(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2019-96149
(P2019-96149A)
(43)公開日　令和1年6月20日(2019.6.20)

(51)Int.Cl.		F I			テーマコード（参考）
G05B 19/048	(2006.01)	G05B	19/048		5H220
G06F 21/55	(2013.01)	G06F	21/55	320	

審査請求 未請求　請求項の数 10　ＯＬ　（全 28 頁）

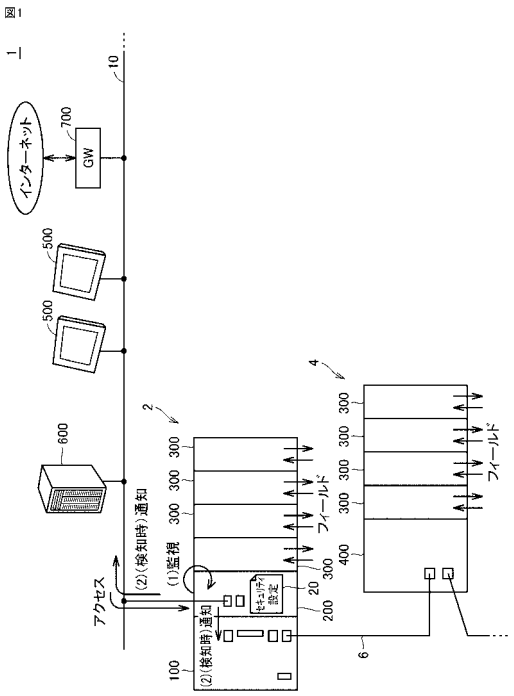
(21)出願番号　特願2017-226145 (P2017-226145)
(22)出願日　平成29年11月24日 (2017.11.24)

(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　北村　安宏
京都府京都市下京区塩小路通堀川東入南不動堂町８０１番地　オムロン株式会社内
(72)発明者　黒川　陽一
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 CC07 CX01 CX05 FF03 FF09 FF10 GG07 JJ12 JJ16 JJ27 JJ28 JJ53 KK06

(54)【発明の名称】制御装置および制御システム

(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】制御装置は、制御対象に応じて作成されたプログラムを実行するプログラム実行部と、制御装置に対する外部からのアクセスにおいてセキュリティ事象が発生したか否かを判断する検知部と、セキュリティ事象が発生したと検知されると、当該発生したセキュリティ事象に応じた通知先へ通知する通知部とを含む。セキュリティ事象は、予め定められた規則に適合しない事象を含む。
【選択図】図１



【特許請求の範囲】
【請求項１】
制御対象を制御する制御装置であって、
前記制御対象に応じて作成されたプログラムを実行するプログラム実行部と、
前記制御装置に対する外部からのアクセスにおいてセキュリティ事象が発生したか否かを判断する検知部と、
前記セキュリティ事象が発生したと検知されると、当該発生したセキュリティ事象に応じた通知先へ通知する通知部とを備え、
前記セキュリティ事象は、予め定められた規則に適合しない事象を含む、制御装置。
【請求項２】
前記セキュリティ事象は、
前記制御装置の動作を停止または性能を低下させる挙動および行為、
前記制御装置におけるプログラムの実行処理を停止または性能を低下させる挙動および行為、ならびに
前記制御対象の動作を停止または性能を低下させる挙動および行為、のいずれかを含む、請求項１に記載の制御装置。
【請求項３】
前記セキュリティ事象は、データの送信先または送信元のネットワークアドレス、物理アドレス、ポート番号のうちいずれかが、予め定められたアクセスを許可されたリストに含まれていない、および、予め定められたアクセスを禁止されたリストに含まれている、のいずれかに該当することを含む、請求項１または２に記載の制御装置。
【請求項４】
前記制御装置は、前記プログラム実行部を含む第１のユニットと、前記検知部を含む第２のユニットを備え、
前記第１のユニットは、ネットワーク接続するためのポートを有しており、
前記セキュリティ事象は、前記第１のユニットのポートが無効化されている場合に、当該ポートがネットワーク接続されることを含む、請求項１～３のいずれか１項に記載の制御装置。
【請求項５】
前記セキュリティ事象は、外部から前記制御装置へのアクセス時に要求されるユーザ認証が失敗したことを含む、請求項１～４のいずれか１項に記載の制御装置。
【請求項６】
前記セキュリティ事象は、前記制御装置で実行されるプログラムの開発が可能なサポート装置が前記制御装置へ接続されることを含む、請求項１～５のいずれか１項に記載の制御装置。
【請求項７】
前記セキュリティ事象は、前記制御装置で実行されるプログラムの追加および変更、ならびに、前記制御装置における設定の変更のうち、いずれかが生じたことを含む、請求項１～６のいずれか１項に記載の制御装置。
【請求項８】
前記通知部は、セキュリティ事象の発生をネットワークを介してイベント通知する、請求項１～７のいずれか１項に記載の制御装置。
【請求項９】
ネットワーク上に配置された報知部は、前記通知部からのイベント通知を受けて、報知動作を開始する、請求項８に記載の制御装置。
【請求項１０】
制御対象を制御する制御システムであって、
前記制御対象に応じて作成されたプログラムを実行するプログラム実行部を含む第１のユニットと、
前記第１のユニットに対する外部からのアクセスにおいてセキュリティ事象が発生した

か否かを判断する検知部、ならびに、前記セキュリティ事象が発生したと検知されると、当該発生したセキュリティ事象に応じた通知先へ通知する通知部を含む第２のユニットとを備え、

前記セキュリティ事象は、予め定められた規則に適合しない事象を含む、制御システム。

【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制御装置および制御システムにおけるセキュリティ監視に関する。

【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、制御対象の設備または装置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、設備もしくは装置に生じた異常、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】

本開示の一例によれば、制御対象を制御する制御装置が提供される。制御装置は、制御対象に応じて作成されたプログラムを実行するプログラム実行部と、制御装置に対する外部からのアクセスにおいてセキュリティ事象が発生したか否かを判断する検知部と、セキュリティ事象が発生したと検知されると、当該発生したセキュリティ事象に応じた通知先へ通知する通知部とを含む。セキュリティ事象は、予め定められた規則に適合しない事象を含む。

【０００９】

この開示によれば、制御装置に対する外部からのアクセスにおいてセキュリティ事象の発生を監視することができ、かつ、何らかのセキュリティ事象が発生した場合に、その発

生および対処などに必要な通知がなされる。これによって、制御装置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。

【００１０】

上述の開示において、セキュリティ事象は、制御装置の動作を停止または性能を低下させる挙動および行為、制御装置におけるプログラムの実行処理を停止または性能を低下させる挙動および行為、ならびに、制御対象の動作を停止または性能を低下させる挙動および行為、のいずれかを含んでいてもよい。

【００１１】

この開示によれば、制御装置が提供する処理が阻害されるような脅威をセキュリティ事象として監視できる。

【００１２】

上述の開示において、セキュリティ事象は、データの送信先または送信元のネットワークアドレス、物理アドレス、ポート番号のうちいずれかが、予め定められたアクセスを許可されたリストに含まれていない、および、予め定められたアクセスを禁止されたリストに含まれている、のいずれかに該当することを含んでいてもよい。

【００１３】

この開示によれば、予め定められた送信先または送信元との間のデータ通信のみが許容され、それ以外のデータ通信については、セキュリティ事象として検知される。そのため、ネットワークを介した脅威に対する保護を実現できる。

【００１４】

上述の開示において、制御装置は、プログラム実行部を含む第１のユニットと、検知部を含む第２のユニットを含む。第１のユニットは、ネットワーク接続するためのポートを有している。セキュリティ事象は、第１のユニットのポートが無効化されている場合に、当該ポートがネットワーク接続されることを含んでいてもよい。

【００１５】

この開示によれば、制御装置に対するネットワークを介した攻撃やネットワークを介した不正な処置がなされる前の段階で、セキュリティ事象として検知できる。

【００１６】

上述の開示において、セキュリティ事象は、外部から制御装置へのアクセス時に要求されるユーザ認証が失敗したことを含む。

【００１７】

この開示によれば、ユーザ認証の失敗は不正なアクセスが予想されるので、そのような不正なアクセスがなされる前の段階で、セキュリティ事象として検知できる。

【００１８】

上述の開示において、セキュリティ事象は、制御装置で実行されるプログラムの開発が可能なサポート装置が制御装置へ接続されることを含む。

【００１９】

この開示によれば、制御装置のプログラム自体を変更できるサポート装置が直接的に接続されることで、実行されるプログラムに対して何らかの悪意をもった攻撃がなされる可能性があるが、このような脅威を事前段階で、セキュリティ事象として検知できる。

【００２０】

上述の開示において、セキュリティ事象は、制御装置で実行されるプログラムの追加および変更、ならびに、制御装置における設定の変更のうち、いずれかが生じたことを含む。

【００２１】

この開示によれば、制御装置で実行されるプログラムに対する改変または制御装置が動作するために必要な設定に対する改変がなされると、セキュリティ事象として検知できる。このようなプログラムまたは設定に対する改変によって、制御装置において異常な制御動作が実行されることもあり、このような脅威を事前に防止できる。

【００２２】
上述の開示において、通知部は、セキュリティ事象の発生をネットワークを介してイベント通知してもよい。
【００２３】
この開示によれば、制御装置とネットワーク接続されている任意のデバイスに対して、制御装置に対する脅威を示すセキュリティ事象の発生を通知できる。
【００２４】
上述の開示において、ネットワーク上に配置された報知部は、通知部からのイベント通知を受けて、報知動作を開始してもよい。
【００２５】
この開示によれば、例えば、制御装置の近傍に配置された報知部が報知動作を開始することで、制御装置の近傍にいる管理者または保全員などがセキュリティ事象の発生を知り、必要な処置を即座に開始できる。
【００２６】
本開示の一例によれば、制御対象を制御する制御システムが提供される。制御システムは、制御対象に応じて作成されたプログラムを実行するプログラム実行部を含む第１のユニットと、第１のユニットに対する外部からのアクセスにおいてセキュリティ事象が発生したか否かを判断する検知部、ならびに、セキュリティ事象が発生したと検知されると、当該発生したセキュリティ事象に応じた通知先へ通知する通知部を含む第２のユニットとを含む。セキュリティ事象は、予め定められた規則に適合しない事象を含む。
【００２７】
この開示によれば、制御システムに対する外部からのアクセスにおいてセキュリティ事象の発生を監視することができ、かつ、何らかのセキュリティ事象が発生した場合に、その発生および対処などに必要な通知がなされる。これによって、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。
【発明の効果】
【００２８】
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を実現できる。
【図面の簡単な説明】
【００２９】
【図１】本実施の形態に係る制御システムの概略構成を示す模式図である。
【図２】本実施の形態に係る制御装置に含まれるＣＰＵユニットのハードウェア構成例を示すブロック図である。
【図３】本実施の形態に係る制御装置に含まれるセキュリティユニットのハードウェア構成例を示すブロック図である。
【図４】本実施の形態に係る制御装置に含まれるセキュリティユニットの機能構成例を示すブロック図である。
【図５】セキュリティ設定に含まれるアクセスコントロールリスト（ＡＣＬ：Access Control List）の一例を示す図である。
【図６】ネットワーク内のノード変化の一例を示す模式図である。
【図７】ネットワークポートへの接続監視を説明する模式図である。
【図８】ＵＳＢポートへの接続監視を説明する模式図である。
【図９】サポート装置からＣＰＵユニットへのアクセス時の処理を説明するための模式図である。
【図１０】サポート装置からＣＰＵユニットに格納されているプログラムおよび／または設定を変更する処理を説明するための模式図である。
【図１１】本実施の形態に係るセキュリティユニットから送信される電子メールの一例を説明するための模式図である。

【図１２】本実施の形態に係るセキュリティユニットから表示装置へのセキュリティ事象の通知の一例を説明するための模式図である。
【図１３】本実施の形態に係るセキュリティユニットからデータベースへのセキュリティ事象の通知の一例を説明するための模式図である。
【図１４】本実施の形態に係るセキュリティユニットから他の制御装置へのセキュリティ事象の通知の一例を説明するための模式図である。
【図１５】本実施の形態に係るセキュリティユニットからネットワークを介してイベント通知する一例を説明するための模式図である。
【図１６】本実施の形態に係るセキュリティユニットにおけるセキュリティ事象を監視する処理手順を示すフローチャートである。
【図１７】本実施の形態の変形例に係る制御システムの概略構成を示す模式図である。
【発明を実施するための形態】
【００３０】
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返さない。
【００３１】
＜Ａ．適用例＞
まず、本発明が適用される場面の一例について説明する。
【００３２】
本明細書において、「セキュリティ事象」は、制御装置の運用者または管理者などによって予め定められた規則に適合しない事象を含む。より具体的には、「セキュリティ事象」は、（ａ）制御装置自体の動作を停止または性能を低下させる挙動および行為、（ｂ）制御装置におけるプログラムの実行処理を停止または性能を低下させる挙動および行為、（ｃ）制御装置の制御対象となる設備、装置またはデバイスなどの動作を停止または性能を低下させる挙動および行為、ならびに、（ｄ）これらに類する挙動および行為を含み得る。
【００３３】
本明細書における「セキュリティ事象」は、基本的には、ネットワークまたはそれに類する電気通信を介して与えられる挙動または行為を包含する概念である。
【００３４】
図１は、本実施の形態に係る制御システム１の概略構成を示す模式図である。図１を参照して、本実施の形態に係る制御システム１は、設備および装置などの制御対象を制御するものであり、制御装置２と、リモートＩＯ（Input Output）装置４と、１または複数の表示装置５００と、１または複数のサーバ装置６００とを含む。制御装置２と、表示装置５００と、サーバ装置６００とは、ネットワーク１０を介して接続されている。ネットワーク１０は、ゲートウェイ７００を介して、外部ネットワークであるインターネットに接続されている。また、制御装置２とリモートＩＯ装置４との間は、フィールドネットワーク６を介して接続されている。
【００３５】
制御装置２は、主として、制御対象を制御する処理を担当する。本実施の形態において、制御装置２は、インターネットからのアクセス、および、ネットワーク１０内の他の装置からのアクセスを監視するとともに、何らかのセキュリティ事象の発生を検知すると、制御装置２の内部または外部へ当該検知したセキュリティ事象に係る通知を行う。
【００３６】
制御装置２は、ＣＰＵユニット１００と、セキュリティユニット２００と、１または複数の機能ユニット３００とを含む。ＣＰＵユニット１００は、制御対象に応じて作成されたプログラムを実行するプログラム実行部を有している。より具体的には、ＣＰＵユニット１００は、システムプログラムおよび各種のユーザプログラムを実行する演算処理部に相当する。
【００３７】

セキュリティユニット２００は、制御装置２に対する外部からのアクセスにおいてセキュリティ事象が発生したか否かを判断する検知部を有している。より具体的には、セキュリティユニット２００は、予め定められたセキュリティ設定２０に従って、セキュリティ事象の発生の有無を常時監視する。図１に示す構成例においては、セキュリティユニット２００は、制御装置２がネットワーク１０を介して送受信するデータを監視可能に配置されている。すなわち、セキュリティユニット２００は、論理的には、ＣＰＵユニット１００とネットワーク１０との間に配置され、ＣＰＵユニット１００から送信されるデータをネットワーク１０へ転送するとともに、ネットワーク１０を介して受信したデータをＣＰＵユニット１００へ転送する。セキュリティユニット２００は、このような処理において送受信されるデータを監視して、何らかのセキュリティ事象の有無を判断する。

【００３８】

セキュリティユニット２００は、何らかのセキュリティ事象の発生を検知すると、予め定められた規則に従って、内部または外部への通知を行う。すなわち、セキュリティユニット２００は、セキュリティ事象が発生したと検知されると、当該発生したセキュリティ事象に応じた通知先へ通知する通知部を有している。

【００３９】

本実施の形態に係る制御システム１においては、ＣＰＵユニット１００、あるいは、ＣＰＵユニット１００を含む装置に対するアクセスについて、予め定められたセキュリティ事象が発生したか否かを常時監視する処理が実装されている。そして、何らかのセキュリティ事象が発生すると、当該発生したセキュリティ事象に応じた通知が、制御装置２の内部または外部へ出力される。このような構成を採用することで、ＣＰＵユニット１００、あるいは、ＣＰＵユニット１００を含む装置に対するセキュリティ耐性を高めることができる。

【００４０】

なお、説明の便宜上、それぞれ独立したＣＰＵユニット１００とセキュリティユニット２００とを用いた別体型の実装例を示すが、これに限らず、両者を一体化したユニットを採用してもよい。あるいは、ＣＰＵユニット１００に接続される「ユニット」の形ではなく、ＣＰＵユニット１００と何らかの手段で接続される別装置として、セキュリティユニット２００が提供する処理を実装してもよい。

【００４１】

＜Ｂ．制御システムの全体構成例＞

引き続いて図１を参照して、制御システム１の全体構成例について説明する。

【００４２】

制御装置２に含まれる機能ユニット３００は、制御対象の設備および装置、ならびに、それらに配置されている各種デバイス（センサやアクチュエータなど）との間で信号を遣り取りする。具体的には、機能ユニット３００は、ＣＰＵユニット１００において算出される指令値をフィールドへ出力、あるいは、フィールドからの入力値を収集する。機能ユニット３００としては、例えば、制御対象からのデジタル信号を受取るＤＩ（Digital Input）モジュール、制御対象に対してデジタル信号を出力するＤＯ（Digital Output）モジュール、制御対象からのアナログ信号を受取るＡＩ（Analog Input）モジュール、制御対象に対してアナログ信号を出力するＡＯ（Analog Output）モジュールのうち１または複数のモジュールを有している。さらに、機能ユニット３００としては、ＰＩＤ（Proportional Integral Derivative）制御やモーション制御といった特殊機能を実装したコントローラを含み得る。

【００４３】

制御装置２とリモートＩＯ装置４とを接続するフィールドネットワーク６は、データの到達時間が保証される、定周期通信を行うバスまたはネットワークを採用することが好ましい。このような定周期通信を行うバスまたはネットワークとして、ＥｔｈｅｒＣＡＴ（登録商標）を採用してもよい。なお、「フィールドネットワーク」と称される通信経路は、「フィールドバス」とも称される。本明細書において、「フィールドネットワーク」と

の用語は、狭義の「フィールドネットワーク」に加えて、「フィールドバス」を含み得る概念として用いる。

【００４４】

リモートＩＯ装置４は、カプラユニット４００と、１または複数の機能ユニット３００とを含む。カプラユニット４００は、フィールドネットワーク６を介してデータを遣り取りするための第１の通信インターフェイスと、リモートＩＯ装置４に含まれる機能ユニット３００との間で内部的にデータを遣り取りする第２の通信インターフェイスとを含む。

【００４５】

機能ユニット３００については、制御装置２に含まれる機能ユニット３００と同様であるので、詳細な説明は繰返さない。

【００４６】

制御装置２と表示装置５００およびサーバ装置６００とを接続するネットワーク１０としては、例えば、一般的なネットワークプロトコルであるイーサネット（登録商標）やＥｔｈｅｒＮｅｔ／ＩＰ（登録商標）が採用されてもよい。

【００４７】

表示装置５００は、ユーザからの操作を受けて、制御装置２に対してユーザ操作に応じたコマンドなどを出力するとともに、制御装置２での演算結果などをグラフィカルに表示する。

【００４８】

サーバ装置６００は、データベースシステム、製造実行システム（ＭＥＳ：Manufacturing Execution System）などが想定される。製造実行システムは、制御対象の製造装置や設備からの情報を取得して、生産全体を監視および管理するものであり、オーダ情報、品質情報、出荷情報などを扱うこともできる。これらに限らず、情報系サービス（制御対象から各種情報を取得して、マクロ的またはミクロ的な分析などを行う処理）を提供する装置をネットワーク１０に接続するようにしてもよい。

【００４９】

ゲートウェイ７００は、ネットワーク１０と外部ネットワーク（インターネット）との間のプロトコル変換およびファイヤウォールとしての処理を実行する。

【００５０】

＜Ｃ．主要なユニットのハードウェア構成例＞

次に、本実施の形態に係る制御装置２に含まれる主要なユニットのハードウェア構成例について説明する。

【００５１】

（ｃ１：ＣＰＵユニット１００）

図２は、本実施の形態に係る制御装置２に含まれるＣＰＵユニット１００のハードウェア構成例を示すブロック図である。図２を参照して、ＣＰＵユニット１００は、プロセッサ１０２と、チップセット１０４と、主メモリ１０６と、ストレージ１０８と、ユニット間インターフェイス１１０と、ＵＳＢ（Universal Serial Bus）インターフェイス１１２と、メモリカードインターフェイス１１４と、ネットワークインターフェイス１１８と、内部バスコントローラ１２０と、フィールドネットワークコントローラ１３０とを含む。

【００５２】

プロセッサ１０２は、ＣＰＵ（Central Processing Unit）、ＭＰＵ（Micro Processing Unit）、ＧＰＵ（Graphics Processing Unit）などで構成される。プロセッサ１０２としては、複数のコアを有する構成を採用してもよいし、プロセッサ１０２を複数配置してもよい。このように、ＣＰＵユニット１００は、１または複数のプロセッサ１０２、および／または、１または複数のコアを有するプロセッサ１０２を有している。チップセット１０４は、プロセッサ１０２および周辺エレメントを制御することで、ＣＰＵユニット１００全体としての処理を実現する。主メモリ１０６は、ＤＲＡＭ（Dynamic Random Access Memory）やＳＲＡＭ（Static Random Access Memory）などの揮発性記憶装置などで構成される。ストレージ１０８は、例えば、フラッシュメモリなどの不揮発性記憶装置など

で構成される。
【００５３】
プロセッサ１０２は、ストレージ１０８に格納された各種プログラムを読出して、主メモリ１０６に展開して実行することで、制御対象に応じた制御を実現する。ストレージ１０８には、基本的な処理を実現するためのシステムプログラム３２に加えて、制御対象の製造装置や設備に応じて作成されたユーザプログラム３０が格納される。
【００５４】
ユニット間インターフェイス１１０は、他のユニットとデータ通信可能に接続するためのデバイスである。本実施の形態においては、ＣＰＵユニット１００のユニット間インターフェイス１１０を介して、セキュリティユニット２００が接続される。ユニット間インターフェイス１１０としては、例えば、公知のデータ伝送規格（例えば、ＰＣＩ　Ｅｘｐｒｅｓｓ）などに従うデバイスを採用できる。
【００５５】
ＵＳＢインターフェイス１１２は、ＵＳＢ接続を介した外部装置（例えば、ユーザプログラムの開発などを行うサポート装置）との間のデータ通信を仲介する。
【００５６】
メモリカードインターフェイス１１４は、メモリカード１１６が着脱可能に構成されており、メモリカード１１６に対してデータを書込み、メモリカード１１６から各種データ（ユーザプログラムやトレースデータなど）を読出すことが可能になっている。
【００５７】
ネットワークインターフェイス１１８は、ネットワーク１０を介したデータ通信の仲介が可能になっている。但し、ＣＰＵユニット１００にセキュリティユニット２００が接続される状態においては、通常、ネットワークインターフェイス１１８の動作は無効化（具体的には、ポート使用が禁止）されている。
【００５８】
内部バスコントローラ１２０は、ＣＰＵユニット１００に装着される機能ユニット３００との間のデータ通信を仲介する。フィールドネットワークコントローラ１３０は、フィールドネットワーク６を介した他のユニットとの間のデータ通信を仲介する。
【００５９】
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処理が実現される構成例を示したが、これらの提供される処理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。
【００６０】
（ｃ２：セキュリティユニット２００）
図３は、本実施の形態に係る制御装置２に含まれ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ブロック図である。図３を参照して、セキュリティユニット２００は、プロセッサ２０２と、チップセット２０４と、主メモリ２０６と、ストレージ２０８と、ユニット間インターフェイス２１０と、ネットワークインターフェイス２２０とを含む。
【００６１】
プロセッサ２０２は、ＣＰＵ、ＭＰＵ、ＧＰＵなどで構成される。上述のＣＰＵユニット１００と同様に、セキュリティユニット２００は、１または複数のプロセッサ２０２、および／または、１または複数のコアを有するプロセッサ２０２を有している。チップセット２０４は、プロセッサ２０２および周辺エレメントを制御することで、セキュリティユニット２００全体としての処理を実現する。主メモリ２０６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２０８は、例えば、フラッシュメモリなどの不揮発性記憶装置などで構成される。
【００６２】
プロセッサ２０２は、ストレージ２０８に格納された各種プログラムを読出して、主メモリ２０６に展開して実行することで、セキュリティ事象の監視などの処理を実現する。

ストレージ２０８には、基本的な処理を実現するためのファームウェア２２に加えて、制御装置の運用者または管理者などが予め定めた規則などを規定するセキュリティ設定２０が格納される。セキュリティ設定２０に基づく、セキュリティ監視処理の詳細については、後述する。

【００６３】

ユニット間インターフェイス２１０は、上述のＣＰＵユニット１００のユニット間インターフェイス１１０と同様に、他のユニットとデータ通信可能に接続するためのデバイスである。ユニット間インターフェイス２１０を介して、セキュリティユニット２００とＣＰＵユニット１００とが接続される。

【００６４】

ネットワークインターフェイス２２０は、ネットワーク１０を介した他の装置との間のデータ通信を仲介する。ネットワークインターフェイス２２０は、主たるコンポーネントとして、送受信部２２２と、コントローラ２２４と、バッファ２２６とを含む。

【００６５】

送受信部２２２は、ＯＳＩ参照モデルの物理層を担当するエレメントであり、ネットワーク１０を介した信号の受信およびデコード、ならびに、送信すべきデータのエンコードおよびネットワーク１０を介したエンコードされた信号の送信を担当する。

【００６６】

コントローラ２２４は、主として、ＯＳＩ参照モデルのデータリンク層、ネットワーク層、トランスポート層を担当するエレメントであり、ルーティング、エラー訂正、再送処理などを担当する。

【００６７】

バッファ２２６は、送信すべきデータおよび受信したデータなどを一時的に蓄える記憶部である。

【００６８】

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処理が提供される構成例を示したが、これらの提供される処理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。

【００６９】

（ｃ３：機能ユニット３００およびカプラユニット４００）

本実施の形態に係る制御装置２およびリモートＩＯ装置４に含まれる機能ユニット３００、ならびに、リモートＩＯ装置４に含まれるカプラユニット４００については、公知の構成であるので、ここでは詳細な説明は繰返さない。

【００７０】

＜Ｄ．機能構成例＞

次に、本実施の形態に係る制御システム１に含まれるセキュリティユニット２００の機能構成の一例について説明する。図４は、本実施の形態に係る制御装置２に含まれるセキュリティユニット２００の機能構成例を示すブロック図である。

【００７１】

図４を参照して、セキュリティユニット２００は、セキュリティ事象の監視に係る機能構成として、フレーム抽出モジュール２５０と、解析モジュール２５２と、状態取得モジュール２６０と、検知モジュール２６２と、通知モジュール２６４と、ユーザ認証モジュール２６６とを含む。

【００７２】

フレーム抽出モジュール２５０は、ネットワーク１０を介して外部装置との間で遣り取りされるデータ（フレームまたはパケット）を、ネットワークインターフェイス２２０から抽出する。フレーム抽出モジュール２５０は、抽出したフレームまたはパケットを解析モジュール２５２へ出力する。

【００７３】

解析モジュール２５２は、フレーム抽出モジュール２５０からのフレームまたはパケッ

トを解析して、その解析結果を検知モジュール２６２へ出力する。解析モジュール２５２における解析の内容は任意に設定できる。図４に示す構成例においては、解析モジュール２５２は、内容解析処理２５４と、特徴抽出処理２５６と、統計処理２５８とが実行可能になっている。

【００７４】

内容解析処理２５４は、処理対象のフレームまたはパケットのヘッダ情報などを参照して、送信先および送信元のネットワークアドレス（例えば、ＩＰ（Internet Protocol）アドレス）、物理アドレス（例えば、ＭＡＣ（Media Access Control address）アドレス）、ポート番号、伝送プロトコルなどの情報を取得する処理を含む。

【００７５】

特徴抽出処理２５６は、処理対象のフレームまたはパケットに含まれるデータの内容から特徴量を抽出する処理を含む。

【００７６】

統計処理２５８は、処理対象のフレームまたはパケットの送受信タイミングや頻度などの統計情報を算出する処理を含む。

【００７７】

それぞれの処理によって算出される情報は、解析結果として、検知モジュール２６２へ出力される。

【００７８】

状態取得モジュール２６０は、ＣＰＵユニット１００における状態を取得し、その取得したＣＰＵユニット状態情報を検知モジュール２６２へ出力する。ＣＰＵユニット状態情報は、例えば、ＣＰＵユニット１００に対してなされた何らかの変更操作（ソフトウェア上およびハードウェア上のいずれも含み得る）を示す。

【００７９】

検知モジュール２６２は、セキュリティ設定２０を参照して、解析モジュール２５２からの解析結果、および／または、状態取得モジュール２６０からのＣＰＵユニット状態情報が、予め定められたセキュリティ事象の条件に合致しているか否かを判断する。なお、セキュリティ事象の具体例については、後述する。

【００８０】

検知モジュール２６２は、解析結果またはＣＰＵユニット状態情報がいずれかの条件に合致している場合には、当該合致した条件に対応する種類のセキュリティ事象が発生したと判断し、その発生したと判断されたセキュリティ事象の発生を示す検知結果を通知モジュール２６４へ出力する。

【００８１】

検知モジュール２６２は、検知したセキュリティ事象を示す情報を履歴情報２４として登録する。

【００８２】

通知モジュール２６４は、検知モジュール２６２からの検知結果に応答して、発生したセキュリティ事象に応じた内容を、発生したセキュリティ事象に応じた通知先へ通知する。通知内容および通知先の具体例については、後述する。

【００８３】

ユーザ認証モジュール２６６は、ネットワーク１０を介してセキュリティユニット２００にアクセスするユーザに対する認証処理を実行する。ユーザ認証モジュール２６６は、ユーザ認証の結果を示すユーザ認証結果を検知モジュール２６２へ出力する。

【００８４】

以上のような機能構成を採用することで、本実施の形態に係るセキュリティ監視処理を実現できる。

【００８５】

＜Ｅ．セキュリティ事象＞

次に、本実施の形態に係る制御システム１において設定されるセキュリティ事象のいく

つかの例について説明する。

【００８６】

（ｅ１－１：アクセスコントロール）

まず、セキュリティ設定２０として、送信先および／または送信元を制限するアクセスコントロールを利用する例について説明する。

【００８７】

アクセスコントロールの一例としては、送信先および／または送信元のネットワークアドレス（例えば、ＩＰアドレス）、物理アドレス（例えば、ＭＡＣアドレス）、ポート番号などを用いることができる。

【００８８】

図５は、セキュリティ設定２０に含まれるアクセスコントロールリスト（ＡＣＬ：Access Control List）の一例を示す図である。図５には、アクセスコントロールを実現するためのアクセスコントロールリストとして、明示的にアクセスを許可する条件を規定するホワイトリストと、明示的にアクセスを禁止する条件を規定するブラックリストとを示す。但し、２種類のリストを用いる必要はなく、要求されるセキュリティレベルなどに応じて、いずれか一方のみを用いるようにしてもよい。

【００８９】

図５（Ａ）には、通信先のネットワークアドレス（ＩＰアドレス）を用いる例を示す。図５（Ａ）のホワイトリストには、ＣＰＵユニット１００へのアクセスを許可されるＩＰアドレスが規定されており、図５（Ａ）のブラックリストには、ＣＰＵユニット１００へのアクセスが禁止されるＩＰアドレスが規定されている。

【００９０】

図５（Ｂ）には、通信先の物理アドレス（ＭＡＣアドレス）を用いる例を示す。図５（Ｂ）のホワイトリストには、ＣＰＵユニット１００へのアクセスを許可されるＭＡＣアドレスが規定されており、図５（Ｂ）のブラックリストには、ＣＰＵユニット１００へのアクセスが禁止されるＭＡＣアドレスが規定されている。

【００９１】

図５（Ｃ）には、通信先とのデータ通信に用いられるポート番号を用いる例を示す。図５（Ｃ）のホワイトリストには、ＣＰＵユニット１００へのアクセスを許可されるポート番号が規定されており、図５（Ｃ）のブラックリストには、ＣＰＵユニット１００へのアクセスが禁止されるポート番号が規定されている。

【００９２】

図５（Ａ）～図５（Ｃ）のホワイトリストに規定されていないデバイスからのアクセス、および、ブラックリストに規定されているデバイスからのアクセスがあると、セキュリティ事象が発生したと判断してもよい。このようなアクセスコントロールリストを用いたセキュリティ事象の監視は、典型的には、図４に示す解析モジュール２５２の内容解析処理２５４により出力される解析結果とアクセスコントロールリストとを比較することで、実現される。

【００９３】

上述した、ネットワークアドレス、物理アドレス、ポート番号のうち複数を組み合せてもよい。例えば、物理アドレスおよびポート番号のいずれもがアクセス許可されている通信先に限ってアクセスを許可するようにしてもよい。

【００９４】

このように、本実施の形態に係るセキュリティ事象は、データの送信先または送信元のネットワークアドレス、物理アドレス、ポート番号のうちいずれかが、予め定められたアクセスを許可されたホワイトリストに含まれていない、および、予め定められたアクセスを禁止されたブラックリストに含まれている、のいずれかに該当することを含んでいてもよい。

【００９５】

（ｅ１－２：データ受信パターン）

次に、セキュリティ設定２０として、データ受信パターンを監視する例について説明する。例えば、大量のリクエストデータなどを送信してサービスを利用停止にするＤｏＳ（Denial of Service）攻撃などを検知するためのセキュリティ設定２０を採用してもよい。

【００９６】

ＤｏＳ攻撃の一例として、ＳＹＮ　ｆｌｏｏｄ攻撃などを考慮すると、受信間隔の短いＳＹＮパケット（あるいは、サイズが所定値以下のパケット）を所定期間に亘って受信し続けた場合などを、セキュリティ事象が発生したと判断するようにしてもよい。

【００９７】

データ受信パターンを用いたセキュリティ事象の監視は、典型的には、図４に示す解析モジュール２５２の特徴抽出処理２５６により出力される特徴量とアクセスコントロールリストとを比較することで、実現される。このように、セキュリティ設定２０として、受信するパケットの種類および受信間隔などによって規定されるデータ受信パターンを規定してもよい。

【００９８】

このように、本実施の形態に係るセキュリティ事象は、受信するパケットの種類および受信間隔などによって規定されるデータ受信パターンが予め規定されたパターンに合致することを含んでいてもよい。

【００９９】

（ｅ１－３：アクセスパターン）

次に、セキュリティ設定２０として、特定のアクセスパターンを監視する例について説明する。

【０１００】

例えば、既知のコンピュータウィルスについては、特有のアクセスパターンが解明されている場合も多く、このような場合には、その特有のアクセスパターンをセキュリティ設定２０として規定しておいてもよい。そして、セキュリティ設定２０に規定されたアクセスパターンに相当するアクセスを受けると、セキュリティ事象が発生したと判断するようにしてもよい。

【０１０１】

このようなアクセスパターンを用いたセキュリティ事象の監視は、典型的には、図４に示す解析モジュール２５２の特徴抽出処理２５６により出力される特徴量とアクセスコントロールリストとを比較することで、実現される。このように、セキュリティ設定２０として、特定のアクセスパターンの監視を規定してもよい。

【０１０２】

このように、本実施の形態に係るセキュリティ事象は、制御装置２へのアクセスのパターンが予め規定されたパターンに合致することを含んでいてもよい。

【０１０３】

（ｅ２：ネットワーク監視）

次に、セキュリティ設定２０として、ネットワーク内のノード変化を監視する例について説明する。

【０１０４】

一般的に、制御装置２が接続されるネットワークは、予め定められたデバイス（ノード）のみが接続されており、新たなデバイス（ノード）が追加される必要性は低い。そのため、ネットワーク内のノード変化をセキュリティ事象とみなすこともできる。

【０１０５】

図６は、ネットワーク内のノード変化の一例を示す模式図である。図６（Ａ）を参照して、制御装置２に加えて、表示装置５００およびサーバ装置６００がネットワーク１０に接続されている状態を標準ノード構成とする。このような標準ノード構成に対して、図６（Ｂ）に示すように、新たなデバイス９００が追加されたとする。

【０１０６】

このようなデバイス９００が追加されてネットワーク１０内のノードに変化が生じると、セキュリティ事象の発生であると判断してもよい。

【０１０７】

具体的には、例えば、標準ノード構成における各ノードのネットワークアドレスを、セキュリティ設定２０として予め取得しておき、この予め取得されたノードとは異なるネットワークアドレスがネットワーク１０内で検知されると、ネットワーク１０内のノード変化が生じたと判断できる。あるいは、ネットワーク１０内に存在するノードの数の変化などに基づいて、ノード変化を検知してもよい。

【０１０８】

なお、ネットワーク１０内のノード変化としては、ノードの追加に限らず、ノードの削除などを検知するようにしてもよい。さらに、ネットワーク１０内のノード変化として、ノード数だけではなく、トポロジーの変化についても検知するようにしてもよい。

【０１０９】

このようなネットワーク内のノード変化が生じると、セキュリティ事象が発生したと判断してもよい。

【０１１０】

このように、本実施の形態に係るセキュリティ事象は、ネットワーク内のノード変化が生じたことを含んでいてもよい。

【０１１１】

（ｅ３－１：ネットワークポートへの接続監視）

次に、セキュリティ設定２０として、ＣＰＵユニット１００のネットワークポートへの接続を監視する例について説明する。

【０１１２】

ＣＰＵユニット１００にセキュリティユニット２００が接続された構成においては、ＣＰＵユニット１００は、セキュリティユニット２００を介してネットワーク１０に接続される。そのため、ＣＰＵユニット１００自体に設けられているネットワークポートの使用は禁止されている（図２に示すネットワークインターフェイス１１８が無効化されている）。

【０１１３】

このような状態において、ＣＰＵユニット１００のネットワークポートに何らかのネットワークが接続された場合には、何らかの意図をもった行為であると想定される。そのため、このような無効化されたネットワークポートに対するネットワーク接続が生じると、セキュリティ事象が発生したと判断してもよい。

【０１１４】

図７は、ネットワークポートへの接続監視を説明する模式図である。図７を参照して、ＣＰＵユニット１００の表面には、ＵＳＢポート１１２Ｐと、メモリカードスロット１１４Ｐと、ネットワークポート１１８Ｐと、フィールドネットワークポート１３０Ｐ１，１３０Ｐ２とが配置されている。ネットワークポート１１８Ｐは、ＣＰＵユニット１００をネットワーク接続するためのポートである。

【０１１５】

制御装置２の運用中においては、使用しないネットワークポート１１８Ｐは無効化されているとする。このような状態において、ネットワークポート１１８Ｐにケーブルが接続されると、セキュリティ事象が発生したと判断してもよい。なお、制御装置２の停止中あるいはメンテナンス中においては、ネットワーク接続されることもあるので、制御装置２が運用中であることを、セキュリティ事象の発生と判断するための条件として付加してもよい。

【０１１６】

このようなネットワークポートへの接続監視は、典型的には、図４に示す状態取得モジュール２６０により出力されるＣＰＵユニット状態情報を監視することで実現される。

【０１１７】

このように、本実施の形態に係るセキュリティ事象は、ＣＰＵユニット１００のネットワークポート１１８Ｐが無効化されている場合に、ネットワークポート１１８Ｐがネットワーク接続されることを含むようにしてもよい。

【０１１８】

（ｅ３－２：ＵＳＢポートへの接続監視）

次に、セキュリティ設定２０として、ＣＰＵユニット１００のＵＳＢポートへの接続を監視する例について説明する。

【０１１９】

例えば、ＣＰＵユニット１００のＵＳＢポートなどを介してサポート装置が接続される。このようなサポート装置の接続は、何らかの意図をもった行為であると想定される。そのため、このような無効化されたネットワークポートに対するネットワーク接続が生じると、セキュリティ事象が発生したと判断してもよい。

【０１２０】

図８は、ＵＳＢポートへの接続監視を説明する模式図である。図８を参照して、ＣＰＵユニット１００の表面には、ＵＳＢポート１１２Ｐと、メモリカードスロット１１４Ｐと、ネットワークポート１１８Ｐと、フィールドネットワークポート１３０Ｐ１，１３０Ｐ２とが配置されている。

【０１２１】

例えば、制御装置２の運用中において、ＵＳＢポート１１２Ｐを介して何らかのデバイスが接続されると、セキュリティ事象が発生したと判断してもよい。なお、制御装置２の停止中あるいはメンテナンス中においては、サポート装置が接続されることもあるので、制御装置２が運用中であることを、セキュリティ事象の発生と判断するための条件として付加してもよい。

【０１２２】

このようなＵＳＢポートへの接続監視は、典型的には、図４に示す状態取得モジュール２６０により出力されるＣＰＵユニット状態情報を監視することで実現される。

【０１２３】

このように、本実施の形態に係るセキュリティ事象は、ＵＳＢポート１１２Ｐに任意のデバイスが接続されることを含むようにしてもよい。なお、ＵＳＢポートに限らず、任意の通信手段を介して、サポート装置などの任意のデバイスが接続されたことをセキュリティ事象とみなすようにしてもよい。そのため、典型的には、セキュリティ事象は、制御装置２で実行されるプログラム（ユーザプログラム３０）の開発が可能なサポート装置が制御装置へ接続されることを含むことになる。

【０１２４】

（ｅ３－３：電源監視）

次に、セキュリティ設定２０として、制御装置２の電源状態を監視する例について説明する。

【０１２５】

例えば、制御装置２の運用中に電源をオン／オフされた場合には、何らかの意図をもった行為であると想定される。そのため、制御装置２の電源がオン／オフされると、セキュリティ事象が発生したと判断してもよい。

【０１２６】

なお、制御装置２において、共通の電源装置からＣＰＵユニット１００およびセキュリティユニット２００へ電源が供給されている場合も想定される。このような構成においては、電源が遮断されることで、セキュリティユニット２００への電源供給も遮断されることが想定される。

【０１２７】

このような場合には、セキュリティユニット２００の内部にバッテリなどを配置しておき、外部電源が遮断された場合であっても、そのバッテリからの電力によりセキュリティ監視を継続するようにしてもよい。

【０１２８】
制御装置２の電源状態の監視は、典型的には、図４に示す状態取得モジュール２６０により出力されるＣＰＵユニット状態情報を監視することで実現される。
【０１２９】
このように、本実施の形態に係るセキュリティ事象は、制御装置２の電源状態が変化したことを含むようにしてもよい。
【０１３０】
（ｅ３－４：ハードスイッチ監視）
次に、セキュリティ設定２０として、制御装置２に設けられたハードスイッチの状態を監視する例について説明する。
【０１３１】
例えば、制御装置２の運用中にＣＰＵユニット１００に設けられたディップスイッチ（通常は、ＣＰＵユニット１００の動作モードなどを設定するために用いられる）が操作された場合には、何らかの意図をもった行為であると想定される。そのため、ＣＰＵユニット１００のハードスイッチ（例えば、ディップスイッチ）が操作されると、セキュリティ事象が発生したと判断してもよい。
【０１３２】
なお、ＣＰＵユニット１００のハードスイッチとしては、ディップスイッチに限らず、ロータリースイッチやトグルスイッチなどが想定される。
【０１３３】
このような制御装置２に設けられたハードスイッチの状態監視は、典型的には、図４に示す状態取得モジュール２６０により出力されるＣＰＵユニット状態情報を監視することで実現される。
【０１３４】
このように、本実施の形態に係るセキュリティ事象は、制御装置２に設けられたハードスイッチの状態が変化したことを含むようにしてもよい。
【０１３５】
（ｅ３－５：周囲環境監視）
次に、セキュリティ設定２０として、制御装置２の周囲環境を監視する例について説明する。
【０１３６】
通常、制御装置２は、所定の上限温度以下になるように、制御盤などに収容されているが、不審者が制御盤の冷却ファンを停止するなどの行為を行うと、制御盤内の温度が上昇し得る。このような制御装置の運用中における周囲環境に変化が生じると、セキュリティ事象が発生したと判断してもよい。具体例としては、最大定格温度が５５℃であるとすれば、それ以下の例えば５０℃に到達すると、セキュリティ事象の発生と判断してもよい。
【０１３７】
このような制御装置２の周囲環境の監視は、典型的には、図４に示す状態取得モジュール２６０により出力されるＣＰＵユニット状態情報を監視することで実現される。
【０１３８】
このように、本実施の形態に係るセキュリティ事象は、制御装置２の周囲環境が予め定められた条件になったことを含むようにしてもよい。
【０１３９】
（ｅ４－１：ユーザ認証：その１）
次に、セキュリティ設定２０として、サポート装置からＣＰＵユニット１００へのアクセスにおいて実施されるユーザ認証の認証結果を監視する例について説明する。
【０１４０】
図９は、サポート装置８００からＣＰＵユニット１００へのアクセス時の処理を説明するための模式図である。図９を参照して、サポート装置８００からＣＰＵユニット１００へのアクセスする際には、両者を接続した上で、ユーザがサポート装置８００を利用して

認証情報（典型的には、ユーザ名およびパスワード）を入力する。ＣＰＵユニット１００は、ユーザからの認証情報に基づいて認証処理を実行する。そして、ＣＰＵユニット１００は、サポート装置８００に対して認証結果を応答する。認証処理が成功した場合には、ＣＰＵユニット１００は、サポート装置８００からのアクセスを許可する。

【０１４１】

一方、認証処理が失敗した場合には、不正アクセスの可能性もあるので、セキュリティ事象の発生と判断してもよい。すなわち、サポート装置８００からＣＰＵユニット１００へのアクセス時の認証処理の失敗をトリガとして、セキュリティ事象の発生と判断してもよい。

【０１４２】

なお、単純な入力ミスの場合も想定されるため、サポート装置８００からＣＰＵユニット１００へのアクセス時の認証処理の失敗が複数回連続した場合に限って、セキュリティ事象の発生と判断してもよい。

【０１４３】

このようなサポート装置８００からＣＰＵユニット１００へのアクセス時におけるユーザ認証の認証結果の監視は、典型的には、図４に示す状態取得モジュール２６０により出力されるＣＰＵユニット状態情報を監視することで実現される。

【０１４４】

このように、本実施の形態に係るセキュリティ事象は、外部から制御装置２またはＣＰＵユニット１００へのアクセス時に要求されるユーザ認証が失敗したことを含むようにしてもよい。

【０１４５】

（ｅ４－２：ユーザ認証：その２）

次に、セキュリティ設定２０として、ネットワークからセキュリティユニット２００へのアクセスにおいて実施されるユーザ認証の認証結果を監視する例について説明する。

【０１４６】

上述の図４に示すように、セキュリティユニット２００は、ユーザ認証モジュール２６６を有しており、ネットワーク１０を介してセキュリティユニット２００へアクセスする際には、ユーザ認証が実行される。

【０１４７】

このユーザ認証が失敗した場合においても、上述の処理と同様に、認証処理の失敗をトリガとして、セキュリティ事象の発生と判断してもよい。すなわち、本実施の形態に係るセキュリティ事象は、外部から制御装置２またはＣＰＵユニット１００へのアクセス時に要求されるユーザ認証が失敗したことを含むようにしてもよい。

【０１４８】

（ｅ４－３：プログラム追加・更新／設定変更）

次に、セキュリティ設定２０として、ＣＰＵユニット１００で実行されるプログラムの追加・更新および／または設定の変更を監視する例について説明する。

【０１４９】

図１０は、サポート装置８００からＣＰＵユニット１００に格納されているプログラムおよび／または設定を変更する処理を説明するための模式図である。図１０を参照して、ユーザは、サポート装置８００上で任意のユーザプログラムを作成または改変した上で、当該作成または改変後のユーザプログラムをＣＰＵユニット１００へ転送する。それによって、ＣＰＵユニット１００に新たにユーザプログラムがインストールされ、あるいは、既に格納されていたユーザプログラムが更新される。

【０１５０】

あるいは、ユーザは、サポート装置８００を操作することで、ＣＰＵユニット１００に保持されている設定を変更することもできる。

【０１５１】

このようなＣＰＵユニット１００に対するプログラムの追加、ＣＰＵユニット１００で

実行されるプログラムの更新、ＣＰＵユニット１００における設定の変更などによって、ＣＰＵユニット１００の挙動が変化するため、このような操作がなされたことをトリガとして、セキュリティ事象の発生と判断してもよい。

【０１５２】

さらに、サポート装置８００からは、ＣＰＵユニット１００の主メモリ１０６に保持されているワーキングデータをオールクリアすることが可能である。このようなオールクリアすることで、ＣＰＵユニット１００のプログラムは初期状態が実行開始されることになる。このような初期状態からの実行は、それ以前の挙動とは異なる挙動を示す可能性があるため、セキュリティ事象の発生と判断してもよい。

【０１５３】

このようなＣＰＵユニット１００におけるプログラムの追加・変更および／または設定の変更のイベントは、典型的には、図４に示す状態取得モジュール２６０により出力されるＣＰＵユニット状態情報を監視することで検知される。同様に、ＣＰＵユニット１００の主メモリ１０６に対するオールクリアのイベントについても、図４に示す状態取得モジュール２６０により出力されるＣＰＵユニット状態情報を監視することで検知される。

【０１５４】

このように、本実施の形態に係るセキュリティ事象は、制御装置２で実行されるプログラムの追加および変更、ならびに、制御装置２における設定の変更のうち、いずれかが生じたことを含むようにしてもよい。また、本実施の形態に係るセキュリティ事象は、ＣＰＵユニット１００の主メモリ１０６に対するオールクリアの操作などがなされたことを含むようにしてもよい。

【０１５５】

＜Ｆ．通知＞

次に、セキュリティ事象の発生の検知に応答した通知のいくつかの例について説明する。

【０１５６】

（ｆ１：電子メールによる通知）

まず、セキュリティユニット２００からの電子メールによりセキュリティ事象の発生を通知する形態について説明する。

【０１５７】

図１１は、本実施の形態に係るセキュリティユニット２００から送信される電子メールの一例を説明するための模式図である。図１１を参照して、電子メールの表示画面５５０は、セキュリティユニット２００からの電子メールに含まれる、サブジェクト表示欄５５２と、送信元表示欄５５４と、受信日時欄５５６と、本文欄５５８とを含む。

【０１５８】

サブジェクト表示欄５５２には、セキュリティ事象の発生を通知するメッセージとともに、当該セキュリティ事象が発生した制御装置２を特定するための情報が表示されている。送信元表示欄５５４には、電子メールを送信したセキュリティユニット２００のサービスを示す情報が表示されている。受信日時欄５５６には、セキュリティユニット２００からの電子メールを受信した日時が表示されている。

【０１５９】

本文欄５５８には、発生したセキュリティ事象の内容を特定するためのコード、発生時刻、発生場所、緊急度等の情報が表示されている。

【０１６０】

さらに、本文欄５５８には、発生したセキュリティ事象の詳細を確認するためのリンク情報５６０が埋め込まれていてもよく、ユーザがリンク情報５６０を選択することで、当該電子メールの送信元であるセキュリティユニット２００、あるいは、セキュリティユニット２００からの情報を収集している任意のサーバ装置へアクセスすることで、発生したセキュリティ事象の詳細情報を取得できるようになっている。

【０１６１】

図１１に示す電子メールの内容は一例であり、任意の内容を電子メールにより通知してもよい。

【０１６２】

なお、通知される電子メールは、任意のデバイスにより閲覧可能である。任意のデバイスとしては、パーソナルコンピュータ、スマートフォン、タブレットなどが想定される。

【０１６３】

このように、本実施の形態に係るセキュリティユニット２００は、何らかのセキュリティ事象の発生を検知すると、その検知したセキュリティ事象を電子メールの手段を用いて、外部へ通知する。

【０１６４】

（ｆ２：表示装置５００への通知）

次に、セキュリティユニット２００から表示装置５００へセキュリティ事象の発生を通知する形態について説明する。

【０１６５】

図１２は、本実施の形態に係るセキュリティユニット２００から表示装置５００へのセキュリティ事象の通知の一例を説明するための模式図である。図１２を参照して、表示装置５００のディスプレイには、操業用の画面表示がなされている。画面表示には、制御対象を示すオブジェクト５０２に加えて、制御装置２を収容している制御盤を示すオブジェクト５０４が表示されていてもよい。

【０１６６】

このようなユーザインターフェイス画面が表示されている状態において、何らかのセキュリティ事象の発生が検知されると、当該セキュリティ事象が発生した制御装置２を収容している制御盤に対応する位置に、通知内容を示すオブジェクト５０６をポップアップ表示してもよい。

【０１６７】

オブジェクト５０６には、セキュリティ事象の発生を示すメッセージとともに、当該セキュリティ事象が発生した日時および緊急度などが表示されてもよい。図１２の表示例に限らず、より多くの情報を表示するようにしてもよいし、逆に、より簡素な表示内容としてもよい。

【０１６８】

さらに、表示装置５００からは、セキュリティ事象の発生を知らせるための通知音５０８を発するようにしてもよい。

【０１６９】

なお、通知先の表示装置５００は、セキュリティユニット２００と同一のネットワークに接続されているものに限らず、セキュリティユニット２００が通信可能であれば、いずれのネットワークに接続されている表示装置５００を通知先としてもよい。

【０１７０】

このように、本実施の形態に係るセキュリティユニット２００は、何らかのセキュリティ事象の発生を検知すると、その検知したセキュリティ事象をネットワーク接続された表示装置へ通知する。

【０１７１】

（ｆ３：データベース／クラウドサービスへの通知）

次に、セキュリティユニット２００からデータベースまたはクラウドサービスへセキュリティ事象の発生を通知する形態について説明する。

【０１７２】

図１３は、本実施の形態に係るセキュリティユニット２００からデータベースへのセキュリティ事象の通知の一例を説明するための模式図である。図１３を参照して、例えば、ネットワーク１０に接続されているサーバ装置６００にデータベースとしての処理を実装するとともに、セキュリティユニット２００が何らかのセキュリティ事象の発生を検知するとその内容をサーバ装置６００に通知する。

【０１７３】
サーバ装置６００は、セキュリティユニット２００からの通知の内容を逐次収集する。そして、サーバ装置６００は、外部からの要求（クエリ）に応答して、指定されたセキュリティ事象の内容を応答するようにしてもよい。
【０１７４】
図１３には、ネットワーク１０に接続されるサーバ装置６００を通知先とする例を示すが、これに限らず、インターネット上の任意のサーバ装置（すなわち、クラウドサービス）へセキュリティ事象の通知を行ってもよい。
【０１７５】
クラウドサービスを利用することで、セキュリティ事象を監視するためだけにサーバ装置６００を用意するような必要がなくなる。
【０１７６】
このように、本実施の形態に係るセキュリティユニット２００は、何らかのセキュリティ事象の発生を検知すると、その検知したセキュリティ事象をネットワーク接続されたデータベース／クラウドサービスへ通知する。
【０１７７】
（ｆ４：他の制御装置への通知）
次に、セキュリティユニット２００から他の制御装置へセキュリティ事象の発生を通知する形態について説明する。
【０１７８】
図１４は、本実施の形態に係るセキュリティユニット２００から他の制御装置へのセキュリティ事象の通知の一例を説明するための模式図である。図１４を参照して、例えば、同一のネットワーク１０に複数の制御装置２が接続されており、それぞれの制御装置２がセキュリティユニット２００を有しているような構成を想定する。
【０１７９】
いずれかのセキュリティユニット２００が何らかのセキュリティ事象の発生を検知すると、他の制御装置２のセキュリティユニット２００に対して、検知したセキュリティ事象の内容を通知する。他のセキュリティユニット２００から通知を受けたセキュリティユニット２００は、その通知の内容を逐次収集する。
【０１８０】
このような構成を採用することで、セキュリティユニット２００間でセキュリティ事象の相互検知が可能になる。
【０１８１】
さらに、セキュリティ事象の通知を受けた他の制御装置２は、その通知の緊急度などに応じて、接続されているフィールドデバイスを用いて、何らかの物理的な報知（音、光、振動など）を行うようにしてもよい。
【０１８２】
このように、本実施の形態に係るセキュリティユニット２００は、何らかのセキュリティ事象の発生を検知すると、その検知したセキュリティ事象をネットワーク接続された他の制御装置２へ通知する。
【０１８３】
（ｆ５：イベント通知）
次に、セキュリティユニット２００からセキュリティ事象の発生を、ネットワークを介してイベント通知する形態について説明する。
【０１８４】
図１５は、本実施の形態に係るセキュリティユニット２００からネットワークを介してイベント通知する一例を説明するための模式図である。図１５を参照して、ネットワーク１０にセキュリティ事象の発生を報知するための報知部１０００を配置した構成を想定する。
【０１８５】

セキュリティユニット２００が何らかのセキュリティ事象の発生を検知すると、ネットワーク１０を介して、報知部１０００に対して通知パケットを送出する。報知部１０００は、セキュリティユニット２００からの通知パケットを受信すると、その通知パケットの内容に従って、物理的な報知（音、光、振動など）を開始する。

【０１８６】

通知パケットとしては、例えば、ＳＮＭＰ（Simple Network Management Protocol）トラップなどを利用できる。ＳＮＭＰトラップに限られず、イベントを通知できるものであれば、どのようなプロコトルを採用してもよい。

【０１８７】

このような構成を採用することで、ネットワーク上の任意の位置に配置された報知部に対してセキュリティ事象の発生を通知できる。

【０１８８】

このように、本実施の形態に係るセキュリティユニット２００は、何らかのセキュリティ事象の発生を検知すると、その検知したセキュリティ事象を、ネットワークを介してイベント通知するようにしてもよい。このようなイベント通知を受けて、ネットワーク上に配置された報知部１０００は報知動作を開始するようにしてもよい。

【０１８９】

（ｆ６：緊急度／優先度表示）

上述したように、本実施の形態に係る制御システム１においては、１または複数の状態値やイベントを監視して、セキュリティ事象の発生の有無を判断する。通常、それぞれのセキュリティ事象は、各事象に応じた緊急度および／または優先度を有しており、必ずしも同一ではない。

【０１９０】

そこで、監視対象のセキュリティ事象毎に緊急度および／または優先度を予め設定しておき、何らかのセキュリティ事象の発生が検知されると、当該検知されたセキュリティ事象の緊急度および／または優先度を併せて通知するようにしてもよい。

【０１９１】

このような緊急度および／または優先度の通知方法としては、上述の図１１および図１２に示すような文字情報を用いてもよいし、図１５に示すような報知部１０００を用いる場合には、報知部１０００が発する色、点灯パターン、音色、音量などを異ならせることで通知してもよい。

【０１９２】

検知されたセキュリティ事象の緊急度および／または優先度を通知することで、その通知を受けたユーザは、どの程度の緊急度および／または優先度で、当該検知されたセキュリティ事象に対する対処を行わなければならないのかを即座に把握できる。

【０１９３】

＜Ｇ．処理手順＞

次に、本実施の形態に係るセキュリティユニット２００におけるセキュリティ事象を監視する処理手順の一例について説明する。

【０１９４】

図１６は、本実施の形態に係るセキュリティユニット２００におけるセキュリティ事象を監視する処理手順を示すフローチャートである。図１６に示す各ステップは、典型的には、セキュリティユニット２００のプロセッサ２０２がファームウェア２２を実行することで実現される。図１６に示す処理手順は、所定周期毎に繰返し実行され、あるいは、予め定められたイベント発生毎に実行される。

【０１９５】

図１６を参照して、セキュリティユニット２００は、ネットワーク１０を介したデータの送受信が発生したか否かを判断する（ステップＳ１００）。ネットワーク１０を介したデータの送受信が発生していなければ（ステップＳ１００においてＮＯ）、ステップＳ１０２～Ｓ１０６の処理はスキップされる。

【０１９６】
ネットワーク１０を介したデータの送受信が発生すれば（ステップＳ１００においてＹＥＳ）、セキュリティユニット２００は、データの送信先および／または送信元がアクセスコントロールによって制限されているか否かを判断する（ステップＳ１０２）。データの送信先および／または送信元がアクセスコントロールによって制限されていれば（ステップＳ１０２においてＹＥＳ）、セキュリティユニット２００は、セキュリティ事象の発生と判断する（ステップＳ１０４）。そして、ステップＳ１２０に規定される通知処理が実行される。
【０１９７】
データの送信先および／または送信元がアクセスコントロールによって制限されていなければ（ステップＳ１０２においてＮＯ）、セキュリティユニット２００は、データの送信または受信のパターンが予め定められたセキュリティ事象の発生と判断されるパターンと合致するか否かを判断する（ステップＳ１０６）。データの送信または受信のパターンが予め定められたセキュリティ事象の発生と判断されるパターンと合致すれば（ステップＳ１０６においてＹＥＳ）、セキュリティユニット２００は、セキュリティ事象の発生と判断する（ステップＳ１０４）。そして、ステップＳ１２０に規定される通知処理が実行される。
【０１９８】
続いて、セキュリティユニット２００は、ＣＰＵユニット１００からＣＰＵユニット状態情報を取得し（ステップＳ１０８）、取得したＣＰＵユニット状態情報がセキュリティ設定２０に規定されたいずれかのセキュリティ事象の条件に合致しているか否かを判断する（ステップＳ１１０）。取得したＣＰＵユニット状態情報がいずれかのセキュリティ事象の条件に合致していれば（ステップＳ１１０においてＹＥＳ）、セキュリティユニット２００は、セキュリティ事象の発生と判断する（ステップＳ１０４）。そして、ステップＳ１２０に規定される通知処理が実行される。
【０１９９】
取得したＣＰＵユニット状態情報がいずれかのセキュリティ事象の条件に合致していなければ（ステップＳ１１０においてＮＯ）、処理は終了する。
【０２００】
ステップＳ１２０において、セキュリティユニット２００は、検知されたセキュリティ事象に応じて、通知処理を実行する。そして、処理は終了する。
【０２０１】
＜Ｈ．変形例＞
（ｈ１：一体型）
上述の本実施の形態に係る制御システム１においては、ＣＰＵユニット１００にセキュリティユニット２００を接続する構成を例示したが、このような分離型ではなく、両者を一体化した構成を採用してもよい。この場合には、ＣＰＵユニット１００の内部に、セキュリティユニット２００が提供する処理を実現するためのソフトウェア実装および／またはハードウェア実装の構成が配置される。
【０２０２】
このような一体型の構成を採用することで、制御システム全体を省スペース化できる。
（ｈ２：外付型）
上述の本実施の形態に係る制御システム１においては、ＣＰＵユニット１００のネットワークポートではなく、セキュリティユニット２００のネットワークポートを利用して、ネットワーク接続する構成を例示したが、本実施の形態に係るセキュリティ事象の監視処理を既存の制御装置に適用する場合には、外付型のセキュリティユニットを採用するようにしてもよい。
【０２０３】
図１７は、本実施の形態の変形例に係る制御システム１Ａの概略構成を示す模式図である。図１７を参照して、制御システム１Ａにおいては、制御装置２Ａは、ＣＰＵユニット

１００と１または複数の機能ユニット３００とにより構成される。セキュリティユニット２００Ａは、ネットワーク１０と制御装置２Ａとの間を仲介するように配置される。

【０２０４】

より具体的には、セキュリティユニット２００Ａは、２つのネットワークポートを有しており、一方のネットワークポートはネットワーク１０に接続されるとともに、他方のネットワークポートは制御装置２Ａに含まれるＣＰＵユニット１００のネットワークポート１１８Ｐに接続されている。このような構成において、ＣＰＵユニット１００は、セキュリティユニット２００Ａを介して、ネットワーク１０に接続されたデバイスとの間でデータ通信を行う。

【０２０５】

セキュリティユニット２００Ａは、ＣＰＵユニット１００から送出されるデータおよびＣＰＵユニット１００で受信されるデータを監視することで、セキュリティ事象の発生の有無を常時監視できる。

【０２０６】

セキュリティユニット２００Ａは、さらに、ＣＰＵユニット１００と別のデータ伝送手段を介して接続されていてもよい。このような別のデータ伝送手段を採用することで、セキュリティユニット２００Ａは、ＣＰＵユニット１００のＣＰＵユニット状態情報を取得することができる。このようなＣＰＵユニット状態情報によって、ＣＰＵユニット１００に対する直接のアクセスによって生じるセキュリティ事象の発生についても常時監視できる。

【０２０７】

（ｈ３：その他）

本実施の形態に係るセキュリティユニットは、ＣＰＵユニット１００およびＣＰＵユニット１００を含む制御装置２におけるセキュリティ事象の発生を監視できるものであれば、どのような形態で実装されてもよい。

【０２０８】

＜Ｉ．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］

制御対象を制御する制御装置（２）であって、

前記制御対象に応じて作成されたプログラムを実行するプログラム実行部（１０２）と、

前記制御装置に対する外部からのアクセスにおいてセキュリティ事象が発生したか否かを判断する検知部（２６２）と、

前記セキュリティ事象が発生したと検知されると、当該発生したセキュリティ事象に応じた通知先へ通知する通知部（２６４）とを備え、

前記セキュリティ事象は、予め定められた規則に適合しない事象を含む、制御装置。

［構成２］

前記セキュリティ事象は、

前記制御装置の動作を停止または性能を低下させる挙動および行為、

前記制御装置におけるプログラムの実行処理を停止または性能を低下させる挙動および行為、ならびに

前記制御対象の動作を停止または性能を低下させる挙動および行為、のいずれかを含む、構成１に記載の制御装置。

［構成３］

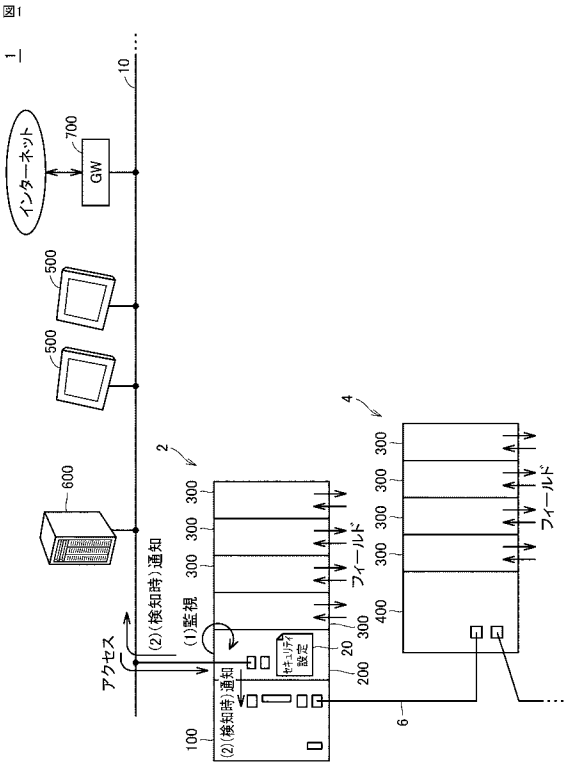
前記セキュリティ事象は、データの送信先または送信元のネットワークアドレス、物理アドレス、ポート番号のうちいずれかが、予め定められたアクセスを許可されたリストに含まれていない、および、予め定められたアクセスを禁止されたリストに含まれている、のいずれかに該当することを含む、構成１または２に記載の制御装置。

［構成４］

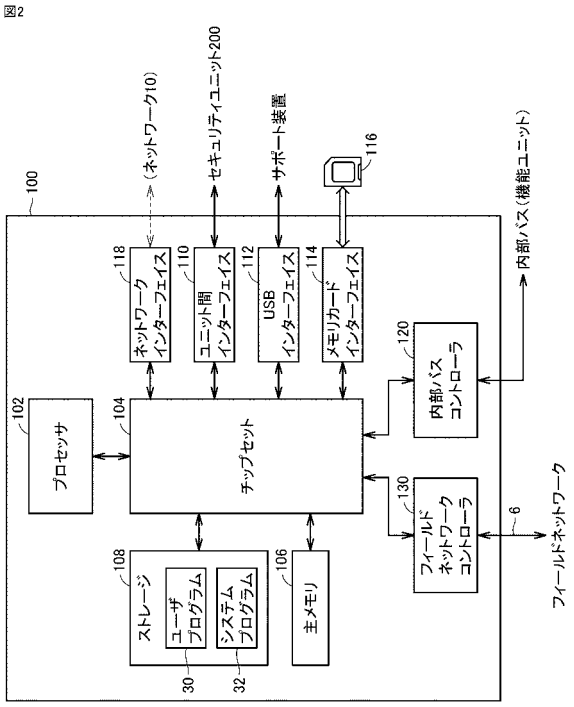
前記制御装置は、前記プログラム実行部を含む第１のユニット（１００）と、前記検知部を含む第２のユニット（２００）を備え、
前記第１のユニットは、ネットワーク接続するためのポート（１１８Ｐ）を有しており、
前記セキュリティ事象は、前記第１のユニットのポートが無効化されている場合に、当該ポートがネットワーク接続されることを含む、構成１～３のいずれか１項に記載の制御装置。
［構成５］
前記セキュリティ事象は、外部から前記制御装置へのアクセス時に要求されるユーザ認証が失敗したことを含む、構成１～４のいずれか１項に記載の制御装置。
［構成６］
前記セキュリティ事象は、前記制御装置で実行されるプログラムの開発が可能なサポート装置が前記制御装置へ接続されることを含む、構成１～５のいずれか１項に記載の制御装置。
［構成７］
前記セキュリティ事象は、前記制御装置で実行されるプログラムの追加および変更、ならびに、前記制御装置における設定の変更のうち、いずれかが生じたことを含む、構成１～６のいずれか１項に記載の制御装置。
［構成８］
前記通知部は、セキュリティ事象の発生をネットワークを介してイベント通知する、構成１～７のいずれか１項に記載の制御装置。
［構成９］
ネットワーク上に配置された報知部（１０００）は、前記通知部からのイベント通知を受けて、報知動作を開始する、構成８に記載の制御装置。
［構成１０］
制御対象を制御する制御システム（１）であって、
前記制御対象に応じて作成されたプログラムを実行するプログラム実行部を含む第１のユニット（１００）と、
前記第１のユニットに対する外部からのアクセスにおいてセキュリティ事象が発生したか否かを判断する検知部（２６２）、ならびに、前記セキュリティ事象が発生したと検知されると、当該発生したセキュリティ事象に応じた通知先へ通知する通知部（２６４）を含む第２のユニット（２００）とを備え、
前記セキュリティ事象は、予め定められた規則に適合しない事象を含む、制御システム。
【０２０９】
＜Ｊ．まとめ＞
本実施の形態に係る制御装置および制御システムによれば、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。
【０２１０】
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】
【０２１１】
１，１Ａ　制御システム、２，２Ａ　制御装置、４　リモートＩＯ装置、６　フィールドネットワーク、１０　ネットワーク、２０　セキュリティ設定、２２　ファームウェア、２４　履歴情報、３０　ユーザプログラム、３２　システムプログラム、１００　ＣＰＵユニット、１０２，２０２　プロセッサ、１０４，２０４　チップセット、１０６，２

０６　主メモリ、１０８，２０８　ストレージ、１１０，２１０　ユニット間インターフェイス、１１２　ＵＳＢインターフェイス、１１２Ｐ　ＵＳＢポート、１１４　メモリカードインターフェイス、１１４Ｐ　メモリカードスロット、１１６　メモリカード、１１８，２２０　ネットワークインターフェイス、１１８Ｐ　ネットワークポート、１２０　内部バスコントローラ、１３０　フィールドネットワークコントローラ、１３０Ｐ１，１３０Ｐ２　フィールドネットワークポート、２００，２００Ａ　セキュリティユニット、２２２　送受信部、２２４　コントローラ、２２６　バッファ、２５０　フレーム抽出モジュール、２５２　解析モジュール、２５４　内容解析処理、２５６　特徴抽出処理、２５８　統計処理、２６０　状態取得モジュール、２６２　検知モジュール、２６４　通知モジュール、２６６　ユーザ認証モジュール、３００　機能ユニット、４００　カプラユニット、５００　表示装置、５０２，５０４，５０６　オブジェクト、５０８　通知音、５５０　表示画面、５５２　サブジェクト表示欄、５５４　元表示欄、５５６　受信日時欄、５５８　本文欄、５６０　リンク情報、６００　サーバ装置、７００　ゲートウェイ、８００　サポート装置、９００　デバイス、１０００　報知部。

【図１】

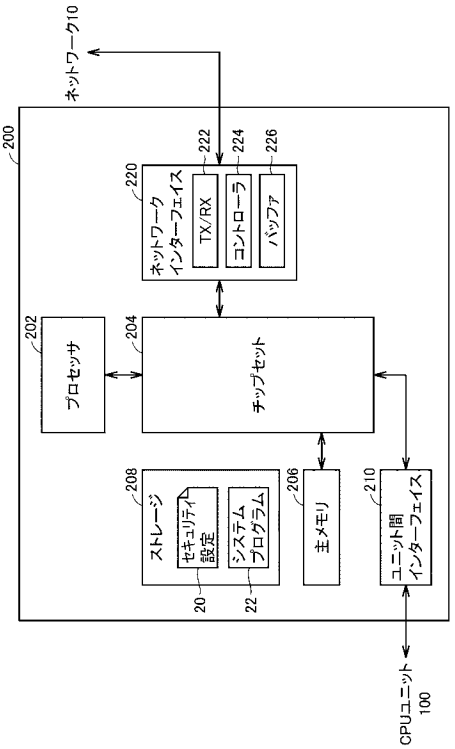


【図２】



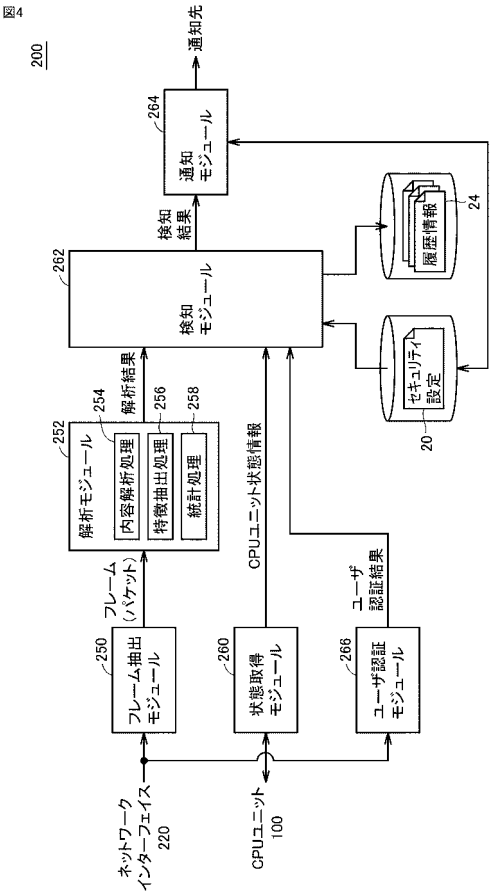
【図３】

図3



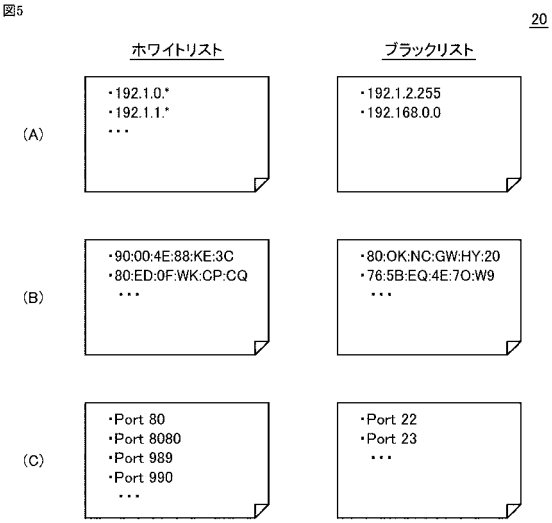
【図４】

図4



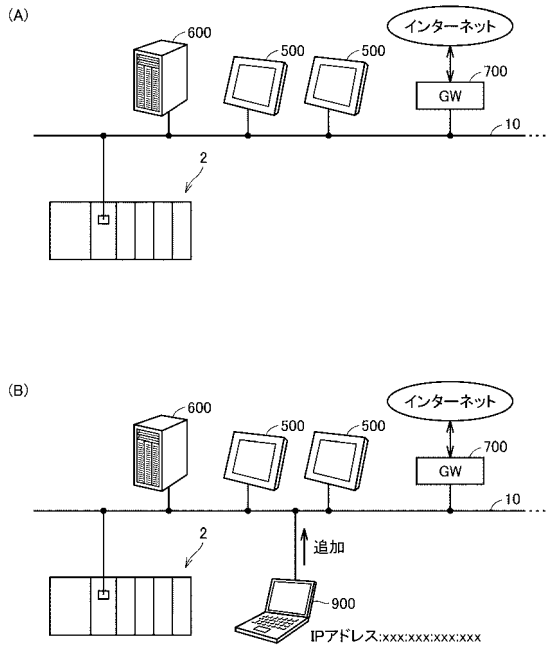
【図５】

図5



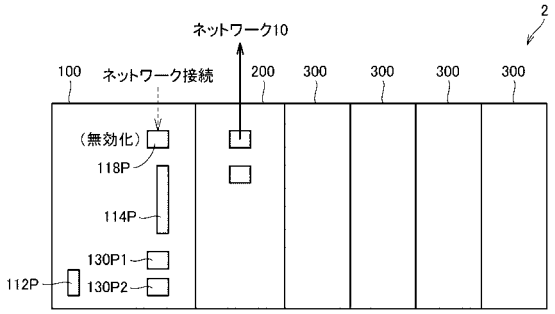
【図６】

図6



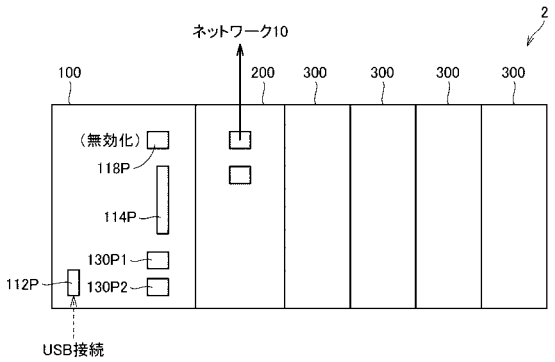
【図７】

図7



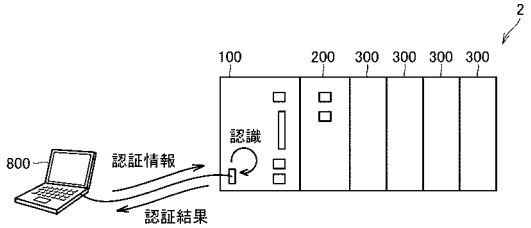
【図８】

図8



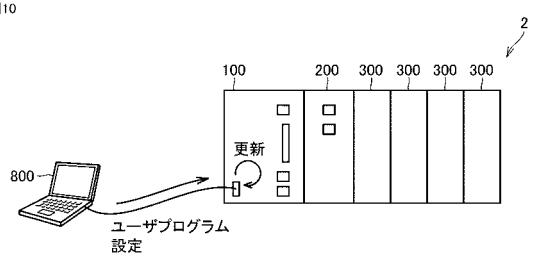
【図９】

図9



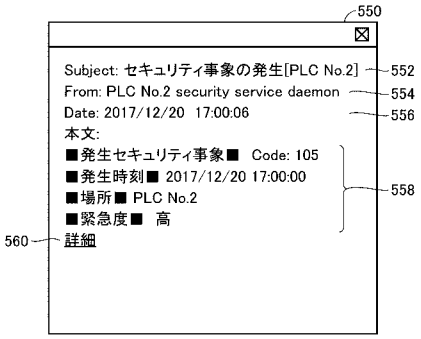
【図１０】

図10



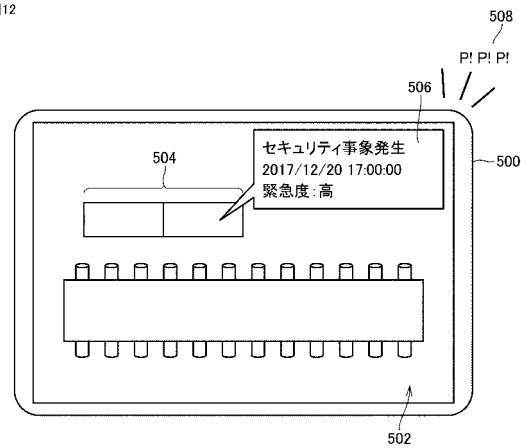
【図１１】

図11



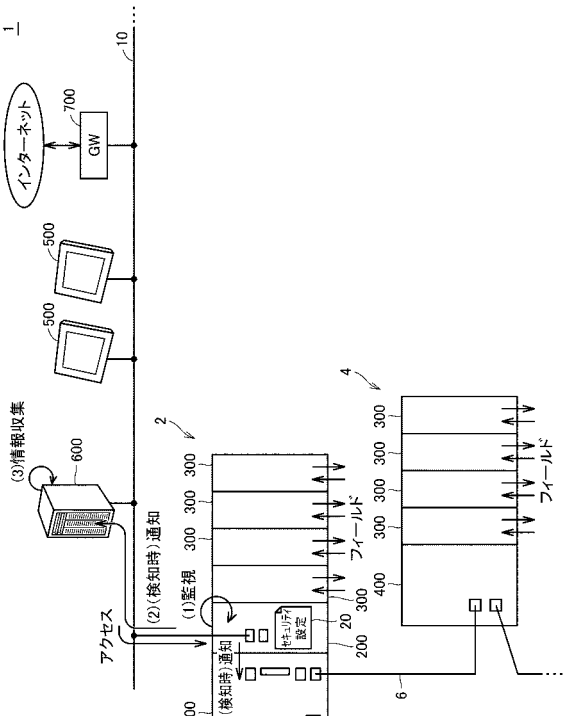
【図１２】

図12



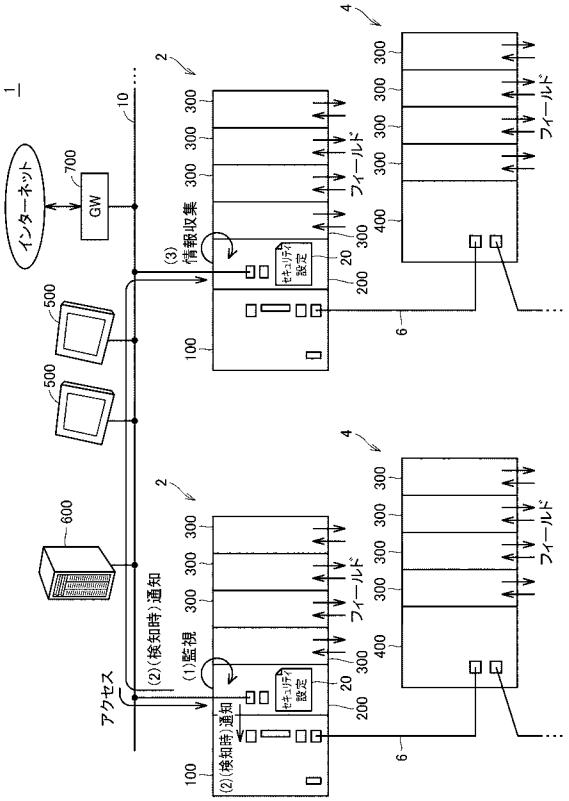
【図１３】

図13



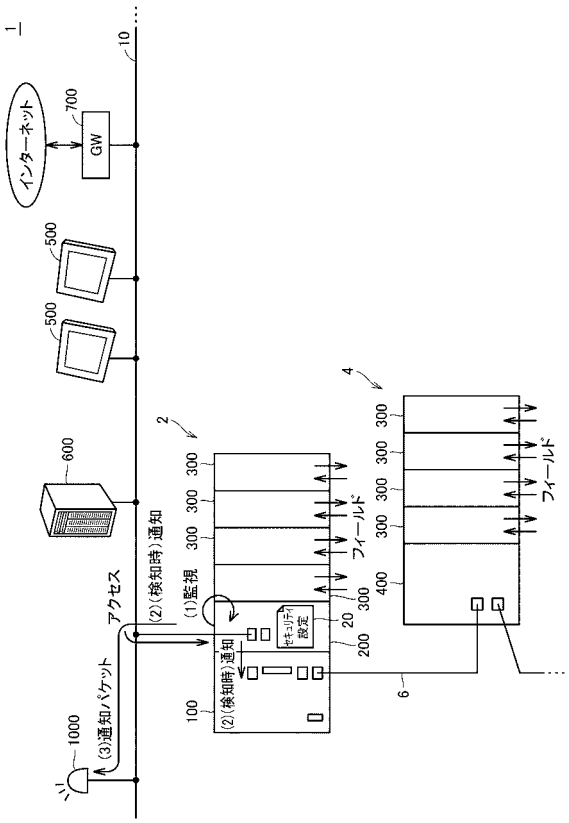
【図１４】

図14



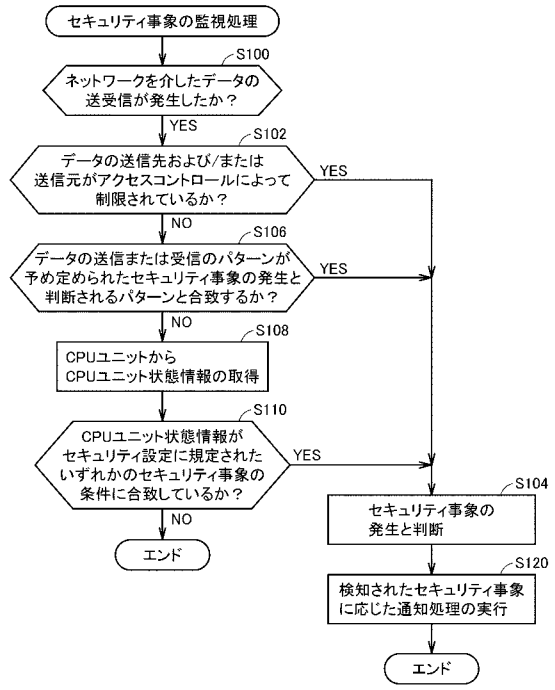
【図１５】

図15



【図１６】

図16



【図１７】

図17