(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7099352号
(P7099352)

(45)発行日　令和4年7月12日(2022.7.12)

(24)登録日　令和4年7月4日(2022.7.4)

(51)国際特許分類
G05B 19/05 (2006.01)

FI
G05B 19/05 D

請求項の数 11 （全37頁）

(21)出願番号　特願2019-24381(P2019-24381)
(22)出願日　平成31年2月14日(2019.2.14)
(65)公開番号　特開2020-135100(P2020-135100A)
(43)公開日　令和2年8月31日(2020.8.31)
審査請求日　令和2年12月15日(2020.12.15)

(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
特許業務法人深見特許事務所
(72)発明者　片岡 仁之
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　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
審査官　黒田 暁子

最終頁に続く

(54)【発明の名称】　制御システム

(57)【特許請求の範囲】
【請求項１】
制御システムであって、
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、前記制御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、
前記制御ユニットは、前記制御対象を接続する通信ポートと、前記セキュリティユニットを接続する通信コントローラと、を有し、
前記セキュリティユニットは、前記制御システムの外部のネットワークに接続するネットワークコントローラを含み、
前記制御ユニットは、前記通信コントローラと、前記セキュリティユニットと、前記ネットワークコントローラとを介して、前記外部のネットワークに接続し、
前記セキュリティユニットは、さらに、
前記ネットワークコントローラまたは前記通信コントローラを介した通信の内容を含む前記制御システムの稼働状態を示す状態情報を収集する収集手段と、
収集される前記状態情報に基き、前記制御システムにおけるインシデントを検知する検知手段と、
検知された前記インシデントへの対処の情報を通知する通知手段と、を含む、制御システム。
【請求項２】

前記検知手段は、さらに、
収集される前記状態情報が、複数種類のインシデントのそれぞれに対応の条件のうちいずれかの条件を満たすことに基づき、当該インシデントの種類を検知する、請求項１に記載の制御システム。
【請求項３】
前記検知手段は、さらに、
収集される前記状態情報が、前記インシデントが前記制御システムのセキュリティにおよぼす影響の深刻度のそれぞれに対応の条件のうちいずれかの条件を満たすことに基づき、当該インシデントの深刻度を検知する、請求項１または２に記載の制御システム。
【請求項４】
前記対処の情報は、前記深刻度に応じた対処の情報を含む、請求項３に記載の制御システム。
【請求項５】
前記通知手段は、さらに、検知された前記深刻度を通知する、請求項３または４に記載の制御システム。
【請求項６】
前記通知手段は、さらに、
収集される前記状態情報および前記深刻度に基く算出値であるセキュリティリスクを通知する、請求項３から５のいずれか１項に記載の制御システム。
【請求項７】
前記対処の情報は、前記セキュリティリスクに応じた対処の情報を含む、請求項６に記載の制御システム。
【請求項８】
前記対処の情報は、前記制御システムの稼働状態を変化させる対処の情報を含む、請求項１から７のいずれか１項に記載の制御システム。
【請求項９】
前記対処の情報は、前記制御ユニットの構成により異なる、請求項１から８のいずれか１項に記載の制御システム。
【請求項１０】
前記対処の情報は、前記制御ユニットを備えるネットワークの構成により異なる、請求項１から９のいずれか１項に記載の制御システム。
【請求項１１】
前記通知手段は、
前記制御ユニットを含む複数の装置を接続するネットワーク構成の情報に基づき決定した装置に、前記対処の情報を通知する、請求項１から１０のいずれか１項に記載の制御システム。
【発明の詳細な説明】
【技術分野】
【０００１】
本開示は、制御対象を制御する制御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】
ＦＡ（Factory Automation)の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２００２－１６３０１５号公報（特許文献１）は、故障監視画面に、各ＰＬＣ別のボード、シーケンサにおける故障箇所、故障内容、対処方法を表示する故障診断シ

ステムを開示する。
【先行技術文献】
【特許文献】
【０００４】
【文献】特開２００２－１６３０１５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）またはＩｏＴの進歩に伴って、ＦＡの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、ＦＡの制御システムにおいて想定され得るセキュリティ上のインシデント（脅威）の種類も増加している。このようなインシデントに対して運転員などの管理者が何ら対処を講じなければ、ＦＡシステムが停止する可能性がある。したがって、管理者からは、各種のインシデントに適切に対処したいとの要望がある。
【０００６】
その一方で、従来の制御装置においては、例えば特許文献１などのように、故障箇所、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、ＦＡの制御システムにおける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セキュリティ上のインシデントに対処する方法を管理者に通知する仕組みは、何ら提供されていない。
【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インシデント（脅威）に応じて対処の情報を通知するという、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】
本開示の一例は、制御システムであって、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、制御ユニットに接続され、制御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、セキュリティユニットは、制御システムの稼働状態を示す状態情報を収集する収集手段と、収集される状態情報に基き、制御システムにおけるインシデントを検知する検知手段と、検知されたインシデントへの対処の情報を通知する通知手段と、を含む。
【０００９】
上述の開示によれば、インシデントを検知して、検知したインシデントに応じて対処の情報を通知することができる。
【００１０】
上述の開示において、検知手段は、さらに、収集される状態情報が、複数種類のインシデントのそれぞれに対応の条件のうちいずれかの条件を満たすことに基づき、当該インシデントの種類を検知する。
【００１１】
上述の開示によれば、インシデントの種類を検知することができる。
上述の開示において、検知手段は、さらに、収集される状態情報が、インシデントがセキュリティにおよぼす影響の深刻度のそれぞれに対応の条件のうちいずれかの条件を満たすことに基づき、当該インシデントの深刻度を検知する。
【００１２】
上述の開示によれば、インシデントが検知された場合に、当該インシデントがセキュリティにおよぼす影響の深刻度も検知することができる。
【００１３】
上述の開示において、対処の情報は、深刻度に応じた対処の情報を含む。
上述の開示によれば、インシデントの深刻度に応じて対処するための情報を通知すること

ができる。
【００１４】
上述の開示において、通知手段は、さらに、検知された深刻度を通知する。
上述の開示によれば、インシデントが検知された場合に、インシデントがセキュリティにおよぼす影響を定量的な深刻度として通知することができる。
【００１５】
上述の開示において、通知手段は、さらに、収集される状態情報および深刻度に基く算出値であるセキュリティリスクを通知する。
【００１６】
上述の開示によれば、インシデントが検知された場合に、インシデントがセキュリティにおよぼす影響を深刻度に基づくリスクとして、定量的な値を通知することができる。
【００１７】
上述の開示において、対処の情報は、セキュリティリスクに応じた対処の情報を含む。
上述の開示によれば、インシデントについて算出されたセキュリティリスク値に応じて、当該インシデントに対処するための情報を通知することができる。
【００１８】
上述の開示において、対処の情報は、制御システムの稼働状態を変化させる対処の情報を含む。
【００１９】
上述の開示によれば、対処の情報に、制御システムの稼働状態を変化させる対処の情報を含めることができる。したがって、通知された対処の情報に従い、ユーザーが対処を実施する結果、制御システムの稼働状態は、例えばインシデントの影響が小さくなるように変化する。
【００２０】
上述の開示において、対処の情報は、制御ユニットの構成により異なる。
上述の開示によれば、同じインシデントが検知されるとしても、制御ユニットの構成情報により、実施されるべき対処を異ならせることができる。
【００２１】
上述の開示において、対処の情報は、制御ユニットを備えるネットワークの構成により異なる。
【００２２】
上述の開示によれば、同じインシデントが検知されるとしても、制御ユニットを備えるネットワークの構成により、実施されるべき対処を異ならせることができる。
【００２３】
上述の開示において、通知手段は、制御ユニットを含む複数の装置を接続するネットワーク構成の情報に基づき決定した装置に、対処の情報を通知する。
【００２４】
上述の開示によれば、インシデントへの対処の情報の通知先となるべき装置を、制御ユニットが接続されるネットワーク構成に基づき決定することができる。
【発明の効果】
【００２５】
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インシデント（脅威）に応じて対処の情報を通知するという、新たな課題を解決できる。
【図面の簡単な説明】
【００２６】
【図１】本実施の形態に係る制御システム１の構成例を示す外観図である。
【図２】本実施の形態に従う制御システム１が備える制御ユニット１００のハードウェア構成例を示す模式図である。
【図３】本実施の形態に従う制御システム１が備え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】本実施の形態に従う制御システム１が備え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５】本実施の形態に従う制御システム１を備える制御システム１０の典型例を示す模式図である。
【図６】本実施の形態に従う制御システム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。
【図７】本実施の形態に従うセキュリティユニット２００が備える機能構成例を示す模式図である。
【図８】本実施の形態に従うサポート装置６００が備える機能構成例を示す模式図である。
【図９】本発明の実施の形態に係るユーザー情報６２の一例を模式的に示す図である。
【図１０】本発明の実施の形態に係る対処ＤＢ６６の一例を模式的に示す図である。
【図１１】本実施の形態に係る対処ＤＢ６６の他の例を模式的に示す図である。
【図１２】本実施の形態に係るアタックツリー６７の構成の一例を模式的に示す図である。
【図１３】本発明の実施の形態に係るインシデントに対する対処の静的決定の方法を模式的に説明する図である。
【図１４】本発明の実施の形態に係るインシデントに対する対処の動的決定の方法を模式的に説明する図である。
【図１５】図１４（Ａ）のステップＲ３におけるリスク計算の一例を示すフローチャートである。
【図１６】本発明の実施の形態に係る全体処理の一例を示すフローチャートである。
【図１７】本発明の実施の形態に係るセキュリティエンジン２５０が実施する所定処理の一例を模式的に示す図である。
【図１８】本発明の実施の形態に係る静的決定による通知処理の一例を示すフローチャートである。
【図１９】本発明の実施の形態に係る動的決定による通知処理の一例を示すフローチャートである。
【図２０】本発明の実施の形態に係る対処の情報の提示方法を説明するための図である。
【図２１】本発明の実施の形態に係る制御ユニット１００の構成情報に基づく対処のメッセージ６８２に切替を例示する図である。
【図２２】本発明の実施の形態に係る対処メッセージの他の例を模式的に示す図である。
【図２３】本発明の実施の形態に係るセキュリティレベルの変化に応じた対処方法の説明する図である。
【図２４】本発明の実施の形態に係る通知６８の出力部の一例を模式的に示す図である。
【図２５】本発明の実施の形態に係る通知６８の出力部の他の例を模式的に示す図である。
【図２６】本発明の実施の形態に係る通知６８の出力態様の一例を模式的に示す図である。
【発明を実施するための形態】
【００２７】
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。
【００２８】
＜適用例＞
図５を参照して、本発明が適用される場面の一例について説明する。図５は、本実施の形態に従う制御システム１を備える制御システム１０の典型例を示す模式図である。本実施の形態では、制御システム１を、ＦＡに適用する例を示すが、適用対象はＦＡに限定されず、例えばプラントまたは車両等に適用してもよい。
【００２９】
一例として、図５に示す制御システム１０は、ＦＡにおける２つの生産ライン（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。
【００３０】
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が制御システム１を構成する。なお、説明の便宜上、図５には、機能ユニットおよび電源ユニットの記載を省略している。
【００３１】
制御システム１のセキュリティユニット２００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１００に接続されて、制御システム１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は、制御システム１の稼働状態を示す状態情報を収集し、収集される状態情報に基き、制御システム１におけるインシデントを検知し、検知されたインシデントへの対処の情報をユーザー（保守者，管理者）に対して通知する。
【００３２】
ここで、本明細書において、「インシデント」は、何らかのＦＡの制御システム１に対してセキュリティ上の脅威となり得る兆候，現象または異常を意味する。また、稼働状態を示す状態情報は、外部ネットワーク５０との通信を監視する通信監視情報５１１およびデータベース９００のＳＱＬ情報１６１を含む。
【００３３】
セキュリティユニット２００は、制御システム１の稼働状態について収集される状態情報に基づき、セキュリティ上のインシデントを検知して、ユーザーに対して、検知したインシデントへの対処の情報を通知することができる。これにより、ユーザーは、専門知識がなくとも、インシデントの発生を検知して、その対処を実施することができる。
【００３４】
セキュリティユニット２００は、インシデントを検知する場合に、インシデントの種類と、インシデントがセキュリティにおよぼす影響の深刻度、および（収集される状態情報および深刻度に基く算出値である）セキュリティリスクを取得し、取得したこれら情報を、対処の情報に追加して通知する。
【００３５】
これにより、ユーザーは専門知識がなくとも、発生したインシデントの種類とともに、セキュリティ上の深刻度およびリスク値を定量的に把握することが可能となる。以下、本実施の形態のより具体的な応用例について説明する。
【００３６】
＜Ａ．制御システム１＞
本実施の形態に従うＦＡに適用される制御システム１の構成について説明する。
【００３７】
図１は、本実施の形態に係る制御システム１の構成例を示す外観図である。図１を参照して、制御システム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。セキュリティユニット２００は、セキュリティガードユニット（ＳＧＵ：security guard unit）とも呼ばれる。
【００３８】
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。
【００３９】
制御ユニット１００は、制御システム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。
【００４０】
セキュリティユニット２００は、制御ユニット１００に接続され、制御システム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。
【００４１】
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。
【００４２】
機能ユニット４００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。
【００４３】
電源ユニット４５０は、制御システム１が備える各ユニットに対して、所定電圧の電源を供給する。
【００４４】
＜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制御システム１が備える各ユニットのハードウェア構成例について説明する。
【００４５】
（ｂ１：制御ユニット１００）
図２は、本実施の形態に従う制御システム１が備える制御ユニット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）または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、を含む。
【００４６】
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。
【００４７】
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。
【００４８】
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。
【００４９】
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。
【００５０】
メモリカードインターフェイス１１４は、記憶媒体である例えばメモリカード１１５を脱着可能（Detachable）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。
【００５１】
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。
【００５２】
内部バスコントローラ１２２は、制御システム１を構成するセーフティユニット３００、または、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。
【００５３】
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デバイスであり、ユニット表面に配置された１または複数のＬＥＤ（Light Emitting Diode）などで構成される。
【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、これら提供される機能の一部または全部は、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）を用いて実装されてもよい。あるいは、制御ユニット１００の主要部は、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）を用いて実現されてもよい。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制御システム１が備え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または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、ディスプレイ２２５および音声出力のためのスピーカ２２６と、を含む。
【００５６】
プロセッサ２０２は、二次記憶装置２０８またはメモリカードなどのメモリカード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、後述するような各種セキュリティ機能を実現する。主記憶装置２０６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２０８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。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、後述するＯＳ２６０１を含む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２６１０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が脱着可能に構成される。メモリカードインターフェイス２１４は、メモリカードなどのメモリカード２１５に対して制御プログラムまたは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または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、ディスプレイ２２５およびスピーカ２２６は、セキュリティユニット２００からの情報を外部に通知するためにデバイスである。通知される情報は、セキュリティユニット２００の動作状態、または制御システム１において検知されたセキュリティ上のインシデントに応じた対処の情報を含む。インジケータ２２４は、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。ディスプレイ２２５は、ユニット表面に配置されたＬＣＤ（Liquid Crystal Display）を含む。スピーカ２２６は、ユニット表面に配置されて、通知される情報を音声で出力する、またはアラーム音などの管理者の注意喚起のための音声を出力する。

【００６３】

メモリカードインターフェイス２１４は、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メモリカード２１５（例えば、ＤＶＤ（Digital Versatile Disc）などの光学記憶媒体）から、その中に格納されたプログラムを読取り、主記憶装置２０６などにインストールする。主記憶装置２０６に格納されるプログラムは、後述するＯＳ２６０１に加えてセキュリティシステムプログラム２６１０を含む。

【００６４】

セキュリティユニット２００で実行されるセキュリティシステムプログラム２６１０などは、コンピュータ読取可能なメモリカード２１５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、またはサポート装置６００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セキュリティユニット２００が提供する機能は、ＯＳ２６０１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。

【００６５】

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。

【００６６】

（ｂ３：セーフティユニット３００）

図４は、本実施の形態に従う制御システム１が備え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または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。

【００６７】

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、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。

【００６８】

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。

【００６９】

メモリカードインターフェイス３１４は、メモリカード３１５を脱着可能に構成される。メモリカードインターフェイス３１４は、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。

【００７０】

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。

【００７１】

インジケータ３２４は、セーフティユニット３００の動作状態を含む各種の情報を通知するデバイスであり、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。

【００７２】

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。

【００７３】

＜Ｃ．制御システム１０＞

再び図５を参照して、本実施の形態に従う制御システム１を備える制御システム１０の典型例について説明する。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。

【００７４】

制御システム１のセキュリティユニット２００は、通信ポート２４２，２４３（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、通信ポート２４２を介してＳＣＡＤＡ（Supervisory Control And Data Acquisition）装置７００が接続され、また、通信ポート２４３を介してサポート装置６００が接続されている。さらに、セキュリティユニット２００は、通信ポート２４２を介して、ＣＰＵなどのプロセッサ（図示せず）を備えるルーター５１が接続される。ル

ーター５１は、セキュリティユニット２００と外部ネットワーク５０との間の通信を中継する機能およびＦＷ（Fire Wall）５２の機能などを備える。ＦＷ５２は、ユーザー名、パスワード、電子的な証明書などを用いた認証処理、中継するデータ（コンテンツ）のウイルスチェック、ホワイトリストまたはブラックリストを用いたマッチングによる不正通信を検知する処理などを実施する。これにより、ルーター５１は、制御システム１から外部ネットワーク５０へ送信されるデータのうち、認証またはマッチングに成功した正当なデータのみを外部ネットワーク５０へ中継し、また、外部ネットワーク５０から制御システム１へ送信されるデータのうち、認証またはマッチングに成功した正当なデータのみを制御システム１へ中継する。

【００７５】

ルーター５１は、ＥＩＰ（EtherNet/IP）のアクセスを監視する通信監視情報５１１を出力する。ルーター５１は、情報認証またはマッチングに成功しなかった、いわゆる不正アクセスの可能性があるデータから通信監視情報５１１を生成し、生成した通信監視情報５１１を、ポート２４２を介してセキュリティエンジン２５０に送信する。また、ポート２４３もＥＩＰのアクセスを監視する通信監視情報５１１を出力する。ポート２４３は、例えばＮＩＣ（Network Interface Car）を含み、ポート２４３を介して内部の第１ネットワーク２から受信するデータのうち、認証またはマッチングに成功しなかった、いわゆる不正アクセスの可能性があるデータから通信監視情報５１１を生成し、生成した通信監視情報５１１をセキュリティエンジン２５０に送信する。

【００７６】

通信監視情報５１１は、ルーター５１から出力される外部ネットワーク５０からの不正アクセスの可能性がある各データに関する情報、またはポート２４３から出力される内部の第１ネットワーク２からの不正アクセスの可能性がある各データに関する情報を含む。このような情報は、例えば、データの送信元および宛先（アドレスなど）、データ内容（ペイロードなど）および通信時間などを含む。

【００７７】

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、制御システム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ーへ提供する。

【００７８】

ＳＣＡＤＡ装置７００は、制御システム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、制御システム１に対して内部コマンドなどを生成する。ＳＣＡＤＡ装置７００は、制御システム１が扱うデータを収集する機能も有している。

【００７９】

制御システム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が接続され得る。

【００８０】

ＨＭＩ８００は、パーソナルコンピュータに相当する。ＨＭＩ８００は、制御システム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、制御システム１に対して内部コマンドなどを生成する。ＨＭＩ８００は、ＦＡの保守者が携帯可能に構成され得る。データベース９００は、制御システム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。

【００８１】

制御システム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。

【００８２】

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。

【００８３】

ここで、制御システム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。

【００８４】

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。

【００８５】

さらに、制御システム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。

【００８６】

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へ各変数の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二次記憶装置１０８のログデータベース１８０に格納されてもよい。

【００８７】

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。

【００８８】

また、情報エンジン１６０は、データベース９００のアクセス（読出,書込）のために発行されるＳＱＬを監視する。具体的には、発行ＳＱＬを予め登録された正当パターンとマッチングし、照合不一致の結果を含むＳＱＬ情報１６１を生成し、ブローカー１７０を経由してセキュリティエンジン２５０に出力する。したがって、ＳＱＬ情報１６１は、不正ＳＱＬが発行されたことを示す情報、すなわちデータベース９００の改ざんを可能にするＳＱＬインジェクションの情報を示す。本実施の形態では、ＳＱＬ情報１６１は、例えば照合不一致のＳＱＬ、当該ＳＱＬの発行時間および発行元の情報を含む。

【００８９】

セキュリティエンジン２５０は、制御システム１においてセキュリティ上のインシデントが発生したか否かを検知する処理を実施する検知手段と、検知された当該インシデントに対してユーザ（管理者）がとるべき当該インシデントの種類に応じた対処の情報の通知を出力する処理を実施する通知手段とを実現する。また、セキュリティエンジン２５０は、検知されたインシデントの種類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、例えば二次記憶装置２０８にセキュリティ情報２６０として保存される。

【００９０】
セキュリティエンジン２５０は、セキュリティ上のインシデントまたはインシデント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上のインシデントまたはイベントのレベルなどを、インジケータ２２４で通知する。図５では、例えば通知を出力するデバイスとして、インジケータ２２４のみを例示したが、インジケータ２２４のみに限定されず、ディスプレイ２２５またはスピーカ２２６であってもよい。
【００９１】
セーフティエンジン３５０は、制御システム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。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二次記憶装置３０８のログデータベース３６０に格納されてもよい。
【００９２】
ブローカー１７０は、例えば、セキュリティエンジン２５０が何らかのインシデントまたは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よう構成されてもよい。
【００９３】
＜Ｄ：サポート装置６００の構成＞
本実施の形態では、サポート装置６００が制御システム１に対する各種の設定を行う。各種の設定には、インシデントの検知およびインシデントの対処に関する情報の設定が含まれる。
【００９４】
図６は、本実施の形態に従う制御システム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。
【００９５】
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６１５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。
【００９６】
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、制御システム１に対する設定処理などを実現する。
【００９７】
メインメモリ６０４は、ＤＲＡＭまたは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またはＳＳＤなどの不揮発性記憶装置などで構成される。
【００９８】
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、制御システム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。
【００９９】
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からの処理結果を含む各種情報を出力する。
【０１００】
ＵＳＢコントローラ６２０は、ＵＳＢ接続を介して、制御システム１などとの間でデータ

を遣り取りする。
【０１０１】
図６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。
【０１０２】
＜Ｅ：インシデント検知と対処のための機能構成＞
本実施の形態に係るインシデント検知と対処のための機能を、図７を参照して説明する。図７は、本実施の形態に従うセキュリティユニット２００が備える機能構成例を示す模式図である。図７を参照して、セキュリティユニット２００は、記憶部２０９（二次記憶装置２０８または主記憶装置２０６を含んで構成される記憶部２０９）は、インシデントを検知するためにインシデントの種類毎のアタックツリー６７、インシデントの種類毎の対処の情報を登録する対処ＤＢ６６、ＯＳ２６０１、セキュリティシステムプログラム２６１０、および制御システム１にネットワーク接続される装置を識別する情報を含むネットワーク構成情報２６２０を格納する。また、記憶部２０９は、出力される（または出力済）通知６８を保持（格納）するための領域２０７、およびセキュリティユニット２００が収集する情報を格納する領域２０８を含む。また、記憶部２０９は、後述するテーブル２２１を格納する。
【０１０３】
領域２０８には、外部情報７１、ＳＧＵ内部情報７２およびＰＬＣ状態情報７３が格納される。外部情報７１は、制御システム１の外部において取得される情報であって、本実施の形態では、例えばルーター５１からの通信監視情報５１１、情報エンジン１６０からのＳＱＬ情報１６１、外部ネットワーク５０を制御システム１に接続/切断しているかの情報などを含む。
【０１０４】
ＳＧＵ内部情報７２は、セキュリティユニット２００の状態情報（正常、異常）およびメモリカード２１５の脱着の状態などの情報を含む。セキュリティユニット２００の状態情報は、例えばプロセッサの処理負荷の大きさが閾値を超えていれば異常を示し、閾値以下であれば正常を示す。
【０１０５】
ＰＬＣ状態情報７３は、制御ユニット１００の状態情報（正常、異常など）およびメモリカード１１５の脱着の状態などの情報を含む。制御ユニット１００の状態情報は、例えばプロセッサの処理負荷の大きさが閾値を超えていれば異常を示す、閾値以下であれば正常を示す。
【０１０６】
セキュリティシステムプログラム２６１０は、セキュリティエンジン２５０を実現するための情報収集プログラム２６１１、インシデント検知プログラム２６１２、通知処理プログラム２６１３、および通知出力プログラム２６１４を含む。
【０１０７】
プロセッサ２０２は、ＯＳ２６０１の元でセキュリティシステムプログラム２６１０を周期的に実行することによりセキュリティエンジン２５０を実現する。この実行周期は、例えば制御ユニット１００の制御プログラムの実行周期に同期する。
【０１０８】
セキュリティエンジン２５０は、情報収集プログラム２６１１を実行することで実現される情報収集部２０、インシデント検知プログラム２６１２を実行することで実現されるインシデント検知部２１、通知処理プログラム２６１３が実行されることで実現される通知処理部２２、および通知出力プログラム２６１４を実行することで実現される通知出力部２３を含む。通知処理部２２および通知出力部２３は、通知手段を構成する。
【０１０９】

情報収集部２０は、外部情報７１（通信監視情報５１１またはＳＱＬ情報１６１を含む）、セキュリティユニット２００のＳＧＵ内部情報７２、およびブローカー１７０を介して制御ユニット１００からＰＬＣ状態情報７３を収集（受信）し、収集した情報を領域２０８に格納する。情報収集部２０は周期的に、これら情報を収集するので、領域２０８には常に最新の情報が格納される。

【０１１０】

インシデント検知部２１は、領域２０８の情報をセキュリティインシ上のインシデントの種類毎のアタックツリー６７と比較し、比較の結果に基き、制御システム１においてインシデントが発生したかの検知、およびインシデントの種類を検知（判断）する。このインシデント検知の詳細は後述する。

【０１１１】

通知処理部２２は、インシデント検知部２１の検知結果に基き対処ＤＢ６６を検索し、検索の結果に従い、対処ＤＢ６６から、検知されたインシデントに応じた対処の情報を読出し、対処情報の通知６８を生成する。また、通知処理部２２は、通知６８を記憶部２０９の領域２０７に格納する。通知６８は、識別子（インシデントの種類、発生した時間、後述する深刻度Ｐｈｉおよびリスク値など）６８１と、メッセージ６８２を含む。通知出力部２３は、通知６８を出力するようにインジケータ２２４、ディスプレイ２２５およびスピーカ２２６などを含む出力部を制御する。また、通知出力部２３は、メッセージ６８２を含む通知６８を、インシデント検知部２１により対応のインシデントの検知がなされた時系列に出力するよう出力部を制御する。

【０１１２】

本実施の形態では、メッセージ６８２は、インシデントに適切に対処するためのガイダンスまたはインシデントへの何らかの対策をガイドする情報を示す。対処または対策は、制御システム１に対する操作を含み得る。したがって、メッセージ６８２は、制御システム１の稼働状態を変化させる対処または対策の情報を含み得る。

【０１１３】

これにより、インシデントが検知された場合は、ユーザーは、出力部を介して出力される対処の情報（ガイダンスなどのメッセージ６８２）から、最新のガイダンスを確認することができ、またガイドされる対処の行動をすることで、インシデントに対処するよう制御システム１を、稼働状態を変化させながら稼働させることができる。また、対処の情報は、インシデントの検知時間に従い時系列に出力され得て、ユーザーは時系列に変化するインシデントに対処することが可能となる。

【０１１４】

＜Ｆ：対処ＤＢとアタックツリーおよび生成のための機能構成＞

本実施の形態に係る対処ＤＢ６６とアタックツリー６７は、サポート装置６００により作成されて、セキュリティユニット２００に転送される。図８は、本実施の形態に従うサポート装置６００が備える機能構成例を示す模式図である。

【０１１５】

図８を参照して、サポート装置６００のストレージ６１０は、サポート装置６００において生成された対処ＤＢ６６およびインシデントの種類毎のアタックツリー６７を格納するとともに、関連する情報を格納する。関連する情報は、制御システム１を管理するユーザ（またはインシデントに対処可能なユーザ）に関して設定されたユーザー情報６２、制御システム１についてのネットワーク構成情報６３および制御ユニット１００の構成を示すＰＬＣ構成情報６５を含む。

【０１１６】

さらに、ストレージ６１０に、ＯＳ６１０２のもとで実行されるサポートプログラム６１０４は、対処ＤＢ生成プログラム６１１、アタックツリー生成プログラム６１２および転送プログラム６１３を含む。

【０１１７】

プロセッサ６０２は、対処ＤＢ生成プログラム６１１を実行することで実現される対処Ｄ

Ｂ生成部６２１、アタックツリー生成プログラム６１２を実行することで実現されるアタックツリー生成部６２３、および転送プログラム６１３を実行することで実現される転送部６２４を備える。

【０１１８】

対処ＤＢ生成部６２１は、入力部６０６を介して受付けるユーザー操作に従い、対処ＤＢ６６を生成する。対処ＤＢ生成部６２１は、ユーザー情報６２を出力部６０８のディスプレイに表示する。したがって、ユーザーは、ユーザー情報６２を参照しつつ、対処ＤＢ６６を生成するための情報の入力操作を実施することができる。また、対処ＤＢ生成部６２１は、ネットワーク構成情報６３に従い、対処ＤＢ６６の内容（メッセージ６８２など）を異ならせる。また、対処ＤＢ生成部６２１は、ＰＬＣ構成情報６５に従い、対処ＤＢ６６の内容（メッセージ６８２など）を異ならせる。

【０１１９】

図９は、本発明の実施の形態に係るユーザー情報６２の一例を模式的に示す図である。図１０は、本発明の実施の形態に係る対処ＤＢ６６の一例を模式的に示す図である。図９を参照して、ユーザー情報６２は、インシデントの深刻度Ｐｈのそれぞれに関連付けて、当該深刻度Ｐｈｉ（ｉ＝１，２，３、・・・）であるインシデントを通知またはインシデントに対処するべきユーザーの識別子６２ａ、当該ユーザーが属する組織名６２ｂ、ユーザーと通信するための電話番号６２ｃおよび電子メールのアドレス６２ｄを含む。

【０１２０】

本実施の形態では、深刻度Ｐｈｉは、インシデントにより、制御システム１のセキュリティに及ぼされる危険度（損失が及ぶ可能性の程度）、緊急度（対処を急がなければならない程度）などの影響の程度を表す。図９の下段に示されるように深刻度Ｐｈｉは例えば「高」（Ｐｈ３）、「中」（Ｐｈ２）および「低」（Ｐｈ１）のいずれかをとり得る。また、図９の下段では、深刻度Ｐｈｉの各レベルに関連付けて、当該レベルの深刻度Ｐｈｉが検出された場合に対処の通知がなされるタイミングおよび当該対処が実施されることで制御システム１が移し得る状態などが示される。なお、本実施の形態では、深刻度をＰｈ１～Ｐｈ３の３段階としているが、段階は３段階に限定されない。

【０１２１】

（ｆ１．対処ＤＢの構成）

図１０を参照して、対処ＤＢ生成部６２１がユーザー操作に基づき生成する対処ＤＢ６６は、想定されるインシデントの種類６８０毎に、当該種類に関連付けて、インシデントの深刻度Ｐｈｉと、各深刻度Ｐｈｉを細分化した値で示すリスク値６８１および対処のメッセージ６８２とを含む。図１０では、例えば、“なりすまし”のインシデントについての対処ＤＢが示されている。図１０に示すように、各深刻度Ｐｈｉ（リスク値６８１）が高くなるほど、メッセージ６８２は、通知の宛先としてより上位組織の責任者（ユーザー）を指定するデータが含まれ、また、より高い危険度または緊急度を示すメッセージが含まれるように対処ＤＢ６６が生成される。なお、後述するように、リスク値６８１は、セキュリティユニット２００による動的決定が実施される場合に参照される。

【０１２２】

図１１は、本実施の形態に係る対処ＤＢ６６の他の例を模式的に示す図である。本実施の形態に係る制御システム１における想定されるインシデントは、図１０の“なりすまし”に限定されず、図１１に示すように、”なりすまし”に追加して、“ＤｏＳ攻撃”および“改ざん”などのインシデントに対応した対処ＤＢも生成することができる。図１１の対処ＤＢ６６も、インシデント毎に、当該インシデントの各深刻度Ｐｈｉ（リスク値６８１）が高くなるほど、メッセージ６８２は、通知の宛先としてより上位組織の責任者（ユーザー）を指定するデータが含まれ、また、より高い危険度または緊急度を示すメッセージが含まれるように生成される。

【０１２３】

（ｆ２．アタックツリーの構成）

アタックツリー生成部６２３は、入力部６０６を介したユーザー操作に基づきアタックツ

リー６７を生成する。図１２は、本実施の形態に係るアタックツリー６７の構成の一例を模式的に示す図である。アタックツリー生成部６２３は、インシデントの種類毎にアタックツリー６７を生成する。図１２には、例えば、“ＤｏＳ攻撃”に対応のアタックツリー６７が示される。図１２のアタックツリー６７は、３階層（深刻度Ｐｈ１～Ｐｈ３）の深さを有した木構造で示される。この木構造は、階層毎に配置される葉要素６７１、６７２および６７３、ならびに木構造の最上位の要素である根要素６７０を含む。階層間の葉要素どうし、および最上位階層の葉要素と根要素６７０どうしは、枝６７５で繋がれる。図１２のアタックツリー６７では、各葉要素には、制御システム１で発生し得るイベントであって、当該インシデント（“ＤｏＳ攻撃”）の要因となり得るイベントが発生したことを判定するための条件が割当てられる。

【０１２４】

図１２のアタックツリー６７によれば、各葉要素に割当てられる条件は、通信ポートに対する同一送信元からのデータ受信であって、制御システム１に対する不正アクセスの可能性があるデータの単位時間当たりの受信回数に基づく条件を示す。この不正アクセスの有無と単位時間当たりの回数は、ルーター５１からの通信監視情報５１１に基づくことで取得することができる。例えば、深刻度Ｐｈ１の葉要素６７３の条件（Ｋ回≦単位時間あたりの不正アクセス回数＜Ｍ回）が満たされると、インシデントは深刻度Ｐｈ１の状態となる。さらに、不正アクセス回数が増加すると、枝６７５を辿り上位階層（深刻度Ｐｈ２）の葉要素６７２の条件が判断される。例えば、深刻度Ｐｈ２の葉要素６７２の条件（Ｍ回≦単位時間あたりの不正アクセス回数＜Ｎ回）が満たされると、インシデントは深刻度Ｐｈ２の状態となる。さらに、不正アクセス回数が増加すると、枝６７５を辿り深刻度Ｐｈ３の葉要素６７１の条件（Ｎ回≦単位時間あたりの不正アクセス回数）が満たされると、インシデントは深刻度Ｐｈ３の状態となる。このように、アタックツリー６７の下位階層から上位階層へ枝６７５を辿りながら各階層の葉要素の条件、すなわち各深刻度Ｐｈｉに対応の条件が満たされるか否かを判定することにより、当該アタックツリー６７のインシデント（“ＤｏＳ攻撃”）の深刻度Ｐｈｉを決定することができる。

【０１２５】

同様にして、“改ざん”に対応のアタックツリー６７も生成することができる。“改ざん”のアタックツリー６７では、各葉要素に割当てられる深刻度Ｐｈｉに対応する条件は、例えば、データベース９００を不正操作する可能性があるＳＱＬインジェクションの単位時間当たりに発行された回数に基づく条件を示す。インシデント検知部２１は、ＳＱＬインジェクションの発行の有無と単位時間当たりの発行回数は、情報エンジン１６０からのＳＱＬ情報１６１に基づくことで取得する。このように、“改ざん”のアタックツリー６７においても、下位階層から上位階層へ枝６７５を辿りながら、ＳＱＬ情報１６１が各階層の葉要素における深刻度Ｐｈｉに対応の条件を満たすか否かを判定することにより、当該アタックツリー６７のインシデント（“改ざん”）の深刻度Ｐｈｉを決定することができる。

【０１２６】

なお、図１２に示すアタックツリー６７の木構造は例示にすぎず、階層の数、葉要素の数などは変更可能である。また、他の種類のインシデント（例えば、“なりすまし”）であっても、アタックツリー生成部６２３は、図１２と同様のアタックツリー６７を生成することができる。

【０１２７】

対処ＤＢ生成部６２１が生成した対処ＤＢ６６およびアタックツリー生成部６２３が生成したアタックツリー６７は、ストレージ６１０に格納される。また、転送部６２４は、対処ＤＢ６６およびアタックツリー６７を、セキュリティユニット２００に転送する。セキュリティユニット２００は、転送部６２４から、各種のインシデントについての対処ＤＢ６６およびアタックツリー６７を受信し、図７の記憶部２０９に格納する。

【０１２８】

＜Ｇ．インシデント検知部２１の検知方法＞

本実施の形態に係るセキュリティユニット２００によるインシデントの検知の方法を説明

する。本実施の形態に係るインシデントに対する対処の情報（メッセージ６８２）を、静的に決定する静的決定と、動的に決定する動的決定を含む。ユーザーがセキュリティユニット２００に対し操作することで、セキュリティユニット２００に静的決定または動的決定のいずれかを設定する（切り替える）ことができる。静的決定は、制御システム１の稼働状態を示す状態情報のうちのインシデントを検知するための所定情報を用いて判定した深刻度Ｐｈｉに基づき対処を決定する方法である。これに対して、動的決定は所定情報に基づく深刻度Ｐｈｉと稼働状態を示す状態情報とを用いてインシデントの深刻度（後述するリスク値６８１）を検知する方法である。

【０１２９】

図１３は、本発明の実施の形態に係るインシデントに対する対処の静的決定の方法を模式的に説明する図である。図１４は、本発明の実施の形態に係るインシデントに対する対処の動的決定の方法を模式的に説明する図である。図１３と図１４では、インシデントとして例えば“ＤｏＳ攻撃”のケースが例示される。

【０１３０】

（ｇ１．静的決定）

図１３（Ａ）は、図１２のアタックツリー６７を簡略化されたものであり、各階層（深刻度Ｐｈ１～Ｐｈ３の各階層）の葉要素のみを示す。図１３（Ｂ）は、“ＤｏＳ攻撃”の対処ＤＢ６６のうち、リスク値６８１が省略されて、インシデントの種類６８０、深刻度Ｐｈおよびメッセージ６８２の項目を含んでいる。静的決定が実施される場合、インシデント検知部２１は、情報収集部２０により収集された通信監視情報５１１に基き図１３（Ａ）のアタックツリー６７の各階層の条件が満たされるかを判断し、判断結果に基づき枝６７５を辿ることで深刻度Ｐｈｉを判断する。通知処理部２２は、インシデント検知部２１からの出力（すなわち、インシデントの種類（“ＤｏＳ攻撃”）と深刻度Ｐｈｉ）に基き図１３（Ｂ）のインシデントの種類（“ＤｏＳ攻撃”）に対応した対処ＤＢ６６を検索する。通知処理部２２は、検索により、対処ＤＢ６６から深刻度Ｐｈｉに対応したメッセージ６８２を読出す。通知出力部２３は、通知処理部２２の出力（メッセージ６８２）を出力する。

【０１３１】

このように静的決定によれば、稼働状態を示す状態情報のうちインシデントの検知のための所定情報（例えば、通信監視情報５１１）のみを用いてインシデント（種類と深刻度Ｐｈｉ）が検知されて、ユーザーに対して深刻度Ｐｈｉに一意に対応付けられた対処の情報（メッセージ６８２）を通知することができる。

【０１３２】

（ｇ２．動的決定）

これに対して、動的決定が実施される場合は、静的決定と同様にして深刻度Ｐｈｉが判定されるが、判定された深刻度Ｐｈｉに応じた対処の情報を、情報収集部２０が収集する状態情報により異ならせることができる。このような動的決定を、図１４を参照して説明する。

【０１３３】

図１４（Ａ）は、動的決定によるリスク値６８１の算出と、対処の情報（メッセージ６８２）の決定の手順を持模式的に示すフローチャートである。図１４（Ｂ）は、“ＤｏＳ攻撃”の対処ＤＢ６６であって、インシデントの種類６８０、深刻度Ｐｈｉ、リスク値６８１およびメッセージ６８２の項目を含んでいる。各深刻度Ｐｈｉのリスク値６８１は、深刻度Ｐｈｉを複数のレベルに細分化した値であって、リスク値６８１の各レベルに、メッセージ６８２が対応付けられている。

【０１３４】

図１４（Ａ）を参照して、まず、インシデント検知部２１は図１３（Ａ）のアタックツリー６７と所定情報（通信監視情報５１１）とを用いてインシデントの種類と深刻度Ｐｈｉを検知する（ステップＲ１）。この検知は、上記に述べた静的決定と同様である。

【０１３５】

次に、通知処理部２２は、稼働状態の情報に基づきリスク値６８１を計算する（ステップ

Ｒ３）。本実施の形態では、この稼働状態の情報は、例えば外部情報７１、ＳＧＵ内部情報７２およびＰＬＣ状態情報７３を含む。ステップＲ３のリスク計算の詳細は後述する。

【０１３６】

通知処理部２２は、ステップＲ３による算出されたリスク値６８１に基き図１４（Ｂ）の対処ＤＢ６６を検索し、対処ＤＢ６６から当該リスク値６８１に対応した対処の情報（メッセージ６８２）を読出す（ステップＲ５）。通知出力部２３は、対処ＤＢ６６から読出された対処の情報を、出力部を介して通知する（ステップＲ７）。

【０１３７】

（ｇ２－１．リスク値の計算）

図１５は、図１４（Ａ）のステップＲ３におけるリスク計算の一例を示すフローチャートである。図１５を参照して、リスク値６８１の算出を説明する。まず、通知処理部２２は、リスク計算のための変数ｋに値０をセットする（ステップＲ３１）。通知処理部２２は、インシデント検知部２１により検出されたインシデントの種類を判定する(ステップＲ３３）。種類は“ＤｏＳ攻撃”と判断されるとステップＲ３５に移行し、“改ざん”と判断されるとステップＲ４９に移行し、“なりすまし”と判断されるとステップＲ６３に移行する。ここでは、“ＤｏＳ攻撃”と“改ざん”のリスク値の算出を説明するが、“なりすまし”であっても、同様の手順でリスク値６８１を算出することができる。

【０１３８】

まず、“ＤｏＳ攻撃”の場合、通知処理部２２は、外部情報７１に基き制御システム１に外部ネットワーク５０が接続されているか否かを判断する（ステップＲ３５）。接続されていると判断すると（ステップＲ３５でＹＥＳ）、通知処理部２２は変数ｋの値に１０を加算（ｋ＝ｋ＋１０）し（ステップＲ３９）、接続されていないと判断すると（ステップＲ３５でＮＯ）、通知処理部２２は変数ｋの値に５を加算（ｋ＝ｋ＋５）する（ステップＲ３７）。

【０１３９】

また、通知処理部２２は、ＳＧＵ内部情報７２またはＰＬＣ状態情報７３に基きプロセッサの負荷が高いか否かを判断する（ステップＲ４１）。負荷が高いと判断すると（ステップＲ４１でＹＥＳ）、通知処理部２２は変数ｋの値に５を加算（ｋ＝ｋ＋５）し（ステップＲ４５）、負荷は高くないと判断すると（ステップＲ４１でＮＯ）、通知処理部２２は変数ｋの値に０を加算（ｋ＝ｋ＋０）する（ステップＲ４３）。その後、通知処理部２２は、深刻度Ｐｈｉの値（ｉ＝１、２、３のいずれか）を用いて（リスク値＝ｉ×ｋ）を算出する（ステップＲ４７）。その後、元の処理に戻る。

【０１４０】

同様に、“改ざん”の場合、通知処理部２２は、外部情報７１に基き制御システム１に外部ネットワーク５０が接続されているか否かを判断し（ステップＲ４９）、接続されていると判断すると（ステップＲ４９でＹＥＳ）、変数ｋの値に１０を加算（ｋ＝ｋ＋１０）し（ステップＲ５３）、接続されていないと判断すると（ステップＲ４９でＮＯ）、変数ｋの値に５を加算（ｋ＝ｋ＋５）する（ステップＲ５１）。

【０１４１】

また、通知処理部２２は、ＳＧＵ内部情報７２またはＰＬＣ状態情報７３に基き、制御システム１に外部から装置（ＰＣまたは外部記憶媒体）などが装着されているかを判断する（ステップＲ５５）。装着されていると判断すると（ステップＲ５５でＹＥＳ）、通知処理部２２は変数ｋの値に５を加算（ｋ＝ｋ＋５）し（ステップＲ５９）、装着されていないと判断すると（ステップＲ５５でＮＯ）、通知処理部２２は変数ｋの値に０を加算（ｋ＝ｋ＋０）する（ステップＲ５７）。その後、通知処理部２２は、深刻度Ｐｈｉの値（ｉ＝１、２、３のいずれか）を用いて（リスク値＝ｉ×ｋ）を算出する（ステップＲ６１）。その後、元の処理に戻る。

【０１４２】

このように、リアルタイムに収集される稼働状態の情報を用いることで、インシデントの種類およびその深刻度Ｐｈｉに応じたリスク値６８１を算出することができる。また、イ

ンシデントの種類に応じて、算出に用いる稼働状態を示す情報の種類を異ならせることで、インシデントの種類に応じたリスク値の算出が可能となる。

【０１４３】

例えば、“ＤｏＳ攻撃”では、インターネットを含む外部ネットワーク５０が攻撃のルートとなっている場合は、そうでない場合に比較して一般的にセキュリティに及ぼされるリスクが大きい。したがって、図１５では、外部情報７１から外部ネットワーク５０が接続されていると判断される場合は（ステップＲ３５でＹＥＳ）、外部ネットワーク５０が接続されていない場合に比較して、リスク値を算出するための係数（変数ｋ）に大きい値を設定する（ステップＲ３９）。また、“ＤｏＳ攻撃”では、攻撃を受けている装置のリソースが過剰に消費されてプロセッサの負荷が高くなり、本来の制御プログラムの実行に悪影響が及ぶリスクがある。したがって、図１５では、プロセッサの負荷が高い場合は（ステップＲ４１でＹＥＳ）、そうでない場合に比較して、リスク値を算出するための係数（変数ｋ）に大きい値を設定する（ステップＲ４５）。同様に、“改ざん”においても、外部ネットワーク５０が接続されている場合（ステップＲ４９でＹＥＳ）および外部装置または記憶媒体が装着されている場合（ステップＲ５５でＹＥＳ）は、そうでない場合に比較して、リスク値を算出する係数（変数ｋ）に大きい値を設定する（ステップＲ５３、ステップＲ５９）。

【０１４４】

このように、情報収集部２０が制御システム１の稼働中に周期的に稼働状態の情報を収集することで、セキュリティエンジン２５０は、セキュリティエンジン２５０の処理と同時に（リアルタイムに）収集される稼働状態の情報を用いてリスク値６８１を算出することができる。したがって、インシデントの深刻度Ｐｈｉに応じたリスク値６８１を制御システム１の稼働状態に応じた値に動的に決定することができ、また、インシデントの種類のリスク値６８１に応じた通知６８も動的に切替えて提供することができる。

【０１４５】

＜Ｈ．全対処理＞

図１６は、本発明の実施の形態に係る全体処理の一例を示すフローチャートである。セキュリティユニット２００のＣＰＵ２０１は、図１６の処理を、周期的に繰り返し実行する。まず、インシデント検知部２１は、情報収集部２０が収集する情報のうち、所定情報に基づきアタックツリー６７に従い、インシデントの有無を検知する（ステップＴ１）。インシデントが検知されない場合（ステップＴ１でＮＯ）、処理は終了するが、検知された場合（ステップＴ１でＹＥＳ）、インシデント検知部２１は、アタックツリー６７を辿ることによりインシデントの種類および深刻度Ｐｈｉを決定する（ステップＴ３）。通知処理部２２は、インシデント検知部２１からの出力に基づき、対処ＤＢ６６を検索することにより、対応する対処の情報（メッセージ６８２）を読出す（ステップＴ５）。通知出力部２３は、読出された対処の情報を、出力部を介して通知する（ステップＴ７）。ユーザーは出力部を介して通知された対処の情報に従い、インシデントに対して対処を実施する（ステップＴ１３）。これにより、制御システム１のセキュリティのレベルが変更される。

【０１４６】

セキュリティエンジン２５０は、所定処理を実施するか否かを判断する（ステップＴ９）。例えば、この判断はユーザー操作に基づき実施される。所定処理を実施しないと判断したとき（ステップＴ９でＹＥＳ）処理は終了するが、実施すると判断した場合（ステップＴ９でＮＯ）、所定処理を実施する（ステップＴ１１）。

【０１４７】

図１７は、本発明の実施の形態に係るセキュリティエンジン２５０が実施する所定処理の一例を模式的に示す図である。所定処理は、制御システム１を備えるネットワーク構成により異ならせることができる。例えば、図１７（Ａ）のように、外部ネットワーク５０には、１台の制御システム１が接続されるネットワーク構成の場合は、通常時は、制御システム１はログ（インシデント検知のための情報（外部情報７１、ＳＧＵ内部情報７２およびＰＬＣ状態情報７３など）を外部ネットワーク５０上のクラウドサーバ（図示せず）に

転送して格納する（ステップＳＳ１）。インシデントが検知される場合に、ステップＴ１１の所定処理では、セキュリティエンジン２５０は外部ネットワーク５０との接続を完全に遮断し（ステップＳＳ３）、当該ログをトレーサビリティのために記憶部２０９の所定領域に格納する（ステップＳＳ２）。また、図１７（Ｂ）のように、複数台（例えば２台）の制御システム１が外部ネットワーク５０に接続されるネットワーク構成の場合は、通常時は、各制御システム１はログ（インシデント検知のための情報（外部情報７１、ＳＧＵ内部情報７２およびＰＬＣ状態情報７３など）を外部ネットワーク５０上のクラウドサーバ（図示せず）に転送して格納する。インシデントが検知される場合に、ステップＴ１１の所定処理では、セキュリティエンジン２５０は外部ネットワーク５０と断続的に接続する（ステップＳＳ４）ことで、インシデントが検知されていない他の制御システム１（制御ユニット１００）には、外部ネットワーク５０に接続できる環境を提供することができて、他の制御システム１の運転に対する影響を少なくできる。

【０１４８】

上記のステップＴ５では、上記に述べた静的決定または動的決定に従い対処の情報（メッセージ６８２）が決定（読出）される。この具体的な処理を、図１８と図１９を参照し説明する。

【０１４９】

（ｈ１．静的決定による通知処理）

まず、静的決定を含む通知処理を説明する。図１８は、本発明の実施の形態に係る静的決定による通知処理の一例を示すフローチャートである。図１８を参照して、通知処理部２２による静的決定を含む処理を説明する。まず、インシデント検知部２１は、所定情報（通信監視情報５１１、またはＳＱＬ情報１６１など）に基き、アタックツリー６７に従いインシデントの発生の有無を検知するとともに、インシデントの種類および深刻度Ｐｈｉを決定する（ステップＳ３）。

【０１５０】

通知処理部２２は、インシデント検知部２１からの出力に基き、インシデントの種類に対応の対処ＤＢ６６を特定し、深刻度Ｐｈｉに基き特定した対処ＤＢ６６を検索することにより、対処ＤＢ６６から深刻度Ｐｈｉに対応のメッセージ６８２を読出す（ステップＳ５）。

【０１５１】

通知処理部２２は、読出されたメッセージ６８２が以前に通知されているかを判断する（ステップＳ７）。具体的には、通知処理部２２は、インシデント検知部２１によるインシデントの種類と検知時間を、記憶部２０９の領域２０７の各通知６８のＩＤ６８３（インシデントの種類と時間）と照合し、照合一致したＩＤ６８３の通知６８がないとき、読出されたメッセージ６８２は以前に通知されていないと判断する（ステップＳ７でＹＥＳ）。通知処理部２２は、読出されたメッセージ６８２から通知６８を生成し、出力部を介して通知するように、通知出力部２３を制御する（ステップＳ９）。

【０１５２】

一方、上記の照合一致した通知６８があるとき、通知処理部２２は読出されたメッセージ６８２は以前に通知されていると判断し（ステップＳ７でＮＯ）、通知処理部２２は、領域２０７の通知６８の検索の結果に基き、ステップＳ３で検知された種類と同一種類のインシデントに対応する２つ以上のメッセージ６８２が通知されているかを判断する（ステップＳ１１）。

【０１５３】

通知処理部２２は、２つ以上のメッセージ６８２が既に通知されていると判断すると（ステップＳ１１でＹＥＳ）、ステップＳ５で読出されたメッセージ６８２が新規であるか否かを判断する（ステップＳ１３）。具体的には、通知処理部２２は、当該読出されたメッセージ６８２を上記の照合一致した通知６８のメッセージ６８２と照合し、照合結果に基き判断する。通知処理部２２は、当該照合結果に基き、当該読出されたメッセージ６８２は新規ではなく既に通知されていると判断すると（ステップＳ１３でＮＯ）、読出された

メッセージ６８２から通知６８を生成し、生成された通知６８を出力部において既存のメッセージ６８２と並列に通知されるように、通知出力部２３を制御する（ステップＳ１７）。

【０１５４】

一方、通知処理部２２は、ステップＳ５で読出されたメッセージ６８２は新規であり未だ通知されていないと判断すると（ステップＳ１３でＹＥＳ）、読出されたメッセージ６８２から通知６８を生成し、生成された通知６８を出力部において既存のメッセージ６８２と並列に通知されるように、通知出力部２３を制御する（ステップＳ１５）。

【０１５５】

また、上記のステップＳ５で読出されたメッセージ６８２は新規ではないと判断されたとき（ステップＳ１３でＮＯ）、メッセージ６８２の上書きが実施されてもよい（ステップＳ１７）。例えば、通知処理部２２は、生成された通知６８が、既存のメッセージ６８２のうちの１つ（例えば、識別子６８３が最も最近の時間を示す（最新の）メッセージ６８２）に上書きされて出力されるよう、通知出力部２３を制御してもよい。

【０１５６】

また、通知処理部２２は、２つ以上のメッセージ６８２は通知されていない（ステップＳ１１でＮＯ）、すなわち以前に通知されているメッセージ６８２は１つであると判断すると、深刻度Ｐｈｉを照合（比較）する。具体的には、通知処理部２２は、ステップＳ５で読出されたメッセージ６８２と以前に通知されているメッセージ６８２との両者の深刻度Ｐｈｉを照合し、照合結果に基き両者は一致するかを判断する（ステップＳ１９）。両方の深刻度Ｐｈｉは同じと判断される場合（ステップＳ１９でＹＥＳ）、通知処理部２２は、ステップＳ５で読出されたメッセージ６８２から通知６８を生成し、生成された通知６８を出力部において既存のメッセージ６８２に上書きして通知するよう、通知出力部２３を制御する（ステップＳ２１）。

【０１５７】

一方、通知処理部２２は、両方の深刻度Ｐｈｉは異なると判断すると（ステップＳ１９でＮＯ）、すなわち、ステップＳ５で読出されたメッセージ６８２は新規であり未だ通知されていないと判断すると、読出されたメッセージ６８２から通知６８を生成し、生成された通知６８を出力部において既存のメッセージ６８２と並列に（すなわち、時系列で）出力されるよう、通知出力部２３を制御する（ステップＳ２３）。

【０１５８】

（ｈ２．動的決定による通知処理）

次に、動的決定を含む通知処理を説明する。図１９は、本発明の実施の形態に係る動的決定による通知処理の一例を示すフローチャートである。図１９を参照して、通知処理部２２による動的決定を含む処理を説明する。図１９の処理は、図１８の処理に比較して、図１４（Ａ）のリスク値６８１を算出するステップＲ３を追加し、また図１８のステップＳ５を図１４（Ａ）のリスク値６８１に基き対処ＤＢ６６を検索するためのステップＲ５に変更し、また図１８のステップＳ１９を、リスク値６８１を用いた処理のステップＳ１９ａに変更した点が異なる。図１９の他の処理は図１８の処理と同様である。したがって、他の処理の説明は繰返さない。

【０１５９】

図１９では、通知処理部２２は、インシデント検知部２１の出力（インシデントの種類と深刻度Ｐｈｉ）に基き、リスク値を計算する（ステップＲ３）。通知処理部２２は、算出されたリスク値６８１に基き対処ＤＢ６６を検索して、リスク値６８１に対応するメッセージ６８２を読出す（ステップＲ５）。また、ステップＳ１９ａでは、ステップＲ５で読出されたメッセージ６８２の深刻度Ｐｈｉ，リスク値６８１は、既に通知されているメッセージ６８２の深刻度Ｐｈｉ，リスク値６８１と一致するかの判断がなされる。

【０１６０】

図１８または図１９の通知処理部２２および通知出力部２３の処理によれば、通知されるメッセージ６８２が示す対処は、制御システム１の稼働状態を変化させる対処の情報（例

えば、制御システム１に対する操作）を含む。したがって、通知されるメッセージ６８２に従いユーザーが対処を実施した場合は、インシデントの深刻度Ｐｈｉまたはリスク値６８１は小さくなることが予想される。したがって、ステップＳ１７またはステップＳ２３などで通知されるメッセージ６８２の深刻度Ｐｈｉまたはリスク値６８１は時間を追って小さくなる。この場合、ユーザーは、通知されるメッセージ６８２（または、通知される深刻度Ｐｈｉ、リスク値６８１）から、インシデントへの対処に成功していることを、リアルタイムに確認することができる。また、逆に、通知されるメッセージ６８２の深刻度Ｐｈｉまたはリスク値６８１が時間を追って大きくなっている、または変化しない場合、ユーザーはインシデントへの対処が十分になされていないことを、リアルタイムに確認することができる。

【０１６１】

＜Ｉ．通知の方法＞

本発明の実施の形態に係る通知出力部２３は、通知処理部２２は出力するメッセージ６８２および識別子６８３を含む通知６８を出力するように、出力部を制御する。これにより、インシデントへの対処の情報であるメッセージ６８２を、出力部を介してユーザーに提示することができる。図２０は、本発明の実施の形態に係る対処の情報の提示方法を説明するための図である。

【０１６２】

図２０を参照して、本実施の形態では、対処の情報を通知する出力部の装置（媒体）として、ＬＥＤ、７セグメントディスプレイ、パトランプ２３１、音、振動、ＨＭＩ、ＰＣツールなどを含む。ＬＥＤは通知（インシデントの種類、深刻度Ｐｈｉ、リスク値）を点灯色または点滅態様で出力する。また、７セグメントディスプレイは通知（インシデントの種類、深刻度Ｐｈｉ、リスク値）を十進法のアラビア数字を、七つの画（例えば、画はＬＥＤで構成される）で表示し、また、ＬＥＤを点滅態様で出力する。

【０１６３】

パトランプ２３１は、通知をライトの点灯色、または点滅（点灯）パターンなどの組合せで出力する。音としては、ビープ音を用いることができて、ビープ音の周期、大きさ、高さなどの組合せで通知を出力する。振動としては、超音波振動または物理的な振動を用いることができて、振動の異なる周期を組合わせることで、通知を出力することができる。また、出力部の装置（媒体）として、ＨＭＩ８００またはＰＣ６００を用いる場合は、ＨＭＩ８００またはＰＣ６００の画面に通知をポップアップ表示する、またはＨＭＩ８００またはＰＣ６００に許可される操作を通知の内容に応じて異ならせることで、ユーザーに対して通知を提示する。

【０１６４】

＜Ｊ．構成に基づく通知の方法＞

本実施の形態では、対処ＤＢ６６が有する対処のメッセージ６８２は、制御ユニット１００の構成、または制御ユニット１００を備えるネットワークの構成により切替えることができる。図２１は、本発明の実施の形態に係る制御ユニット１００の構成情報に基づく対処のメッセージ６８２に切替を例示する図である。図２１を参照して、制御ユニット１００の構成に基き対処ＤＢ６６の切替えを説明する。本実施の形態では、制御ユニット１００の主記憶装置１０６のＳＲＡＭなどには、制御ユニット１００の構成を示す構成情報であるコンフィグデータ（コンフィグレーションデータの略）１０６１が格納される。例えば、コンフィグデータ１０６１は、制御ユニット１００は、無人の工場のＦＡに適用される、または有人の工場のＦＡに適用されるなどの区別を示す情報を有する。セキュリティユニット２００は、ブローカー１７０を介して制御ユニット１００からコンフィグデータ１０６１を受信することができる。なお、制御ユニット１００の構成情報は、無人/有人の情報に限定されない。

【０１６５】

記憶部２０９に格納される対処ＤＢ６６は、図２１（Ａ）の無人のＦＡ向けの対処ＤＢ６６と、図２１（Ｂ）のと有人のＦＡ向けの対処ＤＢ６６を含む。通知処理部２２は、制御

ユニット１００のコンフィグデータ１０６１に基き、記憶部２０９に格納される対処ＤＢ６６のうちから、無人ＦＡ向けの対処ＤＢ６６および有人ＦＡ向けの対処ＤＢ６６のうちの一方を、検索対象に設定する。これにより、制御ユニット１００の構成により対処ＤＢ６６を切替えることができる。

【０１６６】

図２１（Ｂ）の有人のＦＡ向けの対処ＤＢ６６のメッセージ６８２は、“セーフティエリアへの侵入に注意”のメッセージ６８２１および“装置から距離をとってください”のメッセージ６８２２など、制御ユニット１００の周囲に存在する可能性があるユーザーに向けた注意喚起のメッセージが含まれる。これとは異なり、図２１（Ａ）の無人のＦＡ向けの対処ＤＢ６６のメッセージ６８２は制御ユニット１００の周囲のユーザーに向けた注意喚起のメッセージは含まれていない。

【０１６７】

また、コンフィグデータ１０６１が、制御ユニット１００を備えるネットワークの構成の情報を含んでいる場合は、通知処理部２２は、制御ユニット１００からのコンフィグデータ１０６１に基づき、検索対象となる対処ＤＢ６６を切替える。例えば、コンフィグデータ１０６１が制御ユニット１００を備えるネットワークの構成は、１台の制御ユニット１００のみを備えることを示す場合は、図１７（Ａ）で示したように“外部ネットワークを遮断する”とのメッセージ６８２を含む対処ＤＢ６６に切替える、これに対して、例えば、コンフィグデータ１０６１が制御ユニット１００に他の制御ユニット１００が接続されたネットワーク構成を示す場合は、図１７（Ｂ）で示したように他の制御ユニット１００は外部ネットワーク５０と通信できるように“外部ネットワークを完全遮断せずに断続的に遮断する”とのメッセージ６８２を含む対処ＤＢ６６に切替えることができる。

【０１６８】

＜Ｋ．ＰＬＣ状態情報を用いたインシデントの検知＞

本実施の形態では、通知処理部２２は、事前にインシデントが検知されているか否かと制御システム１の稼働状態に基づき、メッセージ６８２を変更するようにしてもよい。ここでは、制御システム１の稼働状態として、制御ユニット１００の稼働状態を例示する。

【０１６９】

図２２は、本発明の実施の形態に係る対処メッセージの他の例を模式的に示す図である。他の例に係る対処メッセージ６８２ａは、記憶部２０９にテーブル２２１として格納される。図２２を参照して、テーブル２２１の他の例に係る対処メッセージ６８２ａは、制御ユニット１００の稼働状態を示すＰＬＣ状態情報７３とデータ７３１とに関連づけ決定される。データ７３１は、事前にインシデントが検知されているか否かを示す。図２２では、ＰＬＣ状態情報７３は、例えば制御ユニット１００の状態として、例えば“全停止フォールト”、“部分停止フォールト”および“軽度フォールト”、ならびにメモリカード１１５の装着を示す“ＳＤカード挿入”および外部デバイスのポート１４２への“ＵＳＢ接続”などを示す。

【０１７０】

インシデント検知部２１はＰＬＣ状態情報７３が“全停止フォールト”を示す場合に、当該“全停止フォールト”は、対応のデータ７３１の条件すなわち「事前にインシデント検知有り」のもとで発生したとの条件が満たされたときインシデントを検知する（図２２のケース１）。一方、インシデント検知部２１は、当該条件が満たされないとき（すなわち、「事前にインシデント検知無し」のもとで発生したとの条件が満たされたとき）、インシデントを検知しない（図２２のケース２）。したがって、ケース１の場合のみ、通知処理部２２は、インシデント検知部２１の出力に基づき、ケース１に対応のメッセージ６８２の“インシデントによる全停止フォールトの可能性があります”を通知する。同様の処理が、ＰＬＣ状態情報７３が“部分停止フォールト”と“軽度停止フォールト”のそれぞれについても同様に実施される。

【０１７１】

また、インシデント検知部２１はＰＬＣ状態情報７３が“ＳＤカード挿入”または“ＵＳＢ接

続”を示す場合は、対応のデータ７３１の条件すなわち「事前にインシデント検知されたか否かにかかわらない」との条件が満たされて、インシデントが検知される。通知処理部２２は、インシデント検知部２１の出力に基づき、対応のメッセージ６８２を出力する。

【０１７２】

＜Ｌ．セキュリティレベルに応じた対処の変更＞

図２３は、本発明の実施の形態に係るセキュリティレベルの変化に応じた対処方法の説明する図である。本実施の形態の背景として、制御システム１が適用されるＦＡ環境におけるセキュリティレベルは、工場のＦＡ毎に異なる場合がある。したがって、本実施の形態では、セキュリティ上のインシデントへの対処を制御システム１が適用される環境のセキュリティレベル毎に異ならせることができる。

【０１７３】

図２３（Ａ）は、制御システム１が適用されるＦＡ環境のセキュリティレベルが低いケースを示し、図２３（Ｂ）は、当該セキュリティレベルが高いケースを示す。図２３（Ａ）ではセキュリティユニット２００のみがセキュリティ上のインシデントに対処する機能を備え、制御システム１にネットワーク接続する他の機器は、セキュリティ上のインシデントの検知などの機能を備えない。この場合は、通知処理部２２が出力するメッセージ６８２は、ＰＣ６００，７００などの装置またはネットワーク構成に対する対処を含んでもよい。これに対して、図２３（Ｂ）では、セキュリティユニット２００に加えて、制御システム１にネットワーク接続する他の機器は、セキュリティ上のインシデントの検知などの機能を備えない。この場合は、ＰＣ６００,７００およびルーター５１などもインシデントに対処する機能を備え、また工場への入出管理がなされている場合は、通知処理部２２が出力するメッセージ６８２はログの確認を促す対処を含むことでよい。

【０１７４】

制御システム１が適用されるＦＡ環境のセキュリティレベルは、例えば二次記憶装置２０８に格納される。また、記憶部２０９にはセキュリティレベル毎の対処ＤＢ６６が格納されて、各対処ＤＢ６６は、対応のセキュリティレベルに応じたメッセージ６８２を有する。通知処理部２２は、セキュリティレベルに基づき検索するべき対処ＤＢ６６を切替える。これにより、通知処理部２２は、インシデントが検知されたとき、セキュリティレベルに応じた対処を示すメッセージ６８２を出力することができる。

【０１７５】

＜Ｍ．出力部のバリエーション＞

図２４は、本発明の実施の形態に係る通知６８の出力部の一例を模式的に示す図である。本実施の形態では、通知６８の出力部を多様化することができる。通知６８の出力部はセキュリティユニット２００に追加して、その他の装置（例えば、制御ユニット１００、カプラ、各種の通信ユニット、ＨＭＩ８００など）を含み得る。

【０１７６】

（ｍ１．セキュリティユニット２００において通知６８を出力するケース）

まず、通知６８を出力する出力部として、例えば、セキュリティユニット２００が備えるインジケータ２２４、ディスプレイ２２５またはスピーカ２２６など含まれる。さらに、図示しない振動部（バイブレータ）またはＬＥＤが含まれてもよい。通知出力部２３は、振動部を通知６８に応じて振動の周期が可変となるように制御し、またはＬＥＤを通知６８に応じて点滅または点灯の周期、または点灯色が可変となるように制御する。これにより、ＦＡを保守する保守者は、セキュリティユニット２００が備える出力部による通知６８を確認することで、通知されたメッセージ６８２に従いインシデントに対処することができる。例えば、制御ユニット１００の停止を防止するように対処を実施することができる。

【０１７７】

（ｍ２．ＨＭＩ８００において通知６８を出力するケース）

通知出力部２３は、ＨＭＩ８００に通知６８を出力することができる。したがって、保守者は、セキュリティユニット２００から離れた場所に居る場合でも、通知６８をＨＭＩ８

００で確認して、インシデントに対処することができる。
【０１７８】
なお、本実施の形態では、ＨＭＩ８００は、セキュリティユニット２００および制御ユニット１００の両方に接続される場合と一方に接続される場合とがあり得る。ＨＭＩ８００が、セキュリティユニット２００および制御ユニット１００の両方に接続される場合は、通知出力部２３は、両方のＨＭＩ８００または一方のＨＭＩ８００に、通知６８を出力する。
【０１７９】
（ｍ３．パトランプ２３１により通知６８を出力するケース）
通知６８の出力部は、制御システム１が備えられる工場に設けられたパトランプ２３１を含み得る。通知出力部２３は、通知６８に従いパトランプ２３１を点灯色、点灯周期などが可変となるよう制御する。したがって、保守者は、セキュリティユニット２００から離れた場所に居る場合でも、工場内に設けられたパトランプ２３１の点灯から対処の情報を得ることができる。
【０１８０】
（ｍ４．サポート装置６００により通知６８を出力するケース）
通知６８の出力部は、保守者が操作するサポート装置６００などのＰＣ（Personal Computer）ツールを含み得る。通知出力部２３は、通知６８を出力するようにサポート装置６００を制御する。したがって、保守者は、セキュリティユニット２００から離れた場所に居る場合でも、サポート装置６００の出力から対処の情報を得ることができる。また、ＰＣツールでは、通知６８に応じてサポート装置６００の操作を制限するように動作してもよい。これにより、保守者の不用意な操作を防ぐことも可能となる。
【０１８１】
なお、本実施の形態では、サポート装置６００は、セキュリティユニット２００および制御ユニット１００の両方に接続される場合と一方に接続される場合とがあり得る。サポート装置６００が、セキュリティユニット２００および制御ユニット１００の両方に接続される場合は、通知出力部２３は、両方のサポート装置６００または一方のサポート装置６００に、通知６８を出力する。
【０１８２】
（ｍ５．監視用ＰＣ２３２により通知６８を出力するケース）
通知６８の出力部は、工場に備えられるＦＡの管理者が操作する監視用ＰＣ２３２を含み得る。通知出力部２３は、通知６８を出力するように監視用ＰＣ２３２を制御する。したがって、監視者は、セキュリティユニット２００から離れた場所に居る場合でも、監視用ＰＣ２３２の出力から対処の情報を得ることができる。なお、監視用ＰＣ２３２は、携帯可能に構成されてもよい。
【０１８３】
図２４では、セキュリティユニット２００にケースｍ１～ｍ５の出力部となる装置が全て接続される状態を示したが、これに限定されない。つまり、制御システム１には、ケースｍ１～ｍ５の出力部となる装置の１つ以上が接続される状態であってもよい。なお、通知出力部２３は、上記に述べたケースｍ１～ｍ５のいずれか１つに従い通知６８に出力する、またはケースｍ１～ｍ５の２つ以上のケースを組み合わせて通知６８を出力することができる。また、いずれのケースを適用するかを指定する情報は、ユーザー（保守者または管理者）がセキュリティユニット２００に設定してもよい。
【０１８４】
また、本実施の形態では、通知出力部２３は、記憶部２０９のネットワーク構成情報２６２０から制御システム１にネットワーク接続される装置を特定し、特定した装置の情報に基づき、出力部（ケースｍ１～ｍ５のいずれを実施するか）を決定してもよい。
【０１８５】
（ｍ６．他のＳＧＵに通知６８を出力するケース）
図２５は、本発明の実施の形態に係る通知６８の出力部の他の例を模式的に示す図である

。本実施の形態では、ＦＡは、複数の制御システム１を備えて構成され得る。この場合には、ある制御システム１の通知６８は、上記のケースｍ１～ｍ５の出力部に加えて、他の制御システム１により出力されてもよい。

【０１８６】

これにより、例えば他の制御システム１の保守者に対して、他のシステムにおいてインシデントが発生し自己が保守するシステムにおいても、セキュリティ上のインシデントが発生する可能性があることを通知できる。

【０１８７】

＜Ｎ．出力態様＞

図２６は、本発明の実施の形態に係る通知６８の出力態様の一例を模式的に示す図である。図２６は、通知６８が、セキュリティユニット２００のディスプレイ２２５またはインジケータ２２４に出力される場合を例示する。図２６（Ａ）および図２６（Ｂ）には、定量化された深刻度Ｐｈｉまたはリスク値６８１をインジケータ２２４で表示する場合の構成例が示される。

【０１８８】

図２６（Ａ）に示すように、通知出力部２３は、セキュリティ上のインシデントへの対処情報（メッセージ６８２）をディスプレイ２２５に表示する。ディスプレイ２２５には、深刻度Ｐｈｉまたは算出されたリスク値６８１または検出したインシデントの種類６８０を対処情報とともに表示してもよい。これによりユーザー（保守者,管理者）に対して、セキュリティ上のインシデントに対してとるべき対処を文章、絵、図などを用いて通知することができる。

【０１８９】

また、図２６（Ａ）と（Ｂ）に示すように、インジケータ２２４においては、３つのＬＥＤが配置されており、深刻度Ｐｈｉまたは算出されたリスク値６８１に応じて点灯数あるいは点灯位置を変化させる。図２６（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、深刻度Ｐｈｉまたは算出されたリスク値に応じて点灯色あるいは点灯強度、または点滅周期などを変化させる。

【０１９０】

このように、セキュリティユニット２００は、インジケータ２２４によりインシデント検知部２１がインシデントを検知したこと、およびその深刻度Ｐｈｉおよびリスク値６８１をユーザーに出力する出力手段を有している。

【０１９１】

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

【０１９２】

また、本実施の形態では、図２６（Ａ）に示す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。

【０１９３】

＜Ｏ．変形例＞

上記の実施の形態では、セキュリティユニット２００を制御ユニット１００に適用した制御システム１を説明したが、セキュリティユニット２００の適用先は制御ユニット１００に限定されない。例えば、セキュリティユニット２００は、制御ユニット１００に代えて、ＦＡのためのＡＧＶ（Automated guided vehicle）に搭載される制御システムに適用することもできる。この場合は、インシデント検知部２１は、ＡＧＶの無線通信を監視して得られる通信監視情報５１１から、インシデントを検知することができる。

【０１９４】

＜Ｐ．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。

【０１９５】

［構成１］

制御システム（１）であって、
制御対象（５００）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、前記制御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、
前記制御システムの稼働状態を示す状態情報（７１，７２，７３）を収集する収集手段（２０）と、
収集される前記状態情報に基き、前記制御システムにおけるインシデント（６８０）を検知する検知手段（２１）と、
検知された前記インシデントへの対処の情報を通知する通知手段（２２，２３）と、を含む、制御システム。

【０１９６】

［構成２］
前記検知手段は、さらに、
収集される前記状態情報が、複数種類のインシデントのそれぞれに対応の条件（６７）のうちいずれかの条件を満たすことに基づき、当該インシデントの種類を検知する、構成１に記載の制御システム。

【０１９７】

［構成３］
前記検知手段は、さらに、
収集される前記状態情報が、前記インシデントが前記セキュリティにおよぼす影響の深刻度（Ｐｈｉ）のそれぞれに対応の条件のうちいずれかの条件を満たすことに基づき、当該インシデントの深刻度を検知する（図１２）、構成１または２に記載の制御システム。

【０１９８】

［構成４］
前記対処の情報は、前記深刻度に応じた対処の情報（図１３（Ｂ））を含む、構成３に記載の制御システム。

［構成５］
前記通知手段は、さらに、検知された前記深刻度を通知する、構成３または４に記載の制御システム。

［構成６］
前記通知手段は、さらに、
収集される前記状態情報および前記深刻度に基く算出値であるセキュリティリスク（６８１）を通知する、構成３から５のいずれか１に記載の制御システム。

【０１９９】

［構成７］
前記対処の情報は、前記セキュリティリスクに応じた対処の情報（図１４（Ｂ））を含む、構成６に記載の制御システム。

【０２００】

［構成８］
前記対処の情報は、前記制御システムの稼働状態を変化させる対処の情報を含む、構成１から７のいずれか１に記載の制御システム。

【０２０１】

［構成９］
前記対処の情報は、前記制御ユニットの構成により異なる（図２２）、構成１から８のいずれか１に記載の制御システム。

【０２０２】

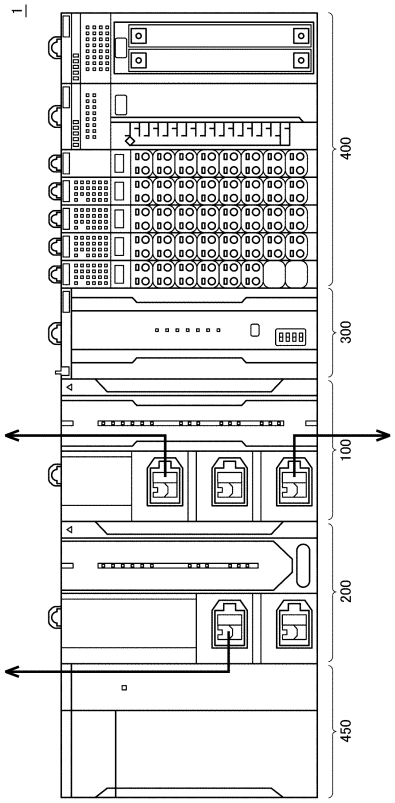
［構成１０］
前記対処の情報は、前記制御ユニットを備えるネットワークの構成（コンフィグデータ１０６１）により異なる、構成１から９のいずれか１に記載の制御システム。

【０２０３】
［構成１１］
前記通知手段は、
前記制御ユニットを含む複数の装置を接続するネットワーク構成の情報（２６２０）に基づき決定した装置に、前記対処の情報を通知する、構成１から１０のいずれか１に記載の制御システム。
【０２０４】
＜Ｑ．利点＞
本実施の形態によれば、ＦＡにおける制御システムのセキュリティの状態（異常/インシデント検知など）を、セキュリティ知識がないユーザー（保守者など）でも通知出力部２３からの通知６８によりすぐに確認することができる。また、セキュリティ異常によりインシデントが検知されたが場合に、通知６８のメッセージ６２８から、保守者が取るべき対処方法を確認し、実施することができる。
【０２０５】
また、この通知６８はＬＥＤ、７セグメントディスプレイ、音声、振動、ＨＭＩ８００などの表示装置、ネットワークを経由したサポート装置６００などのツールにより提供することができる。したがって、ユーザーは、セキュリティユニット２００から離れている場合でも、最寄りの装置から通知６８の受けることができる。
【０２０６】
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】
【０２０７】
１　制御システム、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、２０　情報収集部、２１　インシデント検知部、２２　通知処理部、２３　通知出力部、５０　外部ネットワーク、５１　ルーター、６２　ユーザー情報、６８　通知、６３，２６２０　ネットワーク構成情報、６６　対処ＤＢ、６７　アタックツリー、７１　外部情報、７２　ＳＧＵ内部情報、７３　ＰＬＣ状態情報、１００　制御ユニット、１２４，２２４，３２４　インジケータ、１５０　制御エンジン、１６０　情報エンジン、１７０　ブローカー、２００　セキュリティユニット、２３１　パトランプ、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、５１１　通信監視情報、６００　サポート装置、６８０　種類、６８１　リスク値、６８２，６８２ａ，６８２１，６８２２　メッセージ、２６１０　セキュリティシステムプログラム、２６１１　情報収集プログラム、２６１２　インシデント検知プログラム、２６１３　通知処理プログラム、２６１４　通知出力プログラム、Ｐｈｉ　深刻度。

【図面】

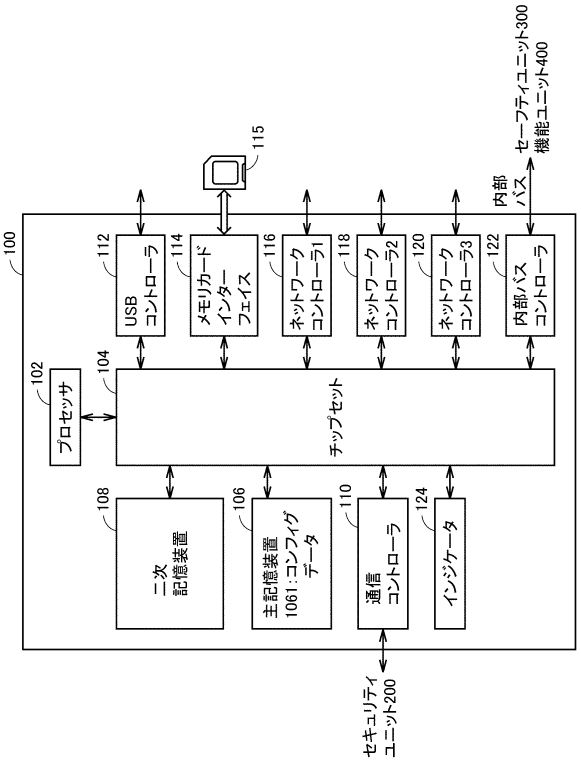
【図１】

図1



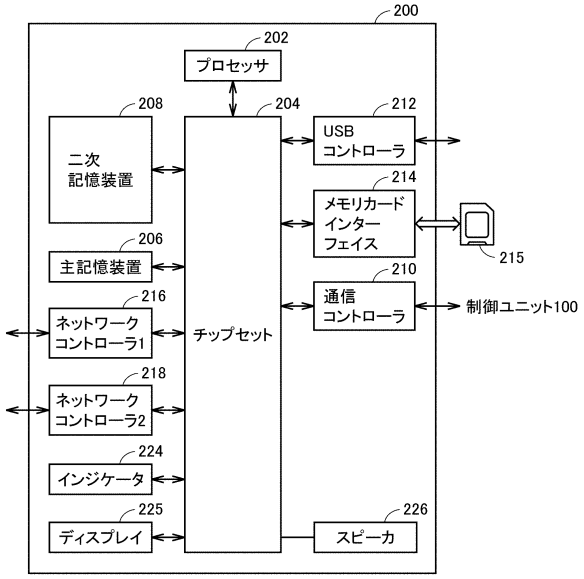
【図２】

図2



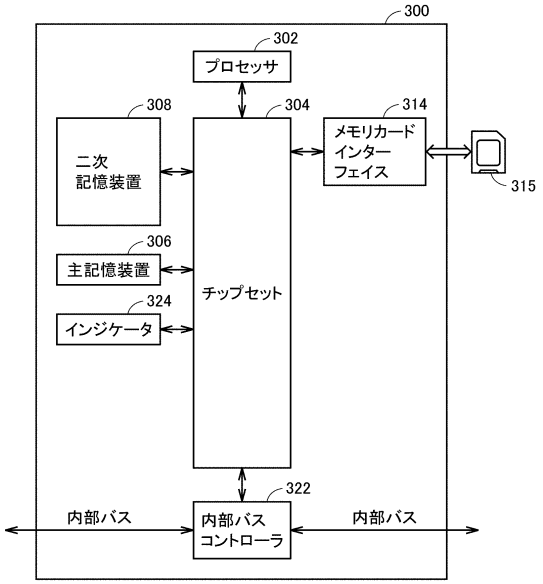
【図３】

図3



【図４】

図4



【図５】

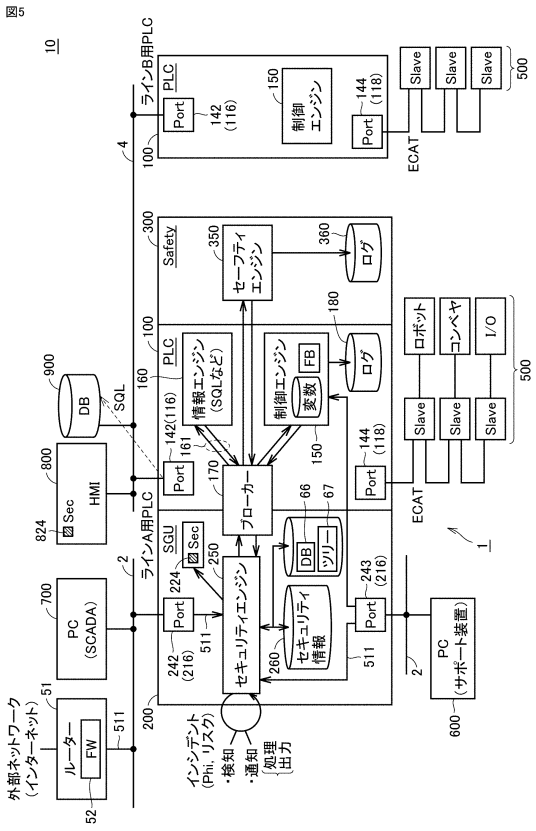


図5
10
ラインB用PLC
PLC
Port
142 (116)
150
制御エンジン
144 (118)
Slave
Slave
Slave
500
ECAT
4
100
300
Safety
350
セーフティエンジン
360
ログ
180
100
PLC
160
情報エンジン (SQLなど)
制御エンジン
FB
変数
ログ
ロボット
コンベヤ
I/O
500
900
DB
SQL
142(116)
161
150
144 (118)
Slave
Slave
Slave
800
HMI
Sec
824
Port
170
ブローカー
66
67
ECAT
1
ラインA用PLC
SGU
Sec
2
250
DB
ツリー
224
Port
243 (216)
700
PC (SCADA)
242 (216)
511
セキュリティエンジン
260
セキュリティ情報
511
PC (サポート装置)
2
51
200
600
外部ネットワーク (インターネット)
ルーター
FW
511
インシデント (Phi, リスク)
・検知
・通知
処理出力
52

【図６】

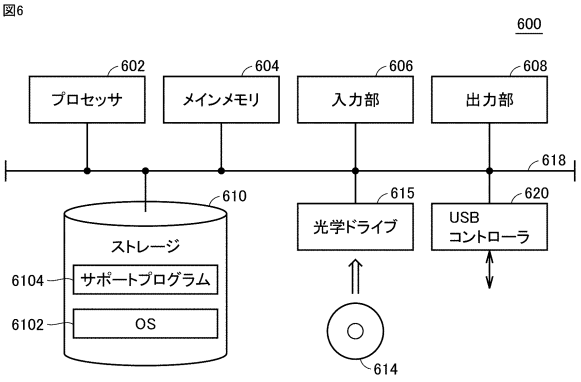


図6
600
602
プロセッサ
604
メインメモリ
606
入力部
608
出力部
618
610
ストレージ
6104
サポートプログラム
6102
OS
615
光学ドライブ
620
USB コントローラ
614

【図７】

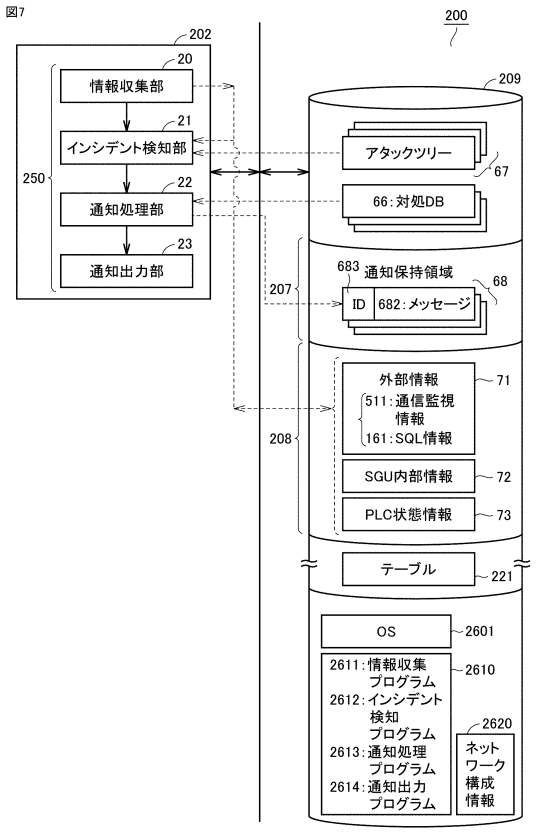


図7
200
202
20
情報収集部
21
インシデント検知部
250
22
通知処理部
23
通知出力部
209
アタックツリー
67
66:対処DB
683 通知保持領域
68
207
ID
682:メッセージ
外部情報
71
511:通信監視情報
161:SQL情報
208
SGU内部情報
72
PLC状態情報
73
テーブル
221
OS
2601
2611:情報収集プログラム
2612:インシデント検知プログラム
2613:通知処理プログラム
2614:通知出力プログラム
2610
2620
ネットワーク構成情報

【図８】

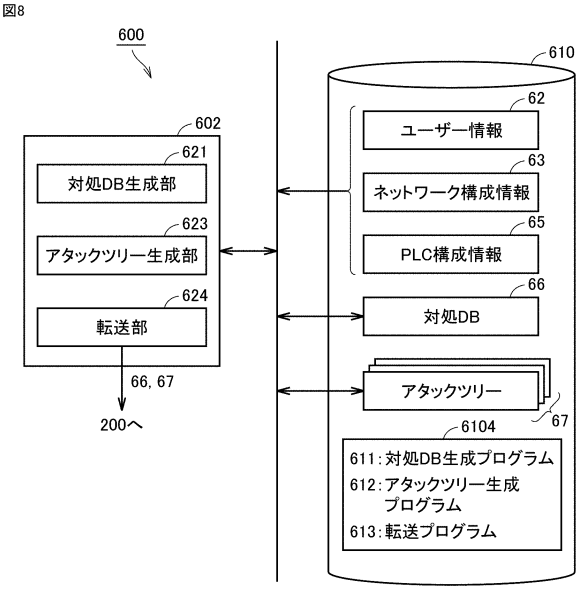


図8
600
602
621
対処DB生成部
623
アタックツリー生成部
624
転送部
66, 67
200へ
610
62
ユーザー情報
63
ネットワーク構成情報
65
PLC構成情報
66
対処DB
アタックツリー
67
6104
611:対処DB生成プログラム
612:アタックツリー生成プログラム
613:転送プログラム

【図９】

図9

62a　62

深刻度Phi	ユーザー識別子	62b：連絡先組織名	62c：電話番号	62d：Eメール
高（Ph3）	SSD	総合安全部	0123-45-1111	abcabc@xxx.co.jp
中（Ph2）	FRP	工場責任者	0123-45-2222	defdef@xxx.co.jp
低（Ph1）	EMD	装置保守部	0123-45-3333	ghighi@xxx.co.jp

深刻度Phi	説明
高	深刻ではなくとも通常時に発生しないイベントが起きたらすぐに対処を通知する。安全性の低い機能は無効になります。装置の動作に必要な機能まで無効になる場合があります。
中	インシデントの深刻度が高まった場合に通知する。安全と確認されている機能は有効にし、通常の装置の動作には影響はありません。
低	インシデントが発生したと検知したあとに通知する。すべての機能の動作を有効にします。装置の運用は従来通りとなりますが、インシデントの深刻度は高い状態となります。

【図１０】

図10

680　681　66

インシデント	Phi	リスク値	682：メッセージ
なりすまし	Ph1	5	不正なポートアクセスが発生しています。
		15	不正なポートアクセスが発生しています。 装置保守部に連絡してください。
	Ph2	10	不正な認証操作が行われています。
		35	不正な認証操作が行われています。 上位ネットワーク接続を切断し、 工場責任者に連絡してください。
	Ph3	40	不正な変更操作が行われています。 上位ネットワーク接続を切断してください。
		60	不正な変更操作が行われています。 ただちに装置を停止し、 総合安全部に連絡してください。 Phone：0123-45-1111

【図１１】

図11

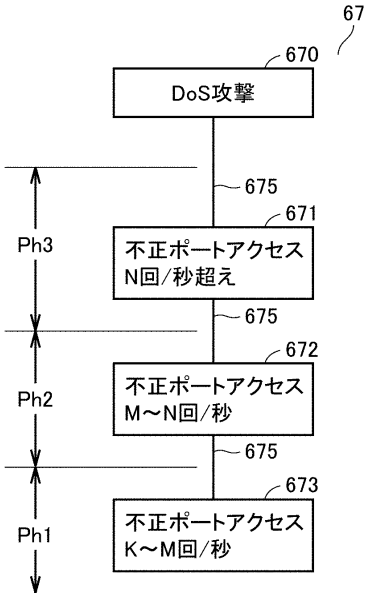
66

インシデント	Phi	リスク値	682：メッセージ
なりすまし	Ph1	5	不正なポートアクセスが発生しています。
		15	不正なポートアクセスが発生しています。管理者に連絡してください。
	Ph2	10	不正な認証操作が行われています。
		35	不正な認証操作が行われています。上位ネットワーク接続を切断し、管理者に連絡してください。
	Ph3	40	不正な変更操作が行われています。上位ネットワーク接続を切断してください。
		60	不正な変更操作が行われています。Phone：0XXX-XX-XXXX ただちに装置を停止し、管理者に連絡してください。
DoS	Ph1	10	不正な高負荷ポートアクセスが発生しています。
		20	不正な高負荷ポートアクセスが発生しています。管理者に連絡してください。
	Ph2	15	不正なネットワークアクセスを検知し、上位ネットワーク接続を切断しました。
		35	不正なネットワークアクセスを検知し、上位ネットワーク接続を切断しました。 管理者に連絡してください。
	Ph3	35	深刻なセキュリティ攻撃により重大な障害が発生しました。 ただちに管理者に連絡してください。Phone：0XXX-XX-XXXX
		60	深刻なセキュリティ攻撃により重大な障害が発生しました。 ただちに装置を停止し、管理者に連絡してください。Phone：0XXX-XX-XXXX
改ざん	Ph1	15	不正な設定変更が行われました。
		30	不正な設定変更が行われました。点検を行ってください。
	Ph2	30	不正な設定変更により重大な障害が発生する可能性があります。点検を行ってください。
		45	不正な設定変更により重大な障害が発生する可能性があります。 ただちに管理者に連絡してください。Phone：0XXX-XX-XXXX
	Ph3	40	不正な設定変更により重大な障害が発生しました。 ただちに装置を停止し、セキュリティチェックを行ってください。
		75	不正な設定変更により重大な障害が発生しました。 ただちに装置を停止し、管理者に連絡してください。Phone：0XXX-XX-XXXX

680　681

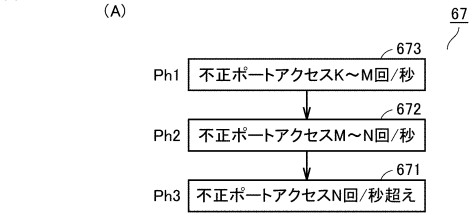
【図１２】

図12



【図１３】

図13



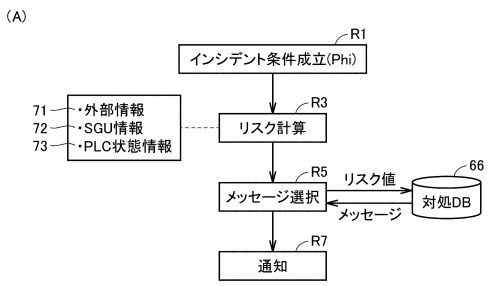
(B)

66

680 インシデント	Phi	682:メッセージ
DoS	Ph1	不正ポートアクセスが発生しています。 管理者に連絡してください。
	Ph2	中負荷の不正ポートアクセスが発生しています。 上位ネットワーク接続を切断し、管理者に 連絡してください。
	Ph3	高負荷の不正ポートアクセスが発生しています。 ただちに装置を停止し、管理者に連絡してください。

【図１４】

図14



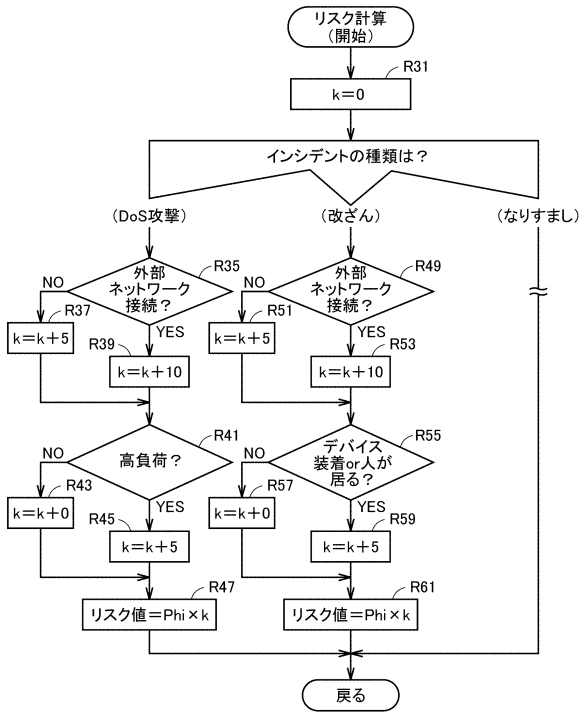
(B)

66

680 インシデント	681 Phi	リスク値	682:メッセージ
DoS	Ph1	5	不正なポートアクセスが発生しています。
		10	・・・
		15	不正ポートアクセスが発生しています。 管理者に連絡してください。
	Ph2	10	中負荷の不正ポートアクセスが 発生しています。
		20	・・・
		30	中負荷の不正ポートアクセスが 発生しています。 上位ネットワーク接続を切断し、 管理者に連絡してください。
	Ph3	15	・・・
		30	高負荷の不正ポートアクセスが 発生しています。 上位ネットワーク接続を切断してください。
		45	高負荷のポートアクセスが発生しています。 ただちに装置を停止し、管理者に連絡 してください。

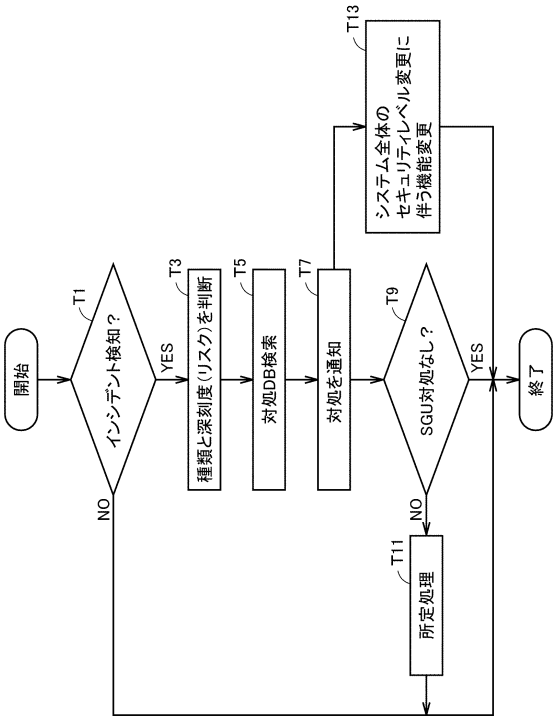
【図１５】

図15



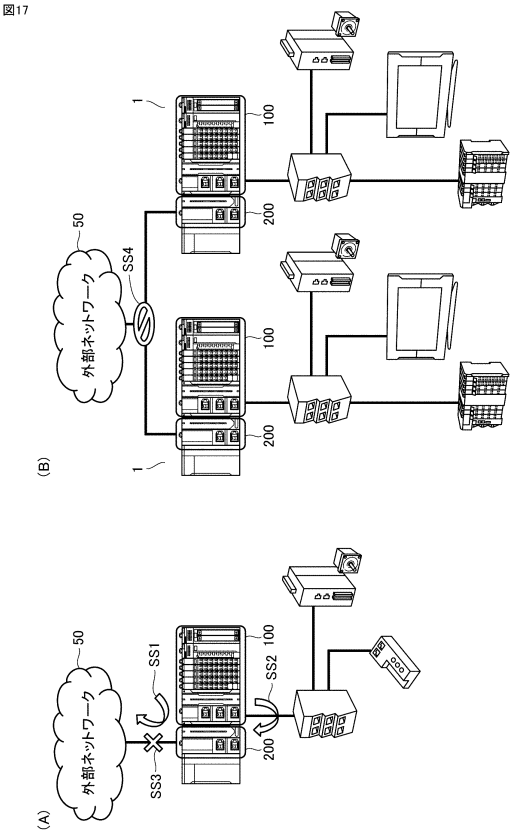
【図１６】

図16



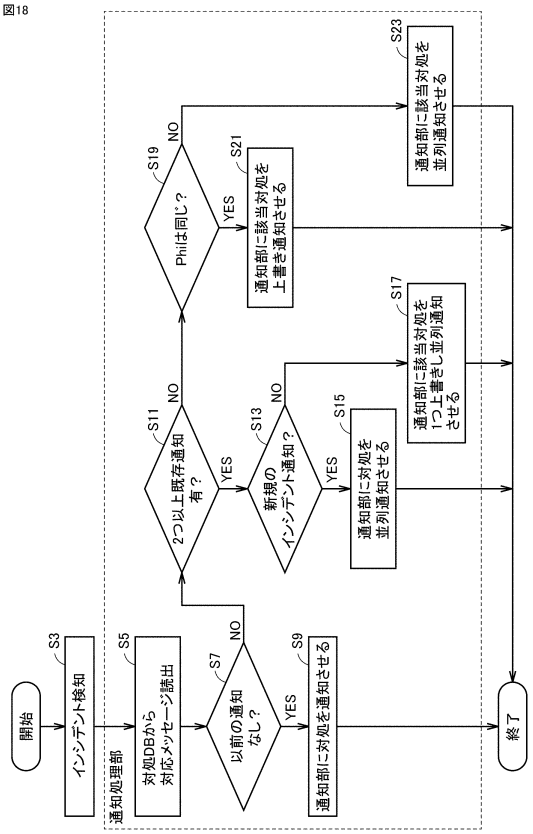
【図１７】

図17



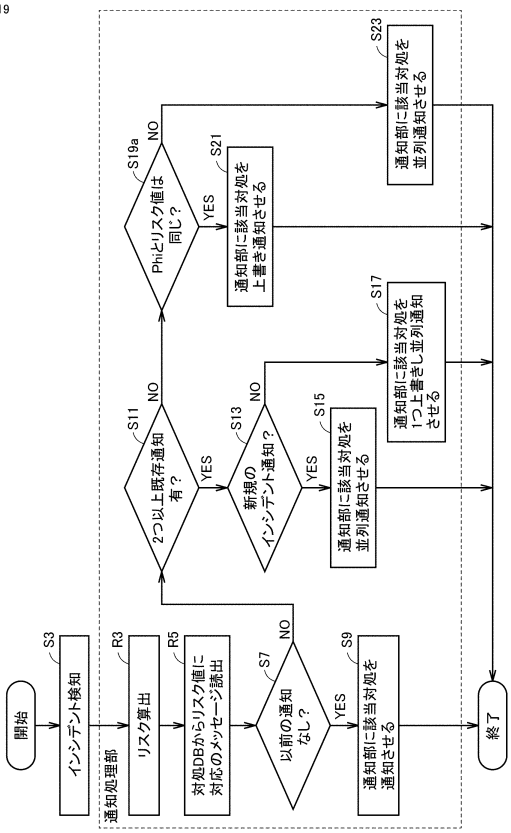
【図１８】

図18



【図１９】

図19



【図２０】

図20

通知の装置(媒体)方法	パターン	通知の態様
LED	色	正常：青LED、異常：赤、注意：黄色
	点滅	正常：常時点灯、異常：高速点滅（パターンで対応通知）、注意：低速点滅（パターンで対応通知）
7セグメントディスプレイ	文字	正常：000、異常：ER1
	点滅	正常：常時点灯、異常：高速点滅（パターンで対応通知）
バトランプ	色	色もしくは点灯のパターンの組み合わせで表示 ・異常：赤色のバトライト1つだけを点灯 ・異常：3色バトライトを全点灯させる ・異常：3色バトライトの点灯パターン（パターンで対応通知） ・異常：色指定できるバトライトで通知内容によって色を変える（紫）
	点滅	正常：常時点灯、異常：高速点滅（パターンで対応通知）
音	ビープ	正常：無音、異常：ビープ音（パターンで対応通知）
振動	超音波振動	正常：振動なし、異常：超音波振動を発生させる（パターンで対応通知）
	物理振動	正常：振動なし、異常：振動発生（パターンで対応通知）
HMI	ポップアップ	・セキュリティ異常の詳細情報表示 ・対応方法の詳細情報表示
	操作制限	正常：全操作可能、異常：セキュリティ状態に応じた操作に限定
PCツール	ポップアップ	・セキュリティ異常の詳細情報表示 ・対応方法の詳細情報表示
	操作制限	正常：全操作可能、異常：セキュリティ状態に応じた操作に限定

【図２１】

図21

(A)

66

インシデント	Phi	682:メッセージ
なりすまし	Ph1	不正なポートアクセスが発生しています。 管理者に連絡してください。
	Ph2	不正な認証操作が行われています。 上位ネットワーク接続を切断し、管理者に連絡してください。
	Ph3	不正な変更操作が行われています。 ただちに装置を停止し、管理者に連絡してください。

(B)

6821 66

インシデント	Phi	682:メッセージ
なりすまし	Ph1	不正なポートアクセスが発生しています。 管理者に連絡してください。
	Ph2	不正な認証操作が行われています。 セーフティエリアへの侵入に注意の上、 上位ネットワーク接続を切断し、管理者に連絡してください。
	Ph3	不正な変更操作が行われています。 暴走する可能性があるため、装置から距離を取ってください。 ただちに管理者に連絡してください。

6822

【図２２】

図22

221

73 PLC状態情報	731 事前インシデント検知有無	682:メッセージ(通知の仕方)
全停止フォールト	有	セキュリティ攻撃による全停止フォールトの可能性があります。
	無	通知(反応)しない。※インシデントは関係ないと考えられるため。
部分停止フォールト	有	セキュリティ攻撃による部分停止フォールトの可能性があります。
	無	通知(反応)しない。※インシデントは関係ないと考えられるため。
軽度フォールト	有	セキュリティ攻撃による軽度フォールトの可能性があります。
	無	通知(反応)しない。※インシデントは関係ないと考えられるため。
SDカード挿入	有無関係なし	SDカードが挿入されました。不正なSDカードかどうか確認してください。
USB接続	有無関係なし	USBポートに機器が接続されました。不正な操作の危険性があります。

【図２３】

図23

(B)

:セキュリティ対応

100

200

1

物理的セキュリティ

(A)

:セキュリティ対応

100

200

1

【図２４】

図24

管理者

外部ネットワーク 50

232:監視用PC

51:ルータ

800:HMI

600:サポート装置

231:パトランプ

1

800:HMI

200:SGU

100:PLC

600:サポート装置

カプラ

IO

保守者

通信ユニット

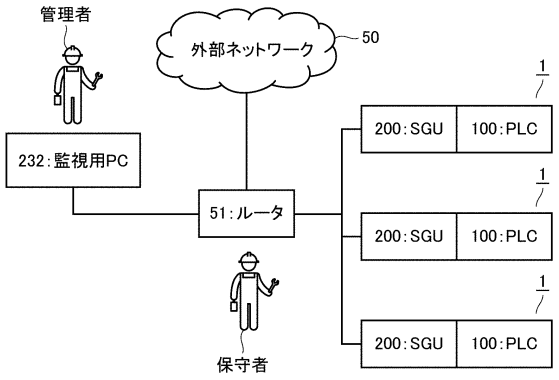
センサアンプ

センサアンプ

500

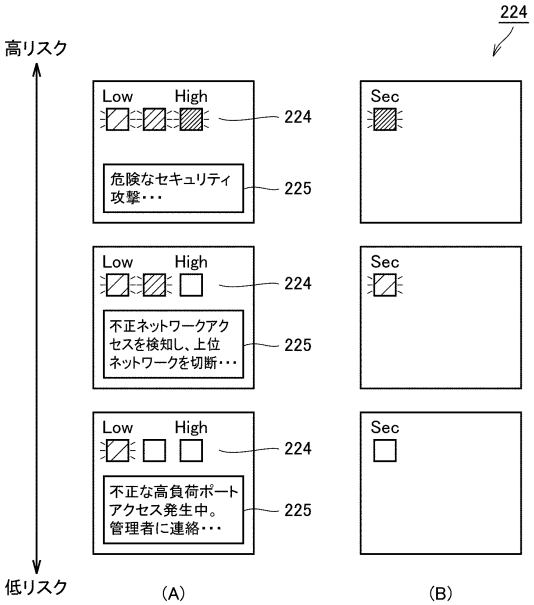
【図２５】

図25



【図２６】

図26



フロントページの続き

(56)参考文献 特開２０１８－１８５７１２（ＪＰ，Ａ）
国際公開第２０１５／００１５９４（WO，Ａ１）
特開２０１７－１７３９４０（ＪＰ，Ａ）
特開２０１５－１７６３６９（ＪＰ，Ａ）
特開２０１４－０３２５９８（ＪＰ，Ａ）
特開２０１７－０６３３３６（ＪＰ，Ａ）

(58)調査した分野 (Int.Cl.，ＤＢ名)
Ｇ０５Ｂ １９／０５