(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2016-201603
(P2016-201603A)
(43)公開日　平成28年12月1日(2016.12.1)

(51)Int.Cl.		F I		テーマコード（参考）
H04L 12/46	(2006.01)	H04L 12/46	M	5K033

審査請求 未請求　請求項の数 10　ＯＬ　（全 13 頁）

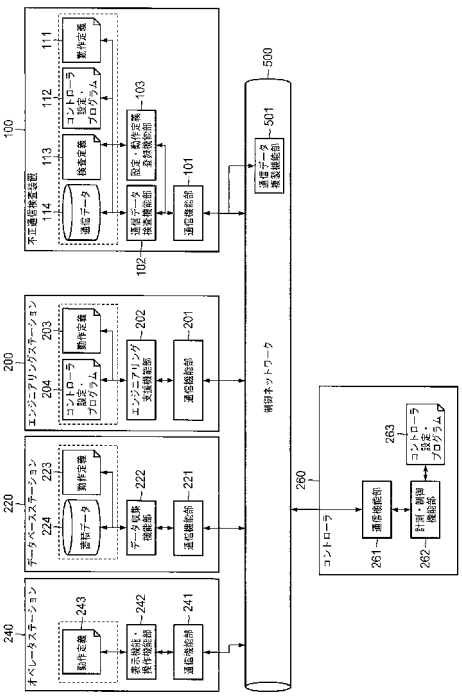
(21)出願番号　特願2015-78796(P2015-78796)
(22)出願日　平成27年4月7日(2015.4.7)

(71)出願人　000005234
富士電機株式会社
神奈川県川崎市川崎区田辺新田１番１号
(74)代理人　100111763
弁理士　松本　隆
(74)代理人　100163832
弁理士　後藤　直哉
(72)発明者　飯島　淳一
神奈川県川崎市川崎区田辺新田１番１号
富士電機株式会社内

Ｆターム(参考)　5K033 AA08　BA02　BA11　CB08　CC01
DB18　DB20　EA02

(54)【発明の名称】不正通信検査装置および通信システム

(57)【要約】
【課題】　ネットワークにおいて発生する通信データを正確に検査し、不正な通信を確実に防止する。
【解決手段】　不正通信検査装置１００において、設定・動作定義登録機能部１０３は、制御ネットワーク５００を利用して通信を行う装置が従うべき動作定義である動作定義２０３およびコントローラの設定・プログラム２０４をエンジニアリングステーション２００から通信機能部１０１等を介して取得し、この動作定義に基づいて、正常な通信データを定義する検査定義１１３を生成する。通信データ検査機能部１０２は、制御ネットワーク５００から通信機能部１０１を介して取得した通信データを検査し、検査定義１１３により定義された通信データのみを許可するとともに、通信機能部１０１を介して取得した通信データを通信データ１１４として記録する。
【選択図】図２



【特許請求の範囲】
【請求項１】
ネットワークを利用して通信を行う装置が従うべき動作定義を取得し、前記動作定義に基づいて、正常な通信データを定義する検査定義を生成する検査定義生成手段と、
前記ネットワークから取得した通信データを検査し、前記検査定義により定義された正常な通信データのみを許可する通信データ検査手段と
を具備することを特徴とする不正通信検査装置。
【請求項２】
前記検査定義における正常な通信データの定義は、前記動作定義における当該通信データを発生させる動作の定義と関連付けられており、前記通信データ検査手段は、検査対象となった通信データに関するデータであって、当該通信データが該当する正常な通信データの定義に関連付けられた動作の定義を示すデータを記録することを特徴とする請求項１に記載の不正通信検査装置。
【請求項３】
前記検査定義生成手段は、前記動作定義を取得する前、所定の基本動作に基づいて検査定義を生成することを特徴とする請求項１または２に記載の不正通信検査装置。
【請求項４】
前記検査定義生成手段は、正常な通信データの送信元、宛先、特徴を定義した検査定義を生成することを特徴とする請求項１～３のいずれか１の請求項に記載の不正通信検査装置。
【請求項５】
前記動作定義は、前記ネットワークを利用した通信を行う装置が実行するプログラムを含み、前記検査定義生成手段は、当該プログラムにおいて定義されたデータを含む前記検査定義を生成することを特徴とする請求項１～４のいずれか１の請求項に記載の不正通信検査装置。
【請求項６】
取得した動作定義および生成した検査定義を記憶する記憶手段を具備し、前記検査定義生成手段は、前記記憶手段における前記動作定義の更新に応じて、前記記憶手段における前記検査定義の更新を行うことを特徴とする請求項１～５のいずれか１の請求項に記載の不正通信検査装置。
【請求項７】
ネットワークを利用して通信を行う装置が従うべき動作定義を生成する動作定義生成手段と、
前記動作定義に基づいて、正常な通信データを定義する検査定義を生成する検査定義生成手段と、
前記ネットワークから取得した通信データのうち前記検査定義により定義された通信データのみを許可する不正通信検査手段と
を具備することを特徴とする通信システム。
【請求項８】
前記動作定義生成手段は、前記ネットワークを利用して通信を行う装置に前記動作定義を取得させるときに、前記動作定義を前記検査定義生成手段に取得させることを特徴とする請求項７に記載の通信システム。
【請求項９】
前記検査定義生成手段は、暗号化通信により前記動作定義を取得することを特徴とする請求項８に記載の通信システム。
【請求項１０】
前記検査定義生成手段は、記憶媒体を介して前記動作定義を取得することを特徴とする請求項７に記載の通信システム。
【発明の詳細な説明】
【技術分野】

【０００１】
この発明は、ネットワークを介した通信を検査する装置に係り、特に制御ネットワークにおいて不正な通信を検査する不正通信検査装置に関する。
【背景技術】
【０００２】
従来、ポンプやアクチュエータ等の制御や、センサ値を読み出す計測を行う制御システムでは、ベンダによる専用機と、独自の信号線や通信規格が用いられていた。しかし、近年の利用者の利便性向上やコストダウン、オープン化、情報連携といった要請により、制御システムにおいても機器間のネットワーク通信を情報システムで用いられているＥｔｈｅｒｎｅｔ（登録商標）やＴＣＰ／ＩＰ、ＵＤＰ／ＩＰといったプロトコルを採用する事例が増えている。
【０００３】
しかしながら、これらの広く採用されているプロトコルを採用すると、悪意のある攻撃者によって制御システムが侵害される可能性が増す。また、制御システムの構成要素として想定されていない情報機器が不意に制御ネットワークに接続されることにより、制御システム全体や制御システムを構成する各装置が意図せぬ挙動を示す危険性がある。
【０００４】
情報システムでは、外部からの攻撃である不正な通信を検査する手段として、パケットフィルタ、ファイアウォールという仕組みが用いられている。これは、基本的には事前に図９に例示するような正常な通信の態様、具体的には送信元と宛先を定義し、定義されていない態様の通信を遮断する仕組みである。
【０００５】
また、不正な通信を検査する手段として、ＩＤＳ（Ｉｎｔｒｕｓｉｏｎ Ｄｅｔｅｃｔｉｏｎ Ｓｙｓｔｅｍ：侵入検査システム）、ＩＰＳ（Ｉｎｔｒｕｓｉｏｎ Ｐｒｅｖｅｎｔｉｏｎ Ｓｙｓｔｅｍ／Ｉｎｔｒｕｓｉｏｎ Ｐｒｏｔｅｃｔｉｏｎ Ｓｙｓｔｅｍ：侵入防止システム／侵入防御システム）という仕組みがある。
【０００６】
ＩＤＳは通信の内容を検査するものであり、シグネチャと呼ばれる検査ルールに基づいて通信を判定することで不正な通信を検知する仕組みである。ここで、シグネチャは、コンピュータウイルスや攻撃者の行う通信のパターンを定義した情報である。
【０００７】
ＩＰＳは、通信に関してＩＤＳと同様な判定を行う仕組みである。ただし、ＩＤＳが不正な通信を検知しても管理者などへの通知のみ行うものであるのに対し、ＩＰＳは不正な通信を遮断するものである。図１０は、ＩＤＳやＩＰＳにおいて用いられる不正通信の検査ルールを例示するものである。また、図１１は、ＩＤＳやＩＰＳにより行われる不正通信の検査の結果を例示するものである。
【０００８】
不正な通信を検査するためには、検査のための検査ルールを如何に正確に作成するかが重要である。不適切な検査ルールは、不正でない通信を誤検出し、また、不正な通信を検出し損なう原因となるからである。そこで、情報システムにおいては、セキュリティベンダ等により特定のウイルスのみ判定するシグネチャ等の作成が行われている。
【先行技術文献】
【特許文献】
【０００９】
【特許文献１】特許第５０８８４０３号
【発明の概要】
【発明が解決しようとする課題】
【００１０】
しかしながら、制御システムにおいては情報システムと比較して利用される通信が限られている。このため、制御システムには、確実に不正な通信を定義するブラックリスト型

ではなく、確実に正常な通信を定義するホワイトリスト型の不正通信の検査が向いている。しかしながら、制御システムの構築者のすべてが通信プロトコルの詳細（利用ポート番号、データフォーマットなど）を把握しているわけではない。また、制御システムの通信プロトコル、特に独自プロトコルや非公開仕様によりシステム構築者も認識していない通信もあり正確なシグネチャを作成することは実際には不可能である。

【００１１】

このような背景から、特に制御システムと他のシステムとの境界で不正な通信を検査し、場合によっては遮断する技術が提案されている。例えば特許文献１では、ネットワーク境界にＩＤＳを拡張した通信検出装置を設け、この通信検出装置により不正な通信を検出し、制御システムを保護する。しかし、この特許文献１に開示の技術では、制御ネットワークの内部の機器がウイルスに感染した場合や、不正な機器が制御ネットワークに接続された場合に、これらの機器による脅威から制御ネットワークを守ることができない。

【００１２】

また、特許文献１に開示された不正通信検査技術では、不正な通信を定義するリストを如何にして作成するかが重要であるが、特許文献１には、このリストの作成方法に関する説明がない。

【００１３】

一方、特許文献１では、情報システムへのＩＰＳ装置導入時に通常行われることと同様、一定期間の通信データを収集・分析し、正常な通信データを定義する情報を通信許可リストに登録する手法が提案されている。しかし、制御システムにおいては仮に２０年連続稼働したとしても一度も発生しないような設備の故障などの際にのみ発生する通信データも存在する。特許文献１に開示の技術を採用した場合、このような発生頻度の著しく低い通信データを定義する情報が通信許可リストに登録されない可能性が高い。しかし、そのような通信許可リストに定義情報が登録されていない通信データが発生した場合には、正常な通信データであるにも拘わらず、不正通信と判定され、通信が遮断される問題が発生する。

【００１４】

この発明は、以上のような事情に鑑みてなされたものであり、ネットワークにおいて発生する通信データを正確に検査し、不正な通信を確実に防止する技術的手段を提供することを目的とする。

【課題を解決するための手段】

【００１５】

この発明による不正通信検査装置は、ネットワークを利用して通信を行う装置が従うべき動作定義を取得し、前記動作定義に基づいて、正常な通信データを定義する検査定義を生成する検査定義生成手段と、前記ネットワークから取得した通信データを検査し、前記検査定義により定義された正常な通信データのみを許可する通信データ検査手段とを具備することを特徴とする。

【発明の効果】

【００１６】

かかる発明によれば、不正通信検査装置は、ネットワークを経由する通信データのうち正常な通信データを正確に漏れなく定義することが可能となる。従って、不正な通信が行われるのを確実に防止することができる。

【図面の簡単な説明】

【００１７】

【図１】この発明の一実施形態による不正通信検査装置を含む通信システムの構成を示すブロック図である。

【図２】同実施形態における制御システムの構成を示すブロック図である。

【図３】同実施形態による不正通信検査装置の動作を示すフローチャートである。

【図４】同実施形態におけるコントローラに記憶されたコントローラ設定・プログラムにおいて定義された制御システム内の通信制御に使用される信号とメモリアドレスのリスト

である。
【図５】同実施形態におけるオペレータステーションに記憶された動作定義の例を示す図である。
【図６】同実施形態におけるデータベースステーションに記憶された動作定義の例を示す図である。
【図７】同不正通信検査装置に記憶された検査定義の例を示す図である。
【図８】同実施形態における通信データの検査結果を示すデータを例示する図である。
【図９】ファイアウォールにおいて用いられる検査ルールを例示する図である。
【図１０】ＩＤＳやＩＰＳにおいて用いられる検査ルールを例示する図である。
【図１１】ＩＤＳやＩＰＳにおいて行われる不正通信の検査の結果を例示する図である。
【発明を実施するための形態】
【００１８】
以下、図面を参照し、この発明の実施形態について説明する。
図１はこの発明の一実施形態による不正通信検査装置１００を含む通信システムの構成を示すブロック図である。図１に示すように、この通信システムは、制御ネットワーク５００に接続された制御システム５００Ｓと、情報ネットワーク７００に接続された情報システム７００Ｓとを有する。ここで、制御システム５００Ｓと情報システム７００Ｓは、ファイアウォール３００などにより隔離されている。
【００１９】
情報ネットワーク７００には、オフィスパソコン等によるクライアント装置３８０が接続されている。このクライアント装置３８０は、インターネットに代表されるネットワーク８００を介してＷｅｂサーバやメールサーバ等（図示略）と通信を行う。この通信のセキュリティを確保するため、情報ネットワーク７００には、ＩＤＳ装置３４０やＩＰＳ装置３６０、ファイアウォール４００等が接続されている。ここで、ファイアウォール３００、ＩＤＳ装置３４０、ＩＰＳ装置３６０、ファイアウォール４００は、自動的または管理者の指示により、セキュリティベンダ等によって運営されるシグネチャ配布サーバ４２０にネットワーク８００を介してアクセスし、このシグネチャ配布サーバ４２０からシグネチャの配布を受け、シグネチャを随時更新する。
【００２０】
制御ネットワーク５００には、本実施形態による不正通信検査装置１００の他に、制御システム５００Ｓを構成するエンジニアリングステーション２００、データベースステーション２２０、オペレータステーション２４０、コントローラ２６０が接続されている。これらの各装置は、制御ネットワーク５００を介して通信を行う。
【００２１】
ここで、コントローラ２６０は、例えばＰＬＣ（Ｐｒｏｇｒａｍｍａｂｌｅ Ｌｏｇｉｃ Ｃｏｎｔｒｏｌｌｅｒ）、ＤＣＳ用コントローラ等である。エンジニアリングステーション２００、データベースステーション２２０、オペレータステーション２４０は、専用装置またはＰＣ（Ｐｅｒｓｏｎａｌ Ｃｏｍｐｕｔｅｒ）である。このエンジニアリングステーション２００、データベースステーション２２０、オペレータステーション２４０の各々は、一台の専用装置またはＰＣにより構成される場合があり、また、冗長性を考慮して複数台の専用装置またはＰＣにより構成される場合もある。また、エンジニアリングステーション２００、データベースステーション２２０、オペレータステーション２４０は、ＶＰＮ装置などを経由して互いに離れた場所に設置される場合もある。
【００２２】
フィールド機器２８０は、制御および計測対象であり、例えば各種センサやアクチュエータ、モータ、ポンプ、バルブなどが代表的である。
【００２３】
コントローラ２６０は、フィールド機器２８０を制御し、またはフィールド機器２８０により計測を行うものである。制御システム５００Ｓの規模や重要度に応じて、一台のコントローラ２６０が設けられる場合もあり、また、複数台のコントローラ２６０からなる

冗長構成が採られる場合もある。また、異機種のコントローラ２６０からなる同一論理構成のコントローラが用いられる場合もある。また、コントローラ２６０は、専用装置であってもよいし、ＰＣ上で動作するアプリケーションにより実現されるソフトウェアＰＬＣであってもよい。

【００２４】

制御システム５００Ｓと情報システム７００Ｓとの間には制御情報ネットワーク６００が介在している。制御ネットワーク５００および制御情報ネットワーク６００の両方に接続された装置（例えばオペレータステーション２４０、データベースステーション２２０）は、制御情報ネットワーク６００およびファイアウォール３００を介して、情報ネットワーク７００に接続された装置（例えばクライアント装置３８０）と通信することが可能である。また、制御ネットワーク５００により接続された制御システム５００Ｓは、制御情報ネットワーク６００を介して生産管理システム３２０等から生産指示や情報の取得を行う。

【００２５】

図２は、図１における制御システム５００Ｓの構成を示すブロック図である。図２に示すように、制御システム５００Ｓは、不正通信検査装置１００と、エンジニアリングステーション２００と、データベースステーション２２０と、オペレータステーション２４０と、コントローラ２６０とを有する。

【００２６】

エンジニアリングステーション２００は、制御ネットワーク５００を利用して通信を行う装置が従うべき動作定義を生成する動作定義生成手段である。このエンジニアリングステーション２００は、制御システム５００Ｓ内の他の装置と通信する手段である通信機能部２０１と、システムの動作定義やコントローラ２６０のプログラムを作成するエンジニアリング支援機能部２０２とを保有する。エンジニアリング支援機能部２０２は、保守画面やトレンド画面といった画面に出す信号の定義や画面の作成、コントローラ２６０のプログラム開発を行う手段であり、エンジニアリング作業の成果として動作定義２０３、コントローラ設定・プログラム２０４を作成する。

【００２７】

データベースステーション２２０は、制御システム５００Ｓ内の他の装置と通信する通信機能部２２１と、制御システム５００Ｓの実績情報などを収集して蓄積データ２２４として蓄積するデータ収集機能部２２２を有する。ここで、データ収集機能部２２２は、エンジニアリングステーション２００によって生成された動作定義２０３から抽出された動作定義２２３に基づいて動作する。

【００２８】

オペレータステーション２４０は、制御システム５００Ｓ内の他の装置と通信するための通信機能部２４１と、制御システム５００Ｓの実績情報などを表示し、必要に応じて操作指示を行う表示機能・操作機能部２４２を有する。ここで、表示機能・操作機能部２４２は、エンジニアリングステーション２００によって生成された動作定義２０３から抽出された動作定義２４３に基づいて動作する。

【００２９】

コントローラ２６０は、制御システム５００Ｓ内の他の装置と通信するための通信機能部２６１と、コントローラ設定・プログラム２６３を元に動作し、デジタル信号やアナログ信号の入出力を通じてセンサやアクチュエータの制御を行う計測・制御機能部２６２とを有する。コントローラ設定・プログラム２６３は、エンジニアリングステーション２００により生成され、通信機能部２６１等（他の手段として、例えばＳＤカードなどの媒体やＵＳＢケーブルによる接続などがある）によって取得されたコントローラ設定・プログラム２０４である。

【００３０】

不正通信検査装置１００は、制御ネットワーク５００に接続された装置を送信元とする通信データ、制御ネットワーク５００に接続された装置を宛先とする通信データが正常な

通信データであるか否かを検査し、正常な通信データの通信のみを許可する装置である。図２に示すように、不正通信検査装置１００は、通信機能部１０１と、通信データ検査機能部１０２と、設定・動作定義登録機能部１０３とを保有する。ここで、通信データ検査機能部１０２と、設定・動作定義登録機能部１０３は、不正通信検査装置１００を構成するＣＰＵが不揮発性メモリに記憶されたプログラムを実行することにより実現される機能である。

【００３１】

通信機能部１０１は、制御ネットワーク５００と直接、または制御ネットワーク５００の通信データを複製する通信データ複製機能部５０１を介して間接的に通信を行う手段である。

【００３２】

設定・動作定義登録機能部１０３は、制御ネットワーク５００を利用して通信を行う装置が従うべき動作定義である動作定義２０３およびコントローラの設定・プログラム２０４をエンジニアリングステーション２００から通信機能部１０１等を介して取得し、この動作定義に基づいて、正常な通信データを定義する検査定義１１３を生成する検査定義生成手段である。

【００３３】

通信データ検査機能部１０２は、制御ネットワーク５００から通信機能部１０１を介して取得した通信データを検査し、検査定義１１３により定義された通信データのみを許可するとともに、通信機能部１０１を介して取得した通信データを通信データ１１４として記録する通信データ検査手段である。

【００３４】

次に本実施形態の動作について説明する。

オペレータがエンジニアリングステーション２００に対して動作定義１１１およびコントローラ設定・プログラム１１２を登録したとする。この場合、エンジニアリングステーション２００のエンジニアリング支援機能部２０２は、通信機能部２０１により、制御ネットワーク５００を介してコントローラ２６０、データベースステーション２２０およびオペレータステーション２４０に動作定義２０３およびコントローラ設定・プログラム２０４を配布する。

【００３５】

コントローラ２６０は、エンジニアリングステーション２００から配布されたコントローラ設定・プログラム２０４をコントローラ設定・プログラム２６３として記憶する。また、データベースステーション２２０およびオペレータステーション２４０は、エンジニアリングステーション２００から配布された動作定義２０３から自装置に関係する情報を抽出し、動作定義２２３および２４３として各々記憶する。

【００３６】

図４は、コントローラ２６０に記憶されたコントローラ設定・プログラム２６３において定義された制御システム５００Ｓ内の通信制御に使用される信号とメモリアドレスのリストである。図５は、オペレータステーション２４０に記憶された動作定義２４３の例である。図６は、データベースステーション２２０によって記憶された動作定義２２３の例である。

【００３７】

エンジニアリングステーション２００のエンジニアリング支援機能部２０２は、コントローラ２６０、データベースステーション２２０およびオペレータステーション２４０に動作定義２０３およびコントローラ設定・プログラム２０４を配布する場合に、同時に不正通信検査装置１００に対して動作定義２０３およびコントローラ設定・プログラム２０４の登録処理を行う。

【００３８】

動作定義２０３およびコントローラ設定・プログラム２０４として正しい情報を登録するための登録方法としては、次のような方法があり得る。

【００３９】
第１の方法では、例えば事前に外部記憶媒体を経由してエンジニアリングステーション２００と不正通信検査装置１００にそれぞれの公開鍵（公開鍵暗号に基づく電子署名証明書検証用の公開鍵）を交換させておき、この公開鍵を利用した暗号通信によりエンジニアリングステーション２００から不正通信検査装置１００に動作定義２０３およびコントローラ設定・プログラム２０４を送信する。
【００４０】
この第１の方法により自動的に不正通信検査装置１００への動作定義２０３およびコントローラ設定・プログラム２０４の登録が行われる場合、次のような運用を行ってもよい。すなわち、現場の人間による不正改ざんを防止するため、不正通信検査装置１００では、動作定義２０３およびコントローラ設定・プログラム２０４の登録後、現場の人間以外の人間の承認が行われるまでの間、登録された動作定義２０３およびコントローラ設定・プログラム２０４を反映していないそれまでの検査定義１１３を用いて検査を継続するのである。
【００４１】
第２の方法では、エンジニアリングステーション２００に登録画面を表示させ、または不正通信検査装置１００にＷｅｂ画面を表示させる。そして、例えばエンジニアリングステーション２００を操作するオペレータに対して、パスワードや二要素認証等を行い、同オペレータに手動でエンジニアリングステーション２００から不正通信検査装置１００への動作定義２０３およびコントローラ設定・プログラム２０４の登録を行わせる。この方法は、システム変更を関係者に意識させることができる利点がある。
【００４２】
第３の方法では、不正通信検査装置１００に外部記憶媒体のインタフェースを設ける。このインタフェースは、不正通信検査装置１００にロックされており、不正通信検査装置１００から取り外し不能であることが好ましい。そして、外部記憶媒体に動作定義２０３およびコントローラ設定・プログラム２０４を書き込み、この外部記憶媒体内の動作定義２０３およびコントローラ設定・プログラム２０４をインタフェース経由で不正通信検査装置１００に入力しない限り、検査定義１１３の更新を行えないように不正通信検査装置１００を構成しておくのである。
【００４３】
図３は、不正通信検査装置１００の処理の流れを示すフローチャートである。不正通信検査装置１００の電源が投入されると、不正通信検査装置１００では、設定・動作定義登録機能部１０３がデータ格納領域内に動作定義１１１およびコントローラ設定・プログラム１１２が登録されているかを判定する（ステップＳ１０１）。ここで、初期状態では、データ格納領域に動作定義１１１およびコントローラ設定・プログラム１１２が登録されていないため、不正通信検査装置１００の設定・動作定義登録機能部１０３は、検査定義１１３として基本動作を定義する（ステップＳ１０３）。この基本動作は、不正通信検査装置１００のベンダが事前に定義しておくこともできるが、システムを確実に運用するためには、ステップＳ１０３においてすべての通信を不正として取り扱う基本動作を検査定義１１３として登録することが望ましい。
【００４４】
検査定義１１３を定義した後、不正通信検査装置１００は、通信データの監視を開始する。さらに詳述すると、不正通信検査装置１００において通信データ検査機能部１０２は、通信機能部１０１が通信データを受信したか否かを判断する（ステップＳ１０６）。この判断結果が「Ｎｏ」である場合、通信データ検査機能部１０２は、一定時間待機（ステップＳ１０７）した後、動作終了指示の有無を確認する（ステップＳ１１０）。そして、動作終了指示がない場合、処理はステップＳ１０１に戻り、不正通信検査装置１００の設定・動作定義登録機能部１０３が動作定義１１１およびコントローラ設定・プログラム１１２の登録の有無を判断する。以下同様であり、不正通信検査装置１００は、ステップＳ１０３→Ｓ１０６→Ｓ１０７→Ｓ１１０の順に各ステップの処理を繰り返す。

【００４５】
ここで、通信機能部１０１が通信データを受信すると、ステップＳ１０６の判断結果が「Ｙｅｓ」となる。この場合、通信データ検査機能部１０２が検査定義１１３に基づいて通信データを検査し、正常な通信か異常な通信かを判定する（ステップＳ１０８）。そして、通信データ検査機能部１０２は、通信機能部１０１が受信した通信データを、その通信データが意味する操作の形式で通信データ１１４として記録する（ステップＳ１０９）。このステップＳ１０９の処理が終わると、処理はステップＳ１１０へ進む。
【００４６】
エンジニアリングステーション２００から不正通信検査装置１００に動作定義１１１およびコントローラ設定・プログラム１１２の登録が行われると、ステップＳ１０１の判断結果が「Ｙｅｓ」となる。この場合、不正通信検査装置１００の設定・動作定義登録機能部１０３は、動作定義１１１およびコントローラ設定・プログラム１１２がデータ格納領域に最後に書き込まれた日時と、検査定義１１３が最後に書き込まれた日時とを比較することにより、検査定義１１３が最新の状態であるか否かを判断する（ステップＳ１０２）。
【００４７】
ここで、動作定義１１１およびコントローラ設定・プログラム１１２がデータ格納領域に最後に書き込まれた日時が、検査定義１１３が最後に書き込まれた日時よりも所定時間以上後の日時である場合、ステップＳ１０２の判断結果は「Ｎｏ」となる。この場合、不正通信検査装置１００の設定・動作定義登録機能部１０３は、データ格納領域内の動作定義１１１およびコントローラ設定・プログラム１１２に基づいて、最新の検査定義１１３を作成し、データ格納領域に格納する（ステップＳ１０４）。このように本実施形態において検査定義生成手段である設定・動作定義登録機能部１０３は、データ格納領域内の動作定義１１１およびコントローラ設定・プログラム１１２の更新に応じて、検査定義１１３の更新を行う。このステップＳ１０４の処理が終わると、処理はステップＳ１０６に進む。
【００４８】
図７は不正通信検査装置１００のデータ格納領域に書き込まれた検査定義１１３の例を示すものである。この検査定義１１３は、動作定義１１１およびコントローラ設定・プログラム１１２を組み合わせた内容となっている。
【００４９】
さらに詳述すると、動作定義１１１のうち例えばオペレータステーション２４０に関する動作定義（図５の動作定義２４３参照）では、Ｎｏ．１の動作として、１００ｍｓの動作タイミングでオペレータステーション２４０がコントローラ２６０のメモリアドレス％ＭＤ１．２０００から信号を取得する動作が定義されている。そこで、検査定義１１３では、図７に示すように、このＮｏ．１の動作に対応した正常な通信データが定義される。このＮｏ．１の動作に対応した正常な通信データの定義では、送信元をオペレータステーション２４０とし、宛先をコントローラ２６０とし、メモリアドレス％ＭＤ１．２０００を使用する通信データが１００ｍｓの発生周期で発生する旨が定義される。この通信データの定義において、利用プロトコルであるＴＣＰや宛先ポート番号である１２３４５は、コントローラ設定・プログラム１１２において定義された情報である。図７に示す検査定義１１３では、同様に、オペレータステーション２４０に関する動作定義（図５の動作定義２４３参照）におけるＮｏ．２～Ｎｏ．９の動作に対応した正常な通信データが定義されている。また、図７に示す検査定義１１３では、動作定義１１１のうちデータベースステーション２２０に関する動作定義（図６の動作定義２２３参照）のＮｏ．１～Ｎｏ．６の動作に対応した正常な通信データが、Ｎｏ．１０～Ｎｏ．１５の正常な通信データとして定義されている。
【００５０】
このように本実施形態では、動作定義１１１およびコントローラ設定・プログラム１１２に基づいて、制御ネットワーク５００において発生する全ての通信データを正確にかつ

漏れなく定義した検査定義１１３が設定・動作定義登録機能部１０３によって生成される。

【００５１】

また、本実施形態において設定・動作定義登録機能部１０３は、検査定義１１３において定義された正常な通信データと、動作定義１１１において定義された当該通信データを発生させる動作とを関連付ける情報を生成して記憶する。例えば図７に示す検査定義１１３において定義されたＮｏ．１の正常な通信データは、動作定義１１１のうちオペレータステーション２４０に関する動作定義（図５の動作定義２４３参照）において定義されたＮｏ．１の動作により発生する。そこで、設定・動作定義登録機能部１０３は、検査定義１１３におけるＮｏ．１の正常な通信データの定義と、オペレータステーション２４０に関する動作定義におけるＮｏ．１の動作の定義とを関連付ける情報を生成して記憶するのである。

【００５２】

図３において、ステップＳ１０２の判断結果が「Ｙｅｓ」となる場合、不正通信検査装置１００の設定・動作定義登録機能部１０３は、データ格納領域内の既存の検査定義１１３を維持する（ステップＳ１０５）。このステップＳ１０５の処理が終わると、処理はステップＳ１０６に進む。

【００５３】

次にステップＳ１０６に進むと、上述したように、通信データ検査機能部１０２は、通信機能部１０１が通信データを受信したか否かを判断する（ステップＳ１０６）。ステップＳ１０６の判断結果が「Ｙｅｓ」となると、通信データ検査機能部１０２が検査定義１１３に基づいて通信データを検査し、正常な通信か異常な通信かを判定する（ステップＳ１０８）。そして、通信データ検査機能部１０２は、通信機能部１０１が受信した通信データを、その通信データが意味する操作の形式で通信データ１１４としてデータ格納領域に記録する（ステップＳ１０９）。

【００５４】

図８はこの通信データ１１４の例を示す図である。図８に示すように、通信データ１１４は、通信データ検査機能部１０２の検査対象となった通信データと、その検査時刻と、検査における判定結果と、判定理由と、通信データが示す操作内容と、通信データそのものであるバイナリデータとからなる。ここで、通信データが検査定義１１３に定義された正常な通信データのいずれかに該当する場合、判定結果は許可となり、その正常な通信データの番号が判定理由となる。また、通信データが検査定義１１３に定義された正常な通信データのいずれにも該当しない場合、判定結果は通知となり、判定理由は空欄となる。操作内容は、検査定義１１３において、検査対象となった通信データが該当する正常な通信データの定義に関連付けられた動作定義を参照することにより生成される情報である。例えば図８に示す例において、最上段に示された通信データの判定理由はＮｏ．１となっている。ここで、検査定義１１３において、Ｎｏ．１の正常な通信データの定義は、オペレータステーション２４０に関する動作定義（図５の動作定義２４３参照）におけるＮｏ．１の動作の定義に関連付けられている。そこで、通信データ検査機能部１０２は、このＮｏ．１の動作の定義を参照し、オペレータステーション２４０からコントローラ２６０に要求することにより行われるポンプ１動作状況取得を操作内容として記録する。

【００５５】

不正通信検査装置１００は、制御システム５００Ｓの責任者から与えられる指示に従い、この通信データ１１４を表示画面に表示し、あるいは印刷装置により印刷することが可能である。

【００５６】

通信データ１１４の記録（ステップＳ１０９）が終わると、処理は、ステップＳ１１０を介してステップＳ１０１に戻る。以下、同様の処理が繰り返される。

【００５７】

以上説明したように、本実施形態による不正通信検査装置１００によれば、エンジニア

リングステーション２００の生成する動作定義２０３およびコントローラ設定・プログラム２０４を活用することで、制御ネットワーク５００において発生し得る正常な通信データの検査ルールである検査定義１１３が生成される。従って、制御ネットワーク５００において起こりうる通信を正確に識別し、不正な通信を確実に検知することが可能となる。

【００５８】

また、本実施形態による不正通信検査装置１００は、検査定義１１３における正常な通信データの定義と、その正常な通信データを発生させる動作定義とを紐付け可能であるので、各通信データがどのような意図で発生されたかを人および機械が理解可能な形式で記録することが可能となる。この結果、不正な操作指令等に由来する異常な通信データの発生についての原因調査を始めとして、それ以外のシステムの異常時や正常運用時においてもどのような操作が行われたのかを調査することが容易になるという効果がある。

【００５９】

＜他の実施形態＞

以上、この発明の一実施形態について説明したが、この発明には他にも実施形態が考えられる。例えば、以下の通りである。

【００６０】

（１）制御システム５００Ｓの各装置が記憶する動作定義１１１、コントローラ設定・プログラム１１２、動作定義２２３、動作定義２４３、コントローラ設定・プログラム２６３は、各装置が必要とするデータがすべて含まれていればよく、すべて同一ファイルとすることも可能である。

【００６１】

（２）上記実施形態において、エンジニアリング支援装置であるエンジニアリングステーション２００は、ネットワークを利用して通信を行う装置が従うべき動作定義を生成する動作定義生成手段として機能し、不正通信検査装置１００は、動作定義に基づいて、正常な通信データを定義する検査定義を生成する検査定義生成手段と、ネットワークから取得した通信データのうち検査定義により定義された通信データのみを許可する不正通信検査手段として機能した。このように、検査定義１１３を不正通信検査装置１００内で生成することは、セキュリティ上望ましいことである。しかし、検査定義生成手段をエンジニアリングステーション２００に設け、このエンジニアリングステーション２００の検査定義生成手段が生成した検査定義を不正通信検査装置１００に登録するようにしてもよい。

【００６２】

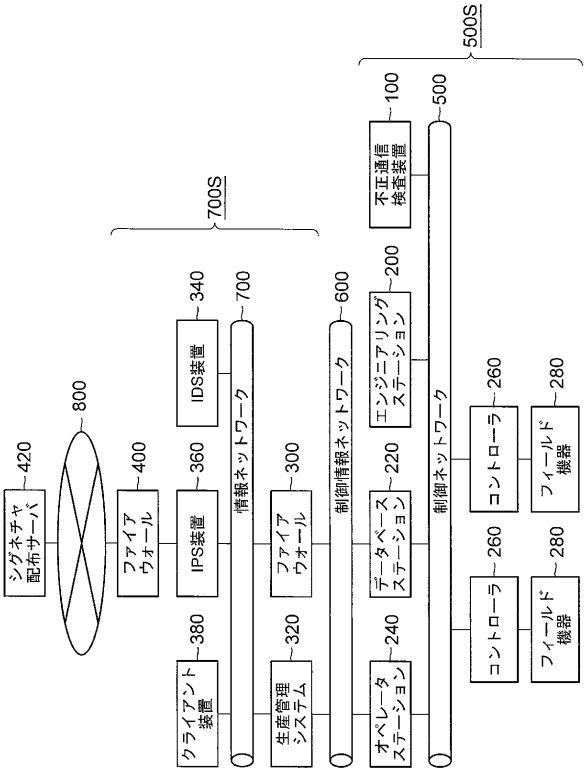
（３）上記実施形態では、動作定義１１１、コントローラ設定・プログラム１１２の存在確認や検査定義１１３の生成を、通信データの検査を行う一連の処理の中で実施した。しかし、不正通信検査装置１００の処理対象となる通信データ量が多い場合あるいはシステム構成を変更する際は停止する等の運用ポリシーが存在する場合には、動作定義１１１、コントローラ設定・プログラム１１２の存在確認や検査定義１１３の生成を定周期で実施してもよいし、起動時のみの実行としてもよい。

【符号の説明】

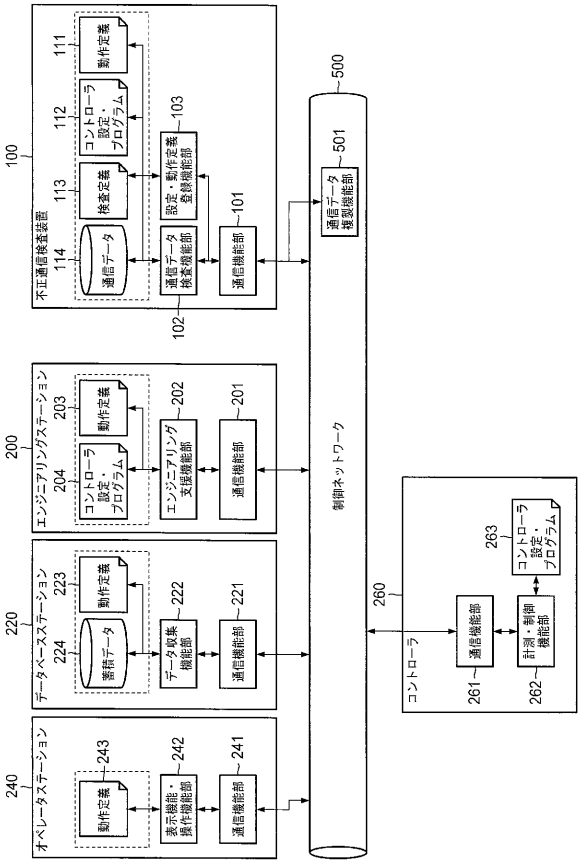
【００６３】

５００……制御ネットワーク、５００Ｓ……制御システム、１００……不正通信検査装置、２００……エンジニアリングステーション、２２０……データベースステーション、２４０……オペレータステーション、２６０……コントローラ、２８０……フィールド機器、１１１，２０３，２２３，２４３……動作定義、１１２，２０４，２６３……コントローラ設定・プログラム、１０３……設定・動作定義登録機能部、１０２……通信データ検査機能部、１０１，２０１，２２１，２４１，２６１……通信機能部、１１４……通信データ、２０２……エンジニアリング支援機能部、２２２……データ収集機能部、２２４……蓄積データ、２４２……表示機能・操作機能部、２６２……計測・制御機能部、５０１……通信データ複製機能部。

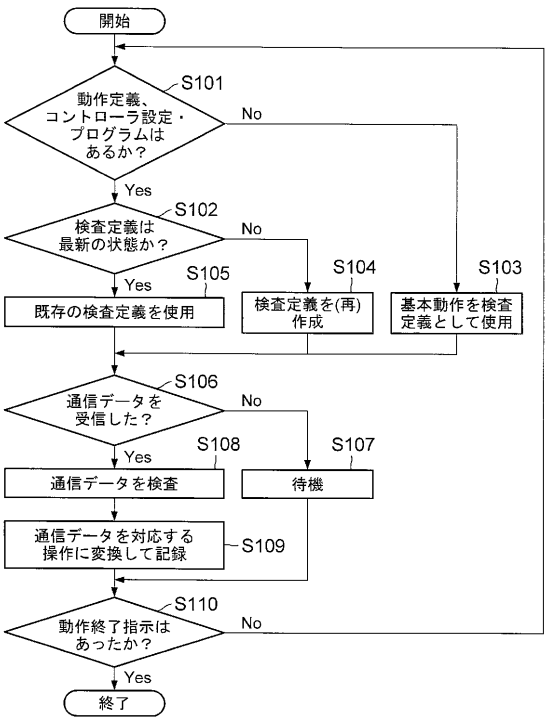
【図１】



【図２】



【図３】



【図４】

263

No.	タグ名	型	範囲	信号名称	メモリアドレス
1	POMP1	DINT	0,1	ポンプ１動作	%MD1.2000
2	POMP2	DINT	0,1	ポンプ２動作	%MD1.2002
3	POMP1_I	DINT	0~10000	ポンプ１電流	%MD1.2004
4	POMP1_V	DINT	0~10000	ポンプ１電圧	%MD1.2006
5	POMP2_I	DINT	0~10000	ポンプ２電流	%MD1.2008
6	POMP2_V	DINT	0~10000	ポンプ２電圧	%MD1.2010
...					

【図５】

243

取得先	取得先型式	取得先IPアドレス
データベースステーション	OS-1000	192.168.0.21
コントローラ	CS-7200	192.168.0.31

No.	動作	取得先	動作タイミング	タグ名	型	範囲	メモリアドレス
1	取得	コントローラ	100ms	POMP1	DINT	0,1	%MD1.2000
2	取得	コントローラ	100ms	POMP2	DINT	0,1	%MD1.2002
3	取得	コントローラ	100ms	POMP1_I	DINT	0~10000	%MD1.2004
4	取得	コントローラ	100ms	POMP1_V	DINT	0~10000	%MD1.2006
5	取得	コントローラ	100ms	POMP2_I	DINT	0~10000	%MD1.2008
6	取得	コントローラ	100ms	POMP2_V	DINT	0~10000	%MD1.2010
7	変更	コントローラ	任意	POMP1	DINT	0,1	%MD1.2000
8	変更	コントローラ	任意	POMP2	DINT	0,1	%MD1.2002
9	取得	データベースステーション	任意	POMP3	DINT	0,1	不要

【図６】

223

取得先	取得先型式	取得先IPアドレス
コントローラ	CS-7200	192.168.0.31

No.	動作	取得先	動作タイミング	タグ名	型	範囲	メモリアドレス
1	取得	コントローラ	100ms	POMP1	DINT	0,1	%MD1.2000
2	取得	コントローラ	100ms	POMP2	DINT	0,1	%MD1.2002
3	取得	コントローラ	100ms	POMP1_I	DINT	0~10000	%MD1.2004
4	取得	コントローラ	100ms	POMP1_V	DINT	0~10000	%MD1.2006
5	取得	コントローラ	100ms	POMP2_I	DINT	0~10000	%MD1.2008
6	取得	コントローラ	100ms	POMP2_V	DINT	0~10000	%MD1.2010

【図７】

113

No.	動作	利用プロトコル	送信元	送信元ポート番号	宛先	宛先ポート番号	発生間隔	検査データパターン
1	許可	TCP	オペレータステーション	任意	コントローラ	12345	100ms	コントローラ用制御プロトコルで、メモリアドレス「%MD1.2000」の取得指示
…								
6	許可	TCP	オペレータステーション	任意	コントローラ	12345	100ms	コントローラ用制御プロトコルで、メモリアドレス「%MD1.2010」の取得指示
7	許可	TCP	オペレータステーション	任意	コントローラ	12345	任意	コントローラ用制御プロトコルで、メモリアドレス「%MD1.2020」の変更指示
8	許可	TCP	オペレータステーション	任意	コントローラ	12345	任意	コントローラ用制御プロトコルで、メモリアドレス「%MD1.2002」の変更指示
9	許可	TCP	オペレータステーション	任意	データベースステーション	24424	任意	データベースステーションに対する、タグ名「PCMP3」の取得指示
10	許可	TCP	データベースステーション	任意	コントローラ	12345	100ms	コントローラ用制御プロトコルで、メモリアドレス「%MD1.2000」の取得指示
…								
15	許可	TCP	データベースステーション	任意	コントローラ	12345	100ms	コントローラ用制御プロトコルで、メモリアドレス「%MD1.2010」の取得指示
16	許可	UDP	コントローラ	任意	ブロードキャスト	5555	任意	コントローラの緊急アラーム通知プロトコルで、先頭1バイトが0x00,0x01,0x02,0x03のもの
…								
—	通知	任意	任意	任意	任意	任意	任意	上記以外

【図８】

114

時刻	判定結果	判定理由	操作内容	データ
2014/08/02 00:00:00	許可	No.1	オペレータステーションからの　ポンプ１動作状況取得	（パケットのバイナリデータすべて）
2014/08/02 00:00:00	許可	No.2	オペレータステーションからの　ポンプ２動作状況取得	（パケットのバイナリデータすべて）
…				
2014/08/02 00:00:00	許可	No.6	オペレータステーションからの　ポンプ２電圧取得	（パケットのバイナリデータすべて）
2014/08/02 00:00:00	許可	No.1	オペレータステーションからの　ポンプ１動作状況取得	（パケットのバイナリデータすべて）
2014/08/02 00:00:01	許可	No.7	オペレータステーションからの　ポンプ１動作状況変更	（パケットのバイナリデータすべて）
2014/08/02 00:00:01	通知	—	データベースステーションからの　ポンプ１動作状況変更	（パケットのバイナリデータすべて）
2014/08/02 00:00:12	許可	NO.16	コントローラからの緊急アラーム通知【機器動作異常】	（パケットのバイナリデータすべて）
…				

【図９】

No.	動作	利用プロトコル	送信元IPアドレス	送信元ポート番号	宛先IPアドレス	宛先ポート番号
1	許可	TCP	192.168.0.20	任意	192.168.0.31	12345

【図１０】

No.	動作	利用プロトコル	送信元IPアドレス	送信元ポート番号	宛先IPアドレス	宛先ポート番号	検査データパターン
1	遮断	TCP	任意	任意	任意	12345	先頭2バイトが「AAAA」で、その後の4バイトが「9090FBFF」のデータ
2	遮断	TCP	任意	任意	任意	12345	先頭2バイトが「AAAA」で、その後の4バイトが「9090FBFF」のデータ
3	通知	任意	任意	任意	任意	任意	データ長が1024バイト以上のデータ
…	許可	任意	任意	任意	任意	任意	上記以外

【図１１】

時刻	判定結果	判定理由	データ
2014/08/01 00:00:00	遮断	No.1	（パケットのバイナリデータすべて）
2014/08/01 00:00:01	遮断	No.2	（パケットのバイナリデータすべて）
2014/08/01 00:00:02	通知	No.3	（パケットのバイナリデータすべて）
2014/08/01 00:00:03	通知	No.3	（パケットのバイナリデータすべて）
2014/08/01 00:00:04	遮断	NO.4	（パケットのバイナリデータすべて）
…			