

(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5月27日(27.05.2021)



(10) 国際公開番号

WO 2021/100527 A1

(51) 国際特許分類:

B60R 16/023 (2006.01) G06F 21/57 (2013.01)
G06F 9/4401 (2018.01)

(21) 国際出願番号: PCT/JP2020/041785

(22) 国際出願日: 2020年11月9日(09.11.2020)

(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 2019-208977 2019年11月19日(19.11.2019) JP

(71) 出願人: 日立 Astemo 株式会社(HITACHI
ASTEMO, LTD.) [JP/JP]; 〒3128503 茨城県ひ
たちなか市高場 2 5 2 0 番地 Ibaraki (JP).

(72) 発明者: 粕谷 桃伽 (KASUYA, Momoka);

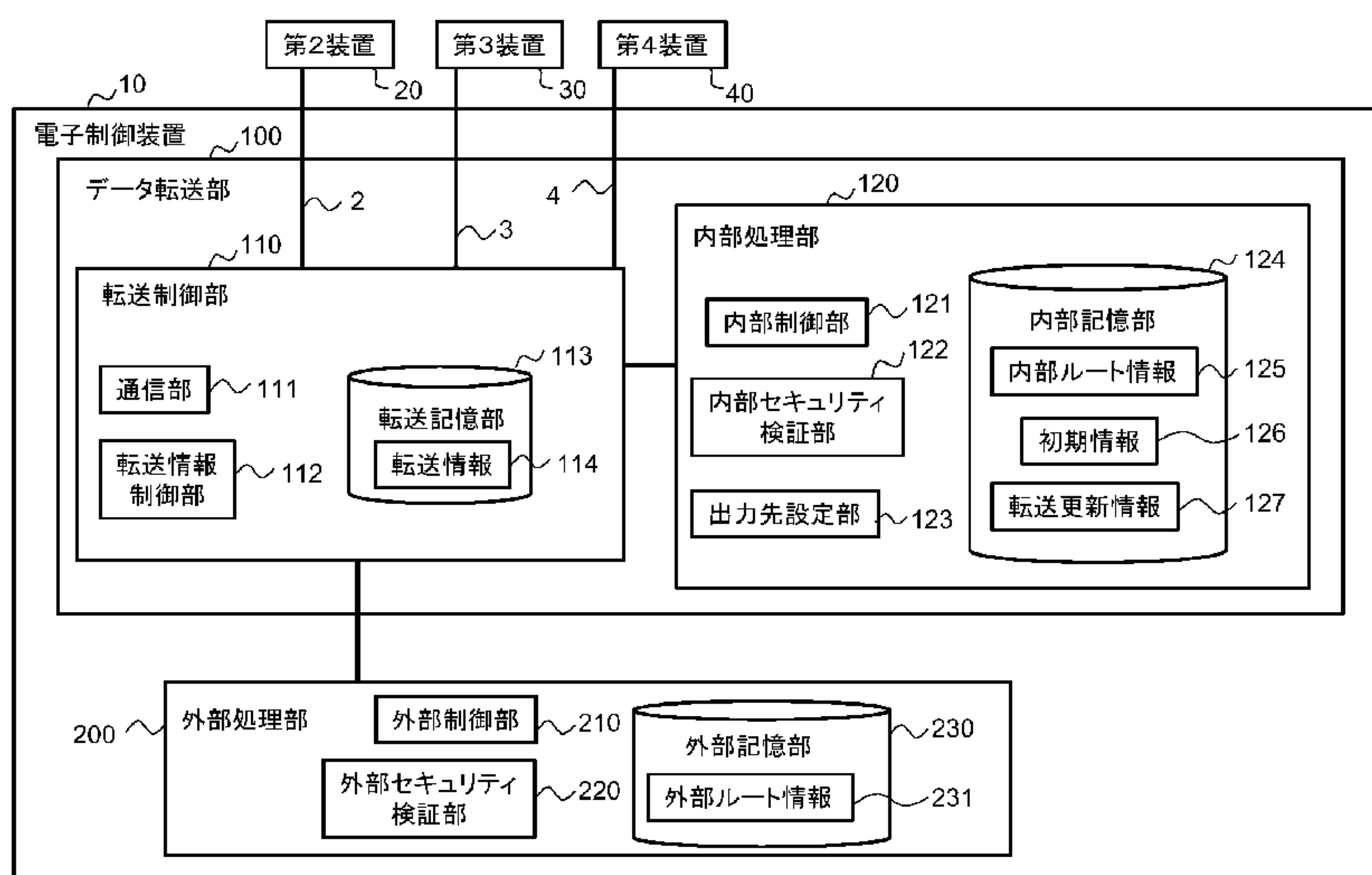
〒1008280 東京都千代田区丸の内一丁目 6 番
6 号 株式会社日立製作所内 Tokyo (JP). 山
▲崎▼ 裕紀(YAMAZAKI, Hiroki); 〒1008280
東京都千代田区丸の内一丁目 6 番 6 号 株
式会社日立製作所内 Tokyo (JP). 森田 伸義
(MORITA, Nobuyoshi); 〒3128503 茨城県ひた
ちなか市高場 2 5 2 0 番地 日立オートモティ
ブシステムズ株式会社内 Ibaraki (JP). 金子 周
平(KANEKO, Shuhei); 〒3128503 茨城県ひたち
な市高場 2 5 2 0 番地 日立オートモティ
ブシステムズ株式会社内 Ibaraki (JP).

(74) 代理人: 特許業務法人サンネクスト国際特許
事務所(SUNNEXT INTERNATIONAL PATENT
OFFICE); 〒1400002 東京都品川区東品川二丁

(54) Title: ELECTRONIC CONTROL DEVICE, AND COMPUTATION METHOD

(54) 発明の名称: 電子制御装置、演算方法

[図1]



10 Electronic control device
20 Second device
30 Third device
40 Fourth device
100 Data transfer unit
110 Transfer control unit
111 Communication unit
112 Transfer information control unit
113 Transfer storage unit
114 Transfer information
120 Internal processing unit
121 Internal control unit
122 Internal security verification unit
123 Output destination setting unit
124 Internal storage unit
125 Internal route information
126 Initial information
127 Transfer update information
200 External processing unit
210 External control unit
220 External security verification unit
230 External storage unit
231 External route information

(57) Abstract: This electronic control device comprises: a first processing unit; a second processing unit; and a transfer control unit. The second processing unit requires a longer time for startup processing than the first processing unit, and the transfer control unit is provided with a communication unit that can transfer communication data received from outside to the first processing unit and the second processing unit. The first processing unit is provided with a first control unit that processes the communication data transferred from the transfer control unit, and the second processing unit is provided with a second control unit that processes the communication data transferred from the transfer control unit. Until the startup

[続葉有]

目 3 番 1 2 号 シーフォートスクエア センタ
ービルディング 1 6 階 Tokyo (JP).

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

processing of the second processing unit is completed, the transfer control unit does not set the second processing unit as a transfer destination for the communication data and instead includes the first processing unit as a transfer destination, and when the startup processing of the second processing unit is completed, the transfer control unit sets at least the second processing unit as a transfer destination for the communication data.

(57) 要約 : 電子制御装置は、第 1 処理部、第 2 処理部、および転送制御部を備え、第 1 処理部よりも第 2 処理部は起動処理に長い時間を要し、転送制御部は、外部から受信する通信データを第 1 処理部および第 2 処理部に転送可能な通信部を備え、第 1 処理部は、転送制御部から転送される通信データを処理する第 1 制御部を備え、第 2 処理部は、転送制御部から転送される通信データを処理する第 2 制御部を備え、転送制御部は、第 2 処理部の起動処理が完了するまでは第 2 処理部を通信データの転送先とせず第 1 処理部を転送先に含め、第 2 処理部の起動処理が完了すると少なくとも第 2 処理部を通信データの転送先とする。

明 細 書

発明の名称：電子制御装置、演算方法

技術分野

[0001] 本発明は、電子制御装置および演算方法に関する。

背景技術

[0002] 車載ネットワークがインターネットや無線LANなどの外部ネットワークに接続され、ユーザーの利便性が向上した反面、車外からのサイバー攻撃によって電子制御装置が乗っ取られる危険性が指摘されている。そのため、自動車が安全であることを証明するために、自動車の起動時に、自動車内のプログラムが改竄されないことを確認した上で、機能を動作させることが望まれる。また、ユーザーの利便性の観点から早期に機能を稼働させることが望まれている。プログラムの安全性を検証する方法として、事前に作成された署名値と現在のプログラムから作成した署名値が一致するか比較する方法が一般的に知られ、安全性を検証した上でプログラムを起動させる方法はセキュアブートと呼ばれる。このセキュアブートを行うことにより、従前よりも起動に長い時間を要することが避けられない。特許文献1には、コンピューターが、システムのプログラム起動毎に、前記プログラムを複数に区分した部分プログラムのうち、ハッシュ値の検証対象となる異なる部分プログラムを選択する選択工程と、前記選択した部分プログラムのハッシュ値を算出する算出工程と、前記算出したハッシュ値が、複数の前記部分プログラムそれぞれの正解のハッシュ値である正解部分ハッシュ値と一致するか否か判定し、一致する場合に前記システムの起動処理を継続し、一致しない場合に前記システムの起動処理を中断する検証工程と、を実行することを特徴とするセキュアブート方法が開示されている。

先行技術文献

特許文献

[0003] 特許文献1：日本国特開2015-022521号公報

発明の概要

発明が解決しようとする課題

[0004] 特許文献 1 に記載されている発明では、起動処理が完了する前は通信データを処理できない。

課題を解決するための手段

[0005] 本発明の第 1 の態様による電子制御装置は、第 1 処理部、第 2 処理部、および転送制御部を備える電子制御装置であって、前記第 1 処理部よりも前記第 2 処理部は起動処理に長い時間を要し、前記転送制御部は、外部から受信する通信データを前記第 1 処理部および前記第 2 処理部に転送可能な通信部を備え、前記第 1 処理部は、前記転送制御部から転送される前記通信データを処理する第 1 制御部を備え、前記第 2 処理部は、前記転送制御部から転送される前記通信データを処理する第 2 制御部を備え、前記転送制御部は、前記第 2 処理部の起動処理が完了するまでは前記第 2 処理部を前記通信データの転送先とせず前記第 1 処理部を転送先に含め、前記第 2 処理部の起動処理が完了すると少なくとも前記第 2 処理部を前記通信データの転送先とする。

本発明の第 2 の態様による演算方法は、第 1 処理部、第 2 処理部、および転送制御部を備える電子制御装置が実行する演算方法であって、前記第 1 処理部よりも前記第 2 処理部は起動処理に長い時間を要し、前記転送制御部は、外部から受信する通信データを前記第 1 処理部および前記第 2 処理部に転送可能であり、前記第 1 処理部が、前記転送制御部から転送される前記通信データを処理することと、前記第 2 処理部は、前記転送制御部から転送される前記通信データを処理することと、前記転送制御部は、前記第 2 処理部の起動処理が完了するまでは前記第 2 処理部を前記通信データの転送先とせず前記第 1 処理部を転送先に含め、前記第 2 処理部の起動処理が完了すると少なくとも前記第 2 処理部を前記通信データの転送先とすることを含む。

発明の効果

[0006] 本発明によれば、起動処理が完了する前でも受信した通信データを処理で

きる。

図面の簡単な説明

- [0007] [図1]第1の実施の形態における電子制御装置の構成図
[図2]第1の実施の形態における電子制御装置のシーケンス図
[図3]内部処理部の処理を示すフローチャート
[図4]転送情報の例を示す図
[図5]転送更新情報の一例を示す図
[図6]内部ルート情報の一例を示す図
[図7]外部ルート情報の一例を示す図
[図8]第2の実施の形態における電子制御装置の構成図
[図9]第2の実施の形態における電子制御装置のシーケンス図
[図10]第2の実施の形態における内部処理部の処理を示すフローチャート
[図11]第3の実施の形態における電子制御装置の構成図
[図12]第3の実施の形態における電子制御装置のシーケンス図
[図13]第4の実施の形態における電子制御装置の構成図
[図14]第4の実施の形態における電子制御装置のシーケンス図

発明を実施するための形態

- [0008] ー第1の実施の形態ー

以下、図1～図7を参照して、電子制御装置の第1の実施の形態を説明する。

- [0009] 図1は、第1の実施の形態における電子制御装置10の構成図である。電子制御装置10はデータ転送部100と外部処理部200とを備える。データ転送部100は転送制御部110と内部処理部120を備える。転送制御部110は通信部111、転送情報制御部112、および転送記憶部113を備える。転送記憶部113には転送情報114が格納される。また、内部処理部120は、内部制御部121、内部セキュリティ検証部122、出力先設定部123、および内部記憶部124を備える。内部記憶部124には、内部ルート情報125、初期情報126、および転送更新情報127が格

納される。

[0010] 外部処理部 200 は、外部制御部 210、外部セキュリティ検証部 220、および外部記憶部 230 を備える。外部記憶部 230 には外部ルート情報 231 が格納される。なお以下では、外部処理部 200 を「第 1 処理部」と呼ぶことがあり、外部セキュリティ検証部 220 を「第 1 セキュリティ検証部」と呼ぶことがある。また内部処理部 120 を「第 2 処理部」と呼ぶことがあり、内部セキュリティ検証部 122 を「第 2 セキュリティ検証部」と呼ぶことがある。

[0011] 電子制御装置 10 は、内部制御部 121、出力先設定部 123、および外部制御部 210 を、次のように実現する。すなわち電子制御装置 10 は、不図示の中央演算装置である CPU が、不図示の書き換え可能な記憶領域に記録されたプログラムを不図示の RAM (Random Access Memory) に展開して実行することにより、内部制御部 121、出力先設定部 123、および外部制御部 210 を実現する。このことは、内部制御部 121、出力先設定部 123、および外部制御部 210 は、第三者により改竄される可能性が存在することを意味する。そのため第 1 セキュリティ検証部や第 2 セキュリティ検証部を用いて、これらの機能ブロックを実現するプログラムを起動前に確認する必要がある。

[0012] 電子制御装置 10 は、転送制御部 110 が備える不図示の複数の通信ポートを介して通信バス 2、3、4 と接続している。また、通信バス 2 は第 2 装置 20 に接続され、通信バス 3 は第 3 装置 30 に接続され、通信バス 4 は第 4 装置 40 に接続される。以下では、第 2 装置 20、第 3 装置 30、および第 4 装置 40 をまとめて「各装置」と呼ぶことがある。

[0013] ここで、電子制御装置 10 の各機能構成を説明する前に、電子制御装置 10 の想定される接続構成を説明する。電子制御装置 10 は、データリンク層またはネットワーク層におけるスイッチ、いわゆる L2 スイッチまたは L3 スイッチである。第 2 装置 20、第 3 装置 30、および第 4 装置 40 は、ある 1 台の車両に搭載される ECU (Electronic Control Unit; 電子制御装

置) またはゲートウェイ装置である。通信バス 2、3、4 の通信規格は特に限定されないが、たとえば C A N (登録商標)、L I N (登録商標)、および I E E E 8 0 2 . 3 などを用いることができる。通信バスは第 2 装置 2 0 だけではなく、その他の電子制御装置に接続され、バス型やスター型のネットワークを構築してもよい。以下では、一例として通信バス 2、3、4 に I E E E 8 0 2 . 3 が利用されているものとして説明する。

[0014] 本実施の形態では、各装置が通信バスに出力するデジタル信号を「通信データ」と呼ぶ。通信データの具体的な名称は通信プロトコルにより異なるが、たとえばフレーム、データグラム、パケットなどが通信データに相当する。

[0015] 次に、図 1 に示した電子制御装置 1 0 の各機能を説明する。電子制御装置 1 0 は、第 2 装置 2 0、第 3 装置 3 0、および第 4 装置 4 0 から送信された通信データを適切な装置に転送する機能を有する。以下に説明するように、転送制御部 1 1 0、内部処理部 1 2 0、および外部処理部 2 0 0 のいずれが通信データの転送における主たる役割を担うかは、状況や通信データの内容により異なる。

[0016] 転送制御部 1 1 0 は、通信部 1 1 1、転送情報制御部 1 1 2、および転送記憶部 1 1 3 を備える。転送制御部 1 1 0 は、ある通信ポートにおいて受信した通信データを他の通信ポートに転送する。ただし転送先の通信ポートの決定は、転送制御部 1 1 0 が行う場合もあるが、内部処理部 1 2 0 や外部処理部 2 0 0 が行う場合もある。通信部 1 1 1 および転送情報制御部 1 1 2 はハードウェア回路で構成されており、改竄の危険性がない。内部処理部 1 2 0 や外部処理部 2 0 0 とは異なり、起動時に通信部 1 1 1 および転送情報制御部 1 1 2 の安全性を確認する必要がない。

[0017] 通信部 1 1 1 は、第 2 装置 2 0、第 3 装置 3 0、第 4 装置 4 0、内部処理部 1 2 0、および外部処理部 2 0 0 からの通信データを送受信する。受信した通信データの転送先は転送情報制御部 1 1 2 から指示される。転送情報制御部 1 1 2 は、通信部 1 1 1 で受信した通信データの転送先を転送情報 1 1

4を参照して決定し、通信部111に受信した通信データの転送先を指示する。転送記憶部113は、揮発性または不揮発性の記憶領域である。

[0018] 転送情報114は、受信した通信データの転送先に関するデータが格納されている。後述するように、転送情報114は内部処理部120の出力先設定部123により書き換えられる。本実施の形態における転送先は、内部処理部120、外部処理部200、第2装置20、第3装置30、および第4装置40がある。転送情報114のデータ構造は、後に図4を参照して説明する。

[0019] 内部処理部120は、受信した通信データの転送先を書き換える機能を有する。たとえば内部処理部120は、スイッチの内部プロセッサ上に実装される。内部制御部121、および出力先設定部123は、不揮発性の記憶領域、たとえば内部記憶部124に格納されたプログラムをCPUがRAMに展開して実行することにより実現される。内部セキュリティ検証部122はハードウェア回路により実現、またはROMやOTP (One Time Program) 領域などの書換え不可能な領域に格納されたプログラムをRAMに読み込むことにより実現される。

[0020] 内部制御部121は、内部ルート情報125に基づいて、受信した通信データの通信ヘッダに記載されている転送先を書き換え、転送制御部110に通信データを送信する。内部セキュリティ検証部122は、内部処理部120に保存されているプログラムやデータが改竄されていないことを確認する機能を有する。なお内部処理部120のプログラムやデータは、プログラムの起動前やデータの読み込み前に内部セキュリティ検証部122で改竄の有無が確認され、安全性が確認された後に用いられる。内部セキュリティ検証部122はたとえば、内部制御部121を実現するためのプログラムのハッシュ値を計算し、その署名値が予め記録されている値と一致する場合には改竄なしと判断し、ハッシュ値が一致しない場合には改竄ありと判断する。ただし、事前に作成されたハッシュ値はHSM (Hardware Security Module) のような読み出し専用メモリに格納する必要がある。

- [0021] 出力先設定部 1 2 3 は転送制御部 1 1 0 の転送記憶部 1 1 3 への書き込みを行い、転送情報 1 1 4 の作成および更新を行う。転送情報 1 1 4 の作成及び更新には、内部記憶部 1 2 4 に格納される初期情報 1 2 6 および転送更新情報 1 2 7 が用いられる。内部記憶部 1 2 4 は、揮発性、または不揮発性の記憶領域である。内部記憶部 1 2 4 が揮発性の場合には、不図示の不揮発性の記憶領域に格納される内部ルート情報 1 2 5、初期情報 1 2 6、および転送更新情報 1 2 7 が電子制御装置 1 0 の起動の際に内部記憶部 1 2 4 に読み込まれる。
- [0022] 内部ルート情報 1 2 5 は、内部制御部 1 2 1 により通信データの転送先の書換えに用いられる。初期情報 1 2 6 は、通信データの転送先に関する情報である。初期情報 1 2 6 は、出力先設定部 1 2 3 を通じて転送記憶部 1 1 3 に書き込まれる。これにより後述するように転送情報 1 1 4 が作成される。初期情報 1 2 6 は、転送情報 1 1 4 と同じデータ構造をとる。転送更新情報 1 2 7 は、通信データの転送先の書換えに必要なデータが格納されており、転送情報 1 1 4 の更新に用いられる。
- [0023] 外部処理部 2 0 0 は、内部処理部 1 2 0 と同様に、受信した通信データの転送先を書き換える。外部処理部 2 0 0 はマイコン上に実装され、内部処理部 1 2 0 と比較すると小規模である。そのため外部処理部 2 0 0 は内部処理部 1 2 0 に比べて処理能力は低いが内部処理部 1 2 0 よりも早く起動処理が完了する。外部制御部 2 1 0 は、外部ルート情報 2 3 1 に基づいて、受信した通信データの通信ヘッダに記載されている転送先を書換え、転送制御部 1 1 0 に通信データを送信する。
- [0024] 外部セキュリティ検証部 2 2 0 は、内部セキュリティ検証部 1 2 2 と同様の機能を持ち、外部処理部 2 0 0 に保存されているプログラムやデータが改竄されていないことを確認する機能を有する。なお以下では、外部セキュリティ検証部 2 2 0 や内部セキュリティ検証部 1 2 2 がプログラムおよびデータの改竄がされていないことを確認して使用可能な状態にすることを「セキュアブート」とも呼ぶ。外部ルート情報 2 3 1 は、受信した通信データの転

送先の書換えに必要な情報である。外部ルート情報 2 3 1 は、内部ルート情報 1 2 5 と同様の構造を有する。

[0025] 図 2 は電子制御装置 1 0 の処理の流れを説明するシーケンス図である。図 2 で示す処理は電子制御装置 1 0 で実行されるものである。内部処理部 1 2 0 の起動処理は 2 段階に分かれており、前半を「第 1 起動処理」と呼び、後半を「第 2 起動処理」と呼ぶ。まず、ステップ S 3 0 0 では、電子制御装置 1 0 の電源がオンにされ、内部処理部 1 2 0、外部処理部 2 0 0、および転送制御部 1 1 0 に電気が供給される。なお図 2 の左端には、電子制御装置 1 0 が通信データを処理する処理能力の時系列変化を示している。この処理能力は、図示横方向の幅が広いほど処理能力が高いことを示している。

[0026] ステップ S 3 0 1 では、外部セキュリティ検証部 2 2 0 が、外部処理部 2 0 0 のプログラムやデータが改竄されていないか検証する。外部セキュリティ検証部 2 2 0 による検証が完了すると、外部処理部 2 0 0 はステップ S 3 0 2 に移行し、プログラムを起動させることで、通信データの転送処理が可能な状態、すなわちルーティング受付状態に遷移する。ルーティング受付状態では、通信データを受信すると、外部制御部 2 1 0 が外部ルート情報 2 3 1 に基づいて、通信ヘッダの転送先を書き換えて転送制御部 1 1 0 の通信部 1 1 1 に送信することで、通信データを他の装置へ転送させる。

[0027] 内部処理部 1 2 0 の第 1 起動処理であるステップ S 3 0 3 では、内部処理部 1 2 0 の全体ではなく、転送制御部 1 1 0 の転送情報 1 1 4 の設定に関するプログラムやデータを内部セキュリティ検証部 1 2 2 で安全性検証をして起動させる。具体的には、内部処理部 1 2 0 の出力先設定部 1 2 3 と初期情報 1 2 6 をセキュアブートさせる。内部処理部 1 2 0 は、出力先設定部 1 2 3 および初期情報 1 2 6 が使用可能になると、ステップ S 3 0 4 に進む。

[0028] ステップ S 3 0 4 では、出力先設定部 1 2 3 が初期情報 1 2 6 を転送制御部 1 1 0 の転送記憶部 1 1 3 に書き込みを行い、転送情報 1 1 4 を生成する。ステップ S 3 0 4 で生成される転送情報 1 1 4 は、転送先の 1 つに外部処理部 2 0 0 が設定されており、転送制御部 1 1 0 で受信した通信データを外

部処理部 200 に転送できるようになる。外部処理部 200 はルーティング受付状態であることから、ルーティング機能を稼働させる。なおステップ S304 で生成される転送情報 114 では、転送先に内部処理部 120 は含まれない。

[0029] 内部処理部 120 は、出力先設定部 123 による転送記憶部 113 への書き込みが終了するとステップ S305 に進む。内部処理部 120 の第 2 起動処理であるステップ S305 では内部セキュリティ検証部 122 は、前述のステップ S303 でセキュアブートしなかった残りのプログラムおよびデータを対象として、セキュアブートを行う。具体的には、内部セキュリティ検証部 122 は内部制御部 121、内部ルート情報 125、転送更新情報 127 を対象としてセキュアブートを行う。これらのセキュアブートが完了するとステップ S306 に進む。

[0030] 内部処理部 120 はステップ S306 では、出力先設定部 123 が転送更新情報 127 を転送記憶部 113 に書き込むことで転送情報 114 を更新する。この更新により転送情報 114 の転送先に内部処理部 120 が含まれるようになる。ステップ S307 では、内部処理部 120 は、通信データの転送処理が可能な状態、すなわちルーティング受付状態に遷移し、転送制御部 110 から受信した通信データを転送情報 114 に従って転送させる。

[0031] 図 2 の左端に示す電子制御装置 10 の処理能力の時系列変化を説明する。ステップ S304 が完了するまでは通信データの処理ができないので処理能力はゼロである。ステップ S304 が完了すると、転送制御部 110 および外部処理部 200 による通信データの処理が可能となる。そしてステップ S306 が完了すると転送制御部 110、外部処理部 200 および内部処理部 120 による通信データの処理が可能となるので処理能力が増強される。

[0032] 図 3 は内部処理部 120 の詳細な処理手順を示すフローチャートである。内部処理部 120 に電源が入力されると、ステップ S400 が開始される。ステップ S400 では、内部セキュリティ検証部 122 がセキュアブートを実行し、転送制御部 110 の転送情報 114 への書き込みに関連する機能が

改竄されていないことを確認する。具体的には、内部処理部 1 2 0 の出力先設定部 1 2 3 および初期情報 1 2 6 をセキュアブートする。

[0033] 続くステップ S 4 0 1 では内部処理部 1 2 0 は、ステップ S 4 0 0 で実施したセキュアブートが成功し、起動できたか否かを確認する。内部処理部 1 2 0 は、セキュアブートが失敗したと判断する場合は、ステップ S 4 0 2 に移行し、処理を停止して図 3 の処理を終了する。内部処理部 1 2 0 はセキュアブートが成功したと判断すると、ステップ S 4 0 3 に移行する。

[0034] ステップ S 4 0 3 では内部処理部 1 2 0 は、外部処理部 2 0 0 のセキュアブートが完了し、すでにルーティング受付状態であるかを確認する。なおこのステップは、内部処理部 1 2 0 のセキュアブートが完了するよりも短時間で外部処理部 2 0 0 のセキュアブートが完了していることが既知の場合や、より短時間で転送機能を起動させたい場合など、状況によりスキップしてもよい。内部処理部 1 2 0 は、外部処理部 2 0 0 がルーティング受付状態であると判断する場合はステップ S 4 0 4 に進む。内部処理部 1 2 0 は、外部処理部 2 0 0 がルーティング受付状態にないと判断する場合は、ステップ S 4 0 2 に移行し、処理を停止して図 3 の処理を終了する。

[0035] ステップ S 4 0 4 では、出力先設定部 1 2 3 が転送制御部 1 1 0 の転送記憶部 1 1 3 に初期情報 1 2 6 の情報を書き込むことで転送情報 1 1 4 を作成する。転送情報 1 1 4 の作成が完了すると、転送制御部 1 1 0 が受信した通信データは外部処理部 2 0 0 に転送可能となる。したがって、転送機能はステップ S 4 0 4 が完了した時点で既に稼動している。

[0036] 続くステップ S 4 0 5 では内部セキュリティ検証部 1 2 2 は、ステップ S 4 0 0 において安全性を検証しなかった内部処理部 1 2 0 の残りのプログラムおよびデータを対象にセキュアブートを実行する。具体的には、内部制御部 1 2 1、内部ルート情報 1 2 5 および転送更新情報 1 2 7 をセキュアブートさせる。

[0037] 続くステップ S 4 0 6 では内部処理部 1 2 0 は、ステップ S 4 0 5 において実施したセキュアブートが成功したか否かを確認する。内部処理部 1 2 0

はセキュアブートに成功したと判断する場合はステップS 4 0 7に進み、セキュアブートに失敗したと判断する場合はステップS 4 0 2に移行し、処理を停止して図3の処理を終了する。

[0038] ステップS 4 0 7では出力先設定部1 2 3が、出力先設定部1 2 3が転送制御部1 1 0の転送記憶部1 1 3に転送更新情報1 2 7の情報を書き込むことで転送情報1 1 4を更新する。続くステップS 4 0 8では、内部処理部1 2 0がルーティング受付状態になり、転送制御部1 1 0で受信した通信データの処理が可能になり、図3に示す処理が終了する。

[0039] 図4は、転送情報1 1 4の一例を示す図である。図4 (a)は、図2のステップS 3 0 4や図3のステップS 4 0 4の処理により作成される転送情報1 1 4である。図4 (b)は、図2のステップS 3 0 6や図3のステップS 4 0 7により作成される転送情報1 1 4である。以下では、図4 (a)に示す転送情報1 1 4を「更新前」の転送情報1 1 4と呼び、図4 (b)に示す転送情報1 1 4を「更新後」の転送情報1 1 4と呼ぶ。

[0040] 転送情報1 1 4は、MACアドレス1 1 3 0および転送先1 1 3 1から構成される。MACアドレス1 1 3 0は受信した通信データを識別し、登録されている転送先を調査するために使用される。転送先1 1 3 1には、受信した通信データの転送先が記載されている。たとえば、内部処理部1 2 0、外部処理部2 0 0、および第2装置2 0や第3装置3 0に接続されるポート番号が記載される。

[0041] 転送情報1 1 4の更新前に受信した通信データは、内部処理部1 2 0には転送されず、いずれかの装置、また外部処理部2 0 0に転送される。これは、内部処理部1 2 0の転送機能の起動が完了していないので、内部処理部1 2 0への転送を避ける意図で更新前の転送情報1 1 4が作成されているためである。転送制御部1 1 0が内部処理部1 2 0、および外部処理部2 0 0から受信した通信データは通信ヘッダに含まれる転送先MACアドレスが書換えられている。そのため転送情報制御部1 1 2は、転送情報1 1 4を再び参照して転送先を検索し、該当する転送先に送信する。

[0042] なお図4では、通信データの識別のためにMACアドレス1130を用いる例を示したが、通信データの転送先を判別可能な値であれば他の値を使用してもよい。たとえば、MACアドレス1130の一部の値を使用したり、IPアドレスやその一部を使用したりすることによって転送先を判別してもよい。

[0043] 図5は、転送更新情報127の一例を示す図である。転送更新情報127は、転送情報114の更新部分、たとえば図4(a)と図4(b)の差分である。出力先設定部123は、転送記憶部113に格納される転送情報114を参照し、転送更新情報127のMACアドレスが一致した場合に転送先1131に格納されている情報を転送先1261の情報に更新する。図5の例では、MACアドレス「00:01:02:03:05」の転送先が内部処理部120に更新される。図4(b)に示す更新後の転送情報114では、通信データの処理負荷分散のため、更新後に外部処理部200と内部処理部120とで分散して処理している。ただし更新後は、外部処理部200は通信データの転送処理を行わず、内部処理部120がすべての通信データを処理してもよい。

[0044] 図6は、内部ルート情報125の一例を示す図である。内部ルート情報125は、IPアドレス1240と転送用MACアドレス1241から構成される。内部制御部121は内部ルート情報125を参照し、受信した通信データのヘッダに含まれるIPアドレスから転送先のMACアドレスを検索し、検索したMACアドレスにヘッダ情報を書換え、転送制御部110に送信する。たとえば、MACアドレスが「00:01:02:03:04:05」でIPアドレスが「255.255.1.3」の通信データを受信した場合、データベースから転送先MACアドレスを検索し、通信ヘッダを「00:01:02:03:04:05」から「1A:2B:3C:4D:5E:6F」に書き換える。

[0045] 図7は、外部ルート情報231の一例を示す図である。外部ルート情報231のデータの構造は図6の内部ルート情報125と同一である。外部処理

部 2 0 0 は、内部処理部 1 2 0 が稼動する前に受信した通信データに対しても、通信データの転送先 M A C アドレスの書換えを実施する必要があるため、外部ルート情報 2 3 1 は内部ルート情報 1 2 5 よりもデータ量が多い。

[0046] 上述した第 1 の実施の形態によれば、次の作用効果が得られる。

(1) 電子制御装置 1 0 は、外部処理部 2 0 0 (第 1 処理部)、内部処理部 1 2 0 (第 2 処理部)、および転送制御部 1 1 0 を備える。外部処理部 2 0 0 よりも内部処理部 1 2 0 は起動処理に長い時間を要する。転送制御部 1 1 0 は、外部から受信する通信データを外部処理部 2 0 0 および内部処理部 1 2 0 に転送可能である。転送制御部 1 1 0 は、図 4 (a) に示すように起動から内部処理部 1 2 0 の起動処理が完了するまでは内部処理部 1 2 0 をデータの転送先とせず外部処理部 2 0 0 を転送先に含め、図 4 (b) に示すように内部処理部 1 2 0 の起動処理が完了すると少なくとも内部処理部 1 2 0 をデータの転送先とする。そのため、内部処理部 1 2 0 が起動処理が完了する以前であっても通信データの処理が可能であり、起動時に受信した通信データの処理能力が担保される。また、内部処理部 1 2 0 の起動処理が完了すれば内部処理部 1 2 0 を用いて通信データを処理するため、処理能力が向上する。

[0047] たとえば、内部処理部 1 2 0 および外部処理部 2 0 0 の全体の起動処理が完了するまでは転送制御部 1 1 0 は通信データを一切処理しない構成も考えられる。その場合は、全体の起動処理が完了するまでは、処理能力はゼロである。これに対して本実施の形態では、外部処理部 2 0 0 の起動処理が完了しなくても転送制御部 1 1 0 および内部処理部 1 2 0 により通信データを処理するので、処理能力が低いながらも起動中から処理を開始することができる。すなわち本実施の形態では、処理能力がゼロの期間を短くすることができる。

[0048] (2) 転送制御部 1 1 0 は、データの識別子とデータの転送先の対応情報である転送情報 1 1 4 を格納する転送記憶部 1 1 3 を備える。転送制御部 1 1 0 は、転送情報 1 1 4 を参照してデータの転送先を決定する。転送制御部 1

1 0 は、内部処理部 1 2 0 により転送情報 1 1 4 が書き換えられることにより通信データの転送先が変更される。

[0049] (3) 転送制御部 1 1 0 は、内部処理部 1 2 0 の起動処理が完了すると転送情報 1 1 4 を参照してデータを、外部処理部 2 0 0 および内部処理部 1 2 0 を含む転送先のいずれかに転送する。そのため、内部処理部 1 2 0 の起動処理が完了すると、外部処理部 2 0 0 だけでなく内部処理部 1 2 0 も利用して通信データの転送処理を実行するので処理がより高速となる。

[0050] (4) 内部処理部 1 2 0 は、改竄を検出する内部セキュリティ検証部 1 2 2 (第 2 セキュリティ検証部) を備える。内部処理部 1 2 0 は、内部処理部 1 2 0 を構成する内部セキュリティ検証部 1 2 2 を除く少なくとも 1 つの構成の改竄の検出を内部セキュリティ検証部 1 2 2 を用いて起動処理の一部として行う。

[0051] (5) 転送制御部 1 1 0 は、データの識別子とデータの転送先の対応情報である転送情報 1 1 4 を格納する転送記憶部 1 1 3 を備える。転送制御部 1 1 0 は、転送情報 1 1 4 を参照してデータの転送先を決定する。内部処理部 1 2 0 は、改竄を検出する内部セキュリティ検証部 1 2 2 (第 2 セキュリティ検証部) を備える。内部処理部 1 2 0 の起動処理は、図 2 の S 3 0 3 である第 1 起動処理と、図 2 の S 3 0 5 である第 2 起動処理とから構成される。第 1 起動処理では、内部セキュリティ検証部 1 2 2 が転送情報 1 1 4 を書き換える出力先設定部 1 2 3 を実現するプログラム、および内部処理部 1 2 0 をデータの転送先としない旨の情報である初期情報 1 2 6 の改竄を検出し、出力先設定部 1 2 3 が初期情報 1 2 6 を転送記憶部 1 1 3 に書き込む。そのため、内部セキュリティ検証部 1 2 2 を用いて改竄がされていないことが確認された安全な転送情報 1 1 4 の作成ができる。

[0052] (変形例 1)

上述した第 1 の実施の形態では、データ転送部 1 0 0 は転送制御部 1 1 0 と内部処理部 1 2 0 とを独立した構成として説明した。しかし、転送制御部 1 1 0 と内部処理部 1 2 0 とが明示的に分離されない構成でもよい。

[0053] (変形例 2)

上述した第 1 の実施の形態では、内部処理部 1 2 0 および外部処理部 2 0 0 の両者ともセキュアブートを行った。しかし内部処理部 1 2 0 および外部処理部 2 0 0 の少なくとも一方は、セキュアブートを行わなくてもよい。セキュアブートを行わなくてもよい場合とはたとえば、プログラムやデータが読み出し専用のメモリに格納される場合や、改竄の可能性を考慮しなくてよい場合などである。セキュアブートを行わない場合であっても、たとえばプログラムやデータのデータサイズが大きいことなどを理由として外部処理部 2 0 0 の起動が内部処理部 1 2 0 よりも長時間を要する場合には、本実施の形態の構成が有効である。すなわち、起動処理に長時間を有する外部処理部 2 0 0 の起動処理が完了するまでは外部処理部 2 0 0 が転送制御部 1 1 0 からの転送先の 1 つとなり、外部処理部 2 0 0 の起動処理が完了すると外部処理部 2 0 0 および内部処理部 1 2 0 が転送制御部 1 1 0 からの転送先に含まれることで、起動処理が完了する前に通信データの処理を開始できる。

[0054] (変形例 3)

上述した第 1 の実施の形態では、内部処理部 1 2 0 の出力先設定部 1 2 3 が転送制御部 1 1 0 の転送記憶部 1 1 3 に書き込みを行った。しかし内部処理部 1 2 0 は転送制御部 1 1 0 に書き込みの指令を送信して転送制御部 1 1 0 が転送記憶部 1 1 3 への書き込みを行ってもよい。この場合には、初期情報 1 2 6 および転送更新情報 1 2 7 が転送制御部 1 1 0 に備えられる。内部処理部 1 2 0 が転送制御部 1 1 0 に書き換え指令を送信し、転送制御部 1 1 0 が自ら転送情報 1 1 4 を書き換える。

[0055] (変形例 4)

上述した第 1 の実施の形態では、内部処理部 1 2 0 の起動処理が完了すると、内部処理部 1 2 0 および外部処理部 2 0 0 の両方を転送先に含むように転送情報 1 1 4 が書き換えられた。しかし転送情報 1 1 4 は、内部処理部 1 2 0 の起動処理が完了すると、内部処理部 1 2 0 は転送先に含むが外部処理部 2 0 0 は転送先に含まないように書き換えられてもよい。この場合はたと

えば、内部処理部 1 2 0 の起動処理が完了すると転送情報 1 1 4 は、図 4 (b) の 3 行目における「外部処理部」を「内部処理部」に書き換えたものとなる。本変形例によれば、内部処理部 1 2 0 の起動処理が完了すると外部処理部 2 0 0 は通信データの転送処理を行わないので、外部処理部 2 0 0 は別の処理を実行することができる。

[0056] (変形例 5)

上述した第 1 の実施の形態では、内部制御部 1 2 1 および出力先設定部 1 2 3 は不図示の CPU がプログラムを実行することにより実現された。しかし内部制御部 1 2 1 および出力先設定部 1 2 3 は、書き換え可能な論理回路である F P G A (Field Programmable Gate Array) を用いて実現されてもよい。F P G A に書き込むコンフィギュレーションデータが書き換え可能な記憶領域に格納される場合には、内部セキュリティ検証部 1 2 2 はセキュアブートの処理として、コンフィギュレーションデータの改竄を検出する。内部セキュリティ検証部 1 2 2 は、コンフィギュレーションデータもプログラムと同様に署名値を計算し、その署名値が予め記録されている値と一致するか否かにより改竄されているか否かを判断する。

[0057] なおプログラムとコンフィギュレーションデータは、読み込まれる対象は異なるが上述した機能ブロックを実現するプログラムコードという点では類似する。以下では、プログラムとコンフィギュレーションデータとをあわせて、「プログラム実現データ」と呼ぶ。この変形例 5 によれば、電子制御装置 1 0 の構成に F P G A が含まれる場合にも第 1 の実施の形態と同様の作用効果を得ることができる。

[0058] (変形例 6)

上述した第 1 の実施の形態では、通信データの一部は転送制御部 1 1 0 だけでも処理可能であった。たとえば図 4 (a) に示す上から 2 つの MAC アドレスを有する通信データは、内部処理部 1 2 0 や外部処理部 2 0 0 に転送することなく転送制御部 1 1 0 だけで処理が完結した。しかし転送制御部 1 1 0 は、転送制御部 1 1 0 だけでは処理を完結させず通信データを常に内部

処理部 1 2 0 や外部処理部 2 0 0 に転送してもよい。

[0059] (変形例 7)

内部制御部 1 2 1 および外部制御部 2 1 0 は、受信した通信データのヘッダ情報を書き換えた。しかし内部制御部 1 2 1 および外部制御部 2 1 0 の少なくとも一方は、受信した通信データのヘッダ情報を書き換えなくてもよい。この場合には内部制御部 1 2 1 および外部制御部 2 1 0 は、通信データを用いる何らかの処理を行う。この処理とはたとえば、通信データが所定の規則に従ったものであるか否かを判断し、所定の規則に従っていなければ通信データを破棄する処理である。

[0060] (変形例 8)

内部処理部 1 2 0 と外部処理部 2 0 0 は、その所在が入れ替わってもよい。すなわち外部処理部 2 0 0 がデータ転送部 1 0 0 に含まれ、内部処理部 1 2 0 はデータ転送部 1 0 0 の外部に存在してもよい。

[0061] ー第 2 の実施の形態ー

図 8 ～図 1 0 を参照して、電子制御装置の第 2 の実施の形態を説明する。以下の説明では、第 1 の実施の形態と同じ構成要素には同じ符号を付して相違点を主に説明する。特に説明しない点については、第 1 の実施の形態と同じである。本実施の形態では、主に、一部のプログラムの改竄の恐れがない点で、第 1 の実施の形態と異なる。

[0062] 図 8 は、第 2 の実施の形態における電子制御装置 1 0 A の構成図である。第 1 の実施の形態における電子制御装置 1 0 と同一の構成には同一の符号を付して説明を省略する。本実施の形態では、内部処理部 1 2 0 の出力先設定部 1 2 3 を実現するプログラム、および初期情報 1 2 6 が H S M や O T P (One Time Program) 領域などの書換え不可のメモリ領域 1 2 9 に保存される。すなわち、転送制御部 1 1 0 の転送記憶部 1 1 3 への書き込みに必要な機能を実現するプログラム、および転送記憶部 1 1 3 に書き込む情報が書換え不可領域に保存される対象である。

[0063] 図 9 は、第 2 の実施の形態における電子制御装置 1 0 A の動作を示すシー

ケンス図である。図2と同様の処理については、同じ番号を付し、説明を省略する。図2のシーケンス図と比較すると、内部処理部120の動作開始直後の処理、すなわち転送制御部110の転送記憶部113へ書き込むための機能を起動させる方法が異なる。

[0064] ステップS900では内部処理部120は、転送記憶部113への書き込みを行うプログラム、すなわち出力先設定部123の起動、および初期情報126の読み出しを行う。本実施の形態では、出力先設定部123を実現するためのプログラムおよび初期情報126は書き込み不可領域に保存されており改竄の危険性がないため、内部セキュリティ検証部122による検証を省略できる。その後の処理は第1の実施の形態と同様なので説明を省略する。

[0065] 図10は、第2の実施の形態における内部処理部120の処理を示すフローチャートである。図3で示したステップと同様の処理については、同じ番号を付して説明を省略する。図3と比較し、ステップS400およびS401がステップS900に代替される。

[0066] ステップS1000では、転送情報114の書き込みに関するプログラムがHSMに保存されているため、改竄の危険性がないことから、セキュアブートせずに、出力先関連部分を読み出して起動させる。具体的には、出力先設定部123および初期情報126を呼び出す。

[0067] 上述した第2の実施の形態によれば、次の作用効果が得られる。

(6) 電子制御装置10Aの転送制御部110は、データの識別子とデータの転送先の対応情報である転送情報114を格納する転送記憶部113を備える。転送制御部110は、転送情報114を参照してデータの転送先を決定する。内部処理部120の起動処理は、第1起動処理と第2起動処理とから構成される。第1起動処理では、読み出し専用領域から、内部セキュリティ検証部122が転送情報114を書き換える出力先設定部123を実現するプログラムコード、および内部処理部120をデータの転送先としない旨の情報である初期情報126を読み出し、出力先設定部123が初期情報1

26を転送記憶部113に書き込む。そのため、本実施の形態では内部セキュリティ検証部122が出力先設定部123および初期情報126のセキュアブートを要しないので、第1の実施の形態よりも早期に第1処理を完了できる。

[0068] ー第3の実施の形態ー

図11～図12を参照して、電子制御装置の第3の実施の形態を説明する。以下の説明では、第1の実施の形態と同じ構成要素には同じ符号を付して相違点を主に説明する。特に説明しない点については、第1の実施の形態と同じである。本実施の形態では、主に、終了時に転送情報が書き換えられる点で、第1の実施の形態と異なる。

[0069] 図11は、第3の実施の形態における電子制御装置10Bの構成図である。第1の実施の形態における電子制御装置10と同一の構成には同一の符号を付して説明を省略する。本実施の形態では、内部処理部120が終了処理部128をさらに備える。また、内部セキュリティ検証部122および出力先設定部123の処理が第1の実施の形態と異なっている。また本実施の形態では、転送記憶部113は不揮発性の記憶装置、たとえばフラッシュメモリ、相変化メモリ、磁気メモリなどである。そのため電子制御装置10Bに電源が供給されると、転送記憶部113には電源供給が停止された際に格納されていた情報がそのまま残っている。

[0070] 本実施の形態では、電子制御装置10Bは、外部からの電源供給が停止される前に動作停止指令信号が入力される。出力先設定部123は、動作停止指令信号が入力されると、転送記憶部113に初期情報126を書き込み、転送情報114を図4(a)に示すように転送先に内部処理部120が含まれないものに書き換える。この書き換えの後に電子制御装置10Bへの電源供給が停止される。

[0071] 電子制御装置10Bは、電源が供給されると内部処理部120と外部処理部200のそれぞれがセキュアブートを開始する。ただし内部処理部120の内部セキュリティ検証部122は、内部制御部121、出力先設定部12

3、内部ルート情報 1 2 5、および転送更新情報 1 2 7 をセキュアブートの対象とする。すなわち起動時には初期情報 1 2 6 はセキュアブートの対象としない。初期情報 1 2 6 は、起動後の処理負荷が低いタイミングで検証が行われる。内部処理部 1 2 0 は、セキュアブートが完了すると出力先設定部 1 2 3 を用いて転送記憶部 1 1 3 に転送更新情報 1 2 7 を書き込むことで、転送情報 1 1 4 を図 4 (b) に示すように転送先に内部処理部 1 2 0 が含まれるものに書き換える。この書き換えが完了すると、内部処理部 1 2 0 はルーティング受付状態に遷移する。

[0072] 図 1 2 は、第 3 の実施の形態における電子制御装置 1 0 B の動作を示すシーケンス図である。第 1 の実施の形態や第 2 の実施の形態と同様の処理については、同じ番号を付し、説明を省略する。図 1 2 に示すシーケンス図の上部では、電子制御装置 1 0 B の起動からしばらく時間が経過し、内部処理部 1 2 0 および外部処理部 2 0 0 の両方ともがルーティング受付状態に遷移している。なおこのときの転送情報 1 1 4 は、図 4 (b) に示すように転送先に内部処理部 1 2 0 が含まれるものである。

[0073] ステップ S 3 9 0 において、動作停止指令信号が入力されると、内部処理部 1 2 0 の出力先設定部 1 2 3 は次の処理を行う。すなわち出力先設定部 1 2 3 は、ステップ S 9 1 0 において内部記憶部 1 2 4 から初期情報 1 2 6 を読み出して、ステップ S 3 1 4 において転送制御部 1 1 0 の転送記憶部 1 1 3 に書き込む。この書き込みの完了の後に、内部処理部 1 2 0 の電源供給が終了する。その後、ステップ S 3 0 0 において内部処理部 1 2 0 に電源が供給される。外部処理部 2 0 0 は、第 1 の実施の形態と同様にステップ S 3 0 1 においてセキュアブートを行い、完了するとルーティング受付状態に遷移する（ステップ S 3 0 2）。

[0074] ステップ S 3 0 1 が完了した段階において、電源がオフになる直前のステップ S 3 1 4 における書き換えにより、第 1 の実施の形態における S 3 0 4 に相当する処理が完了している。そのため、外部処理部 2 0 0 がステップ S 3 0 2 によってルーティング受付状態に遷移すると、外部処理部 2 0 0 を用

いたルーティング処理が可能となる。

[0075] 上述した第3の実施の形態によれば、次の作用効果が得られる。

(7) 転送記憶部113は不揮発性の記憶領域である。電子制御装置10Bの終了処理として、転送先に内部処理部120が含まれないように転送情報114を書き換える終了処理部128を備える。そのため電子制御装置10Bは、第1の実施の形態や第2の実施の形態よりも早期に転送データの処理を開始することができる。

[0076] ー第4の実施の形態ー

図13～図14を参照して、電子制御装置の第4の実施の形態を説明する。以下の説明では、第1の実施の形態と同じ構成要素には同じ符号を付して相違点を主に説明する。特に説明しない点については、第1の実施の形態と同じである。本実施の形態では、主に、内部処理部と外部処理部のいずれが先に起動処理が完了する場合にも対応する点で、第1の実施の形態と異なる。

[0077] 図13は、第4の実施の形態における電子制御装置10Cの構成図である。第1の実施の形態における電子制御装置10と同一の構成には同一の符号を付して説明を省略する。本実施の形態における内部処理部120は、第1の実施の形態における構成に加えて、内部決定部961をさらに備える。また内部記憶部124には、初期情報126の代わりに内部初期情報951が格納される。本実施の形態における外部処理部200は、第1の実施の形態における構成に加えて、外部決定部962と外部出力先設定部963とを備える。外部記憶部230には、外部初期情報952が格納される。

[0078] 内部処理部120の内部セキュリティ検証部122は、起動時には内部制御部121、出力先設定部123、内部決定部961、内部ルート情報125、および内部初期情報951のセキュアブートを行う。第1の実施の形態では内部処理部120は2段階に分けてセキュアブートを行ったが、本実施の形態ではこれらすべてを一気に処理する。

[0079] 外部処理部200の外部セキュリティ検証部220は、起動時に、外部制

御部 2 1 0、外部決定部 9 6 2、外部出力先設定部 9 6 3、外部ルート情報 2 3 1、および外部初期情報 9 5 2 のセキュアブートを行う。

[0080] 内部初期情報 9 5 1 とは、受信した通信データの転送先に関するデータであり、転送先の少なくとも 1 つに内部処理部 1 2 0 が設定され、外部処理部 2 0 0 は転送先に含まないものである。外部初期情報 9 5 2 とは、受信した通信データの転送先に関するデータであり、転送先の少なくとも 1 つに外部処理部 2 0 0 が設定され、内部処理部 1 2 0 は転送先に含まないものである。外部初期情報 9 5 2 はたとえば図 4 (a) に示したものである。

[0081] 内部決定部 9 6 1 は、内部処理部 1 2 0 のセキュアブートが完了すると次の動作を行う。内部決定部 9 6 1 は外部処理部 2 0 0 のセキュアブートが完了しているか否かを判断する。外部処理部 2 0 0 のセキュアブートが完了しているか否かは、たとえば内部決定部 9 6 1 が転送記憶部 1 1 3 の内容を読み込んで判断してもよいし、内部処理部 1 2 0 と外部処理部 2 0 0 がセキュアブートが完了した旨の信号を相互に送りあうことにより実現してもよい。

[0082] 内部決定部 9 6 1 は外部処理部 2 0 0 のセキュアブートが完了していないと判断すると、出力先設定部 1 2 3 を用いて転送記憶部 1 1 3 に内部初期情報 9 5 1 を書き込み、内部処理部 1 2 0 を転送先として含む転送情報 1 1 4 を作成する。内部決定部 9 6 1 は外部処理部 2 0 0 のセキュアブートが完了していないと判断すると、出力先設定部 1 2 3 を用いて転送記憶部 1 1 3 に書き込みを行い転送情報 1 1 4 の転送先に内部処理部 1 2 0 と外部処理部 2 0 0 の両方を含む状態、たとえば図 4 (b) に示す状態に書き換える。

[0083] 外部決定部 9 6 2 は、外部処理部 2 0 0 のセキュアブートが完了すると次の動作を行う。外部決定部 9 6 2 は内部処理部 1 2 0 のセキュアブートが完了しているか否かを判断する。この判断は内部決定部 9 6 1 と同様の手法で実現できる。外部決定部 9 6 2 は内部処理部 1 2 0 のセキュアブートが完了していないと判断すると、外部出力先設定部 9 6 3 を用いて転送記憶部 1 1 3 に外部初期情報 9 5 2 を書き込み、外部処理部 2 0 0 を転送先として含む転送情報 1 1 4 を作成する。外部決定部 9 6 2 は内部処理部 1 2 0 のセキュア

アブートが完了していなると判断すると、外部出力先設定部 963 を用いて転送記憶部 113 に書き込みを行い転送情報 114 の転送先に内部処理部 120 と外部処理部 200 の両方を含む状態、たとえば図 4（b）に示す状態に書き換える。

[0084] 図 14 は、第 4 の実施の形態における電子制御装置 10C の処理の流れを説明するシーケンス図である。ステップ S911 とステップ S921 が同時に開始される。ステップ S911 では、外部セキュリティ検証部 220 が、セキュアブートを開始する。ステップ S921 では、内部セキュリティ検証部 122 が、セキュアブートを開始する。内部セキュリティ検証部 122 によるセキュアブートが完了すると内部決定部 961 が動作を開始し、外部処理部 200 によるセキュアブートが完了しているか否かを判断する。図 14 に示す例では外部処理部 200 によるセキュアブートが完了していないので、内部決定部 961 はステップ S931 において内部初期情報 951 を転送記憶部 113 に書き込み、ステップ S922 においてルーティング受付状態に遷移する。

[0085] 外部処理部 200 は、セキュアブートが 911 が完了すると、外部決定部 962 が内部処理部 120 のセキュアブートがすでに完了していること判断する。そして外部決定部 962 はステップ S932 において転送情報 114 を書き換え、外部処理部 200 はステップ S912 においてルーティング受付状態に遷移する。

[0086] 上述した第 4 の実施の形態によれば、内部処理部 120 および外部処理部 200 のいずれが先に起動した場合であっても、先に起動した方を利用した転送データの処理を開始できる。

[0087] なお本実施の形態では、内部処理部 120 と外部処理部 200 のいずれが先に起動するかで転送情報 114 に記載される情報が変化した。たとえば内部処理部 120 と外部処理部 200 を仮に第 1 演算部と第 2 演算部に呼び換え、転送情報 114 に書き込む情報は第 1 の実施の形態と同様とする。

すなわち最初に作成される転送情報 1 1 4 の転送先には、図 4 (a) に示すように外部処理部 2 0 0 は含まれるが内部処理部 1 2 0 は含まれない。

[0088] そして、第 1 演算部と第 2 演算部のうち、先に起動した方を外部処理部 2 0 0 と呼び、起動が遅い方を内部処理部 1 2 0 と呼ぶ。このように名称を呼び変えることで本実施の形態における動作を表すことができる。すなわち本実施の形態は次のように表現することもできる。

[0089] (8) 電子制御装置 1 0 C において、内部処理部 1 2 0 および外部処理部 2 0 0 のそれぞれは、第 1 演算部および第 2 演算部のいずれかである。電子制御装置 1 0 C は、第 1 演算部および第 2 演算部のうち起動処理が先に完了した方を外部処理部 2 0 0 として転送情報 1 1 4 を書き換え、第 1 演算部および第 2 演算部のうち起動処理が後に完了した方を内部処理部 1 2 0 として転送情報 1 1 4 を書き換える決定部、すなわち内部決定部 9 6 1 および外部決定部 9 6 2 を備える。そのため、内部処理部 1 2 0 および外部処理部 2 0 0 のいずれが先に起動した場合であっても、先に起動した方を利用した転送データの処理を開始できる。

[0090] 上述した各実施の形態および変形例において、機能ブロックの構成は一例に過ぎない。別々の機能ブロックとして示したいくつかの機能構成を一体に構成してもよいし、1つの機能ブロック図で表した構成を2以上の機能に分割してもよい。また各機能ブロックが有する機能の一部を他の機能ブロックが備える構成としてもよい。

[0091] 上述した各実施の形態および変形例は、それぞれ組み合わせてもよい。上記では、種々の実施の形態および変形例を説明したが、本発明はこれらの内容に限定されるものではない。本発明の技術的思想の範囲内で考えられるその他の態様も本発明の範囲内に含まれる。

[0092] 次の優先権基礎出願の開示内容は引用文としてここに組み込まれる。

日本国特許出願 2 0 1 9 - 2 0 8 9 7 7 (2 0 1 9 年 1 1 月 1 9 日出願)

符号の説明

[0093] 1 0、1 0 A、1 0 B…電子制御装置

1 0 0 …データ転送部
1 1 0 …転送制御部
1 1 1 …通信部
1 1 2 …転送情報制御部
1 1 3 …転送記憶部
1 1 4 …転送情報
1 2 0 …内部処理部
1 2 1 …内部制御部
1 2 2 …内部セキュリティ検証部
1 2 3 …出力先設定部
1 2 4 …内部記憶部
1 2 6 …初期情報
1 2 7 …転送更新情報
1 2 8 …終了処理部
1 2 9 …書換え不可のメモリ領域
2 0 0 …外部処理部
2 1 0 …外部制御部
2 2 0 …外部セキュリティ検証部
2 3 0 …外部記憶部
9 5 1 …内部初期情報
9 5 2 …外部初期情報
9 6 1 …内部決定部
9 6 2 …外部決定部
9 6 3 …外部出力先設定部

請求の範囲

[請求項1] 第1処理部、第2処理部、および転送制御部を備える電子制御装置であって、

前記第1処理部よりも前記第2処理部は起動処理に長い時間を要し、

前記転送制御部は、外部から受信する通信データを前記第1処理部および前記第2処理部に転送可能な通信部を備え、

前記第1処理部は、前記転送制御部から転送される前記通信データを処理する第1制御部を備え、

前記第2処理部は、前記転送制御部から転送される前記通信データを処理する第2制御部を備え、

前記転送制御部は、前記第2処理部の起動処理が完了するまでは前記第2処理部を前記通信データの転送先とせず前記第1処理部を転送先に含め、前記第2処理部の起動処理が完了すると少なくとも前記第2処理部を前記通信データの転送先とする、電子制御装置。

[請求項2] 請求項1に記載の電子制御装置において、

前記転送制御部は、前記通信データの識別子と前記通信データの転送先の対応情報である転送情報を格納する転送記憶部をさらに備え、

前記転送制御部は、前記転送情報を参照して前記通信データの転送先を決定し、

前記転送制御部は、前記転送情報を自ら書き換えることにより前記通信データの転送先を変更する、または前記第2処理部により前記転送情報が書き換えられることにより前記通信データの転送先が変更される電子制御装置。

[請求項3] 請求項2に記載の電子制御装置において、

前記転送制御部は、前記通信データの識別子と前記通信データの転送先の対応情報である転送情報を格納する転送記憶部をさらに備え、

前記転送制御部は、前記第2処理部の起動処理が完了すると前記転

送情報を参照して前記通信データを、前記第 1 処理部および前記第 2 処理部を含む転送先のいずれかに転送する電子制御装置。

[請求項4]

請求項 2 に記載の電子制御装置において、

前記第 2 処理部は、前記第 2 処理部の起動処理が完了すると前記転送記憶部の前記転送情報を転送先に前記第 2 処理部が含まれるように書き換える出力先設定部をさらに備える電子制御装置。

[請求項5]

請求項 2 に記載の電子制御装置において、

前記転送記憶部は不揮発性の記憶領域であり、

前記電子制御装置の終了処理として、転送先に前記第 2 処理部が含まれないように前記転送情報を書き換える終了処理部をさらに備える電子制御装置。

[請求項6]

請求項 1 に記載の電子制御装置において、

前記第 2 処理部は、改竄を検出する第 2 セキュリティ検証部を備え、

前記第 2 処理部は、前記第 2 処理部を構成する前記第 2 セキュリティ検証部を除く少なくとも 1 つの構成の改竄を検出を前記第 2 セキュリティ検証部を用いて前記起動処理の一部として行う電子制御装置。

[請求項7]

請求項 1 に記載の電子制御装置において、

前記転送制御部は、前記通信データの識別子と前記通信データの転送先の対応情報である転送情報を格納する転送記憶部をさらに備え、

前記転送制御部は、前記転送情報を参照して前記通信データの転送先を決定し、

前記第 2 処理部は、改竄を検出する第 2 セキュリティ検証部を備え、

前記第 2 処理部の前記起動処理は、第 1 起動処理と第 2 起動処理とから構成され、

前記第 1 起動処理では、前記第 2 セキュリティ検証部が前記転送情報を書き換える出力先設定部を実現するプログラム実現データ、およ

び前記第2処理部を前記通信データの転送先としない旨の情報である初期情報の改竄を検出し、前記出力先設定部が前記初期情報を前記転送記憶部に書き込む、電子制御装置。

[請求項8]

請求項1に記載の電子制御装置において、

前記転送制御部は、前記通信データの識別子と前記通信データの転送先の対応情報である転送情報を格納する転送記憶部をさらに備え、

前記転送制御部は、前記転送情報を参照して前記通信データの転送先を決定し、

前記第2処理部の前記起動処理は、第1起動処理と第2起動処理とから構成され、

前記第1起動処理では、前記第2処理部が読み出し専用領域から、前記転送情報を書き換える出力先設定部を実現するプログラム実現データ、および前記第2処理部を前記通信データの転送先としない旨の情報である初期情報を読み出し、前記出力先設定部が前記初期情報を前記転送記憶部に書き込む、電子制御装置。

[請求項9]

請求項1に記載の電子制御装置において、

前記第1処理部および前記転送制御部はデータ転送部に含まれ、前記第2処理部は前記データ転送部に接続される、電子制御装置。

[請求項10]

請求項1に記載の電子制御装置において、

前記第2処理部および前記転送制御部はデータ転送部に含まれ、前記第1処理部は前記データ転送部に接続される、電子制御装置。

[請求項11]

請求項9に記載の電子制御装置において、

前記データ転送部はデータリンク層またはネットワーク層におけるスイッチであり、

前記転送制御部はスイッチコアであり、

前記第1処理部は前記スイッチの内部プロセッサであり、

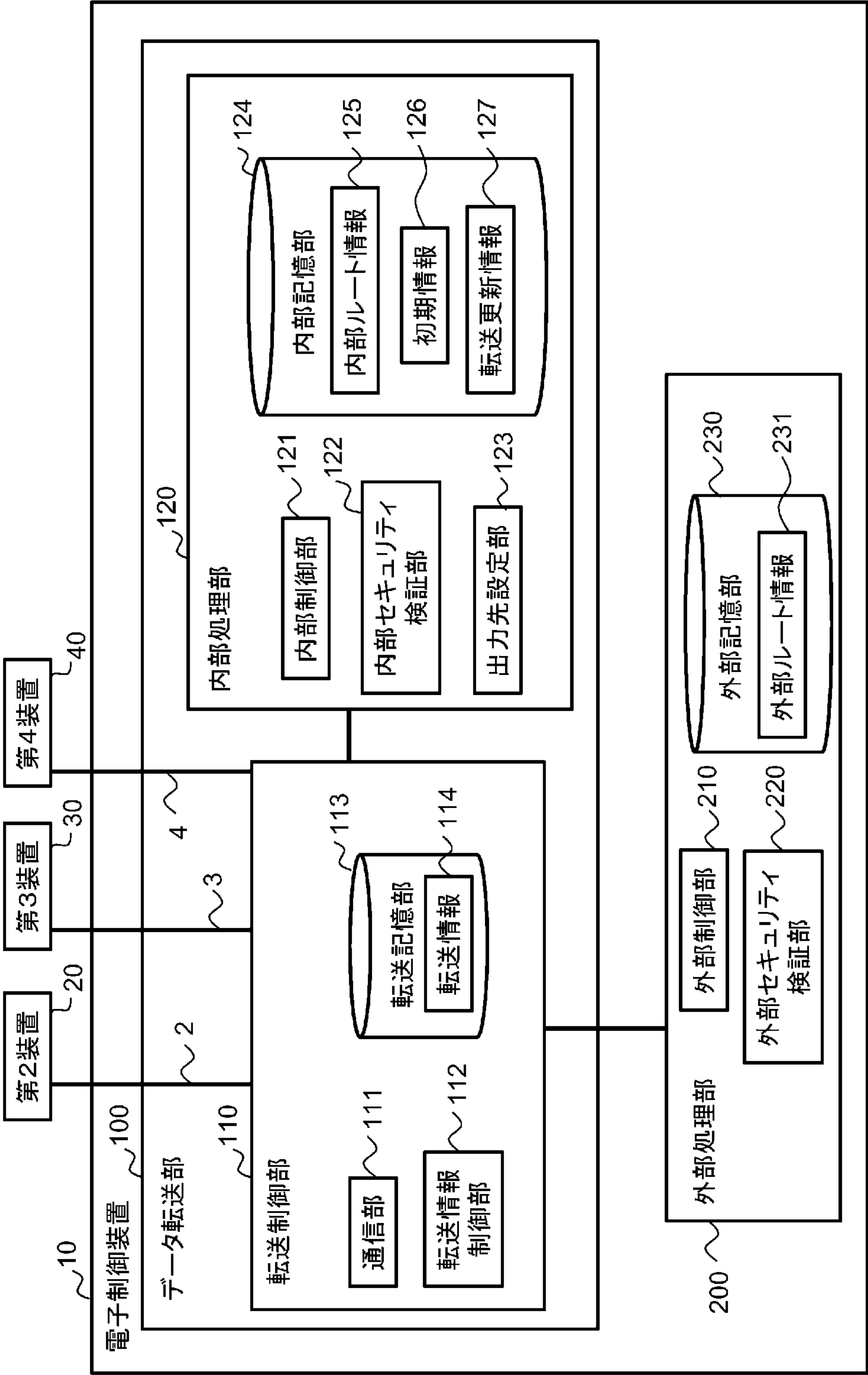
前記第2処理部は前記スイッチに接続されたマイコンである、電子制御装置。

- [請求項12] 請求項10に記載の電子制御装置において、
前記データ転送部はデータリンク層またはネットワーク層における
スイッチであり、
前記転送制御部はスイッチコアであり、
前記第2処理部は前記スイッチの内部プロセッサであり、
前記第1処理部は前記スイッチに接続されたマイコンである、電子
制御装置。
- [請求項13] 請求項2に記載の電子制御装置において、
前記第1処理部および前記第2処理部のそれぞれは、第1演算部お
よび第2演算部のいずれかであり、
前記第1演算部および前記第2演算部のうち起動処理が先に完了し
た方を前記第1処理部として前記転送情報を書き換え、前記第1演算
部および前記第2演算部のうち起動処理が後に完了した方を前記第2
処理部として前記転送情報を書き換える決定部をさらに備える、電子
制御装置。
- [請求項14] 第1処理部、第2処理部、および転送制御部を備える電子制御装置
が実行する演算方法であって、
前記第1処理部よりも前記第2処理部は起動処理に長い時間を要し
、
前記転送制御部は、外部から受信する通信データを前記第1処理部
および前記第2処理部に転送可能であり、
前記第1処理部が、前記転送制御部から転送される前記通信データ
を処理することと、
前記第2処理部は、前記転送制御部から転送される前記通信データ
を処理することと、
前記転送制御部は、前記第2処理部の起動処理が完了するまでは前
記第2処理部を前記通信データの転送先とせず前記第1処理部を転送
先に含め、前記第2処理部の起動処理が完了すると少なくとも前記第

2 処理部を前記通信データの転送先とすることを含む演算方法。

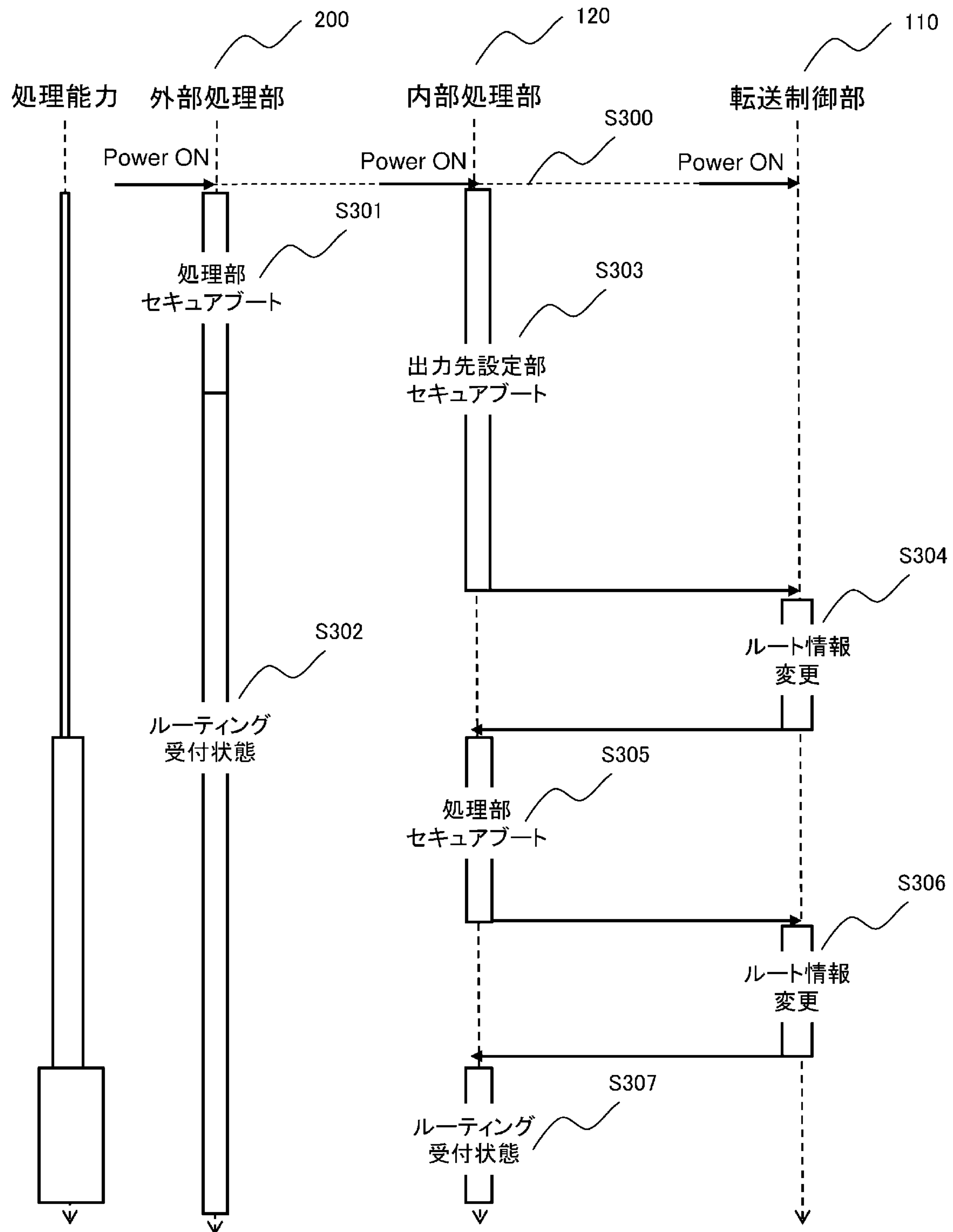
[図1]

図1



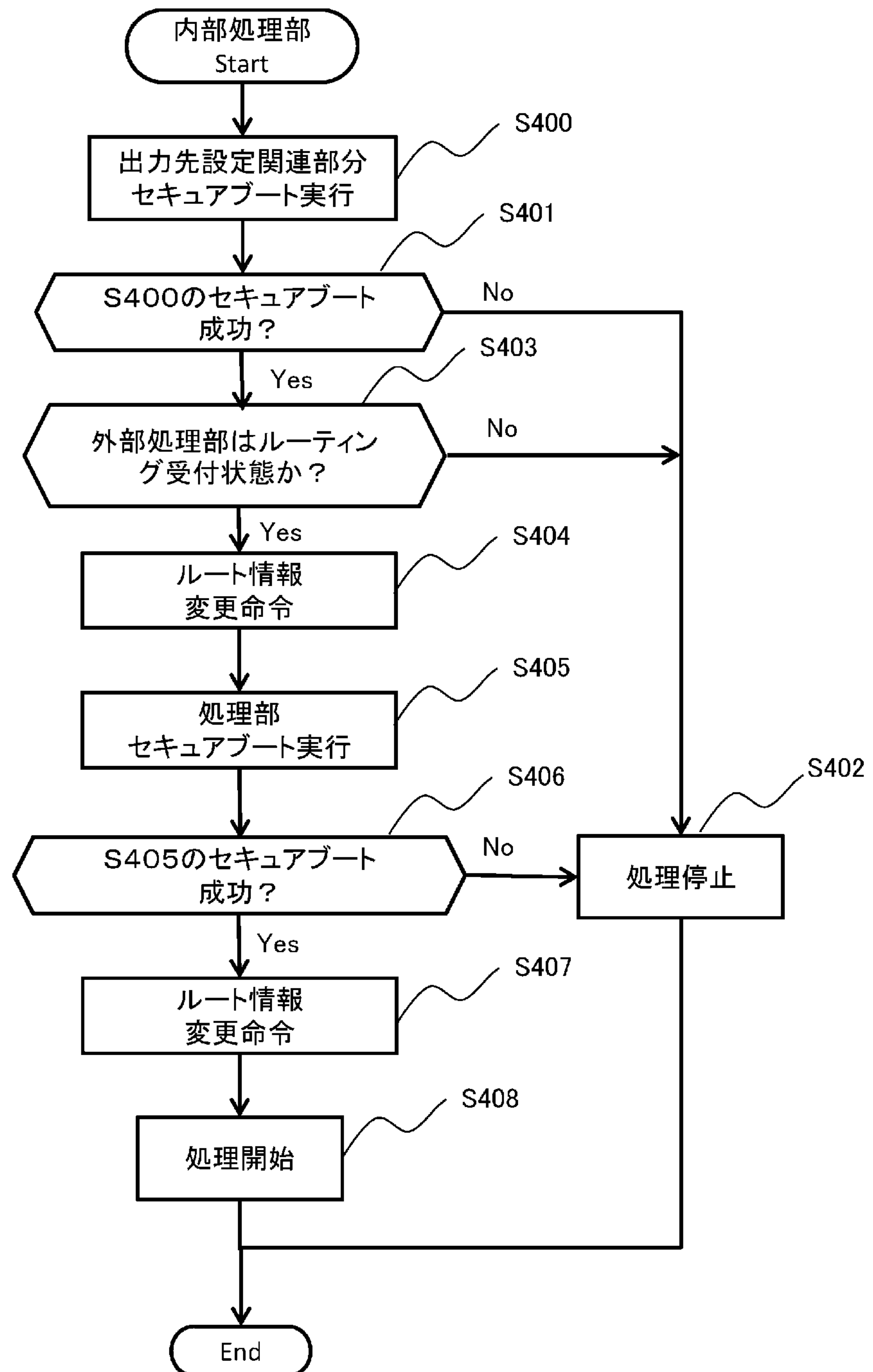
[図2]

図2



[図3]

図3



[図4]

図4

114

1130

1131

MACアドレス	転送先
1A:2B:3C:4D:5E:6F	Port 2
A0:B1:C2:D3:E4:F5	Port 3
20:30:40:50:60:70	外部処理部
00:01:02:03:04:05	外部処理部

(a)

114

1130

1131

MACアドレス	転送先
1A:2B:3C:4D:5E:6F	Port 2
A0:B1:C2:D3:E4:F5	Port 3
20:30:40:50:60:70	外部処理部
00:01:02:03:04:05	内部処理部

(b)

[図5]

図5

127 ↓	
1260	1261
MACアドレス	転送先
00:01:02:03:04:05	内部処理部

[図6]

図6

125
↓

1240		1241	
IPアドレス		転送先MACアドレス	
255.255.1.3		1A:2B:3C:4D:5E:6F	
192.168.1.5		A0:B1:C2:D3:E4:F5	

[図7]

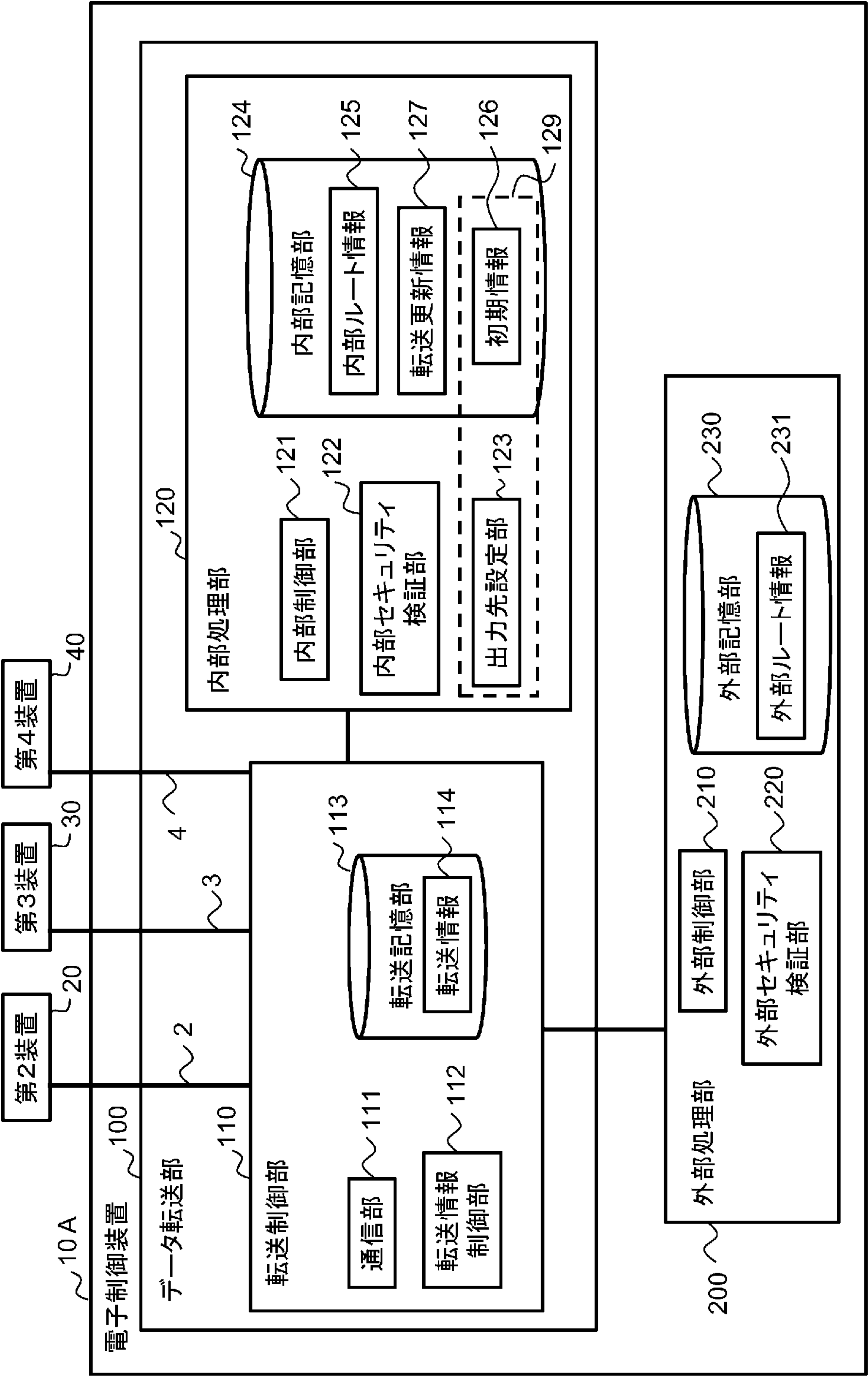
図7

231
↓

2300		2301	
IPアドレス		転送先MACアドレス	
255.255.255.192		1A:2B:3C:4D:5E:6F	
192.128.1.2		A0:B1:C2:D3:E4:F5	
255.255.1.3		1A:2B:3C:4D:5E:6F	
192.168.1.5		A0:B1:C2:D3:E4:F5	

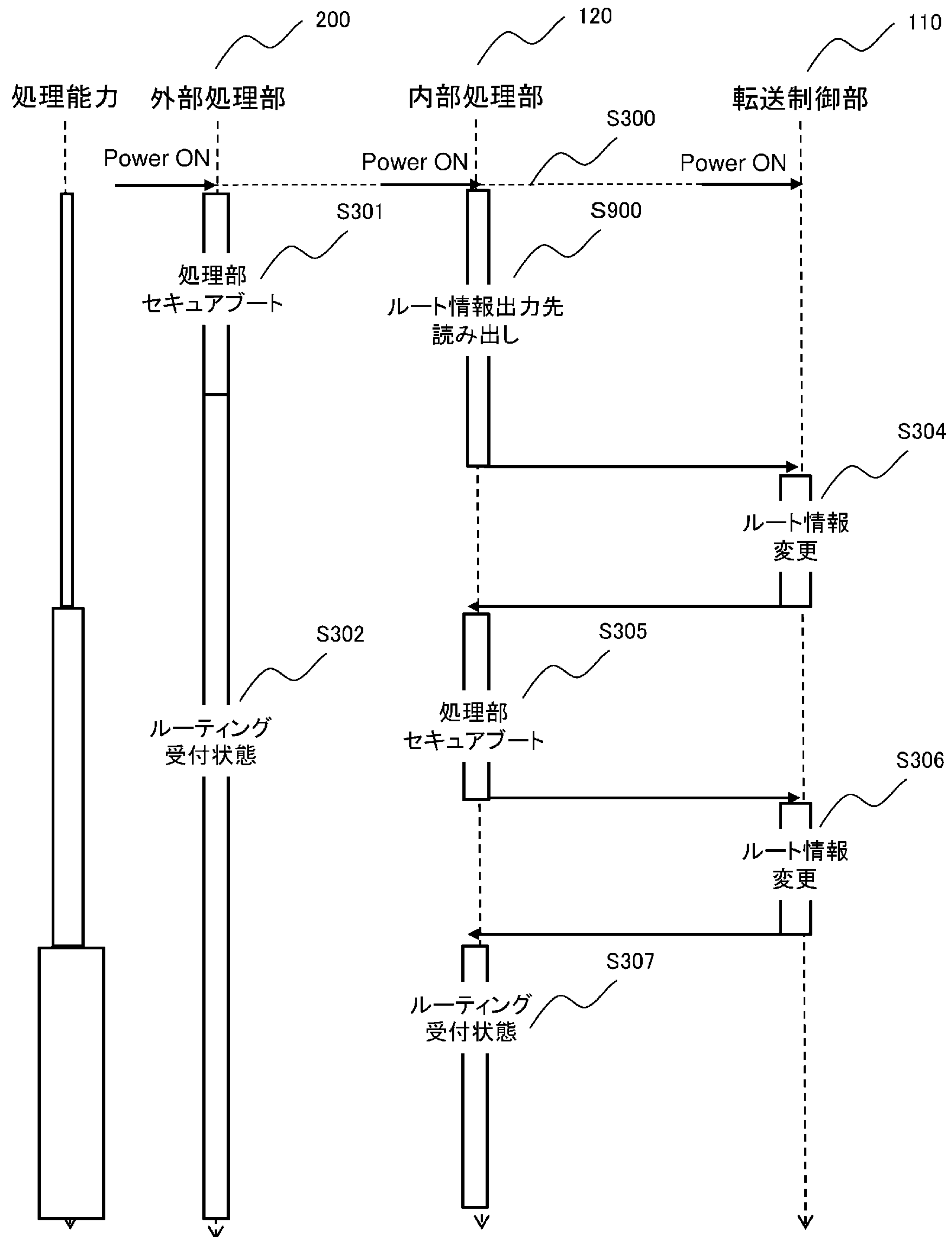
[図8]

図8



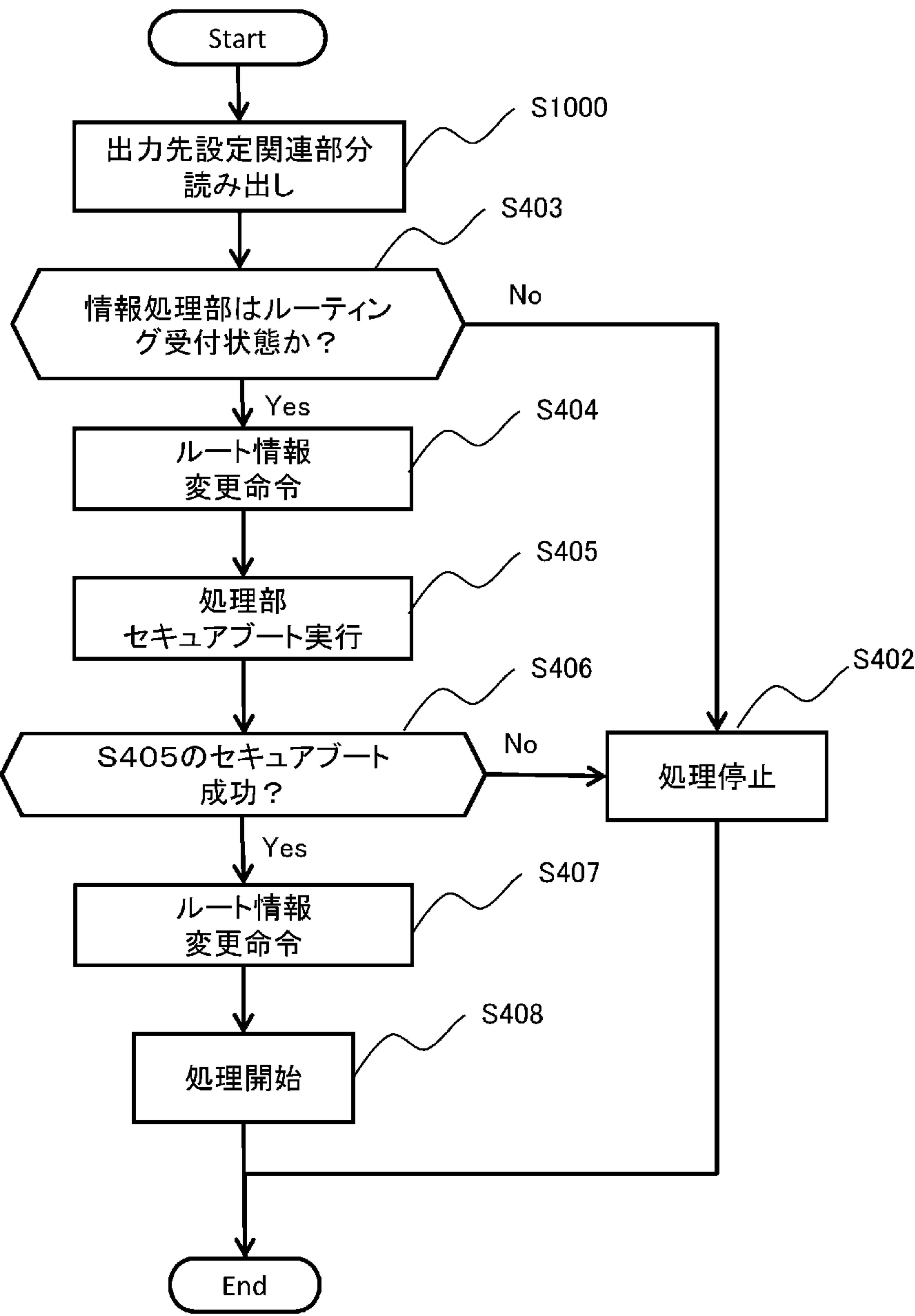
[図9]

図9



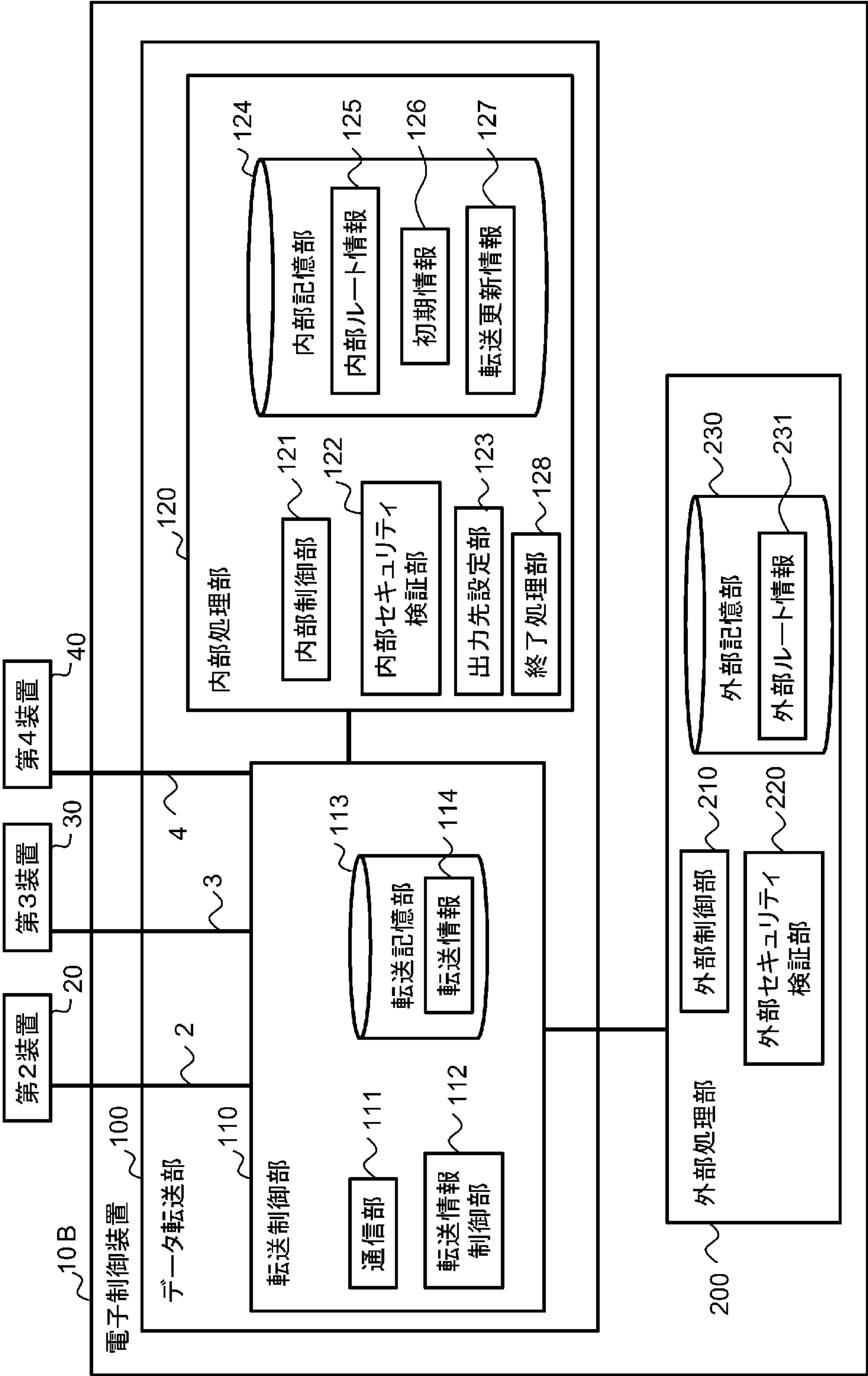
[図10]

図 10

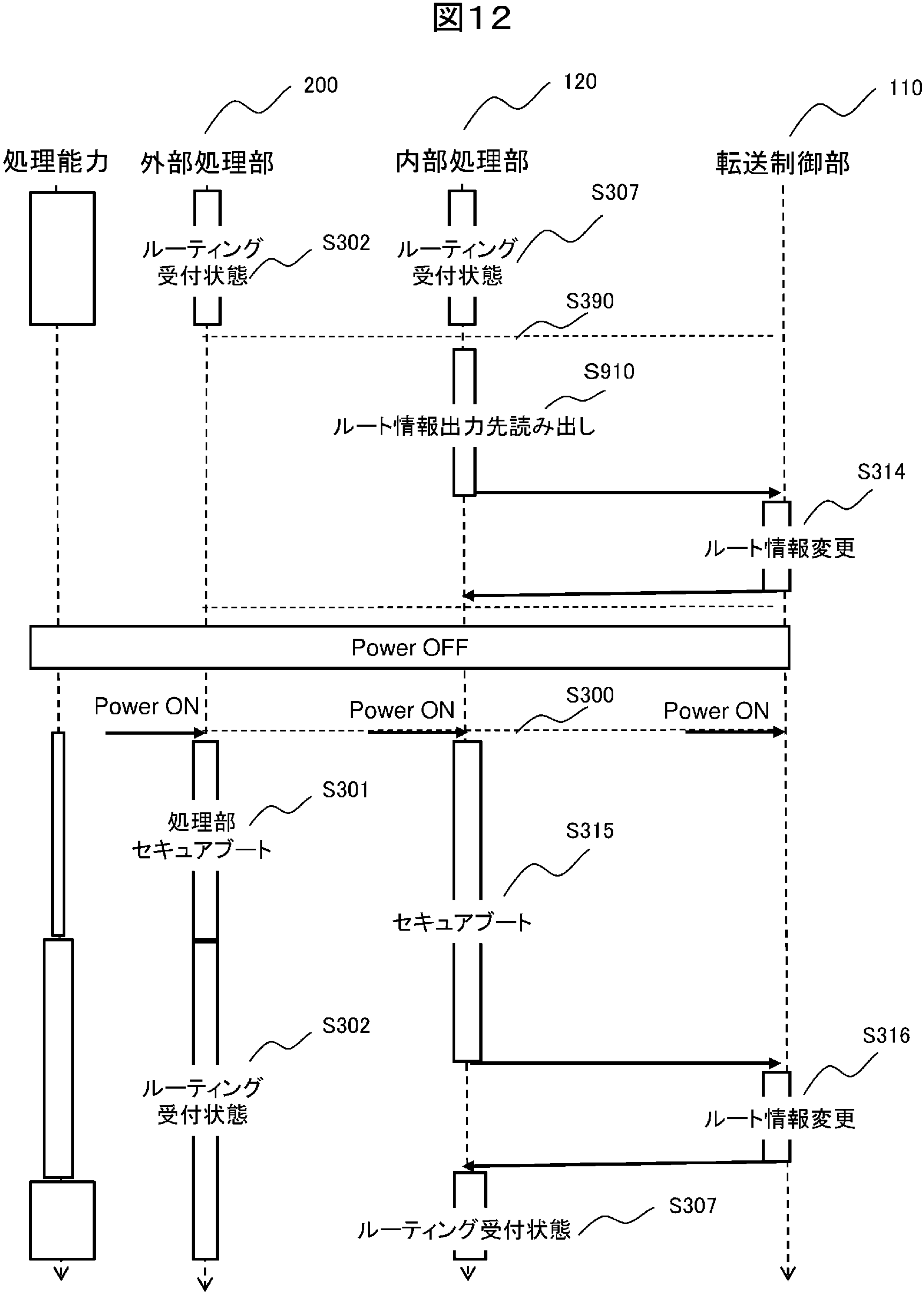


[図11]

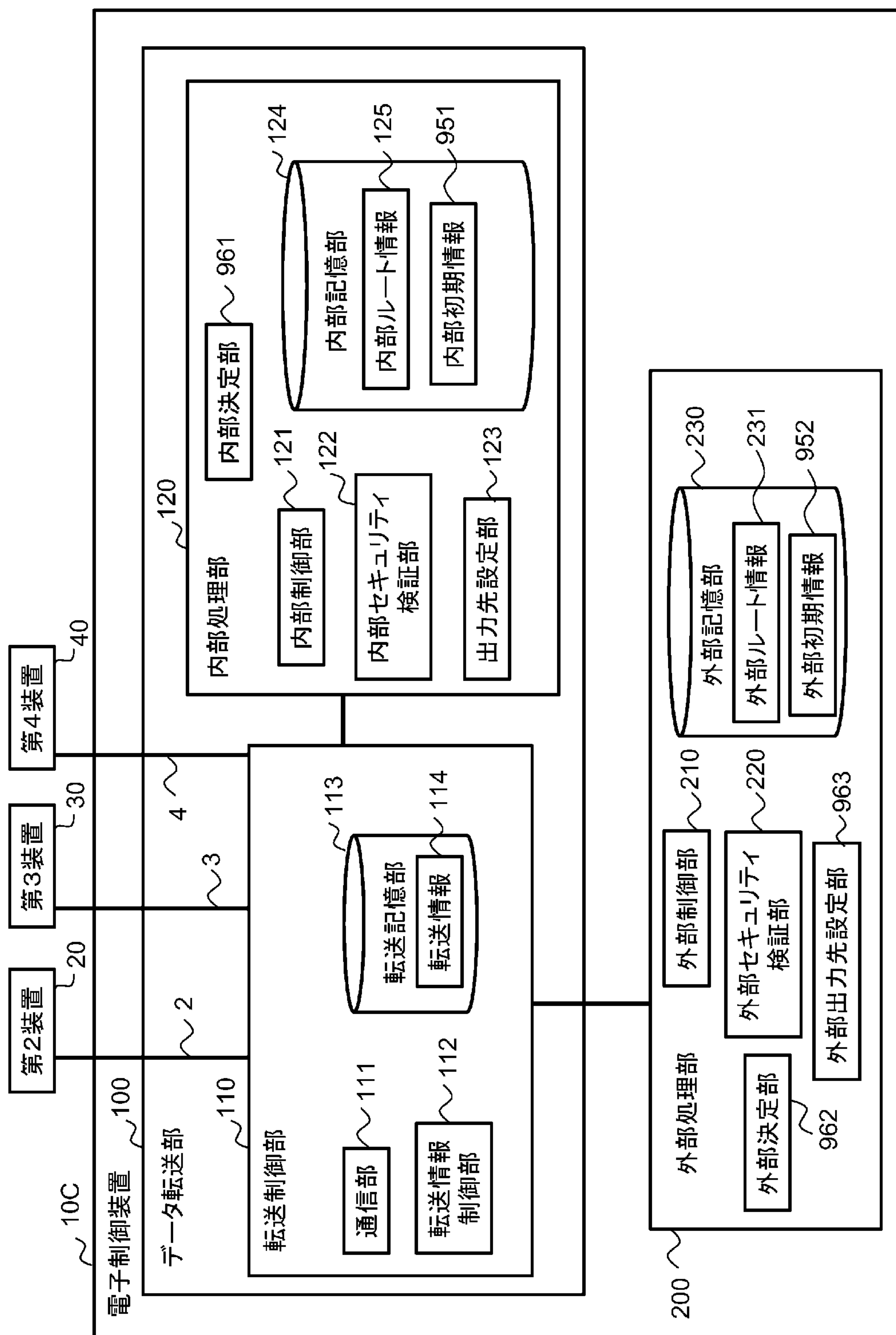
図11



[図12]

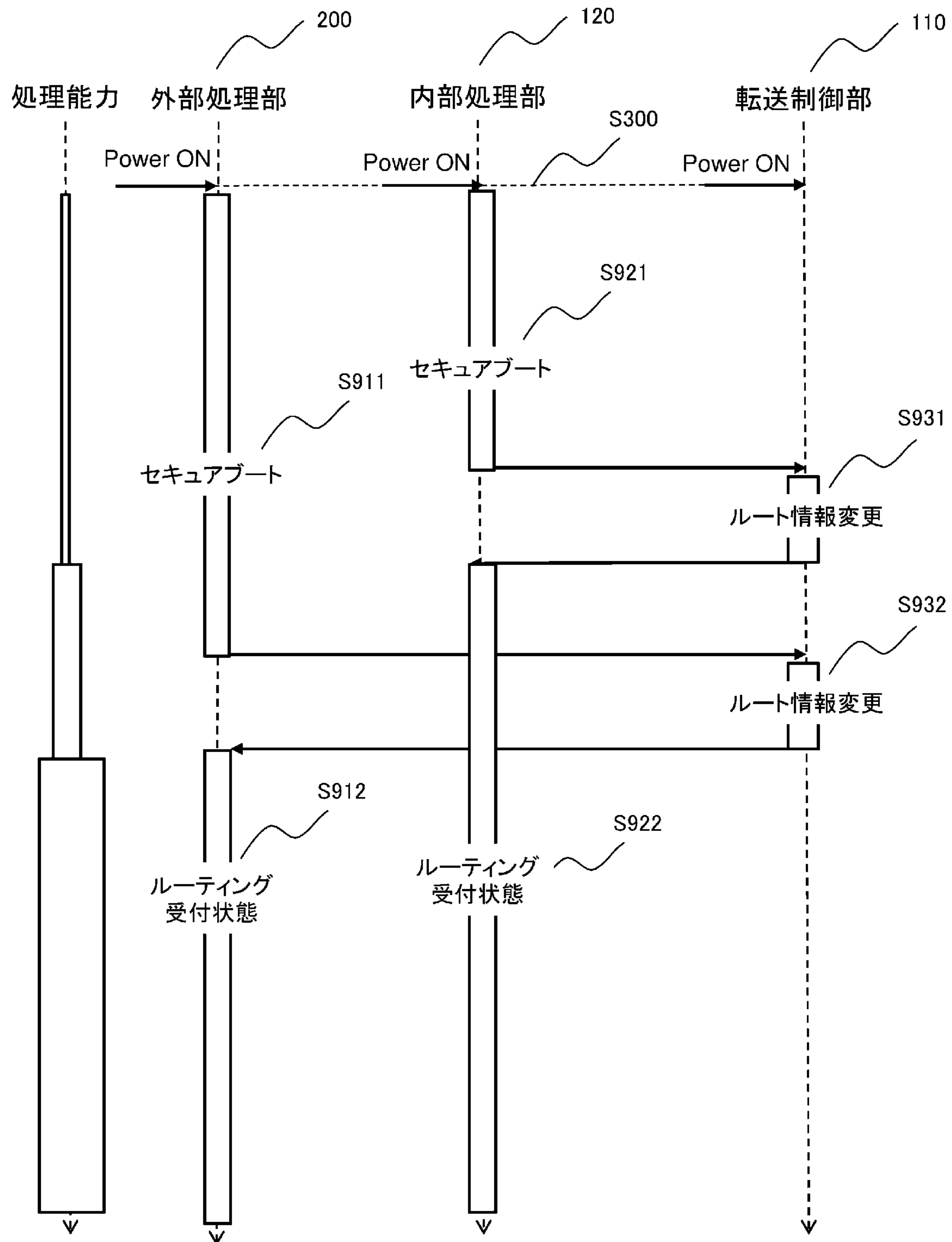


[図13]



[図14]

図 14



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2020/041785

A. CLASSIFICATION OF SUBJECT MATTER B60R 16/023(2006.01)i; G06F 9/4401(2018.01)i; G06F 21/57(2013.01)i FI: G06F9/4401; G06F21/57 350; B60R16/023 P 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) B60R16/023; G06F9/4401; G06F21/57 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 1971-2021 Registered utility model specifications of Japan 1996-2021 Published registered utility model applications of Japan 1994-2021 Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X A A A	JP 2014-85905 A (NEC NETWORK AND SENSOR SYSTEMS, LTD.) 12 May 2014 (2014-05-12) abstract, paragraphs [0015]-[0020], [0024]-[0044], fig. 1-7 US 2010/0174895 A1 (PIERCE, James R.) 08 July 2010 (2010-07-08) abstract, fig. 3 JP 2018-116669 A (AUTONETWORKS TECHNOLOGIES, LTD.) 26 July 2018 (2018-07-26) paragraphs [0044]-[0116], fig. 1-7	1, 6, 9-10, 14 2-5, 7-8, 11-13 1-14 1-14
<div>☐ Further documents are listed in the continuation of Box C.</div> <div>☒ See patent family annex.</div>		
<div>* 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</div>		
Date of the actual completion of the international search 14 January 2021 (14.01.2021)		Date of mailing of the international search report 26 January 2021 (26.01.2021)
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/JP2020/041785

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
JP 2014-85905 A	12 May 2014	(Family: none)	
US 2010/0174895 A1	08 Jul. 2010	(Family: none)	
JP 2018-116669 A	26 Jul. 2018	US 2018/0205414 A1	
		paragraphs [0063]-	
		[0148], fig. 1-7	
		DE 102018100756 A1	
		CN 108337228 A	

国際調査報告		国際出願番号 PCT/JP2020/041785
A. 発明の属する分野の分類（国際特許分類（IPC）） B60R 16/023(2006.01)i; G06F 9/4401(2018.01)i; G06F 21/57(2013.01)i FI: G06F9/4401; G06F21/57 350; B60R16/023 P		
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）） B60R16/023; G06F9/4401; G06F21/57		
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 - 2021年 日本国実用新案登録公報 1996 - 2021年 日本国登録実用新案公報 1994 - 2021年		
国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）		
C. 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求項の番号
X	JP 2014-85905 A（NECネットワーク・センサ株式会社）12.05.2014（2014 - 05 - 12） [要約], 段落[0015]-[0020], [0024]-[0044], 図1-7	1, 6, 9-10, 14
A		2-5, 7-8, 11-13
A	US 2010/0174895 A1（PIERCE, James R.）08.07.2010（2010 - 07 - 08） ABSTRACT, 図3	1-14
A	JP 2018-116669 A（株式会社オートネットワーク技術研究所）26.07.2018（2018 - 07 - 26） 段落[0044]-[0116], 図1-7	1-14
<div>☐ C欄の続きにも文献が列挙されている。</div> <div>☒ パテントファミリーに関する別紙を参照。</div>		
* 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 14.01.2021		国際調査報告の発送日 26.01.2021
名称及びあて先 日本国特許庁(ISA/JP) 〒100-8915 日本国 東京都千代田区霞が関三丁目4番3号		権限のある職員（特許庁審査官） 多賀 実 5B 9367 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/JP2020/041785

引用文献			公表日	パテントファミリー文献	公表日
JP	2014-85905	A	12.05.2014	(ファミリーなし)	
US	2010/0174895	A1	08.07.2010	(ファミリーなし)	
JP	2018-116669	A	26.07.2018	US 2018/0205414 A1	
				段落[0063]-[0148], 図1-7	
				DE 102018100756 A1	
				CN 108337228 A	