(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
2020年9月17日(17.09.2020)

WIPO | PCT

(10) 国際公開番号
WO 2020/184186 A1

(51) 国際特許分類:
G05B 19/05 (2006.01) *H04L 9/08* (2006.01)
G05B 19/048 (2006.01)

(21) 国際出願番号： PCT/JP2020/007796

(22) 国際出願日： 2020年2月26日(26.02.2020)

(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 2019-046723 2019年3月14日(14.03.2019) JP

(71) 出願人: オムロン株式会社 (**OMRON CORPORATION**) [JP/JP]; 〒6008530 京都府京都市下京区塩小路通堀川東入南不動堂町８０１番地 Kyoto (JP).

(72) 発明者: 川合 功 (**KAWAI, Ko**); 〒6008530 京都府京都市下京区塩小路通堀川東入南不動堂町８０１番地 オムロン株式会社内 Kyoto (JP).

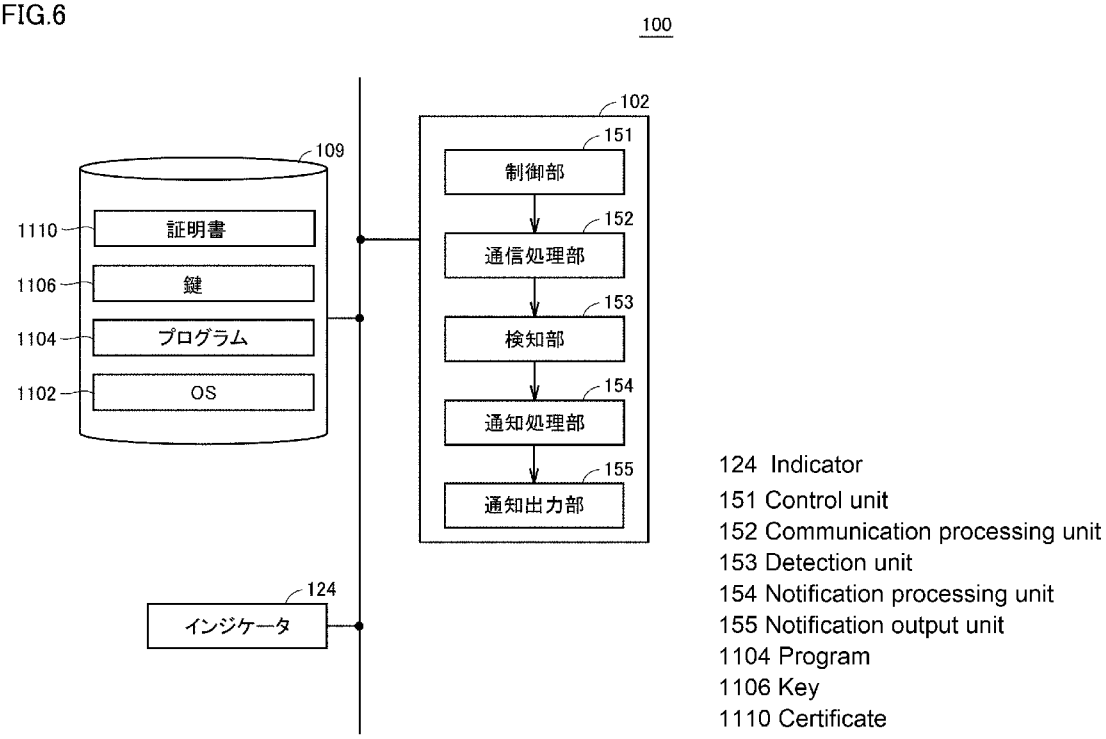
(74) 代理人: 特許業務法人深見特許事務所 (**FUKAMI PATENT OFFICE, P.C.**); 〒5300005 大阪府大阪市北区中之島三丁目２番４号 中之島フェスティバルタワー・ウエスト Osaka (JP).

(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, HR, HU, ID, IL, IN, IR, IS, JO, 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,

(54) **Title:** CONTROL DEVICE AND CONTROL SYSTEM

(54) 発明の名称： 制御装置および制御システム

FIG.6



(57) **Abstract:** This control device (1) includes: a control unit (151) configured to execute a control operation for controlling an object to be controlled; a communication unit (152) that executes processing for secure communication using a certificate; a detection unit (153) that detects that the certificate is about to expire; and a notification unit (124) that executes notification that the certificate is about to expire.

WO 2020/184186 A1

[続葉有]

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))

(57) 要約: 制御装置(1)は、制御対象を制御するための制御演算を実行するように構成された制御部(151)と、証明書を利用したセキュア通信のための処理を実行する通信部(152)と、証明書の寿命が近づいていることを検知する検知部(153)と、証明書の寿命が近づいていることを通知する通知部(124)とを含む。

明　細　書

発明の名称 ： 制御装置および制御システム

技術分野

[0001] 本発明は、制御対象を制御する制御装置、およびその制御装置を含む制御システムに関する。

背景技術

[0002] 通信装置の間でのセキュア通信のため、暗号通信が従来から用いられている。たとえば国際公開第２０１６／１４７５６８号（特許文献１）は、事前共有鍵を用いた暗号通信を開示する。

[0003] 公開鍵電子証明書が失効した場合、その失効した公開鍵電子証明書が更新されるまで、通信装置の間では暗号通信ができない。国際公開第２０１６／１４７５６８号に開示された通信装置は、相手方通信装置の公開鍵電子証明書が失効しているか否かを判定する失効判定部と、失効判定部によって公開鍵電子証明書が失効していると判定された場合に、公開鍵電子証明書の失効通知を相手方通信装置へ送信する失効通知部とを備える。

先行技術文献

特許文献

[0004] 特許文献1：国際公開第２０１６／１４７５６８号

発明の概要

発明が解決しようとする課題

[0005] 各種の製造設備および各設備に配置される各種装置の制御に、ＰＬＣ（プログラマブルロジックコントローラ）などの制御装置が用いられている。近年のＩＣＴ（Information and Communication Technology）の進歩に伴って、制御装置も様々な外部装置とネットワークで接続されるとともに、制御装置において実行される処理も高度化している。このようなネットワーク化あるいはインテリジェント化に伴って、制御装置がさまざまな脅威にさらされることが想定される。したがって想定される脅威から制御装置を守るため

の方策が必要である。

[0006] たとえば、制御装置の通信に上述のような暗号通信を適用することが考えられる。この場合、制御装置には電子証明書が格納される。しかし、電子証明書には期限がある。電子証明書が失効すると、暗号通信を行うことができない。

[0007] 制御装置の電子証明書が有効であるか否かを常時監視することは容易ではない。そのため国際公開第２０１６／１４７５６８号に開示されるように、公開鍵電子証明書の失効通知を相手方通信装置へ送信することが考えられる。しかし、この場合にも、ユーザは通知を受けるまでは、証明書が失効したことを知ることができない。

[0008] 本発明の目的は、制御装置に格納された証明書の寿命を、ユーザが容易に把握できるようにすることである。

課題を解決するための手段

[0009] 本開示の一例では、制御装置は、制御対象を制御するための制御演算を実行するように構成された制御部と、証明書を利用したセキュア通信のための処理を実行する通信部と、証明書の寿命が近づいていることを検知する検知部と、証明書の寿命が近づいていることを通知する通知部とを含む。

[0010] 上記によれば、制御装置に格納された証明書の寿命を、ユーザが容易に把握できる。したがってユーザは、証明書の寿命の前に証明書を更新することができる。「証明書の寿命」とは、証明書が使用できない状態を意味する。たとえば証明書の有効期限が到来することにより証明書が失効した状態が「証明書の寿命」に対応する。暗号寿命により証明書が使用できない状態も「証明書の寿命」に含まれうる。

[0011] 好ましくは、証明書の寿命は証明書の有効期限であり、通知部は、証明書が失効する前の一定のタイミングにおいて、証明書の有効期限が近づいていることを通知する。

[0012] 上記によれば、証明書が一定期間後に失効することをユーザに予告することができる。これにより、ユーザが証明書を更新するための時間を確保する

ことができる。

[0013] 好ましくは、制御装置は、筐体を含む。通知部は、筐体に設けられ、寿命が近づいていることを光により通知するインジケータを含む。

[0014] 上記によれば、ユーザが制御装置を見ることにより、証明書の寿命が近づいていることを確認できる。ユーザは証明書の寿命を確認するためのツールを用意する必要がない。したがって、ユーザの利便性を向上させることができる。

[0015] 好ましくは、通知部は、寿命が近づいていることを通知するための音を発生させる音声出力部を含む。

[0016] 上記によれば、ユーザは、制御装置から発生する音により、証明書の寿命が近づいていることを確認できる。ユーザは証明書の寿命を確認するためのツールを用意する必要がない。したがって、ユーザの利便性を向上させることができる。

[0017] 好ましくは、通知部は、寿命が近づいていることをメールにより通知する。

上記によれば、ユーザは、制御装置から発生する光あるいは音だけでなく、メールのメッセージからも証明書の寿命が近づいていることを確認できる。

[0018] 本開示の一例では、制御システムは、上記のいずれかに記載の制御装置と、証明書が寿命に達する前の通知のタイミングを制御装置に対して設定する設定装置とを備える。

[0019] 上記によれば制御装置に格納された証明書の寿命を、ユーザが容易に把握できる。さらに、ユーザの所望のタイミングで、証明書の寿命が近づいていることを通知することができる。

[0020] 好ましくは、制御装置に複数の証明書が格納されている場合、設定装置は、複数の証明書の有効期限を一括して表示する。

[0021] 上記によれば、制御装置に格納された複数の証明書の各々の有効期限を、ユーザが容易に把握できるので、ユーザの利便性を向上させることができる

。

[0022] 本開示の一例では、制御システムは、上記のいずれかに記載の制御装置と、制御装置との間で通信を行う通信装置とを備え、制御装置は、失効期限の前に新しい証明書を受け付けて、通信装置に更新リクエストを送信し、通信装置が新しい証明書を承認すると、古い証明書を破棄することで証明書を更新する。

[0023] 上記によれば、セキュア通信により制御装置に格納された証明書を更新することができる。

発明の効果

[0024] 本発明によれば、制御装置に格納された電子証明書の寿命を、ユーザが容易に把握できる。

図面の簡単な説明

[0025] [図1]本実施の形態に係る制御装置の構成例を示す外観図である。

[図2]本実施の形態に従う制御装置を構成する制御ユニットのハードウェア構成例を示す模式図である。

[図3]本実施の形態に従う制御装置１を構成するセキュリティユニットのハードウェア構成例を示す模式図である。

[図4]本実施の形態に従う制御装置１を構成するセーフティユニットのハードウェア構成例を示す模式図である。

[図5]本実施の形態に従う制御装置を含む制御システムの典型例を示す模式図である。

[図6]本実施の形態に従う制御ユニットが備える機能構成例を示す模式図である。

[図7]ＯＰＣ－ＵＡ通信システムを示した模式図である。

[図8]証明書の有効期限の通知のための制御装置の構成例を示した図である。

[図9]証明書の有効期限の通知のための制御装置の別の構成例を示した図である。

[図10]通知設定の例を示した図である。

[図11]通知設定の他の例を示した図である。

[図12]ＯＰＣ－ＵＡサーバおよびＯＰＣ－ＵＡクライアントの通常運転時の状態を説明するための模式図である。

[図13]証明書の更新処理における、新証明書の発行ステップを説明するための図である。

[図14]証明書の更新処理における、新証明書の送信ステップおよび更新リクエストの通知ステップを説明するための図である。

[図15]証明書の更新処理における新証明書の承認ステップを説明するための図である。

[図16]証明書の更新処理における、古い証明書の破棄ステップを説明するための図である。

[図17]複数のコアを有するプロセッサの模式図である。

発明を実施するための形態

[0026] 本発明の実施の形態について、図面を参照しながら詳細に説明する。なお、図中の同一または相当部分については、同一符号を付してその説明は繰り返さない。

[0027] ＜Ａ．制御装置１＞

まず、本実施の形態に従う制御装置１の構成について説明する。

[0028] 図１は、本実施の形態に係る制御装置１の構成例を示す外観図である。図１を参照して、制御装置１は、制御ユニット１００と、セキュリティユニット２００と、セーフティユニット３００と、１または複数の機能ユニット４００と、電源ユニット４５０とを含む。

[0029] 制御ユニット１００とセキュリティユニット２００との間は、任意のデータ伝送路（例えば、ＰＣＩ　Ｅｘｐｒｅｓｓ（登録商標）あるいはイーサネット（登録商標）など）を介して接続されている。制御ユニット１００とセーフティユニット３００および１または複数の機能ユニット４００との間は、図示しない内部バスを介して接続されている。

[0030] 制御ユニット１００は、制御装置１において中心的な処理を実行する。制

御ユニット１００は、任意に設計された要求仕様に従って、制御対象を制御するための制御演算を実行する。セーフティユニット３００で実行される制御演算との対比で、制御ユニット１００で実行される制御演算を「標準制御」とも称す。図１に示す構成例において、制御ユニット１００は、１または複数の通信ポートを有している。制御ユニット１００は、標準制御プログラムに従って標準制御を実行する処理実行部に相当する。

[0031] セキュリティユニット２００は、制御ユニット１００に接続され、制御装置１に対するセキュリティ機能を担当する。図１に示す構成例において、セキュリティユニット２００は、１または複数の通信ポートを有している。セキュリティユニット２００が提供するセキュリティ機能の詳細については、後述する。

[0032] セーフティユニット３００は、制御ユニット１００とは独立して、制御対象に関するセーフティ機能を実現するための制御演算を実行する。セーフティユニット３００で実行される制御演算を「セーフティ制御」とも称す。通常、「セーフティ制御」は、ＩＥＣ　６１５０８などに規定されたセーフティ機能を実現するための要件を満たすように設計される。「セーフティ制御」は、設備や機械などによって人の安全が脅かされることを防止するための処理を総称する。

[0033] 機能ユニット４００は、制御装置１による様々な制御対象に対する制御を実現するための各種機能を提供する。機能ユニット４００は、典型的には、Ｉ／Ｏユニット、セーフティＩ／Ｏユニット、通信ユニット、モーションコントローラユニット、温度調整ユニット、パルスカウンタユニットなどを包含し得る。Ｉ／Ｏユニットとしては、例えば、デジタル入力（ＤＩ）ユニット、デジタル出力（ＤＯ）ユニット、アナログ出力（ＡＩ）ユニット、アナログ出力（ＡＯ）ユニット、パルスキャッチ入力ユニット、および、複数の種類を混合させた複合ユニットなどが挙げられる。セーフティＩ／Ｏユニットは、セーフティ制御に係るＩ／Ｏ処理を担当する。

[0034] 電源ユニット４５０は、制御装置１を構成する各ユニットに対して、所定

電圧の電源を供給する。

[0035] ＜Ｂ．各ユニットのハードウェア構成例＞

次に、本実施の形態に従う制御装置１を構成する各ユニットのハードウェア構成例について説明する。

[0036] （ｂ１：制御ユニット１００）

図２は、本実施の形態に従う制御装置１を構成する制御ユニット１００のハードウェア構成例を示す模式図である。図２を参照して、制御ユニット１００は、主たるコンポーネントとして、ＣＰＵ（Central Processing Unit）やＧＰＵ（Graphical Processing Unit）などのプロセッサ１０２と、チップセット１０４と、主記憶装置１０６と、二次記憶装置１０８と、通信コントローラ１１０と、ＵＳＢ（Universal Serial Bus）コントローラ１１２と、メモリカードインターフェイス１１４と、ネットワークコントローラ１１６，１１８，１２０と、内部バスコントローラ１２２と、インジケータ１２４とを含む。

[0037] プロセッサ１０２は、二次記憶装置１０８に格納された各種プログラムを読み出して、主記憶装置１０６に展開して実行することで、標準制御に係る制御演算、および、後述するような各種処理を実現する。プロセッサ１０２としては、複数のコアを有する構成を採用してもよいし、プロセッサ１０２を複数配置してもよい。すなわち、制御ユニット１００は、１または複数のプロセッサ１０２、および／または、１または複数のコアを有するプロセッサ１０２を有している。チップセット１０４は、プロセッサ１０２と各コンポーネントとの間のデータの遣り取りを仲介することで、制御ユニット１００全体としての処理を実現する。

[0038] 二次記憶装置１０８には、システムプログラムに加えて、システムプログラムが提供する実行環境上で動作する制御プログラムが格納される。二次記憶装置１０８には、暗号通信のための鍵（秘密鍵や公開鍵）および証明書が格納されていてもよい。

[0039] 通信コントローラ１１０は、セキュリティユニット２００との間のデータ

の遣り取りを担当する。通信コントローラ１１０としては、例えば、ＰＣＩＥｘｐｒｅｓｓあるいはイーサネットなどに対応する通信チップを採用できる。

[0040] ＵＳＢコントローラ１１２は、ＵＳＢ接続を介して任意の情報処理装置との間のデータの遣り取りを担当する。

[0041] メモリカードインターフェイス１１４は、メモリカード１１５を着脱可能に構成されており、メモリカード１１５に対して制御プログラムや各種設定などのデータを書込み、あるいは、メモリカード１１５から制御プログラムや各種設定などのデータを読出すことが可能になっている。

[0042] ネットワークコントローラ１１６，１１８，１２０の各々は、ネットワークを介した任意のデバイスとの間のデータの遣り取りを担当する。ネットワークコントローラ１１６，１１８，１２０は、ＥｔｈｅｒＣＡＴ（登録商標）、ＥｔｈｅｒＮｅｔ／ＩＰ（登録商標）、ＤｅｖｉｃｅＮｅｔ（登録商標）、ＣｏｍｐｏＮｅｔ（登録商標）などの産業用ネットワークプロトコルを採用してもよい。

[0043] 内部バスコントローラ１２２は、制御装置１を構成するセーフティユニット３００や１または複数の機能ユニット４００との間のデータの遣り取りを担当する。内部バスには、メーカ固有の通信プロトコルを用いてもよいし、いずれかの産業用ネットワークプロトコルと同一あるいは準拠した通信プロトコルを用いてもよい。

[0044] インジケータ１２４は、制御ユニット１００の動作状態などを通知するものであり、ユニット表面に配置された１または複数のＬＥＤなどで構成される。インジケータ１２４は、証明書の寿命が近づいていることを通知する通知部に相当する。したがって、インジケータ１２４は、証明書の寿命が近いことをユーザに予告する予告手段でもある。

[0045] 図２には、プロセッサ１０２がプログラムを実行することで必要な機能が提供される構成例を示したが、これらの提供される機能の一部または全部を、専用のハードウェア回路（例えば、ＡＳＩＣ（Application Specific In

tegrated Circuit）またはＦＰＧＡ（Field-Programmable Gate Array）など）を用いて実装してもよい。あるいは、制御ユニット１００の主要部を、汎用的なアーキテクチャに従うハードウェア（例えば、汎用パソコンをベースとした産業用パソコン）を用いて実現してもよい。この場合には、仮想化技術を用いて、用途の異なる複数のＯＳ（Operating System）を並列的に実行させるとともに、各ＯＳ上で必要なアプリケーションを実行させるようにしてもよい。

[0046] （ｂ２：セキュリティユニット２００）

図３は、本実施の形態に従う制御装置１を構成するセキュリティユニット２００のハードウェア構成例を示す模式図である。図３を参照して、セキュリティユニット２００は、主たるコンポーネントとして、ＣＰＵやＧＰＵなどのプロセッサ２０２と、チップセット２０４と、主記憶装置２０６と、二次記憶装置２０８と、通信コントローラ２１０と、ＵＳＢコントローラ２１２と、メモリカードインターフェイス２１４と、ネットワークコントローラ２１６，２１８と、インジケータ２２４とを含む。

[0047] プロセッサ２０２は、二次記憶装置２０８に格納された各種プログラムを読み出して、主記憶装置２０６に展開して実行することで、後述するような各種セキュリティ機能を実現する。チップセット２０４は、プロセッサ２０２と各コンポーネントとの間のデータの遣り取りを仲介することで、セキュリティユニット２００全体としての処理を実現する。

[0048] 二次記憶装置２０８には、システムプログラムに加えて、システムプログラムが提供する実行環境上で動作するセキュリティシステムプログラムが格納される。二次記憶装置２０８には、暗号通信のための鍵（秘密鍵や公開鍵）および証明書が格納されていてもよい。

[0049] 通信コントローラ２１０は、制御ユニット１００との間のデータの遣り取りを担当する。通信コントローラ２１０としては、制御ユニット１００に通信コントローラ２１０と同様に、例えば、ＰＣＩ Ｅｘｐｒｅｓｓあるいはイーサネットなどに対応する通信チップを採用できる。

[0050] ＵＳＢコントローラ２１２は、ＵＳＢ接続を介して任意の情報処理装置との間のデータの遣り取りを担当する。

[0051] メモリカードインターフェイス２１４は、メモリカード２１５を着脱可能に構成されており、メモリカード２１５に対して制御プログラムや各種設定などのデータを書込み、あるいは、メモリカード２１５から制御プログラムや各種設定などのデータを読出すことが可能になっている。

[0052] ネットワークコントローラ２１６，２１８の各々は、ネットワークを介した任意のデバイスとの間のデータの遣り取りを担当する。ネットワークコントローラ２１６，２１８は、イーサネットなどの汎用的なネットワークプロトコルを採用してもよい。

[0053] インジケータ２２４は、セキュリティユニット２００の動作状態などを通知するものであり、ユニット表面に配置された１または複数のＬＥＤなどで構成される。インジケータ２２４は、セキュリティユニット２００荷か苦悩された証明書の寿命が近づいていることを通知する通知部に相当する。したがって、インジケータ２２４は、証明書の寿命が近いことをユーザに予告する予告手段でもある。

[0054] 図３には、プロセッサ２０２がプログラムを実行することで必要な機能が提供される構成例を示したが、これらの提供される機能の一部または全部を、専用のハードウェア回路（例えば、ＡＳＩＣまたはＦＰＧＡなど）を用いて実装してもよい。あるいは、セキュリティユニット２００の主要部を、汎用的なアーキテクチャに従うハードウェア（例えば、汎用パソコンをベースとした産業用パソコン）を用いて実現してもよい。この場合には、仮想化技術を用いて、用途の異なる複数のＯＳを並列的に実行させるとともに、各ＯＳ上で必要なアプリケーションを実行させるようにしてもよい。

[0055] （ｂ３：セーフティユニット３００）

図４は、本実施の形態に従う制御装置１を構成するセーフティユニット３００のハードウェア構成例を示す模式図である。図４を参照して、セーフティユニット３００は、主たるコンポーネントとして、ＣＰＵやＧＰＵなどの

プロセッサ３０２と、チップセット３０４と、主記憶装置３０６と、二次記憶装置３０８と、メモリカードインターフェイス３１４と、内部バスコントローラ３２２と、インジケータ３２４とを含む。

[0056] プロセッサ３０２は、二次記憶装置３０８に格納された各種プログラムを読み出して、主記憶装置３０６に展開して実行することで、セーフティ制御に係る制御演算、および、後述するような各種処理を実現する。チップセット３０４は、プロセッサ３０２と各コンポーネントとの間のデータの遣り取りを仲介することで、セーフティユニット３００全体としての処理を実現する。

[0057] 二次記憶装置３０８には、システムプログラムに加えて、システムプログラムが提供する実行環境上で動作するセーフティプログラムが格納される。

[0058] メモリカードインターフェイス３１４は、メモリカード３１５を着脱可能に構成されており、メモリカード３１５に対してセーフティプログラムや各種設定などのデータを書込み、あるいは、メモリカード３１５からセーフティプログラムや各種設定などのデータを読出すことが可能になっている。

[0059] 内部バスコントローラ３２２は、内部バスを介した制御ユニット１００との間のデータの遣り取りを担当する。

[0060] インジケータ３２４は、セーフティユニット３００の動作状態などを通知するものであり、ユニット表面に配置された１または複数のＬＥＤなどで構成される。

[0061] 図４には、プロセッサ３０２がプログラムを実行することで必要な機能が提供される構成例を示したが、これらの提供される機能の一部または全部を、専用のハードウェア回路（例えば、ＡＳＩＣまたはＦＰＧＡなど）を用いて実装してもよい。あるいは、セーフティユニット３００の主要部を、汎用的なアーキテクチャに従うハードウェア（例えば、汎用パソコンをベースとした産業用パソコン）を用いて実現してもよい。この場合には、仮想化技術を用いて、用途の異なる複数のＯＳを並列的に実行させるとともに、各ＯＳ上で必要なアプリケーションを実行させるようにしてもよい。

[0062] ＜Ｃ．制御システム１０＞

次に、本実施の形態に従う制御装置１を含む制御システム１０の典型例について説明する。図５は、本実施の形態に従う制御装置１を含む制御システム１０の典型例を示す模式図である。

[0063] 一例として、図５に示す制御システム１０は、２つのライン（ラインＡおよびラインＢ）を制御対象とする。典型的には、各ラインは、ワークを搬送するコンベアに加えて、コンベア上のワークに対して任意の物理的作用を与えることが可能なロボットが配置されているとする。

[0064] ラインＡおよびラインＢのそれぞれに制御ユニット１００が配置されている。ラインＡを担当する制御ユニット１００に加えて、セキュリティユニット２００およびセーフティユニット３００が制御装置１を構成する。なお、説明の便宜上、図５には、機能ユニット４００および電源ユニット４５０の記載を省略している。

[0065] 制御装置１のセキュリティユニット２００は、通信ポート２４２（図３のネットワークコントローラ２１６）を介して第１ネットワーク２に接続されている。第１ネットワーク２には、サポート装置６００およびＳＣＡＤＡ（Supervisory Control And Data Acquisition）装置７００が接続されているとする。第１ネットワーク２には、イーサネットあるいはＯＰＣ－ＵＡ（Object Linking and Embedding for Process Control Unified Architecture）などを採用することができる。

[0066] サポート装置６００は、少なくとも制御ユニット１００にアクセス可能になっており、制御装置１に含まれる各ユニットで実行されるプログラムの作成、デバッグ、各種パラメータの設定などの機能をユーザへ提供する。サポート装置６００には開発等の目的のためのツールがインストールされていてもよい。ツールはたとえばオムロン社製の「Ｓｙｓｍａｃ　Ｓｔｕｄｉｏ」である。

[0067] ＳＣＡＤＡ装置７００は、制御装置１での制御演算によって得られる各種情報をオペレータへ提示するとともに、オペレータからの操作に従って、制

御装置１に対して内部コマンドなどを生成する。ＳＣＡＤＡ装置７００は、制御装置１が扱うデータを収集する機能も有している。

[0068] 制御装置１の制御ユニット１００は、通信ポート１４２（図２のネットワークコントローラ１１６）を介して第２ネットワーク４に接続されている。第２ネットワーク４には、ＨＭＩ（Human Machine Interface）８００およびデータベース９００が接続されているとする。

[0069] ＨＭＩ８００は、パーソナルコンピュータにより実現可能である。ＨＭＩ８００は、制御装置１での制御演算によって得られる各種情報をオペレータへ提示するとともに、オペレータからの操作に従って、制御装置１に対して内部コマンドなどを生成する。ＨＭＩ８００は、制御装置１との暗号通信のための証明書を格納してもよい。ＨＭＩ８００は、証明書が寿命に達する前の通知のタイミングを制御装置１に対して設定する設定装置である。

[0070] ＨＭＩ８００は、ＦＡの保守者が携帯可能に構成され得る。データベース９００は、制御装置１から送信される各種データ（例えば、各ワークから計測されたトレーサビリティに関する情報など）を収集する。

[0071] 制御装置１の制御ユニット１００は、通信ポート１４４（図２のネットワークコントローラ１１８）を介して、１または複数のフィールドデバイス５００と接続されている。フィールドデバイス５００は、制御対象から制御演算に必要な各種情報を収集するセンサや検出器、および、制御対象に対して何らかの作用を与えるアクチュエータなどを含む。図５に示す例では、フィールドデバイス５００は、ワークに対して何らかの外的な作用を与えるロボット、ワークを搬送するコンベヤ、フィールドに配置されたセンサやアクチュエータとの間で信号を遣り取りするＩ／Ｏユニットなどを含む。

[0072] 同様に、ラインＢを担当する制御ユニット１００についても同様に、通信ポート１４４（図２のネットワークコントローラ１１８）を介して、１または複数のフィールドデバイス５００と接続されている。

[0073] ここで、制御装置１の機能面に着目すると、制御ユニット１００は、標準制御に係る制御演算を実行する処理実行部である制御エンジン１５０と、外

部装置との間でデータを遣り取りする情報エンジン１６０とを含む。セキュリティユニット２００は、後述するようなセキュリティ機能を実現するためのセキュリティエンジン２５０を含む。セーフティユニット３００は、セーフティ制御に係る制御演算を実行する処理実行部であるセーフティエンジン３５０を含む。

[0074] 各エンジンは、各ユニットのプロセッサなどの任意のハードウェア要素または各種プログラムなどの任意のソフトウェア要素、あるいは、それら要素の組合せによって実現される。各エンジンは任意の形態で実装できる。

[0075] さらに、制御装置１は、エンジン同士の遣り取りを仲介するブローカー１７０を含む。ブローカー１７０の実体は、制御ユニット１００およびセキュリティユニット２００の一方または両方に配置してもよい。

[0076] 制御エンジン１５０は、制御対象を制御するための制御演算の実行に必要な変数テーブルおよびファンクションブロック（ＦＢ）などを保持している。変数テーブルに格納される各変数は、Ｉ／Ｏリフレッシュ処理により、フィールドデバイス５００から取得された値で周期的に収集されるとともに、フィールドデバイス５００へ各値が周期的に反映される。制御エンジン１５０での制御演算のログはログデータベース１８０に格納されてもよい。

[0077] 情報エンジン１６０は、制御ユニット１００が保持するデータ（変数テーブルで保持される変数値）に対して任意の情報処理を実行する。典型的には、情報エンジン１６０は、制御ユニット１００が保持するデータを周期的にデータベース９００などへ送信する処理を含む。このようなデータの送信には、ＳＱＬなどが用いられる。

[0078] セキュリティエンジン２５０は、制御装置１に発生する不正侵入の検知、検知された不正侵入に応じた処理、インシデントの発生有無判断、発生したインシデントに応じた処理などを実行する。セキュリティエンジン２５０の挙動は、セキュリティ情報２６０として保存される。

[0079] セキュリティエンジン２５０は、セキュリティに関する何らかのイベントが発生したこと、あるいは発生しているセキュリティに関するイベントのレ

ベルなどを、インジケータ２２４で通知する。

[0080] セーフティエンジン３５０は、制御装置１において何らかの不正侵入が発生したか否かを検知する検知手段に相当する。セーフティエンジン３５０は、制御ユニット１００を介して、セーフティ制御に係る制御演算の実行に必要なセーフティＩ／Ｏ変数を取得および反映する。セーフティエンジン３５０でのセーフティ制御のログはログデータベース３６０に格納されてもよい。

[0081] ブローカー１７０は、例えば、セキュリティエンジン２５０が何らかのイベントを検知すると、制御エンジン１５０、情報エンジン１６０およびセーフティエンジン３５０の動作などを変化させる。

[0082] ＜Ｄ．制御ユニット１００の機能構成例＞

図６は、本実施の形態に従う制御ユニット１００が備える機能構成例を示す模式図である。図６を参照して、制御ユニット１００において、記憶部１０９（二次記憶装置１０８または主記憶装置１０６を含む）は、ＯＳ１１０２、プログラム１１０４、鍵１１０６および証明書１１１０を格納する。鍵１１０６は、たとえば秘密鍵、公開鍵等である。

[0083] プロセッサ１０２は、ＯＳ１１０２の元でプログラム１１０４を周期的に実行することにより、制御部１５１、通信処理部１５２、検知部１５３、通知処理部１５４および通知出力部１５５を実現する。

[0084] 制御部１５１は、制御対象を制御するための制御演算を実行する。したがって制御部１５１は、制御エンジン１５０の主要な部分である。通信処理部１５２は、証明書を利用したセキュア通信のための処理を実行するための通信部を実現する。

[0085] 検知部１５３は、証明書の寿命が近づいていることを検知する。たとえば検知部１５３は、証明書の有効期限を予め取得しておいて、現時点が有効期限前の一定期間内にあるかどうかを判定する。現時点が証明書の有効期限前の一定期間内にある場合に、検知部１５３は、証明書の有効期限が近づいていることを検知する。通知処理部１５４は、証明書の寿命が近づいているこ

とを通知するための処理を実行する。通知出力部１５５は、通知を出力するようにインジケータ１２４を含む通知部を制御する。

[0086] ＜Ｅ．暗号通信について＞

以下では本実施の形態に適用可能な規格としてＯＰＣ－ＵＡを例示する。ＯＰＣ－ＵＡは、産業オートメーション分野、およびその他業界における、安全で信頼性あるデータ交換を目的とした相互運用を行なうための標準規格である。ＯＰＣ－ＵＡにおけるセキュリティ対策としては、メッセージの盗聴の防止、メッセージの改ざん防止、システム稼働率を低下させるメッセージ攻撃への対策等がある。

[0087] 図７は、ＯＰＣ－ＵＡ通信システムを示した模式図である。ＯＰＣ－ＵＡサーバ１１とＯＰＣ－ＵＡクライアント１２とは、ＯＰＣ－ＵＡに従う通信を行う。ＯＰＣ－ＵＡで通信を行うには、認証のための証明書が必要になる。ＯＰＣ－ＵＡサーバ１１とＯＰＣ－ＵＡクライアント１２の各々は、サーバ証明書２１およびクライアント証明書２２を格納する。

[0088] なお、ＯＰＣ－ＵＡサーバ１１とＯＰＣ－ＵＡクライアント１２とは情報をやり取りする関係に従って定義される。たとえば制御ユニット１００は、ＯＰＣ－ＵＡサーバ１１として機能する。たとえばＨＭＩ８００がＯＰＣ－ＵＡクライアント１２になることができる。以下では、「ＯＰＣ－ＵＡサーバ１１」および「ＯＰＣ－ＵＡクライアント１２」を、単に「サーバ１１」および「クライアント１２」と記載する。

[0089] 認証のための証明書として自己署名証明書を使用する場合の手順は以下の通りである。まず、サーバ１１およびクライアント１２の各々に自己署名証明書が作成される。次に、サーバ１１に、クライアントの自己署名証明書をインポートする。一方、クライアント１２には、サーバの自己署名証明書がインポートされる。サーバ１１およびＯＰクライアント１２の各々は、自身の証明書を相手に送付する。サーバ１１およびクライアント１２の各々は、相手から送付された証明書とインポート済みの証明書とを照合することにより、認証を行う。

[0090] 認証のための証明書としてＣＡ（認証局）署名証明書を用いてもよい。この場合、たとえばＧＤＳ（Global Discovery Server）がＣＡ証明書を作成する。ＧＤＳは、サーバ１１およびクライアント１２のＣＡ署名証明書を作成する。サーバ１１およびクライアント１２は、ＣＡ署名証明書とＣＡ証明書とを受信する。

[0091] サーバ１１およびクライアント１２は、お互いのＣＡ署名証明書を送付するとともに、相手から送付されたＣＡ署名証明書をＣＡ証明書により照合する。これにより認証が行なわれる。証明書の受け渡しの方法は特に限定されない。たとえばメールを利用してもよく、ＵＳＢメモリ等の媒体を利用してもよい。

[0092] ＜Ｆ．証明書の寿命に関する課題＞

この実施の形態では、「証明書が寿命に達した状態」とは、証明書の有効期限の到来あるいは、暗号の脆弱性等の理由により、現在の証明書が使用できなくなることを意味する。

[0093] 上記の通り、証明書には有効期限がある。有効期限が経過した場合、証明書が失効するためにＯＰＣ－ＵＡ通信ができなくなる。たとえば図５に示した制御システム１０において、ＯＰＣ－ＵＡ通信ができない場合、製造ラインの停止が起こりえる。

[0094] 証明書の有効期限を確認する方法として、ツール（たとえば上述の「Ｓｙｓｍａｃ　Ｓｔｕｄｉｏ」）を用いる方法がある。しかし、この方法では、ユーザが能動的に情報を監視しなければならない。このため、ユーザが証明書の有効期限が近づいていること、あるいは有効期限が切れた（証明書が失効した）ことに気が付かない可能性を考慮する必要がある。

[0095] また、多数のＯＰＣ－ＵＡ機器（たとえばＰＬＣ）がネットワークに接続されている場合、ユーザは、各機器を監視する必要がある。証明書を更新する場合、ユーザは機器ごとに証明書を更新しなければならない。このためユーザの工数が増大する。

[0096] さらに、暗号技術には「寿命」があることも考慮する必要がある。たとえ

ば証明書の有効期限が切れる前に、暗号の脆弱性が発見される可能性がある。このような場合には、証明書を更新する必要がある。

[0097] さらに、サーバ１１とクライアント１２とが、異なるメーカにより提供される可能性がある。また、ＯＰＣ－ＵＡクライアント１２の数が複数の可能性もある。このような場合にも、証明書の更新のためのユーザの工数が増大する。

[0098] ＜Ｇ．証明書の寿命の通知＞

本実施の形態では、証明書が寿命に達する前の一定のタイミングにおいて、証明書の寿命が近づいていることを通知する。たとえば証明書の有効期限が間近である場合、ユーザは、制御装置１からの通知を受けることによって、証明書が失効間近であることを知ることができる。したがって、証明書の有効期限の管理のためのユーザの工数を低減することができる。また、ツールを制御装置１に接続しなくとも、証明書の有効期限の管理を行うことができる。さらに、証明書が失効する前に通知を受けることにより、ユーザが証明書を更新するための時間を確保することができる。

[0099] 図８は、証明書の有効期限の通知のための制御装置１の構成例を示した図である。図８を参照して、制御ユニット１００は、筐体１Ａを有する。証明書が期限に達する前の一定期間（たとえば３０日間）、制御ユニット１００は、インジケータ１２４（ＬＥＤ）を点滅させる。したがって、ユーザは制御ユニット１００を見ることにより、証明書の寿命が近づいていることを容易に把握できる。なお、制御ユニット１００に替えて、セキュリティユニット２００が、セキュリティユニット２００のインジケータ２２４（ＬＥＤ）を点滅させるのでもよい。

[0100] 通知期間はユーザが設定してもよい。また、失効までの残り日数に応じて、点滅の間隔、あるいは発光色を変更させてもよい。

[0101] 図８では、インジケータ１２４は１つのＬＥＤとして示されているが、インジケータ１２４はポートごとに設けられたＬＥＤを含んでもよい。各ＬＥＤが証明書の失効の間近になると点滅を開始するのでもよい。

[0102] 図９は、証明書の有効期限の通知のための制御装置１の別の構成例を示した図である。図９を参照して、制御ユニット１００は、証明書の有効期限が近づくと音を発生させてもよい。あるいは制御ユニット１００は、スピーカ１５から音を出力させてもよい。スピーカ１５は、ＡＩスピーカ（スマートスピーカ）であってもよい。また、制御ユニット１００に替えて、セキュリティユニット２００が音を発生させてもよく、セキュリティユニット２００がスピーカ１５から音を出力させてもよい。

[0103] また、制御ユニット１００に接続される通知デバイスはスピーカと限定されない。たとえば通知デバイスは表示灯であってもよい。

[0104] また、制御ユニット１００は、証明書の有効期限が近づいていることをＨＭＩ８００を介して通知してもよく、ＳＭＳ／メール等により通知してもよい。なお通知はサーバ側の設定だけでなく、クライアント側の設定も可能であってよい。ユーザは制御ユニット１００から発生する光あるいは音だけでなく、メールのメッセージからも、証明書の寿命が近づいていることを確認できる。

[0105] 図１０は、通知設定の例を示した図である。図１０に示したユーザインターフェイス画面８５０は、たとえばＨＭＩ８００に表示される。ユーザインターフェイス画面８５０は、通信ポート、セキュアな経路（ＯＰＣ－ＵＡ／ＶＰＮ）、証明書のステータス、証明書の有効期限、証明書の現時点からの残りの有効期限を一覧形式で表示する。制御装置１に格納された複数の証明書の各々の有効期限をユーザが容易に把握できるので、ユーザの利便性を向上させることができる。

[0106] さらに、ユーザインターフェイス画面８５０は、失効通知時期の設定および詳細設定を受け付ける。失効通知時期は、通信ポートごと（言い換えると証明書ごと）に個別に設定されてもよく、一括で設定されてもよい。たとえばカラム８５１の「失効通知時期」の表示にマウスのカーソルを重ねてマウスをクリックする。これにより、一括設定が可能である。この場合、たとえば、通知時期が「失効３０日前」に設定される。同じように、カラム８５２

の「詳細設定」の表示にマウスのカーソルを重ねてマウスをクリックすることにより、一括設定が可能である。

[0107] 図１１は、通知設定の他の例を示した図である。ユーザインターフェイス画面８６０がたとえばＨＭＩ８００に表示される。ユーザインターフェイス画面８６０は、タブの選択により、通知方法の選択を受け付ける。ユーザインターフェイス画面８６０は、ＬＥＤタブ８６１、ＨＭＩタブ８６２、およびＳＭＳタブ８６３を有する。ＳＭＳタブ８６３が選択されると、選択タブが有効であることを指定するためのカラム８６５と、メールアドレスを入力するための入力カラム８６６と、失効時期を入力するための入力領域８６７とが表示される。サーバ側、クライアント側の両方について失効時期が通知できるよう、入力カラム８６６は、複数のメールアドレスを受け付けることができる。３以上のメールアドレスが入力可能なように入力カラム８６６が構成されていてもよい。

[0108] 通知のタイミングは、入力された失効時期の前の所定期間（たとえば３０日）にデフォルトで設定されるのでもよい。あるいは、通知タイミングについてのユーザの入力を受け付けるようにユーザインターフェイス画面８６０が構成されていてもよい。

[0109] なお、たとえばセキュリティホールが見つかるなど暗号そのものが寿命に達した場合には、ＨＭＩ８００は、暗号強度を高める必要があることをユーザに通知する表示を行ってもよい。

[0110] ＜Ｈ．証明書の更新＞

証明書の更新は、ＯＰＣ－ＵＡサーバ側とＯＰＣ－ＵＡクライアント側との両方に通知する必要がある。しかし、クライアント側の通知対象者がサーバ側の通知対象者と異なる可能性がある。たとえばサーバとクライアントとでメーカが異なる場合に、このような事例が生じうる。そのためサーバ側とクライアント側との両方に証明書の更新を求めるのは制御システムのユーザにとっての負担が増大する。さらに、図５に例示される制御システム１０の場合、証明書の更新対象となる機器の数が多数（たとえば数百台単位）とな

る可能性もある。

[0111] 証明書を自動的に更新する場合、上記のような負担を軽減することはできる。しかし、セキュリティ確保の点では、ユーザの認証後に証明書を更新することが望ましい。証明書の失効する前の環境であれば、セキュア通信の下で証明書を更新することができる。すなわち更新前の証明書（古い証明書）を利用したセキュア通信により、証明書を更新することができる。

[0112] 図１２は、ＯＰＣ－ＵＡサーバおよびＯＰＣ－ＵＡクライアントの通常運転時の状態を説明するための模式図である。図１２に示すように、サーバ１１（ＯＰＣ－ＵＡサーバ）およびクライアント１２（ＯＰＣ－ＵＡクライアント）の各々は、サーバ証明書２１およびクライアント証明書２２を有しており、サーバ１１およびクライアント１２の間でセキュア通信が行われる。サーバ側（あるいはＯＴ（Operation Technology）側）ユーザ３１は、サーバ１１のメンテナンスを行う。一方、クライアント側（あるいはＩＴ（Information Technology）側）ユーザ３２は、クライアント１２のメンテナンスを行う。

[0113] 図１３は、証明書の更新処理における、新証明書の発行ステップを説明するための図である。なお、以下ではサーバ証明書２１の更新を代表的に説明するが、クライアント証明書２２の更新も、以下に説明する手順と同様の手順により更新することができる。

[0114] 新証明書の発行は、まずステップＳ１において、サーバ側ユーザ３１は、ログイン認証を用いてサーバ１１にログインする。ログインに成功すると、ステップＳ２において、サーバ側ユーザ３１は、サーバ１１のサーバ証明書を更新する。具体的には、サーバ証明書２３がサーバ１１に格納される。したがって、古いサーバ証明書（サーバ証明書２１）と新しいサーバ証明書（サーバ証明書２３）との両方が、サーバ１１に格納される。古いサーバ証明書（サーバ証明書２１）は、失効直前であるもののまだ有効である。したがって、サーバ１１およびクライアント１２の間でセキュア通信が可能である。

[0115] 図１４は、証明書の更新処理における、新証明書の送信ステップおよび更新リクエストの通知ステップを説明するための図である。ステップＳ３において、サーバ１１は、セキュアな経路で新しいサーバ証明書（サーバ証明書２３）をクライアント１２に送付する。さらにステップＳ４Ａにおいて、サーバ１１は、サーバ証明書の更新のリクエストをクライアント１２に通知する。ステップＳ４Ｂにおいて、クライアント側ユーザ３２は、サーバ証明書の更新リクエストの通知をクライアント１２から受ける。なお、更新リクエストの通知を受けるための方法は特に限定されない。たとえば、クライアント側ユーザ３２は、クライアント１２から送信されたメールにより、サーバ証明書の更新リクエストの通知を受け取ってもよい。

[0116] 図１５は、証明書の更新処理における新証明書の承認ステップを説明するための図である。ステップＳ５において、クライアント側ユーザ３２は、ログイン認証を用いてクライアント１２へのログインを行う。ステップＳ６において、クライアント側ユーザ３２は、クライアント１２に格納された新しいサーバ証明書（サーバ証明書２３）を承認する。これにより、ステップＳ７において、クライアント１２は、サーバ１１に承認通知を送信する。

[0117] 図１６は、証明書の更新処理における、古い証明書の破棄ステップを説明するための図である。ステップＳ８において、サーバ１１およびクライアント１２の各々は、ログイン認証を用いてクライアント１２へのログインを行う。ステップＳ６において、クライアント側ユーザ３２は、古いサーバ証明書（サーバ証明書２１）を破棄する。これにより、サーバ１１およびクライアント１２の各々においてサーバ証明書の更新が完了する。

[0118] 図１３から図１６に示すように、本実施の形態では、古い証明書を利用することにより、サーバとクライアントとの間のセキュアな経路を確保しながら、証明書を更新することができる。加えて、ユーザの承認後に証明書を更新することができる。証明書の更新対象となる機器の数が多数となる場合には、有効期限が近づいている証明書をリスト化して、そのリストから選択されたものを更新してもよい。リストの中から更新対象のものをユーザが選択

することによって、ユーザの承認後に証明書を更新することができるとともに、証明書を一括して更新することができる。

[0119] なお、上述のような証明書の管理あるいは更新（あるいはファームウェアのアップデート）が制御処理に影響を与えることをできるだけ避けることが好ましい。図１７に示すように、制御ユニット１００のプロセッサ１０２が複数のコア（コア１０２Ａ、コア１０２Ｂ、・・・）を有する場合に、ユーザプログラムを実行するコアとは別のコアにより、証明書の更新処理を実行してもよい。プログラムを周期的に実行するコアでなく、システムコアにより証明書の更新処理を実行するのでもよい。

[0120] あるいは、制御ユニット１００に替えてセキュリティユニット２００が一括して証明書の管理を行ってもよい。したがって、プロセッサ１０２に替えてプロセッサ２０２が検知手段を実現してもよく、インジケータ１２４に替えてインジケータ２２４が通知手段を実現してもよい。

[0121] なお、上記の実施の形態ではＯＰＣ－ＵＡを例示したが、セキュア通信として、ＳＳＬ（Secure Socket Layer）を実施の形態に適用することも可能である。

[0122] ＜Ｉ．付記＞

以上説明したように、本実施形態は以下に列挙する開示を含む。

[0123] １．制御対象を制御するための制御演算を実行するように構成された制御部（１５１）と、

証明書を利用したセキュア通信のための処理を実行する通信部（１５２）と、

前記証明書の寿命が近づいていることを検知する検知部（１５３）と、

前記証明書の前記寿命が近づいていることを通知する通知部（１２４）とを含む、制御装置（１）。

[0124] ２．前記証明書の前記寿命は前記証明書の有効期限であり、

前記通知部は、前記証明書が失効する前の一定のタイミングにおいて、前記証明書の前記有効期限が近づいていることを通知する、１．に記載の制御

装置（１）。

[0125] ３．前記制御装置（１）は、筐体（１Ａ）を含み、

前記通知部（１２４）は、

前記筐体（１Ａ）に設けられ、前記寿命が近づいていることを光により通知するインジケータ（１２４）を含む、１．または２．に記載の制御装置（１）。

[0126] ４．前記通知部は、

前記寿命が近づいていることを通知するための音を発生させる音声出力部を含む、１．または２．に記載の制御装置（１）。

[0127] ５．前記通知部は、前記寿命が近づいていることをメールにより通知する、請求項３または請求項４に記載の制御装置（１）。

[0128] ６．１．から５．のいずれかに記載の制御装置（１）と、

前記証明書が前記寿命に達する前の通知のタイミングを前記制御装置（１）に対して設定する設定装置（８００）とを備える、制御システム（１０）。

[0129] ７．前記制御装置（１）に複数の前記証明書が格納されている場合、

前記設定装置（８００）は、前記複数の証明書の有効期限を一括して表示する、６．に記載の制御システム（１０）。

[0130] ８．１．から５．のいずれかに記載の制御装置（１）と、

前記制御装置（１）との間で通信を行う通信装置（８００）とを備え、

前記制御装置（１）は、前記失効期限の前に新しい証明書を受け付けて、前記通信装置に更新リクエストを送信し、前記通信装置（８００）が前記新しい証明書を承認すると、古い証明書を破棄することで前記証明書を更新する、制御システム（１０）。

[0131] 今回開示された実施の形態はすべての点で例示であって制限的なものでないと考えられるべきである。本発明の範囲は上記した説明ではなくて請求の範囲によって示され、請求の範囲と均等の意味および範囲内でのすべての変更が含まれることが意図される。

符号の説明

[0132] １　制御装置、１Ａ　筐体、２　第１ネットワーク、４　第２ネットワーク、１０　制御システム、１１　ＯＰＣ－ＵＡサーバ、１２　ＯＰＣ－ＵＡクライアント、１５　スピーカ、２１，２３　サーバ証明書、２２　クライアント証明書、３１　サーバ側／ＯＴ側ユーザ、３２　クライアント側／ＩＴ側ユーザ、１００　制御ユニット、１０２，２０２，３０２　プロセッサ、１０２Ａ，１０２Ｂ　コア、１０４，２０４，３０４　チップセット、１０６，２０６，３０６　主記憶装置、１０８，２０８，３０８　二次記憶装置、１０９　記憶部、１１０，２１０　通信コントローラ、１１２，２１２　ＵＳＢコントローラ、１１４，２１４，３１４　メモリカードインターフェイス、１１５，２１５，３１５　メモリカード、１１６，１１８，１２０，２１６，２１８　ネットワークコントローラ、１２２，３２２　内部バスコントローラ、１２４，２２４，３２４　インジケータ、１４２，１４４，２４２　通信ポート、１５０　制御エンジン、１５１　制御部、１５２　通信処理部、１５３　検知部、１５４　通知処理部、１５５　通知出力部、１６０　情報エンジン、１７０　ブローカー、１８０，３６０　ログデータベース、２００　セキュリティユニット、２５０　セキュリティエンジン、２６０　セキュリティ情報、３００　セーフティユニット、３５０　セーフティエンジン、４００　機能ユニット、４５０　電源ユニット、５００　フィールドデバイス、６００　サポート装置、７００　ＳＣＡＤＡ装置、８５０，８６０　ユーザインターフェイス画面、８５１，８５２，８６５　カラム、８６１，８６２，８６３　タブ、８６６　入力カラム、８６７　入力領域、９００　データベース、１１０４　プログラム、１１０６　鍵、１１１０　証明書、Ｓ１～Ｓ８　ステップ。

請求の範囲

[請求項1] 制御対象を制御するための制御演算を実行するように構成された制御部と、

証明書を利用したセキュア通信のための処理を実行する通信部と、

前記証明書の寿命が近づいていることを検知する検知部と、

前記証明書の前記寿命が近づいていることを通知する通知部とを含む、制御装置。

[請求項2] 前記証明書の前記寿命は前記証明書の有効期限であり、

前記通知部は、前記証明書が失効する前の一定のタイミングにおいて、前記証明書の前記有効期限が近づいていることを通知する、請求項１に記載の制御装置。

[請求項3] 前記制御装置は、筐体を含み、

前記通知部は、

前記筐体に設けられ、前記寿命が近づいていることを光により通知するインジケータを含む、請求項１または請求項２に記載の制御装置。

[請求項4] 前記通知部は、

前記寿命が近づいていることを通知するための音を発生させる音声出力部を含む、請求項１または請求項２に記載の制御装置。

[請求項5] 前記通知部は、前記寿命が近づいていることをメールにより通知する、請求項３または請求項４に記載の制御装置。

[請求項6] 請求項１から請求項５のいずれか１項に記載の制御装置と、

前記証明書が前記寿命に達する前の通知のタイミングを前記制御装置に対して設定する設定装置とを備える、制御システム。

[請求項7] 前記制御装置に複数の前記証明書が格納されている場合、

前記設定装置は、前記複数の証明書の有効期限を一括して表示する、請求項６に記載の制御システム。

[請求項8] 前記請求項１から請求項５のいずれか１項に記載の制御装置と、

前記制御装置との間で通信を行う通信装置とを備え、

前記制御装置は、前記失効期限の前に新しい証明書を受け付けて、前記通信装置に更新リクエストを送信し、前記通信装置が前記新しい証明書を承認すると、古い証明書を破棄することで前記証明書を更新する、制御システム。

[図1]

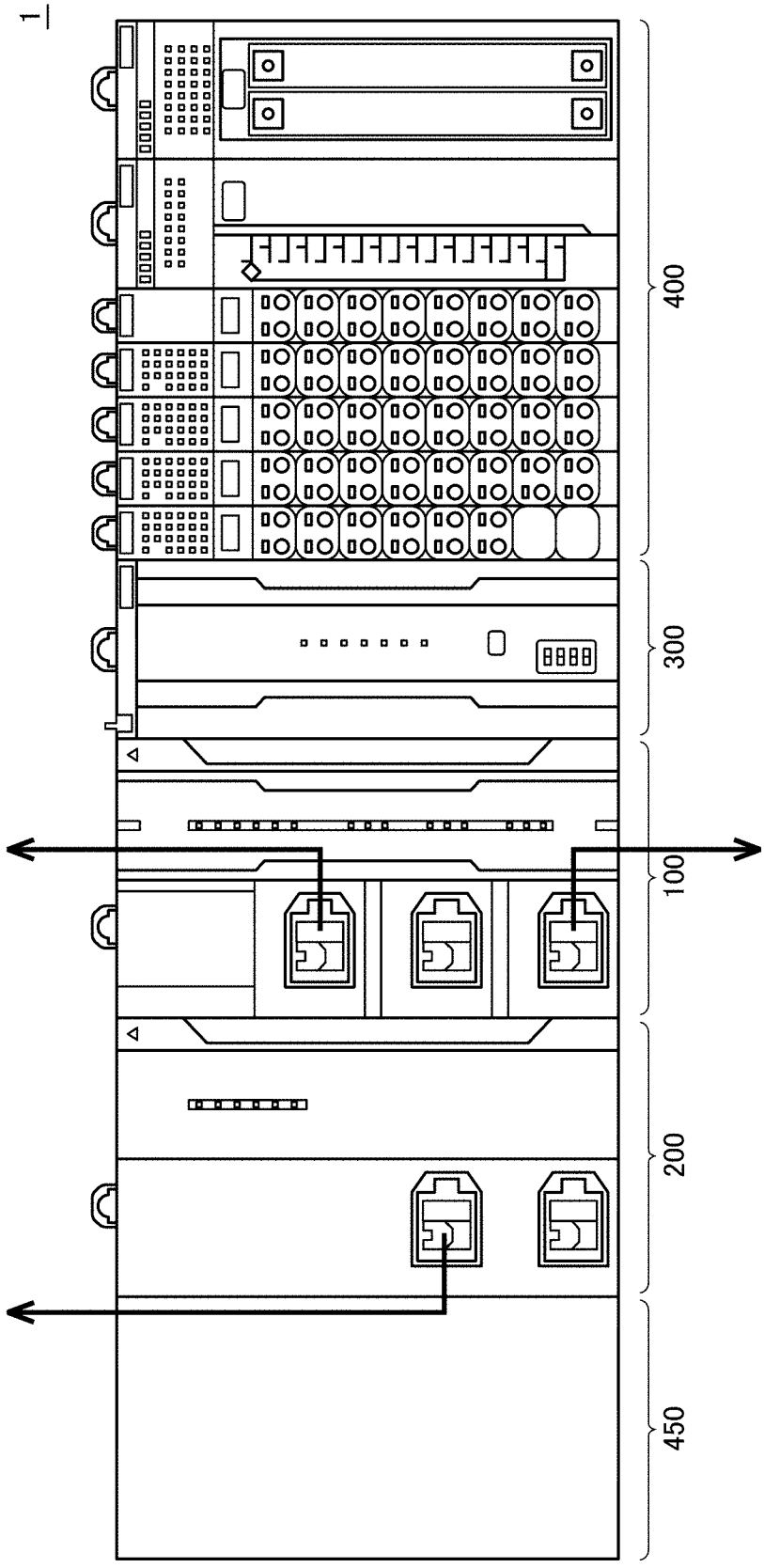


FIG.1

[図2]

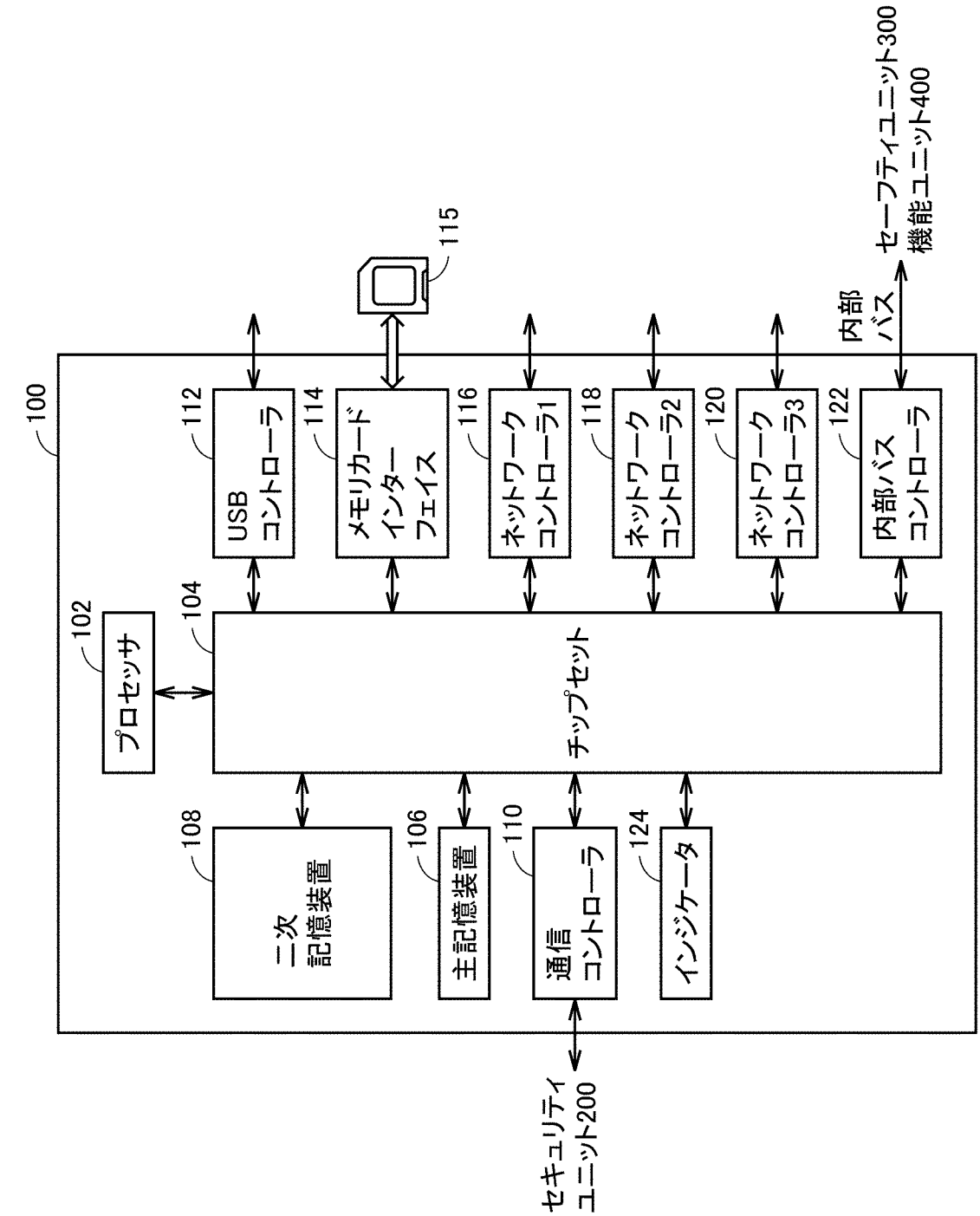
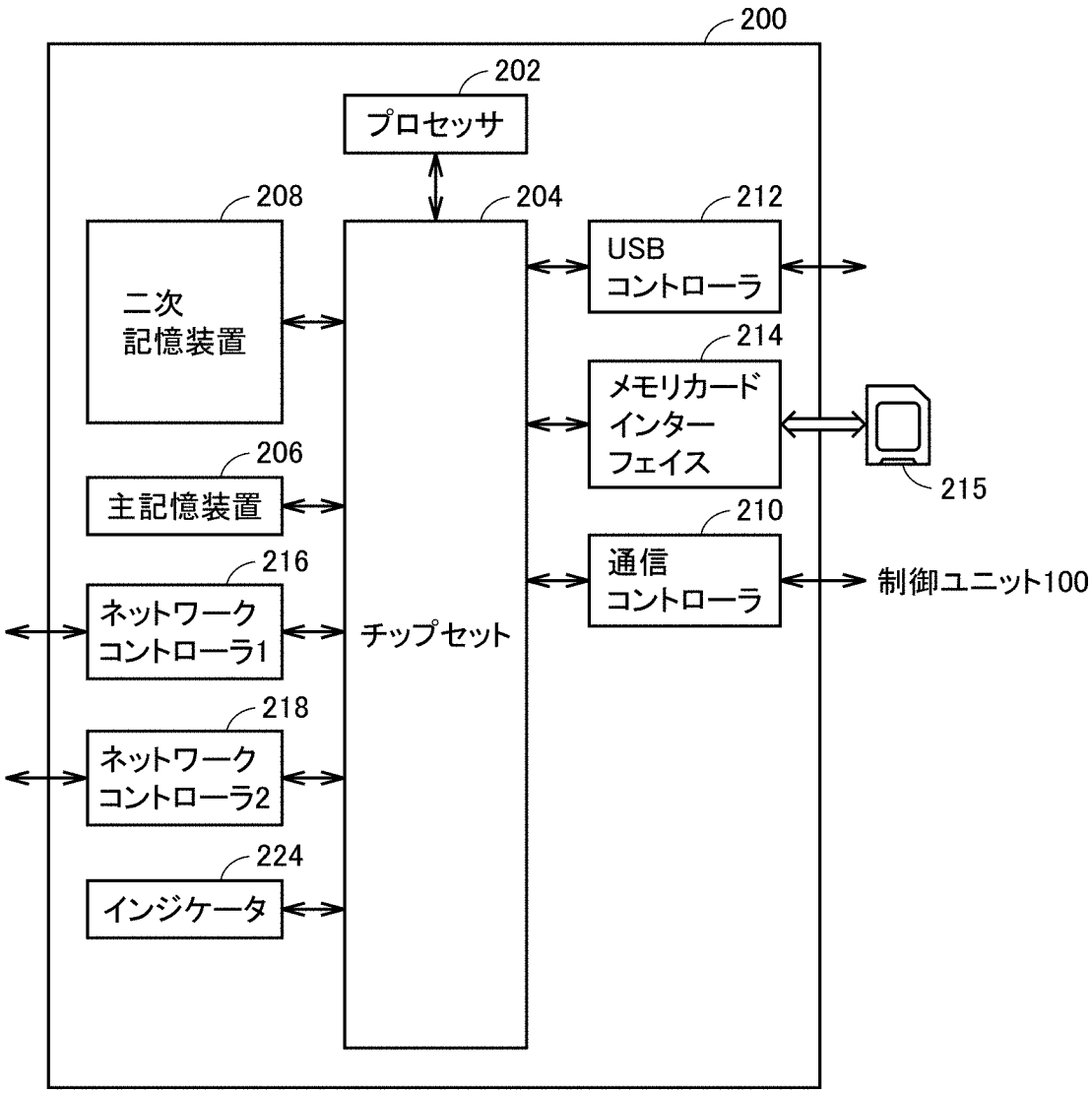

100
102
プロセッサ
104
チップセット
108
二次
記憶装置
106
主記憶装置
110
通信
コントローラ
124
インジケータ
112
USB
コントローラ
114
メモリカード
インター
フェイス
116
ネットワーク
コントローラ1
118
ネットワーク
コントローラ2
120
ネットワーク
コントローラ3
122
内部バス
コントローラ
115
内部
バス
セーフティユニット300
機能ユニット400
セキュリティ
ユニット200

FIG.2

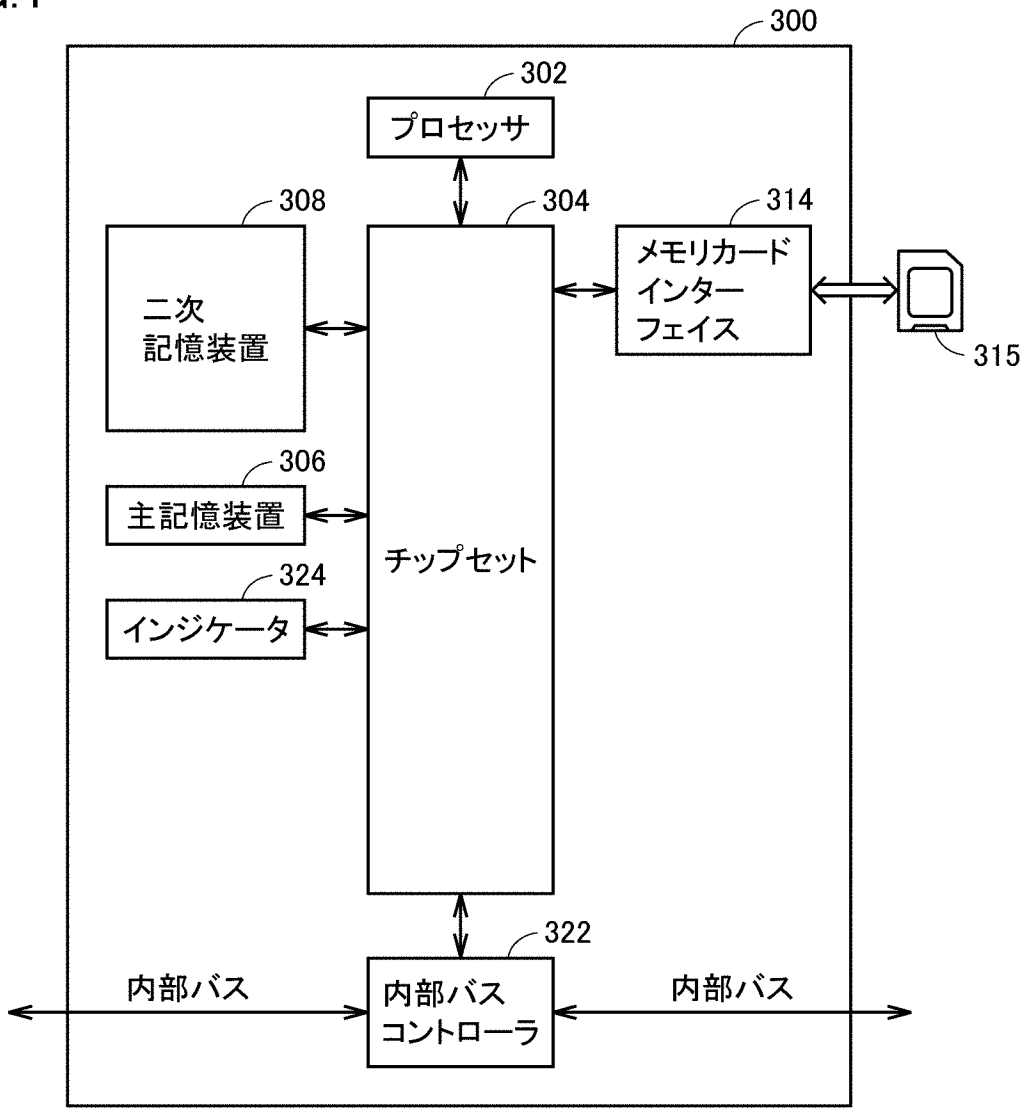
[図3]

FIG.3


200
202
プロセッサ
208
二次
記憶装置
204
212
USB
コントローラ
214
メモリカード
インター
フェイス
215
206
主記憶装置
210
通信
コントローラ
制御ユニット100
216
ネットワーク
コントローラ1
チップセット
218
ネットワーク
コントローラ2
224
インジケータ

[図4]

FIG.4


300
302
プロセッサ
308
304
314
二次
記憶装置
メモリカード
インター
フェイス
315
306
主記憶装置
チップセット
324
インジケータ
322
内部バス
内部バス
コントローラ
内部バス

[図5]

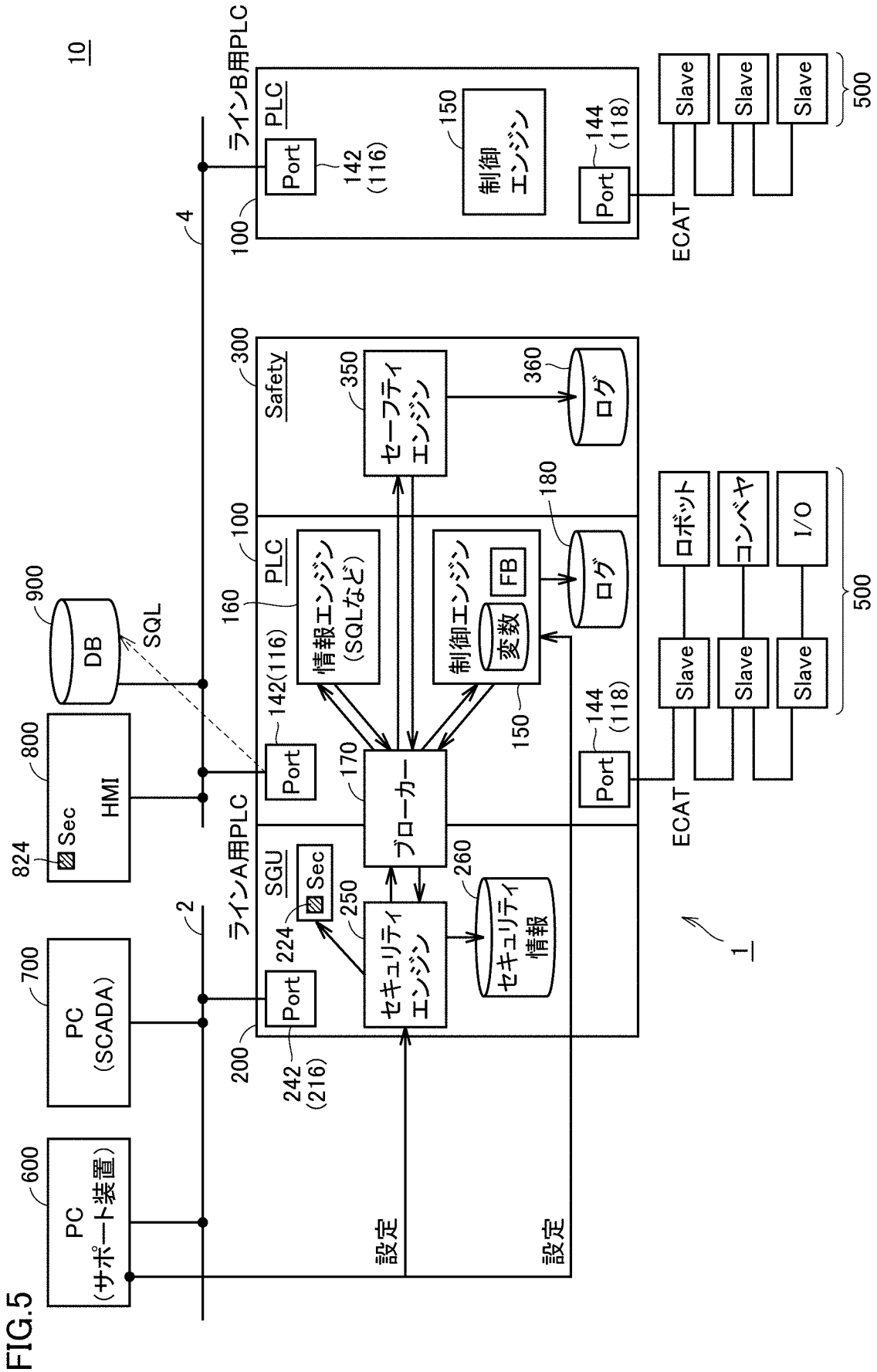
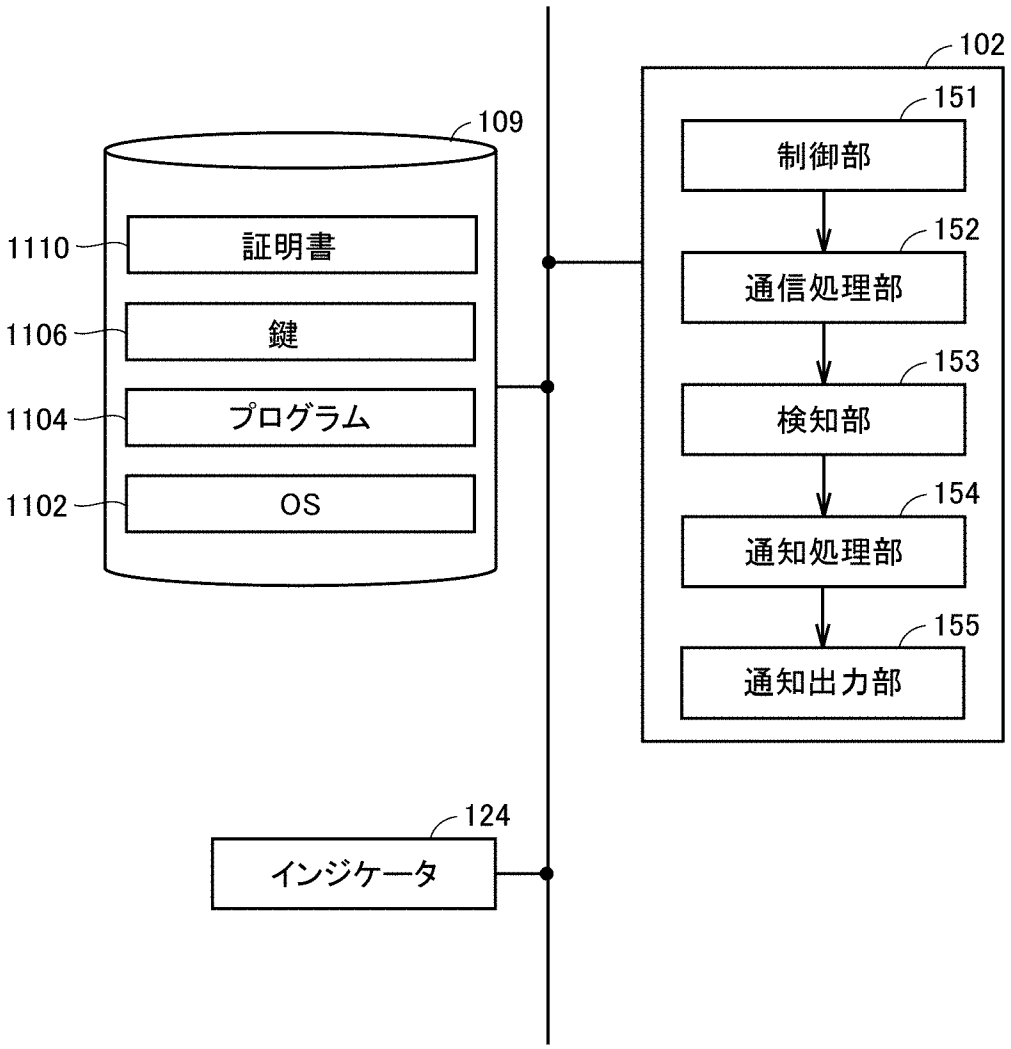

10
ラインB用PLC
PLC
Port
142
(116)
100
4
150
制御
エンジン
144
(118)
Port
Slave
Slave
Slave
500
ECAT
Safety
300
350
セーフティ
エンジン
360
ログ
100
PLC
160
情報エンジン
(SQLなど)
142(116)
Port
900
DB
SQL
800
HMI
Sec
824
ラインA用PLC
2
700
PC
(SCADA)
600
PC
(サポート装置)
SGU
Sec
224
Port
200
242
(216)
250
セキュリティ
エンジン
170
ブローカー
260
セキュリティ
情報
180
ログ
制御エンジン
FB
変数
150
144
(118)
Port
ロボット
コンベヤ
I/O
Slave
Slave
Slave
500
ECAT
1
設定
設定

FIG.5

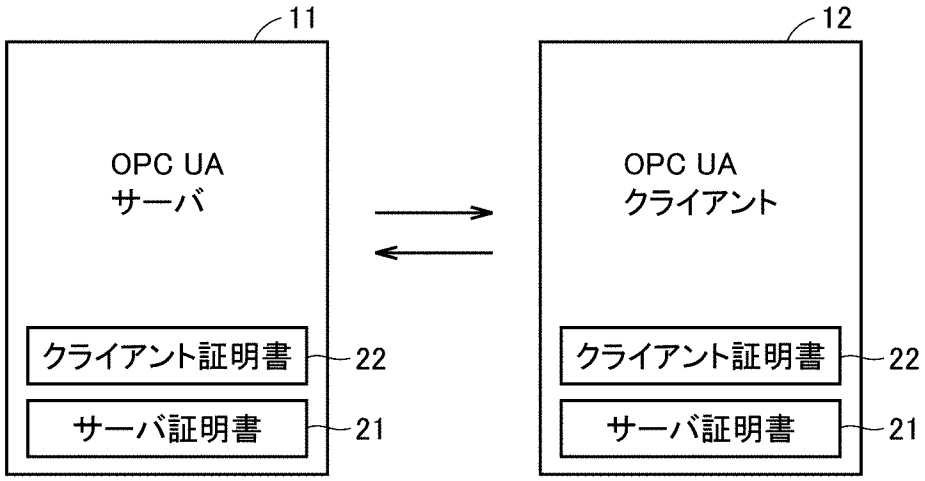
[図6]

FIG.6



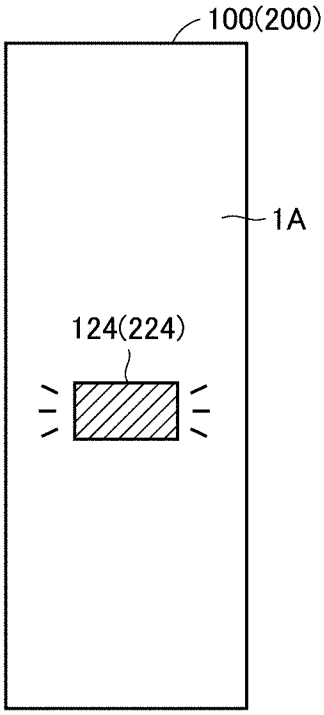
[図7]

FIG.7



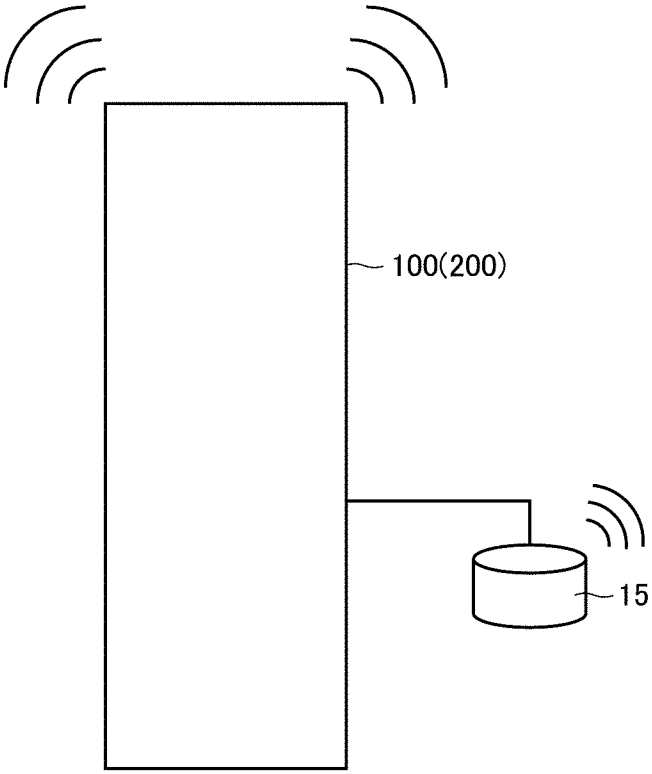
[図8]

FIG.8



[図9]

FIG.9



[図10]

850

通信ポート	OPCUA/VPN	ステータス	有効期限	残り期限	失効通知時期	詳細設定
A	VPN	有効	2020/1/xx	1年	失効30日前	
B	VPN	失効	2017/1/xx	–	失効30日前	
C	VPN	暗号寿命	–	–	失効30日前	
D	OPCUA	有効	2020/1/xx	1年	失効30日前	
E	OPCUA	失効	2017/1/xx	–	失効30日前	
F	OPCUA	暗号寿命	–	–	失効30日前	

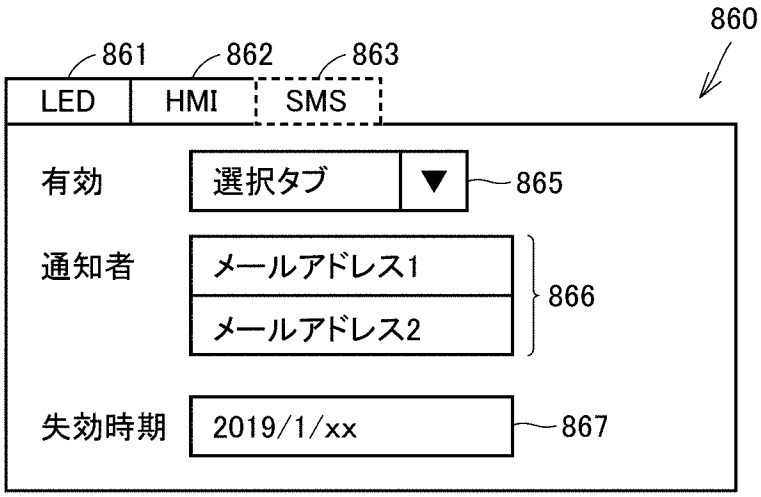
851

852

FIG.10

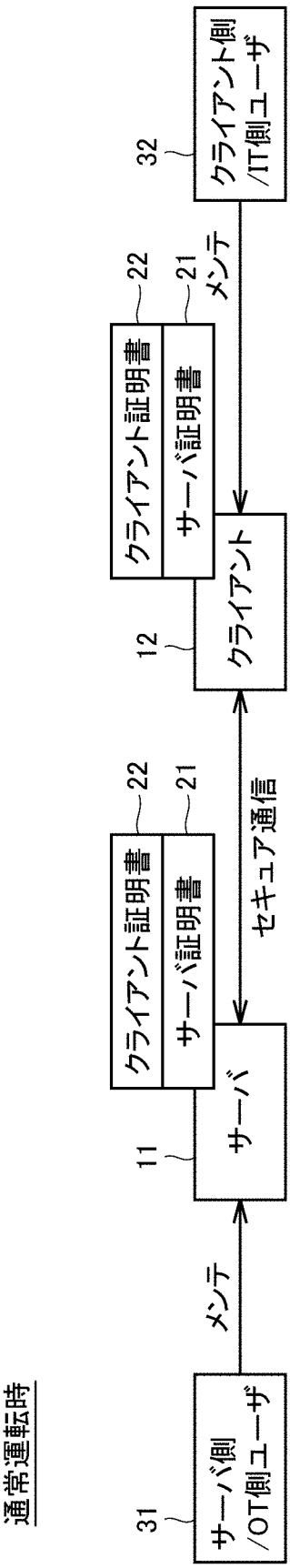
[図11]

FIG.11


860
861
862
863
LED
HMI
SMS
有効
選択タブ
865
通知者
メールアドレス1
メールアドレス2
866
失効時期
2019/1/xx
867

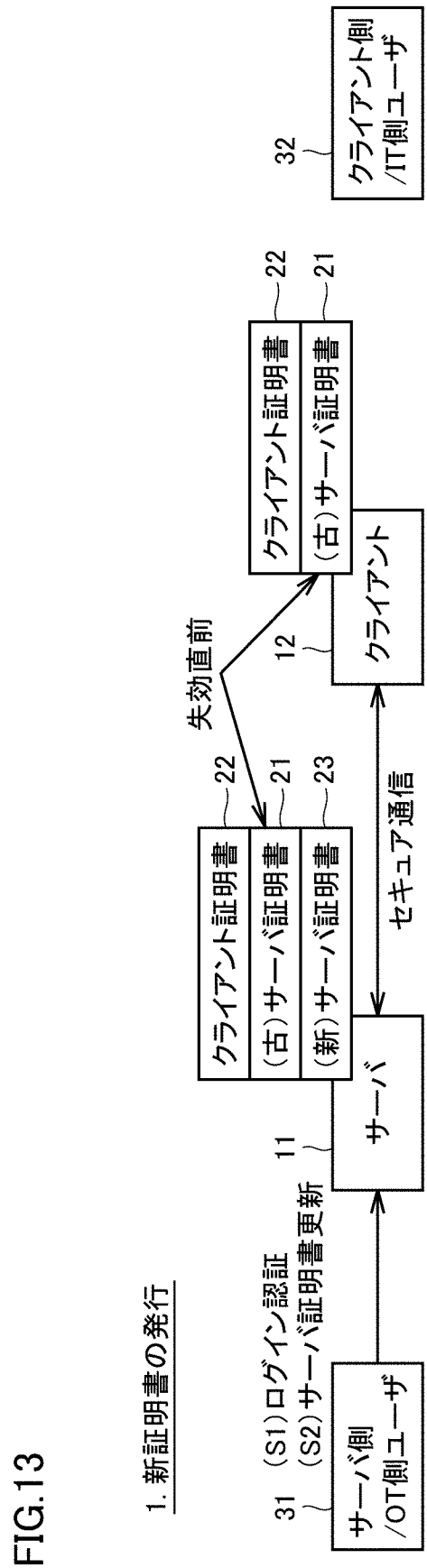
[図12]

FIG.12


通常運転時
31
サーバ側
/OT側ユーザ
メンテ
11
サーバ
22
クライアント証明書
21
サーバ証明書
セキュア通信
12
クライアント
22
クライアント証明書
21
サーバ証明書
メンテ
32
クライアント側
/IT側ユーザ

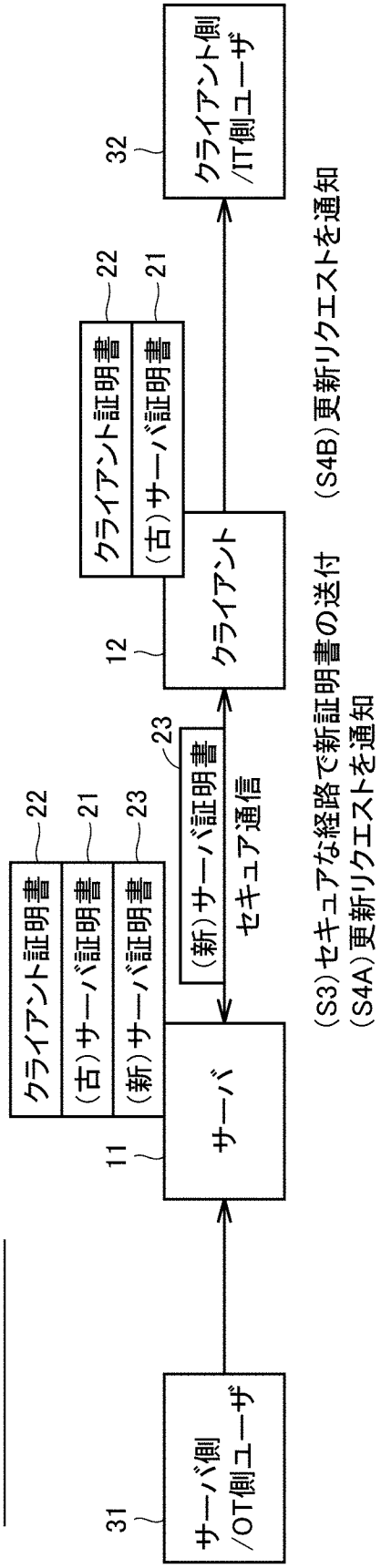
[図13]

FIG.13


1. 新証明書の発行
31
(S1)ログイン認証
(S2)サーバ証明書更新
サーバ側
/OT側ユーザ
11
サーバ
クライアント証明書
(古)サーバ証明書
(新)サーバ証明書
22
21
23
セキュア通信
失効直前
12
クライアント
クライアント証明書
(古)サーバ証明書
22
21
32
クライアント側
/IT側ユーザ

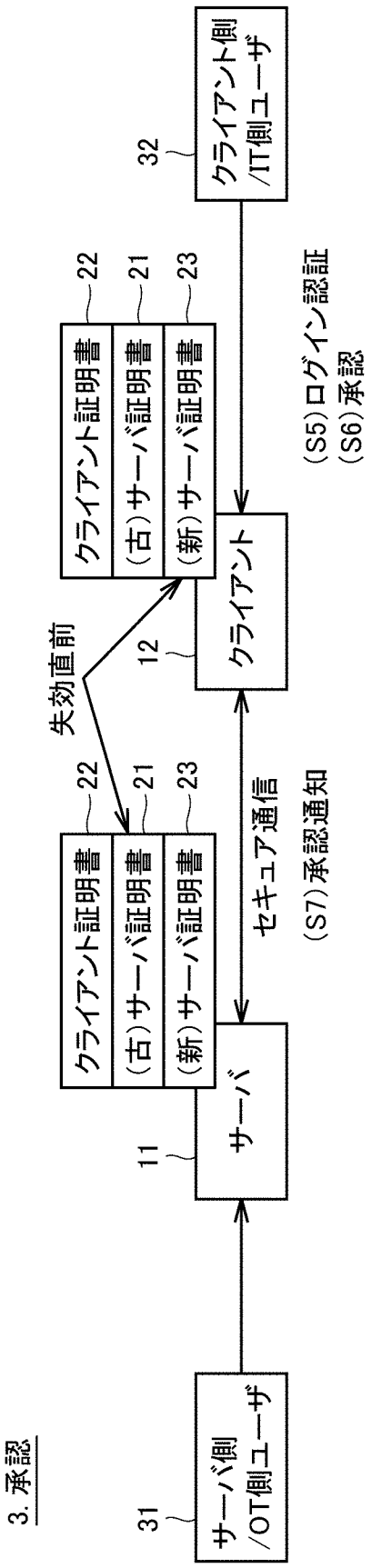
[図14]

FIG.14


2. 送信およびリクエスト
31
サーバ側
/OT側ユーザ
11
サーバ
クライアント証明書
(古)サーバ証明書
(新)サーバ証明書
22
21
23
(新)サーバ証明書
23
セキュア通信
12
クライアント
クライアント証明書
(古)サーバ証明書
22
21
32
クライアント側
/IT側ユーザ
(S3)セキュアな経路で新証明書の送付
(S4A)更新リクエストを通知
(S4B)更新リクエストを通知

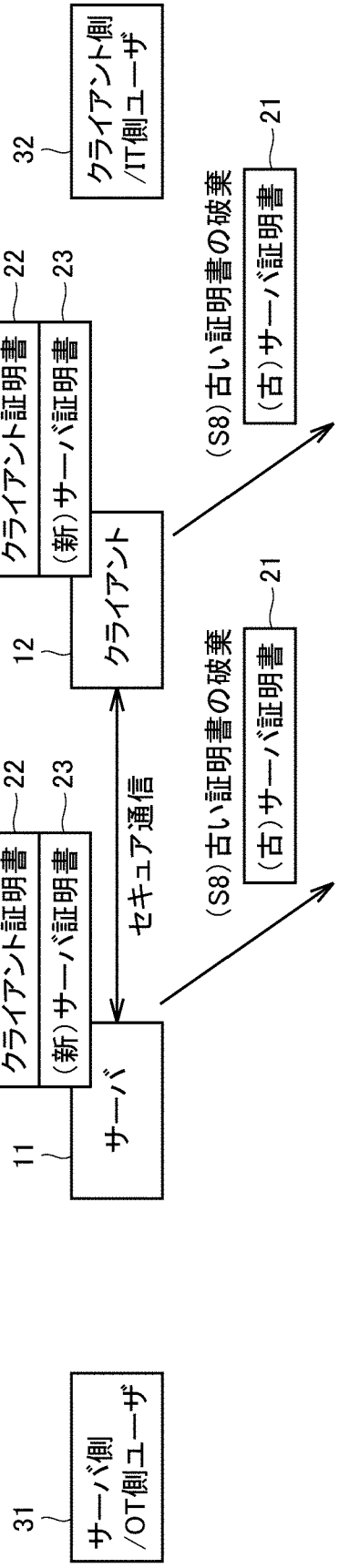
[図15]

FIG.15


3. 承認
サーバ側
/OT側ユーザ
31
サーバ
11
クライアント証明書
(古)サーバ証明書
(新)サーバ証明書
22
21
23
セキュア通信
(S7)承認通知
失効直前
クライアント
12
クライアント証明書
(古)サーバ証明書
(新)サーバ証明書
22
21
23
(S5)ログイン認証
(S6)承認
クライアント側
/IT側ユーザ
32

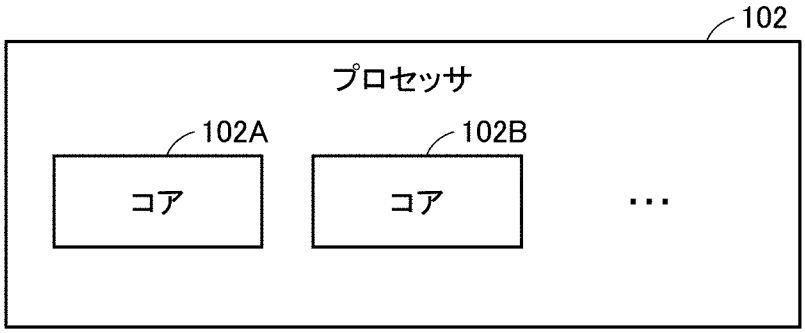
[図16]

FIG.16


4. 古い証明書の破棄
31
サーバ側
/OT側ユーザ
11
サーバ
クライアント証明書
(新)サーバ証明書
22
23
セキュア通信
12
クライアント
クライアント証明書
(新)サーバ証明書
22
23
32
クライアント側
/IT側ユーザ
(S8)古い証明書の破棄
(古)サーバ証明書
21
(S8)古い証明書の破棄
(古)サーバ証明書
21

[図17]

FIG.17



INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2020/007796

A. CLASSIFICATION OF SUBJECT MATTER
G05B 19/05(2006.01)i; G05B 19/048(2006.01)i; H04L 9/08(2006.01)i
FI: G05B19/05 N; G05B19/048; H04L9/00 601F

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; G05B19/048; H04L9/08

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	1971-2020
Registered utility model specifications of Japan	1996-2020
Published registered utility model applications of Japan	1994-2020

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.
Y	JP 2013-232190 A (GENERAL ELECTRIC CO.) 14.11.2013 (2013-11-14) paragraphs [0019]-[0026], fig. 1-4	1-8
Y	JP 2017-195517 A (MITSUBISHI ELECTRIC CORP.) 26.10.2017 (2017-10-26) paragraphs [0025]-[0065], fig. 2-6	1-8

☐ 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	Date of mailing of the international search report
03 April 2020 (03.04.2020)	14 April 2020 (14.04.2020)

Name and mailing address of the ISA/	Authorized officer
Japan Patent Office 3-4-3, Kasumigaseki, Chiyoda-ku, Tokyo 100-8915, Japan	Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/JP2020/007796

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
JP 2013-232190 A	14 Nov. 2013	US 2013/0291085 A1 paragraphs [0021]-[0028], fig. 1-4 US 2015/0143500 A1 US 2016/0330187 A1 US 2018/0302388 A1 EP 2660669 A2 CN 103376766 A	
JP 2017-195517 A	26 Oct. 2017	(Family: none)	

国際調査報告

国際出願番号
PCT/JP2020/007796

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; G05B 19/048(2006.01)i; H04L 9/08(2006.01)i
FI: G05B19/05 N; G05B19/048; H04L9/00 601F

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; G05B19/048; H04L9/08

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

日本国実用新案公報	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２０２０年
日本国実用新案登録公報	１９９６－２０２０年
日本国登録実用新案公報	１９９４－２０２０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
Y	JP 2013-232190 A (ゼネラル・エレクトリック・カンパニイ) 14.11.2013 (2013-11-14) 段落[0019]-[0026],図1-4	1-8
Y	JP 2017-195517 A (三菱電機株式会社) 26.10.2017 (2017-10-26) 段落[0025]-[0065],図2-6	1-8

☐ 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。

＊ 引用文献のカテゴリー
“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
“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
“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）
“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
“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
“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
“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
“&” 同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
03.04.2020	14.04.2020

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/JP2020/007796

引用文献	公表日	パテントファミリー文献	公表日
JP 2013-232190 A	14.11.2013	US 2013/0291085 A1 段落[0021]-[0028],図1-4 US 2015/0143500 A1 US 2016/0330187 A1 US 2018/0302388 A1 EP 2660669 A2 CN 103376766 A	
JP 2017-195517 A	26.10.2017	（ファミリーなし）	