(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
2017 年 3 月 9 日(09.03.2017)

WIPO | PCT

(10) 国際公開番号
WO 2017/038009 A1

(51) 国際特許分類:
H04L 9/14 (2006.01) *H04L 9/08* (2006.01)
G06F 21/44 (2013.01) *H04L 9/32* (2006.01)

(21) 国際出願番号: PCT/JP2016/003595

(22) 国際出願日: 2016 年 8 月 4 日(04.08.2016)

(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 2015-170760 2015 年 8 月 31 日(31.08.2015) JP

(71) 出願人: パナソニック I P マネジメント株式会社 (PANASONIC INTELLECTUAL PROPERTY MANAGEMENT CO., LTD.) [JP/JP]; 〒5406207 大阪府大阪市中央区城見２丁目１番６１号 Osaka (JP).

(72) 発明者: 高添 智樹(TAKAZOE, Tomoki). 増田 洋一(MASUDA, Yoichi). 松島 秀樹(MATSUSHIMA, Hideki). 海上 勇二(UNAGAMI, Yuji).

(74) 代理人: 鎌田 健司, 外(KAMATA, Kenji et al.); 〒5406207 大阪府大阪市中央区城見２丁目１番６１号パナソニック I P マネジメント株式会社内 Osaka (JP).

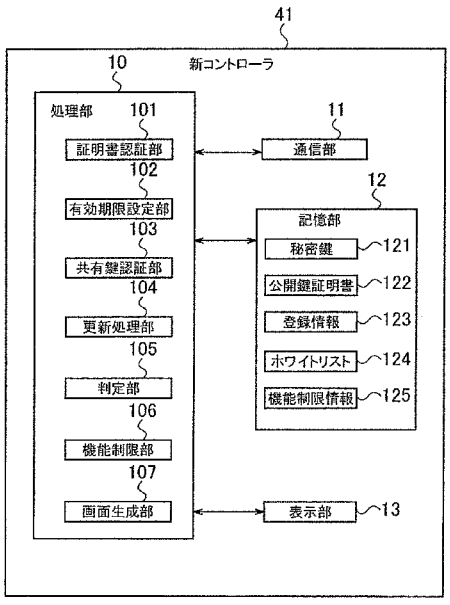
(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, 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, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, 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,

[続葉有]

(54) **Title**: CONTROLLER, COMMUNICATION METHOD, AND COMMUNICATION SYSTEM

(54) 発明の名称 : コントローラ、通信方法、及び通信システム



10 Processing unit
11 Communication unit
12 Storage unit
13 Display unit
41 Novel controller
101 Certificate authentication unit
102 Expiration date setting unit
103 Shared key authentication unit
104 Update processing unit
105 Determination unit
106 Function-limiting unit
107 Screen generation unit
121 Secret key
122 Public key certificate
123 Registration information
124 White list
125 Function limitation information

(57) **Abstract**: Provided is a novel controller (that supports apparatus authentication) (41) for performing encrypted communication with an apparatus that succeeds in mutual authentication in which an electronic certificate is used, wherein the novel controller is provided with: a determination unit (105) for determining whether an apparatus to be communicated with is an authentication-supporting apparatus that supports mutual authentication; a function-limiting unit (106) which, when it is determined by the determination unit (105) that the apparatus to be communicated with is not an authentication-supporting apparatus, limits a function among the functions of the apparatus to be communicated with that can be operated from the novel controller (that supports apparatus authentication) (41); and a communication unit (11) for performing communication in plain text with the apparatus to be communicated with under the function limitation by the function-limiting unit (106).

(57) 要約:

[続葉有]

WO 2017/038009 A1

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:

— 国際調査報告（条約第 21 条(3)）

新コントローラ（機器認証対応）（４１）は、電子証明書を用いた相互認証に成功した機器と暗号化通信を行うコントローラであって、通信対象の機器が相互認証に対応している認証対応機器であるか否かを判定する判定部（１０５）と、判定部（１０５）により認証対応機器でないと判定された場合、その通信対象の機器が有する機能のうち、新コントローラ（機器認証対応）（４１）から操作可能な機能を制限する機能制限部（１０６）と、機能制限部（１０６）による機能制限のもと通信対象の機器と平文で通信を行う通信部（１１）とを備える。

明　細　書

発明の名称 ： コントローラ、通信方法、及び通信システム

技術分野

[0001] 本発明は、電子証明書を用いた相互認証に成功した機器と暗号化通信を行うコントローラ、通信方法、及び通信システムに関する。

背景技術

[0002] 近年、ホームエリアネットワークにコントローラを接続し、機器と外部のサーバとの間の通信をコントローラを介して行う場合がある（例えば特許文献１参照）。そこで、コントローラと各機器との接続を安全に設定することで家庭内の通信を制御し、不正機器のなりすましによる接続、又は、通信内容の傍受による情報漏洩などを防止することが求められる。

[0003] 例えば、認証局により発行された公開鍵証明書（電子証明書）を用いて機器同士が相互認証を行う認証システムにおいて、各機器が初回登録時に公開鍵証明書を用いて共有鍵を生成し、この共有鍵を用いて以後の認証を簡略化する技術が知られている（例えば特許文献２参照）。

先行技術文献

特許文献

[0004] 特許文献1：特開２０１４－２１７０７３号公報

特許文献2：特開２００４－２４７７９９号公報

発明の概要

発明が解決しようとする課題

[0005] ところで、実運用としては、上述したような電子証明書を用いた相互認証（以下、「機器認証」という。）に対応している機器と対応していない機器とが混在する環境がある。このような環境でも、機器認証に対応していない機器を安全に操作することが望まれる。

[0006] 本発明は、上記問題点を鑑み、機器認証に対応している機器と対応していない機器とが混在する環境でも、機器認証に対応していない機器を安全に操

作することができるコントローラ、通信方法、及び通信システムを提供することを目的とする。

課題を解決するための手段

[0007] 上記目的を達成するために、本発明の第１の態様に係るコントローラは、電子証明書を用いた相互認証に成功した機器と暗号化通信を行うコントローラであって、通信対象の機器が前記相互認証に対応している認証対応機器であるか否かを判定する判定部と、前記判定部により前記認証対応機器でないと判定された場合、前記通信対象の機器が有する機能のうち、当該コントローラから操作可能な機能を制限する機能制限部と、前記機能制限部による機能制限のもと前記通信対象の機器と平文で通信を行う通信部とを備えるコントローラであることを要旨とする。

[0008] 本発明の第２の態様に係る通信方法は、コントローラが電子証明書を用いて相互認証に成功した機器と暗号化通信を行う場合の通信方法であって、前記コントローラが、通信対象の機器が前記相互認証に対応している認証対応機器であるか否かを判定する判定ステップと、前記コントローラが、前記判定ステップで前記認証対応機器でないと判定した場合、前記通信対象の機器が有する機能のうち、当該コントローラから操作可能な機能を制限する機能制限ステップと、前記コントローラが、前記機能制限ステップにおける機能制限のもと前記通信対象の機器と平文で通信を行う通信ステップとを含む通信方法であることを要旨とする。

[0009] 本発明の第３の態様に係る通信システムは、コントローラが電子証明書を用いて相互認証に成功した機器と暗号化通信を行う通信システムであって、前記コントローラが、通信対象の機器が前記相互認証に対応している認証対応機器であるか否かを判定する判定部と、前記判定部により前記認証対応機器でないと判定された場合、前記通信対象の機器が有する機能のうち、当該コントローラから操作可能な機能を制限する機能制限部と、前記機能制限部による機能制限のもと前記通信対象の機器と平文で通信を行う通信部とを備える通信システムであることを要旨とする。

発明の効果

[0010] 本発明によれば、機器認証に対応している機器と対応していない機器とが混在する環境でも、機器認証に対応していない機器を安全に操作することができるコントローラ、通信方法、及び通信システムを提供することができる。

図面の簡単な説明

[0011] [図1]図１は、本発明の実施の形態に係る認証システムの基本的な構成を説明するブロック図である。

[図2]図２は、本発明の実施の形態に係る認証システムが備えるコントローラの基本的な構成を説明するブロック図である。

[図3]図３は、本発明の実施の形態に係る認証システムに用いる公開鍵証明書の基本的なデータ構成を説明するブロック図である。

[図4]図４は、本発明の実施の形態に係る認証システムに用いる登録情報の基本的なデータ構成を説明するブロック図である。

[図5]図５は、本発明の実施の形態に係る認証システムが備える機器の基本的な構成を説明するブロック図である。

[図6]図６は、本発明の実施の形態に係る認証システムに用いる登録情報の基本的なデータ構成を説明するブロック図である。

[図7]図７は、本発明の実施の形態に係る認証システムの動作を説明するシーケンス図である。

[図8]図８は、本発明の実施の形態に係る認証システムにおける公開鍵証明書を用いた相互認証の処理を説明するシーケンス図である。

[図9]図９は、本発明の実施の形態に係る認証システムにおける共有鍵を用いた相互認証の処理を説明するシーケンス図である。

[図10]図１０は、本発明の実施の形態に係る認証システムにおける公開鍵証明書の更新の処理を説明するシーケンス図である。

[図11]図１１は、本発明の実施の形態に係る通信システムにおいてレガシー機器への対応が必要なケースを説明するための概念図である。

[図12]図１２は、本発明の実施の形態に係る通信システムが備える新コントローラ（機器認証対応）の基本的な構成を説明するブロック図である。

[図13]図１３は、本発明の実施の形態に係る通信システムが備える新コントローラ（機器認証対応）と他の機器との接続例を示すブロック図である。

[図14]図１４は、本発明の実施の形態に係る通信システムが備える新コントローラ（機器認証対応）の動作を示すフローチャートである。

[図15]図１５は、本発明の実施の形態に係る通信システムが備える新コントローラ（機器認証対応）の表示部に表示される画面例を示す図である。

[図16]図１６は、本発明の実施の形態に係る通信システムが備える新コントローラ（機器認証対応）の表示部に表示される別の画面例を示す図である。

[図17]図１７は、本発明の実施の形態に係る通信システムが備える新コントローラ（機器認証対応）の記憶部に記憶される機能制限情報の一例を示す図である。

発明を実施するための形態

[0012] 以下、本実施の形態に係るコントローラ等について、図面を参照しながら説明する。なお、以下に説明する実施の形態は、いずれも本発明の好ましい一具体例を示すものである。したがって、以下の実施の形態で示される、数値、形状、材料、構成要素、構成要素の配置位置や接続形態、及び、工程（ステップ）や工程の順序などは、一例であって本発明を限定する主旨ではない。よって、以下の実施の形態における構成要素のうち、本発明の最上位概念を示す独立請求項に記載されていない構成要素については、任意の構成要素として説明される。なお、各図は、模式図であり、必ずしも厳密に図示されたものではない。

[0013] 以下の図面の記載において、同一又は類似の部分には同一又は類似の符号を付し、重複する説明を省略している部分もある。

[0014] （実施の形態）

≪基本構成≫

本実施の形態に係る通信システムは、以下に説明する認証システムを前提

としている。

[0015] （認証システム）

本実施の形態に係る認証システムは、図１に示すように、コントローラ１と、複数の機器２と、通信回線であるインターネット３を介して、コントローラ１に通信可能に接続されるサーバ４とを備える。サーバ４は、コントローラ１及び複数の機器２に対して公開鍵証明書を発行し、発行した公開鍵証明書を管理する認証局である。

[0016] コントローラ１（第１機器）は、例えば、複数の機器２の使用電力量、発電余剰電力量等を管理するホームエネルギーマネジメントシステム（ＨＥＭＳ）におけるコントローラである。コントローラ１は、複数の機器２と通信可能に接続される通信機器である。コントローラ１は、複数の機器２と相互認証して複数の機器２を登録することにより、複数の機器２とＨＥＭＳ５を構成する。

[0017] コントローラ１は、図２に示すように、処理部１０と、処理部１０の制御に応じて他と通信する通信部１１と、プログラムや各種データ等の情報を記憶する記憶部１２とを備える。通信部１１が行う通信は、無線通信であっても有線通信であってもよい。記憶部１２は、コントローラ１自身の秘密鍵１２１及び公開鍵証明書１２２と、既に登録した機器２に関する情報である登録情報１２３とを記憶する。

[0018] 公開鍵証明書１２２は、図３に示すように、公開鍵証明書１２２のバージョン、発行者、有効期間の開始時、有効期間の終了時（有効期限）、証明書ＩＤ（識別子）、コントローラ１の公開鍵、及び、サーバ４の署名を含む。公開鍵証明書１２２の公開鍵は、秘密鍵１２１に対応する。公開鍵証明書１２２の署名は、サーバ４の秘密鍵を用いて作成される。公開鍵証明書１２２は、サーバ４により発行され、コントローラ１の製造時に記憶部１２に記憶される。

[0019] 登録情報１２３は、図４に示すように、既に登録された機器２を識別する機器ＩＤ、各機器２の公開鍵証明書２２２（図６参照）を識別する証明書Ｉ

Ｄ、共有鍵（事前共有鍵）、グループ鍵、セッション鍵、及び、セッション残り時間を含む。共有鍵は、コントローラ１と各機器２との間でそれぞれ共有される。グループ鍵は、コントローラ１が各機器２に一斉送信する情報の暗号化及び復号化に用いられる。同一のグループに属する機器２は、同一のグループ鍵をコントローラ１と共有する。セッション鍵は、コントローラ１と各機器２との間のユニキャスト通信の暗号化及び復号化に用いられる。セッション残り時間は、コントローラ１と各機器２との間で設定される、セッションが有効である残り時間である。

[0020] 処理部１０は、証明書認証部１０１と、有効期限設定部１０２と、共有鍵認証部１０３と、更新処理部１０４とを論理構造として有する。処理部１０は、中央演算装置（ＣＰＵ）等の処理装置からなる。

[0021] 証明書認証部１０１は、公開鍵証明書１２２及び認証する対象機器である機器２の公開鍵証明書２２２を用いて、機器２と相互認証することにより、機器２と共有する共有鍵を生成する。有効期限設定部１０２は、公開鍵証明書１２２及び公開鍵証明書２２２のいずれかの有効期限を、証明書認証部１０１により生成された共有鍵に設定する。

[0022] 共有鍵認証部１０３は、共有鍵に設定された有効期限が切れていない場合において、公開鍵証明書１２２及び公開鍵証明書２２２を用いず、証明書認証部１０１により生成された共有鍵を用いて機器２と相互認証する。更新処理部１０４は、共有鍵に設定された有効期限が切れている場合において、公開鍵証明書１２２を新たな公開鍵証明書１２２に更新する。

[0023] 機器２（第２機器）は、例えば、エアコン、冷蔵庫、照明装置等の負荷機器、太陽電池、蓄電池等の電源機器の他、スマートメータ等からそれぞれ構成される。機器２は、コントローラ１に登録されることによりＨＥＭＳ５に加入し、コントローラ１と暗号化通信を行う通信機器である。機器２は、制御機能、管理機能等を有するコントローラ１と同等の機器であってもよい。なお、管理機能を有する機器が同一ネットワークにおいて複数存在する場合、先に接続される機器のみが管理機能を発現し、後に接続される機器は管理

機能を発現しない。

[0024] 各機器２は、図５に示すように、処理部２０と、処理部２０の制御に応じてコントローラ１と通信する通信部２１と、プログラムや各種データを記憶する記憶部２２とを備える。通信部２１が行う通信は、無線通信であっても有線通信であってもよい。記憶部２２は、機器２自身の秘密鍵２２１及び公開鍵証明書２２２と、機器２自身が登録されるコントローラ１に関する情報である登録情報２２３とを記憶する。

[0025] 公開鍵証明書２２２は、公開鍵証明書１２２と同様に、公開鍵証明書２２２のバージョン、発行者、有効期間の開始時、有効期間の終了時（有効期限）、証明書ＩＤ、機器２の公開鍵、及び、サーバ４の署名を含む。公開鍵証明書２２２の公開鍵は、秘密鍵２２１に対応する。公開鍵証明書２２２の署名は、サーバ４の秘密鍵を用いて作成される。公開鍵証明書２２２は、サーバ４により発行され、機器２の製造時に記憶部２２に記憶される。

[0026] 登録情報２２３は、図６に示すように、機器２自身が登録されるコントローラ１を識別するコントローラＩＤ、コントローラ１の公開鍵証明書１２２を識別する証明書ＩＤ、共有鍵、グループ鍵、セッション鍵、及び、セッション残り時間を含む。共有鍵は、コントローラ１と各機器２との間で共有される。グループ鍵は、コントローラ１が機器２に対して一斉送信する情報の暗号化及び復号化に用いられる。セッション鍵は、コントローラ１との間のユニキャスト通信の暗号化及び復号化に用いられる。セッション残り時間は、コントローラ１との間で設定される、セッションが有効な残り時間である。

[0027] 処理部２０は、証明書認証部２０１と、有効期限設定部２０２と、共有鍵認証部２０３と、更新処理部２０４とを論理構造として有する。処理部２０は、ＣＰＵ等の処理装置からなる。

[0028] 証明書認証部２０１は、公開鍵証明書２２２及び認証の対象機器であるコントローラ１の公開鍵証明書１２２を用いて、コントローラ１と相互認証することにより、コントローラ１と共有する共有鍵を生成する。有効期限設定

部２０２は、公開鍵証明書２２２及び公開鍵証明書１２２のいずれかの有効期限を、証明書認証部２０１により生成された共有鍵に設定する。

[0029] 共有鍵認証部２０３は、共有鍵に設定された有効期限が切れていない場合において、公開鍵証明書２２２及び公開鍵証明書１２２を用いず、証明書認証部２０１により生成された共有鍵を用いて機器２と相互認証する。更新処理部２０４は、共有鍵に設定された有効期限が切れている場合において、公開鍵証明書２２２を新たな公開鍵証明書２２２に更新する。

[0030] （認証方法）

図７のシーケンス図を参照して、本実施の形態に係る認証システムによる認証方法を説明する。

[0031] 先ず、ステップＳ１において、機器２の証明書認証部２０１は、通信部２１を介して、公開鍵証明書を用いた認証を要求する認証要求、自身の機器ＩＤ及び公開鍵証明書２２２をコントローラ１に送信する。コントローラ１の通信部１１は、ステップＳ１において機器２から送信された認証要求、機器ＩＤ及び公開鍵証明書２２２を受信する。

[0032] ステップＳ２において、コントローラ１の証明書認証部１０１は、通信部１１を介して取得した認証要求に応じて、証明書認証部２０１と共に、公開鍵証明書１２２及び公開鍵証明書２２２を用いた相互認証を行う。ステップＳ２における相互認証は、公開鍵基盤（ＰＫＩ）に基づく相互認証である。

[0033] 証明書認証部１０１及び証明書認証部２０１は、互いの公開鍵証明書の正当性を確認し、相互認証が成功することにより、鍵交換方式により共有鍵を生成する。有効期限設定部１０２及び有効期限設定部２０２は、証明書認証部１０１及び証明書認証部２０１により、コントローラ１及び機器２に共有された共有鍵に、公開鍵証明書１２２及び公開鍵証明書２２２のいずれかの有効期限を設定する。なお、証明書認証部１０１及び証明書認証部２０１は、公開鍵証明書を用いた相互認証が失敗した場合、処理を終了する。

[0034] ステップＳ３において、共有鍵認証部１０３及び共有鍵認証部２０３は、コントローラ１及び機器２に共有された共有鍵に設定された有効期限が切れ

ていない場合において、公開鍵証明書１２２及び公開鍵証明書２２２を用いず、共有鍵を用いて相互認証する。共有鍵認証部１０３及び共有鍵認証部２０３は、互いの共有鍵の正当性を確認し、相互認証が成功することにより、必要な場合、グループ鍵、セッション鍵及びセッション有効期間等を設定する。なお、共有鍵認証部１０３及び共有鍵認証部２０３は、共有鍵を用いた相互認証が失敗した場合、処理を終了する。

[0035] ステップＳ４において、共有鍵認証部２０３は、共有鍵、設定したグループ鍵、セッション鍵及びセッション有効期間等を、コントローラ１のコントローラＩＤ及び公開鍵証明書１２２の証明書ＩＤと関連付けて登録情報２２３として登録する。

[0036] ステップＳ５において、共有鍵認証部１０３は、コントローラ１のコントローラＩＤ及び公開鍵証明書１２２の証明書ＩＤと、機器２の機器ＩＤ及び公開鍵証明書２２２の証明書ＩＤとを、通信部１１を介して、サーバ４に送信する。このとき通信部１１は、サーバ４とＳＳＬ（Ｓｅｃｕｒｅ Ｓｏｃｋｅｔ Ｌａｙｅｒ）通信を行う。

[0037] ステップＳ６において、共有鍵認証部１０３は、共有鍵、設定したグループ鍵、セッション鍵及びセッション有効期間等を、機器２の機器及び公開鍵証明書２２２の証明書ＩＤと関連付けて登録情報２２３として登録する。

[0038] ステップＳ７において、サーバ４は、ステップＳ５において送信されたコントローラ１のコントローラＩＤ及び公開鍵証明書１２２の証明書ＩＤと、機器２の機器ＩＤ及び公開鍵証明書２２２の証明書ＩＤとを受信し、認証された通信機器として登録する。なお、ステップＳ５とステップＳ７の動作を省略してもよい。

[0039] （公開鍵証明書を用いた相互認証）

図８のシーケンス図を参照して、図７のシーケンス図のステップＳ２における公開鍵証明書を用いた相互認証の処理の一例を説明する。

[0040] ステップＳ２１において、証明書認証部１０１は、機器２から送信された公開鍵証明書２２２の有効性を、証明書失効リスト（ＣＲＬ）等で検証する

。その他、証明書認証部１０１は、公開鍵証明書２２２の有効期限を検証する。証明書認証部１０１は、公開鍵証明書２２２が有効と確認される場合、ステップＳ２２に処理を進め、失効と判断される場合、処理を終了する。

[0041] ステップＳ２２において、証明書認証部１０１は、公開鍵証明書２２２の署名を、サーバ４の公開鍵を用いて検証する。証明書認証部１０１は、公開鍵証明書２２２の署名が正当と確認される場合、ステップＳ２３に処理を進め、失効と判断される場合、処理を終了する。

[0042] ステップＳ２３において、証明書認証部１０１は、通信部１１を介して、コントローラ１のコントローラＩＤ及び公開鍵証明書１２２を、認証要求を送信した機器２に送信する。機器２の証明書認証部２０１は、コントローラ１から送信されたコントローラＩＤ及び公開鍵証明書１２２を、通信部２１を介して取得する。

[0043] ステップＳ２４において、証明書認証部２０１は、公開鍵証明書１２２の有効性を、ＣＲＬ、有効期限等で検証する。証明書認証部２０１は、公開鍵証明書２２２が有効と確認される場合、ステップＳ２５に処理を進め、失効と判断される場合、処理を終了する。

[0044] ステップＳ２５において、証明書認証部２０１は、公開鍵証明書１２２の署名を、サーバ４の公開鍵を用いて検証する。証明書認証部２０１は、公開鍵証明書１２２の署名が正当と確認される場合、ステップＳ２６に処理を進め、失効と判断される場合、処理を終了する。

[0045] ステップＳ２６において、証明書認証部２０１は、公開鍵証明書１２２に対する検証が成功した旨を通知する成功通知をコントローラ１に送信する。なお、ステップＳ２１～ステップＳ２６における電子署名方式及び検証方法は、楕円曲線デジタル署名アルゴリズム（ＥＣＤＳＡ）に基づくものとすることができる。

[0046] ステップＳ２７及びステップＳ２８において、証明書認証部１０１及び証明書認証部２０１は、鍵交換方式により、共有鍵を生成する。この鍵交換方式は、楕円曲線ディフィー・ヘルマン鍵共有（ＥＣＤＨ）方式とすることが

できる。また、共有鍵は、高度暗号化標準（ＡＥＳ）の鍵長１２８ビットを用いることとし、上記で共有した値からハッシュ値を計算し、計算したハッシュ値の上位１２８ビットとすることができる。

[0047] 有効期限設定部１０２及び有効期限設定部２０２は、証明書認証部１０１及び証明書認証部２０１により生成された共有鍵に、公開鍵証明書１２２及び公開鍵証明書２２２のいずれかの有効期限を設定する。有効期限設定部１０２及び有効期限設定部２０２は、例えば、公開鍵証明書１２２及び公開鍵証明書２２２の有効期限のうち、短い方の有効期限を共有鍵の有効期限として設定する。記憶部１２及び記憶部２２は、共有鍵及び共有鍵に設定された有効期限を互いに関連付けて記憶する。

[0048] （共有鍵を用いた相互認証）

図９のシーケンス図を参照して、図７のシーケンス図のステップＳ３における共有鍵を用いた相互認証の処理の一例を説明する。共有鍵を用いた相互認証は、チャレンジレスポンス認証方式により行われる。

[0049] ステップＳ３０１及びステップＳ３０２において、共有鍵認証部１０３及び共有鍵認証部２０３は、共有鍵に設定された有効期限を確認する。有効期限の確認は、所定のタイミングで行われる。有効期限の確認は、例えば、コントローラ１と機器２との通信のセッション更新時に行われるようにしてもよい。

[0050] 共有鍵の有効期限が切れている場合、証明書認証部１０１は、現在の処理を停止して機器２からの新たな認証要求を待機する。或いは、証明書認証部１０１は、現状の公開鍵証明書１２２を用いて新たな認証要求を機器２に送信するようにしてもよい。共有鍵認証部１０３は、有効期限が切れていない場合、ステップＳ３０３に処理を進める。ステップＳ３０３において、共有鍵認証部１０３は、任意の乱数Ａを生成し、通信部１１を介して機器２に送信する。

[0051] ステップＳ３０４において、共有鍵認証部２０３は、コントローラ１から送信され、通信部２１を介して取得した乱数Ａを、共有鍵を用いて暗号化し

、暗号化乱数ａを算出する。また、共有鍵認証部２０３は、任意の乱数Ｂを生成する。ステップＳ３０５において、共有鍵認証部２０３は、算出した暗号化乱数ａ及び生成した乱数Ｂを、通信部２１を介してコントローラ１に送信する。

[0052] ステップＳ３０６において、共有鍵認証部１０３は、機器２から送信された暗号化乱数ａ及び乱数Ｂを、通信部１１を介して取得し、暗号化乱数ａを、共有鍵を用いて復号化する。共有鍵認証部１０３は、復号結果と乱数Ａとが一致した場合、乱数Ａに対する検証が成功したものとして、ステップＳ３０７に処理を進め、復号結果と乱数Ａとが一致しない場合、処理を終了する。

[0053] ステップＳ３０７において、共有鍵認証部１０３は、機器２から送信された乱数Ｂを、共有鍵を用いて暗号化し、暗号化乱数ｂを算出する。

[0054] ステップＳ３０８において、共有鍵認証部１０３は、必要な場合、グループ鍵を生成する。グループ鍵は、例えばＡＥＳの鍵長１２８ビットとすることができる。或いは、共有鍵認証部１０３は、登録情報１２３を参照し、既に生成済みのグループ鍵を取得する。ステップＳ３０９において、共有鍵認証部１０３は、セッション鍵を生成する。セッション鍵は、例えばＡＥＳの鍵長１２８ビットとすることができる。

[0055] ステップＳ３１０において、共有鍵認証部１０３は、所定のセッション有効期間（例えば２４時間、７２時間等）を設定する。ステップＳ３１１において、共有鍵認証部１０３は、ステップＳ３０８及びステップＳ３０９において取得したグループ鍵及びセッション鍵を、共有鍵を用いて暗号化する。なお、ステップＳ３０８～ステップＳ３１１における処理は、通信のためにグループ鍵及びセッション鍵の生成が必要な場合に行われる処理であり、省略可能である。

[0056] ステップＳ３１２において、共有鍵認証部１０３は、暗号化乱数ｂ、暗号化されたグループ鍵及びセッション鍵、セッション有効期間を、通信部１１を介して機器２に送信する。機器２の通信部２１は、コントローラ１から送

信された暗号化乱数ｂ、暗号化されたグループ鍵及びセッション鍵、セッション有効期間を受信する。

[0057] ステップＳ３１３において、共有鍵認証部２０３は、通信部２１から取得した暗号化乱数ｂを、共有鍵を用いて復号化する。共有鍵認証部２０３は、復号結果と乱数Ｂとが一致した場合、乱数Ｂに対する検証が成功したものとして、ステップＳ３１４に処理を進め、復号結果と乱数Ｂとが一致しない場合、処理を終了する。

[0058] ステップＳ３１４において、共有鍵認証部２０３は、暗号化されたグループ鍵及びセッション鍵を、共有鍵を用いて復号化する。また、ステップＳ３１５において、乱数Ｂに対する検証が成功した旨を通知する成功通知をコントローラ１に送信する。

[0059] （有効期限切れの場合の処理）

図１０のシーケンス図を参照して、図９のシーケンス図のステップＳ３０１及びステップＳ３０２において、共有鍵の有効期限を確認した結果、有効期限が切れていた場合の他の処理の一例を説明する。

[0060] ステップＳ１１において、更新処理部１０４は、新たな秘密鍵１２１及び新たな秘密鍵１２１に対応する新たな公開鍵を生成する。ステップＳ１２において、更新処理部１０４は、生成した新たな公開鍵を、通信部１１を介してサーバ４に送信する。

[0061] ステップＳ１３において、サーバ４は、ステップＳ１２において送信された公開鍵を受信し、公開鍵にサーバ４の署名等を付し、新たな公開鍵証明書１２２を発行する。ステップＳ１４において、サーバ４は、新たな公開鍵証明書１２２をコントローラ１に送信する。

[0062] ステップＳ１５において、更新処理部１０４は、ステップＳ１４において送信された新たな公開鍵証明書１２２を受信し、記憶部１２に既に記憶される公開鍵証明書１２２を新たな公開鍵証明書１２２に置き換えて記憶させる。このようにコントローラ１は、有効な新たな公開鍵証明書１２２を用いて機器２と相互認証を行い、新たな有効期限が設定された共有鍵を生成するこ

とができる。

[0063] 本実施の形態に係る認証システムによれば、公開鍵証明書１２２又は公開鍵証明書２２２の有効期限を共有鍵に設定することにより、公開鍵証明書の有効期限を考慮して共有鍵による相互認証が可能であり、通信の安全性及び信頼性を向上することができる。

[0064] また、本実施の形態に係る認証システムによれば、公開鍵証明書１２２及び公開鍵証明書２２２の有効期限のうち、短い方の期限を共有鍵に設定することにより、通信の安全性及び信頼性を更に向上することができる。

[0065] また、本実施の形態に係る認証システムによれば、有効期限の確認をセッション更新毎に行うことにより、有効でない共有鍵を検知する効率を向上し、通信の安全性及び信頼性を更に向上することができる。

[0066] ≪レガシー機器への対応≫

ところで、実運用としては、上述したような電子証明書を用いた相互認証（以下、「機器認証」という。）に対応している機器と対応していない機器とが混在する環境がある。このような環境でも、機器認証に対応していない機器を安全に操作することが望まれる。

[0067] 以下、本実施の形態に係る通信システムについて説明する。以下の説明では、機器認証に対応している機器を「認証対応機器」といい、機器認証に対応していない機器を「レガシー機器」という。機器認証については、≪基本構成≫において説明した通りである。

[0068] （通信システム）

図１１は、本実施の形態に係る通信システムにおいてレガシー機器への対応が必要なケースを説明するための概念図である。ここでは、図１１の左側に示すように、コントローラ（レガシー）３１、機器（レガシー）３２、及び、メディアコンバータ（レガシー）３３等のレガシー機器のみで通信システムが構成されている場合を想定している。

[0069] このような通信システムにおいて、ケース１は、新機器（機器認証対応）４２を新たに導入したケースを示している。コントローラ（レガシー）３１

から新機器（機器認証対応）４２を操作することは禁止されているため、新たに導入した新機器（機器認証対応）４２を操作することができない問題がある。この問題の対策としては、コントローラ（レガシー）３１をファームアップ又は交換することが考えられる。

[0070] 次に、ケース２は、新コントローラ（機器認証対応）４１を新たに導入したケースを示している。新コントローラ（機器認証対応）４１は、機器認証に対応しているものの、機器（レガシー）３２等のレガシー機器は、機器認証に対応していない。そのため、新コントローラ（機器認証対応）４１と機器（レガシー）３２との相互認証は失敗することになる。すなわち、新たに導入した新コントローラ（機器認証対応）４１からレガシー機器を操作することができない問題がある。この問題の対策としては、新コントローラ（機器認証対応）４１によるレガシー機器の操作を条件付きで許容することが考えられる（後述する）。

[0071] 最後に、ケース３は、新機器（機器認証対応）４２と新コントローラ（機器認証対応）４１を新たに導入したケースを示している。このケース３でも、機器（レガシー）３２等のレガシー機器が混在する以上、ケース２と同様の問題がある。

[0072] （新コントローラ）

図１２は、本実施の形態に係る通信システムが備える新コントローラ（機器認証対応）４１の基本的な構成を説明するブロック図である。新コントローラ（機器認証対応）４１は、電子証明書を用いた相互認証に成功した機器と暗号化通信を行うコントローラであって、図１２に示すように、処理部１０と、通信部１１と、記憶部１２と、表示部１３とを備える。処理部１０には、判定部１０５と、機能制限部１０６と、画面生成部１０７が含まれる。記憶部１２には、ホワイトリスト１２４と、機能制限情報１２５とが含まれる。

[0073] 判定部１０５は、通信対象の機器が認証対応機器であるか否かを判定する。機能制限部１０６は、判定部１０５により認証対応機器でないと判定され

た場合、その通信対象の機器が有する機能のうち、新コントローラ（機器認証対応）４１から操作可能な機能を制限する。通信部１１は、機能制限部１０６による機能制限のもと通信対象の機器と平文で通信を行う。これにより、新コントローラ（機器認証対応）４１とレガシー機器とを接続し、新コントローラ（機器認証対応）４１によるレガシー機器の操作を条件付きで許容することが可能である。

[0074] 画面生成部１０７は、各種の画面を生成する。表示部１３は、画面生成部１０７により生成された各種の画面を表示する表示装置である。ホワイトリスト１２４は、ＡＩＦ等の特定の規格に合致する機器に関する情報（メーカー、型番等）を列挙した許可リストである。機能制限情報１２５は、段階的なセキュリティレベルに応じて異なる強度の機能制限を規定した情報であり、機能制限部１０６によって参照される。その他の各処理部については、上述の≪基本構成≫において説明した通りである。

[0075] なお、新コントローラ（機器認証対応）４１と表示部１３とは一体でなくてもよい。すなわち、表示部１３は、新コントローラ（機器認証対応）４１と通信可能な表示装置であればよく、例えば、スマートフォンなどの別端末機であってもよい。

[0076] （ＡＩＦ）

エアコン、照明、蓄電池、給湯機、電気自動車充放電器、燃料電池、太陽光発電及びスマートメータは、ＨＥＭＳにおいて相互接続がより重要な機器と位置付けられている。ＡＩＦ（Application Interface）は、このような重要な機器について、相互接続性向上のため、ＥＣＨＯＮＥＴ－Ｌｉｔｅのアプリケーションレベルでの使い方を規定した仕様書である。

[0077] ＡＩＦに対応している機器は、ユニバーサルなＥＣＨＯＮＥＴ－Ｌｉｔｅ規格に準拠しているレガシー機器に比べて認証の機能は高いと言える。そのため、ＡＩＦに対応している機器に対する機能制限は、レガシー機器に対する機能制限に比べて緩和する。

[0078] 具体的には、判定部１０５は、通信対象の機器が認証対応機器でないと判

定した場合、更に、通信対象の機器が許可リスト（ホワイトリスト１２４）に合致した許可機器であるか許可リストに合致しない非許可機器（レガシー機器）であるかを判定する。このようにすれば、判定部１０５により許可機器であると判定された場合は非許可機器であると判定された場合に比べて機能制限を少なくすることができる。

[0079] （接続例）

以下、新コントローラ（機器認証対応）４１の構成をその動作とともに説明する。ここでは、図１３に示すように、新機器（機器認証対応）４２、機器（ＡＩＦ対応）５２、機器（レガシー）３２等の様々な機器が混在する環境を想定している。また、機器認証は、ボタン押下をトリガーとして実行されるものとする。

[0080] まず、ユーザが新コントローラ（機器認証対応）４１と新機器（機器認証対応）４２のボタンを押下したとする。これにより、新コントローラ（機器認証対応）４１は、新機器（機器認証対応）４２と機器認証を実行することで、認証対応機器であるか否かを判定する（図１４、ステップＳ３１→Ｓ３２→Ｓ３３）。そして、新機器（機器認証対応）４２から機器ＩＤや公開鍵証明書２２２等を受信すると、認証対応機器であると判定する（図１４、ステップＳ３３：ＹＥＳ）。このように認証対応機器であると判定した場合、セキュリティレベルを「３」と判定し（図１４、ステップＳ３４）、通常通り新機器（機器認証対応）４２に接続する。この場合、暗号化通信により安全に接続することが可能である。

[0081] 次に、ユーザが新コントローラ（機器認証対応）４１と機器（ＡＩＦ対応）５２のボタンを押下したとする。これにより、新コントローラ（機器認証対応）４１は、機器（ＡＩＦ対応）５２と機器認証を実行することで、認証対応機器であるか否かを判定する（図１４、ステップＳ３１→Ｓ３２→Ｓ３３）。そして、機器（ＡＩＦ対応）５２から平文を受信すると、認証対応機器でないと判定する（図１４、ステップＳ３３：ＮＯ）。すなわち、相互認証の開始時に平文（ＥＣＨＯＮＥＴに準拠したパケット）を受信した場合は

、認証対応機器でないと判定するようになっている。このように認証対応機器でないと判定した場合、更に、ホワイトリスト１２４に合致した許可機器（ＡＩＦ対応）であるか否かを判定する（図１４、ステップＳ３５）。ＡＩＦ対応であるかどうかの判定は、機器（ＡＩＦ対応）５２から受信したＥＣＨＯＮＥＴに準拠したパケットに基づいて行う。このとき、ＡＩＦ対応であるかどうかを判定できなければ、機器（ＡＩＦ対応）５２から更なる情報を取得してもよい。機器（ＡＩＦ対応）５２は、ホワイトリスト１２４に合致するため、許可機器（ＡＩＦ対応）であると判定することになる（図１４、ステップＳ３５：ＹＥＳ）。このように許可機器（ＡＩＦ対応）であると判定した場合、セキュリティレベルを「２」と判定し（図１４、ステップＳ３６）、ユーザ確認のもと機器（ＡＩＦ対応）５２に接続する。なお、この場合、機能制限をして機器（ＡＩＦ対応）５２に接続するようにしてもよい。

[0082] 次に、ユーザが新コントローラ（機器認証対応）４１と機器（レガシー）３２のボタンを押下したとする。これにより、新コントローラ（機器認証対応）４１は、機器（レガシー）３２と機器認証を実行し、認証対応機器であるか否かを判定する（図１４、ステップＳ３１→Ｓ３２→Ｓ３３）。そして、機器（レガシー）３２から平文を受信すると、認証対応機器でないと判定し（図１４、ステップＳ３３：ＮＯ）、更に、ホワイトリスト１２４に合致した許可機器（ＡＩＦ対応）であるか否かを判定する（図１４、ステップＳ３５）。機器（レガシー）３２は、ホワイトリスト１２４に合致しないため、許可機器（ＡＩＦ対応）でないと判定することになる（図１４、ステップＳ３５：ＮＯ）。このように許可機器（ＡＩＦ対応）でないと判定した場合、セキュリティレベルを「１」と判定し（図１４、ステップＳ３７）、ユーザ確認のもと機能制限をして機器（レガシー）３２に接続する。

[0083] 以上のように、本実施の形態に係る通信システムでは、段階的なセキュリティレベルを判定し、この段階的なセキュリティレベルに応じて異なる強度の機能制限を課すようにしている。これにより、機器認証に対応している機器と対応していない機器とが混在する環境でも、機器認証に対応していない

機器を安全に操作することが可能である。

[0084] なお、機器（レガシー）３２や機器（ＡＩＦ対応）５２への接続期間（運用マター）に問題があった場合は、新コントローラ（機器認証対応）４１から接続を切断してもよい。すなわち、機能制限やユーザ確認があった場合でも、あらかじめ定められた期間制限を許容しない場合は接続を切断するようになっている。これにより、より安全に機器認証に対応していない機器を操作することが可能である。

[0085] （画面例）

図１５は、新コントローラ（機器認証対応）４１の表示部１３に表示される画面例を示す図である。既に説明した通り、機器（レガシー）３２や機器（ＡＩＦ対応）５２に接続する場合は、これら機器への接続許可をユーザに問い合わせる。例えば、機器（ＡＩＦ対応）５２がエアコンＢである場合、図１５に示すように、「エアコンＢは新しい接続方式に対応していませんが、接続しますか？」等のメッセージを表示部１３に表示し、「はい」又は「いいえ」をユーザに選択させてもよい。この確認画面１３Ａにおいて「はい」が選択された場合は、機器（ＡＩＦ対応）５２と通信を行う。

[0086] すなわち、機器（レガシー）３２や機器（ＡＩＦ対応）５２は、機器認証に対応していないため、新コントローラ（機器認証対応）４１からエラーを受信するか、一定時間後にタイムアウトとなる。このような場合でも、新コントローラ（機器認証対応）４１の表示部１３に確認画面１３Ａをポップアップさせ、ユーザによる確認のもと、機器（レガシー）３２や機器（ＡＩＦ対応）５２を新コントローラ（機器認証対応）４１と接続することが可能となっている。

[0087] なお、ここでは、接続許可をユーザに問い合わせることとしているが、確認画面はこれに限定されるものではない。例えば、機器（レガシー）３２や機器（ＡＩＦ対応）５２のファームアップ又は交換を促すメッセージを表示部１３に表示してもよい。これにより、機器（レガシー）３２や機器（ＡＩＦ対応）５２が新機器（機器認証対応）４２に交換された場合は、暗号化通

信により安全に接続することが可能である。

[0088] 図１６は、新コントローラ（機器認証対応）４１の表示部１３に表示される別の画面例を示す図である。この図に示すように、機能制限部１０６による機能制限の一覧を確認するための確認画面１３Ｂを表示部１３に表示してもよい。このような機能制限の一覧は、機能制限情報１２５に基づいて生成することができる。ここでは、機器毎に「セキュリティレベル」「機能制限」「機器削除」を対応付けた場合を例示している。この確認画面１３Ｂにおいて、ユーザ責任で「機能制限」を変更（解除を含む。）することも可能である。ユーザにより「機能制限」が変更された場合、その変更後の機能制限のもとで通信を行う。

[0089] （機能制限情報）

図１７は、新コントローラ（機器認証対応）４１の記憶部１２に記憶される機能制限情報１２５の一例を示す図である。この機能制限情報１２５は、段階的なセキュリティレベルに応じて異なる強度の機能制限を規定したテーブルである。エアコン、蓄電池、太陽光発電、及び、瞬間式給湯器等の機器毎に機能制限情報１２５が規定されている。このようにすれば、新コントローラ（機器認証対応）４１は、各機器の特性に応じた機能制限を実現することが可能である。

[0090] 図１７に示すように、セキュリティレベル１の場合は「機能制限あり」、セキュリティレベル２の場合は「一部機能制限あり」、セキュリティレベル３の場合は「機能制限なし」としている。具体的には、セキュリティレベル１の場合は、新コントローラ（機器認証対応）４１は、基本的な情報（動作状態及び設定情報）の取得コマンドのみ許可する。また、セキュリティレベル２の場合は、新コントローラ（機器認証対応）４１は、セキュリティレベル１の場合に加えて、一部の操作系及び設定系のコマンドを許可する。ただし、課金及びプライバシーに関わる情報の取得と、運転動作状態の設定及び変更に関しては禁止する。セキュリティレベル３でない場合（機器認証に対応していない場合）は、コマンドの改ざんの恐れがあるためである。以下、

エアコン、蓄電池、太陽光発電、及び、瞬間式給湯器等の機器毎に更に詳しく説明する。

[0091] 新コントローラ（機器認証対応）４１は、エアコンについては、セキュリティレベル１の場合、情報取得のみ可とし、操作系は全て禁止する。また、セキュリティレベル２の場合、不安全ではない温度上下限範囲内の温度設定は可とする。

[0092] 新コントローラ（機器認証対応）４１は、蓄電池については、セキュリティレベル１の場合、基本的な情報取得のみ可とし、操作系や電力売買等の課金に関わる電力量情報取得は禁止する。また、セキュリティレベル２の場合、不安全な動作や電力系統に影響を与える可能性のある動作を禁止する。

[0093] 新コントローラ（機器認証対応）４１は、太陽光発電については、セキュリティレベル１の場合、基本的な情報取得のみ可とする。また、セキュリティレベル２の場合、課金に関わる積算発電電力量計測値取得を禁止する。

[0094] 新コントローラ（機器認証対応）４１は、瞬間式給湯器については、セキュリティレベル１の場合もセキュリティレベル２の場合も、基本的な情報取得のみ可とし、ユーザの意図しない給湯器運転の可能性がある風呂自動モード設定を禁止する。

[0095] 以上説明したように、本実施の形態に係る通信システムが備える新コントローラ（機器認証対応）４１は、電子証明書を用いた相互認証に成功した機器と暗号化通信を行うコントローラであって、判定部１０５と、機能制限部１０６と、通信部１１とを備える。判定部１０５は、通信対象の機器が相互認証に対応している認証対応機器であるか否かを判定する。機能制限部１０６は、判定部１０５により認証対応機器でないと判定された場合、その通信対象の機器が有する機能のうち、新コントローラ（機器認証対応）４１から操作可能な機能を制限する。通信部１１は、機能制限部１０６による機能制限のもと通信対象の機器と平文で通信を行う。これにより、機器認証に対応している機器と対応していない機器とが混在する環境でも、機器認証に対応していない機器を安全に操作することが可能である。

[0096] また、判定部１０５は、通信対象の機器が認証対応機器でないと判定した場合、更に、通信対象の機器がホワイトリスト１２４に合致した許可機器であるかホワイトリスト１２４に合致しないレガシー機器であるか否かを判定してもよい。機能制限部１０６は、判定部１０５により許可機器であると判定された場合はレガシー機器であると判定された場合に比べて機能制限が少なくてもよい。これにより、例えば、ＡＩＦに対応している機器に対する機能制限は、レガシー機器に対する機能制限に比べて緩和することが可能である。

[0097] また、機能制限部１０６は、判定部１０５によりレガシー機器であると判定された場合、動作状態及び設定情報の取得コマンドのみ許可してもよい。これにより、レガシー機器が脅威にさらされる可能性を極力抑えることが可能である。

[0098] また、機能制限部１０６は、判定部１０５により許可機器であると判定された場合、動作状態及び設定情報の取得コマンドを許可するほか、操作系及び設定系のコマンドを許可してもよい（ただし、課金及びプライバシーに関わる情報の取得と、運転動作状態の設定及び変更を除く）。これにより、許可機器が脅威にさらされる可能性を低減しながらも、許可機器の特性に応じたコマンドを利用することが可能である。

[0099] 更に、判定部１０５により認証対応機器でないと判定された場合、通信対象の機器への接続許可をユーザに問い合わせるため、新コントローラ（機器認証対応）４１と通信可能な表示部１３に確認画面１３Ａを表示させてもよい。これにより、ユーザ確認のもと通信対象の機器への接続を許可することができるため、必要以上に機能制限される不都合を回避することが可能である。

[0100] 更に、機能制限部１０６による機能制限を変更するため、新コントローラ（機器認証対応）４１と通信可能な表示部１３に確認画面１３Ｂを表示させてもよい。これにより、ユーザ確認のもと機能制限を変更（解除を含む。）することができるため、必要以上に機能制限される不都合を回避することが

可能である。

[0101] また、判定部１０５は、相互認証の開始時にＥＣＨＯＮＥＴに準拠したパケットを受信した場合、認証対応機器でないと判定してもよい。これにより、確実かつ容易に認証対応機器であるかどうかを判定することが可能である。

[0102] なお、上記の説明では、通信対象の機器が認証対応機器であるか許可機器であるかレガシー機器であるかによって３段階のセキュリティレベルを判定することとしているが、セキュリティレベルは２段階以上であればよい。最も高いセキュリティレベルである場合を除き、何らかの機能制限を課すようにすれば、同様の効果が得られる。

[0103] また、許可機器としてＡＩＦに対応している機器を例示したが、何らかの規格に対応している機器であれば、許可機器として採用することができる。複数種類の許可機器を採用する場合は、許可機器毎に異なるセキュリティレベルを設定してもよい。この場合、許可機器毎に異なるセキュリティレベルに応じて異なる強度の機能制限を課すようにしてもよいのはもちろんである。

[0104] また、機器（レガシー）３２や機器（ＡＩＦ対応）５２に接続する場合に確認画面１３Ａを表示することとしているが（図１５参照）、機器（レガシー）３２に接続する場合と機器（ＡＩＦ対応）５２に接続する場合とで異なる確認画面を表示してもよい。これにより、セキュリティレベルが低いほどユーザが接続許可を出しにくくすることも可能である。

[0105] また、判定部１０５は、相互認証の開始時にＥＣＨＯＮＥＴに準拠したパケットを受信した場合、認証対応機器でないと判定することとしているが、認証対応機器を判定するタイミングや判定の方法は特に限定されるものではない。例えば、機器（レガシー）３２や機器（ＡＩＦ対応）５２がＥＣＨＯＮＥＴ以外の規格に準拠している場合は、そのＥＣＨＯＮＥＴ以外の規格に準拠したパケットを受信したかどうかを判定すればよい。

[0106] また、新コントローラ（機器認証対応）４１として実現することができる

だけでなく、新コントローラ（機器認証対応）４１が備える特徴的な処理部を各ステップとする通信方法として実現したり、それらの各ステップをコンピュータに実行させる通信プログラムとして実現したりすることも可能である。このようなプログラムは、ＣＤ－ＲＯＭ等の記録媒体やインターネット等の伝送媒体を介して配信することができるのはいうまでもない。

[0107] （その他の実施の形態）

上記のように、実施の形態を記載したが、この開示の一部をなす論述及び図面は本実施の形態を限定するものであると理解すべきではない。この開示から当業者には様々な代替実施の形態、実施例及び運用技術が明らかとなろう。

[0108] 例えば、既に述べた実施の形態において、図７～図１０のシーケンス図は、コントローラ１と機器２とが逆であっても同様の処理を行うことができるようにしてもよい。

[0109] 上記の他、ここでは記載していない様々な実施の形態等を含むことは勿論である。したがって、本実施の形態の技術的範囲は上記の説明から妥当な請求の範囲に係る発明特定事項によってのみ定められるものである。

符号の説明

[0110] １１、２１ 通信部

１３ 表示部

１３Ａ、１３Ｂ 確認画面

４１ 新コントローラ（機器認証対応），コントローラ

１０５ 判定部

１０６ 機能制限部

１２４ ホワイトリスト（許可リスト）

請求の範囲

[請求項1] 電子証明書を用いた相互認証に成功した機器と暗号化通信を行うコントローラであって、

通信対象の機器が前記相互認証に対応している認証対応機器であるか否かを判定する判定部と、

前記判定部により前記認証対応機器でないと判定された場合、前記通信対象の機器が有する機能のうち、当該コントローラから操作可能な機能を制限する機能制限部と、

前記機能制限部による機能制限のもと前記通信対象の機器と平文で通信を行う通信部とを備える

コントローラ。

[請求項2] 前記判定部は、前記通信対象の機器が前記認証対応機器でないと判定した場合、更に、前記通信対象の機器が許可リストに合致した許可機器であるか前記許可リストに合致しない非許可機器であるか否かを判定し、

前記機能制限部は、前記判定部により前記許可機器であると判定された場合は前記非許可機器であると判定された場合に比べて機能制限が少ない

請求項１に記載のコントローラ。

[請求項3] 前記機能制限部は、前記判定部により前記非許可機器であると判定された場合、動作状態及び設定情報の取得コマンドのみ許可する

請求項２に記載のコントローラ。

[請求項4] 前記機能制限部は、前記判定部により前記許可機器であると判定された場合、動作状態及び設定情報の取得コマンドを許可するほか、課金及びプライバシーに関わる情報の取得と、運転動作状態の設定及び変更を除き、操作系及び設定系のコマンドを許可する

請求項２に記載のコントローラ。

[請求項5] 更に、前記判定部により前記認証対応機器でないと判定された場合

、前記通信対象の機器への接続許可をユーザに問い合わせるため、当該コントローラと通信可能な表示部に確認画面を表示させる

請求項１から４のいずれか１項に記載のコントローラ。

[請求項6] 更に、前記機能制限部による機能制限を変更するため、当該コントローラと通信可能な表示部に確認画面を表示させる

請求項１から５のいずれか１項に記載のコントローラ。

[請求項7] 前記判定部は、前記相互認証の開始時にＥＣＨＯＮＥＴに準拠したパケットを受信した場合、前記認証対応機器でないと判定する

請求項１から６のいずれか１項に記載のコントローラ。

[請求項8] コントローラが電子証明書を用いて相互認証に成功した機器と暗号化通信を行う場合の通信方法であって、

前記コントローラが、通信対象の機器が前記相互認証に対応している認証対応機器であるか否かを判定する判定ステップと、

前記コントローラが、前記判定ステップで前記認証対応機器でないと判定した場合、前記通信対象の機器が有する機能のうち、当該コントローラから操作可能な機能を制限する機能制限ステップと、

前記コントローラが、前記機能制限ステップにおける機能制限のもと前記通信対象の機器と平文で通信を行う通信ステップとを含む

通信方法。

[請求項9] 更に、前記判定ステップで前記認証対応機器でないと判定された場合、前記通信対象の機器への接続許可をユーザに問い合わせるため、当該コントローラと通信可能な表示部に確認画面を表示させる表示ステップを含む

請求項８に記載の通信方法。

[請求項10] 更に、前記機能制限ステップにおける機能制限を変更するため、当該コントローラと通信可能な表示部に確認画面を表示させる表示ステップを含む

請求項８又は９に記載の通信方法。

[請求項11] コントローラが電子証明書を用いて相互認証に成功した機器と暗号化通信を行う通信システムであって、

前記コントローラが、

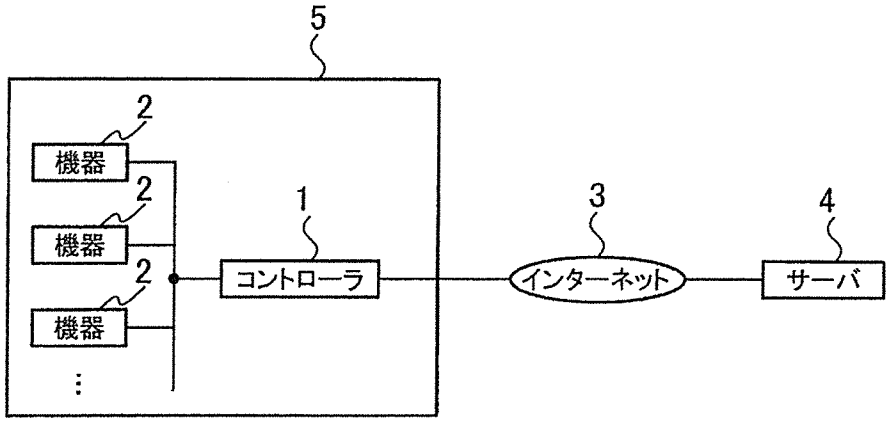
通信対象の機器が前記相互認証に対応している認証対応機器であるか否かを判定する判定部と、

前記判定部により前記認証対応機器でないと判定された場合、前記通信対象の機器が有する機能のうち、当該コントローラから操作可能な機能を制限する機能制限部と、

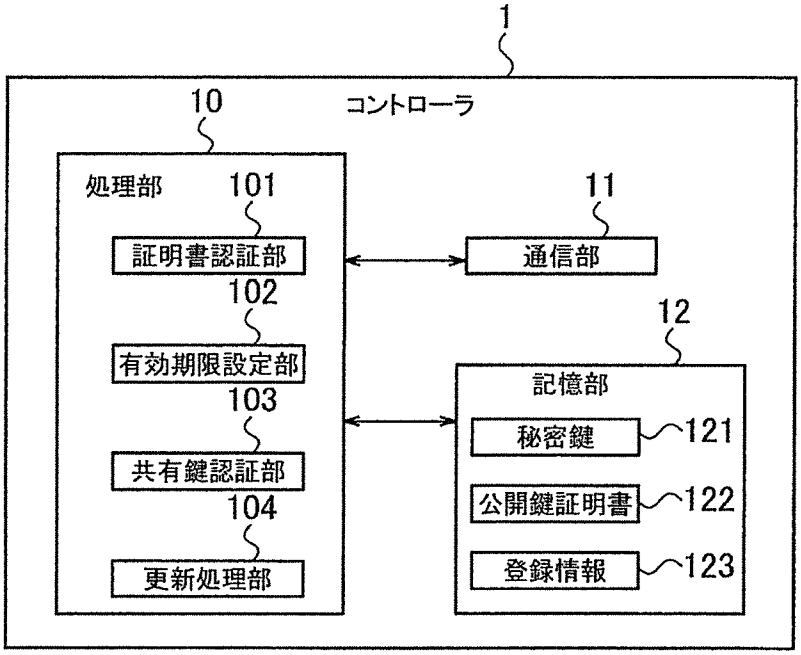
前記機能制限部による機能制限のもと前記通信対象の機器と平文で通信を行う通信部とを備える

通信システム。

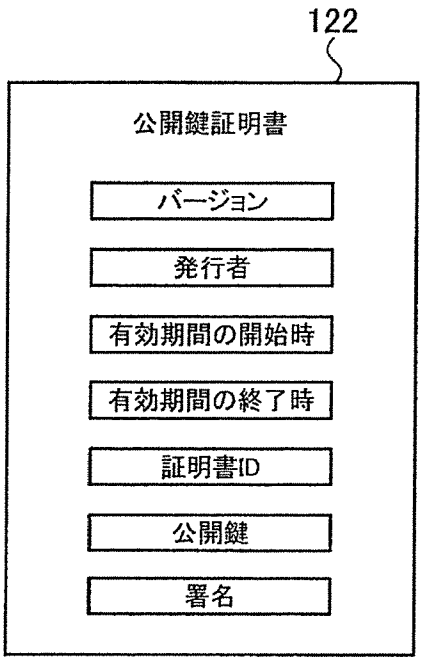
[図1]


5
2
機器
2
機器
2
機器
1
コントローラ
3
インターネット
4
サーバ

[図2]


1
10
コントローラ
処理部
101
証明書認証部
102
有効期限設定部
103
共有鍵認証部
104
更新処理部
11
通信部
12
記憶部
秘密鍵
121
公開鍵証明書
122
登録情報
123

[図3]

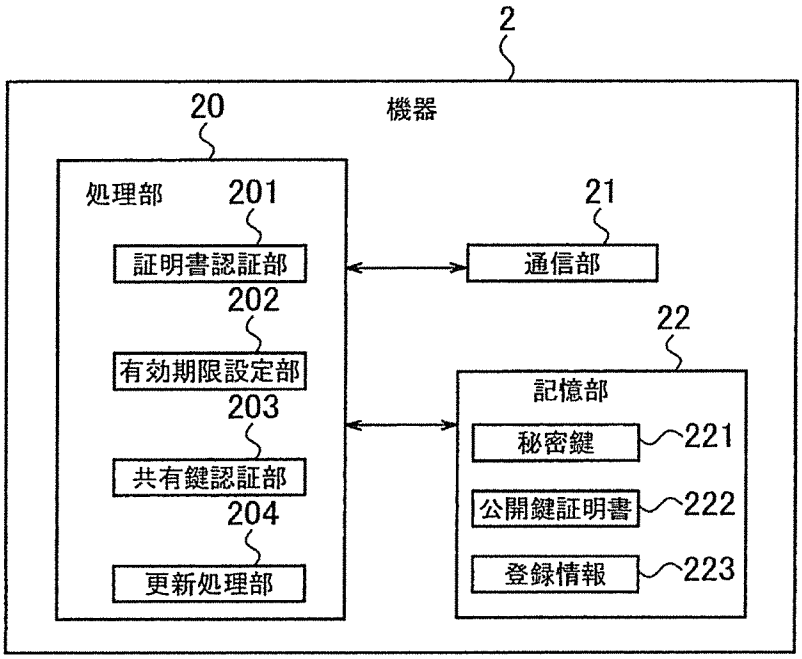

122
公開鍵証明書
バージョン
発行者
有効期間の開始時
有効期間の終了時
証明書ID
公開鍵
署名

[図4]

123

機器ID	証明書ID	共有鍵	グループ鍵	セッション鍵	セッション残り時間
D1	P1	01234…	11223…	11122…	13:40:50
D2	P2	98765…		22233…	13:41:24
D3	P3	19283…		33344…	16:02:13
…	…	…		…	…

[図5]

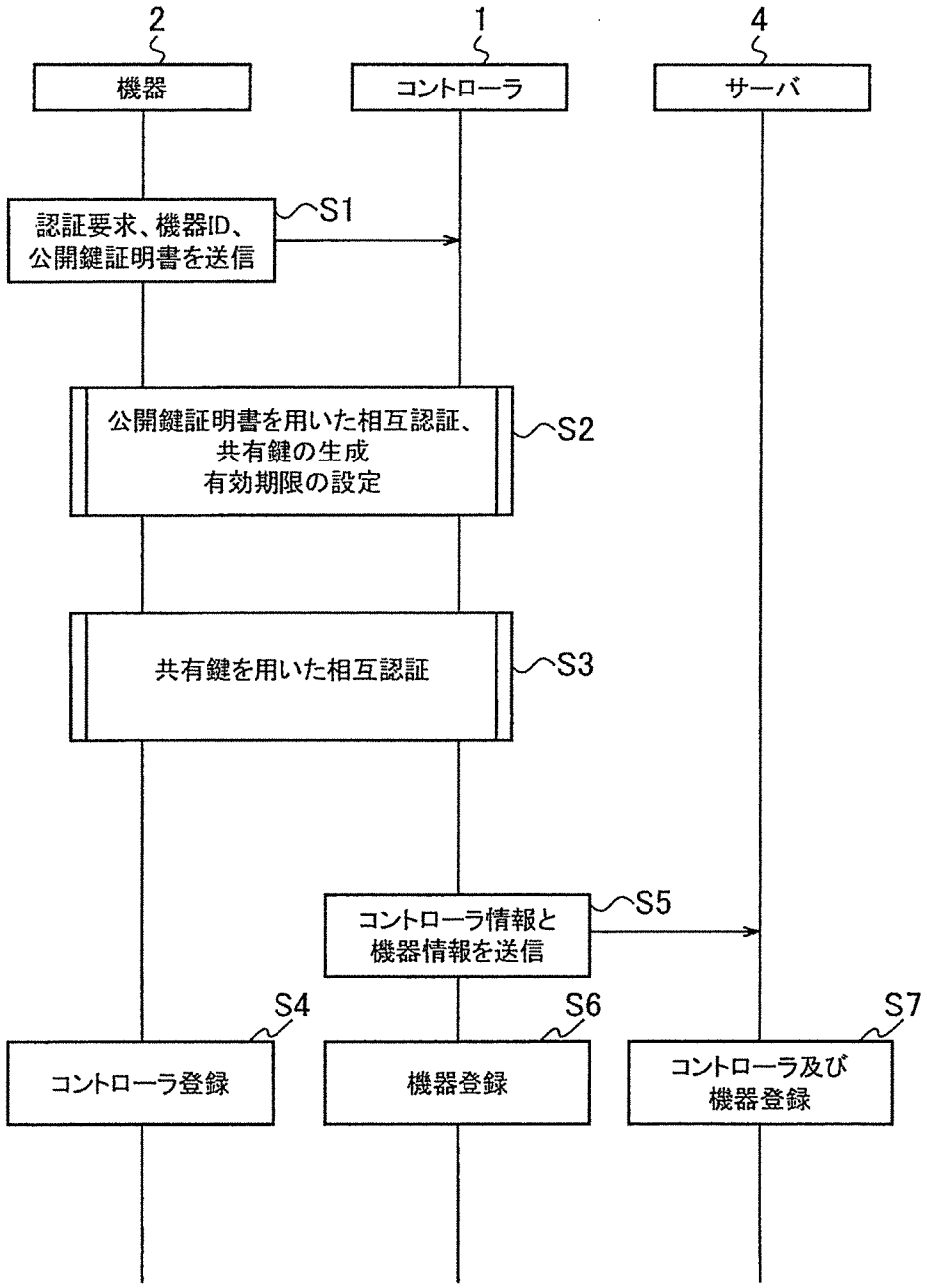


[図6]

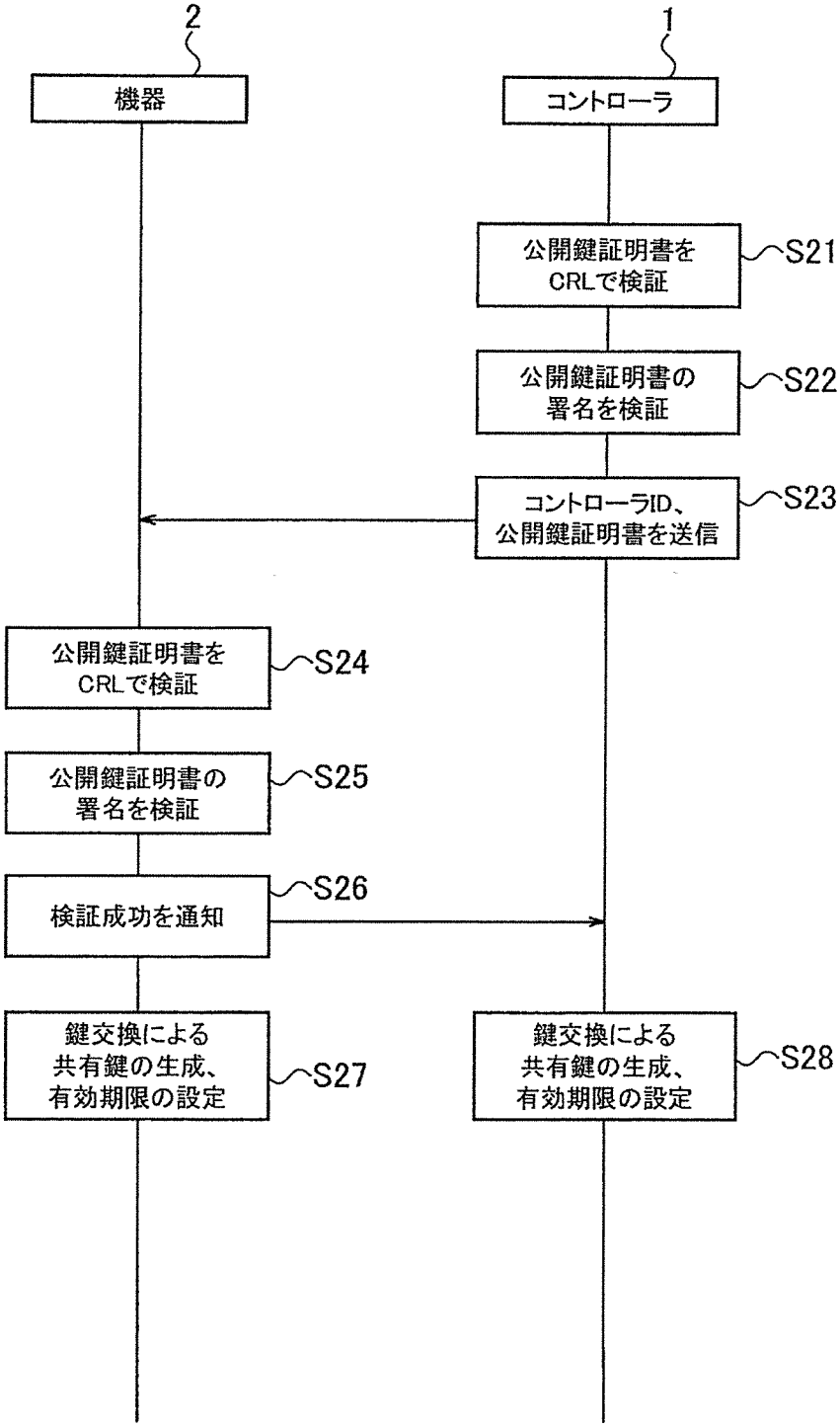
223

コントローラID	証明書ID	共有鍵	グループ鍵	セッション鍵	セッション残り時間
C1	Q1	01234…	11223…	11122…	13:40:50
…	…	…	…	…	…

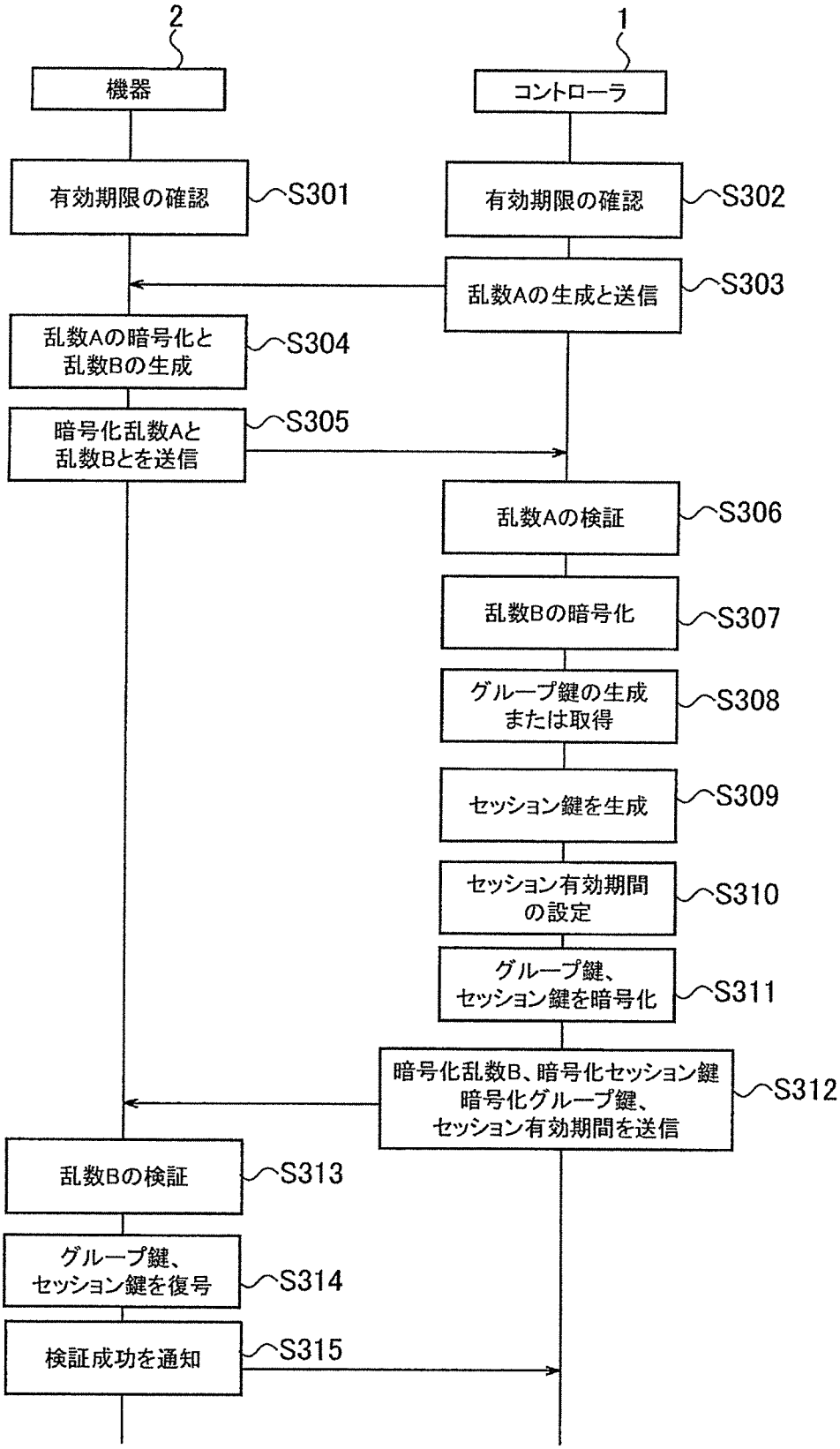
[図7]


2
1
4
機器
コントローラ
サーバ
認証要求、機器ID、
公開鍵証明書を送信
S1
公開鍵証明書を用いた相互認証、
共有鍵の生成
有効期限の設定
S2
共有鍵を用いた相互認証
S3
コントローラ情報と
機器情報を送信
S5
S4
S6
S7
コントローラ登録
機器登録
コントローラ及び
機器登録

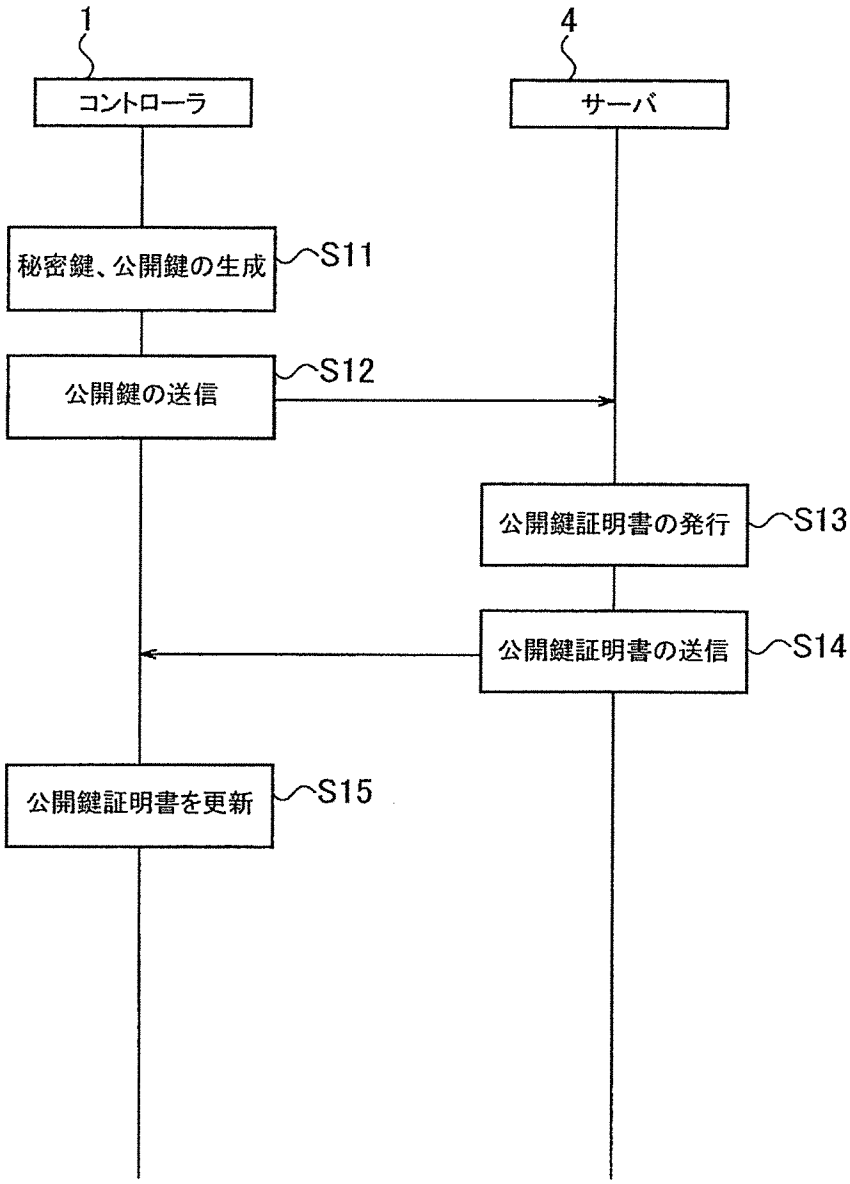
[図8]


2
1
機器
コントローラ
公開鍵証明書を
CRLで検証
S21
公開鍵証明書の
署名を検証
S22
コントローラID、
公開鍵証明書を送信
S23
公開鍵証明書を
CRLで検証
S24
公開鍵証明書の
署名を検証
S25
検証成功を通知
S26
鍵交換による
共有鍵の生成、
有効期限の設定
S27
鍵交換による
共有鍵の生成、
有効期限の設定
S28

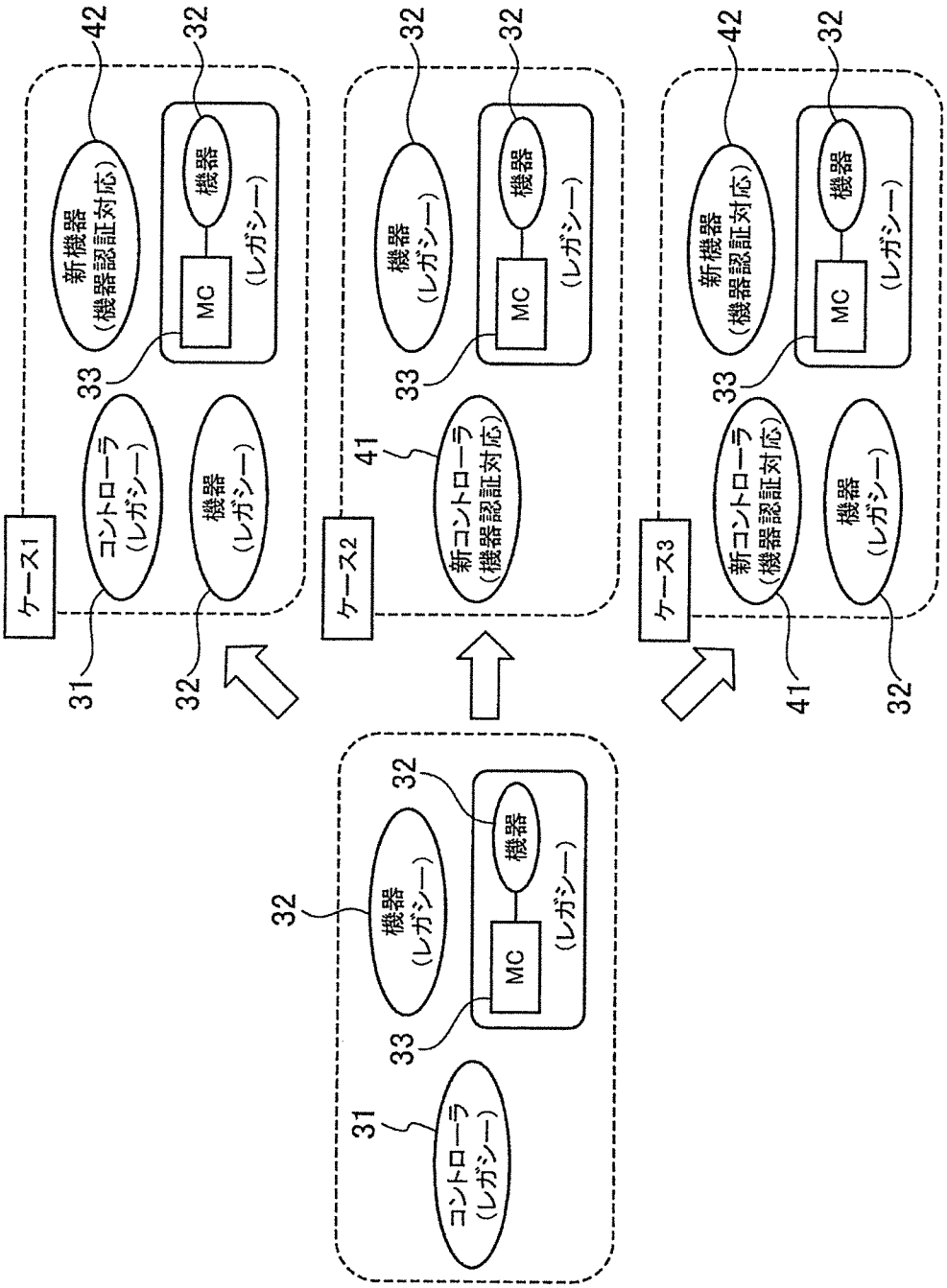
[図9]


2
1
機器
コントローラ
有効期限の確認
S301
有効期限の確認
S302
乱数Aの生成と送信
S303
乱数Aの暗号化と
乱数Bの生成
S304
暗号化乱数Aと
乱数Bとを送信
S305
乱数Aの検証
S306
乱数Bの暗号化
S307
グループ鍵の生成
または取得
S308
セッション鍵を生成
S309
セッション有効期間
の設定
S310
グループ鍵、
セッション鍵を暗号化
S311
暗号化乱数B、暗号化セッション鍵
暗号化グループ鍵、
セッション有効期間を送信
S312
乱数Bの検証
S313
グループ鍵、
セッション鍵を復号
S314
検証成功を通知
S315

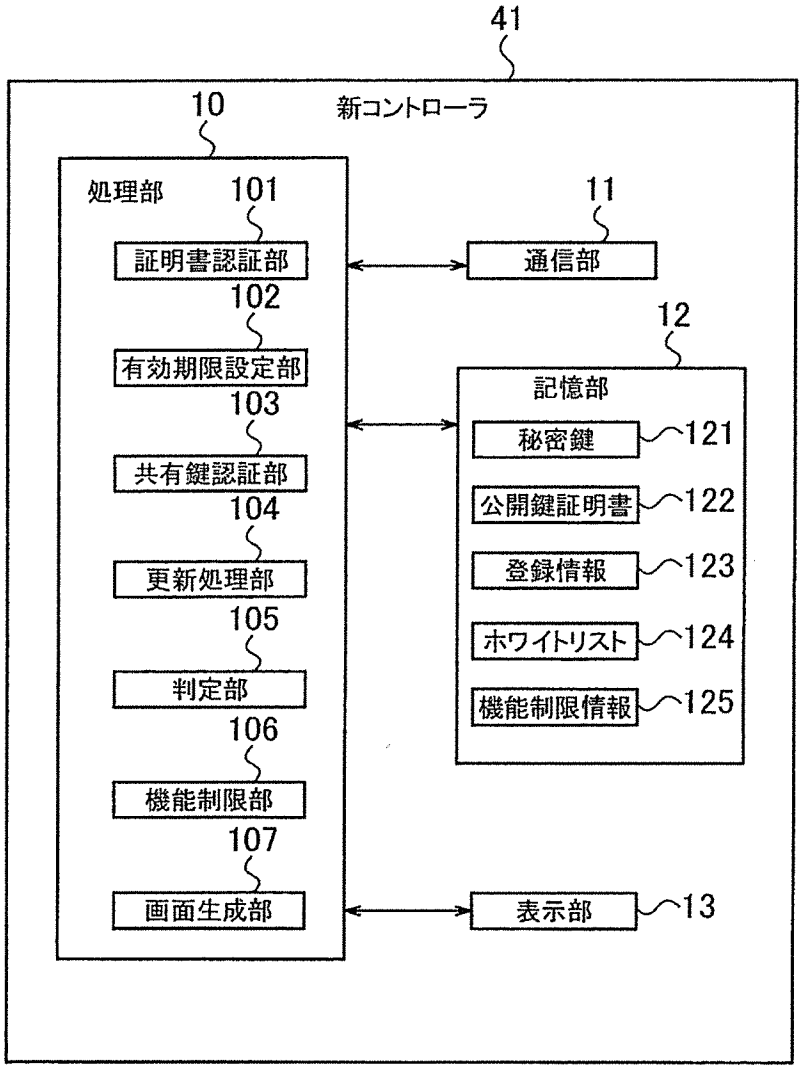
[図10]


1
4
コントローラ
サーバ
秘密鍵、公開鍵の生成
S11
公開鍵の送信
S12
公開鍵証明書の発行
S13
公開鍵証明書の送信
S14
公開鍵証明書を更新
S15

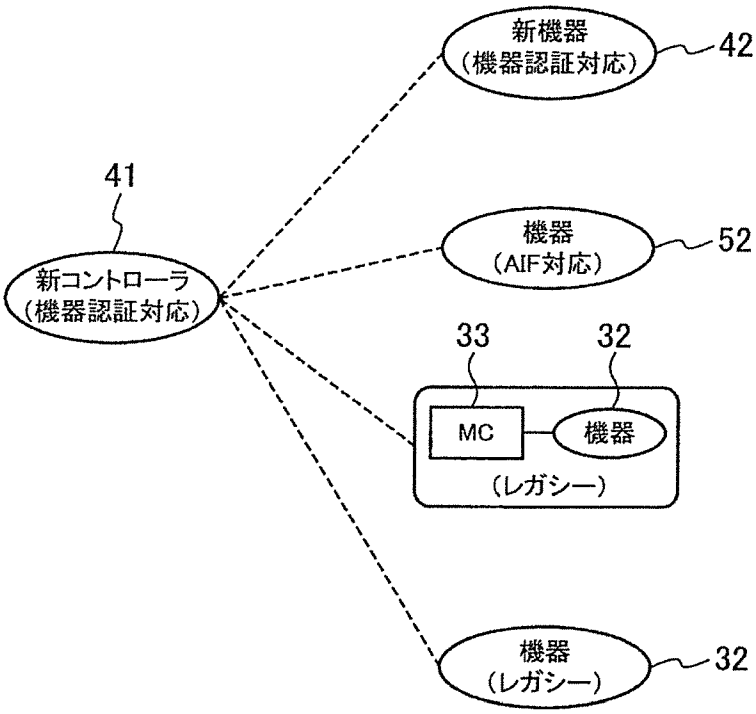
[図11]


ケース1
コントローラ
(レガシー)
31
機器
(レガシー)
32
新機器
(機器認証対応)
42
33
MC
機器
32
(レガシー)
ケース2
新コントローラ
(機器認証対応)
41
機器
(レガシー)
32
33
MC
機器
32
(レガシー)
ケース3
新コントローラ
(機器認証対応)
41
機器
(レガシー)
32
新機器
(機器認証対応)
42
33
MC
機器
32
(レガシー)
コントローラ
(レガシー)
31
機器
(レガシー)
32
33
MC
機器
32
(レガシー)

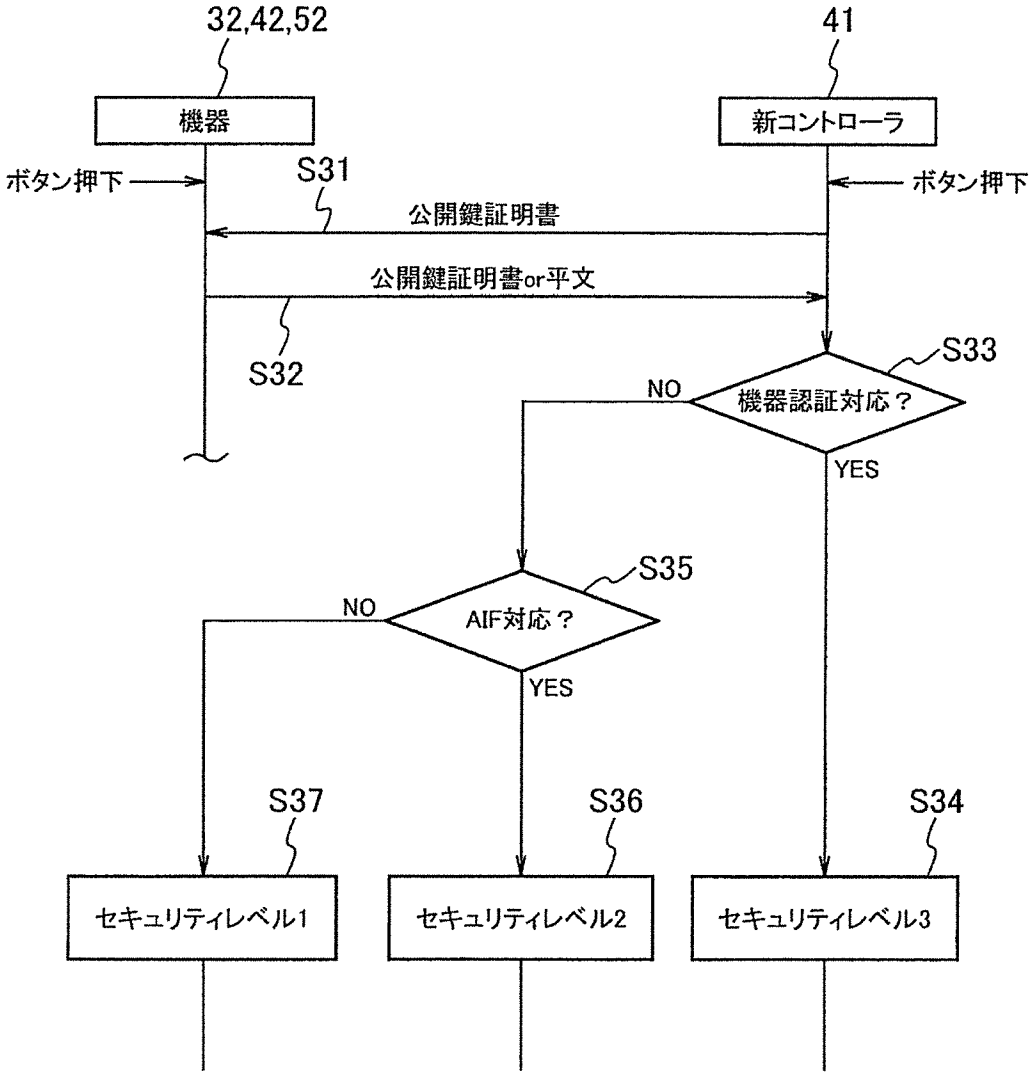
[図12]


41
新コントローラ
10
処理部
101
証明書認証部
102
有効期限設定部
103
共有鍵認証部
104
更新処理部
105
判定部
106
機能制限部
107
画面生成部
11
通信部
12
記憶部
秘密鍵
121
公開鍵証明書
122
登録情報
123
ホワイトリスト
124
機能制限情報
125
表示部
13

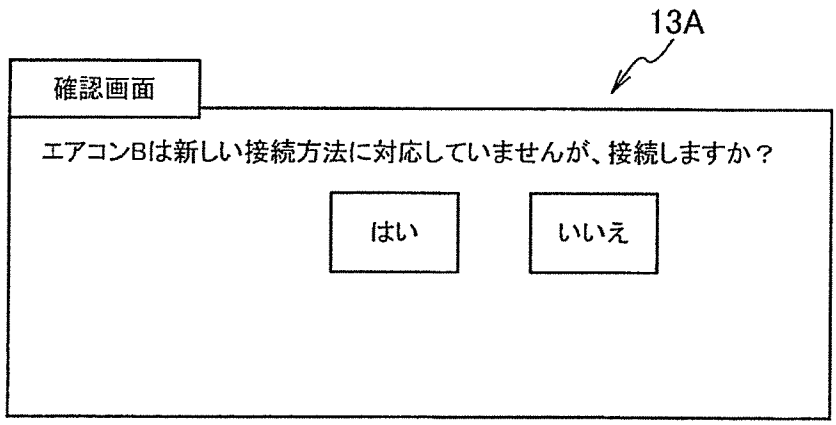
[図13]


新機器
(機器認証対応)
42
41
新コントローラ
(機器認証対応)
機器
(AIF対応)
52
33
32
MC
機器
(レガシー)
機器
(レガシー)
32

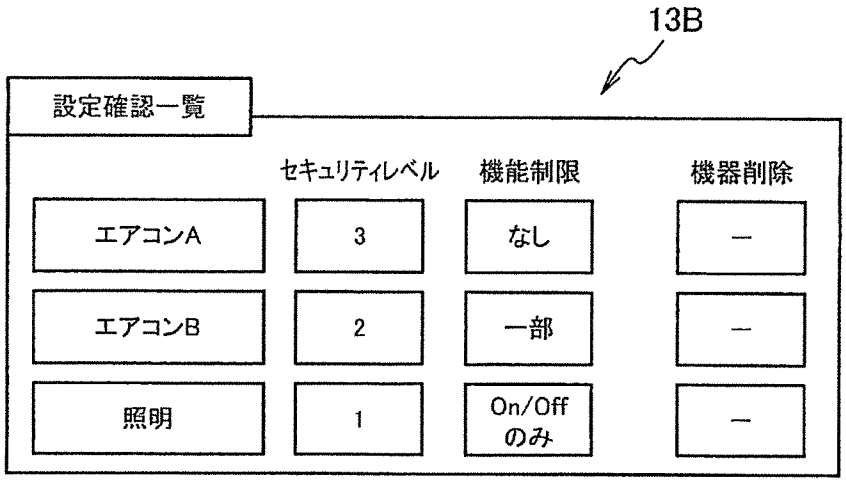
[図14]


32,42,52
41
機器
新コントローラ
ボタン押下
S31
ボタン押下
公開鍵証明書
公開鍵証明書or平文
S32
S33
NO
機器認証対応？
YES
S35
NO
AIF対応？
YES
S37
S36
S34
セキュリティレベル1
セキュリティレベル2
セキュリティレベル3

[図15]


13A
確認画面
エアコンBは新しい接続方法に対応していませんが、接続しますか？
はい
いいえ

[図16]


13B
設定確認一覧
セキュリティレベル
機能制限
機器削除
エアコンA
3
なし
—
エアコンB
2
一部
—
照明
1
On/Off
のみ
—

[図17]

125

セキュリティレベル / 機器	3(機器認証対応) 機能制限なし	2(AIF対応) 一部機能制限あり	1(レガシー機器) 機能制限あり
エアコン	(1) 動作状態・設定情報等取得可 (2) 温度設定可 (3) 電源ON/OFF可	(1) 動作状態・設定情報等取得可 (2) 温度設定可 **(3) 電源ON/OFF不可**	(1) 動作状態・設定情報等取得可 **(2) 温度設定不可** **(3) 電源ON/OFF不可**
蓄電池	(1) 動作状態・設定情報等取得可 (2) 電力量情報取得可 (3) 運転モード設定可 (急速充電/充電/放電/待機/テスト/自動/その他)	(1) 動作状態・設定情報等取得可 (2) 電力量情報取得可 **(3) 運転モード設定不可** **(急速充電/充電/放電/待機/テスト/自動/その他)**	(1) 動作状態・設定情報等取得可 **(2) 電力量情報取得不可** **(3) 運転モード設定不可** **(急速充電/充電/放電/待機/テスト/自動/その他)**
太陽光発電	(1) 動作状態・設定情報等取得可 (2) 瞬時発電電力量計測値取得可 (3) 積算発電電力量計測値取得可	(1) 動作状態・設定情報等取得可 (2) 瞬時発電電力量計測値取得可 **(3) 積算発電電力量計測値取得不可**	(1) 動作状態・設定情報等取得可 **(2) 瞬時発電電力量計測値取得不可** **(3) 積算発電電力量計測値取得不可**
瞬間式給湯器	(1) 動作状態・設定情報等取得可 (2) 風呂自動モード設定可	(1) 動作状態・設定情報等取得可 **(2) 風呂自動モード設定不可**	(1) 動作状態・設定情報等取得可 **(2) 風呂自動モード設定不可**

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2016/003595

A. CLASSIFICATION OF SUBJECT MATTER
H04L9/14(2006.01)i, *G06F21/44*(2013.01)i, *H04L9/08*(2006.01)i, *H04L9/32*(2006.01)i

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)
H04L9/14, G06F21/44, H04L9/08, H04L9/32

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

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2016
Kokai Jitsuyo Shinan Koho	1971-2016	Toroku Jitsuyo Shinan Koho	1994-2016

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	Kosuke MATSUISHI et al., "ECHONET Lite Protocol ni Taio shita Kaden Ninshiki Smart Tap no Teian", Symposium on Multimedia, Distributed, Cooperative and Mobile Systems (DICOMO2015) Ronbunshu [CD-ROM], 08 July 2015 (08.07.2015), vol.2015, no.1, pages 217 to 223	1-11
A	JP 2015-132943 A (Panasonic Intellectual Property Management Co., Ltd.), 23 July 2015 (23.07.2015), paragraphs [0019] to [0045], [0057] to [0064], [0068]; fig. 1 to 3, 6 to 7 & WO 2015/104628 A1	1-11

☒ 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
08 September 2016 (08.09.16)	20 September 2016 (20.09.16)

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

International application No.
PCT/JP2016/003595

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2008-186354 A (Toshiba Corp.), 14 August 2008 (14.08.2008), paragraphs [0013] to [0027]; fig. 2 (Family: none)	1-11
A	US 2013/0232556 A1 (PANASONIC CORP.), 05 September 2013 (05.09.2013), paragraphs [0112] to [0136]; fig. 4 & JP 5451950 B1 & JP 2014-75970 A & WO 2013/118511 A1 & CN 103597691 A	1-11
A	JP 2011-211537 A (Nippon Telegraph and Telephone Corp.), 20 October 2011 (20.10.2011), abstract (Family: none)	1-11

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２０１６／００３５９５

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　H04L9/14(2006.01)i, G06F21/44(2013.01)i, H04L9/08(2006.01)i, H04L9/32(2006.01)i

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））

Int.Cl.　H04L9/14, G06F21/44, H04L9/08, H04L9/32

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	１９７１－２０１６年
日本国実用新案登録公報	１９９６－２０１６年
日本国登録実用新案公報	１９９４－２０１６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	松石　浩輔、他，ＥＣＨＯＮＥＴ　Ｌｉｔｅプロトコルに対応した家電認識スマートタップの提案，マルチメディア，分散，協調とモバイル（ＤＩＣＯＭＯ２０１５）シンポジウム論文集［ＣＤ－ＲＯＭ］，2015.07.08，Ｖｏｌ．２０１５、Ｎｏ．１，ｐ．２１７－２２３	１－１１

☑ 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矛盾するものではなく、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
０８．０９．２０１６	２０．０９．２０１６

国際調査機関の名称及びあて先	特許庁審査官（権限のある職員）	５Ｓ　４２２９
日本国特許庁（ＩＳＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	青木　重徳 電話番号　０３－３５８１－１１０１　内線　３５４６	

Ｃ（続き）．　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 2015-132943 A (パナソニックＩＰマネジメント株式会社) 2015.07.23, 段落［００１９］－［００４５］、［００５７］－［００６４］、［００６８］、［図１］－［図３］、［図６］－［図７］ & WO 2015/104628 A1	１－１１
A	JP 2008-186354 A (株式会社東芝) 2008.08.14, 段落［００１３］－［００２７］、［図２］（ファミリーなし）	１－１１
A	US 2013/0232556 A1 (PANASONIC CORPORATION) 2013.09.05, 段落［０１１２］－［０１３６］、ＦＩＧ．４ & JP 5451950 B1 & JP 2014-75970 A & WO 2013/118511 A1 & CN 103597691 A	１－１１
A	JP 2011-211537 A (日本電信電話株式会社) 2011.10.20, ［要約］（ファミリーなし）	１－１１