(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7608833号
(P7608833)

(45)発行日　令和7年1月7日(2025.1.7)

(24)登録日　令和6年12月23日(2024.12.23)

(51)国際特許分類
Ｇ０６Ｆ　21/44　(2013.01)

ＦＩ
Ｇ０６Ｆ　21/44

請求項の数　7　（全26頁）

(21)出願番号　特願2021-2808(P2021-2808)
(22)出願日　令和3年1月12日(2021.1.12)
(65)公開番号　特開2022-108027(P2022-108027A)
(43)公開日　令和4年7月25日(2022.7.25)
審査請求日　令和5年11月9日(2023.11.9)

(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　村山 信次
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
審査官　塩澤 如正

最終頁に続く

(54)【発明の名称】　制御装置、管理方法およびセキュリティプログラム

(57)【特許請求の範囲】
【請求項１】
複数のデバイスを含む制御装置であって、
制御プログラムを実行する制御エンジンと、
前記制御エンジンでの前記制御プログラムの実行可否を管理するセキュリティエンジンとを備え、
前記セキュリティエンジンは、
前記複数のデバイスの各々から取得された識別情報を用いて固有情報を生成する生成手段と、
予め生成された第１の固有情報を保持する保持手段と、
照合の要求に従って前記生成手段により生成される第２の固有情報と、前記第１の固有情報とを照合する照合手段と、
前記制御プログラムの実行開始要求に応答して、前記照合の要求を行い、前記照合手段から得られる照合結果に基づいて、前記制御プログラムの実行可否を判定する許可手段とを含み、
前記生成手段は、前記複数のデバイスのうち第１のグループに属する第１のデバイスについて、当該デバイスの種別を識別する第１の識別情報を前記識別情報として選択し、前記複数のデバイスのうち第２のグループに属する第２のデバイスについて、当該デバイスを個別に識別する第２の識別情報を前記識別情報として選択する、制御装置。
【請求項２】

前記複数のデバイスの各々は、前記第２の識別情報を保持し、
前記第２の識別情報は、前記第１の識別情報と、前記第１の識別情報によって識別される種別のデバイスの個体に対してユニークに割り当てられる第３の識別情報との組み合わせであり、
前記生成手段は、前記第２の識別情報から前記第１の識別情報を取得する、請求項１に記載の制御装置。
【請求項３】
前記複数のデバイスは、前記制御エンジンを有する制御デバイスと、前記セキュリティエンジンを有するセキュリティデバイスとを含む、請求項１または２に記載の制御装置。
【請求項４】
前記保持手段は、外部装置との間で、分散型台帳の形式で前記第１の固有情報を保持する、請求項１から３のいずれか１項に記載の制御装置。
【請求項５】
前記照合手段は、前記第２の固有情報と前記外部装置が保持する前記第１の固有情報とをさらに照合する、請求項４に記載の制御装置。
【請求項６】
複数のデバイスを含む制御装置において実行される管理方法であって、
予め生成された第１の固有情報を保持するステップと、
制御プログラムの実行開始要求に応答して、前記複数のデバイスの各々から取得された識別情報を用いて第２の固有情報を生成するステップと、
前記第１の固有情報と前記第２の固有情報とを照合するステップと、
照合結果に基づいて、前記制御プログラムの実行可否を判定するステップとを備え、
前記生成するステップは、
前記複数のデバイスのうち第１のグループに属する第１のデバイスについて、当該デバイスの種別を識別する第１の識別情報を前記識別情報として選択するステップと、
前記複数のデバイスのうち第２のグループに属する第２のデバイスについて、当該デバイスを個別に識別する第２の識別情報を前記識別情報として選択するステップとを含む、管理方法。
【請求項７】
複数のデバイスを含む制御装置において実行される管理方法をコンピュータに実行させるセキュリティプログラムであって、
前記管理方法は、
予め生成された第１の固有情報を保持するステップと、
制御プログラムの実行開始要求に応答して、前記複数のデバイスの各々から取得された識別情報を用いて第２の固有情報を生成するステップと、
前記第１の固有情報と前記第２の固有情報とを照合するステップと、
照合結果に基づいて、前記制御プログラムの実行可否を判定するステップとを備え、
前記生成するステップは、
前記複数のデバイスのうち第１のグループに属する第１のデバイスについて、当該デバイスの種別を識別する第１の識別情報を前記識別情報として選択するステップと、
前記複数のデバイスのうち第２のグループに属する第２のデバイスについて、当該デバイスを個別に識別する第２の識別情報を前記識別情報として選択するステップとを含む、セキュリティプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本開示は、制御装置、管理方法およびセキュリティプログラムに関する。
【背景技術】
【０００２】
様々な製造現場において、ＰＬＣ（Programmable Logic Controller）などの制御装

置が導入されている。このような制御装置は、一種のコンピュータであり、製造装置または製造設備などに応じて設計された制御プログラムを実行する。

【０００３】

近年では、既に製造現場での稼働実績のある制御装置から制御プログラムを抜き取り、別の製造現場内で新たな制御装置が作られて、抜き取られた制御プログラムが利用されるという問題が発生している。

【０００４】

特開２００８－０６５６７８号公報（特許文献１）は、このような問題に対処する一の方法を開示する。具体的には、特許文献１は、ＰＬＣが、制御プログラムを暗号化したプログラムが設備機器に固有なプログラムであるか否かを判断し、設備機器に固有なプログラムであれば、当該プログラムから制御プログラムを復号し、制御プログラムを実行して設備機器を制御する方法を開示する。

【先行技術文献】

【特許文献】

【０００５】

【文献】特開２００８－０６５６７８号公報

【発明の概要】

【発明が解決しようとする課題】

【０００６】

特許文献１で示された方法では、ＰＬＣは、予め入力された識別データと暗号ルールとを格納する記憶手段を備え、当該識別データを用いて、暗号化したプログラムが設備機器に固有なプログラムであるか否かを判断する。暗号化したプログラムが設備機器に固有なプログラムであると判断された場合、ＰＬＣは、暗号ルールに従って、暗号化したプログラムを復号することにより制御プログラムを得て、当該制御プログラムを利用する。そのため、暗号化したプログラムだけでなく、識別データおよび暗号ルールも抜き取られた場合、制御プログラムの利用が図られてしまう。すなわち、特許文献１で示された方法では、制御プログラムという知的財産の保護を図る上で改善の余地があった。

【０００７】

本開示は、制御プログラムという知的財産の保護を図ることを一つの目的とする。

【課題を解決するための手段】

【０００８】

本開示の一例に従うと、１以上のデバイスを含む制御装置は、制御プログラムを実行する制御エンジンと、制御エンジンでの制御プログラムの実行可否を管理するセキュリティエンジンとを備える。セキュリティエンジンは、生成手段と、保持手段と、照合手段と、許可手段とを含む。生成手段は、１以上のデバイスの各々から取得された識別情報を用いて固有情報を生成する。保持手段は、予め生成された第１の固有情報を保持する保持手段と、照合手段は、照合の要求に従って生成手段により生成される第２の固有情報と、第１の固有情報とを照合する。許可手段は、制御プログラムの実行開始要求に応答して、照合の要求を行い、照合手段から得られる照合結果に基づいて、制御プログラムの実行可否を判定する。生成手段は、１以上のデバイスの各々について、当該デバイスの種別を識別する第１の識別情報および当該デバイスを個別に識別する第２の識別情報からセキュリティポリシーに応じて識別情報を選択する。

【０００９】

この構成によれば、セキュリティエンジンは、予め生成された第１の固有情報を基準に、制御プログラムの実行開始要求に応答して生成される第２の固有情報を照合し、その照合結果に応じて制御プログラムの実行可否を判定する。固有情報は、各デバイスの種別を識別する第１の識別情報および各デバイスを個別に識別する第２の識別情報から選択された識別情報から生成される。そのため、制御装置のソフトウェア（第１の固有情報および制御プログラムを含む）およびハードウェアをコピーすることにより新たな制御装置を作製した場合、当該新たな制御装置に含まれるデバイスの識別情報から生成される第２の固

有情報は、第１の固有情報と不一致となり得る。その結果、セキュリティエンジンによって管理された環境下とは異なる環境下での制御プログラムの起動を防ぐことができる。すなわち、制御プログラムという知的財産を保護することができる。

【００１０】

さらに、デバイスの種別を識別する第１の識別情報およびデバイスを個別に識別する第２の識別情報からセキュリティポリシーに応じて識別情報が選択される。そのため、制御プログラムの開発者は、制御プログラムに対するセキュリティ対策の優先度を考慮して、セキュリティポリシーを適宜設定できる。その結果、セキュリティエンジンにおけるセキュリティレベルを任意に変更できる。

【００１１】

上述の開示において、セキュリティポリシーは、第１のポリシー、第２のポリシーおよび第３のポリシーの中から予め設定される。第１のポリシーは、１以上のデバイスの各々について第１の識別情報を選択するポリシーである。第２のポリシーは、１以上のデバイスのうち第１のグループに属する第１のデバイスについて第１の識別情報を選択し、１以上のデバイスのうち、第１のグループよりもセキュリティ対策の優先度の高い第２のグループに属する第２のデバイスについて第２の識別情報を選択するポリシーである。第３のポリシーは、１以上のデバイスの各々について第２の識別情報を選択するポリシーである。

【００１２】

この開示によれば、開発者は、制御プログラムに対するセキュリティ対策の優先度を考慮して、セキュリティエンジンにおけるセキュリティレベルを任意に変更できる。

【００１３】

上述の開示において、１以上のデバイスの各々は、第２の識別情報を保持する。第２の識別情報は、第１の識別情報と、第１の識別情報によって識別される種別のデバイスの個体に対してユニークに割り当てられる第３の識別情報との組み合わせである。生成手段は、第２の識別情報から第１の識別情報を取得する。この開示によれば、各デバイスは、第２の識別情報のみを記憶しておけばよい。

【００１４】

上述の開示において、１以上のデバイスは、制御エンジンを有する制御デバイスと、セキュリティエンジンを有するセキュリティデバイスとを含む。

【００１５】

この開示によれば、制御プログラムに対する変更の自由度を満たす必要のある制御エンジンと、セキュリティ上、変更の自由度が好まれないセキュリティエンジンとを、互いに異なるデバイスによって実現することで、各エンジンの特性に応じたデバイス設計を可能にする。

【００１６】

上述の開示において、保持手段は、外部装置との間で、分散型台帳の形式で第１の固有情報を保持する。

【００１７】

この開示によれば、第１の固有情報は、より改竄困難な状態で保持される。これにより、制御プログラムという知的財産のセキュリティレベルを高めることができる。

【００１８】

上述の開示において、照合手段は、第２の固有情報と外部装置が保持する第１の固有情報とをさらに照合する。

【００１９】

この開示によれば、不正に制御装置をコピーした第三者は、制御プログラムを実行させるために、外部装置が保持する第１の固有情報を改竄する必要が生じる。そのため、制御プログラムのセキュリティレベルをさらに高めることができる。

【００２０】

本開示の別の一例によれば、１以上のデバイスを含む制御装置において実行される管理方法は、第１～第４のステップを備える。第１のステップは、予め生成された第１の固有

情報を保持するステップである。第２のステップは、制御プログラムの実行開始要求に応答して、１以上のデバイスの各々から取得された識別情報を用いて第２の固有情報を生成するステップである。第３のステップは、第１の固有情報と第２の固有情報とを照合するステップである。第４のステップは、照合結果に基づいて、制御プログラムの実行可否を判定するステップである。第２のステップ（生成するステップ）は、１以上のデバイスの各々について、当該デバイスの種別を識別する第１の識別情報および当該デバイスを個別に識別する第２の識別情報からセキュリティポリシーに応じて識別情報を選択するステップを含む。

【００２１】

本開示の別の一例によれば、セキュリティプログラムは、上記の管理方法をコンピュータに実行させる。

【００２２】

これらの開示によっても、制御プログラムという知的財産の保護を図ることができる。

【発明の効果】

【００２３】

本開示によれば、制御プログラムという知的財産の保護を図ることができる。

【図面の簡単な説明】

【００２４】

【図１】実施の形態に係る制御装置を適用した場面の一例を示す図である。

【図２】本実施の形態に係る制御装置１を含む制御システム１０の全体構成を示す模式図である。

【図３】本実施の形態に従う制御装置１を構成する制御ユニット１００のハードウェア構成例を示す模式図である。

【図４】本実施の形態に従う制御装置１を構成するセキュリティユニット２００のハードウェア構成例を示す模式図である。

【図５】制御装置１に含まれる各デバイスが有する識別情報４０の一例を示す図である。

【図６】制御プログラム１４０の実行可否の判断方法の流れを示す図である。

【図７】制御ユニット１００およびセキュリティユニット２００の機能構成の一例を示すブロック図である。

【図８】本実施の形態における、制御プログラム１４０の実行開始要求を受けたときの処理手順を示すシーケンス図である。

【図９】分散型台帳の形式で保持される管理情報３０の一例を示す図である。

【図１０】新たなブロック５０が生成される際に機能するセキュリティユニット２００の機能構成を示す図である。

【図１１】変形例１における、制御プログラム１４０の実行開始要求を受けたときの処理手順を示すシーケンス図である。

【図１２】変形例２における、制御プログラム１４０の実行開始要求を受けたときの処理手順の別の例を示すシーケンス図である。

【発明を実施するための形態】

【００２５】

以下、図面を参照しつつ、本発明に従う各実施の形態について説明する。以下の説明では、同一の部品および構成要素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、これらについての詳細な説明は繰り返さない。なお、以下で説明される各実施の形態および各変形例は、適宜選択的に組み合わせてもよい。

【００２６】

§１．適用例

本実施の形態にかかる制御システムの概略について説明する。図１は、実施の形態に係る制御装置１を適用した場面の一例を示す図である。図１に示されるように、制御装置１は、制御対象を制御するための制御プログラム１４０と、制御プログラム１４０を実行する制御エンジン１４２と、制御エンジン１４２での制御プログラム１４０の実行可否を管

理するセキュリティエンジン２３０とを備える。
【００２７】
制御装置１は、１以上のデバイスを含む。制御プログラム１４０が実行されることで各デバイスが制御され、各デバイスが制御されることで、制御対象である製造設備などが制御される。
【００２８】
セキュリティエンジン２３０は、許可部２３２と、生成部２３４と、保持部２３６と、照合部２３８とを含む。
【００２９】
許可部２３２は、制御エンジン１４２から制御プログラム１４０の開始要求を受けて、当該制御プログラム１４０の実行可否を判断する。
【００３０】
生成部２３４は、制御装置１を構成する１以上のデバイスの各々から取得された識別情報を用いて固有情報を生成する。生成部２３４は、１以上のデバイスの各々について、当該デバイスの種別を識別する第１の識別情報および当該デバイスを個別に識別する第２の識別情報からセキュリティポリシーに応じて識別情報を選択する。固有情報は、このようにして取得された識別情報を用いて生成されるため、制御装置１の構成が変わることに応じて変化する。
【００３１】
保持部２３６は、制御装置１について予め生成された固有情報２０を含む管理情報３０を保持する。保持部２３６は、固有情報２０が不正に改竄されることを防止するため、所定条件を満たす場合にのみ管理情報３０の更新を許可する。所定条件とは、たとえば予め設定されたアクセスＩＤおよびパスワードと入力情報とが一致するという条件である。
【００３２】
照合部２３８は、照合の要求に従って生成部２３４によって生成された固有情報２２と、管理情報３０に含まれる固有情報２０とを照合する。照合とは、一致するか否かを判定することを意味する。
【００３３】
次に、図１に示すステップ１から順に、制御装置１において実行される制御プログラムの実行可否の管理方法について説明する。なお、図１および以下の説明において、ステップを単に「Ｓ」と記す。
【００３４】
Ｓ１：生成部２３４は、予め、制御装置１の固有情報２０を生成する。保持部２３６は、予め生成された固有情報２０を含む管理情報３０を保持する。
【００３５】
Ｓ２：許可部２３２は、制御プログラム１４０の開始要求を受ける。なお、図１に示す例では、制御エンジン１４２が、開始要求を行うものとしているが、セキュリティエンジン２３０が開始要求を受け付ける受付部を備えていてもよい。
【００３６】
Ｓ３：許可部２３２は、制御プログラム１４０の開始要求に応じて、照合部２３８に照合の要求を行う。
【００３７】
Ｓ４：照合部２３８は、照合の要求に応じて、生成部２３４に対して固有情報２２の生成を要求する。
【００３８】
Ｓ５：生成部２３４は、生成の要求に応じて、制御装置１が備える１以上のデバイスから識別情報を取得し、取得した識別情報を用いて固有情報２２を生成する。生成部２３４は、各デバイスについて、当該デバイスの種別を識別する第１の識別情報および当該デバイスを個別に識別する第２の識別情報からセキュリティポリシーに応じて識別情報を選択する。なお、生成部２３４は、１以上のデバイスの全てについて第１の識別情報を選択し

てもよいし、１以上のデバイスの全てについて第２の識別情報を選択してもよい。あるいは、生成部２３４は、１以上のデバイスのうちの一部のデバイスについて第１の識別情報を選択し、残りのデバイスについて第２の識別情報を選択してもよい。セキュリティポリシーは、制御装置１に対して予め設定される。

【００３９】

Ｓ６：照合部２３８は、管理情報３０に含まれている、予め生成された固有情報２０と、照合の要求を受けたタイミングで生成された固有情報２２とを照合して照合結果を得る。

【００４０】

Ｓ７：照合部２３８は、得られた照合結果を許可部２３２に提供する。許可部２３２は、提供された照合結果に基づいて、制御プログラム１４０の実行可否を判定する。具体的には、許可部２３２は、照合結果が一致を示すことに応じて、制御プログラム１４０の実行を許可する。許可部２３２は、照合結果が不一致を示すことに応じて、制御プログラム１４０の実行を禁止する。

【００４１】

Ｓ８：許可部２３２は、照合結果に基づいて判定した結果（許可または禁止）を、制御エンジン１４２に対して提供する。制御エンジン１４２は、許可部２３２の判定結果が「許可」である場合に限って、制御プログラム１４０を実行する。

【００４２】

制御装置１によって管理された環境を実現するための制御プログラム１４０の開発は、制御装置１を利用する会社とは別の会社が行うこともある。このような場合に、制御プログラム１４０および制御プログラム１４０を利用できる環境が容易に模倣されてしまうと、制御プログラム１４０を開発する会社の知的財産を十分に保護することができない。

【００４３】

制御装置１を模倣する場合、制御プログラム１４０を実行するために、制御装置１のハードウェアおよびソフトウェアの双方がコピーされる。ソフトウェアがコピーされるということは、制御プログラム１４０だけでなく、制御エンジン１４２およびセキュリティエンジン２３０を動作させるためのシステムプログラムもコピーされる。さらに、ソフトウェアのコピーにより、セキュリティエンジン２３０によって保持されている管理情報３０についてもコピーされる。

【００４４】

一方、ハードウェアについては、制御装置１を構成する各デバイスに代わるデバイスを設置することにより、制御装置１が模倣される。制御装置１を模倣した別の制御装置では、制御装置１とは異なるデバイスから取得された識別情報を用いて固有情報２２が生成される。そのため、固有情報２２は、コピーされた管理情報３０に含まれる固有情報２０と不一致となり得る。特に、少なくとも１つのデバイスについて第２の識別情報を取得するようにセキュリティポリシーを設定することにより、固有情報２２は、固有情報２０と一致しない。あるいは、制御装置１を構成する少なくとも１つのデバイスについて、当該デバイスと同じ機能を有する別の機種のデバイスを用いて模倣した場合、当該デバイスについて第１の識別情報を取得したとしても、固有情報２２は、固有情報２０と一致しない。その結果、セキュリティエンジン２３０によって管理された環境下とは異なる環境下での制御プログラム１４０の起動を防ぐことができる。すなわち、制御プログラム１４０という知的財産を保護することができる。

【００４５】

なお、制御装置１を模倣した別の制御装置において、各デバイスの識別情報を改竄することにより、固有情報２２が固有情報２０と一致し得る。しかしながら、制御装置１を構成するデバイスの個数は数十となることもあり、このような場合に、数十のデバイスすべてについて、当該デバイスの識別情報を改竄する必要が生じる。そのため、制御プログラム１４０によって管理される制御装置１を模倣するには、多くの労力を要することとなる。

【００４６】

また、本実施の形態では、デバイスの種別を識別する第１の識別情報およびデバイスを

個別に識別する第２の識別情報からセキュリティポリシーに応じて識別情報が選択される。たとえば、制御プログラム１４０の開発者は、故障や定期メンテナンスなどで交換が想定されるデバイスについて、第１の識別情報を選択することによりセキュリティ対策の優先度を低くしてもよい。これにより、開発者は、デバイス交換などの保守性と知的財産保護とのバランスをとることができる。

【００４７】

§２．具体例

＜Ａ．制御システム＞

図２は、本実施の形態に係る制御装置１を含む制御システム１０の全体構成を示す模式図である。図２を参照して、制御システム１０は、１以上の制御装置１と、上位機器３とを備える。

【００４８】

制御装置１は、制御対象を制御する。制御対象は、生産工程を自動化するための種々の産業用機器を含み、製造装置や生産ラインなど（以下、「フィールド」とも総称する。）に対して何らかの物理的な作用を与える装置と、フィールドとの間で情報を遣り取りする入出力装置とを含む。なお、生産ライン全体を制御対象としてもよい。

【００４９】

制御装置１は、情報系ネットワーク２を介して、上位機器３および他の制御装置１と通信可能に接続される。情報系ネットワーク２は、たとえば、ＥｔｈｅｒＮｅｔ／ＩＰ（登録商標）または、ベンダやＯＳ（Operating System）の種類などに依存することなくデータ交換を実現することができるＯＰＣ　ＵＡ（Object Linking and Embedding for Process Control Unified Architecture）などの通信規格に従ったネットワークである。

【００５０】

制御装置１は、１以上のデバイスを含む。図２に示す例では、制御装置１は、制御ユニット１００、セキュリティユニット２００、Ｉ／Ｏ（Input/Output）ユニット３００、通信カプラ４００などから構成される。なお、以下では、制御装置１を構成する各ユニットおよび通信カプラを総じて「デバイス」とも称する。

【００５１】

制御ユニット１００は、制御装置１を構成する制御デバイスの一例であって、制御対象を制御するための制御プログラムを実行し、制御装置１において中心的な処理を実行する。

【００５２】

セキュリティユニット２００は、制御装置１を構成するセキュリティデバイスの一例であって、制御ユニット１００での制御プログラムの実行可否を管理する。制御プログラムの実行可否の管理方法は、後述する。

【００５３】

制御ユニット１００とセキュリティユニット２００との間は、たとえば、任意のデータ伝送路（例えば、ＰＣＩ　Ｅｘｐｒｅｓｓあるいは ＥｔｈｅｒＮｅｔ／ＩＰ（登録商標）など）を介して接続されている。

【００５４】

Ｉ／Ｏユニット３００は、制御装置１を構成するデバイスの一例であって、一般的な入出力処理に関するユニットである。Ｉ／Ｏユニット３００は、各種センサ、各種スイッチ、エンコーダなどを含むＩＯデバイスから検出値を収集する。

【００５５】

制御ユニット１００とＩ／Ｏユニット３００とは、内部バスを介して通信可能に接続されている。制御ユニット１００は、Ｉ／Ｏユニット３００により収集された検出値を用いて制御プログラムの演算を実行し、演算結果の値をＩ／Ｏユニット３００に出力する。

【００５６】

通信カプラ４００は、フィールドネットワーク４を介して制御ユニット１００と通信可能に接続される。通信カプラ４００は、フィールドネットワーク４でのデータ伝送にかかる処理を行う。通信カプラ４００は、たとえば、内部バスを介して１または複数のＩ／Ｏ

ユニット３００と通信可能に接続される。通信カプラ４００に接続された１または複数のＩ／Ｏユニット３００の各々により収集された検出値は、フィールドネットワーク４を介して制御ユニット１００に出力される。

【００５７】

フィールドネットワーク４としては、典型的には、各種の産業用イーサネット（登録商標）を用いることができる。産業用イーサネット（登録商標）としては、例えば、ＥｔｈｅｒＣＡＴ（登録商標）、Ｐｒｏｆｉｎｅｔ ＩＲＴ、ＭＥＣＨＡＴＲＯＬＩＮＫ（登録商標）－ＩＩＩ、Ｐｏｗｅｒｌｉｎｋ、ＳＥＲＣＯＳ（登録商標）－ＩＩＩ、ＣＩＰ Ｍｏｔｉｏｎなどが知られており、これらのうちのいずれを採用してもよい。さらに、産業用イーサネット（登録商標）以外のフィールドネットワークを用いてもよい。例えば、モーション制御を行わない場合であれば、ＤｅｖｉｃｅＮｅｔ、ＣｏｍｐｏＮｅｔ／ＩＰ（登録商標）などを用いてもよい。

【００５８】

制御装置１を構成する各デバイスは、識別情報４０を有する。典型的には、識別情報４０は、ＳＧＴＩＮ（Serialized Global Trade Item Number）のような個体識別コードである。

【００５９】

なお、制御装置１を構成するデバイスは、図２に示したデバイスに限られない。制御装置１を構成するデバイスは、たとえば、電源を供給する電源ユニット、Ｉ／Ｏユニット３００ではサポートしない機能を有する特殊ユニット、設備や機械などによって人の安全が脅かされることを防止するためのセーフティ機能を提供するセーフティユニットなどを含み得る。また、制御装置１を構成するデバイスは、たとえば、制御ユニット１００または他のユニットでの制御演算によって得られる各種情報をオペレータへ提示するとともに、オペレータからの操作に従って、制御ユニット１００または他のユニットに対して内部コマンドなどを生成するＨＭＩ（Human Machine Interface）を含み得る。

【００６０】

上位機器３は、制御システム１００内のサーバ、またはクラウドサーバ等のような外部サーバ、または制御装置１に比較して高い性能を備えたＰＬＣ、または産業用のコンピュータ（所謂ＩＰＣ：Industrial Personal Computer）として構成される。

【００６１】

＜Ｂ．ハードウェア構成＞

本実施の形態に従う制御装置１を構成する主なデバイスのハードウェア構成例について説明する。

【００６２】

（ｂ１．制御ユニット）

図３は、本実施の形態に従う制御装置１を構成する制御ユニット１００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１００は、主たるコンポーネントとして、ＣＰＵ（Central Processing Unit）やＧＰＵ（Graphical Processing Unit）などのプロセッサ１０２と、チップセット１０４と、主記憶装置１０６と、二次記憶装置１０８と、通信コントローラ１１０と、ＵＳＢコントローラ１１２と、メモリカードインターフェイス１１４と、フィールドネットワークコントローラ１１６と、内部バスコントローラ１１８と、情報系ネットワークコントローラ１２０とを含む。

【００６３】

プロセッサ１０２は、二次記憶装置１０８またはメモリカード１１５に格納された各種プログラムを読み出して、主記憶装置１０６に展開して実行することで、制御対象を制御するための制御演算、および、後述するような、制御プログラムの実行開始要求にかかる処理を実現する。

【００６４】

主記憶装置１０６は、ＤＲＡＭ（Dynamic Random Access Memory)またはＳＲＡＭ（Static Random Access Memory)などの揮発性記憶装置などで構成される。二次記憶

装置１０８は、例えば、ＨＤＤ（Hard Disc Drive）またはＳＳＤ（Solid State Drive）などの不揮発性記憶装置などで構成される。

【００６５】

チップセット１０４は、プロセッサ１０２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１００全体としての処理を実現する。

【００６６】

二次記憶装置１０８には、制御ユニット１００の基本的な機能を実現するためのシステムプログラム１０８２に加えて、設備や機械などの制御対象に応じて作成される制御プログラム１４０と、制御ユニット１００を識別するための識別情報４０とが格納されている。

【００６７】

システムプログラム１０８２には、認証プログラム１３０が組み込まれている。認証プログラム１３０は、制御プログラム１４０を起動する際に実行されるプログラムであって、セキュリティユニット２００に向けて、起動する制御プログラム１４０の実行の許可を要求するためのプログラムである。また、システムプログラム１０８２は、制御プログラム１４０を実行する制御エンジンとしての機能を提供する。

【００６８】

制御プログラム１４０は、たとえば、基本的なアルゴリズムがプログラム開発会社によって作成された知的財産である。たとえば、ユーザは、制御装置１に応じてパラメータを設定することで、プログラム開発会社により提供された制御プログラム１４０を実行可能な環境を整える。

【００６９】

通信コントローラ１１０は、セキュリティユニット２００との間のデータの遣り取りを担当する。通信コントローラ１１０としては、例えば、ＰＣＩ Ｅｘｐｒｅｓｓあるいはイーサネット（登録商標）などに対応する通信チップを採用できる。

【００７０】

ＵＳＢコントローラ１１２は、ＵＳＢ接続を介して任意の情報処理装置との間のデータの遣り取りを担当する。任意の情報処理装置は、たとえば、制御プログラム１４０の作成または編集、デバッグ、各種パラメータの設定などの機能をユーザに提供するサポート装置などを含む。

【００７１】

メモリカードインターフェイス１１４は、記憶媒体の一例であるメモリカード１１５を着脱可能に構成される。メモリカードインターフェイス１１４は、メモリカード１１５に対して制御プログラム１４０や各種設定などのデータを書込み、あるいは、メモリカード１１５から制御プログラム１４０や各種設定などのデータを読出すことが可能になっている。

【００７２】

フィールドネットワークコントローラ１１６は、フィールドネットワーク４を介した他の装置との間のデータの遣り取りを制御する。

【００７３】

内部バスコントローラ１１８は、内部バスを介した他の装置（Ｉ／Ｏユニット３００など）との間のデータの遣り取りを制御する。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。

【００７４】

情報系ネットワークコントローラ１２０は、情報系ネットワーク２を介した他の制御装置１との間のデータの遣り取りを制御する。

【００７５】

図３には、プロセッサ１０２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またはＦＰＧＡなど）を用いて実装してもよい。あるいは、制御ユニ

ット１００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。

【００７６】

（ｂ２．セキュリティユニット）

図４は、本実施の形態に従う制御装置１を構成するセキュリティユニット２００のハードウェア構成例を示す模式図である。図４を参照して、セキュリティユニット２００は、主たるコンポーネントとして、ＣＰＵやＧＰＵなどのプロセッサ２０２と、チップセット２０４と、主記憶装置２０６と、二次記憶装置２０８と、通信コントローラ２１０と、ＵＳＢコントローラ２１２と、メモリカードインターフェイス２１４と、情報系ネットワークコントローラ２２０とを含む。

【００７７】

プロセッサ２０２は、二次記憶装置２０８またはメモリカード２１５に格納された各種プログラムを読み出して、主記憶装置２０６に展開して実行することで、制御ユニット１００での制御プログラムの実行可否を管理する機能を実現する。主記憶装置２０６は、ＤＲＡＭまたはＳＲＡＭなどの揮発性記憶装置などで構成される。二次記憶装置２０８は、例えば、ＨＤＤまたはＳＳＤなどの不揮発性記憶装置などで構成される。

【００７８】

チップセット２０４は、プロセッサ２０２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、セキュリティユニット２００全体としての処理を実現する。

【００７９】

二次記憶装置２０８には、セキュリティユニット２００の基本的な機能を実現するためのシステムプログラム２０８２に加えて、識別情報４０および管理情報３０が格納されている。

【００８０】

システムプログラム２０８２には、セキュリティプログラム２４０が組み込まれている。セキュリティプログラム２４０は、制御装置１において実行される制御プログラム１４０の実行可否を管理するためのプログラムである。すなわち、セキュリティプログラム２４０は、制御プログラム１４０の実行可否を管理するセキュリティエンジンとしての機能を提供する。

【００８１】

管理情報３０は、制御装置１を構成する１以上のデバイスから取得した識別情報４０を用いて生成される固有情報を管理するための情報である。固有情報は、制御プログラム１４０の実行を許可するか否かを判定する際の基準となる情報として利用される。固有情報については、後述する。

【００８２】

通信コントローラ２１０は、制御ユニット１００との間のデータの遣り取りを担当する。通信コントローラ２１０としては、制御ユニット１００に通信コントローラ２１０と同様に、例えば、ＰＣＩ　Ｅｘｐｒｅｓｓあるいはイーサネット（登録商標）などに対応する通信チップを採用できる。

【００８３】

ＵＳＢコントローラ２１２は、ＵＳＢ接続を介して任意の情報処理装置との間のデータの遣り取りを担当する。任意の情報処理装置は、たとえば、セキュリティプログラム２４０の設定などの機能をユーザに提供するサポート装置などを含む。

【００８４】

メモリカードインターフェイス２１４は、記憶媒体の一例であるメモリカード２１５を着脱可能に構成される。メモリカードインターフェイス２１４は、メモリカード２１５に対してプログラムや各種設定などのデータを書込み、あるいは、メモリカード２１５からプログラムや各種設定などのデータを読出すことが可能になっている。

【００８５】
情報系ネットワークコントローラ２２０は、情報系ネットワーク２を介した他の制御装置１との間のデータの遣り取りを制御する。情報系ネットワークコントローラ２２０は、イーサネット（登録商標）などの汎用的なネットワークプロトコルを採用してもよい。
【００８６】
図４には、プロセッサ２０２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またはＦＰＧＡなど）を用いて実装してもよい。あるいは、セキュリティユニット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。
【００８７】
なお、図３および図４を参照して、制御装置１は、情報系ネットワーク２へ、制御ユニット１００の情報系ネットワークコントローラ１２０を介して接続されていてもよく、また、セキュリティユニット２００の情報系ネットワークコントローラ２２０を介して接続されていてもよい。本実施の形態において、制御装置１は、セキュリティユニット２００の情報系ネットワークコントローラ２２０を介して接続されているものとして説明する。
【００８８】
＜Ｃ．識別情報＞
図５は、制御装置１に含まれる各デバイスが有する識別情報４０の一例を示す図である。図５には、ＳＧＴＩＮである識別情報４０が示される。ＳＧＴＩＮは、流通システム標準化機関ＧＳ１によって標準化された電子タグに書き込むための識別コードの１つであり、商品用の個別識別コードである。識別情報４０は、デバイスを個別に識別するため、第２の識別情報である。
【００８９】
図５に示されるように、識別情報４０は、デバイスの種別を識別する商品識別コードである識別情報４２と、当該識別情報４２によって識別される種別のデバイスの個体に対してユニークに割り当てられるシリアル番号４４（第３の識別情報）との組み合わせである。識別情報４２は、デバイスの種別を識別するため、第１の識別情報である。
【００９０】
識別情報４２は、流通システム標準化機関ＧＳ１によって標準化された商品識別コードＧＴＩＮ（Global Trade Item Number）である。ＧＴＩＮは、インジケータと、事業者コードと、商品アイテムコードと、チェックデジットとによって構成される。
【００９１】
＜Ｄ．セキュリティポリシー＞
制御プログラム１４０の開発者は、制御プログラム１４０に対するセキュリティポリシーを設定する。なお、セキュリティポリシーの設定は、制御プログラム１４０の開発者に限定されず、他の者によって実行されてもよい。セキュリティポリシーは、セキュリティプログラム２４０に予め設定される。
【００９２】
本実施の形態では、セキュリティポリシーは、以下のポリシー（Ａ）～（Ｃ）の中から予め設定される。
ポリシー（Ａ）：全てのデバイスについて識別情報４０（第２の識別情報）を選択する。
ポリシー（Ｂ）：第１のグループに属する第１のデバイスについて識別情報４２（第１の識別情報）を選択し、第１のグループよりもセキュリティ対策の優先度の高い第２のグループに属する第２のデバイスについて識別情報４０（第２の識別情報）を選択する。
ポリシー（Ｃ）：全てのデバイスについて識別情報４２（第１の識別情報）を選択する。
【００９３】
たとえば、開発者は、制御プログラム１４０が模倣される可能性が高く、かつ、制御プ

ログラム１４０のセキュリティレベルを高めたい場合、ポリシー（Ａ）を設定する。開発者は、制御プログラム１４０が模倣される可能性が低い場合、あるいは、制御プログラム１４０の知的財産としての価値が高くない場合、ポリシー（Ｂ）またはポリシー（Ｃ）を設定する。

【００９４】

ポリシー（Ｂ）を設定する場合、開発者は、第１のグループに属するデバイスの商品識別コードＧＴＩＮ（識別情報４２）と、第２のグループに属するデバイスの商品識別コードＧＴＩＮ（識別情報４２）とを予め設定する。

【００９５】

＜Ｅ．制御プログラムの実行可否の判断方法の概略＞

図６は、制御プログラム１４０の実行可否の判断方法の流れを示す図である。なお、図６に示す例では、図面を簡略にするため、制御装置１を構成する制御ユニット１００およびセキュリティユニット２００以外のユニット（Ｉ／Ｏユニット３００、通信カプラ４００など）の記載を省略している。

【００９６】

制御ユニット１００は、まず、セキュリティユニット２００に向けて制御プログラム１４０の実行可否判定を要求する（図中の（１））。

【００９７】

制御ユニット１００からの判定要求を受けて、セキュリティユニット２００は、制御装置１を構成する１以上のデバイスから識別情報４０の収集を行う（図中の（２））。

【００９８】

セキュリティユニット２００は、予め設定されたセキュリティポリシーに従って、各デバイスの識別情報４０（ＳＧＴＩＮ）および識別情報４０に含まれる識別情報４２（ＧＴＩＮ）のうちの一方を選択する（図中の（３））。上記のポリシー（Ａ）が設定されている場合、セキュリティユニット２００は、全てのデバイスについて、識別情報４０を選択する。上記のポリシー（Ｂ）が設定されている場合、セキュリティユニット２００は、第１のグループに設定されている商品識別コードＧＴＩＮに対応するデバイスについて識別情報４２を選択する。さらに、セキュリティユニット２００は、第２のグループに設定されている商品識別コードＧＴＩＮに対応するデバイスについて識別情報４０を選択する。上記のポリシー（Ｃ）が設定されている場合、セキュリティユニット２００は、全てのデバイスについて、識別情報４２を選択する。

【００９９】

セキュリティユニット２００は、各デバイスについて選択された識別情報（識別情報４０または識別情報４２）に基づいて、固有情報２２としてシステムハッシュ値を生成する（図中の（４））。システムハッシュ値は、制御装置１を構成するデバイスのうちセキュリティユニット２００を除く他のデバイスの識別情報４０を引数とし、公知のハッシュ関数を利用することで得られる。

【０１００】

セキュリティユニット２００は、識別情報４０を用いて生成された固有情報２２（システムハッシュ値）と管理情報３０によって管理されている固有情報２０とを照合し、一致するか否かを判定する（図中の（５））。

【０１０１】

図中の（５）において、新たに生成された固有情報２２と、管理情報３０によって管理されている固有情報２０とを照合し、一致する場合、制御装置１は、正規に管理された装置であることが保証される。一方、一致しない場合、制御装置１は、管理情報３０によって管理されていない制御装置である可能性がある。

【０１０２】

セキュリティユニット２００は、（５）の処理で得られた照合結果に基づいて、（１）で要求された制御プログラム１４０の実行可否判定を行う（図中の（６））。セキュリティユニット２００は、照合結果が「一致」を示すことに応じて、制御プログラム１４０の

実行を許可する。
【０１０３】
セキュリティユニット２００は、制御ユニット１００に向けて制御プログラム１４０の実行可否を示す判定結果を通知する（図中の（７））。
【０１０４】
＜Ｆ．機能構成＞
図７は、制御ユニット１００およびセキュリティユニット２００の機能構成の一例を示すブロック図である。図７において、破線の矢印は、指示に関する流れを示す。実線の矢印は、情報の流れを示す。
【０１０５】
図７に示されるように、制御ユニット１００は、制御プログラム実行部１４４と、認証部１３２とを含む。これらの各機能は、制御ユニット１００のプロセッサ１０２がシステムプログラム１０８２を実行することで実現する。
【０１０６】
制御プログラム実行部１４４は、制御プログラム１４０を実行するために機能する。制御プログラム実行部１４４は、制御プログラム１４０の実行開始要求を受けて、認証部１３２に対して、制御プログラム１４０の認証を要求する。認証とは、制御プログラム１４０の実行環境が、制御装置１が保持する管理情報３０によって管理されている環境であるか否かを認証することであって、制御プログラム１４０を実行してよい環境であるかを認証することである。
【０１０７】
認証部１３２は、判定要求部１３４と、識別情報送信部１３６と、識別情報収集部１３８とを含む。制御プログラム実行部１４４から認証の要求を受けると、判定要求部１３４は、セキュリティユニット２００の許可部２３２に対して、制御プログラム１４０の実行可否判定を要求する。
【０１０８】
識別情報送信部１３６は、識別情報収集部１３８が収集した制御装置１を構成する各デバイスの識別情報４０をセキュリティユニット２００に送信する。
【０１０９】
識別情報収集部１３８は、セキュリティユニット２００の生成部２３４からの要求を受けて、制御装置１を構成する各デバイスの識別情報４０を収集する。識別情報収集部１３８は、制御プログラム１４０の実行可否を判定するときに加えて、新たな固有情報（システムハッシュ値）を管理情報３０に登録するときにも、セキュリティユニット２００から識別情報４０の収集を要求される。なお、本実施の形態においては、識別情報収集部１３８は、制御装置１を構成するデバイスのうち、セキュリティユニット２００を除くデバイスの各々から識別情報４０を収集する。なお、固有情報であるシステムハッシュ値の生成に用いられる識別情報４０に、セキュリティユニット２００の識別情報４０を含めてもよい。
【０１１０】
認証部１３２は、制御プログラム実行部１４４から制御プログラム１４０の認証が要求された後、セキュリティユニット２００の許可部２３２から制御プログラム１４０の実行可否の判定結果を受ける。認証部１３２は、セキュリティユニット２００から受けた判定結果に従った処理をする。認証部１３２は、実行を許可できる旨の判定結果を得た場合、制御プログラム実行部１４４に向けて、制御プログラム１４０の実行を開始するように通知する。一方、認証部１３２は、実行が許可できない旨の判定結果を得た場合、制御プログラム実行部１４４に向けて、制御プログラム１４０の実行を禁止するよう指示する。
【０１１１】
セキュリティユニット２００は、許可部２３２と、生成部２３４と、保持部２３６と、照合部２３８とを含む。これらの各機能は、セキュリティユニット２００のプロセッサ２０２がセキュリティプログラム２４０を実行することで実現する。

【０１１２】
許可部２３２は、判定部２３２２と照合要求部２３２４とを含む。判定部２３２２は、判定部２３２２が含まれるセキュリティユニット２００の照合部２３８および他のセキュリティユニット２００の照合部２３８から得られる照合結果に基づいて、制御プログラム１４０の実行を許可するか否かを判定し、判定結果を制御ユニット１００の認証部１３２に通知する。照合要求部２３２４は、照合部２３８に対して、固有情報の照合を要求する。
【０１１３】
生成部２３４は、固有情報であるシステムハッシュ値を生成する。生成部２３４は、収集要求部２３４２とシステムハッシュ値演算部２３４４とを含む。
【０１１４】
収集要求部２３４２は、照合部２３８から、または、保持部２３６からシステムハッシュ値の生成を要求されたときに機能する。照合部２３８は、照合を開始するときにシステムハッシュ値の生成を要求する。保持部２３６は、たとえば、制御装置１が正規に変更された場合など、制御装置１を構成するデバイスが変更されて、変更後の制御装置１の固有情報を管理情報３０に新たに登録するときにシステムハッシュ値の生成を要求する。収集要求部２３４２は、制御ユニット１００の識別情報収集部１３８に対して、識別情報４０の収集を要求する。
【０１１５】
システムハッシュ値演算部２３４４は、識別情報送信部１３６から送られた各デバイスの識別情報４０を用いてシステムハッシュ値を生成する。システムハッシュ値演算部２３４４は、典型的には、公知のハッシュ関数に利用されるアルゴリズムを利用してシステムハッシュ値を生成する。
【０１１６】
システムハッシュ値演算部２３４４は、予め設定されているセキュリティポリシーに従って、識別情報４０（ＳＧＴＩＮ）および識別情報４０の一部である識別情報４２（ＧＴＩＮ）の中から、システムハッシュ値の生成に用いる識別情報を選択する。システムハッシュ値演算部２３４４は、各デバイスについて選択した識別情報（識別情報４０または識別情報４２）を用いて、固有情報としてシステムハッシュ値を生成する。
【０１１７】
システムハッシュ値演算部２３４４は、照合部２３８からシステムハッシュ値の生成が要求されている場合には、照合部２３８に生成したシステムハッシュ値を送る。また、システムハッシュ値演算部２３４４は、保持部２３６からシステムハッシュ値の生成が要求されている場合には、保持部２３６に生成したシステムハッシュ値を送る。
【０１１８】
保持部２３６は、保持部２３６からの要求に応じて生成された固有情報２０（システムハッシュ値）を含む管理情報３０を保持する。保持部２３６は、登録部２３６２を含む。
【０１１９】
登録部２３６２は、制御装置１を構成するデバイスが変更され、変更後の制御装置１の固有情報２０を新たに管理情報３０内に登録し、当該固有情報２０の管理を開始するときに機能する。登録部２３６２は、予め設定されたアクセスＩＤおよびパスワードと入力情報とが一致するという条件が満たされたことに応じて、処理を開始する。
【０１２０】
登録部２３６２は、生成部２３４に向けて固有情報２０の生成を要求する。登録部２３６２は、生成部２３４が生成した固有情報２０を管理情報３０の一部として登録する。
【０１２１】
保持部２３６は、照合部２３８からの要求に応じて、管理情報３０に含まれる固有情報２２を照合部２３８に送信する。
【０１２２】
照合部２３８は、照合要求部２３２４の要求を受けて、生成部２３４に対して、固有情報２２の生成を要求する。また、照合部２３８は、照合要求部２３２４の要求を受けて、

保持部２３６に対して、管理情報３０に含まれる固有情報２０の送信を要求する。照合部２３８は、システムハッシュ値演算部２３４４から送られた固有情報２２と、保持部２３６から送られた固有情報２０とを照合し、照合した結果を判定部２３２２に送る。

【０１２３】

＜Ｇ．シーケンス図＞

図８は、本実施の形態における、制御プログラム１４０の実行開始要求を受けたときの処理手順を示すシーケンス図である。なお、以下では、シーケンスを単に「ＳＱ」と記載する。

【０１２４】

ＳＱ１０２において、制御ユニット１００は、制御プログラムの開始要求をセキュリティユニット２００に向けて通知する。

【０１２５】

ＳＱ１０４において、セキュリティユニット２００は、識別情報４０の収集を制御ユニット１００に向けて要求する。

【０１２６】

ＳＱ１０６において、制御ユニット１００は、制御装置１を構成する各デバイスの識別情報４０をセキュリティユニット２００に向けて送る。

【０１２７】

ＳＱ１０８において、セキュリティユニット２００は、セキュリティポリシーに従って、各デバイスについて識別情報４０（ＳＧＴＩＮ）および識別情報４０の一部である識別情報４２（ＧＴＩＮ）のうちの１つの識別情報を選択する。

【０１２８】

ＳＱ１１０において、セキュリティユニット２００は、各デバイスについて選択された識別情報を用いて固有情報２２（システムハッシュ値）を生成する。

【０１２９】

ＳＱ１１２において、セキュリティユニット２００は、生成された固有情報２２と、管理情報３０内の固有情報２０（システムハッシュ値）とを照合して照合結果を得る。

【０１３０】

ＳＱ１１４において、セキュリティユニット２００は、ＳＱ１１２によって得られる照合結果に基づいて、制御プログラムの実行の可否を判定する。具体的には、セキュリティユニット２００は、照合結果が「一致」を示すことに応じて、制御プログラムの実行を許可する。一方、セキュリティユニット２００は、照合結果が「不一致」を示すことに応じて、制御プログラムの実行を禁止する。

【０１３１】

Ｓ１１６において、セキュリティユニット２００は、制御ユニット１００に向けて判定結果を通知する。

【０１３２】

＜Ｈ．変形例＞

（ｈ１．変形例１）

セキュリティエンジン２３０の保持部２３６は、他の装置との間で、分散型台帳の形式で管理情報３０を保持してもよい。たとえば、管理情報３０は、上位機器３との間で、分散型台帳の形式で保持される。この場合、管理情報３０は、公知の分散型台帳技術を利用して制御装置１および上位機器３によって管理および共有される。あるいは、管理情報３０は、他の制御装置１との間で、分散型台帳の形式で保持されてもよい。この場合、管理情報３０は、公知の分散型台帳技術を利用して複数の制御装置１によって管理および共有される。あるいは、管理情報３０は、クラウド上において、分散型台帳の形式で保持されてもよい。管理情報３０は、分散型台帳の形式で保持されるため、改竄されにくくなる。

【０１３３】

図９は、分散型台帳の形式で保持される管理情報３０の一例を示す図である。図９に示されるように、管理情報３０は、ひと繋ぎの複数のブロック５０で構成される。各ブロッ

ク５０は、あるタイミングにおける制御装置１の構成から得られる固有情報２０（システムハッシュ値）を少なくとも含む。ブロック５０は、制御装置１を構成するデバイスに変更が生じた場合に生成される。各ブロック５０内の情報は更新されることがなく、新たなブロック５０は、最新のブロック５０に関連して生成される。

【０１３４】

具体的には、各ブロック５０は、ブロックハッシュ値５２と、システム構成情報５４と、ナンス５６とを含む。システム構成情報５４は、セキュリティユニット２００の識別情報４０と、当該セキュリティユニット２００を含む制御装置１の固有情報２０（システムハッシュ値）とを含む。

【０１３５】

ブロックハッシュ値５２は、前ブロックの情報を示すユニークな情報である。ブロックハッシュ値５２は、たとえば、前ブロックの情報を引数とし、公知のハッシュ関数に従って得られた戻り値である。

【０１３６】

図９には、ブロック５０－１から順にブロック５０－ｎまでが管理情報３０に含まれている状況で、制御装置１のデバイス構成に変更が生じ、新たなブロック５０－ｎ＋１が管理情報３０に追加されたときの管理情報３０が示される。ブロック５０－ｎ+１は、ブロックハッシュ値５２－ｎを含む。ブロックハッシュ値５２－ｎは、ブロック５０－ｎの情報を引数とし、公知のハッシュ関数に従って得られた戻り値である。

【０１３７】

ナンス５６は、ブロック５０を新たに生成する際に生成される数値であって、ブロック５０が生成される度に生成される数値である。ナンス５６は、ブロック５０ごとにユニークな値となる。

【０１３８】

図１０は、新たなブロック５０が生成される際に機能するセキュリティユニット２００の機能構成を示す図である。なお、図７を参照して説明した機能については、再度の説明を省略する。また、図１０には、ブロック５０－ｎまで格納されており、制御装置１を構成するデバイスが変更されたことに基づいて、新たにブロック５０－ｎ＋１が格納されるときのデータの流れが示されている。また、図１０に示す例では、管理情報３０は、上位機器３との間で分散型台帳の形式で保持される。

【０１３９】

上述のように、生成部２３４の収集要求部２３４２は、保持部２３６からの固有情報２０（システムハッシュ値）の生成要求を受けて、制御ユニット１００に対して識別情報４０の収集を要求する。システムハッシュ値演算部２３４４は、制御ユニット１００から送られた、制御装置１を構成する各デバイスの識別情報４０に基づいて、固有情報２０を生成する。

【０１４０】

保持部２３６の登録部２３６２は、配布部２３６Ａと、マイニング部２３６Ｂと、ブロックハッシュ値演算部２３６Ｃとを含む。システムハッシュ値演算部２３４４は、生成した固有情報２０を配布部２３６Ａに送る。

【０１４１】

上位機器３は,マイニング部２３６Ｄと、ブロックハッシュ値演算部２３６Ｅと、管理情報３０とを備える。

【０１４２】

配布部２３６Ａは、固有情報２０と、セキュリティユニット２００の識別情報４０とからシステム構成情報５４を生成し、マイニング部２３６Ｂと上位機器３とに配布する。

【０１４３】

登録部２３６２のマイニング部２３６Ｂは、上位機器３のマイニング部２３６Ｄと協働してブロック５０－ｎ＋１を生成する。

【０１４４】

登録部２３６２のブロックハッシュ値演算部２３６Ｃは、管理情報３０に最後に登録されたブロック５０からブロックハッシュ値５２を生成する。図８に示す例では、最後に登録されたブロック５０は、ブロック５０－ｎであるから、ブロック５０－ｎに基づいてブロックハッシュ値５２－ｎが生成される。同様に、上位機器３のブロックハッシュ値演算部２３６Ｅも、管理情報３０に最後に登録されたブロック５０からブロックハッシュ値５２を生成する。

【０１４５】

登録部２３６２のマイニング部２３６Ｂは、システム構成情報５４およびブロックハッシュ値５２－ｎに基づいて、生成するブロック５０から得られる情報が所定の条件を満たすようにナンス５６を設定してブロック５０を生成する。なお、このように、ナンス５６を設定して所定の条件を満たすブロック５０を生成する処理は、マイニングと呼ばれる。上位機器３のマイニング部２３６Ｄもマイニングを行う。マイニング部２３６Ｂ，２３６Ｄのうち、最も早くに所定の条件を満たすナンス５６を見つけたマイニング部が生成したブロック５０が、制御装置１および上位機器３の各々の管理情報３０に格納される。

【０１４６】

すなわち、システム構成情報５４を生成した主体と、ブロック５０を生成した主体とは、異なる場合がある。

【０１４７】

このように、ブロック５０は、制御装置１および上位機器３の各々の管理情報３０に格納される。すなわち、制御装置１および上位機器３の各々の管理情報３０は、改ざんされない限り、共通している。

【０１４８】

管理情報３０に含まれる各ブロック５０は、前のブロック５０に基づいて得られるブロックハッシュ値５２を含む。すなわち、一つのブロック５０を改ざんした場合に、連鎖的に他のブロック５０も改ざんする必要が生じることとなり、管理情報３０の改竄には、多くの労力を要する。すなわち、管理情報３０は、改竄困難な情報であるといえる。このような改竄困難な管理情報３０に含まれる固有情報２０を照合対象とすることにより、制御プログラム１４０の不正な複製利用を抑制できる。

【０１４９】

なお、一のブロック５０を生成する方法は、図９および図１０を参照して説明した方法に限られない。一のブロック５０を生成する方法は、任意に設計されるものであってもよい。

【０１５０】

たとえば、制御装置１のセキュリティレベルに応じて、ブロック５０の生成方法は選択されてもよい。たとえば、制御装置１のセキュリティレベルが高い場合、ブロック５０を生成する過程のセキュリティレベル（透明性、厳格性）を下げることができる。一方、制御装置１のセキュリティレベルが低い場合、ブロック５０を生成する過程のセキュリティレベル（透明性、厳格性）を上げる必要がある。

【０１５１】

具体的には、プライベート型またはコンソーシアム型のブロックチェーン技術を利用して分散型台帳の形式で管理情報３０が保持されている場合、合意形成のハードルを下げ、合意形成に要する時間、すなわち、一のブロック５０を生成して管理情報３０に格納するまでに要する時間を短くできる。一方、パブリック型のブロックチェーン技術を利用して分散型台帳の形式で管理情報３０が保持されている場合、合意形成のハードルを上げる必要がある。

【０１５２】

図１１は、変形例１における、制御プログラム１４０の実行開始要求を受けたときの処理手順を示すシーケンス図である。なお、図１１において、図８と共通するＳＱ番号は、共通の処理であるものとする。以下、図８と異なる処理についてのみ説明する。すなわち、ＳＱ１０２～ＳＱ１１２，ＳＱ１１６の処理は、図８と共通しており、追加されたＳＱ

１２０～ＳＱ１２６について説明する。
【０１５３】
具体的には、ＳＱ１１２のあとのＳＱ１２０において、セキュリティユニット２００は、上位機器３に向けて、ＳＱ１１０で生成した固有情報２２（システムハッシュ値）を送信する。
【０１５４】
ＳＱ１２２において、上位機器３は、管理情報３０内の最新のブロック５０に含まれる固有情報２０と固有情報２２とを照合して照合結果を得る。
【０１５５】
ＳＱ１２４において、上位機器３は、ＳＱ１２２で得られた照合結果をセキュリティユニット２００に向けて送信する。
【０１５６】
ＳＱ１２６において、セキュリティユニット２００は、ＳＱ１１２の照合結果とＳＱ１２４で得られた照合結果とに基づいて、制御プログラムの実行の可否を判定する。具体的には、セキュリティユニット２００は、２つの照合結果のいずれも「一致」を示すことに応じて、制御プログラムの実行を許可する。一方、セキュリティユニット２００は、２つの照合結果の少なくとも一方が「不一致」を示すことに応じて、制御プログラムの実行を禁止する。
【０１５７】
たとえば、制御装置１を不正に模倣することにより別の制御装置が生成された場合に、当該別の制御装置が保持する管理情報３０が改竄され、当該別の制御装置の固有情報２０が管理情報３０内に登録されたものとする。この場合に、当該別の制御装置のセキュリティプログラムは、自装置内の管理情報３０だけでなく、上位機器３の管理情報３０との間でも照合を行う。そのため、上位機器３の管理情報３０についても改竄しなければ制御プログラムの実行が許可されないため、セキュリティレベルを上げることができる。
【０１５８】
（ｈ２．変形例２）
変形例２は、変形例１と同様に、管理情報３０が他の装置（たとえば上位機器３）との間で分散型台帳の形式で保持される例であり、制御プログラム１４０の実行開始要求を受けたときの処理手順の点で異なる。
【０１５９】
図１２は、変形例２における、制御プログラム１４０の実行開始要求を受けたときの処理手順の別の例を示すシーケンス図である。図１２において、図１１と共通するＳＱ番号は、共通の処理であるものとする。図１２に示されるように、変形例２では、ＳＱ１１２が省略され、ＳＱ１２６の代わりにＳＱ１２８が実行される。
【０１６０】
ＳＱ１２８では、セキュリティユニット２００は、ＳＱ１２４で得られた照合結果に基づいて、制御プログラムの実行の可否を判定する。具体的には、セキュリティユニット２００は、照合結果が「一致」を示すことに応じて、制御プログラムの実行を許可する。一方、セキュリティユニット２００は、照合結果が「不一致」を示すことに応じて、制御プログラムの実行を禁止する。
【０１６１】
このように、変形例２によれば、照合結果は、制御装置１が保持している管理情報３０内の固有情報２０と照合することで得られるものではなく、他の装置（たとえば上位機器３）が保持している管理情報３０内の固有情報２０と照合することにより得られる。
【０１６２】
制御装置１を不正に模倣することにより別の制御装置を設置する場合に、当該別の制御装置内のデータを改竄するよりも、上位機器３内のデータを改竄することの方が困難である。そのため、変形例２によれば、上位機器３の管理情報３０についても改竄しなければ制御プログラムの実行が許可されないため、セキュリティレベルを上げることができる。

【０１６３】
（ｈ３．その他の変形例）
上記実施の形態において、制御プログラムを実行するプロセッサ１０２と、セキュリティプログラムを実行するプロセッサ２０２とは、互いに異なるデバイスが備えているものとした。なお、一のデバイスが、セキュリティプログラムを実行するプロセッサ２０２と、制御プログラムを実行するプロセッサ１０２とを備えていてもよい。
【０１６４】
§３．付記
以上のように、上記の実施の形態および変形例による開示は以下のような開示を含む。
【０１６５】
＜構成１＞
１以上のデバイスを含む制御装置（１）であって、
制御プログラム（１４０）を実行する制御エンジン（１４２）と、
前記制御エンジンでの前記制御プログラムの実行可否を管理するセキュリティエンジン（２３０）とを備え、
前記セキュリティエンジンは、
前記１以上のデバイスの各々から取得された識別情報を用いて固有情報を生成する生成手段（２３４）と、
予め生成された第１の固有情報を保持する保持手段（２３６）と、
照合の要求に従って前記生成手段により生成される第２の固有情報と、前記第１の固有情報とを照合する照合手段（２３８）と、
前記制御プログラムの実行開始要求に応答して、前記照合の要求を行い、前記照合手段から得られる照合結果に基づいて、前記制御プログラムの実行可否を判定する許可手段（２３２）とを含み、
前記生成手段は、前記１以上のデバイスの各々について、当該デバイスの種別を識別する第１の識別情報（４２）および当該デバイスを個別に識別する第２の識別情報（４２）からセキュリティポリシーに応じて前記識別情報を選択する、制御装置。
【０１６６】
＜構成２＞
前記セキュリティポリシーは、第１のポリシー、第２のポリシーおよび第３のポリシーの中から予め設定され、
前記第１のポリシーは、前記１以上のデバイスの各々について前記第１の識別情報を選択するポリシーであり、
前記第２のポリシーは、前記１以上のデバイスのうち第１のグループに属する第１のデバイスについて前記第１の識別情報を選択し、前記１以上のデバイスのうち、前記第１のグループよりもセキュリティ対策の優先度の高い第２のグループに属する第２のデバイスについて前記第２の識別情報を選択するポリシーであり、
前記第３のポリシーは、前記１以上のデバイスの各々について前記第２の識別情報を選択するポリシーである、構成１に記載の制御装置。
【０１６７】
＜構成３＞
前記１以上のデバイスの各々は、前記第２の識別情報を保持し、
前記第２の識別情報は、前記第１の識別情報と、前記第１の識別情報によって識別される種別のデバイスの個体に対してユニークに割り当てられる第３の識別情報（４４）との組み合わせであり、
前記生成手段は、前記第２の識別情報から前記第１の識別情報を取得する、請求項１または２に記載の制御装置。
【０１６８】
＜構成４＞
前記１以上のデバイスは、前記制御エンジンを有する制御デバイス（１００）と、前記

セキュリティエンジンを有するセキュリティデバイス（２００）とを含む、構成１から３のいずれかに記載の制御装置。

【０１６９】

＜構成５＞

前記保持手段は、外部装置（３）との間で、分散型台帳の形式で前記第１の固有情報を保持する、構成１から４のいずれかに記載の制御装置。

【０１７０】

＜構成６＞

前記照合手段は、前記第２の固有情報と前記外部装置が保持する前記第１の固有情報とをさらに照合する、構成５に記載の制御装置。

【０１７１】

＜構成７＞

１以上のデバイスを含む制御装置（１）において実行される管理方法であって、

予め生成された第１の固有情報を保持するステップ（Ｓ１）と、

制御プログラム（１４０）の実行開始要求に応答して、前記１以上のデバイスの各々から取得された識別情報を用いて第２の固有情報を生成するステップ（Ｓ５，ＳＱ１０８，ＳＱ１１０）と、

前記第１の固有情報と前記第２の固有情報とを照合するステップ（Ｓ６，ＳＱ１１２）と、

照合結果に基づいて、前記制御プログラムの実行可否を判定するステップ（Ｓ８，ＳＱ１１４）とを備え、

前記生成するステップは、前記１以上のデバイスの各々について、当該デバイスの種別を識別する第１の識別情報および当該デバイスを個別に識別する第２の識別情報からセキュリティポリシーに応じて前記識別情報を選択するステップ（ＳＱ１０８）を含む、管理方法。

【０１７２】

＜構成８＞

１以上のデバイスを含む制御装置（１）において実行される管理方法をコンピュータに実行させるセキュリティプログラム（２３０）であって、

前記管理方法は、

予め生成された第１の固有情報を保持するステップ（Ｓ１）と、

制御プログラム（１４０）の実行開始要求に応答して、前記１以上のデバイスの各々から取得された識別情報を用いて第２の固有情報を生成するステップ（Ｓ５，ＳＱ１０８，ＳＱ１１０）と、

前記第１の固有情報と前記第２の固有情報とを照合するステップ（Ｓ６，ＳＱ１１２）と、

照合結果に基づいて、前記制御プログラムの実行可否を判定するステップ（Ｓ８，ＳＱ１１４）とを備え、

前記生成するステップは、前記１以上のデバイスの各々について、当該デバイスの種別を識別する第１の識別情報および当該デバイスを個別に識別する第２の識別情報からセキュリティポリシーに応じて前記識別情報を選択するステップ（ＳＱ１０８）を含む、セキュリティプログラム。

【０１７３】

今回開示された実施の形態はすべ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。本発明の範囲は、上記した説明ではなく、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および範囲内でのすべ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発明は、可能な限り、単独でも、組み合わせても、実施することが意図される。

【符号の説明】

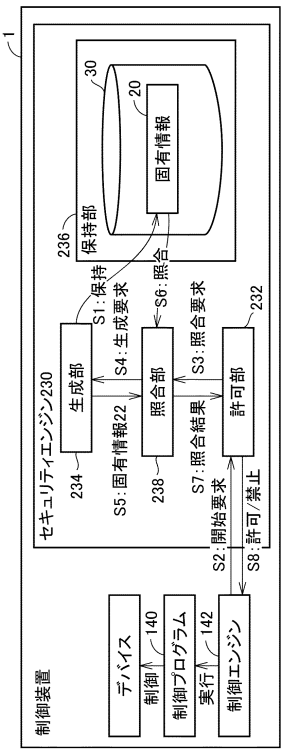
【０１７４】

１　制御装置、２　情報系ネットワーク、３　上位機器、４　フィールドネットワーク、１０　制御システム、２０　固有情報（第１の固有情報）、２２　固有情報（第２の固有情報、３０　管理情報、４０　識別情報（第２の識別情報）、４２　識別情報（第１の識別情報）、４４　シリアル番号（第３の識別情報）、５０　ブロック、５２　ブロックハッシュ値、５４　システム構成情報、５６　ナンス、１００　制御ユニット、１０２，２０２　プロセッサ、１０４，２０４　チップセット、１０６，２０６　主記憶装置、１０８，２０８　二次記憶装置、１１０，２１０　通信コントローラ、１１２，２１２　ＵＳＢコントローラ、１１４，２１４　メモリカードインターフェイス、１１５，２１５　メモリカード、１１６　フィールドネットワークコントローラ、１１８　内部バスコントローラ、１２０，２２０　情報系ネットワークコントローラ、１３０　認証プログラム、１３２　認証部、１３４　判定要求部、１３６　識別情報送信部、１３８　識別情報収集部、１４０　制御プログラム、１４２　制御エンジン、１４４　制御プログラム実行部、２００　セキュリティユニット、２３０　セキュリティエンジン、２３２　許可部、２３４　生成部、２３６　保持部、２３６Ａ　配布部、２３６Ｂ，２３６Ｄ　マイニング部、２３６Ｃ，２３６Ｅ　ブロックハッシュ値演算部、２３８　照合部、２４０　セキュリティプログラム、３００　Ｉ／Ｏユニット、４００　通信カプラ、１０８２，２０８２　システムプログラム、２３２２　判定部、２３２４　照合要求部、２３４２　収集要求部、２３４４　システムハッシュ値演算部、２３６２　登録部。

【図面】

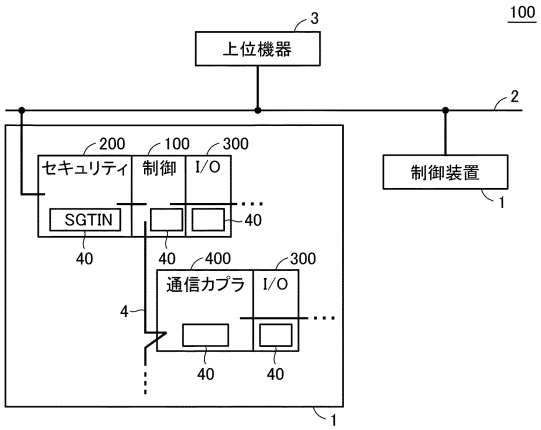
【図１】

図1



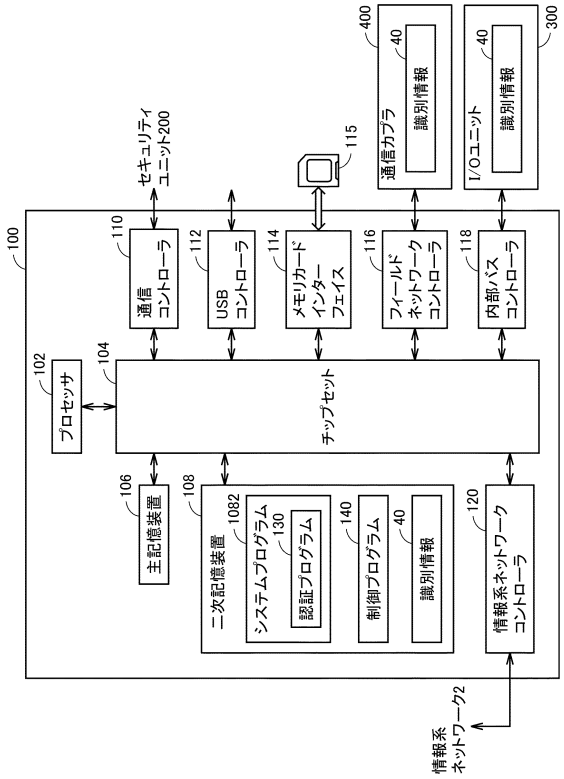
【図２】

図2



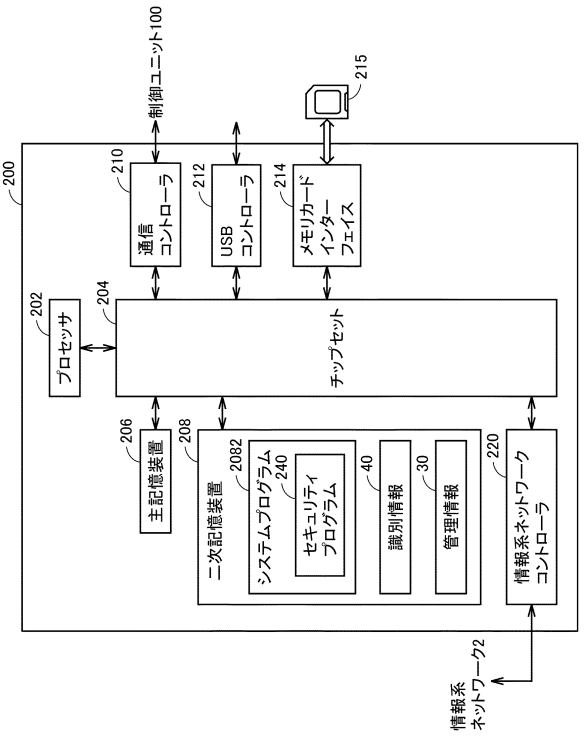
【図３】

図3



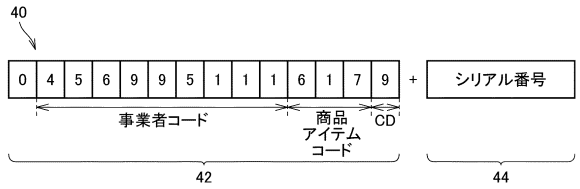
【図４】

図4



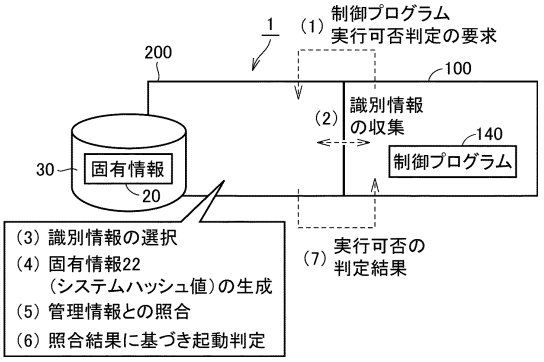
【図５】

図5



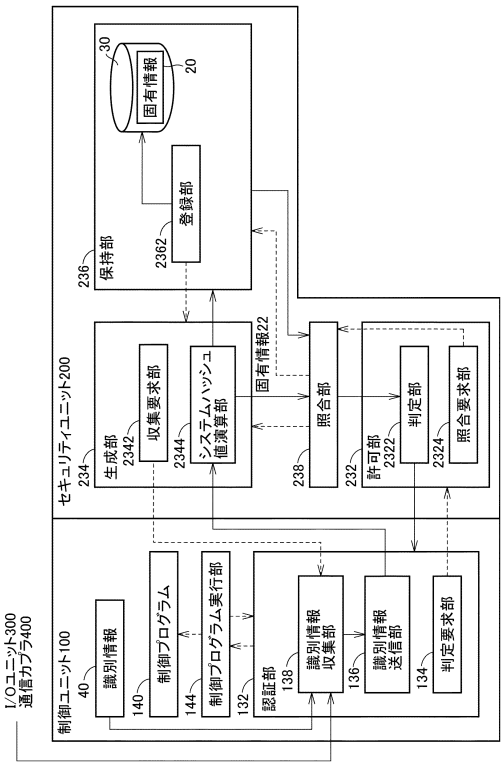
【図６】

図6



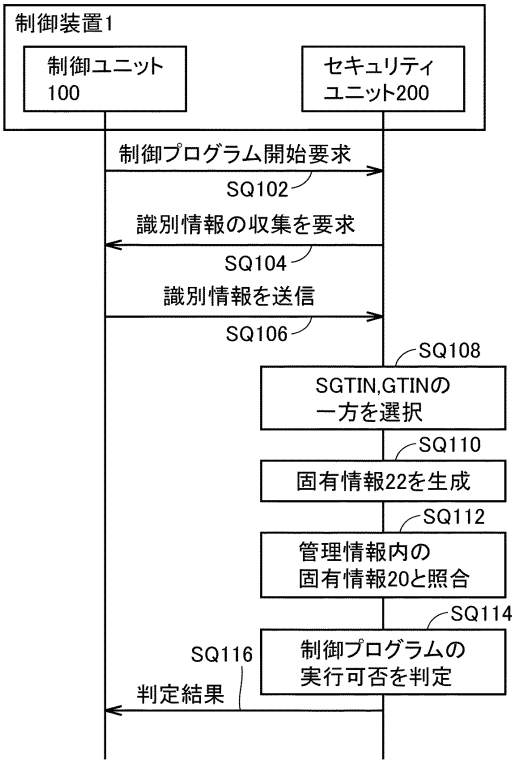
【図７】

図7



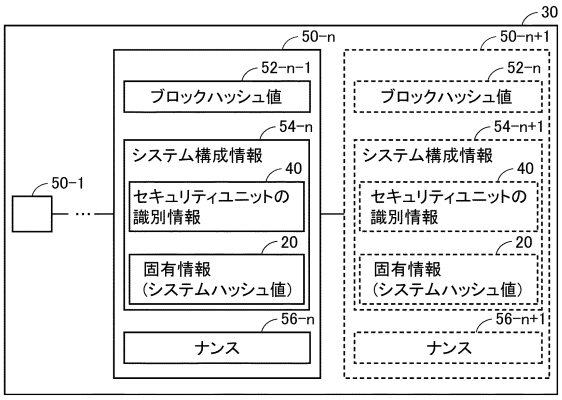
【図８】

図8



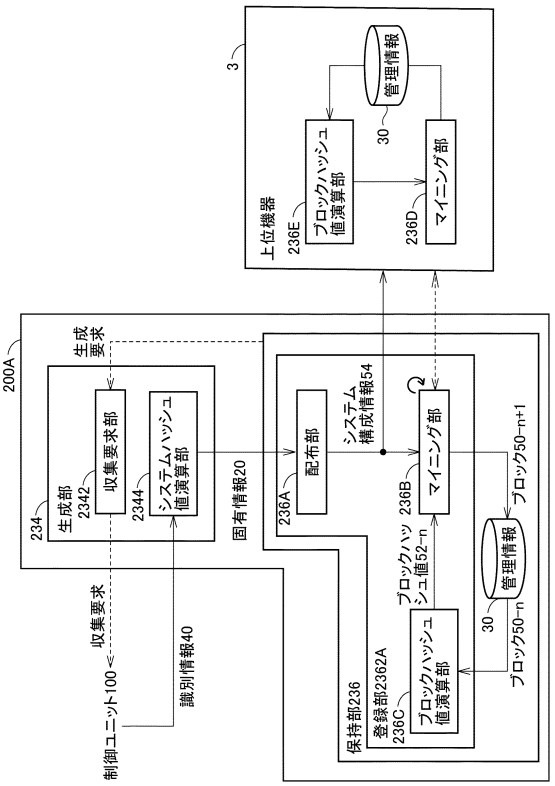
【図９】

図9



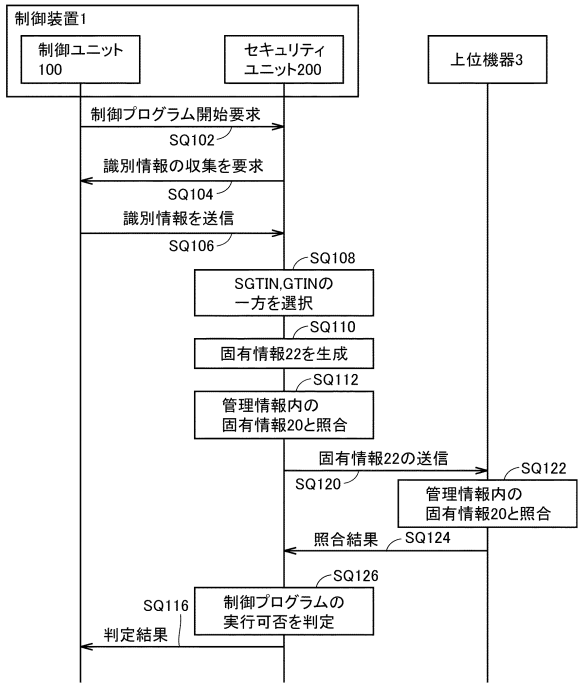
【図１０】

図10



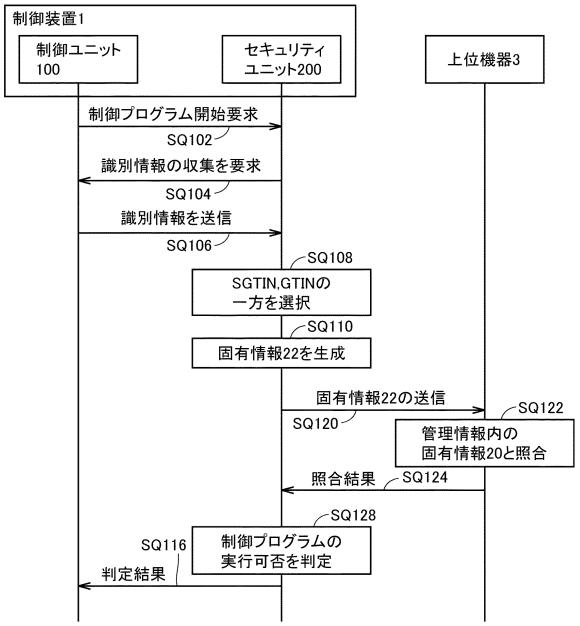
【図１１】

図11



【図１２】

図12



フロントページの続き

(56)参考文献　　国際公開第２０２０／２６１６５４（WO，Ａ１）
国際公開第２０１５／１８１９２５（WO，Ａ１）

(58)調査した分野　(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／４４