

(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2022年12月15日(15.12.2022)



(10) 国際公開番号

WO 2022/259384 A1

- (51) 国際特許分類:
G05B 19/05 (2006.01)
- (21) 国際出願番号: PCT/JP2021/021794
- (22) 国際出願日: 2021年6月8日(08.06.2021)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (71) 出願人:三菱電機株式会社(MITSUBISHI ELECTRIC CORPORATION) [JP/JP]; 〒1008310 東京都千代田区丸の内二丁目7番3号 Tokyo (JP).
- (72) 発明者:市川 英嗣(ICHIKAWA Eiji); 〒4618670 愛知県名古屋市東区矢田南五丁目1番14号 三菱電機メカトロニクスソフトウェア

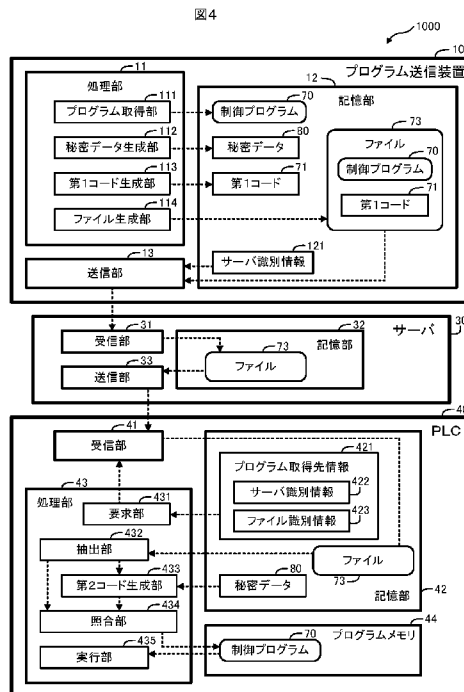
株式会社内 Aichi (JP). 佐々木 亮一(SASAKI Ryoichi); 〒1008310 東京都千代田区丸の内二丁目7番3号 三菱電機株式会社内 Tokyo (JP). 谷出 新(TANIDE Hajime); 〒1008310 東京都千代田区丸の内二丁目7番3号 三菱電機株式会社内 Tokyo (JP).

(74) 代理人:木村 満(KIMURA Mitsuru); 〒1010054 東京都千代田区神田錦町二丁目7番地 協販ビル2階 Tokyo (JP).

(81) 指定国(表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN,

(54) Title: CONTROL SYSTEM, PROGRAMMABLE CONTROLLER, CONTROL PROGRAM TRANSMISSION METHOD AND CONTROLLER PROGRAM

(54) 発明の名称: 制御システム、プログラマブルコントローラ、制御プログラム送信方法及びコントローラプログラム



- 10 Program transmission device
11, 43 Processing unit
12, 32, 42 Storage unit
13, 33 Transmission unit
30 Server
31, 41 Receiving unit
44 Program memory
70 Control program
71 First code
80 Confidential data
73 File
111 Program acquisition unit
112 Confidential data generation unit
113 First code generation unit
114 File generation unit
121, 422 Server identification information
421 Program acquisition destination information
423 File identification information
431 Request unit
432 Extraction unit
433 Second code generation unit
434 Collation unit
435 Execution unit

(57) Abstract: This control system (1000) is equipped with a PLC (40) for controlling a device and a program transmission device (10) for transmitting a control program (70) for causing said PLC (40) to control the device. The program transmission device (10) has a first code generation unit (113) for generating, from the control program (70) and confidential data (80), a first code (71) for verifying whether or not there has been a change from the control program (70).

HR, HU, ID, IL, IN, IR, IS, IT, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

- (84) 指定国(表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, RU, TJ, TM), ヨーロッパ (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

添付公開書類：

一 国際調査報告 (条約第21条(3))

The PLC (40) has: a second code generation unit (433) for generating a second code from a receiving program as the control program (70) and from the confidential data (80) which is shared with the program transmission device (10); and an execution unit (435) for executing the receiving program when the first code (71) is the same as the second code.

(57) 要約：制御システム（１０００）は、機器を制御するＰＬＣ（４０）と、ＰＬＣ（４０）に機器を制御させるための制御プログラム（７０）を送信するプログラム送信装置（１０）と、を備える。プログラム送信装置（１０）は、制御プログラム（７０）からの変更の有無を検証するための第１コード（７１）を、制御プログラム（７０）及び秘密データ（８０）から生成する第１コード生成部（１１３）を有する。ＰＬＣ（４０）は、制御プログラム（７０）としての受信プログラム及びプログラム送信装置（１０）と共有される秘密データ（８０）から第２コードを生成する第２コード生成部（４３３）と、第１コード（７１）が第２コードに等しい場合に、受信プログラムを実行する実行部（４３５）と、を有する。

明 細 書

発明の名称：

制御システム、プログラマブルコントローラ、制御プログラム送信方法及びコントローラプログラム

技術分野

[0001] 本開示は、制御システム、プログラマブルコントローラ、制御プログラム送信方法及びコントローラプログラムに関する。

背景技術

[0002] F A (Factory Automation) の現場では、P L C (Programmable Logic Controller) が他の機器を制御することで、製造ラインに代表される種々の工程が実現されることが多い。機器を制御するためのプログラムをP L Cの内部メモリに書き込むためには、P C (Personal Computer) をP L Cに接続した上で、当該P C上で動作する専用のエンジニアリングツールを用いることが一般的である。

[0003] そのため、P Cにエンジニアリングツールをインストールする必要がある。また、エンジニアリングツールの使い方に習熟していないユーザの誤操作により、適当なプログラムがP L Cに書き込まれないおそれがある。そこで、装置が実行すべきプログラムを自ら外部から取得する技術をP L Cに適用することが考えられる（例えば、特許文献1を参照）。

[0004] 特許文献1には、P L Cに接続されて、制御システムにおける操作端末として機能するプログラマブル表示器について記載されている。このプログラマブル表示器は、起動時に、その動作を制御するプログラムをサーバから取得して内蔵のデータメモリに書き込む。

先行技術文献

特許文献

[0005] 特許文献1：特開2007-179115号公報

発明の概要

発明が解決しようとする課題

[0006] しかしながら、特許文献1の技術では、サーバから送信されるプログラムに関して、破損及び改ざんの可能性が考慮されていない。このため、特許文献1の技術をPLCに適用した場合には、ユーザの意図から外れたプログラムがPLCに取り込まれ、適当な工程が実現されなくなるおそれがある。したがって、PLCが外部から取得するプログラムに関する安全性を向上させる余地がある。

[0007] 本開示は、上記の事情に鑑みてなされたものであり、PLCが外部から取得するプログラムに関する安全性を向上させることを目的とする。

課題を解決するための手段

[0008] 上記目的を達成するため、本開示の制御システムは、機器を制御するプログラマブルコントローラと、プログラマブルコントローラに機器を制御させるための制御プログラムを送信するプログラム送信装置と、を備える制御システムであって、プログラム送信装置は、制御プログラムを取得するプログラム取得手段と、制御プログラムからの変更の有無を検証するための第1コードを、制御プログラム及び予め定められたデータから予め定められた手順で生成する第1コード生成手段と、制御プログラム及び第1コードを送信する送信手段と、を有し、プログラマブルコントローラは、送信手段によって送信された制御プログラムとしての受信プログラム及び第1コードを受信する受信手段と、受信プログラム及び予めプログラム送信装置と共有されるデータから上記手順で第2コードを生成する第2コード生成手段と、第1コードが第2コードに等しい場合に、受信プログラムを実行する実行手段と、を有する。

発明の効果

[0009] 本開示によれば、プログラマブルコントローラとしてのPLCが外部から取得するプログラムに関する安全性を向上させることができる。

図面の簡単な説明

[0010] [図1]実施の形態1に係る制御システムの構成を示す図

[図2]実施の形態1に係るプログラム送信装置、サーバ及びP L Cのハードウェア構成を示す図

[図3]実施の形態1に係る制御プログラムの伝送について説明するための図

[図4]実施の形態1に係るプログラム送信装置、サーバ及びP L Cの機能的な構成を示す図

[図5]実施の形態1に係るファイル生成処理を示すフローチャート

[図6]実施の形態1に係るアップロード処理を示すフローチャート

[図7]実施の形態1に係るダウンロード処理を示すフローチャート

[図8]比較例に係る制御プログラムの伝送について説明するための図

[図9]比較例に係る制御プログラムの改変について説明するための図

[図10]実施の形態2に係る秘密データについて説明するための図

[図11]実施の形態3に係る秘密データについて説明するための図

[図12]変形例に係るファイルの構成を示す図

発明を実施するための形態

[0011] 以下、本開示の実施の形態に係る制御システム1000について、図面を参照しつつ詳細に説明する。制御システム1000では、P L Cが実行すべきプログラムがサーバ装置に格納される以前に当該プログラムに固有のコードを作成しておき、このように作成されたコードが、P L Cに提供されたプログラムに基づいて作成されるコードと一致するか否かが検証される。

[0012] 実施の形態1.

図1には、本実施の形態に係る制御システム1000の構成例が示されている。制御システム1000は、工場に代表される施設内において構築される。制御システム1000は、例えば、製品の製造ライン、又は、ワークの加工ラインに代表される種々の工程を、機器50を制御することで実現するシステムである。制御システム1000は、図1に示されるように、ユーザU1によって操作されるプログラム送信装置10と、プログラム送信装置10にネットワーク20を介して接続されるサーバ30と、サーバ30にネッ

トワーク２０を介して接続されるＰＬＣ４０と、ＰＬＣによる制御の対象となる機器５０と、を有する。

[0013] ネットワーク２０は、施設内に形成される産業用のフィールドネットワークであってもよいし、ＬＡＮ（Local Area Network）に代表される情報ネットワークであってもよい。プログラム送信装置１０、サーバ３０及びＰＬＣ４０はそれぞれ、ネットワーク２０を介してデータを送受信することにより、他の装置と通信する。

[0014] プログラム送信装置１０は、例えば、ＩＰＣ（Industrial Personal Computer）に代表されるＰＣ、スマートホン、タブレット端末、その他の端末である。ユーザＵ１は、プログラム送信装置１０を操作することにより、ＰＬＣ４０に機器５０を制御させるための制御プログラムを作成し、当該制御プログラムをサーバ３０にアップロードして保存させる。制御プログラムは、例えば、ＰＬＣ４０における実行形式のラダープログラムである。

[0015] なお、プログラム送信装置１０は、既に完成した制御プログラムの提供を他の装置から受けて、ユーザＵ１の操作に従って当該制御プログラムをサーバ３０にアップロードしてもよいし、プログラム送信装置１０において作成された制御プログラムを、他の装置を介してサーバ３０にアップロードしてもよい。また、プログラム送信装置１０は、常にネットワーク２０に接続されていてもよいし、一時的にネットワーク２０に接続されてもよい。

[0016] サーバ３０は、ネットワーク２０上の記憶装置として機能するコンピュータである。サーバ３０は、プログラム送信装置１０からアップロードされた制御プログラムを保持し、ＰＬＣ４０に制御プログラムを提供する。サーバ３０については、通常、ネットワーク２０に接続されている状態が維持される。サーバ３０に保持されている制御プログラムは、ユーザによる誤操作、複数のユーザ間における意思の不統一、及び、第三者による改ざんに代表される要因によって、不適当に変更され得る。

[0017] ＰＬＣ４０は、機器５０を制御するプログラマブルコントローラである。ＰＬＣ４０は、制御プログラムを実行することで機器５０を制御する。なお

、P L C 4 0 は、制御プログラムを実行することにより、不図示の他のP L C 4 0 と協働して機器5 0 を制御してもよい。P L C 4 0 は、常にネットワーク2 0 に接続されていてもよいし、制御プログラムを取得する時に限って一時的にネットワーク2 0 に接続されてもよい。

[0018] 機器5 0 は、センサ、アクチュエータ、モータ、バルブ及びロボットに代表されるF A 機器である。機器5 0 は、信号線を介してP L C 4 0 に接続されて、電圧信号又は電流信号をP L C 4 0 との間で送受信する。例えば、ロボットである機器5 0 は、内蔵のセンサによるセンシング結果をP L C 4 0 に通知し、このセンシング結果に基づいてP L C 4 0 から出力される制御命令に従ってロボットアームを移動させる。なお、図1 には、1 つの機器5 0 が代表的に示されているが、P L C 4 0 に接続される機器5 0 は、2 つ以上であってもよい。

[0019] 図2 には、プログラム送信装置1 0 のハードウェア構成例が示されている。なお、サーバ3 0 及びP L C 4 0 の構成も図2 に示されるものと同様であるから、図中には、プログラム送信装置1 0 、サーバ3 0 、P L C 4 0 それぞれの符号を記載して、合わせて説明する。図2 に示されるように、プログラム送信装置1 0 、サーバ3 0 及びP L C 4 0 はそれぞれ、プロセッサ6 1 と、主記憶部6 2 と、補助記憶部6 3 と、入力部6 4 と、出力部6 5 と、通信部6 6 と、を有する。主記憶部6 2 、補助記憶部6 3 、入力部6 4 、出力部6 5 及び通信部6 6 はいずれも、内部バス6 7 を介してプロセッサ6 1 に接続される。

[0020] プロセッサ6 1 は、集積回路であるM P U (Micro Processing Unit) 又はC P U (Central Processing Unit) を含む。プロセッサ6 1 は、補助記憶部6 3 に記憶されるプログラムP 1 を実行することにより、種々の機能を実現して、後述の処理を実行する。P L C 4 0 のプログラムP 1 は、P L C 4 0 を後述の手段として機能させるためのコントローラプログラムの一例に相当する。

[0021] 主記憶部6 2 は、R A M (Random Access Memory) を含む。主記憶部6 2

には、補助記憶部 6 3 からプログラム P 1 がロードされる。そして、主記憶部 6 2 は、プロセッサ 6 1 の作業領域として用いられる。

[0022] 補助記憶部 6 3 は、EEPROM (Electrically Erasable Programmable Read-Only Memory)、HDD (Hard Disk Drive) 及び脱着可能なメモリーカードに代表される不揮発性メモリを含む。補助記憶部 6 3 は、プログラム P 1 の他に、プロセッサ 6 1 の処理に用いられる種々のデータを記憶する。補助記憶部 6 3 は、プロセッサ 6 1 の指示に従って、プロセッサ 6 1 によって利用されるデータをプロセッサ 6 1 に供給し、プロセッサ 6 1 から供給されたデータを記憶する。なお、図 2 では、1 つのプログラム P 1 が代表的に示されているが、補助記憶部 6 3 は、複数のプログラムを記憶してもよいし、主記憶部 6 2 には、複数のプログラムがロードされてもよい。

[0023] 入力部 6 4 は、入力キー、キーボード、ポインティングデバイス、スイッチ及びボタンに代表される入力デバイスを含む。入力部 6 4 は、ユーザによって入力された情報を取得して、取得した情報をプロセッサ 6 1 に通知する。

[0024] 出力部 6 5 は、LED (Light Emitting Diode)、LCD (Liquid Crystal Display) 及びスピーカに代表される出力デバイスを含む。出力部 6 5 は、プロセッサ 6 1 の指示に従って、種々の情報をユーザに提示する。

[0025] 通信部 6 6 は、外部の装置と通信するためのネットワークインタフェース回路を含む。通信部 6 6 は、外部から信号を受信して、この信号により示されるデータをプロセッサ 6 1 へ出力する。また、通信部 6 6 は、プロセッサ 6 1 から出力されたデータを示す信号を外部の装置へ送信する。

[0026] 続いて、本実施の形態に係る制御プログラムの伝送の概略について、図 3 を参照して説明する。

[0027] 図 3 に示されるように、プログラム送信装置 1 0 は、制御プログラム 7 0 及び秘密データ 8 0 の組み合わせに固有の第 1 コード 7 1 を生成する第 1 コード生成部 1 1 3 を有する。秘密データ 8 0 は、予め定められたデータであって、例えば、2 5 6 ビット又は 1 0 2 4 ビットのランダムなビット列であ

る。第1コード71は、例えば、制御プログラム70及び秘密データ80をこの順に連結した1つのデータを、SHA-2 (Secure Hash Algorithm 2) 及びSHA-3に代表されるハッシュ関数に入力することにより出力値として得られるハッシュ値であってもよいし、他の手法により求められた値であってもよい。

[0028] プログラム送信装置10は、制御プログラム70及び第1コード71を含むファイル73をサーバ30に送信する。サーバ30は、このファイル73を保持して、PLC40からの要求に応じてファイル73をPLC40に提供する。

[0029] PLC40は、取得したファイル73に制御プログラム70として含まれている受信プログラム70a、及び、予めプログラム送信装置10との間で共有する秘密データ80から、これら受信プログラム70a及び秘密データ80の組み合わせに固有の第2コード72を生成する第2コード生成部433を有する。ユーザの意図した通りにファイル73がPLC40に提供される場合においては、ファイル73に含まれる受信プログラム70aは、制御プログラム70と同一のプログラムである。この場合には、第1コード71は、第2コード72に等しい。一方、サーバ30において保持されているファイル73が何らかの要因により改変された場合には、PLC40に提供されたファイル73に含まれる受信プログラム70aは、ユーザの意図から外れて、制御プログラム70とは異なるプログラムとなる。この場合には、第1コード71は、第2コード72とは異なる。また、第2コード生成部433による第2コード72を生成する手法は、プログラム送信装置10の第1コード生成部113による第1コード71を生成する手法と同一である。

[0030] そして、PLC40の照合部434が、ファイル73に含まれる第1コード71と第2コード72とを照合する。両コードが一致する場合には、受信プログラム70aが制御プログラム70に等しいため、PLC40の実行部435が、制御プログラム70である受信プログラム70aを実行する。

[0031] 続いて、プログラム送信装置10、サーバ30及びPLC40の機能的な

構成について、図４を参照して説明する。

- [0032] プログラム送信装置１０は、図４に示されるように、種々の処理を実行する処理部１１と、種々のデータを記憶する記憶部１２と、サーバ３０に情報を送信する送信部１３と、を有する。
- [0033] 処理部１１は、主としてプログラム送信装置１０のプロセッサ６１によって実現される。処理部１１は、制御プログラム７０を取得するプログラム取得部１１１と、秘密データ８０を生成する秘密データ生成部１１２と、第１コード７１を生成する第１コード生成部１１３と、制御プログラム７０と第１コード７１とを含むファイル７３を生成するファイル生成部１１４と、を有する。
- [0034] プログラム取得部１１１は、ユーザＵ１が入力部６４を操作して入力した制御プログラム７０を取得する。なお、プログラム取得部１１１は、ユーザＵ１から指定された補助記憶部６３のアドレス又は外部装置のアドレスから制御プログラム７０を読み出すことで、制御プログラム７０を取得してもよい。プログラム取得部１１１は、取得した制御プログラム７０を記憶部１２に格納する。プログラム取得部１１１は、プログラム送信装置１０において、制御プログラム７０を取得するプログラム取得手段の一例に相当する。
- [0035] 秘密データ生成部１１２は、例えば、プログラム取得部１１１が制御プログラム７０を取得した時刻、又は、ユーザから秘密データ８０の生成を指示された時刻をシード値として、秘密データ８０を生成して記憶部１２に格納する。
- [0036] 第１コード生成部１１３は、記憶部１２から制御プログラム７０及び秘密データ８０を読み出して、制御プログラム７０及び秘密データ８０に基づいて第１コード７１を生成して記憶部１２に格納する。詳細には、第１コード生成部１１３は、秘密データ８０及び制御プログラム７０のハッシュ値を第１コード７１として生成する。第１コード生成部１１３は、プログラム送信装置１０において、制御プログラム７０からの変更の有無を検証するための第１コード７１を、制御プログラム７０及び予め定められたデータから予め

定められた手順で生成する第１コード生成手段の一例に相当する。

[0037] ファイル生成部１１４は、記憶部１２から制御プログラム７０及び第１コード７１を読み出して、制御プログラム７０及び第１コード７１を圧縮及び暗号化してファイル７３を生成する。圧縮及び暗号化の方式は任意であるが、計算リソースが不十分であるＰＬＣ４０においても展開及び復号を可能とするため、展開及び復号時の計算負荷が低い方式であることが望ましい。なお、ファイル生成部１１４は、制御プログラム７０及び第１コード７１を圧縮することなくファイル７３を生成してもよいし、暗号化することなくファイル７３を生成してもよい。ファイル生成部１１４は、プログラム送信装置１０において、制御プログラム７０及び第１コード７１を暗号化する暗号化手段の一例に相当する。

[0038] 記憶部１２は、主として、プログラム送信装置１０の主記憶部６２及び補助記憶部６３の少なくとも一方によって実現される。記憶部１２には、ユーザＵ１によってサーバ識別情報１２１が予め格納される。サーバ識別情報１２１は、例えば、サーバ３０のネットワーク２０上の所在を表すＩＰ（Internet Protocol）アドレス又は局番である。

[0039] 送信部１３は、主としてプログラム送信装置１０のプロセッサ６１及び通信部６６の協働により実現される。送信部１３は、ユーザＵ１の操作に従って、記憶部１２からサーバ識別情報１２１及びファイル７３を読み出して、サーバ識別情報１２１により示されるサーバ３０にファイル７３を送信する。送信部１３は、プログラム送信装置１０において、制御プログラム７０及び第１コード７１を送信する送信手段の一例に相当し、暗号化手段によって暗号化された制御プログラム７０及び第１コード７１を送信する送信手段の一例に相当する。

[0040] サーバ３０は、プログラム送信装置１０からファイル７３を受信する受信部３１と、ファイル７３を記憶する記憶部３２と、ファイル７３をＰＬＣ４０に送信する送信部３３と、を有する。受信部３１及び送信部３３はそれぞれ、主としてサーバ３０の通信部６６によって実現される。記憶部３２は、

主としてサーバ30の主記憶部62及び補助記憶部63の少なくとも一方によって実現される。

[0041] 受信部31は、プログラム送信装置10の送信部13によって送信されたファイル73を受信して、当該ファイル73を記憶部32に格納する。

[0042] 送信部33は、PLC40からの要求に対して、制御プログラム70を記憶部32から読み出してPLC40に送信することでPLC40に応答する。サーバ30は、制御システム1000において、プログラム送信装置10の送信手段によって送信された制御プログラム70及び第1コード71を受信し、受信した制御プログラム70としての受信プログラム70a及び第1コード71をプログラマブルコントローラに送信するサーバの一例に相当する。

[0043] PLC40は、サーバ30からファイル73を受信する受信部41と、種々のデータを記憶する記憶部42と、種々の処理を実行する処理部43と、実行すべき制御プログラム70が格納されるプログラムメモリ44と、を有する。

[0044] 受信部41は、主としてPLC40の通信部66によって実現される。受信部41は、処理部43の要求部431の指示に従って、サーバ30に対してファイル73の送信を要求し、当該要求に対する応答としてサーバ30から送信されるファイル73を受信して記憶部42に格納する。受信部41は、PLC40において、プログラム送信装置10の送信手段によって送信された制御プログラムとしての受信プログラム70a及び第1コード71を受信する受信手段の一例に相当し、暗号化された受信プログラム70a及び第1コード71を受信する受信手段の一例に相当する。

[0045] 記憶部42は、主としてPLC40の主記憶部62及び補助記憶部63の少なくとも一方によって実現される。記憶部42には、制御プログラム70の取得先を示すプログラム取得先情報421と、プログラム送信装置10に記憶される秘密データ80と同一の秘密データ80と、が予め格納される。

[0046] プログラム取得先情報421は、ネットワーク20におけるサーバ30の

所在を示すサーバ識別情報 4 2 2 と、サーバ 3 0 に記憶されるファイル 7 3 を識別するためのファイル識別情報 4 2 3 と、を含む。サーバ識別情報 4 2 2 は、例えば、サーバ 3 0 の I P アドレス又は局番である。ファイル識別情報 4 2 3 は、例えば、ファイル名又はサーバ 3 0 の記憶部 3 2 に格納されるファイル 7 3 のアドレスである。プログラム取得先情報 4 2 1 は、処理部 4 3 の要求部 4 3 1 によって記憶部 4 2 から読み出されて、受信部 4 1 が、サーバ 3 0 の送信すべきファイル 7 3 をサーバ 3 0 に対して指定するために用いられる。

[0047] 秘密データ 8 0 は、任意の手法により、プログラム送信装置 1 0 と P L C 4 0 との間で共有され、サーバ 3 0 には提供されない。例えば、ユーザ U 1 がプログラム送信装置 1 0 を操作して、メモリーカードに代表される記録媒体に秘密データ 8 0 を格納して、当該記録媒体を P L C 4 0 のカードスロットに挿入することで秘密データ 8 0 を P L C 4 0 の記憶部 4 2 に格納してもよい。また、ユーザ U 1 が、U S B (Universal Serial Bus) に代表される通信線で、ネットワーク 2 0 を介することなくプログラム送信装置 1 0 を P L C 4 0 に接続して、秘密データ 8 0 を P L C 4 0 に転送してもよい。また、サーバ 3 0 を介することなく、或いはサーバ 3 0 を介して、ネットワーク 2 0 を経由してプログラム送信装置 1 0 から P L C 4 0 に秘密データ 8 0 が伝送されてもよい。ネットワーク 2 0 を経由して秘密データ 8 0 が伝送される場合には、セキュアな通信を確立した上で秘密データ 8 0 を伝送することが望ましい。この場合には、プログラム送信装置 1 0 の送信部 1 3 が、秘密データ 8 0 を送信し、受信部 4 1 が秘密データ 8 0 を受信する。

[0048] 処理部 4 3 は、主として P L C 4 0 のプロセッサ 6 1 によって実現される。処理部 4 3 は、サーバ 3 0 に対してファイル 7 3 を要求する要求部 4 3 1 と、受信したファイル 7 3 から受信プログラム 7 0 a 及び第 1 コード 7 1 を抽出する抽出部 4 3 2 と、抽出部 4 3 2 によって抽出された受信プログラム 7 0 a に基づいて第 2 コード 7 2 を生成する第 2 コード生成部 4 3 3 と、第 1 コード 7 1 及び第 2 コード 7 2 を照合する照合部 4 3 4 と、両コードがー

致した場合に制御プログラム 70 を実行する実行部 435 と、を有する。

[0049] 要求部 431 は、PLC 40 の起動時に、記憶部 42 からプログラム取得先情報 421 を読み出して、サーバ識別情報 422 により示されるサーバ 30 に対して、ファイル識別情報 423 により示されるファイル 73 の提供を、受信部 41 に要求させる。

[0050] 抽出部 432 は、受信部 41 によって受信されて記憶部 42 に格納されたファイル 73 を読み出して、展開及び復号することにより、ファイル 73 から受信プログラム 70a 及び第 1 コード 71 を抽出する。抽出部 432 は、PLC 40 において、暗号化された受信プログラム 70a 及び第 1 コード 71 を復号する復号手段の一例に相当する。

[0051] 第 2 コード生成部 433 は、抽出部 432 によって抽出された受信プログラム 70a と、記憶部 42 から読み出した秘密データ 80 とから、プログラム送信装置 10 の第 1 コード生成部 113 と同一の手法により第 2 コード 72 を生成する。詳細には、第 2 コード生成部 433 は、秘密データ 80 及び受信プログラム 70a のハッシュ値を第 2 コード 72 として生成する。より詳細には、第 2 コード生成部 433 は、第 1 コード生成部 113 と同様のハッシュ関数を施すアプリケーションソフトウェアに、受信プログラム 70a 及び秘密データ 80 を入力することにより出力されるハッシュ値として、第 2 コード 72 を得る。第 2 コード生成部 433 は、PLC 40 において、受信プログラム及び予めプログラム送信装置と共有されるデータから予め定められた手順で第 2 コード 72 を生成する第 2 コード生成手段の一例に相当する。

[0052] 照合部 434 は、抽出部 432 によって抽出された第 1 コード 71 と、第 2 コード生成部 433 によって生成された第 2 コード 72 と、を照合する。そして、照合部 434 は、2 つのコードが一致する場合には、抽出部 432 によって抽出された受信プログラム 70a である制御プログラム 70 を、プログラムメモリ 44 に格納する。

[0053] 実行部 435 は、プログラムメモリ 44 から制御プログラム 70 を読み出

して実行することにより、機器50を制御する。実行部435が制御プログラム70を実行するタイミングは、PLC40の起動時であってもよいし、PLC40に配設された実行ボタンの押下、或いはRUNスイッチがオン状態に移行されたときであってもよい。実行部435は、PLC40において、第1コード71が第2コード72に等しい場合に、受信プログラムを実行する実行手段の一例に相当する。

[0054] プログラムメモリ44は、主として、PLC40の主記憶部62及び補助記憶部63の少なくとも一方によって実現される。

[0055] 続いて、制御システム1000において実行される処理について、図5～7を用いて説明する。なお、図5～7に示されるフローチャートは一例であり、各ステップの実行順序を任意に変更してもよい。

[0056] 図5には、プログラム送信装置10がファイル73を生成するファイル生成処理の流れが示されている。図5に示されるように、ファイル生成処理において、プログラム送信装置10は、秘密データ80を生成して、生成した秘密データ80をPLC40と共有する（ステップS11）。具体的には、秘密データ生成部112が、メッセージ認証符号における鍵としての秘密データ80を生成して、上述した任意の手法によりPLC40と秘密データ80を共有する。

[0057] 次に、プログラム送信装置10が、制御プログラム70を取得する（ステップS12）。具体的には、プログラム取得部111が、ユーザU1によって入力されたソースコード又はユーザU1から指定されたアドレスから読み出したソースコードを実行形式に変換することにより制御プログラム70を取得してもよいし、既に実行形式への変換が完了した制御プログラム70をユーザから指定されたアドレスから読み出すことで制御プログラム70を取得してもよい。

[0058] 次に、プログラム送信装置10が、ステップS11で生成した秘密データ80、及び、ステップS12で取得した制御プログラム70を用いて第1コード71を生成する（ステップS13）。具体的には、第1コード生成部1

１３が、秘密データ８０を鍵とし、制御プログラム７０をメッセージとして、メッセージ認証符号に相当する第１コード７１を算出する。

[0059] 次に、プログラム送信装置１０のファイル生成部１１４が、ステップＳ１２で取得した制御プログラム７０及びステップＳ１３で生成した第１コード７１を含むファイル７３を生成し、生成したファイル７３を圧縮及び暗号化した上で記憶部１２に格納する（ステップＳ１４）。その後、ファイル生成処理が終了する。

[0060] 図６には、生成されたファイル７３をサーバ３０にアップロードするアップロード処理の流れが示されている。図６に示されるように、アップロード処理においては、プログラム送信装置１０が、サーバ識別情報１２１に基づいてファイル７３を保存すべきサーバ３０を特定する（ステップＳ２１）。具体的には、送信部１３が、サーバ３０のネットワークアドレスを特定する。

[0061] 次に、送信部１３は、ステップＳ２１で特定したサーバ３０が存在するかどうかを判定する（ステップＳ２２）。具体的には、送信部１３は、ステップＳ２１で特定したネットワークアドレスを有する装置と通信を確立することができるか否かを判定する。サーバ３０と通信を確立することができず、サーバ３０からの応答を得ることができない場合には、ステップＳ２２の判定が否定される。

[0062] サーバ３０が存在しないと判定された場合（ステップＳ２２；Ｎｏ）、プログラム送信装置１０は、アップロード処理を異常終了させる（ステップＳ２３）。一方、サーバ３０が存在すると判定された場合（ステップＳ２２；Ｙｅｓ）、プログラム送信装置１０がファイル７３を記憶部１２から読み出してサーバ３０に送信する（ステップＳ２４）。サーバ３０は、このファイル７３を受信して記憶部３２に格納し（ステップＳ２５）、アップロード処理が完了する。

[0063] 図７には、サーバ３０に保存されたファイル７３をＰＬＣ４０にダウンロードするダウンロード処理の流れが示されている。図７に示されるように、

ダウンロード処理では、P L C 4 0の管理者によってP L C 4 0の電源ボタンが押下されることでP L C 4 0が起動する（ステップS 3 1）。

[0064] 次に、P L C 4 0が、取得先情報に基づいてサーバ3 0及びファイル7 3を特定する（ステップS 3 2）。具体的には、P L C 4 0の要求部4 3 1が、プログラム取得先情報4 2 1に含まれるサーバ識別情報4 2 2及びファイル識別情報4 2 3を記憶部4 2から読み出す。

[0065] 次に、P L C 4 0が、ステップS 3 2で特定したサーバ3 0に対して、ステップS 3 2で特定したファイル7 3の送信を要求する（ステップS 3 3）。例えば、ステップS 3 2において「1 9 2. 1 6 8. 2 0. 1 0 0」というI Pアドレスがサーバ識別情報4 2 2として特定され、「C T R L _ P R O G R A M 4 0」というファイル名がファイル識別情報4 2 3として特定された場合には、受信部4 1が、要求部4 3 1の指示に従って、上記I Pアドレスに対して上記ファイル名が付されたファイル7 3の送信を要求するためのパケットを送信する。

[0066] 次に、P L C 4 0は、ステップS 3 3における要求の送信先であるサーバ3 0から応答があるかを判定する（ステップS 3 4）。具体的には、受信部4 1が、ステップS 3 3で送信したパケットに対する応答が、ステップS 3 3でパケットを送信してから一定時間内にあるか否かを判定する。

[0067] サーバ3 0から応答がないと判定された場合（ステップS 3 4 ; N o）、P L C 4 0は、異常が発生したと判断して（ステップS 3 5）、ダウンロード処理を終了する。サーバ3 0から応答がない場合としては、ステップS 3 2で特定したサーバ3 0がネットワーク2 0上に存在しない場合、及び、ステップS 3 2で特定したファイル7 3がサーバ3 0内に保存されていない場合が考えられる。ステップS 3 5において、P L C 4 0は、出力部6 5から異常の発生を管理者に対して報知してもよい。

[0068] 一方、サーバから応答があると判定された場合（ステップS 3 4 ; Y e s）、サーバ3 0が、ステップS 3 3の要求に対して、P L C 4 0にファイル7 3を送信する（ステップS 3 6）。具体的には、サーバ3 0の送信部3 3

が、ステップS 3 3の要求においてP L C 4 0から指定されたファイル名を有するファイル7 3を記憶部3 2から読み出して、P L C 4 0に送信する。

[0069] 次に、P L C 4 0の受信部4 1が、ファイル7 3を受信して記憶部4 2に格納し（ステップS 3 7）、抽出部4 3 2が、ファイル7 3を展開及び復号して、受信プログラム7 0 a及び第1コード7 1を抽出する（ステップS 3 8）。

[0070] 次に、P L C 4 0の第2コード生成部4 3 3が、P L C 4 0の記憶部4 2が記憶する秘密データ8 0、及び、ステップS 3 8で抽出された受信プログラム7 0 aから第2コード7 2を生成する（ステップS 3 9）。具体的には、第2コード生成部4 3 3が、秘密データ8 0を鍵とし、受信プログラム7 0 aをメッセージとして、メッセージ認証符号に相当する第2コード7 2を算出する。

[0071] 次に、P L C 4 0の照合部4 3 4が、ステップS 3 8で抽出された第1コード7 1と、ステップS 3 9で生成された第2コード7 2とを照合して、2つのコードが一致するか否かを判定する（ステップS 4 0）。具体的には、照合部4 3 4が、第1コード7 1と第2コード7 2とを比較して、これらのコードが同一のビット列であるか否かを判定する。

[0072] 2つのコードが一致しないと判定された場合（ステップS 4 0 ; N o）、P L C 4 0は、受信した受信プログラム7 0 aを実行することなく破棄して（ステップS 4 1）、ステップS 3 5に処理を移行する。一方、2つのコードが一致すると判定された場合（ステップS 4 0 ; Y e s）、照合部4 3 4は、受信プログラム7 0 aについて制御プログラム7 0からの欠損及び改ざんが無いと判断して、プログラムメモリ4 4に制御プログラム7 0を書き込む（ステップS 4 2）。

[0073] 次に、P L C 4 0の実行部4 3 5は、制御プログラム7 0の実行指示があるか否かを判定する（ステップS 4 3）。実行指示がないと判定した場合（ステップS 4 3 ; N o）、実行部4 3 5は、ステップS 4 3の判定を繰り返して、実行指示を受けるまで待機する。一方、実行指示があると判定した場

合（ステップS 4 3 ; Y e s）、実行部4 3 5は、プログラムメモリ4 4から制御プログラム7 0を読み出して実行する（ステップS 4 4）。これにより、P L C 4 0は、プログラム送信装置1 0から提供された制御プログラム7 0に従って機器5 0を制御することとなる。

[0074] 以上、説明したように、プログラム送信装置1 0の第1コード生成部1 1 3が、制御プログラム7 0及び秘密データ8 0から第1コード7 1を生成する。また、P L C 4 0の受信部4 1は、P L C 4 0の起動時に受信プログラム7 0 aを受信し、第2コード生成部4 3 3は、受信プログラム7 0 a及び秘密データ8 0から第2コード7 2を生成し、実行部4 3 5は、第1コード7 1が第2コード7 2に等しい場合に、受信プログラム7 0 aを実行する。このため、サーバ3 0から受信された受信プログラム7 0 aは、プログラム送信装置1 0から送信された制御プログラム7 0に等しい場合において実行される。したがって、プログラマブルコントローラとしてのP L C 4 0が外部から取得するプログラムに関する安全性を向上させることができる。

[0075] 図8には、比較例に係る制御プログラム7 0の伝送について模式的に示されている。この比較例では、コードの比較によるプログラムの改変が検証されることなく、制御プログラム7 0がそのままプログラム送信装置1 0からサーバ3 0にアップロードされてP L C 4 0に提供される。

[0076] しかしながら、このような比較例において、図9に示されるように、悪意のあるユーザの端末1 0 bから、制御プログラム7 0から改ざんされた改ざんプログラム7 0 bがアップロードされて、制御プログラム7 0と置き換えられるケースが考えられる。このようなケースにおいては、P L C 4 0は、その起動時に、サーバ3 0から制御プログラム7 0として改ざんプログラム7 0 bを取得し、当該改ざんプログラム7 0 bを実行してしまう。

[0077] これに対して本実施の形態に係る制御システム1 0 0 0は、制御プログラム7 0と秘密データ8 0との組み合わせによってユニークに生成されるコードを制御プログラム7 0と一組にしてサーバ3 0に格納して管理する。このため、P L C 4 0が制御プログラム7 0としての受信プログラム7 0 aを取

得した際に、第1コード71及び第2コード72を用いて制御プログラム70からの改変の有無を検証することができる。そして、第1コード71が第2コード72とは異なる場合には、PLC40の実行部435は、受信プログラム70aをプログラムメモリ44に書き込まずに、当該受信プログラム70aを実行することなく破棄する。これにより、PLC40が、ネットワーク通信によってサーバ30から実行すべきプログラムを取得するネットブート機能を有する場合において、当該PLC40に対する意図しない受信プログラム70aの書き込みを防ぎ、より安全なプログラム更新を実現することができる。

[0078] また、制御システム1000においては、サーバ30に記憶されているプログラムの改変を検知するために、プログラム送信装置10とPLC40との間におけるメッセージ認証符号に相当する第1コード71が用いられる。このような第1コード71を用いる手法の計算負荷は、伝送されるデータの改変を検知することが可能なデジタル署名を用いる場合の計算負荷よりも小さい。このため、PLC40の起動時におけるブート時間を短縮して、制御システム1000における生産効率の低下を回避することができる。

[0079] また、制御システム1000においては、プログラム送信装置10のファイル生成部114が暗号化されたファイル73を生成して、PLC40の抽出部432がファイル73を復号する。これにより、サーバ30には、暗号化されたファイル73が格納され、データの漏洩に代表されるリスクに対して安全性を向上させることができる。

[0080] 実施の形態2.

続いて、実施の形態2について、上述の実施の形態1との相違点を中心に説明する。なお、上記実施の形態1と同一又は同等の構成については、同等の符号を用いる。本実施の形態は、プログラム送信装置10を使用する複数のユーザで異なる秘密データ80が用いられる点で、実施の形態1とは異なる。

[0081] 図10に示されるように、本実施の形態に係るプログラム送信装置10は

、複数の秘密データ 80 を生成する。詳細には、プログラム送信装置 10 は、プログラム送信装置 10 を使用するユーザ U1 に対応する秘密データ 81 と、プログラム送信装置 10 を使用するユーザ U2 に対応する秘密データ 82 と、を秘密データ 80 として予め生成する。そして、プログラム送信装置 10 の第 1 コード生成部 113 は、ユーザ U1, U2 のうちの制御プログラム 70 を提供したユーザの秘密データ 80 を用いて、第 1 コード 71 を生成する。図 10 の例では、ユーザ U1 に対応する秘密データ 81 を用いて第 1 コード 71 が生成されている。

[0082] PLC40 は、秘密データ 81, 82 のうちの、予め特定されたデータである秘密データ 81 のみを記憶し、秘密データ 82 を記憶しない。そして、PLC40 は、秘密データ 81 を用いて第 2 コード 72 を生成する。受信プログラム 70a が制御プログラム 70 に等しく、かつ、当該制御プログラム 70 がユーザ U1 によって提供された場合には、この制御プログラム 70 が PLC40 によって実行される。受信プログラム 70a が制御プログラム 70 に等しい場合であっても、当該制御プログラム 70 がユーザ U2 によって提供されたときには、第 1 コード 71 と第 2 コード 72 とが異なるため、PLC40 は、制御プログラム 70 を実行することなく破棄する。

[0083] 以上、説明したように、プログラム送信装置 10 のプログラム取得部 111 は、複数のユーザのうちのいずれかから提供される制御プログラム 70 を取得し、第 1 コード生成部 113 は、制御プログラム 70 及び制御プログラム 70 を提供したユーザに対応する秘密データ 80 から第 1 コード 71 を生成する。また、PLC40 の第 2 コード生成部 433 は、受信プログラム 70a 及び複数のユーザのうちの特定のユーザに対応する秘密データ 80 から第 2 コード 72 を生成する。これにより、ユーザごとに制御プログラム 70 の実行の可否を管理することが可能になる。

[0084] なお、第 1 コード生成部 113 が、制御プログラム 70 を提供したユーザの秘密データ 80 を用いて第 1 コード 71 を生成する例について説明したが、これには限定されない。例えば、第 1 コード生成部 113 は、制御プログ

ラム 7 0 の送信指示を入力したユーザの秘密データ 8 0 を用いて第 1 コード 7 1 を生成してもよい。これにより、複数のユーザが 1 つの制御プログラム 7 0 を協同して編集する場合において、P L C 4 0 への送信権限を有するユーザによってサーバ 3 0 にアップロードされたときに P L C 4 0 に当該制御プログラム 7 0 を実行させ、送信権限を有しないユーザによってアップロードされたときに当該制御プログラム 7 0 の実行を回避することができる。第 1 コード生成部 1 1 3 は、複数のユーザのうちの、制御プログラム 7 0 を使用する一のユーザに対応する秘密データ 8 0 から第 1 コード 7 1 を生成すればよい。

[0085] 実施の形態 3.

続いて、実施の形態 3 について、上述の実施の形態 1 との相違点を中心に説明する。なお、上記実施の形態 1 と同一又は同等の構成については、同等の符号を用いる。本実施の形態は、複数のプログラム送信装置それぞれで異なる秘密データ 8 0 が使用される点で、実施の形態 1 とは異なる。

[0086] 図 1 1 に示されるように、本実施の形態に係る制御システム 1 0 0 0 は、複数のプログラム送信装置 1 0, 1 0 a を有し、プログラム送信装置 1 0, 1 0 a はそれぞれ、異なる秘密データ 8 0 を生成する。詳細には、プログラム送信装置 1 0 は、秘密データ 8 3 を生成し、プログラム送信装置 1 0 a は、秘密データ 8 3 とは異なる秘密データ 8 4 を生成する。そして、プログラム送信装置 1 0, 1 0 a の第 1 コード生成部 1 1 3 は、第 1 コード生成部 1 1 3 を有するプログラム送信装置の秘密データ 8 0 を用いて、第 1 コード 7 1 を生成する。図 1 1 の例では、プログラム送信装置 1 0 において秘密データ 8 3 を用いて第 1 コード 7 1 が生成されている。

[0087] P L C 4 0 は、秘密データ 8 3, 8 4 のうちの、予め特定されたデータである秘密データ 8 3 のみを記憶し、秘密データ 8 4 を記憶しない。そして、P L C 4 0 は、秘密データ 8 3 を用いて第 2 コード 7 2 を生成する。受信プログラム 7 0 a が制御プログラム 7 0 に等しく、かつ、当該制御プログラム 7 0 がプログラム送信装置 1 0 から提供された場合には、この制御プログラ

ム 7 0 が P L C 4 0 によって実行される。受信プログラム 7 0 a が制御プログラム 7 0 に等しい場合であっても、当該制御プログラム 7 0 がプログラム送信装置 1 0 a から提供されたときには、第 1 コード 7 1 と第 2 コード 7 2 とが異なるため、P L C 4 0 は、制御プログラム 7 0 を実行することなく破棄する。

[0088] 以上、説明したように、複数のプログラム送信装置 1 0, 1 0 a の第 1 コード生成部 1 1 3 はそれぞれ、制御プログラム 7 0 及び第 1 コード生成部 1 1 3 を有するプログラム送信装置に対応する秘密データ 8 0 から第 1 コード 7 1 を生成する。また、P L C 4 0 の第 2 コード生成部 4 3 3 は、受信プログラム 7 0 a 及び複数のプログラム送信装置 1 0, 1 0 a のうち特定のプログラム送信装置と予め共有される秘密データ 8 0 から第 2 コード 7 2 を生成する。これにより、プログラム送信装置ごとに制御プログラム 7 0 の実行の可否を管理することが可能になる。

[0089] なお、上記実施の形態 2 においてユーザが 2 人である例を説明したが、プログラム送信装置 1 0 を使用するユーザの数は 3 人以上であってもよい。また、上記実施の形態 3 においてプログラム送信装置が 2 つである例を説明したが、プログラム送信装置の数は 3 つ以上であってもよい。

[0090] また、P L C 4 0 が 1 つの秘密データ 8 0 を記憶する例を説明したが、P L C 4 0 は、特定の複数の秘密データ 8 0 を記憶して、それぞれの秘密データ 8 0 を用いて生成した第 2 コード 7 2 と第 1 コード 7 1 との照合を繰り返して、いずれかの第 2 コード 7 2 が第 1 コード 7 1 に等しいときに、受信プログラム 7 0 a を制御プログラム 7 0 としてプログラムメモリ 4 4 に格納してもよい。

[0091] また、上記実施の形態 2, 3 において、P L C 4 0 は、サーバ 3 0 を介して制御プログラム 7 0 を P L C 4 0 に書き込む権限のないユーザ又はプログラム送信装置に対応する秘密データ 8 0 を合わせて記憶していてもよい。P L C 4 0 は、当該権限のないユーザ又はプログラム送信装置に対応する秘密データ 8 0 を、照合部 4 3 4 による照合の対象から除外すればよい。

[0092] 以上、本開示の実施の形態について説明したが、本開示は上記実施の形態によって限定されるものではない。

[0093] 例えば、上記実施の形態では、制御システム 1000 を構成するプログラム送信装置 10、サーバ 30 及び PLC 40 のすべてが施設内に配置されるケースが想定されたが、これには限定されない。例えば、プログラム送信装置 10、サーバ 30 が、インターネットに代表される広域通信網であるネットワーク 20 を介して施設内の PLC 40 に接続されてもよい。

[0094] また、プログラム送信装置 10、サーバ 30 及び PLC 40 は、単一のネットワーク 20 を介して接続されていなくともよい。例えば、プログラム送信装置 10 及びサーバ 30 は、LAN に代表される情報ネットワークを介して互いに接続され、サーバ 30 及び PLC 40 は、産業用ネットワークを介して互いに接続されてもよい。また、プログラム送信装置 10 とサーバ 30 とを接続する伝送路と、サーバ 30 と PLC 40 とを接続する伝送路と、の一方又は双方を、ネットワークに代えて専用線で実現してもよい。

[0095] また、制御プログラム 70 について 1 つの第 1 コード 71 を生成する例について説明したが、これには限定されない。例えば、図 12 に示されるように、プログラム送信装置 10 は、制御プログラム 70 を構成するモジュール 701、702...70n それぞれについて、秘密データ 80 を用いて第 1 コード 711、712...71n を生成してもよい。そして、プログラム送信装置 10 は、制御プログラム 70 と、生成した複数の第 1 コード 711、712...71n を含むファイル 73 を生成してもよい。図 12 に示される例においては、PLC 40 は、個々のモジュールについて、上記実施の形態と同様に第 2 コード 72 を生成し、2 つのコードを比較すればよい。

[0096] また、プログラム送信装置 10 が秘密データ 80 を生成する例について説明したが、これには限定されない。PLC 40 によって生成された秘密データ 80 をプログラム送信装置 10 が PLC 40 と共有してもよいし、他の装置によって生成された秘密データ 80 を、プログラム送信装置 10 及び PLC 40 に共有させてもよい。

- [0097] また、プログラム送信装置 10 とサーバ 30 とが別個に構成される例について説明したが、これには限定されない。例えば、端末であるプログラム送信装置 10 が、サーバ 30 の機能を有することにより、プログラム送信装置 10 とサーバ 30 とが一体的に構成されてもよい。また、上述の制御システム 1000 からサーバ 30 を省略して、端末又はサーバ装置であるプログラム送信装置 10 が、制御プログラム 70 を PLC 40 に直接送信してもよい。サーバ 30 が省略される場合においても、制御プログラム 70 が伝送される際の改変を検知することにより、PLC 40 が外部から取得するプログラムに関する安全性を向上させることができる。
- [0098] また、プログラム送信装置 10、サーバ 30 及び PLC 40 の機能は、専用のハードウェアによっても、また、通常のコンピュータシステムによっても実現することができる。
- [0099] 例えば、プロセッサ 61 によって実行されるプログラム P1 を、コンピュータ読み取り可能な非一時的な記録媒体に格納して配布し、そのプログラム P1 をコンピュータにインストールすることにより、上述の処理を実行する装置を構成することができる。このような記録媒体としては、例えばフレキシブルディスク、CD-ROM (Compact Disc Read-Only Memory)、DVD (Digital Versatile Disc)、MO (Magneto-Optical Disc) が考えられる。
- [0100] また、プログラム P1 をインターネットに代表される通信ネットワーク上のサーバ装置が有するディスク装置に格納しておき、例えば、搬送波に重畳させて、コンピュータにダウンロードするようにしてもよい。
- [0101] また、通信ネットワークを介してプログラム P1 を転送しながら起動実行することによっても、上述の処理を達成することができる。
- [0102] さらに、プログラム P1 の全部又は一部をサーバ装置上で実行させ、その処理に関する情報をコンピュータが通信ネットワークを介して送受信しながらプログラムを実行することによっても、上述の処理を達成することができる。

[0103] なお、上述の機能を、OS (Operating System) が分担して実現する場合又はOSとアプリケーションとの協働により実現する場合には、OS以外の部分のみを媒体に格納して配布してもよく、また、コンピュータにダウンロードしてもよい。

[0104] また、プログラム送信装置10、サーバ30及びPLC40の機能を実現する手段は、ソフトウェアに限られず、その一部又は全部を、回路を含む専用のハードウェアによって実現してもよい。

[0105] 本開示は、本開示の広義の精神と範囲を逸脱することなく、様々な実施の形態及び変形が可能とされるものである。また、上述した実施の形態は、本開示を説明するためのものであり、本開示の範囲を限定するものではない。つまり、本開示の範囲は、実施の形態ではなく、請求の範囲によって示される。そして、請求の範囲内及びそれと同等の開示の意義の範囲内で施される様々な変形が、本開示の範囲内とみなされる。

産業上の利用可能性

[0106] 本開示は、実行すべきプログラムを外部から取得するプログラマブルコントローラを有するシステムに適している。

符号の説明

[0107] 1000 制御システム、 10、 10a プログラム送信装置、 10b 端末、 11 処理部、 111 プログラム取得部、 112 秘密データ生成部、 113 第1コード生成部、 114 ファイル生成部、 12 記憶部、 121 サーバ識別情報、 13 送信部、 20 ネットワーク、 30 サーバ、 31 受信部、 32 記憶部、 33 送信部、 40 PLC、 41 受信部、 42 記憶部、 421 プログラム取得先情報、 422 サーバ識別情報、 423 ファイル識別情報、 43 処理部、 431 要求部、 432 抽出部、 433 第2コード生成部、 434 照合部、 435 実行部 44 プログラムメモリ、 50 機器、 61 プロセッサ、 62 主記憶部、 63 補助記憶部、 64 入力部、 65 出力部、 66 通信部、 67

内部バス、 70 制御プログラム、 70a 受信プログラム、 70b
プログラム、 701, 702, 70n モジュール、 71, 711,
712, 71n 第1コード、 72 第2コード、 73 ファイル、
80~84 秘密データ、 P1 プログラム、 U1, U2 ユーザ。

請求の範囲

- [請求項1] 機器を制御するプログラマブルコントローラと、前記プログラマブルコントローラに前記機器を制御させるための制御プログラムを送信するプログラム送信装置と、を備える制御システムであって、
- 前記プログラム送信装置は、
- 前記制御プログラムを取得するプログラム取得手段と、
- 前記制御プログラムからの変更の有無を検証するための第1コードを、前記制御プログラム及び予め定められたデータから予め定められた手順で生成する第1コード生成手段と、
- 前記制御プログラム及び前記第1コードを送信する送信手段と、を有し、
- 前記プログラマブルコントローラは、
- 前記送信手段によって送信された前記制御プログラムとしての受信プログラム及び前記第1コードを受信する受信手段と、
- 前記受信プログラム及び予め前記プログラム送信装置と共有される前記データから前記手順で第2コードを生成する第2コード生成手段と、
- 前記第1コードが前記第2コードに等しい場合に、前記受信プログラムを実行する実行手段と、を有する、
- 制御システム。
- [請求項2] 前記実行手段は、前記第1コードが前記第2コードとは異なる場合に、前記受信プログラムを実行することなく破棄する、
- 請求項1に記載の制御システム。
- [請求項3] 前記第1コード生成手段は、前記データ及び前記制御プログラムのハッシュ値を前記第1コードとして生成し、
- 前記第2コード生成手段は、前記データ及び前記受信プログラムのハッシュ値を前記第2コードとして生成する、
- 請求項1又は2に記載の制御システム。

[請求項4] 前記プログラム送信装置の前記第1コード生成手段は、前記制御プログラム及び複数のユーザのうちの前記制御プログラムを使用する一のユーザに対応する前記データから前記第1コードを生成し、

前記プログラマブルコントローラの前記第2コード生成手段は、前記受信プログラム、及び、予め前記プログラム送信装置と共有される前記データであって、前記複数のユーザのうちの特定のユーザに対応する前記データから前記第2コードを生成する、

請求項1から3のいずれか一項に記載の制御システム。

[請求項5] 前記プログラマブルコントローラと、複数の前記プログラム送信装置と、を備える制御システムであって、

複数の前記プログラム送信装置の前記第1コード生成手段はそれぞれ、前記制御プログラム及び該第1コード生成手段を有する前記プログラム送信装置に対応する前記データから前記第1コードを生成し、

前記プログラマブルコントローラの前記第2コード生成手段は、前記受信プログラム及び複数の前記プログラム送信装置のうちの特定の前記プログラム送信装置と予め共有される前記データから前記第2コードを生成する、

請求項1から4のいずれか一項に記載の制御システム。

[請求項6] 前記プログラム送信装置は、前記制御プログラム及び前記第1コードを暗号化する暗号化手段、をさらに有し、

前記送信手段は、前記暗号化手段によって暗号化された前記制御プログラム及び前記第1コードを送信し、

前記受信手段は、暗号化された前記受信プログラム及び前記第1コードを受信し、

前記プログラマブルコントローラは、暗号化された前記受信プログラム及び前記第1コードを復号する復号手段、をさらに有する、

請求項1から5のいずれか一項に記載の制御システム。

[請求項7] 前記プログラマブルコントローラと、前記プログラム送信装置と、

サーバと、を備える制御システムであって、

前記プログラム送信装置の前記送信手段は、前記制御プログラム及び前記第 1 コードを前記サーバに送信し、

前記サーバは、前記送信手段によって送信された前記制御プログラム及び前記第 1 コードを受信し、受信した前記制御プログラムとしての前記受信プログラム及び前記第 1 コードを前記プログラマブルコントローラに送信する、

請求項 1 から 6 のいずれか一項に記載の制御システム。

[請求項 8]

機器を制御するための、プログラム送信装置によって送信された制御プログラムとしての受信プログラムを受信するプログラマブルコントローラであって、

前記受信プログラムと、前記制御プログラムからの変更の有無を検証するための第 1 コードであって、該制御プログラム及び前記プログラム送信装置が記憶するデータから予め定められた手順で生成された前記第 1 コードと、を受信する受信手段と、

前記受信プログラム及び予め前記プログラム送信装置と共有される前記データから前記手順で第 2 コードを生成する第 2 コード生成手段と、

前記第 1 コードが前記第 2 コードに等しい場合に、前記受信プログラムを実行する実行手段と、

を備えるプログラマブルコントローラ。

[請求項 9]

機器を制御するプログラマブルコントローラと、前記プログラマブルコントローラに前記機器を制御させるための制御プログラムを送信するプログラム送信装置と、によって実行される制御プログラム送信方法であって、

前記プログラム送信装置が、前記制御プログラムからの変更の有無を検証するための第 1 コードを、前記制御プログラム及び予め定められたデータから予め定められた手順で生成し、

前記プログラム送信装置が、前記制御プログラム及び前記第1コードを送信し、

前記プログラマブルコントローラが、前記プログラム送信装置によって送信された前記制御プログラムとしての受信プログラム及び前記第1コードを受信し、

前記プログラマブルコントローラが、前記受信プログラム及び予め前記プログラム送信装置と共有される前記データから前記手順で第2コードを生成し、

前記プログラマブルコントローラが、前記第1コードが前記第2コードに等しい場合に、前記受信プログラムを実行する、

ことを含む制御プログラム送信方法。

[請求項10]

機器を制御するための、プログラム送信装置によって送信された制御プログラムとしての受信プログラムを受信するプログラマブルコントローラを、

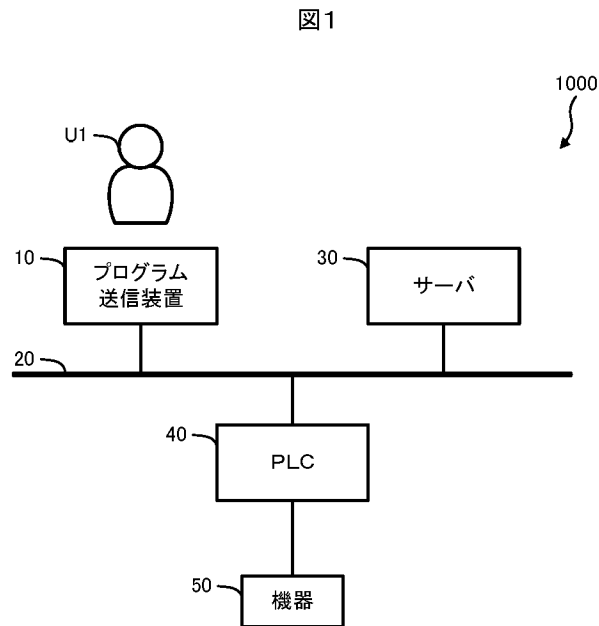
前記受信プログラムと、前記制御プログラムからの変更の有無を検証するための第1コードであって、該制御プログラム及び前記プログラム送信装置が記憶するデータから予め定められた手順で生成された前記第1コードと、を受信する受信手段、

前記受信プログラム及び予め前記プログラム送信装置と共有される前記データから前記手順で第2コードを生成する第2コード生成手段、

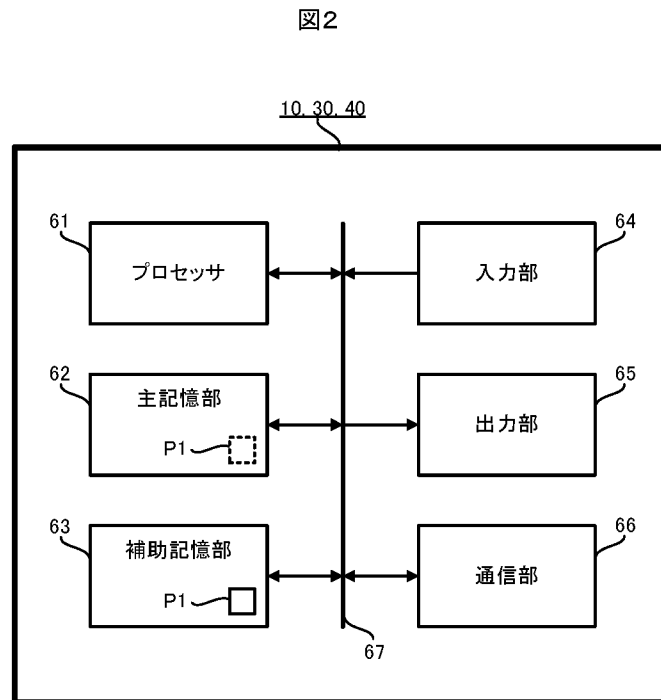
前記第1コードが前記第2コードに等しい場合に、前記受信プログラムを実行する実行手段、

として機能させるためのコントローラプログラム。

[図1]

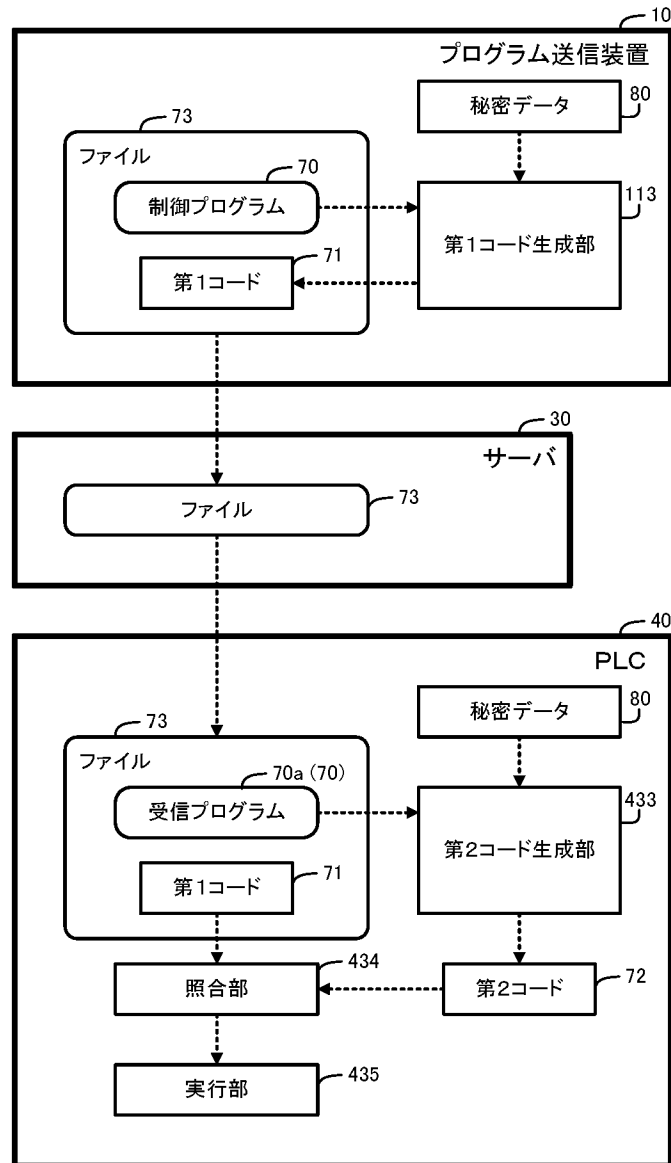


[図2]



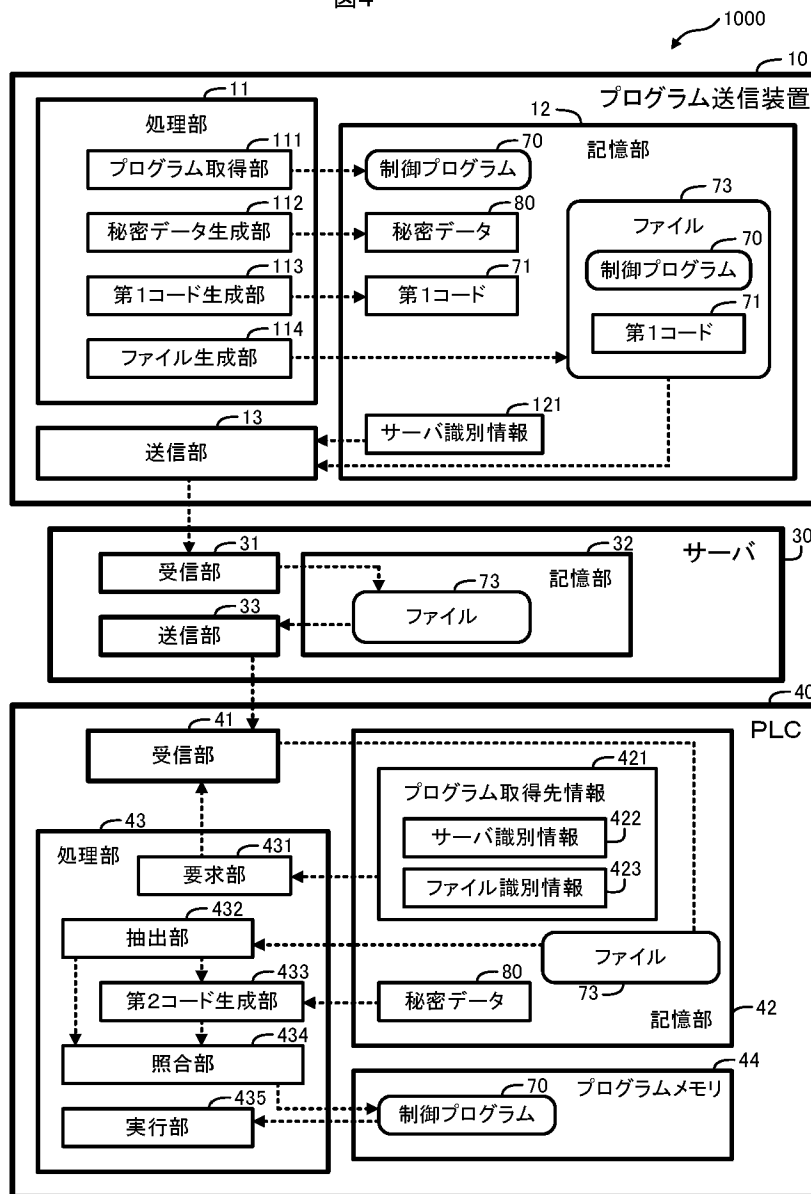
[図3]

図3



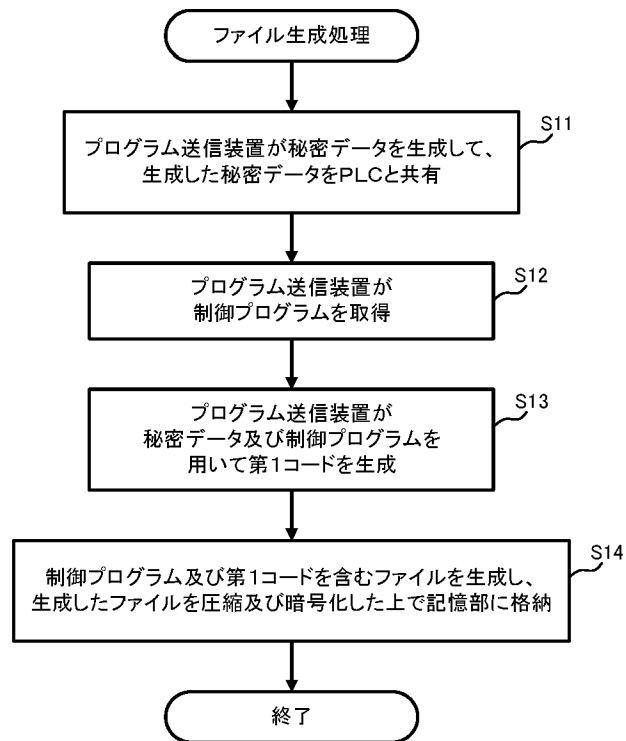
[図4]

図4



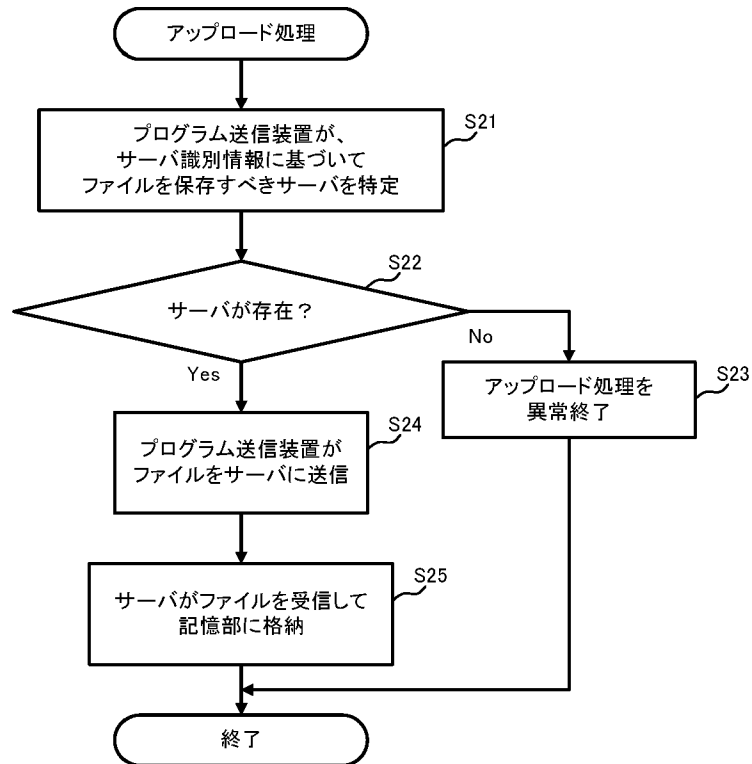
[図5]

図5



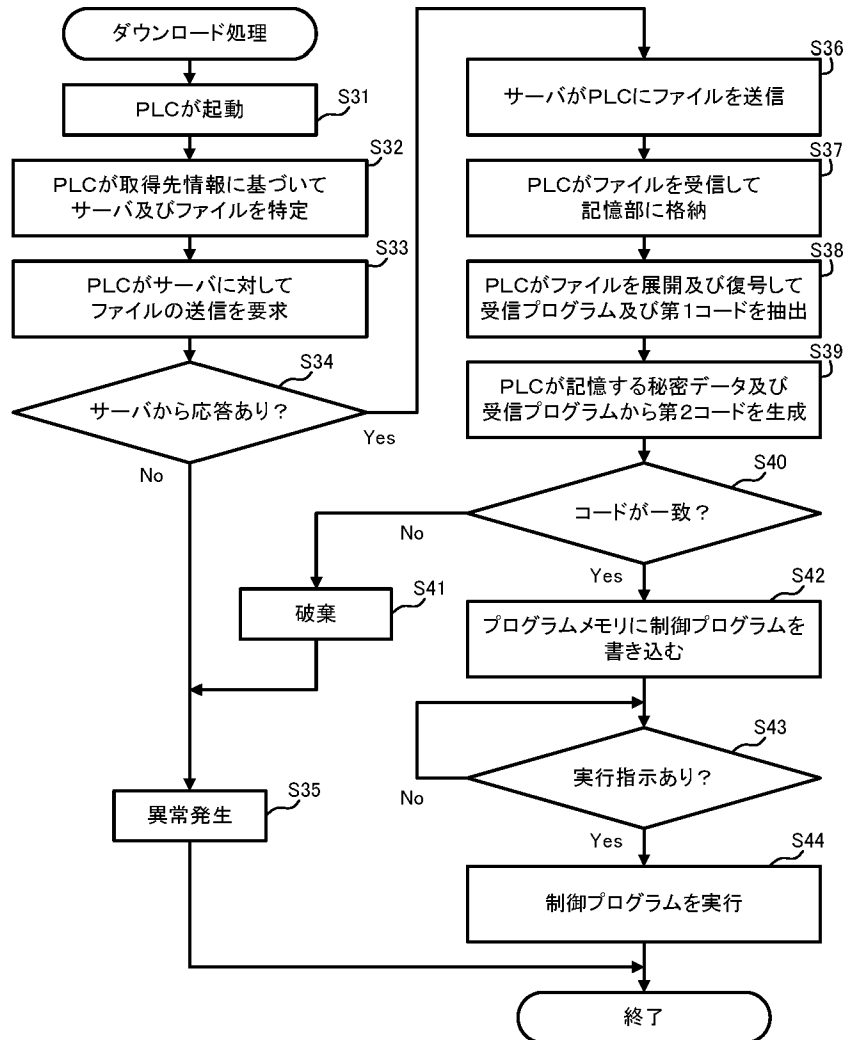
[図6]

図6



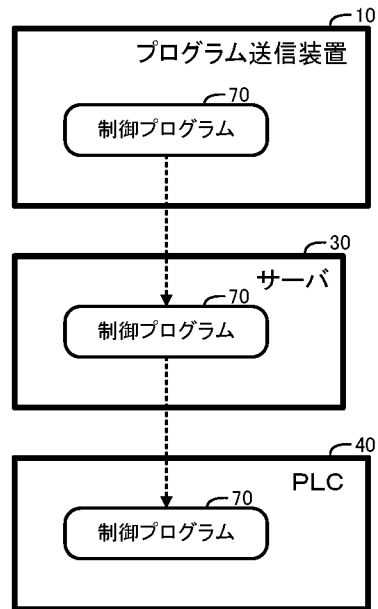
[図7]

図7

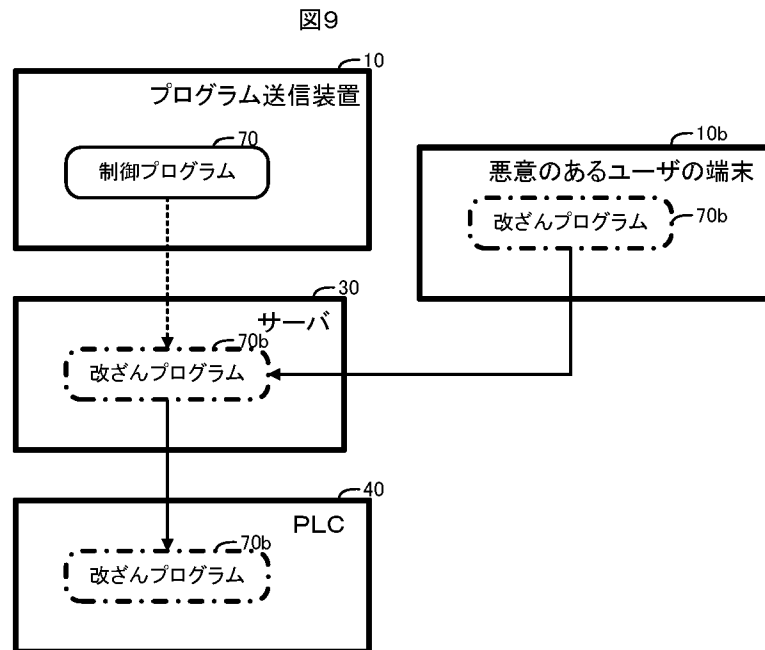


[図8]

図8

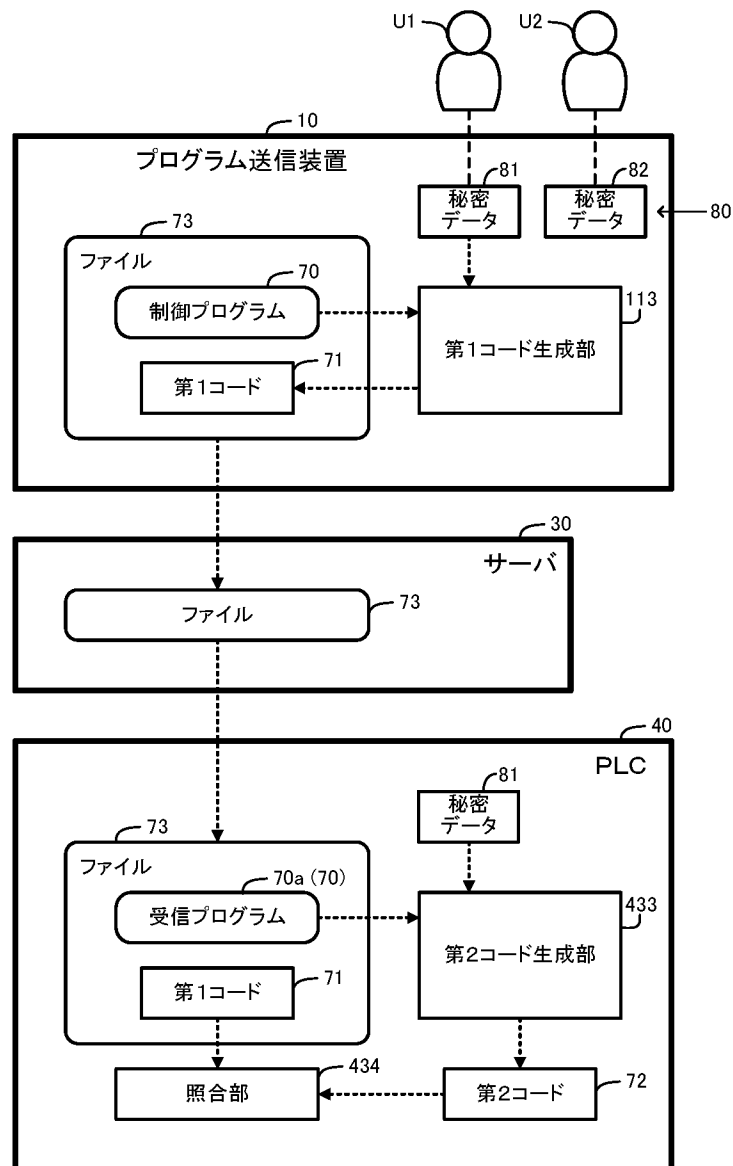


[図9]



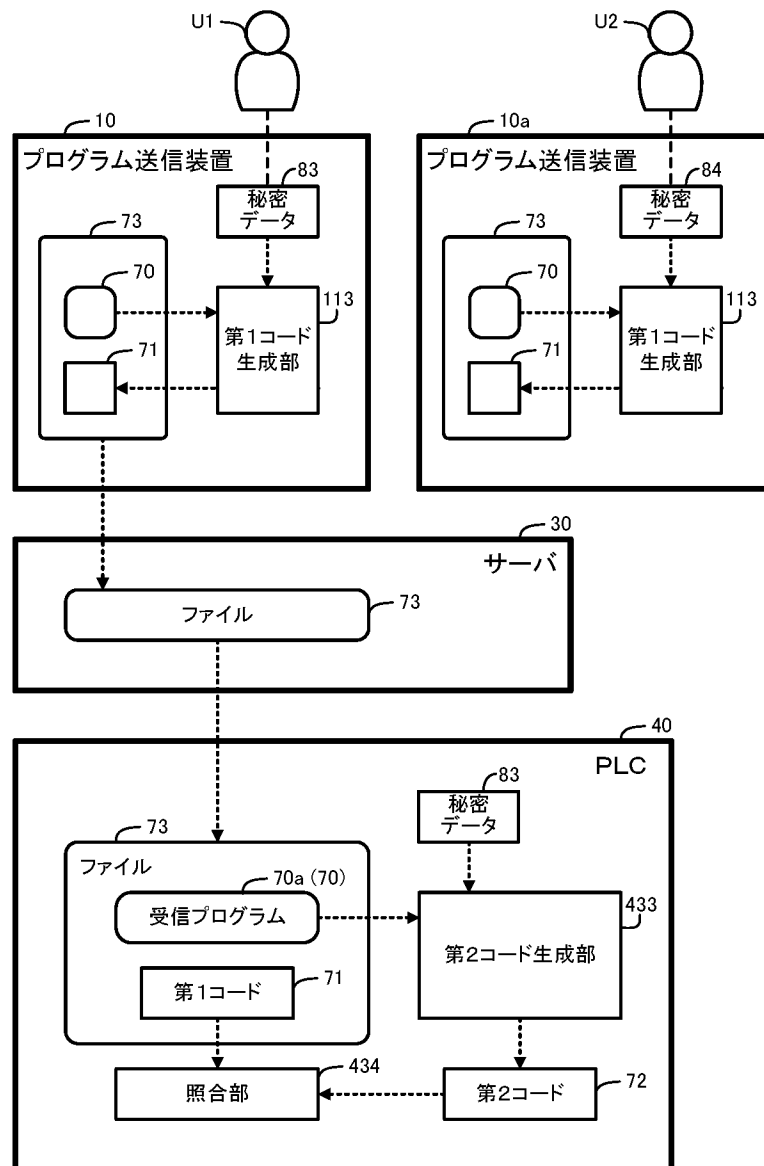
[図10]

図10



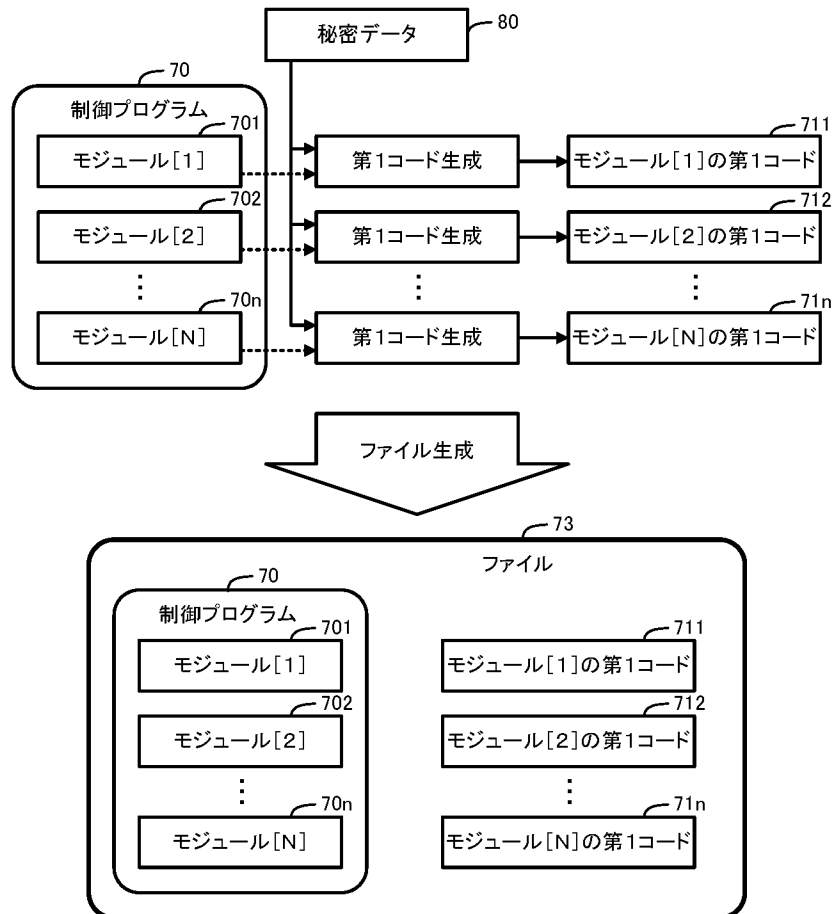
[図11]

図11



[図12]

図12



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2021/021794

A. CLASSIFICATION OF SUBJECT MATTER

G05B 19/05(2006.01)i

FI: G05B19/05 A

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G05B19/05

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Published examined utility model applications of Japan 1922-1996

Published unexamined utility model applications of Japan 1971-2021

Registered utility model specifications of Japan 1996-2021

Published registered utility model applications of Japan 1994-2021

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	US 2020/0193000 A1 (ROCKWELL AUTOMATION TECHNOLOGIES, INC) 18 June 2020 (2020-06-18) paragraphs [0024]-[0057], fig. 1-8	1-5, 8-10 6, 7
Y	WO 2014/097444 A1 (MITSUBISHI ELECTRIC CORPORATION) 26 June 2014 (2014-06-26) paragraphs [0017]-[0023]	6
Y	JP 2018-128722 A (HITACHI INDUSTRY EQUIPMENT SYSTEMS CO LTD) 16 August 2018 (2018-08-16) paragraph [0013]	7

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

28 July 2021 (28.07.2021)

Date of mailing of the international search report

10 August 2021 (10.08.2021)

Name and mailing address of the ISA/

Japan Patent Office
3-4-3, Kasumigaseki, Chiyoda-ku,
Tokyo 100-8915, Japan

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application no.

PCT/JP2021/021794

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
US 2020/0193000 A1	18 Jun. 2020	EP 3667526 A1	
WO 2014/097444 A1	26 Jun. 2014	US 2015/0271161 A1	
		paragraphs [0050]- [0061]	
		KR 10-2015-0086358 A	
		CN 104871098 A	
JP 2018-128722 A	16 Aug. 2018	(Family: none)	

A. 発明の属する分野の分類（国際特許分類（IPC）） G05B 19/05(2006.01)i FI: G05B19/05 A														
B. 調査を行った分野 調査を行った最小限資料（国際特許分類（IPC）） G05B19/05 最小限資料以外の資料で調査を行った分野に含まれるもの <table border="0"> <tr> <td>日本国実用新案公報</td> <td>1922 - 1996年</td> </tr> <tr> <td>日本国公開実用新案公報</td> <td>1971 - 2021年</td> </tr> <tr> <td>日本国実用新案登録公報</td> <td>1996 - 2021年</td> </tr> <tr> <td>日本国登録実用新案公報</td> <td>1994 - 2021年</td> </tr> </table> 国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）			日本国実用新案公報	1922 - 1996年	日本国公開実用新案公報	1971 - 2021年	日本国実用新案登録公報	1996 - 2021年	日本国登録実用新案公報	1994 - 2021年				
日本国実用新案公報	1922 - 1996年													
日本国公開実用新案公報	1971 - 2021年													
日本国実用新案登録公報	1996 - 2021年													
日本国登録実用新案公報	1994 - 2021年													
C. 関連すると認められる文献														
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求項の番号												
X	US 2020/0193000 A1 (ROCKWELL AUTOMATION TECHNOLOGIES, INC.) 18.06.2020 (2020 - 06 - 18) 段落[0024]-[0057], 図1-8	1-5, 8-10												
Y		6, 7												
Y	WO 2014/097444 A1 (三菱電機株式会社) 26.06.2014 (2014 - 06 - 26) 段落[0017]-[0023]	6												
Y	JP 2018-128722 A (株式会社日立産機システム) 16.08.2018 (2018 - 08 - 16) 段落[0013]	7												
☐ C欄の続きにも文献が列挙されている。 ☒ パテントファミリーに関する別紙を参照。														
<table border="0"> <tr> <td>* 引用文献のカテゴリー</td> <td>"T" 国際出願日又は優先日後に公表された文献であって出願と抵触するものではなく、発明の原理又は理論の理解のために引用するもの</td> </tr> <tr> <td>"A" 特に関連のある文献ではなく、一般的な技術水準を示すもの</td> <td>"X" 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの</td> </tr> <tr> <td>"E" 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの</td> <td>"Y" 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの</td> </tr> <tr> <td>"L" 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）</td> <td>"&" 同一パテントファミリー文献</td> </tr> <tr> <td>"O" 口頭による開示、使用、展示等に言及する文献</td> <td></td> </tr> <tr> <td>"P" 国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献</td> <td></td> </tr> </table>			* 引用文献のカテゴリー	"T" 国際出願日又は優先日後に公表された文献であって出願と抵触するものではなく、発明の原理又は理論の理解のために引用するもの	"A" 特に関連のある文献ではなく、一般的な技術水準を示すもの	"X" 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの	"E" 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの	"Y" 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの	"L" 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）	"&" 同一パテントファミリー文献	"O" 口頭による開示、使用、展示等に言及する文献		"P" 国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献	
* 引用文献のカテゴリー	"T" 国際出願日又は優先日後に公表された文献であって出願と抵触するものではなく、発明の原理又は理論の理解のために引用するもの													
"A" 特に関連のある文献ではなく、一般的な技術水準を示すもの	"X" 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの													
"E" 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの	"Y" 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの													
"L" 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）	"&" 同一パテントファミリー文献													
"O" 口頭による開示、使用、展示等に言及する文献														
"P" 国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献														
国際調査を完了した日 28.07.2021	国際調査報告の発送日 10.08.2021													
名称及びあて先 日本国特許庁(ISA/JP) 〒100-8915 日本国 東京都千代田区霞が関三丁目4番3号	権限のある職員（特許庁審査官） 影山 直洋 3U 5785 電話番号 03-3581-1101 内線 3364													

国際調査報告
 パテントファミリーに関する情報

国際出願番号

PCT/JP2021/021794

引用文献			公表日	パテントファミリー文献			公表日
US	2020/0193000	A1	18.06.2020	EP	3667526	A1	
WO	2014/097444	A1	26.06.2014	US	2015/0271161	A1	
				段落[0050]-[0061]			
				KR	10-2015-0086358	A	
				CN	104871098	A	
JP	2018-128722	A	16.08.2018	(ファミリーなし)			