

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第6977507号  
(P6977507)

(45) 発行日 令和3年12月8日(2021.12.8)

(24) 登録日 令和3年11月15日(2021.11.15)

(51) Int.Cl. F I  
**G05B 19/048 (2006.01)** G O 5 B 19/048  
**G06F 21/55 (2013.01)** G O 6 F 21/55 3 2 0

請求項の数 10 (全 29 頁)

<p>(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)                  (65) 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)                  審査請求日 令和2年3月4日(2020.3.4)</p>	<p>(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 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                  審査官 大古 健一</p>
---	---

最終頁に続く

(54) 【発明の名称】 制御装置および制御システム

(57) 【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、  
ネットワーク接続するためのポートとを備え、  
前記セキュリティ事象は、前記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、 制御装置。

10

【請求項2】

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、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、 制御装置。

20

## 【請求項 3】

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 または 2に記載の制御装置。

## 【請求項 4】

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 ~ 3 のいずれか 1 項に記載の制御装置。

10

## 【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 ~ 5 のいずれか 1 項に記載の制御装置。

## 【請求項 7】

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 ~ 6 のいずれか 1 項に記載の制御装置。

20

## 【請求項 8】

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 7 に記載の制御装置。

## 【請求項 9】

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、

30

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、制御システム。

## 【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、

40

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、前記制御システム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システムへ接続されることを含む、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

50

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。

10

【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。

20

【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。

30

【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。

40

【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】

50

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。

【 0 0 1 2 】

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。

【 0 0 1 3 】

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。

10

【 0 0 1 4 】

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。

【 0 0 1 5 】

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。

【 0 0 1 6 】

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。

20

【 0 0 1 7 】

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。

【 0 0 1 8 】

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。

【 0 0 1 9 】

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。

30

【 0 0 2 0 】

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。

【 0 0 2 1 】

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。

40

【 0 0 2 2 】

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。

【 0 0 2 3 】

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。

【 0 0 2 4 】

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。

50

## 【 0 0 2 5 】

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。

## 【 0 0 2 6 】

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

10

## 【 0 0 2 7 】

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 】

## 【 0 0 2 8 】

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。

20

## 【 図面の簡単な説明 】

## 【 0 0 2 9 】

【 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。

30

【 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。

40

【 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

50

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 I/O (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 I/O 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

10

20

30

40

50

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。

【 0 0 3 8 】

セキュリティユニット 2 0 0 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 2 0 0 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。

【 0 0 3 9 】

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 1 0 0、あるいは、CPU ユニット 1 0 0 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 1 0 0、あるいは、CPU ユニット 1 0 0 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。

【 0 0 4 0 】

なお、説明の便宜上、それぞれ独立した CPU ユニット 1 0 0 とセキュリティユニット 2 0 0 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 1 0 0 に接続される「ユニット」の形ではなく、CPU ユニット 1 0 0 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 2 0 0 が提供する処理を実装してもよい。

【 0 0 4 1 】

< B . 制御システムの全体構成例 >

引き続き図 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。

【 0 0 4 2 】

制御装置 2 に含まれる機能ユニット 3 0 0 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 3 0 0 は、CPU ユニット 1 0 0 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 3 0 0 としては、例えば、制御対象からのデジタル信号を受取る D I (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 D O (Digital Output) モジュール、制御対象からのアナログ信号を受取る A I (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 A O (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 3 0 0 としては、P I D (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。

【 0 0 4 3 】

制御装置 2 とリモート I O 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、E t h e r C A T (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。

【 0 0 4 4 】

リモート I O 装置 4 は、カプラユニット 4 0 0 と、1 または複数の機能ユニット 3 0 0 とを含む。カプラユニット 4 0 0 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 I O 装置 4 に含まれる機能ユニット 3 0 0 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。

【 0 0 4 5 】

機能ユニット 3 0 0 については、制御装置 2 に含まれる機能ユニット 3 0 0 と同様であ

10

20

30

40

50

るので、詳細な説明は繰返さない。

【 0 0 4 6 】

制御装置 2 と表示装置 5 0 0 およびサーバ装置 6 0 0 とを接続するネットワーク 1 0 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。

【 0 0 4 7 】

表示装置 5 0 0 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。

【 0 0 4 8 】

サーバ装置 6 0 0 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 1 0 に接続するようにしてもよい。

【 0 0 4 9 】

ゲートウェイ 7 0 0 は、ネットワーク 1 0 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。

【 0 0 5 0 】

< 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。

【 0 0 5 1 】

（ c 1 : CPU ユニット 1 0 0 ）

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 1 0 0 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 1 0 0 は、プロセッサ 1 0 2 と、チップセット 1 0 4 と、主メモリ 1 0 6 と、ストレージ 1 0 8 と、ユニット間インターフェイス 1 1 0 と、USB（Universal Serial Bus）インターフェイス 1 1 2 と、メモリカードインターフェイス 1 1 4 と、ネットワークインターフェイス 1 1 8 と、内部バスコントローラ 1 2 0 と、フィールドネットワークコントローラ 1 3 0 とを含む。

【 0 0 5 2 】

プロセッサ 1 0 2 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 1 0 2 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 1 0 2 を複数配置してもよい。このように、CPU ユニット 1 0 0 は、1 または複数のプロセッサ 1 0 2、および / または、1 または複数のコアを有するプロセッサ 1 0 2 を有している。チップセット 1 0 4 は、プロセッサ 1 0 2 および周辺エレメントを制御することで、CPU ユニット 1 0 0 全体としての処理を実現する。主メモリ 1 0 6 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 1 0 8 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。

【 0 0 5 3 】

プロセッサ 1 0 2 は、ストレージ 1 0 8 に格納された各種プログラムを読み出して、主メモリ 1 0 6 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 1 0 8 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 3 2 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 3 0 が格納される。

【 0 0 5 4 】

ユニット間インターフェイス 1 1 0 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 1 0 0 のユニット間インタ

10

20

30

40

50

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、P C I E x p r e s s）などに従うデバイスを採用できる。

【0055】

U S Bインターフェイス112は、U S B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리카ードインターフェイス114は、メモ리카ード116が着脱可能に構成されており、メモ리카ード116に対してデータを書込み、メモ리카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）を読み出すことが可能になっている。

10

【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、C P U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、C P U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】

20

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、A S I CまたはF P G A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を含む。

30

【0061】

プロセッサ202は、C P U、M P U、G P Uなどで構成される。上述のC P U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、D R A MやS R A M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み出して、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。

40

【0063】

ユニット間インターフェイス210は、上述のC P U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C P Uユニット100とが接続される。

50

## 【 0 0 6 4 】

ネットワークインターフェイス 2 2 0 は、ネットワーク 1 0 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 2 2 0 は、主たるコンポーネントとして、送受信部 2 2 2 と、コントローラ 2 2 4 と、バッファ 2 2 6 とを含む。

## 【 0 0 6 5 】

送受信部 2 2 2 は、OS I 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 1 0 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 1 0 を介したエンコードされた信号の送信を担当する。

## 【 0 0 6 6 】

コントローラ 2 2 4 は、主として、OS I 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。

## 【 0 0 6 7 】

バッファ 2 2 6 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。

## 【 0 0 6 8 】

図 3 には、プロセッサ 2 0 2 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。

## 【 0 0 6 9 】

（ c 3 : 機能ユニット 3 0 0 およびカプラユニット 4 0 0 ）

本実施の形態に係る制御装置 2 およびリモート I O 装置 4 に含まれる機能ユニット 3 0 0、ならびに、リモート I O 装置 4 に含まれるカプラユニット 4 0 0 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。

## 【 0 0 7 0 】

< 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 2 0 0 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 2 0 0 の機能構成例を示すブロック図である。

## 【 0 0 7 1 】

図 4 を参照して、セキュリティユニット 2 0 0 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 2 5 0 と、解析モジュール 2 5 2 と、状態取得モジュール 2 6 0 と、検知モジュール 2 6 2 と、通知モジュール 2 6 4 と、ユーザ認証モジュール 2 6 6 とを含む。

## 【 0 0 7 2 】

フレーム抽出モジュール 2 5 0 は、ネットワーク 1 0 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 2 2 0 から抽出する。フレーム抽出モジュール 2 5 0 は、抽出したフレームまたはパケットを解析モジュール 2 5 2 へ出力する。

## 【 0 0 7 3 】

解析モジュール 2 5 2 は、フレーム抽出モジュール 2 5 0 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 2 6 2 へ出力する。解析モジュール 2 5 2 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 2 5 2 は、内容解析処理 2 5 4 と、特徴抽出処理 2 5 6 と、統計処理 2 5 8 とが実行可能になっている。

## 【 0 0 7 4 】

内容解析処理 2 5 4 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。

10

20

30

40

50

## 【 0 0 7 5 】

特徴抽出処理 2 5 6 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。

## 【 0 0 7 6 】

統計処理 2 5 8 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。

## 【 0 0 7 7 】

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 2 6 2 へ出力される。

## 【 0 0 7 8 】

状態取得モジュール 2 6 0 は、CPU ユニット 1 0 0 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 2 6 2 へ出力する。CPU ユニット状態情報は、例えば、CPU ユニット 1 0 0 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。

## 【 0 0 7 9 】

検知モジュール 2 6 2 は、セキュリティ設定 2 0 を参照して、解析モジュール 2 5 2 からの解析結果、および/または、状態取得モジュール 2 6 0 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。

## 【 0 0 8 0 】

検知モジュール 2 6 2 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 2 6 4 へ出力する。

## 【 0 0 8 1 】

検知モジュール 2 6 2 は、検知したセキュリティ事象を示す情報を履歴情報 2 4 として登録する。

## 【 0 0 8 2 】

通知モジュール 2 6 4 は、検知モジュール 2 6 2 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。

## 【 0 0 8 3 】

ユーザ認証モジュール 2 6 6 は、ネットワーク 1 0 を介してセキュリティユニット 2 0 0 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 2 6 6 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 2 6 2 へ出力する。

## 【 0 0 8 4 】

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。

## 【 0 0 8 5 】

< 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。

## 【 0 0 8 6 】

( e 1 - 1 : アクセスコントロール )

まず、セキュリティ設定 2 0 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。

## 【 0 0 8 7 】

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。

10

20

30

40

50

## 【 0 0 8 8 】

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。

## 【 0 0 8 9 】

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。

10

## 【 0 0 9 0 】

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。

## 【 0 0 9 1 】

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。

20

## 【 0 0 9 2 】

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。

## 【 0 0 9 3 】

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わせてもよい。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。

30

## 【 0 0 9 4 】

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。

## 【 0 0 9 5 】

（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。

40

## 【 0 0 9 6 】

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。

## 【 0 0 9 7 】

50

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イルスについては、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】

10

20

30

40

50

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리카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

10

20

30

40

50

。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。

【 0 1 2 0 】

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 1 0 0 の表面には、USB ポート 1 1 2 P と、メモ리카ードスロット 1 1 4 P と、ネットワークポート 1 1 8 P と、フィールドネットワークポート 1 3 0 P 1 , 1 3 0 P 2 とが配置されている。

【 0 1 2 1 】

例えば、制御装置 2 の運用中において、USB ポート 1 1 2 P 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。

10

【 0 1 2 2 】

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 2 6 0 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。

【 0 1 2 3 】

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 1 1 2 P 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 3 0 ）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。

20

【 0 1 2 4 】

（ e 3 - 3 : 電源監視 ）

次に、セキュリティ設定 2 0 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。

【 0 1 2 5 】

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。

30

【 0 1 2 6 】

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 1 0 0 およびセキュリティユニット 2 0 0 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 2 0 0 への電源供給も遮断されることが想定される。

【 0 1 2 7 】

このような場合には、セキュリティユニット 2 0 0 の内部にバッテリー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、そのバッテリー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。

40

【 0 1 2 8 】

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 2 6 0 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。

【 0 1 2 9 】

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。

【 0 1 3 0 】

（ e 3 - 4 : ハードスイッチ監視 ）

次に、セキュリティ設定 2 0 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

50

監視する例について説明する。

【 0 1 3 1 】

例えば、制御装置 2 の運用中に CPU ユニット 1 0 0 に設けられたディップスイッチ（通常は、CPU ユニット 1 0 0 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 1 0 0 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。

【 0 1 3 2 】

なお、CPU ユニット 1 0 0 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。

10

【 0 1 3 3 】

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 2 6 0 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。

【 0 1 3 4 】

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。

【 0 1 3 5 】

（ e 3 - 5 : 周囲環境監視 ）

次に、セキュリティ設定 2 0 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。

20

【 0 1 3 6 】

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 5 5 であるとするれば、それ以下の例えば 5 0 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。

【 0 1 3 7 】

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 2 6 0 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。

30

【 0 1 3 8 】

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。

【 0 1 3 9 】

（ e 4 - 1 : ユーザ認証 : その 1 ）

次に、セキュリティ設定 2 0 として、サポート装置から CPU ユニット 1 0 0 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。

【 0 1 4 0 】

図 9 は、サポート装置 8 0 0 から CPU ユニット 1 0 0 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 8 0 0 から CPU ユニット 1 0 0 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 8 0 0 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 1 0 0 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 1 0 0 は、サポート装置 8 0 0 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 1 0 0 は、サポート装置 8 0 0 からのアクセスを許可する。

40

【 0 1 4 1 】

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 8 0 0 から CPU ユニット 1 0 0 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。

50

## 【 0 1 4 2 】

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 8 0 0 から CPU ユニット 1 0 0 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。

## 【 0 1 4 3 】

このようなサポート装置 8 0 0 から CPU ユニット 1 0 0 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 2 6 0 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。

## 【 0 1 4 4 】

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 1 0 0 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。

10

## 【 0 1 4 5 】

( e 4 - 2 : ユーザ認証 : その 2 )

次に、セキュリティ設定 2 0 として、ネットワークからセキュリティユニット 2 0 0 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。

## 【 0 1 4 6 】

上述の図 4 に示すように、セキュリティユニット 2 0 0 は、ユーザ認証モジュール 2 6 6 を有しており、ネットワーク 1 0 を介してセキュリティユニット 2 0 0 へアクセスする際には、ユーザ認証が実行される。

20

## 【 0 1 4 7 】

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 1 0 0 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。

## 【 0 1 4 8 】

( e 4 - 3 : プログラム追加・更新 / 設定変更 )

次に、セキュリティ設定 2 0 として、CPU ユニット 1 0 0 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。

## 【 0 1 4 9 】

図 1 0 は、サポート装置 8 0 0 から CPU ユニット 1 0 0 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 1 0 を参照して、ユーザは、サポート装置 8 0 0 上で任意のユーザプログラムを作成または変更した上で、当該作成または変更後のユーザプログラムを CPU ユニット 1 0 0 へ転送する。それによって、CPU ユニット 1 0 0 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。

30

## 【 0 1 5 0 】

あるいは、ユーザは、サポート装置 8 0 0 を操作することで、CPU ユニット 1 0 0 に保持されている設定を変更することもできる。

## 【 0 1 5 1 】

このような CPU ユニット 1 0 0 に対するプログラムの追加、CPU ユニット 1 0 0 で実行されるプログラムの更新、CPU ユニット 1 0 0 における設定の変更などによって、CPU ユニット 1 0 0 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。

40

## 【 0 1 5 2 】

さらに、サポート装置 8 0 0 からは、CPU ユニット 1 0 0 の主メモリ 1 0 6 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 1 0 0 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。

50

## 【 0 1 5 3 】

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。

## 【 0 1 5 4 】

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。

## 【 0 1 5 5 】

< 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。

## 【 0 1 5 6 】

( f 1 : 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。

## 【 0 1 5 7 】

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。

## 【 0 1 5 8 】

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。

## 【 0 1 5 9 】

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。

## 【 0 1 6 0 】

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。

## 【 0 1 6 1 】

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。

## 【 0 1 6 2 】

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。

## 【 0 1 6 3 】

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。

10

20

30

40

50

## 【 0 1 6 4 】

( f 2 : 表示装置 5 0 0 への通知 )

次に、セキュリティユニット 2 0 0 から表示装置 5 0 0 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。

## 【 0 1 6 5 】

図 1 2 は、本実施の形態に係るセキュリティユニット 2 0 0 から表示装置 5 0 0 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 1 2 を参照して、表示装置 5 0 0 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 5 0 2 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 5 0 4 が表示されていてもよい。

10

## 【 0 1 6 6 】

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 5 0 6 をポップアップ表示してもよい。

## 【 0 1 6 7 】

オブジェクト 5 0 6 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 1 2 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。

20

## 【 0 1 6 8 】

さらに、表示装置 5 0 0 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 5 0 8 を発するようにしてもよい。

## 【 0 1 6 9 】

なお、通知先の表示装置 5 0 0 は、セキュリティユニット 2 0 0 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 2 0 0 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 5 0 0 を通知先としてもよい。

## 【 0 1 7 0 】

このように、本実施の形態に係るセキュリティユニット 2 0 0 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。

30

## 【 0 1 7 1 】

( f 3 : 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 2 0 0 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。

## 【 0 1 7 2 】

図 1 3 は、本実施の形態に係るセキュリティユニット 2 0 0 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 1 3 を参照して、例えば、ネットワーク 1 0 に接続されているサーバ装置 6 0 0 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 2 0 0 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 6 0 0 に通知する。

40

## 【 0 1 7 3 】

サーバ装置 6 0 0 は、セキュリティユニット 2 0 0 からの通知の内容を逐次収集する。そして、サーバ装置 6 0 0 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。

## 【 0 1 7 4 】

図 1 3 には、ネットワーク 1 0 に接続されるサーバ装置 6 0 0 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。

## 【 0 1 7 5 】

50

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。

10

【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。

20

【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。

30

【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。

40

【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、どのようなプロトコルを採用してもよい。

【0187】

50

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】

10

20

30

40

50

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 >

( h 1 : 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。

( h 2 : 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。

10

20

30

40

50

## 【 0 2 0 5 】

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。

## 【 0 2 0 6 】

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。

10

## 【 0 2 0 7 】

( h 3 : 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。

## 【 0 2 0 8 】

< 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 ]

20

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 ]

30

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。

40

## [ 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

50

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 ( 1 0 0 0 ) 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 1 0 ]

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 ( 1 0 0 ) 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 ( 2 6 2 )、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 ( 2 6 4 ) を含む第 2 のユニット ( 2 0 0 ) 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。

【 0 2 0 9 】

< 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。

【 0 2 1 0 】

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 】

【 0 2 1 1 】

1, 1 A 制御システム、2, 2 A 制御装置、4 リモート I O 装置、6 フィールドネットワーク、1 0 ネットワーク、2 0 セキュリティ設定、2 2 ファームウェア、2 4 履歴情報、3 0 ユーザプログラム、3 2 システムプログラム、1 0 0 C P U ユニット、1 0 2, 2 0 2 プロセッサ、1 0 4, 2 0 4 チップセット、1 0 6, 2 0 6 主メモリ、1 0 8, 2 0 8 ストレージ、1 1 0, 2 1 0 ユニット間インターフェイス、1 1 2 U S B インターフェイス、1 1 2 P U S B ポート、1 1 4 メモリカードインターフェイス、1 1 4 P メモリカードスロット、1 1 6 メモリカード、1 1 8, 2 2 0 ネットワークインターフェイス、1 1 8 P ネットワークポート、1 2 0 内部バスコントローラ、1 3 0 フィールドネットワークコントローラ、1 3 0 P 1, 1 3 0 P 2 フィールドネットワークポート、2 0 0, 2 0 0 A セキュリティユニット、2 2 2 送受信部、2 2 4 コントローラ、2 2 6 バッファ、2 5 0 フレーム抽出モジュール、2 5 2 解析モジュール、2 5 4 内容解析処理、2 5 6 特徴抽出処理、2 5 8 統計処理、2 6 0 状態取得モジュール、2 6 2 検知モジュール、2 6 4 通知

10

20

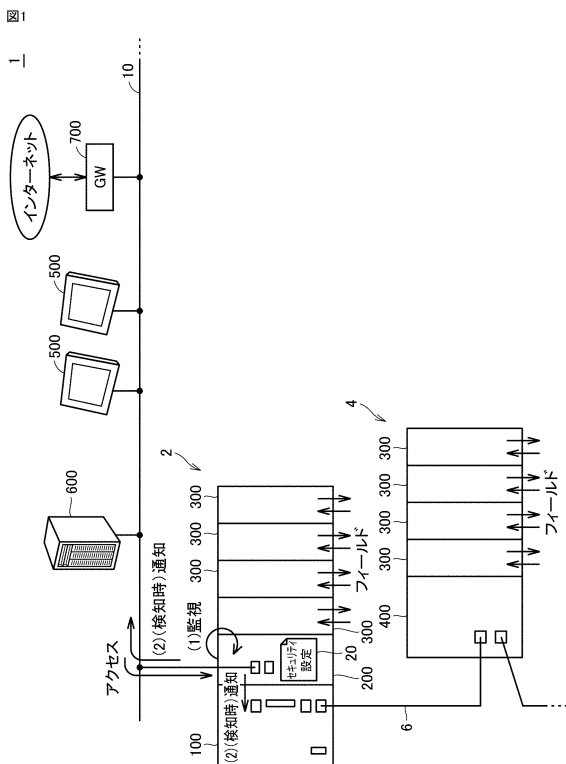
30

40

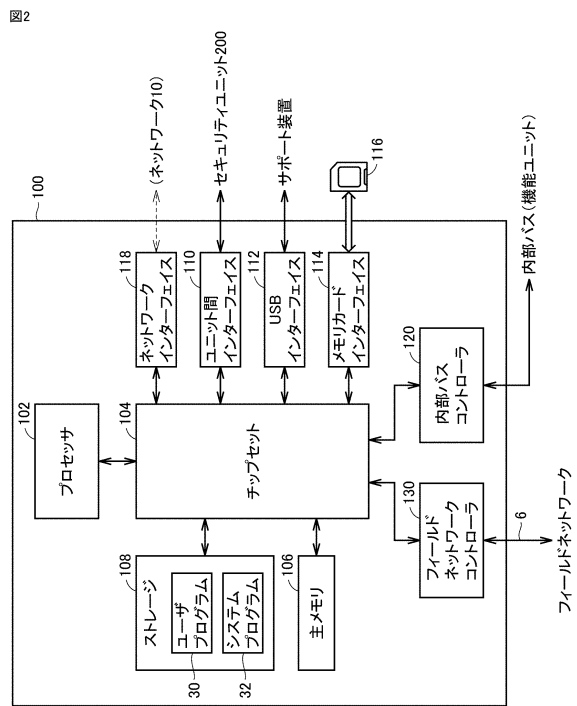
50

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】

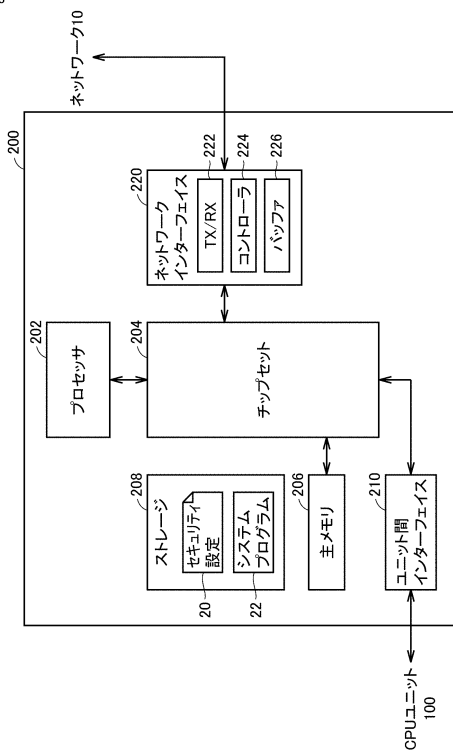


【図2】



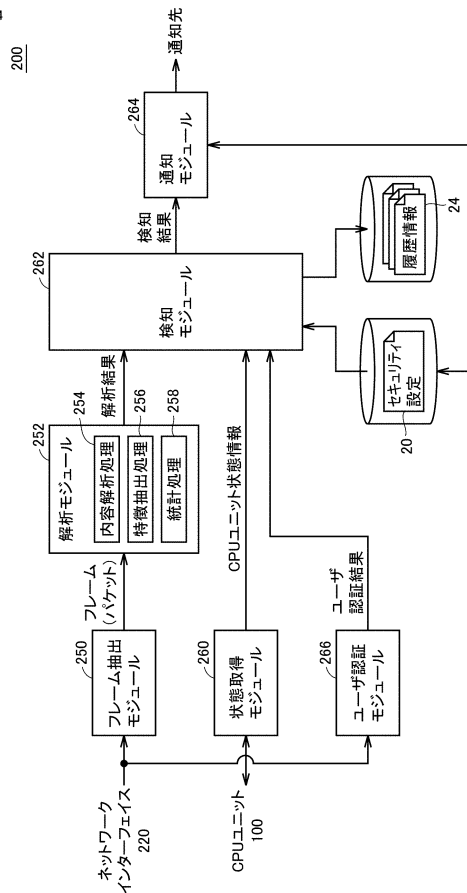
【図3】

図3



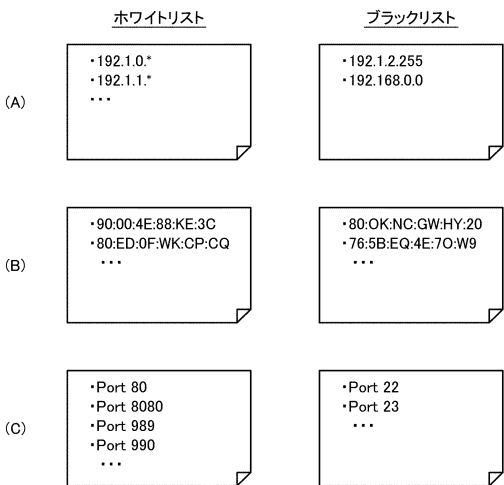
【図4】

図4



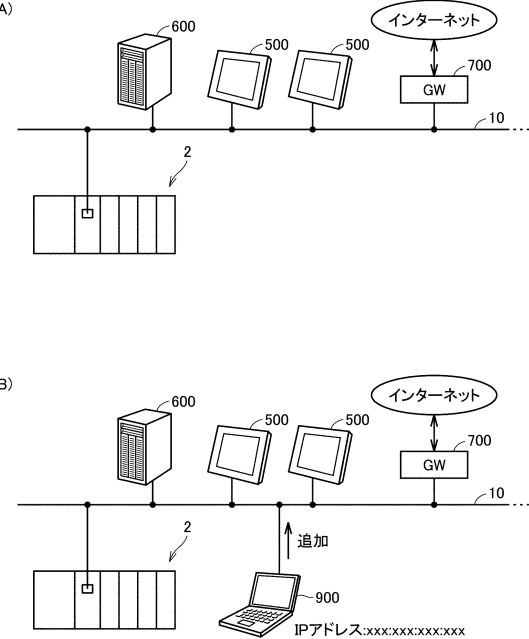
【図5】

図5



【図6】

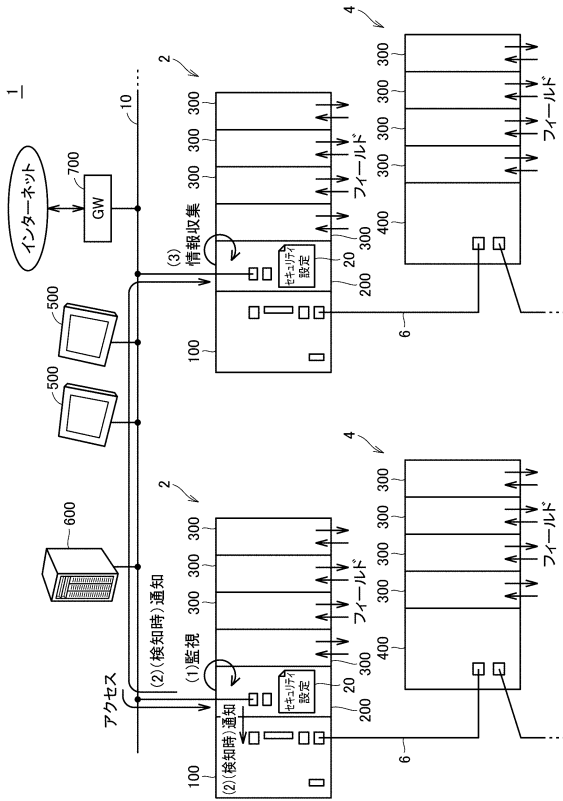
図6





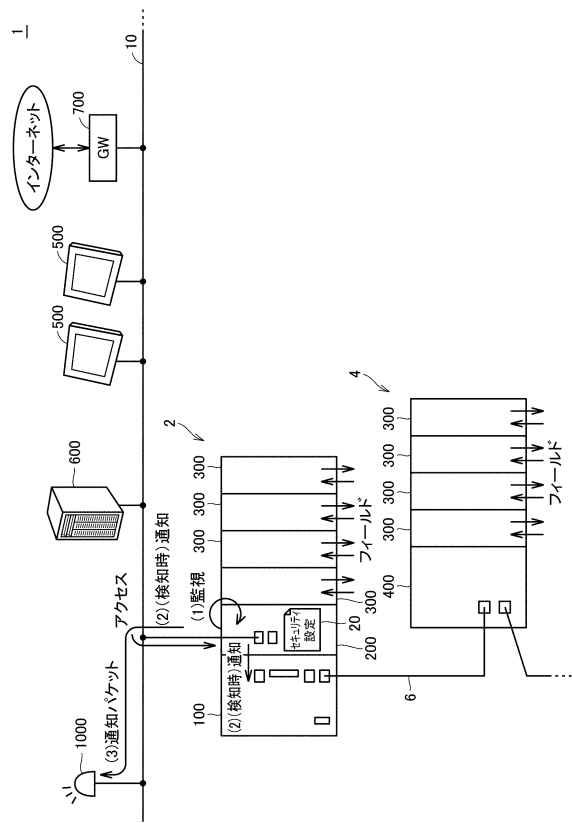
【図 14】

図14



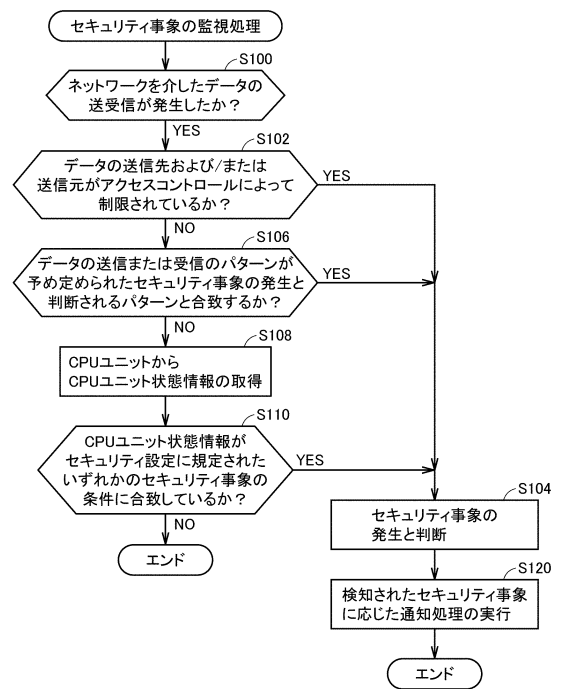
【図 15】

図15



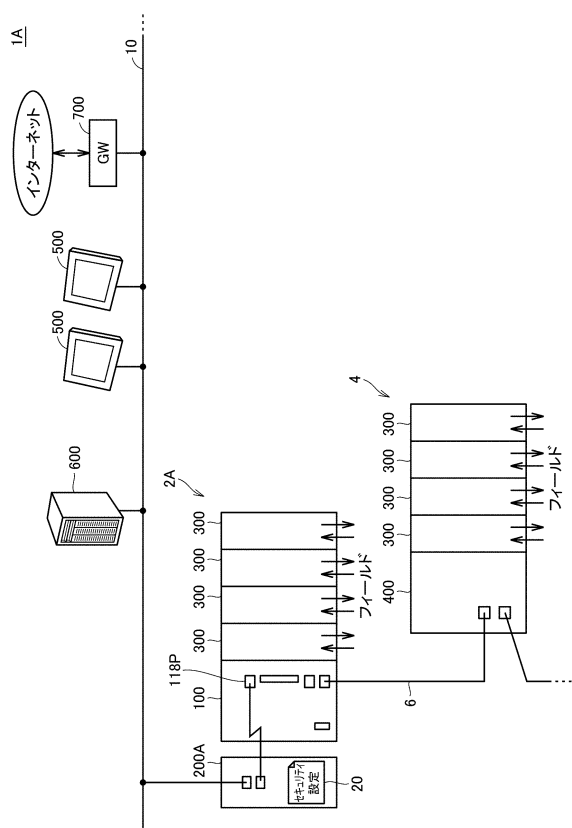
【図 16】

図16



【図 17】

図17



---

フロントページの続き

(56)参考文献 国際公開第2015/001594(WO, A1)

特開2017-103677(JP, A)

特表2014-531087(JP, A)

特開2008-160587(JP, A)

特開2013-88887(JP, A)

(58)調査した分野(Int.Cl., DB名)

G05B 19/04 - 19/05

G06F 21/12 - 21/16

G06F 21/50 - 21/57