(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2021年6月10日(10.06.2021)

WIPO | PCT

(10) 国際公開番号
WO 2021/111681 A1

(51) 国際特許分類:
G06F 11/07 (2006.01) *G05B 23/02* (2006.01)

(21) 国際出願番号： PCT/JP2020/032015

(22) 国際出願日： 2020年8月25日(25.08.2020)

(25) 国際出願の言語： 日本語

(26) 国際公開の言語： 日本語

(30) 優先権データ：
特願 2019-220231 2019年12月5日(05.12.2019) JP

(71) 出願人:パナソニックＩＰマネジメント株式会社(**PANASONIC INTELLECTUAL PROPERTY MANAGEMENT CO., LTD.**) [JP/JP]; 〒5406207 大阪府大阪市中央区城見２丁目１番６１号 Osaka (JP).

(72) 発明者: 伊藤 貴佳 (**ITO, Takayoshi**). 田村 健人 (**TAMURA, Kento**). 今本 吉治 (**IMAMOTO, Yoshiharu**). 鶴見 淳一 (**TSURUMI, Junichi**). 和田 紘幸 (**WADA, Hiroyuki**).

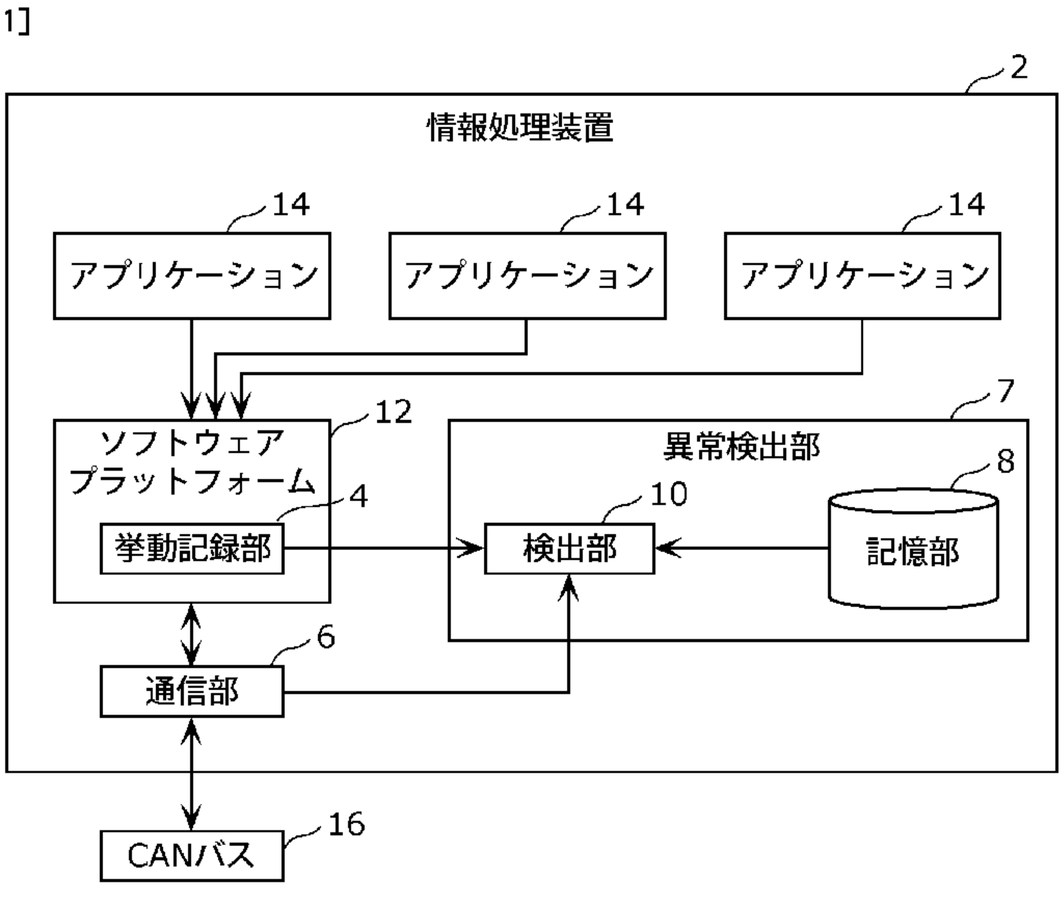
(74) 代理人: 新居 広守, 外 (**NII, Hiromori** et al.); 〒5320011 大阪府大阪市淀川区西中島５丁目３番１０号タナカ・イトーピア新大阪ビル６階新居国際特許事務所内 Osaka (JP).

(81) 指定国(表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT, JO, KE, KG, KH,

(54) **Title:** INFORMATION PROCESSING DEVICE, CONTROL METHOD, AND PROGRAM

(54) 発明の名称： 情報処理装置、制御方法及びプログラム

[図1]



2... INFORMATION PROCESSING DEVICE
4... BEHAVIOR RECORDING UNIT
6... COMMUNICATION UNIT
7... ABNORMALITY DETECTION UNIT
8... STORAGE UNIT
10... DETECTION UNIT
12... SOFTWARE PLATFORM
14... APPLICATION
16... CAN BUS

(57) **Abstract:** This information processing device (2) is provided with: a storage unit (8) which stores determination criteria information that indicates determination criteria on which determination on whether the behavior of an application (14) operating on an in-vehicle apparatus mounted in a vehicle is normal is based; and a detection unit (10) which acquires behavior log information that indicates a history of the behavior of the application (14) and detects an abnormality of the behavior of the application (14) on the basis of the acquired behavior log information and the determination criteria information stored in the storage unit (8).

(57) 要約：情報処理装置（２）は、車両に搭載された車載機器上で動作するアプリケーション（１４）の挙動が正常であるか否かの判断基準を示す判断基準情報を記憶する記憶部（８）と、アプリケーション（１４）の挙動の履歴を示す挙動ログ情報を取得し、取得した挙動ログ情報及び記憶部（８）に記憶された判断基準情報に基づいて、アプリケーション（１４）の挙動の異常を検出する検出部（１０）とを備える。

［続葉有］

WO 2021/111681 A1

KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

(84) 指定国(表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, RU, TJ, TM), ヨーロッパ (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

添付公開書類:

一　国際調査報告（条約第21条(3)）

明　細　書

発明の名称 ： 情報処理装置、制御方法及びプログラム

技術分野

[0001]　本開示は、情報処理装置、制御方法及びプログラムに関する。

背景技術

[0002]　特許文献１は、ボット等のコンピュータウイルスによる異常を検出する異常検出装置を開示する。特許文献１の異常検出装置では、プロセスによるファイルへのアクセス等をＬＳＭ（Ｌｉｎｕｘ（登録商標）　Ｓｅｃｕｒｉｔｙ　Ｍｏｄｕｌｅ）により監視し、例えばプロセスが本来アクセスすべきファイル以外のファイルにアクセスした場合に、コンピュータウイルスによる異常が発生したと判定する。

先行技術文献

特許文献

[0003] 特許文献1：特開２０１０－１８２０１９号公報

発明の概要

発明が解決しようとする課題

[0004]　近年、車両の加減速、操舵及び制動等の運転操作を自動で行う自動運転システムの開発が進められている。この自動運転システムでは、悪意のある第三者が、例えば車両に搭載されたＥＣＵ（Ｅｌｅｃｔｒｏｎｉｃ　Ｃｏｎｔｒｏｌ　Ｕｎｉｔ）に対して不正なＣＡＮ（Ｃｏｎｔｒｏｌｌｅｒ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）メッセージを送信することにより、車両が攻撃されるおそれがある。上述した特許文献１の異常検出装置では、このような車両への攻撃について考慮されておらず、車両におけるセキュリティ対策が十分とは言えないという課題が生じる。

[0005]　そこで、本開示は、モビリティにおけるセキュリティ対策を高めることができる情報処理装置、制御方法及びプログラムを提供する。

課題を解決するための手段

[0006] 本開示の一態様に係る情報処理装置は、モビリティに搭載されたモビリティネットワークに接続される情報処理装置であって、前記モビリティに搭載された機器上で動作するアプリケーションの挙動が正常であるか否かの判断基準を示す判断基準情報を記憶する記憶部と、前記アプリケーションの挙動を示す挙動情報を取得し、取得した前記挙動情報及び前記記憶部に記憶された前記判断基準情報に基づいて、前記アプリケーションの挙動の異常を検出する検出部と、を備える。

[0007] なお、これらの包括的又は具体的な態様は、システム、方法、集積回路、コンピュータプログラム又はコンピュータで読み取り可能なＣＤ－ＲＯＭ（Ｃｏｍｐａｃｔ　Ｄｉｓｃ－Ｒｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙ）等の記録媒体で実現されてもよく、システム、方法、集積回路、コンピュータプログラム及び記録媒体の任意な組み合わせで実現されてもよい。

発明の効果

[0008] 本開示の一態様に係る情報処理装置等によれば、モビリティにおけるセキュリティ対策を高めることができる。

図面の簡単な説明

[0009] [図1]図１は、実施の形態１に係る情報処理装置の構成を示すブロック図である。

[図2]図２は、実施の形態１に係る挙動ログ情報の一例を示す図である。

[図3]図３は、実施の形態１に係る状態ログ情報の一例を示す図である。

[図4A]図４Ａは、実施の形態１に係る状態ログ情報の他の例を示す図である。

[図4B]図４Ｂは、実施の形態１に係る状態ログ情報の他の例を示す図である。

[図5]図５は、実施の形態１に係る情報処理装置の検出部の動作の流れを示すフローチャートである。

[図6]図６は、実施の形態１に係る情報処理装置の検出部により取得される挙動ログ情報及び状態ログ情報の一例を示す図である。

[図7]図７は、図５のフローチャートのステップＳ１０４の処理を説明するための概念図である。

[図8]図８は、実施の形態２に係る情報処理装置の構成を示すブロック図である。

[図9]図９は、実施の形態２に係る判断基準情報の一例を示す図である。

[図10]図１０は、実施の形態２に係る情報処理装置の検出部の動作の流れを示すフローチャートである。

[図11]図１１は、実施の形態２に係る情報処理装置の検出部により取得される挙動ログ情報及び状態ログ情報、並びに、記憶部に記憶された判断基準情報の一例を示す図である。

[図12]図１２は、実施の形態３に係る情報処理装置の構成を示すブロック図である。

[図13]図１３は、実施の形態３に係る情報処理装置の検出部の動作の流れを示すフローチャートである。

[図14]図１４は、実施の形態４に係る情報処理装置の構成を示すブロック図である。

[図15]図１５は、実施の形態５に係る情報処理装置の構成を示すブロック図である。

発明を実施するための形態

[0010] 本開示の一態様に係る情報処理装置は、モビリティに搭載されたモビリティネットワークに接続される情報処理装置であって、前記モビリティに搭載された機器上で動作するアプリケーションの挙動が正常であるか否かの判断基準を示す判断基準情報を記憶する記憶部と、前記アプリケーションの挙動を示す挙動情報を取得し、取得した前記挙動情報及び前記記憶部に記憶された前記判断基準情報に基づいて、前記アプリケーションの挙動の異常を検出する検出部と、を備える。

[0011] 本態様によれば、検出部は、アプリケーションの挙動を示す挙動情報を取得し、取得した挙動情報及び記憶部に記憶された判断基準情報に基づいて、

アプリケーションの挙動の異常を検出する。これにより、モビリティへの攻撃に起因するアプリケーションの挙動の異常を確実に検出することができ、モビリティにおけるセキュリティ対策を高めることができる。

[0012] 例えば、前記検出部は、前記モビリティネットワークから取得した前記モビリティの状態を示す状態情報と、前記挙動情報と、前記記憶部に記憶された前記判断基準情報とに基づいて、前記アプリケーションの挙動の異常を検出するように構成してもよい。

[0013] 本態様によれば、検出部は、挙動情報に加えて状態情報をも考慮して、アプリケーションの挙動の異常を検出する。これにより、モビリティへの攻撃に起因するアプリケーションの挙動の異常をより一層確実に検出することができ、モビリティにおけるセキュリティ対策をより一層高めることができる。

[0014] 例えば、前記判断基準情報は、前記アプリケーションの挙動の異常を検出するための判定モデルとして、前記アプリケーションの挙動及び前記モビリティの状態の少なくとも一方に関するルールベースモデル又は機械学習モデルを含み、前記検出部は、前記挙動情報及び前記状態情報に前記判定モデルを適用することにより、前記アプリケーションの挙動の異常を検出するように構成してもよい。

[0015] 本態様によれば、挙動情報及び状態情報に対して、ルールベースモデル又は機械学習モデルである判定モデルを適用することにより、アプリケーションの挙動の異常を精度良く検出することができる。

[0016] 例えば、前記判断基準情報は、前記アプリケーションの正常な挙動の履歴を示す正常挙動ログ情報、及び、前記モビリティの正常な状態の履歴を示す正常状態ログ情報を含み、前記検出部は、取得した前記挙動情報の履歴及び前記状態情報の履歴と、前記判断基準情報に含まれる前記正常挙動ログ情報及び前記正常状態ログ情報とをそれぞれ比較することにより、前記アプリケーションの挙動の異常を検出するように構成してもよい。

[0017] 本態様によれば、判定基準情報により、モビリティの状態毎にアプリケー

ションの正常な挙動を定義することが可能となる。その結果、検出部は、取得した挙動情報の履歴及び状態情報の履歴と、判断基準情報に含まれる正常挙動ログ情報及び正常状態ログ情報とをそれぞれ比較することにより、アプリケーションの挙動の異常を精度良く検出することができる。

[0018] 例えば、前記判断基準情報は、前記アプリケーションの異常な挙動の履歴を示す異常挙動ログ情報、及び、前記モビリティの異常な状態の履歴を示す異常状態ログ情報を含み、前記検出部は、取得した前記挙動情報の履歴及び前記状態情報の履歴と、前記判断基準情報に含まれる前記異常挙動ログ情報及び前記異常状態ログ情報とをそれぞれ比較することにより、前記アプリケーションの挙動の異常を検出するように構成してもよい。

[0019] 本態様によれば、判定基準情報により、モビリティの状態毎にアプリケーションの異常な挙動を定義することが可能となる。その結果、検出部は、取得した挙動情報の履歴及び状態情報の履歴と、判断基準情報に含まれる異常挙動ログ情報及び異常状態ログ情報とをそれぞれ比較することにより、アプリケーションの挙動の異常を精度良く検出することができる。

[0020] 例えば、前記判断基準情報は、機械学習により予め生成された、前記アプリケーションの挙動の正常らしさを判定するための判定モデルを含み、前記検出部は、前記判定モデルを用いて、取得した前記挙動情報の履歴から第１の特徴量を算出し、且つ、前記状態情報の履歴から第２の特徴量を算出し、算出した前記第１の特徴量及び前記第２の特徴量から前記アプリケーションの挙動の正常らしさを示す評価値を算出し、前記評価値の尤度と閾値とを比較することにより、前記アプリケーションの挙動の異常を検出するように構成してもよい。

[0021] 本態様によれば、検出部は、判定基準情報に含まれる機械学習の判定モデルを用いて、アプリケーションの挙動の異常を精度良く検出することができる。

[0022] 例えば、前記情報処理装置は、さらに、前記状態情報に基づいて、前記モビリティの状態を推論する推論部を備え、前記検出部は、前記推論部の推論

結果を加味して、前記アプリケーションの挙動の異常を検出するように構成してもよい。

[0023] 本態様によれば、検出部は、推論部の推論結果を加味して、アプリケーションの挙動の異常をより一層精度良く検出することができる。

[0024] 例えば、前記情報処理装置は、さらに、前記検出部が前記アプリケーションの挙動の異常を検出した際に、外部にその旨を通知する通知部を備えるように構成してもよい。

[0025] 本態様によれば、通知部は、アプリケーションの挙動の異常を外部に通知するので、例えばアプリケーションを強制的に停止するなどの処置を迅速に行うことができる。

[0026] 本開示の一態様に係る制御方法は、モビリティに搭載されたモビリティネットワークに接続される情報処理装置における制御方法であって、前記モビリティに搭載された機器上で動作するアプリケーションの挙動を示す挙動情報を取得するステップと、取得した前記挙動情報、及び、前記アプリケーションの挙動が正常であるか否かの判断基準を示し且つ記憶部に予め記憶された判断基準情報に基づいて、前記アプリケーションの挙動の異常を検出するステップと、を含む。

[0027] 本態様によれば、アプリケーションの挙動の履歴を示す挙動情報を取得し、取得した挙動情報及び記憶部に記憶された判断基準情報に基づいて、アプリケーションの挙動の異常を検出する。これにより、モビリティへの攻撃に起因するアプリケーションの挙動の異常を確実に検出することができ、モビリティにおけるセキュリティ対策を高めることができる。

[0028] 本開示の一態様に係るプログラムは、上述した制御方法をコンピュータに実行させる。

[0029] なお、これらの包括的又は具体的な態様は、システム、方法、集積回路、コンピュータプログラム又はコンピュータで読み取り可能なＣＤ－ＲＯＭ等の記録媒体で実現されてもよく、システム、方法、集積回路、コンピュータプログラム又は記録媒体の任意な組み合わせで実現されてもよい。

[0030] 以下、実施の形態について、図面を参照しながら具体的に説明する。

[0031] なお、以下で説明する実施の形態は、いずれも包括的又は具体的な例を示すものである。以下の実施の形態で示される数値、形状、材料、構成要素、構成要素の配置位置及び接続形態、ステップ、ステップの順序等は、一例であり、本開示を限定する主旨ではない。また、以下の実施の形態における構成要素のうち、最上位概念を示す独立請求項に記載されていない構成要素については、任意の構成要素として説明される。

[0032] （実施の形態１）

［１．情報処理装置の構成］

まず、図１～図４Ｂを参照しながら、実施の形態１に係る情報処理装置２の構成について説明する。図１は、実施の形態１に係る情報処理装置２の構成を示すブロック図である。図２は、実施の形態１に係る挙動ログ情報の一例を示す図である。図３は、実施の形態１に係る状態ログ情報の一例を示す図である。図４Ａ及び図４Ｂは、実施の形態１に係る状態ログ情報の他の例を示す図である。

[0033] 本実施の形態の情報処理装置２は、例えば自動車等の車両（モビリティの一例）に搭載されている。車両には、当該車両の加減速、操舵及び制動等の運転操作を自動で行うように制御するための自動運転システムが搭載されている。

[0034] 図１に示すように、情報処理装置２は、挙動記録部４と、通信部６と、異常検出部７とを備えている。

[0035] 挙動記録部４は、ソフトウェアプラットフォーム１２上で動作する複数のアプリケーション１４の各々の挙動（振る舞い）の履歴を示す挙動ログ情報を記録する。なお、挙動ログ情報は、アプリケーションの挙動を示す挙動情報の履歴の一例である。挙動記録部４は、例えばプロセスがＯＳ（Ｏｐｅｒａｔｉｎｇ　Ｓｙｓｔｅｍ）に対して発行するシステムコール処理をフックすることにより、挙動ログ情報を収集し記録する。挙動記録部４は、記録した挙動ログ情報を検出部１０に出力する。

[0036] なお、アプリケーション１４は、例えば車両の車載機器（機器の一例）上で動作するアプリケーションプログラムである。具体的には、アプリケーション１４は、例えば、ａ）動画を配信するための動画配信アプリケーション、ｂ）バックグラウンドで動作し、ユーザに対して広告を提示するための広告配信アプリケーション、ｃ）車両のトランクを宅配ボックスとして使用するための宅配ボックスアプリケーション、ｄ）カーシェアサービスを利用するためのカーシェアアプリケーション、ｅ）ライドシェアサービスを利用するためのライドシェアアプリケーション、及び、ｆ）先進運転者支援システム（ＡＤＡＳ：Ａｄｖａｎｃｅｄ Ｄｒｉｖｅｒ Ａｓｓｉｓｔａｎｃｅ Ｓｙｓｔｅｍ）を実行するための自動運転アプリケーション等である。

[0037] ソフトウェアプラットフォーム１２は、例えばハイパーバイザー上で動作する仮想マシンであり、モビリティサービスプラットフォームとして機能する。なお、ハイパーバイザー上で動作する仮想マシンとしては、上述したモビリティサービスプラットフォーム用の仮想マシンの他に、例えばＡＤＡＳ用の仮想マシン等が存在する。

[0038] ここで、図２を参照しながら、挙動記録部４により記録される挙動ログ情報の一例について説明する。図２に示す例では、挙動ログ情報は、ａ）タイムスタンプ、ｂ）プロセス名、ｃ）プロセスＩＤ（Ｉｄｅｎｔｉｆｉｃａｔｉｏｎ）、ｄ）フックポインタ名称、ｅ）フックポインタ属性１、及び、ｆ）フックポインタ属性２等を含んでいる。タイムスタンプは、挙動ログ情報が記録された時刻を示す情報である。プロセス名及びプロセスＩＤは、ＯＳに対してシステムコール処理を発行したプロセスを示す情報である。フックポインタ名称及びフックポインタ属性は、プロセスがＯＳに対して発行したシステムコール処理を示す情報である。

[0039] 図１に戻り、通信部６は、ＣＡＮバス１６（モビリティネットワークの一例）に接続されており、ＣＡＮバス１６から車両の状態の履歴を示す状態ログ情報を受信する。なお、状態ログ情報は、車両の状態を示す状態情報の履歴の一例である。通信部６は、受信した状態ログ情報を検出部１０に出力す

る。ＣＡＮバス１６は、ＣＡＮプロトコルに従ったＣＡＮメッセージを通信するための車載ネットワークであり、車両に搭載されている。

[0040] ここで、図３を参照しながら、通信部６により受信される状態ログ情報の一例について説明する。図３に示す例では、状態ログ情報は、ａ）タイムスタンプ、ｂ）車速、ｃ）加速度、及び、ｄ）操舵角等を含んでいる。タイムスタンプは、状態ログ情報が記録された時刻を示す情報である。車速は、車両の速度を示す情報である。加速度は、車両の加速度を示す情報である。操舵角は、車両のステアリングホイールの操舵角を示す情報である。なお、車速、加速度及び操舵角等は、車両に搭載された各種センサにより取得される。

[0041] 状態ログ情報は、上述した例の他に、例えば図４Ａに示すように、ａ）タイムスタンプ、ｂ）通信部名称、ｃ）通信部属性１、ｄ）通信部属性２、及び、ｅ）通信部属性３等を含んでいてもよい。あるいは、状態ログ情報は、例えば図４Ｂに示すように、ａ）タイムスタンプ、ｂ）ＩＤフィールド、及び、ｃ）データフィールド等を含んでいてもよい。

[0042] 図１に戻り、異常検出部７は、記憶部８と、検出部１０とを備えている。記憶部８は、アプリケーション１４の挙動が正常であるか否かの判断基準を示す判断基準情報を予め記憶している。本実施の形態では、判断基準情報は、機械学習により予め生成された、アプリケーション１４の挙動の正常らしさを判定するための機械学習モデルである判定モデルを含んでいる。なお、本実施の形態では、個々のアプリケーション１４毎に正常な挙動を定義（学習）するようにしたが、これに限定されず、関連する複数のアプリケーション１４を含むアプリケーション群毎に、又は、情報処理装置２を含むシステム単位で、正常な挙動を定義するようにしてもよい。

[0043] 検出部１０は、挙動記録部４からの挙動ログ情報と、通信部６からの状態ログ情報とを取得する。検出部１０は、取得した挙動ログ情報及び状態ログ情報、並びに、記憶部８に記憶された判断基準情報に基づいて、アプリケーション１４の挙動の異常を検出する。具体的には、検出部１０は、判断基準

情報に含まれる判定モデルを用いて、取得した挙動ログ情報の第１の特徴量及び状態ログ情報の第２の特徴量を算出する。検出部１０は、算出した第１の特徴量及び第２の特徴量からアプリケーション１４の挙動の正常らしさを示す評価値を算出し、評価値の尤度と閾値とを比較することにより、アプリケーション１４の挙動の異常を検出する。

[0044] ［１－２．検出部の動作］

次に、図５～図７を参照しながら、検出部１０の動作について説明する。図５は、実施の形態１に係る情報処理装置２の検出部１０の動作の流れを示すフローチャートである。図６は、実施の形態１に係る情報処理装置２の検出部１０により取得される挙動ログ情報及び状態ログ情報の一例を示す図である。図７は、図５のフローチャートのステップＳ１０４の処理を説明するための概念図である。

[0045] 以下、アプリケーション１４が動画配信アプリケーションであり、且つ、車両が高速道路を約８０ｋｍ／ｈで走行中に、悪意のある第三者がアプリケーション１４の脆弱性を突き、アプリケーション１４のプロセス制御を不正に乗っ取る（いわゆる、ハッキング）場合について説明する。この場合、不正に乗っ取られたアプリケーション１４は、通信部６に対して、緊急ブレーキを行うＣＡＮメッセージを送信するように命令するためのＡＰＩ（Ａｐｐｌｉｃａｔｉｏｎ　Ｐｒｏｇｒａｍｍｉｎｇ　Ｉｎｔｅｒｆａｃｅ）（以下、「緊急ブレーキＡＰＩ」という）を発行する。これにより、車両が高速道路を走行中に、緊急ブレーキが意図せず発動するおそれがある。前提として、緊急ブレーキＡＰＩは、低速走行中の緊急時のみに発行されるものとする。

[0046] 図５に示すように、検出部１０は、挙動記録部４からの挙動ログ情報、及び、通信部６からの状態ログ情報を取得する（Ｓ１０１）。ここで、検出部１０は、例えば図６に示すような挙動ログ情報及び状態ログ情報を、０．１ｓｅｃ毎に取得する。図６に示す例では、挙動ログ情報は、ａ）タイムスタンプ、ｂ）フックポイントＡ発現数、ｃ）フックポイントＢ発現数、ｄ）フ

ックポインタＣ発現数、ｅ）フックポインタＤ発現数、ｆ）通信メッセージＡ、及び、ｇ）通信メッセージＢを含んでいる。また、状態ログ情報は、ａ）タイムスタンプ、ｂ）車速、ｃ）加速度、及び、ｄ）操舵角を含んでいる。

[0047] 検出部１０は、記憶部８に記憶された判断基準情報に含まれる判定モデルを用いて、取得した挙動ログ情報の第１の特徴量及び状態ログ情報の第２の特徴量を算出する（Ｓ１０２）。検出部１０は、算出した第１の特徴量及び第２の特徴量からアプリケーション１４の挙動の正常らしさを示す評価値を算出する（Ｓ１０３）。

[0048] 検出部１０は、評価値（正常らしさ）の尤度と閾値とを比較することにより（Ｓ１０４）、アプリケーション１４の挙動が異常であるか否かを判定する。なお、検出部１０は、いわゆるタイムドリブン方式により、例えば０．１ｓｅｃ毎にアプリケーション１４の挙動が異常であるか否かを判定する。

[0049] 評価値の尤度が閾値を下回る場合には（Ｓ１０４でＹＥＳ）、検出部１０は、アプリケーション１４の挙動が異常であると判定する（Ｓ１０５）。一方、評価値の尤度が閾値を下回らない場合には（Ｓ１０４でＮＯ）、検出部１０は、アプリケーション１４の挙動が正常であると判定する（Ｓ１０６）。

[0050] ここで、図６及び図７を参照しながら、上述したステップＳ１０４の処理について具体的に説明する。検出部１０は、所定の機械学習法を用いて、図６に示す６次元空間の挙動ログ情報及び３次元空間の状態ログ情報を合計９次元空間の入力データとし、この９次元空間の入力データを２次元空間に写像することにより、図６に示すタイムスタンプ「０．１」、「０．２」、「０．３」及び「０．４」における各観測データを分離する。

[0051] これにより、例えば図７に示すように、タイムスタンプ「０．１」、「０．２」、「０．３」及び「０．４」における各観測データが２次元空間に写像される。この時、タイムスタンプ「０．１」及び「０．３」における各観測データは、事前に学習された正常な挙動群（図７において破線で囲まれた

領域）に含まれるが、タイムスタンプ「０．２」及び「０．４」における各観測データは、事前に学習された正常な挙動群に含まれない。

[0052] 具体的には、図６に示すように、タイムスタンプ「０．２」において、挙動ログ情報のフックポインタＡ発現数が「１８」と異常値を示している。これは、アプリケーション１４のプロセス制御が不正に乗っ取られた際に、異常なメモリアクセスが実行されたためであると考えられる。これにより、タイムスタンプ「０．２」における挙動ログ情報のフックポインタＡ発現数が異常値であることに起因して、図７に示すようにタイムスタンプ「０．２」における観測データが事前に学習された正常な挙動群に含まれなくなる。その結果、評価値の尤度が閾値を下回るため、検出部１０は、タイムスタンプ「０．２」におけるアプリケーション１４の挙動が異常であると判定する。

[0053] また、図６に示すように、タイムスタンプ「０．４」において、挙動ログ情報の通信メッセージＡが「緊急ブレーキ指示」であり、且つ、状態ログ情報の車速が「７９ｋｍ／ｈ」である。これは、車両が高速道路を走行中に、アプリケーション１４から通信部６に対して緊急ブレーキＡＰＩが発行されたためであると考えられる。これにより、タイムスタンプ「０．４」における挙動ログ情報の通信メッセージＡが「緊急ブレーキ指示」であり、且つ、状態ログ情報の車速が「７９ｋｍ／ｈ」であることに起因して、図７に示すようにタイムスタンプ「０．４」における観測データが事前に学習された正常な挙動群に含まれなくなる。その結果、評価値の尤度が閾値を下回るため、検出部１０は、タイムスタンプ「０．４」におけるアプリケーション１４の挙動が異常であると判定する。

[0054] ［１－３．効果］

上述したように、検出部１０は、取得した挙動ログ情報及び状態ログ情報、並びに、記憶部８に記憶された判断基準情報に基づいて、アプリケーション１４の挙動の異常を検出する。これにより、情報処理装置２は、例えばハッキング等の車両への攻撃に起因するアプリケーション１４の挙動の異常を確実に検出することができ、車両におけるセキュリティ対策を高めることが

できる。

[0055] （実施の形態２）

［２－１．情報処理装置の構成］

次に、図８及び図９を参照しながら、実施の形態２に係る情報処理装置２Ａの構成について説明する。図８は、実施の形態２に係る情報処理装置２Ａの構成を示すブロック図である。図９は、実施の形態２に係る判断基準情報の一例を示す図である。なお、以下に示す各実施の形態において、上記実施の形態１と同一の構成には同一の符号を付して、その説明を省略する。

[0056] 図８に示すように、実施の形態２に係る情報処理装置２Ａの異常検出部７Ａは、上記実施の形態１で説明した構成要素に加えて、ログ記憶部１８及び通知部２０を備えている。

[0057] ログ記憶部１８は、挙動記録部４からの挙動ログ情報、及び、通信部６からの状態ログ情報を記憶（蓄積）する。検出部１０Ａは、ログ記憶部１８に記憶された挙動ログ情報及び状態ログ情報を読み出して取得し、取得した挙動ログ情報及び状態ログ情報、並びに、記憶部８Ａに記憶された判断基準情報に基づいて、アプリケーション１４の挙動の異常を検出する。

[0058] 通知部２０は、検出部１０Ａによりアプリケーション１４の挙動の異常が検出された際に、外部（例えば外部サーバ又はユーザの端末装置等）にその旨を通知する。これにより、例えば異常な挙動をしているアプリケーション１４を強制的に停止するなどの処置を行うことができる。

[0059] 記憶部８Ａは、アプリケーション１４の挙動が正常であるか否かの判断基準を示す、ホワイトリスト型のルールベースである判断基準情報を予め記憶している。すなわち、判断基準情報は、アプリケーション１４の挙動が正常であるか否かを判定するためのルールベースモデルである判定モデルを含んでいる。ここで、図９を参照しながら、記憶部８Ａに記憶された判断基準情報の一例について説明する。図９に示す例では、判断基準情報は、イベント毎に定義された、アプリケーション１４の正常な挙動の履歴を示す正常挙動ログ情報、及び、車両の正常な状態の履歴を示す正常状態ログ情報を含んで

いる。

[0060] 検出部１０Ａは、いわゆるイベントドリブン方式により、イベント毎（例えば、タスクが生成される毎）に、取得した挙動ログ情報及び状態ログ情報と、判断基準情報に含まれる正常挙動ログ情報及び正常状態ログ情報とをそれぞれ比較することにより、アプリケーション１４の挙動の異常を検出する。

[0061] 具体的には、判断基準情報の全てのイベント（イベント１、イベント２、・・・、イベントｎ）において、取得した挙動ログ情報及び状態ログ情報と、判断基準情報に含まれる正常挙動ログ情報及び正常状態ログ情報とがそれぞれマッチする場合に、検出部１０Ａは、アプリケーション１４の挙動が正常であると検出する。一方、判断基準情報のいずれかのイベントにおいて、取得した挙動ログ情報（又は状態ログ情報）と、判断基準情報に含まれる正常挙動ログ情報（又は正常状態ログ情報）とがマッチしない場合に、検出部１０Ａは、アプリケーション１４の挙動が異常であると検出する。

[0062] ［２－２．検出部の動作］

次に、図１０及び図１１を参照しながら、検出部１０Ａの動作について説明する。図１０は、実施の形態２に係る情報処理装置２Ａの検出部１０Ａの動作の流れを示すフローチャートである。図１１は、実施の形態２に係る情報処理装置２Ａの検出部１０Ａにより取得される挙動ログ情報及び状態ログ情報、並びに、記憶部８Ａに記憶された判断基準情報の一例を示す図である。

[0063] 以下、アプリケーション１４がカーシェアアプリケーションであることを前提として、悪意のある第三者がアプリケーション１４の脆弱性を突き、アプリケーション１４のプロセス制御を不正に乗っ取る場合について説明する。ここで、アプリケーション１４により登録されたユーザの顧客情報（例えば、利用者名及びアプリケーション１４の利用履歴等を含む）は、例えば、カーシェアの開始時（車両の停車時（０ｋｍ／ｈ））にのみ外部サーバに送信されるものと仮定する。しかしながら、不正に乗っ取られたアプリケーシ

ョン１４は、カーシェアの開始時以外のタイミング（例えば車両の走行時）で顧客情報を読み出し、通信部６を介して外部サーバに当該顧客情報を送信する。これにより、ユーザの顧客情報が外部に流出するおそれがある。

[0064] 図１０に示すように、検出部１０Ａは、ログ記憶部１８から挙動ログ情報及び状態ログ情報を読み出して取得する（Ｓ２０１）。ここで、検出部１０Ａは、例えば図１１の（ａ）に示すような挙動ログ情報及び状態ログ情報を取得する。図１１の（ａ）に示す例では、挙動ログ情報は、ａ）タイムスタンプ、ｂ）プロセスＩＤ、ｃ）フックポインタ名称、ｄ）フックポインタ属性１、及び、ｅ）フックポインタ属性２を含んでいる。また、状態ログ情報は、ａ）タイムスタンプ、ｂ）車速、ｃ）加速度、及び、ｄ）操舵角を含んでいる。

[0065] 検出部１０Ａは、取得した挙動ログ情報及び状態ログ情報と、記憶部８Ａに記憶されたホワイトリスト型のルールベースである判断基準情報とのパターンマッチングを行う（Ｓ２０２）。ここで、記憶部８Ａは、例えば図１１の（ｂ）に示すようなホワイトリスト型のルールベースである判断基準情報を記憶している。図１１の（ｂ）に示す例では、判断基準情報の正常挙動ログ情報は、ａ）タイムスタンプ、ｂ）フックポインタ名称、ｃ）フックポインタ属性１、及び、ｄ）フックポインタ属性２を含んでいる。また、判断基準情報の正常状態ログ情報は、ａ）タイムスタンプ、及び、ｂ）車速を含んでいる。

[0066] ホワイトリスト型のルールベースである判断基準情報の正常挙動ログ情報（又は正常状態ログ情報）とマッチしない挙動ログ情報（又は状態ログ情報）が存在する場合には（Ｓ２０３でＹＥＳ）、検出部１０Ａは、アプリケーション１４の挙動が異常であると判定する（Ｓ２０４）。一方、ホワイトリスト型のルールベースである判断基準情報の正常挙動ログ情報（又は正常状態ログ情報）とマッチしない挙動ログ情報（又は状態ログ情報）が存在しない場合には（Ｓ２０３でＮＯ）、検出部１０Ａは、アプリケーション１４の挙動が正常であると判定する（Ｓ２０５）。

[0067] ここで、図１１を参照しながら、上述したステップＳ２０３の処理について具体的に説明する。図１１に示す例では、検出部１０Ａは、イベント毎に、挙動ログ情報に含まれるフックポインタ名称、フックポインタ属性１及びフックポインタ属性２と、判断基準情報の正常挙動ログ情報に含まれるフックポインタ名称、フックポインタ属性１及びフックポインタ属性２とのパターンマッチングを行うとともに、状態ログ情報に含まれる車速と、判断基準情報の正常状態ログ情報に含まれる車速とのパターンマッチングを行う。

[0068] 図１１に示すように、イベント１では、判断基準情報とマッチしない挙動ログ情報及び／又は状態ログ情報が存在しないため、検出部１０Ａは、アプリケーション１４の挙動が正常であると判定する。

[0069] また、イベント２では、挙動ログ情報のフックポインタ属性１「ｆｉｌｅＢ」及びフックポインタ属性２「ｗｒｉｔｅ」はそれぞれ、判断基準情報の正常挙動ログ情報のフックポインタ属性１「ｆｉｌｅＡ」及びフックポインタ属性２「ｒｅａｄ」とマッチしない。これは、通常行われないファイルへの書き込みが行われたためであると考えられる。これにより、判断基準情報の正常挙動ログ情報とマッチしない挙動ログ情報が存在するため、検出部１０Ａは、イベント２におけるアプリケーション１４の挙動が異常であると判定する。

[0070] また、イベント３では、状態ログ情報のフックポインタ属性１「通信機器」及びフックポインタ属性２「データ送信」はそれぞれ、判断基準情報の正常状態ログ情報のフックポインタ属性１「通信機器」及びフックポインタ属性２「データ送信」とマッチするが、状態ログ情報の車速「５７（ｋｍ／ｈ）」は、判断基準情報の正常状態ログ情報の車速「０（ｋｍ／ｈ）」とマッチしない。これは、カーシェアの開始時（車両の停止時）以外のタイミング（車両の走行時）で、外部サーバへの顧客情報の送信が行われたためであると考えられる。これにより、判断基準情報の正常状態ログ情報とマッチしない状態ログ情報が存在するため、検出部１０Ａは、イベント３におけるアプリケーション１４の挙動が異常であると判定する。

[0071] したがって、本実施の形態においても、上記実施の形態１と同様の効果を得ることができる。

[0072] ［２－３．車両への他の攻撃例］

以下、車両への他の攻撃例１～３について説明する。

[0073] ［２－３－１．攻撃例１］

攻撃例１として、アプリケーション１４が自動運転アプリケーションであることを前提として、悪意のある第三者がアプリケーション１４の脆弱性を突き、アプリケーション１４のプロセス制御を不正に乗っ取る場合について説明する。

[0074] ここで、アプリケーション１４は、ユーザに対して車両の状態に関する情報を提示するために、車両に搭載されたセンサからのセンサ情報を取得する。なお、センサは、例えば車両の周囲に存在する物体を検出するためのＬｉＤＡＲ（Ｌｉｇｈｔ　Ｄｅｔｅｃｔｉｏｎ　Ａｎｄ　Ｒａｎｇｉｎｇ）、ミリ波センサ又はカメラセンサ等である。

[0075] この場合、不正に乗っ取られたアプリケーション１４は、本来は許可されていないセンサ情報を送信する権限を奪取し、通信部６を介して不正なセンサ情報を例えば車両のＡＤＡＳに送信する。なお、不正なセンサ情報は、例えば前方車両が存在しないにも拘らず、前方車両の存在を検出したことを示すセンサ情報等である。ＡＤＡＳがアプリケーション１４からの不正なセンサ情報を受信することにより、車両の誤操作が誘発されるおそれがある。

[0076] この攻撃例１においても、検出部１０Ａは、取得した挙動ログ情報及び状態ログ情報、並びに、記憶部８Ａに記憶された判断基準情報に基づいて、アプリケーション１４の挙動の異常を検出する。具体的には、不正なセンサ情報に基づく状態ログ情報（例えば、「前方車両あり」を示す状態ログ情報）が、他のセンサ情報に基づく状態ログ情報（例えば、「前方車両無し」を示す状態ログ情報）とは反しているため、検出部１０Ａは、アプリケーション１４の挙動が異常であると判定する。

[0077] ［２－３－２．攻撃例２］

攻撃例２として、アプリケーション１４が宅配ボックスアプリケーションであることを前提として、悪意のある第三者がアプリケーション１４の脆弱性を突き、アプリケーション１４のプロセス制御を不正に乗っ取る場合について説明する。ここで、アプリケーション１４は、車両の停車時（０ｋｍ／ｈ）にのみ使用され、車両の走行中は使用されない。

[0078] この場合、不正に乗っ取られたアプリケーション１４は、車両のトランクのロックを開錠するための認証プロセスを実行し、通信部６に対して、車両のトランクのロックを開錠するように命令するためのＡＰＩを発行する。これにより、車両の走行中にトランクのロックが開錠され、トランクが不意に開くおそれがある。

[0079] この攻撃例２においても、検出部１０Ａは、取得した挙動ログ情報及び状態ログ情報、並びに、記憶部８Ａに記憶された判断基準情報に基づいて、アプリケーション１４の挙動の異常を検出する。具体的には、状態ログ情報のフックポインタ属性１「（宅配ボックスアプリケーションの）認証プロセスの実行」は、判断基準情報の正常状態ログ情報のフックポインタ属性１「（宅配ボックスアプリケーションの）認証プロセスの実行」とマッチするが、状態ログ情報の車速「５７（ｋｍ／ｈ）」は、判断基準情報の正常状態ログ情報の車速「０（ｋｍ／ｈ）」とマッチしないため、検出部１０Ａは、アプリケーション１４の挙動が異常であると判定する。

[0080] ［２－３－３．攻撃例３］

攻撃例３として、アプリケーション１４が広告配信アプリケーションであることを前提として、悪意のある第三者がアプリケーション１４の脆弱性を突き、アプリケーション１４のプロセス制御を不正に乗っ取る場合について説明する。ここで、アプリケーション１４は、主に車両の停車時（０ｋｍ／ｈ）に動作して、ユーザに対して広告を表示するものであり、車両の走行中にはほとんど動作しない。

[0081] この場合、不正に乗っ取られたアプリケーション１４は、マイニングツールのダウンロード及びインストールを実行し、高負荷の演算を行う。これに

より、ＣＰＵ（Ｃｅｎｔｒａｌ　Ｐｒｏｃｅｓｓｉｎｇ　Ｕｎｉｔ）リソースが枯渇し、他のアプリケーション１４の動作に悪影響を与えるおそれがある。

[0082] この攻撃例３においても、検出部１０Ａは、取得した挙動ログ情報及び状態ログ情報、並びに、記憶部８Ａに記憶された判断基準情報に基づいて、アプリケーション１４の挙動の異常を検出する。具体的には、状態ログ情報の車速「５７（ｋｍ／ｈ）」におけるフックポインタＡ発現数が異常であるため、検出部１０Ａは、アプリケーション１４の挙動が異常であると判定する。

[0083] （実施の形態３）

［３－１．情報処理装置の構成］

次に、図１２を参照しながら、実施の形態３に係る情報処理装置２Ｂの構成について説明する。図１２は、実施の形態３に係る情報処理装置２Ｂの構成を示すブロック図である。

[0084] 図１２に示すように、実施の形態３に係る情報処理装置２Ｂの異常検出部７Ｂは、上記実施の形態１で説明した構成要素に加えて、ログ記憶部１８及び推論部２２を備えている。ログ記憶部１８については実施の形態２で既述したので、ここでの説明を省略する。

[0085] 推論部２２は、ログ記憶部１８に記憶された状態ログ情報に基づいて、車両の状態を推論する。車両の状態とは、例えば車両の車速、加速度及び操舵角等である。推論部２２は、推論結果を検出部１０Ｂに出力する。

[0086] 記憶部８Ｂは、アプリケーション１４の挙動が正常であるか否かの判断基準を示す、ブラックリスト型のルールベースである判断基準情報を予め記憶している。すなわち、判断基準情報は、アプリケーション１４の挙動が正常であるか否かを判定するためのルールベースモデルである判定モデルを含んでいる。この判断基準情報は、イベント毎に定義された、アプリケーション１４の異常な挙動の履歴を示す異常挙動ログ情報、及び、車両の異常な状態の履歴を示す異常状態ログ情報を含んでいる。

[0087] 検出部１０Ｂは、いわゆるイベントドリブン方式により、イベント毎に、取得した挙動ログ情報及び状態ログ情報と、判断基準情報に含まれる異常挙動ログ情報及び異常状態ログ情報とをそれぞれ比較することにより、アプリケーション１４の挙動の異常を検出する。また、検出部１０Ｂは、推論部からの推論結果を加味して、アプリケーション１４の挙動の異常を検出する。

[0088] ［３－２．検出部の動作］

次に、図１３を参照しながら、検出部１０Ｂの動作について説明する。図１３は、実施の形態３に係る情報処理装置２Ｂの検出部１０Ｂの動作の流れを示すフローチャートである。

[0089] 図１３に示すように、検出部１０Ｂは、ログ記憶部１８から挙動ログ情報及び状態ログ情報を読み出して取得する（Ｓ３０１）。検出部１０Ｂは、取得した挙動ログ情報及び状態ログ情報と、記憶部８Ｂに記憶されたブラックリスト型のルールベースである判断基準情報とのパターンマッチングを行う（Ｓ３０２）。

[0090] ブラックリスト型のルールベースである判断基準情報の異常挙動ログ情報（又は異常状態ログ情報）とマッチする挙動ログ情報（又は状態ログ情報）が存在する場合には（Ｓ３０３でＹＥＳ）、検出部１０Ｂは、アプリケーション１４の挙動が異常であると判定する（Ｓ３０４）。一方、ブラックリスト型のルールベースである判断基準情報の異常挙動ログ情報（又は異常状態ログ情報）とマッチする挙動ログ情報（又は状態ログ情報）が存在しない場合には（Ｓ３０３でＮＯ）、検出部１０Ｂは、アプリケーション１４の挙動が正常であると判定する（Ｓ３０５）。

[0091] したがって、本実施の形態においても、上記実施の形態１と同様の効果を得ることができる。

[0092] （実施の形態４）

次に、図１４を参照しながら、実施の形態４に係る情報処理装置２Ｃの構成について説明する。図１４は、実施の形態４に係る情報処理装置２Ｃの構成を示すブロック図である。

[0093] 図１４に示すように、実施の形態４に係る情報処理装置２Ｃの異常検出部７Ｃは、上記実施の形態１で説明した構成要素に加えて、ログ記憶部１８及び推論部２２Ｃを備えている。ログ記憶部１８については実施の形態２で既述したので、ここでの説明を省略する。

[0094] 推論部２２Ｃは、通信部６により受信された状態ログ情報に基づいて、車両の状態を推論する。推論部２２Ｃは、推論結果を状態ログ情報としてログ記憶部１８に記憶させる。なお、推論部２２Ｃは、通信部６により受信された複数の状態ログ情報のうち、アプリケーション１４の異常の検出に有用な状態ログ情報のみをフィルタリングしてもよい。この場合、推論部２２Ｃは、フィルタリングした状態ログ情報に基づいて、車両の状態を推論する。

[0095] したがって、本実施の形態においても、上記実施の形態１と同様の効果を得ることができる。

[0096] （実施の形態５）

次に、図１５を参照しながら、実施の形態５に係る情報処理装置２Ｄの構成について説明する。図１５は、実施の形態５に係る情報処理装置２Ｄの構成を示すブロック図である。

[0097] 図１５に示すように、実施の形態５に係る情報処理装置２Ｄの異常検出部７Ｄは、上記実施の形態１で説明した構成要素に加えて、推論部２２Ｄを備えている。推論部２２Ｄは、通信部６により受信された状態情報に基づいて、車両の状態を推論する。推論部２２Ｄは、推論結果を状態情報として検出部１０Ｄに出力する。なお、推論部２２Ｄは、通信部６により受信された複数の状態情報のうち、アプリケーション１４の異常の検出に有用な状態情報のみをフィルタリングしてもよい。この場合、推論部２２Ｄは、フィルタリングした状態情報に基づいて、車両の状態を推論する。

[0098] 検出部１０Ｄは、挙動記録部４からの挙動情報と、推論部２２Ｄからの状態情報（推論結果）とを取得する。検出部１０Ｄは、取得した挙動情報及び状態情報、並びに、記憶部８に記憶された判断基準情報に基づいて、アプリケーション１４の挙動の異常を検出する。

[0099] なお、状態情報及び挙動情報は必ずしもログ情報というわけではなく、例えば、挙動情報の履歴とあるタイミングにおける状態情報とに基づいて異常を検出したり、あるタイミングにおける挙動情報と状態情報の履歴とに基づいて異常を検出することもできる。

[0100] したがって、本実施の形態においても、上記実施の形態１と同様の効果を得ることができる。

[0101] （変形例等）

以上、一つ又は複数の態様に係る情報処理装置及び制御方法について、上記各実施の形態に基づいて説明したが、本開示は、上記各実施の形態に限定されるものではない。本開示の趣旨を逸脱しない限り、当業者が思い付く各種変形を上記各実施の形態に施したものや、異なる実施の形態における構成要素を組み合わせて構築される形態も、一つ又は複数の態様の範囲内に含まれてもよい。

[0102] 上記各実施の形態では、本開示に係る情報処理装置の適用例として、自動車等の車両に搭載される車載ネットワークにおけるセキュリティ対策への適用について説明したが、本開示に係る情報処理装置の適用範囲はこれに限定されない。本開示に係る情報処理装置は、自動車等の車両に限定されず、例えば、建機、農機、船舶、鉄道又は飛行機等の任意のモビリティに適用してもよい。

[0103] 上記各実施の形態では、通信部６は、ＣＡＮバス１６に接続されているとしたが、これに限定されず、例えばＥｔｈｅｒｎｅｔ（登録商標）又はＦｌｅｘＲａｙ（登録商標）等の任意の車載ネットワークに接続されていてもよいし、あるいは、ソフトウェアプラットフォーム１２以外の他の仮想マシンに接続されていてもよい。

[0104] なお、上記各実施の形態において、各構成要素は、専用のハードウェアで構成されるか、各構成要素に適したソフトウェアプログラムを実行することによって実現されてもよい。各構成要素は、ＣＰＵ又はプロセッサ等のプログラム実行部が、ハードディスク又は半導体メモリなどの記録媒体に記録さ

れたソフトウェアプログラムを読み出して実行することによって実現されてもよい。

[0105] また、上記各実施の形態に係る情報処理装置の機能の一部又は全てを、ＣＰＵ等のプロセッサがプログラムを実行することにより実現してもよい。

[0106] 上記の各装置を構成する構成要素の一部又は全部は、各装置に脱着可能なＩＣカード又は単体のモジュールから構成されているとしても良い。前記ＩＣカード又は前記モジュールは、マイクロプロセッサ、ＲＯＭ、ＲＡＭ等から構成されるコンピュータシステムである。前記ＩＣカード又は前記モジュールは、上記の超多機能ＬＳＩを含むとしても良い。マイクロプロセッサが、コンピュータプログラムにしたがって動作することにより、前記ＩＣカード又は前記モジュールは、その機能を達成する。このＩＣカード又はこのモジュールは、耐タンパ性を有するとしても良い。

[0107] 本開示は、上記に示す方法であるとしても良い。また、これらの方法をコンピュータにより実現するコンピュータプログラムであるとしても良いし、前記コンピュータプログラムからなるデジタル信号であるとしても良い。また、本開示は、前記コンピュータプログラム又は前記デジタル信号をコンピュータ読み取り可能な記録媒体、例えばフレキシブルディスク、ハードディスク、ＣＤ－ＲＯＭ、ＭＯ、ＤＶＤ、ＤＶＤ－ＲＯＭ、ＤＶＤ－ＲＡＭ、ＢＤ（Ｂｌｕ－ｒａｙ（登録商標）　Ｄｉｓｃ）、半導体メモリ等に記録したものとしても良い。また、これらの記録媒体に記録されている前記デジタル信号であるとしても良い。また、本開示は、前記コンピュータプログラム又は前記デジタル信号を、電気通信回線、無線又は有線通信回線、インターネットを代表とするネットワーク、データ放送等を経由して伝送するものとしても良い。また、本開示は、マイクロプロセッサとメモリを備えたコンピュータシステムであって、前記メモリは、上記コンピュータプログラムを記憶しており、前記マイクロプロセッサは、前記コンピュータプログラムにしたがって動作するとしても良い。また、前記プログラム又は前記デジタル信号を前記記録媒体に記録して移送することにより、又は前記プログラム又は前

記デジタル信号を前記ネットワーク等を経由して移送することにより、独立した他のコンピュータシステムにより実施するとしても良い。

産業上の利用可能性

[0108] 本開示は、例えば車両の車載機器上で動作するアプリケーションの異常を検出するための情報処理装置等に有用である。

符号の説明

[0109] ２，２Ａ，２Ｂ，２Ｃ，２Ｄ　情報処理装置

４　挙動記録部

６　通信部

７，７Ａ，７Ｂ，７Ｃ，７Ｄ　異常検出部

８，８Ａ，８Ｂ　記憶部

１０，１０Ａ，１０Ｂ，１０Ｄ　検出部

１２　ソフトウェアプラットフォーム

１４　アプリケーション

１６　ＣＡＮバス

１８　ログ記憶部

２０　通知部

２２，２２Ｃ，２２Ｄ　推論部

請求の範囲

[請求項1] モビリティに搭載されたモビリティネットワークに接続される情報処理装置であって、

前記モビリティに搭載された機器上で動作するアプリケーションの挙動が正常であるか否かの判断基準を示す判断基準情報を記憶する記憶部と、

前記アプリケーションの挙動を示す挙動情報を取得し、取得した前記挙動情報及び前記記憶部に記憶された前記判断基準情報に基づいて、前記アプリケーションの挙動の異常を検出する検出部と、を備える

情報処理装置。

[請求項2] 前記検出部は、前記モビリティネットワークから取得した前記モビリティの状態を示す状態情報と、前記挙動情報と、前記記憶部に記憶された前記判断基準情報とに基づいて、前記アプリケーションの挙動の異常を検出する

請求項１に記載の情報処理装置。

[請求項3] 前記判断基準情報は、前記アプリケーションの挙動の異常を検出するための判定モデルとして、前記アプリケーションの挙動及び前記モビリティの状態の少なくとも一方に関するルールベースモデル又は機械学習モデルを含み、

前記検出部は、前記挙動情報及び前記状態情報に前記判定モデルを適用することにより、前記アプリケーションの挙動の異常を検出する

請求項２に記載の情報処理装置。

[請求項4] 前記判断基準情報は、前記アプリケーションの正常な挙動の履歴を示す正常挙動ログ情報、及び、前記モビリティの正常な状態の履歴を示す正常状態ログ情報を含み、

前記検出部は、取得した前記挙動情報の履歴及び前記状態情報の履歴と、前記判断基準情報に含まれる前記正常挙動ログ情報及び前記正常状態ログ情報とをそれぞれ比較することにより、前記アプリケーシ

ョンの挙動の異常を検出する

請求項２に記載の情報処理装置。

[請求項5] 前記判断基準情報は、前記アプリケーションの異常な挙動の履歴を示す異常挙動ログ情報、及び、前記モビリティの異常な状態の履歴を示す異常状態ログ情報を含み、

前記検出部は、取得した前記挙動情報の履歴及び前記状態情報の履歴と、前記判断基準情報に含まれる前記異常挙動ログ情報及び前記異常状態ログ情報とをそれぞれ比較することにより、前記アプリケーションの挙動の異常を検出する

請求項２に記載の情報処理装置。

[請求項6] 前記判断基準情報は、機械学習により予め生成された、前記アプリケーションの挙動の正常らしさを判定するための判定モデルを含み、

前記検出部は、前記判定モデルを用いて、取得した前記挙動情報の履歴から第１の特徴量を算出し、且つ、前記状態情報の履歴から第２の特徴量を算出し、算出した前記第１の特徴量及び前記第２の特徴量から前記アプリケーションの挙動の正常らしさを示す評価値を算出し、前記評価値の尤度と閾値とを比較することにより、前記アプリケーションの挙動の異常を検出する

請求項２に記載の情報処理装置。

[請求項7] 前記情報処理装置は、さらに、前記状態情報に基づいて、前記モビリティの状態を推論する推論部を備え、

前記検出部は、前記推論部の推論結果を加味して、前記アプリケーションの挙動の異常を検出する

請求項２～６のいずれか１項に記載の情報処理装置。

[請求項8] 前記情報処理装置は、さらに、前記検出部が前記アプリケーションの挙動の異常を検出した際に、外部にその旨を通知する通知部を備える

請求項１～７のいずれか１項に記載の情報処理装置。

[請求項9] モビリティに搭載されたモビリティネットワークに接続される情報処理装置における制御方法であって、

前記モビリティに搭載された機器上で動作するアプリケーションの挙動を示す挙動情報を取得するステップと、

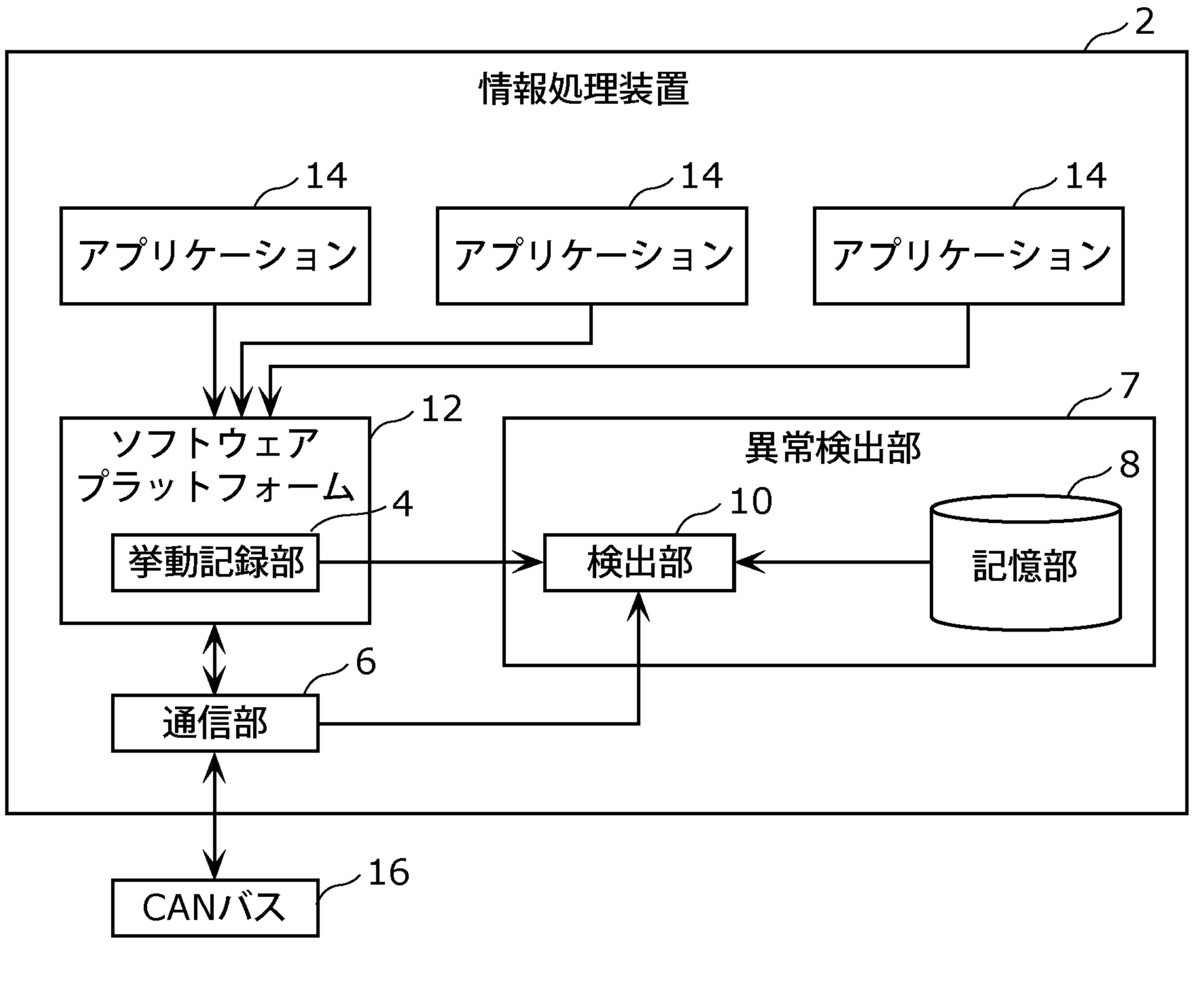
取得した前記挙動情報、及び、前記アプリケーションの挙動が正常であるか否かの判断基準を示し且つ記憶部に予め記憶された判断基準情報に基づいて、前記アプリケーションの挙動の異常を検出するステップと、を含む

制御方法。

[請求項10] 請求項９に記載の制御方法をコンピュータに実行させる

プログラム。

[図1]


2
情報処理装置
14
アプリケーション
14
アプリケーション
14
アプリケーション
12
ソフトウェア
プラットフォーム
4
挙動記録部
7
異常検出部
10
検出部
8
記憶部
6
通信部
16
CANバス

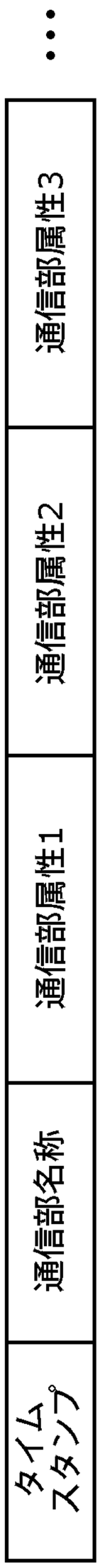
[図2]

タイムスタンプ	プロセス名	プロセスID	フックポイント名称	フックポイント属性1	フックポイント属性2	・・・

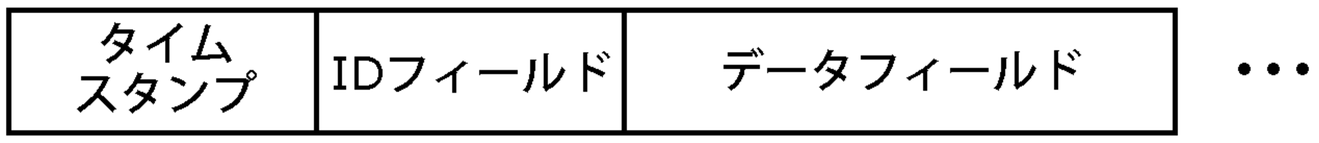
[図3]

タイムスタンプ	車速	加速度	操舵角	・・・

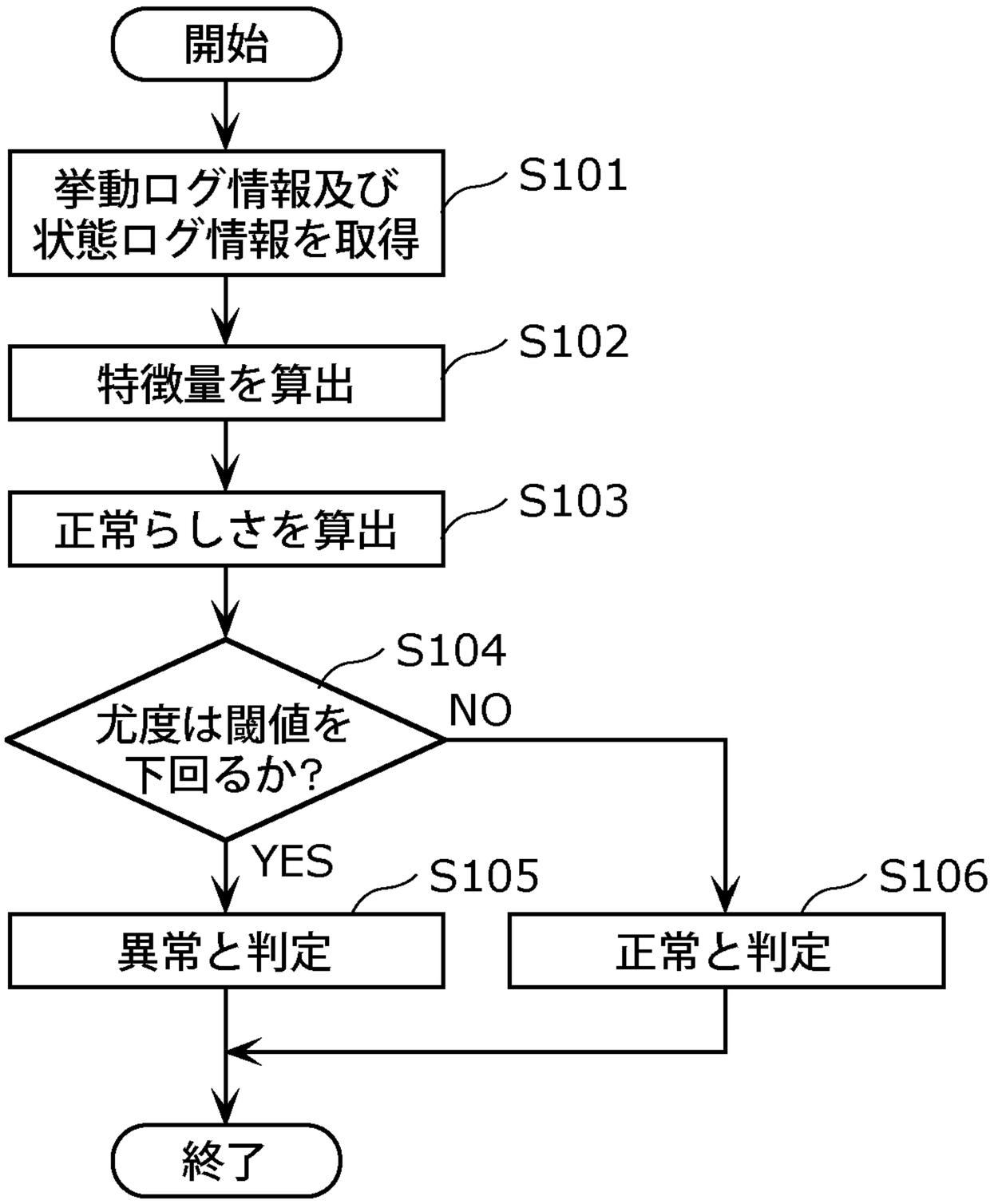
[図4A]


タイムスタンプ
通信部名称
通信部属性1
通信部属性2
通信部属性3
・・・

[図4B]


タイムスタンプ
IDフィールド
データフィールド
・・・

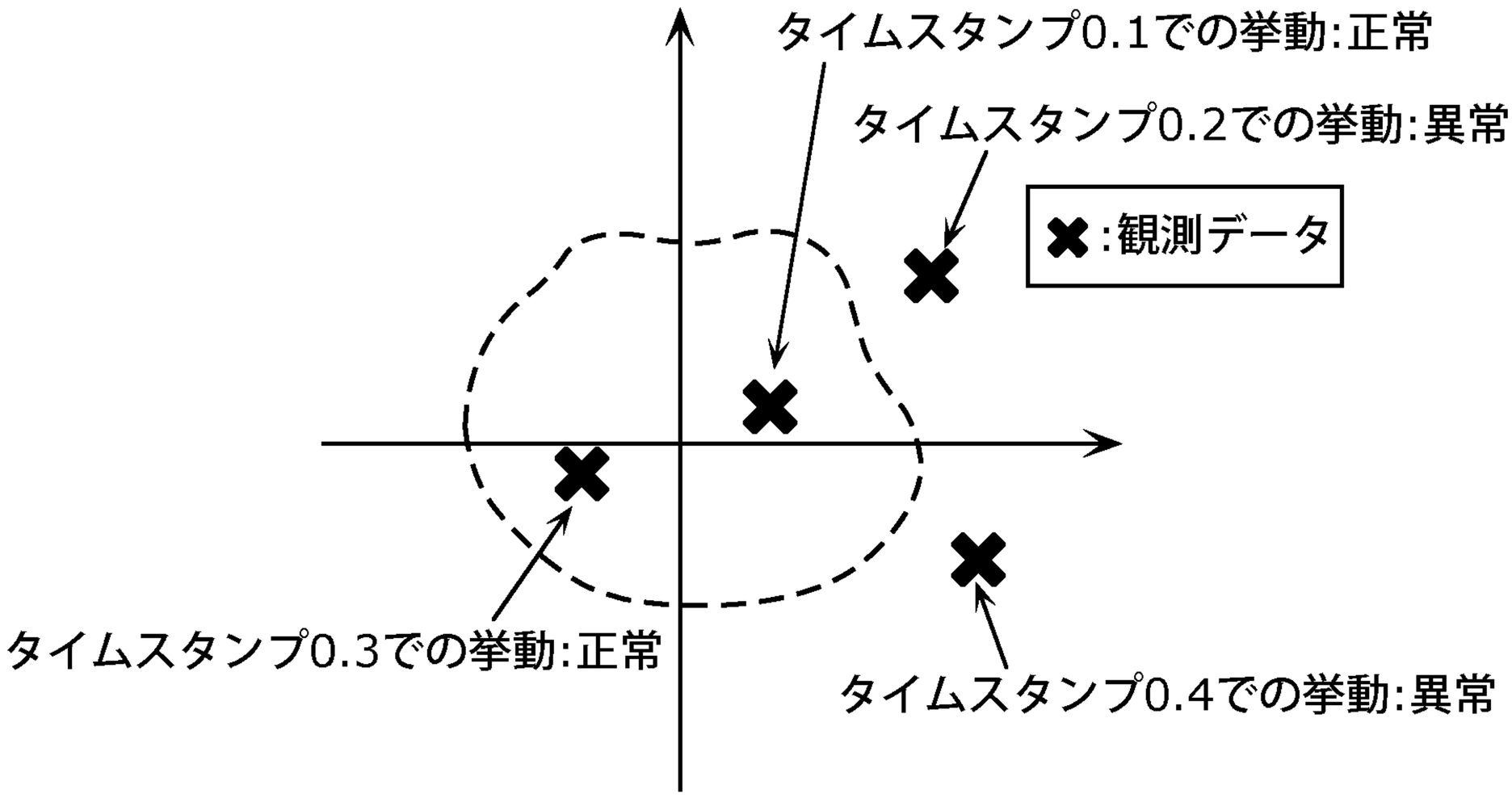
[図5]


開始
挙動ログ情報及び
状態ログ情報を取得
S101
特徴量を算出
S102
正常らしさを算出
S103
尤度は閾値を
下回るか?
S104
NO
YES
異常と判定
S105
正常と判定
S106
終了

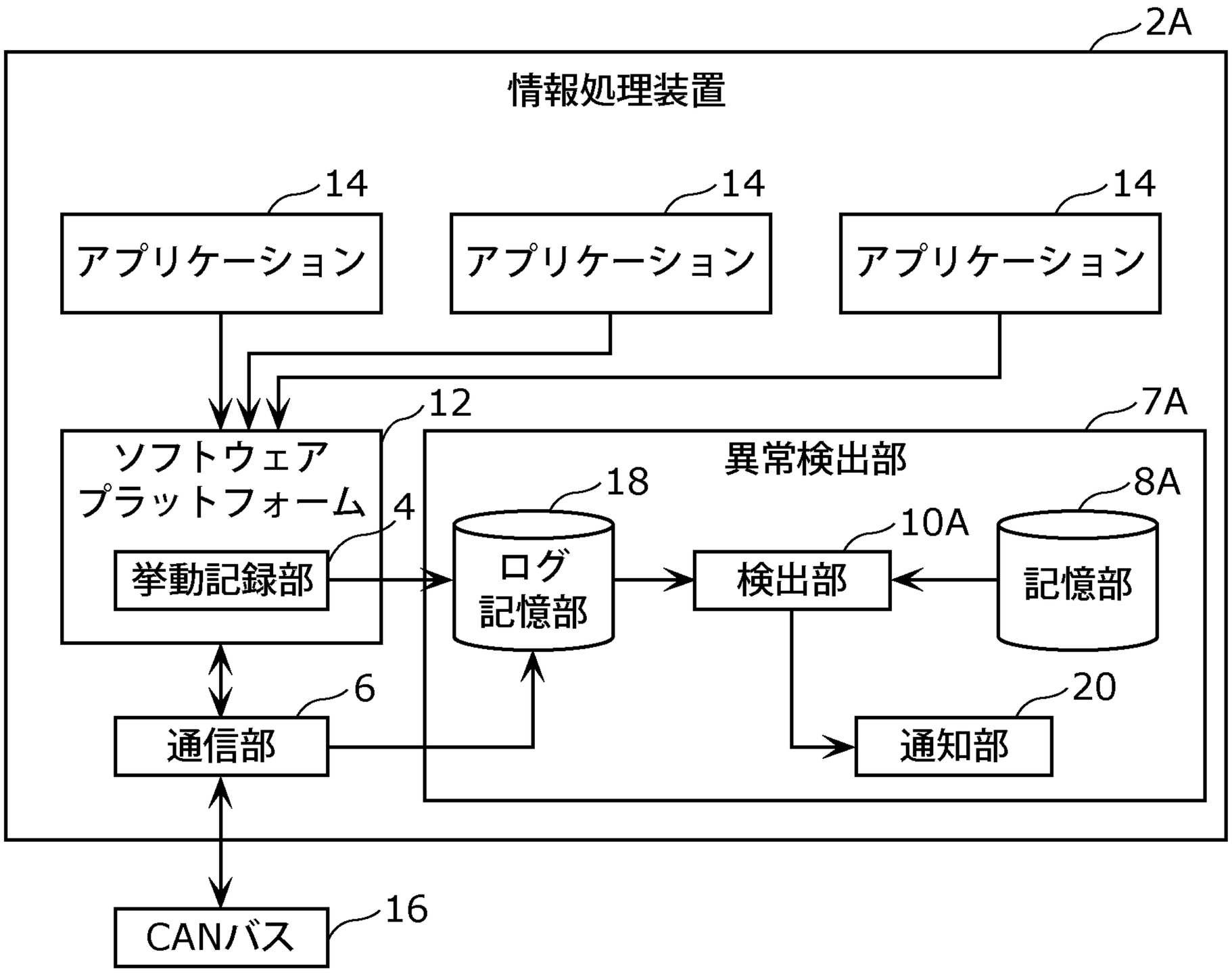
[図6]

挙動ログ情報							状態ログ情報			
	タイムスタンプ	フックポインタA 発現数	フックポインタB 発現数	フックポインタC 発現数	フックポインタD 発現数	通信 メッセージA	通信 メッセージB	車速[km/h]	加速度[m/s²]	操舵角[度]
	0.1	10	0	2	5	ー	5	78	2	1
	0.2	18	2	2	3	ー	3	80	-1	-2
	0.3	0	0	3	0	ー	5	79	0	0
	0.4	1	0	8	0	緊急ブレーキ指示	3	79	-25	30

[図7]


タイムスタンプ0.1での挙動:正常
タイムスタンプ0.2での挙動:異常
:観測データ
タイムスタンプ0.3での挙動:正常
タイムスタンプ0.4での挙動:異常

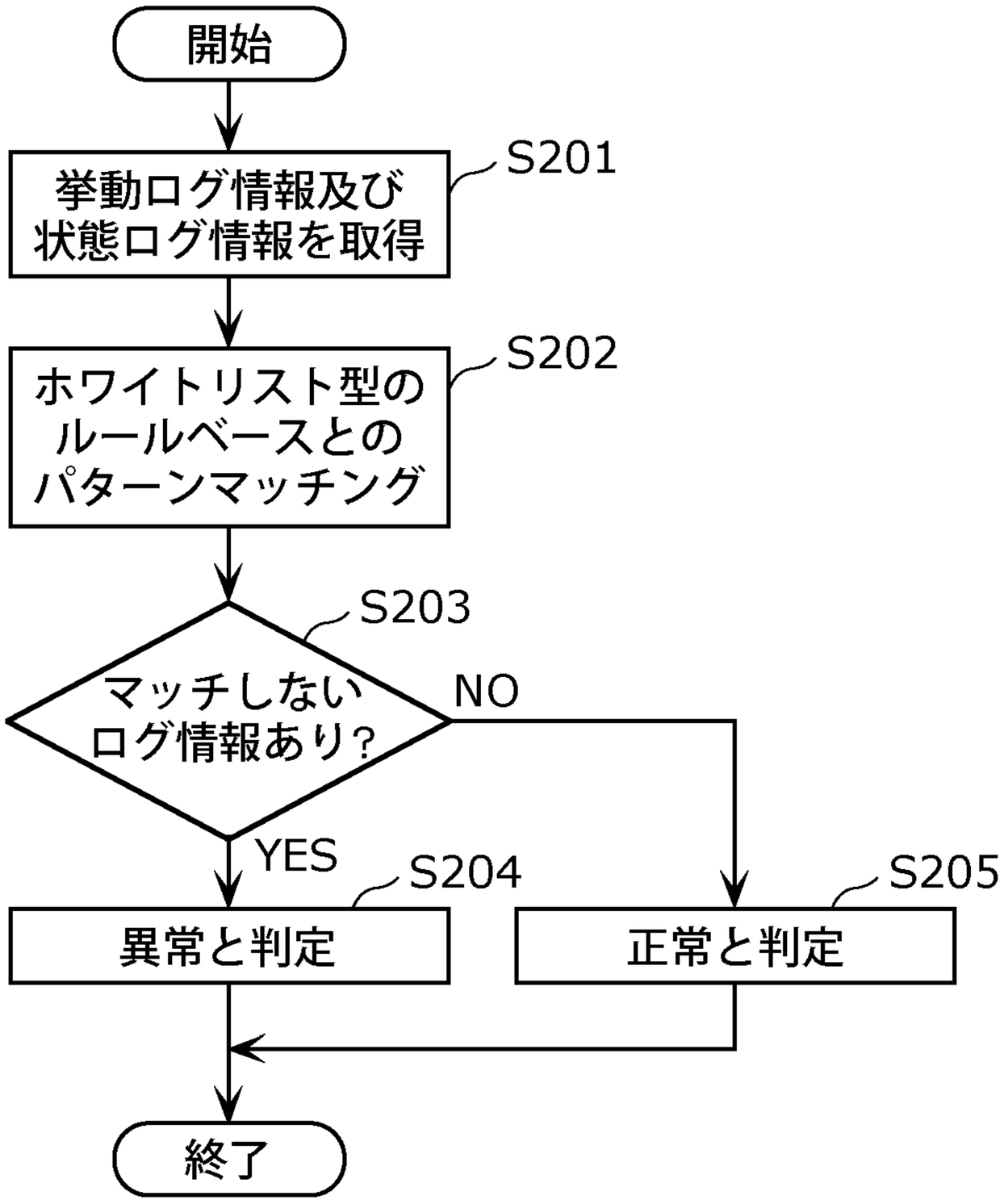
[図8]


2A
情報処理装置
14
アプリケーション
14
アプリケーション
14
アプリケーション
12
ソフトウェア
プラットフォーム
4
挙動記録部
18
ログ
記憶部
7A
異常検出部
10A
検出部
8A
記憶部
6
通信部
20
通知部
CANバス
16

[図9]

イベント1	正常挙動ログ情報	正常状態ログ情報	
イベント2	正常挙動ログ情報	正常状態ログ情報	
イベント3	正常挙動ログ情報	正常状態ログ情報	
⋮	⋮	⋮	
イベントn	正常挙動ログ情報	正常状態ログ情報	“正常”

[図10]



[図11]

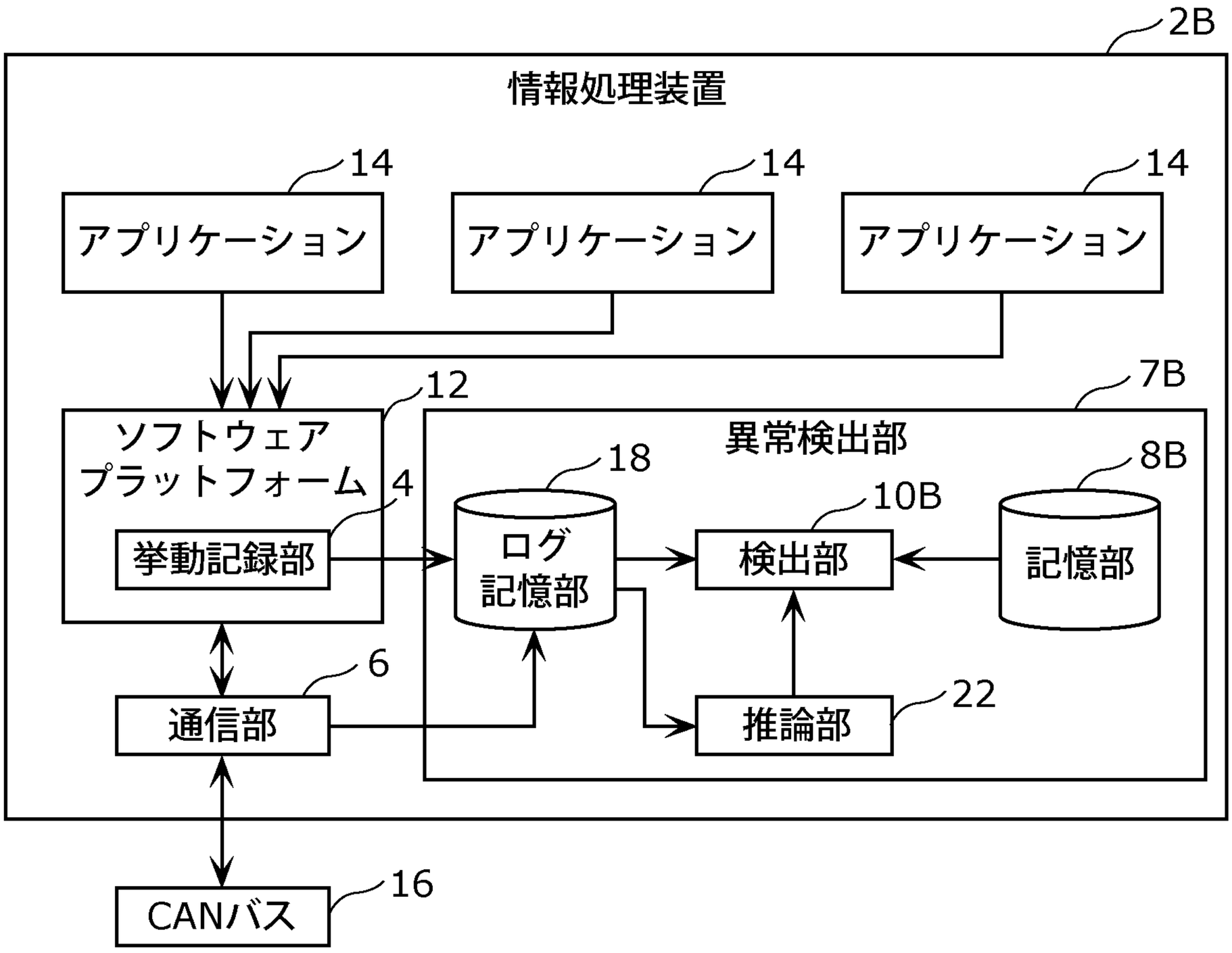
(a)

		挙動ログ情報			状態ログ情報		
	タイムスタンプ	プロセスID	フックポインタ名称	フックポインタ属性1	フックポインタ属性2	車速[km/h]	加速度[m/s²]	操舵角[度]
イベント1	0.120	1125	task_create	-	-	0	0	0
	0.123	1125	file_permission	fileA	read	0	0	0
	0.126	1125	mmap_addr	addr1	-	0	0	0
	0.128	1125	file_ioctl	通信機器	データ送信	0	0	0
	0.130	1125	task_free	-	-	0	0	0
	⋮			⋮				⋮
イベント2	1854.1254	2565	task_create	-	-	56	0	1
	1854.1354	2565	file_permission	fileB	write	56	0	1
	1854.1454	2565	mmap_addr	addr1	-	56	1	-2
	1854.1600	2565	task_free	8	0	55	0	0
	⋮			⋮				⋮
イベント3	2152.120	6548	task_create	-	-	56	0	1
	2152.123	6548	file_permission	fileA	read	56	0	1
	2152.126	6548	mmap_addr	addr1	-	56	1	-2
	2152.128	6548	file_ioctl	通信機器	データ送信	57	-2	0
	2152.130	6548	task_free	8	0	55	0	0

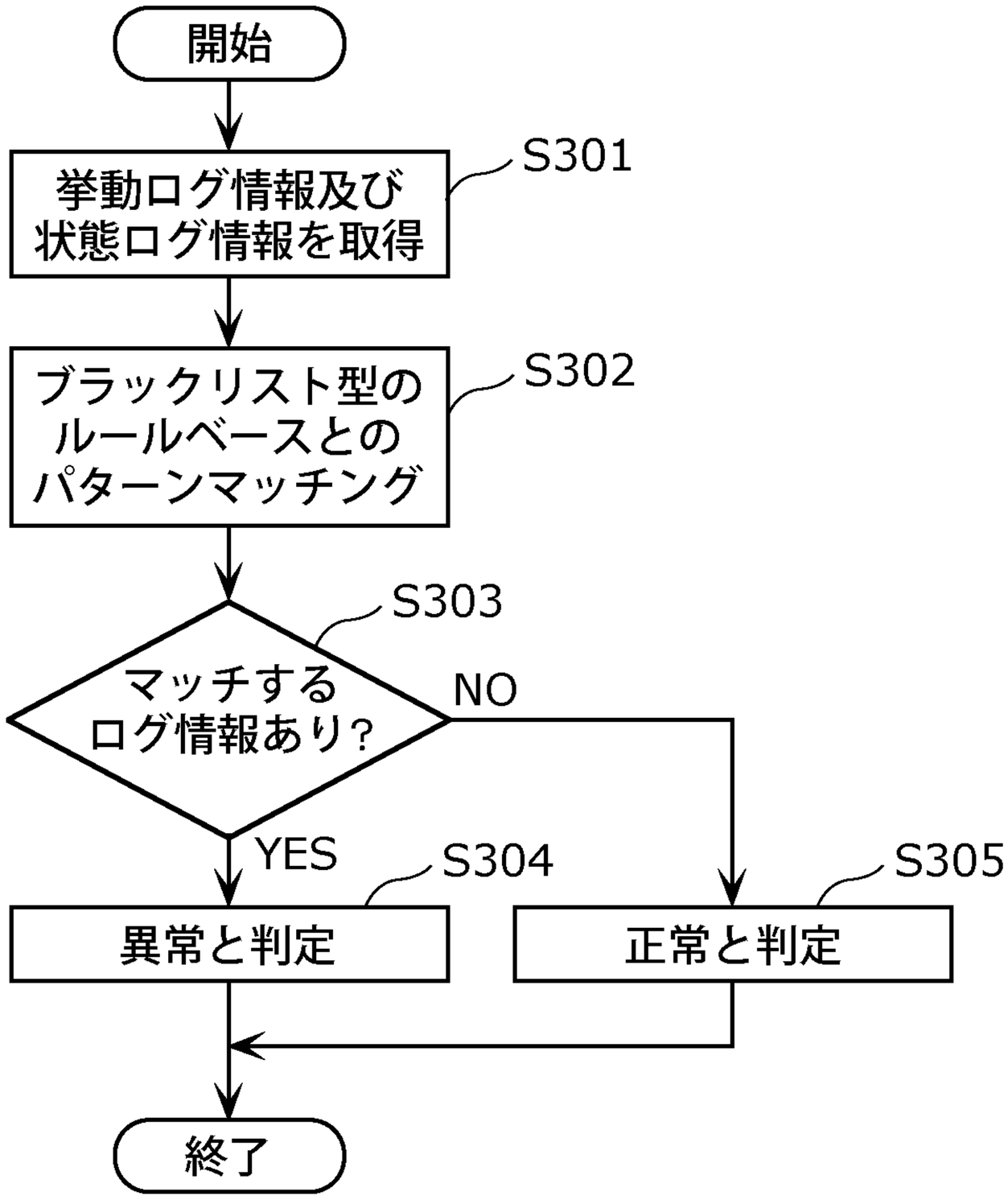
(b)

ルール	正常挙動ログ情報				正常状態ログ情報		
タイムスタンプ	プロセスID	フックポインタ名称	フックポインタ属性1	フックポインタ属性2	車速[km/h]	加速度[m/s²]	操舵角[度]
<20	-	task_create	-	-	0	-	-
<20	-	file_permission	fileA	read	0	-	-
<20	-	mmap_addr	addr1	-	0	-	-
<20	-	file_ioctl	通信機器	データ送信	0	-	-
<20	-	task_free	-	-	0	-	-

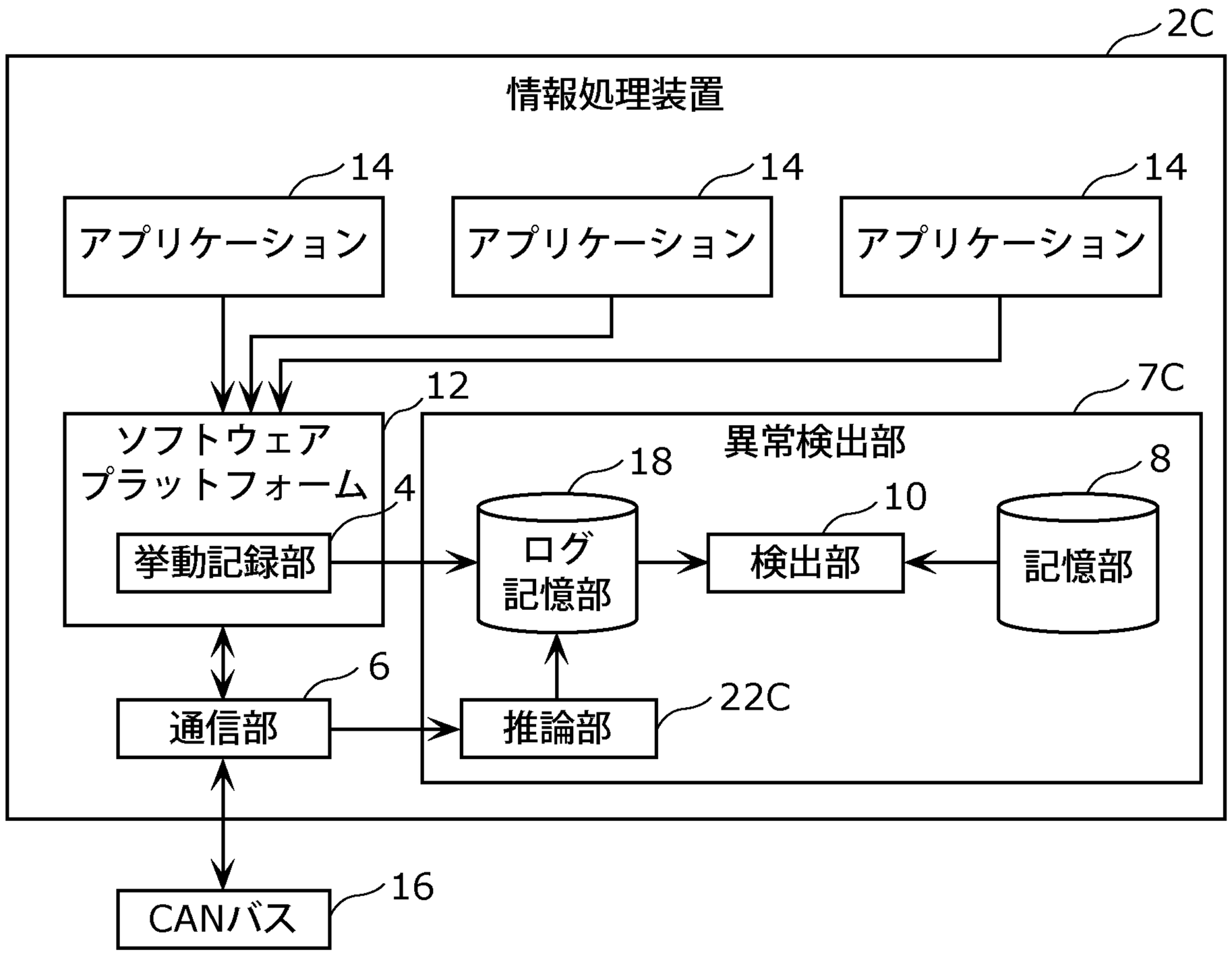
[図12]


2B
情報処理装置
14
アプリケーション
14
アプリケーション
14
アプリケーション
12
ソフトウェア
プラットフォーム
4
挙動記録部
7B
異常検出部
18
ログ
記憶部
8B
記憶部
10B
検出部
6
通信部
22
推論部
CANバス
16

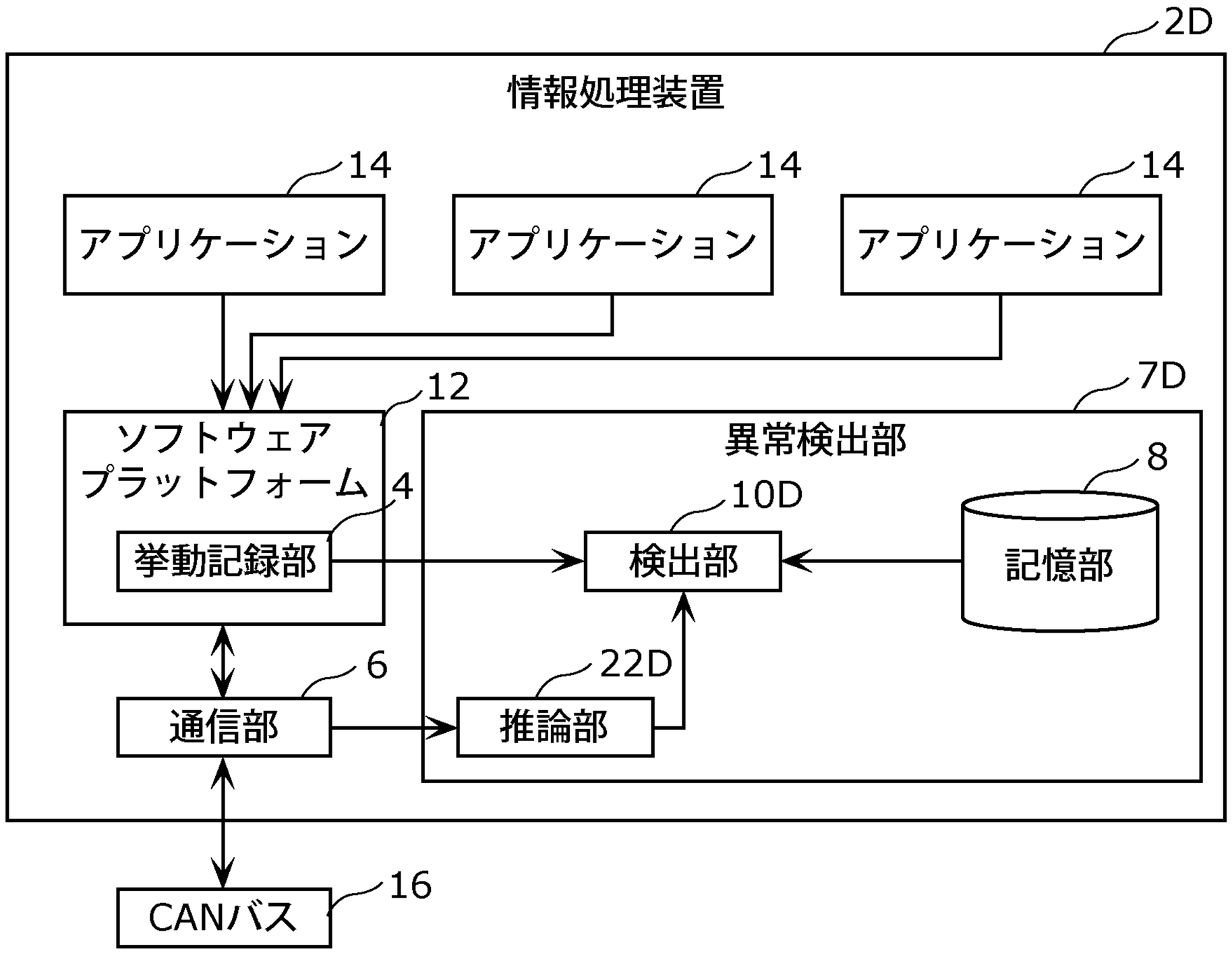
[図13]


開始
挙動ログ情報及び
状態ログ情報を取得
S301
ブラックリスト型の
ルールベースとの
パターンマッチング
S302
S303
マッチする
ログ情報あり？
NO
YES
S304
異常と判定
S305
正常と判定
終了

[図14]


2C
情報処理装置
14
アプリケーション
14
アプリケーション
14
アプリケーション
12
ソフトウェア
プラットフォーム
4
挙動記録部
7C
異常検出部
18
ログ
記憶部
10
検出部
8
記憶部
6
通信部
22C
推論部
16
CANバス

[図15]


2D
情報処理装置
14
アプリケーション
14
アプリケーション
14
アプリケーション
12
ソフトウェア
プラットフォーム
4
挙動記録部
7D
異常検出部
10D
検出部
8
記憶部
6
通信部
22D
推論部
16
CANバス

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2020/032015

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl. G06F11/07(2006.01)i, G05B23/02(2006.01)i
FI: G06F11/07151, G05B23/02302K, G06F11/07140R

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)
Int.Cl. G06F11/07, G05B23/02, B60R16/02

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Published examined utility model applications of Japan 1922-1996
Published unexamined utility model applications of Japan 1971-2020
Registered utility model specifications of Japan 1996-2020
Published registered utility model applications of Japan 1994-2020

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y A	WO 2017/081985 A1 (HITACHI AUTOMOTIVE SYSTEMS LTD.) 18 May 2017 (2017-05-18), abstract, paragraphs [0044]-[0048]	1, 8-10 2-7
Y A	JP 2015-88948 A (NISSAN MOTOR CO., LTD.) 07 May 2015 (2015-05-07), paragraphs [0009], [0010], [0030], [0031]	1, 8-10 2-7
A	JP 2012-22380 A (KDDI CORPORATION) 02 February 2012 (2012-02-02), abstract, paragraphs [0040], [0041]	7
P, X	WO 2020/075800 A1 (NIPPON TELEGRAPH AND TELEPHONE CORPORATION) 16 April 2020 (2020-04-16), paragraphs [0023]-[0035]	1-3, 8-10

☐ 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
05 November 2020	17 November 2020
Name and mailing address of the ISA/ Japan Patent Office 3-4-3, Kasumigaseki, Chiyoda-ku, Tokyo 100-8915, Japan	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/JP2020/032015

WO 2017/081985 A1	18 May 2017	JP 2017-91234 A	
JP 2015-88948 A	07 May 2015	(Family: none)	
JP 2012-22380 A	02 February 2012	(Family: none)	
WO 2020/075800 A1	16 April 2020	(Family: none)	

国際調査報告

国際出願番号 PCT/JP2020/032015

A. 発明の属する分野の分類（国際特許分類（ＩＰＣ））

G06F 11/07(2006.01)i; G05B 23/02(2006.01)i
FI: G06F11/07 151; G05B23/02 302K; G06F11/07 140R

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））

G06F11/07; G05B23/02; B60R16/02

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２０２０年
日本国実用新案登録公報	１９９６－２０２０年
日本国登録実用新案公報	１９９４－２０２０年

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

C. 関連すると認められる文献

引用文献のカテゴリー*	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求項の番号
Y	WO 2017/081985 A1（日立オートモティブシステムズ株式会社）18.05.2017（2017-05-18） [要約]及び段落[0044]-[0048]	1，8-10
A		2-7
Y	JP 2015-88948 A（日産自動車株式会社）07.05.2015（2015-05-07） 段落[0009]-[0010]及び[0030]-[0031]	1，8-10
A		2-7
A	JP 2012-22380 A（ＫＤＤＩ株式会社）02.02.2012（2012-02-02） [要約]及び段落[0040]-[0041]	7
P，X	WO 2020/075800 A1（日本電信電話株式会社）16.04.2020（2020-04-16） 段落[0023]-[0035]	1-3，8-10

☐ C欄の続きにも文献が列挙されている。

☑ パテントファミリーに関する別紙を参照。

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

国際調査を完了した日	国際調査報告の発送日
05.11.2020	17.11.2020

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

権限のある職員（特許庁審査官）
渡部　博樹 5B 1599
電話番号 03-3581-1101 内線 3545

国際調査報告
パテントファミリーに関する情報

国際出願番号
PCT/JP2020/032015

引用文献			公表日	パテントファミリー文献			公表日
WO	2017/081985	A1	18.05.2017	JP	2017-91234	A	
JP	2015-88948	A	07.05.2015	（ファミリーなし）			
JP	2012-22380	A	02.02.2012	（ファミリーなし）			
WO	2020/075800	A1	16.04.2020	（ファミリーなし）			