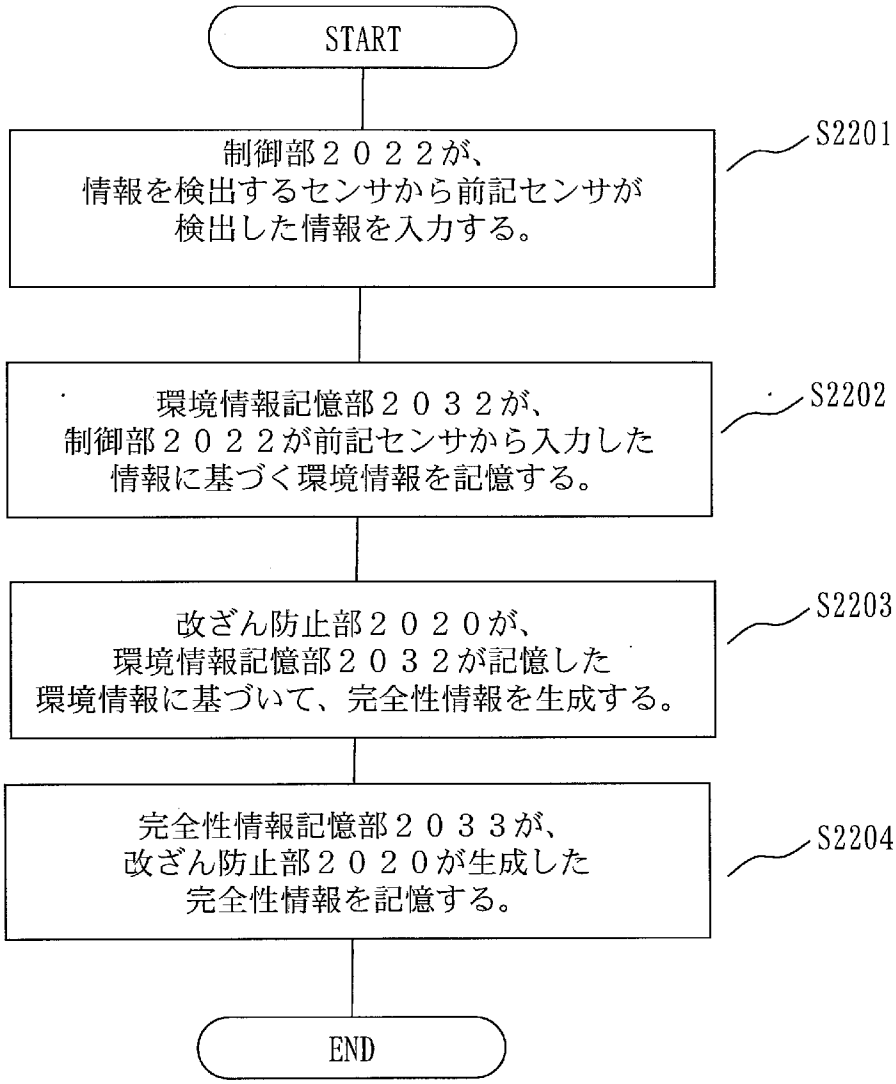

物
センサ
制御部
時計部
改ざん
防止部
記憶部
2001
2002
2003
2060
2022
2020
2021

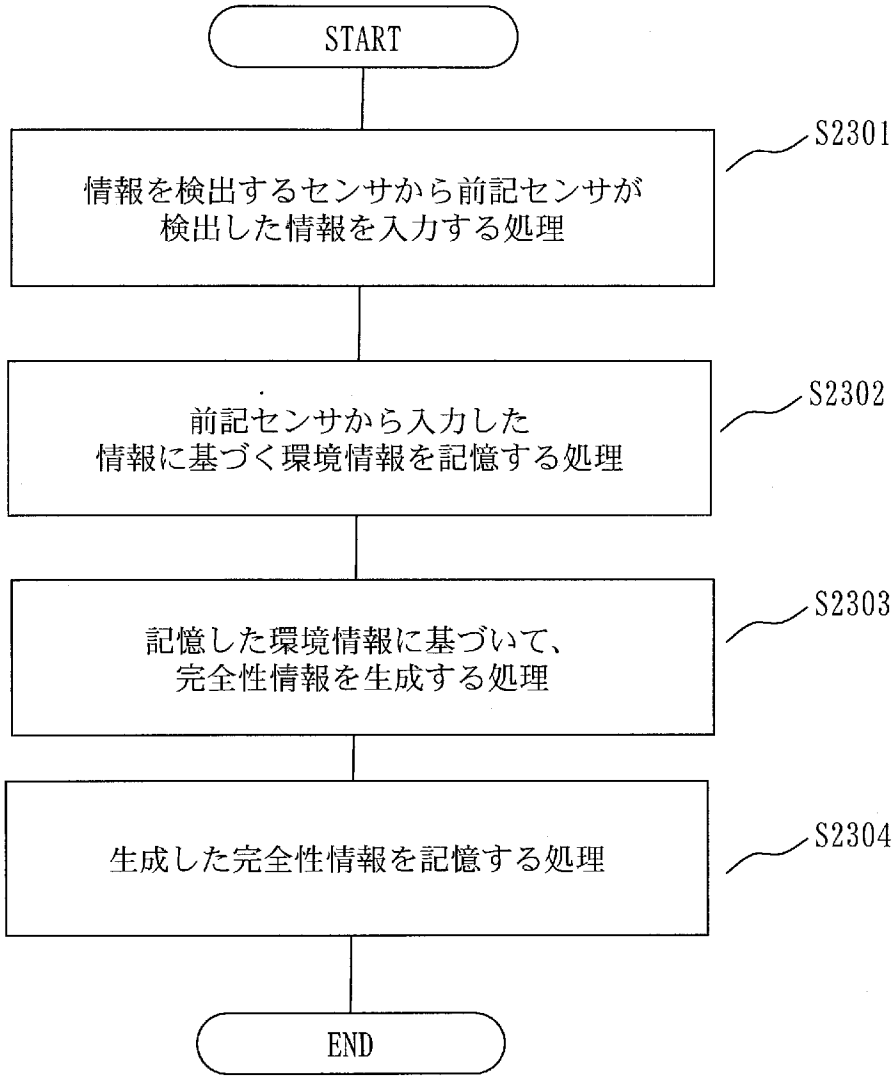
図 59


物
センサ
制御部
時計部
改ざん
防止部
記憶部
自動調整部
2001
2002
2003
2022
2060
2020
2021
2061

[図60]


START
制御部２０２２が、
情報を検出するセンサから前記センサが
検出した情報を入力する。
S2201
環境情報記憶部２０３２が、
制御部２０２２が前記センサから入力した
情報に基づく環境情報を記憶する。
S2202
改ざん防止部２０２０が、
環境情報記憶部２０３２が記憶した
環境情報に基づいて、完全性情報を生成する。
S2203
完全性情報記憶部２０３３が、
改ざん防止部２０２０が生成した
完全性情報を記憶する。
S2204
END

[図61]


START
情報を検出するセンサから前記センサが検出した情報を入力する処理
S2301
前記センサから入力した情報に基づく環境情報を記憶する処理
S2302
記憶した環境情報に基づいて、完全性情報を生成する処理
S2303
生成した完全性情報を記憶する処理
S2304
END

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2006/315427

A. CLASSIFICATION OF SUBJECT MATTER
G08G1/00(2006.01)i, *G06F3/06*(2006.01)i, *G06F21/24*(2006.01)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)
G08G1/00, G06F3/06, G06F21/24

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 1996-2006
Kokai Jitsuyo Shinan Koho 1971-2006 Toroku Jitsuyo Shinan Koho 1994-2006

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	JP 2003-168006 A (Hitachi, Ltd.), 13 June, 2003 (13.06.03), Par. Nos. [0029] to [0034], [0037], [0040], [0046], [0047], [0067], [0077], [0078]; Figs. 1, 8 (Family: none)	1-32
Y	JP 2003-22218 A (Robert Bosch GmbH), 24 January, 2003 (24.01.03), Par. Nos. [0035], [0036]; Fig. 2 & US 2003/0018905 A1 & DE 10126451 A1	1-32

☒ 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
21 September, 2006 (21.09.06)	03 October, 2006 (03.10.06)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2006/315427

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2001-255953 A (Bayerische Motoren Werke AG., Ernst Schmidt), 21 September, 2001 (21.09.01), Par. Nos. [0062] to [0068]; Fig. 7 & US 2002/0023223 A1 & EP 1127756 A2 & EP 1127756 A3 & DE 10008973 A1 & ES 2237500 T	1-32
Y	JP 9-102088 A (Honda Motor Co., Ltd.), 15 April, 1997 (15.04.97), Par. Nos. [0020], [0021], [0025]; Figs. 1 to 3 (Family: none)	3-9
A	JP 2004-338607 A (Denso Corp.), 02 December, 2004 (02.12.04), Full text (Family: none)	1-32
A	JP 2004-352128 A (Hitachi, Ltd.), 16 December, 2004 (16.12.04), Full text (Family: none)	1-32
A	JP 2003-21536 A (Yazaki Corp.), 24 January, 2003 (24.01.03), Full text (Family: none)	1-32

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２００６／３１５４２７

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　G08G1/00(2006.01)i, G06F3/06(2006.01)i, G06F21/24(2006.01)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.　G08G1/00, G06F3/06, G06F21/24

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	１９７１－２００６年
日本国実用新案登録公報	１９９６－２００６年
日本国登録実用新案公報	１９９４－２００６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	関連する請求の範囲の番号
Y	JP 2003-168006 A (株式会社日立製作所) 2003.06.13, 段落【0029】-【0034】, 【0037】, 【0040】, 【0046】, 【0047】, 【0067】, 【0077】, 【0078】, 図1,8 (ファミリーなし)	1-32
Y	JP 2003-22218 A (ローベルト　ボツシユ　ゲゼルシヤフト　ミツトベシユレンクテル　ハフツング) 2003.01.24, 段落【0035】, 【0036】, 図2 & US 2003/0018905 A1 & DE 10126451 A1	1-32
Y	JP 2001-255953 A (バイエリッシェ　モートーレン　ウエルケ　ア	1-32

☑　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 ２１．０９．２００６	国際調査報告の発送日 ０３．１０．２００６
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）　３Ｈ　３４２８ 村上　哲 電話番号　０３－３５８１－１１０１　内線　３３１６

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	関連する請求の範囲の番号
	クチエンゲゼルシャフト エルンスト　シュミット）2001.09.21, 段落【0062】-【0068】,図7 & US 2002/0023223 A1 & EP 1127756 A2 & EP 1127756 A3 & DE 10008973 A1 & ES 2237500 T	
Y	JP 9-102088 A（本田技研工業株式会社）1997.04.15, 段落【0020】, 【0021】, 【0025】,図1-3　（ファミリーなし）	3-9
A	JP 2004-338607 A（株式会社デンソー）2004.12.02, 全文　（ファミリーなし）	1-32
A	JP 2004-352128 A（株式会社日立製作所）2004.12.16, 全文　（ファミリーなし）	1-32
A	JP 2003-21536 A（矢崎総業株式会社）2003.01.24, 全文　（ファミリーなし）	1-32