(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2020-95672
(P2020-95672A)
(43)公開日　令和2年6月18日(2020.6.18)

| (51)Int.Cl. | | F I | | テーマコード（参考） |
|---|---|---|---|---|
| G05B 19/042 | (2006.01) | G05B | 19/042 | 5H220 |
| G06F 21/55 | (2013.01) | G06F | 21/55 | |

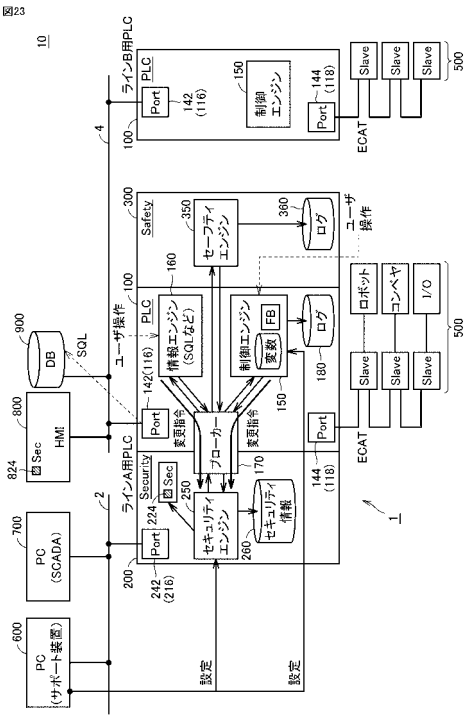
審査請求 未請求　請求項の数 15　ＯＬ　（全 40 頁）

(21)出願番号　特願2019-114336 (P2019-114336)
(22)出願日　令和1年6月20日 (2019.6.20)
(31)優先権主張番号　特願2018-222649 (P2018-222649)
(32)優先日　平成30年11月28日 (2018.11.28)
(33)優先権主張国・地域又は機関
日本国 (JP)

(71)出願人　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
特許業務法人深見特許事務所
(72)発明者　岡　実
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　山本　真之
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　小島　訓
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】コントローラシステム

(57)【要約】
【課題】制御装置および制御システムのネットワーク化あるいはインテリジェント化に伴って生じ得る脅威に対する保護という新たな課題を解決する。
【解決手段】コントローラシステムは、制御対象を制御するための制御演算を実行する制御ユニットと、制御ユニットに接続され、コントローラシステムに対するセキュリティ機能を担当するセキュリティユニットとを含む。セキュリティユニットは、コントローラシステムにおいて何らかの不正侵入が発生したか否かを検知する検知手段を含む。制御ユニットは、セキュリティユニットの検知手段の挙動を変更するための指令を送信する指令送信手段を含む。
【選択図】図２３



【特許請求の範囲】
【請求項１】
コントローラシステムであって、
制御対象を制御するための制御演算を実行する制御ユニットと、
前記制御ユニットに接続され、前記コントローラシステムに対するセキュリティ機能を担当するセキュリティユニットとを備え、
前記セキュリティユニットは、前記コントローラシステムにおいて何らかの不正侵入が発生したか否かを検知する検知手段を含み、
前記制御ユニットは、前記セキュリティユニットの前記検知手段の挙動を変更するための指令を送信する指令送信手段を含む、コントローラシステム。
【請求項２】
前記検知手段の挙動を変更するための指令は、前記検知手段による不正侵入の検知を復旧するための指令を含む、請求項１に記載のコントローラシステム。
【請求項３】
前記検知手段の挙動を変更するための指令は、前記検知手段による不正侵入が発生したか否かを検知するレベルを変更するための指令を含む、請求項１または２に記載のコントローラシステム。
【請求項４】
前記指令送信手段は、ユーザ操作に応じて、前記検知手段の挙動を変更するための指令を送信する、請求項１～３のいずれか１項に記載のコントローラシステム。
【請求項５】
前記制御ユニットは、前記制御演算に係る命令を含むユーザプログラムを実行するように構成され、
前記ユーザプログラムは、前記検知手段の挙動を変更するための指令を送信するための命令を含む、請求項１～４のいずれか１項に記載のコントローラシステム。
【請求項６】
コントローラシステムであって、
制御対象を制御するための制御演算を実行する制御ユニットと、
前記制御ユニットに接続され、前記コントローラシステムに対するセキュリティ機能を担当するセキュリティユニットと、
少なくとも前記制御ユニットにアクセス可能なサポート装置とを備え、
前記セキュリティユニットは、前記コントローラシステムにおいて何らかの不正侵入が発生したか否かを検知する検知手段を含み、
前記制御ユニットは、前記検知手段により検知された不正侵入に応じた制御演算を実行するように構成されており、
前記サポート装置は、前記検知手段により検知された不正侵入に応じて前記制御ユニットにより実行される制御演算に係る設定を受け付ける、コントローラシステム。
【請求項７】
前記サポート装置は、前記検知手段により不正侵入が検知されたときに前記制御ユニットにより実行されるプログラムの指定を受け付ける、請求項６に記載のコントローラシステム。
【請求項８】
前記サポート装置は、前記制御ユニットによりプログラムが実行される条件として、不正侵入の種類の指定を受け付ける、請求項７に記載のコントローラシステム。
【請求項９】
前記サポート装置は、制御動作の典型的な挙動を規定する複数のモデル設定を有しており、ユーザ操作に応じて、前記複数のモデル設定のうちいずれかを前記制御ユニットに反映する、請求項６～８のいずれか１項に記載のコントローラシステム。
【請求項１０】
前記複数のモデル設定の各々は、設備種別に関連付けられており、

前記サポート装置は、ユーザによる設備の選択に応じて、対応するモデル設定を選択および反映する、請求項９に記載のコントローラシステム。
【請求項１１】
前記サポート装置は、対話型インターフェイスを介して、１または複数の質問をユーザに呈示するとともに、各質問に対するユーザの選択に応じて、前記複数のモデル設定のうち対象となるモデル設定を選択および反映する、請求項９に記載のコントローラシステム。
【請求項１２】
コントローラシステムであって、
制御対象を制御するための制御演算を実行する制御ユニットと、
前記制御ユニットに接続され、前記コントローラシステムに対するセキュリティ機能を担当するセキュリティユニットとを備え、
前記セキュリティユニットは、
前記コントローラシステムにおいて何らかの不正侵入が発生したか否かを検知する検知手段と、
前記検知手段による検知動作から算出されるセキュリティリスクをユーザに提示する提示手段とを含む、コントローラシステム。
【請求項１３】
前記提示手段は、前記セキュリティリスクを視覚的に提示するためのインジケータを含む、請求項１２に記載のコントローラシステム。
【請求項１４】
前記提示手段は、前記セキュリティリスクを聴覚的に提示するための音声発生部を含む、請求項１２または１３に記載のコントローラシステム。
【請求項１５】
前記提示手段は、前記算出されるセキュリティリスクの度合いに応じて、提示態様を変化させる、請求項１２～１４のいずれか１項に記載のコントローラシステム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、制御対象を制御するコントローラシステムに対するセキュリティ機能に関する。
【背景技術】
【０００２】
各種設備および各設備に配置される各種装置の制御には、ＰＬＣ（プログラマブルロジックコントローラ）などの制御装置が用いられる。制御装置は、制御対象の設備や機械に生じる異常を監視するとともに、制御装置自体の異常を監視することも可能である。何らかの異常が検知されると、制御装置から外部に対して何らかの方法で通知がなされる。
【０００３】
例えば、特開２０００－１３７５０６号公報（特許文献１）は、異常履歴が登録されたとき、または、予め定められた時間が到来したときに、予め指定された宛先に電子メールを送信するプログラマブルコントローラを開示する。
【先行技術文献】
【特許文献】
【０００４】
【特許文献１】特開２０００－１３７５０６号公報
【発明の概要】
【発明が解決しようとする課題】
【０００５】
近年のＩＣＴ（Information and Communication Technology）の進歩に伴って、制御装置も様々な外部装置とネットワーク接続されるとともに、制御装置において実行される処

理も高度化している。このようなネットワーク化あるいはインテリジェント化に伴って、想定される脅威の種類も増加している。

【０００６】

従来の制御装置においては、設備や機械に生じた異常、または、制御装置自体に生じた異常を検知するのみであり、ネットワーク化あるいはインテリジェント化に伴って生じ得る脅威については、何ら想定されていない。

【０００７】

本発明は、制御装置および制御システムのネットワーク化あるいはインテリジェント化に伴って生じ得る脅威に対する保護という新たな課題を解決することを一つの目的としている。

【課題を解決するための手段】

【０００８】

本発明のある局面に従うコントローラシステムは、制御対象を制御するための制御演算を実行する制御ユニットと、制御ユニットに接続され、コントローラシステムに対するセキュリティ機能を担当するセキュリティユニットとを含む。セキュリティユニットは、コントローラシステムにおいて何らかの不正侵入が発生したか否かを検知する検知手段を含む。制御ユニットは、セキュリティユニットの検知手段の挙動を変更するための指令を送信する指令送信手段を含む。

【０００９】

この局面によれば、何らかの不正侵入が検知された後に、その不正侵入に関する要因が取り除かれた後、制御対象を正常運転に復帰する際に、セキュリティユニットの挙動を柔軟に制御できる。

【００１０】

検知手段の挙動を変更するための指令は、検知手段による不正侵入の検知を復旧するための指令を含んでいてもよい。この局面によれば、不正侵入の検知後の復旧を容易化できる。

【００１１】

検知手段の挙動を変更するための指令は、検知手段による不正侵入が発生したか否かを検知するレベルを変更するための指令を含んでいてもよい。この局面によれば、制御ユニット側から検知するレベルを変更できるので、状況に応じた柔軟な制御動作を実現できる。

【００１２】

指令送信手段は、ユーザ操作に応じて、検知手段の挙動を変更するための指令を送信するようにしてもよい。この局面によれば、ユーザの明示的な操作を受けて復旧などの処理が開始されるので、セキュリティリスクを低減できる。

【００１３】

制御ユニットは、制御演算に係る命令を含むユーザプログラムを実行するように構成されてもよく、ユーザプログラムは、検知手段の挙動を変更するための指令を送信するための命令を含んでいてもよい。この局面によれば、制御動作に加えて、検知手段の挙動を制御するための命令をユーザプログラムに含めることができるので、柔軟な制御動作を実現できる。

【００１４】

本発明の別の局面に従うコントローラシステムは、制御対象を制御するための制御演算を実行する制御ユニットと、制御ユニットに接続され、コントローラシステムに対するセキュリティ機能を担当するセキュリティユニットと、少なくとも制御ユニットにアクセス可能なサポート装置とを含む。セキュリティユニットは、コントローラシステムにおいて何らかの不正侵入が発生したか否かを検知する検知手段を含む。制御ユニットは、検知手段により検知された不正侵入に応じた制御演算を実行するように構成されている。サポート装置は、検知手段により検知された不正侵入に応じて制御ユニットにより実行される制御演算に係る設定を受け付ける。

【００１５】
この局面によれば、何らかの不正侵入が検知された後に、その不正侵入に対応する処理を実行するための設定を容易に行うことができる。
【００１６】
サポート装置は、検知手段により不正侵入が検知されたときに制御ユニットにより実行されるプログラムの指定を受け付けるようにしてもよい。この局面によれば、検知手段により不正侵入が検知されたときに、対処に必要なプログラムの指定を容易化できる。
【００１７】
サポート装置は、制御ユニットによりプログラムが実行される条件として、不正侵入の種類の指定を受け付けるようにしてもよい。この局面によれば、様々な不正侵入のうち、特定の種類の不正侵入が検知されたときには、特定のプログラムを実行させることができる。
【００１８】
サポート装置は、制御動作の典型的な挙動を規定する複数のモデル設定を有しており、ユーザ操作に応じて、複数のモデル設定のうちいずれかを制御ユニットに反映するようにしてもよい。この局面によれば、専門知識を有していないユーザであっても、必要な設定を行うことができる。
【００１９】
複数のモデル設定の各々は、設備種別に関連付けられていてもよく、サポート装置は、ユーザによる設備の選択に応じて、対応するモデル設定を選択および反映するようにしてもよい。この局面によれば、対象の設備を選択するだけで、必要な設定を反映できる。
【００２０】
サポート装置は、対話型インターフェイスを介して、１または複数の質問をユーザに呈示するとともに、各質問に対するユーザの選択に応じて、複数のモデル設定のうち対象となるモデル設定を選択および反映するようにしてもよい。この局面によれば、質問に対して回答するだけで、必要な設定を反映できる。
【００２１】
本発明のさらに別の局面に従うコントローラシステムは、制御対象を制御するための制御演算を実行する制御ユニットと、制御ユニットに接続され、コントローラシステムに対するセキュリティ機能を担当するセキュリティユニットと、少なくとも制御ユニットにアクセス可能なサポート装置とを含む。セキュリティユニットは、コントローラシステムにおいて何らかの不正侵入が発生したか否かを検知する検知手段と、検知手段による検知動作から算出されるセキュリティリスクをユーザに提示する提示手段とを含む。
【００２２】
この局面によれば、不正侵入自体は検知されていないが、そのリスクが高まっているか否かを一見して把握できる。
【００２３】
提示手段は、セキュリティリスクを視覚的に提示するためのインジケータを含んでいてもよい。この局面によれば、セキュリティリスクを一見して把握できる。
【００２４】
提示手段は、セキュリティリスクを聴覚的に提示するための音声発生部を含んでいてもよい。この局面によれば、セキュリティリスクを即座に把握できる。
【００２５】
提示手段は、算出されるセキュリティリスクの度合いに応じて、提示態様を変化させるようにしてもよい。この局面によれば、ユーザは、提示態様によって、セキュリティリスクの度合いを容易に把握できる。
【００２６】
本発明のさらに別の局面に従うコントローラシステムは、制御対象を制御するための制御演算を実行する制御ユニットと、制御ユニットに接続され、コントローラシステムに対するセキュリティ機能を担当するセキュリティユニットとを含む。セキュリティユニット

は、コントローラシステムにおいて何らかの不正侵入が発生したか否かを検知する検知手段と、検知手段により検知された不正侵入の属性を示すインシデント特性を制御ユニットへ通知する通知手段とを含む。制御ユニットは、通知手段から通知されたインシデント特性に応じて、制御動作を変更する。

【００２７】

この局面によれば、制御ユニットは、検知された不正侵入に応じた制御動作を実現できる。

【００２８】

制御ユニットは、制御動作を変更することにより、制御対象の動作を停止するようにしてもよい。この局面によれば、不正侵入が検知されることで、制御対象の動作を安全に停止できる。

【００２９】

制御ユニットは、制御動作を変更することにより、制御対象の動作を制限するようにしてもよい。この局面によれば、不正侵入が検知されることで、制御対象の動作を制限し、万が一、インシデントが発生しても、制御対象の破損などを防止できる。

【００３０】

制御ユニットは、制御動作を変更することにより、コントローラシステムに含まれる装置の動作を制限するようにしてもよい。この局面によれば、不正侵入が検知されることで、コントローラシステムに含まれる装置の動作を制限し、インシデントへの進展などを防止できる。

【００３１】

制御ユニットは、通知されるインシデント特性に対応付けられたプログラムを実行することで、制御動作を変更するようにしてもよい。この局面によれば、インシデント特性毎に対応するプログラムを予め用意できるため、各種の不正侵入に応じた制御動作を実現できる。

【発明の効果】

【００３２】

本発明によれば、制御装置および制御システムのネットワーク化あるいはインテリジェント化に伴って生じ得る脅威に対する保護という新たな課題を解決できる。

【図面の簡単な説明】

【００３３】

【図１】本実施の形態に係るコントローラシステムの構成例を示す外観図である。

【図２】本実施の形態に従うコントローラシステムを構成する制御ユニットのハードウェア構成例を示す模式図である。

【図３】本実施の形態に従うコントローラシステムを構成するセキュリティユニット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コントローラシステムを構成するセーフティユニットのハードウェア構成例を示す模式図である。

【図５】本実施の形態に従うコントローラシステムを含む制御システムの典型例を示す模式図である。

【図６】セキュリティ脅威に対する対策サイクルの一例を示す模式図である。

【図７】本実施の形態に従うコントローラシステムを含む制御システムにおける不正侵入検知時の対応の一例を示す模式図である。

【図８】生産機械および検査装置を含むラインに対する攻撃例を示す模式図である。

【図９】本実施の形態に従うコントローラシステムにおけるインシデント特性に応じた設備別の制御動作の一例を示す図である。

【図１０】本実施の形態に従うコントローラシステムにおけるインシデント特性に応じた設備別の制御動作の別の一例を示す図である。

【図１１】本実施の形態に従うコントローラシステムにおけるインシデント特性に応じた各設備における状態別の制御動作の一例を示す図である。

【図１２】本実施の形態に従うコントローラシステムにおけるセキュリティ脅威が検知された場合の処理手順を示すフローチャートである。
【図１３】本実施の形態に従うコントローラシステムに接続されるサポート装置のハードウェア構成例を示す模式図である。
【図１４】本実施の形態に従うコントローラシステムに対する不正侵入検知時の対処を設定するためのユーザインターフェイス画面の一例を示す模式図である。
【図１５】本実施の形態に従うコントローラシステムに対する不正侵入検知時の対処を設定するためのユーザインターフェイス画面の一例を示す模式図である。
【図１６】本実施の形態に従うコントローラシステムに対する不正侵入検知時の対処を設定するためのユーザインターフェイス画面の一例を示す模式図である。
【図１７】本実施の形態に従うコントローラシステムに対する不正侵入検知時の対処を設定するためのユーザインターフェイス画面の一例を示す模式図である。
【図１８】本実施の形態に従うコントローラシステムが提供するインシデント特性に応じた制御動作のモデル設定の一例を示す図である。
【図１９】本実施の形態に従うコントローラシステムにおける制御動作を設定する処理手順を説明するための図である。
【図２０】本実施の形態に従うコントローラシステムにおける制御動作を設定する別の処理手順を説明するための図である。
【図２１】本実施の形態に従うコントローラシステムにおける制御動作を設定するさらに別の処理手順を説明するための図である。
【図２２】本実施の形態に従うコントローラシステムにおける制御動作の設定を変更するためのユーザインターフェイス画面の一例を示す模式図である。
【図２３】本実施の形態に従うコントローラシステムにおけるセキュリティユニットに対する変更指令の遣り取りを説明するための模式図である。
【図２４】本実施の形態に従うコントローラシステムにおけるセキュリティユニットの動作を変更するためのプログラム命令の一例を示す図である。
【図２５】本実施の形態に従うコントローラシステムに採用されるインジケータの一例を示す模式図である。
【図２６】本実施の形態に従うコントローラシステムに採用されるスピーカの動作例を示す模式図である。
【図２７】本実施の形態に従うコントローラシステムの構成の変形例を示す模式図である。

【発明を実施するための形態】

【００３４】

本発明の実施の形態について、図面を参照しながら詳細に説明する。なお、図中の同一または相当部分については、同一符号を付してその説明は繰り返さない。

【００３５】

＜Ａ．コントローラシステム１＞

まず、本実施の形態に従うコントローラシステム１の構成について説明する。

【００３６】

図１は、本実施の形態に係るコントローラシステム１の構成例を示す外観図である。図１を参照して、コントローラシステム１は、制御ユニット１００と、セキュリティユニット２００と、セーフティユニット３００と、１または複数の機能ユニット４００と、電源ユニット４５０とを含む。

【００３７】

制御ユニット１００とセキュリティユニット２００との間は、任意のデータ伝送路（例えば、ＰＣＩ　Ｅｘｐｒｅｓｓあるいはイーサネット（登録商標）など）を介して接続されている。制御ユニット１００とセーフティユニット３００および１または複数の機能ユニット４００との間は、図示しない内部バスを介して接続されている。

【００３８】

制御ユニット１００は、コントローラシステム１において中心的な処理を実行する。制御ユニット１００は、任意に設計された要求仕様に従って、制御対象を制御するための制御演算を実行する。後述のセーフティユニット３００で実行される制御演算との対比で、制御ユニット１００で実行される制御演算を「標準制御」とも称す。図１に示す構成例において、制御ユニット１００は、１または複数の通信ポートを有している。

【００３９】

セキュリティユニット２００は、制御ユニット１００に接続され、コントローラシステム１に対するセキュリティ機能を担当する。図１に示す構成例において、セキュリティユニット２００は、１または複数の通信ポートを有している。セキュリティユニット２００が提供するセキュリティ機能の詳細については、後述する。

【００４０】

セーフティユニット３００は、制御ユニット１００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。セーフティユニット３００で実行される制御演算を「セーフティ制御」とも称す。通常、「セーフティ制御」は、ＩＥＣ　６１５０８などに規定されたセーフティ機能を実現するための要件を満たすように設計される。「セーフティ制御」は、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処理を総称する。

【００４１】

機能ユニット４００は、コントローラシステム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４００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などを包含し得る。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などが挙げられる。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。

【００４２】

電源ユニット４５０は、コントローラシステム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。

【００４３】

＜Ｂ．各ユニットのハードウェア構成例＞

次に、本実施の形態に従うコントローラシステム１を構成する各ユニットのハードウェア構成例について説明する。

【００４４】

（ｂ１：制御ユニット１００）

図２は、本実施の形態に従うコントローラシステム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２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（Universal Serial Bus）コントローラ１１２と、メモリカードインターフェイス１１４と、ネットワークコントローラ１１６，１１８，１２０と、内部バスコントローラ１２２と、インジケータ１２４と、スピーカ１２６とを含む。

【００４５】

プロセッサ１０２は、二次記憶装置１０８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、標準制御に係る制御演算、および、後述するような各種処理を実現する。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。

【００４６】

二次記憶装置１０８には、システムプログラムに加えて、システムプログラムが提供する実行環境上で動作する制御プログラムが格納される。

【００４７】

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などに対応する通信チップを採用できる。

【００４８】

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。

【００４９】

メモリカードインターフェイス１１４は、メモリカード１１５を着脱可能に構成されており、メモリカード１１５に対して制御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１１５から制御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。

【００５０】

ネットワークコントローラ１１６，１１８，１２０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１１６，１１８，１２０は、ＥｔｈｅｒＣＡＴ（登録商標）、ＥｔｈｅｒＮｅｔ／ＩＰ（登録商標）、ＤｅｖｉｃｅＮｅｔ（登録商標）、ＣｏｍｐｏＮｅｔ（登録商標）などの産業用ネットワークプロトコルを採用してもよい。

【００５１】

内部バスコントローラ１２２は、コントローラシステム１を構成するセーフティユニット３００や１または複数の機能ユニット４００との間のデータの遣り取りを担当する。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。

【００５２】

インジケータ１２４は、制御ユニット１００の動作状態など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などで構成される。

【００５３】

スピーカ１２６は、制御ユニット１００の動作状態などを通知するものであり、ユニット表面に配置されて音声を出力する。

【００５４】

図２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（Application Specific Integrated Circuit）またはＦＰＧＡ（Field-Programmable Gate Array）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（Operating System）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。

【００５５】

（ｂ２：セキュリティユニット２００）

図３は、本実施の形態に従うコントローラシステム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３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、ネットワークコントローラ２１６，２１８と、インジケータ２２４とを含む。

【００５６】

プロセッサ２０２は、二次記憶装置２０８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、後述するような各種セキュリティ機能を実現する。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。

【００５７】

二次記憶装置２０８には、システムプログラムに加えて、システムプログラムが提供する実行環境上で動作するセキュリティシステムプログラムが格納される。

【００５８】

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などに対応する通信チップを採用できる。

【００５９】

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。

【００６０】

メモリカードインターフェイス２１４は、メモリカード２１５を着脱可能に構成されており、メモリカード２１５に対して制御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から制御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。

【００６１】

ネットワークコントローラ２１６，２１８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２１６，２１８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。

【００６２】

インジケータ２２４は、セキュリティユニット２００の動作状態など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などで構成される。

【００６３】

スピーカ２２６は、セキュリティユニット２００の動作状態などを通知するものであり、ユニット表面に配置されて音声を出力する。

【００６４】

図３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。

【００６５】

（ｂ３：セーフティユニット３００）

図４は、本実施の形態に従うコントローラシステム１を構成するセーフティユニット３００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、セーフティユニット３００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３０２と、チップセット３０４と、主記憶装置３０６と、二次記憶装置３０８と、メモリカードインターフェイス３１４と、内部バスコントローラ３２２と、インジケータ３２４とを含む。

【００６６】

プロセッサ３０２は、二次記憶装置３０８に格納された各種プログラムを読み出して、主記憶装置３０６に展開して実行することで、セーフティ制御に係る制御演算、および、後述するような各種処理を実現する。チップセット３０４は、プロセッサ３０２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、セーフティユニット３００全体としての処理を実現する。

【００６７】
二次記憶装置３０８には、システムプログラムに加えて、システムプログラムが提供する実行環境上で動作するセーフティプログラムが格納される。
【００６８】
メモリカードインターフェイス３１４は、メモリカード３１５を着脱可能に構成されており、メモリカード３１５に対してセーフティ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３１５からセーフティ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。
【００６９】
内部バスコントローラ３２２は、内部バスを介した制御ユニット１００との間のデータの遣り取りを担当する。
【００７０】
インジケータ３２４は、セーフティユニット３００の動作状態など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などで構成される。
【００７１】
図４には、プロセッサ３０２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、セーフティユニット３００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。
【００７２】
＜Ｃ．制御システム１０＞
次に、本実施の形態に従うコントローラシステム１を含む制御システム１０の典型例について説明する。図５は、本実施の形態に従うコントローラシステム１を含む制御システム１０の典型例を示す模式図である。
【００７３】
一例として、図５に示す制御システム１０は、２つのライン（ラインＡおよびラインＢ）を制御対象とする。典型的には、各ラインは、ワークを搬送するコンベアに加えて、コンベア上のワークに対して任意の物理的作用を与えることが可能なロボットが配置されているとする。
【００７４】
ラインＡおよびラインＢのそれぞれに制御ユニット１００が配置されている。ラインＡを担当する制御ユニット１００に加えて、セキュリティユニット２００およびセーフティユニット３００がコントローラシステム１を構成する。なお、説明の便宜上、図５には、機能ユニット４００および電源ユニット４５０の記載を省略している。
【００７５】
コントローラシステム１のセキュリティユニット２００は、通信ポート２４２（図３のネットワークコントローラ２１６）を介して第１ネットワーク２に接続されている。第１ネットワーク２には、サポート装置６００およびＳＣＡＤＡ（Supervisory Control And Data Acquisition）装置７００が接続されているとする。
【００７６】
サポート装置６００は、少なくとも制御ユニット１００にアクセス可能になっており、コントローラシステム１に含まれる各ユニットで実行されるプログラムの作成、デバッグ、各種パラメータの設定などの機能をユーザへ提供する。
【００７７】
ＳＣＡＤＡ装置７００は、コントローラシステム１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、コントローラシステム１に対して内部コマンドなどを生成する。ＳＣＡＤＡ装置７００は、コントローラ

システム１が扱うデータを収集する機能も有している。
【００７８】
コントローラシステム１の制御ユニット１００は、通信ポート１４２（図２のネットワークコントローラ１１６）を介して第２ネットワーク４に接続されている。第２ネットワーク４には、ＨＭＩ（Human Machine Interface）８００およびデータベース９００が接続されているとする。
【００７９】
ＨＭＩ８００は、コントローラシステム１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、コントローラシステム１に対して内部コマンドなどを生成する。データベース９００は、コントローラシステム１から送信される各種データ（例えば、各ワークから計測されたトレーサビリティに関する情報など）を収集する。
【００８０】
コントローラシステム１の制御ユニット１００は、通信ポート１４４（図２のネットワークコントローラ１１８）を介して、１または複数のフィールドデバイス５００と接続されている。フィールドデバイス５００は、制御対象から制御演算に必要な各種情報を収集するセンサや検出器、および、制御対象に対して何らかの作用を与えるアクチュエータなどを含む。図５に示す例では、フィールドデバイス５００は、ワークに対して何らかの外的な作用を与えるロボット、ワークを搬送するコンベヤ、フィールドに配置されたセンサやアクチュエータとの間で信号を遣り取りするＩ／Ｏユニットなどを含む。
【００８１】
同様に、ラインＢを担当する制御ユニット１００についても同様に、通信ポート１４４（図２のネットワークコントローラ１１８）を介して、１または複数のフィールドデバイス５００と接続されている。
【００８２】
ここで、コントローラシステム１の機能面に着目すると、制御ユニット１００は、標準制御に係る制御演算を実行する処理実行部である制御エンジン１５０と、外部装置との間でデータを遣り取りする情報エンジン１６０とを含む。セキュリティユニット２００は、後述するようなセキュリティ機能を実現するためのセキュリティエンジン２５０を含む。セーフティユニット３００は、セーフティ制御に係る制御演算を実行する処理実行部であるセーフティエンジン３５０を含む。
【００８３】
各エンジンは、各ユニットのプロセッサなどの任意のハードウェア要素または各種プログラムなどの任意のソフトウェア要素、あるいは、それら要素の組合せによって実現される。各エンジンは任意の形態で実装できる。
【００８４】
さらに、コントローラシステム１は、エンジン同士の遣り取りを仲介するブローカー１７０を含む。ブローカー１７０の実体は、制御ユニット１００およびセキュリティユニット２００の一方または両方に配置してもよい。
【００８５】
制御エンジン１５０は、制御対象を制御するための制御演算の実行に必要な変数テーブルおよびファンクションブロック（ＦＢ）などを保持している。変数テーブルに格納される各変数は、Ｉ／Ｏリフレッシュ処理により、フィールドデバイス５００から取得された値で周期的に収集されるとともに、フィールドデバイス５００へ各値が周期的に反映される。制御エンジン１５０での制御演算のログはログデータベース１８０に格納されてもよい。
【００８６】
情報エンジン１６０は、制御ユニット１００が保持するデータ（変数テーブルで保持される変数値）に対して任意の情報処理を実行する。典型的には、情報エンジン１６０は、制御ユニット１００が保持するデータを周期的にデータベース９００などへ送信する処理

を含む。このようなデータの送信には、ＳＱＬなどが用いられる。

【００８７】

セキュリティエンジン２５０は、コントローラシステム１に発生する不正侵入の検知、検知された不正侵入に応じた処理、インシデントの発生有無判断、発生したインシデントに応じた処理などを実行する。セキュリティエンジン２５０の挙動は、セキュリティ情報２６０として保存される。

【００８８】

セキュリティエンジン２５０は、セキュリティに関する何らかのイベントが発生したこと、あるいは発生しているセキュリティに関するイベントのレベルなどを、インジケータ２２４で通知する。

【００８９】

セーフティエンジン３５０は、コントローラシステム１において何らかの不正侵入が発生したか否かを検知する検知手段に相当する。セーフティエンジン３５０は、制御ユニット１００を介して、セーフティ制御に係る制御演算の実行に必要なセーフティＩ／Ｏ変数を取得および反映する。セーフティエンジン３５０でのセーフティ制御のログはログデータベース３６０に格納されてもよい。

【００９０】

ブローカー１７０は、例えば、セキュリティエンジン２５０が何らかのイベントを検知すると、制御エンジン１５０、情報エンジン１６０およびセーフティエンジン３５０の動作などを変化させる。

【００９１】

＜Ｄ．セキュリティ脅威に対する対策サイクル＞

本実施の形態に従うコントローラシステム１は、設備や機械を正常運転することを妨げる任意のセキュリティ脅威を検知し、必要な対策を実行可能になっている。

【００９２】

本明細書において、「セキュリティ脅威」は、設備や機械を正常運転することを妨げる任意の事象を意味する。ここで、「正常運転」は、システム設計通りおよび生産計画通りに、設備や機械を運転継続できる状態を意味する。なお、システム設計通りおよび生産計画通りに、設備や機械を運転継続するための、設備や機械の立ち上げ、メンテナンス、段取り替えなども付属的な処理も「正常運転」の概念には含まれる。

【００９３】

ＰＬＣを中心とする制御装置においては、典型的には、（１）データベースなどの上位装置からの攻撃、（２）フィールドデバイスからの攻撃、（３）サポート装置を介した攻撃、（４）メモリカードなどの制御装置に装着される記憶媒体を介した攻撃、といった４つの局面からのセキュリティ脅威が考えられる。さらに、制御装置に搭載されているすべての物理ポートは攻撃を受けるセキュリティリスクが存在している。

【００９４】

本実施の形態に従うセキュリティユニット２００は、これらの各局面で生じるセキュリティ脅威あるいはリスクを検知し、必要な対策が実行できるようにするための処理を実行する。

【００９５】

通常、セキュリティ脅威は順次進化するため、セキュリティ脅威に対する対策は継続的に実行する必要がある。このようなセキュリティ脅威に対する継続的な対策について説明する。

【００９６】

図６は、セキュリティ脅威に対する対策サイクルの一例を示す模式図である。図６を参照して、セキュリティ脅威に対する対策サイクルは、主として、（１）開発時の対策（ステップＳ１，Ｓ２，Ｓ９）および（２）運用時の対策（ステップＳ３～Ｓ８）に大別される。（１）開発時の対策は、主として、制御対象の設備や機械の設計・仕様を決定する段階における対策を意味し、（２）運用時の対策は、主として、制御対象の設備や機械を運

転する段階における対策を意味する。
【００９７】
より具体的には、まず、制御対象の設備や機械に対する脅威分析が実行される（ステップＳ１）。ステップＳ１の脅威分析においては、セキュリティ要件定義が決定される。続いて、セキュリティ機能設計が実行される（ステップＳ２）。このセキュリティ機能設計においては、暗号方式、認証方式、アクセス制限などのセキュリティ機能が設計される。
【００９８】
これらのステップＳ１およびＳ２において設計された内容が制御対象の設備や機械に反映された上で、運用が開始される。この時点では、通常は正常運転となる（ステップＳ３）。上述したように、正常運転は、設備や機械の立ち上げ、本稼働、メンテナンス、段取り替えなどの処理を含む。
【００９９】
このような正常運転中において、何らかの不正侵入を検知したとする。すると、セキュリティ脅威１次対応が実行される（ステップＳ４）。
【０１００】
ここで、本明細書において、「不正侵入の検知」あるいは「不正侵入検知」は、何らかのセキュリティ脅威となり得る現象または異常を検知することを意味する。言い換えれば、不正侵入の検知は、通常とは異なる現象または状態の発生を検知することを意味するのみであり、通常インシデントが発生しておらず（但し、インシデントの発生のリスク存在している）、また、通常とは異なる現象または状態が不正なものであるか否かを確実に判断することまではできない。そのため、不正侵入が検知されただけでは、すべての処理やイベントをブロックすることは、生産活動を維持する観点からは好ましくない。
【０１０１】
そのため、図６に示されるセキュリティ脅威に対する対策サイクルにおいては、不正侵入が検知されると、１次的な措置として、セキュリティ脅威１次対応が実行される（ステップＳ４）。
【０１０２】
セキュリティ脅威１次対応は、インシデント発生のリスクがある状況における１次的な措置であり、インシデント発生への進展を防止できる場合もある。仮にインシデントが発生したとしても、セキュリティ脅威１次対応を実行することで、被害を最小限に抑えることができる。本実施の形態に従うコントローラシステム１においては、事前設定することで、セキュリティ脅威１次対応を自動的に実行するようになっている。
【０１０３】
典型的には、セキュリティ脅威１次対応は、継続、縮退、停止の３つに大別できる。
セキュリティ脅威１次対応の「継続」は、不正侵入が検知される直前と同様に稼働を続行することを意味する。但し、セキュリティ脅威をアラームなどで通知することにより、さらなる対応を迅速に取れる状態としておくのが好ましい。
【０１０４】
セキュリティ脅威１次対応の「縮退」は、コントローラシステムの部分停止（一部のみ稼働）、性能縮小（性能低下）、機能制限などの、限定的ながら稼働を続行することを意味する。すなわち、「縮退」においては、不正侵入が検知される直前の稼働に比較して、ハード面あるいはソフト面で何らかの制限を受けながらも稼働自体は継続する。
【０１０５】
セキュリティ脅威１次対応の「縮退」は、一般的な縮退運転（フォールバック）も含み得る。このような一般的な縮退運転は、システムの機能や性能を部分的に停止させた状態で稼働を維持することを意味する。縮退運転に切り替えた後には、利用できる機能が最低限に抑制され、あるいは、応答速度が低下するといた状態になることが多い。
【０１０６】
セキュリティ脅威１次対応の「停止」は、安全にシステムの動作を止めることを意味する。

【０１０７】
このようなセキュリティ脅威１次対応が実行された後に、復旧作業が実行される。図５に示すような制御システム１０においては、コントローラシステム１およびコントローラシステム１のフィールド側は、ＯＴ（Operation Technology）部門の作業者が担当し、コントローラシステム１の上位側（第１ネットワーク２および第２ネットワーク４ならびに各ネットワークに接続される装置）については、ＩＴ（Information Technology）部門の作業者が担当する。
【０１０８】
より具体的には、ＯＴ部門の作業者は、制御対象の設備や機械に対して必要な処理を行う（現場対応）（ステップＳ５）。具体的には、設備や機械の復旧作業や監視などの作業が実行される。一方、ＩＴ部門の作業者は、発生したセキュリティ脅威に対する脅威解析およびその対策などを行う（ステップＳ６）。ＩＴ部門の作業者による対策は、暫定的なものと、恒久的なものとを含み得る場合もある。
【０１０９】
ＯＴ部門およびＩＴ部門の作業者による対策が完了すると、試運転が実行される（ステップＳ７）。この試運転が問題なければ、運用が再開され、正常運転に復帰する（ステップＳ３）。
【０１１０】
一方、セキュリティ脅威１次対応を実行したものの（ステップＳ４）、インシデントが発生すると、インシデント対応が実行される（ステップＳ８）。インシデント対応は、インシデントが発生した後の対応であり、現場復旧や影響範囲を限定するために緊急的に行う措置を含む。本実施の形態に従うコントローラシステム１においては、事前設定することで、インシデント対応についても自動的に実行するようになっている。
【０１１１】
インシデント対応が実行された後に、ＯＴ部門の作業者は、制御対象の設備や機械に対して必要な処理を行う（現場対応）（ステップＳ５）とともに、ＩＴ部門の作業者は、発生したセキュリティ脅威に対する脅威解析およびその対策などを行う（ステップＳ６）。さらに、インシデントレポートが作成され（ステップＳ９）、その作成されたインシデントレポートの内容に基づいて、脅威分析（ステップＳ１）およびセキュリティ機能設計（ステップＳ２）などが再度実行される。
【０１１２】
このように、インシデントが発生した場合には、その発生したインシデントの内容が開発段階までフィードバックされることになる。
【０１１３】
なお、インシデントレポートは、インシデントが発生していなくても作成するようにしてもよい。
【０１１４】
後述するように、本実施の形態に従うコントローラシステム１は、図６に示すセキュリティ脅威に対する対策サイクルを確実に実行できるような仕組みを提供する。
【０１１５】
＜Ｅ．セキュリティ脅威１次対応＞
次に、図６に示されるセキュリティ脅威１次対応（ステップＳ４）について説明する。
【０１１６】
（ｅ１：制御システム１０でのセキュリティ脅威１次対応）
まず、制御システム１０に生じる不正侵入（セキュリティ脅威）の検知およびそれに応じたセキュリティ脅威１次対応の一例について説明する。
【０１１７】
図７は、本実施の形態に従うコントローラシステム１を含む制御システム１０における不正侵入検知時の対応の一例を示す模式図である。図７には、図５に示す制御システム１０において、ＳＣＡＤＡ装置７００がウィルスに感染して、第１ネットワーク２およびセ

キュリティユニット２００の通信ポート２４２から攻撃された例を示す。
【０１１８】
図７に示す例では、ラインＡを担当するコントローラシステム１に対してのみ攻撃されており、ラインＢを担当する制御ユニット１００に対する攻撃はないものとする。セキュリティユニット２００は、不正侵入を検知すると、その検知した不正侵入のインシデント特性を制御ユニット１００などへ通知する。
【０１１９】
本明細書において、「インシデント特性」は、検知された不正侵入（セキュリティ脅威）の属性（例えば、攻撃種類、攻撃特性、攻撃レベル、深刻度、緊急度など）を包含する用語である。セキュリティユニット２００のセキュリティエンジン２５０は、予め定められた検知ロジックに基づいて、検知した不正侵入（セキュリティ脅威）のインシデント特性を決定し、制御ユニット１００などへ出力する。すなわち、セキュリティユニット２００のセキュリティエンジン２５０は、検知機能により検知された不正侵入の属性を示すインシデント特性を制御ユニット１００へ通知する通知手段として機能する。
【０１２０】
制御ユニット１００は、セキュリティユニット２００からのインシデント特性に応じた、セキュリティ脅威１次対応および／またはインシデント対応を実行する。すなわち、制御ユニット１００は、セキュリティユニット２００のセキュリティエンジン２５０から通知されたインシデント特性に応じて、制御動作を変更する。
【０１２１】
図７には、セキュリティ脅威１次対応が実行される例を示す。具体的には、コンベア上を搬送されるワークをロボットで加工するようなラインＡを想定する。このようなラインＡにおいて、不正侵入が検知されることで、一例として、ワークを加工するロボットを安全に停止させるとともに、コンベア上の仕掛品のワークを倉庫へ退避する処理がセキュリティ脅威１次対応として実行される。
【０１２２】
このようなセキュリティ脅威１次対応を実現するにあたって、制御ユニット１００の制御エンジン１５０は、ラインＡについて、ロボットを安全に停止するとともに、コンベア上の仕掛品を倉庫に移動する処理を実行する（ステップＳ４１）。制御エンジン１５０が出力する命令に従って、フィールドデバイス５００のロボットは安全停止（停止）し（ステップＳ４２）、フィールドデバイス５００のコンベアは搬送のスピードを低速に切り替えるとともに、仕掛品を倉庫へ移動させるための特殊仕分け処理を実行（縮退）する（ステップＳ４３）。一方、フィールドデバイス５００のＩ／Ｏユニットは、運転（動作）を継続する（ステップＳ４４）。Ｉ／Ｏユニットが周期的に更新する入出力データは、制御エンジン１５０が適切に処理を実行するために必要になるからである。
【０１２３】
また、上述したように、図７に示すＳＣＡＤＡ装置７００からの攻撃では、ラインＢを担当する制御ユニット１００には影響はないので、ラインＢを担当する制御ユニット１００の制御エンジン１５０は運転を継続する（ステップＳ４５）。
【０１２４】
また、制御ユニット１００の通信ポート１４２については、生産継続のための最小限の通信のみを許可するようにしてもよい（ステップＳ４６）。すなわち、制御ユニット１００の通信物理ポートの通信を制御するようにしてもよい。なお、制御ユニット１００の通信物理ポートに限らず、何らかの不正侵入（セキュリティ脅威）が検知されると、セキュリティユニット２００および／またはセーフティユニット３００の任意の通信物理ポートの通信を制限するようにしてもよい。
【０１２５】
また、制御ユニット１００は、不正侵入（セキュリティ脅威）が検知を知らせるアラームをＨＭＩ８００のインジケータ８２４に表示する（ステップＳ４７）。
【０１２６】

さらに、制御ユニット１００は、セキュリティユニット２００からインシデントの発生を受けると、インシデントレポートをＨＭＩ８００に表示してもよい（ステップＳ４８）。

【０１２７】

図７に示すように、コントローラシステム１は、不正侵入（セキュリティ脅威）を検知すると、当該検知された不正侵入のインシデント特性に応じたセキュリティ脅威１次対応を実行できる。

【０１２８】

（ｅ２：その他の設備／機械でのセキュリティ脅威１次対応）

上述の図７においては、コンベア上のワークに対して任意の物理的作用を与えることが可能なロボットが配置されたラインを制御対象とする制御システム１０において、ＳＣＡＤＡ装置から攻撃を受けた場合のセキュリティ脅威１次対応について例示した。しかしながら、セキュリティ脅威１次対応は、少なくとも、制御対象に含まれる設備や機械、および、インシデント特性に応じて、対応内容を異ならせることが好ましい。

【０１２９】

（ｉ）加工機に対するデータ改ざんの攻撃

例えば、ＮＣ（Numerical Control）などによるワークの加工機に対して、加工データ（仕上がり形状などを規定したデータ）が改ざんされたような場合を想定する。この場合、加工機および加工機の周辺設備の制御に関しては、セキュリティ脅威１次対応として停止が採用され、人の安全が優先されることになる。

【０１３０】

一方、情報通信処理に関しては、基本的には、通信を遮断して他の設備から隔離する（情報通信処理）とともに、データ改ざんの攻撃を受けた後に加工されたワークを特定する（情報処理）といったセキュリティ脅威１次対応が採用される。

【０１３１】

（ｉｉ）充填機に対するＤＤｏＳ攻撃

例えば、缶や瓶などへの液体の充填機（ボトリングマシーン）に対するＤＤｏＳ（Distributed Denial of Service）攻撃を想定する。通常、充填機は高速に充填動作を行っているので、急停止させることは、設備に対するダメージおよび充填中の缶または瓶の後処理といった面で問題が生じ得る。一方で、ＤＤｏＳ攻撃は、外部との通信が影響を受けるだけであり、充填機自体を動作させることは可能である場合が多い。そのため、充填機は正常運転または縮退運転（例えば、搬送速度を緩やかに低下させる）といったセキュリティ脅威１次対応がとられる。

【０１３２】

一方、制御ユニット１００における情報通信処理に関しては、基本的には、通信を遮断して他の設備から隔離する（通信処理）とともに、データ改ざんの攻撃を受けた後に加工されたワークを特定する（情報処理）といったセキュリティ脅威１次対応が採用される。

【０１３３】

一方、情報通信処理に関しては、情報を受信する処理（すなわち、ＤＤｏＳ攻撃の対象）については遮断し、情報を送信する処理（例えば、上位サーバへの生産情報の送信）については有効化を継続する。

【０１３４】

このように、制御対象に含まれる設備や機械、および、インシデント特性に応じて、対応内容を異ならせることが好ましい。

【０１３５】

＜Ｆ．インシデント対応＞

次に、図６に示されるインシデント対応（ステップＳ８）について説明する。

【０１３６】

図８は、生産機械および検査装置を含むラインに対する攻撃例を示す模式図である。図８を参照して、例えば、生産機械が製品を生産するとともに、生産機械の下流側に配置さ

れた検査装置によって生産機械が生産した製品を検査した上で出荷するようなラインを想定する。

【０１３７】

このようなラインに対して、攻撃者は、不良品を市場に流出させることを目論んだとする。このような目論みを実現するために、攻撃者は、不良品を生産するように生産機械を改ざんし、さらに、その不良品を検出できないように検査装置を改ざんする。

【０１３８】

このような攻撃の具体的な内容としては、例えば、検査装置に対して、良否判定ロジックを改ざんする。すなわち、検査装置が不良品であると判断しないように、良否判定ロジックを意図的に書き換えるといった攻撃がなされる。

【０１３９】

併せて、生産機械に対して、レシピ情報および／または制御ロジックを改ざんする。すなわち、生産機械が不良品を生産するように制御内容を変更するといった攻撃がなされる。

【０１４０】

このような攻撃を受けた場合には、インシデントの発生となり、インシデントに応じた対応が必要となる。インシデントに応じた対応についても、インシデント特性に応じてその対応内容を変化させることが好ましい。

【０１４１】

本事例において、具体的なインシデントに応じた対応としては、以下のようなものが想定される。

【０１４２】

・改ざんされた可能性のある検査装置を使用せずに、別の検査装置に切り替える（検査装置を冗長化しておく、あるいは、別のラインにある安全な検査装置へ製品を流す）

・改ざん前のロジック（良否判定ロジックあるいは制御ロジック）をバックアップしておき、自動的にリストアする（自動的にリストアすることで、エンドユーザが定期的にバックアップをとらなくてもよく、また、安全と判断できる過去のバックアップがどれなのかを特定できる）

・リスクが存在し得る工程の生産を停止する一方で、その他の脅威がない工程については生産を継続する（仕掛品が増加するが、全工程を止める必要はない）

・既に生産された製品の良否判定結果も疑わしいので、正規の倉庫へ保管するのではなく、再度検査を行うことで、そのまま市場へ流通させない（再検査用のラインへ流すようにしてもよいし、人手で再検査してもよい）

上述したように本実施の形態においては、検知された不正侵入（セキュリティ脅威）のインシデント特性を利用できるので、例えば、製品の良否判定が適切に実行されていることが保証できれば、生産ラインを全停止する必要はない。また、再検査の対象となる商品を絞り込むことができれば、全品回収などの被害拡大を回避できる。

【０１４３】

＜Ｇ．インシデント特性に応じた対応＞

上述したように、本実施の形態に従うコントローラシステム１においては、セキュリティユニット２００が不正侵入（セキュリティ脅威）を検知すると、その検知された不正侵入（セキュリティ脅威）のインシデント特性を制御ユニット１００などに通知する（図７など参照）。制御ユニット１００およびセーフティユニット３００においては、インシデント特性に基づいて、セキュリティ脅威に対する適切な範囲および内容の対応が可能となる（図６のステップＳ４およびＳ８）。

【０１４４】

本実施の形態に従うコントローラシステム１は、検知された不正侵入（セキュリティ脅威）のインシデント特性に応じて、制御ユニット１００および／またはセーフティユニット３００における制御（すなわち、セキュリティ脅威１次対応またはインシデント対応）の内容を異ならせることができる。以下、このようなインシデント特性に応じた制御内容

の決定例について説明する。

【０１４５】

図９は、本実施の形態に従うコントローラシステム１におけるインシデント特性に応じた設備別の制御動作の一例を示す図である。図１０は、本実施の形態に従うコントローラシステム１におけるインシデント特性に応じた設備別の制御動作の別の一例を示す図である。図１１は、本実施の形態に従うコントローラシステム１におけるインシデント特性に応じた各設備における状態別の制御動作の一例を示す図である。

【０１４６】

図９には、インシデント特性として、攻撃の種類あるいは攻撃後の状態（例えば、無作為改ざん、リソース枯渇、ＤＤｏＳ攻撃など）がセキュリティユニット２００から出力される例を示す。セキュリティユニット２００から出力される各インシデント特性に応じた対応が実行されることになる。このようなインシデント特性に応じた対応は、設備や機械毎にさらに細かく設定されてもよい。

【０１４７】

インシデント特性に応じた対応としては、設備制御についての対応、および、情報通信についての対応に大別できる。設備制御は、主として、制御ユニット１００の制御エンジン１５０および／またはセーフティユニット３００のセーフティエンジン３５０（いずれも図５参照）が担当する処理を意味し、制御対象の設備や機械の動作についての対応を意味する。情報通信は、主として、制御ユニット１００の情報エンジン１６０が担当する処理を意味し、制御ユニット１００と外部装置との間のデータの遣り取りや、制御ユニット１００内部での情報の取り扱いなどについての対応を意味する。

【０１４８】

図９に示す制御動作のうち、「正常運転」は、システム設計通りおよび生産計画通りに、設備や機械を運転継続できる状態を意味する。「縮退」（図中には、「縮退」に「Ａ１」などの識別情報を付加して表現している。）は、コントローラシステム１の部分停止（一部のみ稼働）、性能縮小（性能低下）、機能制限などの、限定的ながら稼働を続行することを意味する。「停止」は、安全に、対象の設備や機械あるいはコントローラシステム１の動作を止めることを意味する。なお、図１０および図１１においても同様である。

【０１４９】

図１０には、インシデント特性としては、検知された不正侵入（セキュリティ脅威）のレベル（重篤度あるいは緊急度など）がセキュリティユニット２００から出力される例を示す。各レベルは、検知された攻撃の種類あるいは攻撃後の状態などに基づいて算出される。セキュリティユニット２００から出力される各インシデント特性に応じた対応が実行されることになる。このようなインシデント特性に応じた対応は、設備や機械毎にさらに細かく設定されてもよい。

【０１５０】

図１１には、各設備や機械の状態毎に各インシデント特性に応じた対応を設定する例を示す。例えば、設備毎に運転中、メンテナンス中、段取り替え中などの状態を特定するとともに、検知されたインシデント特性と、現在の状態とに基づいて、各設備に対する対応を決定してもよい。

【０１５１】

なお、図１１には、設備や機械の状態を例示するが、これに限らず、例えば、ＰＬＣの動作状態（通常運転中、リモートアクセス中、デバッグ中など）に応じて、対応の内容を異ならせてもよい。さらに、各インシデント特性に応じた対応を状態のみに基づいて決定してもよい。すなわち、設備や機械の違いによらず、セキュリティ脅威が検知されたときの状態のみに基づいて対応を決定するようにしてもよい。

【０１５２】

また、図１１に示すインシデント特性として、図１０に示すレベルを用いてもよい。

図９～図１１に示すように、本実施の形態に従うコントローラシステム１においては、セキュリティユニット２００から出力されるインシデント特性に応じて、設備毎および／

または状態毎に必要な対応を動的に決定できる。このような対応の内容を動的に決定することで、設備や機械の運転を継続することによる生産性の維持と、セキュリティに対する対処とを柔軟に実行できる。なお、図９～図１１には、標準制御に関する制御動作を例示するが、セーフティ制御についても同様の制御動作を定義できる。

【０１５３】

次に、図９～図１１に示す「縮退」の一例について説明する。

（１）設備制御の縮退

設備制御の縮退は、範囲、機能、生産性などの面において制限を受けた状態で運転することを意味する。

【０１５４】

範囲としては、制御対象となるゾーンを制限することができる。制御対象となるゾーンとしては、例えば、制御装置、制御装置に装着されるモジュール、制御装置に装着されるユニットなどの制御側を制限することができる。あるいは、特定の機械、ライン、フロア、工場全体といった被制御側（制御対象）を制限することができる。

【０１５５】

機能としては、コントローラシステム１が提供する処理のうち特定の処理（例えば、情報制御、標準制御、セーフティ制御など）を制限することができる。

【０１５６】

生産性としては、安全、安心のために一時的に生産性（例えば、ラインスピード、単位時間あたりの生産数、単位時間あたりの生産量など）を制限することができる。

【０１５７】

（２）情報通信の縮退

情報通信の縮退は、範囲、方向、帯域、ＱｏＳ（Quality of Service）、データなどの面において制限を受けた状態で運転することを意味する。

【０１５８】

範囲としては、例えば、通信物理ポート、通信論理ポート、ネットワーク離脱などを制限できる。

【０１５９】

通信物理ポートを制限する場合には、制御ユニット１００およびセキュリティユニット２００にそれぞれ配置されている通信ポートのうち特定のポート使用を制限することができる。あるいは、コントローラシステム１に実装される通信ポートのうち、上位側あるいはフィールド側のみを有効化してもよい。

【０１６０】

通信論理ポートを制限する場合には、利用可能なＴＣＰ／ＵＤＰポートを制限してもよいし、利用可能な通信プロトコルを制限してもよい。さらに、アクセスを受け付けるＭＡＣアドレスやＩＰアドレスを制限してもよい。

【０１６１】

方向としては、例えば、各ポートにおいてデータが流れる方向を一方向のみに制限してもよい。例えば、特定のポートについて、データの受信のみ許可、あるいは、データの送信のみ許可といった具合である。このような一方向のデータのみを許可することで、何らかのセキュリティ脅威が検知されたときに、コントローラシステム１からデータが流出することを防止できる。

【０１６２】

帯域としては、コントローラシステム１の通信負荷あるいは処理負荷を低減させるために、通信速度を制限（例えば、１Ｇｂｐｓから１００Ｍｂｐｓに変更）してもよい。

【０１６３】

ＱｏＳとしては、通過させるパケットの優先度を動的に変化させてもよい。例えば、何らかのセキュリティ脅威が検知された場合には、通過させるパケットの優先度を高く変更してもよい。

【０１６４】

データとしては、例えば、ＥｔｈｅｒＣＡＴなどの産業用ネットワークプロトコルにおいては、プロセスデータ通信の有効／無効の切り替えや、出力値の更新を制限（更新停止／ゼロクリア／前回値を保持など）してもよい。

【０１６５】

上述したものに限らず、「縮退」は、正常運転に対して任意の制限が加えられた状態での運転を包含し得る。なお、「縮退」は、部分停止と見なすこともでき、「停止」は、特定の機能を全面的に停止することを包含し得るので、「縮退」を拡張した概念と見なすこともできる。

【０１６６】

図１２は、本実施の形態に従うコントローラシステム１におけるセキュリティ脅威が検知された場合の処理手順を示すフローチャートである。図１２に示す各ステップは、制御ユニット１００のプロセッサ１０２、セキュリティユニット２００のプロセッサ２０２、およびセーフティユニット３００のプロセッサ３０２がそれぞれプログラムを実行することで実現される。

【０１６７】

図１２を参照して、セキュリティユニット２００は、制御ユニット１００で生じる処理、および、ネットワーク上を流れるパケットなどに基づいて、不正侵入が生じているか否かを判断する（ステップＳ１００）。不正侵入が生じていなければ（ステップＳ１００においてＮＯ）、ステップＳ１００の処理が繰り返される。

【０１６８】

不正侵入が生じていなければ（ステップＳ１００においてＹＥＳ）、セキュリティユニット２００は、検知した不正侵入（セキュリティ脅威）に対応するインシデント特性を制御ユニット１００へ通知する（ステップＳ１０２）。制御ユニット１００は、セキュリティユニット２００からのインシデント特性の通知を受けて、予め定められた動作の変更に係る条件に合致するか否かを判断する（ステップＳ１０４）。

【０１６９】

予め定められた動作の変更に係る条件に合致すれば（ステップＳ１０４においてＹＥＳ）、制御ユニット１００は、当該合致した条件に対応する対象の設備や機械の動作を変更する（ステップＳ１０６）。

【０１７０】

これに対して、予め定められた動作の変更に係る条件に合致しなければ（ステップＳ１０４においてＮＯ）、ステップＳ１０６の処理はスキップされる。そして、ステップＳ１００以下の処理が繰り返される。

【０１７１】

＜Ｈ．不正侵入検知時の処理の設定＞

次に、上述したようなコントローラシステム１における不正侵入の検知時の処理を設定するためのユーザインターフェイスの一例について説明する。図５に示すように、サポート装置６００がコントローラシステム１に対する設定を行う。

【０１７２】

（ｈ１：サポート装置６００）

図１３は、本実施の形態に従うコントローラシステム１に接続されるサポート装置６００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６００は、一例として、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）を用いて実現される。

【０１７３】

図１３を参照して、サポート装置６００は、プロセッサ６０２と、メインメモリ６０４と、入力部６０６と、出力部６０８と、ストレージ６１０と、光学ドライブ６１２と、ＵＳＢコントローラ６２０とを含む。これらのコンポーネントは、プロセッサバス６１８を介して接続されている。

【０１７４】

プロセッサ６０２は、ＣＰＵやＧＰＵなどで構成され、ストレージ６１０に格納された

プログラム（一例として、ＯＳ６１０２およびサポートプログラム６１０４）を読出して、メインメモリ６０４に展開して実行することで、コントローラシステム１に対する設定処理などを実現する。

【０１７５】

メインメモリ６０４は、ＤＲＡＭやＳＲＡＭなどの揮発性記憶装置などで構成される。ストレージ６１０は、例えば、ＨＤＤやＳＳＤなどの不揮発性記憶装置などで構成される。

【０１７６】

ストレージ６１０には、基本的な機能を実現するためのＯＳ６１０２に加えて、サポート装置６００としての機能を提供するためのサポートプログラム６１０４が格納される。すなわち、サポートプログラム６１０４は、コントローラシステム１に接続されるコンピュータにより実行されることで、本実施の形態に係るサポート装置６００を実現する。

【０１７７】

入力部６０６は、キーボードやマウスなどで構成され、ユーザ操作を受け付ける。出力部６０８は、ディスプレイ、各種インジケータ、プリンタなどで構成され、プロセッサ６０２からの処理結果などを出力する。

【０１７８】

ＵＳＢコントローラ６２０は、ＵＳＢ接続を介して、コントローラシステム１などとの間のデータを遣り取りする。

【０１７９】

サポート装置６００は、光学ドライブ６１２を有しており、コンピュータ読取可能なプログラムを非一過的に格納する記録媒体６１４（例えば、ＤＶＤ（Digital Versatile Disc）などの光学記録媒体）から、その中に格納されたプログラムが読取られてストレージ６１０などにインストールされる。

【０１８０】

サポート装置６００で実行されるサポートプログラム６１０４などは、コンピュータ読取可能な記録媒体６１４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などからダウンロードする形でインストールするようにしてもよい。また、本実施の形態に係るサポート装置６００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る場合もある。

【０１８１】

図１３には、プロセッサ６０２がプログラムを実行することで、サポート装置６００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など）を用いて実装してもよい。

【０１８２】

（ｈ２：不正侵入検知時の対処設定）

図１４～図１７は、本実施の形態に従うコントローラシステム１に対する不正侵入検知時の対処を設定するためのユーザインターフェイス画面の一例を示す模式図である。図１４～図１７には、一例として、不正侵入通知イベントタスクとして制御ユニット１００に設定される場合の設定手順の一例を示す。なお、図１４～図１７に示すユーザインターフェイス画面は、典型的には、サポート装置６００のプロセッサ６０２がサポートプログラム６１０４を実行することで実現される。

【０１８３】

図１４に示すユーザインターフェイス画面６５０は、セキュリティユニット２００から通知される不正侵入のインシデント特性の設定および登録を受け付ける。具体的には、ユーザインターフェイス画面６５０は、インシデント特性の設定登録領域６５２を有している。設定登録領域６５２には、セキュリティユニット２００において検知可能な不正侵入（セキュリティ脅威）が一覧表示されている。

【０１８４】

図１４の設定登録領域６５２は、「攻撃タイプ」のカラム６５６を含んでおり、ユーザは、「有効」のカラム６５４において、通知を有効化する攻撃タイプ（検知される不正侵入の種類）をチェックする。図１４に示す例では、３つの攻撃タイプが有効化されている。すなわち、図１４に示すユーザインターフェイス画面６５０においてチェックされている攻撃タイプについては、セキュリティユニット２００により検知されると、対応するインシデント特性が制御ユニット１００へ通知されることになる。

【０１８５】

図１５に示すユーザインターフェイス画面６６０は、セキュリティユニット２００からインシデント特性を通知されたときに実行されるプログラムの作成が可能になっている。具体的には、ユーザインターフェイス画面６６０は、プログラム編集領域６６２を有しており、ユーザはプログラム編集領域６６２に特定のインシデント特性が通知されたときに実行されるべきプログラム（典型的には、縮退または停止といったセキュリティ脅威１次対応を実現するためのプログラム）が記述される。図１５に示す例では、縮退を実現するためのプログラムが記述され、「縮退処理Ａ」として登録されるものとする。

【０１８６】

図１６に示すユーザインターフェイス画面６７０は、イベントタスクの設定を受け付ける。イベントタスクは、予め定められた条件が満たされたときのみ実行されるタスクを意味する。より具体的には、ユーザインターフェイス画面６７０のカラム６７２において、タスクタイプとして「イベントタスク」が指定される。そして、カラム６７４において、タスク名として「Security_RiskDetected_A」が指定される。なお、このタスク名は任意に指定できる。さらに、カラム６７６において、周期／実行条件として、「不正侵入検知」が指定される。「不正侵入検知」が指定されることで、セキュリティユニット２００からインシデント特性が通知されたことをイベントとして実行されることが規定される。

【０１８７】

このように、サポート装置６００は、ユーザインターフェイス画面６７０において、セキュリティユニット２００により不正侵入が検知されたときに制御ユニット１００により実行されるプログラムの指定を受け付ける。

【０１８８】

さらに、カラム６７８において、セキュリティユニット２００から通知されるインシデント特性に対する条件、すなわちインシデント特性の種別が設定される。図１６に示す例では、「無作為改ざん」、「リソース枯渇」、「ＤＤｏＳ攻撃」の３種類が提示されており、ユーザはこれらのインシデント特性のうち１または複数を選択する。このように、サポート装置６００は、ユーザインターフェイス画面６７０において、制御ユニット１００によりプログラムが実行される条件として、不正侵入の種類の指定を受け付ける。

【０１８９】

図１７に示すユーザインターフェイス画面６８０は、図１５に示すユーザインターフェイス画面６６０上で作成したプログラムを、図１６に示すユーザインターフェイス画面６７０において設定したタスクに割り当てる設定を受け付ける。

【０１９０】

「Security_RiskDetected_A」と表示されたタスク名を示すオブジェクト６８２を選択し、「縮退処理Ａ」として登録されたプログラムを入力欄６８４に設定することで、セキュリティユニット２００からのインシデント特性の通知を条件に、「縮退処理Ａ」のプログラムがイベント実行されるようになる。

【０１９１】

以上のような設定手順によって、セキュリティユニット２００での不正侵入の検知、セキュリティユニット２００から制御ユニット１００へのインシデント特性の通知、制御ユニット１００でのインシデント特性に応じた動作の変更（予め登録されたプログラムの実行）が実現される。このように、サポート装置６００は、セキュリティユニット２００のセキュリティエンジン２５０により検知された不正侵入に応じて制御ユニット１００により実行される制御演算に係る設定およびプログラムなどを受け付ける。

【０１９２】
制御ユニット１００は、通知されるインシデント特性に対応付けられたプログラムを実行することで、制御動作を変更する。同様に、制御ユニット１００は、制御動作を変更することにより、制御対象の動作を停止することもできる。あるいは、制御ユニット１００は、制御動作を変更することにより、制御対象の動作を制限すること（縮退動作）もできる。
【０１９３】
また、制御ユニット１００は、制御動作を変更することにより、コントローラシステム１に含まれる装置の動作を制限することもできる。
【０１９４】
上述の説明においては、不正侵入通知イベントタスクとして処理を設定する例を説明したが実装形態はこれに限られない。例えば、セキュリティユニット２００からインシデント特性の通知を示すシステム変数を用意するとともに、当該システム変数を起動条件とした、縮退処理や停止処理に必要なプログラムを作成するようにしてもよい。
【０１９５】
さらに、システム変数をユーザ定義変数にマッピングすることで、ユーザプログラム内の任意の命令で参照可能にしてもよい。
【０１９６】
（ｈ３：設備別／状態別の制御動作設定）
次に、本実施の形態に従うコントローラシステムにおけるインシデント特性に応じた設備別の制御動作および状態別の制御動作の設定を支援するための機能について説明する。
【０１９７】
制御対象の設備や機械の特性や仕様などに応じて、発生したインシデントに応じた処理を最適化することが好ましいが、このような制御動作の設定には、ある程度の専門知識が必要となる。そこで、以下に説明するような、制御動作の設定を支援する機能を実装してもよい。
【０１９８】
図１８は、本実施の形態に従うコントローラシステムが提供するインシデント特性に応じた制御動作のモデル設定６３０の一例を示す図である。図１８を参照して、モデル設定６３０は、予め定められた１または複数の類型毎にインシデント特性に応じた制御動作を含む。すなわち、サポート装置６００は、制御動作の典型的な挙動を規定する複数のモデル設定６３０を有している。
【０１９９】
各類型の制御動作は典型的な挙動を示すものであり、後述するように、適宜変更することもできる。なお、図１８には、設備毎のモデル設定の一例を示すが、設備および状態のそれぞれに対応するモデル設定（図１１など参照）を採用してもよい。この点は、以下の説明においても同様である。
【０２００】
サポート装置６００は、ユーザ操作に応じて、複数のモデル設定６３０のうちいずれかを制御ユニット１００に反映する。このようなインシデント特性に応じた制御動作（モデル設定６３０）を決定する方法としては、対象の設備種別を選択する方法に加えて、対話形式で選択する方法を採用してもよい。
【０２０１】
まず、対象の設備種別を選択する方法について説明する。図１９は、本実施の形態に従うコントローラシステムにおける制御動作を設定する処理手順を説明するための図である。
【０２０２】
例えば、サポート装置６００において、図１９（Ａ）に示すようなユーザインターフェイス画面６４０が提供される。ユーザインターフェイス画面６４０は、選択可能な設備種別の一覧６４２を含むとともに、ユーザがいずれかの設備種別を選択した後に、決定ボタ

ン６４４を選択すると、対応するモデル設定が設定される。
【０２０３】
サポート装置６００は、図１９（Ｂ）に示すような対応テーブル６３２を有しており、ユーザがいずれかの設備種別を選択すると、対応する類型を決定する。そして、モデル設定６３０（図１８参照）を参照して、決定された類型に対応する制御動作が設定される。
【０２０４】
このように、複数のモデル設定６３０の各々は、設備種別に関連付けられている。そして、サポート装置６００は、ユーザによる設備の選択に応じて、対応するモデル設定を選択および反映する。図１９に示すような対象の設備種別を選択する方法を採用することで、専門知識のないユーザであっても、インシデント特性に応じた最適な制御動作を設定できる。
【０２０５】
次に、対話形式で選択する方法について説明する。
図２０は、本実施の形態に従うコントローラシステムにおける制御動作を設定する別の処理手順を説明するための図である。図２０を参照して、サポート装置６００は、類型を決定するための判定モデル６３４を有している。判定モデル６３４は、対象の設備の特性や仕様などを決定するための１または複数の質問項目を含む。
【０２０６】
サポート装置６００は、判定モデル６３４に沿った質問をユーザに対して提供するとともに、当該質問に対するユーザからの回答に従ってステートを順次遷移させる。サポート装置６００は、いずれかの類型に到達すると、当該到達した類型に対応する制御動作を決定する。
【０２０７】
図２１は、本実施の形態に従うコントローラシステムにおける制御動作を設定するさらに別の処理手順を説明するための図である。図２１（Ａ）を参照して、サポート装置６００は、類型を決定するための質問項目群６３６を有している。質問項目群６３６は、対象の設備の特性や仕様などを決定するための１または複数の質問項目を含む。
【０２０８】
サポート装置６００は、質問項目群６３６に含まれる１または複数の質問をユーザに対して提供するとともに、当該質問に対するユーザからの回答を受け付ける。サポート装置６００は、すべての質問に対する回答に基づいて、図２１（Ｂ）に示すような対応テーブル６３８を参照して、対応する類型を決定する。そして、サポート装置６００は、モデル設定６３０（図１８参照）を参照して、決定された類型に対応する制御動作を設定する。
【０２０９】
このように、サポート装置６００は、対話型インターフェイスを介して、１または複数の質問をユーザに呈示するとともに、各質問に対するユーザの選択に応じて、複数のモデル設定６３０のうち対象となるモデル設定６３０を選択および反映する。質問の提供および各質問に対する回答の受け付けといった対話形式を採用することで、専門知識のないユーザであっても、インシデント特性に応じた最適な制御動作を設定できる。
【０２１０】
上述したような手順に従って決定された制御動作については、ユーザが任意に変更できるようにしてもよい。
【０２１１】
図２２は、本実施の形態に従うコントローラシステムにおける制御動作の設定を変更するためのユーザインターフェイス画面の一例を示す模式図である。図２２に示すユーザインターフェイス画面６４６においては、現在設定されている制御動作の内容が一覧表示されている。ユーザが任意の項目を選択すると、当該選択された項目に対応付けてサブウィンドウ６４８が表示される。サブウィンドウ６４８には、選択可能な複数の設定値が表示されており、ユーザは所望する設定値を選択する。このような変更操作によって、モデル設定に対してユーザが所望する任意の変更を行うことができる。

【０２１２】
＜Ｉ．セキュリティユニット２００に対する指令＞
上述したように、セキュリティユニット２００は不正侵入を検知すると、検知した不正侵入に対応するインシデント特性を制御ユニット１００およびセーフティユニット３００へ通知する。制御ユニット１００および／またはセーフティユニット３００は、セキュリティユニット２００からのインシデント特性に応じて制御動作を適宜変更することができる。
【０２１３】
図６のセキュリティ脅威に対する対策サイクルに示すように、セキュリティ脅威１次対応が実行された後、あるいは、インシデント対応が実行された後、対策が完了すると、試運転を経て運用が再開される。このような正常運転に復旧するにあたっては、制御ユニット１００あるいはセーフティユニット３００からセキュリティユニット２００に対して、復旧するための指令を与える必要がある。
【０２１４】
また、制御ユニット１００またはセーフティユニット３００で実行される制御演算において、セキュリティユニット２００のセキュリティ監視レベルや有効化されたセキュリティ機能を変更したいというニーズも存在する。例えば、他のコントローラシステム１において不正侵入が検知されたとの通知を受けて、自コントローラシステム１におけるセキュリティ監視レベルを高めるといった処理や、制御ユニット１００がリモートメンテナンスされる場合に、セキュリティ監視レベルを緩和するといった処理が要求されることもある。
【０２１５】
そこで、本実施の形態に従うコントローラシステム１は、制御ユニット１００またはセーフティユニット３００からセキュリティユニット２００に対して、動作状態を変更するための指令が送信可能であってもよい。
【０２１６】
図２３は、本実施の形態に従うコントローラシステム１におけるセキュリティユニット２００に対する変更指令の遣り取りを説明するための模式図である。図２３を参照して、例えば、制御ユニット１００の制御エンジン１５０および情報エンジン１６０は、ユーザ操作などを受けて、セキュリティユニット２００のセキュリティエンジン２５０に各種の変更指令を出力可能になっている。
【０２１７】
このように、制御ユニット１００の制御エンジン１５０および情報エンジン１６０は、セキュリティユニット２００のセキュリティエンジン２５０（検知手段）の挙動を変更するための指令を送信する指令送信手段に相当する。上述したように、セキュリティユニット２００のセキュリティエンジン２５０の挙動を変更するための指令は、セキュリティエンジン２５０による不正侵入の検知を復旧するための指令を含んでいてもよいし、セキュリティエンジン２５０による不正侵入が発生したか否かを検知するレベルを変更するための指令を含んでいてもよい。
【０２１８】
制御ユニット１００の制御エンジン１５０および情報エンジン１６０は、ユーザ操作に応じて、セキュリティユニット２００のセキュリティエンジン２５０の挙動を変更するための指令を送信するようにしてもよいし、予め定められた条件が成立すると、自動的に送信するようにしてもよい。
【０２１９】
図２４は、本実施の形態に従うコントローラシステム１におけるセキュリティユニット２００の動作を変更するためのプログラム命令の一例を示す図である。図２４を参照して、例えば、制御ユニット１００で実行されるユーザプログラムに、セキュリティユニット２００の動作を変更するための命令１９０を含めることができる。図２４に示す例では、命令１９０をファンクションブロックの形式で記述しているが、任意の言語または形式で

記述できるようにしてもよい（例えば、ＩＥＣ　６１１３１－３に規定されたいずれかの言語）。

【０２２０】

このように、制御ユニット１００において実行される制御演算に係る命令を含むユーザプログラムには、セキュリティエンジン２５０（検知手段）の挙動を変更するための指令を送信するための命令を含むようにしてもよい。図２４に示すようなユーザプログラムで利用できる命令を用意することで、制御対象や動作状態などに応じて、セキュリティ機能を柔軟に運用できる。

【０２２１】

セキュリティユニット２００の動作を変更する命令としては、例えば、（１）検知対象の攻撃タイプ（インシデント特性）の変更・削除・追加、（２）不正侵入検知の有効化／無効化、（３）不正侵入の検知レベルの変更、（４）インシデント特性の通知先の変更・追加・削除などが挙げられる。これらに限らず、セキュリティユニット２００の動作を変更するための任意の命令を採用できる。

【０２２２】

なお、セキュリティユニット２００に対する不正な命令が発行されることにより、セキュリティユニット２００自体が無効化されることを防止するために、セキュリティレベルを上げる方向の指令のみを有効化してもよい。

【０２２３】

あるいは、セキュリティユニット２００に対して命令を発行する制御ユニット１００またはセーフティユニット３００を公知の方法で事前認証または都度認証するようにしてもよい。

【０２２４】

上述したように、制御ユニット１００またはセーフティユニット３００からセキュリティユニット２００に対して動作の変更を指示する機構を採用することで、コントローラシステム１全体として、適切なセキュリティレベルを維持しつつ、柔軟な生産を実現できる。

【０２２５】

＜Ｊ．セキュリティ情報の可視化・ユーザ支援＞

通常、セキュリティ事象は目に見えないので、特に、ＯＴ部門の作業者にとってみれば、現在どのようなステータスであるのかを把握することが難しい。そのため、本実施の形態に従うコントローラシステム１は、セキュリティ情報を可視化するとともに、不正侵入が検知されたときなどのユーザ支援を提供する。

【０２２６】

（ｊ１：ステータス）

セキュリティユニット２００が何らかの不正侵入を検知した場合には、セキュリティユニット２００の表面に配置されたインジケータ２２４、制御ユニット１００の表面に配置されたインジケータ１２４、ＨＭＩ８００のインジケータ８２４（いずれも図５参照）などを用いて、ユーザに通知を行うようにしてもよい。この場合、不正侵入の検知前後で、点灯色変更、点灯開始、点滅開始などの任意の表示態様の変化を利用すればよい。さらに、表示だけではなく、音や音声メッセージなどを用いてもよい。

【０２２７】

セキュリティ脅威は、セキュリティリスクに応じて定量化することもできる。本明細書において、「セキュリティリスク」は、不正侵入として検知される確率あるいは度合いを定量的に示す用語である。「セキュリティリスク」は、例えば、無作為改ざんを行うためのパケットの到来頻度やＤＤｏＳ攻撃の度合いなどにより算出できる。このような定量化されたセキュリティリスクが得られる場合には、制御ユニット１００の表面に配置されたインジケータ１２４、ＨＭＩ８００のインジケータ８２４には、算出される度合いを表示するようにしてもよい。

【０２２８】

図２５は、本実施の形態に従うコントローラシステム１に採用されるインジケータの一例を示す模式図である。図２５（Ａ）および図２５（Ｂ）には、定量化されたセキュリティリスクを表示する場合の構成例を示す。

【０２２９】

図２５（Ａ）に示すインジケータ２２４においては、３つのＬＥＤ（Light Emitting Diode）が配置されており、算出されたセキュリティリスクに応じて点灯数あるいは点灯位置を変化させる。図２５（Ｂ）に示すインジケータ２２４においては、１つのＬＥＤが配置されており、算出されたセキュリティリスクに応じて点灯色あるいは点灯強度を変化させる。

【０２３０】

このように、セキュリティユニット２００は、検知手段であるセキュリティエンジン２５０による検知動作から算出されるセキュリティリスクをユーザに視覚的に提示する提示手段の一例である、インジケータ２２４を有している。

【０２３１】

上述したようなインジケータ２２４を配置することで、専門知識のない作業者であっても、現在のセキュリティリスクのステータスを容易に把握できる。

【０２３２】

図２５に示すようなインジケータに限らず、セキュリティリスクを提示できる形態であれば、どのようなインジケータを採用してもよい。

【０２３３】

また、音や音声メッセージなどを用いてユーザに通知するようにしてもよい。

図２６は、本実施の形態に従うコントローラシステムに採用されるスピーカの動作例を示す模式図である。図２６に示す例では、セキュリティユニット２００のスピーカ２２６から、セキュリティリスクに応じた音声あるいは音声メッセージが出力される。

【０２３４】

例えば、セキュリティリスクが高くなるほど、出力される音声の音量が大きくなるようにしてもよいし、音声の発生間隔が短くなるようにしてもよい。また、セキュリティリスクが高くなるほど、周波数の主成分を高くしてもよい。さらに、セキュリティリスクに応じて音色を異ならせてもよい。

【０２３５】

スピーカ２２６から音声メッセージを出力する場合には、セキュリティリスクに応じて、音声メッセージの内容あるいは音量を異ならせてもよい。例えば、セキュリティリスクの大きさに応じて、「軽微なセキュリティリスクを検知しました」、「セキュリティリスクが高まっています」、「重大なセキュリティ脅威が生じています」というようにメッセージの内容を異ならせてもよい。

【０２３６】

このように、セキュリティユニット２００は、検知手段であるセキュリティエンジン２５０による検知動作から算出されるセキュリティリスクをユーザに聴覚的に提示する提示手段の一例である、スピーカ２２６（音声発生部）を有している。

【０２３７】

上述したようなスピーカ２２６を配置することで、専門知識のない作業者であっても、現在のセキュリティリスクのステータスを容易に把握できる。

【０２３８】

図２５および図２６に示すように、インジケータ２２４やスピーカ２２６などの提示手段は、算出されるセキュリティリスクの度合いに応じて、提示態様を変化させてもよい。このような提示態様の変化によって、ユーザは、現在のセキュリティリスクを即座に把握できる。

【０２３９】

（ｊ２：ログ）

セキュリティユニット２００での不正侵入検知の結果などは、セキュリティユニット２

００のセキュリティ情報２６０として保存されてもよい（図５など参照）。さらに、必要なログは、コントローラシステム１の内部あるいはコントローラシステム１の外部に配置されたデータベースに適宜格納するようにしてもよい。

【０２４０】

（ｊ３：アラーム履歴）

上述のログと同様に、セキュリティユニット２００が不正侵入を検知してアラームを発生した場合などは、そのアラーム履歴をセキュリティユニット２００のセキュリティ情報２６０として保存するようにしてもよい（図５など参照）。さらに、必要なアラーム履歴は、コントローラシステム１の内部あるいはコントローラシステム１の外部に配置されたデータベースに適宜格納するようにしてもよい。

【０２４１】

（ｊ４：トラブルシュート）

図６に示すように、不正侵入が検知され、セキュリティ脅威１次対応が実行されると（ステップＳ４）、ＯＴ部門の作業者は、制御対象の設備や機械に対して必要な処理を行う（現場対応）（ステップＳ５）必要がある。このようなＯＴ部門の作業者の作業を支援する目的で、ＨＭＩ８００などに、検知された不正侵入の種類、および、実行されたセキュリティ脅威１次対応の内容などに応じたトラブルシュート用の情報を提示するようにしてもよい。

【０２４２】

このようなトラブルシュート用の情報を提示することで、正常運転での運用再開までに要する時間を短縮できる。

【０２４３】

＜Ｋ．変形例＞

上述の実施の形態においては、制御ユニット１００と、セキュリティユニット２００と、セーフティユニット３００とが互いに独立したユニットとして構成されたコントローラシステム１について例示した。互いに独立したユニットとして構成することで、柔軟性や可用性を高めることができる。

【０２４４】

但し、必ずしも、各機能を互いに独立したユニットとして構成する必要はなく、制御ユニット１００、セキュリティユニット２００およびセーフティユニット３００の全部または一部を共通のユニットとして構成してもよい。この場合には、筐体をコンパクト化できるなどの利点がある。

【０２４５】

図２７は、本実施の形態に従うコントローラシステム１の構成の変形例を示す模式図である。図２７には、制御ユニット１００、セキュリティユニット２００およびセーフティユニット３００の一部または全部が一体化された構成例を示す。

【０２４６】

図２７（Ａ）に示されるコントローラシステム１Ａは、制御ユニット１００およびセーフティユニット３００を一体化した統合ユニット５０Ａと、セキュリティユニット２００とから構成される。すなわち、コントローラシステム１Ａの統合ユニット５０Ａにおいては、標準制御およびセーフティ制御が同一のユニット内で実行される。

【０２４７】

図２７（Ｂ）に示されるコントローラシステム１Ｂは、セキュリティユニット２００および制御ユニット１００を一体化した統合ユニット５０Ｂと、セーフティユニット３００とから構成される。すなわち、コントローラシステム１Ｂの統合ユニット５０Ｂにおいては、他の装置との間の通信処理および標準制御が同一のユニット内で実行される。

【０２４８】

図２７（Ｃ）に示されるコントローラシステム１Ｃは、制御ユニット１００、セキュリティユニット２００およびセーフティユニット３００を一体化した統合ユニット５０Ｃから構成される。すなわち、コントローラシステム１Ｃの統合ユニット５０Ｃにおいては、

他の装置との間の通信処理、標準制御およびセーフティ制御が同一のユニット内で実行される。

【０２４９】

このように、制御ユニット１００、セキュリティユニット２００およびセーフティユニット３００が担当する機能および処理の実装形態はどのようなものであってもよい。さらに、制御ユニット１００、セキュリティユニット２００およびセーフティユニット３００が担当する機能の一部同士を共通の処理ユニットに実装してもよい。

【０２５０】

＜Ｌ．付記＞

上述したような本実施の形態は、以下のような技術思想を含む。

［構成１］

コントローラシステム（１）であって、

制御対象を制御するための制御演算を実行する制御ユニット（１００）と、

前記制御ユニットに接続され、前記コントローラシステムに対するセキュリティ機能を担当するセキュリティユニット（２００）とを備え、

前記セキュリティユニットは、前記コントローラシステムにおいて何らかの不正侵入が発生したか否かを検知する検知手段（２５０）を含み、

前記制御ユニットは、前記セキュリティユニットの前記検知手段の挙動を変更するための指令を送信する指令送信手段（１５０，１６０）を含む、コントローラシステム。

［構成２］

前記検知手段の挙動を変更するための指令は、前記検知手段による不正侵入の検知を復旧するための指令を含む、構成１に記載のコントローラシステム。

［構成３］

前記検知手段の挙動を変更するための指令は、前記検知手段による不正侵入が発生したか否かを検知するレベルを変更するための指令を含む、構成１または２に記載のコントローラシステム。

［構成４］

前記指令送信手段は、ユーザ操作に応じて、前記検知手段の挙動を変更するための指令を送信する、構成１～３のいずれか１項に記載のコントローラシステム。

［構成５］

前記制御ユニットは、前記制御演算に係る命令を含むユーザプログラムを実行するように構成され、

前記ユーザプログラムは、前記検知手段の挙動を変更するための指令を送信するための命令を含む、構成１～４のいずれか１項に記載のコントローラシステム。

［構成６］

コントローラシステム（１）であって、

制御対象を制御するための制御演算を実行する制御ユニット（１００）と、

前記制御ユニットに接続され、前記コントローラシステムに対するセキュリティ機能を担当するセキュリティユニット（２００）と、

少なくとも前記制御ユニットにアクセス可能なサポート装置（８００）とを備え、

前記セキュリティユニットは、前記コントローラシステムにおいて何らかの不正侵入が発生したか否かを検知する検知手段（２５０）を含み、

前記制御ユニットは、前記検知手段により検知された不正侵入に応じた制御演算を実行するように構成されており、

前記サポート装置は、前記検知手段により検知された不正侵入に応じて前記制御ユニットにより実行される制御演算に係る設定を受け付ける、コントローラシステム。

［構成７］

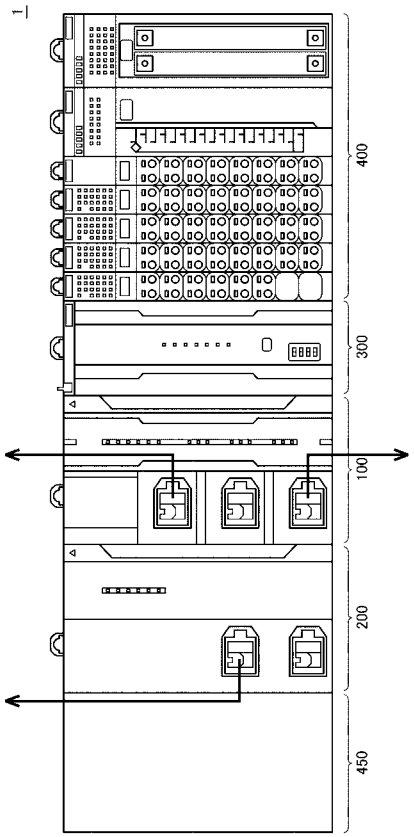
前記サポート装置は、前記検知手段により不正侵入が検知されたときに前記制御ユニットにより実行されるプログラムの指定を受け付ける、構成６に記載のコントローラシステム。

［構成８］
前記サポート装置は、前記制御ユニットによりプログラムが実行される条件として、不正侵入の種類の指定を受け付ける、構成７に記載のコントローラシステム。
［構成９］
前記サポート装置は、制御動作の典型的な挙動を規定する複数のモデル設定（６３０）を有しており、ユーザ操作に応じて、前記複数のモデル設定のうちいずれかを前記制御ユニットに反映する、構成６～８のいずれか１項に記載のコントローラシステム。
［構成１０］
前記複数のモデル設定の各々は、設備種別に関連付けられており、
前記サポート装置は、ユーザによる設備の選択に応じて、対応するモデル設定を選択および反映する、構成９に記載のコントローラシステム。
［構成１１］
前記サポート装置は、対話型インターフェイス（６３４，６３６）を介して、１または複数の質問をユーザに呈示するとともに、各質問に対するユーザの選択に応じて、前記複数のモデル設定のうち対象となるモデル設定を選択および反映する、構成９に記載のコントローラシステム。
［構成１２］
コントローラシステム（１）であって、
制御対象を制御するための制御演算を実行する制御ユニット（１００）と、
前記制御ユニットに接続され、前記コントローラシステムに対するセキュリティ機能を担当するセキュリティユニット（２００）とを備え、
前記セキュリティユニットは、
前記コントローラシステムにおいて何らかの不正侵入が発生したか否かを検知する検知手段（２５０）と、
前記検知手段による検知動作から算出されるセキュリティリスクをユーザに提示する提示手段（２５０）とを含む、コントローラシステム。
［構成１３］
前記提示手段は、前記セキュリティリスクを視覚的に提示するためのインジケータ（２２４）を含む、構成１２に記載のコントローラシステム。
［構成１４］
前記提示手段は、前記セキュリティリスクを聴覚的に提示するための音声発生部（２２６）を含む、構成１２または１３に記載のコントローラシステム。
［構成１５］
前記提示手段は、前記算出されるセキュリティリスクの度合いに応じて、提示態様を変化させる、構成１２～１４のいずれか１項に記載のコントローラシステム。
【０２５１】
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。
【符号の説明】
【０２５２】
１　コントローラシステム、２　第１ネットワーク、４　第２ネットワーク、１０　制御システム、１００　制御ユニット、１０２，２０２，３０２，６０２　プロセッサ、１０４，２０４，３０４　チップセット、１０６，２０６，３０６　主記憶装置、１０８，２０８，３０８　二次記憶装置、１１０，２１０　通信コントローラ、１１２，２１２，６２０　ＵＳＢコントローラ、１１４，２１４，３１４　メモリカードインターフェイス、１１５，２１５，３１５　メモリカード、１１６，１１８，１２０，２１６，２１８　ネットワークコントローラ、１２２，３２２　内部バスコントローラ、１２４，２２４，３２４，８２４　インジケータ、１４２，１４４，２４２　通信ポート、１５０　制御エ

ンジン、１６０　情報エンジン、１７０　ブローカー、１８０，３６０　ログデータベース、１９０　命令、２００　セキュリティユニット、２５０　セキュリティエンジン、２６０　セキュリティ情報、３００　セーフティユニット、３５０　セーフティエンジン、４００　機能ユニット、４５０　電源ユニット、５００　フィールドデバイス、６００　サポート装置、６０４　メインメモリ、６０６　入力部、６０８　出力部、６１０　ストレージ、６１２　光学ドライブ、６１４　記録媒体、６１８　プロセッサバス、６３０　モデル設定、６３２，６３８　対応テーブル、６３４　判定モデル、６３６　質問項目群、６４０，６４６，６５０，６６０，６７０，６８０　ユーザインターフェイス画面、６４２　一覧、６４４　決定ボタン、６４８　サブウィンドウ、６５２　設定登録領域、６５４，６５６，６７２，６７４，６７６，６７８　カラム、６６２　プログラム編集領域、６８２　オブジェクト、６８４　入力欄、７００　装置、８００　ＨＭＩ、９００　データベース、６１０２　ＯＳ、６１０４　サポートプログラム。

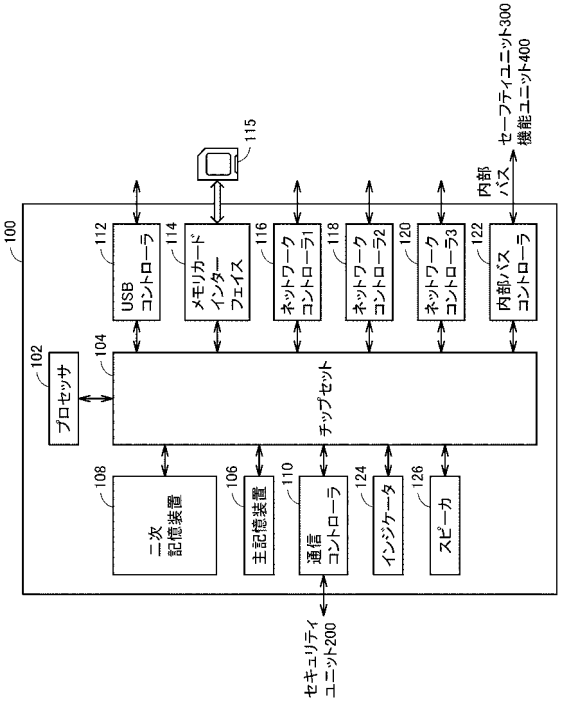
【図１】

図1



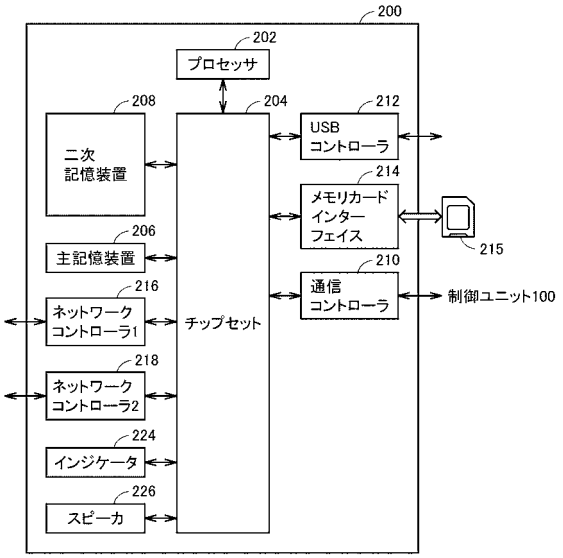

【図２】

図2



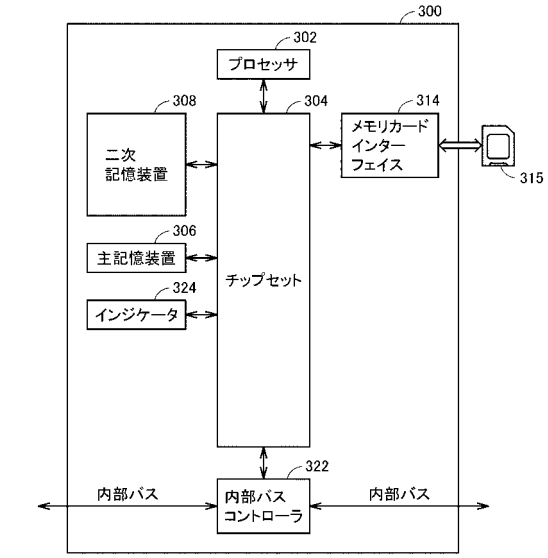
【図３】

図3



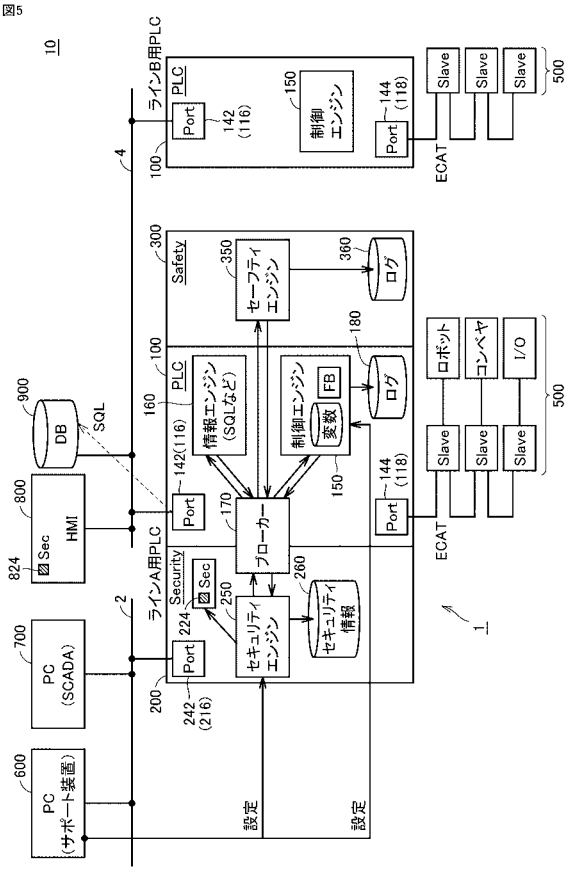

【図４】

図4



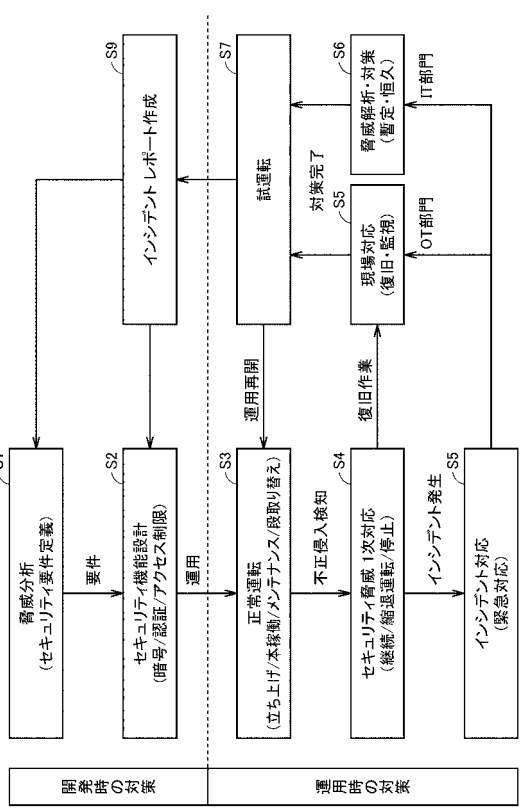

【図５】

図5



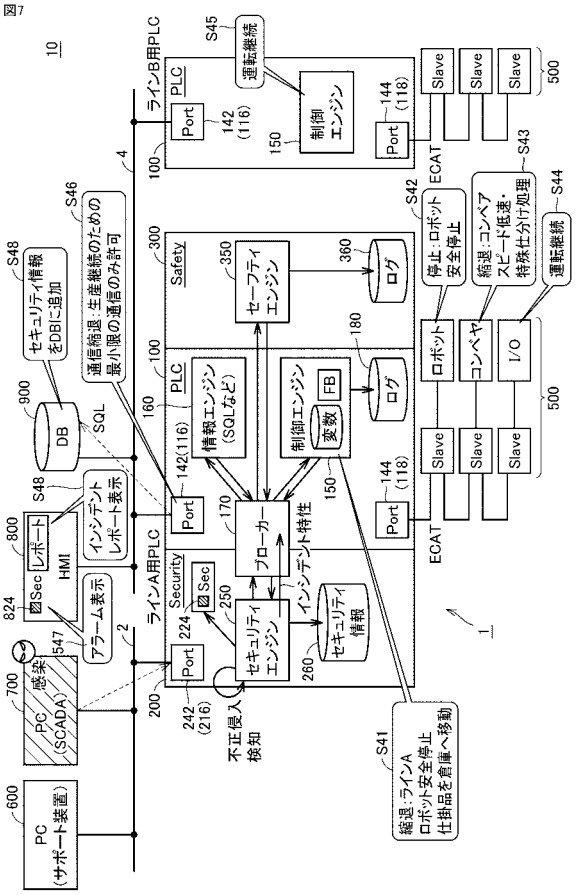

【図６】

図6



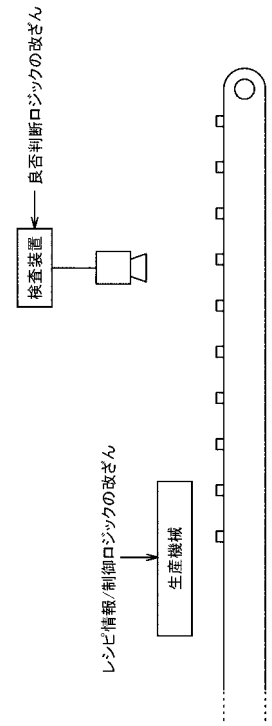
【図７】

図7




【図８】

図8




【図９】

図9

| インシデント特性 | 設備A | 設備B | 設備C |
|---|---|---|---|
| 無し(正常運転) | 設備制御:正常運転<br>情報通信:正常運転 | 設備制御:正常運転<br>情報通信:正常運転 | 設備制御:正常運転<br>情報通信:正常運転 |
| 無作為改ざん | 設備制御:正常運転<br>情報通信:縮退A1 | 設備制御:正常運転<br>情報通信:正常運転 | 設備制御:縮退C1<br>情報通信:縮退C2 |
| リソース枯渇 | 設備制御:縮退A2<br>情報通信:縮退A3 | 設備制御:縮退B1<br>情報通信:縮退B2 | 設備制御:停止<br>情報通信:縮退C3 |
| DDoS攻撃 | 設備制御:停止<br>情報通信:縮退A4 | 設備制御:正常運転<br>情報通信:縮退B3 | 設備制御:停止<br>情報通信:縮退C4 |
| … | | | |

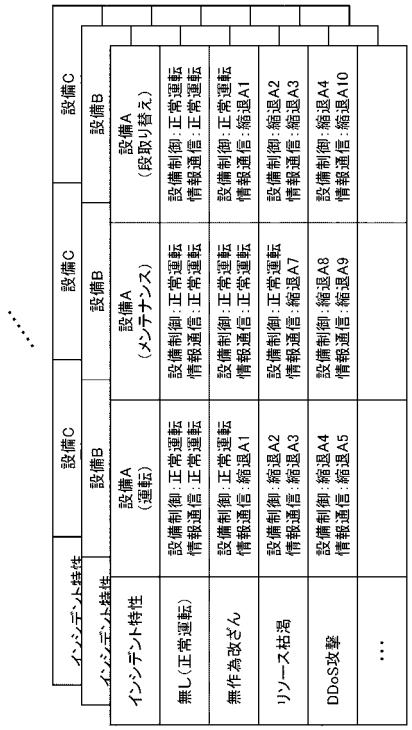
【図１０】

図10

| インシデント特性 | 設備A | 設備B | 設備C |
|---|---|---|---|
| 無し(正常運転) | 設備制御:正常運転<br>情報通信:正常運転 | 設備制御:正常運転<br>情報通信:正常運転 | 設備制御:正常運転<br>情報通信:正常運転 |
| レベル1 | 設備制御:正常運転<br>情報通信:縮退A1 | 設備制御:正常運転<br>情報通信:正常運転 | 設備制御:正常運転<br>情報通信:縮退C1 |
| レベル2 | 設備制御:縮退A2<br>情報通信:縮退A3 | 設備制御:縮退B1<br>情報通信:縮退B2 | 設備制御:正常運転<br>情報通信:縮退C2 |
| レベル3 | 設備制御:停止<br>情報通信:縮退A4 | 設備制御:停止<br>情報通信:縮退B3 | 設備制御:縮退C3<br>情報通信:縮退C4 |

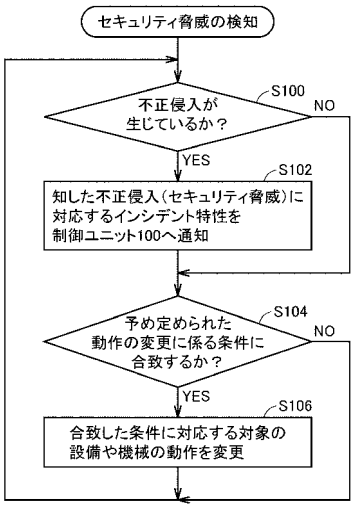
【図１１】

図11



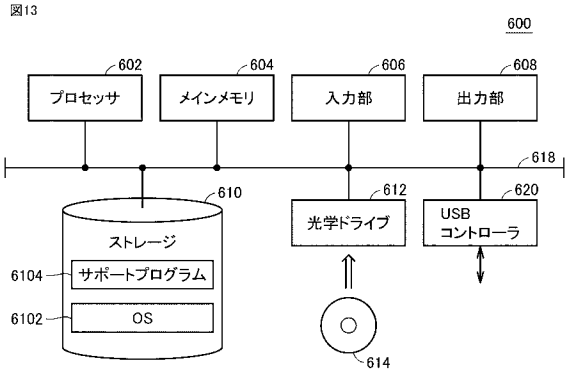

【図１２】

図12



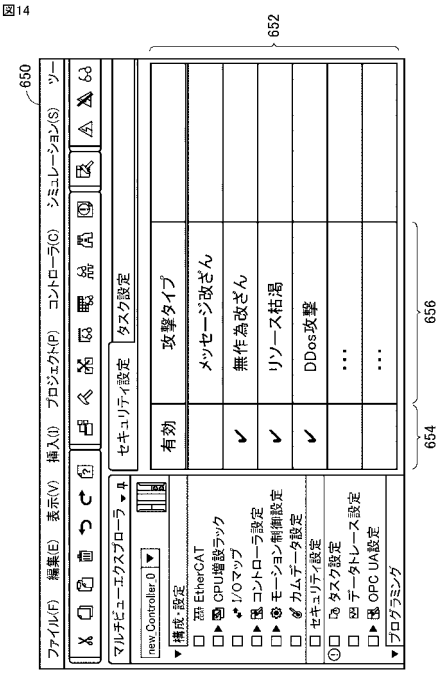

【図１３】

図13



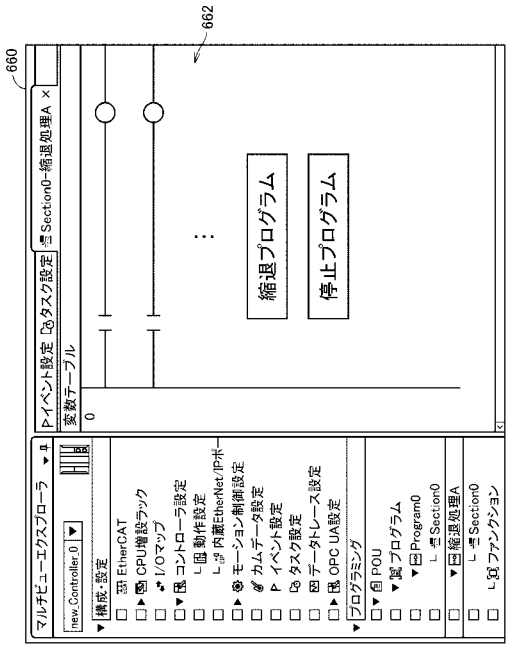

【図１４】

図14



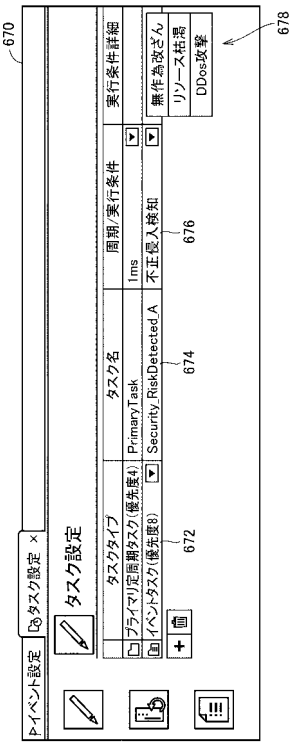
【図１５】

図15



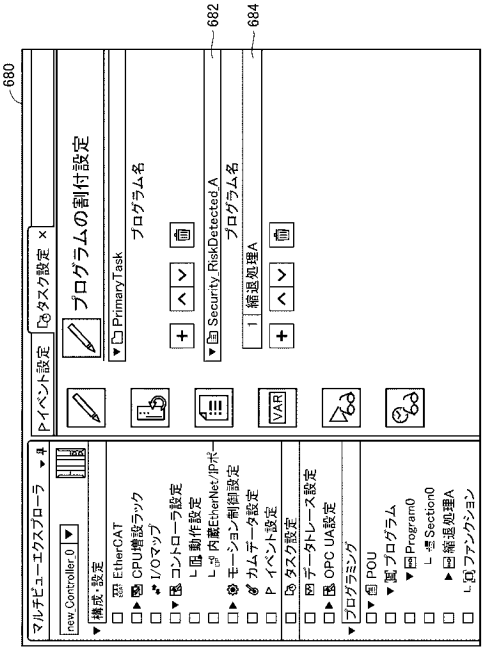

【図１６】

図16




【図１７】

図17




【図１８】

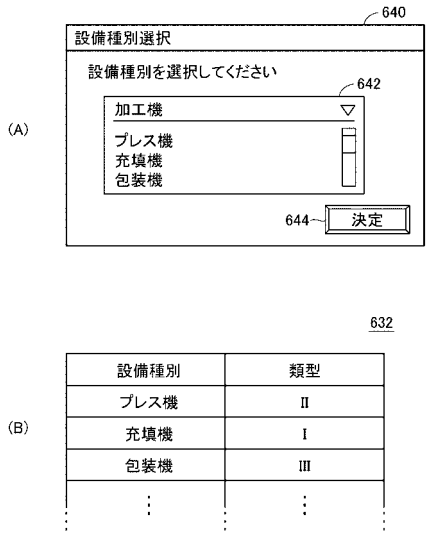
図18

630

| インシデント特性 | 類型I | 類型II | 類型III | |
|---|---|---|---|---|
| 無し(正常運転) | 設備制御:正常運転<br>情報通信:正常運転 | 設備制御:正常運転<br>情報通信:正常運転 | 設備制御:正常運転<br>情報通信:正常運転 | ... |
| レベル1 | 設備制御:正常運転<br>情報通信:縮退A1 | 設備制御:正常運転<br>情報通信:正常運転 | 設備制御:正常運転<br>情報通信:縮退C1 | ... |
| レベル2 | 設備制御:縮退A2<br>情報通信:縮退A3 | 設備制御:縮退B1<br>情報通信:縮退B2 | 設備制御:正常運転<br>情報通信:縮退C2 | ... |
| レベル3 | 設備制御:停止<br>情報通信:縮退A4 | 設備制御:停止<br>情報通信:縮退B3 | 設備制御:縮退C3<br>情報通信:縮退C4 | ... |

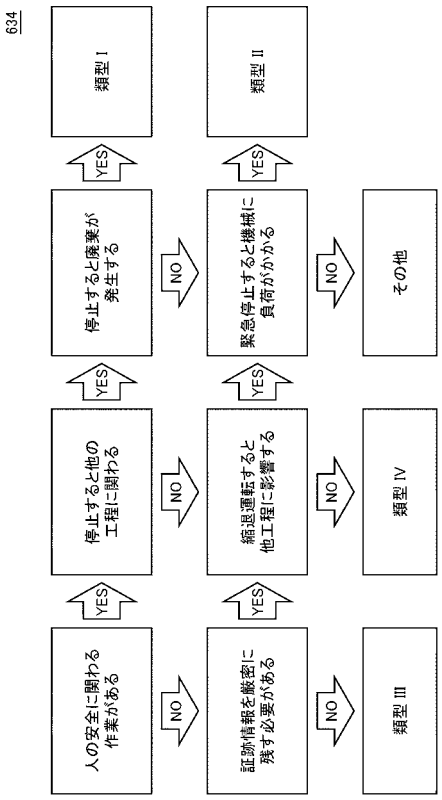
【図１９】

図19



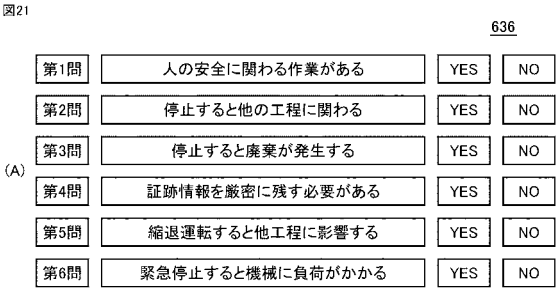

【図２０】

図20




【図２１】

図21



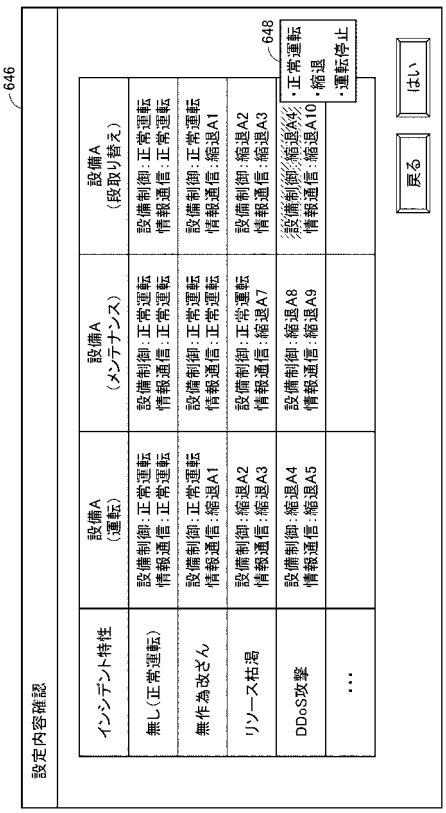

(B)

638

| 1 | 2 | 3 | 4 | 5 | 6 | 類型 |
|---|---|---|---|---|---|---|
| YES | NO | NO | NO | NO | NO | Ⅰ |
| YES | YES | NO | NO | NO | NO | Ⅱ |
| YES | YES | YES | NO | NO | NO | Ⅲ |
| YES | YES | YES | YES | NO | NO | |
| YES | YES | YES | YES | YES | NO | |
| YES | NO | YES | NO | NO | NO | Ⅳ |
| … | … | … | … | … | … | … |

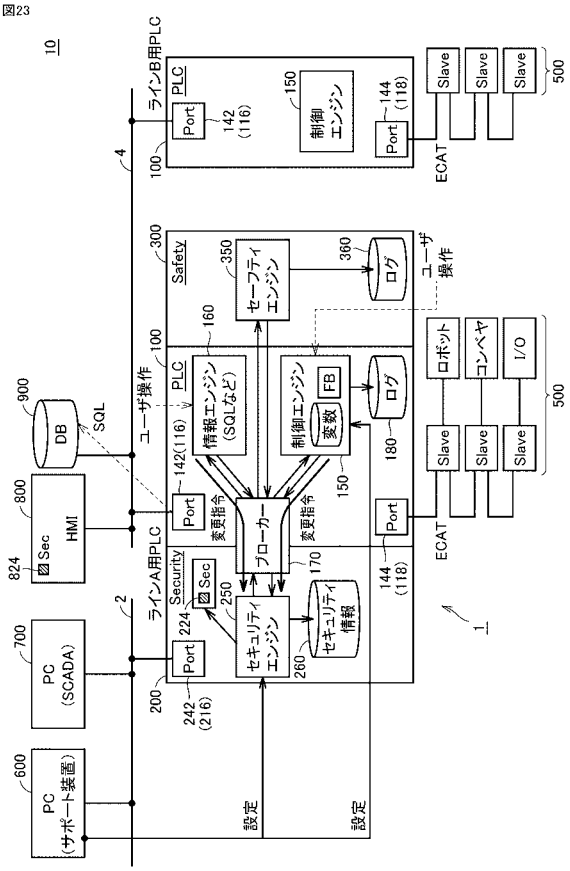
【図２２】

図22



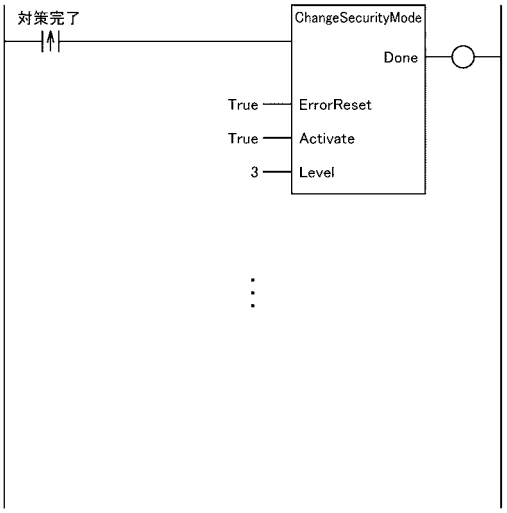
【図２３】

図23



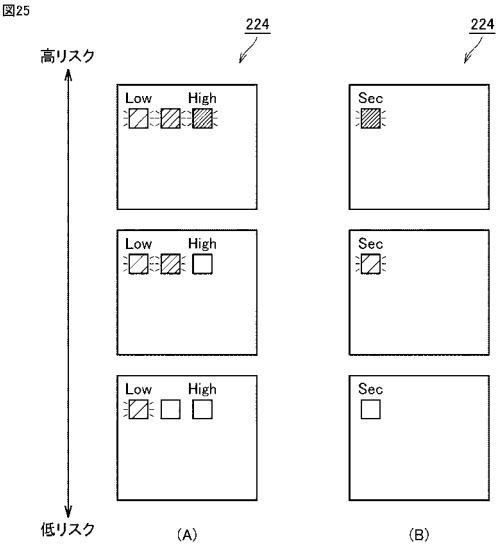

【図２４】

図24



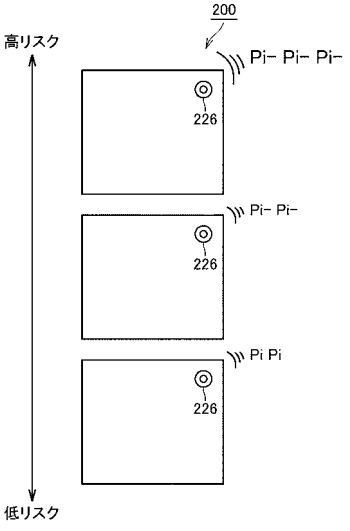

【図２５】

図25



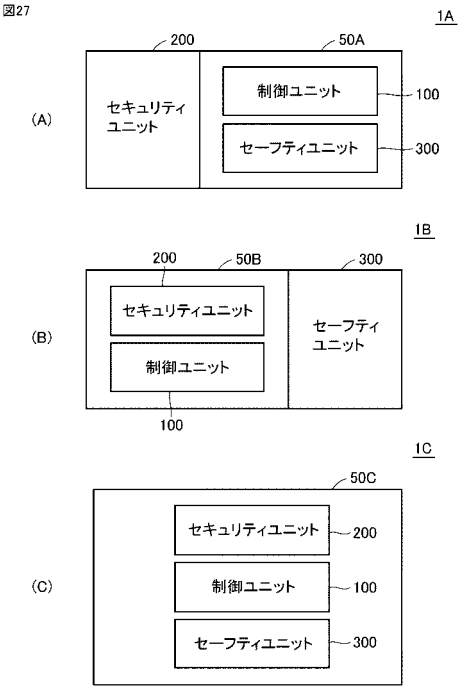

【図２６】

図26



【図２７】

図27


1A
200
50A
セキュリティユニット
制御ユニット
100
セーフティユニット
300
(A)
1B
200
50B
300
セキュリティユニット
制御ユニット
セーフティユニット
100
(B)
1C
50C
セキュリティユニット
200
制御ユニット
100
セーフティユニット
300
(C)

フロントページの続き

(72)発明者　奥村　剛
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　宗田　靖男
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　田原　豊
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
(72)発明者　永田　雄大
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

Ｆターム(参考) 5H220 AA04　BB09　CC03　CC05　CX01　EE01　EE03　HH01　JJ02　JJ12
JJ16　JJ42　JJ53