(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
2016 年 11 月 17 日(17.11.2016)

WIPO | PCT

(10) 国際公開番号
WO 2016/181586 A1

(51) 国際特許分類:
H04L 9/08 (2006.01) *H04L 9/32* (2006.01)
G06F 21/44 (2013.01) *H04Q 9/00* (2006.01)

(21) 国際出願番号: PCT/JP2016/000946

(22) 国際出願日: 2016 年 2 月 23 日(23.02.2016)

(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:
62/158,906 2015 年 5 月 8 日(08.05.2015) US
特願 2016-007554 2016 年 1 月 19 日(19.01.2016) JP

(71) 出願人: パナソニック インテレクチュアル プロパティ コーポレーション オブ アメリカ (PANASONIC INTELLECTUAL PROPERTY CORPORATION OF AMERICA) [US/US]; 90503 カリフォルニア州トーランス, スイート ２００, マリナー アベニュー ２０００００ California (US).

(72) 発明者: 海上 勇二(UNAGAMI, Yuji); 〒5718501 大阪府門真市大字門真１００６番地パナソニック株式会社内 Osaka (JP). 前田 学(MAEDA, Manabu). 松島 秀樹(MATSUSHIMA, Hideki).

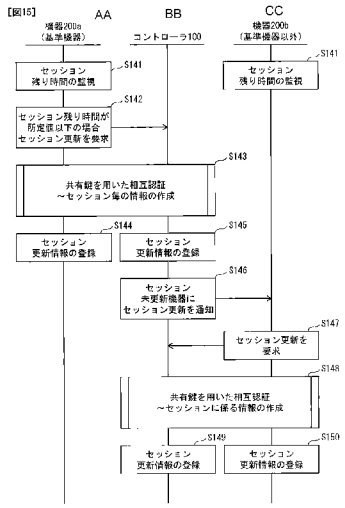
(74) 代理人: 徳田 佳昭, 外(TOKUDA, Yoshiaki et al.); 〒5718501 大阪府門真市大字門真１００６番地パナソニック株式会社内 Osaka (JP).

(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,

[続葉有]

(54) Title: AUTHENTICATION METHOD AND AUTHENTICATION SYSTEM

(54) 発明の名称 : 認証方法及び認証システム



S141 Monitor time remaining in session
S142 If time remaining in session is less than or equal to prescribed value, request session update
S143 Perform mutual authentication using shared key
Create information for each session
S144, S145, S149, S150 Register session update information
S146 Notify not-yet-updated device of session update
S147 Request session update
S148 Perform mutual authentication using shared key
Create session-related information
AA Device 200a (reference device)
BB Controller 100
CC Device 200b (other than reference device)

(57) **Abstract**: In this authentication method, mutual authentication is performed between a controller and a first device, a group key is created and shared with the controller and the first device, and the first device is set as a reference device. Next, at a group key update time, at which the controller and the reference device update the group key, mutual authentication is performed between the controller and a second device that is not a reference device, and the updated group key is shared with the second device. Transmission data is encrypted using the group key, and encrypted data is generated. A MAC is generated from the transmission data, a header, a transmission source address, and a transmission destination address. Simultaneous multi-address communication of a message containing the encrypted data, the header, the transmission source address, the transmission destination address, and the MAC is carried out.

(57) 要約: コントローラと第１機器とは相互認証を実行し、グループ鍵を作成して共有すると共に、第１機器を基準機器として設定する。その後、コントローラと基準機器とがグループ鍵を更新するグループ鍵更新タイミングにおいて、コントローラと基準機器ではない第２機器とが相互認証を実行し、更新後のグループ鍵を第２機器にも共有させる。また、グループ鍵を用いて送信データを暗号化して暗号化データを生成し、送信データと、ヘッダと、送信元アドレスと、送信先アドレスとからＭＡＣを生成し、暗号化データと、ヘッダと、送信元アドレスと、送信先アドレスと、ＭＡＣとを含むメッセージの一斉同報通信を行う。

WO 2016/181586 A1

FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, 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, 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)）

明　細　書

発明の名称 ： 認証方法及び認証システム

技術分野

[0001] 本開示は、エリアネットワークに接続する機器を認証する技術に関し、特に、コントローラと機器との間で相互認証しグループ鍵を更新する技術に関する。

背景技術

[0002] 近年、ネットワーク接続機能を有する家電機器やＡＶ機器、住宅設備機器などの機器類（以下、単に「機器」と呼ぶ。）からクラウドサーバに収集される各種履歴情報を用いたサービスが期待されている。家庭内に設置されている機器同士を接続することで形成されるネットワークを、以下ではホームエリアネットワークと呼ぶ。

[0003] このようなホームエリアネットワークに特定の機器（以下、「コントローラ」と呼ぶ。）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。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や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。例えば、前者に対しては接続機器の認証、後者に対しては通信の暗号化などの対策が考えられ、正当性が認証されたコントローラと機器とは暗号鍵を共有し、当該暗号鍵を用いた暗号通信を行う。コントローラと接続する機器が複数存在する場合、コントローラと当該機器とが同一の暗号鍵（以下、「グループ鍵」と呼ぶ。）を共有することで、コントローラが複数機器に対して同一情報を一斉送信するマルチキャスト通信やブロードキャスト通信の暗号化が行われる。

先行技術文献

非特許文献

[0004] 非特許文献1：ＮＳＡ　Ｓｕｉｔｅ　Ｂ　Ｉｍｐｌｅｍｅｎｔｅｒ‘ｓ　Ｇｕ

ｉｄｅ ｔｏ ＦＩＰＳ １８６－４ （ＥＣＤＳＡ）

非特許文献2：ＮＩＳＴ Ｓｐｅｃｉａｌ Ｐｕｂｌｉｃａｔｉｏｎ ８００－５６Ａ Ｒｅｖｉｓｉｏｎ ２

非特許文献3：ＲＦＣ５１９１ Ｐｒｏｔｏｃｏｌ ｆｏｒ Ｃａｒｒｙｉｎｇ Ａｕｔｈｅｎｔｉｃａｔｉｏｎ ｆｏｒ Ｎｅｔｗｏｒｋ Ａｃｃｅｓｓ（ＰＡＮＡ）

発明の概要

発明が解決しようとする課題

[0005] 上記、従来の認証システムでは、グループ鍵に関する更なる改善が必要とされていた。

課題を解決するための手段

[0006] コントローラと第１機器と第２機器とがグループ鍵を共有し、前記コントローラが前記第１機器と前記第２機器とに対して、前記グループ鍵を用いて暗号化した情報の一斉同報通信を行う認証システムにおける、前記コントローラと前記第１機器及び前記第２機器との認証方法であって、前記コントローラと前記第１機器とが相互認証を実行し、グループ鍵を作成して共有すると共に、前記第１機器を基準機器として設定する第１相互認証ステップと、前記コントローラと前記第２機器とが相互認証を実行し、前記第１相互認証ステップで作成したグループ鍵を前記第２機器にも共有させる第２相互認証ステップと、前記第２相互認証ステップの後に、前記コントローラと前記基準機器である前記第１機器とが再び相互認証を実行し、前記グループ鍵を更新し、更新後のグループ鍵を共有する第３相互認証ステップと、前記コントローラと前記基準機器とが前記グループ鍵を更新するグループ鍵更新タイミングにおいて、前記コントローラと前記基準機器ではない前記第２機器とが相互認証を実行し、前記更新後のグループ鍵を前記第２機器にも共有させる第４相互認証ステップと、前記グループ鍵を用いて送信データを暗号化して暗号化データを生成し、当該送信データと、ヘッダと、送信元アドレスと、送信先アドレスとからＭＡＣを生成し、当該暗号化データと、当該ヘッダと

、当該送信元アドレスと、当該送信先アドレスと、当該ＭＡＣとを含むメッセージの前記一斉同報通信を行う暗号化ステップとを含むことを特徴とする。

[0007] なお、これらの包括的または具体的な態様は、システム、装置、集積回路、コンピュータプログラム、または、記録媒体で実現されてもよく、システム、装置、方法、集積回路、コンピュータプログラムおよび記録媒体の任意な組み合わせで実現されてもよい。

発明の効果

[0008] 本開示によれば、認証システムにおけるグループ鍵に関する更なる改善を実現できる。

図面の簡単な説明

[0009] [図1]図１は、認証システム１０のシステム構成を示す概略図である。

[図2]図２は、コントローラ１００の主要部の機能ブロック図である。

[図3]図３は、接続機器管理テーブル１０００のデータ構造とデータの一例を示す図である。

[図4]図４は、公開鍵証明書のデータ構成の一例を示す図である。

[図5]図５は、ＣＲＬのデータ構成の一例を示す図である。

[図6]図６は、機器２００ａの主要部の機能ブロック図である。

[図7]図７は、接続コントローラ管理テーブル１１００のデータ構造とデータの一例を示す図である。

[図8]図８は、サーバ３００の主要部の機能ブロック図である。

[図9]図９は、機器情報管理テーブル１３００のデータ構造とデータの一例を示す図である。

[図10]図１０は、機器における機器登録処理の手順の一例を示したフローチャートである。

[図11]図１１は、コントローラにおける機器登録処理の手順の一例を示したフローチャートである。

[図12]図１２は、機器登録処理の手順の一例を示したシーケンス図である。

[図13]図１３は、機器におけるセッション更新処理の手順の一例を示したフローチャートである。

[図14]図１４は、コントローラにおけるセッション更新処理の手順の一例を示したフローチャートである。

[図15]図１５は、セッション更新処理の手順の一例を示したシーケンス図である。

[図16]図１６は、機器におけるＰＫＩに基づく相互認証～共有鍵の作成の手順の一例を示したフローチャートである。

[図17]図１７は、コントローラにおけるＰＫＩに基づく相互認証～共有鍵の作成の手順の一例を示したフローチャートである。

[図18]図１８は、ＰＫＩに基づく相互認証～共有鍵の作成の手順の一例を示したシーケンス図である。

[図19]図１９は、機器における共有鍵を用いた相互認証～セッションに係る情報の作成の手順の一例を示したフローチャートである。

[図20]図２０は、コントローラにおける共有鍵を用いた相互認証～セッションに係る情報の作成の手順の一例を示したフローチャートである。

[図21]図２１は、共有鍵を用いた相互認証～セッションに係る情報の作成の手順の一例を示したシーケンス図である。

[図22]図２２は、機器履歴情報送信処理の手順の一例を示したシーケンス図である。

[図23]図２３は、制御情報送信処理の手順の一例を示したシーケンス図である。

[図24]図２４は、暗号化前と暗号化後のメッセージフォーマットのデータ構成図である。

[図25]図２５は、機器履歴情報ＭＡＣ送信処理の手順の一例を示したシーケンス図である。

[図26]図２６は、制御情報ＭＡＣ送信処理の手順の一例を示したシーケンス図である。

[図27]図２７は、実施の形態２に係る接続機器管理テーブル２０００のデータ構造とデータの一例を示す図である。

[図28]図２８は、実施の形態２に係る機器におけるセッション更新処理の手順の一例を示したフローチャートである。

[図29]図２９は、実施の形態２に係るコントローラにおけるセッション更新処理の手順の一例を示したフローチャートである。

[図30]図３０は、実施の形態２に係るセッション更新処理の手順の一例を示したシーケンス図である。

[図31]図３１は、実施の形態３に係る接続機器管理テーブル３０００のデータ構造とデータの一例を示す図である。

[図32]図３２は、実施の形態３に係る接続コントローラ管理テーブル３１００のデータ構造とデータの一例を示す図である。

[図33]図３３は、実施の形態３に係る機器におけるセッション更新処理の手順の一例を示したフローチャートである。

[図34]図３４は、実施の形態３に係るコントローラにおけるセッション更新処理の手順の一例を示したフローチャートである。

[図35]図３５は、実施の形態３に係るセッション更新処理の手順の一例を示したシーケンス図である。

発明を実施するための形態

[0010] （本開示の基礎となった知見）

機器とコントローラとの間のセキュリティを保持するためには、接続時に相互認証を行って以降、同じグループ鍵を使い続けるのではなく、機器とコントローラとが改めて相互認証を行い、グループ鍵を更新することが望まれる。

[0011] しかしながら、それぞれの機器がそれぞれのタイミングでグループ鍵の更新を行うと、各機器が異なるグループ鍵を保持することになる。例えば、一の機器は更新後のグループ鍵を保持しているが、二の機器は更新前のグループ鍵を保持しているような場合、コントローラはグループ鍵を用いた暗号化

情報の一斉送信を行うことができない。

[0012] 本開示は係る課題に鑑みてなされたものであり、各機器とコントローラとの間におけるグループ鍵の更新タイミングを合わせることができる認証方法を提供するものである。

[0013] 本開示の一態様に係る認証方法は、コントローラに接続する機器の中から基準機器を設定し、当該基準機器におけるグループ鍵更新のタイミングに基づき、他の機器がグループ鍵の更新を行うことで、複数の機器間におけるグループ鍵更新のタイミングを合わせることが可能となる。

[0014] これにより、コントローラと各機器とが相互認証及びグループ鍵更新を行っても、コントローラは暗号化した情報の一斉送信を行うことができる。

[0015] 以下図面を参照しながら、本開示の実施の形態について説明する。なお、以下の実施の形態は、本開示を具体化した一例であって、本開示の技術的範囲を限定するものではない。

[0016] ＜１．実施形態１＞

＜１－１．概要＞

以下、本開示に係る認証方法を用いた一実施形態としての認証システム１０について、図を用いながら説明する。

[0017] 図１は、本実施の形態に係る認証システム１０のシステム構成の一例を示す概略図である。

[0018] 認証システム１０は、ホームエリアネットワーク４００に接続するコントローラ１００及び機器２００ａ、機器２００ｂ、機器２００ｃを含む構成である。認証システム１０におけるコントローラ１００は、インターネットなどの通信網であるネットワーク５００を介して、サーバ３００と接続する。

[0019] コントローラ１００及び機器２００ａ～機器２００ｃは、１つのホームエリアネットワーク４００に接続する。図には示していないが、ネットワーク機器（例えば、ハブ、ルータ等）を介して接続してもよい。また、コントローラ１００または各機器を設置する場所は、屋内及び屋外を問わない。

[0020] コントローラ１００と機器２００ａ～機器２００ｃのそれぞれとは、接続

を開始する際に相互認証を行う。そして、相互認証の結果、互いの正当性が確認できた場合は暗号鍵を共有し暗号通信を行う。コントローラと各機器とは、以降、それぞれの所定のタイミングでセッション更新処理を行い、セッション更新処理の都度、相互認証を行い、その結果が正当である場合に暗号鍵を更新し、暗号通信を継続する。

[0021] このようなコントローラ１００と各機器とは、接続時の相互認証において互いの正当性を確認した後、３種類の共有鍵を共有する。

[0022] 一の共有鍵は、コントローラ１００とそれぞれの機器との間において、セッション更新処理時の相互認証に用いる共有鍵である。コントローラと機器とが接続する際には、まず、公開鍵認証基盤（ＰＫＩ：Ｐｕｂｌｉｃ Ｋｅｙ Ｉｎｆｒａｓｔｒｕｃｔｕｒｅ）に基づく相互認証を行う。一方、当該ＰＫＩによる相互認証以降、セッション更新処理時において、コントローラと機器とが行う相互認証は、当該一の共有鍵を用いて行う。以下、単に、「共有鍵」と記述している場合、当該相互認証に用いる共有鍵を示すものとする。ただし、明らかに、以下で説明するグループ鍵及びセッション鍵を示す記載をしている場合は除く。

[0023] コントローラと機器との間の暗号通信には、共有鍵暗号方式を用いるため、コントローラと機器とは共有鍵を共有する。

[0024] 二の共有鍵と三の共有鍵とは、この暗号通信に用いるための共有鍵であり、それぞれを、グループ鍵とセッション鍵と呼ぶ。グループ鍵は、コントローラが複数機器に対して同一情報を一斉送信するために使用する暗号鍵であり、コントローラは、コントローラに接続する全ての機器と同一のグループ鍵を共有する。セッション鍵は、コントローラと各機器とが１対１のユニキャスト通信を行うために使用する暗号鍵であり、コントローラは、それぞれの機器との間で、個別の暗号鍵を共有する。

[0025] ここで、コントローラと各機器との間の通信には、セッション有効期間を設けるものとし、グループ鍵及びセッション鍵は、当該セッション有効期間において利用可能とする。セッションを設定して以降、セッション有効期間

を超過した場合は、グループ鍵及びセッション鍵を利用不可とするように制御する。なお、セッション有効期間経過後も暗号通信を継続するためには、コントローラとそれぞれの機器との間でセッション更新処理を行い、新たなグループ鍵及びセッション鍵を作成し、新たなセッションを設定する必要がある。

[0026] また、コントローラは、接続する複数機器のうちの１つの機器を、基準機器として設定する。そして、コントローラ１００と各々の機器とがグループ鍵を更新するタイミングは、基準機器がセッション更新処理を行い、グループ鍵を更新するタイミングに基づくものとし、具体的な方法は後述する。なお、基準機器は、例えば、コントローラ１００が最初に接続する機器とする。

[0027] サーバ３００は、機器２００ａ～機器２００ｃに対して、サービス提供などを行う外部のサーバである。サーバ３００と各機器とが通信する際には、コントローラ１００を介して行う。

[0028] 例えば、各機器は、機器の動作を示す機器履歴情報を、コントローラ１００を介して、サーバ３００に送信する。また、サーバ３００は、コントローラ１００を介して、それぞれの機器にサービス情報を送信する。ここでは、サーバ３００は、各機器に所定の機能を実行させるための制御依頼情報を送信するものとする。コントローラ１００は、当該制御依頼情報を受信して解読し、各機器に実行させるための制御コマンドを作成して送信する。そして、当該制御コマンドを受信したそれぞれの機器は、サーバ３００から依頼された機能を実行する。

[0029] ＜１－２．構成＞

本実施の形態に係る認証システム１０の主要な構成要素であるコントローラ１００及び機器２００ａ～機器２００ｃと、当該認証システム１０に接続するサーバ３００の各構成について、以下、図を用いながら説明する。

[0030] ＜１－２－１．コントローラ１００＞

図２は、コントローラ１００の主要部の機能ブロック図であり、コントロ

ーラ１００は、機器管理部１０１、機器情報保持部１０２、認証処理部１０３、認証情報保持部１０４、通信部１０５を含む構成である。また、コントローラ１００は、図示してはいないが、プロセッサ及びメモリを含む構成であり、機器管理部１０１、機器情報保持部１０２、認証処理部１０３、認証情報保持部１０４、通信部１０５の各機能は、メモリに記憶されているプログラムをプロセッサが実行することにより実現される。機器情報保持部１０２、認証情報保持部１０４における各データの保持は、メモリによって実現される。

[0031] （機器管理部１０１）

機器管理部１０１は、コントローラ１００と機器２００ａ～機器２００ｃとの接続を制御するために、次のような機能を有する。

[0032] 機器管理部１０１は、コントローラ１００に対する、機器からの接続要求やセッション更新要求を、通信部１０５を介して受付ける。そして、当該機器との間の相互認証処理を、認証処理部１０３に実行させる。

[0033] 機器管理部１０１は、認証処理部１０３にて行われた認証処理の結果、当該機器の正当性が認められた場合、機器情報保持部１０２で保持する接続機器管理テーブル１０００に接続機器管理データを登録する。接続機器管理テーブル１０００が保持する接続機器管理データの詳細については後述する。

[0034] 機器管理部１０１は、基準機器の設定を行う。例えば、コントローラ１００と最初に接続する機器を基準機器として設定してもよい。また、基準機器として登録されている機器との接続が切断された場合、機器情報保持部１０２の保持する接続機器管理テーブル１０００から、別の機器を抽出して基準機器として設定する。このとき、電源が常時ＯＮである機器を基準機器として設定してもよい。機器管理部１０１は、当該基準機器の設定についても、接続機器管理テーブル１０００に登録する。機器との接続時においては、当該機器を基準機器として設定するか否かの判断を、認証処理部１０３が行い、その判断結果を受けて、機器管理部１０１が接続機器管理テーブル１０００に登録する。

[0035] 機器管理部１０１は、接続機器管理テーブル１０００の項目であるセッション更新状態を参照し、セッションが未更新である機器に対して、通信部１０５を介して、セッション更新通知を行う。当該セッション更新通知は、機器に対してセッション更新を促すためのものであり、その後、改めて、機器側からのコントローラ１００に対するセッション更新要求を受付けることで、セッションを更新する。

[0036] 機器管理部１０１は、接続機器管理テーブル１０００の項目であるセッション残り時間の値を参照し、セッションが更新されないままセッション有効期間を超過した機器、すなわちセッション残り時間がゼロである機器に対して、当該機器との間で保持する、グループ鍵やセッション鍵などの暗号鍵の情報を削除することで、当該機器との暗号通信を禁止する。

[0037] また、機器管理部１０１は、機器２００ａ～機器２００ｃより、通信部１０５を介して受信する、暗号化された機器履歴情報を復号する。復号した機器履歴情報は、通信部１０５を介して、サーバ３００に送信する。

[0038] さらに、機器管理部１０１は、サーバ３００より、通信部１０５を介して受信する、機器の制御依頼情報を機器に指示可能な形式に加工した後、グループ鍵またはセッション鍵にて暗号化し、通信部１０５を介して、機器に送信する。

[0039] （機器情報保持部１０２）

機器情報保持部１０２は、コントローラ１００に接続する機器２００ａ～機器２００ｃの情報を保持する。図３は、機器情報保持部１０２が、機器の情報を管理するために保持する、接続機器管理テーブル１０００のデータ構造とデータの一例を示す図である。

[0040] 接続機器管理テーブル１０００は、機器毎の接続機器管理レコード群からなる。接続機器管理レコードは、機器とコントローラとが接続する際に行う機器登録処理において、機器が正当な機器であると認められた場合に登録するデータであり、機器ＩＤ１０１０、証明書ＩＤ１０２０、共有鍵１０３０、グループ鍵１０４０、セッション鍵１０５０、セッション残り時間１０６

０、セッション更新状態１０７０、基準機器１０８０の項目が含まれる。

[0041] 図３のデータの例示を用いながら、各項目について説明する。

[0042] 機器ＩＤ１０１０は、機器を一意に定める識別子である。

[0043] 証明書ＩＤ１０２０は、機器の公開鍵証明書の証明書ＩＤである。

[0044] 共有鍵１０３０は、コントローラ１００と機器との間で共有する共有鍵のデータである。

[0045] グループ鍵１０４０は、コントローラ１００が複数機器に対して一斉送信する情報の暗号化に用いるグループ鍵のデータである。図３は、コントローラに接続する全ての機器である機器ＩＤ１～機器ＩＤ３と、同一のグループ鍵“１１２２３・・・”を共有していることを示している。なお、図３の例示では、機器ＩＤ１～機器ＩＤ３が、１つのグループ鍵の項目欄を共有する例を示しているが、機器ＩＤごとに個別の項目欄を有し、当該項目を登録する際に、基準機器以外の機器は、基準機器と同じグループ鍵のデータを設定するとしてもよい。

[0046] セッション鍵１０５０は、コントローラ１００と機器との間のユニキャスト通信を暗号化するために用いるセッション鍵のデータである。図３の例でも、コントローラは、機器ＩＤ１～機器ＩＤ３の各機器との間で、それぞれ別のセッション鍵を共有していることを示している。

[0047] セッション残り時間１０６０は、コントローラ１００と機器との間で設定するセッション有効期間の残余期間である。コントローラ１００と機器との間には、予め定めた所定のセッション有効期間を設ける。セッションを設定あるいは更新する都度、セッション残り時間１０６０には、セッション有効期間を登録する。以降、時間の経過とともに、当該項目の値をカウントダウンさせることで、セッション残り時間１０６０はセッション有効期間の残余期間を表す。

[0048] なお、セッション残り時間がゼロになった機器は、機器管理部１０１により、当該機器との間で保持するグループ鍵、セッション鍵の情報が削除され、暗号通信が禁止される。

[0049] セッション更新状態１０７０は、コントローラ１００と基準機器との間でセッション更新を行って以降の期間において、機器ＩＤが示す機器がコントローラ１００とのセッション更新を行ったか否かを示すデータである。コントローラ１００が基準機器とのセッション更新を行った時点で、基準機器以外の機器に係るセッション更新状態１０７０を“未更新”に更新する。その後、コントローラ１００が当該機器とのセッション更新処理を行った時点で、セッション更新状態１０７０を“更新済”に更新する。

[0050] 基準機器１０８０の項目は、機器が基準機器であるか否かを示すデータである。

[0051] セッション更新状態１０７０及び基準機器１０８０の項目について、図３の例示では、機器ＩＤ１の機器が基準機器であることを示している。また、コントローラ１００と基準機器である機器ＩＤ１の機器とがセッション更新を行った以降において、コントローラは、機器ＩＤ２の機器とは既にセッションを更新した状態であり、機器ＩＤ３の機器とはセッションが未更新であることを表している。

[0052] （認証処理部１０３）

認証処理部１０３は、コントローラ１００と接続する機器との相互認証処理を行う機能を有する。機器との接続時においては、ＰＫＩに基づく相互認証を行い、セッション更新時においては、共有鍵と乱数とを用いたチャレンジレスポンス認証による相互認証を行う。

[0053] 認証処理部１０３は、機器管理部１０１から、機器の認証依頼とともに当該機器の公開鍵証明書を受け付け、ＰＫＩに基づく認証処理を行う。具体的には、まず、認証情報保持部１０４に格納されているＣＲＬ（Ｃｅｒｔｉｆｉｃａｔｅ Ｒｅｖｏｃａｔｉｏｎ Ｌｉｓｔ）に基づき、取得した機器の公開鍵証明書に係る証明書ＩＤがＣＲＬに記載されていないことを確認する。そして、公開鍵証明書に付されている署名を認証局の公開鍵を用いて検証する。ここでは、認証局はサーバ３００とする。

[0054] また、認証処理部１０３は、コントローラ１００と機器との間でセッショ

ン更新を行う際、共有鍵を用いた相互認証であるチャレンジレスポンス認証を行う。認証処理部１０３は、機器との間で、鍵交換により当該共有鍵を作成する機能も有する。認証処理部１０３は乱数を生成し、通信部１０５を介して、機器に送信する。そして、機器が共有鍵で暗号化して返送した乱数を、コントローラが保持する共有鍵で復号し、自身が作成した乱数と照合することで機器の正当性を確認する。また、同様に、認証処理部１０３が、機器から受信した乱数を共有鍵で暗号化して返送することで、機器側での検証も行われる。

[0055] さらに、認証処理部１０３は、セッションの設定及び更新に必要な処理を実行する機能を有する。具体的には、コントローラ１００と機器との通信を暗号化するための共有鍵である、グループ鍵とセッション鍵とを作成する。また、セッション有効期間を設定し、セッション鍵及びグループ鍵とともに、機器管理部１０１を介して、機器情報保持部１０２が保持する接続機器管理テーブル１０００に登録する。

[0056] （認証情報保持部１０４）

認証情報保持部１０４は、コントローラ１００自身の秘密鍵と公開鍵証明書とを保持する。また、ＰＫＩに基づく相互認証において、相手機器の公開鍵証明書が失効していないことを確認するために使用するＣＲＬを保持している。このような、秘密鍵と公開鍵証明書とＣＲＬとは、コントローラ１００の製造時に埋め込むものとする。

[0057] 図４は、公開鍵証明書の標準的なデータ構成例である公開鍵証明書１５００のデータ構成を示す図である。公開鍵証明書１５００は、当該証明書に係るバージョン１５１０、発行者１５２０、有効期間の開始１５３０、有効期間の終了１５４０、証明書ＩＤ１５５０、公開鍵１５６０、認証局であるサーバ３００の署名１５７０を含む構成である。ここで、公開鍵１５６０はコントローラ自身の公開鍵のデータであり、署名１５７０は認証局の秘密鍵を用いて作成して付与された署名である。

[0058] 図５は、ＣＲＬの標準的なデータ構成例であるＣＲＬ１６００を示す図で

ある。ＣＲＬ１６００は、当該ＣＲＬに係るＣＲＬバージョン１６１０、発行者１６２０、発行日１６３０、次回発行日１６４０、失効した証明書ＩＤ１６５０、認証局であるサーバの署名１６６０を含む構成である。ここで、失効した証明書ＩＤ１６５０は、１つのＩＤに限定するわけではなく、複数の失効した証明書ＩＤを保持してもよい。また、署名１６６０は認証局の秘密鍵を用いて作成して付与された署名である。

[0059] （通信部１０５）

通信部１０５は、コントローラ１００が、機器２００ａ～機器２００ｃ及びサーバ３００のそれぞれと接続するための通信インターフェイスである。例えば、機器情報保持部１０２の接続機器管理テーブル１０００に保持するセッション鍵及びグループ鍵を用いて、機器２００ａ～機器２００ｃと暗号通信を行う機能を有する。

[0060] また、通信部１０５は、サーバ３００と暗号通信を行う機能を有しており、例えば、ＳＳＬ（Ｓｅｃｕｒｅ　Ｓｏｃｋｅｔ　Ｌａｙｅｒ）通信を行う。ここで、ＳＳＬ通信に必要であるＳＳＬサーバ証明書は、通信部１０５で保持する。

[0061] ＜１－２－２．機器２００ａ＞

機器２００ａ～機器２００ｃは、ネットワークに接続する機能を有する家電機器やＡＶ機器及び住宅設備機器であり、具体的には、例えば、テレビ、レコーダ、エアコン、冷蔵庫、蓄電池などである。

[0062] 以下、機器の構成については、代表として機器２００ａを用いて説明する。なお、各機器はそれぞれ固有の機能を有し、その点において、機器が別種の機器であれば他の機器とは共通しない。例えば、洗濯機であれば洗濯機能、エアコンであれば暖房や冷房などの機能のことであり、一般的な機能であるため説明は省略する。本願の発明である認証方法に係る機能についてのみ説明を行い、この点については、機器２００ａに限らず、他の機器も同じ機能を有することは言うまでもない。

[0063] 図６は、機器２００ａの主要部の機能ブロック図であり、機器２００ａは

、機器管理部２０１、機器履歴保持部２０２、機器情報保持部２０３、認証処理部２０４、認証情報保持部２０５、通信部２０６を含む構成である。また、機器２００ａは、図示してはいないが、プロセッサ及びメモリを含む構成であり、機器管理部２０１、機器履歴保持部２０２、機器情報保持部２０３、認証処理部２０４、認証情報保持部２０５、通信部２０６の各機能は、メモリに記憶されているプログラムをプロセッサが実行することにより実現される。機器履歴保持部２０２、機器情報保持部２０３、認証情報保持部２０５における各データの保持は、メモリによって実現される。

[0064] （機器管理部２０１）

機器管理部２０１は、コントローラ１００との接続を制御する。具体的には次のような機能を有する。

[0065] 機器管理部２０１は、コントローラ１００に接続する際、通信部２０６を介して、接続要求をコントローラ１００に送信する。

[0066] また、機器管理部２０１は、コントローラ１００の公開鍵証明書を、通信部２０６を介して受信すると、認証処理部２０４にＰＫＩに基づく認証処理を実行させる。

[0067] 機器管理部２０１は、認証処理部２０４にて行われた認証処理の結果、コントローラ１００の正当性が認められた場合、機器情報保持部２０３で保持する接続コントローラ管理テーブル１１００に、接続コントローラデータを登録する。接続コントローラ管理テーブル１１００が保持する接続コントローラデータの詳細については後述する。

[0068] また、機器履歴保持部２０２に記録されている機器の動作履歴に係る機器履歴情報をセッション鍵で暗号化し、通信部２０６を介してコントローラ１００に送信する。このような機器の動作に係る機器履歴情報の送信は、定期的または非定期的に行い、コントローラ１００を経由してサーバ３００に送信される。

[0069] さらに、機器管理部２０１は、機器情報保持部２０３の接続コントローラ管理テーブルが保持するセッション残り時間の項目を参照し、セッション残

り時間の値が事前に定めた所定の閾値以下となった時点で、セッション更新を開始する。所定の閾値は、例えば、セッション有効期間の１０％の値、または、セッション更新処理に必要な時間の２倍の値などとする。ただし、機器管理部２０１が、コントローラ１００からのセッション更新通知を受信した場合には、当該セッション残り時間の値に関わらず、セッション更新を開始する。

[0070] セッション更新を開始すると、機器管理部２０１は、認証処理部２０４に処理を実行させる。その後、認証処理部２０４が作成した、グループ鍵、セッション鍵、セッション有効期間を受け取り、機器情報保持部２０３で保持する接続コントローラ管理テーブル１１００に登録する。

[0071] （機器履歴保持部２０２）

機器履歴保持部２０２は、機器２００ａの動作を機器履歴情報として記録し、保持する機能を有する。機器履歴保持部２０２は、機器２００ａが操作されたり、機能を実行したりする都度、これらの動作を示す情報を機器履歴情報として記録する。なお、機器履歴情報は、機器２００ａがコントローラ１００を介して、サーバ３００に送信する情報の一例として示すものであるものの、本願の発明の主たる構成要素ではないため、データ項目等の詳細な説明は省略する。

[0072] （機器情報保持部２０３）

機器情報保持部２０３は、機器２００ａに接続するコントローラ１００の情報を保持する。図７は、機器情報保持部２０３が、コントローラの情報を管理するために保持する、接続コントローラ管理テーブル１１００のデータ構造とデータの一例を示す図である。

[0073] 接続コントローラ管理テーブル１１００は、接続コントローラ管理レコード群からなる。接続コントローラ管理レコードは、機器とコントローラとが接続する際に行う機器登録処理において、コントローラが正当な機器であると認められた場合に登録するデータであり、コントローラＩＤ１１１０、証明書ＩＤ１１２０、共有鍵１１３０、グループ鍵１１４０、セッション鍵１

１５０、セッション残り時間１１６０の項目が含まれる。

[0074] 図７の例を用いながら、各項目について説明する。

[0075] コントローラＩＤ１１１０は、コントローラを一意に定める識別子である。

[0076] 証明書ＩＤ１１２０は、コントローラの公開鍵証明書の証明書ＩＤである。

[0077] 共有鍵１１３０は、機器２００ａがコントローラ１００との間で共有する共有鍵のデータである。

[0078] グループ鍵１１４０は、コントローラ１００が機器に対して一斉送信する情報を暗号化するために用いる共有鍵のデータである。機器側では、受信した情報を当該グループ鍵を用いて復号する。

[0079] セッション鍵１１５０は、コントローラ１００との暗号化ユニキャスト通信を行うために用いる共有鍵のデータである。

[0080] セッション残り時間１１６０は、コントローラ１００との間で設定するセッション有効期間の残余期間である。機器２００ａとコントローラ１００との間には、予め定めた所定のセッション有効期間を設ける。セッションを設定あるいは更新する都度、セッション有効期間をセッション残り時間１１６０に登録する。以降、時間の経過とともに、当該項目の値をカウントダウンさせることで、セッション残り時間１１６０はセッション有効期間の残余期間を表す。

[0081] （認証処理部２０４）

認証処理部２０４は、コントローラ１００との相互認証処理を行う機能を有する。コントローラとの接続時においては、ＰＫＩに基づく相互認証を行い、セッション更新時においては、共有鍵と乱数とを用いたチャレンジレスポンス認証による相互認証を行う。

[0082] 機器管理部２０１から、コントローラの認証依頼とともに当該コントローラの公開鍵証明書を受け付け、ＰＫＩに基づく認証処理を行う。具体的には、まず、認証情報保持部２０５に格納されているＣＲＬに基づき、取得した

コントローラの公開鍵証明書の証明書ＩＤがＣＲＬに記載されていないことを確認する。また、公開鍵証明書の署名を認証局の公開鍵を用いて検証する。ここでは、認証局はサーバ３００とする。

[0083] また、認証処理部２０４は、コントローラ１００との間で、セッション更新を行う際、共有鍵を用いた相互認証であるチャレンジレスポンス認証を行う。認証処理部２０４は、コントローラ１００との間で、鍵交換により当該共有鍵を作成する機能も有する。認証処理部２０４は乱数を生成し、通信部２０６を介して、コントローラ１００に送信する。そして、認証処理部２０４は、コントローラ１００が共有鍵で暗号化して返送した乱数を、機器が保持する共有鍵で復号し、自身が作成した乱数と照合することでコントローラの正当性を確認する。また、同様に、認証処理部２０４が、機器から受信した乱数を共有鍵で暗号化して返送することで、機器側での検証も行われる。

[0084] さらに、認証処理部２０４は、セッションの作成及び更新に必要な処理を実行する機能を有する。具体的には、セッション更新処理の開始を、機器管理部２０１から受け付けると、通信部２０６を介して、セッション更新要求をコントローラ１００に対して送信する。また、認証処理部２０４は、通信部２０６を介して、コントローラ１００から、更新後のセッション鍵とグループ鍵とセッション有効期間とを受信し、機器管理部２０１を介して、機器情報保持部２０３が保持する接続コントローラ管理テーブル１１００に登録する。

[0085] （認証情報保持部２０５）

認証情報保持部２０５は、機器２００ａ自身の秘密鍵と公開鍵証明書とを保持する。また、ＰＫＩに基づく相互認証において公開鍵証明書が失効していないことを確認するために使用するＣＲＬを保持している。このような、秘密鍵と公開鍵証明書とＣＲＬとは、機器の製造時に埋め込むものとする。

[0086] ＣＲＬ及び公開鍵証明書のデータ構成は、コントローラ１００の認証情報保持部１０４が保持するものと同様のため説明は省略する。ただし、機器２００ａの公開鍵証明書が保持する公開鍵は、機器２００ａの公開鍵であるこ

とは勿論である。

[0087] （通信部２０６）

通信部２０６は、コントローラ１００と接続するための通信インターフェイスである。例えば、機器情報保持部２０３の接続コントローラ管理テーブル１１００が保持するセッション鍵及びグループ鍵を用いて、コントローラ１００との間で暗号通信を行う機能を有する。

[0088] ＜１－２－３．サーバ３００＞

図８は、サーバ３００の主要部の機能ブロック図であり、サーバ３００は、機器情報管理部３０１、機器情報保持部３０２、ＣＲＬ管理部３０３、ＣＲＬ保持部３０４、通信部３０５を含む構成である。また、サーバ３００は、図示してはいないが、プロセッサ及びメモリを含む構成であり、機器情報管理部３０１、機器情報保持部３０２、ＣＲＬ管理部３０３、ＣＲＬ保持部３０４、通信部３０５の各機能は、メモリに記憶されているプログラムをプロセッサが実行することにより実現される。機器情報保持部３０２、ＣＲＬ保持部３０４における各データの保持は、メモリによって実現される。

[0089] （機器情報管理部３０１）

機器情報管理部３０１は、機器情報保持部３０２を制御し、サーバ３００に接続するコントローラの情報を、コントローラに接続する機器情報を含めて管理するために、以下の機能を有する。

[0090] 機器情報管理部３０１は、通信部３０５を介して、コントローラより受信したコントローラ及び機器の情報を機器情報保持部３０２が保持する機器情報管理テーブル１３００に登録する。

[0091] また、コントローラから、コントローラと機器との相互認証において、正当でないと判断された機器の情報を受信した場合には、当該機器の公開鍵証明書の証明書ＩＤをＣＲＬ管理部３０３に通知する。

[0092] （機器情報保持部３０２）

機器情報保持部３０２は、サーバ３００に接続するコントローラ及び機器の情報を保持しており、図９は、機器情報保持部３０２が有する、機器情報

管理テーブル１３００のデータ構造とデータの一例を示す図である。

[0093] 機器情報管理テーブル１３００には、コントローラに係るコントローラＩＤ１３１０及び証明書ＩＤ１３２０の項目が含まれる。また、コントローラと接続する機器に係る機器ＩＤ１３３０、証明書ＩＤ１３４０、機器履歴情報１３５０の項目が含まれる。図９の例を用いながら、各項目について説明する。

[0094] コントローラＩＤ１３１０は、コントローラを一意に定める識別子である。

[0095] コントローラの証明書ＩＤ１３２０は、コントローラの公開鍵証明書の証明書ＩＤである。

[0096] 機器ＩＤ１３３０は、コントローラに接続する機器を識別する機器ＩＤである。図９の例では、コントローラＩＤ１で識別されるコントローラには、機器ＩＤ１、機器ＩＤ２、機器ＩＤ３で識別される３つの機器が接続していることを表している。

[0097] 機器の証明書ＩＤ１３４０は、機器の公開鍵証明証の証明書ＩＤである。

[0098] 機器履歴情報１３５０は、機器から収集した機器履歴情報のデータである。ここで、機器履歴情報そのものは、別のテーブルで機器毎に保持し、当該機器履歴情報１３５０の項目には、前記別テーブルへのリンク情報を保持するとしてもよい。

[0099] （ＣＲＬ管理部３０３）

ＣＲＬ管理部３０３は、機器情報管理部３０１から不正な機器の公開鍵証明書の証明書ＩＤを受付けると、ＣＲＬを発行する。

[0100] また、ＣＲＬ管理部３０３は、サーバ３００の公開鍵と秘密鍵とを保持している。

[0101] ＣＲＬ管理部３０３は、ＣＲＬを発行する際、サーバ３００の秘密鍵を用いて作成した署名を、ＣＲＬに付与する。当該ＣＲＬを使用する、コントローラ及び機器は、ＣＲＬに付された署名を、サーバ３００の公開鍵を用いて検証することにより、ＣＲＬが正当であることを確認する。

[0102] ＣＲＬ管理部が発行したＣＲＬは、通信部３０５を介して、コントローラ及び機器に送信する。

[0103] （ＣＲＬ保持部３０４）

ＣＲＬ保持部３０４は、ＣＲＬ管理部３０３が発行したＣＲＬを保持する。ＣＲＬのデータ構成は、コントローラ１００の認証情報保持部１０４が保持するものと同様のため説明は省略する。

[0104] （通信部３０５）

通信部３０５は、コントローラ１００と通信を行うための通信インターフェイスである。サーバ３００とコントローラ１００との通信は、例えば、ＳＳＬ通信により行われる。ＳＳＬ通信に必要な証明書は、通信部３０５で保持する。

[0105] ＜１－３．動作＞

以下、認証システム１０で行う、“機器登録処理”、“セッション更新処理”、“ＰＫＩに基づく相互認証～共有鍵の作成”、“共有鍵を用いた相互認証～セッションに係る情報の作成”、“機器履歴情報送信処理”、“制御情報送信処理”、“機器履歴情報ＭＡＣ（Ｍｅｓｓａｇｅ Ａｕｔｈｅｎｔｉｃａｔｉｏｎ Ｃｏｄｅ）送信処理”、“制御情報ＭＡＣ送信処理”について順に説明する。なお、“ＰＫＩに基づく相互認証～共有鍵の作成”は、“機器登録処理”において、“共有鍵を用いた相互認証～セッションに係る情報の作成”は、“機器登録処理”及び“セッション更新処理”において実行する処理であるが、便宜的にサブルーチン化して記載している。

[0106] （機器登録処理）

図１０及び図１１は、機器とコントローラとのそれぞれにおける機器登録処理の手順の一例を示したフローチャート図であり、図１２は、機器とコントローラとのやりとりを含む、機器登録処理の手順の一例を示したシーケンス図である。

[0107] 機器登録処理は、コントローラ１００と機器とが接続する際に行う処理であり、機器がコントローラ１００に接続要求をし、相互認証を行ってから互

いを登録する手順である。まず、図１０及び図１１のフローチャートに沿って、機器及びコントローラのそれぞれにおける処理の概要を説明してから、図１２のシーケンス図に沿って、機器とコントローラとのやりとりを含む、機器登録処理のより詳細な手順について説明する。

[0108] 図１０のフローチャートに沿って、機器における機器登録処理の概要について説明する。

[0109] まず、機器はコントローラに対して、接続要求とともに、機器自身の機器ＩＤ及び公開鍵証明書を送信する（ステップＳ１０１０）。

[0110] 次に、機器は、“ＰＫＩに基づく相互認証～共有鍵の作成”のサブルーチンを実行することで、コントローラとの相互認証を行った後、共有鍵を共有する（ステップＳ１０２０）。当該サブルーチン処理の詳細は後述する。

[0111] ステップＳ１０２０のサブルーチンの戻り値が「正常」である場合（ステップＳ１０３０のＹＥＳ）、機器は“共有鍵を用いた相互認証～セッションに係る情報の作成”のサブルーチンを実行することにより、コントローラと共有鍵を用いた相互認証を行った後、セッションに係る情報である、グループ鍵及びセッション鍵の作成、セッション有効期間の設定を行う（ステップＳ１０４０）。当該、サブルーチン処理の詳細は後述する。

[0112] ステップＳ１０４０のサブルーチンの戻り値が「正常」である場合（ステップＳ１０５０のＹＥＳ）、機器は、正当な接続相手としてコントローラの情報を登録する（ステップＳ１０６０）。

[0113] 一方、ステップＳ１０２０のサブルーチンの戻り値が「エラー」である場合（ステップＳ１０３０のＮＯ）、あるいは、ステップＳ１０４０のサブルーチンの戻り値が「エラー」である場合（ステップＳ１０５０のＮＯ）、機器は、機器登録処理を終了する。

[0114] 次に、図１１のフローチャートに沿って、コントローラにおける機器登録処理の概要について説明する。

[0115] コントローラは、機器の接続要求、機器ＩＤ及び公開鍵証明書を待ち受ける（ステップＳ１１１０）。これらを受信しない場合（ステップＳ１１１０

のＮＯ）、コントローラは、機器からの接続要求を待ち続ける。

[0116] 接続要求を受信した場合（ステップＳ１１１０のＹＥＳ）、コントローラは“ＰＫＩに基づく相互認証～共有鍵の作成”のサブルーチンを実行することで、機器との相互認証を行った後、共有鍵を共有する（ステップＳ１１２０）。当該サブルーチン処理の詳細は後述する。

[0117] ステップＳ１１２０のサブルーチンの戻り値が「正常」である場合（ステップＳ１１３０のＹＥＳ）、コントローラは、“共有鍵を用いた相互認証～セッションに係る情報の作成”のサブルーチンを実行することで、機器と共有鍵を用いた相互認証を行った後、セッションに係る情報である、グループ鍵及びセッション鍵の作成、セッション有効期間の設定を行う（ステップＳ１１４０）。また、コントローラは、当該機器を基準機器として設定するか否かを判断する（ステップＳ１１４０）。当該サブルーチン処理の詳細は後述する。

[0118] ステップＳ１１４０のサブルーチンの戻り値が「正常」である場合（ステップＳ１１５０のＹＥＳ）、コントローラは、コントローラと機器の情報をサーバ３００に送信する（ステップＳ１１６０）。

[0119] そして、コントローラは、正当な接続相手として機器の情報を登録する（ステップＳ１１７０）。

[0120] 一方、ステップＳ１１２０のサブルーチンの戻り値が「エラー」である場合（ステップＳ１１３０のＮＯ）、あるいは、ステップＳ１１４０のサブルーチンの戻り値が「エラー」である場合（ステップＳ１１５０のＮＯ）、コントローラは機器登録処理を終了する。

[0121] ここからは、図１２のシーケンス図に沿って、より詳細な処理の内容を機器とコントローラとのやりとりを含めて説明する。機器については、機器２００ａの例示で説明するが、機器２００ｂ及び機器２００ｃに関する処理も機器２００ａと同様の手順であることは言うまでもない。また、シーケンス図としては、エラーが発生しない場合の例を示しているが、エラー発生時の処理については、文章にて補足を行っている。

[0122] 機器登録処理は、コントローラ１００に新たな機器が接続する際に行う処理である。例えば、コントローラの属するホームエリアネットワークに新たな機器が追加されるタイミングや、当該ネットワークに電源ＯＦＦの状態で存在する機器の電源がＯＮになったタイミングなどに実行する。

[0123] 機器２００ａの機器管理部２０１は、通信部２０６を介し、コントローラ１００に対する接続要求を送信する（ステップＳ１０１）。このとき、機器２００ａの機器ＩＤ及び公開鍵証明書も合わせて送信する。

[0124] コントローラ１００の機器管理部１０１は、通信部１０５を介して、接続要求を受け付け、認証処理部１０３にＰＫＩに基づく相互認証を実行させる。これを受け、コントローラ１００の認証処理部１０３と機器２００ａの認証処理部２０４とは、ＰＫＩに基づく相互認証処理を行い、互いの正当性を確認する（ステップＳ１０２）。

[0125] そして、コントローラ１００の認証処理部１０３と機器２００ａの認証処理部２０４とは、鍵交換方式により、共有鍵を作成する（ステップＳ１０２）。当該共有鍵は、以降において行う相互認証において使用する。上記ステップＳ１０２の、“ＰＫＩに基づく相互認証～共有鍵の作成”は便宜的にサブルーチン化しており、手順は後述する。なお、当該サブルーチン処理からの戻り値が「エラー」である場合、コントローラと機器とは、機器登録処理を終了する。

[0126] 続いて、コントローラ１００の認証処理部１０３と機器２００ａの認証処理部２０４とは、作成した共有鍵を用いて相互認証を行うとともに、セッションに係る情報の作成を行う（ステップＳ１０３）。ステップＳ１０３において、改めて共有鍵を用いた相互認証を行うのは、共有鍵自体を検証するためでもある。ステップＳ１０２における共有鍵の作成は鍵交換方式により行っている。したがって、コントローラ１００と機器２００ａとのそれぞれにおいて、所定の手順により共有鍵を作成するため、それぞれで作成した共有鍵が同一であることを確認するためにも、ステップＳ１０３において、共有鍵を用いた相互認証を行うことが有用である。

[0127] 共有鍵を用いた相互認証が成功した場合、セッションに係る情報である、グループ鍵、セッション鍵、セッション有効期間の作成を行う（ステップＳ１０３）。また、機器２００ａを基準機器として設定するか否かを判断する（ステップＳ１０３）。ステップＳ１０３の、“共有鍵を用いた相互認証～セッションに係る情報作成”は便宜的にサブルーチン化しており、手順は後述する。なお、当該サブルーチン処理からの戻り値が「エラー」である場合、コントローラと機器とは機器登録処理を終了する。

[0128] 機器２００ａの認証処理部２０４は、機器管理部２０１を介して、コントローラ１００のコントローラＩＤ及び、当該コントローラ１００と共有する、共有鍵、グループ鍵、セッション鍵の情報を、機器情報保持部２０３の有する接続コントローラ管理テーブル１１００に登録する。また、セッション有効期間を、接続コントローラ管理テーブル１１００のセッション残り時間の項目に登録する（ステップＳ１０４）。

[0129] コントローラ１００の機器管理部１０１は、コントローラ１００に係るコントローラＩＤ及び公開鍵証明書の証明書ＩＤ、並びに、機器２００ａに係る機器ＩＤ及び公開鍵証明書の証明書ＩＤをサーバ３００に送信する（ステップＳ１０５）。このとき、サーバとはＳＳＬ（Ｓｅｃｕｒｅ　Ｓｏｃｋｅｔ　Ｌａｙｅｒ）通信を行う。

[0130] また、コントローラ１００の機器管理部１０１は、機器２００ａの機器ＩＤ及び、機器２００ａと共有する共有鍵、グループ鍵、セッション鍵の情報を、機器情報保持部１０２の有する接続機器管理テーブル１０００に登録する。このとき、セッション有効期間を、接続機器管理テーブル１０００のセッション残り時間の項目に登録する。また、機器２００ａを基準機器として設定する場合、接続機器管理テーブル１０００の基準機器の項目に、基準機器であることを登録する（ステップＳ１０６）。ステップＳ１０３の“共有鍵を用いた相互認証～セッションに係る情報作成”において、基準機器として設定するか否かの判断が行われており、例えば、コントローラに最初に接続した機器が、基準機器として設定される。

[0131] サーバ３００は、通信部３０５を介して、コントローラ１００からコントローラ及び機器の情報を受信する。そして、機器情報管理部３０１は、当該コントローラのコントローラＩＤ及び証明書ＩＤ、並びに、認証された機器の機器ＩＤ及び証明書ＩＤを、機器情報保持部３０２が有する機器情報管理テーブル１３００に登録する（ステップＳ１０７）。

[0132] （セッション更新処理）

図１３及び図１４は、機器とコントローラとのそれぞれにおけるセッション更新処理の手順の一例を示したフローチャート図であり、図１５は、機器とコントローラとのやりとりを含む、セッション更新処理の手順の一例を示したシーケンス図である。

[0133] セッション更新処理において、機器とコントローラ１００とは、改めて相互認証を行った上で、グループ鍵、セッション鍵、セッション残り時間の更新を行う。図１３及び図１４のフローチャートに沿って、機器及びコントローラのそれぞれにおける処理の概要を説明した後、図１５のシーケンス図に沿って、機器とコントローラとのやりとりを含む処理の詳細について説明する。

[0134] まず、図１３のフローチャートに沿って、機器におけるセッション更新処理の概要について説明する。機器は、基準機器であるか、基準機器以外の機器であるかを問わず、次の手順で処理を行う。

[0135] 機器はセッション更新の開始を判定するために、セッション残り時間を監視する。または、コントローラからのセッション更新通知を待ち受ける（ステップＳ１２１０）。セッション残り時間が予め定めた所定値より大きい、かつ、コントローラからのセッション更新通知も受信しない場合（ステップＳ１２１０のＮＯ）、監視を続ける。

[0136] セッション残り時間が予め定めた所定値以下となるか、あるいは、コントローラからセッション更新通知を受信した場合（ステップＳ１２１０のＹＥＳ）、機器はセッション更新を行うために、コントローラに対して、セッション更新要求を送信する（ステップＳ１２２０）。

[0137] そして、“共有鍵を用いた相互認証～セッションに係る情報の作成”のサブルーチンを実行することで、コントローラと共有鍵を用いた相互認証を行った後、セッションに係る情報である、グループ鍵及びセッション鍵の作成、セッション有効期間の設定を行う（ステップＳ１２３０）。当該、サブルーチン処理の詳細は後述する。

[0138] ステップＳ１２３０のサブルーチンの戻り値が「正常」である場合（ステップＳ１２４０のＹＥＳ）、機器は、ステップＳ１２３０にて作成した新たなセッションに係る情報を、セッション更新情報として登録する（ステップＳ１２５０）。

[0139] 一方、ステップＳ１２３０のサブルーチンの戻り値が「エラー」である場合（ステップＳ１２４０のＮＯ）、セッションの更新を行わずに、機器はセッション更新処理を終了する。

[0140] 次に、図１４のフローチャートに沿って、コントローラにおけるセッション更新処理の概要について説明する。

[0141] コントローラは、機器からのセッション更新要求を待ち受ける（ステップＳ１３１０）。受信しなければ（ステップＳ１３１０のＮＯ）、機器からのセッション更新要求を待ち続ける。

[0142] 機器からセッション更新要求を受信すると（ステップＳ１３１０のＹＥＳ）、“共有鍵を用いた相互認証～セッションに係る情報の作成”のサブルーチンを実行することで、機器と共有鍵を用いた相互認証を行った後、セッションに係る情報である、グループ鍵及びセッション鍵の作成、セッション有効期間の設定を行う（ステップＳ１３２０）。当該、サブルーチン処理の詳細は後述する。

[0143] ステップＳ１３２０のサブルーチンの戻り値が「正常」である場合（ステップＳ１３３０のＹＥＳ）、コントローラは、ステップＳ１３２０にて作成した新たなセッションに係る情報を、セッション更新情報として登録する（ステップＳ１３４０）。このとき、機器が基準機器である場合は、コントローラに接続するその他の各機器がセッション未更新であることを示す情報を

登録する。また、機器が基準機器でない場合は、当該機器がセッション更新済であることを示す情報を登録する。すなわち、基準機器がセッション更新を行って以降、その他の各機器がセッションを更新済であるか、未更新であるかを、機器毎に管理する。

[0144] 一方、ステップＳ１３２０のサブルーチンの戻り値が「エラー」である場合（ステップＳ１３３０のＮＯ）、当該機器については、セッション更新情報の登録を行わないことで、セッションを更新しない。

[0145] 当該機器とのセッション更新を行ったか行っていないかに関わらず、他にセッションを更新していない機器が存在する場合（ステップＳ１３５０のＹＥＳ）、当該セッション未更新機器に対して、セッション更新通知を送信する（ステップＳ１３６０）。このとき、セッションが未更新である機器全てに対して、一斉にセッション更新通知を行ってもよいし、そのうちの一部、あるいは１つの機器に対して送ってもよいが、最終的には全ての未更新機器に対して、セッション更新通知を行い、セッションを更新することで全ての機器とのセッションを更新する。勿論、ステップＳ１３２０において、エラーが発生した機器は除く。

[0146] 全ての機器について、セッション更新処理が完了した場合（ステップＳ１３５０のＮＯ）、セッション更新処理を終了する。

[0147] ここからは、図１５のシーケンス図に沿って、より詳細な処理を機器とコントローラとのやりとりを含めて説明する。機器については、一例として、機器２００ａが基準機器であり、機器２００ｂが基準機器以外の機器であるとする。また、シーケンス図については、エラーが発生しない場合の例を示しているが、エラー発生時の処理については、文章にて補足している。

[0148] 機器２００ａの機器管理部２０１は、接続コントローラ管理テーブル１１００が保持するセッション残り時間１１６０を監視し、予め定めた所定の閾値以下であるかを確認する。セッション残り時間が所定値より大きい場合、セッション残り時間の監視を続ける（ステップＳ１４１）。なお、機器２００ｂの機器管理部２０１も、機器２００ａと同様に、セッション残り時間の

監視を行うが、機器２００ａよりも長いセッション残り時間を有するものとする。仮に、基準機器以外の機器が、基準機器よりも短いセッション残り時間を有することで、先にセッション更新処理を行っても問題ない。このとき、グループ鍵については、後述する“共有鍵を用いた相互認証～セッションに係る情報作成”のサブルーチンにおいて、基準機器が使用しているグループ鍵を取得することとなる。すなわち、現在使用しているグループ鍵と同じグループ鍵を取得することとなり、グループ鍵については更新が行われない。しかし、基準機器がセッション更新処理を行った時点で、基準機器以外の機器のセッション更新状態がクリアされることにより、当該機器はセッション未更新機器であると判定され、コントローラからセッション更新通知を受信する。この通知を受けて、当該機器がセッション更新を行うことで、基準機器がグループ鍵を更新するタイミングに合わせて、当該機器もグループ鍵の更新を行うこととなる。

[0149] セッション残り時間が所定の閾値以下になった時点で、機器２００ａの機器管理部２０１は、認証処理部２０４にセッション更新を実行させる。認証処理部２０４は、まず、通信部２０６を介して、セッション更新要求をコントローラ１００に送信する（ステップＳ１４２）。

[0150] コントローラ１００の機器管理部１０１は、通信部１０５を介して、セッション更新要求を受け付け、認証処理部１０３に、相互認証処理を実行させる。これを受け、コントローラ１００の認証処理部１０３と機器２００ａの認証処理部２０４とは、共有鍵を用いたチャレンジレスポンス認証による相互認証により、互いの正当性を確認する（ステップＳ１４３）。また、相互認証により互いの正当性が確認できた場合には、セッションに係る情報である、グループ鍵、セッション鍵、セッション有効期間の作成を行う（ステップＳ１４３）。

[0151] ステップＳ１４３の、“共有鍵を用いた相互認証～セッションに係る情報作成”は、機器登録処理におけるステップＳ１０３と同様の処理であり、便宜的にサブルーチン化しており、手順は後述する。なお、当該サブルーチン

処理からの戻り値が「エラー」である場合、コントローラと当該機器２００ａとはセッションを更新しない。すなわち、ステップＳ１４４及びステップＳ１４５のセッション更新情報の登録処理を行わずに、ステップＳ１４６へ進む。そして、後の“共有鍵を用いた相互認証～セッションに係る情報作成”のサブルーチンにおいて、機器２００ｂが基準機器として設定されることとなる。

[0152] 機器２００ａの機器管理部２０１は、ステップＳ１４３にて作成した、セッション鍵、グループ鍵、及びセッション有効期間を、機器情報保持部２０３の有する、接続コントローラ管理テーブル１１００に登録する（ステップＳ１４４）。このとき、セッション有効期間は、セッション残り時間の項目に登録する。

[0153] また、コントローラ１００の機器管理部１０１は、ステップＳ１４３にて作成した、グループ鍵、セッション鍵、セッション有効期間を、機器情報保持部１０２の有する、接続機器管理テーブル１０００に登録する。セッション有効期間は、セッション残り時間１０６０の項目に登録する。このとき、機器２００ａに係るセッション更新状態１０７０は“更新済”に設定する。また、機器２００ａ以外の機器、すなわち、基準機器以外の機器に係るレコードに対しては、セッション更新状態１０７０の項目を“未更新”に更新する（ステップＳ１４５）。

[0154] コントローラ１００の機器管理部１０１は、機器情報保持部１０２が保持する、接続機器管理テーブル１０００のセッション更新状態１０７０の項目を参照し、“未更新”の機器の有無を確認する。セッション更新状態１０７０の項目が“未更新”である機器が存在しない場合、全ての機器のセッション更新処理が行われたと判断し、処理を終了する。

[0155] セッション更新状態１０７０が“未更新”である機器が存在する場合、コントローラ１００の機器管理部１０１は、当該機器に対して、セッション更新通知を行う（ステップＳ１４６）。図１５の例では、セッションが未更新である機器２００ｂに対するセッション更新通知を行う。なお、他にもセッ

ション未更新の機器が存在する場合、当該機器に対してもセッション更新通知を行い、以降の処理を実施するものとする。このとき、セッションが未更新である機器全てに対して、一斉にセッション更新通知を行ってもよい。または、未更新機器のうちの１つの機器に対して送ってもよいし、いくつかの機器毎に送ってもよい。

[0156] 機器２００ｂの機器管理部２０１は、通信部２０６を介して、コントローラ１００が送信したセッション更新通知を受け付け、認証処理部２０４にセッション更新を実行させる。認証処理部２０４は、まず、通信部２０６を介して、コントローラ１００にセッション更新要求を送信する（ステップＳ１４７）。

[0157] それから、基準機器以外の機器である機器２００ｂも、基準機器である機器２００ａに係るステップＳ１４３～Ｓ１４５と同様の手順でセッション更新を行う（ステップＳ１４８～ステップＳ１５０）。

[0158] ただし、ステップＳ１４９において、コントローラ１００の機器管理部１０１は、ステップＳ１４８にて作成した、グループ鍵、セッション鍵、セッション有効期間を、機器情報保持部１０２の有する、接続機器管理テーブル１０００に登録するとともに、セッション更新状態１０７０の項目は“更新済”に更新する（ステップＳ１４９）。

[0159] 上記ステップＳ１４５において、全てのセッション未更新機器に対してセッション更新通知を送信することにより、コントローラは全ての機器とのセッション更新を行い、更新したグループ鍵を共有する。

[0160] （ＰＫＩに基づく相互認証～共有鍵の作成）

図１６及び図１７は、機器とコントローラとのそれぞれにおけるＰＫＩに基づく相互認証～共有鍵の作成の手順処理の手順の一例を示したフローチャート図であり、図１８は、機器とコントローラとのやりとりを含む、同処理の手順の一例を示したシーケンス図である。図１６及び図１７のフローチャートに沿って、機器及びコントローラのそれぞれにおける処理の概要を説明した後、図１８のシーケンス図に沿って、機器とコントローラとのやりとり

を含む処理の詳細について説明する。

[0161] まず、図１６のフローチャートに沿って、機器における処理の概要について説明する。

[0162] 機器は、コントローラから、コントローラＩＤ及び公開鍵証明書を待ち受ける。これらを受信せずに（ステップＳ１４１０のＮＯ）、エラーを受信した場合（ステップＳ１４２０のＹＥＳ）、当該サブルーチンの戻り値として、「エラー」をセットする（ステップＳ１４６０）。

[0163] コントローラから、コントローラＩＤ及び公開鍵証明書、あるいは、エラーのいずれも受信しない場合（ステップＳ１４１０のＮＯ及びステップＳ１４２０のＮＯ）、コントローラからの情報を待ち続ける。

[0164] コントローラＩＤ及び公開鍵証明書を受信した場合（ステップＳ１４１０のＹＥＳ）、コントローラから受信した公開鍵証明書について、証明書ＩＤがＣＲＬにないことを確認する（ステップＳ１４３０）。

[0165] そして、証明書ＩＤがＣＲＬに記載されておらず失効していない場合（ステップＳ１４３０のＮＯ）、公開鍵証明書に付されている署名を検証する（ステップＳ１４４０）。

[0166] ステップＳ１４４０において、コントローラの公開鍵証明書の署名の検証に成功した場合（ステップＳ１４４０のＹＥＳ）、機器はコントローラに検証成功を通知する（ステップＳ１４７０）。

[0167] そして、機器はコントローラとの鍵交換により、共有鍵を共有する（ステップＳ１４８０）。当該鍵は、以降の相互認証に利用する。また、機器は、当該サブルーチンの戻り値として、「正常」をセットする（ステップＳ１４９０）。

[0168] 一方、公開鍵証明書の証明書ＩＤがＣＲＬ記載されていた場合（ステップＳ１４３０のＹＥＳ）、あるいは、署名検証に成功しなかった場合（ステップＳ１４４０のＮＯ）のいずれかである場合、コントローラの公開鍵証明書の検証が失敗したと判断して、機器は、コントローラに対して、エラー通知を送信する（ステップＳ１４５０）。そして、当該サブルーチンの戻り値と

しては、「エラー」をセットする（ステップＳ１４６０）。

[0169] ステップＳ１４９０あるいはステップＳ１４６０にてセットされた戻り値を当該サブルーチンの処理結果として、呼び出し元の処理に返す（ステップＳ１５００）。

[0170] 次に、図１７のフローチャートに沿って、コントローラにおける処理の概要について説明する。

[0171] まず、コントローラは、機器から受信した公開鍵証明書の証明書ＩＤがＣＲＬにないことを確認する（ステップＳ１６１０）。

[0172] そして、証明書ＩＤがＣＲＬに記載されておらず失効していない場合（ステップＳ１６１０のＮＯ）、公開鍵証明書に付されている署名を検証する（ステップＳ１６２０）。

[0173] 公開鍵証明書の証明書ＩＤがＣＲＬ記載されていた場合（ステップＳ１６１０のＹＥＳ）、あるいは、署名御検証に成功しなかった場合（ステップＳ１６２０のＮＯ）のいずれかである場合、機器の公開鍵証明書の検証が失敗したとして、コントローラは機器に対してエラー通知を送信する（ステップＳ１６３０）。

[0174] そして、当該サブルーチンの戻り値としては、「エラー」をセットする（ステップＳ１６７０）。

[0175] ステップＳ１６２０にて、コントローラの公開鍵証明書の署名の検証に成功した場合（ステップＳ１６２０のＹＥＳ）、機器側の、コントローラの公開鍵証明書の検証結果を待ち受ける（ステップＳ１６５０）。

[0176] 機器から検証成功を受信せずに（ステップＳ１６５０のＮＯ）、エラー通知を受信した場合（ステップＳ１６６０のＹＥＳ）、当該サブルーチンの戻り値としては、「エラー」をセットする（ステップＳ１６７０）。

[0177] 機器から検証成功を受信せず（ステップＳ１６５０のＮＯ）、かつ、エラー受信もしない場合（ステップＳ１６６０のＮＯ）、機器からの検証結果を待ち続ける。

[0178] 機器から検証成功を受信した場合（ステップＳ１６５０のＹＥＳ）、コン

トローラと機器とは鍵交換により、共有鍵を共有する（ステップＳ１６８０）。当該鍵は、以降の相互認証に利用する。

[0179] そして、コントローラは、当該サブルーチンの戻り値として、「正常」をセットする（ステップＳ１６９０）。

[0180] ステップＳ１６９０あるいはステップＳ１６７０にてセットされた戻り値を当該サブルーチンの処理結果として、呼び出し元の処理に返す（ステップＳ１７００）。

[0181] ここからは、図１８のシーケンス図に沿って、より詳細な処理を機器とコントローラとのやりとりを含めて説明する。機器については、機器２００ａの例示で説明するが、機器２００ｂ、機器２００ｃについても、同じ手順で処理が行われることはいうまでもない。また、シーケンス図については、エラーが発生しない場合の例を示しているが、エラー発生時の処理については、文章にて補足している。

[0182] コントローラ１００の認証処理部１０３は、機器２００ａの公開鍵証明書の証明書ＩＤが、認証情報保持部１０４で保持するＣＲＬに記載されていないことを確認する（ステップＳ１１１）。

[0183] ステップＳ１１１において、機器２００ａの証明書ＩＤがＣＲＬに記載されていない場合、コントローラ１００の認証処理部１０３は、機器２００ａの公開鍵証明書に付与されている認証局の電子署名が適切なものであるかを検証する（ステップＳ１１２）。このとき用いる電子署名方式及び検証方法は、ＥＣＤＳＡ（Ｅｌｌｉｐｔｉｃ Ｃｕｒｖｅ Ｄｉｇｉｔａｌ Ｓｉｇｎａｔｕｒｅ Ａｌｇｏｒｉｔｈｍ）に基づくものとする。ＥＣＤＳＡによる電子署名及び検証方法については、非特許文献１などに記載されている一般的な技術を用いるため説明は省略する。

[0184] ステップＳ１１１において機器２００ａの証明書ＩＤがＣＲＬに記載されている場合、あるいは、ステップＳ１１２において電子署名の検証が成功しない場合、認証処理部１０３は、機器２００ａが正当な機器ではないと判断し、機器２００ａに対するエラー通知を行い、当該サブルーチンの呼び出し

元である機器登録処理に対して、戻り値「エラー」を返す。このとき、エラー通知を受信した機器２００ａ側でも、戻り値「エラー」を返し、コントローラと機器との双方が当該サブルーチン処理を終了する。

[0185] ステップＳ１１２において、電子署名の検証が成功した場合、コントローラ１００の認証処理部１０３は、機器２００ａが正当な機器であると判断し、通信部１０５を介して、コントローラ自身のコントローラＩＤ及び公開鍵証明書を機器２００ａに送信する（ステップＳ１１３）。

[0186] 機器２００ａの機器管理部２０１は、通信部２０６を介して、コントローラ１００のコントローラＩＤ及び公開鍵証明書を受け付け、認証処理部２０４にＰＫＩに基づく認証処理を実行させる。認証処理部２０４は、まず、コントローラの公開鍵証明書の証明書ＩＤが、認証情報保持部２０５で保持するＣＲＬに記載されていないことを確認する（ステップＳ１１４）。

[0187] ステップＳ１１４において、コントローラ１００の証明書ＩＤがＣＲＬに記載されていない場合、機器２００ａの認証処理部２０４は、コントローラ１００の公開鍵証明書に付与されている認証局の電子署名が適切なものであるかを検証する（ステップＳ１１５）。このとき用いる電子署名方式及び検証方法は、ステップＳ１１２と同様に、ＥＣＤＳＡ（Ｅｌｌｉｐｔｉｃ Ｃｕｒｖｅ Ｄｉｇｉｔａｌ Ｓｉｇｎａｔｕｒｅ Ａｌｇｏｒｉｔｈｍ）に基づくものとし、説明は省略する。

[0188] ステップＳ１１４においてコントローラの証明書ＩＤがＣＲＬに記載されている場合、あるいは、ステップＳ１１５において電子署名の検証が成功しない場合、認証処理部２０４は、コントローラ１００が正当な機器ではないと判断し、コントローラに対するエラー通知を行い、当該サブルーチンの呼び出し元である機器登録処理に対して、戻り値「エラー」を返す。このとき、エラー通知を受信したコントローラ側でも、戻り値「エラー」を返し、コントローラと機器との双方が当該サブルーチン処理を終了する。

[0189] ステップＳ１１５において、電子署名の検証が成功した場合、機器２００ａの認証処理部２０４は、コントローラ１００が正当なコントローラである

と判断し、コントローラ１００に対して検証成功を通知する（ステップＳ１１６）。

[0190] 次に、機器２００ａの認証処理部２０４とコントローラ１００の認証処理部１０３とは、共有鍵を共有するための処理として、鍵交換を行う（ステップＳ１１７、Ｓ１１８）。ここで、実施する鍵交換方式は、楕円曲線暗号を用いた鍵交換方式であるＥＣＤＨ（Ｅｌｌｉｐｔｉｃ Ｃｕｒｖｅ Ｄｉｆｉｅ－Ｈｅｌｌｍａｎ）とする。ＥＣＤＨについては、非特許文献２などに記載されている一般的な技術を用いるため詳細な説明は省略する。

[0191] ＥＣＤＨによる鍵交換において、コントローラ１００の認証処理部１０３は、コントローラ自身の秘密鍵と機器２００ａの公開鍵証明書に含まれている機器２００ａの公開鍵とを用いて所定の手順により値を算出する。一方、機器２００ａの認証処理部２０４は、機器自身の秘密鍵とコントローラ１００の公開鍵証明書に含まれているコントローラ１００の公開鍵とを用いて、所定の手順により値を算出する。ここで、コントローラ１００と機器２００ａとのそれぞれにおいて算出された値は同じ結果となる。このようにして共有した値から共有鍵を算出する。本実施形態では、ＡＥＳ（Ａｄｖａｎｃｅｄ Ｅｎｃｒｙｐｔｉｏｎ Ｓｔａｎｄａｒｄ）の鍵長１２８ビットを共有鍵として用いることとし、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ビットを共有鍵とする。

[0192] （共有鍵を用いた相互認証～セッションに係る情報の作成）

図１９及び図２０は、それぞれ機器とコントローラとのそれぞれにおける共有鍵を用いた相互認証～セッションに係る情報の作成処理の手順の一例を示したフローチャート図であり、図２１は、機器とコントローラとのやりとりを含む同処理の手順の一例を示したシーケンス図である。

[0193] 本実施形態においては、共有鍵を用いた相互認証として、乱数を使用したチャレンジレスポンス認証を行うこととする。

[0194] 図１９及び図２０のフローチャートに沿って、機器及びコントローラのそれぞれにおける処理の概要を説明した後、図２１のシーケンス図に沿って、

機器とコントローラとのやりとりを含む処理の詳細について説明する。

[0195] まず、図１９のフローチャートに沿って、機器における共有鍵を用いた相互認証～セッションに係る情報の作成処理の概要について説明する。

[0196] 機器は、コントローラから、コントローラが作成した乱数Ａの受信を待ち受け、受信しない場合（ステップＳ１８１０のＮＯ）は待ち続ける。

[0197] コントローラから乱数Ａを受信した場合（ステップＳ１８１０のＹＥＳ）、機器は、受信した乱数Ａの暗号化を行うとともに、別の乱数である乱数Ｂの作成を行う（ステップＳ１８２０）。

[0198] そして、機器は、暗号化した乱数Ａである暗号化乱数Ａ’及び乱数Ｂをコントローラに送信する（ステップＳ１８３０）。

[0199] その後、機器は、コントローラ側での処理を待ち受ける。コントローラから、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受信せずに（ステップＳ１８４０のＮＯ）、エラーを受信した場合（ステップＳ１８５０のＹＥＳ）、当該サブルーチンの戻り値として、「エラー」をセットする（ステップＳ１８８０）。

[0200] コントローラから暗号化乱数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受信せずに（ステップＳ１８４０のＮＯ）、エラーも受信しない場合（ステップＳ１８５０のＮＯ）、コントローラからのいずれかの情報の受信を待ち続ける。

[0201] 機器は、コントローラらか、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受信した場合（ステップＳ１８４０のＹＥＳ）、まず、乱数Ｂに関する検証を行う（ステップＳ１８６０）。機器は、保持している共有鍵で、受信した暗号化乱数Ｂ’を復号する。復号結果の値が、ステップＳ１８２０において機器自身が作成した乱数Ｂと合致する場合、乱数Ｂの検証が成功したと判断する。

[0202] 乱数Ｂの検証が成功しなかった場合（ステップＳ１８６０のＮＯ）、コントローラへエラー通知を行う（ステップＳ１８７０）。

[0203] そして、当該サブルーチンの戻り値として、「エラー」をセットする（ス

テップＳ１８８０）。

[0204] 乱数Ｂの検証が成功した場合（ステップＳ１８６０のＹＥＳ）、コントローラから受信した、グループ鍵及びセッション鍵を復号する（ステップＳ１８９０）。

[0205] そして、機器は、コントローラに対して、検証成功を通知する（ステップＳ１９００）。

[0206] 当該サブルーチンの戻り値としては、「正常」をセットする（ステップＳ１９１０）。

[0207] ステップＳ１９１０あるいはステップＳ１８８０にてセットされた戻り値を当該サブルーチンの処理結果として、呼び出し元の処理に返す（ステップＳ１９２０）。

[0208] 次に、図２０のフローチャートに沿って、コントローラにおける共有鍵を用いた相互認証～セッションに係る情報の作成処理の概要について説明する。

[0209] コントローラは乱数Ａを作成し、機器に送信する（ステップＳ２０１０）。

[0210] そして、機器側での処理で作成される暗号化乱数Ａ’と乱数Ｂとを待ち受ける。機器から暗号化乱数Ａ’及び乱数Ｂを受信しない場合（ステップＳ２０２０のＮＯ）、受信するまで待ち続ける。

[0211] 暗号化乱数Ａ’、乱数Ｂを受信した場合（ステップＳ２０２０のＹＥＳ）、乱数Ａに関する検証を行う（ステップＳ２０３０）。機器は、保持している共有鍵で、受信した暗号化乱数Ａ’を復号する。復号結果の値が、ステップＳ２０１０においてコントローラ自身が作成した乱数Ａと合致する場合、乱数Ａの検証が成功したと判断する。

[0212] 乱数Ａの検証が成功しなかった場合（ステップＳ２０３０のＮＯ）、機器へエラー通知を行う（ステップＳ２０４０）。そして、当該サブルーチンの戻り値として、「エラー」をセットする（ステップＳ２１５０）。

[0213] 乱数Ａの検証が成功した場合（ステップＳ２０３０のＹＥＳ）、機器から

受信した乱数Ｂを暗号化する（ステップＳ２０５０）。

[0214] そして、機器が基準機器であるか否かを確認する（ステップＳ２０６０）。機器がコントローラに対して、最初に接続要求を行った機器である場合、基準機器である機器との接続が切断された場合などで、基準機器の設定がなされていない場合は、当該機器を基準機器とする。

[0215] 機器が基準機器である場合（ステップＳ２０６０のＹＥＳ）、グループ鍵を作成する（ステップＳ２０７０）。一方、機器が基準機器でない場合（ステップＳ２０６０のＮＯ）、既に作成して保持しているグループ鍵を当該機器とも共有するために、グループ鍵のデータを取得する（ステップＳ２０８０）。

[0216] また、コントローラは、セッション鍵の作成とセッション有効期間の設定とを行う（ステップＳ２０９０）。

[0217] そして、グループ鍵及びセッション鍵を共有鍵で暗号化する（ステップＳ２１００）。

[0218] その後、ステップＳ２０５０～ステップＳ２１００の処理で取得した、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、機器に送信する（ステップＳ２１１０）。

[0219] 機器側の検証結果を待ち受け、検証成功を受信しない場合（ステップＳ２１２０のＮＯ）、かつ、エラーを受信した場合（ステップＳ２１４０のＹＥＳ）、当該サブルーチンの戻り値として、「エラー」をセットする（ステップＳ２１５０）。

[0220] 機器側の検証結果を受信しない場合（ステップＳ２１２０のＮＯ）、かつ、エラーも受信しない場合（ステップＳ２１４０のＮＯ）、機器からの結果を待ち続ける。

[0221] 機器から検証成功を受信した場合（ステップＳ２１２０のＹＥＳ）、当該サブルーチンの戻り値としては、「正常」をセットする（ステップＳ２１３０）。

[0222] ステップＳ２１３０あるいはステップＳ２１５０にてセットされた戻り値

を当該サブルーチンの呼び出し元の処理に返す（ステップＳ２１６０）。

[0223] ここからは、図２１のシーケンス図に沿って、より詳細な処理を機器とコントローラとのやりとりを含めて説明する。機器については、機器２００ａを用いて説明を行うが、機器２００ｂ及び機器２００ｃについても同様の手順にて処理を行うことは言うまでもない。また、シーケンス図については、エラーが発生しない場合の例を示しているが、エラー発生時の処理については、文章にて補足している。

[0224] まず、コントローラ１００の認証処理部１０３は、任意の乱数Ａを作成し、機器２００ａへ送信する（ステップＳ１２１）。

[0225] 機器２００ａの認証処理部２０４は、通信部２０６を介して受信した乱数Ａを、保持している共有鍵を用いて暗号化し、暗号化乱数Ａ’を作成する（ステップＳ１２２）。また、認証処理部２０４は、任意の乱数Ｂを作成する（ステップＳ１２２）。

[0226] 機器２００ａの認証処理部２０４は、ステップＳ１２２において暗号化した暗号化乱数Ａ’と乱数Ｂとを、コントローラ１００に送信する（ステップＳ１２３）。

[0227] コントローラ１００の認証処理部１０３は、暗号化乱数Ａ’と乱数Ｂとを受信する。認証処理部１０３は、暗号化乱数Ａ’を共有鍵で復号する。復号結果の値と、ステップＳ１２１においてコントローラ自身が作成した乱数Ａとが一致した場合、認証処理部１０３は、乱数Ａに関する検証が成功したと判断する（ステップＳ１２４）。

[0228] ステップＳ１２４において、乱数Ａの検証が成功しない場合、コントローラの認証処理部１０３は、機器に対するエラー通知を行い、当該サブルーチンの呼び出し元に対して、戻り値「エラー」を返す。このとき、エラー通知を受信した機器側でも、戻り値「エラー」を返し、コントローラと機器との双方が当該サブルーチン処理を終了する。

[0229] ステップＳ１２４において、乱数Ａの検証が成功した場合、コントローラの認証処理部１０３は、機器２００ａより受信した乱数Ｂを共有鍵で暗号化

し、暗号化乱数Ｂ’を作成する（ステップＳ１２５）。

[0230] 続いて、コントローラの認証処理部１０３は、機器情報保持部１０２の接続機器管理テーブル１０００の基準機器１０８０の項目を参照し、機器２００ａが基準機器であるかを確認する。機器２００ａが基準機器である場合、グループ鍵を作成する（ステップＳ１２６）。グループ鍵はＡＥＳの鍵長１２８ビットとし、任意の一般的技術を用いて作成するため説明は省略する。また、機器２００ａがコントローラに対して、最初に接続要求を行った機器である場合や基準機器である機器との接続が切断された場合などで、基準機器の設定がなされていない場合は、当該機器２００ａを基準機器として設定し、グループ鍵の作成を行う。

[0231] 一方、接続機器管理テーブル１０００を参照し、機器２００ａが基準機器ではないことが確認された場合、認証処理部１０３は、機器情報保持部１０２の保持する接続機器管理テーブル１０００より、既に作成済のグループ鍵の情報を取得する。

[0232] また、コントローラの認証処理部１０３は、セッション鍵を作成する（ステップＳ１２７）。セッション鍵についても、グループ鍵と同様、ＡＥＳの鍵長１２８ビットとし、任意の一般的技術を用いて作成する。

[0233] 続いて、コントローラの認証処理部１０３は、セッション有効期間を設定する（ステップＳ１２８）。このとき、認証処理部１０３は、予め定めた所定値（例えば、２４時間あるいは７２時間など）を、セッション有効期間とする。

[0234] コントローラの認証処理部１０３は、ステップＳ１２６、Ｓ１２７で得られた、グループ鍵及びセッション鍵の情報を、共有鍵を用いて暗号化する（ステップＳ１２９）。

[0235] 認証処理部１０３は、ステップＳ１２５で暗号化した暗号化乱数Ｂ’、ステップＳ１２９で暗号化した暗号化グループ鍵、暗号化セッション鍵、及びステップＳ１２８で設定したセッション有効期間を、通信部１０５を介して、機器２００ａに送信する（ステップＳ１３０）。

[0236] 機器２００ａの認証処理部２０４は、コントローラ１００より受信した暗号化乱数Ｂ’を検証する（ステップＳ１３１）。認証処理部２０４は、保持している共有鍵で暗号化乱数Ｂ’を復号する。復号結果の値が、ステップＳ１２２において機器２００ａ自身が作成した乱数Ｂと合致する場合、認証処理部２０４は、乱数Ｂの検証が成功したと判断する。

[0237] ステップＳ１３１において、乱数Ｂの検証が成功しない場合、認証処理部２０４は、コントローラ１００が正当なコントローラではないと判断し、コントローラ１００に対するエラー通知を行い、当該サブルーチンの呼び出し元に対して、戻り値「エラー」を返す。このとき、エラー通知を受信したコントローラ側でも、戻り値「エラー」を返し、コントローラと機器との双方が当該サブルーチン処理を終了する。

[0238] ステップＳ１３１において、乱数Ｂの検証が成功した場合、機器２００ａの認証処理部２０４は、暗号化グループ鍵及び暗号化セッション鍵を共有鍵で復号する（ステップＳ１３２）。

[0239] また、機器２００ａの認証処理部２０４は、コントローラ１００に対して検証成功を通知する（ステップＳ１３３）。

[0240] （機器履歴情報送信処理）

図２２は、機器２００ａからサーバ３００に対して、機器履歴情報を送信する手順の一例を示したシーケンス図である。このような機器履歴情報の送信は、定期的、あるいは不定期に行う。また、以下では機器２００ａの例示として手順の説明を行うが、機器２００ｂ、機器２００ｃについても処理の手順は同様である。

[0241] 機器の機器管理部２０１は、機器履歴保持部２０２に蓄積した機器履歴情報をセッション鍵で暗号化し、機器自身の機器ＩＤとともにコントローラ１００に送信する（ステップＳ１６１）。

[0242] コントローラ１００の機器管理部１０１は、通信部１０５を介して、機器ＩＤ及び暗号化された機器履歴情報を受信する。そして、機器情報保持部１０２が有する接続機器管理テーブル１０００より、機器ＩＤに紐づくセッシ

ョン鍵を取得し、受信した機器履歴情報を復号する（ステップＳ１６２）。

[0243] コントローラ１００の通信部１０５とサーバ３００の通信部３０５とは、ＳＳＬ認証を行い、暗号通信路を確立する（ステップＳ１６３）。ここで、ＳＳＬ認証は一般的な技術を用いることから説明を省略する。

[0244] コントローラ１００の機器管理部１０１は、通信部１０５を介して、コントローラ自身のコントローラＩＤ、機器から受信した機器ＩＤ、復号した機器履歴情報を、サーバ３００に送信する（ステップＳ１６４）。

[0245] サーバ３００の機器情報管理部３０１は、通信部３０５を介して受信した、コントローラＩＤ、機器ＩＤ、機器履歴情報を、機器情報保持部３０２が有する機器情報管理テーブル１３００に登録する（ステップＳ１６５）。

[0246] （制御情報送信処理）

図２３は、サーバ３００が機器２００ａの制御を実行する手順の一例を示したシーケンス図である。サーバ３００は、コントローラ１００に対して、機器２００ａを制御するための制御依頼情報を送信する。制御依頼を受付けたコントローラ１００は、機器２００ａに対する制御コマンドを作成及び送信し、制御依頼に応じた機能を機器２００ａに実行させる。このようなサーバ３００から機器２００ａに対する制御依頼は、定期的、あるいは不定期に行われる。制御依頼には、例えば、機器に実行させる機能、ディスプレイに表示させる内容などが含まれる。

[0247] 以下では機器２００ａの例示として手順の説明を行うが、機器２００ｂ、機器２００ｃについても処理の手順は同様である。

[0248] サーバ３００の通信部３０５とコントローラ１００の通信部１０５とは、ＳＳＬ認証を行い、暗号通信路を確立する（ステップＳ１７１）。

[0249] サーバ３００の機器情報管理部３０１は、機器２００ａに所定の動作を実行させるための制御依頼情報を作成する。そして、通信部３０５を介して、コントローラ１００に送信する（ステップＳ１７２）。

[0250] コントローラ１００の機器管理部１０１は、通信部１０５を介して、制御依頼情報を受信する。そして、機器管理部１０１は、当該制御依頼情報が、

ネットワーク内のどの機器に対するどのような制御依頼であるかを確認し、当該制御依頼に応じて、機器２００ａに実行させるための制御コマンドを作成する（ステップＳ１７３）。

[0251] そして、ステップＳ１７３で作成した制御コマンドが、複数の機器向けの指示である場合、コントローラ１００の機器管理部１０１は、グループ鍵を用いて、制御コマンドを暗号化する（ステップＳ１７４）。このとき、グループ鍵を用いて暗号化した旨を意味する情報を、送信する制御コマンドのヘッダ部分に付与してもよい。

[0252] ステップＳ１７３で作成した制御コマンドが、単一の機器向けの指示である場合、コントローラ１００の機器管理部１０１は、セッション鍵を用いて、制御コマンドを暗号化する（ステップＳ１７５）。このとき、セッション鍵を用いて暗号化した旨を意味する情報を、送信する制御コマンドのヘッダ部分に付与してもよい。

[0253] コントローラ１００の通信部１０５は、グループ鍵あるいはセッション鍵を用いて暗号化した制御コマンドを、対象の機器に送信する（ステップＳ１７６）。

[0254] 機器２００ａは、通信部１０５を介して、暗号化された制御コマンドを受信し、グループ鍵またはセッション鍵で復号化する（ステップＳ１７７）。このとき、グループ鍵あるいはセッション鍵のどちらを用いて復号するかの判断は、ステップＳ１７４またはステップＳ１７５において、ヘッダ部分に付与した情報を用いて判断してもよい。または、グループ鍵とセッション鍵とのそれぞれを用いて、制御コマンドを復号し、復号結果を用いて判断するとしてもよい。

[0255] （機器履歴情報ＭＡＣ送信処理）

機器からコントローラに機器履歴情報を送信する場合において、本来機器履歴情報の送信が認められていない第三者による、送信元機器への成りすまし送信が問題となることがある。

[0256] ここで説明する機器履歴情報ＭＡＣ送信処理は、上記成りすまし送信に対

抗するために、送信元機器が、機器履歴情報の暗号化に加えて、ヘッダ、送信元アドレス、送信先アドレスを含めたＭＡＣを生成し、暗号化された機器履歴情報と共に生成したＭＡＣを送信する。

[0257] このため、例えば、第三者が、ヘッダ、送信元アドレス、送信先アドレス等を書き換える改ざんによる成りすまし送信を行ったとしても、ヘッダ、送信元アドレス、送信先アドレス、機器履歴情報を含むＭＡＣについてのＭＡＣ検証を行うことでその改ざんを検出することができる。

[0258] 以下、機器履歴情報ＭＡＣ送信処理について、図２４、図２５を参照しながら、機器２００ａが、ホームエリアネットワーク４００に接続する他の全ての機器（ここでは、機器２００ｂとしている。）及びコントローラ１００に対して、機器履歴情報をマルチキャスト送信する場合を例に挙げて説明する。

[0259] 図２４は、暗号化前と暗号化後のメッセージフォーマットのデータ構成図である。

[0260] 図２４（ａ）は、暗号化前の機器履歴情報（以下、この暗号化前の機器履歴情報と、後述する制御情報ＭＡＣ送信処理における暗号化前の制御情報とのことを、便宜上「送信データ」とも呼ぶ。）を含む、暗号化前のメッセージフォーマットのデータ構造図である。

[0261] 同図に示される通り、暗号化前のメッセージフォーマットは、ヘッダ２４０１と、送信元アドレス２４０２と、送信先アドレス２４０３と、送信データ２４０４とから構成される。

[0262] ヘッダ２４０１は、送信データが複数のパケットに分割される場合に付与されるフラグメントのフラグ、フラグメントの番号等を含む。

[0263] 送信元アドレス２４０２は、送信データ２４０４を送信する機器のアドレス、例えば、ＩＰ（Internet Protocol）アドレス、ＭＡＣ（Media Access Control）アドレス等であり、送信する機器を識別する情報を含む。

[0264] 送信先アドレス２４０３は、送信データ２４０４を受信する機器又はコントローラのアドレス、例えば、ＩＰアドレス、ＭＡＣアドレス等であり、受

信する機器又はコントローラを識別する情報を含む。マルチキャスト送信におけるマルチキャストアドレスを含むとしてもよい。

[0265] 機器２００は、送信データ２４０４を平文として暗号化する。また、ヘッダ２４０１と、送信元アドレス２４０２と、送信先アドレス２４０３と、送信データ２４０４とを平文としてＭＡＣを生成する。このとき、暗号化は、ＡＥＳで暗号化し、ＭＡＣの生成は、ＡＥＳのＣＢＣ－ＭＡＣ（Cipher Block Chaining MAC）、ＨＭＡＣ（Hash-based MAC）で生成するとしてもよい。また、暗号化と認証用データの作成を、ＡＥＳ－ＣＣＭ（Counter with CBC MAC）やＡＥＳ－ＧＣＭ（Galois/Counter Mode）等の認証付暗号化で行うとしてもよい。認証付暗号化を行う場合でも、暗号化は、送信データ２４０４を平文とし、ＭＡＣ生成は、ヘッダ２４０１と、送信元アドレス２４０２と、送信先アドレス２４０３と、送信データ２４０４とを平文として実施する。

[0266] 図２４（ｂ）は、暗号化後のメッセージフォーマットのデータ構造図である。

[0267] 同図に示される通り、暗号化後のメッセージフォーマットは、ヘッダ２４０１と、送信元アドレス２４０２と、送信先アドレス２４０３と、認証付暗号化データ２４０５とから構成される。

[0268] 認証付暗号化データ２４０５は、暗号化した送信データとＭＡＣとを結合したデータである。

[0269] 図２５は、機器履歴情報ＭＡＣ送信処理手順の一例として、機器２００ａから、ホームエリアネットワーク４００に接続する他の全ての機器及びコントローラ（ここでは、機器２００ｂ、コントローラ１００であるとしている。）に対して、機器履歴情報をマルチキャスト送信する場合の手順を示したシーケンス図である。

[0270] このような機器履歴情報の送信は、定期的、あるいは不定期に行う。

[0271] 機器２００ａは、機器履歴保持部２０２に蓄積した機器履歴情報をグループ鍵で暗号化する。このとき、グループ鍵で暗号化した旨の情報を、送信す

る履歴情報のヘッダ部分に付与するとしてもよい。

[0272] そして、機器２００ａは、ヘッダと、送信元アドレスと、送信先アドレスと、履歴情報とからＭＡＣを生成する（ステップＳ２５０１）。

[0273] ＭＡＣを生成すると、機器２００ａは、一斉同報通信を利用して、機器２００ｂと、コントローラ１００とに対して、図２４（ｂ）に示された暗号化後のメッセージフォーマットの形式で、認証付暗号化データを送信する（ステップＳ２５０２）。また、この際、機器２００ａは、自身の機器ＩＤも併せて送信する。

[0274] コントローラ１００は、機器２００ａから受信した暗号化した送信データをグループ鍵で復号して機器履歴情報を取得し、ヘッダと、送信元アドレスと、送信先アドレスと、送信データとを用いてＭＡＣ検証を行う（ステップＳ２５０３）。このとき、ヘッダに、グループ鍵で暗号化した旨の情報が付与されている場合には、その情報を参照して、グループ鍵で復号することを決定するとしてもよい。

[0275] ステップＳ２５０４の処理において、ＭＡＣ検証に成功した場合に（ステップＳ２５０４：Ｙｅｓ）、コントローラ１００は、サーバ３００との間でＳＳＬ認証を行い、暗号通信路を確立する（ステップＳ２５０５）。

[0276] コントローラ１００は、自身のコントローラＩＤ、機器２００ａから受信した機器ＩＤ、復号した機器履歴情報を、サーバ３００に送信する（ステップＳ２５０６）。

[0277] サーバ３００は、コントローラ１００から受信したコントローラＩＤ、機器ＩＤ、機器履歴情報を、機器情報保持部３０２が有する機器情報管理テーブル１３００に登録する（ステップＳ２５０７）。

[0278] ステップＳ２５０４の処理において、ＭＡＣ検証に成功しなかった場合に（ステップＳ２５０４：Ｎｏ）、コントローラ１００は、サーバ３００への機器履歴情報の送信を行わない。また、ＭＡＣ検証に成功しなかった場合に、ホームエリアネットワーク４００に接続する他の全ての機器及びコントローラに対して、ＭＡＣ検証に成功しなかった旨の通知を行ってもよい。

[0279] 機器２００ｂは、機器２００ａから受信した暗号化した送信データをグループ鍵で復号して機器履歴情報を取得し、ヘッダと、送信元アドレスと、送信先アドレスと、送信データとを用いてＭＡＣ検証を行う（ステップＳ２５０８）。このとき、ヘッダに、グループ鍵で暗号化した旨の情報が付与されている場合には、その情報を参照して、グループ鍵で復号することを決定するとしてもよい。

[0280] ステップＳ２５０９の処理において、ＭＡＣ検証に成功した場合に（ステップＳ２５０９：Ｙｅｓ）、機器２００ｂは、機器履歴情報を利用した処理を行うことができる（ステップＳ２５１０）。

[0281] ステップＳ２５０９の処理において、ＭＡＣ検証に成功しなかった場合に（ステップＳ２５０９：Ｙｅｓ）、機器２００ｂは、機器履歴情報を利用した処理を行わない。また、ＭＡＣ検証に成功しなかった場合に、ホームエリアネットワーク４００に接続する他の全ての機器２００及びコントローラ１００に対して、ＭＡＣ検証に成功しなかった旨の通知を行ってもよい。

[0282] ここでは、機器履歴情報ＭＡＣ送信処理について、機器２００ａが、機器履歴情報を、ホームエリアネットワーク４００に接続する他の全ての機器２００及びコントローラ１００に対してマルチキャスト送信する場合を例に挙げて説明した。

[0283] これに対して、ステップＳ２５０２の処理において、機器２００ａが、機器履歴情報を、コントローラ１００にのみ送信し、ホームエリアネットワーク４００に接続する他の機器には送信しない場合の例も考えられる。

[0284] この場合には、ステップＳ２５０８～ステップＳ２５１０の処理が発生することはない。また、この場合には、ステップＳ２５０１の処理において、機器２００ａは、機器履歴情報の暗号化を、セッション鍵で暗号化し、ステップＳ２５０３の処理において、コントローラ１００は、機器履歴情報の復号化を、セッション鍵で復号化するとしてもよい。

[0285] （制御情報ＭＡＣ送信処理）

コントローラから機器に制御コマンドを送信する場合において、本来制御

コマンドの送信が認められていない第三者による、送信元コントローラへの成りすまし送信が問題となることがある。

[0286] ここで説明する制御情報ＭＡＣ送信処理は、上記成りすまし送信に対抗するために、送信元コントローラが、制御コマンドの暗号化に加えて、ヘッダ、送信元アドレス、送信先アドレス、制御コマンドを含めたＭＡＣを生成し、暗号化された制御コマンドと共に生成したＭＡＣを送信する。

[0287] このため、例えば、第三者が、ヘッダ、送信元アドレス、送信先アドレス等を書き換える改ざんによる成りすまし送信を行ったとしても、ヘッダ、送信元アドレス、送信先アドレスを含むＭＡＣについてのＭＡＣ検証を行うことでその改ざんを検出することができる。

[0288] 以下、制御情報送信処理（図２３等参照）から、その一部の処理が変更された制御情報ＭＡＣ送信処理について、図２４、２６を参照しながら説明する。

[0289] 図２４（ａ）は、前述した通り、暗号化前のメッセージフォーマットのデータ構造図である。

[0290] 機器履歴情報ＭＡＣ送信処理において、送信データ２４０４が、暗号化前の機器履歴情報である場合について説明したが、この制御情報ＭＡＣ送信処理においては、送信データ２４０４が、暗号化前の制御コマンドである場合の例となっている。

[0291] 図２４（ｂ）は、前述した通り、暗号化後のメッセージフォーマットのデータ構成図である。

[0292] 機器履歴情報ＭＡＣ送信処理において、認証付暗号化データ２４０５が、暗号化した履歴情報とＭＡＣとを結合したデータである場合について説明したが、この制御情報ＭＡＣ処理においては、認証付暗号化データ２４０５が、暗号化した制御コマンドとＭＡＣとを結合したデータである場合の例となっている。

[0293] 図２６は、制御情報ＭＡＣ送信処理手順の一例を示すシーケンス図である。

[0294] この制御情報ＭＡＣ送信処理は、前述した制御情報送信処理からその処理の一部が変更されたものとなっている。

[0295] このような制御情報ＭＡＣ送信処理は、定期的、あるいは不定期に行う。

[0296] ステップＳ２６０１～ステップＳ２６０３の処理は、制御情報送信処理におけるステップＳ１７１～ステップＳ１７３の処理と同様の処理である。このため、これらの処理の説明は、既に説明済であるため、省略する。

[0297] ステップＳ２６０３の処理が終了すると、ステップＳ２６０３の処理において生成した制御コマンドが複数の機器向けの指示である場合、コントローラ１００は、生成した制御コマンドをグループ鍵で暗号化する。このとき、グループ鍵で暗号化した旨の情報を、送信する制御コマンドのヘッダ部分に付与するとしてもよい。

[0298] そして、コントローラ１００は、ヘッダと、送信元アドレスと、送信先アドレスと、制御コマンドとからＭＡＣを生成する（ステップＳ２６０４）。

[0299] ステップＳ２６０３の処理において生成した制御コマンドが単一の機器向けの指示である場合、コントローラ１００は、生成した制御コマンドをセッション鍵で暗号化する。このとき、グループ鍵で暗号化した旨の情報を、送信する制御コマンドのヘッダ部分に付与するとしてもよい。

[0300] そして、コントローラ１００は、ヘッダと、送信元アドレスと、送信先アドレスと、制御コマンドとからＭＡＣを生成する（ステップＳ２６０５）。

[0301] ＭＡＣを生成すると、コントローラは、対象となる機器に対して、図２４（ｂ）に示された暗号化後のメッセージフォーマットの形式で、認証付暗号化データを送信する（ステップＳ２６０６）。

[0302] 認証付暗号化データを受信した機器（ここでは、認証付暗号化データを受信した機器の代表として、例えば、機器２００ａを用いて説明する。）は、コントローラ１００から受信した暗号化した送信データを、グループ鍵又はセッション鍵で復号して制御コマンドを取得し、ヘッダと、送信元アドレスと、送信先アドレスと、送信データとを用いてＭＡＣ検証を行う（ステップＳ２６０７）。このとき、ヘッダに、グループ鍵で暗号化した旨の情報又は

セッション鍵で暗号化した旨の情報が付与されている場合には、その情報を参照して、グループ鍵とセッション鍵とのいずれを用いて復号するかを決定するとしてもよい。

[0303] ステップＳ２６０８の処理において、ＭＡＣ処理に成功した場合に（ステップＳ２６０８：Ｙｅｓ）、機器２００ａは、復号された制御コマンドの指示に従って動作を行う（ステップＳ２６０９）。

[0304] ステップＳ２６０８の処理において、ＭＡＣ処理に成功しなかった場合に（ステップＳ２６０８：Ｎｏ）、機器２００ａは、復号された制御コマンドの指示に従わない。また、ＭＡＣ検証に成功しなかった場合に、ホームエリアネットワーク４００に接続する他の全ての機器２００及びコントローラ１００に対して、ＭＡＣ検証に成功しなかった旨の通知を行ってもよい。

[0305] ここでは、ＭＡＣ対象（図２４（ａ）参照）が、ヘッダ２４０１、送信元アドレス２４０２、送信先アドレス２４０３、送信データ２４０４からなるとして説明した。なお、セッション鍵を利用して送信データを暗号化する場合には、ＭＡＣ対象が送信データ２４０４からのみなるとしてもよい。この場合には、送信データ２４０４に、カウンターやシーケンス番号等が含まれる。セッション鍵は、コントローラ１００と該当する機器２００とのみが共有するため、第三者による成りすましや再送攻撃は難しい。

[0306] 本開示の一態様では、制御コマンドの送信において次のようにしてもよい。

[0307] コントローラ１００から機器２００への制御コマンドが複数の制御コマンドから構成される場合、複数の制御コマンドを複数の送信データとして送信するとしてもよい。このとき、複数の送信データのヘッダにフラグメントのフラグ、フラグメントの番号等を付与して送信する。送信データを受信した機器２００は、ヘッダにフラグメントのフラグが立っている場合、制御コマンドが複数の送信データから構成されるため、複数の送信データを受信してから制御コマンドを実行する。このとき、すべての送信データに暗号化及びＭＡＣを生成した場合において、複数の送信データのうち、いずれかのＭＡ

Ｃ検証が成功しなかったときには、制御コマンドを実行しない。また、複数の送信データのうち、いずれかのＭＡＣ検証が成功しなかった場合に、以降のフラグメントフラグの付与された送信データのＭＡＣ検証をせずに送信データを破棄するとしてもよい。これにより、受信した機器２００やコントローラ１００の処理を軽くすることができる。

[0308] すべての送信データについてＭＡＣを生成しない場合に、すべての送信データのヘッダ、送信元アドレス、送信先アドレス、及び制御コマンドを結合し、ＭＡＣを生成して、最後の送信データにＭＡＣを付与するとしてもよい。これにより、ＭＡＣ検証を１回実行するだけで、すべての送信データについての完全性を検証することができ、受信した機器２００やコントローラ１００の処理を軽くすることができる。

[0309] ここでは、制御情報ＭＡＣ送信処理について、送信データ２４０４が制御コマンドであるとして説明したが、必ずしも送信データ２４０４が制御コマンドである場合に限られず、例えば、送信データ２４０４が、サーバ３００から機器２００ａに対する通知である場合の例も考えられる。

[0310] この場合には、ステップＳ２６０３の処理は発生せず、コントローラ１００は、サーバ３００から受信した通知を、そのまま送信データ２４０４として利用して、ステップＳ２６０４以降の処理を行う。また、この場合には、ステップＳ２６０８の処理において、機器２００ａは、ＭＡＣ処理に成功した場合に（ステップＳ２６０８：Ｙｅｓ）、ステップＳ２６０９の処理を行う代わりに、復号された通知を記憶する処理を行い、ＭＡＣ処理に成功しなかった場合に（ステップＳ２６０８：Ｎｏ）、復号された通知を記憶する処理を行わない。

[0311] ＜１．４　まとめ＞

本実施の形態は、コントローラと接続する複数機器の中から基準機器を設け、基準機器におけるグループ鍵更新のタイミングで、コントローラが他の機器に対する更新通知を行うことにより、他の機器にグループ鍵の更新を実行させる。これにより、コントローラに接続する複数機器のグループ鍵更新

タイミングを合わせることが可能となり、コントローラと各機器とが相互認証及びグループ鍵更新を行っても、コントローラは暗号化した情報の一斉送信を行うことができる。

[0312] また、コントローラと機器との相互認証において、２種類の手続きを採用している。コントローラと機器とが接続する際には、ＰＫＩに基づく公開鍵証明書を用いた相互認証を行う、一方、以後のセッション更新処理時には、共有鍵を用いた相互認証を行う。一般にＰＫＩに基づく相互認証に比較すると、共有鍵を用いた相互認証は処理にかかる負荷が低い。したがって、セッション更新時の相互認証処理として、共有鍵を用いた手続を採用することにより、相互認証に係る処理の負荷を軽減することができる。

[0313] ＜２．実施形態２＞

＜２－１．概要＞

本実施の形態に係る認証システムは、コントローラが、各機器との間のセッション残り時間を、同時刻においては同様の値を有するように設定する点が異なる。

[0314] 以下、説明の便宜上、実施の形態１と同様の構成については、同じ符号を用いる。また、実施の形態１と同様の構成については、説明を省略し、異なる点を重点的に説明する。

[0315] ＜２－２．構成＞

本実施の形態における、認証システム、コントローラ、機器、サーバの構成は、各々実施の形態１における、認証システム１０、コントローラ１００、機器２００ａ～機器２００ｃ、サーバ３００と同様の構成である。しかし、コントローラ１００の機器情報保持部１０２が保持する接続機器管理テーブルのデータ構造が、実施の形態１とは一部異なる。

[0316] 図２４は、本実施の形態における接続機器管理テーブル２０００のデータ構造とデータの一例を示した図である。

[0317] 接続機器管理テーブル２０００は、接続している機器毎のデータである接続機器管理レコード群を保持しており、各レコードには、機器ＩＤ２０１０

、証明書ＩＤ２０２０、共有鍵２０３０、グループ鍵２０４０、セッション鍵２０５０、セッション残り時間２０６０、セッション更新状態２０７０、基準機器２０８０の項目が含まれる。実施の形態１と異なる点は、同一のグループ鍵２０４０を有する機器に対して、セッション残り時間２０６０を共通の値で設定する点である。例えば、図２４では、機器ＩＤ１と機器ＩＤ２とは、同一のグループ鍵である“１１２２３・・・”を保持しており、セッション残り時間についても共に“１３：４０：５０”という同じ値を有している。

[0318] ＜２－３．動作＞

実施の形態１と同様に、本実施の形態においても、認証システム１０は、“機器登録処理”、“セッション更新処理”、“ＰＫＩに基づく相互認証～共有鍵の作成”、“共有鍵を用いた相互認証～セッションに係る情報の作成”、“機器履歴情報送信処理”、“制御情報送信処理”を行う。まず、“共有鍵を用いた相互認証～セッションに係る情報の作成”の手順について説明し、その他の各処理についても、順に、実施の形態１と異なる点を中心に説明する。

[0319] （共有鍵を用いた相互認証～セッションに係る情報の作成）

実施の形態１と同様に、図２１のシーケンス図におけるステップＳ１２１からステップＳ１３３に沿って、コントローラと機器とは、共有鍵を用いた相互認証を行い、セッションに係る情報である、グループ鍵、セッション鍵、セッション有効期間を作成する。

[0320] ただし、ステップＳ１２８における、コントローラ１００のセッション有効期間の設定方法が実施の形態１とは異なる。

[0321] 本実施の形態において、コントローラ１００の認証処理部１０３は、機器が基準機器である場合、予め定めた所定値（例えば、２４時間あるいは７２時間など）を、セッション有効期間として設定する。しかし、機器が基準機器ではない場合、セッション有効期間を以下のように設定する（ステップＳ１２８）。

[0322] コントローラ１００の認証処理部１０３は、機器情報保持部１０２が有する接続機器管理テーブル２０００のセッション残り時間２０６０を参照して、基準機器のセッション残り時間値を取得する。そして、取得した値を、当該機器のセッション有効期間として設定する。

[0323] 図２４に示す接続機器管理テーブル２０００のデータを例に説明すると、基準機器ではない機器ＩＤ２の機器に係るセッション有効期間を設定する際、接続機器管理テーブル２０００から基準機器である機器ＩＤ１のセッション残り時間を取得し、機器ＩＤ２のセッション有効期間として設定する。

[0324] このように、基準機器ではない機器のセッション有効期間を、当該セッション有効期間の設定時点における、基準機器のセッション残り期間に合わせて設定することにより、基準機器と、基準機器以外の機器とが、近似するセッション残り時間を有することとなる。

[0325] （機器登録処理）

実施の形態１と同様に、図１２のシーケンス図における、ステップＳ１０１からステップＳ１０７に沿って、コントローラと機器とは、接続要求、ＰＫＩに基づく相互認証～共有鍵の作成、共有鍵を用いた相互認証～セッションに係る情報の作成、各コントローラ及び機器の登録を行う。

[0326] 上述の“共有鍵を用いた相互認証～セッションに係る情報の作成”の手順に記載のとおり、ステップＳ１０３において、基準機器ではない機器のセッション有効期間は、基準機器のセッション残り時間が設定される。

[0327] ステップＳ１０４において、機器側が登録するセッション有効期間は、機器が基準機器であるかないかに関わらず、コントローラ１００より受信したセッション有効期間をセッション残り時間として登録する点は、実施の形態１と同様である。

[0328] ステップＳ１０６において、コントローラが、基準機器ではない機器の機器登録を行う際、セッション残り期間の項目は、基準機器のセッション残り時間を共有する形で登録してもよいし、ステップＳ１０３において設定したセッション有効期間をセッション残り時間として登録してもよい。いずれの

形式で登録する場合においても、図１２のシーケンス図におけるステップＳ１０３とステップＳ１０４及びステップＳ１０６は、間をおかずに実施されるものであり、コントローラ１００の接続機器管理テーブル２０００に設定する基準機器と基準機器ではない機器に係るセッション残り時間、及び機器側の接続コントローラ管理テーブル１１００に設定するセッション残り時間は、近似値を有することとなる。

[0329] （セッション更新処理）

図２５及び図２６は、機器とコントローラとのそれぞれにおける、本実施形態でのセッション更新処理の手順の一例を示したフローチャート図であり、図２７は、機器とコントローラとのやりとりを含む、セッション更新処理の手順の一例を示すシーケンス図である。

[0330] 図２５及び図２６のフローチャートに沿って、機器及びコントローラのそれぞれにおける処理の概要を説明した後、図２７のシーケンス図に沿って、機器とコントローラとのやりとりを含む処理の詳細について説明する。

[0331] まず、図２５のフローチャートに沿って、機器におけるセッション更新処理の概要について説明する。

[0332] 機器は、コントローラとの間で設定しているセッション残り時間を監視し、予め定めた所定値以下であるか否かを確認する（ステップＳ３０１０）。セッション残り時間が所定値より大きい場合（ステップＳ３０１０のＮＯ）、監視を続ける。

[0333] セッション残り時間が予め定めた所定値以下である場合（ステップＳ３０１０のＹＥＳ）、機器はセッション更新を行うために、コントローラに対して、セッション更新要求を送信する（ステップＳ３０２０）。

[0334] そして、“共有鍵を用いた相互認証～セッションに係る情報の作成”のサブルーチンを実行することで、コントローラと共有鍵を用いた相互認証を行った後、セッションに係る情報である、グループ鍵及びセッション鍵の作成、セッション有効期間の設定を行う（ステップＳ３０３０）。

[0335] ステップＳ３０３０のサブルーチンの戻り値が「正常」である場合（ステ

ップＳ３０４０のＹＥＳ）、機器は、ステップＳ３０３０にて作成した新たなセッションに係る情報を、セッション更新情報として登録する（ステップＳ３０５０）。

[0336] 一方、ステップＳ３０３０のサブルーチンの戻り値が「エラー」である場合（ステップＳ３０４０のＮＯ）、セッションの更新を行わずに、セッション更新処理を終了する。

[0337] 次に、図２６のフローチャートに沿って、コントローラにおけるセッション更新処理の概要について説明する。

[0338] コントローラは、機器からのセッション更新要求を待ち受ける（ステップＳ３１１０）。受信しなければ（ステップＳ３１１０のＮＯ）、機器からのセッション更新要求を待ち続ける。

[0339] コントローラは機器からセッション更新要求を受信すると（ステップＳ３１１０のＹＥＳ）、“共有鍵を用いた相互認証～セッションに係る情報の作成”のサブルーチンを実行することで、機器と共有鍵を用いた相互認証を行った後、セッションに係る情報である、グループ鍵、セッション鍵、セッション有効期間の設定を行う（ステップＳ３１２０）。

[0340] ステップＳ３１３０のサブルーチンの戻り値が「正常」である場合（ステップＳ３１３０のＹＥＳ）、コントローラは、ステップＳ３１２０にて作成した新たなセッションに係る情報を、セッション更新情報として登録する（ステップＳ３１４０）。

[0341] 一方、ステップＳ３１２０のサブルーチンの戻り値が「エラー」である場合（ステップＳ３１３０のＮＯ）、当該セッション更新を実行中の機器とのセッション更新は行わない。

[0342] そして、他にセッションを更新していない機器が存在する場合（ステップＳ３１５０のＹＥＳ）、最初のステップに戻り、当該セッション未更新機器からのセッション更新要求を待ち受ける（ステップＳ３１１０）。

[0343] 全ての機器について、セッション更新処理が完了した場合（ステップＳ３１５０のＮＯ）、セッション更新処理を終了する。

[0344] ここからは、図２７のシーケンス図に沿って、実施の形態１との差分を中心に、機器とコントローラとのやりとりを含めて説明する。機器については、一例として、機器２００ａが基準機器であり、機器２００ｂが基準機器以外の機器であるとする。

[0345] 機器の機器管理部２０１は、セッション残り時間が所定の閾値以下になった時点で、認証処理部２０４にセッション更新を指示する。指示を受付けた認証処理部２０４は、通信部２０６を介して、セッション更新要求をコントローラ１００に送信する（ステップＳ２０２、ステップＳ２０７）。

[0346] ここで、本実施の形態において、基準機器以外の機器は、基準機器が保持するセッション残り時間と近似のセッション残り時間を有している。したがって、ステップＳ２０２とステップＳ２０７とが近似するタイミングで実施されることにより、コントローラと各機器との間のグループ鍵更新は同じようなタイミングで実施されることとなる。

[0347] “ＰＫＩに基づく相互認証～共有鍵の作成”、“機器履歴情報送信処理”、“制御情報送信処理”については、実施の形態１と同様であるため、説明を省略する。

[0348] ＜２－４．まとめ＞

本実施の形態に係る認証システムでは、基準機器以外のセッション有効期間を、当該セッション有効期間設定時点における基準機器のセッション残り時間に基づき設定することで、基準機器と基準機器以外の機器とが、セッション残り時間として近似する値を有する。したがって、各機器が当該セッション残り時間に基づきセッション更新処理を行うことで、グループ鍵の更新を近似するタイミングで実施することとなり、コントローラと各機器とが相互認証及びグループ鍵更新を行っても、コントローラは暗号化した情報の一斉送信を行うことができる。

[0349] ＜３．実施形態３＞

＜３－１．概要＞

本実施の形態に係る認証システムは、コントローラと各機器とが、現在使

用するためのグループ鍵と更新後に使用するためのグループ鍵との２種類のグループ鍵を保持する点が異なる。

[0350] 以下、説明の便宜上、上記実施の形態と同様の構成については、同じ符号を用いる。また、上記実施の形態と同様の構成については、説明を省略し、異なる点を重点的に説明する。

[0351] ＜３－２．構成＞

本実施の形態における、認証システム、コントローラ、機器、サーバの構成は、各々実施の形態２における、認証システム１０、コントローラ１００、機器２００ａ～機器２００ｃ、サーバ３００と同様の構成である。しかし、コントローラ１００の機器情報保持部１０２が保持する接続機器管理テーブルのデータ構成の一部、及び機器の機器情報保持部２０３が保持する接続コントローラ管理テーブルのデータ構造の一部が、上記実施の形態とは異なる。

[0352] 図２８は、本実施の形態において、コントローラ１００の機器情報保持部１０２が有する接続機器管理テーブル３０００のデータ構造及びデータの一例を示した図である。

[0353] 接続機器管理テーブル３０００は、接続している機器毎のデータである接続機器管理レコード群を格納しており、各レコードには、機器ＩＤ３０１０、証明書ＩＤ３０２０、共有鍵３０３０、グループ鍵（現）３０４０、グループ鍵（新）３０５０、セッション鍵３０６０、セッション残り時間３０７０、セッション更新状態３０８０、基準機器３０９０の項目が含まれる。グループ鍵については、グループ鍵（現）とグループ鍵（新）の２つの項目を有している。

[0354] 図２９は、本実施の形態において、機器の機器情報保持部２０３が有する接続コントローラ管理テーブル３１００のデータ構造及びデータの一例を示した図である。

[0355] 接続コントローラ管理テーブル３１００は、接続しているコントローラのデータである接続コントローラ管理レコード群を格納しており、各レコード

には、コントローラＩＤ３１１０、証明書ＩＤ３１２０、共有鍵３１３０、グループ鍵（現）３１４０、グループ鍵（新）３１５０、セッション鍵３１６０、セッション残り時間３１７０の項目が含まれる。グループ鍵については、接続機器管理テーブル３０００と同様に、グループ鍵（現）とグループ鍵（新）の２つの項目を有している。

[0356] ここで、コントローラが各機器に対して一斉送信する情報の暗号化は、コントローラ及び各機器が、グループ鍵（現）として保持している暗号鍵を用いて行われる。一方、グループ鍵（新）は、コントローラと基準機器との間のセッション更新処理において、新たに作成したグループ鍵を保持する項目である。

[0357] ＜３－３．動作＞

実施の形態２と同様に、本実施の形態における認証システム１０は、“機器登録処理”、“セッション更新処理”、“ＰＫＩに基づく相互認証～共有鍵の作成”、“共有鍵を用いた相互認証～セッションに係る情報の作成”、“機器履歴情報送信処理”、“制御情報送信処理”を行う。

[0358] （機器登録処理）

実施の形態２と同様に、図１２のシーケンス図における、ステップＳ１０１からステップＳ１０７に沿って、コントローラと機器とは、接続要求、ＰＫＩに基づく相互認証～共有鍵の作成、共有鍵を用いた相互認証～セッションに係る情報の作成、各コントローラ及び機器の登録を行う。

[0359] ただし、ステップＳ１０４において、機器２００ａの認証処理部２０４が、機器管理部２０１を介して、接続コントローラ管理テーブル３１００を登録する際、ステップＳ１０３において作成したグループ鍵の情報は、グループ鍵（現）３１４０の項目に登録する（ステップＳ１０４）。

[0360] また、ステップＳ１０６において、コントローラ１００の機器管理部１０１が、接続機器管理テーブル３０００を登録する際も、グループ鍵の情報は、グループ鍵（現）３０４０の項目に登録する（ステップＳ１０６）。

[0361] （セッション更新処理）

図３０及び図３１は、機器とコントローラとのそれぞれにおける、本実施形態のセッション更新処理の手順の一例を示したフローチャート図であり、図３２は、機器とコントローラとのやりとりを含む、セッション更新処理の手順の一例を示すシーケンス図である。

[0362] 図３０及び図３１のフローチャートに沿って、機器及びコントローラにおける処理の概要を説明した後、図３２のシーケンス図に沿って、機器とコントローラとのやりとりを含む処理の詳細について説明する。

[0363] まず、図３０のフローチャートに沿って、機器におけるセッション更新処理の概要について説明する。

[0364] 機器は、コントローラとの間で設定しているセッション残り時間を監視し、予め定めた所定値以下であるか否かを確認する（ステップＳ４０１０）。セッション残り時間が所定値より大きい場合（ステップＳ４０１０のＮＯ）、監視を続ける。

[0365] セッション残り時間が予め定めた所定値以下である場合（ステップＳ４０１０のＹＥＳ）、機器はセッション更新を行うために、コントローラに対して、セッション更新要求を送信する（ステップＳ４０２０）。

[0366] そして、“共有鍵を用いた相互認証～セッションに係る情報の作成”のサブルーチンを実行することで、コントローラと共有鍵を用いた相互認証を行った後、セッションに係る情報である、グループ鍵及びセッション鍵の作成、セッション有効期間の設定を行う（ステップＳ４０３０）。

[0367] ステップＳ４０３０のサブルーチンの戻り値が「正常」である場合（ステップＳ４０４０のＹＥＳ）、ステップＳ４０５０に進み、機器は、ステップＳ４０３０にて作成した新たなセッションに係る情報を、セッション更新情報として登録する（ステップＳ４０５０）。

[0368] そして、機器は、コントローラからのグループ鍵更新通知を待ち受ける（ステップＳ４０６０）。グループ鍵更新通知を受信しない場合（ステップＳ４０６０のＮＯ）、受信するまで待ち続ける。

[0369] グループ鍵更新通知を受信した場合（ステップＳ４０６０のＹＥＳ）、現

在使用しているグループ鍵と、ステップＳ４０３０にて新たに作成したグループ鍵を入れ替えることで、グループ鍵の更新を行う（ステップＳ４０７０）。

[0370] 一方、ステップＳ４０３０のサブルーチンの戻り値が「エラー」である場合（ステップＳ４０４０のＮＯ）、セッション更新を行わずに、セッション更新処理を終了する。

[0371] 次に、図３１のフローチャートに沿って、コントローラにおけるセッション更新処理の概要について説明する。

[0372] コントローラは、機器からのセッション更新要求を待ち受ける（ステップＳ４１１０）。受信しなければ（ステップＳ４１１０のＮＯ）、機器からのセッション更新要求を待ち続ける。

[0373] 機器からセッション更新要求を受信すると（ステップＳ４１１０のＹＥＳ）、コントローラは、“共有鍵を用いた相互認証～セッションに係る情報の作成”のサブルーチンを実行することで、機器と共有鍵を用いた相互認証を行った後、セッションに係る情報である、グループ鍵及びセッション鍵の作成、セッション有効期間の設定を行う（ステップＳ４１２０）。

[0374] ステップＳ４１２０のサブルーチンの戻り値が「正常」である場合（ステップＳ４１３０のＹＥＳ）、コントローラは、ステップＳ４１２０にて作成した新たなセッションに係る情報を、セッション更新情報として登録する（ステップＳ４１４０）。

[0375] 一方、ステップＳ４１２０のサブルーチンの戻り値が「エラー」である場合（ステップＳ４１３０のＮＯ）、当該セッション更新を実行中の機器についてのセッション更新は行わない。

[0376] 他にセッションを更新していない機器が存在する場合（ステップＳ４１５０のＹＥＳ）、最初のステップに戻り、当該セッション未更新機器からのセッション更新要求を待ち受ける（ステップＳ４１１０）。

[0377] 全ての機器について、セッション更新処理が完了した場合（ステップＳ４１５０のＮＯ）、同一のグループ鍵を使用する機器に対して、グループ鍵更

新通知を送信する（ステップＳ４１６０）。

[0378] そして、コントローラ自身も、現在使用しているグループ鍵と、ステップＳ４１２０にて新たに作成したグループ鍵を入れ替えることで、グループ鍵の更新を行う（ステップＳ４１７０）。

[0379] ここからは、図３２のシーケンス図に沿って、実施の形態２との差分を中心に、機器とコントローラとのやりとりを含めて説明する。機器については、一例として、機器２００ａが基準機器であり、機器２００ｂが基準機器以外の機器であるとする。

[0380] 本実施の形態では、実施の形態２と同様に、各機器はセッション残り時間に応じて、コントローラに対するセッション更新を要求し、共有鍵を用いた相互認証～セッションに係る情報の作成を行う。そして、機器とコントローラとは、セッション更新情報を登録する。

[0381] ステップＳ３０４及びステップＳ３１０において、各機器の機器管理部２０１は、作成した、セッション鍵、グループ鍵、及びセッション有効時間を、機器情報保持部２０３の保持する、接続コントローラ管理テーブル３１００に登録する。このとき、作成したグループ鍵の情報はグループ鍵（新）３１５０の項目に登録する。

[0382] また、ステップＳ３０５及びステップＳ３０９において、コントローラの機器管理部１０１は、作成した、セッション鍵、グループ鍵、及びセッション有効時間を、機器情報保持部１０２の有する、接続機器管理テーブル３０００に登録する。このとき、作成したグループ鍵の情報はグループ鍵（新）３０５０の項目に登録する。セッション更新状態３０８０については、上述の実施の形態と同様に、基準機器とのセッション更新を行う際に、基準機器以外の機器に係るセッション更新状態３０８０の値を、“未更新”に設定する。そして、基準機器以外の機器とのセッション更新を行う際には“更新済”に更新する。

[0383] そして、コントローラ１００の機器管理部１０１は、接続機器管理テーブル３０００のセッション更新状態３０８０の項目を参照し、“未更新”の機

器がないかを確認する。このとき、セッション更新状態の項目が“未更新”の機器が存在する場合、当該機器からのセッション更新要求を待ち受ける。セッション更新状態が“未更新”である機器が存在しない場合、コントローラの機器管理部１０１は、同一グループ鍵を用いて暗号通信を行う全ての機器に対して、グループ鍵更新通知を行う（ステップＳ３１１）。

[0384] 機器の機器管理部２０１は、グループ鍵更新通知を受信すると、接続コントローラ管理テーブル３１００のグループ鍵（新）３１５０が保持する値で、グループ鍵（現）３１４０の値を上書き更新し、グループ鍵（新）３１５０に設定されている値は削除する。

[0385] コントローラ１００の機器管理部１０１も同様に、接続機器管理テーブル３０００のグループ鍵（新）３０５０が保持する値で、グループ鍵（現）３０４０を上書き更新した上で、グループ鍵（新）３０５０に設定されている値は削除する。

[0386] “ＰＫＩに基づく相互認証～共有鍵の作成”、“共有鍵を用いた相互認証～セッションに係る情報の作成”、“機器履歴情報送信処理”、“制御情報送信処理”については、上述の実施の形態２と同様であるため、説明を省略する。

[0387] ただし、コントローラが機器に一斉送信する情報の暗号化に用いる暗号鍵は、コントローラ及び機器の各々が「グループ鍵（現）」として保持する暗号鍵を用いる。

[0388] ＜３－４．まとめ＞

本実施の形態に係る認証システムでは、コントローラと各機器とのセッション更新処理において新たに作成したグループ鍵を、暗号通信に用いるグループ鍵とは別の場所に保持する。そして、コントローラと接続する全ての機器との間でセッション更新処理を行った時点で、コントローラが機器に対するグループ鍵更新通知を行い、コントローラと各機器とは、グループ鍵の切り替えを実施する。こうすることにより、コントローラと複数の機器とが同じタイミングでグループ鍵の更新を行うことが可能となり、コントローラと

各機器とが相互認証及びグループ鍵更新を行っても、コントローラは暗号化した情報の一斉送信を行うことができる。

[0389] ＜４．変形例＞

以上、本開示に係る認証方法を用いた認証システムについて、実施の形態に基づき説明したが、以下のように変形することも可能であり、本開示は上述した実施の形態で示した通りの認証方法に限られないことは勿論である。

[0390] （１）上記実施の形態において、コントローラ及び機器は１つのネットワークに接続する。当該ネットワークは、ホームエリアネットワークであってもよいし、その他のエリアネットワークであってもよい。

[0391] （２）上記実施の形態では、１つのコントローラに対して、１つのグループ鍵を設定しているが、複数のグループ鍵を設定してもよい。このとき、同じグループ鍵を用いる機器毎に、１つの基準機器を設定する。

[0392] （３）上記実施の形態において、コントローラと基準機器との接続が削除された場合、コントローラは、機器情報保持部の保持する接続機器管理テーブルから、別の機器を抽出し基準機器として設定する。このとき、基準機器は、常に電源が入っている機器を指定するとしてもよい。例えば、冷蔵庫などの常に電源が入って動作している機器を指定してもよい。

[0393] （４）上記実施の形態における共有鍵を用いた相互認証では、共有鍵と乱数とを用いるチャレンジレスポンス認証を行っているが、これに限定するわけではない。例えば、ＲＦＣ５１９１ Ｐｒｏｔｏｃｏｌ ｆｏｒ Ｃａｒｒｙｉｎｇ Ａｕｔｈｅｎｔｉｃａｔｉｏｎ ｆｏｒ Ｎｅｔｗｏｒｋ Ａｃｃｅｓｓ（ＰＡＮＡ）の認証方式を用いてもよい。ＲＦＣ５１９１については、非特許文献３に記載されている一般的な技術を用いるため、説明は省略する。

[0394] ＲＦＣ５１９１を用いる場合において、更にＥＡＰ－ＰＳＫを用いて認証を行うとしてもよい。また、セッション鍵は、ＥＡＰ－ＰＳＫのネゴシエーションの結果として導出されるＥＭＳＫを用いて導出するとしてもよい。更に、このときの鍵導出関数として、ＨＭＡＣ＿ＳＨＡ２＿２５６を用いても

よい。

[0395] （５）上記実施の形態では、機器登録処理時及びセッション更新処理時において、コントローラがグループ鍵を作成し、機器に対して配信している。しかし、これに限定するものではなく、コントローラと基準機器との間でＥＣＤＨやＤＨ（Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎ）による鍵交換を行うことで、グループ鍵を共有してもよい。

[0396] また、コントローラと基準機器とのそれぞれが、乱数を生成し、生成した乱数を共有鍵で暗号化して相手に送信する。そして、受信した暗号化乱数を共有鍵で復号し、自らが生成した乱数と復号した乱数との排他的論理和演算した結果をグループ鍵としてもよい。

[0397] これらは、コントローラと各機器とにおけるセッション鍵の作成手順として用いてもよい。

[0398] （６）本開示に係るコントローラは、コントローラのための専用機器であってもよい。また、家庭に設置される分電盤であってもよい。その他のテレビなどのＡＶ機器であってもよいし、家電機器などであってもよい。

[0399] （７）コントローラは、接続する機器の消費電力量や蓄電池の電力量、太陽光発電の発電量を表示する機能を有していてもよい。

[0400] （８）本開示に係るコントローラと機器との間の通信方式は、Ｅｔｈｅｒｎｅｔ（登録商標）、Ｗｉ－Ｆｉ（Ｗｉｒｅｌｅｓｓ Ｆｉｄｅｌｉｔｙ）、特定小電力無線、電力線通信、Ｂｌｕｅｔｏｏｔｈ（登録商標）であってもよい。

[0401] （９）上記実施の形態１では、セッション更新処理において、セッション未更新の機器が存在した場合、当該機器に対してセッション更新通知を送信することで、機器にセッション更新を開始させている。ここで、当該機器の電源が入っていない場合、コントローラは当該機器に対して、定期的にセッション更新通知を送信するとしてもよい。

[0402] （１０）上記実施の形態１では、セッション更新処理において、セッション未更新の機器が存在した場合、当該機器に対してセッション更新通知を送

信することで、機器にセッション更新を開始させている。ここで、当該機器において実行中の処理がある等により、機器が、セッション更新処理の開始が不可であると判断する場合、当該機器からコントローラに対して、セッション更新の延期時間を通知して、当該延期時間の経過後にセッション更新処理を行うとしてもよい。

[0403] （１１）上記実施の形態では、接続機器管理テーブルや接続コントローラ管理テーブルが有するセッションの残り時間でセッションの有効期限を管理している。しかし、これに限定するものではなく、セッションの開始日時やセッションの終了日時で管理するとしてもよい。例えば、セッションの開始日時で管理する場合、所定のセッション有効期間を予め設定し、セッション開始日時にセッション有効期間を追加した日時と、現在の日時とを比較し、セッションを更新するかを判断してもよい。また、例えば、セッションの終了日時で管理する場合、現在の日時とセッションの終了日時とを比較し、セッションを更新するかを判断してもよい。

[0404] （１２）上記実施の形態では、セッション更新処理において、機器側で、セッション残り時間に基づき、セッション更新のタイミングを判断し、コントローラにセッション更新要求を送信することで、セッション更新を開始している。しかし、これに限定するものではなく、コントローラ側で、セッション残り時間に基づき、セッション更新のタイミングを判断し、セッション更新を開始するとしてもよい。

[0405] （１３）上記実施の形態では、機器とコントローラとの間で、１対１の暗号化ユニキャスト通信を行うためのセッション鍵を共有している。しかし、セッション鍵を共有せずに、機器とコントローラ間の暗号化通信の全てをグループ鍵で行うとしてもよい。

[0406] （１４）上記実施の形態では、セッション更新処理において、グループ鍵とセッション鍵との両方を更新しているが、これに限定するものではなく、セッション更新処理時において、グループ鍵のみまたはセッション鍵のみを更新するとしてもよい。

[0407] （１５）上記実施の形態における認証システムに係る装置である、コントローラ、機器、サーバは、具体的には、プロセッサ、メモリなどから構成される。メモリには、コンピュータプログラムが記録されている。プロセッサが、メモリに記録されているコンピュータプログラムにしたがって動作することにより、各装置はその機能を達成する。ここで、コンピュータプログラムは、所定の機能を達成するために、コンピュータに対する指令を示す命令コードが複数個組み合わされて構成されたものである。

[0408] （１６）上記実施の形態における認証システムに係る各装置を構成する構成要素の一部または全部は、１個のシステムＬＳＩ（Ｌａｒｇｅ　Ｓｃａｌｅ　Ｉｎｔｅｇｒａｔｉｏｎ：大規模集積回路）から構成されているとしてもよい。上記の各装置を構成する構成要素の各部は、個別に１チップ化されていても良いし、一部または全てを含むように１チップ化されてもよい。

[0409] また、ここでは、システムＬＳＩと記述したが、集積度の違いにより、ＩＣ（Ｉｎｔｅｇｒａｔｅｄ　Ｃｉｒｃｕｉｔ）、ＬＳＩ、スーパーＬＳＩ、ウルトラＬＳＩと呼称されることもある。また、集積回路化の手法はＬＳＩに限るものではなく、専用回路または汎用プロセッサで実現してもよい。ＬＳＩ製造後に、プログラムすることが可能なＦＰＧＡ（Ｆｉｅｌｄ　Ｐｒｏｇｒａｍｍａｂｌｅ　Ｇａｔｅ　Ａｒｒａｙ）や、ＬＳＩ内部の回路セルの接続や設定を再構成可能なリコンフィギュラブル・プロセッサを利用しても良い。

[0410] さらには、半導体技術の進歩又は派生する別技術によりＬＳＩに置き換わる集積回路化の技術が登場すれば、当然、その技術を用いて機能ブロックの集積化を行ってもよい。バイオ技術の適用等が可能性としてありえる。

[0411] （１７）上記実施の形態における認証システムに係る各装置を構成する構成要素の一部または全部は、各装置に脱着可能なＩＣカードまたは単体のモジュールから構成されているとしてもよい。このＩＣカードまたはこのモジュールは、耐タンパ性を有するとしてもよい。

[0412] （１８）本開示は、上記に示す方法であるとしてもよい。また、これらの

方法をコンピュータにより実現するコンピュータプログラムであるとしてもよいし、前記コンピュータプログラムからなるデジタル信号であるとしてもよい。これらのコンピュータプログラムをメモリに記憶し、プロセッサにより実行するとしてもよい。

[0413] また、本開示は、前記コンピュータプログラムまたは前記デジタル信号をコンピュータ可読記録媒体、例えば、フレキシブルディスク、ハードディスク、ＣＤ－ＲＯＭ、ＭＯ、ＤＶＤ、ＤＶＤ－ＲＯＭ、ＤＶＤ－ＲＡＭ、ＢＤ（Ｂｌｕ－ｒａｙ（登録商標）　Ｄｉｓｃ）、半導体メモリなどに記録したものとしてもよい。また、これらの記録媒体に記録されている前記デジタル信号であるとしてもよい。

[0414] また、本開示は、前記コンピュータプログラムまたは前記デジタル信号を、電気通信回線、無線または有線通信回線、インターネットを代表とするネットワーク、データ放送等を経由して伝送するものとしてもよい。

[0415] また、本開示は、プロセッサとメモリを備えたコンピュータシステムであって、前記メモリは、上記コンピュータプログラムを記録しており、前記プロセッサは、前記コンピュータプログラムにしたがって動作するとしてもよい。

[0416] また、前記コンピュータプログラムまたは前記デジタル信号を前記記録媒体に記録して移送することにより、または前記コンピュータプログラムまたは前記デジタル信号を前記ネットワーク等を経由して移送することにより、独立した他のコンピュータシステムにより実施するとしてもよい。

[0417] （１９）本開示は、上記各実施の形態及び上記各変形例を部分的に組み合わせるとしてもよい。

[0418] ＜５．補足＞

以下、更に本開示に係る認証方法の一実施形態とその効果について説明する。

[0419] （ａ）本開示に係る認証方法は、コントローラと第１機器と第２機器とがグループ鍵を共有し、前記コントローラが前記第１機器と前記第２機器とに

対して、前記グループ鍵を用いて暗号化した情報の一斉送信を行う認証システムにおける、前記コントローラと前記第１機器及び前記第２機器との認証方法であって、前記コントローラと前記第１機器とが相互認証を実行し、グループ鍵を作成して共有すると共に、前記第１機器を基準機器として設定する第１相互認証ステップと、前記コントローラと前記第２機器とが相互認証を実行し、前記第１相互認証ステップで作成したグループ鍵を前記第２機器にも共有させる第２相互認証ステップと、前記第２相互認証ステップの後に、前記コントローラと前記基準機器である前記第１機器とが再び相互認証を実行し、前記グループ鍵を更新し、更新後のグループ鍵を共有する第３相互認証ステップと、前記コントローラと前記基準機器とが前記グループ鍵を更新するグループ鍵更新タイミングにおいて、前記コントローラと前記基準機器ではない前記第２機器とが相互認証を実行し、前記更新後のグループ鍵を前記第２機器にも共有させる第４相互認証ステップとを含むことを特徴とする。

[0420] これにより、コントローラに接続する機器の中から基準機器を設定し、当該基準機器におけるグループ鍵更新のタイミングに基づき、他の機器がグループ鍵の更新を行うことで、複数の機器間におけるグループ鍵更新のタイミングを合わせることが可能となり、コントローラと各機器とが相互認証及びグループ鍵更新を行っても、コントローラは暗号化した情報の一斉送信を行うことができる。

[0421] （ｂ）上記（ａ）に係る認証方法において、前記コントローラと前記第１機器と前記第２機器とは、１つのホームエリアネットワークに接続することとしてもよい。

[0422] これにより、ホームエリアネットワークに接続するコントローラとそれぞれの機器とのグループ鍵更新タイミングを合わせることが可能となり、コントローラと各機器とが相互認証及びグループ鍵更新を行っても、コントローラは暗号化した情報の一斉送信を行うことができる。

[0423] （ｃ）上記（ａ）に係る認証方法において、更に、前記コントローラは、

前記基準機器である前記第１機器と前記グループ鍵を更新して共有すると、当該更新後のグループ鍵を共有していない前記第２機器に対して、グループ鍵更新通知を送信するグループ鍵更新通知ステップを含み、前記グループ鍵更新タイミングは、前記第２機器が、前記グループ鍵更新通知を受信するタイミングであることとしてもよい。

[0424] これにより、コントローラと基準機器との間でグループ鍵を更新して以降において、当該更新後のグループ鍵を共有していない機器が、コントローラからグループ鍵更新通知を受信しグループ鍵を更新することで、コントローラに接続する複数機器のグループ鍵更新タイミングを合わせることができる。

[0425] （ｄ）上記（ａ）に係る認証方法において、前記第１相互認証ステップにおいて、更に、前記コントローラと前記第１機器とは第１セッション期間を設定し、前記第２相互認証ステップにおいて、更に、前記コントローラと前記第２機器とは、前記第１セッション期間と前記第１セッション期間設定時点からの経過期間とに基づく第２セッション期間を設定し、前記コントローラと前記第１機器とは、前記第１セッション期間設定時点からの経過期間と前記第１セッション期間とに基づき、前記第３相互認証ステップを開始し、前記グループ鍵更新タイミングは、前記第２セッション期間設定時点からの経過期間と前記第２セッション期間とに基づくタイミングであることとしてもよい。

[0426] これにより、コントローラと基準機器以外の機器との間のセッション期間は、コントローラと基準機器との間のセッション残り期間に基づき設定され、コントローラと接続する各機器とが当該セッション期間に基づきグループ鍵更新を行うことで、コントローラと接続する複数機器のグループ鍵更新タイミングを合わせることができる。

[0427] （ｅ）上記（ａ）に係る認証方法において、前記コントローラは、コントローラ自身の秘密鍵と公開鍵証明書とを所有し、前記第１機器は、第１機器自身の秘密鍵と公開鍵証明書とを所有し、更に、前記コントローラと前記第

１機器とが、第１共有鍵を作成して共有する第１共有鍵共有ステップを含み、前記第１相互認証ステップにおける相互認証は、公開鍵基盤に基づき、互いの所有する前記公開鍵証明書を用いて相互認証を行う公開鍵認証であり、前記第３相互認証ステップにおける相互認証は、前記第１共有鍵を用いて相互認証を行う共有鍵認証であることとしてもよい。

[0428] ここでは、例えば、コントローラと機器とが接続する際には、ＰＫＩに基づく公開鍵証明書を用いた相互認証を行う一方で、以降のセッション更新処理時には、共有鍵を用いた相互認証を行う。一般にＰＫＩに基づく相互認証に比較すると、共有鍵を用いた相互認証は処理にかかる負荷が低いことから、共有鍵を用いた手続を採用することにより、相互認証に係る処理の負荷を軽減することができる。

[0429] （ｆ）上記（ｅ）に係る認証方法において、前記第１共有鍵共有ステップは、前記コントローラと前記第１機器とが鍵交換により第１共有鍵を共有し、前記共有鍵認証は、前記コントローラと前記第１機器とが、互いに作成した乱数と前記第１共有鍵とを用いて行うチャレンジレスポンス認証により相互認証することとしてもよい。

[0430] これにより、コントローラと機器とは共有鍵と乱数とを用いたチャレンジレスポンス認証により、互いの正当性を確認することができる。

[0431] （ｇ）上記（ｅ）に係る認証方法において、前記第２機器は、第２機器自身の秘密鍵と公開鍵証明書とを所有し、更に、前記コントローラと前記第２機器とが、第２共有鍵を作成して共有する第２共有鍵共有ステップを含み、前記第２相互認証ステップにおける相互認証は、公開鍵基盤に基づき、互いの所有する前記公開鍵証明書を用いて相互認証を行う公開鍵認証であり、前記第４相互認証ステップにおける相互認証は、前記第２共有鍵を用いて相互認証を行う共有鍵認証であることとしてもよい。

[0432] これにより、コントローラは、コントローラと接続する全ての機器と、ＰＫＩに基づく相互認証と、共有鍵を用いる相互認証との２種類の手続きを組み合わせて行うことで、相互認証に係る処理の負荷を軽減することができる

。

[0433] （ｈ）本開示に係る認証システムは、コントローラと第１機器と第２機器とがグループ鍵を共有し、前記コントローラが前記第１機器と前記第２機器とに対して、前記グループ鍵を用いて暗号化した情報の一斉送信を行う認証システムであって、前記コントローラと前記第１機器とが相互認証を実行し、グループ鍵を作成して共有すると共に、前記第１機器を基準機器として設定する第１相互認証手段と、前記コントローラと前記第２機器とが相互認証を実行し、前記第１相互認証ステップで作成したグループ鍵を、前記第２機器にも共有させる第２相互認証手段と、前記第２相互認証ステップの後に、前記コントローラと前記基準機器である前記第１機器とが再び相互認証を実行し、前記グループ鍵を更新し、更新後のグループ鍵を共有する第３相互認証手段と、前記コントローラと前記基準機器とが前記グループ鍵を更新するグループ鍵更新タイミングにおいて、前記コントローラと前記基準機器ではない前記第２機器とに相互認証を実行させ、前記更新後のグループ鍵を、前記第２の機器にも共有させる第４相互認証手段とを備えることを特徴とする

。

[0434] これにより、コントローラに接続する機器の中から基準機器を設定し、当該基準機器におけるグループ鍵更新のタイミングに基づき、他の機器がグループ鍵の更新を行うことで、複数の機器間におけるグループ鍵更新のタイミングを合わせることが可能となり、コントローラと各機器とが相互認証及びグループ鍵更新を行っても、コントローラは暗号化した情報の一斉送信を行うことができる。

産業上の利用可能性

[0435] 本開示に係る認証方法は、コントローラが接続する複数機器に対してグループ鍵を用いて暗号化した情報の一斉送信を行うネットワークシステムにおいて、コントローラと各機器との相互認証及びグループ鍵更新等に活用することができる。

符号の説明

[0436] １０　認証システム

１００　コントローラ

１０１　機器管理部

１０２　機器情報保持部

１０３　認証処理部

１０４　認証情報保持部

１０５　通信部

２００ａ，２００ｂ，２００ｃ　機器

２０１　機器管理部

２０２　機器履歴保持部

２０３　機器情報保持部

２０４　認証処理部

２０５　認証情報保持部

２０６　通信部

３００　サーバ

３０１　機器情報管理部

３０２　機器情報保持部

３０３　ＣＲＬ管理部

３０４　ＣＲＬ保持部

３０５　通信部

４００　ホームエリアネットワーク

５００　ネットワーク

１０００　接続機器管理テーブル

１１００　接続コントローラ管理テーブル

１３００　機器情報管理テーブル

２０００　接続機器管理テーブル

３０００　接続機器管理テーブル

３１００　接続コントローラ管理テーブル

請求の範囲

[請求項1] コントローラと第１機器と第２機器とがグループ鍵を共有し、前記コントローラが前記第１機器と前記第２機器とに対して、前記グループ鍵を用いて暗号化した情報の一斉同報通信を行う認証システムにおける、前記コントローラと前記第１機器及び前記第２機器との認証方法であって、

前記コントローラと前記第１機器とが相互認証を実行し、グループ鍵を作成して共有すると共に、前記第１機器を基準機器として設定する第１相互認証ステップと、

前記コントローラと前記第２機器とが相互認証を実行し、前記第１相互認証ステップで作成したグループ鍵を前記第２機器にも共有させる第２相互認証ステップと、

前記第２相互認証ステップの後に、前記コントローラと前記基準機器である前記第１機器とが再び相互認証を実行し、前記グループ鍵を更新し、更新後のグループ鍵を共有する第３相互認証ステップと、

前記コントローラと前記基準機器とが前記グループ鍵を更新するグループ鍵更新タイミングにおいて、前記コントローラと前記基準機器ではない前記第２機器とが相互認証を実行し、前記更新後のグループ鍵を前記第２機器にも共有させる第４相互認証ステップと、

前記グループ鍵を用いて送信データを暗号化して暗号化データを生成し、当該送信データと、ヘッダと、送信元アドレスと、送信先アドレスとからＭＡＣを生成し、当該暗号化データと、当該ヘッダと、当該送信元アドレスと、当該送信先アドレスと、当該ＭＡＣとを含むメッセージの前記一斉同報通信を行う暗号化ステップとを含む

ことを特徴とする認証方法。

[請求項2] 前記第１機器と前記第２機器とのうちの少なくとも１つの機器が、前記コントローラから前記メッセージを受信し、当該メッセージに含まれる前記暗号化データを復号し、当該メッセージに含まれるＭＡＣ

を検証する復号化ステップを更に含む

ことを特徴とする請求項１記載の認証方法。

[請求項3] 前記暗号化ステップは、

前記送信データが複数ある場合には、当該複数の送信データそれぞれについて、前記ヘッダに所定のフラグを付与して、前記暗号化データの生成と、前記ＭＡＣの生成と、前記一斉同報通信とを行い、

前記復号化ステップは、

前記ヘッダに前記所定のフラグが付与されたメッセージを複数受信する場合において、当該複数のメッセージのうちの一のメッセージに対する前記ＭＡＣの検証に成功しなかったとき、当該複数のメッセージの中に未だ前記暗号化データの復号が実行されていないメッセージが存在すれば、当該復号が実行されていないメッセージに対する前記復号の実行を抑制する

ことを特徴とする請求項２記載の認証方法。

[請求項4] 前記送信データは、前記第１機器と前記第２機器とのうちの少なくとも１つの機器に対する制御コマンド、又は、前記第１機器と前記第２機器とのうちの少なくとも１つの機器に対する通知のいずれかである

ことを特徴とする請求項１記載の認証方法。

[請求項5] 前記グループ鍵を用いて前記第１機器と前記第２機器とのうちの少なくとも１つの機器についての履歴情報を暗号化して履歴情報暗号化データを生成し、当該履歴情報暗号化データと、ヘッダと、送信元アドレスと、送信先アドレスとからＭＡＣを生成し、当該ＭＡＣと当該履歴情報暗号化データとを含めて暗号化した履歴情報を生成し、当該ヘッダと、当該送信元アドレスと、当該送信先アドレスとを利用して、当該暗号化した履歴情報を、当該１つの機器から前記コントローラへ送信する履歴情報暗号化ステップを更に含む

ことを特徴とする請求項１記載の認証方法。

[請求項6] 前記暗号化ステップは、前記暗号化データの生成と、前記ＭＡＣの生成とを、ＡＥＳ－ＣＣＭの認証付暗号化法を利用して行う

ことを特徴とする請求項１記載の認証方法。

[請求項7] コントローラと第１機器と第２機器とがグループ鍵を共有し、前記コントローラが前記第１機器と前記第２機器とに対して、前記グループ鍵を用いて暗号化した情報の一斉同報通信を行う認証システムであって、

前記コントローラと前記第１機器とが相互認証を実行し、グループ鍵を作成して共有すると共に、前記第１機器を基準機器として設定する第１相互認証手段と、

前記コントローラと前記第２機器とが相互認証を実行し、前記第１相互認証手段によって作成されたグループ鍵を前記第２機器にも共有させる第２相互認証手段と、

前記第２相互認証手段による前記共有が行われた後に、前記コントローラと前記基準機器である前記第１機器とが再び相互認証を実行し、グループ鍵を更新し、更新後のグループ鍵を共有する第３相互認証手段と、

前記コントローラと前記基準機器とが前記グループ鍵を更新するグループ鍵更新タイミングにおいて、前記コントローラと前記基準機器ではない前記第２機器とが相互認証を実行し、前記更新後のグループ鍵を前記第２機器にも共有させる第４相互認証手段と、

前記グループ鍵を用いて送信データを暗号化して暗号化データを生成し、当該送信データと、ヘッダと、送信元アドレスと、送信先アドレスとからＭＡＣを生成し、当該暗号化データと、当該ヘッダと、当該送信元アドレスと、当該送信先アドレスと、当該ＭＡＣとを含むメッセージの前記一斉同報通信を行う暗号化手段とを備える

ことを特徴とする認証方法。

[請求項8] グループ鍵を用いて暗号化した情報の一斉同報通信を行う認証シス

テムで利用されるコントローラであって、

第１機器との間で相互認証を実行し、グループ鍵を生成して共有すると共に、前記第１機器を基準機器として設定する第１相互認証手段と、

第２機器との間で相互認証を実行し、前記第１相互認証手段によって生成されたグループ鍵を、前記第２機器とも共有する第２相互認証手段と、

前記第２相互認証手段による前記共有が行われた後に、前記基準機器である前記第１機器との間で再び相互認証を実行し、グループ鍵を更新し、更新後のグループ鍵を前記第１機器と共有する第３相互認証手段と、

前記第３相互認証手段による前記グループ鍵を更新するタイミングにおいて、前記基準機器ではない前記第２機器との間で相互認証を実行し、前記更新後のグループ鍵を、前記第２機器とも共有する第４相互認証手段と、

前記グループ鍵を用いて送信データを暗号化して暗号化データを生成し、当該送信データと、ヘッダと、送信元アドレスと、送信先アドレスとからＭＡＣを生成し、当該暗号化データと、当該ヘッダと、当該送信元アドレスと、当該送信先アドレスと、当該ＭＡＣとを含むメッセージの前記一斉同報通信を行う暗号化手段とを備える

ことを特徴とするコントローラ。

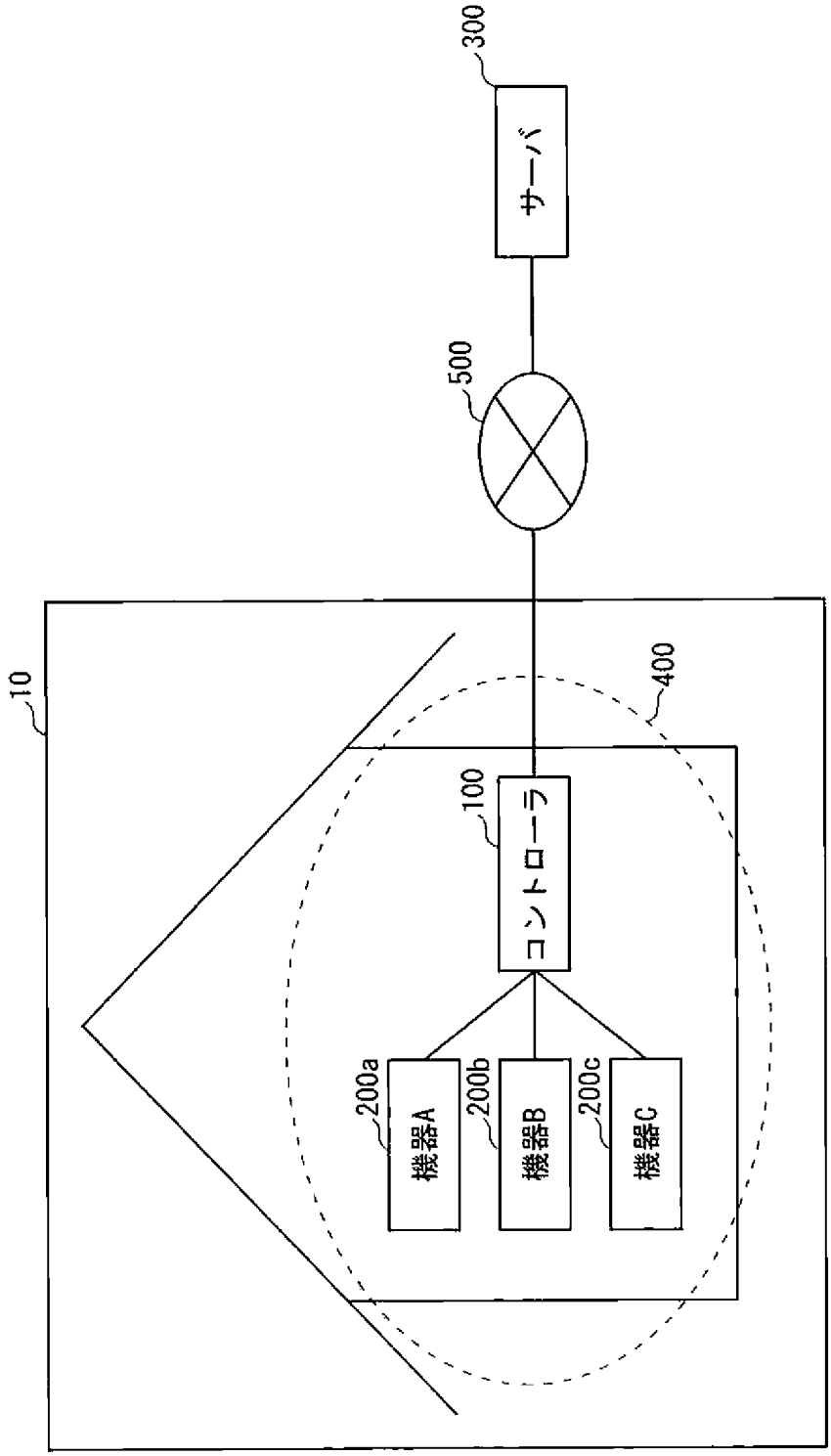
[請求項9] グループ鍵を用いて暗号化した情報の一斉同報通信を行う認証システムで利用される機器であって、

前記認証システムを構成するコントローラから、グループ鍵を用いて送信データを暗号化した暗号化データと、ヘッダと、送信元アドレスと、送信先アドレスと、当該送信データ、当該ヘッダ、当該送信元アドレス、及び当該送信先アドレスから生成されたＭＡＣとを含むメッセージを受信し、当該メッセージに含まれる前記暗号化データを復

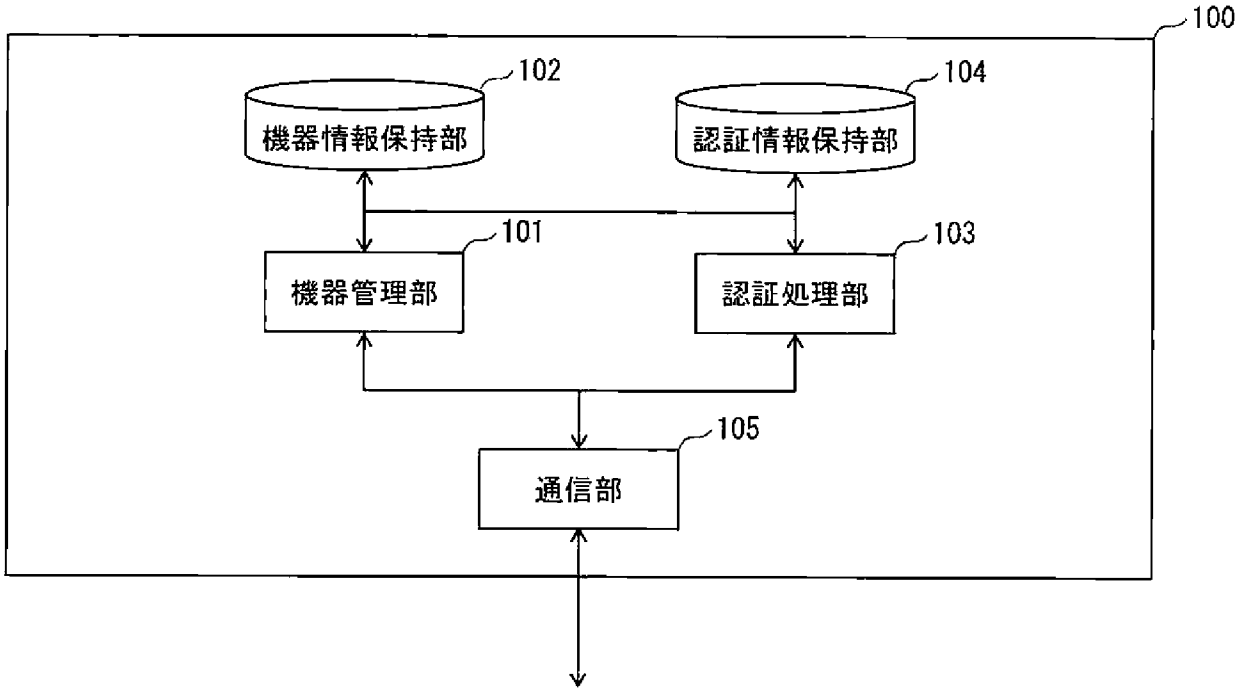
号し、当該メッセージに含まれるＭＡＣを検証する復号化手段を備える

ことを特徴とする機器。

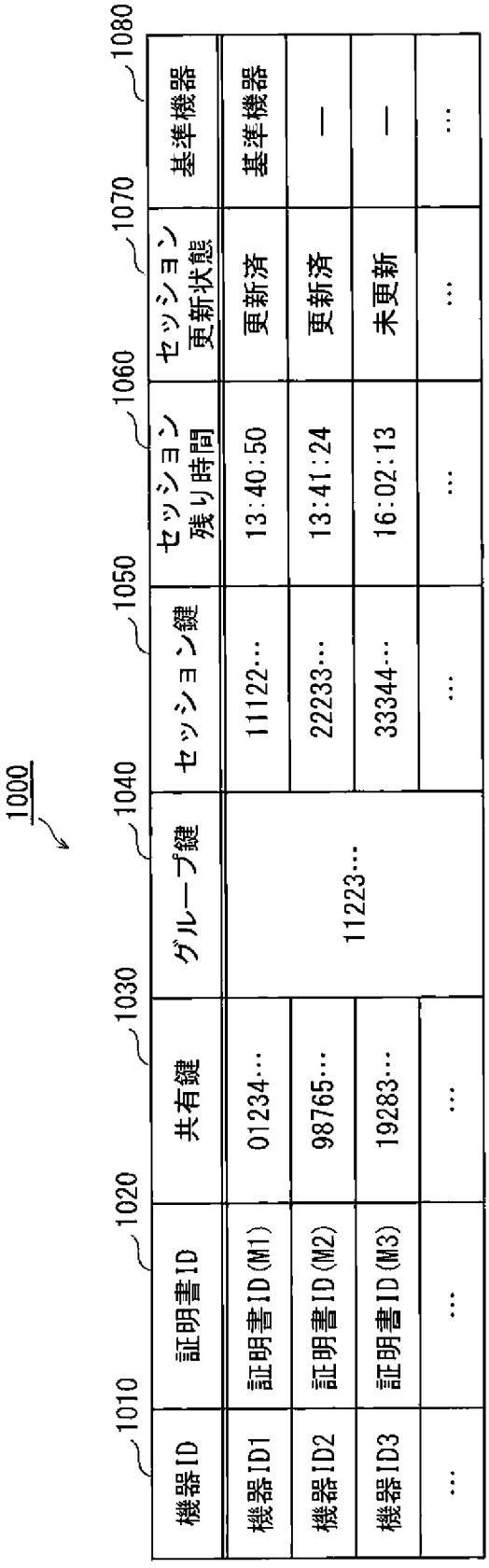
[図1]



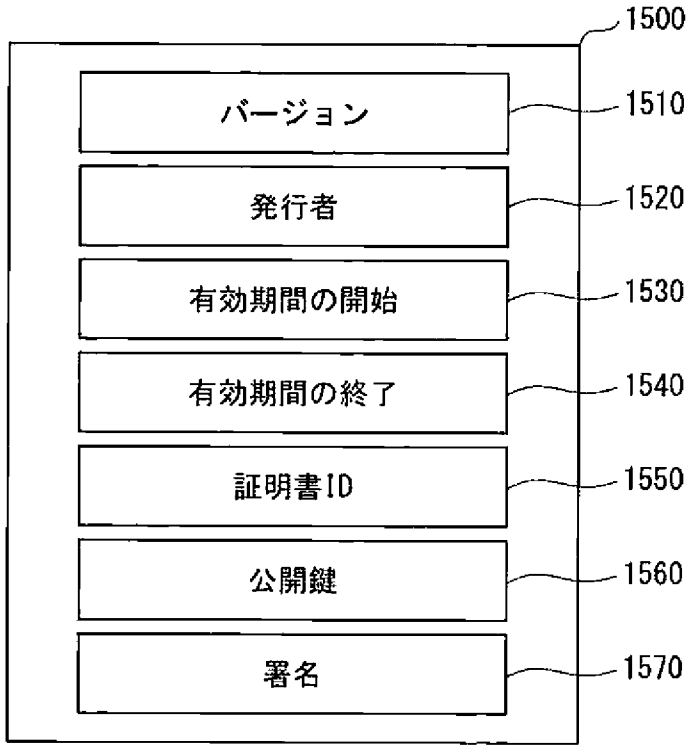
[図2]



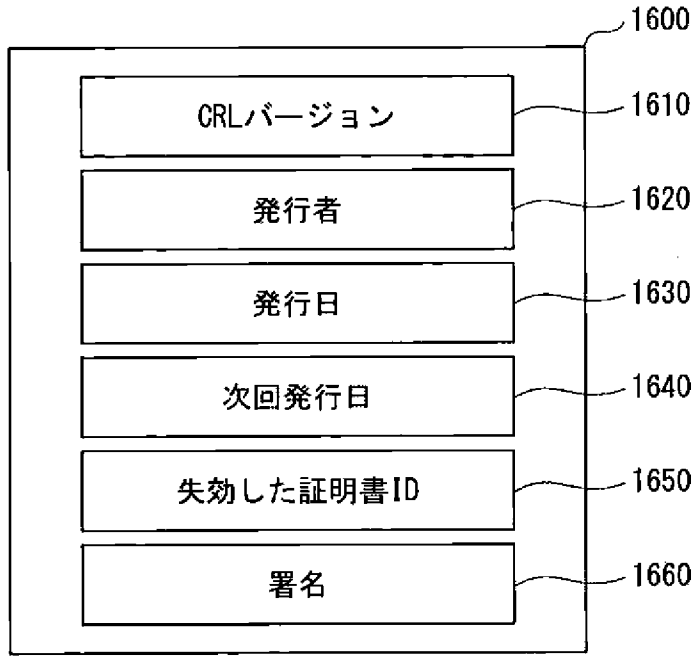
[図3]


1000
1010
機器ID
機器ID1
機器ID2
機器ID3
…
1020
証明書ID
証明書ID(M1)
証明書ID(M2)
証明書ID(M3)
…
1030
共有鍵
01234…
98765…
19283…
…
1040
グループ鍵
11223…
1050
セッション鍵
11122…
22233…
33344…
…
1060
セッション残り時間
13:40:50
13:41:24
16:02:13
…
1070
セッション更新状態
更新済
更新済
未更新
…
1080
基準機器
基準機器
—
—
…

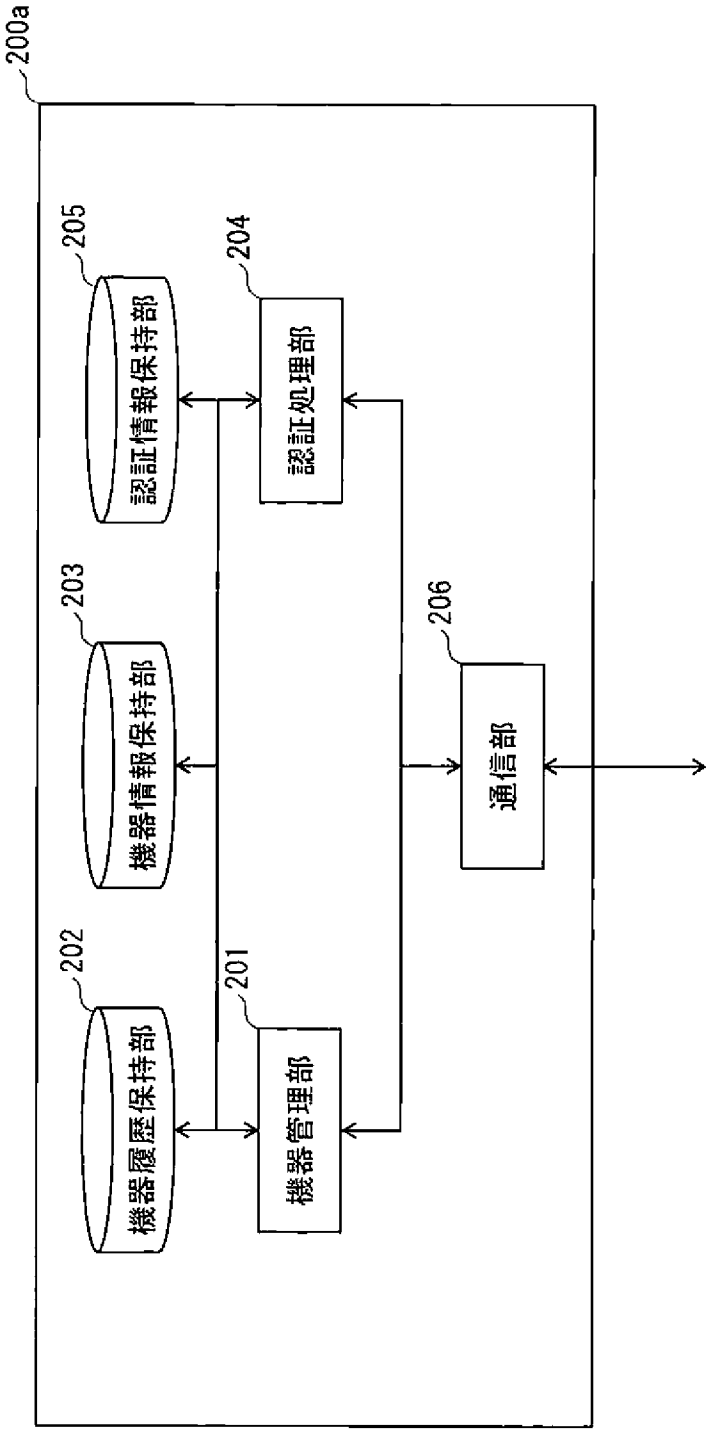
[図4]


1500
バージョン
1510
発行者
1520
有効期間の開始
1530
有効期間の終了
1540
証明書ID
1550
公開鍵
1560
署名
1570

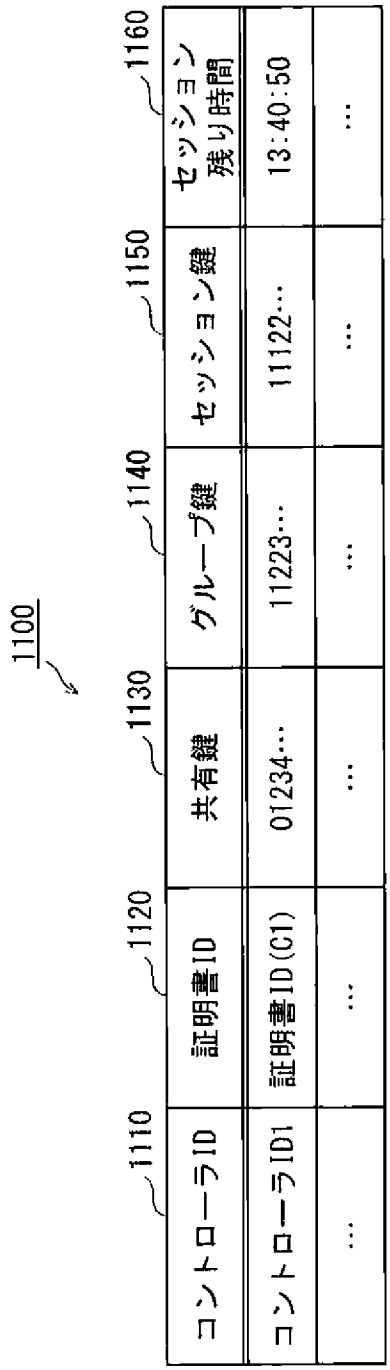
[図5]


1600
CRLバージョン
1610
発行者
1620
発行日
1630
次回発行日
1640
失効した証明書ID
1650
署名
1660

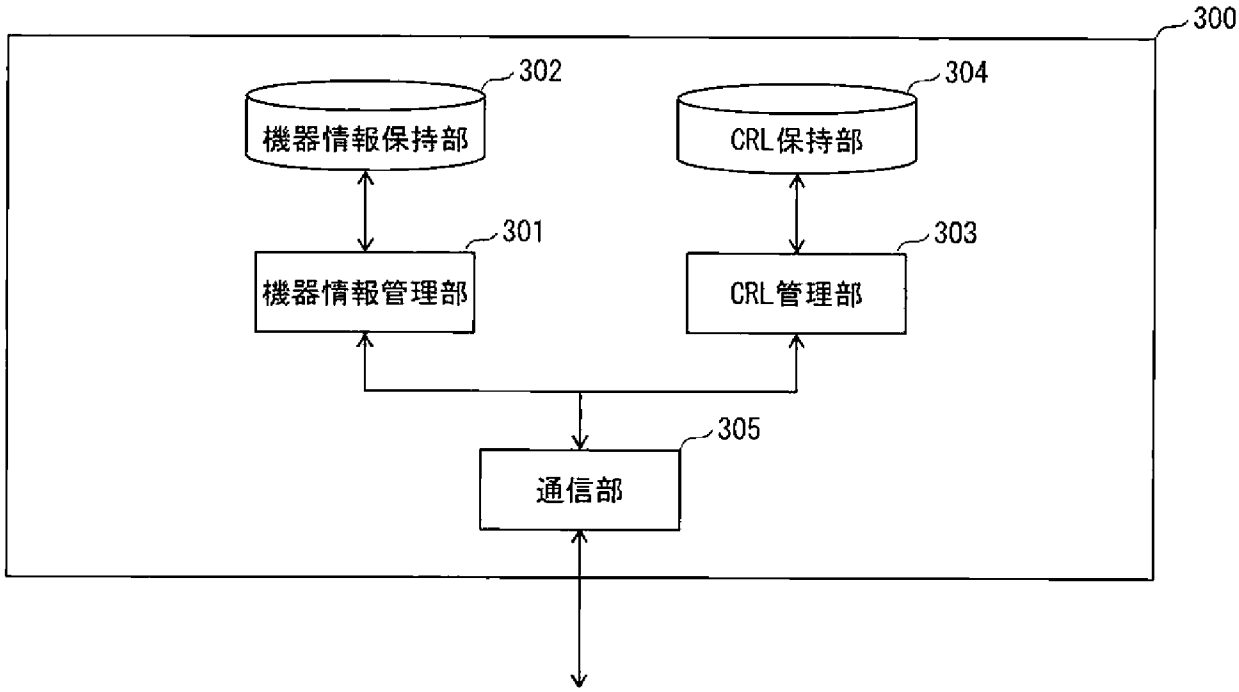
[図6]


200a
205
認証情報保持部
204
認証処理部
203
機器情報保持部
206
通信部
202
機器履歴保持部
201
機器管理部

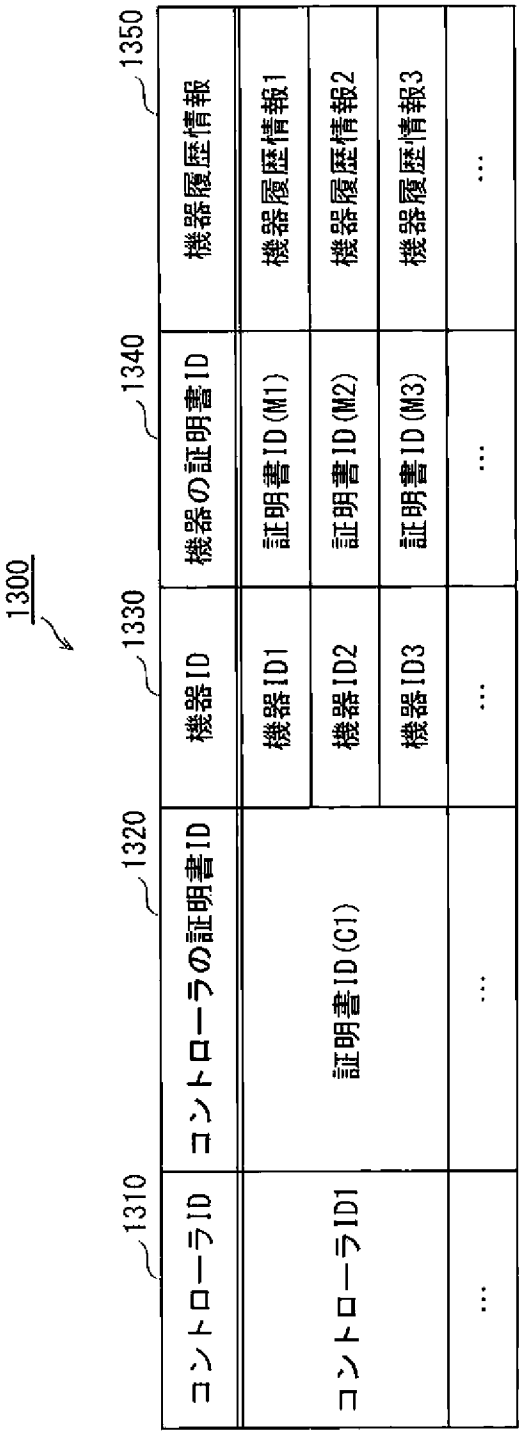
[図7]


1100
1110
コントローラID
コントローラID1
…
1120
証明書ID
証明書ID(C1)
…
1130
共有鍵
01234…
…
1140
グループ鍵
11223…
…
1150
セッション鍵
11122…
…
1160
セッション残り時間
13:40:50
…

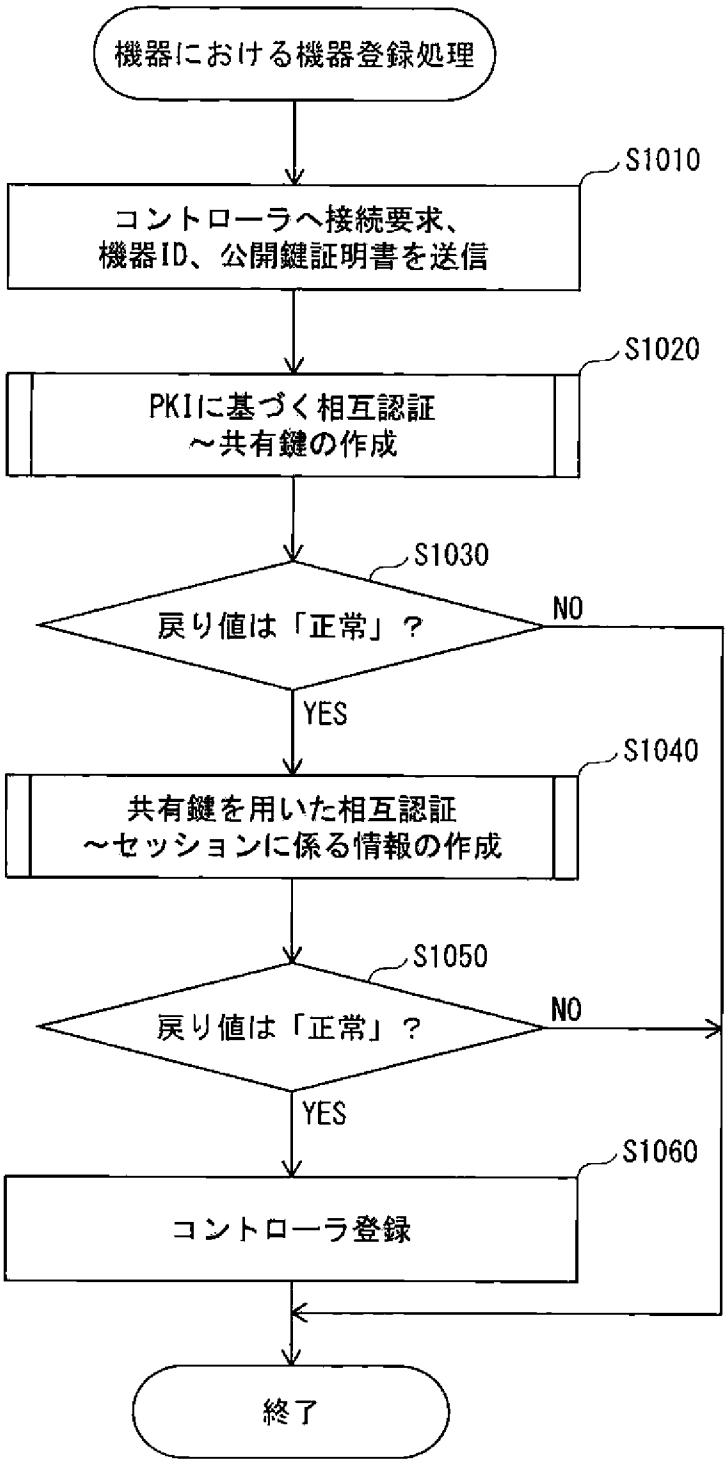
[図8]



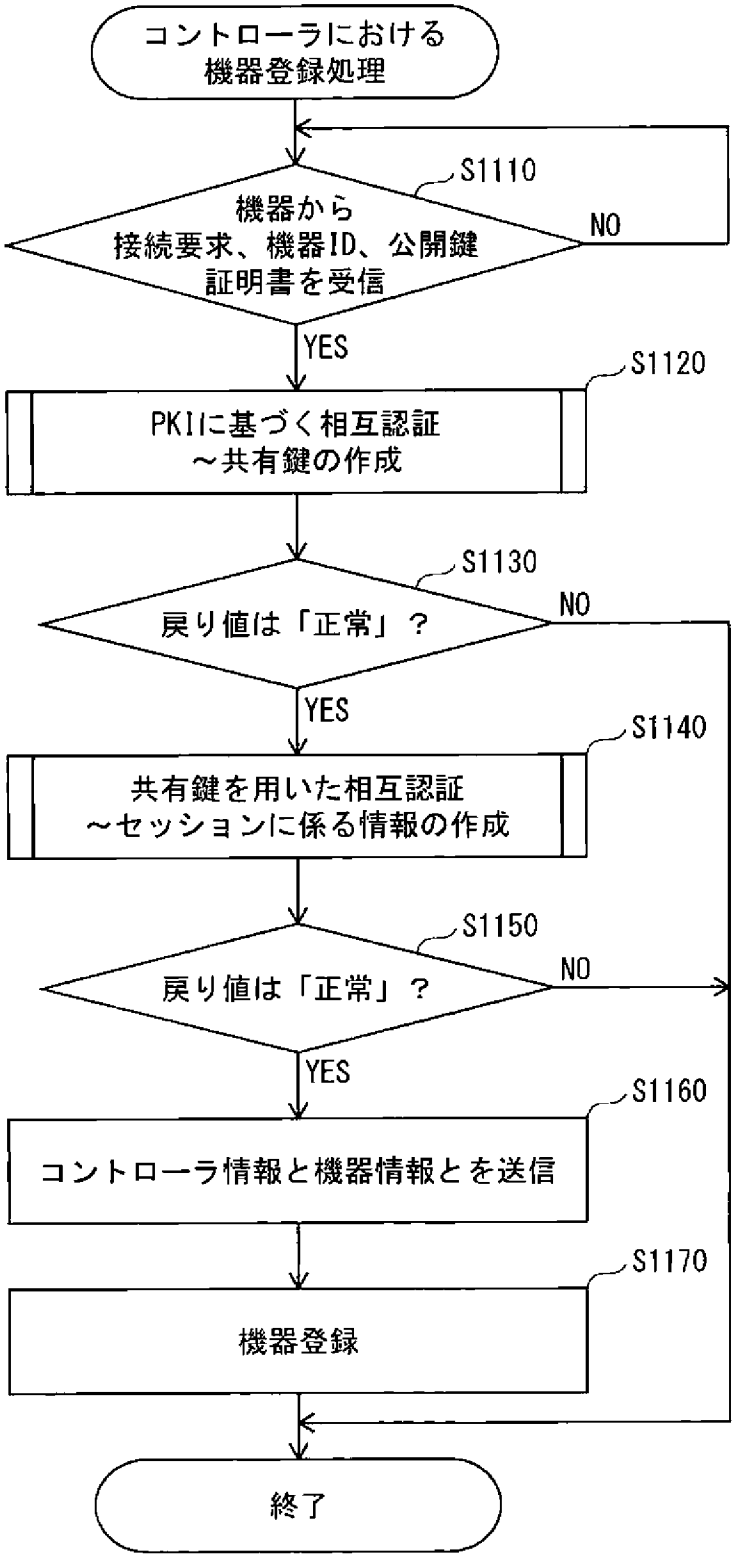
[図9]


1300
1310
1320
1330
1340
1350
コントローラID
コントローラの証明書ID
機器ID
機器の証明書ID
機器履歴情報
コントローラID1
証明書ID(C1)
機器ID1
証明書ID(M1)
機器履歴情報1
機器ID2
証明書ID(M2)
機器履歴情報2
機器ID3
証明書ID(M3)
機器履歴情報3
…
…
…
…
…

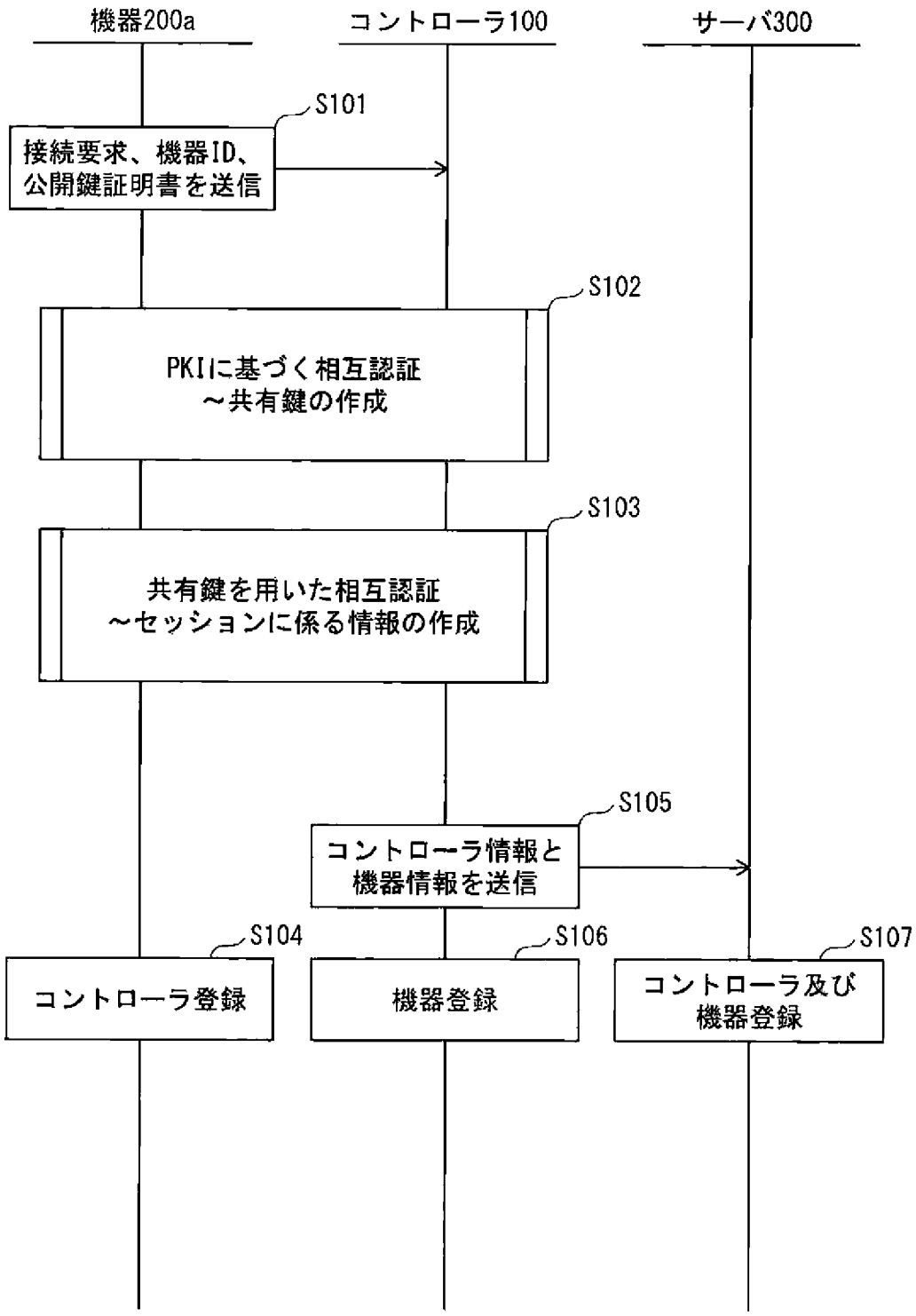
[図10]


機器における機器登録処理
S1010
コントローラへ接続要求、
機器ID、公開鍵証明書を送信
S1020
PKIに基づく相互認証
～共有鍵の作成
S1030
戻り値は「正常」？
NO
YES
S1040
共有鍵を用いた相互認証
～セッションに係る情報の作成
S1050
戻り値は「正常」？
NO
YES
S1060
コントローラ登録
終了

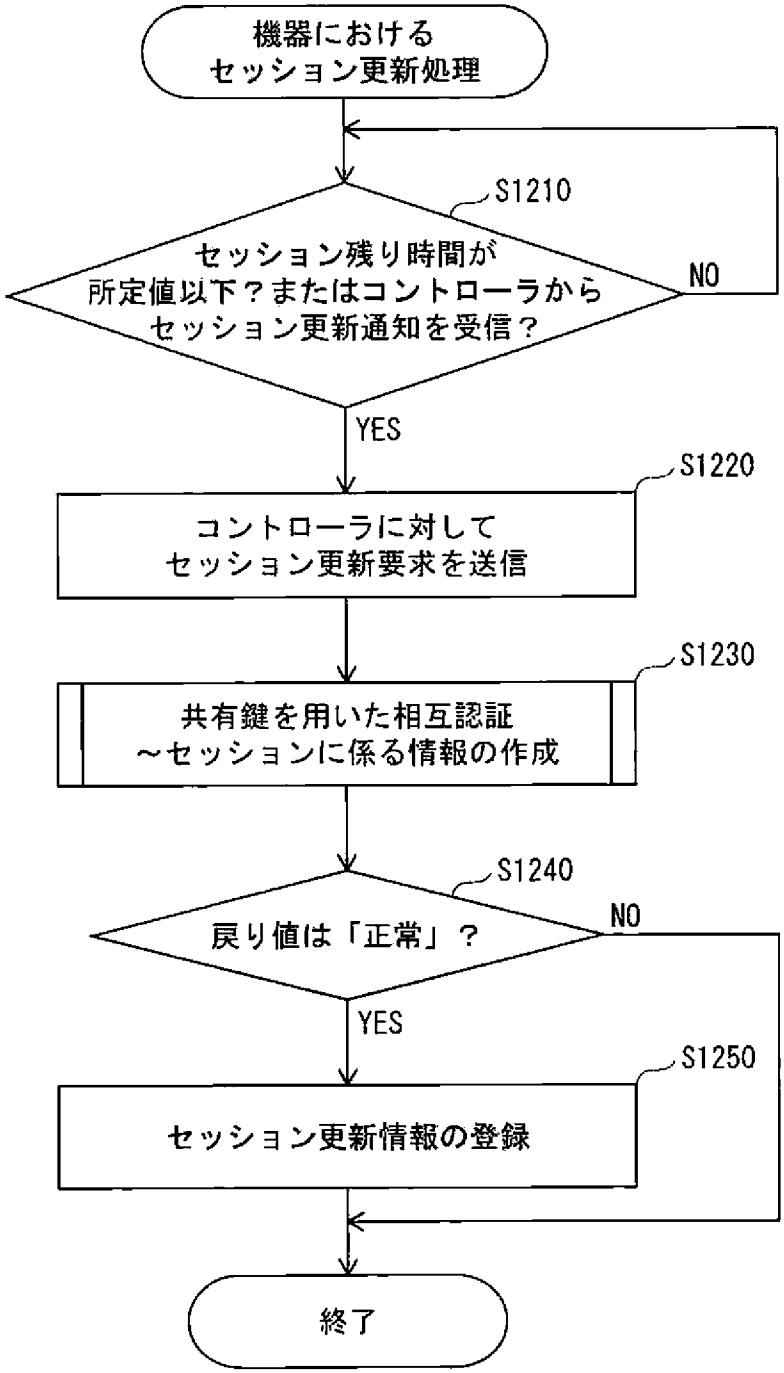
[図11]


コントローラにおける
機器登録処理
S1110
機器から
接続要求、機器ID、公開鍵
証明書を受信
NO
YES
S1120
PKIに基づく相互認証
～共有鍵の作成
S1130
戻り値は「正常」？
NO
YES
S1140
共有鍵を用いた相互認証
～セッションに係る情報の作成
S1150
戻り値は「正常」？
NO
YES
S1160
コントローラ情報と機器情報とを送信
S1170
機器登録
終了

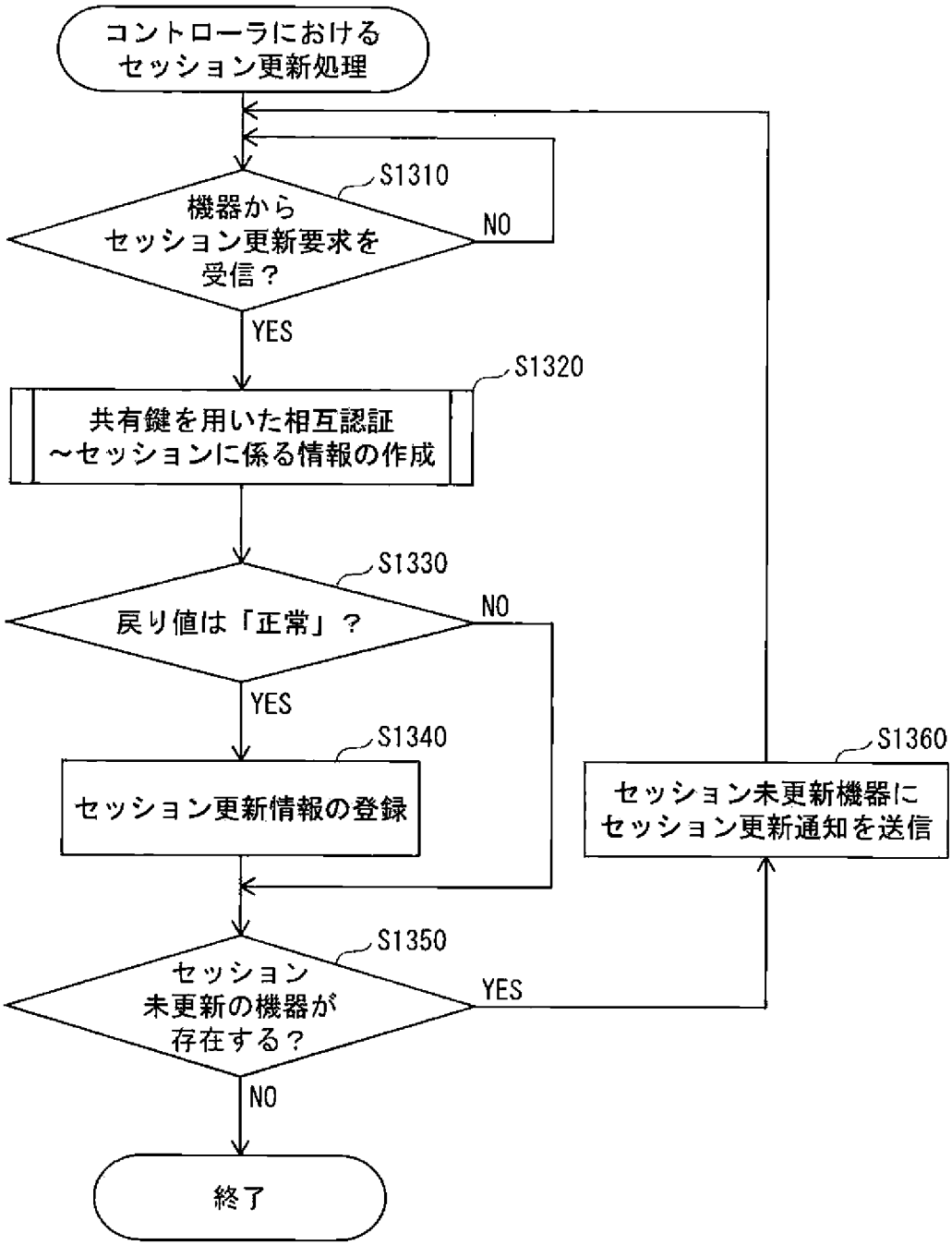
[図12]


機器200a
コントローラ100
サーバ300
S101
接続要求、機器ID、
公開鍵証明書を送信
S102
PKIに基づく相互認証
～共有鍵の作成
S103
共有鍵を用いた相互認証
～セッションに係る情報の作成
S105
コントローラ情報と
機器情報を送信
S104
コントローラ登録
S106
機器登録
S107
コントローラ及び
機器登録

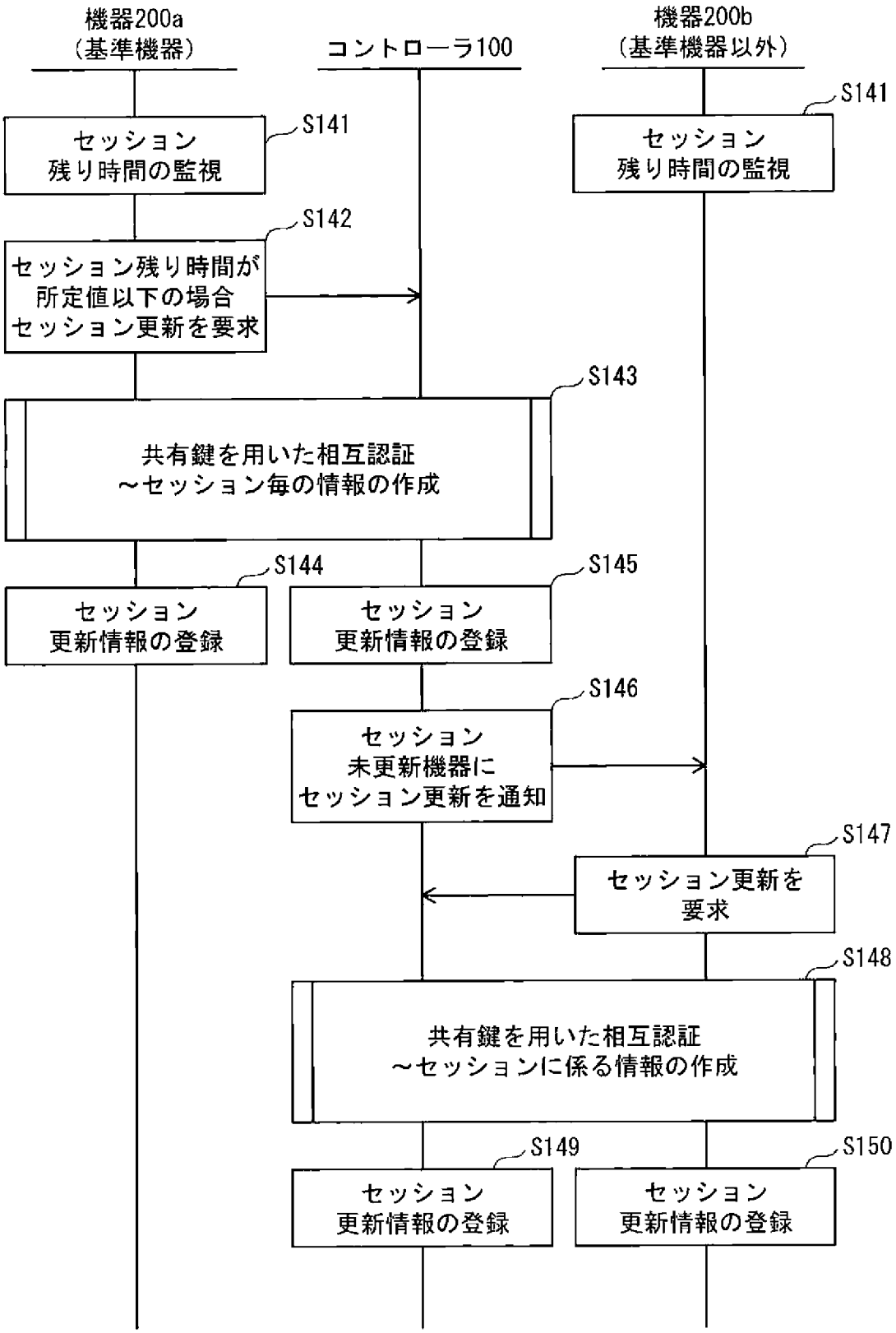
[図13]


機器における
セッション更新処理
S1210
セッション残り時間が
所定値以下？またはコントローラから
セッション更新通知を受信？
NO
YES
S1220
コントローラに対して
セッション更新要求を送信
S1230
共有鍵を用いた相互認証
～セッションに係る情報の作成
S1240
戻り値は「正常」？
NO
YES
S1250
セッション更新情報の登録
終了

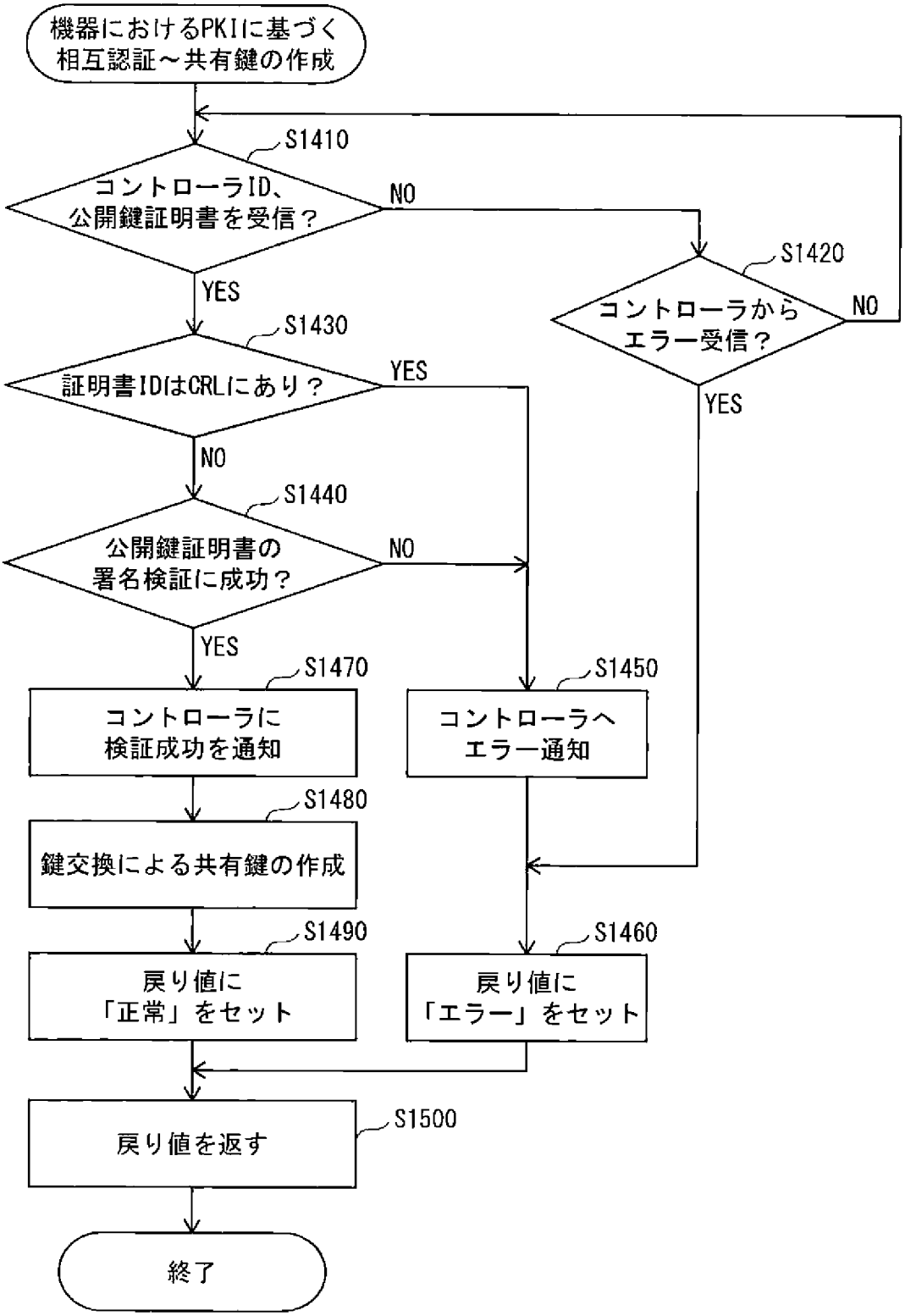
[図14]


コントローラにおける
セッション更新処理
S1310
機器から
セッション更新要求を
受信？
NO
YES
S1320
共有鍵を用いた相互認証
～セッションに係る情報の作成
S1330
戻り値は「正常」？
NO
YES
S1340
セッション更新情報の登録
S1360
セッション未更新機器に
セッション更新通知を送信
S1350
セッション
未更新の機器が
存在する？
YES
NO
終了

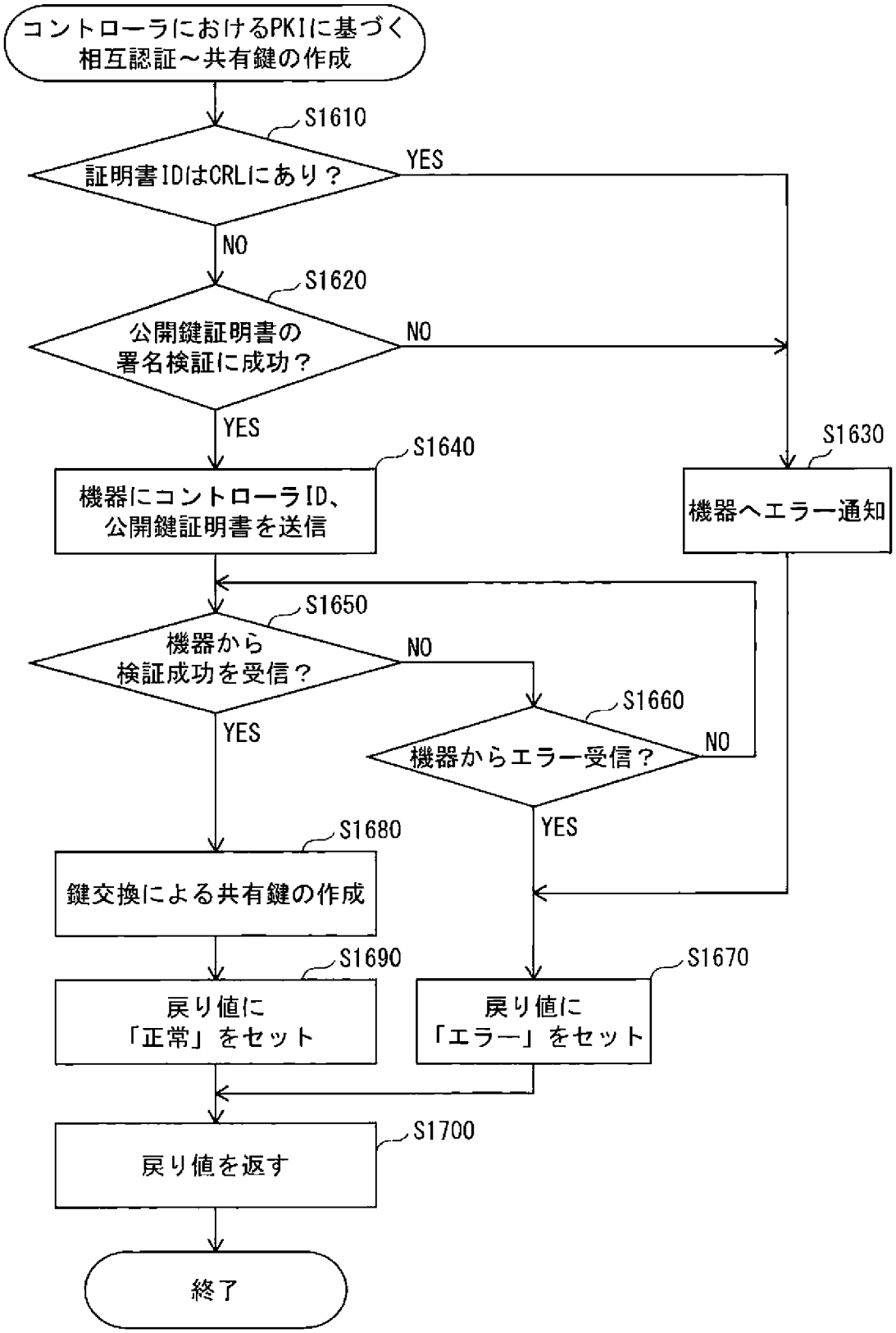
[図15]


機器200a
（基準機器）
コントローラ100
機器200b
（基準機器以外）
S141
セッション
残り時間の監視
S141
セッション
残り時間の監視
S142
セッション残り時間が
所定値以下の場合
セッション更新を要求
S143
共有鍵を用いた相互認証
～セッション毎の情報の作成
S144
セッション
更新情報の登録
S145
セッション
更新情報の登録
S146
セッション
未更新機器に
セッション更新を通知
S147
セッション更新を
要求
S148
共有鍵を用いた相互認証
～セッションに係る情報の作成
S149
セッション
更新情報の登録
S150
セッション
更新情報の登録

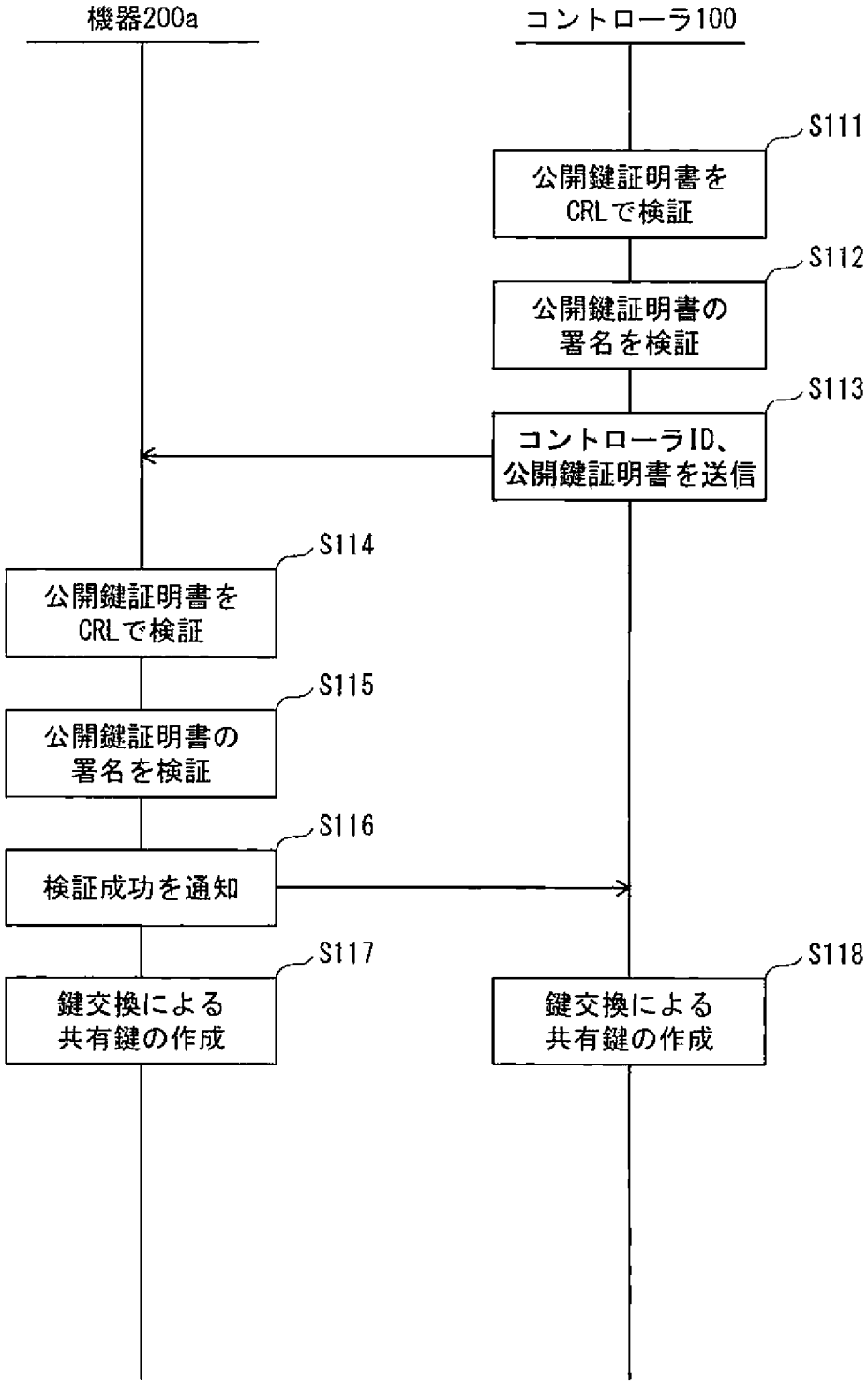
[図16]


機器におけるPKIに基づく
相互認証～共有鍵の作成
S1410
コントローラID、
公開鍵証明書を受信？
NO
YES
S1420
コントローラから
エラー受信？
NO
YES
S1430
証明書IDはCRLにあり？
YES
NO
S1440
公開鍵証明書の
署名検証に成功？
NO
YES
S1470
コントローラに
検証成功を通知
S1450
コントローラへ
エラー通知
S1480
鍵交換による共有鍵の作成
S1490
戻り値に
「正常」をセット
S1460
戻り値に
「エラー」をセット
S1500
戻り値を返す
終了

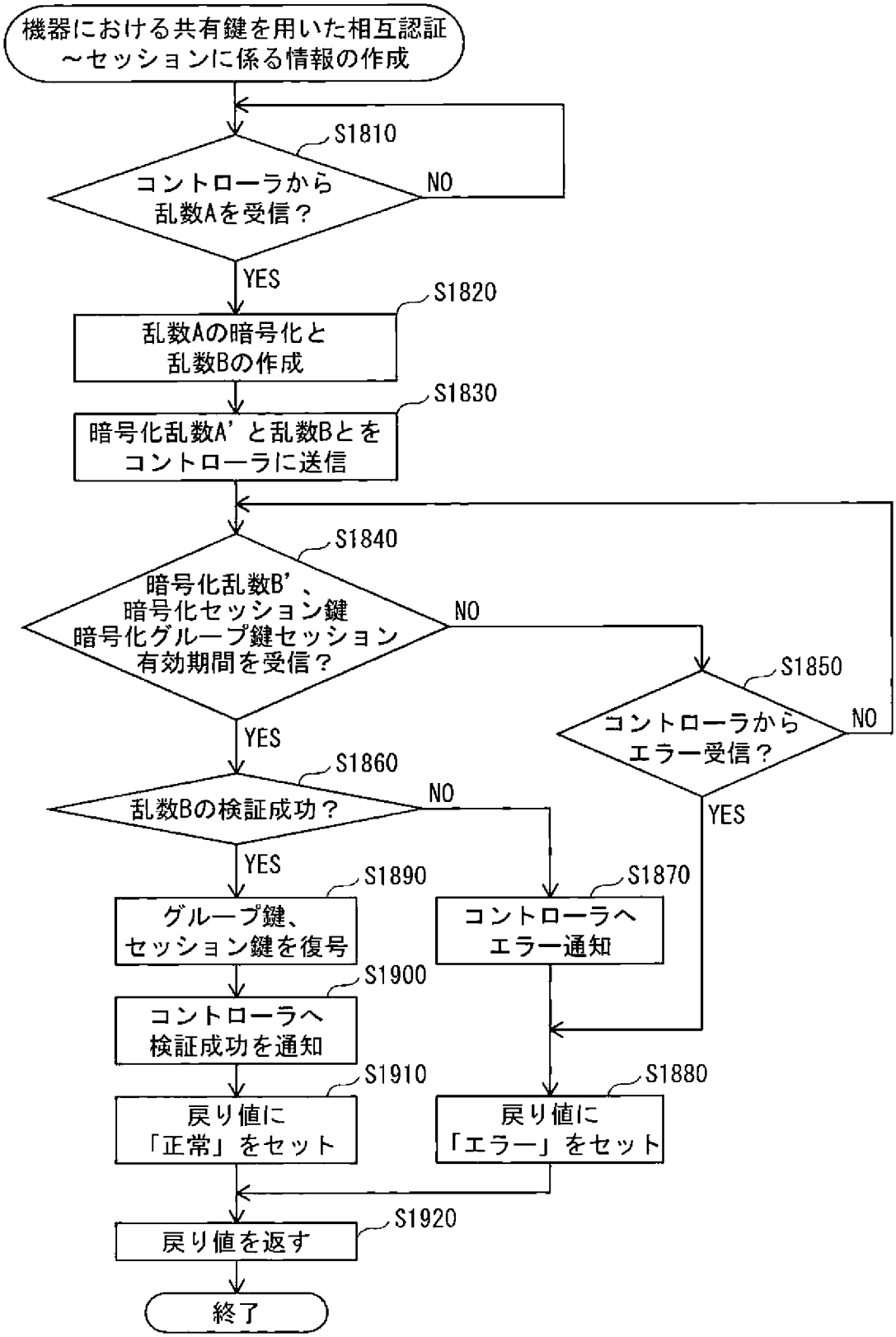
[図17]


コントローラにおけるPKIに基づく
相互認証～共有鍵の作成
S1610
証明書IDはCRLにあり？
YES
NO
S1620
公開鍵証明書の
署名検証に成功？
NO
YES
S1640
機器にコントローラID、
公開鍵証明書を送信
S1630
機器へエラー通知
S1650
機器から
検証成功を受信？
NO
YES
S1660
機器からエラー受信？
NO
YES
S1680
鍵交換による共有鍵の作成
S1690
戻り値に
「正常」をセット
S1670
戻り値に
「エラー」をセット
S1700
戻り値を返す
終了

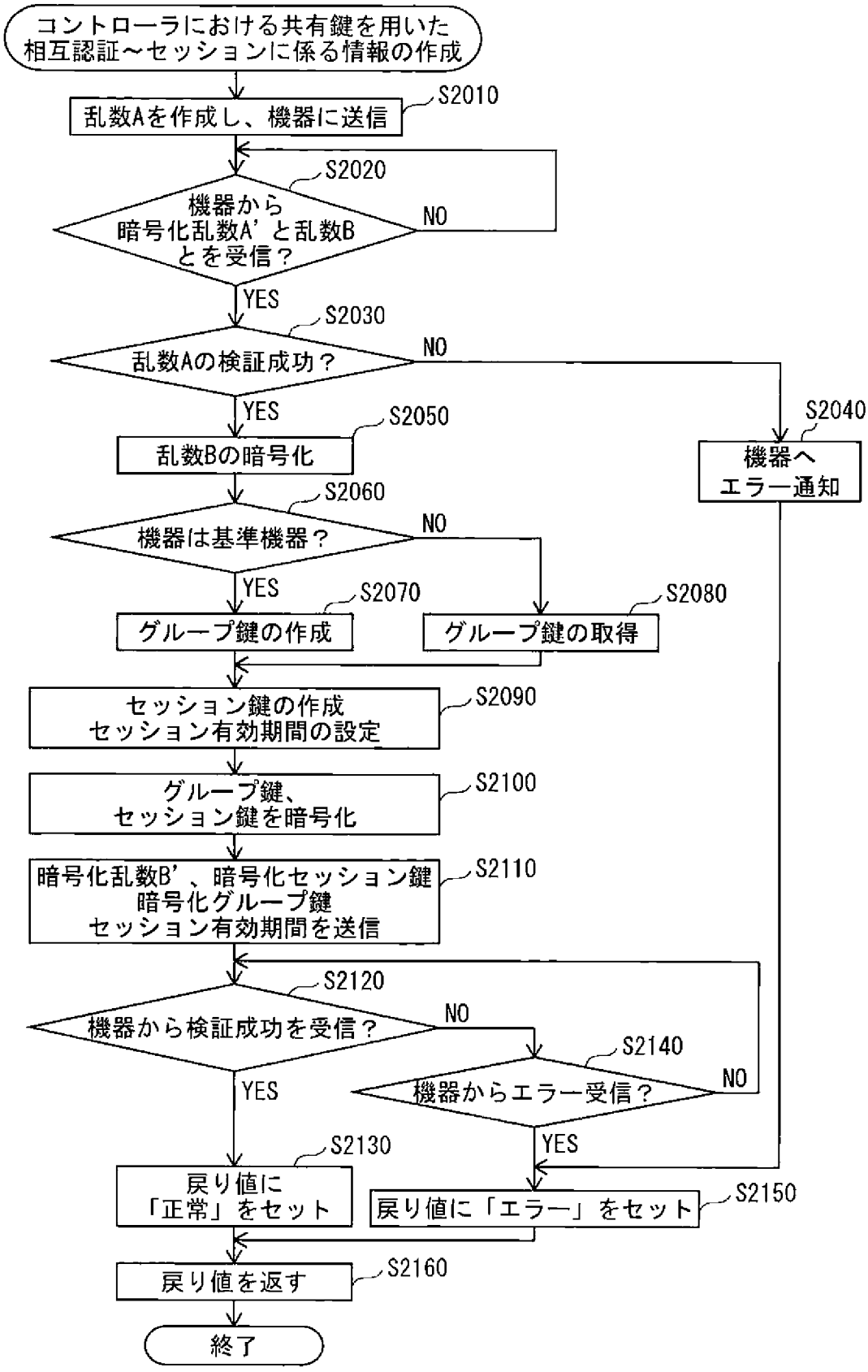
[図18]


機器200a
コントローラ100
S111
公開鍵証明書を
CRLで検証
S112
公開鍵証明書の
署名を検証
S113
コントローラID、
公開鍵証明書を送信
S114
公開鍵証明書を
CRLで検証
S115
公開鍵証明書の
署名を検証
S116
検証成功を通知
S117
鍵交換による
共有鍵の作成
S118
鍵交換による
共有鍵の作成

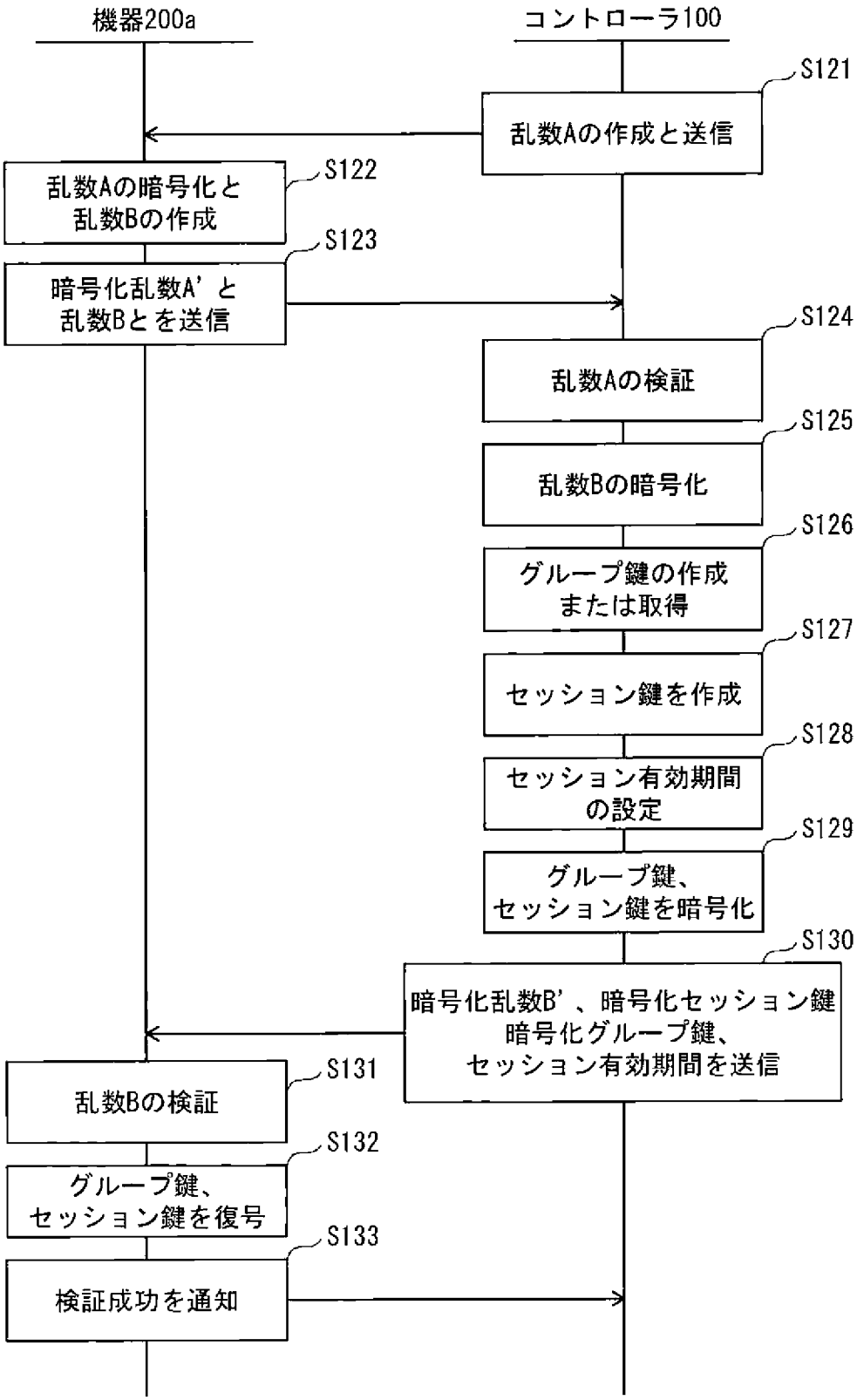
[図19]


機器における共有鍵を用いた相互認証
～セッションに係る情報の作成
S1810
コントローラから
乱数Aを受信？
NO
YES
S1820
乱数Aの暗号化と
乱数Bの作成
S1830
暗号化乱数A'と乱数Bとを
コントローラに送信
S1840
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
有効期間を受信？
NO
YES
S1850
コントローラから
エラー受信？
NO
YES
S1860
乱数Bの検証成功？
NO
YES
S1890
グループ鍵、
セッション鍵を復号
S1870
コントローラへ
エラー通知
S1900
コントローラへ
検証成功を通知
S1910
戻り値に
「正常」をセット
S1880
戻り値に
「エラー」をセット
S1920
戻り値を返す
終了

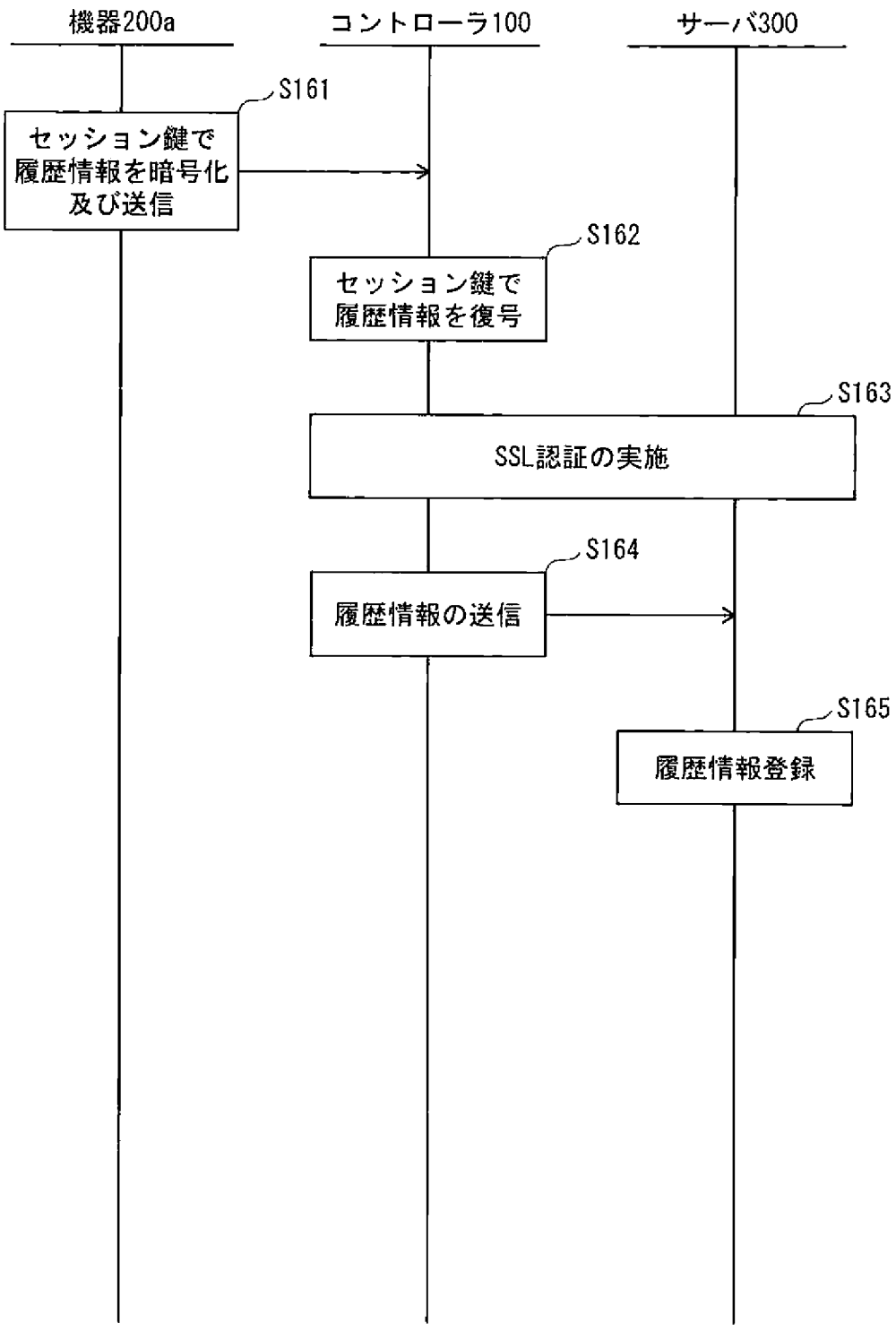
[図20]


コントローラにおける共有鍵を用いた
相互認証～セッションに係る情報の作成
乱数Aを作成し、機器に送信
S2010
機器から
暗号化乱数A'と乱数B
とを受信？
S2020
NO
YES
乱数Aの検証成功？
S2030
NO
YES
乱数Bの暗号化
S2050
機器へ
エラー通知
S2040
機器は基準機器？
S2060
NO
YES
グループ鍵の作成
S2070
グループ鍵の取得
S2080
セッション鍵の作成
セッション有効期間の設定
S2090
グループ鍵、
セッション鍵を暗号化
S2100
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
S2110
機器から検証成功を受信？
S2120
NO
YES
機器からエラー受信？
S2140
NO
YES
戻り値に
「正常」をセット
S2130
戻り値に「エラー」をセット
S2150
戻り値を返す
S2160
終了

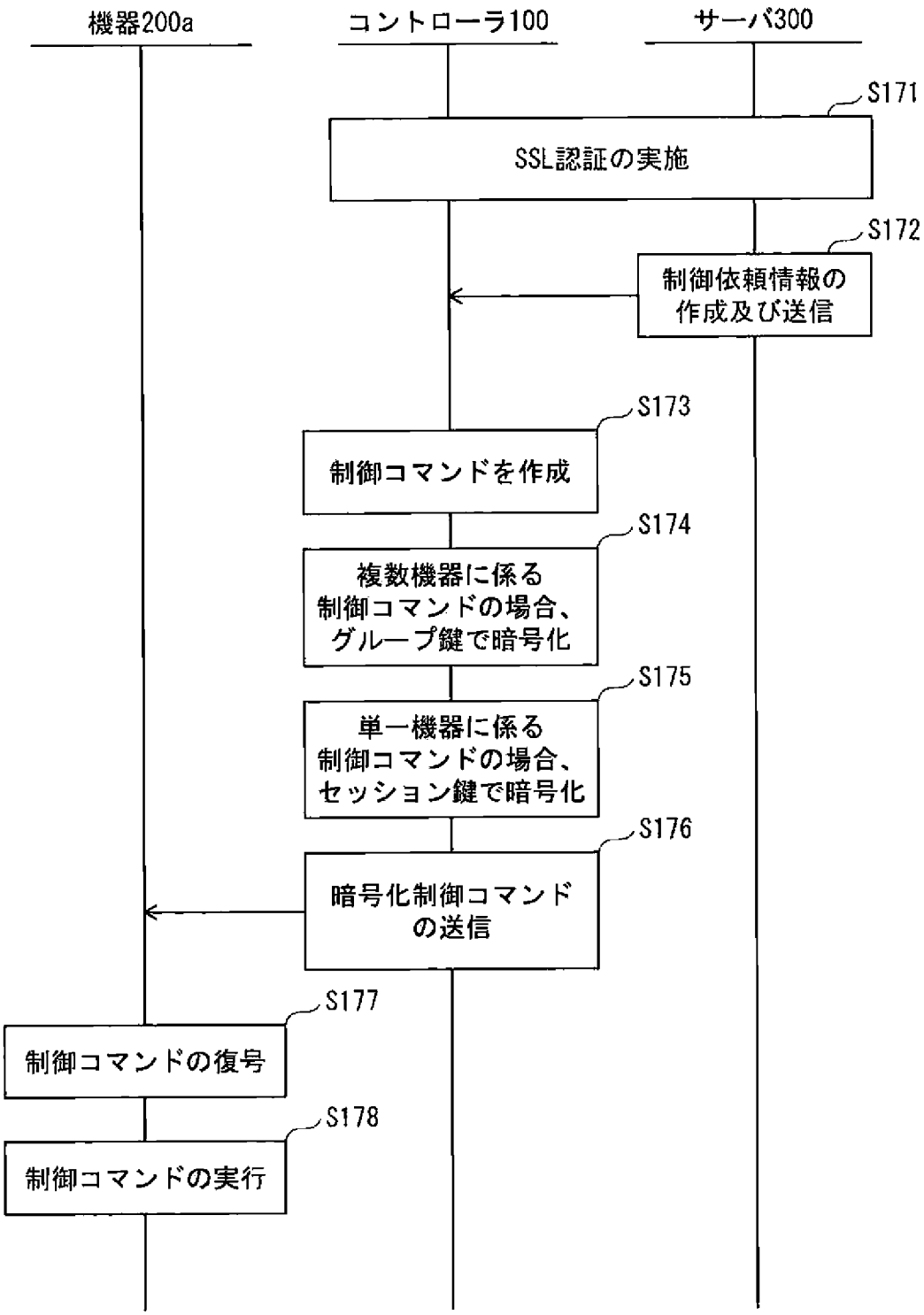
[図21]


機器200a
コントローラ100
S121
乱数Aの作成と送信
乱数Aの暗号化と
乱数Bの作成
S122
S123
暗号化乱数A'と
乱数Bとを送信
S124
乱数Aの検証
S125
乱数Bの暗号化
S126
グループ鍵の作成
または取得
S127
セッション鍵を作成
S128
セッション有効期間
の設定
S129
グループ鍵、
セッション鍵を暗号化
S130
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
乱数Bの検証
S131
S132
グループ鍵、
セッション鍵を復号
S133
検証成功を通知

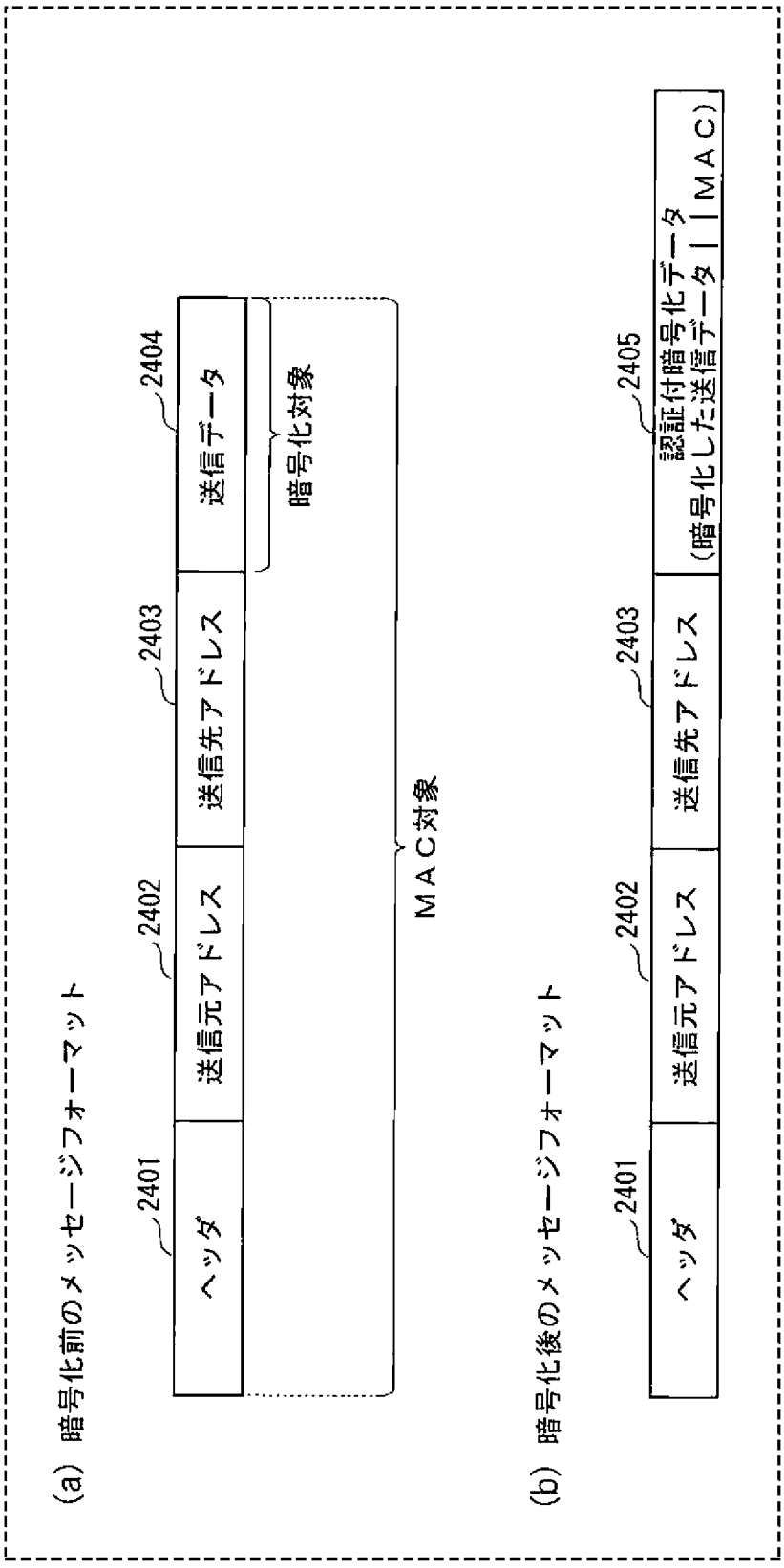
[図22]


機器200a
コントローラ100
サーバ300
S161
セッション鍵で
履歴情報を暗号化
及び送信
S162
セッション鍵で
履歴情報を復号
S163
SSL認証の実施
S164
履歴情報の送信
S165
履歴情報登録

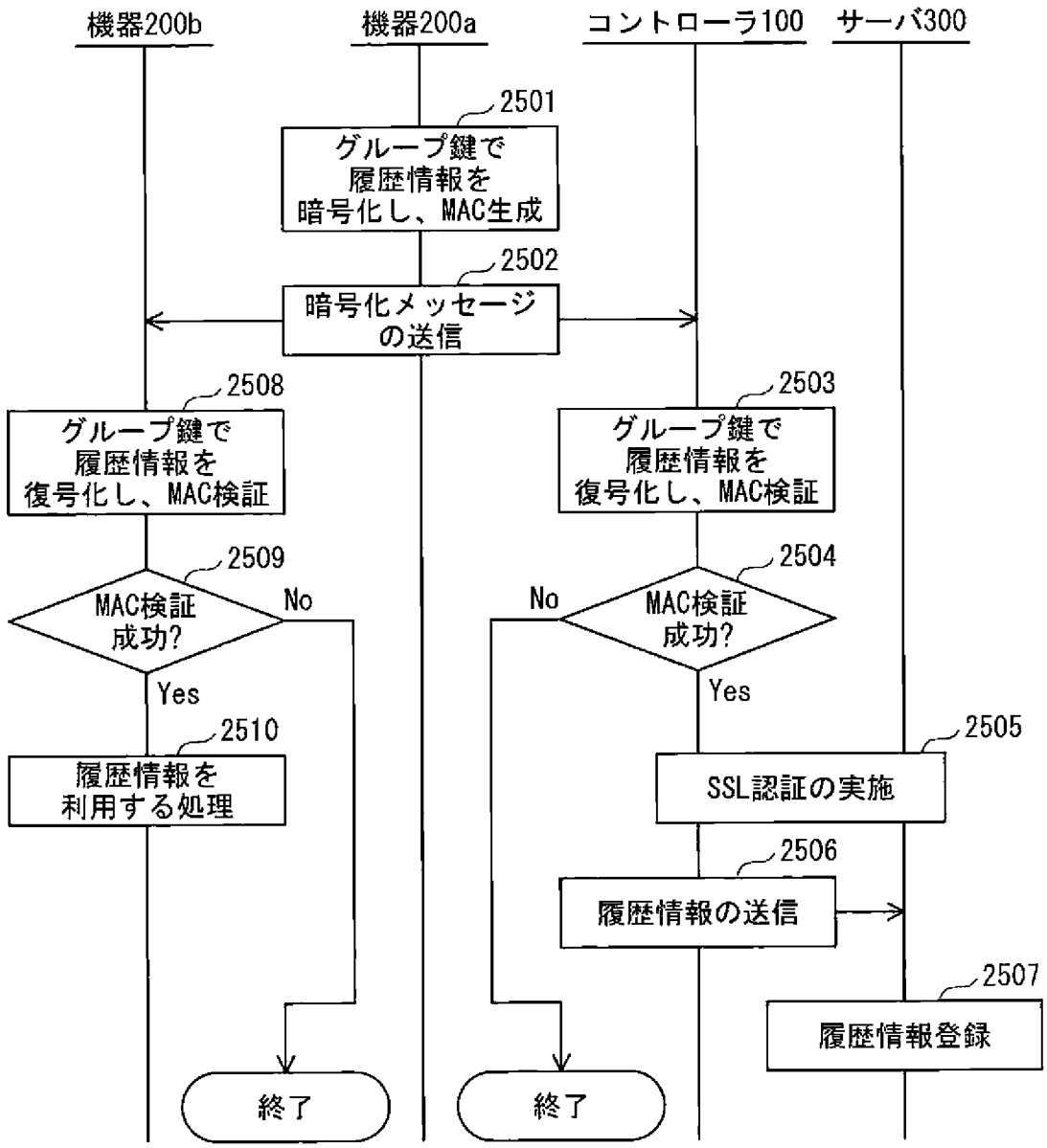
[図23]


機器200a
コントローラ100
サーバ300
S171
SSL認証の実施
S172
制御依頼情報の
作成及び送信
S173
制御コマンドを作成
S174
複数機器に係る
制御コマンドの場合、
グループ鍵で暗号化
S175
単一機器に係る
制御コマンドの場合、
セッション鍵で暗号化
S176
暗号化制御コマンド
の送信
S177
制御コマンドの復号
S178
制御コマンドの実行

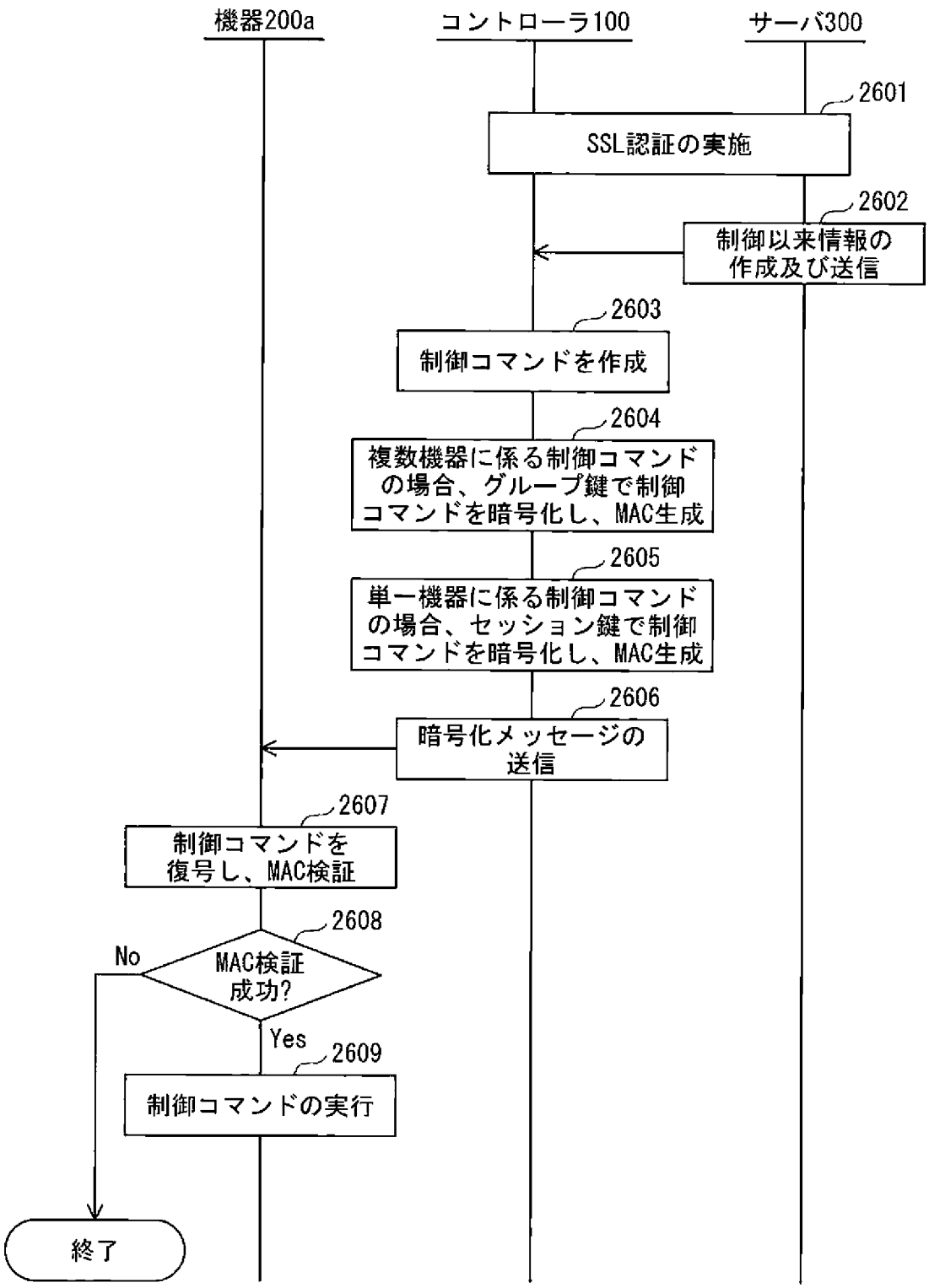
[図24]


(a) 暗号化前のメッセージフォーマット
2401
ヘッダ
2402
送信元アドレス
2403
送信先アドレス
2404
送信データ
暗号化対象
MAC対象
(b) 暗号化後のメッセージフォーマット
2401
ヘッダ
2402
送信元アドレス
2403
送信先アドレス
2405
認証付暗号化データ
(暗号化した送信データ||MAC)

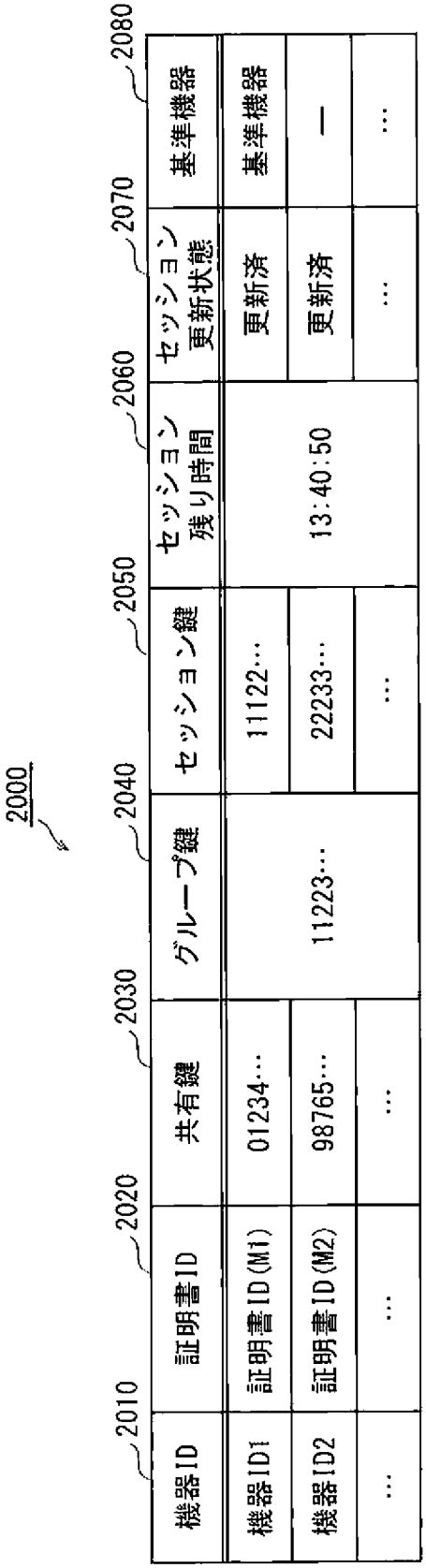
[図25]


機器200b
機器200a
コントローラ100
サーバ300
2501
グループ鍵で
履歴情報を
暗号化し、MAC生成
2502
暗号化メッセージ
の送信
2508
グループ鍵で
履歴情報を
復号化し、MAC検証
2503
グループ鍵で
履歴情報を
復号化し、MAC検証
2509
MAC検証
成功?
No
Yes
2504
No
MAC検証
成功?
Yes
2510
履歴情報を
利用する処理
2505
SSL認証の実施
2506
履歴情報の送信
2507
履歴情報登録
終了
終了

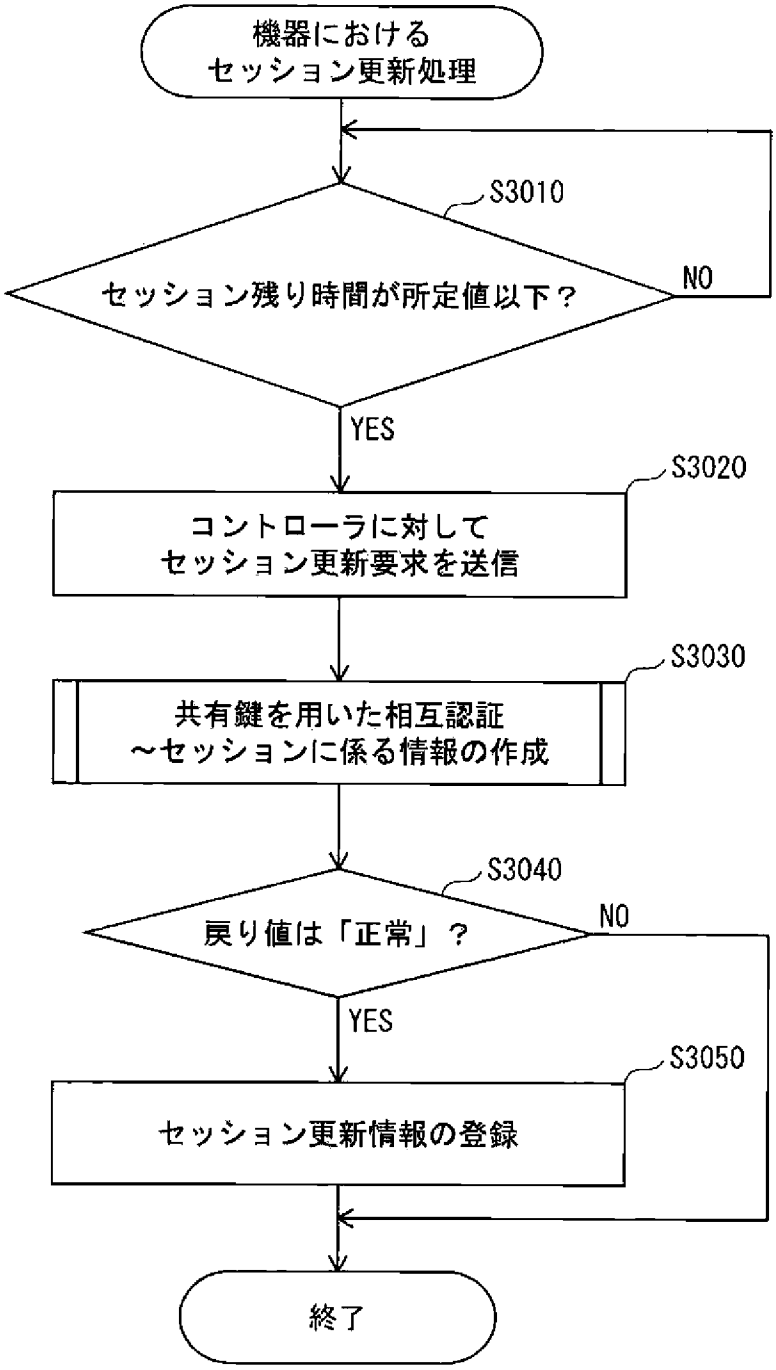
[図26]


機器200a
コントローラ100
サーバ300
2601
SSL認証の実施
2602
制御以来情報の作成及び送信
2603
制御コマンドを作成
2604
複数機器に係る制御コマンドの場合、グループ鍵で制御コマンドを暗号化し、MAC生成
2605
単一機器に係る制御コマンドの場合、セッション鍵で制御コマンドを暗号化し、MAC生成
2606
暗号化メッセージの送信
2607
制御コマンドを復号し、MAC検証
2608
MAC検証成功?
No
Yes
2609
制御コマンドの実行
終了

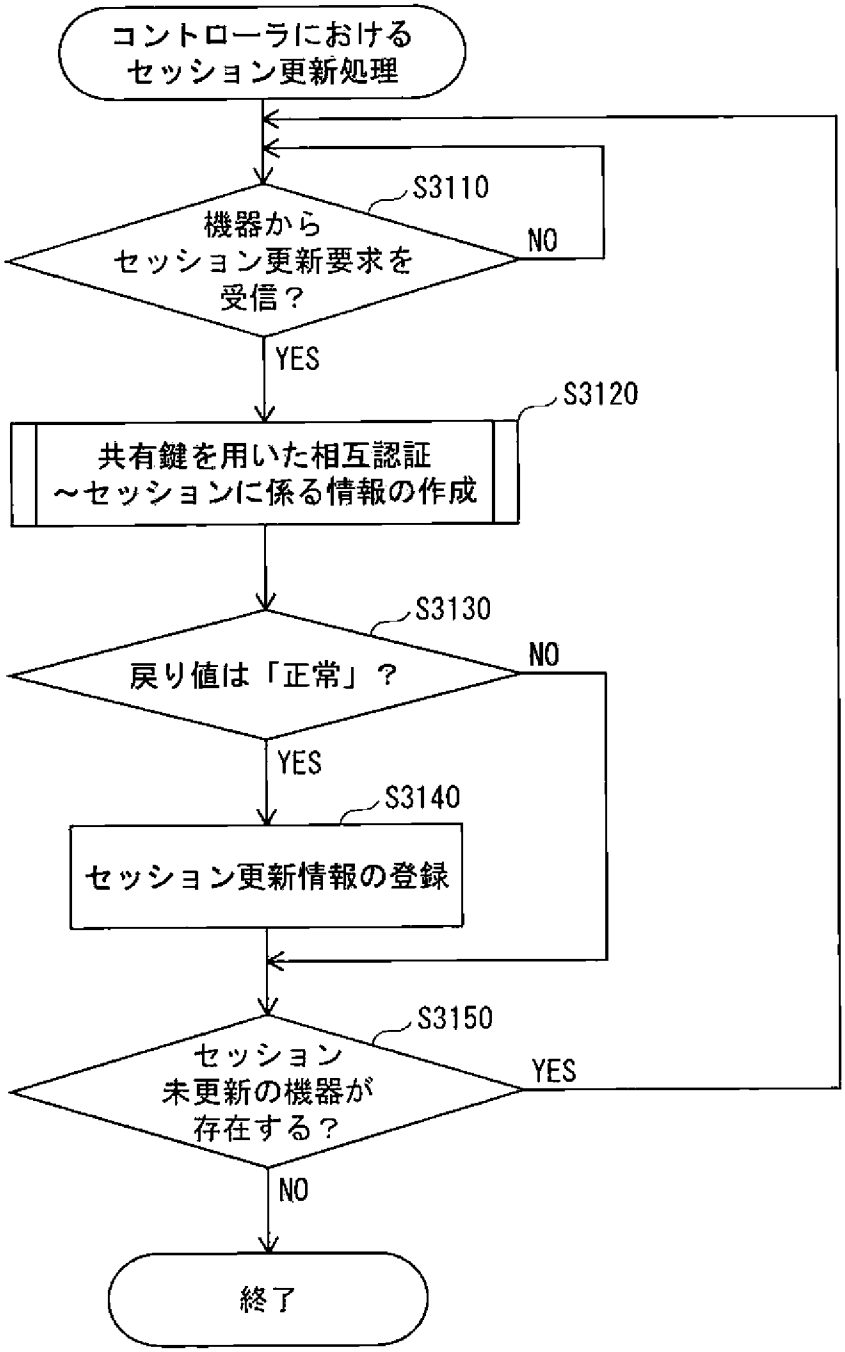
[図27]


2000
2010
2020
2030
2040
2050
2060
2070
2080
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
セッション更新状態
基準機器
機器ID1
証明書ID(M1)
01234…
11223…
11122…
13:40:50
更新済
基準機器
機器ID2
証明書ID(M2)
98765…
22233…
更新済
—
…
…
…
…
…
…

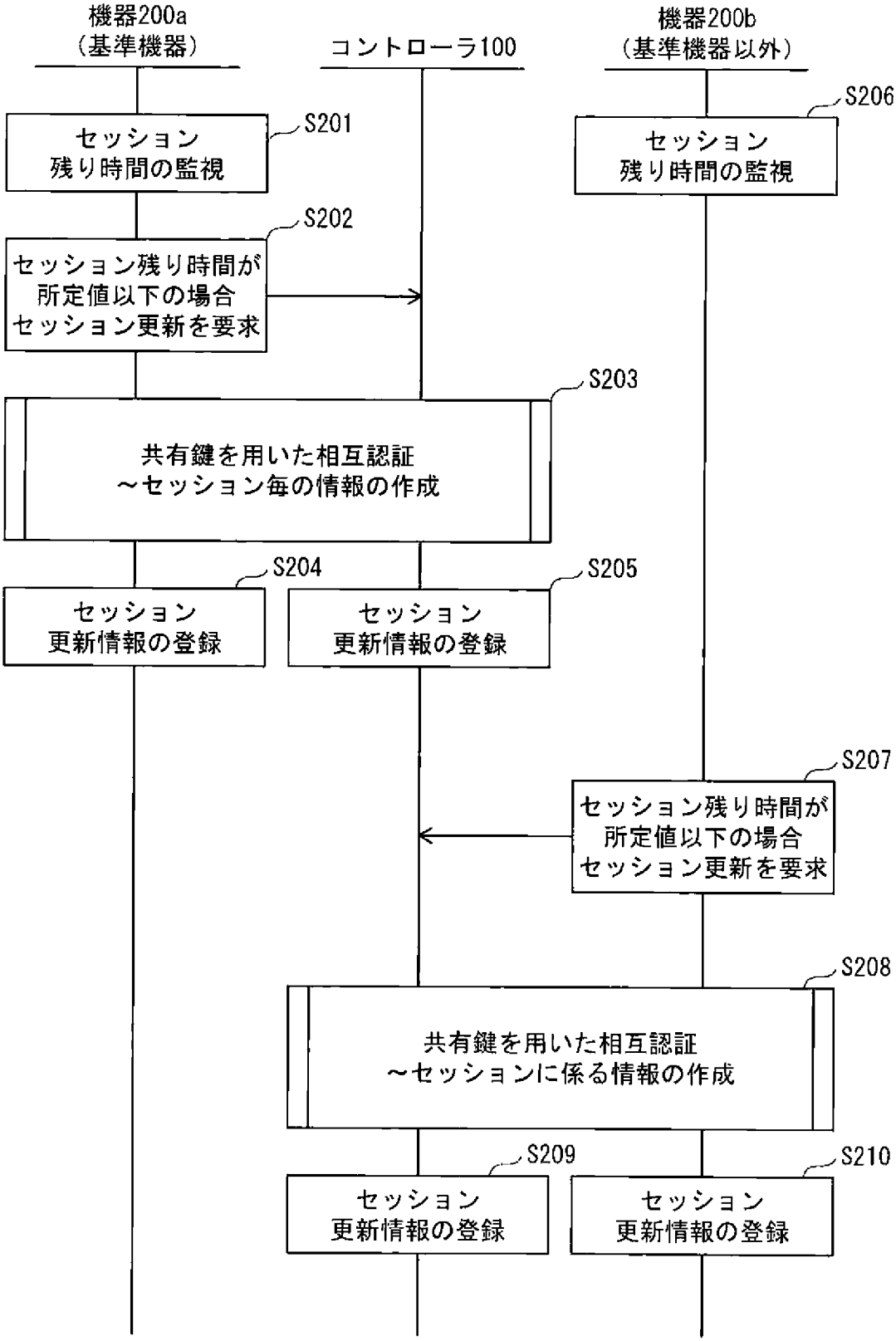
[図28]


機器における
セッション更新処理
S3010
セッション残り時間が所定値以下？
NO
YES
S3020
コントローラに対して
セッション更新要求を送信
S3030
共有鍵を用いた相互認証
～セッションに係る情報の作成
S3040
戻り値は「正常」？
NO
YES
S3050
セッション更新情報の登録
終了

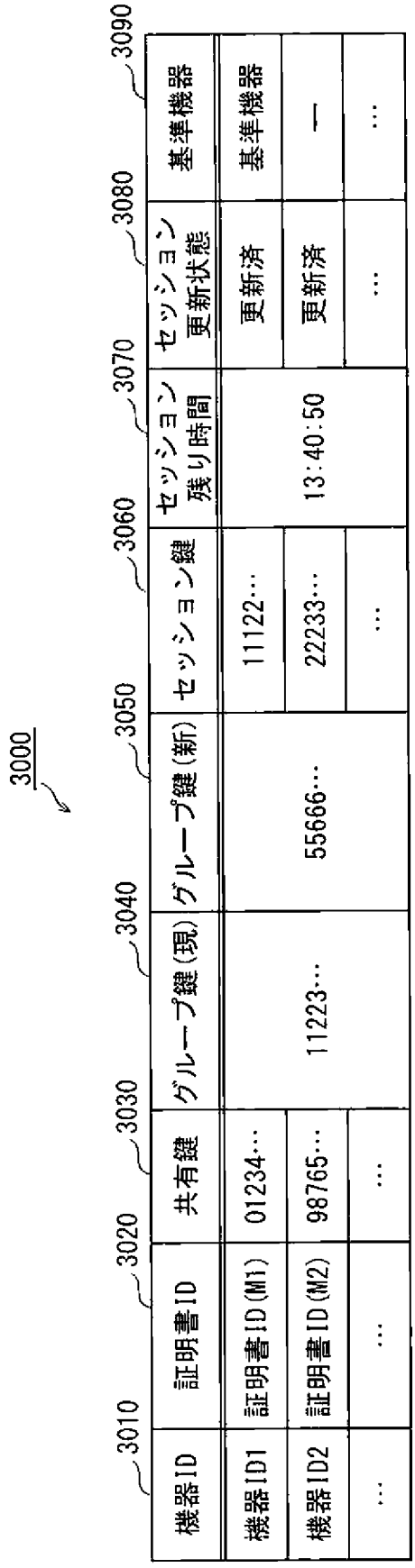
[図29]


コントローラにおける
セッション更新処理
S3110
機器から
セッション更新要求を
受信？
NO
YES
S3120
共有鍵を用いた相互認証
～セッションに係る情報の作成
S3130
戻り値は「正常」？
NO
YES
S3140
セッション更新情報の登録
S3150
セッション
未更新の機器が
存在する？
YES
NO
終了

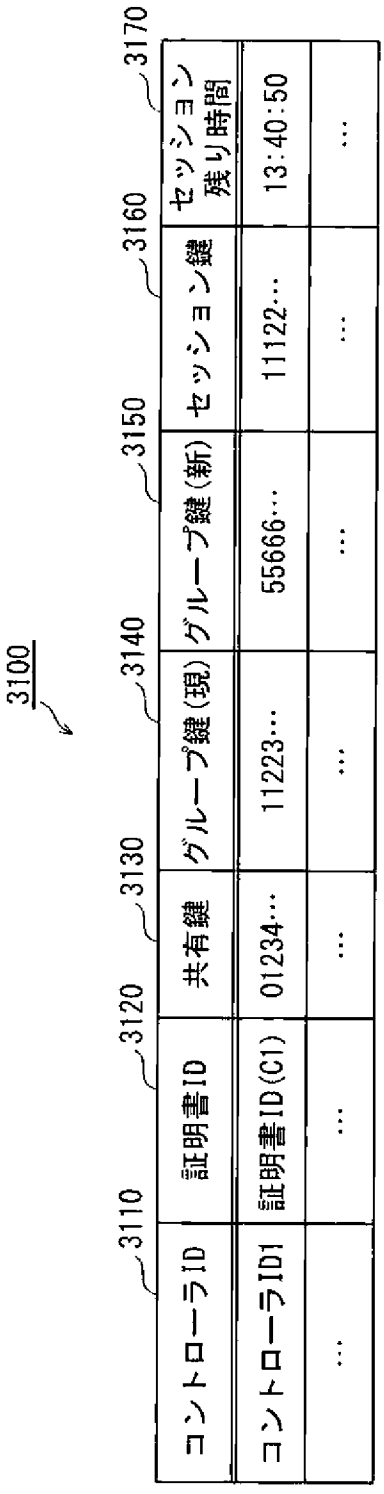
[図30]


機器200a
（基準機器）
コントローラ100
機器200b
（基準機器以外）
S201
セッション
残り時間の監視
S202
セッション残り時間が
所定値以下の場合
セッション更新を要求
S203
共有鍵を用いた相互認証
～セッション毎の情報の作成
S204
セッション
更新情報の登録
S205
セッション
更新情報の登録
S206
セッション
残り時間の監視
S207
セッション残り時間が
所定値以下の場合
セッション更新を要求
S208
共有鍵を用いた相互認証
～セッションに係る情報の作成
S209
セッション
更新情報の登録
S210
セッション
更新情報の登録

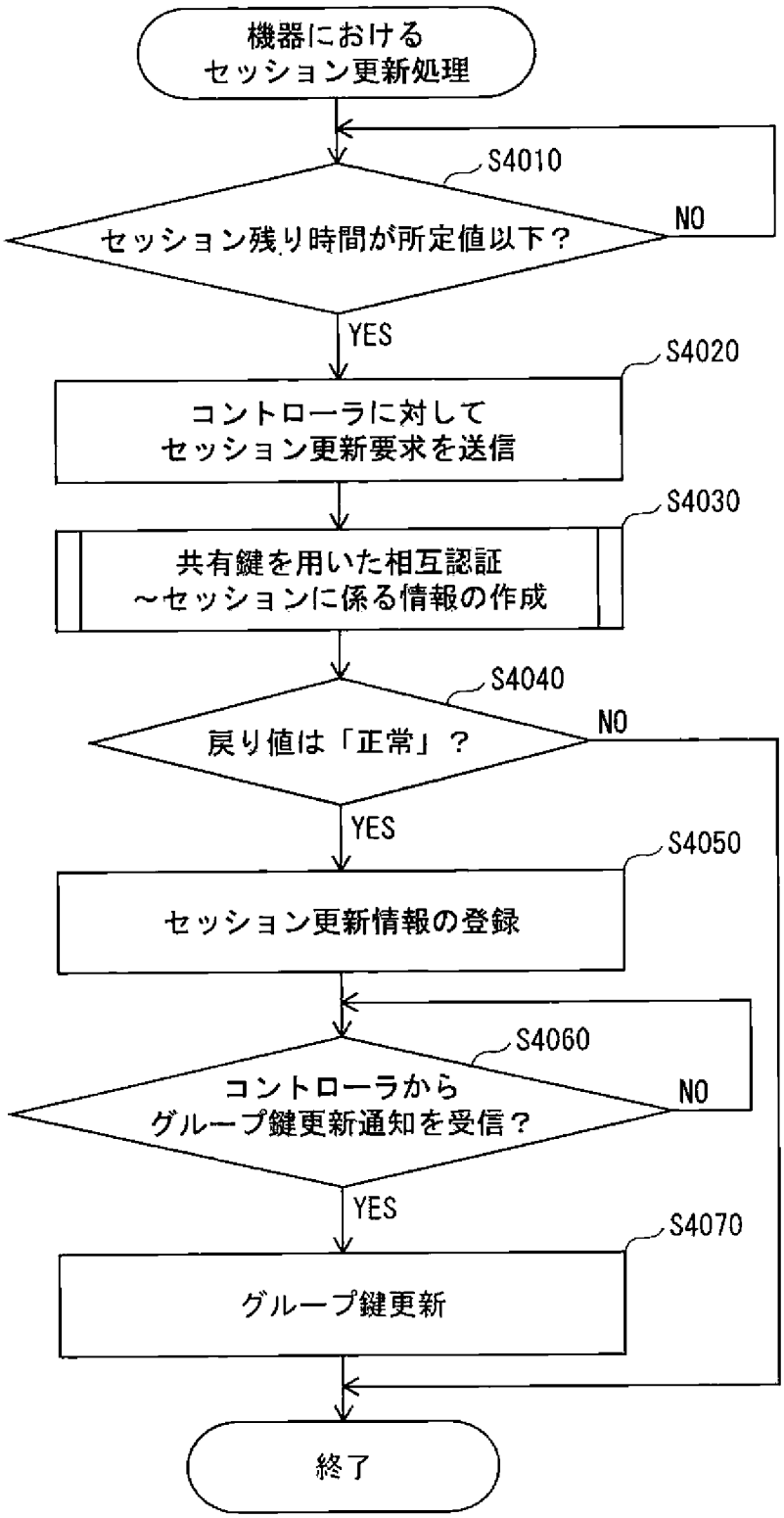
[図31]


3000
3010
3020
3030
3040
3050
3060
3070
3080
3090
機器ID
証明書ID
共有鍵
グループ鍵(現)
グループ鍵(新)
セッション鍵
セッション残り時間
セッション更新状態
基準機器
機器ID1
証明書ID(M1)
01234…
11223…
55666…
11122…
13:40:50
更新済
基準機器
機器ID2
証明書ID(M2)
98765…
22233…
更新済
—
…
…
…
…
…
…

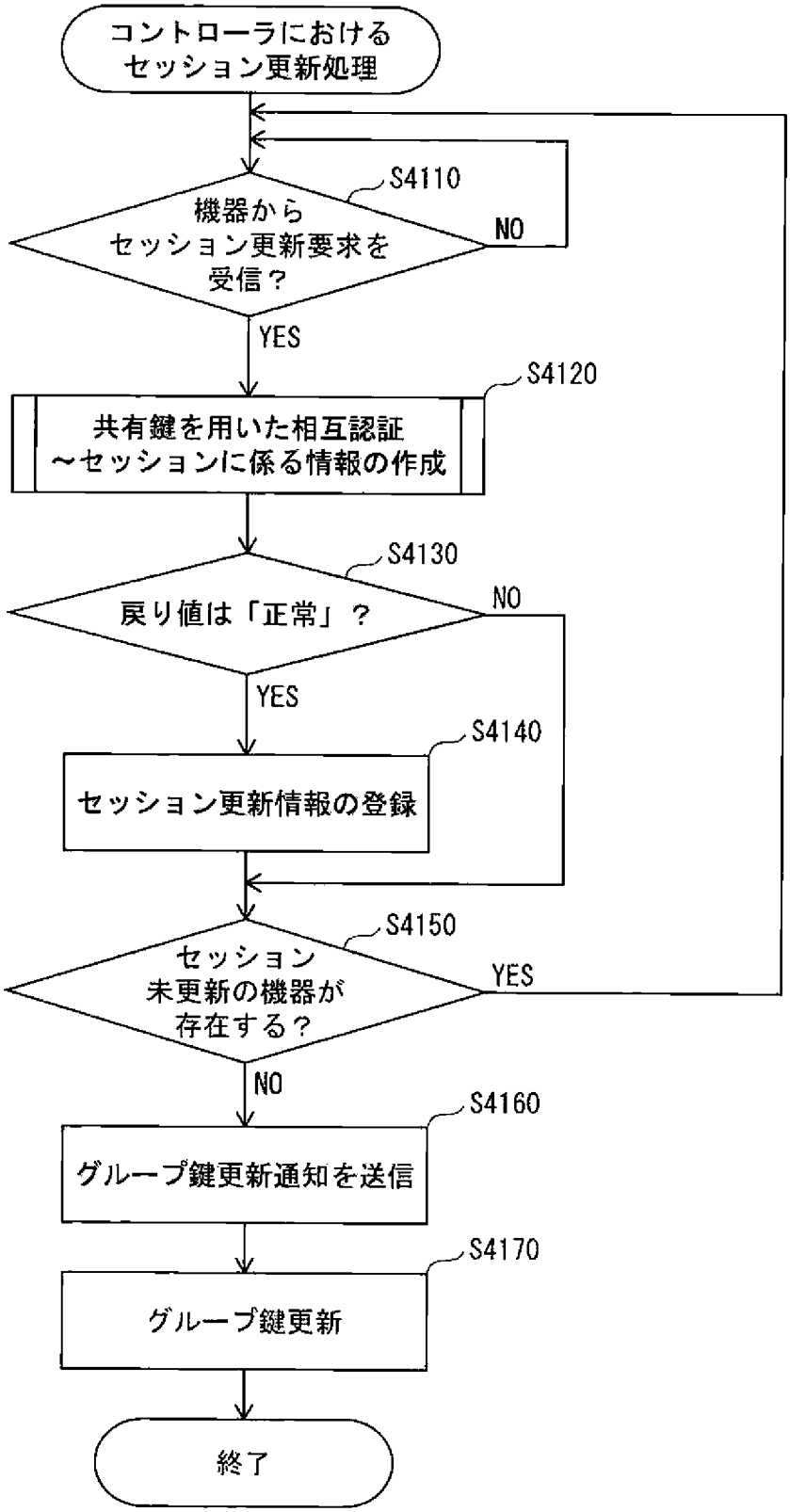
[図32]


3100
3110
コントローラID
コントローラID1
…
3120
証明書ID
証明書ID(C1)
…
3130
共有鍵
01234…
…
3140
グループ鍵(現)
11223…
…
3150
グループ鍵(新)
55666…
…
3160
セッション鍵
11122…
…
3170
セッション残り時間
13:40:50
…

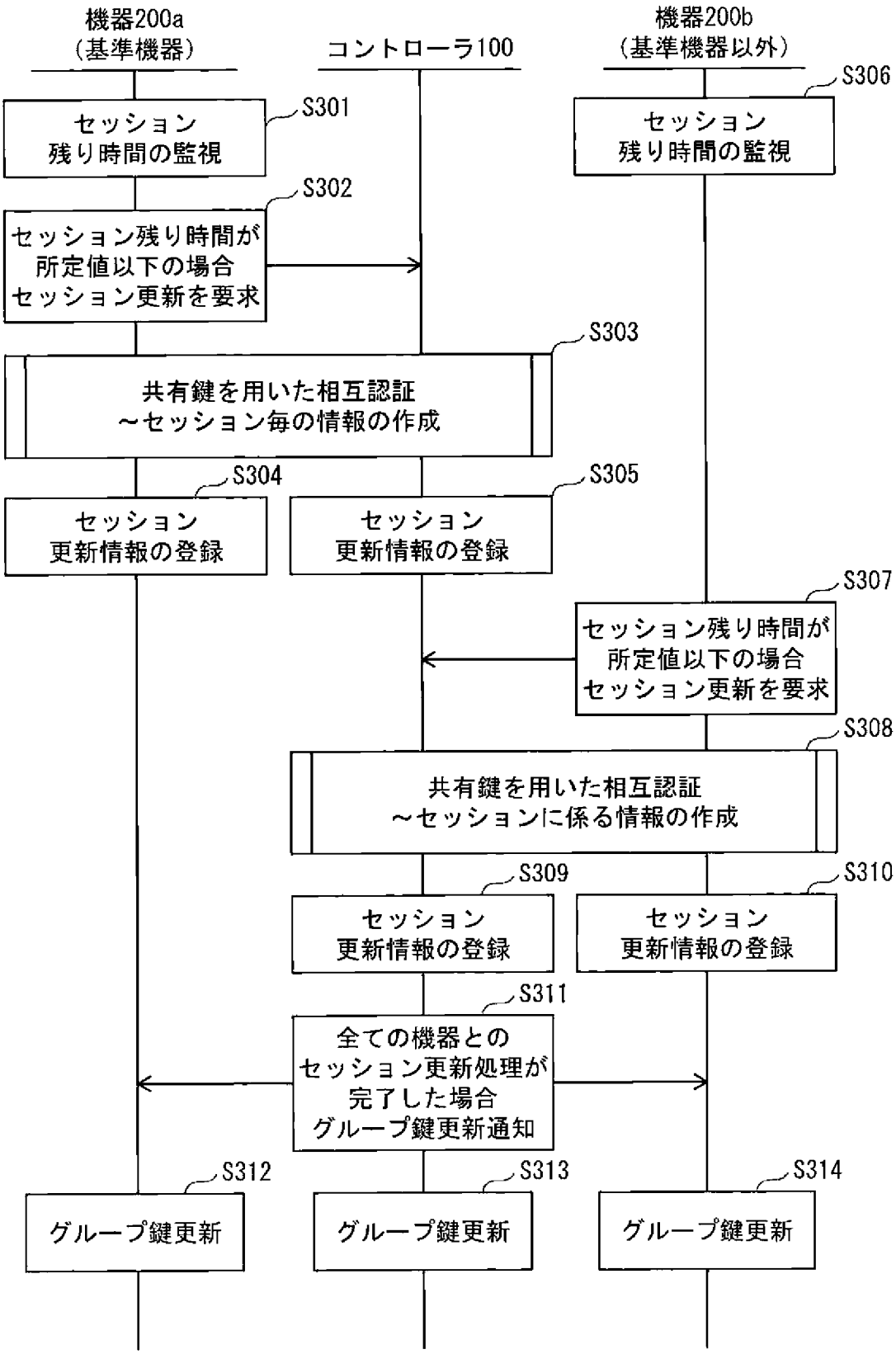
[図33]


機器における
セッション更新処理
S4010
セッション残り時間が所定値以下？
NO
YES
S4020
コントローラに対して
セッション更新要求を送信
S4030
共有鍵を用いた相互認証
～セッションに係る情報の作成
S4040
戻り値は「正常」？
NO
YES
S4050
セッション更新情報の登録
S4060
コントローラから
グループ鍵更新通知を受信？
NO
YES
S4070
グループ鍵更新
終了

[図34]


コントローラにおける
セッション更新処理
S4110
機器から
セッション更新要求を
受信？
NO
YES
S4120
共有鍵を用いた相互認証
～セッションに係る情報の作成
S4130
戻り値は「正常」？
NO
YES
S4140
セッション更新情報の登録
S4150
セッション
未更新の機器が
存在する？
YES
NO
S4160
グループ鍵更新通知を送信
S4170
グループ鍵更新
終了

[図35]


機器200a
（基準機器）
コントローラ100
機器200b
（基準機器以外）
S301
セッション
残り時間の監視
S302
セッション残り時間が
所定値以下の場合
セッション更新を要求
S303
共有鍵を用いた相互認証
～セッション毎の情報の作成
S304
セッション
更新情報の登録
S305
セッション
更新情報の登録
S306
セッション
残り時間の監視
S307
セッション残り時間が
所定値以下の場合
セッション更新を要求
S308
共有鍵を用いた相互認証
～セッションに係る情報の作成
S309
セッション
更新情報の登録
S310
セッション
更新情報の登録
S311
全ての機器との
セッション更新処理が
完了した場合
グループ鍵更新通知
S312
グループ鍵更新
S313
グループ鍵更新
S314
グループ鍵更新

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2016/000946

A. CLASSIFICATION OF SUBJECT MATTER
H04L9/08(2006.01)i, *G06F21/44*(2013.01)i, *H04L9/32*(2006.01)i, *H04Q9/00*(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)
H04L9/08, G06F21/44, H04L9/32, H04Q9/00

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)
JSTPlus/JMEDPlus/JST7580(JDreamIII), IEEE Xplore, broad cast, multi cast, encryption

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y A	JP 2013-192169 A (Hitachi, Ltd.), 26 September 2013 (26.09.2013), paragraphs [0051] to [0105]	9 1-8
Y A	JP 2001-148715 A (Mitsubishi Electric Corp.), 29 May 2001 (29.05.2001), paragraph [0022]	9 1-8
A	JP 2012-205088 A (Toshiba Corp.), 22 October 2012 (22.10.2012), paragraphs [0009] to [0048]	1-9
A	WO 2011/163073 A1 (ENTROPIC COMMUNICATIONS, INC.), 29 December 2011 (29.12.2011), paragraphs [0002] to [0073]	1-9

☒ 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
25 April 2016 (25.04.16)	10 May 2016 (10.05.16)
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

International application No.
PCT/JP2016/000946

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 2010-74225 A (Yokogawa Electric Corp.), 02 April 2010 (02.04.2010), paragraphs [0019] to [0067]	1-9
A	US 6330671 B1 (Sun Microsystems, Inc.), 11 December 2001 (11.12.2001), column 6, line 2 to column 12, line 64	1-9

JP 2013-192169 A	2013.09.26	(Family: none)
JP 2001-148715 A	2001.05.29	(Family: none)
JP 2012-205088 A	2012.10.22	US 8855306 B2 2014.10.07 column 2, line 15 to column 11, line 55 CN 102694647 A 2012.09.26
WO 2011/163073 A1	2011.12.29	JP 2013-539248 A 2013.10.17 US 2011/0173435 A1 2011.07.14 EP 2586180 A1 2013.05.01 CN 102948128 A 2013.02.27 KR 10-2013-0111960 A 2013.10.11
JP 2010-74225 A	2010.04.02	(Family: none)
US 6330671 B1	2001.12.11	JP 11-95658 A 1999.04.09 EP 887982 A2 1998.12.30 CA 2241701 A1 1998.12.23

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２０１６／０００９４６

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　H04L9/08(2006.01)i, G06F21/44(2013.01)i, H04L9/32(2006.01)i, H04Q9/00(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.　H04L9/08, G06F21/44, H04L9/32, H04Q9/00

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）

JSTPlus/JMEDPlus/JST7580 (JDreamIII), IEEE Xplore
broad cast, multi cast, encryption

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 2013-192169 A（株式会社日立製作所）2013.09.26, 段落[0051]-[0105]	9
A		1-8
Y	JP 2001-148715 A（三菱電機株式会社）2001.05.29, 段落[0022]	9
A		1-8
A	JP 2012-205088 A（株式会社東芝）2012.10.22, 段落[0009]-[0048]	1-9

☑　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
２５．０４．２０１６	１０．０５．２０１６

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	９３６４
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	中里　裕正 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	WO 2011/163073 A1 (ENTROPIC COMMUNICATIONS, INC.) 2011.12.29, 段落[0002]-[0073]	1-9
A	JP 2010-74225 A (横河電機株式会社) 2010.04.02, 段落[0019]-[0067]	1-9
A	US 6330671 B1 (Sun Microsystems, Inc.) 2001.12.11, 6欄2行-12欄64行	1-9

JP 2013-192169 A	2013.09.26	ファミリーなし	
JP 2001-148715 A	2001.05.29	ファミリーなし	
JP 2012-205088 A	2012.10.22	US 8855306 B2, 2欄15行-11欄55行	2014.10.07
		CN 102694647 A	2012.09.26
WO 2011/163073 A1	2011.12.29	JP 2013-539248 A	2013.10.17
		US 2011/0173435 A1	2011.07.14
		EP 2586180 A1	2013.05.01
		CN 102948128 A	2013.02.27
		KR 10-2013-0111960 A	2013.10.11
JP 2010-74225 A	2010.04.02	ファミリーなし	
US 6330671 B1	2001.12.11	JP 11-95658 A	1999.04.09
		EP 887982 A2	1998.12.30
		CA 2241701 A1	1998.12.23