

明 細 書

発明の名称：

複数の制御システムの異常を検知する異常検知システム

技術分野

[0001] 複数の制御システムの異常を検知する異常検知システムに関する。

背景技術

[0002] 工業システムおよびインフラストラクチャシステムの管理および制御をする産業制御システム（ICS）が知られている（例えば、非特許文献1参照）。従来、産業制御システムは、外部ネットワークとは接続されず、固有のプロトコルで動作するものが多かった。しかし、近年、産業制御システムは、インターネットプロトコル等の一般的なプロトコルにより接続され、また、外部ネットワークと接続されたシステムも多くなってきた。このため、複数の産業制御システム同士が互いに連携を取ることが可能となってきた。

[0003] 非特許文献1 “SCADA”、[online]、ウィキペディア、[2011年3月30日検索]、インターネット〈URL：<http://ja.wikipedia.org/wiki/SCADA>〉

特許文献1 特表2007-506353号公報

発明の概要

発明が解決しようとする課題

[0004] ところで、それぞれの産業制御システムでは、内部に備える機器等に異常が発生していないかどうかを常時監視している。しかし、これまで、複数の産業制御システム同士が連携して異常を監視していなかった。

課題を解決するための手段

[0005] 上記課題を解決するために、本発明の第1の態様においては、複数の制御システムの異常を検知する異常検知システムであって、前記複数の制御システムのそれぞれに対応して設けられ、対応する制御システムで発生するイベントを取得して異常の有無を解析する複数の解析装置を備え、前記複数の解

析装置のうち第１の解析装置は、対応する前記制御システムで発生したイベントを、前記複数の解析装置のうち第２の解析装置に通知すべきか否かを判定し、前記第２の解析装置は、前記第１の解析装置から通知されたイベントと、前記第１の解析装置以外の解析装置から通知されたイベントとの相関があることを条件として、異常と判断する異常検知システム、方法およびプログラムを提供する。

[0006] なお、上記の発明の概要は、本発明の必要な特徴の全てを列挙したものではない。また、これらの特徴群のサブコンビネーションもまた、発明となりうる。

図面の簡単な説明

[0007] [図１]本実施形態に係るコンピューティングシステム１０の構成を示す。

[図２]本実施形態に係る第１の解析装置３０－１および第２の解析装置３０－２の構成を示す。

[図３]本実施形態に係る第１の解析装置３０－１および第２の解析装置３０－２の処理フローを示す。

[図４]第１の解析装置３０－１が取得したイベントの一例および第１の解析装置３０－１が送信するイベントの一例を示す。

[図５]付加情報を秘匿化するためのテーブルの一例を示す。

[図６]本実施形態に係るコンピュータ１９００のハードウェア構成の一例を示す。

発明を実施するための形態

[0008] 以下、発明の実施の形態を通じて本発明を説明するが、以下の実施形態は特許請求の範囲にかかる発明を限定するものではない。また、実施形態の中で説明されている特徴の組み合わせの全てが発明の解決手段に必須であるとは限らない。

[0009] 図１は、本実施形態に係るコンピューティングシステム１０の構成を示す。本実施形態に係るコンピューティングシステム１０は、複数の制御システム２０と、複数の解析装置３０と、ネットワーク４０とを備える。

- [0010] 複数の制御システム 20 のそれぞれは、複数のコンピュータおよび複数の機器が接続されたシステムである。複数の制御システム 20 のそれぞれは、一例として、工業システムおよびインフラストラクチャ（交通およびエネルギー等）システム等の各オブジェクトの管理および制御をする産業制御システム（ICS）である。この場合、制御システム 20 は、複数の機器、機器を制御する PLC（Programmable Logic Controller）およびサーバ等を備える。
- [0011] 複数の制御システム 20 のそれぞれは、一例として、一つのビル内のネットワークに接続された様々なデバイス（例えば、電気、ガス、水道、空調およびセキュリティシステム等）を管理するシステムである。また、複数の制御システム 20 のそれぞれは、一つの大きな制御システム内における一部分のシステムであってもよい。例えば、複数の制御システム 20 のそれぞれは、都市全体を管理するシステムを構成する部分的な管理システム（例えば、ビル管理システム、工場管理システム、水道管理システム、および電気管理システム等）であってもよい。
- [0012] また、制御システム 20 は、一例として、オフィス内または家庭内のネットワークに接続された様々なデバイス（例えば電話機およびコピー機、等々）を管理するシステムであってもよい。また、制御システム 20 は、企業等内のネットワークに接続された複数のコンピュータを管理するシステムであってもよいし、データセンタ等のネットワークに接続された多数のサーバを管理するシステムであってもよい。
- [0013] 複数の解析装置 30 のそれぞれは、複数の制御システム 20 のそれぞれに対応して設けられる。複数の解析装置 30 のそれぞれは、一つの制御システム 20 に対応して設けられてもよいし、2 以上の制御システム 20 に対応して設けられてもよい。そして、複数の解析装置 30 のそれぞれは、対応する制御システム 20 で発生するイベントを取得して、対応する制御システム 20 の異常の有無を解析する。
- [0014] ここで、イベントとは、対応する制御システム 20 において生じる事象で

あって、例えばセンサまたはコンピュータ等によって検出が可能な事象をいう。イベントは、一例として、制御システム20内の機器等に対して設けられたセンサにより検出された物理量（電力、温度、湿度、質量、体積および流量等）であってよい。また、イベントは、一例として、制御システム20内の情報処理装置等に入出力されるデータの測定値（例えば、データレート、データの送受信のレスポンス、エラーレート等）であってもよい。また、イベントは、一例として、制御システム20内の各機器の状態（例えば、可動の有無および動作モード等）、または、制御システム20内の情報処理装置を構成するリソースの状態（例えば、メモリのデータ占有量およびプロセッサの使用率等）であってもよい。

[0015] 複数の解析装置30のそれぞれは、対応する制御システム20で発生するイベントを取得し、予め定められたイベントが取得されたか否かを判定する。複数の解析装置30のそれぞれは、予め定められたイベントが取得された場合には、対応する制御システム20が異常であると判定する。そして、複数の解析装置30のそれぞれは、対応する制御システム20が異常を有すると判定した場合、異常に応じた対処処理を実行する。

[0016] ネットワーク40は、複数の制御システム20および複数の解析装置30の間を互いに接続して、データの送受信を可能とする。ネットワーク40は、一例として、インターネット等の汎用プロトコルによりデータの伝送を行う。

[0017] 図2は、本実施形態に係る第1の解析装置30-1および第2の解析装置30-2の構成を示す。本実施形態に係るコンピューティングシステム10において、複数の解析装置30は、互いに協働することにより、複数の制御システム20の異常を検知する異常検知システムとして機能する。

[0018] より詳しくは、複数の解析装置30のうち第1の解析装置30-1は、対応する制御システム20から取得したイベントを、複数の解析装置30のうち第2の解析装置30-2へと通知する。そして、第2の解析装置30-2は、第1の解析装置30-1および第1の解析装置30-1以外の他の解析

装置 30 から通知されたイベントの間に相関があるか否かを検出し、相関があることを条件として異常と判断する。

[0019] なお、本実施形態において、コンピューティングシステム 10 に備えられる複数の解析装置 30 のうちの少なくとも 1 つは、第 2 の解析装置 30-2 として機能する。また、複数の制御システム 20 のうち第 2 の解析装置 30-2 以外の他の解析装置 30 は、第 1 の解析装置 30-1 として機能する。

[0020] 第 1 の解析装置 30-1 は、対応する制御システム 20 で発生するイベントを取得して異常の有無を解析する解析部 50 を少なくとも備える。また、第 2 の解析装置 30-2 は、複数の制御システム 20 の何れかでの異常の有無を解析する解析制御部 70 を少なくとも備える。第 2 の解析装置 30-2 は、解析部 50 更に備えてもよい。

[0021] 解析部 50 は、取得部 52 と、判定部 54 と、標準化部 56 と、秘匿部 58 と、イベント送信部 60 と、異常受信部 62 と、監視部 64 とを有する。また、解析制御部 70 は、イベント受信部 72 と、相関検出部 74 と、異常送信部 76 とを有する。

[0022] 取得部 52 は、対応する制御システム 20 で発生するイベントを取得する。取得部 52 は、一例として、制御システム 20 内の各箇所に設けられた物理的なセンサにより検知された物理量（電力、温度、湿度、質量、体積および流量等）を、イベントとして取得する。また、取得部 52 は、一例として、制御システム 20 内の情報処理装置に入出力されるデータの測定値（例えば、データレート、データの送受信のレスポンス、エラーレート等）をイベントとして取得する。また、取得部 52 は、一例として、制御システム 20 内の各機器の状態、または、制御システム 20 内の情報処理装置を構成するリソース（例えば、メモリおよびプロセッサ等）の状態をイベントとして取得する。

[0023] 判定部 54 は、取得したイベントに基づき、対応する制御システム 20 が異常であるか否かを判定する。判定部 54 は、一例として、取得したイベントの値が予め定められた値であるか否かを判定する。

[0024] 判定部 54 は、一例として、センサにより検出された物理量が、予め定められた通常範囲外の値となった場合には、対応する制御システム 20 が異常であると判定する。また、判定部 54 は、一例として、制御システム 20 内の情報処理装置に入出力されるデータの測定値が、予め定められた通常範囲外の値となった場合、対応する制御システム 20 が異常であると判定する。また、判定部 54 は、一例として、制御システム 20 内の各機器の状態、または、制御システム 20 内の情報処理装置を構成するリソースの状態が、予め定められた状態となった場合、対応する制御システム 20 が異常であると判定する。

[0025] 判定部 54 は、対応する制御システム 20 が異常であると判定した場合には、異常であることを監視部 64 に通知する。監視部 64 は、判定部 54 から異常であることの通知を受けたことに応じて、異常が発生した場合にすべき処理を実行する。監視部 64 は、一例として、異常に対応する制御システム 20 の管理者に報告する。また、監視部 64 は、一例として、対応する制御システム 20 の監視頻度を増加させる。この場合、例えば、監視部 64 は、取得部 52 に対してイベントの取得頻度を高める。また、監視部 64 は、一例として、異常の機器を停止したり、電源を止めたりする。

[0026] さらに、判定部 54 は、対応する制御システム 20 が異常ではないと判定される場合であっても、対応する制御システム 20 で発生したイベントを第 2 の解析装置 30-2 に通知すべきか否かを判定する。本実施形態においては、判定部 54 は、取得したイベントの値が、異常であるとは判定はされない値であって且つ異常と判定する閾値からの差分が予め定められた範囲内である場合、当該イベントを第 2 の解析装置 30-2 に通知すべきと判定する。なお、判定部 54 は、対応する制御システム 20 が異常であると判定したイベントも、第 2 の解析装置 30-2 に通知すべきと判定してもよい。

[0027] 判定部 54 は、一例として、センサにより検出された物理量、または、制御システム 20 内の情報処理装置に入出力されるデータの測定値が、予め定められた通常範囲（正常と判定される範囲）内であって、異常と判定される

閾値からの差分が所定値以下の範囲内である場合、当該イベントを第2の解析装置30-2に通知すべきと判定する。また、判定部54は、一例として、制御システム20内の各機器の状態または制御システム20内の情報処理装置を構成するリソースの状態が、正常であると判定される状態であって且つ予め設定された所定状態となった場合、当該イベントを第2の解析装置30-2に通知すべきと判定する。

[0028] 標準化部56は、判定部54によって第2の解析装置30-2に通知すべきと判定された、対応する制御システム20で発生したイベントのデータ形式を標準化する。より詳しくは、標準化部56は、第2の解析装置30-2に通知すべきと判定されたイベントのデータ形式を、第2の解析装置30-2におけるデータ形式に変換して、イベントを標準化する。また、標準化部56は、一例として、対応する制御システム20で発生したイベントのデータ形式を、複数の制御システム20における標準のデータ形式に変換して、イベントを標準化してもよい。これにより、標準化部56は、第2の解析装置30-2に通知するイベントを、第2の解析装置30-2によって読み取り可能なデータ形式に変換することができる。

[0029] 秘匿部58は、判定部54によって第2の解析装置30-2に通知すべきと判定された、対応する制御システム20で発生したイベントの内容を表すデータの一部を秘匿化する。秘匿部58は、一例として、イベントの内容のうち、他の解析装置30に知られたくない部分のデータを秘匿化する。秘匿部58は、一例として、セキュリティを確保するために他の制御システム20の管理者には知られたくない内容（例えば、センサの取り付け位置およびセンサの性能等）を表すデータを秘匿化する。

[0030] イベント送信部60は、標準化部56により標準化され且つ秘匿部58によりデータの一部が秘匿化された、対応する制御システム20で発生したイベントを、第2の解析装置30-2の解析制御部70に通知する。第1の解析装置30-1に備えられる解析部50は、イベントをメッセージ化して、ネットワーク40を介して第2の解析装置30-2の解析制御部70に通知

する。第2の解析装置30-2に備えられる解析部50は、イベントをネットワーク40を介して解析制御部70に通知してもよいし、イベントをネットワーク40を介さずに解析制御部70に通知してもよい。

[0031] 解析制御部70のイベント受信部72は、複数の解析装置30のそれぞれから通知されたイベントを受信する。より具体的には、イベント受信部72は、第1の解析装置30-1の解析部50から通知されたイベント、および、第2の解析装置30-2の解析部50から通知されたイベントを受信する。

[0032] 解析制御部70の相関検出部74は、複数の解析装置30から通知されたイベント同士を比較して、予め定められた相関値以上の相関を有するかどうかを検出する。相関検出部74は、一例として、複数の解析装置30から通知された複数のイベントが、予め定められた相関値以上で相関を有する場合、複数の解析装置30の何れかが異常であると判断する。

[0033] 解析制御部70の異常送信部76は、相関検出部74が異常と判断した場合に、複数の第1の解析装置30-1のそれぞれの解析部50および当該第2の解析装置30-2の解析部50に、異常を通知する。この場合において、異常送信部76は、複数の解析装置30のそれぞれに対して、その解析装置30から送信されたイベントであって、他の解析装置30から送信されたイベントと相関があり異常と判断されたイベントに含まれる秘匿化した部分のデータを、異常情報に含めて解析部50に通知する。

[0034] 異常受信部62は、第2の解析装置30-2の解析制御部70から通知された異常情報を受信する。異常受信部62は、受信した異常情報を秘匿部58に転送する。

[0035] 秘匿部58は、異常情報に含まれる秘匿化した部分のデータの秘匿状態を解除する。秘匿部58は、異常情報および秘匿化を解除したデータを監視部64に転送する。

[0036] 監視部64は、第2の解析装置30-2の解析制御部70から異常情報が通知されたことに応じて、第2の解析装置30-2により通知された異常の

内容を特定する。例えば、監視部 64 は、秘匿部 58 がセンサの取り付け位置を秘匿化してイベントを通知した場合、秘匿化を解除したデータからセンサの取り付け位置を検出する。これにより、秘匿部 58 は、第 2 の解析装置 30-2 により異常と判断されたイベントを発生したセンサの位置を特定することができる。そして、監視部 64 は、異常が発生した場合にすべき対応処理を実行する。

[0037] 図 3 は、本実施形態に係る第 1 の解析装置 30-1 および第 2 の解析装置 30-2 の処理フローを示す。図 4 は、第 1 の解析装置 30-1 が取得したイベントの一例および第 1 の解析装置 30-1 が送信するイベントの一例を示す。図 5 は、付加情報を秘匿化するためのテーブルの一例を示す。

[0038] まず、ステップ S 11 において、第 1 の解析装置 30-1 は、対応する制御システム 20 で発生するイベントを、一定時間毎に取得する。図 4 の例においては、第 1 の解析装置 30-1 は、対応する制御システム 20 が管理するビルの裏庭に設けられた機器の温度をイベントとして、10 分毎に取得する。

[0039] 続いて、ステップ S 12 において、第 1 の解析装置 30-1 は、一定時間毎に取得したイベントのそれぞれについて、第 2 の解析装置 30-2 へと通知すべきか否かを判定する。第 1 の解析装置 30-1 は、一例として、イベントの変化が予め定められた変化量よりも大きい場合、当該イベントを第 2 の制御システム 20-2 へと通知すべきと判定する。

[0040] 図 4 の例においては、第 1 の解析装置 30-1 は、対応する制御システム 20 が管理するビルの裏庭の機器の温度（イベント）が 10 分前から予め定められた範囲以上変化した場合、当該温度（イベント）を第 2 の制御システム 20-2 へと通知すべきと判定する。第 1 の解析装置 30-1 は、通知すべきと判断した場合（S 12 の YES）、処理をステップ S 13 に進める。

[0041] 続いて、ステップ S 13 において、第 1 の解析装置 30-1 は、通知すべきイベントのデータ形式を標準化する。第 1 の解析装置 30-1 は、一例として、イベントの内容を表す識別情報、および、イベントの値を表すイベ

ント値を、第2の解析装置30-2により読み取り可能なデータ形式(例えば当該コンピュータインゲシステム10において共通のデータ形式)に変換する。

[0042] 図4の例においては、第1の解析装置30-1は、「温度」と表された個別の識別情報を「温度センサ」と表された共通の識別情報に変換する。また、図4の例においては、第1の解析装置30-1は、12時間形式で表された「時刻」(個別のイベント値)を、24時間形式で表された「時刻」(共通のイベント値)に変換する。また、図4の例においては、華氏で表された「温度」(個別のイベント値)を、摂氏で表された「温度」(共通のイベント値)に変換する。

[0043] 続いて、ステップS14において、第1の解析装置30-1は、通知するべきイベントの内容を表すデータのうち、他の解析装置30に内容を知られたくない部分のデータ(例えば、セキュリティに関するデータ、および、イベントの詳細な測定ポイントを表すデータ等)を秘匿化する。第1の解析装置30-1は、一例として、イベントの付加情報であるセンサ位置情報を秘匿化する。図4の例においては、第1の解析装置30-1は、「バックヤード#1」と表されたセンサ位置情報を、「39485」と表されたランダムコードに秘匿化する。

[0044] また、第1の解析装置30-1は、一例として、秘匿化前のデータと秘匿化後のデータと対応関係を示した変換テーブルを参照してデータの秘匿化をする。この場合、第1の解析装置30-1は、例えば、図5に示すような、センサ位置を表すセンサ位置情報(バックヤード#1、バックヤード#2、メインプロファイル#1、メインプロファイル#2)を、対応するランダムコード(39485、13456、27321、53884)に変換する変換テーブルを格納する。

[0045] 続いて、ステップS15において、第1の解析装置30-1は、イベントの送信先として、複数の解析装置30の中から少なくとも1つの第2の解析装置30-2を選択する。第1の解析装置30-1は、一例として、複数の

解析装置 30 からイベントを受け取って異常が発生したか否かを判断することができる解析装置 30 が複数存在する場合、これらの中から 1 つまたは 2 以上の解析装置 30 を第 2 の解析装置 30-2 として選択する。

[0046] なお、第 1 の解析装置 30-1 は、複数の解析装置 30 のうちのいずれを第 2 の解析装置 30-2 とするかを動的に変更してもよい。例えば、第 1 の解析装置 30-1 は、一定期間（例えば、1 日毎、1 週間毎）において、いずれを第 2 の解析装置 30-2 とするかを設定する。

[0047] この場合において、第 1 の解析装置 30-1 は、複数の解析装置 30 のうちレスポンス時間が短い解析装置 30 を優先して第 2 の解析装置 30-2 として選択してもよい。これにより、第 1 の解析装置 30-1 は、より早く異常の通知を受けることができる。また、第 1 の解析装置 30-1 は、一定期間以上同一の第 2 の解析装置 30-2 に対してイベントの通知を継続したことを条件として、新たな第 2 の解析装置 30-2 を選択してもよい。これにより、第 1 の解析装置 30-1 は、第 2 の解析装置 30-2 を一つに固定させないことができる。

[0048] 続いて、ステップ S 16 において、ステップ S 15 で選択した第 2 の解析装置 30-2 へと、ステップ S 13 で標準化され且つステップ S 14 で秘匿化されたイベントを通知する。続いて、ステップ S 17 において、第 2 の解析装置 30-2 は、第 1 の解析装置 30-1 からイベントを受信する。

[0049] 続いて、ステップ S 18 において、第 2 の解析装置 30-2 は、複数の解析装置 30 から通知されたイベントの相関を検出して、複数の制御システム 20 の何れかにおいて異常が発生したか否かを判断する。より具体的には、第 2 の解析装置 30-2 は、第 1 の解析装置 30-1 から通知されたイベントと、第 1 の解析装置 30-1 以外の解析装置 30 から通知されたイベントとの相関があることを条件として、異常と判断する。第 2 の解析装置 30-2 は、一例として、第 1 の解析装置 30-1 から通知されたイベントの変化と、第 1 の解析装置 30-1 以外の他の解析装置 30 から通知されたイベントの変化に、予め定められた相関値以上の相関があることを条件として、異

常と判断する。

[0050] 例えば、相関検出部 74 は、一例として、複数の制御システム 20 のそれぞれに設置された複数の温度センサの温度が、互いに相関をもって変化した場合、異常と判断する。図 4 の場合、20 時 20 分～30 分に温度センサの温度が上昇し、20 時 30 分～40 分の間に温度センサの温度が下降する変化が、一つの制御システム 20 内において発生している。そこで、このような場合、第 2 の解析装置 30-2 は、複数の制御システム 20 に設けられた温度センサが、図 4 と同様の温度変化をしていることを条件として異常と判断する。

[0051] 続いて、ステップ S 19 において、第 2 の解析装置 30-2 は、ステップ S 18 で異常と判断した場合、第 1 の解析装置 30-1 に異常を通知する。この場合において、第 2 の解析装置 30-2 は、第 1 の解析装置 30-1 から送信されたイベントであって、他の解析装置 30 から送信されたイベントと相関があり異常と判断したイベントに含まれていた秘匿化された部分のデータを、異常情報に含めて解析部 50 に通知する。

[0052] 続いて、ステップ S 20 において、第 1 の解析装置 30-1 は、第 2 の解析装置 30-2 から通知された異常情報を受信する。続いて、ステップ S 21 において、第 1 の解析装置 30-1 は、第 2 の解析装置 30-2 から通知された異常情報に基づき、対応する制御システム 20 において発生した異常の内容を特定する。

[0053] 第 1 の解析装置 30-1 は、第 2 の解析装置 30-2 から通知された異常情報に含まれる秘匿化された部分のデータを、変換テーブルを参照して秘匿化していないデータに戻す。そして、第 1 の解析装置 30-1 は、秘匿化が解除されたイベントから、対応する制御システムで発生した異常を特定する。例えば、第 1 の解析装置 30-1 は、図 5 に示されるような変換テーブルを参照して、異常が発生した箇所がビルの裏庭のセンサであることを特定する。

[0054] 続いて、ステップ S 22 において、第 1 の解析装置 30-1 は、対応する

制御システム 20 を制御するためのモードを警戒モードに変更する。第 1 の解析装置 30-1 は、異常に対応する制御システム 20 の管理者に報告する。また、第 1 の解析装置 30-1 は、一例として、対応する制御システム 20 の監視頻度を増加させる。この場合、例えば、第 1 の解析装置 30-1 は、イベントの取得頻度を高めることにより、監視頻度を増加させてもよい。また、第 1 の解析装置 30-1 は、一例として、異常の機器を停止したり、電源を止めたりする。

[0055] 以上のように、本実施形態に係るコンピューティングシステム 10 によれば、一つの制御システム 20 において単独では異常と検出されないような事象（イベント）が発生した場合であっても、複数の解析装置 30 の間において相関のある事象（イベント）が発生した場合には、異常と判断することができる。これにより、コンピューティングシステム 10 によれば、複数の解析装置 30 が連携して、より正確に且つ感度良く異常を検知することができる。

[0056] なお、第 2 の解析装置 30-2 は、第 1 の解析装置 30-1 から通知されたイベントと、第 1 の解析装置 30-1 以外の解析装置 30 から通知されたイベントとの相関がある場合に、第 1 の解析装置 30-1 に対して秘匿化されていないイベントの通知を要求してもよい。この場合、第 1 の解析装置 30-1 は、秘匿化されていないイベントの通知の要求に応じて、イベントを秘匿化せずに第 2 の解析装置 30-2 に通知する。

[0057] そして、第 2 の解析装置 30-2 は、第 1 の解析装置 30-1 から秘匿化されていないイベントを受け取って、第 1 の解析装置 30-1 から通知された秘匿化されていないイベントと、第 1 の解析装置 30-1 以外の解析装置 30 から通知されたイベントとの相関を再度検知する。そして、第 2 の解析装置 30-2 は、相関があることを条件として異常と判断する。これにより、第 2 の解析装置 30-2 は、異常が発生しているかどうかをより正確に判断することができる。

[0058] 図 6 は、本実施形態に係るコンピュータ 1900 のハードウェア構成の一

例を示す。本実施形態に係るコンピュータ 1900 は、ホスト・コントローラ 2082 により相互に接続される CPU 2000、RAM 2020、グラフィック・コントローラ 2075、及び表示装置 2080 を有する CPU 周辺部と、入出力コントローラ 2084 によりホスト・コントローラ 2082 に接続される通信インターフェイス 2030、ハードディスクドライブ 2040、及び CD-ROM ドライブ 2060 を有する入出力部と、入出力コントローラ 2084 に接続される ROM 2010、フレキシブルディスク・ドライブ 2050、及び入出力チップ 2070 を有するレガシー入出力部とを備える。

[0059] ホスト・コントローラ 2082 は、RAM 2020 と、高い転送レートで RAM 2020 をアクセスする CPU 2000 及びグラフィック・コントローラ 2075 とを接続する。CPU 2000 は、ROM 2010 及び RAM 2020 に格納されたプログラムに基づいて動作し、各部の制御を行う。グラフィック・コントローラ 2075 は、CPU 2000 等が RAM 2020 内に設けたフレーム・バッファ上に生成する画像データを取得し、表示装置 2080 上に表示させる。これに代えて、グラフィック・コントローラ 2075 は、CPU 2000 等が生成する画像データを格納するフレーム・バッファを、内部に含んでもよい。

[0060] 入出力コントローラ 2084 は、ホスト・コントローラ 2082 と、比較的高速な入出力装置である通信インターフェイス 2030、ハードディスクドライブ 2040、CD-ROM ドライブ 2060 を接続する。通信インターフェイス 2030 は、ネットワークを介して他の装置と通信する。ハードディスクドライブ 2040 は、コンピュータ 1900 内の CPU 2000 が使用するプログラム及びデータを格納する。CD-ROM ドライブ 2060 は、CD-ROM 2095 からプログラム又はデータを読み取り、RAM 2020 を介してハードディスクドライブ 2040 に提供する。

[0061] また、入出力コントローラ 2084 には、ROM 2010 と、フレキシブルディスク・ドライブ 2050、及び入出力チップ 2070 の比較的低速な

入出力装置とが接続される。ROM 2010は、コンピュータ1900が起動時に実行するブート・プログラム、及び／又は、コンピュータ1900のハードウェアに依存するプログラム等を格納する。フレキシブルディスク・ドライブ2050は、フレキシブルディスク2090からプログラム又はデータを読み取り、RAM 2020を介してハードディスクドライブ2040に提供する。入出力チップ2070は、フレキシブルディスク・ドライブ2050を入出力コントローラ2084へと接続すると共に、例えばパラレル・ポート、シリアル・ポート、キーボード・ポート、マウス・ポート等を介して各種の入出力装置を入出力コントローラ2084へと接続する。

[0062] RAM 2020を介してハードディスクドライブ2040に提供されるプログラムは、フレキシブルディスク2090、CD-ROM 2095、又はICカード等の記録媒体に格納されて利用者によって提供される。プログラムは、記録媒体から読み出され、RAM 2020を介してコンピュータ1900内のハードディスクドライブ2040にインストールされ、CPU 2000において実行される。

[0063] コンピュータ1900にインストールされ、コンピュータ1900を解析部50として機能させるプログラムは、取得モジュールと、判定モジュールと、標準化モジュールと、秘匿モジュールと、イベント送信モジュールと、異常受信モジュールと、監視モジュールとを備える。これらのプログラム又はモジュールは、CPU 2000等に働きかけて、コンピュータ1900を、取得部52、判定部54、標準化部56、秘匿部58、イベント送信部60、異常受信部62、および監視部64としてそれぞれ機能させる。

[0064] これらのプログラムに記述された情報処理は、コンピュータ1900に読込まれることにより、ソフトウェアと上述した各種のハードウェア資源とが協働した具体的手段である取得部52、判定部54、標準化部56、秘匿部58、イベント送信部60、異常受信部62、および監視部64として機能する。そして、これらの具体的手段によって、本実施形態におけるコンピューティングシステム10の使用目的に応じた情報の演算又は加工を実現する

ことにより、使用目的に応じた特有の解析部 50 が構築される。

[0065] また、コンピュータ 1900 にインストールされ、コンピュータ 1900 を解析制御部 70 として機能させるプログラムは、イベント受信モジュールと、相関検出モジュールと、異常送信モジュールとを備える。これらのプログラム又はモジュールは、CPU 2000 等に働きかけて、コンピュータ 1900 を、イベント受信部 72、相関検出部 74 および異常送信部 76 としてそれぞれ機能させる。

[0066] これらのプログラムに記述された情報処理は、コンピュータ 1900 に読み込まれることにより、ソフトウェアと上述した各種のハードウェア資源とが協働した具体的手段であるイベント受信部 72、相関検出部 74 および異常送信部 76 として機能する。そして、これらの具体的手段によって、本実施形態におけるコンピューティングシステム 10 の使用目的に応じた情報の演算又は加工を実現することにより、使用目的に応じた特有の解析制御部 70 が構築される。

[0067] 一例として、コンピュータ 1900 と外部の装置等との間で通信を行う場合には、CPU 2000 は、RAM 2020 上にロードされた通信プログラムを実行し、通信プログラムに記述された処理内容に基づいて、通信インターフェイス 2030 に対して通信処理を指示する。通信インターフェイス 2030 は、CPU 2000 の制御を受けて、RAM 2020、ハードディスクドライブ 2040、フレキシブルディスク 2090、又は CD-ROM 2095 等の記憶装置上に設けた送信バッファ領域等に記憶された送信データを読み出してネットワークへと送信し、もしくは、ネットワークから受信した受信データを記憶装置上に設けた受信バッファ領域等へと書き込む。このように、通信インターフェイス 2030 は、DMA（ダイレクト・メモリ・アクセス）方式により記憶装置との間で送受信データを転送してもよく、これに代えて、CPU 2000 が転送元の記憶装置又は通信インターフェイス 2030 からデータを読み出し、転送先の通信インターフェイス 2030 又は記憶装置へとデータを書き込むことにより送受信データを転送してもよい。

[0068] また、CPU2000は、ハードディスクドライブ2040、CD-ROMドライブ2060 (CD-ROM2095)、フレキシブルディスク・ドライブ2050 (フレキシブルディスク2090) 等の外部記憶装置に格納

されたファイルまたはデータベース等の中から、全部または必要な部分をD

MA転送等によりRAM2020へと読み込ませ、RAM2020上のデー

タに対して各種の処理を行う。そして、CPU2000は、処理を終えたデ

ータを、DMA転送等により外部記憶装置へと書き戻す。このような処理に

おいて、RAM2020は、外部記憶装置の内容を一時的に保持するものと

みなせるから、本実施形態においてはRAM2020および外部記憶装置等

をメモリ、記憶部、または記憶装置等と総称する。本実施形態における各種

のプログラム、データ、テーブル、データベース等の各種の情報は、このよ

うな記憶装置上に格納されて、情報処理の対象となる。なお、CPU200

0は、RAM2020の一部をキャッシュメモリに保持し、キャッシュメモ

リ上で読み書きを行うこともできる。このような形態においても、キャッシ

ュメモリはRAM2020の機能の一部を担うから、本実施形態においては

、区別して示す場合を除き、キャッシュメモリもRAM2020、メモリ、

及び/又は記憶装置に含まれるものとする。

[0069] また、CPU2000は、RAM2020から読み出したデータに対して

、プログラムの命令列により指定された、本実施形態中に記載した各種の演

算、情報の加工、条件判断、情報の検索・置換等を含む各種の処理を行い、

RAM2020へと書き戻す。例えば、CPU2000は、条件判断を行う

場合においては、本実施形態において示した各種の変数が、他の変数または

定数と比較して、大きい、小さい、以下、以上、等しい等の条件を満たすか

どうかを判断し、条件が成立した場合 (又は不成立であった場合) に、異な

る命令列へと分岐し、またはサブルーチンを呼び出す。

[0070] また、CPU2000は、記憶装置内のファイルまたはデータベース等に

格納された情報を検索することができる。例えば、第1属性の属性値に対し

第2属性の属性値がそれぞれ対応付けられた複数のエントリが記憶装置に格納されている場合において、CPU2000は、記憶装置に格納されている複数のエントリの中から第1属性の属性値が指定された条件と一致するエントリを検索し、そのエントリに格納されている第2属性の属性値を読み出すことにより、所定の条件を満たす第1属性に対応付けられた第2属性の属性値を得ることができる。

[0071] 以上に示したプログラム又はモジュールは、外部の記録媒体に格納されてもよい。記録媒体としては、フレキシブルディスク2090、CD-ROM2095の他に、DVD又はCD等の光学記録媒体、MO等の光磁気記録媒体、テープ媒体、ICカード等の半導体メモリ等を用いることができる。また、専用通信ネットワーク又はインターネットに接続されたサーバシステムに設けたハードディスク又はRAM等の記憶装置を記録媒体として使用し、ネットワークを介してプログラムをコンピュータ1900に提供してもよい。

[0072] 以上、本発明を実施の形態を用いて説明したが、本発明の技術的範囲は上記実施の形態に記載の範囲には限定されない。上記実施の形態に、多様な変更または改良を加えることが可能であることが当業者に明らかである。その様な変更または改良を加えた形態も本発明の技術的範囲に含まれ得ることが、特許請求の範囲の記載から明らかである。

[0073] 特許請求の範囲、明細書、および図面中において示した装置、システム、プログラム、および方法における動作、手順、ステップ、および段階等の各処理の実行順序は、特段「より前に」、「先立って」等と明示しておらず、また、前の処理の出力を後の処理で用いるのでない限り、任意の順序で実現しうることに留意すべきである。特許請求の範囲、明細書、および図面中の動作フローに関して、便宜上「まず、」、「次に、」等を用いて説明したとしても、この順で実施することが必須であることを意味するものではない。

符号の説明

[0074] 10 コンピューティングシステム

- 2 0 制御システム
- 3 0 解析装置
- 4 0 ネットワーク
- 5 0 解析部
- 5 2 取得部
- 5 4 判定部
- 5 6 標準化部
- 5 8 秘匿部
- 6 0 イベント送信部
- 6 2 異常受信部
- 6 4 監視部
- 7 0 解析制御部
- 7 2 イベント受信部
- 7 4 相関検出部
- 7 6 異常送信部
- 1 9 0 0 コンピュータ
- 2 0 0 0 C P U
- 2 0 1 0 R O M
- 2 0 2 0 R A M
- 2 0 3 0 通信インターフェイス
- 2 0 4 0 ハードディスクドライブ
- 2 0 5 0 フレキシブルディスク・ドライブ
- 2 0 6 0 C D - R O Mドライブ
- 2 0 7 0 入出力チップ
- 2 0 7 5 グラフィック・コントローラ
- 2 0 8 0 表示装置
- 2 0 8 2 ホスト・コントローラ
- 2 0 8 4 入出力コントローラ

2090 フレキシブルディスク

2095 CD-ROM

請求の範囲

- [請求項1] 複数の制御システムの異常を検知する異常検知システムであって、
前記複数の制御システムのそれぞれに対応して設けられ、対応する制御システムで発生するイベントを取得して異常の有無を解析する複数の解析装置を備え、
前記複数の解析装置のうち第1の解析装置は、対応する前記制御システムで発生したイベントを、前記複数の解析装置のうち第2の解析装置に通知すべきか否かを判定し、
前記第2の解析装置は、前記第1の解析装置から通知されたイベントと、前記第1の解析装置以外の解析装置から通知されたイベントとの相関があることを条件として、異常と判断する異常検知システム。
- [請求項2] 前記複数の解析装置のそれぞれは、対応する前記制御システムで発生したイベントのデータ形式を、前記第2の解析装置におけるデータ形式に変換して、前記イベントを標準化する標準化部を有する請求項1に記載の異常検知システム。
- [請求項3] 前記第1の解析装置の標準化部は、対応する前記制御システムで発生したイベントのデータ形式を、前記複数の制御システムにおける標準のデータ形式に変換して、前記イベントを標準化する請求項2に記載の異常検知システム。
- [請求項4] 前記複数の解析装置のそれぞれは、対応する前記制御システムで発生したイベントの内容を表すデータの一部を秘匿化する秘匿部を有する請求項1から3のいずれか一項に記載の異常検知システム。
- [請求項5] 前記第1の解析装置の前記秘匿部は、秘匿化前のデータと秘匿化後のデータと対応関係を示した変換テーブルを格納し、
前記第2の解析装置は、異常と判断した場合、前記第1の解析装置から受け取った秘匿後のイベントに含まれる秘匿化後のデータを含む

異常情報を前記第 1 の解析装置へと通知し、

前記第 1 の解析装置の前記秘匿部は、前記第 2 の解析装置から通知された前記異常情報に含まれる秘匿化されたデータを前記変換テーブルを参照して秘匿化前のデータに変換して、対応する前記制御システムで発生した異常を特定する

請求項 4 に記載の異常検知システム。

[請求項 6]

前記第 2 の解析装置は、

前記第 1 の解析装置から通知されたイベントと、前記第 1 の解析装置以外の解析装置から通知されたイベントとの相関がある場合に、前記第 1 の解析装置に対して秘匿化されていないイベントの通知を要求し、

前記第 1 の解析装置から秘匿化されていないイベントを受け取って、前記第 1 の解析装置から通知された秘匿化されていないイベントと、前記第 1 の解析装置以外の解析装置から通知されたイベントとの相関があることを条件として異常と判断する

請求項 4 または 5 に記載の異常検知システム。

[請求項 7]

前記第 2 の解析装置は、前記複数の解析装置の少なくとも一部に対して異常を通知し、異常の通知を受けた前記複数の解析装置の少なくとも一部は、対応する前記制御システムの監視頻度を増加させる

請求項 1 から 6 のいずれか一項に記載の異常検知システム。

[請求項 8]

前記第 1 の解析装置は、前記複数の解析装置のうちのいずれを前記第 2 の解析装置とするかを動的に変更する請求項 1 から 7 のいずれか一項に記載の異常検知システム。

[請求項 9]

前記第 1 の解析装置は、一定期間以上同一の前記第 2 の解析装置に対してイベントの通知を継続したことを条件として、新たな前記第 2 の解析装置を選択する請求項 8 に記載の異常検知システム。

[請求項 10]

前記第 1 の解析装置は、前記複数の解析装置のうちレスポンス時間が短い解析装置を優先して前記第 2 の解析装置として選択する請求項

8 または 9 に記載の異常検知システム。

[請求項11]

前記第 1 の解析装置は、対応する前記制御システムで発生するイベントを取得して異常の有無を解析する解析部を有し、

前記第 2 の解析装置は、前記複数の制御システムの何れかでの異常の有無を解析する解析制御部を有し、

前記第 1 の解析装置の前記解析部は、対応する前記制御システムで発生するイベントを取得して前記第 2 の解析装置に通知すべきか否かを判定し、前記第 2 の解析装置に通知すべきと判定した場合には、取得したイベントを前記第 2 の解析装置の前記解析制御部へと転送し、

前記第 2 の解析装置の前記解析制御部は、複数の前記第 1 の解析装置からのイベント同士の相関を検出し、相関があることを条件として異常と判断し、異常と判断した場合に前記第 1 の解析装置の前記解析部へと通知し、

前記第 1 の解析装置の前記解析部は、前記第 2 の解析装置から通知された異常に対応する前記制御システムの管理者に対して報告する

請求項 1 から 10 のいずれか一項に記載の異常検知システム。

[請求項12]

前記第 2 の解析装置は、異常と判断した場合、前記第 1 の解析装置に異常を通知し、

前記第 1 の解析装置は、前記第 2 の解析装置から通知された異常を前記制御システムの管理者に対して報告する

請求項 1 から 11 のいずれか一項に記載の異常検知システム。

[請求項13]

前記第 2 の解析装置は、前記第 1 の解析装置から通知されたイベントの変化と、前記第 1 の解析装置以外の解析装置から通知されたイベントの変化との間の相関があることを条件として異常と判断する

請求項 1 から 12 のいずれか一項に記載の異常検知システム。

[請求項14]

請求項 11 に記載された異常検知システムにおける前記解析部として機能する装置。

[請求項15]

請求項 11 に記載された異常検知システムにおける前記解析制御部

として機能する装置。

[請求項16] コンピュータを、請求項14に記載の装置として機能させるプログラム。

[請求項17] コンピュータを、請求項15に記載の装置として機能させるプログラム。

[請求項18] 複数の制御システムの異常を検知する異常検知方法であって、
前記複数の制御システムのそれぞれに対応して、対応する制御システムで発生するイベントを取得して異常の有無を解析する複数の解析装置を設け、

前記複数の解析装置のうち第1の解析装置が、対応する前記制御システムで発生したイベントを、前記複数の解析装置のうち第2の解析装置に通知すべきか否かを判定するステップと、

前記第2の解析装置が、前記第1の解析装置から通知されたイベントと、前記第1の解析装置以外の解析装置から通知されたイベントとの相関があることを条件として、異常と判断するステップとを

備える異常検知方法。