

(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1月6日(06.01.2022)



(10) 国際公開番号

WO 2022/004544 A1

(51) 国際特許分類:
G05B 19/18 (2006.01) *G06F 21/60* (2013.01)
G05B 19/414 (2006.01)

(21) 国際出願番号: PCT/JP2021/023913

(22) 国際出願日: 2021年6月24日(24.06.2021)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願 2020-112468 2020年6月30日(30.06.2020) JP

(71) 出願人: ファナック株式会社 (FANUC CORPORATION) [JP/JP]; 〒4010597 山梨県

南都留郡忍野村忍草字古馬場 3 5 8
0 番地 Yamanashi (JP).

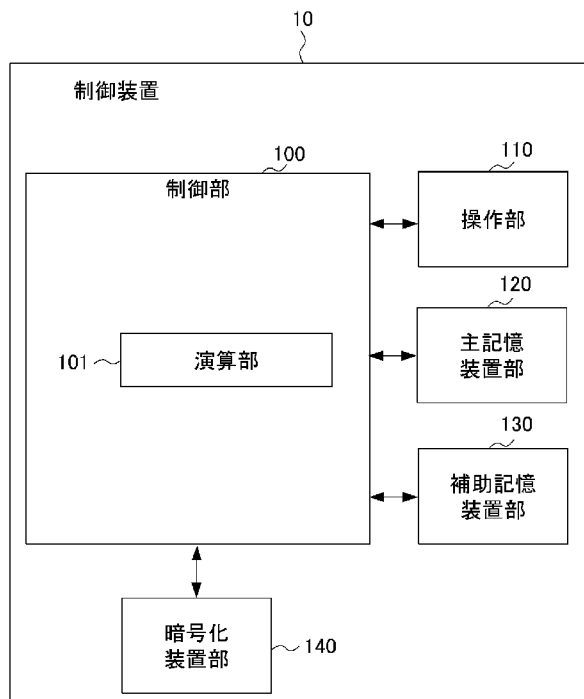
(72) 発明者: 由井 夢樹 (YUI Yumeki); 〒4010597 山梨県南都留郡忍野村忍草字古馬場 3 5 8 0 番地 ファナック株式会社内 Yamanashi (JP). 木村 剛史 (KIMURA Takeshi); 〒4010597 山梨県南都留郡忍野村忍草字古馬場 3 5 8 0 番地 ファナック株式会社内 Yamanashi (JP).

(74) 代理人: 正林 真之, 外 (SHOBAYASHI Masayuki et al.); 〒1000005 東京都千代田区丸の内 1 - 7 - 1 2 サビアタワー 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,

(54) Title: CONTROL DEVICE

(54) 発明の名称: 制御装置



10 Control device
100 Control unit
101 Calculation unit
110 Operating unit
120 Main storage device unit
130 Auxiliary storage device unit
140 Encryption device unit

(57) Abstract: Reduce inventory cost without preparing a control device for each destination in advance. This control device is for controlling industrial machinery and includes an encryption unit, and comprises: an encryption device unit that includes a plurality of encryption units corresponding to each of a plurality of destinations, and a plurality of invalidation units that invalidate any one of the plurality of encryption units or invalidate the plurality of encryption units; and an operating unit that, depending on the destination of the control device, selects invalidation of the encryption units by

CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ,
EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN,
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))

specifying to each of the plurality of invalidation units to invalidate one of the plurality of encryption units or to invalidate the plurality of encryption units.

(57) 要約: 仕向け先毎の制御装置を予め用意することなく、在庫コストを低減すること。制御装置は、産業機械を制御し暗号化部を含む制御装置であって、複数の仕向け先毎に対応した複数の前記暗号化部と複数の前記暗号化部のいずれかを無効化するもしくは複数の前記暗号化部を無効化する複数の無効化部とを含む暗号化装置部と、前記制御装置の仕向け先に応じて前記複数の無効化部それぞれに複数の前記暗号化部のいずれかを無効化させるか複数の前記暗号化部を無効化させるかを指定して、暗号化部の無効化を選択する操作部と、を備える。

明 細 書

発明の名称 ： 制御装置

技術分野

[0001] 本発明は、制御装置に関する。

背景技術

[0002] エンドユーザの数値制御装置においては、予め設定された通信設定情報に基づいて、暗号化された加工プログラムを工作機械メーカーのホストコンピュータに要求して、受信した暗号化された加工プログラムを復号し、復号された加工プログラムを実行して工作機械を制御することで、加工プログラムが不正に再利用されることを防止する技術が知られている。例えば、特許文献1 参照。

先行技術文献

特許文献

[0003] 特許文献1：特開2015-138527号公報

発明の概要

発明が解決しようとする課題

[0004] 工作機械やロボット等の産業機械を制御する制御装置の内部データ（例えば、機械メーカーのプログラム等）の保護やファームウェアの改ざんを防ぐために、信頼のおける暗号機能を有した暗号化チップを制御装置に搭載することが今後重要となる。

一方で、制御装置の販売者は販売する同じ制御装置の暗号技術に関しては仕向け先国（地域）それぞれの法規に従う必要があり、加えて、ある仕向け先国（地域）に対応できる暗号技術を使用可能な状態で別の仕向け国（地域）に販売できない法規もあることから、一種類の暗号化チップでは、すべての仕向け先国（地域）の法規を満たせない場合がある。

そのため、制御装置の販売者は、仕向け先の国（地域）毎に適切な暗号化チップを使う必要等があるため、国（地域）毎に異なる暗号化チップを実装

した制御装置を複数用意する必要がある。

また、制御装置を工作機械や生産システムに組み込んで商品開発する機械メーカーは、それぞれ異なる国に出荷する場合に、それぞれの国に対応した暗号化チップを実装した制御装置の在庫を持つ必要があり、機械メーカーにとっても在庫コスト（製造コスト）がかかるという問題もある。

[0005] そこで、仕向け先毎の制御装置を予め用意することなく、在庫コストを低減することが望まれている。

課題を解決するための手段

[0006] 本開示の制御装置の一態様は、産業機械を制御し暗号化部を含む制御装置であって、複数の仕向け先毎に対応した複数の前記暗号化部と複数の前記暗号化部のいずれかを無効化するもしくは複数の前記暗号化部を無効化する複数の無効化部とを含む暗号化装置部と、前記制御装置の仕向け先に応じて前記複数の無効化部それぞれに複数の前記暗号化部のいずれかを無効化させるか複数の前記暗号化部を無効化させるかを指定して、暗号化部の無効化を選択する操作部と、を備える。

発明の効果

[0007] 一態様によれば、仕向け先毎の制御装置を予め用意することなく、在庫コストを低減することができる。

図面の簡単な説明

[0008] [図1]一実施形態に係る制御装置の機能的構成の一例を示す機能ブロック図である。

[図2]補助記憶装置部に格納されるデータの一例を示す図である。

[図3]暗号化装置部の構成例を示す図である。

[図4]制御装置の仕向け先で使用不可のセキュリティチップの削除処理について説明するフローチャートである。

[図5]制御装置の起動時の処理について説明するフローチャートである。

[図6]暗号化装置部の構成例を示す図である。

発明を実施するための形態

[0009] 以下、一実施形態について図面を用いて説明する。ここでは、産業機械として工作機械を、制御装置として数値制御装置を例示する。なお、本発明は、工作機械に限定されず、例えば産業用ロボット、サービス用ロボット等にも適用可能である。この場合、制御装置は、ロボット制御装置である。

[0010] <一実施形態>

図1は、一実施形態に係る制御装置の機能的構成例を示す機能ブロック図である。

制御装置10は、当業者にとって公知の数値制御装置であり、制御情報に基づいて動作指令を生成し、生成した動作指令を工作機械（図示しない）に出力する。これにより、制御装置10は、工作機械（図示しない）の動作を制御する。なお、工作機械（図示しない）がロボット等の場合、制御装置10は、ロボット制御装置等でもよい。

[0011] 制御装置10は、図示しない接続インタフェースを介して工作機械（図示しない）と互いに直接接続されてもよい。なお、制御装置10と工作機械（図示しない）とは、LAN（Local Area Network）やインターネット等の図示しないネットワークを介して相互に接続されていてもよい。この場合、制御装置10は、かかる接続によって相互に通信を行うための図示しない通信部を備えている。

[0012] ここで、図示しない工作機械は、例えば、工作機械やロボット、周辺装置等である。なお、図示しない工作機械は、工作機械やロボット、周辺装置に限定されず、産業機械全般に広く適用することができる。産業機械とは、例えば、工作機械、産業用ロボット、サービス用ロボット、鍛圧機械及び射出成形機といった様々な機械を含む。

[0013] 図1に示すように、制御装置10は、制御部100、操作部110、主記憶装置部120、補助記憶装置部130、及び暗号化装置部140を有する。そして、制御部100、操作部110、主記憶装置部120、補助記憶装置部130、及び暗号化装置部140は、図示しないバスを介して通信可能

に接続されている。

[0014] <操作部 110>

操作部 110 は、例えば、制御装置 10 に含まれる図示しない MDI ユニットのキーボードや表示器のタッチパネルあるいは物理的なロータリスイッチ等であり、制御装置 10 の販売者や機械メーカーの設計者等からの操作を受け付ける。

具体的には、操作部 110 は、機械メーカーの設計者等による操作に基づいて、制御装置 10 の仕向け先の指定を受け付け、受け付けた仕向け先に応じて後述する暗号化装置部 140 に含まれる n 個のセキュリティチップのうち無効化対象のセキュリティチップを指定する（ n は 2 以上の整数）。

なお、後述する補助記憶装置部 130 が、例えば、暗号化装置部 140 の n 個のセキュリティチップそれぞれと仕向け先とを対応付けした仕向け先テーブル（図示しない）を予め記憶し、操作部 110 が制御装置 10 の仕向け先の指定を受け付け、指定された仕向け先に対応する有効のままとするセキュリティチップを選択した場合、後述する制御部 100 は、選択されたセキュリティチップと仕向け先テーブル（図示しない）とに基づいて、無効化対象のセキュリティチップを判定するようにしてもよい。

[0015] <主記憶装置部 120>

主記憶装置部 120 は、例えば、RAM（Random Access Memory）等のメモリであり、後述する制御部 100 がプログラムを実行する上で一時的に必要とされるデータを格納する。

[0016] <補助記憶装置部 130>

補助記憶装置部 130 は、例えば、ROM（Read Only Memory）や HDD（Hard Disk Drive）やフラッシュメモリ等である。

図 2 は、補助記憶装置部 130 に格納されるデータの一例を示す図である。

図 2 に示すように、補助記憶装置部 130 は、後述する制御部 100 が実

行するシステムプログラム及びアプリケーションプログラム等を格納する既存ソフトウェア領域 131 を有する。また、補助記憶装置部 130 は、後述する暗号化装置部 140 に含まれる n 個のセキュリティチップそれぞれを実行するセキュリティチップ制御ソフトウェア 134 (1) – 134 (n) を格納するセキュリティ領域 132 を有する。

セキュリティチップ制御ソフトウェア 134 (1) – 134 (n) それぞれは、後述する暗号化装置部 140 に含まれる暗号化部としての n 個のセキュリティチップのうち対応する 1 つのセキュリティチップを実行することにより、制御装置 10 の仕向け先（例えば、第 1 地域（国）から第 n 地域（国）のいずれかの地域（国））に応じた暗号化処理を実現する。

[0017] なお、補助記憶装置部 130 は、既存ソフトウェア領域 131 の格納されたソフトウェア、及びセキュリティ領域 132 に格納されたセキュリティチップ制御ソフトウェア 134 (1) – 134 (n) の各々をファイル名ベースで管理してもよい。そうすることで、補助記憶装置部 130 は、後述する制御部 100 からファイル名に基づいて削除指示されたソフトウェアを削除することができる。あるいは、補助記憶装置部 130 は、既存ソフトウェア領域 131 に格納されたソフトウェア、及びセキュリティ領域 132 に格納されたセキュリティチップ制御ソフトウェア 134 (1) – 134 (n) の各々をファイルシステム上でアドレス管理してもよい。そうすることで、補助記憶装置部 130 は、各ソフトウェアが格納されているアドレスと範囲とを予め分かっていることから、後述する制御部 100 からのアドレスに基づいて削除指示されたソフトウェアを削除することができる。

[0018] また、補助記憶装置部 130 は、セキュリティチップ制御抽象化プログラム 133 及び起動時チェック処理プログラム 135 を格納してもよい。

後述する制御部 100（具体的には演算部 101）によりセキュリティチップ制御抽象化プログラム 133 を実行することにより、抽象化された共通インタフェースにより、セキュリティチップ (j) ($1 \leq j \leq n$) に対応する制御を実行するセキュリティチップ制御ソフトウェア 134 (j) に対し

て、指示することを可能とする。なお、このような抽象化処理は、当業者に取って公知であり、詳細な説明は省略する。

また、制御装置 10 の起動時に、制御部 100（具体的には演算部 101）により起動時チェック処理プログラム 135 を実行することにより、制御装置 10 の構成や設定等のチェック処理を実行する。なお、起動時チェック処理プログラム 135 を実行することにより提供される起動時チェック処理機能部（起動時チェック処理部）については後述する。

[0019] <暗号化装置部 140>

図 3 は、暗号化装置部 140 の構成の一例を示す図である。

図 3 に示すように、暗号化装置部 140 は、暗号化部として、 n 個のヒューズ 141 (1) - 141 (n)、 n 個のセキュリティチップ 142 (1) - 142 (n)、 n 個のスイッチ SW1 - SW n 、ダイオード 143、スイッチ 144、及び電源 145 を有する。 n 個のヒューズ 141 (1) - 141 (n)、 n 個のセキュリティチップ 142 (1) - 142 (n)、 n 個のスイッチ SW (1) - SW (n)、ダイオード 143、スイッチ 144、及び電源 145 は、図示しない 1 つの制御回路に配置されてもよい。

なお、電源 150 は、例えば、セキュリティチップ 142 (1) - 142 (n) それぞれが動作するのに必要な電力を供給する、外部の定電流源である。

[0020] ヒューズ 141 (1) - 141 (n) は、セキュリティチップ 142 (1) - 142 (n) それぞれと接続され、無効化部として動作する。

[0021] 暗号化部としてのセキュリティチップ 142 (1) - 142 (n) としては、例えば、TCG (Trusted Computing Group)（登録商標）で定義されたセキュリティの仕様に準拠したセキュリティチップ TPM (Trusted Platform Module) を適用することができる。なお、セキュリティチップ 142 (1) - 142 (n) は、TPM としたが、これに限定されない。例えば、セキュリティチップ 142 (1) - 142 (n) は、暗号化部として、TPM 準拠の専用チップで実装

されたディスクリーTPMでもよく、前記ディスクリーTPMによる暗号化でもよい。また、セキュリティチップ142(1)－142(n)は、暗号化部として、マイコン内部のセキュリティ領域で実行されるファームウェアTPMでもよく、前記ファームウェアTPMによる暗号化でもよい。あるいは、セキュリティチップ142(1)－142(n)は、暗号化部として、TPM規格に準拠しないディスクリーICでもよく、前記ディスクリーICによる暗号化でもよい。また、セキュリティチップ142(1)－142(n)は、暗号化部として、マイコンによるソフトウェア暗号化でもよい。

前述したように、例えば仕向け先(第1地域(国)から第n地域(国)のいずれかの地域(国))毎に指定されるそれぞれのセキュリティチップ142(1)－142(n)は、セキュリティ領域132に格納された、対応するそれぞれのセキュリティチップ制御ソフトウェア134(1)－134(n)を実行することにより、仕向け先に特化したそれぞれに対応した暗号化処理を行うことができる。

[0022] スイッチSW(1)－SW(n)、ダイオード143、スイッチ144、及び電源145は、例えば、後述する制御部100からの制御指示に基づいて、加負荷回路として動作する。

具体的には、操作部110が、例えば、制御装置10の仕向け先として第i地域(国)の指定を受け付けた場合、セキュリティチップ142(i)以外の無効化対象のセキュリティチップ142(j)(j≠i)を制御回路から切断するために、後述する制御部100からの制御指示に基づいて、スイッチSW(i)はOFFになり、スイッチSW(i)以外のスイッチSW(j)(j≠i)はONになる。なお、iは1からnの整数である。この場合、後述する制御部100からの指示に基づきスイッチ144がONになると、電源145からの電力がヒューズ141(i)以外のヒューズ141(j)(j≠i)に印加されることで、ヒューズ141(i)以外のヒューズ141(j)が焼き切られる。これにより、セキュリティチップ142(i)

以外のセキュリティチップ１４２（ｊ）が制御回路から切断され無効化される。

なお、加負荷回路として動作するスイッチＳＷ（１）－ＳＷ（ｎ）及びスイッチ１４４は、セキュリティチップ１４２（ｉ）以外のセキュリティチップ１４２（ｊ）（ $j \neq i$ ）全てが制御回路から切断されている場合、無効化処理を行わない誤作動防止機能を有してもよい。

また、加負荷回路としてのダイオード１４３及びスイッチ１４４があることにより、無効化処理のタイミングを決定することができ、電源投入時にすぐに無効化処理にならないことで、誤って仕向け先が決まってしまうことを避けることができる。ただし、ダイオード１４３及びスイッチ１４４は加負荷回路になくてもよい。

[0023] 電源１４５は、ヒューズ１４１（１）－１４１（ｎ）を焼き切るのに必要な電力を供給する定電流源である。

[0024] <制御部１００>

制御部１００は、演算部１０１を備え、例えば制御装置１０を全体的に制御するプロセッサである。制御部１００は、図示しないバスを介して主記憶装置部１２０、及び補助記憶装置部１３０と通信可能に接続される。

演算部１０１は、補助記憶装置部１３０の既存ソフトウェア領域１３１に格納されたシステムプログラム及びアプリケーションプログラムを、バスを介して読み出し、前記システムプログラム及びアプリケーションプログラムに従って制御装置１０全体を制御する。

同様に、演算部１０１は、補助記憶装置部１３０に格納されたセキュリティチップ制御抽象化プログラム１３３、セキュリティチップ制御ソフトウェア１３４（１）－１３４（ｎ）、及び起動時チェック処理プログラム１３５を、バスを介して読み出し、前記システムプログラム及びアプリケーションプログラムに従って、制御装置１０に係るセキュリティ処理を制御する。

これにより、図１に示すように、制御部１００は、前述したセキュリティチップ制御抽象化機能、及び起動時チェック処理機能を実現するように構成

される。

[0025] 制御部100は、暗号化装置部140に配置されるスイッチSW(1)－SW(n)及びスイッチ144の加負荷回路の作動により、セキュリティチップ142(i)以外の少なくとも1つの無効化対象のセキュリティチップ142(j)(j≠i)が無効化された場合、無効化されたセキュリティチップ142(j)に対応するセキュリティチップ制御ソフトウェア134(j)(j≠i)を補助記憶装置部130から削除するようにしてもよい。

具体的には、制御部100は、例えば、操作部110が制御装置10の仕向け先として第i地域(国)の指定を機械メーカーの設計者等から受け付けた場合、セキュリティチップ142(i)以外のセキュリティチップ142を制御回路から切断するために、スイッチSW(i)をOFFにし、スイッチSW(i)以外のスイッチSWをONにする。そして、制御部100は、スイッチ144をONにすることで、ヒューズ141(i)以外のヒューズ141(j)(j≠i)を焼き切り、セキュリティチップ142(i)以外の無効化対象のセキュリティチップ142(j)を制御回路から切断し無効化する。その際、制御部100は、セキュリティチップ制御ソフトウェア134(i)以外のセキュリティチップ制御ソフトウェア134(j)(j≠i)全てを補助記憶装置部130から削除するようにしてもよい。

[0026] そうすることで、制御装置10の販売者は出荷時に機械メーカー等にどの仕向け地仕向けかを設定せずに販売することができ、機械メーカーの設計者等は機械の出荷までに、制御装置10の仕向け先の設定操作を行うことで、選択された仕向け先向けの暗号機能のみを有する制御装置10とすることができる。

なお、無効化対象のセキュリティチップ142(j)(j≠i)は仕向け先では使われないため、仕向け先とは関係ないセキュリティ情報を含むセキュリティチップ制御ソフトウェア134(i)以外のセキュリティチップ制御ソフトウェア134(j)(j≠i)を残さないようにすることで、ハッキングされるリスクを減らすことができる。また、仕向け先へのお荷前に、セキュリティチップ制御ソフトウェア134(i)以外のセキュリティチッ

プ制御ソフトウェア134(j) (j ≠ i) を削除することによって、セキュリティチップ制御ソフトウェア134(i) 以外のセキュリティチップ制御ソフトウェア134(j) (j ≠ i) が仕向け先の法律による開示要求等の影響を受けずに済むという効果を奏することができる。

なお、セキュリティチップ制御ソフトウェア134(j) (j ≠ i) の削除は、当業者にとって公知のゼロ上書き後削除や、乱数上書き後削除等で行われてもよい。

[0027] ところで、例えば、セキュリティチップ142(i) 以外の無効化対象のセキュリティチップ142(j) (j ≠ i) を制御回路から切断するため、ヒューズ141(i) 以外のヒューズ141(j) (j ≠ i) を焼き切っているときに、機械メーカーの設計者等が誤って制御装置10の電源を落としてしまう等の場合が考えられる。この場合、ヒューズ141(i) 以外のヒューズ141(j) (j ≠ i) の一部が焼き切られず、無効化対象のセキュリティチップ142(j) (j ≠ i) の一部が制御回路に接続された状態のままとなるリスクが発生する可能性がある。

[0028] そこで、制御部100は、例えば、制御装置10の仕向け先に対応するセキュリティチップ142(i) の識別情報を補助記憶装置部130に記憶してもよい。そうすることで、制御部100は、制御装置10が起動されたとき、起動時チェック処理プログラム135を起動することで、補助記憶装置部130に記憶されたセキュリティチップ142(i) の識別情報と、公知の断線検知の手法と、に基づいて、セキュリティチップ142(i) 以外のセキュリティチップ142(j) (j ≠ i) 全てが制御回路から切断されているか否かを判定するようにしてもよい。

具体的には、制御部100は、起動時チェック処理プログラム135を実行することで、例えば、セキュリティチップ142(i) 以外の無効化対象のセキュリティチップ142(j) (j ≠ i) それぞれに制御用コマンドを送信する。制御部100は、前記制御用コマンドに対する応答を受けたか否かで、無効化対象のセキュリティチップ142(j) (j ≠ i) 全てが制御

回路から切断されているか否かを判定してもよい。すなわち、制御部１００は、起動時チェック処理プログラム１３５を実行することで、無効化対象のセキュリティチップ１４２（ j ）（ $j \neq i$ ）から正しい応答が帰る場合、接続と判定し、正しくない応答若しくは応答がない場合、切断されていると判定するようにしてもよい。

[0029] なお、起動時に、万が一、無効化対象のセキュリティチップ１４２が制御回路から切断されていないことを検知した場合、制御装置１０を起動できないようにするとともに、無効化対象のセキュリティチップ１４２（ j ）（ $j \neq i$ ）が制御回路から切断されていないことを示すアラートを出力し、制御装置１０の図示しない表示器に表示してもよい。その後、例えば、制御装置１０の販売者等により、セキュリティチップ１４２の再設定を行うようにしてもよい。

ただし、一度無効化処理を実行した場合、機械メーカーの設計者等が誤って違う仕向け先に変えないように、制御部１００は、一度目の無効化処理で残す地域（国）を補助記憶装置部１３０に記憶してもよい。そして、機械メーカーの設計者等が一度目に設定した仕向け先と違う仕向け先を設定しようとした場合、制御部１００は、一度目に設定した仕向け先と違う仕向け先を設定しようとしていることを示すアラート等を出力し、制御装置１０の図示しない表示器に表示するようにしてもよい。

そうすることで、制御装置１０は、仕向け先が一度指定されると、ユーザにより制御装置１０が使用可能となる前に、無効化対象のセキュリティチップ１４２（ j ）（ $j \neq i$ ）を確実に無効化することができ、無効化対象のセキュリティチップ１４２（ j ）（ $j \neq i$ ）に対応するセキュリティチップ制御ソフトウェア１３４（ j ）（ $j \neq i$ ）を補助記憶装置部１３０から確実に削除することができる。

[0030] ＜制御装置１０の仕向け先で使用不可のセキュリティチップの削除処理＞

次に、本実施形態に係る制御装置１０の削除処理に係る動作について説明する。

図4は、制御装置10の仕向け先で使用不可のセキュリティチップの削除処理について説明するフローチャートである。ここで示すフローは、制御装置10の仕向け先が指定される度に実行される。

[0031] ステップS11において、操作部110は、機械メーカーの設計者等による入力操作に基づいて、制御装置10の仕向け先の指定を受け付ける。

[0032] ステップS12において、制御部100は、ステップS11で指定された仕向け先に対応するセキュリティチップ142(i)以外の無効化対象のセキュリティチップ142(j)(j≠i)を制御回路から切断するために、スイッチSW(i)をOFFに、スイッチSW(i)以外のスイッチSW(j)(j≠i)をONにそれぞれ設定する。

[0033] ステップS13において、制御部100は、スイッチ144をONにすることにより、ヒューズ141(i)以外のヒューズ141(j)(j≠i)を焼き切り、無効化対象のセキュリティチップ142(j)(j≠i)を制御回路から切断する。

[0034] ステップS14において、演算部101は、無効化対象のセキュリティチップ142(j)に対応するセキュリティチップ制御ソフトウェア134(j)を補助記憶装置部130から削除する。

[0035] <制御装置10の起動時の処理>

次に、本実施形態に係る制御装置10の起動時の処理に係る動作について説明する。

図5は、制御装置10の起動時の削除処理について説明するフローチャートである。ここで示すフローは、制御装置10が起動される度に実行される。

[0036] ステップS21において、制御部100は、起動時チェック処理プログラム135を実行することで、起動時に仕向け先のセキュリティチップ142(i)以外の無効化対象のセキュリティチップ142(j)(j≠i)全てが制御回路から切断されているか否かを判定する。無効化対象のセキュリティチップ142(j)(j≠i)全てが制御回路から切断されている場合、

ステップS 2 3に進む。一方、無効化対象のセキュリティチップ1 4 2 (j) (j ≠ i) 全てが制御回路から切断されていない場合、処理はステップS 2 2に進む。

[0037] ステップS 2 2において、制御部1 0 0は、制御装置1 0を起動できないようにするとともに、無効化対象のセキュリティチップ1 4 2 (j) (j ≠ i) が制御回路から切断されていないことを示すアラートを出力し、図示しない表示器に表示して、起動処理を終了する。

[0038] ステップS 2 3において、制御部1 0 0は、制御装置1 0の通常の起動処理を行う。

[0039] 以上により、一実施形態の制御装置1 0は、複数の地域の各々に対応した暗号化機能を有するセキュリティチップ1 4 2 (1) - 1 4 2 (n) を予め有する。制御装置1 0は、機械メーカーの設計者等による入力操作に基づいて、制御装置1 0の仕向け先の指定を受け付けた場合、指定された仕向け先に対応するセキュリティチップ1 4 2 (i) 以外の無効化対象のセキュリティチップ1 4 2 (j) (j ≠ i) を制御回路から切断することで無効化することができる。

これにより、仕向け先毎の制御装置1 0を予め用意することなく、在庫コストを低減することができる。すなわち、制御装置1 0の販売者は、仕向け先毎に在庫を用意する必要がなくなり、制御装置1 0の販売者の在庫コストを低減することができる。また、機械メーカーや生産システムインテグレータは、仕向け先毎に制御装置1 0の在庫を用意する必要がなくなり、在庫コストを低減することができる。

また、制御装置1 0は、無効化対象のセキュリティチップ1 4 2 (j) (j ≠ i) に対応するセキュリティチップ制御ソフトウェア1 3 4 (j) (j ≠ i) 全てを削除することにより、ハッキングされるリスクを減らすことができる。

また、制御装置1 0は、起動時に、仕向け先に対応するセキュリティチップ1 4 2 (i) 以外の無効化対象のセキュリティチップ1 4 2 (j) (j ≠

i) 全てが制御回路から切断されているか否かを判定する。そして、制御装置 10 は、無効化対象のセキュリティチップ 142 (j) (j ≠ i) 全てが切断されていない場合、制御装置 10 を起動できないようにするとともに、無効化対象のセキュリティチップ 142 (j) (j ≠ i) が制御回路から切断されていないことを示すアラートを、制御装置 10 の図示しない表示器に表示してもよい。そうすることで、例えば、制御装置 10 の販売者等により、セキュリティチップ 142 の再設定を行うようにしてもよい。

[0040] 以上、一実施形態について説明したが、制御装置 10 は、上述の実施形態に限定されるものではなく、目的を達成できる範囲での変形、改良等を含む。

[0041] <変形例 1>

上述の実施形態では、暗号化装置部 140 は、図 3 に示すような構成を有したが、これに限定されない。

図 6 は、暗号化装置部 140 の構成例を示す図である。なお、図 3 の暗号化装置部 140 の要素と同様の機能を有する要素については、同じ符号を付し、詳細な説明は省略する。

図 6 に示すように、ヒューズ 141 (1) - 141 (n) それぞれと、スイッチ SW (1) - SW (n) のそれぞれと、セキュリティチップ 142 (1) - 142 (n) のそれぞれと、が直列に接続される。そして、演算部 101 は、例えば、制御装置 10 の仕向け先として第 i 地域 (国) の指定を受け付けた場合、図 3 の場合と同様に、スイッチ SW (i) を OFF にし、スイッチ SW (i) 以外のスイッチ SW を ON にすることにより、セキュリティチップ 142 (i) 以外の無効化対象のセキュリティチップ 142 を制御回路から切断してもよい。

[0042] <変形例 2>

また例えば、上述の実施形態では、制御部 100 は、起動時チェック処理プログラム 135 を実行することで、起動時に仕向け先のセキュリティチップ 142 (i) 以外の無効化対象のセキュリティチップ 142 (j) (j ≠

i) 全てが制御回路から切断されていない場合、無効化対象のセキュリティチップ142(j) (j ≠ i) が制御回路から切断されていないことを示すアラートを出力し、制御装置10の図示しない表示器に表示したが、これに限定されない。

例えば、制御部100は、制御装置10の再起動時に、起動時チェック処理プログラム135を実行することで、再度無効化対象のセキュリティチップ142(j) (j ≠ i) 全てを制御回路から切断するようにしてもよい。また、制御部100は、無効化対象のセキュリティチップ142(j) (j ≠ i) に対応するセキュリティチップ制御ソフトウェア134(j) (j ≠ i) を補助記憶装置部130から削除してもよい。

そうすることで、制御装置10は、セキュリティチップ142(i) 以外の無効化対象のセキュリティチップ142(j) (j ≠ i) 全てを確実に無効化することができ、無効化対象のセキュリティチップ142(j) (j ≠ i) に対応するセキュリティチップ制御ソフトウェア134(j) (j ≠ i) 全てを補助記憶装置部130から確実に削除することができる。

[0043] なお、一実施形態に係る制御装置10に含まれる各機能は、ハードウェア、ソフトウェア又はこれらの組み合わせによりそれぞれ実現することができる。ここで、ソフトウェアによって実現されるとは、コンピュータがプログラムを読み込んで実行することにより実現されることを意味する。

また、制御装置10に含まれる各構成部は、電子回路等を含むハードウェア、ソフトウェア又はこれらの組み合わせにより実現することができる。

[0044] プログラムは、様々なタイプの非一時的なコンピュータ可読媒体 (Non-transitory computer readable medium) を用いて格納され、コンピュータに供給することができる。非一時的なコンピュータ可読媒体は、様々なタイプの実体のある記録媒体 (Tangible storage medium) を含む。非一時的なコンピュータ可読媒体の例は、磁気記録媒体 (例えば、フレキシブルディスク、磁気テープ、ハードディスクドライブ)、光磁気記録媒体 (例えば、光磁気ディス

ク)、CD-ROM (Read Only Memory)、CD-R、CD-R/W、半導体メモリ (例えば、マスクROM、PROM (Programmable ROM)、EPROM (Erasable PROM)、フラッシュROM、RAM) を含む。また、プログラムは、様々なタイプの一時的なコンピュータ可読媒体 (Transitory computer readable medium) によってコンピュータに供給されてもよい。一時的なコンピュータ可読媒体の例は、電気信号、光信号、及び電磁波を含む。一時的なコンピュータ可読媒体は、電線及び光ファイバ等の有線通信路、又は、無線通信路を介して、プログラムをコンピュータに供給できる。

[0045] なお、記録媒体に記録されるプログラムを記述するステップは、その順序に沿って時系列的に行われる処理はもちろん、必ずしも時系列的に処理されなくとも、並列的あるいは個別に実行される処理をも含むものである。

[0046] 以上を換言すると、本開示の制御装置は、次のような構成を有する各種各様の実施形態を取ることができる。

[0047] (1) 本開示の制御装置10は、産業機械を制御し暗号化部を含む制御装置であって、複数の仕向け先毎に対応した複数のセキュリティチップ142と複数のセキュリティチップ142のいずれかを無効化するもしくは複数のセキュリティチップ142を無効化する複数の無効化部とを含む暗号化装置部140と、制御装置10の仕向け先に応じて複数の無効化部それぞれに複数のセキュリティチップ142のいずれかを無効化させるか複数のセキュリティチップ142を無効化させるかを指定して、セキュリティチップ142の無効化を選択する操作部110と、を備える。

この制御装置10によれば、仕向け先毎の制御装置10を予め用意することなく、在庫コストを低減することができる。

[0048] (2) (1)に記載の制御装置10において、セキュリティチップ142(1) - 142(n)は、少なくともTPM、TPM準拠の専用チップで実装されたディスクリットTPM、マイコン内部のセキュリティ領域で実行

されるファームウェアTPM、又はTPM規格に準拠しないディスクリートリCのいずれかのセキュリティチップであってもよい。

そうすることで、制御装置10は、所望のセキュリティチップを使用することができる。

- [0049] (3) (1)又は(2)に記載の制御装置10において、無効化部はヒューズ141(1)－141(n)であり、暗号化装置部140は、仕向け先に対応するセキュリティチップ142(1)以外の無効化対象のセキュリティチップ142(j)(j≠i)を無効化するようにヒューズ141(j)(j≠i)を動作させる加負荷回路を備えてもよい。

そうすることで、制御装置10は、無効化対象のセキュリティチップ142(j)(j≠i)を確実に切断することができる。

- [0050] (4) (3)に記載の制御装置10において、複数のセキュリティチップ142(1)－142(n)の各々の動作を制御する複数のセキュリティチップ制御ソフトウェア134(1)－134(n)を記憶する補助記憶装置部130と、ヒューズ141(1)－141(n)により少なくとも1つの無効化対象のセキュリティチップ142が無効化された場合、無効化されたセキュリティチップ142に対応するセキュリティチップ制御ソフトウェア134を補助記憶装置部130から削除する演算部101とを、を備えてもよい。

そうすることで、制御装置10は、ハッキングされるリスクを減らすことができる。

- [0051] (5) (4)に記載の制御装置10において、制御装置10の起動時に、無効化対象のセキュリティチップ142(j)(j≠i)全てが無効化されているか否かを判定する起動時チェック処理部をさらに備え、演算部101は、起動時チェック処理部により無効化対象のセキュリティチップ142(j)(j≠i)全てが無効化されていないと判定された場合、無効化対象のセキュリティチップ142(j)(j≠i)全てが無効化されていないことを示すアラートを出力してもよい。

そうすることで、制御装置 10 は、ユーザにより制御装置 10 が使用可能となる前に、無効化対象のセキュリティチップ 142 (j) (j ≠ i) 全てを確実に無効化することができる。

[0052] (6) (5) に記載の制御装置 10 において、加負荷回路は、起動時チェック処理部により無効化対象のセキュリティチップ 142 (j) (j ≠ i) 全てが無効化されたと判定された場合、無効化処理を行わない誤作動防止機能を有してもよい。

そうすることで、制御装置 10 は、無効化対象のセキュリティチップ 142 全てを安全に無効化することができる。

[0053] (7) (4) から (6) のいずれかに記載の制御装置 10 において、演算部 101 は、制御装置 10 の仕向け先を補助記憶装置部 130 に記憶し、操作部 110 が補助記憶装置部 130 に記憶された仕向け先と異なる仕向け先を受け付けた場合、補助記憶装置部 130 に記憶された仕向け先と異なることを示すアラートを出力してもよい。

そうすることで、制御装置 10 は、機械メーカーの設計者等が一度設定した仕向け先を再度仕向け先を変えようとした場合、既に仕向け先が設定されている旨を機械メーカーの設計者等に通知することができる。

符号の説明

[0054] 10 制御装置
100 制御部
101 演算部
110 操作部
120 主記憶装置部
130 補助記憶装置部
131 既存ソフトウェア領域
132 セキュリティ領域
134 (1) - 134 (n) セキュリティチップ制御ソフトウェア
135 起動時チェック処理プログラム

1 4 0 暗号化装置部

1 4 1 (1) - 1 4 1 (n) ヒューズ

1 4 2 (1) - 1 4 2 (n) セキュリティチップ

SW (1) - SW (n)、1 4 4 スイッチ

請求の範囲

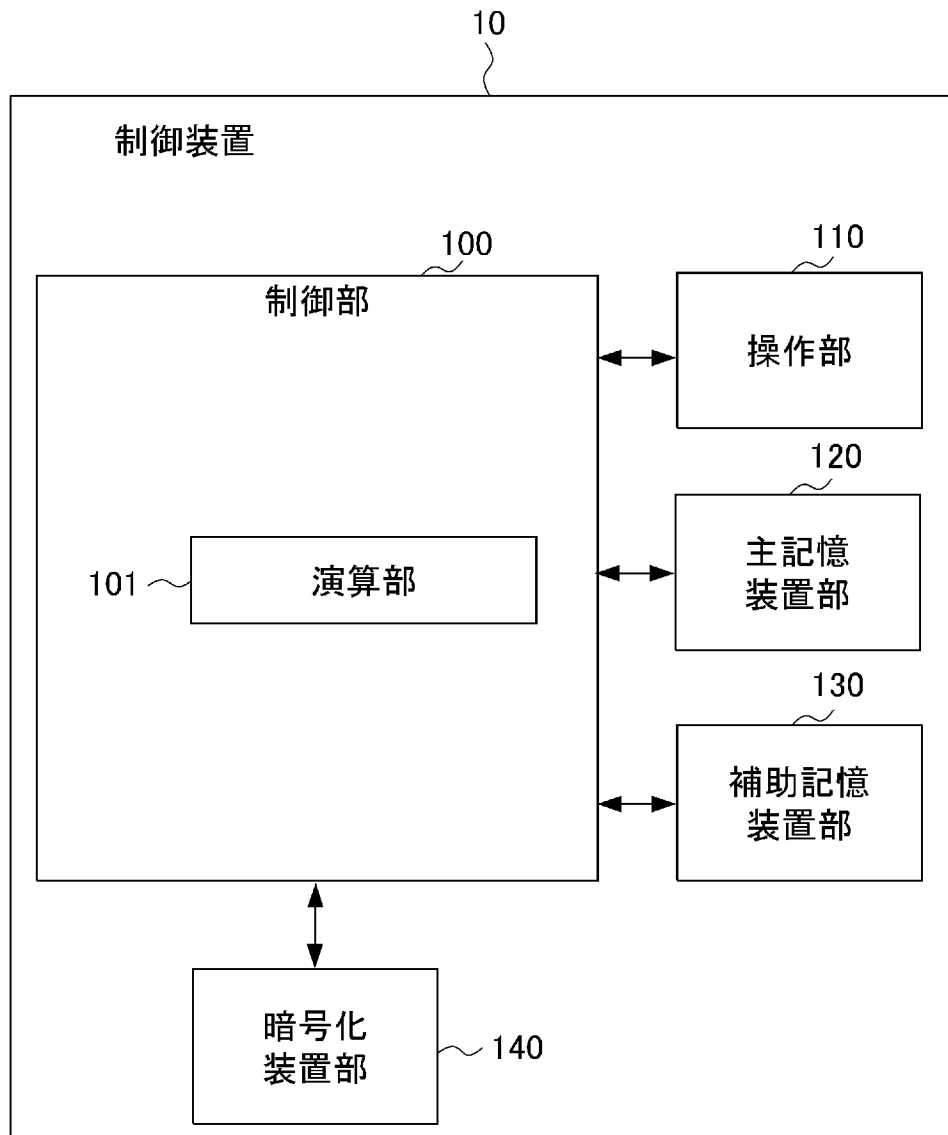
- [請求項1] 産業機械を制御し暗号化部を含む制御装置であって、
複数の仕向け先毎に対応した複数の前記暗号化部と複数の前記暗号化部のいずれかを無効化するもしくは複数の前記暗号化部を無効化する複数の無効化部とを含む暗号化装置部と、
前記制御装置の仕向け先に応じて前記複数の無効化部それぞれに複数の前記暗号化部のいずれかを無効化させるか複数の前記暗号化部を無効化させるかを指定して、暗号化部の無効化を選択する操作部と、
を備える制御装置。
- [請求項2] 前記暗号化部は、少なくともTPM (Trusted Platform Module)、TPM準拠の専用チップで実装されたディスクリットTPM、マイコン内部のセキュリティ領域で実行されるファームウェアTPM、又はTPM規格に準拠しないディスクリットICのいずれかのセキュリティチップである、請求項1に記載の制御装置。
- [請求項3] 前記無効化部はヒューズであり、
前記暗号化装置部は、
前記仕向け先に対応する暗号化部以外の無効化対象の暗号化部を無効化するように前記無効化部を動作させる加負荷回路を備える、請求項1又は請求項2に記載の制御装置。
- [請求項4] 前記複数の暗号化部の各々の動作を制御する複数の制御ソフトウェアを記憶する補助記憶装置部と、
前記無効化部により少なくとも1つの無効化対象の暗号化部が無効化された場合、無効化された前記無効化対象の暗号化部に対応する制御ソフトウェアを前記補助記憶装置部から削除する演算部と、を備える、請求項3に記載の制御装置。
- [請求項5] 前記制御装置の起動時に、前記無効化対象の暗号化部全てが無効化されているか否かを判定する起動時チェック処理部をさらに備え、

前記演算部は、前記起動時チェック処理部により前記無効化対象の暗号化部全てが無効化されていないと判定された場合、前記無効化対象の暗号化部全てが無効化されていないことを示すアラートを出力する、請求項 4 に記載の制御装置。

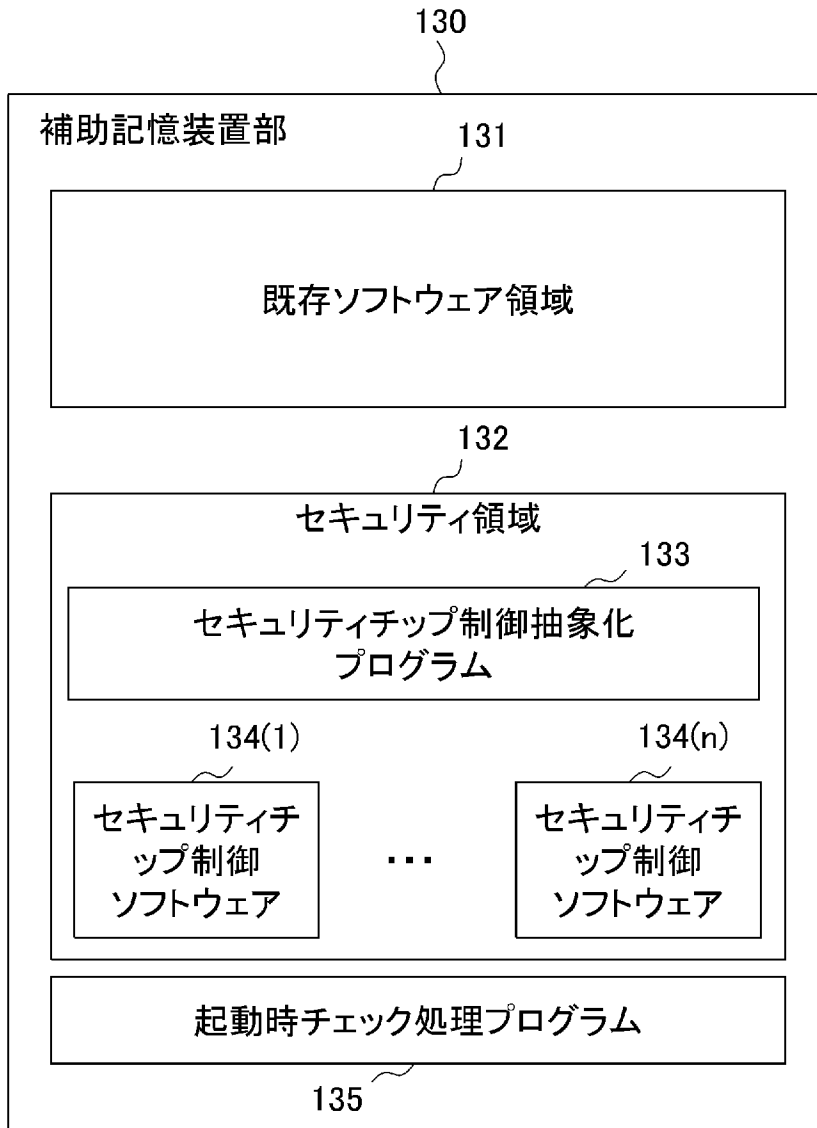
[請求項6] 前記加負荷回路は、前記起動時チェック処理部により前記無効化対象の暗号化部全てが無効化されたと判定された場合、無効化処理を行わない誤作動防止機能を有する、請求項 5 に記載の制御装置。

[請求項7] 前記演算部は、前記制御装置の仕向け先を前記補助記憶装置部に記憶し、前記操作部が前記補助記憶装置部に記憶された仕向け先と異なる仕向け先を受け付けた場合、前記補助記憶装置部に記憶された仕向け先と異なることを示すアラートを出力する、請求項 4 から請求項 6 のいずれか 1 項に記載の制御装置。

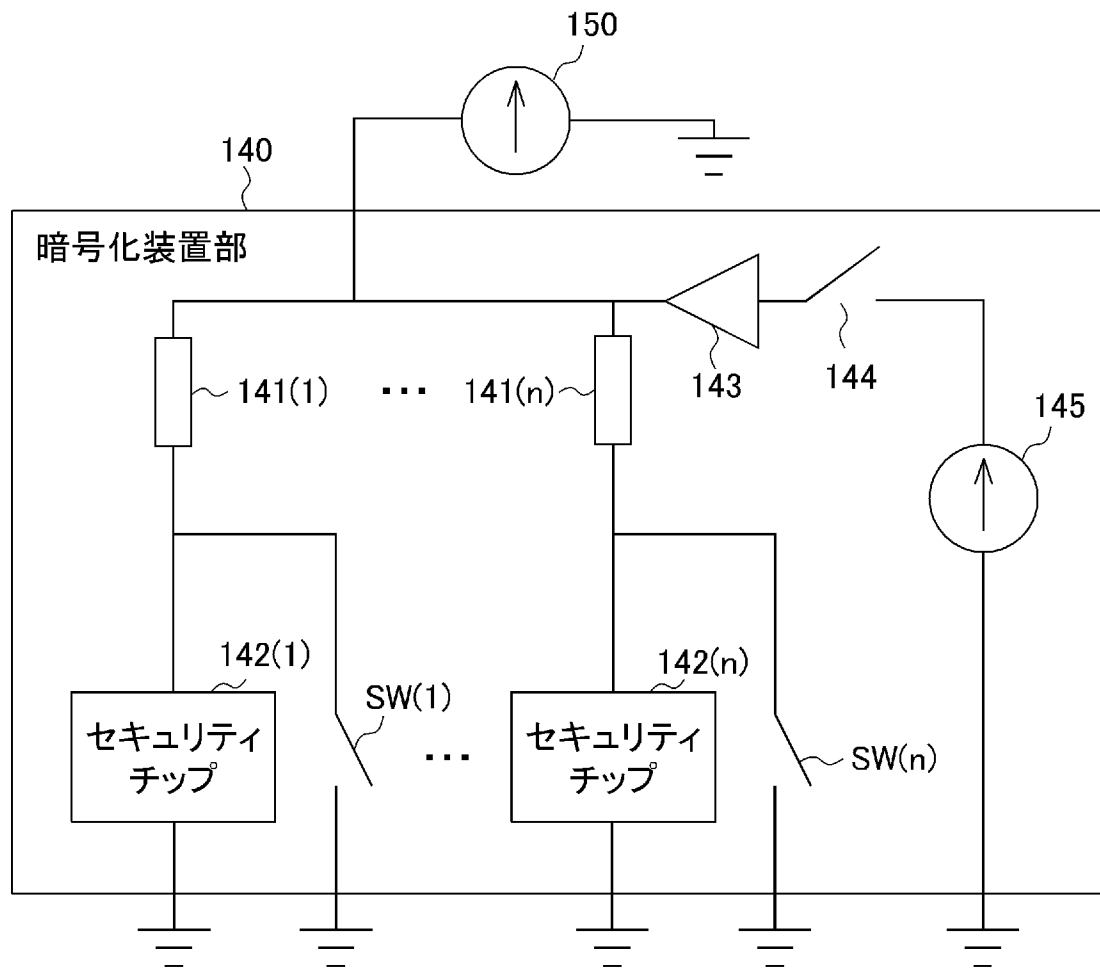
[図1]



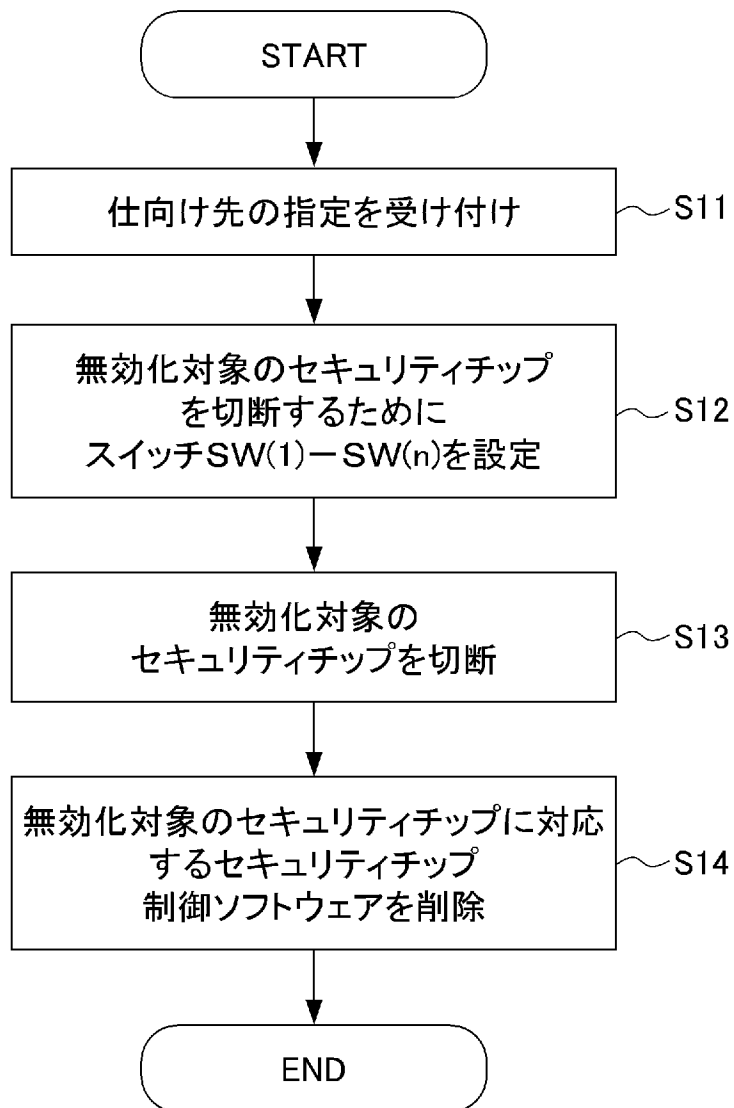
[図2]



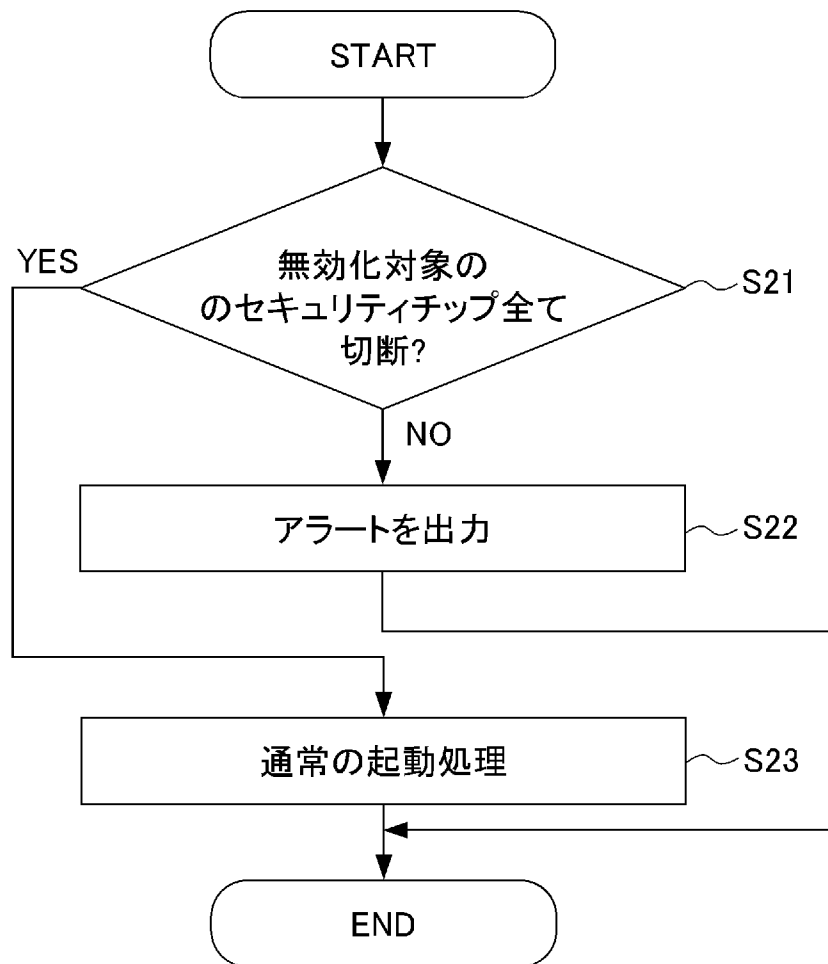
[図3]



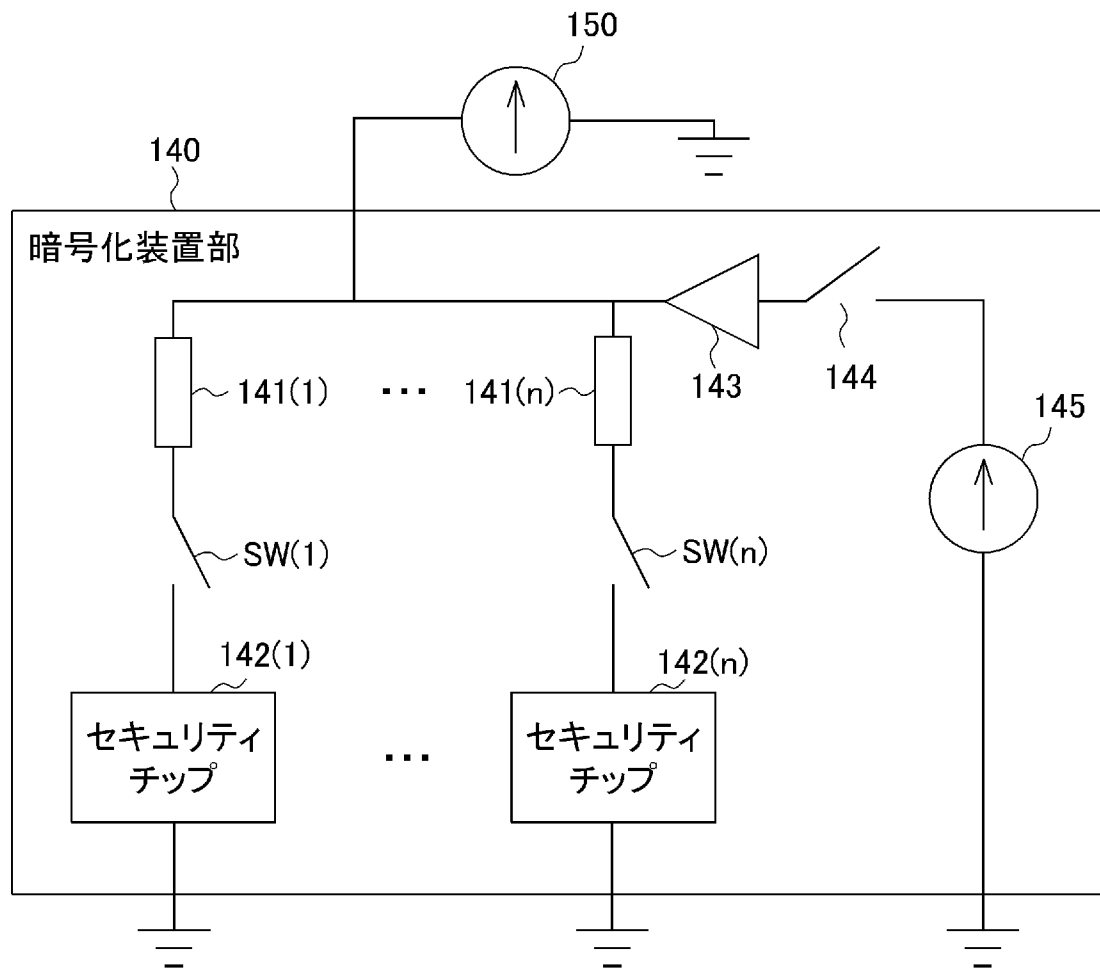
[図4]



[図5]



[図6]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2021/023913

A. CLASSIFICATION OF SUBJECT MATTER

G05B 19/18 (2006.01) i; G05B 19/414 (2006.01) i; G06F 21/60 (2013.01) i
FI: G05B19/18 X; G06F21/60 320; G05B19/414 Q

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)

G05B19/18; G05B19/414; G06F21/60

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.
A	JP 2010-98367 A (SONY CORP.) 30 April 2010 (2010-04-30) claim 1	1-7
P, A	WO 2021/019637 A1 (OMRON CORP.) 04 February 2021 (2021-02-04) claim 1	1-7

☐ 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	"I" 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 19 August 2021 (19.08.2021)	Date of mailing of the international search report 07 September 2021 (07.09.2021)
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/JP2021/023913

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
JP 2010-98367 A	30 Apr. 2010	US 2010/0180118 A1 claim 1 EP 2182461 A1 CN 101727603 A (Family: none)	
WO 2021/019637 A1	04 Feb. 2021		

A. 発明の属する分野の分類（国際特許分類（IPC）） G05B 19/18(2006.01)i; G05B 19/414(2006.01)i; G06F 21/60(2013.01)i FI: G05B19/18 X; G06F21/60 320; G05B19/414 Q														
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）） G05B19/18; G05B19/414; G06F21/60														
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>			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													
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）														
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												
A	JP 2010-98367 A（ソニー株式会社）30.04.2010（2010 - 04 - 30） 請求項1	1-7												
P, A	WO 2021/019637 A1（オムロン株式会社）04.02.2021（2021 - 02 - 04） 請求項1	1-7												
☐ 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>* 参考文献のカテゴリー</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>			* 参考文献のカテゴリー	“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	
* 参考文献のカテゴリー	“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 19.08.2021	国際調査報告の発送日 07.09.2021													
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） 牧 初 3U 9064 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/JP2021/023913

引用文献			公表日	パテントファミリー文献			公表日
JP	2010-98367	A	30.04.2010	US	2010/0180118	A1	
				claim1			
				EP	2182461	A1	
				CN	101727603	A	
WO	2021/019637	A1	04.02.2021	(ファミリーなし)			