(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7581987号
(P7581987)

(45)発行日　令和6年11月13日(2024.11.13)

(24)登録日　令和6年11月5日(2024.11.5)

(51)国際特許分類

Ｇ０６Ｆ　21/62　(2013.01)		Ｇ０６Ｆ	21/62	３１８	
Ｇ０５Ｂ　19/05　(2006.01)		Ｇ０５Ｂ	19/05	Ｌ	

請求項の数　7　（全28頁）

(21)出願番号　特願2021-40012(P2021-40012)
(22)出願日　令和3年3月12日(2021.3.12)
(65)公開番号　特開2022-139565(P2022-139565A)
(43)公開日　令和4年9月26日(2022.9.26)
審査請求日　令和6年1月16日(2024.1.16)

(73)特許権者　000002945
オムロン株式会社
京都府京都市下京区塩小路通堀川東入南不動堂町８０１番地
(74)代理人　110001195
弁理士法人深見特許事務所
(72)発明者　北村 安宏
京都府京都市下京区塩小路通堀川東入南不動堂町８０１番地 オムロン株式会社内
(72)発明者　五十嵐 久則
京都府京都市下京区塩小路通堀川東入南不動堂町８０１番地 オムロン株式会社内
(72)発明者　岡村 弘太郎
京都府京都市下京区塩小路通堀川東入南不動堂町８０１番地 オムロン株式会社内
最終頁に続く

(54)【発明の名称】　制御システムおよびその制御方法

(57)【特許請求の範囲】
【請求項１】
制御対象を制御する制御部と、
前記制御部によって実行されるプログラムと、前記プログラムで参照される複数のデータの各々に対する各アクセス権限とを格納する記憶部と、
前記複数のデータのいずれかに対するアクセス要求を受け付ける入力部と、
前記プログラムを作成するための装置とを備え、
各前記アクセス権限は、異なる権限を持つユーザの各々が実行可能な操作の情報を含み、
前記複数のデータの各々は、前記プログラム内の変数または物理メモリのアドレスにより示されるデータであり、
前記装置は、
変数名ごとのアクセス権限を定義した第１のルール、または、物理メモリごとのアクセス権限を定義した第２のルールに基づいて、前記プログラムを解析し、
解析結果に基づいて、各前記アクセス権限を生成し、
各前記アクセス権限を前記記憶部に出力し、
前記制御部は、
前記入力部から前記複数のデータのいずれかに対するアクセス要求を取得したことに基づいて、各前記アクセス権限を参照し、
各前記アクセス権限に基づいて、前記アクセス要求を送信したユーザが、当該アクセスを要求したデータに対するアクセス権限を有するか否かを判断する、制御システム。

【請求項２】
制御対象を制御する制御部と、
前記制御部によって実行されるプログラムと、前記プログラムで参照される複数のデータの各々に対する各アクセス権限とを格納する記憶部と、
前記複数のデータのいずれかに対するアクセス要求を受け付ける入力部とを備え、
各前記アクセス権限は、異なる権限を持つユーザの各々が実行可能な操作の情報を含み、
前記複数のデータの各々は、前記プログラム内の変数または物理メモリのアドレスにより示されるデータであり、
前記記憶部は、変数名ごとのアクセス権限を定義した第１のルール、または、物理メモリごとのアクセス権限を定義した第２のルールをさらに格納し、
前記制御部は、
他の装置から前記プログラムを取得したことに基づいて、前記第１のルールまたは前記第２のルールを用いて、前記プログラムを解析し、
解析結果に基づいて、各前記アクセス権限を生成し、
各前記アクセス権限を前記記憶部に出力し、
前記入力部から前記複数のデータのいずれかに対するアクセス要求を取得したことに基づいて、各前記アクセス権限を参照し、
各前記アクセス権限に基づいて、前記アクセス要求を送信したユーザが、当該アクセスを要求したデータに対するアクセス権限を有するか否かを判断する、制御システム。
【請求項３】
前記記憶部は、さらに、前記変数または前記物理メモリの各々に対する書込範囲の情報を格納し、
前記制御部は、前記書込範囲の情報に基づいて、アクセス要求のあった前記変数または前記物理メモリに対する書込可能な値の範囲を制限する、請求項１または２に記載の制御システム。
【請求項４】
前記制御部は、前記プログラムで参照される複数のデータのいずれかが更新されたことに基づいて、更新履歴を前記記憶部に格納し、
前記更新履歴は、更新されたデータを示す変数名または物理メモリのアドレスと、前記更新されたデータと、データを更新したユーザのユーザ識別子とを含む、請求項１～３のいずれかに記載の制御システム。
【請求項５】
制御装置の制御方法であって、
前記制御装置によって実行されるプログラムと、前記プログラムで参照される複数のデータの各々に対する各アクセス権限とにアクセスするステップを含み、
各前記アクセス権限は、異なる権限を持つユーザの各々が実行可能な操作の情報を含み、
前記複数のデータの各々は、前記プログラム内の変数または物理メモリのアドレスにより示されるデータであり、
変数名ごとのアクセス権限を定義した第１のルール、または、物理メモリごとのアクセス権限を定義した第２のルールに基づいて、前記プログラムを解析するステップと、
解析結果に基づいて、各前記アクセス権限を生成するステップと、
各前記アクセス権限を出力するステップと、
前記複数のデータのいずれかに対するアクセス要求を取得したことに基づいて、各前記アクセス権限を参照するステップと、
各前記アクセス権限に基づいて、前記アクセス要求を送信したユーザが、当該アクセスを要求したデータに対するアクセス権限を有するか否かを判断するステップとをさらに含む、制御方法。
【請求項６】
前記変数または前記物理メモリの各々に対する書込範囲の情報にアクセスするステップと、

前記書込範囲の情報に基づいて、アクセス要求のあった前記変数または前記物理メモリに対する書込可能な値の範囲を制限するステップとをさらに含む、請求項５に記載の制御方法。

【請求項７】

前記プログラムで参照される複数のデータのいずれかが更新されたことに基づいて、更新履歴を生成するステップをさらに含み、

前記更新履歴は、更新されたデータを示す変数名または物理メモリのアドレスと、前記更新されたデータと、データを更新したユーザのユーザ識別子とを含む、請求項５または６に記載の制御方法。

【発明の詳細な説明】

【技術分野】

【０００１】

本開示は、制御システムに関し、より特定的には、制御システムのアクセスコントロールに関する。

【背景技術】

【０００２】

ＦＡ（Factory Automation）を用いた生産現場で使用される機械や設備は、典型的には、プログラマブルコントローラ（Programmable Logic Controller；以下「ＰＬＣ」とも称す。）等の制御装置によって制御される。これらの制御装置は、変数または物理メモリにより示されるデータを格納する。ユーザは、これらの変数または物理メモリにより示されるデータを参照または変更することで制御装置の設定を確認または変更し得る。また、いくつかのデータは重要な設定を含み得る。そのため、変数または物理メモリ、または変数または物理メモリにより示されるデータごとにセキュリティレベルを適切に設定するアクセスコントロール技術が必要とされている。

【０００３】

制御装置のアクセスコントロールに関し、例えば、特開２０１６－１３４１３７号公報（特許文献１）は、「プログラマブル表示器にアクセスするユーザを識別するためのユーザ管理手段と、ユーザ管理手段によって識別されたユーザに付与されている権限に応じて、制御装置からの情報を含むインターフェイス画面を生成する生成手段と、インターフェイス画面を出力する表示部と、外部装置からのユーザのアクセス要求に応答して、ユーザ管理手段による当該ユーザの識別結果に基づいて当該外部装置との接続を確立するとともに、インターフェイス画面を接続が確立された外部装置へ送出する接続管理手段とを含み、ユーザ管理手段は、それぞれ異なる権限が付与されている複数のユーザのプログラマブル表示器への同時アクセスを阻害する」プログラマブル表示器を開示している（［要約］参照）。

【先行技術文献】

【特許文献】

【０００４】

【文献】特開２０１６－１３４１３７号公報

【発明の概要】

【発明が解決しようとする課題】

【０００５】

特許文献１に開示された技術によると、プログラム内で参照されるデータごとにアクセス権限を設定することができない。したがって、プログラム内で参照されるデータごとにアクセス権限を設定するための技術が必要とされている。

【０００６】

本開示は、上記のような背景に鑑みてなされたものであって、ある局面における目的は、プログラム内で参照されるデータごとにアクセス権限を設定するための技術を提供することにある。

【課題を解決するための手段】

【０００７】
本開示の一例に従えば、制御システムが提供される。制御システムは、制御対象を制御する制御部と、制御部によって実行されるプログラムと、プログラムで参照される複数のデータの各々に対する各アクセス権限とを格納する記憶部と、複数のデータのいずれかに対するアクセス要求を受け付ける入力部とを備える。各アクセス権限は、異なる権限を持つユーザの各々が実行可能な操作の情報を含む。制御部は、入力部から複数のデータのいずれかに対するアクセス要求を取得したことに基づいて、各アクセス権限を参照し、各アクセス権限に基づいて、アクセス要求を送信したユーザが、当該アクセスを要求したデータに対するアクセス権限を有するか否かを判断する。
【０００８】
この開示によれば、制御システムは、プログラムで参照される複数のデータの各々に対する各アクセス権限に基づいて、プログラムで参照される複数のデータの各々に対するアクセス要求を受け付けるか否かを判断することができる。
【０００９】
上記の開示において、複数のデータの各々は、プログラム内の変数または物理メモリのアドレスにより示されるデータである。
【００１０】
この開示によれば、制御システムは、プログラムで参照される複数のデータの各々に対する各アクセス権限に基づいて、各変数または各物理メモリに対するアクセス要求を受け付けるか否かを判断することができる。
【００１１】
上記の開示において、記憶部は、さらに、変数または物理メモリの各々に対する書込範囲の情報を格納する。制御部は、書込範囲の情報に基づいて、アクセス要求のあった変数または物理メモリに対する書込可能な値の範囲を制限する。
【００１２】
この開示によれば、制御システムは、アクセス要求のあった変数または物理メモリに対する書込可能な値の範囲を制限することができる。
【００１３】
上記の開示において、複数のデータの各々に対するアクセス権限は、変数名ごとのアクセス権限を定義した第１のルール、または、物理メモリごとのアクセス権限を定義した第２のルールに基づいて生成される。
【００１４】
この開示によれば、制御システムは、第１のルールまたは第２のルールに基づいて、複数のデータの各々に対するアクセス権限を自動的に生成することができる。
【００１５】
上記の開示において、制御システムは、プログラムを作成するための装置をさらに備える。装置は、第１のルールまたは第２のルールに基づいて、プログラムを解析し、解析結果に基づいて、各アクセス権限を生成し、各アクセス権限を記憶部に出力する。
【００１６】
この開示によれば、制御システムは、装置により、複数のデータの各々に対するアクセス権限を生成することができる。
【００１７】
上記の開示において、記憶部は、第１のルールまたは第２のルールをさらに格納する。制御部は、他の装置からプログラムを取得したことに基づいて、第１のルールまたは第２のルールを用いて、プログラムを解析し、解析結果に基づいて、各アクセス権限を生成し、各アクセス権限を記憶部に出力する。
【００１８】
この開示によれば、制御システムは、制御部により、複数のデータの各々に対するアクセス権限を生成することができる。
【００１９】

上記の開示において、制御部は、プログラムで参照される複数のデータのいずれかが更新されたことに基づいて、更新履歴を記憶部に格納する。更新履歴は、更新されたデータを示す変数名または物理メモリのアドレスと、更新されたデータと、データを更新したユーザのユーザ識別子とを含む。

【００２０】

この開示によれば、制御システムは、プログラムで参照される複数のデータのいずれかが更新されたことに基づいて、更新履歴を生成することができる。また、ユーザは更新履歴を見ることで不正な更新処理があったか否かを確認することができる。

【００２１】

本開示の別の例に従えば、制御システムの制御方法が提供される。制御方法は、制御装置によって実行されるプログラムと、プログラムで参照される複数のデータの各々に対する各アクセス権限とにアクセスするステップを含む。各アクセス権限は、異なる権限を持つユーザの各々が実行可能な操作の情報を含む。制御方法は、複数のデータのいずれかに対するアクセス要求を取得したことに基づいて、各アクセス権限を参照するステップと、各アクセス権限に基づいて、アクセス要求を送信したユーザが、当該アクセスを要求したデータに対するアクセス権限を有するか否かを判断するステップとをさらに含む。

【００２２】

この開示によれば、プログラムで参照される複数のデータの各々に対する各アクセス権限に基づいて、プログラムで参照される複数のデータの各々に対するアクセス要求を受け付けるか否かを判断することができる。

【００２３】

上記の開示において、複数のデータの各々は、プログラム内の変数または物理メモリのアドレスにより示されるデータである。

【００２４】

この開示によれば、プログラムで参照される複数のデータの各々に対する各アクセス権限に基づいて、各変数または各物理メモリに対するアクセス要求を受け付けるか否かを判断することができる。

【００２５】

上記の開示において、制御方法は、変数または物理メモリの各々に対する書込範囲の情報にアクセスするステップと、書込範囲の情報に基づいて、アクセス要求のあった変数または物理メモリに対する書込可能な値の範囲を制限するステップとをさらに含む。

【００２６】

この開示によれば、アクセス要求のあった変数または物理メモリに対する書込可能な値の範囲を制限することができる。

【００２７】

上記の開示において、複数のデータの各々に対するアクセス権限は、変数名ごとのアクセス権限を定義した第１のルール、または、物理メモリごとのアクセス権限を定義した第２のルールに基づいて生成される。

【００２８】

この開示によれば、第１のルールまたは第２のルールに基づいて、複数のデータの各々に対するアクセス権限を自動的に生成することができる。

【００２９】

上記の開示において、制御方法は、または第２のルールに基づいて、プログラムを解析するステップと、解析結果に基づいて、各アクセス権限を生成するステップと、各アクセス権限を出力するステップとをさらに含む。

【００３０】

この開示によれば、複数のデータの各々に対するアクセス権限を生成することができる。

【００３１】

上記の開示において、制御方法は、プログラムで参照される複数のデータのいずれかが更新されたことに基づいて、更新履歴を生成するステップをさらに含む。更新履歴は、更

新されたデータを示す変数名または物理メモリのアドレスと、更新されたデータと、データを更新したユーザのユーザ識別子とを含む。

【００３２】

この開示によれば、プログラムで参照される複数のデータのいずれかが更新されたことに基づいて、更新履歴を生成することができる。また、ユーザは更新履歴を見ることで不正な更新処理があったか否かを確認することができる。

【発明の効果】

【００３３】

ある実施の形態に従うと、プログラム内で参照されるデータごとにアクセス権限を設定することが可能である。

【００３４】

この開示内容の上記および他の目的、特徴、局面および利点は、添付の図面と関連して理解される本開示に関する次の詳細な説明から明らかとなるであろう。

【図面の簡単な説明】

【００３５】

【図１】ある実施の形態に従う制御システム１を備えるネットワークシステム１００の全体構成を模式的に示す図である。

【図２】ある実施の形態に従う制御システム１の構成例を示す外観図である。

【図３】ある実施の形態に従う制御システム１を構成する制御ユニット２００のハードウェア構成例を示す模式図である。

【図４】ある実施の形態に従う制御システム１に接続され得るサポート装置１１０のハードウェア構成例を示す模式図である。

【図５】変数の操作権限情報５００および物理メモリの操作権限情報５１０の一例を示す図である。

【図６】変数の書込範囲情報６００および物理メモリの書込範囲情報６１０の一例を示す図である。

【図７】ユーザアカウント情報７００の一例を示す図である。

【図８】変数のルール８００および物理メモリのルール８１０の一例を示す図である。

【図９】変数マスタ９００および物理メモリマスタ９１０の一例を示す図である。

【図１０】制御ユニット２００に対するアクセス要求の一例を示す図である。

【図１１】アクセスコントロール情報３２２の生成手順の一例を示す図である。

【図１２】制御ユニット２００によるアクセスコントロールの手順の一例を示す図である。

【発明を実施するための形態】

【００３６】

以下、図面を参照しつつ、本開示に係る技術思想の実施の形態について説明する。以下の説明では、同一の部品には同一の符号を付してある。それらの名称および機能も同じである。したがって、それらについての詳細な説明は繰り返さない。

【００３７】

＜Ａ．適用例＞

図１は、本実施の形態に従う制御システム１を備えるネットワークシステム１００の全体構成を模式的に示す図である。図１に示す構成を例に、本実施の形態に従う技術が適用される場面について説明する。

【００３８】

ネットワークシステム１００は、構成として、制御システム１、サーバ装置１２０、表示装置１４０およびゲートウェイ（GW: Gateway）１３０を備える。これらの構成は、ネットワーク１５０を介して、相互に接続され得る。また、ネットワーク１５０は、ゲートウェイ１３０を介して、外部ネットワークであるインターネットに接続されている。ある局面において、ネットワーク１５０は、一般的なネットワークプロトコルであるイーサネット（登録商標）またはＥｔｈｅｒＮｅｔ／ＩＰ（登録商標）により実現されてもよい。

【００３９】

制御システム１は、フィールドネットワーク１６０を介して、フィールドの設備および装置、ならびに、それらに配置されている各種デバイス（センサまたはアクチュエータ等）を含む制御対象１７０に接続されている。

【００４０】

フィールドネットワーク１６０は、データの到達時間が保証される、定周期通信を行うバスまたはネットワークを採用することが好ましい。ある局面において、フィールドネットワーク１６０は、このような定周期通信を行うバスまたはネットワークとして、ＥｔｈｅｒＣＡＴ（登録商標）により実現されてもよい。

【００４１】

サポート装置１１０は、ユーザが制御システム１を運用するのを支援する支援ツールを提供する。また、サポート装置１１０は、制御システム１にプログラムをインストールする機能を備えていてもよい。ある局面において、サポート装置１１０は、パーソナルコンピュータ、タブレット、スマートフォン、またはその他の任意の情報処理装置であってもよい。

【００４２】

一例として、サポート装置１１０は、ＵＳＢ（Universal Serial Bus）により、着脱可能に制御システム１に接続される。このＵＳＢ通信には、通信のセキュリティを確保するために、ユーザ認証を行なうための通信プロトコルが採用され得る。他の例として、サポート装置１１０は、ネットワーク１５０を介して制御システム１と通信してもよい。

【００４３】

サーバ装置１２０は、一例として、データベースシステム、製造実行システム（ＭＥＳ：Manufacturing Execution System）等である。製造実行システムは、制御対象の製造装置または設備からの情報を取得して、生産全体を監視および管理するものであり、オーダ情報、品質情報、出荷情報等を扱うこともできる。また、他の例として、サーバ装置１２０は、情報系サービス（制御対象から各種情報を取得して、マクロ的またはミクロ的な分析等を行う処理）を提供する装置であってもよい。

【００４４】

表示装置１４０は、ユーザからの操作を受けて、制御システム１に対してユーザ操作に応じたコマンド等を出力するとともに、制御システム１での演算結果等をグラフィカルに表示する。ある局面において、表示装置１４０は、液晶ディスプレイまたは有機ＥＬ（Electro-Luminescence）ディスプレイ等の任意の出力装置を備えていてもよい。また、表示装置１４０は、タッチパネルまたはスイッチ等の任意の入力装置を備えていてもよい。

【００４５】

ゲートウェイ１３０は、ネットワーク１５０と外部ネットワーク（インターネット）との間のプロトコル変換と、ファイヤウォールとしての処理とを実行する。

【００４６】

図１に示す構成において、制御システム１（より具体的には制御ユニット２００（図２参照））は、インストールされたプログラムに基づいて、フィールドネットワーク１６０上の制御対象１７０を制御すると共に、ネットワーク１５０上の各装置と通信し得る。ユーザは、制御システム１にインストールされるプログラム内で使用される変数が示す値、または制御システム１の物理メモリが示す値を参照または変更することで、制御システム１の機能を確認または変更し得る。ユーザは、制御ユニット２００にインストールされるプログラムで参照される値として、制御ユニット２００の設定値を参照または更新し得る。当該値は、プログラム中の変数または物理メモリに格納された値として定義される。そのため、ユーザは、プログラム中の変数または物理メモリを指定することで、当該値を参照または更新することができる。なお、制御システム１にインストールされるプログラムで参照される変数が示す値、および制御システム１の物理メモリが示す値は、数値だけでなくキャラクタ等の任意のフォーマットの情報を含むデータであってもよい。

【００４７】

制御システム１は、一例として、ポートクローズ、ＶＰＮ（Virtual Private Network

）有効／無効、および、アクセスコントロールの変更等の重要な命令を含む。これらの重要な命令の変更は、制御システム１が提供する機能およびセキュリティ等に大きな影響を及ぼし得る。そのため、制御システム１は、変数または物理メモリにより示される値ごとにアクセスコントロールを行うための機能を備えることで、制御システム１のセキュリティ機能を向上させる。

【００４８】

より具体的には、制御システム１は、変数の操作権限情報５００および物理メモリの操作権限情報５１０の両方または片方を備える（図５参照）。変数の操作権限情報５００は、変数が示す値ごとのアクセス権限を含む。一例として、変数が示す値とは、ある変数が示す物理メモリのアドレスに格納される値である。物理メモリの操作権限情報５１０は、物理メモリが示す値ごとのアクセス権限を含む。一例として、物理メモリが示す値とは、ある物理メモリのアドレスに格納される値である。また、値とは、変数または物理メモリが示す任意の値を含み、例えば、ＮＵＬＬ等の空を意味する値も含み得る。なお、本実施の形態におけるアクセスとは、読込処理および書込処理等を含み得る。また、本実施の形態におけるアクセス権限とは、読込処理の権限および書込処理等の権限を含み得る。

【００４９】

ある局面において、変数または物理メモリが示す値ごとのアクセス権限は、ユーザアカウントの権限または属性（管理者または設計者等）ごとに設定されていてもよい。他の局面において、変数または物理メモリが示す値ごとのアクセス権限は、個別のユーザアカウントごとに設定されていてもよい。なお、これ以降、アクセス権限をデータ（値）へのアクセス権限として説明するが、本実施の形態におけるアクセス権限は参照（Reference）のアクセス権限であるとも言える。ここでの参照とは、データの所在を示す変数および物理アドレス等を意味する。そのため、変数が示すデータ（値）または物理アドレスが示すデータ（値）に対するアクセス権限とは、参照に対するアクセス権限であるとも言える。

【００５０】

そのため、変数または物理アドレスが示すデータ（値）に対するアクセス要求およびアクセス権限を参照（変数または物理アドレス）に対するアクセス要求およびアクセス権限と読み替えても本開示の技術は成立する。この場合、図５および図６に示す変数５０１，６０１および物理メモリ５１１，６１１等は、参照に読み替えることもできる。また、図８に示す変数名ルール８１０および物理メモリ範囲８１１は、参照名ルールおよび参照の範囲と読み替えることもできる。

【００５１】

制御システム１は、変数または物理メモリが示す値に対するアクセス要求を受け付けたことに基づいて、ユーザアカウントの権限を特定する。次に、制御システム１は、変数の操作権限情報５００または物理メモリの操作権限情報５１０を参照して、アクセス要求を送信したユーザアカウントが、アクセス要求のあった変数の値を変更する権限を有するか否かを判定する。変数の操作権限情報５００および物理メモリの操作権限情報５１０およびその生成方法等については後述する。

【００５２】

なお、あるユーザアカウントが値Ｘに対して読込または書込権限を有するとは、当該ユーザアカウントは変数または物理メモリが示す値Ｘを参照または更新する権限があることを意味する。また、あるユーザアカウントが変数Ａに対して読込または書込権限を有するとは、当該ユーザアカウントは変数Ａが示す値を参照または更新する権限を有することを意味する。また、あるユーザアカウントが、物理メモリＢに対して読込または書込権限を有するとは、当該ユーザアカウントは物理メモリＢが示す値（物理メモリＢに格納された値）を参照または更新する権限があることを意味する。

【００５３】

＜Ｂ．ハードウェア構成＞

次に、本実施の形態に従うネットワークシステム１００が備える各装置のハードウェア構成について説明する。

【００５４】
（ａ．制御システム１の外観）
図２は、本実施の形態に従う制御システム１の構成例を示す外観図である。図２を参照して、制御システム１は、制御ユニット２００、セキュリティユニット２１０、セーフティユニット２２０、１または複数の機能ユニット２３０、および電源ユニット２４０を含む。
【００５５】
制御ユニット２００とセキュリティユニット２１０との間は、ＰＣＩ Ｅｘｐｒｅｓｓのバス等を介して接続される。また、制御ユニット２００、セーフティユニット２２０、１または複数の機能ユニット２３０、および電源ユニット２４０は、内部バスを介して相互に接続されている。
【００５６】
制御ユニット２００は、例えばＰＬＣ（プログラムブルコントローラ）を含む。制御ユニット２００は、制御プログラムを実行することで、制御対象を制御する。制御プログラムは、制御対象である設備および装置、ならびに、それらに配置されている各種デバイス（センサまたはアクチュエータ等）との間で信号を遣り取りするＩＯリフレッシュ、制御演算処理等のプログラムを含む。具体的には、ＩＯリフレッシュは、制御ユニット２００において算出される指令値を制御対象へ出力、あるいは、制御対象からの入力値を収集する。制御演算処理は、例えば、ＩＯリフレッシュにより収集した入力値に基づいた指令値または制御量を算出する。このような機能を備える制御プログラムは、制御対象の要求仕様に従ってユーザまたは開発会社が作成するプログラムを含む「ユーザプログラム」の一例でもある。
【００５７】
セキュリティユニット２１０は、制御システム１の、より特定的には制御ユニット２００のセキュリティを設定する。このセキュリティの設定には、制御プログラムの意図しない複製、すなわち不正な複製を防止するための設定が含まれる。セーフティユニット２２０は、制御ユニット２００とは独立して、制御対象に関するセーフティ機能を実現するための制御演算を実行する。機能ユニット２３０は、制御システム１による様々な制御対象に対する制御を実現するための各種機能を提供する。機能ユニット２３０は、典型的には、Ｉ／Ｏユニット、セーフティＩ／Ｏユニット、通信ユニット、モーションコントローラユニット、温度調整ユニット、パルスカウンタユニット等を包含し得る。Ｉ／Ｏユニットとしては、例えば、デジタル入力（ＤＩ）ユニット、デジタル出力（ＤＯ）ユニット、アナログ出力（ＡＩ）ユニット、アナログ出力（ＡＯ）ユニット、パルスキャッチ入力ユニット、および、複数の種類を混合させた複合ユニット等が挙げられる。セーフティＩ／Ｏユニットは、セーフティ制御に係るＩ／Ｏ処理を担当する。電源ユニット２４０は、制御システム１を構成する各ユニットに対して、所定電圧の電源を供給する。
【００５８】
（ｂ．制御ユニット２００のハードウェア構成）
次に、本実施の形態に従う制御システム１が含む制御ユニット２００のハードウェア構成例について説明する。
【００５９】
図３は、本実施の形態に従う制御システム１を構成する制御ユニット２００のハードウェア構成例を示す模式図である。図３を参照して、制御ユニット２００は、主たるコンポーネントとして、ＣＰＵ（Central Processing Unit）またはＧＰＵ（Graphical Processing Unit）等のプロセッサ３０１、チップセット３０２、二次記憶装置３０３、主記憶装置３０４、通信コントローラ３０５、ＵＳＢコントローラ３１４、メモリカードインターフェイス３１３、ネットワークコントローラ３１０，３１１，３１２、内部バスコントローラ３０９、インジケータ３０６、およびスイッチインターフェイス３０７を含む。
【００６０】
プロセッサ３０１は、二次記憶装置３０３に格納された各種プログラムを読み出して、

主記憶装置３０４に展開して実行することで、制御演算およびサービス処理を含む各種の処理を実現する。チップセット３０２は、プロセッサ３０１と各コンポーネントとの間のデータの遣り取りを仲介することで、制御ユニット２００全体としての処理を実現する。

【００６１】

主記憶装置３０４は、ＤＲＡＭ（Dynamic Random Access Memory）またはＳＲＡＭ（Static Random Access Memory）等の揮発性記憶装置を備える。これら揮発性記憶装置の少なくとも一部は、復号済み制御プログラム３２６を格納するための揮発性記憶領域３２５を構成する。

【００６２】

二次記憶装置３０３は、典型的には、例えば、ＨＤＤ（Hard Disk Drive）またはＳＳＤ（Solid State Drive）、ＲＯＭ（Read Only Memory）、ＥＰＲＯＭ（Erasable Programmable Read Only Memory)、ＥＥＰＲＯＭ（Electrically Erasable Programmable Read-Only Memory）等の不揮発性記憶装置を備える。これら不揮発性記憶装置の少なくとも一部は、暗号化済み制御プログラム３２４を格納するための不揮発性記憶領域３２３を構成する。

【００６３】

二次記憶装置３０３は、さらに、ＯＳを含むシステムプログラム３２０、サービスプログラム３２１、およびアクセスコントロール情報３２２等を格納する。アクセスコントロール情報３２２は、図５～図９に示す、変数または物理メモリが示す値におけるアクセスコントロールのために使用される各種情報を含む。システムプログラム３２０は、復号済み制御プログラム３２６およびサービスプログラム３２１等のユーザプログラムが動作するためのプログラム実行環境を提供する。

【００６４】

通信コントローラ３０５は、バス３３０を介して、セキュリティユニット２１０とデータを送受信する。通信コントローラ３０５は、例えば、ＰＣＩ Ｅｘｐｒｅｓｓ等のバスに対応した通信チップにより実現され得る。

【００６５】

インジケータ３０６は、制御ユニット２００の動作状態等を通知するものであり、ユニット表面に配置された１または複数のＬＥＤ（Light Emitting Diode）等で構成される。スイッチインターフェイス３０７は、一例として、ディップスイッチ３０８と接続されており、当該ディップスイッチ３０８のＯＮまたはＯＦＦの信号をプロセッサ３０１に出力する。

【００６６】

内部バスコントローラ３０９は、制御システム１を構成するセーフティユニット２２０と、１または複数の機能ユニット２３０との間で、内部バスを介してデータを送受信する。この内部バスには、メーカ固有の通信プロトコルを用いてもよいし、いずれかの産業用ネットワークプロトコルと同一あるいは準拠した通信プロトコルを用いてもよい。

【００６７】

ネットワークコントローラ３１０，３１１，３１２の各々は、ネットワークを介した任意のデバイスとの間のデータの遣り取りを担当する。ネットワークコントローラ３１０，３１１，３１２は、ＥｔｈｅｒＣＡＴ（登録商標）、ＥｔｈｅｒＮｅｔ／ＩＰ（登録商標）、ＤｅｖｉｃｅＮｅｔ（登録商標）、ＣｏｍｐｏＮｅｔ（登録商標）等の産業用ネットワークプロトコルを採用してもよい。

【００６８】

メモリカードインターフェイス３１３は、メモリカード３４０を着脱可能に構成されており、メモリカード３４０に対してユーザプログラムまたは各種設定等のデータを書込み、あるいは、メモリカード３４０から当該プログラムまたは各種設定等のデータを読出すことが可能になっている。ＵＳＢコントローラ３１４は、ＵＳＢ接続を介して、サポート装置１１０を含む任意の情報処理装置とデータを送受信し得る。

【００６９】

図３には、プロセッサ３０１がプログラムを実行することで必要な機能が提供される構成例を示したが、これらの提供される機能の一部または全部を、専用のハードウェア回路（例えば、ＡＳＩＣ（Application Specific Integrated Circuit）またはＦＰＧＡ（Field-Programmable Gate Array）等）を用いて実装してもよい。あるいは、制御ユニット２００の主要部を、汎用的なアーキテクチャに従うハードウェア（例えば、汎用パソコンをベースとした産業用パソコン）を用いて実現してもよい。この場合には、仮想化技術を用いて、用途の異なる複数のＯＳを並列的に実行させるとともに、各ＯＳ上で必要なアプリケーションを実行させるようにしてもよい。

【００７０】

（ｃ．サポート装置１１０のハードウェア構成）

次に、本実施の形態に従う制御システム１に接続され得るサポート装置１１０のハードウェア構成例について説明する。

【００７１】

図４は、本実施の形態に従う制御システム１に接続され得るサポート装置１１０のハードウェア構成例を示す模式図である。サポート装置１１０は、一例として、汎用的なアーキテクチャに従う装置（パーソナルコンコンピュータまたはタブレット等）を用いて実現され得る。

【００７２】

図４を参照して、サポート装置１１０は、ＣＰＵまたはＧＰＵ等のプロセッサ４０１、主記憶装置４０２、入力部４０３、出力部４０４、二次記憶装置４０５、光学ドライブ４０６、および通信インターフェイス４０７を含む。これらのコンポーネントは、プロセッサバス４１０を介して接続されている。主記憶装置４０２および二次記憶装置４０５は、それぞれ、制御ユニット２００の主記憶装置３０４および二次記憶装置３０３と同様に構成することができるので、それらの説明を繰返さない。

【００７３】

プロセッサ４０１は、二次記憶装置４０５に格納されたプログラム（一例として、ＯＳ４２４およびサポートプログラム４２３）を読出して、主記憶装置４０２に展開して実行することで、各種処理を実現する。

【００７４】

二次記憶装置４０５は、基本的な機能を実現するためのＯＳ４２４に加えて、サポート装置１１０としての機能を提供するためのサポートプログラム４２３を格納する。サポート装置１１０（実質的にはプロセッサ４０１）は、サポートプログラム４２３を実行することで、サポート装置１１０が提供する各種サポートツールの機能を実現する。当該サポートツールは、サポート装置１１０におけるプログラムの開発環境を提供する。

【００７５】

また、二次記憶装置４０５は、サポートツールを用いて作成された制御プログラム４２０と、変数／物理メモリの操作権限情報生成プログラム４２１と、変数／物理メモリの書込範囲情報生成プログラム４２２とを格納する。制御プログラム４２０は、制御ユニット２００で実行されるプログラムのソースコードであってもよい。また、制御プログラム４２０は、制御ユニット２００で実行されるプログラムの実行ファイルを含んでいてもよい。

【００７６】

変数／物理メモリの操作権限情報生成プログラム４２１は、変数のルール８００および物理メモリのルール８１０（図８参照）を参照して、制御プログラム４２０に含まれる変数または物理メモリが示す値の各々のアクセス権限を含む変数の操作権限情報５００または物理メモリの操作権限情報５１０を生成する。

【００７７】

変数／物理メモリの書込範囲情報生成プログラム４２２は、制御プログラム４２０に含まれる変数または物理メモリの各々における、書き込み可能な値の範囲を含む変数の書込範囲情報６００または物理メモリの書込範囲情報６１０（図６参照）を生成する。ある局面において、変数／物理メモリの書込範囲情報生成プログラム４２２は、操作権限情報５

００または物理メモリの操作権限情報５１０に基づいて、変数の書込範囲情報６００または物理メモリの書込範囲情報６１０（図６参照）を生成してもよい。この場合、二次記憶装置４０５は、変数または物理メモリのセキュリティレベルごとに予め定められた書き込み範囲の情報を格納する。変数または物理メモリのセキュリティレベルは、例えば、どの権限（管理者、設計者等）のユーザアカウントが当該変数または物理メモリが示す値にアクセス可能なのかによって決定され得る。

【００７８】

また、ある局面において、二次記憶装置４０５は、制御プログラム４２０を暗号化した暗号化済み制御プログラムを格納してもよい。さらに、二次記憶装置４０５は、制御プログラム４２０の暗号化のための鍵、および暗号化処理プログラムを格納してもよい。また、二次記憶装置４０５は、簡易暗号化処理プログラムを格納してもよい。プロセッサ４０１は、簡易暗号化処理プログラムを実行することで、簡易暗号化済み制御プログラムを生成し得る。

【００７９】

入力部４０３は、キーボードまたはマウス等で構成され、ユーザ操作を受け付ける。出力部４０４は、ディスプレイ、各種インジケータ、プリンタ等で構成され、プロセッサ４０１からの処理結果等を出力する。

【００８０】

サポート装置１１０は、光学ドライブ４０６を有する。光学ドライブ４０６は、記録媒体４５０（例えば、ＤＶＤ（Digital Versatile Disc）等の光学記録媒体）から、その中に格納されたプログラムを読み取り、当該プログラムを二次記憶装置４０５等にインストールする。

【００８１】

通信インターフェイス４０７は、ＵＳＢまたはイーサネット等の任意の通信媒体を介して、制御システム１が備える制御ユニット２００またはセキュリティユニット２１０とデータを送受信し得る。

【００８２】

サポート装置１１０で実行されるサポートプログラム４２３等は、コンピュータ読取可能な記録媒体４５０を介してインストールされてもよいが、ネットワーク上のサーバ装置等からダウンロードする形でインストールされてもよい。また、本実施の形態に従うサポート装置１１０が提供する機能は、ＯＳが提供するモジュールの一部を利用する形で実現され得る。

【００８３】

図４には、プロセッサ４０１がプログラムを実行することで、サポート装置１１０として必要な機能が提供される構成例を示したが、これらの提供される機能の一部または全部を、専用のハードウェア回路（例えば、ＡＳＩＣまたはＦＰＧＡ等）を用いて実装してもよい。また、本実施の形態では、制御システム１の稼動中に、サポート装置１１０が、制御システム１から取り外されていてもよい。

【００８４】

サポート装置１１０は、生成した制御プログラム４２０または暗号化済み制御プログラムを制御ユニット２００に送信する。さらに、サポート装置１１０は、変数の操作権限情報５００または物理メモリの操作権限情報５１０と、変数の書込範囲情報６００または物理メモリの書込範囲情報６１０とを制御ユニット２００に送信する。制御ユニット２００は、受信した変数の操作権限情報５００または物理メモリの操作権限情報５１０と、変数の書込範囲情報６００または物理メモリの書込範囲情報６１０とをアクセスコントロール情報３２２の一部として、二次記憶装置３０３に格納する。

【００８５】

制御ユニット２００は、制御プログラム４２０内で参照される変数または物理メモリが示す値に対してアクセス要求があった場合、変数の操作権限情報５００または物理メモリの操作権限情報５１０を参照することで、アクセス要求を受け付けるか拒否するかを判断

し得る。

【００８６】

また、制御ユニット２００は、アクセス要求が書込要求であった場合に、変数の書込範囲情報６００または物理メモリの書込範囲情報６１０を参照することで、当該書込要求を受け付けるか拒否するかを判断し得る。

【００８７】

ある局面において、制御ユニット２００は、変数／物理メモリの操作権限情報生成プログラム４２１と、変数／物理メモリの書込範囲情報生成プログラム４２２とを二次記憶装置３０３に予め格納してもよい。この場合、制御ユニット２００は、受信した制御プログラム４２０または暗号化済み制御プログラムから、変数の操作権限情報５００または物理メモリの操作権限情報５１０と、変数の書込範囲情報６００または物理メモリの書込範囲情報６１０とを生成する。

【００８８】

＜Ｃ．アクセスコントロール情報＞

次に、変数または物理メモリが示す値ごとのアクセスコントロールを実現するためのアクセスコントロール情報３２２が含む各種情報について説明する。

【００８９】

図５は、変数の操作権限情報５００および物理メモリの操作権限情報５１０の一例を示す図である。変数の操作権限情報５００は、ユーザアカウントの権限ごとの各変数に対する読出および書込の操作制限（アクセス権限）を示す。物理メモリの操作権限情報５１０は、ユーザアカウントの権限ごとの各物理メモリに対する読出および書込の操作制限（アクセス権限）を示す。

【００９０】

ある局面において、変数の操作権限情報５００および物理メモリの操作権限情報５１０は、リレーショナルデータベースのテーブルとして表現されてもよいし、ＪＳＯＮ（JavaScript（登録商標） Object Notation）等の他の任意のデータ形式で表現されてもよい。

【００９１】

変数の操作権限情報５００は、データ項目として、変数５０１と、操作５０２と、ユーザアカウントの権限ごとのアクセス制限５０３とを含む。さらに、変数の操作権限情報５００は、各レコードを一意に識別するための識別子を含んでいてもよい。

【００９２】

変数５０１は、制御プログラム４２０に含まれる各々の変数名を含む。操作５０２は、少なくとも２つの操作方法である読出および書込を含む。読出は、ある変数が示す値を参照する操作である。書込は、ある変数が示す値を変更または上書きする操作である。アクセス制限５０３は、ユーザアカウントの権限ごとの読出および書込の制限である。

【００９３】

図５に示す例では、「管理者」のユーザアカウントは、変数「ＡＡＡＡＡＡＡ」に対して読出および書込の両方の権限を有する。逆に、「操作者」のユーザアカウントは、変数「ＡＡＡＡＡＡＡ」に対して読出および書込の両方の権限を有さない。また、変数「ＡＡＡＡＡＡ」に関して、「管理者、設計者」のみが読出および書込の両方の権限を有する。一方で、変数「ＢＢＢＢＢＢＢ」に関して、より多くのユーザアカウント「管理者、設計者、保全者」が読出および書込の両方の権限を有する。この場合、変数「ＡＡＡＡＡＡＡ」のセキュリティレベルは、変数「ＢＢＢＢＢＢＢ」のセキュリティレベルよりも高いといえる。

【００９４】

物理メモリの操作権限情報５１０は、データ項目として、物理メモリ５１１と、操作５１２と、ユーザアカウントの権限ごとのアクセス制限５１３とを含む。さらに、物理メモリの操作権限情報５１０は、各レコードを一意に識別するための識別子を含んでいてもよい。

【００９５】

物理メモリ５１１は、制御プログラム４２０に含まれる各々の物理メモリのアドレスを含む。ある局面において、物理メモリ５１１は、物理メモリのアドレスの範囲を含んでいてもよい。操作５１２は、少なくとも２つの操作方法である読出および書込を含む。読出は、ある物理メモリが示す値を参照する操作である。書込は、ある物理メモリが示す値を変更または上書きする操作である。アクセス制限５１３は、ユーザアカウントの権限ごとの読出および書込の制限である。

【００９６】

図５に示す例では、「管理者」のユーザアカウントは、物理メモリ「Ｄ００００」に対して読出および書込の両方の権限を有する。逆に、「操作者」のユーザアカウントは、物理メモリ「Ｄ００００」に対して読出および書込の両方の権限を有さない。また、物理メモリ「Ｄ００００」に関して、「管理者、設計者」のみが読出および書込の両方の権限を有する。一方で、物理メモリ「Ｄ００００１」に関して、より多くのユーザアカウント「管理者、設計者、保全者」が読出および書込の両方の権限を有する。この場合、物理メモリ「Ｄ００００」のセキュリティレベルは、物理メモリ「Ｄ００００１」のセキュリティレベルよりも高いといえる。

【００９７】

制御プログラム４２０が変数を含む場合、制御ユニット２００またはサポート装置１１０は、変数の操作権限情報５００を生成する。逆に、制御プログラム４２０が物理メモリを含む場合、制御ユニット２００またはサポート装置１１０は、物理メモリの操作権限情報５１０を生成する。ある局面において、制御プログラム４２０が変数および物理メモリの両方を含む場合、制御ユニット２００またはサポート装置１１０は、変数の操作権限情報５００および物理メモリの操作権限情報５１０を組み合わせた情報を生成し、当該情報をアクセスコントロールに使用してもよい。

【００９８】

制御ユニット２００は、変数の操作権限情報５００または物理メモリの操作権限情報５１０と、ユーザアカウント情報７００（図７参照）とに基づいて、変数または物理メモリが示す値に対するアクセス要求を受け付けるか否かを判断する。

【００９９】

図６は、変数の書込範囲情報６００および物理メモリの書込範囲情報６１０の一例を示す図である。変数の書込範囲情報６００は、ユーザアカウントの権限ごとの各変数に書き込み可能な値の範囲を示す。物理メモリの書込範囲情報６１０は、ユーザアカウントの権限ごとの各物理メモリに書き込み可能な値の範囲を示す。

【０１００】

ある局面において、変数の書込範囲情報６００および物理メモリの書込範囲情報６１０は、リレーショナルデータベースのテーブルとして表現されてもよいし、ＪＳＯＮ（JavaScript（登録商標） Object Notation）等の他の任意のデータ形式で表現されてもよい。

【０１０１】

変数の書込範囲情報６００は、データ項目として、変数６０１と、書込範囲６０２と、ユーザアカウントの権限ごとの書込操作制限６０３とを含む。さらに、変数の書込範囲情報６００は、各レコードを一意に識別するための識別子を含んでいてもよい。

【０１０２】

変数６０１は、制御プログラム４２０に含まれる各々の変数名を含む。書込範囲６０２は、ある変数に書き込むことができる値の範囲である。書込操作制限６０３は、ユーザアカウントの権限ごとの書込範囲６０２が示す値の書込操作制限である。

【０１０３】

図６に示す例では、「管理者」のユーザアカウントは、変数「ＣＣＣＣＣＣＣ」に対して値「０－１００」を書き込むことができる。「保全者」のユーザアカウントは、変数「ＣＣＣＣＣＣＣ」に対して値「５０－９０」を書き込むことができる。「操作者」のユーザアカウントは、変数「ＣＣＣＣＣＣＣ」に対して値「５０」のみを書き込むことができる。

【０１０４】
物理メモリの書込範囲情報６１０は、データ項目として、物理メモリ６１１と、書込範囲６１２と、ユーザアカウントの権限ごとの書込操作制限６１３とを含む。さらに、物理メモリの書込範囲情報６１０は、各レコードを一意に識別するための識別子を含んでいてもよい。
【０１０５】
物理メモリ６１１は、制御プログラム４２０に含まれる各々の物理メモリのアドレスを含む。ある局面において、物理メモリ５１１は、物理メモリのアドレスの範囲を含んでいてもよい。書込範囲６１２は、ある物理メモリに書き込むことができる値の範囲である。書込操作制限６１３は、ユーザアカウントの権限ごとの書込操作制限である。
【０１０６】
図６に示す例では、「管理者」のユーザアカウントは、物理メモリのアドレス「Ｄ０００２」に対して値「０－１００」を書き込むことができる。「保全者」のユーザアカウントは、変数「Ｄ０００２」に対して値「５０－９０」を書き込むことができる。「操作者」のユーザアカウントは、変数「Ｄ０００２」に対して値「５０」のみを書き込むことができる。
【０１０７】
制御プログラム４２０が変数を含む場合、制御ユニット２００またはサポート装置１１０は、変数の書込範囲情報６００を生成する。逆に、制御プログラム４２０が物理メモリを含む場合、制御ユニット２００またはサポート装置１１０は、物理メモリの書込範囲情報６１０を生成する。ある局面において、制御プログラム４２０が変数および物理メモリの両方を含む場合、制御ユニット２００またはサポート装置１１０は、変数の書込範囲情報６００および物理メモリの書込範囲情報６１０を組み合わせた情報を生成して、当該情報をアクセスコントロールに使用してもよい。
【０１０８】
制御ユニット２００は、変数の書込範囲情報６００または物理メモリの書込範囲情報６１０と、ユーザアカウント情報７００とに基づいて、書込要求を受け付けるか否かを判断する。
【０１０９】
図７は、ユーザアカウント情報７００の一例を示す図である。ある局面において、ユーザアカウント情報７００は、リレーショナルデータベースのテーブルとして表現されてもよいし、ＪＳＯＮ（JavaScript（登録商標） Object Notation）等の他の任意のデータ形式で表現されてもよい。ユーザアカウント情報７００は、ユーザ識別子７０１と、パスワード７０２と、権限７０３とを含む。
【０１１０】
ユーザ識別子７０１は、ユーザを一意に示す。ある局面において、ユーザは、人間だけでなく装置またはシステムを含み得る。一例として、他の装置またはシステムは、ユーザとして、制御ユニット２００の変数または物理メモリが示す値に対するアクセス要求を送信し得る。パスワード７０２は、ユーザ毎の認証用のパスワードである。権限７０３は、各ユーザの権限（または属性）である。
【０１１１】
図７に示す例では、ユーザ識別子「Ｋｉｔａ」が示すユーザのパスワードは「１１１１」である。また、ユーザ識別子７０１「Ｋｉｔａ」が示すユーザの権限は「設計者」である。この場合、ユーザ識別子７０１「Ｋｉｔａ」が示すユーザは、変数「ＡＡＡＡＡＡＡＡ，ＢＢＢＢＢＢＢＢ，ＣＣＣＣＣＣＣＣ」または物理メモリ「Ｄ００００，Ｄ０００１，Ｄ０００２」に対して、読出および書込の権限を有する（図５参照）。また、ユーザ識別子７０１「Ｋｉｔａ」が示すユーザは、変数「ＣＣＣＣＣＣＣＣ」または物理メモリ「Ｄ０００２」に対して、値「０－１００」を書き込む権限を有する（図６参照）。なお、パスワードは、実際には暗号化されていてもよい。
【０１１２】

図８は、変数のルール８００および物理メモリのルール８１０の一例を示す図である。変数のルール８００は、変数の命名規則と、各変数名に対応付けられたアクセス制限とを含む。物理メモリのルール８１０は、物理メモリの範囲と、各物理メモリの範囲に対応付けられたアクセス制限とを含む。

【０１１３】

ある局面において、変数のルール８００および物理メモリのルール８１０は、リレーショナルデータベースのテーブルとして表現されてもよいし、ＪＳＯＮ（JavaScript（登録商標） Object Notation）等の他の任意のデータ形式で表現されてもよい。

【０１１４】

変数のルール８００は、データ項目として、変数名ルール８０１と、操作８０２と、ユーザアカウントの権限ごとのアクセス制限８０３とを含む。

【０１１５】

変数名ルール８０１は、正規表現等の任意のフォーマットによる変数名の命名規則を含む。操作８０２は、読出および書込の操作を含む。アクセス制限８０３は、ユーザアカウントの権限ごとの読出および書込の制限である。

【０１１６】

図８に示す例では、「管理者、設計者」のみが、変数名が「ＯＥＭ」から始まる変数に対しての読込および書込の権限を有する。また、「管理者、設計者、保全者」は、変数名が「ＡＣＬ」から始まる変数に対しての読込および書込の権限を有する。さらに、「操作者、観察者」は、変数名が「ＡＣＬ」から始まる変数に対しての読込権限のみを有する。

【０１１７】

物理メモリのルール８１０は、データ項目として、物理メモリ範囲８１１と、操作８１２と、ユーザアカウントの権限ごとのアクセス制限８１３とを含む。

【０１１８】

一例として、物理メモリ範囲８１１は、物理メモリの開始アドレスおよび終了アドレスによって示される範囲を含む。他の例として、物理メモリ範囲８１１は、１つの物理メモリのアドレス、または、連続しない複数の物理メモリのアドレスを含んでいてもよい。操作８０２は、読出および書込の操作を含む。アクセス制限８０３は、アクセス制限８０３は、ユーザアカウントの権限ごとの読出および書込の制限である。

【０１１９】

図８に示す例では、「管理者、設計者」のみが、物理メモリ「Ｄ００００－Ｄ０１００」に対しての読込および書込の権限を有する。また、「管理者、設計者、保全者」は、物理メモリ「Ｄ０２０１－Ｄ０３００」に対しての読込および書込の権限を有する。さらに、「操作者、観察者」は、物理メモリ「Ｄ０２０１－Ｄ０３００」に対しての読込権限のみを有する。

【０１２０】

変数／物理メモリの操作権限情報生成プログラム４２１は、変数のルール８００と物理メモリのルール８１０とを参照して、制御プログラム４２０から、変数の操作権限情報５００と物理メモリの操作権限情報５１０とを生成する。

【０１２１】

サポート装置１１０が変数／物理メモリの操作権限情報生成プログラム４２１を実行する場合、サポート装置１１０は変数のルール８００および／または物理メモリのルール８１０を二次記憶装置４０５に格納する。また、制御ユニット２００が変数／物理メモリの操作権限情報生成プログラム４２１を実行する場合、制御ユニット２００は変数のルール８００および／または物理メモリのルール８１０を二次記憶装置３０３に格納する。

【０１２２】

また、一例として、ユーザは、サポート装置１１０（サポートツール等）を用いて、予め変数のルール８００および物理メモリのルール８１０を作成し得る。作成された変数のルール８００および物理メモリのルール８１０は、二次記憶装置４０５に格納されてもよいし、制御ユニット２００に送信されてもよい。

【０１２３】
図９は、変数マスタ９００および物理メモリマスタ９１０の一例を示す図である。変数マスタ９００は、制御プログラム４２０内で定義された全ての変数を含む。変数マスタ９００は、制御プログラム４２０内で使用できる全ての物理メモリを含む。
【０１２４】
ある局面において、変数マスタ９００および物理メモリマスタ９１０は、リレーショナルデータベースのテーブルとして表現されてもよいし、ＪＳＯＮ（JavaScript（登録商標） Object Notation）等の他の任意のデータ形式で表現されてもよい。
【０１２５】
変数マスタ９００は、データ項目として、変数識別子９０１と、変数９０２を含む。変数識別子９０１は、変数を一意に識別する。変数９０２は、制御プログラム４２０内で定義された変数の名称を含む。
【０１２６】
物理メモリマスタ９１０は、データ項目として、物理メモリ識別子９１１と、物理メモリ９１２を含む。物理メモリ識別子９１１は、物理メモリまたは物理メモリの範囲を一意に識別する。物理メモリ９１２は、制御プログラム４２０内で使用可能な物理メモリまたは物理メモリの範囲を含む。
【０１２７】
ある局面において、サポート装置１１０または制御ユニット２００は、制御プログラム４２０から、最初に変数マスタ９００または物理メモリマスタ９１０を生成してもよい。この場合、サポート装置１１０または制御ユニット２００は、変数マスタ９００または物理メモリマスタ９１０と、変数のルール８００または物理メモリのルール８１０とに基づいて、変数の操作権限情報５００または物理メモリの操作権限情報５１０を生成し得る。
【０１２８】
他の局面において、サポート装置１１０または制御ユニット２００は、変数マスタ９００または物理メモリマスタ９１０を使用せずに、変数の操作権限情報５００または物理メモリの操作権限情報５１０を生成してもよい。
【０１２９】
＜Ｄ．アクセスコントロールの手順＞
次に、本実施の形態に従う制御ユニット２００によるアクセスコントロールの手順について説明する。
【０１３０】
図１０は、制御ユニット２００に対するアクセス要求の一例を示す図である。制御ユニット２００は、端末１０００から、ある変数または物理メモリが示す値に対するアクセス要求１０１０を受信したとする。端末１０００は、サポート装置１１０、表示装置１４０、他の制御システム１または他の任意の装置であってもよい。
【０１３１】
図１０に示すアクセス要求１０１０は、書込要求であり、一例として、ユーザ識別子１０１１、パスワード１０１２、書込コマンド１０１３、変数１０１４、および、書込値１０１５を含む。
【０１３２】
他の例として、アクセス要求１０１０が読出要求の場合、アクセス要求１０１０は、一例として、書込コマンド１０１３および書込値１０１５の代わりに、読出コマンドを含み得る。また、アクセス要求１０１０は変数１０１４の代わりに物理メモリを含み得る。
【０１３３】
ユーザ識別子１０１１は、アクセス要求１０１０を送信したユーザを一意に識別する。パスワード１０１２は、ユーザを認証するためのパスワードである。書込コマンド１０１３は、制御ユニット２００に実行させるコマンドである。変数１０１４は、書込処理の対象の変数名である。書込値１０１５は、変数に書き込む値である。
【０１３４】

制御ユニット２００は、アクセス要求１０１０を受信したことに基づいて、ユーザアカウント情報７００を参照して、アクセス要求１０１０を送信したユーザアカウントを認証する。次に、制御ユニット２００は、変数の操作権限情報５００または物理メモリの操作権限情報５１０に基づいて、アクセス要求１０１０を受け付けるか否かを判断する。

【０１３５】

さらに、制御ユニット２００は、アクセス要求１０１０が書込要求であることに基づいて、変数の書込範囲情報６００または物理メモリの書込範囲情報６１０を参照して、書込要求を受け付けるか否かを判断する。制御ユニット２００は、変数または物理メモリに書き込まれる値が、アクセス要求１０１０を送信したユーザアカウントの権限の範囲内であれば、書込要求を受け付け、そうでなければ書込要求を拒否する。

【０１３６】

さらに、制御ユニット２００は、アクセス要求１０１０を受け付けたときに、各変数または物理メモリが示す値に変更があった（書込処理があった）ことに基づいて、変更履歴を生成する。当該変更履歴は、二次記憶装置３０３に格納される。ある局面において、変更履歴は、更新された値を示す変数名または物理メモリのアドレスと、更新された値と、値を更新したユーザのユーザ識別子とを含んでいてもよい。

【０１３７】

変更履歴は、アクセスログとは別に、各変数または物理メモリが示す値の変更記録のみを記録したものであってもよい。変更履歴およびログを分けることにより、変更履歴は膨大なログに埋もれることはなくなり、制御システム１の管理者は、当該変更履歴を確認することで、不正なアクセス等があったか否かを容易に確認することができる。変更履歴は、一例として、変更のあった変数名または物理メモリのアドレスと、変更前後の値と、書込処理を実行したユーザのユーザ識別子とを含む。

【０１３８】

図１１は、アクセスコントロール情報３２２の生成手順の一例を示す図である。ある局面において、図１１に示す処理は、制御ユニット２００およびサポート装置１１０のいずれかによって実行されてもよい。

【０１３９】

制御ユニット２００が図１１に示す処理を実行する場合、プロセッサ３０１は、図１１の処理を行うためのプログラムを二次記憶装置３０３から主記憶装置３０４に読み込んで、当該プログラムを実行してもよい。他の局面において、当該処理の一部または全部は、当該処理を実行するように構成された回路素子の組み合わせとしても実現され得る。

【０１４０】

サポート装置１１０が図１１に示す処理を実行する場合、プロセッサ４０１は、図１１の処理を行うためのプログラムを二次記憶装置４０５から主記憶装置４０２に読み込んで、当該プログラムを実行してもよい。他の局面において、当該処理の一部または全部は、当該処理を実行するように構成された回路素子の組み合わせとしても実現され得る。

【０１４１】

これ以降、制御ユニット２００が図１１に示す処理を実行するものとして説明するが、サポート装置１１０が図１１に示す処理を実行する場合も、生成後のアクセスコントロール情報３２２を制御ユニット２００に送信する以外の手順は同じである。

【０１４２】

ステップＳ１１１０において、サポート装置１１０から制御プログラム４２０を取得する。制御プログラム４２０は、暗号化されていてもよいし、暗号化されていなくてもよい。制御ユニット２００は、暗号化されている制御プログラム４２０を取得した場合、復号処理を実行する。

【０１４３】

ステップＳ１１２０において、プロセッサ３０１は、変数のルール８００と、物理メモリのルール８１０とを取得する。ある局面において、プロセッサ３０１は、二次記憶装置３０３に格納されている変数のルール８００および物理メモリのルール８１０を取得して

もよい。他の局面において、プロセッサ３０１は、サポート装置１１０から、変数のルール８００と、物理メモリのルール８１０とを受信してもよい。

【０１４４】

ステップＳ１１３０において、プロセッサ３０１は、変数マスタ９００と、物理メモリマスタ９１０とを生成または更新する。制御プログラム４２０内で変数が使用されている場合、プロセッサ３０１は、制御プログラム４２０内で参照される全ての変数を含む変数マスタ９００を生成する。制御プログラム４２０内で物理メモリが使用されている場合、プロセッサ３０１は、制御ユニット２００が提供する全ての物理メモリを含む物理メモリマスタ９１０を生成する。なお、物理メモリマスタ９１０は、二次記憶装置３０３に予め格納されていてもよい。

【０１４５】

ステップＳ１１４０において、プロセッサ３０１は、変数の操作権限情報５００および／または物理メモリの操作権限情報５１０を生成する。より具体的には、プロセッサ３０１は、変数のルール８００と、変数マスタ９００とに基づいて変数の操作権限情報５００を生成する。また、プロセッサ３０１は、物理メモリのルール８１０と、物理メモリマスタ９１０とに基づいて物理メモリの操作権限情報５１０を生成する。なお、プロセッサ３０１は、ステップＳ１１３０の処理を省略して、ステップＳ１１４０の処理内で制御プログラム４２０から変数または物理メモリを抽出してもよい。

【０１４６】

ステップＳ１１５０において、プロセッサ３０１は、変数の書込範囲情報６００および／または物理メモリの書込範囲情報６１０を生成する。より具体的には、二次記憶装置３０３（サポート装置１１０が図１１に示す処理を実行する場合は二次記憶装置４０５）は、変数または物理メモリのセキュリティレベル（どの権限を持つユーザアカウントによるアクセスが可能か）に基づく書込範囲のルール（図示せず）を予め備えていてもよい。プロセッサ３０１は、変数の操作権限情報５００と、変数のセキュリティレベルに基づく書込範囲のルールとに基づいて、変数の書込範囲情報６００を生成し得る。また、プロセッサ３０１は、物理メモリの操作権限情報５１０と、物理メモリのセキュリティレベルに基づく書込範囲のルールとに基づいて、物理メモリの書込範囲情報６１０を生成し得る。

【０１４７】

なお、サポート装置１１０が図１１に示す処理を実行する場合、各ステップで生成した情報をアクセスコントロール情報３２２の一部として、制御ユニット２００に送信する。

【０１４８】

図１２は、制御ユニット２００によるアクセスコントロールの手順の一例を示す図である。ある局面において、プロセッサ３０１は、図１２の処理を行うためのプログラムを二次記憶装置３０３から主記憶装置３０４に読み込んで、当該プログラムを実行してもよい。他の局面において、当該処理の一部または全部は、当該処理を実行するように構成された回路素子の組み合わせとしても実現され得る。

【０１４９】

ステップＳ１２１０において、プロセッサ３０１は、終了要求があるまでループ内の処理を繰り返し実行する。終了要求は、ユーザによって制御ユニット２００に入力されてもよいし、外部機器から制御ユニット２００に送信されてもよい。または、プロセッサ３０１は、制御ユニット２００が動作している間は、常にステップＳ１２２０以降の処理を実行し続けてもよい。

【０１５０】

ステップＳ１２２０において、プロセッサ３０１は、変数または物理メモリへのアクセス要求があるか否かを判定する。プロセッサ３０１は、変数または物理メモリへのアクセス要求があると判定した場合（ステップＳ１２２０にてＹＥＳ）、制御をステップＳ１２３０に移す。そうでない場合（ステップＳ１２２０にてＮＯ）、プロセッサ３０１は、制御をステップＳ１２１０に移す。

【０１５１】

ステップＳ１２３０において、プロセッサ３０１は、ユーザアカウント情報７００を取得する。ユーザアカウント情報７００は、予め二次記憶装置３０３に格納されていてもよい。

【０１５２】

ステップＳ１２４０において、プロセッサ３０１は、アクセス要求を送信したユーザが、アクセス要求のあった変数または物理メモリが示す値に対してアクセス権限を有するか否かを判定する。プロセッサ３０１は、アクセス要求を送信したユーザが、アクセス要求のあった変数または物理メモリが示す値に対してアクセス権限を有すると判定した場合（ステップＳ１２４０にてＹＥＳ）、制御をステップＳ１２５０に移す。そうでない場合（ステップＳ１２４０にてＮＯ）、プロセッサ３０１は、制御をステップＳ１２６０に移す。

【０１５３】

ステップＳ１２５０において、プロセッサ３０１は、アクセス要求を許可する（受け付ける）。より具体的には、プロセッサ３０１は、アクセス要求に含まれる命令に基づいて、変数または物理メモリが示す値の読出処理、または変数または物理メモリへの書込処理を実行する。ある局面において、変更履歴は、更新された値を示す変数名または物理メモリのアドレスと、更新された値と、値を更新したユーザのユーザ識別子とを含んでいてもよい。なお、プロセッサ３０１は、書込処理を実行した場合、変更履歴を生成または更新して、当該変更履歴を二次記憶装置３０３に格納する。

【０１５４】

ステップＳ１２６０において、プロセッサ３０１は、アクセス要求を拒否する。ステップＳ１２７０において、プロセッサ３０１は、終了要求を受け付けたか否かを判定する。プロセッサ３０１は、終了要求を受け付けたと判定した場合（ステップＳ１２７０にてＹＥＳ）、処理を終了する。そうでない場合（ステップＳ１２７０にてＮＯ）、プロセッサ３０１は、制御をステップＳ１２１０に戻す。

【０１５５】

以上説明した通り、本実施の形態に従う制御ユニット２００は、変数または物理メモリごとのアクセスコントロール情報３２２を有する。これにより、制御ユニット２００は、変数または物理メモリごとに、アクセス要求を受け付けるか否かを判断し得る。さらに、本実施の形態に従う制御ユニット２００は、変数または物理メモリのセキュリティレベルに基づいて、変数または物理メモリごとに書込範囲を制限し得る。

【０１５６】

また、ある局面において、本実施の形態に従う制御ユニット２００またはサポート装置１１０は、制御プログラム４２０に基づいて、変数の操作権限情報を生成し得る。これにより、ユーザは、制御プログラム４２０において、予め定められた命名規則で変数を定義することにより、容易に変数の操作権限情報５００を生成し得る。

【０１５７】

また、他の局面において、本実施の形態に従う制御ユニット２００またはサポート装置１１０は、物理メモリの操作権限情報５１０を予め保持していてもよい。これにより、制御ユニット２００は、自動的に、物理メモリごとに、アクセス要求を受け付けるか否かを判断し得る。

【０１５８】

＜Ｅ．付記＞

以上のように、本実施の形態では以下のような開示を含む。

【０１５９】

（構成１）

制御対象を制御する制御部（３０１）と、

上記制御部（３０１）によって実行されるプログラム（４２０）と、上記プログラム（４２０）で参照される複数のデータの各々に対する各アクセス権限（５００，５１０）とを格納する記憶部（３０３）と、

上記複数のデータのいずれかに対するアクセス要求を受け付ける入力部（３０５，３１

４）とを備え、
各上記アクセス権限（５００，５１０）は、各権限を持つユーザの各々が実行可能な操作の情報を含み、
上記制御部（３０１）は、
上記入力部（３０５，３１４）から上記複数のデータのいずれかに対するアクセス要求を取得したことに基づいて、各上記アクセス権限（５００，５１０）を参照し、
各上記アクセス権限（５００，５１０）に基づいて、上記アクセス要求を送信したユーザが、当該アクセスを要求したデータに対するアクセス権限（５００，５１０）を有するか否かを判断する、制御システム（１，２００）。
【０１６０】
（構成２）
上記複数のデータの各々は、上記プログラム（４２０）内の変数または物理メモリのアドレスにより示されるデータである、構成１の制御システム（１，２００）。
【０１６１】
（構成３）
上記記憶部（３０３）は、さらに、上記変数または上記物理メモリの各々に対する書込範囲の情報（６００，６１０）を格納し、
上記制御部（３０１）は、上記書込範囲の情報（６００，６１０）に基づいて、アクセス要求のあった上記変数または上記物理メモリに対する書込可能な値の範囲を制限する、構成２の制御システム（１，２００）。
【０１６２】
（構成４）
上記複数のデータの各々に対するアクセス権限（５００，５１０）は、変数名ごとのアクセス権限（５００，５１０）を定義した第１のルール（８００）、または、物理メモリごとのアクセス権限（５００，５１０）を定義した第２のルール（８１０）に基づいて生成される、構成２または３の制御システム（１，２００）。
【０１６３】
（構成５）
上記プログラム（４２０）を作成するための装置（１１０）をさらに備え、
上記装置（１１０）は、
上記第１のルール（８００）または上記第２のルール（８１０）に基づいて、上記プログラム（４２０）を解析し、
解析結果に基づいて、各上記アクセス権限（５００，５１０）を生成し、
各上記アクセス権限（５００，５１０）を上記記憶部（３０３）に出力する、構成４の制御システム（１，２００）。
【０１６４】
（構成６）
上記記憶部（３０３）は、上記第１のルール（８００）または上記第２のルール（８１０）をさらに格納し、
上記制御部（３０１）は、
他の装置から上記プログラム（４２０）を取得したことに基づいて、上記第１のルール（８００）または上記第２のルール（８１０）を用いて、上記プログラム（４２０）を解析し、
解析結果に基づいて、各上記アクセス権限（５００，５１０）を生成し、
各上記アクセス権限（５００，５１０）を上記記憶部（３０３）に出力する、構成４の制御システム（１，２００）。
【０１６５】
（構成７）
上記制御部（３０１）は、上記プログラム（４２０）で参照される複数のデータのいずれかが更新されたことに基づいて、更新履歴を上記記憶部（３０３）に格納し、

上記更新履歴は、更新されたデータを示す変数名または物理メモリのアドレスと、上記更新されたデータと、データを更新したユーザのユーザ識別子とを含む、構成２～６の記載の制御システム（１，２００）。

【０１６６】

（構成８）

制御装置の制御方法であって、

上記制御装置によって実行されるプログラム（４２０）と、上記プログラム（４２０）で参照される複数のデータの各々に対する各アクセス権限（５００，５１０）とにアクセスするステップを含み、

各上記アクセス権限（５００，５１０）は、各権限を持つユーザの各々が実行可能な操作の情報を含み、

上記複数のデータのいずれかに対するアクセス要求を取得したことに基づいて、各上記アクセス権限（５００，５１０）を参照するステップと、

各上記アクセス権限（５００，５１０）に基づいて、上記アクセス要求を送信したユーザが、当該アクセスを要求したデータに対するアクセス権限（５００，５１０）を有するか否かを判断するステップとをさらに含む、制御方法。

【０１６７】

（構成９）

上記複数のデータの各々は、上記プログラム（４２０）内の変数または物理メモリのアドレスにより示されるデータである、構成８の制御方法。

【０１６８】

（構成１０）

上記変数または上記物理メモリの各々に対する書込範囲の情報（６００，６１０）にアクセスするステップと、

上記書込範囲の情報（６００，６１０）に基づいて、アクセス要求のあった上記変数または上記物理メモリに対する書込可能な値の範囲を制限するステップとをさらに含む、構成９の制御方法。

【０１６９】

（構成１１）

上記複数のデータの各々に対するアクセス権限（５００，５１０）は、変数名ごとのアクセス権限（５００，５１０）を定義した第１のルール（８００）、または、物理メモリごとのアクセス権限（５００，５１０）を定義した第２のルール（８１０）に基づいて生成される、構成９または１０の制御方法。

【０１７０】

（構成１２）

上記第１のルール（８００）または上記第２のルール（８１０）に基づいて、上記プログラム（４２０）を解析するステップと、

解析結果に基づいて、各上記アクセス権限（５００，５１０）を生成するステップと、

各上記アクセス権限（５００，５１０）を出力するステップとをさらに含む、構成１１の制御方法。

【０１７１】

（構成１３）

上記プログラム（４２０）で参照される複数のデータのいずれかが更新されたことに基づいて、更新履歴を生成するステップをさらに含み、

上記更新履歴は、更新されたデータを示す変数名または物理メモリのアドレスと、上記更新されたデータと、データを更新したユーザのユーザ識別子とを含む、構成９～１２の制御方法。

【０１７２】

今回開示された実施の形態は全ての点で例示であって制限的なものではないと考えられるべきである。本開示の範囲は上記した説明ではなくて特許請求の範囲によって示され、

特許請求の範囲と均等の意味及び範囲内で全ての変更が含まれることが意図される。また、実施の形態および各変形例において説明された開示内容は、可能な限り、単独でも、組合わせても、実施することが意図される。

【符号の説明】

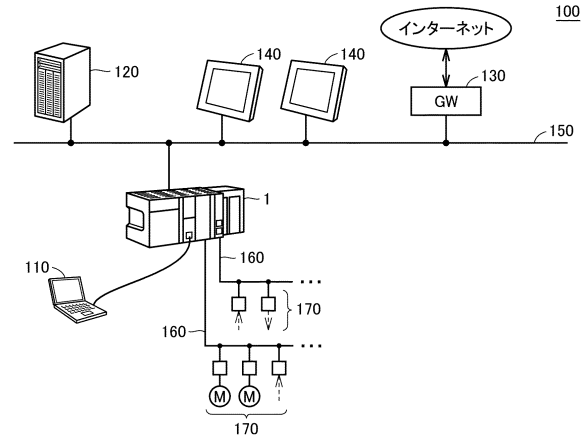
【０１７３】

１　制御システム、１００　ネットワークシステム、１１０　サポート装置、１２０　サーバ装置、１３０　ゲートウェイ、１４０　表示装置、１５０　ネットワーク、１６０　フィールドネットワーク、１７０　制御対象、２００　制御ユニット、２１０　セキュリティユニット、２２０　セーフティユニット、２３０　機能ユニット、２４０　電源ユニット、３０１，４０１　プロセッサ、３０２　チップセット、３０３，４０５　二次記憶装置、３０４，４０２　主記憶装置、３０５　通信コントローラ、３０６　インジケータ、３０７　スイッチインターフェイス、３０８　ディップスイッチ、３０９　内部バスコントローラ、３１０，３１１，３１２　ネットワークコントローラ、３１３　メモリカードインターフェイス、３１４　コントローラ、３２０　システムプログラム、３２１　サービスプログラム、３２２　アクセスコントロール情報、３２３　不揮発性記憶領域、３２４　暗号化済み制御プログラム、３２５　揮発性記憶領域、３２６　復号済み制御プログラム、３３０　バス、３４０　メモリカード、４０３　入力部、４０４　出力部、４０６　光学ドライブ、４０７　通信インターフェイス、４１０　プロセッサバス、４２０　制御プログラム、４２１　操作権限情報生成プログラム、４２２　書込範囲情報生成プログラム、４２３　サポートプログラム、４２４　ＯＳ、４５０　記録媒体、５００，５１０　操作権限情報、５０１，６０１，９０２，１０１４　変数、５０２，５１２，８０２，８１２　操作、５０３，５１３，８０３，８１３　アクセス制限、５１１，６１１，９１２　物理メモリ、６００，６１０　書込範囲情報、６０２，６１２　書込範囲、６０３，６１３　書込操作制限、７００　ユーザアカウント情報、７０１，１０１１　ユーザ識別子、７０２，１０１２　パスワード、７０３　権限、８００，８１０　ルール、８０１　変数名ルール、８１１　物理メモリ範囲、９００　変数マスタ、９０１　変数識別子、９１０　物理メモリマスタ、９１１　物理メモリ識別子、１０００　端末、１０１０　アクセス要求、１０１３　書込コマンド、１０１５　書込値。

【図面】

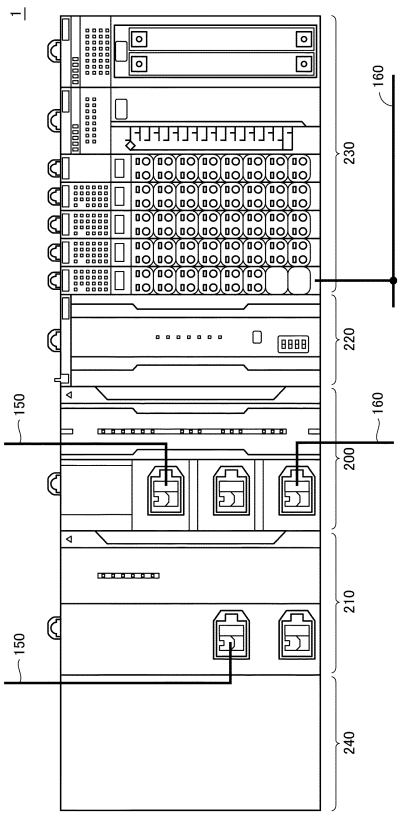
【図１】

図1


100
インターネット
120
140
140
130
GW
150
1
110
160
170
160
170

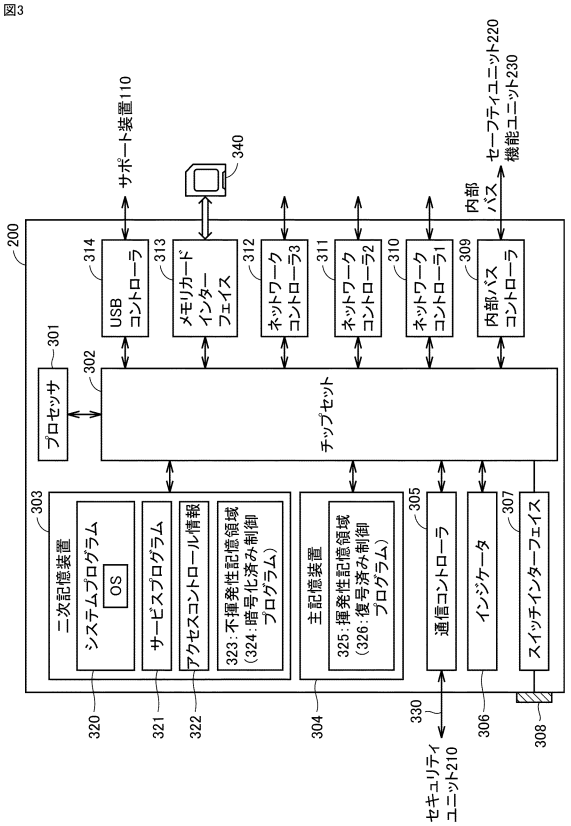
【図２】

図2


1
160
230
220
150
160
200
210
150
240

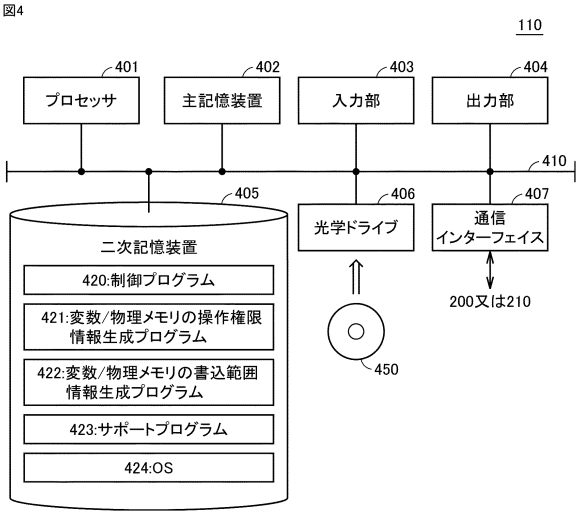
【図３】

図3



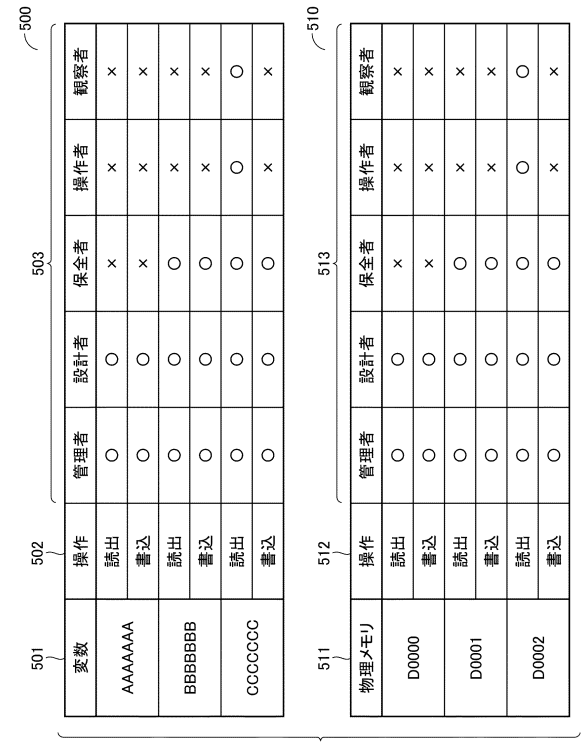
【図４】

図4



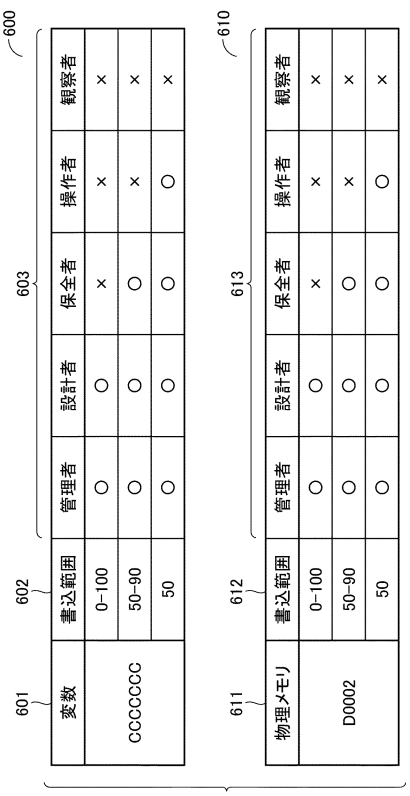
【図５】

図5



【図６】

図6



【図７】

図7

700

701 ユーザ識別子	702 パスワード	703 権限
Kita	1111	設計者
Ken	2222	管理者
Mike	3333	操作者

【図８】

図8

801 変数名ルール	802 操作	803 管理者	設計者	保全者	操作者	観察者
OEM****	読出	○	○	×	×	×
	書込	○	○	×	×	×
Secure***	読出	○	○	○	×	×
	書込	○	○	○	×	×
ACL****	読出	○	○	○	○	○
	書込	○	○	○	×	×

800

811 物理メモリ範囲	812 操作	813 管理者	設計者	保全者	操作者	観察者
D0000-D0100	読出	○	○	×	×	×
	書込	○	○	×	×	×
D0101-D0200	読出	○	○	○	×	×
	書込	○	○	○	×	×
D0201-D0300	読出	○	○	○	○	○
	書込	○	○	○	×	×

810

【図９】

図9

900

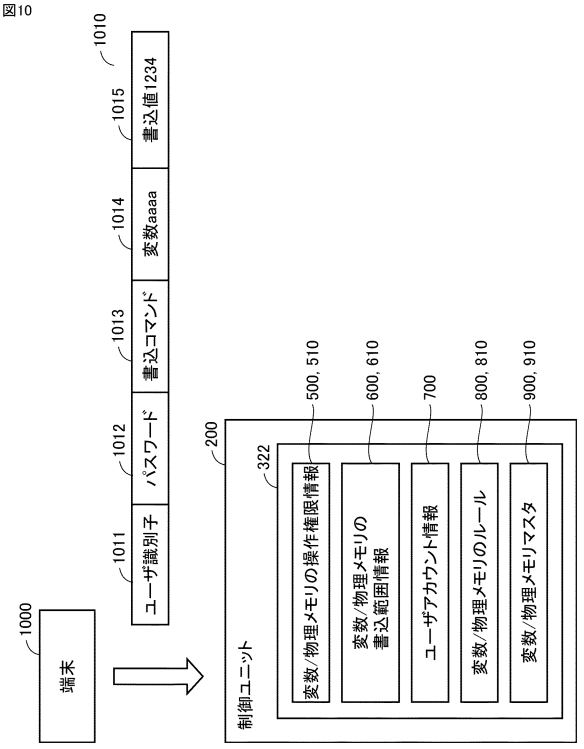
901 変数識別子	902 変数
1	AAAAAAA
2	BBBBBBB
3	CCCCCCC

910

911 物理メモリ識別子	912 物理メモリ
1	D0000-D0100
2	D0101-D0200
3	D0201-D0300

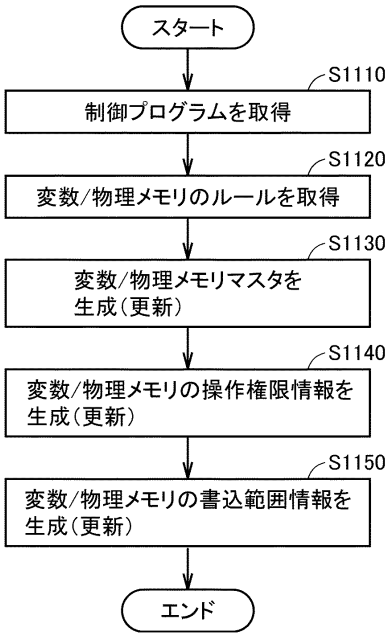
【図１０】

図10



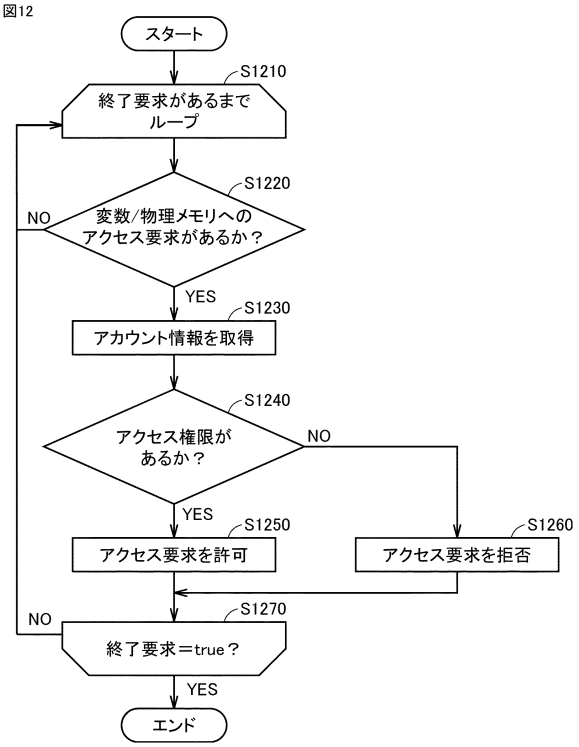
【図１１】

図11



【図１２】

図12



フロントページの続き

審査官　上島 拓也
(56)参考文献　特開２０１７－２２０１１４（ＪＰ，Ａ）
米国特許出願公開第２０１５／０１９２９１８（ＵＳ，Ａ１）
特開２０１８－１５９９８１（ＪＰ，Ａ）
特開２００６－１０６９９８（ＪＰ，Ａ）
(58)調査した分野　(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／６２
Ｇ０５Ｂ　１９／０５