(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2015-200971
(P2015-200971A)
(43)公開日　平成27年11月12日(2015.11.12)

(51)Int.Cl.		F I		テーマコード（参考）
G05B 19/05	(2006.01)	G05B 19/05	N	5H220

審査請求 未請求　請求項の数 4　ＯＬ　（全 17 頁）

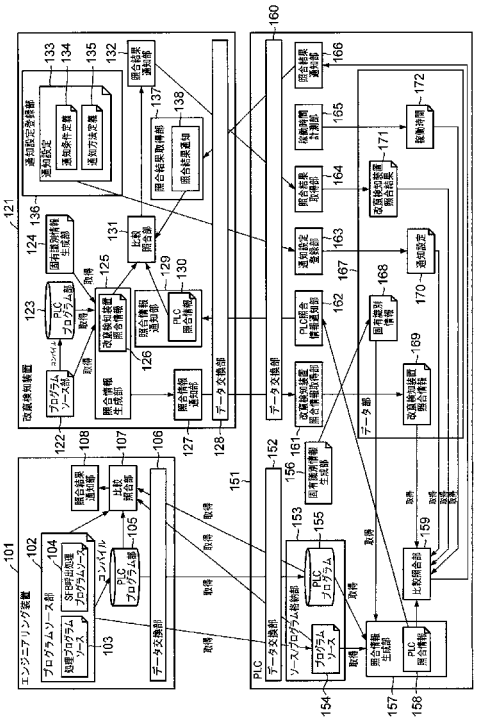
(21)出願番号　特願2014-78116(P2014-78116)
(22)出願日　平成26年4月4日(2014.4.4)

(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)　5H220 BB12　CC07　CX06　JJ12　JJ26

(54)【発明の名称】改竄検知機能を備えた制御システム

(57)【要約】
【課題】　エンジニアリング装置とＰＬＣとのデータ交換機能がコンピュータウイルスに乗っ取られた状況においても、ＰＬＣにアップロードされたプログラムの改竄を検知することを可能にする。
【解決手段】　改竄検知装置１２１は、エンジニアリング装置１０１がＰＬＣ１５１に送信するプログラムソースおよびプログラムの内容に依存した改竄検知装置照合情報１２６を生成してＰＬＣ１５１に送信し、ＰＬＣ１５１は、エンジニアリング装置１０１から取得したプログラムソースおよびＰＬＣプログラムの内容に依存したＰＬＣ照合情報１５８を生成し、改竄検知装置１２１から取得した改竄検知装置照合情報１２６と比較照合することによりプログラムの改竄を検知する。
【選択図】　図２



【特許請求の範囲】
【請求項１】
エンジニアリング装置と、プログラムを実行することにより機器を制御する制御装置と、改竄検知装置とを有し、
前記改竄検知装置は、少なくとも前記エンジニアリング装置が前記制御装置に送信するプログラムの内容に依存した改竄検知装置照合情報を生成する第1の照合情報生成手段と、前記改竄検知装置照合情報を前記制御装置に送信する第1の照合情報通知手段とを有し、
前記制御装置は、少なくとも前記エンジニアリング装置から取得したプログラムの内容に依存した制御装置照合情報を生成する第２の照合情報生成手段と、前記制御装置照合情報と前記改竄検知装置照合情報とを比較照合することによりプログラムの改竄を検知する第1の比較照合手段を有することを特徴とする制御システム。
【請求項２】
前記制御装置は、制御装置照合情報を前記改竄検知装置に送信する第２の照合情報通知手段を有し、
前記改竄検知装置は、前記改竄検知装置照合情報と前記制御装置照合情報とを比較照合することによりプログラムの改竄を検知する第２の比較照合手段を有することを特徴とする請求項１に記載の制御システム。
【請求項３】
前記改竄検知装置は、前記改竄検知装置照合情報と前記制御装置照合情報との比較照合結果を前記制御装置に通知する第1の照合結果通知手段を有し、
前記第1の比較照合手段は、前記制御装置照合情報と前記改竄検知装置照合情報との比較照合結果と、前記第1の照合結果通知手段から通知された前記改竄検知装置照合情報と前記制御装置照合情報との比較照合結果とに基づいて、プログラムの改竄を検知することを特徴とする請求項２に記載の制御システム。
【請求項４】
前記第1の照合情報生成手段は、前記エンジニアリング装置が前記制御装置に送信するプログラムソースおよびプログラムと固有情報から前記改竄検知装置照合情報を生成し、
前記第２の照合情報生成手段は、前記エンジニアリング装置から取得したプログラムソースおよびプログラムと固有情報から前記制御装置照合情報を生成することを特徴とする請求項１～３のいずれか１の請求項に記載の制御システム。

【発明の詳細な説明】
【技術分野】
【０００１】
この発明は、プログラムの改竄を検知する技術に係り、特に製造業や生産制御システム分野などで利用されるＰＬＣ（プログラマブルロジックコントローラ；Ｐｒｏｇｒａｍｍａｂｌｅ　Ｌｏｇｉｃ　Ｃｏｎｔｒｏｌｌｅｒ）のプログラムに対する改竄を検知する技術に関する。
【背景技術】
【０００２】
一般に、パーソナルコンピュータ（以下、パソコンという）によって実行されるアプリケーションプログラムの改竄を検知する方法として次の方法がある。まず、プログラム作成者が、アプリケーションプログラムにハッシュ処理を施し、この結果得られたハッシュ値をアプリケーションプログラムとともにプログラム利用者に引き渡す。次にプログラム利用者が、入手したアプリケーションプログラムにハッシュ処理を施し、この結果得られたハッシュ値とプログラム作成者から入手したハッシュ値とを照合するのである。また、他に知られた方法として、プログラムの実行時にコード署名を検証する技術がある。このコード署名は、公開鍵暗号技術によりプログラムに付与された電子署名である。
【０００３】

これらの一般的に知られている方法は、制御システム内のＰＬＣにも適用可能である。しかし、パソコンとは異なり、ＰＬＣのＣＰＵ性能やメモリ容量には制限がある。このため、ＰＬＣにこれらの一般的に知られている方法を適用することは困難である。さらに、ＰＬＣは、パソコンと異なり、インターネットに直接接続されておらず、制御システム内の制御系ネットワークに接続された状態で稼働する。このため、ＰＬＣは、プログラムの正当性を証明する証明書の失効をインターネット経由で検知するのが困難である。また、制御システムでは、エンジニアがＰＬＣの設置された現場においてＰＬＣに対する作業を行う。この現場のエンジニアにＰＬＣのプログラムの改竄検知のための煩雑な手続きを行わせるのは酷である。

【０００４】

そのため一般的には、制御システムのパソコン等のエンジニアリング装置がプログラムをＰＬＣにアップロードする際に、意図したＰＬＣのプログラムがアップロードされたのかの確認を行う。この場合の確認方法としては、ＣＲＣ（巡回冗長検査符号；Ｃｙｃｌｉｃ　Ｒｅｄｕｎｄａｎｃｙ　Ｃｈｅｃｋ）やハッシュ値を用いた方法やプログラムコードの完全比較などの方法が採られる。

【０００５】

この種の技術に関する文献として、例えば特許文献１がある。特許文献１では、ＰＬＣが実行するプログラムおよびそのプログラムソースの両方についても改竄が行われていないかの確認を行い、プログラムもしくはプログラムソースに改竄が行われている場合にその改竄箇所を表示する。

【先行技術文献】

【特許文献】

【０００６】

【特許文献１】特開２００８－２７６５２５号公報

【発明の概要】

【発明が解決しようとする課題】

【０００７】

従来、制御システムは、独自のアーキテクチャやネットワークを有していたが、オープン化が進むにつれ、汎用製品やＴＣＰ／ＩＰなどの標準プロトコルに置き換えられてきている。この結果として、パソコンであるエンジニアリング端末に悪意の動作をさせるプログラム（以降、コンピュータウイルス）を感染させることが容易となった。一例として、ある種のコンピュータウイルスは、エンジニアリング装置とＰＬＣとのデータ交換機能を乗っ取り、エンジニアリング装置からＰＬＣに不正なプログラムをアップロードさせる。この場合、ＰＬＣにアップロードされたプログラムが改竄されているのかどうかの確認をエンジニアリング装置で行おうとすると、エンジニアリング装置とＰＬＣとのデータ交換機能がＰＬＣ内の不正なプログラムから悪質なコードを除去したプログラムをエンジニアリング装置に供給する。このため、エンジニアリング装置の使用者はＰＬＣにアップロードされたプログラムが改竄されていることに気付かない。

【０００８】

特許文献１の方法では、ＰＬＣのプログラムだけでなくＰＬＣのプログラムソースも比較している。しかし、エンジニアリング装置とＰＬＣとのデータ交換機能がコンピュータウイルスに乗っ取られると、上述したように、ＰＬＣにアップロードされたプログラムが改竄されているのかどうかの確認をエンジニアリング装置で行おうとすると、エンジニアリング装置とＰＬＣとのデータ交換機能がＰＬＣ内の不正なプログラムから悪質なコードを除去したプログラムをエンジニアリング装置に供給する。従って、エンジニアリング装置の使用者は、エンジニアリング装置からＰＬＣにアップロードしたＰＬＣのプログラムが改竄されていることを検知することができない。

【０００９】

この発明は、以上説明した事情に鑑みてなされたものであり、エンジニアリング装置とＰＬＣとのデータ交換機能がコンピュータウイルスに乗っ取られた状況においても、ＰＬ

Ｃにアップロードされたプログラムの改竄を検知することを可能に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】

【００１０】

この発明は、エンジニアリング装置と、プログラムを実行することにより機器を制御する制御装置と、改竄検知装置とを有し、前記改竄検知装置は、少なくとも前記エンジニアリング装置が前記制御装置に送信するプログラムの内容に依存した改竄検知装置照合情報を生成する第1の照合情報生成手段と、前記改竄検知装置照合情報を前記制御装置に送信する第1の照合情報通知手段とを有し、前記制御装置は、少なくとも前記エンジニアリング装置から取得したプログラムの内容に依存した制御装置照合情報を生成する第２の照合情報生成手段と、前記制御装置照合情報と前記改竄検知装置照合情報とを比較照合することによりプログラムの改竄を検知する第1の比較照合手段を有することを特徴とする制御システムを提供する。

【発明の効果】

【００１１】

この発明において、エンジニアリング装置から制御装置に送信されたプログラムが改竄されている場合には、制御装置照合情報と改竄検知装置照合情報との比較照合結果が不一致となる。従って、この発明によれば、エンジニアリング装置と制御装置とのデータ交換機能がコンピュータウイルスに乗っ取られている状況においてもプログラムの改竄を検知することができる。

【図面の簡単な説明】

【００１２】

【図１】この発明の一実施形態である制御システムの構成を示すブロック図である。

【図２】同制御システムにおけるエンジニアリング装置、改竄検知装置およびＰＬＣの構成を示すブロック図である。

【図３】同実施形態における通知設定例を示す図である。

【図４】同改竄検査装置の動作を示すフローチャートである。

【図５】同ＰＬＣの照合情報生成部、比較照合部および照合結果通知部の動作を示すフローチャートである。

【発明を実施するための形態】

【００１３】

以下、図面を参照しつつ、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である制御システム１００の構成を示すブロック図である。この制御システム１００は、エンジニアリング装置１０１、改竄検知装置１２１、制御装置の一例であるＰＬＣ１５１、通信ケーブル１９１、外部記憶装置１９２、通信ケーブル１９３および外部記憶装置１９４を有している。

【００１４】

エンジニアリング装置１０１は例えばパソコン等であり、改竄検知装置１２１は例えばサーバ等である。通信ケーブル１９１と通信ケーブル１９３は、例えばＥｔｈｅｒｎｅｔ（登録商標）や産業用ネットワーク等のネットワークである。外部記憶装置１９２および１９４は例えばメモリカード等である。なお、外部記憶装置１９２および１９４は、同一の外部記憶装置であってもよい。また、図１では、ゲートウェイ装置を介して通信ケーブル１９１もしくは通信ケーブル１９３に接続されている外部のネットワークや、ＰＬＣ１５１に接続されている機器の図示は省略されている。

【００１５】

エンジニアリング装置１０１は通信ケーブル１９１を介してＰＬＣ１５１に接続されており、改竄検知装置１２１は通信ケーブル１９３を介してＰＬＣ１５１に接続されている。外部記憶装置１９２はエンジニアリング装置１０１に接続されており、外部記憶装置１９４は改竄装置１２１に接続されている。なお、エンジニアリング装置１０１、改竄検知装置１２１およびＰＬＣ１５１は、計測対象や制御対象に応じて図１よりもさらに多くの

台数で構成してもよいし、全てを一台の装置としてもよい。なお、エンジニアリング装置１０１、改竄検知装置１２１およびＰＬＣ１５１を一台の装置とする場合、通信ケーブル１９１と通信ケーブル１９３は、制御システム１００の内部に構築された仮想的ネットワークの一部を形成する。

【００１６】

図２は、本実施形態におけるエンジニアリング装置１０１、改竄検知装置１２１およびＰＬＣ１５１の構成を示すブロック図である。ただし、ＰＬＣ１５１は、演算処理を行うＣＰＵモジュールについてのみ図示している。

【００１７】

エンジニアリング装置１０１は、プログラムソース部１０２、ＰＬＣプログラム部１０５、データ交換部１０６、比較照合部１０７および照合結果通知部１０８を有している。ここで、データ交換部１０６は、ＰＬＣ１５１とデータの授受を行うための手段である。ＰＬＣ１５１からエンジニアリング装置１０１宛てに送信される各種のデータは、このデータ交換部１０６のバッファに格納され、エンジニアリング装置１０１内の処理に引き渡される。

【００１８】

プログラムソース部１０２は、処理プログラムソース１０３およびＳＦＢ（Ｓｙｓｔｅｍ　Ｆｕｎｃｔｉｏｎ　Ｂｌｏｃｋ；システムファンクションブロック）呼出処理プログラムソース１０４を記憶する手段である。ここで、処理プログラムソース１０３は、ＰＬＣ１５１に実行させるプログラムの元となるプログラムソースである。また、ＳＦＢ呼出処理プログラムソース１０４は、処理プログラムソース１０３において繰り返し呼び出すプログラムをファンクションブロック化したプログラムソースである。処理プログラムソース１０３とＳＦＢ呼出処理プログラムソース１０４は、エンジアリング装置１０１により作成してもよいし、エンジニアリング装置１０１とは別の装置により作成して外部記憶装置１９２に格納し、この外部記憶装置１９２からプログラムソース部１０２に転送してもよい。なお、設備保護や不正利用防止の観点から、エンジニアリング装置１０１にプログラムソース部１０２を設けない態様も考えられる。この態様では、後述する照合情報の生成のために使用する情報からプログラムソースを除外する。

【００１９】

ＰＬＣプログラム部１０５は、処理プログラムソース１０３およびＳＦＢ呼出処理プログラムソース１０４をコンパイルすることにより得られる実行形式のＰＬＣプログラムを記憶する手段である。なお、ＰＬＣプログラム部１０５を省略し、処理プログラムソース１０３とＳＦＢ呼出処理プログラムソース１０４のコンパイルをエンジニアリング装置１０１とは異なる装置で行ってもよい。

【００２０】

比較照合部１０７は、プログラムソース部１０２に記憶された処理プログラムソース１０３およびＳＦＢ呼出処理プログラムソース１０４と、ＰＬＣ１５１のソース／プログラム格納部１５３に記憶されたプログラムソース１５４とを比較照合するとともに、ＰＬＣプログラム部１０５に記憶されたＰＬＣプログラムと、ＰＬＣ１５１のソース／プログラム格納部１５３に記憶されたＰＬＣプログラム１５５とを比較照合する手段である。ここで、比較照合部１０７は、プログラムソース同士もしくはＰＬＣプログラム同士が一致するか否かの比較照合を行ってもよいし、プログラムソースのハッシュ値同士もしくはＰＬＣプログラムのハッシュ値同士が一致するか否かの比較照合を行ってもよい。比較照合部１０７は、各照合結果を照合結果通知部１０８に供給する。なお、エンジニアリング装置１０１に比較照合部１０７を設けない態様も考えられる。この場合は、照合結果通知部１０８も不要である。

【００２１】

照合結果通知部１０８は、比較照合部１０７から供給される照合結果を例えばエンジニアリング装置１０１のモニタに表示することにより使用者に通知する手段である。なお、エンジニアリング装置１０１に照合結果通知部１０８を設けない態様も考えられる。

【００２２】
改竄検知装置１２１は、プログラムソース部１２２、ＰＬＣプログラム部１２３、固有識別情報生成部１２４、照合情報生成部１２５、照合情報通知部１２７、データ交換部１２８、照合情報取得部１２９、比較照合部１３１、照合結果通知部１３２、通知設定登録部１３６および照合結果取得部１３７を有している。ここで、データ交換部１２８は、ＰＬＣ１５１とデータの授受を行うための手段である。ＰＬＣ１５１から改竄検知装置１２１宛てに送信される各種のデータは、このデータ交換部１２８のバッファに格納され、改竄検知装置１２１内の処理に引き渡される。
【００２３】
プログラムソース部１２２は、エンジニアリング装置１０１のプログラムソース部１０２に記憶される処理プログラムソース１０３およびＳＦＢ呼出処理プログラムソース１０４と同様なプログラムソースを記憶する手段である。好ましい態様では、プログラムソースは例えば外部記憶装置１９４に格納され、この外部記憶装置１９４からプログラムソース部１２２に転送される。なお、プログラムソース部１２２をエンジニアリング装置１０１のプログラムソース部１０２に接続してもよい。この態様では、エンジニアリング装置１０１のプログラムソース部１０２に処理プログラムソース１０３とＳＦＢ呼出処理プログラムソース１０４が格納されると、プログラムソース部１０２は直ちに改竄検知装置１２１のプログラムソース部１２２に処理プログラムソース１０３とＳＦＢ呼出処理プログラムソース１０４を転送する。
【００２４】
ＰＬＣプログラム部１２３は、プログラムソース部１２２に記憶されたプログラムソースをコンパイルすることにより得られる実行形式のＰＬＣプログラムを記憶する手段である。
【００２５】
固有識別情報生成部１２４は、改竄検知装置１２１の固有識別情報を生成して記憶する手段である。この固有識別情報は、例えば改竄検知装置１２１の固有の番号であるシリアルナンバやネットワークアダプタのＭＡＣアドレス、エンジニアリング装置１０１の使用者が登録した値などを元に生成したパスフレーズである。なお、改竄検知装置１２１のＣＰＵ性能が十分である場合、改竄検知装置１２１が暗号技術に基づいて生成した鍵や証明書を固有識別情報としてもよい。また、固有識別情報は、１つの改竄検知装置１２１について１回のみ生成するようにしてもよいし、エンジニアリング装置１０１の使用者が値を変更することができるようにしてもよい。あるいは固有識別情報生成部１２４が定期的かつ自動的に固有識別情報を生成するようにしてもよい。
【００２６】
照合情報生成部１２５は、プログラムソース部１２２に記憶されたプログラムソース、ＰＬＣプログラム部１２３に記憶されたＰＬＣプログラムおよび固有識別情報生成部１２４に記憶された固有識別情報から改竄検知装置照合情報１２６を生成する手段である。
【００２７】
この改竄検知装置照合情報１２６は、例えばプログラムソースやＰＬＣプログラムのプログラムデータ全体もしくはファンクションブロック化したプログラムデータに固有識別情報を加えてハッシュ処理を行うことにより得られる。あるいは例えばプログラムソースやＰＬＣプログラムのプログラムデータ全体もしくはファンクションブロック化したプログラムデータに対し、固有識別情報に基づく圧縮や暗号化処理を行うことにより改竄検知装置照合情報１２６を生成してもよい。あるいはプログラムソースやＰＬＣプログラムのプログラムデータ全体もしくはファンクションブロック化したプログラムデータにハッシュ処理を行った結果に対して、固有識別情報を加えてハッシュ処理を行うことにより改竄検知装置照合情報１２６を生成してもよい。あるいはプログラムソースやＰＬＣプログラムのプログラムデータ全体もしくはファンクションブロック化したプログラムデータにハッシュ処理を行った結果に対して、固有識別情報に基づく圧縮や暗号化処理を行うことにより改竄検知装置照合情報１２６を生成してもよい。本実施形態において生成される改竄

検知装置照合情報１２６の内容は、プログラムソース部１２２のプログラムソースとＰＬＣプログラム部１２３のＰＬＣプログラムの両方に依存する。

【００２８】

照合情報通知部１２７は、照合情報生成部１２５が生成した改竄検知装置照合情報１２６をＰＬＣ１５１に送信する手段である。

【００２９】

照合情報取得部１２９は、ＰＬＣ１５１のＰＬＣ照合情報通知部１６２から制御装置照合情報であるＰＬＣ照合情報１５８を取得し、そのＰＬＣ照合情報１５８をＰＬＣ照合情報１３０として比較照合部１３１に供給する手段である。さらに詳述すると、本実施形態では、改竄検知装置１２１の照合情報生成部１２５が改竄検知装置照合情報１２６を生成するとともに、ＰＬＣ１５１の照合情報生成部１５７がエンジニアリング装置１０１から取得したプログラムソースおよびＰＬＣプログラムに基づいて制御装置照合情報であるＰＬＣ照合情報１５８を生成する。比較照合部１３１に供給されるＰＬＣ照合情報１３０は、このＰＬＣ１５１の照合情報生成部１５７によって生成されるＰＬＣ照合情報１５８である。

【００３０】

比較照合部１３１は、照合情報生成部１２５が生成した改竄検知装置照合情報１２６と、照合情報取得部１２９が取得したＰＬＣ照合情報１３０とを比較照合し、その比較照合の結果である改竄検知装置照合結果（図示略）を生成する。

【００３１】

ＰＬＣ１５１は、改竄検知装置１２１の比較照合部１３１と同様な比較照合部１５９を有している。この比較照合部１５９は、ＰＬＣ１５１の照合情報生成部１５７が生成したＰＬＣ照合情報１５８と改竄検知装置１２１から取得した改竄検知装置照合情報１２６に相当する改竄検知装置照合情報１６９とを比較照合し、その比較照合の結果であるＰＬＣ照合結果（図示略）を生成する。

【００３２】

照合結果取得部１３７は、このＰＬＣ照合結果を示す照合結果通知をＰＬＣ１５１の照合結果通知部１６６から取得し、その照合結果通知を照合結果通知１３８として比較照合部１３１に供給する手段である。この照合結果通知１３８が供給された場合、比較照合部１３１は、改竄検知装置照合情報１２６とＰＬＣ照合情報１３０の比較照合した結果である改竄検知装置照合結果と、照合結果取得部１３７の照合結果通知１３８を照合結果通知部１３２に送信する。

【００３３】

照合結果通知部１３２は、比較照合部１３１から改竄検知装置照合結果と照合結果通知１３８を取得し、改竄検知装置照合結果と照合結果通知１３８をエンジニアリング装置１０１の使用者に通知し、改竄検知装置照合結果をＰＬＣ１５１の照合結果取得部１６４に送信する。ここで、改竄検知装置照合結果と照合結果通知１３８の使用者への通知は、改竄検知装置１２１やエンジニアリング装置１０１のモニタに表示し、もしくはメールを送信することにより行う。あるいは改竄検知装置１２１やエンジニアリング装置１０１に付属したランプを点灯させたりすることにより使用者への通知を行ってもよい。また、照合結果通知の内容によりエンジニアリング装置１０１の使用者への通知の態様を変更してもよい。

【００３４】

通知設定登録部１３６は、通知設定１３３を記憶する手段である。この通知設定１３３は、ＰＬＣ１５１に適用される設定であり、通知条件定義１３４と通知方法定義１３５から構成されており、エンジニアリング装置１０１の使用者によって定義される。通知設定登録部１３６は、通知設定１３３をＰＬＣ１５１の通知設定登録部１６３に送信する。なお、通知設定登録部１３６を改竄検知装置１２１ではなく、ＰＬＣ１５１やエンジニアリング装置１０１に設置してもよい。さらに、通知設定１３３は、エンジニアリング装置１０１の使用者が定義を変更できるようにしてもよい。なお、この通知設定１３３の内容に

ついては、ＰＬＣ１５１の構成の説明において詳細を明らかにする。

【００３５】

ＰＬＣ１５１は、プログラムを実行することにより機器を制御する制御装置である。このＰＬＣ１５１は、データ交換部１５２、ソース／プログラム格納部１５３、固有識別情報生成部１５６、照合情報生成部１５７、比較照合部１５９、データ交換部１６０、改竄検知装置照合情報取得部１６１、ＰＬＣ照合情報通知部１６２、通知設定登録部１６３、照合結果取得部１６４、稼働時間計測部１６５、照合結果通知部１６６およびデータ部１６７を有する。

【００３６】

ここで、データ交換部１５２は、エンジニアリング装置１０１とデータの授受を行うための手段である。エンジニアリング装置１０１からＰＬＣ１５１宛てに送信される各種のデータは、このデータ交換部１５２のバッファに格納され、ＰＬＣ１５１内の処理に引き渡される。また、データ交換部１６０は、改竄検知装置１２１とデータの授受を行うための手段である。改竄検知装置１２１からＰＬＣ１５１宛てに送信される各種のデータは、このデータ交換部１６０のバッファに格納され、ＰＬＣ１５１内の処理に引き渡される。

【００３７】

ソース／プログラム格納部１５３は、エンジニアリング装置１０１のプログラムソース部１０２から処理プログラムソース１０３とＳＦＢ呼出処理プログラムソース１０４を取得し、プログラムソース１５４として記憶する。また、ソース／プログラム格納部１５３は、エンジニアリング装置１０１のＰＬＣプログラム部１０５からＰＬＣプログラムを取得し、ＰＬＣプログラム１５５として記憶する。

【００３８】

固有識別情報生成部１５６は、ＰＬＣ１５１の固有識別情報（図示略）を生成して、データ部１６７に記憶させる手段である。この固有識別情報は、改竄検知装置１２１の固有識別情報と同様、ＰＬＣ１５１に固有の番号であるシリアルナンバやネットワークアダプタのＭＡＣアドレス、制御システム１００の使用者が登録した値などを元に生成したパスフレーズである。あるいはＰＬＣ１５１のＣＰＵ性能が十分である場合には、暗号技術に基づく鍵や証明書をＰＬＣ１５１の固有識別情報として生成してもよい。

【００３９】

照合情報生成部１５７は、ソース／プログラム格納部１５３に記憶されたプログラムソース１５４およびＰＬＣプログラム１５５と、データ部１６７に記憶された固有識別情報１６８から制御装置照合情報であるＰＬＣ照合情報１５８を生成し、このＰＬＣ照合情報１５８をＰＬＣ照合情報通知部１６２と比較照合部１５９に供給する。なお、ＰＬＣ照合情報１５８の生成方法は、改竄検知装置照合情報１２６と同様である。ＰＬＣ照合情報１５８の内容は、ソース／プログラム格納部１５３に記憶されたプログラムソース１５４とＰＬＣプログラム１５５の両方に依存する。

【００４０】

改竄検知装置照合情報取得部１６１は、改竄検知装置１２１の照合情報通知部１２７から改竄検知装置照合情報１２６を取得し、その改竄検知装置照合情報１２６を改竄検知装置照合情報１６９としてデータ部１６７に書き込む。ＰＬＣ照合情報通知部１６２は、照合情報生成部１５７からＰＬＣ照合情報１５８を取得し、そのＰＬＣ照合情報１５８を改竄検知装置１２１の照合情報通知部１２９に送信する。通知設定登録部１６３は、改竄検知装置１２１の通知設定登録部１３６から通知設定１３３を取得し、その通知設定１３３を通知設定１７０としてデータ部１６７に書き込む。照合結果取得部１６４は、改竄検知装置１２１の照合結果通知部１３２から改竄検知装置照合結果を取得し、その改竄検知装置照合結果を改竄検知装置照合結果１７１としてデータ部１６７に書き込む。稼働時間計測部１６５は、ＰＬＣ１５１の稼働時間を計測し、計測結果である稼働時間１７２をデータ部１６７に書き込む。

【００４１】

比較照合部１５９は、照合情報生成部１５７が生成したＰＬＣ照合情報１５８と、デー

タ部１６７に記憶された改竄検知装置照合情報１６９、通知設定１７０、改竄検知装置照合結果１７１および稼働時間１７２とを取得する。

【００４２】

上述したように、改竄検知装置１２１は、このＰＬＣ１５１の比較照合部１５９と同様な比較照合部１３１を有している。この比較照合部１３１が生成した改竄検知装置照合結果は、照合結果取得部１６４によって改竄検知装置照合結果１７１としてデータ部１６７に書き込まれる。そして、比較照合部１５９は、ＰＬＣ照合情報１５８と改竄検知装置照合情報１６９の比較照合を行い、ＰＬＣ照合結果を生成する。比較照合部１５９は、生成したＰＬＣ照合結果と、稼働時間１７２と、改竄検知装置照合結果１７１を基に通知設定１７０の条件に従って照合結果通知部１６６に照合結果通知を送信する。

【００４３】

照合結果通知部１６６は、比較照合部１５９の照合結果とデータ部１６７の通知設定１７０に従って照合結果通知を改竄検知装置１２１の照合結果取得部１３７に送信する。図３（ａ）は通常時における通知設定の設定例を示す。また、図３（ｂ）は、検証時における通知設定の設定例を示す。この検証時における通知設定は、制御システムのシステム開発段階等において使用される。ＰＬＣ１５１は、通常動作時、図３（ａ）の通知設定１３３を利用し、照合結果通知を行う。また、ＰＬＣ１５１は、システム開発時には図３（ｂ）の通知設定１３３を利用する。図３（ａ）および（ｂ）の通知条件は通知条件定義１３４により定義され、図３（ａ）および（ｂ）の照合結果通知は通知方法定義１３５により定義される。例えば、図３（ａ）の条件番号２は、ＰＬＣ照合結果においてプログラムソースのみ不一致であり、改竄検知装置照合結果においてプログラムソースのみが一致である場合に、即座（稼働時間）に重故障である旨の照合結果通知を行うことを指示している。また、例えば、図３（ｂ）の条件番号２は、ＰＬＣ照合結果においてプログラムソースのみ不一致であり、改竄検知装置照合結果においてプログラムソースのみ一致している場合、即座（稼働時間）に特定アドレスに照合結果を書き込む旨が指示されている。この特定アドレスとは、ＰＬＣ１５１のデータ部１６７や外部記憶装置等の任意の記憶領域を指している。図３（ｂ）の条件番号３は、ＰＬＣ照合結果においてプログラムソースのみ不一致であり、改竄検知装置照合結果においてプログラムソースのみ一致している場合、３０分以上の稼働時間が経過したときに、軽故障である旨の照合結果通知を送信する旨が指示されている。

以上が、エンジニアリング装置１０１、改竄検知装置１２１およびＰＬＣ１５１の構成である。

【００４４】

次に、本実施形態の動作を説明する。使用者が処理プログラムソース１０３とＳＦＢ呼出処理プログラムソース１０４を作成してエンジニアリング装置１０１のプログラムソース部１０２に格納する。エンジニアリング装置１０１は、このプログラムソース部１０２に格納された処理プログラムソース１０３およびＳＦＢ呼出処理プログラムソース１０４をＰＬＣ１５１に送信する。また、ＰＬＣプログラム部１０５は、プログラムソース部１０２に格納された処理プログラムソース１０３およびＳＦＢ呼出処理プログラムソース１０４をコンパイルすることにより得られるＰＬＣプログラムをＰＬＣ１５１に送信する。

【００４５】

一方、改竄検知装置１２１は、エンジニアリング装置１０１の使用者からの指示により、もしくはエンジニアリング装置１０１等の装置からの指示により図４に示す処理を実行する。なお、図４に示す処理はプログラムソースを照合情報の生成に利用する態様であり、プログラムソースを照合情報の生成に利用しない態様とする場合には、ステップＳ４０３～Ｓ４０５の処理はＰＬＣプログラムを有しているかの判定に置き換えられる。

【００４６】

まず、ステップＳ４０１において照合情報生成部１２５が動作を開始する。次にステップＳ４０２において、照合情報生成部１２５が改竄検知装置照合情報１２６を生成もしくは再生成する必要があるのかどうかを判断する。

【００４７】
ここで、例えば改竄検知装置１２１が初めて動作を開始した場合等、照合情報生成部１２５が改竄検知装置照合情報１２６を記憶していない場合、このステップＳ４０２では、照合情報生成部１２５が改竄検知装置照合情報１２６を生成する必要があると判断する。
【００４８】
また、プログラムソース部１２２内のプログラムソース、ＰＬＣプログラム部１２３内のＰＬＣプログラムおよび固有識別情報生成部１２４内の固有識別情報の何れかが更新されていた場合、このステップＳ４０２では、照合情報生成部１２５が改竄検知装置照合情報１２６を再生成する必要があると判断する。
【００４９】
これに対し、照合情報生成部１２５に改竄検知装置照合情報１２６が記憶されており、かつ、プログラムソース部１２２のプログラムソース、ＰＬＣプログラム部１２３のＰＬＣプログラムおよび固有識別情報生成部１２４の固有識別情報の何れも更新されていない場合、このステップＳ４０２では、照合情報生成部１２５が改竄検知装置照合情報１２６を生成もしくは再生成する必要がないと判断する。
【００５０】
ステップＳ４０２において、照合情報生成部１２５が改竄検知装置照合情報１２６を生成もしくは再生成する必要があると判断した場合にはステップＳ４０３に進み、その必要がないと判断した場合にはステップＳ４０８に進む。
【００５１】
図示は省略するが、エンジニアリング装置１０１の使用者がプログラムソース部１２２のプログラムソースを更新すると、エンジニアリング装置１０１から照合情報生成部１２５に、プログラムソース部１２２のプログラムソースの更新が通知される。また、エンジニアリング装置１０１の使用者が固有識別情報生成部１２４の固有識別情報を更新すると、照合情報生成部１２５に固有識別情報の更新が通知される。従って、これらの更新の通知に基づいて、このステップＳ４０２の判断をすることができる。
【００５２】
ステップＳ４０３において、照合情報生成部１２５は、プログラムソース部１２２がプログラムソースを記憶しているかどうかの判断を行う。プログラムソース部１２２がプログラムソースを記憶していない場合、ステップＳ４１４に進む。逆に、プログラムソース部１２２がプログラムソースを記憶している場合、ステップＳ４０４に進む。
【００５３】
ステップＳ４０４では、プログラムソース部１２２に記憶されたプログラムソースのコンパイルを行い、ＰＬＣプログラムを生成する。このステップＳ４０４の実行時点において既にＰＬＣプログラム部１２３がＰＬＣプログラムを記憶している場合、ＰＬＣプログラム部１２３に既に記憶されたＰＬＣプログラムに対して、コンパイルにより生成したＰＬＣプログラムを上書きする。そして、ステップＳ４０５に進む。
【００５４】
ステップＳ４０５では、照合情報生成部１２５が、コンパイルが成功したかどうかの判断を行う。そして、コンパイルが成功しなかった場合にはステップＳ４１４に進み、コンパイルが成功した場合にはステップＳ４０６に進む。
【００５５】
ステップＳ４０６では、照合情報生成部１２５が、固有識別情報生成部１２４における固有識別情報の有無の判断を行う。そして、固有識別情報生成部１２４が固有識別情報を記憶していない場合、ステップＳ４１４に進み、固有識別情報を記憶している場合はステップ４０７に進む。なお、ステップＳ４０６の動作は、ステップＳ４０１とステップＳ４０２の間に行ってもよい。
【００５６】
ステップＳ４０７では、照合情報生成部１２５が、プログラムソース部１２２に記憶されたプログラムソースと、ＰＬＣプログラム部１２３に記憶されたＰＬＣプログラムと、

固有識別情報生成部１２４に記憶された固有識別情報から改竄検知装置照合情報１２６を生成する。そして、ステップＳ４０８に進む。

【００５７】

ステップＳ４０８では、照合情報生成部１２５が生成した改竄検知装置照合情報１２６を照合情報通知部１２７に送信し、照合情報通知部１２７が改竄検知装置照合情報１２６をＰＬＣ１５１に送信する。そして、ステップＳ４０９に進む。なお、改竄検知装置照合情報１２６は、データ交換部１２８とＰＬＣ１５１のデータ交換部１６０とを経由することにより、遅延されてＰＬＣ１５１の改竄検知装置照合情報取得部１６１に届くため、照合情報通知部１２７が改竄検知装置照合情報１２６の送信を完了する前にステップＳ４０９に進んでもよい。

【００５８】

ステップＳ４０９では、照合情報取得部１２９が、データ交換部１２８のバッファにＰＬＣ１５１のＰＬＣ照合情報通知部１６２からのＰＬＣ照合情報１５８があるか否かを確認し、ＰＬＣ照合情報１５８があれば、そのＰＬＣ照合情報１５８をＰＬＣ照合情報１３０として取得する。そして、ステップＳ４１０に進む。なお、ＰＬＣ１５１のＰＬＣ照合情報通知部１６２からのＰＬＣ照合情報１５８は、ＰＬＣ１５１のデータ交換部１６０とデータ交換部１２８とを経由することにより、遅延されて照合情報取得部１２９に届く。従って、照合情報取得部１２９がステップＳ４０９の処理が完了する前にステップＳ４１０に進んでも良い。

【００５９】

ステップＳ４１０では、照合結果取得部１３７が、データ交換部１２８のバッファにＰＬＣ１５１の照合結果通知部１６６からの照合結果通知があるか否かを確認し、照合結果通知があれば、その照合結果通知を照合結果通知１３８として取得する。バッファに照合結果通知がない場合、このステップＳ４１０において照合結果取得部１３７は照合結果通知を取得しない。そして、ステップＳ４１１に進む。なお、ステップＳ４１１に進む際には、ステップＳ４０９とステップＳ４１０の動作が完了している必要がある。

【００６０】

ステップＳ４１１では、比較照合部１３１が、照合情報生成部１２５が生成した改竄検知装置照合情報１２６と、照合情報取得部１２９が取得したＰＬＣ照合情報１３０と、照合結果取得部１３７が取得した照合結果通知１３８を取得する。照合結果取得部１３７が照合結果通知１３８を取得していない場合は、比較照合部１３１は、改竄検知装置照合情報１２６とＰＬＣ照合情報１３０のみを取得してステップＳ４１１の動作を完了する。そして、ステップＳ４１２に進む。

【００６１】

ステップＳ４１２では、比較照合部１３１が、取得した改竄検知装置照合情報１２６とＰＬＣ照合情報１３０が一致するか否かの比較照合を行い、改竄検知装置照合結果を生成する。そして、ステップＳ４１３に進む。

【００６２】

ステップＳ４１３では、比較照合部１３１が、ステップＳ４１２で生成した改竄検知装置照合結果と照合結果取得部１３７から取得した照合結果通知１３８が一致するか否かの比較照合を行う。なお、ステップＳ４１０において照合結果取得部１３７がＰＬＣ１５１の照合結果通知部１６６からの照合結果通知を取得しなかった場合、このステップＳ４１３では何も処理が行われない。ステップＳ４１３が完了すると、ステップＳ４１４に進む。

【００６３】

ステップＳ４１３からステップＳ４１４に進むと、照合結果通知部１３２が、比較照合部１３１から改竄検知装置照合結果を取得するとともに、照合結果取得部１３７から照合結果通知１３８を取得し、改竄検知装置照合結果と照合結果通知１３８をエンジニアリング装置１０１の使用者に通知する。また、照合結果通知部１３２は、改竄検知装置照合結果をＰＬＣ１５１の照合結果取得部１６４に送信する。

【００６４】
なお、ステップＳ４０３、ステップＳ４０５およびステップＳ４０６からステップＳ４１４に進んだ場合は、改竄検知装置照合結果が生成されない。この場合、ステップＳ４１４では、エンジニアリング装置１０１から改竄検知装置照合結果が生成されなかった旨のアラームが出力される。ステップＳ４１４が終了すると、改竄検知装置１２１の動作が終了する（ステップＳ４１５）。
以上が、改竄検知装置１２１の動作である。
【００６５】
次に、ＰＬＣ１５１の動作について説明する。まず、エンジニアリング装置１０１が送信した処理プログラムソース１０３、ＳＦＢ呼出処理プログラムソース１０４およびＰＬＣプログラムは、ＰＬＣ１５１のソース／プログラム格納部１５３に格納される。これによりＰＬＣ１５１では、照合情報生成部１５７と比較照合部１５９と照合結果通知部１６６の動作が行われる。図５は、ＰＬＣ１５１の照合情報生成部１５７、比較照合部１５９および照合結果通知部１６６の動作を示すフローチャートである。
【００６６】
まず、ステップＳ５０１では、照合情報生成部１５７がＰＬＣ照合情報１５８を生成もしくは再生成する必要があるか否かを判断する。そして、ＰＬＣ照合情報１５８を生成もしくは再生成する必要があると判断した場合はステップＳ５０２へ進み、ＰＬＣ照合情報１５８を生成もしくは再生成する必要がないと判断した場合はステップＳ５０３へ進む。例えばＰＬＣ１５１が初めて動作を開始した場合等、照合情報生成部１５７にＰＬＣ照合情報１５８が記憶されていない場合、照合情報生成部１５７は、ＰＬＣ照合情報１５８を生成する必要があると判断する。また、ソース／プログラム格納部１５３のプログラムソース１５４、ＰＬＣプログラム１５３およびデータ部１６７の固有識別情報１６８の何れかが更新されている場合、照合情報生成部１５７はＰＬＣ照合情報１５８を再生成する必要があると判断する。これに対し、照合情報生成部１５７にＰＬＣ照合情報１５８が記憶されており、かつ、プログラムソース１５４、ＰＬＣプログラム１５５および固有識別情報１６８の何れも更新されていない場合、照合情報生成部１５７は、ＰＬＣ照合情報１５８を生成もしくは再生成する必要がないと判断する。
【００６７】
図示は省略したが、エンジニアリング装置１０１の使用者がプログラムソース部１０２の処理プログラムソース１０３やＳＦＢ呼出処理プログラムソース１０４を更新すると、エンジニアリング装置１０１から照合情報生成部１５７にプログラムソース１５４の更新が通知される。また、エンジニアリング装置１０１の使用者が固有識別情報生成部１５６の固有識別情報を更新すると、改竄検知装置１２１から照合情報生成部１５７にデータ部１６７内の固有識別情報１６８の更新が通知される。従って、照合情報生成部１５７は、これらの通知に基づいてステップＳ５０１の判断を行うことができる。
【００６８】
次にステップＳ５０２では、照合情報生成部１５７が、ソース／プログラム部１５３に記憶されたプログラムソース１５４およびＰＬＣプログラム１５５と、データ部１６７に記憶された固有識別情報１６８からＰＬＣ照合情報１５８を生成する。照合情報生成部１５７は、このＰＬＣ照合情報をＰＬＣ照合情報通知部１６２に送信し、ＰＬＣ照合情報通知部１６２はＰＬＣ照合情報１５８を改竄検知装置１２１に送信する。そして、ステップＳ５０３に進む。
【００６９】
ステップＳ５０３では、比較照合部１５９の処理を開始させる。そして、ステップＳ５０４に進む。ステップＳ５０４では、比較照合部１５９が、照合情報生成部１５７の生成したＰＬＣ照合情報１５８と、データ部１６７に記憶された改竄検知装置照合情報１６９とが一致しているか否かの比較照合を行う。そして、ＰＬＣ照合情報１５８と改竄検知装置照合情報１６９とが一致している場合には、ステップＳ５０５に進み、一致していない場合はステップＳ５０６に進む。

【００７０】
次にステップＳ５０５に進むと、比較照合部１５９は、改竄検知装置照合結果１７１と、稼働時間１７２と、通知設定１７０の通知条件に基づき照合結果通知を生成する。この場合、ステップＳ５０４からステップＳ５０５に進んでいるので、ＰＬＣ照合情報１５８と改竄検知装置照合情報１６９とが一致しており、プログラムソースおよびプログラムが完全一致している。従って、例えば通常時には、図３（ａ）の条件番号１または５が該当する。そして、改竄検知装置照合結果１７１において、プログラムソースおよびプログラムが完全一致している場合、比較照合部１５９は、条件番号５をステップＳ５０５の処理結果として決定する。一方、改竄検知装置照合結果１７１において、プログラムソースまたはプログラムの一方が不一致である場合、比較照合部１５９は、条件番号１をステップＳ５０５の処理結果として決定する。そして、ステップＳ５０７に進む。
【００７１】
ステップＳ５０５からステップＳ５０７に進むと、ステップＳ５０５において決定した条件番号１に従って照合結果通知部１６６を動作させる。この場合、照合結果通知部１６６は照合結果通知を送信しない。
【００７２】
一方、ステップＳ５０４からステップＳ５０６に進むと、比較照合部１５９は、ステップＳ５０３で生成したＰＬＣ照合結果、改竄検知装置照合結果１７１と、稼働時間１７２と、通知設定１７０に基づき、照合結果通知を生成する。この場合、ステップＳ５０４からステップＳ５０６に進んでいるので、プログラムソースまたはプログラムの少なくとも一方が不一致、もしくは改竄検知装置照合結果１７１が取得されていない。従って、例えば通常時には、図３（ａ）の条件番号２～４または６～９が該当する。そこで、比較照合部１５９は、条件番号２～４または６～９の中に、ステップＳ５０３で生成したＰＬＣ照合結果と改竄検知装置照合結果１７１とが満たす条件番号があるか否かを判断する。そして、該当する条件番号がある場合には、その条件番号をステップＳ５０６の処理結果として決定し、ステップＳ５０７に進む。
【００７３】
ステップＳ５０６からステップＳ５０７に進むと、ステップＳ５０５において決定した条件番号に従って照合結果通知部１６６を動作させる。例えばステップＳ５０５において決定した条件番号が２である場合、照合結果通知部１６６は、重故障である旨の照合結果通知を即座に改竄検知装置１２１に送信する。そして、照合情報生成部１５７、比較照合部１５９および照合結果通知部１６６の動作が終了する（ステップＳ５０８）。
【００７４】
一方、ステップＳ５０６において、条件番号２～４または６～９の中に、ステップＳ５０３で生成したＰＬＣ照合結果と改竄検知装置照合結果１７１とが満たす条件番号がなかった場合、ステップＳ５０７は実行されることなく、照合情報生成部１５７、比較照合部１５９および照合結果通知部１６６の動作が終了する（ステップＳ５０８）。
【００７５】
図５に示す処理を終了した場合、その後、ＰＬＣ１５１は、ソース／プログラム格納部１５３のＰＬＣプログラム１５５を実行する。
【００７６】
図５に示す処理において、重故障である旨の照合結果通知を送信した場合、ＰＬＣ１５１は、ソース／プログラム格納部１５３のＰＬＣプログラム１５５の実行を停止する。このように、本実施形態では、ＰＬＣ１５１が改竄されたプログラムを実行するのを阻止することができる。
【００７７】
システム開発時等において、データ部１６７における通知設定１７０が図３（ｂ）の検証時の通知設定となっている場合の動作は次のようになる。この場合、例えばＰＬＣ照合結果においてプログラムソースのみが不一致となっており、改竄検知装置照合結果においてプログラムソースのみが一致している場合、条件番号２を満たすこととなり、比較照合

部１５９は、ＰＬＣ照合結果および改竄検知装置照合結果をＰＬＣ１５１のメモリの特定アドレスに書き込む。条件番号６が満たされる場合も同様である。システム開発時には、このようにして特定アドレスに書き込まれるＰＬＣ照合結果および改竄検知装置照合結果を解析することによりシステムのデバッグ等を行うことが可能である。

以上が、ＰＬＣ１５１の動作である。

【００７８】

次に本実施形態の効果を説明する。エンジニアリング装置１０１のデータ交換部１０６が悪意あるコンピュータウイルス等に感染すると、エンジニアリング装置１０１のプログラムソース部１０２に記憶された処理プログラムソース１０３およびＳＦＢ呼出処理プログラムソース１０４と、ＰＬＣプログラム部１０５に記憶されたＰＬＣプログラムがデータ交換部１０６を介してＰＬＣ１５１に送信されるとき、データ交換部１０６によってプログラムソースまたはプログラムが改竄される。

【００７９】

そのため、ＰＬＣ１５１のソース／プログラム格納部１５３に記憶されたプログラムソース１５４やＰＬＣプログラム１５５は、エンジニアリング装置１０１のプログラムソース部１０２の処理プログラムソース１０３およびＳＦＢ呼出処理プログラムソース１０４やＰＬＣプログラム部１０５のＰＬＣプログラムと一致しなくなる。

【００８０】

ここで、エンジニアリング装置１０１の比較照合部１０７は、エンジニアリング装置１０１のプログラムソース部１０２の処理プログラムソース１０３およびＳＦＢ呼出処理プログラムソース１０４とＰＬＣ１５１のソース／プログラム格納部１５３のプログラムソース１５４とを比較照合し、エンジニアリング装置１０１のＰＬＣプログラム部１０５のＰＬＣプログラムと、ＰＬＣ１５１のソース／プログラム格納部１５３のＰＬＣプログラム１５５とを比較照合する。

【００８１】

しかし、ＰＬＣ１５１のプログラムソース１５４やＰＬＣプログラム１５５がエンジニアリング装置１０１のデータ交換部１０６を介して比較照合部１０７に転送されるとき、データ交換部１０６がプログラムソースおよびプログラムを改竄前の状態に書き換えると、エンジニアリング装置１０１の処理プログラムソース１０３、ＳＦＢ呼出処理プログラムソース１０４およびＰＬＣプログラムと、データ交換部１０６を介して取得されるＰＬＣ１５１のプログラムソース１５４、ＰＬＣプログラム１５５は一致することとなる。この場合、たとえ比較照合部１０７による比較照合を行ったとしても、プログラムの改竄を検知することができない。

【００８２】

しかし、本実施形態によれば、ＰＬＣ１５１の比較照合部１５９は、同ＰＬＣ１５１の照合情報生成部１５７がＰＬＣ１５１のプログラムソース１５４およびＰＬＣプログラム１５５から生成したＰＬＣ照合情報１５８と、改竄検知装置１２１の照合情報生成部１２５がエンジニアリング装置１０１の処理プログラムソース１０３、ＳＦＢ呼出処理プログラムソース１０４およびＰＬＣプログラムから生成した改竄検知装置照合情報１２６との比較照合を行う。ここで、エンジニアリング装置１０１からＰＬＣ１５１に送信されたプログラムソース１５４またはＰＬＣプログラム１５５が改竄されている場合には、ＰＬＣ照合情報１５８と改竄検知装置照合情報１２６とが一致しなくなる。従って、データ交換部１０６が悪意あるコンピュータウイルス等に感染した場合においても、ＰＬＣ照合情報１５８と改竄検知装置照合情報１２６との比較照合によりプログラムの改竄を検知することができる。

【００８３】

また、本実施形態によれば、改竄検知装置１２１の比較照合部１３１は、同改竄検知装置１２１の照合情報生成部１２５がエンジニアリング装置１０１の処理プログラムソース１０３、ＳＦＢ呼出処理プログラムソース１０４およびＰＬＣプログラムから生成した改竄検知装置照合情報１２６と、ＰＬＣ１５１の照合情報生成部１５７がＰＬＣ１５１内の

プログラムソース１５４およびＰＬＣプログラム１５５から生成したＰＬＣ照合情報１５８との比較照合を行う。この比較照合によってもプログラムの改竄を検知することができる。

【００８４】

さらに、本実施形態によれば、ＰＬＣ１５１の比較照合部１５９は、同比較照合部１５９において行ったＰＬＣ照合情報１５８と改竄検知装置照合情報１６９との比較照合結果と、改竄検知装置１２１の比較照合部１３１が行ったＰＬＣ照合情報１３０と改竄検知装置照合情報１２６との比較照合結果と、データ部１６７の通知設定１７０に基づいて、照合結果通知１６６による照合結果通知の送信を行わせる。従って、プログラムの改竄の深刻度に応じて、適切な照合結果通知の送信を行わせることができる。

【００８５】

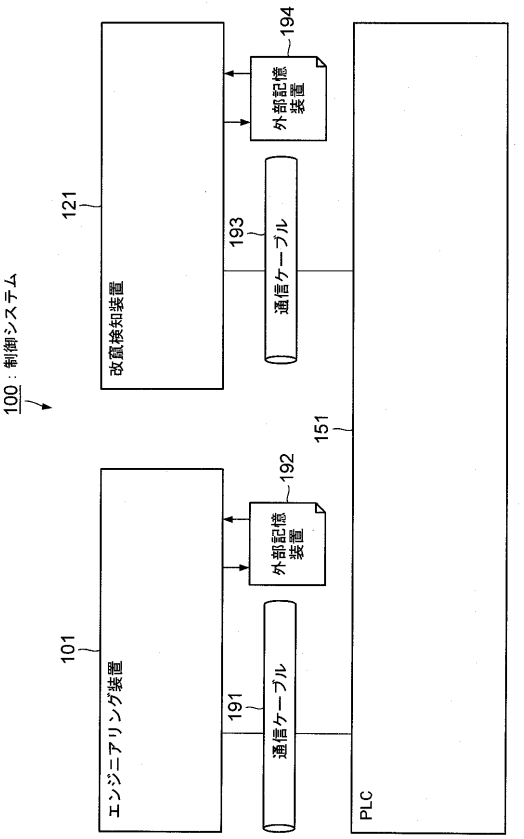
以上、この発明の一実施形態について説明したが、この発明には他にも実施形態が考えられる。例えば上記実施形態における制御システムでは、プログラムを実行することにより機器を制御する制御装置として、ＰＬＣを用いたが、ＤＣＳ（分散型制御装置）を制御装置として用いてもよい。このＤＣＳは、強力な２重化制御機能を有しており、ＰＬＣに比べて高い信頼性を有している。ＰＬＣが一般的にＦＡ（Ｆａｃｔｏｒｙ　Ａｕｔｏｍａｔｉｏｎ）などに適用されるのに対し、ＤＣＳは高信頼が要求されるプラント設備などに適用される。このＤＣＳを制御装置として使用する制御システムに本発明を適用してもよい。この態様によれば、エンジニアリング装置とＤＣＳとの間のデータ交換機能がコンピュータウイルスに乗っ取られている状況においても、上記実施形態と同様、ＤＣＳのプログラムの改竄を検知することができる。

【符号の説明】

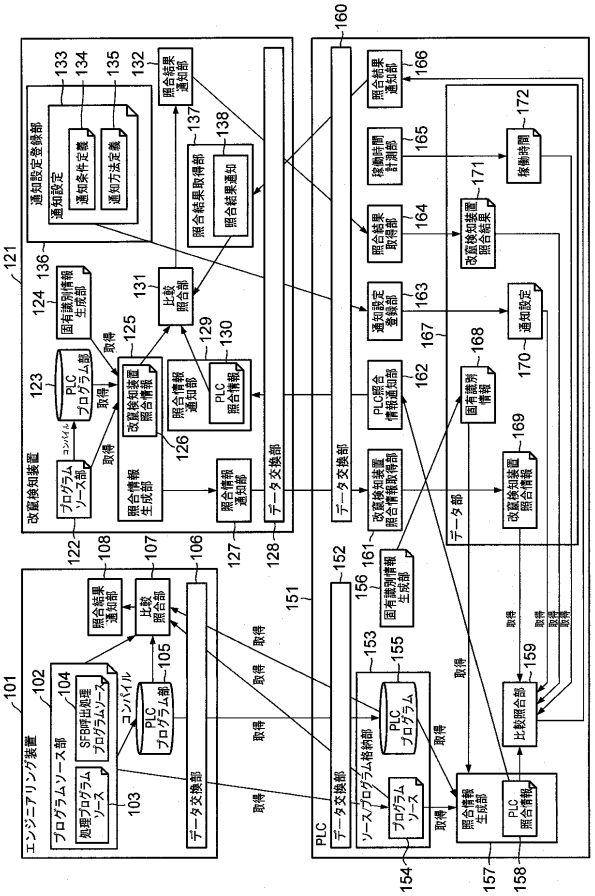
【００８６】

１００……制御システム、１０１……エンジニアリング装置、１０２……プログラムソース部、１０３……処理プログラムソース、１０４……ＳＦＢ呼出処理プログラムソース、１０５……ＰＬＣプログラム部、１０６……データ交換部、１０７……比較照合部、１０８……照合結果通知部、１２１……改竄検査装置、１２２……プログラムソース部、１２３……ＰＬＣプログラム部、１２４……固有識別情報生成部、１２５……照合情報生成部、１２６……改竄検知装置照合情報、１２７……照合情報通知部、１２８……データ交換部、１２９……照合情報通知部、１３０……ＰＬＣ照合情報、１３１……比較照合部、１３２……照合結果通知部、１３３……通知設定、１３４……通知条件定義、１３５……通知方法定義、１３６……通知設定登録部、１３７……照合結果取得部、１３８……照合結果通知、１５１……ＰＬＣ、１５２……データ交換部、１５３……ソース／プログラム格納部、１５４……プログラムソース、１５５……ＰＬＣプログラム、１５６……固有識別情報生成部、１５７……照合情報生成部、１５８……ＰＬＣ照合情報、１５９……比較照合部、１６０……データ交換部、１６１……改竄検知装置照合情報取得部、１６２……ＰＬＣ照合情報通知部、１６３……通知設定登録部、１６４……照合結果取得部、１６５……稼働時間計測部、１６６……照合結果通知部、１６７……データ部、１６８……固有識別情報、１６９……改竄検知装置照合情報、１７０……通知設定、１７１……改竄検知装置照合結果、１７２……稼働時間、１９１……通信ケーブル、１９２……外部記憶装置、１９３……通信ケーブル、１９４……外部記憶装置

【図１】



【図２】



【図３】

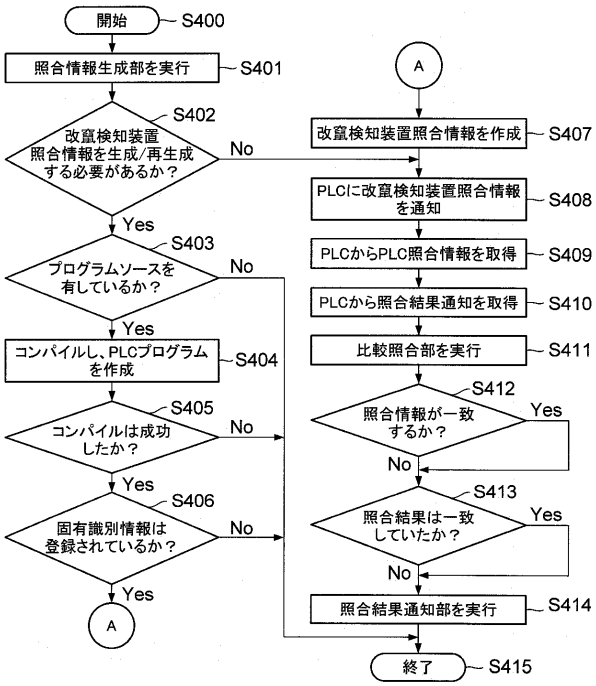
(a) 通常時における通知設定の設定例

条件番号	通知条件 比較結果 PLC照合結果	改竄検知装置照合結果	稼働時間	照合結果通知 通知する(通知内容) /通知しない
1	完全一致	プログラムソース、プログラムの一方が不一致	即座	通知しない
2	プログラムソースのみ不一致	プログラムソースのみ一致	即座	通知する(重故障)
3	プログラムのみ不一致	プログラムのみ一致	即座	通知する(重故障)
4	完全不一致	プログラムソース、プログラムの一方が不一致	即座	通知する(重故障)
5	完全一致	完全一致	即座	通知しない
6	プログラムソースのみ不一致	プログラムソースのみ不一致	即座	通知する(重故障)
7	プログラムのみ不一致	プログラムのみ不一致	即座	通知する(重故障)
8	完全不一致	完全不一致	即座	通知する(重故障)
9	照合結果無し	照合結果無し	即座	通知する(重故障)

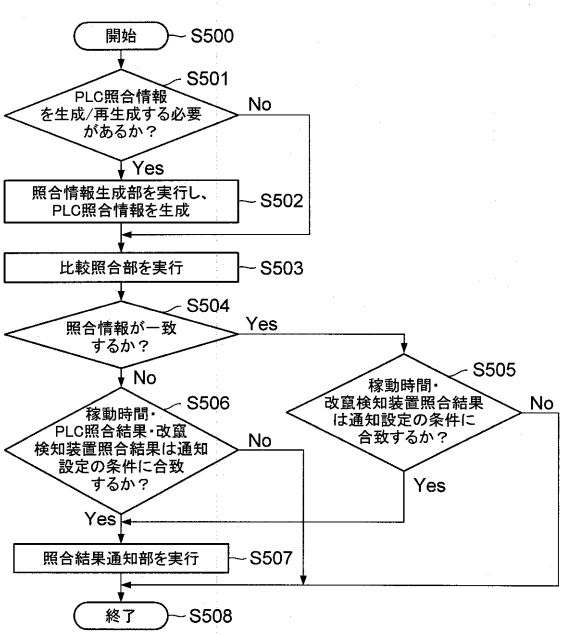
(b) 検証時における通知設定の設定例

条件番号	通知条件 比較結果 PLC照合結果	改竄検知装置照合結果	稼働時間	照合結果通知 通知する(通知内容) /通知しない
1	完全一致	完全一致以外	即座	通知しない
2	プログラムソースのみ不一致	プログラムソースのみ一致	即座	特定アドレスに照合結果書き込み
3	プログラムソースのみ不一致	プログラムソースのみ一致	30分以上	通知する(軽故障)
4	プログラムのみ不一致	プログラムのみ一致	即座	通知する(軽故障)
5	プログラムのみ不一致	プログラムのみ一致	1日以上	通知する(重故障)
6	完全不一致	完全不一致以外	即座	特定アドレスに照合結果書き込み
7	完全一致	完全一致	即座	通知しない
8	プログラムソースのみ不一致	プログラムソースのみ不一致	即座	通知しない
9	プログラムのみ不一致	プログラムのみ不一致	即座	通知しない
10	完全不一致	完全不一致	即座	通知しない
11	照合結果無し	照合結果無し	即座	通知しない

【図４】



【図５】


開始
S500
S501
PLC照合情報を生成/再生成する必要があるか？
No
Yes
照合情報生成部を実行し、PLC照合情報を生成
S502
比較照合部を実行
S503
S504
照合情報が一致するか？
Yes
No
S505
稼動時間・改竄検知装置照合結果は通知設定の条件に合致するか？
No
Yes
S506
稼動時間・PLC照合結果・改竄検知装置照合結果は通知設定の条件に合致するか？
No
Yes
照合結果通知部を実行
S507
終了
S508