(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2014-204315
(P2014-204315A)
(43)公開日　平成26年10月27日(2014.10.27)

(51)Int.Cl.			F I			テーマコード（参考）
H04L	12/28	(2006.01)	H04L	12/28	200M	5K033
B60R	16/023	(2006.01)	B60R	16/02	665P	

審査請求 未請求　請求項の数 11　ＯＬ　（全 23 頁）

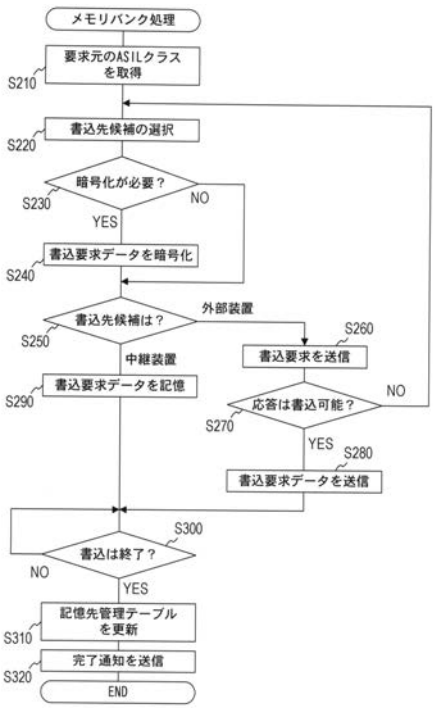
(21)出願番号　特願2013-79556(P2013-79556)
(22)出願日　平成25年4月5日(2013.4.5)

(71)出願人　000004260
株式会社デンソー
愛知県刈谷市昭和町１丁目１番地
(74)代理人　110000578
名古屋国際特許業務法人
(72)発明者　井本　礼一郎
愛知県刈谷市昭和町１丁目１番地　株式会社デンソー内

Ｆターム(参考)　5K033 AA05　BA06　DA13　DB18　DB20　EA07

(54)【発明の名称】中継装置

(57)【要約】　（修正有）
【課題】車載システムにおいて、可能な限り費用を抑制しつつ、信頼性の高い装置を情報の記憶先とする。
【解決手段】書込要求データが発生したメモリレス制御装置からのメモリバンク要求を受信した中継装置は、記憶機能付制御装置のうち、要求元レベルと同レベルの安全要求レベルが割り当てられ、かつ、書込要求データのデータサイズよりも大きな空き容量が存在する記憶部を有した一つの記憶機能付制御装置を書込先候補として選択する（Ｓ２２０）。その選択した書込先候補に対して書込要求を出力し（Ｓ２６０）、当該書込要求を取得した書込先候補から応答が、書込要求データを書込可能であれば（Ｓ２７０：ＹＥＳ）、書込先候補を書込先装置として特定して書込要求データを出力する（Ｓ２８０）。これにより、書込先装置の記憶部には、書込要求データが書き込まれ記憶される。
【選択図】図４



【特許請求の範囲】
【請求項１】
それぞれに定められ、互いに異なる機能である実現要求機能を実現する複数の制御装置（２０，３０，４０）として、
電力供給が遮断されても記憶内容を保持する不揮発性記憶装置（２６）を有した前記制御装置である少なくとも一つの記憶機能付制御装置（２０）と、
前記不揮発性記憶装置を有していない前記制御装置である少なくとも一つのメモリレス制御装置（３０）とが混在し、
前記実現要求機能の実現に対して要求される安全性の水準を表す安全要求レベルが前記実現要求機能を実現する制御装置ごとに割り当てられた車載ネットワークにて、前記制御装置間の情報通信を中継する中継装置（４０）であって、
前記不揮発性記憶装置へのデータの書き込みを要求するメモリバンク要求を、前記制御装置から取得する要求取得手段（４４）と、
前記メモリバンク要求によって書き込みが要求されるデータを書込要求データとし、前記制御装置ごとに割り当てられた前記安全要求レベルを表した記憶先管理テーブルに従って、前記要求取得手段にて取得したメモリバンク要求に基づいて、当該メモリバンク要求の要求元に割り当てられた安全要求レベルである要求元レベル以上に高い安全要求レベルが割り当てられた前記記憶機能付制御装置を書込先装置として特定する書込先特定手段（４６，Ｓ２１０～Ｓ２７０）と、
前記書込先特定手段にて特定した書込先装置が有する不揮発性記憶装置に前記書込要求データを書き込むデータ記憶制御手段（４６，Ｓ２８０，Ｓ２９０）と
を備えることを特徴とする中継装置。
【請求項２】
前記書込先特定手段は、
前記記憶先管理テーブルに従って、前記要求元レベルと同レベルの安全要求レベルである安全要求同レベルが割り当てられた前記記憶機能付制御装置から順に、当該記憶機能付制御装置を書込先候補として選択する選択手段（４６，Ｓ２２０）と、
前記選択手段にて選択された書込先候補に、前記書込要求データの書き込みの可否を問い合わせる書込要求を出力する要求出力手段（４６，Ｓ２６０）と、
前記要求出力手段にて書込要求を出力した先である書込先候補からの前記書込要求に対する返答が前記書込要求データの書き込み可能であれば、当該書込要求の送信先である前記書込先候補を前記書込先装置として特定する可否確認手段（４６，Ｓ２７０）と、
前記要求出力手段にて書込要求を出力した先である書込先候補からの前記書込要求に対する返答が前記書込要求データの書き込み不可であれば、前記選択手段に新たな書込先候補を選択させる再選択手段（４６，Ｓ２７０）と
を備えることを特徴とする請求項１に記載の中継装置。
【請求項３】
前記再選択手段は、
前記安全要求同レベルが割り当てられ、かつ未選択である前記記憶機能付制御装置が存在すれば、当該未選択である記憶機能付制御装置の一つを書込先候補として、前記選択手段に選択させ、
前記安全要求同レベルが割り当てられた前記記憶機能付制御装置が存在しなければ、前記安全要求同レベルよりも高い安全要求レベルが割り当てられた前記記憶機能付制御装置の中から前記書込先候補を前記選択手段に選択させる
ことを特徴とする請求項２に記載の中継装置。
【請求項４】
前記記憶先管理テーブルは、
各記憶機能付制御装置が有する不揮発性記憶装置の空き容量が、前記記憶機能付制御装置ごとに対応付けられており、
前記選択手段は、

前記書込要求データのデータサイズよりも大きな空き容量が存在する前記不揮発性記憶装置を有した記憶機能付制御装置を、前記書込先候補として選択する
ことを特徴とする請求項２または請求項３に記載の中継装置。
【請求項５】
当該中継装置自身は、
前記不揮発性記憶装置（４２）を有し、
前記書込先特定手段は、
当該中継装置自身を前記記憶機能付制御装置の一つとして、前記書込先装置を特定する
ことを特徴とする請求項１から請求項４のいずれか一項に記載の中継装置。
【請求項６】
前記データ記憶制御手段は、
前記書込要求データに対して暗号化を実行して、前記書込先装置に書き込む
ことを特徴とする請求項１から請求項５のいずれか一項に記載の中継装置。
【請求項７】
前記メモリバンク要求には、
前記書込要求データに対する暗号化の要否が含まれており、
前記データ記憶制御手段は、
前記メモリバンク要求に含まれる暗号化の要否が、前記暗号化が必要であることを表していれば、当該メモリバンク要求に対応する書込要求データに対して暗号化を実行する
ことを特徴とする請求項６に記載の中継装置。
【請求項８】
前記データ記憶制御手段による前記書込先装置への前記書込要求データの書き込みが完了したことを表す完了通知を、前記書込先装置から受信する完了受信手段（４６，Ｓ３００）と、
前記完了受信手段にて完了通知を受信すると、前記データ記憶制御手段にて当該書込先装置に書き込んだ前記書込要求データに関する情報を、前記記憶先管理テーブルに追加するテーブル更新手段（４６，Ｓ３１０）と
を備えることを特徴とする請求項１から請求項７のいずれか一項に記載の中継装置。
【請求項９】
前記不揮発性記憶装置としてのデータ蓄積装置（４２）を備え、
当該データ蓄積装置には、前記記憶先管理テーブルが格納され、
外部からの指令が入力されると、前記データ蓄積装置に記憶された前記記憶先管理テーブルを書き換える第一書換手段を備える
ことを特徴とする請求項１から請求項８のいずれか一項に記載の中継装置。
【請求項１０】
前記各手段は、当該中継装置が処理プログラムを実行することで実現され、
外部からの指令が入力されると、前記処理プログラムを書き換える第二書換手段を備える
ことを特徴とする請求項１から請求項９のいずれか一項に記載の中継装置。
【請求項１１】
前記メモリバンク要求の出力元が前記メモリレス制御装置である
ことを特徴とする請求項１から請求項１０のいずれか一項に記載の中継装置。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、車載ネットワークに接続される中継装置に関する。
【背景技術】
【０００２】
従来、自動車に搭載される車載システムであって、複数の電子制御装置が車載ネットワークを介して接続され、電子制御装置間で情報通信を実行する車載システムが知れられて

いる。電子制御装置それぞれは、電子制御装置自身に接続された各種センサや各種装置を制御対象として制御し、予め規定された機能（以下、「実現要求機能」と称す）を実現する。

【０００３】

実現要求機能は、通常、当該実現要求機能の実行中に発生した情報を不揮発性記憶装置に記憶する必要があるが、一方で、不揮発性記憶装置に情報を記憶する必要性が低い実現要求機能も存在する。不揮発性記憶装置に情報を記憶する必要性が低い機能を実現する電子制御装置においては、不揮発性記憶装置が省略されている場合がある。つまり、車載システムにおいては、不揮発性記憶装置を有していないメモリレス制御装置と、不揮発性記憶装置を有している記憶機能付装置との両方が電子制御装置として混在している。

【０００４】

ところで、電子制御装置自身や電子制御装置の制御対象である各種センサや各種装置に不具合が発生した場合、当該電子制御装置に規定された実現要求機能を実現することが困難となる。そこで、不具合の原因を解明するために、車載システムには、各電子制御装置や電子制御装置の制御対象に関するログ情報を記憶することが求められる。

【０００５】

ログ情報の記憶を簡易に実現する車載システムにおいては、電子制御装置とは異なる装置として、車載ネットワークを介して各電子制御装置との間で情報通信を実行すると共に、その情報通信によって取得した情報を記憶する不揮発性メモリを有した車載情報収集装置を備えることが提案されている（特許文献１参照）。

【０００６】

この特許文献１に記載された車載システムにおける車載情報収集装置は、特定の実現要求機能にて不具合が発生した場合、その不具合の発生を検出した電子制御装置に対して、電子制御装置自身の不揮発性記憶装置にログ情報を記憶可能であるか否かを問い合わせる。その問い合わせの結果、電子制御装置からの返答がログ情報を記憶不可能（例えば、自身がメモリレス制御装置）であれば、車載情報収集装置は、電子制御装置からログ情報を直ちに取得して車載情報収集装置の不揮発性メモリに記憶する。また、電子制御装置からの返答がログ情報を記憶可能であれば、車載情報収集装置は、電子制御装置にログ情報を所定時間保持させた後、当該ログ情報を取得して車載情報収集装置の不揮発性メモリに記憶する。

【先行技術文献】

【特許文献】

【０００７】

【特許文献１】特開２００９－２８６２９５号公報

【発明の概要】

【発明が解決しようとする課題】

【０００８】

ところで、各実現要求機能に対しては、当該実現要求機能の実現に対して要求される安全性の水準を表す安全要求レベルが割り当てられており、電子制御装置や電子制御装置の制御対象それぞれに対しても安全要求レベルを担保するために必要となる信頼性の水準が規定されている（例えば、ＡＳＩＬ）。

【０００９】

そして、ログ情報の記憶先は、信頼性の高い装置であることが求められ、不具合が発生した実現要求機能を実現する電子制御装置に割り当てられた安全要求レベルと同じ水準以上の安全要求レベルを有していることが求められる。

【００１０】

特許文献１に記載された車載システムにて、これを実現するためには、各電子制御装置の信頼性よりも信頼性が高くなるように、車載情報収集装置自身を構成する必要が生じる。このように信頼性の高い車載情報収集装置を構成するためには、信頼性の高い部品を用いて構成する必要がある。この信頼性の高い部品は、費用が高いことから、信頼性の高い

車載情報収集装置を構築するための費用が高くなるという課題が生じる。

【００１１】

つまり、従来の技術では、車載システムにおいて、可能な限り費用を抑制しつつ、信頼性の高い装置を情報の記憶先とすることが困難であるという課題があった。

そこで、本発明においては、可能な限り費用を抑制しつつ、信頼性の高い装置を情報の記憶先とすることを目的とする。

【課題を解決するための手段】

【００１２】

上記目的を達成するためになされた本発明は、車載ネットワークにて、制御装置間の情報通信を中継する中継装置に関する。車載ネットワークは、それぞれに定められ、互いに異なる機能である実現要求機能を実現する複数の制御装置として、不揮発性記憶装置を有した制御装置である少なくとも一つの記憶機能付制御装置と、不揮発性記憶装置を有していない制御装置である少なくとも一つのメモリレス制御装置とが混在したものである。そして、各制御装置には、実現要求機能の実現に対して要求される安全性の水準を表す安全要求レベルが割り当てられている。なお、ここで言う不揮発性記憶装置とは、電力供給が遮断されても記憶内容を保持すると共に、記憶内容を書換可能な記憶装置である。

【００１３】

そして、本発明の中継装置は、要求取得手段と、書込先特定手段と、データ記憶制御手段とを備える。

このうち、要求取得手段は、不揮発性記憶装置へのデータの書き込みを要求するメモリバンク要求を、制御装置から取得する。そして、メモリバンク要求によって書き込みが要求されるデータを書込要求データとし、制御装置ごとに割り当てられた安全要求レベルを表した記憶先管理テーブルに従って、書込先特定手段が、要求取得手段にて取得したメモリバンク要求に基づいて、当該メモリバンク要求の要求元に割り当てられた安全要求レベル（以下、「要求元レベル」と称す）以上に高い安全要求レベルが割り当てられた記憶機能付制御装置を書込先装置として特定する。その特定した書込先装置が有する不揮発性記憶装置に、データ記憶制御手段が、書込要求データを書き込む。

【００１４】

このような中継装置によれば、要求元レベル以上に高い安全要求レベルが割り当てられた記憶機能付制御装置を書込先装置とすることができ、その書込先装置の安全要求レベル、ひいては、書込先装置が備える不揮発性記憶装置の信頼性を担保することができる。

【００１５】

しかも、本発明において、書込先装置の選定に用いる安全要求レベルは、実現要求機能を実現する制御装置ごとに予め割り当てられたものである。

したがって、本発明においては、書込先装置の信頼性を担保することを目的として、中継装置や制御装置（即ち、車載ネットワーク）に新たな構成を付加したり、従来の部品を変更したりする必要がない。このため、本発明においては、費用が増加することを可能な限り抑制できる。

【００１６】

これらのことから、本発明によれば、可能な限り費用を抑制しつつ、情報（書込要求データ）の記憶先を信頼性の高い装置とすることができる。

さらに、本発明における書込先特定手段は、選択手段と、要求出力手段と、可否確認手段と、再選択手段とを備えていても良い。

【００１７】

この場合、選択手段は、記憶先管理テーブルに従って、要求元レベルと同レベルの安全要求レベル（以下、「安全要求同レベル」と称す）が割り当てられた記憶機能付制御装置から順に、当該記憶機能付制御装置を書込先候補として選択する。その選択された書込先候補に、要求出力手段が、書込要求データの書き込みの可否を問い合わせる書込要求を出力する。そして、書込要求を出力した先である書込先候補からの書込要求に対する返答が書込要求データの書き込み可能であれば、可否確認手段は、当該書込要求の送信先である

書込先候補を書込先装置として特定する。また、書込要求を出力した先である書込先候補からの書込要求に対する返答が書込要求データの書き込み不可であれば、再選択手段が、選択手段に新たな書込先候補を選択させる。

【００１８】

本発明の中継装置によれば、適切な書込先装置が特定されるまで、書込先装置の選定を繰り返し実行することができる。これにより、本発明によれば、適切な記憶機能付制御装置を書込先装置として特定することができ、その書込先装置の不揮発性記憶装置に書込要求データをより確実に記憶することができる。

【００１９】

ところで、一般的な車載システムにおいては、安全要求レベルが高い実現要求機能を実現する制御装置からの書込要求データほど、高い安全性（信頼性）が求められる。

このため、本発明における再選択手段は、安全要求同レベルが割り当てられ、かつ未選択である記憶機能付制御装置が存在すれば、当該未選択である記憶機能付制御装置の一つを書込先候補として、選択手段に選択させても良い。さらに、再選択手段は、安全要求同レベルが割り当てられた記憶機能付制御装置が存在しなければ、安全要求同レベルよりも高い安全要求レベルが割り当てられた記憶機能付制御装置の中から書込先候補を選択手段に選択させても良い。

【００２０】

このような本発明によれば、高い安全性が要求される書込要求データほど、安全要求レベルが高い実現要求機能を実現する記憶機能付制御装置の不揮発性記憶装置に記憶することができる。すなわち、本発明によれば、書込要求データに対して要求される安全性（信頼性）に適した書き込み先を決定でき、リソースを無駄なく有効に利用できる。

【図面の簡単な説明】

【００２１】

【図１】車載通信システムの概略構成を示すブロック図である。

【図２】記憶先管理テーブルを示す説明図である。

【図３】電子制御装置が実行する機能実現処理の処理手順を示すフローチャートである。

【図４】中継装置が実行するメモリバンク処理の処理手順を示すフローチャートである。

【図５】書込先装置が実行する書込処理の処理手順を示すフローチャートである。

【図６】書込先装置に書込要求データを書き込む動作を説明する説明図である。

【発明を実施するための形態】

【００２２】

以下に本発明の実施形態を図面と共に説明する。

〈全体構成〉

図１に示す車載通信システム１は、自動車に搭載される車載システムであり、電子制御装置（ＥＣＵ（Ｅｌｅｃｔｒｏｎｉｃ　Ｃｏｎｔｒｏｌ　Ｕｎｉｔ））２０，３０の間で必要な情報を通信するシステムである。

【００２３】

この車載通信システム１は、複数のサブネットワーク10_1，10_2，…10_nと、通信端末１４と、コネクタ（ＣＮＴ）１６と、複数の電子制御装置20_1，20_2，…20_Nと、複数の電子制御装置30_1，30_2，…，30_Mと、中継装置４０とを備えている。本実施形態においては、複数のサブネットワーク１０と、中継装置４０とによって、一つの車載ネットワーク５が構成され、サブネットワーク１０ごとに異なるプロトコルが用いられている。なお、本実施形態においては、符号“ｎ”，“Ｎ”，“Ｍ”は、自然数を表す。

【００２４】

各サブネットワーク１０にて用いられるプロトコルの一例として、車載ＬＡＮで一般的に利用されているＣＡＮ（Ｒｏｂｅｒｔ　Ｂｏｓｃｈ社が提案した「Ｃｏｎｔｒｏｌｌｅｒ　Ａｒｅａ　Ｎｅｔｗｏｒｋ」）プロトコルや、ＦｌｅｘＲａｙ、Ｌｉｎ（Ｌｏｃａｌ　Ｉｎｔｅｒｃｏｎｎｅｃｔ　Ｎｅｔｗｏｒｋ）などが考えられる。

【００２５】

通信端末１４は、車載通信システム１の外部に配置された装置（以下、「外部機器」とも称す）との間で情報通信を実行する。この通信端末１４が情報通信を実行する外部機器には、不揮発性の記憶装置からなるストレージ８２を備えた外部サーバ８０を含む。

【００２６】

コネクタ１６は、外部ツール８４を接続するコネクタである。外部ツール８４は、各種情報の入力を受け付ける入力受付部（図示せず）と、入力受付部にて受け付けた各種情報を車載通信システム１に送信すると共に、車載通信システム１からの情報を取得する通信部（図示せず）と、通信部にて取得した情報を報知する報知部（図示せず）とを少なくとも備えている。

【００２７】

サブネットワーク10_1，10_2，…10_nは、それぞれ、バス状の伝送路を備えている。

電子制御装置２０，３０は、車両の各所に配置され、サブネットワーク１０に接続されている。電子制御装置２０，３０は、それぞれが、予め割り当てられた機能（以下、「実現要求機能」と称す）を実現する。

【００２８】

このうち、電子制御装置２０は、それぞれ、通信部２２と、制御部２４と、記憶部２６とを備えている。

通信部２２は、トランシーバ（図示せず）と、コントローラ（図示せず）とを備えている。この通信部２２のトランシーバは、自身が接続されたサブネットワーク１０へのデータの送出、自身が接続されたサブネットワーク１０からのデータの取り込みを行う。また、通信部２２のコントローラは、当該サブネットワーク１０にて用いられるプロトコルに従って通信を制御する。

【００２９】

制御部２４は、ＲＯＭ，ＲＡＭ，ＣＰＵを少なくとも備えた周知のマイクロコンピュータを中心に構成されている。

記憶部２６は、電力供給が遮断された場合（即ち、電源オフ時）にも記憶内容が保持され、かつ、記憶内容を書き換え可能な不揮発性記憶装置である。

【００３０】

そして、電子制御装置２０の制御部２４は、電子制御装置２０自身に割り当てられた実現要求機能を実現する機能実現処理や、他の電子制御装置２０，３０との通信を実行する通信処理、他の電子制御装置２０，３０からの書込要求データを記憶部２６に格納する書込処理を実行する。

【００３１】

このため、制御部２４のＲＯＭは、電気的に書換可能な記憶領域であり、各種処理プログラムが格納される書換可能領域が設けられている。この書換可能領域には、機能実現処理、通信処理、及び書込処理を制御部２４が実行するための各処理プログラムが格納されている。

【００３２】

つまり、本実施形態では、電子制御装置２０の一つとして、各種センサの検知結果に従って、内燃機関を制御する機能が実現要求機能として割り当てられたエンジンＥＣＵや、パワートレイン機構を制御する機能が実現要求機能として割り当てられたパワートレインＥＣＵを含む。さらに、本実施形態では、電子制御装置２０として、周知のナビゲーション装置を構成する各部を制御対象とし、目的地までの経路を案内する機能が実現要求機能として割り当てられたナビゲーションＥＣＵなどを含む。

【００３３】

なお、以下では、電子制御装置２０を記憶機能付制御装置２０とも称す。

一方、電子制御装置３０は、それぞれ、通信部３２と、制御部３４とを備えている。

通信部３２は、トランシーバ（図示せず）と、コントローラ（図示せず）とを備えている。この通信部３２のトランシーバは、自身が接続されたサブネットワーク１０へのデー

タの送出、自身が接続されたサブネットワーク１０からのデータの取り込みを行う。また、通信部３２のコントローラは、当該サブネットワーク１０にて用いられるプロトコルに従って通信を制御する。

【００３４】

制御部３４は、ＲＯＭ，ＲＡＭ，ＣＰＵを少なくとも備えた周知のマイクロコンピュータを中心に構成されている。この制御部３４は、電子制御装置３０自身に割り当てられた実現要求機能を実現する機能実現処理や、他の電子制御装置２０，３０との通信を実行する通信処理、各種処理によって発生した書込要求データの書き込みを要求するメモリバンク要求を出力する書込要求処理を実行する。

【００３５】

このため、制御部３４のＲＯＭには、電気的に書換可能な記憶領域であり、各種処理プログラムが格納される書換可能領域が設けられている。この書換可能領域には、機能実現処理や、通信処理、書込要求処理を制御部３４が実行するための各処理プログラムが格納されている。

【００３６】

つまり、電子制御装置３０は、記憶機能付制御装置２０を構成する各部のうち、記憶部２６が省略された電子制御装置である。

このような電子制御装置３０の一つとして、各種センサでの検知結果に従って、ブレーキ機構を制御するアンチロックブレーキシステムが実現要求機能として割り当てられたＡＢＳ電子制御装置や、ドアに設けられた錠を制御対象として施錠・解錠する機能が実現要求機能として割り当てられたドアＥＣＵを含む。さらに、メモリレス制御装置３０の一つとして、パワーウインドウを制御対象として制御する機能が実現要求機能として割り当てられたウインドウＥＣＵや、電動ミラーを制御対象として制御する機能が実現要求機能として割り当てられたミラーＥＣＵ、ワイパー機構を制御対象として制御する機能が実現要求機能として割り当てられたワイパーＥＣＵを含む。さらには、電子制御装置３０の一つとして、自車両に搭載されたエアコンディショナを制御対象として制御する機能が実現要求機能として割り当てられたエアコンＥＣＵや、シート（座席）を制御対象として制御する機能が実現要求機能として割り当てられたシートＥＣＵが含まれていても良い。

【００３７】

以下では、電子制御装置３０をメモリレス制御装置３０とも称す。

本実施形態における各記憶機能付制御装置２０と、各メモリレス制御装置３０とには、電子制御装置自身の名前（以下、「ＥＣＵ名」と称す）と共に、各電子制御装置を識別する識別情報（以下、「ＥＣＵＩＤ」と称す）が予め規定されている。

【００３８】

また、本実施形態においては、一つのサブネットワーク１０には、同種の区分に分類される実現要求機能を実現する記憶機能付制御装置２０及びメモリレス制御装置３０が接続される。すなわち、各サブネットワーク１０は、自動車において周知のパワートレイン系、シャーシ（安全）系、ボデー系、マルチメディア系といった区分ごとに用意され、車載通信システム１全体では、記憶機能付制御装置２０とメモリレス制御装置３０とが混在している。

〈安全要求レベル〉

自動車においては、実現要求機能それぞれに対して要求される安全性の水準を表す安全要求レベルが規定される。この安全要求レベルは、各実現要求機能を実現する電子制御装置２０，３０に対しても規定される。

【００３９】

具体的に、本実施形態における安全要求レベルは、ＩＳＯ２６２６２によって規定される指標であるＡＳＩＬ（Ａｕｔｏｍｏｔｉｖｅ Ｓａｆｅｔｙ Ｉｎｔｅｇｒｉｔｙ Ｌｅｖｅｌ）クラスである。

【００４０】

このＡＳＩＬクラスは、予想される障害一つ一つの危険性に応じた安全対策の要求レベ

ルである。ＡＳＩＬクラスは、障害によって被る被害の大きさを表す危険度（Ｓ）と、障害に遭遇する頻度（Ｅ）と、障害が発生した場合に危険を回避する行動の容易さを表す制御可能性（Ｃ）との組み合わせによって決定される。

【００４１】

具体的には、危険度（Ｓ）と制御可能性（Ｃ）は３段階、頻度（Ｅ）は４段階で評価されている。そして、これらの危険度（Ｓ）と制御可能性（Ｃ）と頻度（Ｅ）とによって表されるマトリクスに従って、ＡＳＩＬクラスは決定される。そのＡＳＩＬクラスは、要求される安全性の水準が低いものから順に、ＱＭ（Ｑｕａｌｉｔｙ　Ｍａｎａｇｅｍｅｎｔ：システムは安全な状態），Ａ，Ｂ，Ｃ，Ｄと表される。

【００４２】

さらに、各電子制御装置２０，３０を構成する各部、電子制御装置２０，３０が実行する処理プログラム、及び電子制御装置２０，３０が制御する制御対象それぞれに対しては、ＡＳＩＬクラスの一部として、ＡＳＩＬクラスを担保するために必要となる信頼性レベルが設定される。この信頼性レベルには、各電子制御装置２０，３０を構成する各部、電子制御装置２０，３０が実行する処理プログラム、及び電子制御装置２０，３０が制御する制御対象それぞれでの不具合の発生確率が含まれる。

〈中継装置〉

中継装置４０は、サブネットワーク10_1，10_2，…10_nに接続されている電子制御装置２０，３０間の情報通信を中継するゲートウェイ機能を有した装置、即ち、セントラルゲートウェイ装置である。

【００４３】

この中継装置４０は、記憶部４２と、通信部４４と、制御部４６とを備えている。

記憶部４２は、電源オフ時にも記憶内容が保持され、かつ、記憶内容を書き換え可能な不揮発性メモリである。この記憶部４２には、ルーティング情報ＲＩが格納されるルーティング情報格納領域と、記憶先管理テーブルＭＩが格納される管理テーブル格納領域とが確保されている。

【００４４】

ここで言うルーティング情報ＲＩとは、互いに異なるサブネットワーク１０に接続された複数の電子制御装置２０，３０の間でのデータフレームの通信経路を表す情報である。なお、記憶先管理テーブルＭＩについては、詳しくは後述する。

【００４５】

通信部４４は、サブネットワーク１０に接続された電子制御装置２０，３０間の情報通信を中継する。具体的には、本実施形態における通信部４４は、互いに異なるサブネットワーク１０に接続された複数の電子制御装置２０，３０の間でのデータフレームの送受信を、記憶部４２に記憶されたルーティング情報ＲＩに基づいて実行する。

【００４６】

すなわち、通信部４４が、ルーティング情報ＲＩに基づいて、電子制御装置からのデータフレームを、当該データフレームの受信先が接続されたサブネットワーク１０へと出力する。当該データフレームの送信元が接続されたサブネットワーク１０と、当該データフレームの受信先が接続されたサブネットワーク１０でプロトコルが異なる場合は、プロトコルを変換し、受信先が接続されたサブネットワーク１０へと出力する。これにより、中継装置４０は、周知のゲートウェイ装置として機能する。

【００４７】

制御部４６は、ＲＯＭ，ＲＡＭ，ＣＰＵを少なくとも有した周知のマイクロコンピュータを中心に構成されている。制御部４６のＲＯＭには、メモリレス制御装置３０からのメモリバンク要求に対応する書込要求データを、特定条件を満たす記憶機能付制御装置２０に格納するメモリバンク処理を実行するための処理プログラムが格納されている。ＲＯＭにおいて、メモリバンク処理を実行するための処理プログラムが格納される領域は、電気的に書換可能な不揮発性の記憶領域である。

〈記憶先管理テーブル〉

次に、中継装置４０の記憶部４２に格納される記憶先管理テーブルＭＩは、図２に示すように、ＥＣＵ情報と、記憶データ情報とを備えている。

【００４８】

このうち、ＥＣＵ情報は、車載通信システム１を構成する電子制御装置２０，３０に関する情報である。

このＥＣＵ情報には、電子制御装置２０，３０それぞれのＥＣＵ名と、ＥＣＵＩＤと、各電子制御装置２０，３０に割り当てられた安全要求レベル（ＡＳＩＬクラス）とが含まれている。さらに、ＥＣＵ情報には、当該記憶機能付制御装置２０が備える記憶部２６の記憶可能サイズ（即ち、空き容量）が含まれる。

【００４９】

なお、本実施形態においては、外部サーバ８０や中継装置４０自身は、記憶機能付制御装置２０の一つとして規定される。よって、外部サーバ８０や中継装置４０の名称や、識別情報、安全要求レベル（ＡＳＩＬクラス）、及び外部サーバ８０や中継装置４０が備える不揮発性記憶装置（ストレージ８２、記憶部４２）の空き容量を含む情報が、外部サーバ８０や中継装置４０に関するＥＣＵ情報として作成される。なお、本実施形態の中継装置４０には、ＡＳＩＬクラス（Ｂ）が割り当てられている。また、本実施形態の外部サーバ８０には、最も低い安全性の水準を表す安全要求レベル（即ち、ＡＳＩＬクラス（ＱＭ））が割り当てられている。

【００５０】

そして、外部サーバ８０や中継装置４０に関するＥＣＵ情報は、記憶先管理テーブルＭＩに含まれる。

一方、記憶データ情報は、メモリバンク処理が実行されることで特定条件を満たす記憶機能付制御装置２０の記憶部２６に格納される書込要求データに関する情報である。具体的に、各書込要求データの記憶データ情報には、当該書込要求データの書き込みを要求した要求元のＥＣＵ名（図２中、依頼元ＥＣＵ）、当該書込要求データを識別するデータＩＤ、当該書込要求データのデータサイズが含まれる。さらに、各書込要求データの記憶データ情報には、当該書込要求データに対する暗号化の要否を表す暗号化フラグや、暗号化に用いる鍵を識別する鍵ＩＤが含まれる。

〈書込要求処理〉

次に、各メモリレス制御装置３０の制御部３４が実行する書込要求処理について説明する。

【００５１】

書込要求処理は、起動指令が入力されると起動される。起動指令とは、例えば、イグニッションスイッチがオンされることで発生するイグニッション信号などである。

この書込要求処理が実行されると、図３に示すように、まず、機能実行処理を含む各種処理を実行した結果、書込要求データが発生したか否かを判定する（Ｓ１２０）。

【００５２】

なお、書込要求データとは、メモリレス制御装置３０において各種処理を実行することで発生し、不揮発性記憶装置に記憶する必要が生じたデータである。

この書込要求データとして生成されるデータは、周知のダイアグノーシスの結果や、制御対象に対する周知の故障診断処理の結果として生成された故障情報を含む。例えば、メモリレス制御装置３０がＡＢＳ電子制御装置であれば、ＡＢＳ電子制御装置を構成する部品の故障や、ブレーキ機構の故障を表す故障情報が書込要求データとして生成され発生する。また、書込要求データとして生成されるデータは、当該メモリレス制御装置３０が機能実現処理を実行することで実現する実現要求機能における各種履歴、バックアップデータ、各種設定であっても良い。

【００５３】

そして、Ｓ１２０での判定の結果、書込要求データが未発生であれば（Ｓ１２０：ＮＯ）、書込要求データが発生するまで待機する。書込要求データが発生すると（Ｓ１２０：ＹＥＳ）、その発生した書込要求データを、制御部２４が備える主記憶装置（ＲＡＭ）に

格納する（Ｓ１３０）。
【００５４】
続いて、メモリバンク要求を中継装置４０に対して出力する（Ｓ１４０）。このメモリバンク要求とは、記憶機能付制御装置２０が有する記憶部２６への書込要求データの書き込みを要求する要求信号である。メモリバンク要求には、書込要求データ自身に加えて、当該メモリバンク要求の出力元（当該メモリレス制御装置３０）に割り当てられているＥＣＵＩＤ（以下、「送信元ＩＤ」とも称す）と、当該メモリバンク要求の出力元に割り当てられている安全要求レベルと、暗号化フラグとが含まれている。
【００５５】
さらに、書込要求処理では、中継装置４０からの完了通知を受信したか否かを判定する（Ｓ１５０）。ここで言う完了通知とは、先のＳ１４０にて出力したメモリバンク要求に含まれる書込要求データの書き込みが完了したことを表す信号である。
【００５６】
その完了通知を受信していなければ（Ｓ１５０：ＮＯ）、完了通知を受信するまで待機する。そして、完了通知を受信すると（Ｓ１５０：ＹＥＳ）、先のＳ１３０にて、制御部３４の主記憶装置（ＲＡＭ）に格納した書込要求データを消去する（Ｓ１６０）。
【００５７】
その後、Ｓ１２０へと戻る。
つまり、メモリレス制御装置３０が実行する書込要求処理では、書込要求データが発生した場合、当該書込要求データをメモリレス制御装置３０の制御部２４における主記憶装置に記憶すると共に、中継装置４０に対してメモリバンク要求を出力する。
〈メモリバンク処理〉
次に、中継装置４０の制御部４６が実行するメモリバンク処理について説明する。
【００５８】
このメモリバンク処理は、メモリレス制御装置３０からのメモリバンク要求を通信部４４が受信すると、割り込みで起動されるものである。
このメモリバンク処理は、起動されると、図４に示すように、まず、当該メモリバンク処理の起動要因となったメモリバンク要求から、当該メモリバンク要求に含まれる安全要求レベル（即ち、ＡＳＩＬクラス、以下、「要求元レベル」とも称す）を取得する（Ｓ２１０）。
【００５９】
続いて、Ｓ２１０にて取得した要求元レベル及び記憶部４２に記憶されている記憶先管理テーブルＭＩに基づいて、記憶機能付制御装置２０の一つを書込先候補として選択する（Ｓ２２０）。このＳ２２０では、記憶先管理テーブルＭＩに含まれるＥＣＵ情報において、安全要求レベル（ＡＳＩＬクラス）が要求元レベルと同レベル以上である記憶機能付制御装置２０を書込先候補として選択する。
【００６０】
具体的に、本Ｓ２２０へと最初に移行した場合には、まず、要求元レベルと同レベルの安全要求レベル（以下、「安全要求同レベル」と称す）が割り当てられた記憶機能付制御装置２０であり、かつ、書込要求データのデータサイズよりも大きな空き容量が存在する記憶部２６を有した記憶機能付制御装置２０を書込先候補として選択する。
【００６１】
なお、本実施形態においては、Ｓ２２０にて書込先候補として選択の対象となる記憶機能付制御装置２０には、外部サーバ８０や中継装置４０自身も含まれている。
さらに、メモリバンク処理では、当該メモリバンク処理の起動要因となったメモリバンク要求に基づいて、書込要求データに対する暗号化の要否を判定する（Ｓ２３０）。具体的に、本実施形態のＳ２３０では、メモリバンク要求に含まれている暗号化フラグが立っていれば、書込要求データに対する暗号化が必要であるものと判定し、暗号化フラグが落とされていれば、書込要求データに対する暗号化が不要であるものと判定する。
【００６２】

このＳ２３０での判定の結果、書込要求データに対する暗号化が必要であれば（Ｓ２３０：ＹＥＳ）、書込要求データを暗号化する（Ｓ２４０）。このＳ２４０での暗号化は、予め規定された条件に基づいて選択された鍵を用いた共通鍵暗号にて実施すれば良い。

【００６３】

その後、Ｓ２５０へと移行する。

一方、Ｓ２３０での判定の結果、書込要求データに対する暗号化が不要であれば（Ｓ２３０：ＮＯ）、Ｓ２４０を実行することなく、Ｓ２５０へと移行する。

【００６４】

そのＳ２５０では、先のＳ２２０にて選択した書込先候補が、中継装置４０自身であるか外部装置であるかを判定する。ここで言う外部装置とは、記憶機能付制御装置２０、または外部サーバ８０である。

【００６５】

このＳ２５０での判定の結果、Ｓ２２０にて選択した書込先候補が外部装置であれば、当該書込先候補に対して、書込要求データの書き込みの可否を問い合わせる書込要求を出力する（Ｓ２６０）。続いて、Ｓ２６０にて書込要求を出力した書込先候補からの応答が、書込要求データの書き込みが可能である旨の内容であるか否かを判定する（Ｓ２７０）。

【００６６】

このＳ２７０での判定の結果、書込先候補からの応答が、書込要求データの書き込みが不可能である旨の内容であれば（Ｓ２７０：ＮＯ）、Ｓ２２０へと戻る。そのＳ２２０では、安全要求同レベルが割り当てられ、かつ未選択である記憶機能付制御装置２０が存在すれば、当該未選択である記憶機能付制御装置２０の中から、書込要求データのデータサイズよりも大きな空き容量が存在する記憶部２６を有した一つの記憶機能付制御装置２０を新たな書込先候補として選択する。一方、安全要求同レベルが割り当てられた記憶機能付制御装置２０が存在しなければ、安全要求同レベルよりも高い安全要求レベルが割り当てられた記憶機能付制御装置２０の中から、書込要求データのデータサイズよりも大きな空き容量が存在する記憶部２６を有した一つの記憶機能付制御装置２０を新たな書込先候補として選択する。その後、Ｓ２３０へと移行する。

【００６７】

つまり、Ｓ２２０では、記憶先管理テーブルＭＩに従って、安全要求同レベルが割り当てられた記憶機能付制御装置２０から順に書込先候補を選択する。

一方、Ｓ２７０での判定の結果、書込先候補からの応答が、書込要求データの書き込みが可能である旨の内容であれば（Ｓ２７０：ＹＥＳ）、当該書込先候補を書込先装置として特定し、その当該書込先装置に対して書込要求データを送信する（Ｓ２８０）。この書込要求データを受信した書込先装置は、書込先装置自身が備える記憶部２６に書込要求データを記憶する。その後、Ｓ３００へと移行する。

【００６８】

ところで、Ｓ２５０での判定の結果、Ｓ２２０にて選択した書込先候補が中継装置４０自身であれば、当該中継装置４０自身を書込先装置として特定し、記憶部４２に書込要求データを記憶する（Ｓ２９０）。その後、Ｓ３００へと移行する。

【００６９】

そのＳ３００では、不揮発性記憶装置への書込要求データの書き込みが終了したか否かを判定する。具体的には、書込先装置が外部装置であれば、当該書込先装置からの終了通知を受信した場合に、不揮発性記憶装置への書込要求データの書き込みが終了したものと判定する。一方、書込先装置が中継装置４０自身であれば、中継装置４０の内部にて通知される終了通知に従って不揮発性記憶装置への書込要求データの書き込みが終了したものと判定する。なお、ここで言う終了通知とは、書込要求データの書き込みが終了したことを表す信号である。

【００７０】

このＳ３００での判定の結果、不揮発性記憶装置への書込要求データの書き込みが終了

していなければ（Ｓ３００：ＮＯ）、不揮発性記憶装置への書込要求データの書き込みが終了するまで待機する。そして、不揮発性記憶装置への書込要求データの書き込みが終了すると（Ｓ３００：ＹＥＳ）、記憶部４２に格納されている記憶先管理テーブルＭＩを更新する（Ｓ３１０）。

【００７１】

このＳ３１０における記憶先管理テーブルＭＩの更新では、当該書込要求データを記憶した記憶機能付制御装置２０における記憶部２６の記憶可能サイズを、当該書込要求データを記憶した後の記憶可能サイズへと書き換える。すなわち、記憶先管理テーブルＭＩにおける記憶部２６の記憶可能サイズは、書込要求データのデータサイズ分減少される。

【００７２】

さらに、Ｓ３１０における記憶先管理テーブルＭＩの更新では、当該書込要求データに関する記憶データ情報を、当該書込要求データを記憶した記憶機能付制御装置２０と対応付けて記憶する。すなわち、記憶先管理テーブルＭＩには、記憶データ情報が追加される。

【００７３】

続いて、メモリバンク要求の出力元であるメモリレス制御装置３０に対して完了通知を出力する（Ｓ３２０）。その後、本メモリバンク処理を終了する。

つまり、中継装置４０が実行するメモリバンク処理では、安全要求レベル（ＡＳＩＬクラス）が要求元レベルと同レベル以上である記憶機能付制御装置２０を書込先候補として選択し、当該書込先候補に対して書込要求を出力する。そして、書込要求に対する応答が、書込要求データの書き込みが不可能であれば、安全要求レベルが要求元レベルと同レベル以上である記憶機能付制御装置２０の中から、一つの記憶機能付制御装置２０を新たな書込先候補として選択して書込要求を出力する。

【００７４】

さらに、メモリバンク処理では、書込要求に対する応答が、書込要求データの書き込みが可能であれば、当該書込先候補を書込先装置として特定し、その書込先装置に対して書込要求データを送信する。この書込要求データを受信した書込先装置が、書込先装置自身の不揮発性記憶装置に書込要求データを記憶する。

〈書込処理〉

次に、記憶機能付制御装置２０が実行する書込処理について説明する。

【００７５】

この書込処理は、中継装置４０からの書込要求を通信部２２にて受信すると、割り込みで起動されるものである。

この書込処理は、起動されると、図５に示すように、まず、当該書込処理の起動要因となった書込要求に対応する書込要求データを記憶部２６に書込可能であるか否かを判定する（Ｓ４１０）。Ｓ４１０では、例えば、書込要求データのデータサイズが、記憶部２６の空き容量よりも小さいこと、かつ、記憶機能付制御装置２０が書込処理以外の処理を実行すべき状況でない場合に、書込要求データを記憶部２６に書込可能であるものと判定すれば良い。

【００７６】

このＳ４１０での判定の結果、書込要求データを記憶部２６に書込不可であれば（Ｓ４１０：ＮＯ）、その旨を表す応答を中継装置４０に返答する（Ｓ４２０）。そして、本書込処理を終了する。

【００７７】

一方、Ｓ４１０での判定の結果、書込要求データを記憶部２６に書込可能であれば（Ｓ４１０：ＹＥＳ）、書込要求データを記憶部２６に書込可能である旨を表す応答を中継装置４０に返答する（Ｓ４３０）。続いて、中継装置４０から書込要求データを受信したか否かを判定する（Ｓ４４０）。

【００７８】

このＳ４４０での判定の結果、書込要求データを受信していなければ（Ｓ４４０：ＮＯ

）、受信するまで待機する。そして、書込要求データを受信すると（Ｓ４４０）、その受信した書込要求データを自身の記憶部２６に書き込み格納する（Ｓ４５０）。さらに、Ｓ４５０での記憶部２６への書込要求データの格納が終了すると、中継装置４０に対して終了通知を出力する（Ｓ４６０）。その後、本書込処理を終了する。

【００７９】

つまり、記憶機能付制御装置２０が実行する書込処理では、書込要求に基づく書込要求データを記憶部２６に書き込むことが不可能であれば、不可能である旨を応答し、書き込み可能であれば、可能である旨を応答する。そして、書込処理では、書込要求データを受信すると、記憶機能付制御装置２０が備える不揮発性記憶装置（記憶部２６）に書込要求データを書き込み記憶する。

〈動作例〉

ここで、車載通信システム１の動作例について説明する。

【００８０】

図６に示すように、メモリレス制御装置３０にて書込要求データが発生すると、そのメモリレス制御装置３０は、書込要求処理にて中継装置４０に対してメモリバンク要求を出力する。

【００８１】

そのメモリバンク要求を受信した中継装置４０は、メモリバンク処理を起動する。そして、要求元レベルと同レベルの安全要求レベルが割り当てられた記憶機能付制御装置２０であり、かつ、書込要求データのデータサイズよりも大きな空き容量が存在する記憶部２６を有した一つの記憶機能付制御装置２０を書込先候補（以下、「第一書込先候補」と称す）として選択する。さらに、選択した第一書込先候補に対して書込要求を出力する。

【００８２】

その書込要求を取得した第一書込先候補は、書込要求データを記憶部２６に書き込み可能であれば、書込要求データを書込可能である旨を表す応答を中継装置４０に返答する。その返答を受信した中継装置４０は、第一書込先候補を書込先装置として特定し、その書込先装置に対して書込要求データを出力する。そして、書込要求データを受信した書込先装置（第一書込先候補）は、当該書込要求データを記憶部２６に書き込んで記憶し、終了通知を中継装置４０に出力する。

【００８３】

その終了通知を取得した中継装置４０は、メモリバンク要求を出力したメモリレス制御装置３０に対して完了通知を出力する。

ところで、第一書込先候補が、書込要求データを記憶部２６に書き込み不可能であれば、書込要求データを書込不可能である旨を表す応答を中継装置４０に返答する。その返答を受信した中継装置４０は、安全要求同レベルが割り当てられ、かつ未選択である記憶機能付制御装置２０が存在すれば、当該未選択である記憶機能付制御装置２０の中から、書込要求データのデータサイズよりも大きな空き容量が存在する記憶部２６を有した一つの記憶機能付制御装置２０を新たな書込先候補として選択する。一方、安全要求同レベルが割り当てられた記憶機能付制御装置２０が存在しなければ、安全要求同レベルよりも高い安全要求レベルが割り当てられた記憶機能付制御装置２０の中から、書込要求データのデータサイズよりも大きな空き容量が存在する記憶部２６を有した一つの記憶機能付制御装置２０を新たな書込先候補として選択する。以下、このように選択された新たな書込先候補を、第二書込先候補と称す。

【００８４】

中継装置４０は、第二書込先候補に対して書込要求を出力する。その書込要求を取得した第二書込先候補は、書込要求データを記憶部２６に書き込み可能であれば、書込要求データを書込可能である旨を表す応答を中継装置４０に返答する。その返答を受信した中継装置４０は、第二書込先候補を書込先装置として特定し、その書込先装置に対して書込要求データを出力する。そして、書込要求データを受信した書込先装置（第二書込先候補）は、当該書込要求データを記憶部２６に書き込んで記憶し、終了通知を中継装置４０に出

力する。
【００８５】
その終了通知を取得した中継装置４０は、メモリバンク要求を出力したメモリレス制御装置３０に対して完了通知を出力する。
［実施形態の効果］
以上説明したように、中継装置４０では、メモリバンク要求に基づく書込要求データの書き込み先として適切な書込先装置が特定されるまで、書込先装置の選定を繰り返し実行している。その書込先装置の選定は、書き込み先として適切な記憶機能付制御装置２０が特定されるまで、要求元レベルと同レベルの安全要求レベルが割り当てられた記憶機能付制御装置２０であり、かつ、書込要求データのデータサイズよりも大きな空き容量が存在する記憶部２６を有した一つの記憶機能付制御装置２０から順に、書込先候補として選択することで実施されている。
【００８６】
したがって、中継装置４０によれば、書込先装置の安全要求レベル、ひいては、不揮発性記憶装置の信頼性が担保された記憶機能付制御装置２０を書込先装置として特定することができる。
【００８７】
しかも、車載通信システム１において、書込先装置の選定に用いる安全要求レベルは、実現要求機能を実現する電子制御装置ごとに予め割り当てられたものである。すなわち、車載通信システム１においては、書込先装置の安全レベル（信頼性）を担保する目的で、車載通信システムに新たな構成を付加したり、従来の部品を信頼性が高い部品に変更したりする必要がない。
【００８８】
換言すれば、車載通信システム１においては、信頼性が担保された不揮発性記憶装置に書込要求データを書き込むために、費用が増加することを可能な限り抑制できる。
以上のことから、中継装置４０によれば、可能な限り費用を抑制しつつ、情報の記憶先を信頼性の高い装置とすることができる。
【００８９】
ところで、一般的な車載通信システムにおいては、安全要求レベルが高い実現要求機能を実現する電子制御装置からの書込要求データほど、高い安全性が求められる。
そこで、上記実施形態のメモリバンク処理においては、書込先装置を選定する際に、まず、安全要求同レベルである記憶機能付制御装置２０を書込先候補として選択する。そして、安全要求同レベルであり、かつ未選択の記憶機能付制御装置２０がなくなると、安全要求同レベルよりも高い安全要求レベルが割り当てられた記憶機能付制御装置２０の中から、書込先候補を選択している。
【００９０】
したがって、中継装置４０によれば、書込要求データに対して要求される安全性に応じた書込先装置を決定できる。これにより、車載通信システム１におけるリソースを無駄なく有効に利用できる。
【００９１】
また、上記実施形態のメモリバンク処理では、書込要求データのデータサイズよりも大きな空き容量が存在する記憶部２６を備えた記憶機能付制御装置２０を書込先候補として特定している。この結果、中継装置４０によれば、書込要求データを複数の書込先に分散させることなく、一つの書込先に記憶させることができる。
【００９２】
さらに、メモリバンク処理では、メモリバンク要求に含まれる暗号化フラグが、暗号化が必要である旨を表していれば、書込要求データを暗号化して書込先装置に書き込んでいる。
【００９３】
このため、車載通信システム１によれば、各書込先装置に書き込まれたデータが不正に

取得されたとしても、不正に取得した人物によって当該データの内容が認識させることを防止できる。

【００９４】

しかも、暗号化の要否は、メモリバンク要求に含まれる暗号化フラグに基づいて判定されるため、車載通信システム１によれば、暗号化不要なデータについて暗号化されることを防止でき、不要な処理が実行されることを防止できる。

【００９５】

さらに、メモリバンク処理では、書込先装置の不揮発性記憶装置への書込要求データの書き込みが終了すると、記憶先管理テーブルＭＩとして、当該書込要求データに関する記憶データ情報を、当該書込要求データを記憶した記憶機能付制御装置２０と対応付けて記憶している。

【００９６】

中継装置４０によれば、このような記憶先管理テーブルＭＩに従って、各書込先装置の不揮発性記憶装置に書き込んだ書込要求データを読み出すことができる。このため、中継装置４０によれば、当該データを読み出す際の処理量を低減できる。

【００９７】

なお、メモリバンク処理においては、書込先装置として、中継装置４０自身や外部サーバ８０を特定することができる。中継装置４０が備える記憶部４２や、外部サーバ８０が備えるストレージ８２は、記憶領域のサイズが大きいことから、電子制御装置にて実行される処理プログラムや当該処理プログラムにおける各種設定情報を最新のものへと更新する場合に、古い処理プログラムや設定情報の退避先とすることができる。そして、メモリバンク処理を実行することにより、古い処理プログラムや設定情報を退避させれば、新しい処理プログラムや各種設定情報への更新に失敗したとしても、古い処理プログラムや設定情報へと復元することができる。

［その他の実施形態］

以上、本発明の実施形態について説明したが、本発明は上記実施形態に限定されるものではなく、本発明の要旨を逸脱しない範囲において、様々な態様にて実施することが可能である。

【００９８】

例えば、中継装置４０は、外部ツール８４を介して指令が入力されると、記憶部４２に記憶された記憶先管理テーブルＭＩを書き換えるように構成されていても良いし、制御部４６のＲＯＭにおける書換可能領域に格納された処理プログラムを書き換えるように構成されていても良い。すなわち、中継装置４０は、特許請求の範囲に記載された第一書換手段及び第二書換手段のうちの少なくとも一方を備えていても良い。

【００９９】

前者であれば、車載通信システム１の装置構成が変更された場合などに、新たな記憶先管理テーブルＭＩへと容易に変更することができる。また、後者であれば、処理プログラムを最新のものへと容易に変更することができる。

【０１００】

また、上記実施形態では、メモリバンク要求の出力元をメモリレス制御装置３０としていたが、メモリバンク要求の出力元はメモリレス制御装置３０に限るものではない。例えば、メモリバンク要求の出力元は、記憶機能付制御装置２０であっても良いし、その他の車載装置であっても良い。すなわち、書込要求処理を実行する電子制御装置は、メモリレス制御装置３０に限るものではなく、記憶機能付制御装置２０が書込要求処理を実行しても良い。

【０１０１】

さらに、上記実施形態のメモリバンク処理における書込先候補の選定では、メモリバンク要求に含まれる安全要求レベルに基づいて、安全要求同レベル以上が割り当てられた記憶機能付制御装置２０を書込先候補として選択していたが、この書込先候補の選定では、メモリバンク要求に含まれる送信元ＩＤに基づいて実施しても良い。すなわち、記憶先管

理テーブルＭＩに送信元ＩＤを照合し、当該送信元ＩＤに対応するメモリレス制御装置３０の安全要求レベルを記憶先管理テーブルＭＩから取得して記憶先候補を選択しても良い。

【０１０２】

なお、上記実施形態においては、記憶先管理テーブルＭＩには、メモリレス制御装置３０に関するＥＣＵ情報も含まれていたが、記憶先管理テーブルＭＩに、メモリレス制御装置３０に関するＥＣＵ情報は含まれていなくとも良い。

【０１０３】

ところで、上記実施形態では、各電子制御装置２０，３０として、エンジンＥＣＵや、パワートレインＥＣＵ、ＡＢＳＥＣＵ、ドアＥＣＵなどを想定していたが、本発明における制御装置は、上記実施形態にて想定した要求実現機能を実現する電子制御装置に限るものではない。

【０１０４】

また、上記実施形態における中継装置４０には、ＡＳＩＬクラス（Ｂ）が割り当てられ、外部サーバ８０には、最も低い安全性の水準を表す安全要求レベル（即ち、ＡＳＩＬクラス（ＱＭ））が割り当てられていたが、これらの中継装置４０や外部サーバ８０に割り当てられる安全要求レベルは、これに限るものでない。例えば、中継装置４０及び外部サーバ８０のそれぞれに割り当てられる安全要求レベルは、最も高い安全性の水準を表す安全要求レベル（ＡＳＩＬクラス（Ｄ））であっても良いし、二番目に高い安全性の水準を表す安全要求レベル（ＡＳＩＬクラス（Ｃ））であっても良いし、その他の安全性の水準を表す安全要求レベルであっても良い。

【０１０５】

そして、上記実施形態における車載通信システム１においては、サブネットワーク１０ごとに異なるプロトコルを用いていたが、車載通信システム１においては、複数のサブネットワーク１０にて共通するプロトコルを用いても良いし、全てのサブネットワーク１０において共通のプロトコルを用いても良い。

【０１０６】

また、上記実施形態の車載通信システム１は、通信端末１４や、コネクタ１６を備えていたが、本発明においては、これらの通信端末１４や、コネクタ１６を備えていなくとも良い。

【０１０７】

なお、上記実施形態の構成の一部を、課題を解決できる限りにおいて省略した態様も本発明の実施形態である。また、上記実施形態と変形例とを適宜組み合わせて構成される態様も本発明の実施形態である。また、特許請求の範囲に記載した文言によって特定される発明の本質を逸脱しない限度において考え得るあらゆる態様も本発明の実施形態である。

【０１０８】

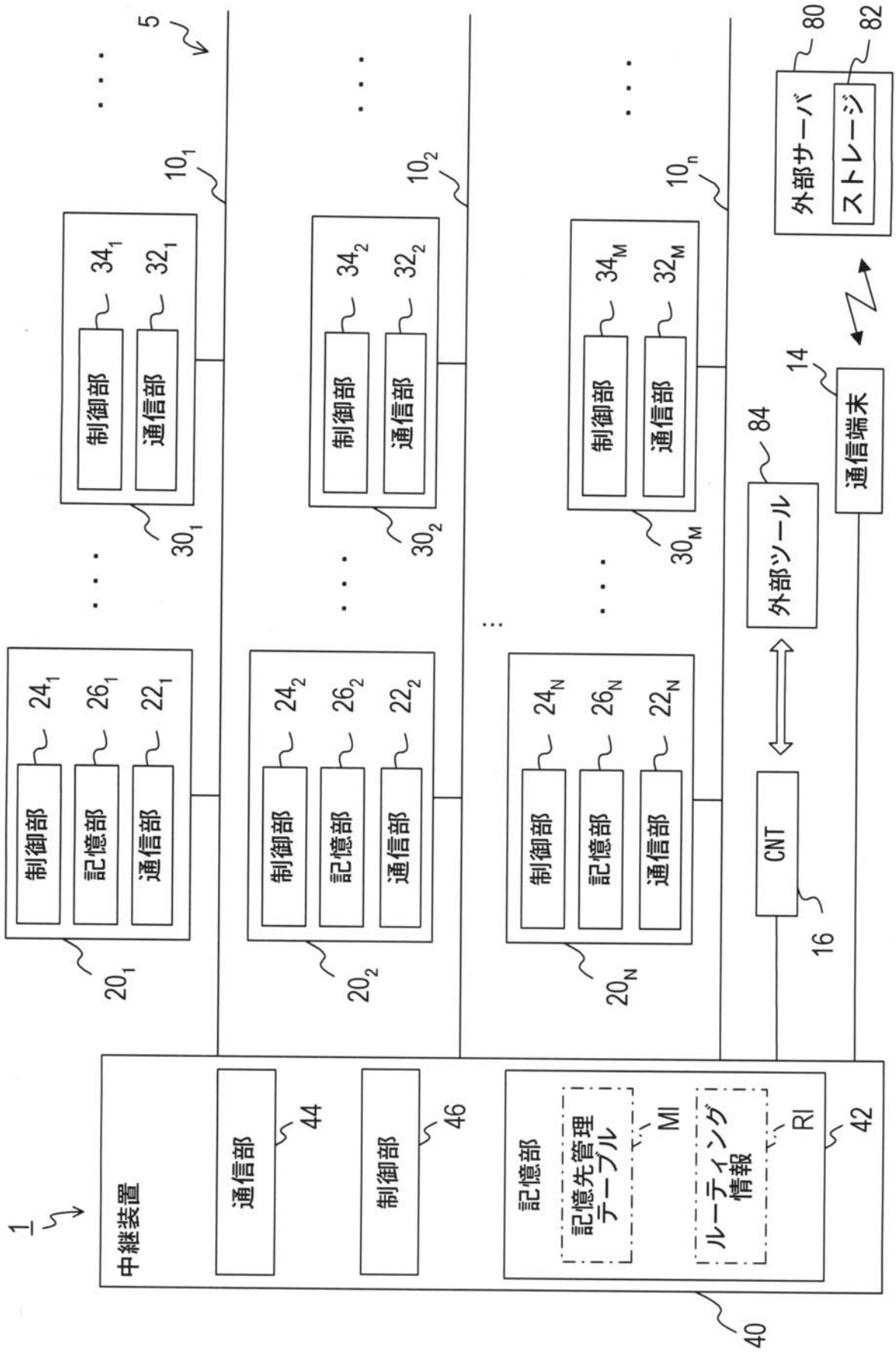
上記実施形態の説明で用いる符号を特許請求の範囲にも適宜使用しているが、各請求項に係る発明の理解を容易にする目的で使用しており、各請求項に係る発明の技術的範囲を限定する意図ではない。

【符号の説明】

【０１０９】

１…車載通信システム　５…車載ネットワーク　１０…サブネットワーク　１４…通信端末　１６…コネクタ　２０，３０…電子制御装置（記憶機能付制御装置，メモリレス制御装置）　２２，３２…通信部、　２４，３４…制御部　２６…記憶部　４０…中継装置　４２…記憶部　４４…通信部　４６…制御部　８０…外部サーバ　８２…ストレージ　８４…外部ツール

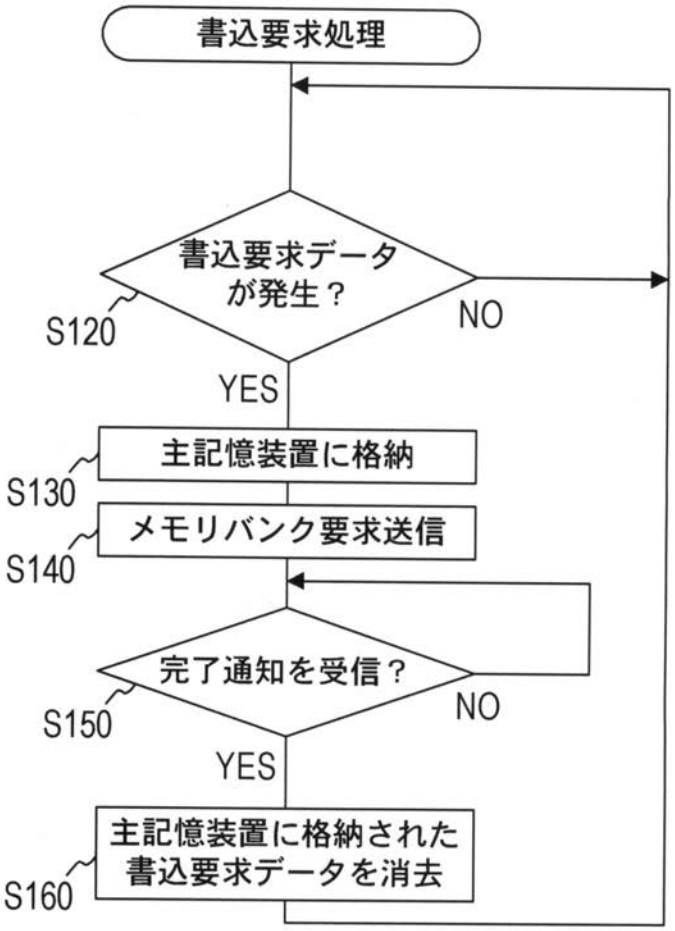
【図１】


1
中継装置
通信部
44
制御部
46
記憶部
記憶先管理テーブル
MI
ルーティング情報
RI
42
40
制御部
記憶部
通信部
24_1
26_1
22_1
20_1
24_2
26_2
22_2
20_2
24_N
26_N
22_N
20_N
10_1
10_2
10_n
5
34_1
32_1
30_1
34_2
32_2
30_2
34_M
32_M
30_M
CNT
16
外部ツール
84
14
通信端末
外部サーバ
80
ストレージ
82

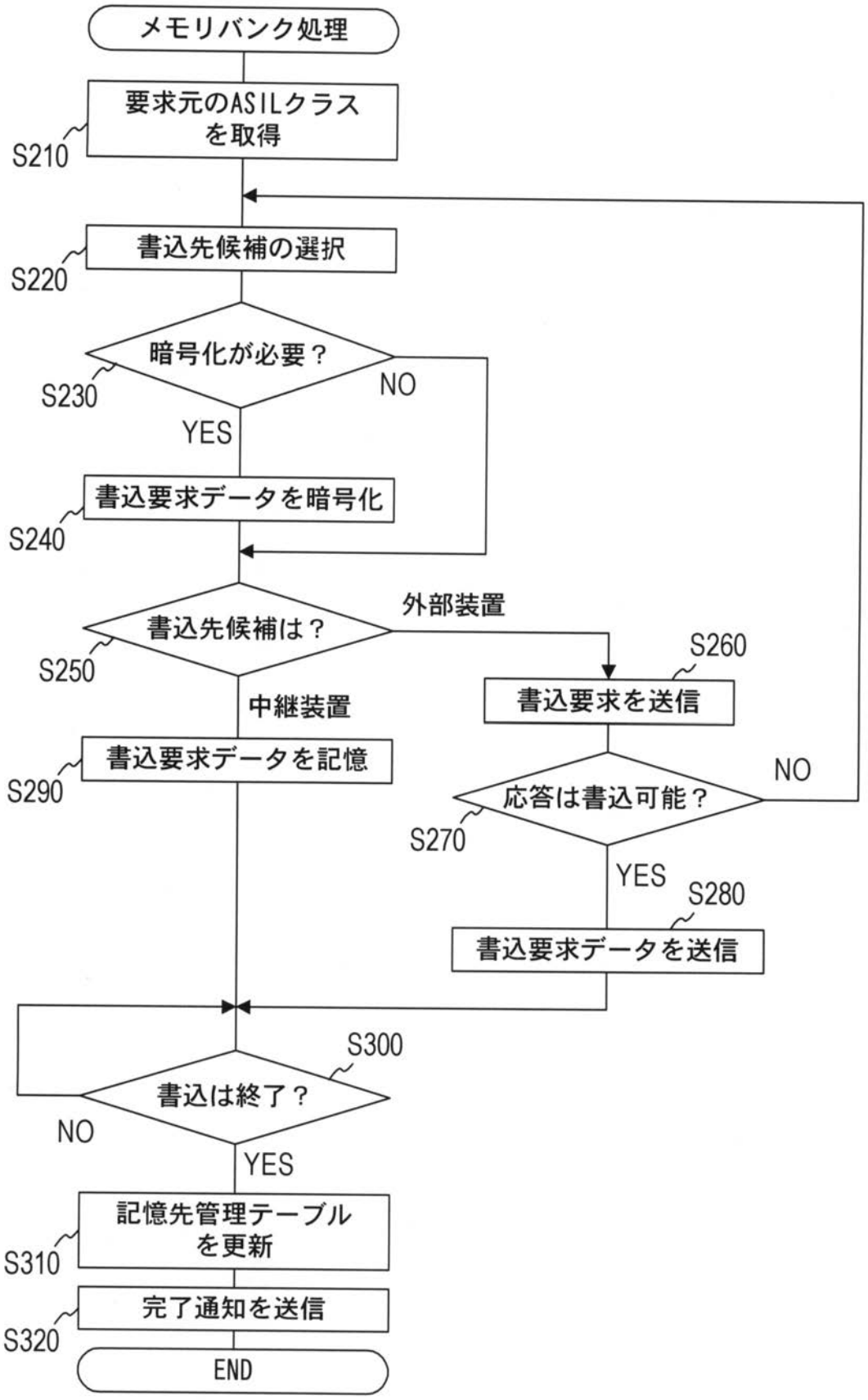
【図２】

ECU 情報				記憶データ情報				
ECU名	ECU ID	ASIL クラス	記憶可能サイズ (空き容量)	依頼元ECU	データ ID	データ サイズ	暗号化 フラグ	鍵 ID
ECU A	aaa	D	64 [kB]	●●	▲▲	8 [B]	ON	#1
				○○	△△	8 [B]	OFF	—
				⋮	⋮	⋮	⋮	⋮
ECU B	bbb	C	16 [kB]	□□	■■	2048 [B]	ON	#2
ECU C	ccc	B	32 [kB]	—	—	—	—	—
⋮	⋮	⋮	⋮		⋮	⋮	⋮	⋮
ECU N	nnn	A	2048 [kB]	—	—	—	—	—
中継装置	abc	B	xxxx [kB]	—	—	—	—	—
外部サーバ	def	—	∞ [kB]	—	—	—	—	—

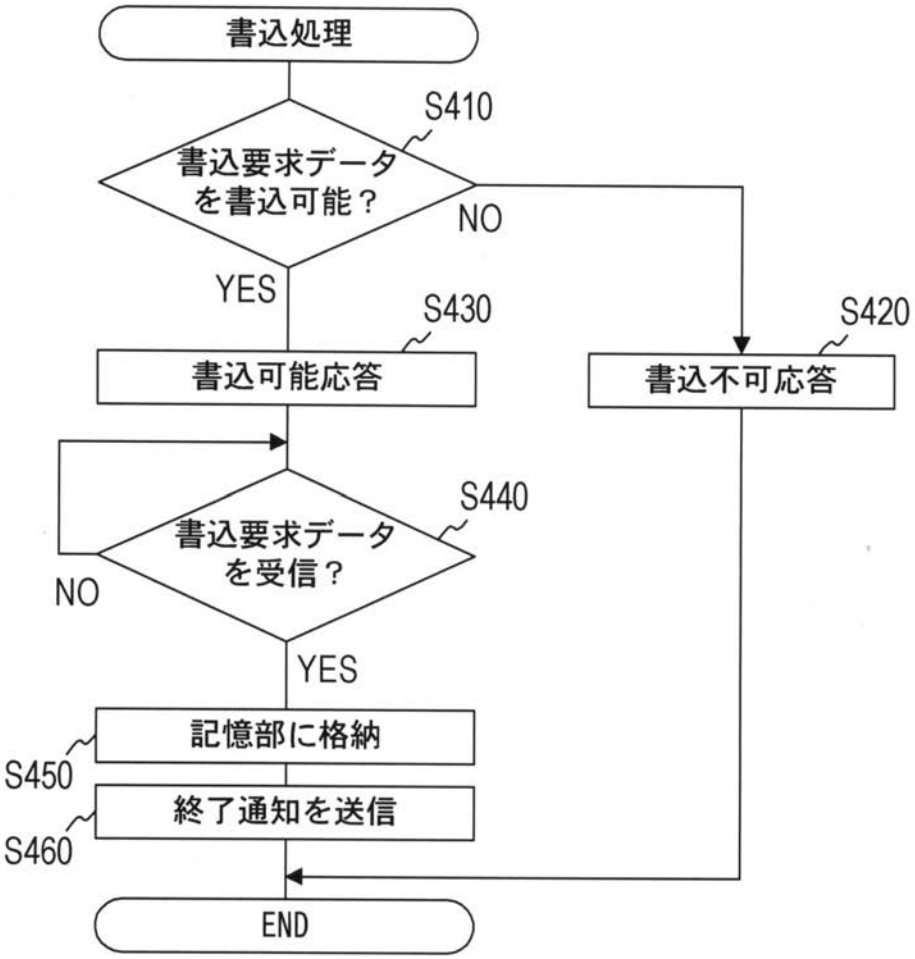
【図３】


書込要求処理
書込要求データが発生？
S120
NO
YES
主記憶装置に格納
S130
メモリバンク要求送信
S140
完了通知を受信？
S150
NO
YES
主記憶装置に格納された書込要求データを消去
S160

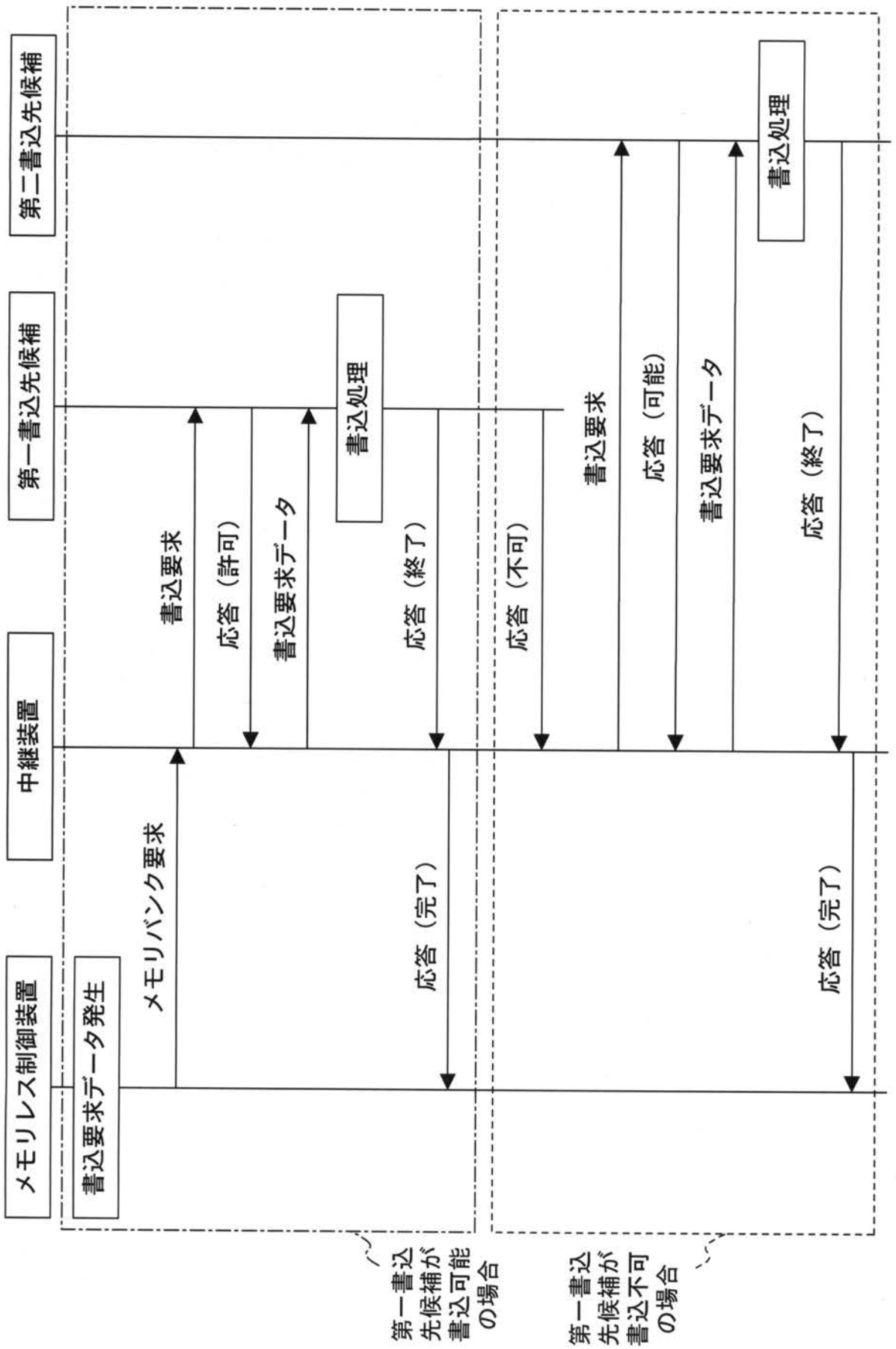
【図４】


メモリバンク処理
要求元のASILクラスを取得
S210
書込先候補の選択
S220
暗号化が必要？
S230
NO
YES
書込要求データを暗号化
S240
書込先候補は？
S250
外部装置
中継装置
S260
書込要求を送信
応答は書込可能？
S270
NO
YES
S280
書込要求データを送信
書込要求データを記憶
S290
書込は終了？
S300
NO
YES
記憶先管理テーブルを更新
S310
完了通知を送信
S320
END

【図５】


書込処理
S410
書込要求データを書込可能？
NO
YES
S420
書込不可応答
S430
書込可能応答
S440
書込要求データを受信？
NO
YES
記憶部に格納
S450
終了通知を送信
S460
END

【図６】


メモリレス制御装置
中継装置
第一書込先候補
第二書込先候補
書込要求データ発生
メモリバンク要求
書込要求
応答（許可）
書込要求データ
書込処理
応答（終了）
応答（完了）
応答（不可）
書込要求
応答（可能）
書込要求データ
書込処理
応答（終了）
応答（完了）
第一書込先候補が書込可能の場合
第一書込先候補が書込不可の場合