(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第6653484号
(P6653484)

(45)発行日　令和2年2月26日(2020.2.26)　(24)登録日　令和2年1月30日(2020.1.30)

(51)Int.Cl.		F I		
G06F 21/44	(2013.01)	G06F	21/44	
G06F 15/00	(2006.01)	G06F	15/00	420B
H04L 9/32	(2006.01)	H04L	9/00	673B
H04L 9/08	(2006.01)	H04L	9/00	601C

請求項の数 6　(全 16 頁)

(21)出願番号　特願2015-245007(P2015-245007)
(22)出願日　平成27年12月16日(2015.12.16)
(65)公開番号　特開2017-111599(P2017-111599A)
(43)公開日　平成29年6月22日(2017.6.22)
審査請求日　平成30年10月24日(2018.10.24)

(73)特許権者　314012076
パナソニックＩＰマネジメント株式会社
大阪府大阪市中央区城見２丁目１番６１号
(74)代理人　100095500
弁理士　伊藤　正和
(74)代理人　100141449
弁理士　松本　隆芳
(74)代理人　100142446
弁理士　細川　覚
(74)代理人　100170575
弁理士　森　太士
(72)発明者　安　健司
大阪府門真市大字門真１００６番地　パナソニック株式会社内

最終頁に続く

(54)【発明の名称】認証装置、認証システム及び認証方法

(57)【特許請求の範囲】

【請求項１】

機器と認証処理を行う認証装置であって、

前記認証処理の開始を要求する認証開始要求を前記機器から受信する通信インターフェースと、

前記認証開始要求を送信した前記機器を識別する機器識別子と、前記認証開始要求に対応するセッションを識別するセッション識別子と、前記セッションにおける段階を示す認証状態とを、前記セッション毎のレコードとして有するセッション管理テーブルを記憶する記憶装置と、

前記通信インターフェースが前記認証開始要求を受信し、前記セッション管理テーブルにおいて、前記機器識別子が前記認証開始要求を送信した前記機器を示し、且つ、前記認証状態が第１状態である前記レコードがある場合、前記セッション管理テーブルへの新たなレコードを追加することなく前記セッション識別子を更新する処理装置とを備え、

前記第１状態は、前記通信インターフェースが、前記認証開始要求に対する認証開始応答を前記機器に送信した後に前記機器から送信される、前記認証開始応答に対する応答を未だ受信していない状態であることを特徴とする認証装置。

【請求項２】

前記処理装置は、前記通信インターフェースが前記認証開始要求を受信し、前記セッション管理テーブルにおいて、前記機器識別子が前記認証開始要求を送信した前記機器を示し、且つ、前記認証状態が前記第１状態である前記レコードがある場合、前記認証開始要

求を受け入れることを特徴とする請求項１に記載の認証装置。
【請求項３】
前記処理装置は、前記機器との認証処理が開始されたことに応じて、対応する前記レコードの前記認証状態を第２状態に変更し、
前記処理装置は、前記通信インターフェースが前記認証開始要求を受信し、前記セッション管理テーブルにおいて、前記機器識別子が前記認証開始要求を送信した前記機器を示し、且つ、前記認証状態が前記第２状態である前記レコードがある場合、前記認証開始要求を破棄することを特徴とする請求項１に記載の認証装置。
【請求項４】
前記処理装置は、前記機器との認証処理が成功したことに応じて、対応する前記レコードの前記認証状態を第３状態に変更し、
前記処理装置は、前記通信インターフェースが前記認証開始要求を受信し、前記セッション管理テーブルにおいて、前記機器識別子が前記認証開始要求を送信した前記機器を示し、且つ、前記認証状態が前記第３状態である前記レコードがある場合、前記認証開始要求を受け入れることを特徴とする請求項１に記載の認証装置。
【請求項５】
機器と、前記機器と認証処理を行う認証装置とを備える認証システムであって、
前記機器は、前記認証処理の開始を要求する認証開始要求を前記認証装置に送信し、
前記認証装置は、
前記認証開始要求を受信する通信インターフェースと、
前記認証開始要求を送信した前記機器を識別する機器識別子と、前記認証開始要求に対応するセッションを識別するセッション識別子と、前記セッションにおける段階を示す認証状態とを、前記セッション毎のレコードとして有するセッション管理テーブルを記憶する記憶装置と、
前記通信インターフェースが前記認証開始要求を受信し、前記セッション管理テーブルにおいて、前記機器識別子が前記認証開始要求を送信した前記機器を示し、且つ、前記認証状態が第１状態である前記レコードがある場合、前記セッション管理テーブルへの新たなレコードを追加することなく前記セッション識別子を更新する処理装置とを備え、
前記第１状態は、前記通信インターフェースが、前記認証開始要求に対する認証開始応答を前記機器に送信した後、前記機器から前記認証開始応答に対する応答を未だ受信していない状態であることを特徴とする認証システム。
【請求項６】
機器と認証処理を行う認証装置の認証方法であって、
通信インターフェースが、前記認証処理の開始を要求する認証開始要求を前記機器から受信することと、
記憶装置が、前記認証開始要求を送信した前記機器を識別する機器識別子と、前記認証開始要求に対応するセッションを識別するセッション識別子と、前記セッションにおける段階を示す認証状態とを、前記セッション毎のレコードとして有するセッション管理テーブルを記憶することと、
処理装置が、前記通信インターフェースが前記認証開始要求を受信し、前記セッション管理テーブルにおいて、前記機器識別子が前記認証開始要求を送信した前記機器を示し、且つ、前記認証状態が第１状態である前記レコードがある場合、前記セッション管理テーブルへの新たなレコードを追加することなく前記セッション識別子を更新することとを含み、
前記第１状態は、前記通信インターフェースが、前記認証開始要求に対する認証開始応答を前記機器に送信した後、前記機器から前記認証開始応答に対する応答を未だ受信していない状態であることを特徴とする認証方法。
【発明の詳細な説明】
【技術分野】
【０００１】

本発明は、認証装置、認証システム及び認証方法に関する。
【背景技術】
【０００２】
所定の認証プロトコルにより機器同士が相互認証を行い、相互認証が成功した機器の間で暗号化通信を行う技術が知られている。特許文献１は、ＲＦＣ５１５９に規定のネットワークアクセス認証プロトコル（ＰＡＮＡ）を用いたシステムにおいて、認証手続きの軽装化するものである。
【先行技術文献】
【特許文献】
【０００３】
【特許文献１】特開２０１３－０６２７６４号公報
【発明の概要】
【発明が解決しようとする課題】
【０００４】
しかしながら、特許文献１に記載の技術は、認証開始要求を受信する機器が全ての認証開始要求を記録する構成となっている。その為、例えば不正な認証開始要求を連続的に受信する場合、リソースの不要な消費を招いてしまい、正当な認証開始要求に応じた手続きを継続できなくなる可能性がある。
【０００５】
本発明は、上記問題点を鑑み、リソースの消費量を削減し、堅牢性を向上することができる認証装置、認証システム及び認証方法を提供することを目的とする。
【課題を解決するための手段】
【０００６】
上記目的を達成するために、本発明の第１の態様は、機器と認証処理を行う認証装置であって、認証処理の開始を要求する認証開始要求を機器から受信する通信インターフェースと、認証開始要求を送信した機器を識別する機器識別子と、認証開始要求に対応するセッションを識別するセッション識別子と、セッションにおける段階を示す認証状態とを、セッション毎のレコードとして有するセッション管理テーブルを記憶する記憶装置と、通信インターフェースが認証開始要求を受信し、セッション管理テーブルにおいて、機器識別子が認証開始要求を送信した機器を示し、且つ、認証状態が第１状態であるレコードがある場合、セッション識別子を更新する処理装置とを備える認証装置であることを要旨とし、第１状態が、通信インターフェースが、認証開始要求に対する認証開始応答を機器に送信した後に機器から送信される、認証開始応答に対する応答を未だ受信していない状態であることを特徴とする。
【０００７】
本発明の第２の態様は、機器と、機器と認証処理を行う認証装置とを備える認証システムであって、機器は、認証処理の開始を要求する認証開始要求を認証装置に送信し、認証装置は、認証開始要求を受信する通信インターフェースと、認証開始要求を送信した機器を識別する機器識別子と、認証開始要求に対応するセッションを識別するセッション識別子と、セッションにおける段階を示す認証状態とを、セッション毎のレコードとして有するセッション管理テーブルを記憶する記憶装置と、通信インターフェースが認証開始要求を受信し、セッション管理テーブルにおいて、機器識別子が認証開始要求を送信した機器を示し、且つ、認証状態が第１状態であるレコードがある場合、セッション識別子を更新する処理装置とを備え、第１状態は、通信インターフェースが、認証開始要求に対する認証開始応答を機器に送信した後、機器から認証開始応答に対する応答を未だ受信していない状態であることを特徴とする。
【０００８】
本発明の第３の態様は、機器と認証処理を行う認証装置の認証方法であって、通信インターフェースが、前記認証処理の開始を要求する認証開始要求を前記機器から受信することと、記憶装置が、前記認証開始要求を送信した前記機器を識別する機器識別子と、前記

認証開始要求に対応するセッションを識別するセッション識別子と、前記セッションにおける段階を示す認証状態とを、前記セッション毎のレコードとして有するセッション管理テーブルを記憶することと、処理装置が、前記通信インターフェースが前記認証開始要求を受信し、前記セッション管理テーブルにおいて、前記機器識別子が前記認証開始要求を送信した前記機器を示し、且つ、前記認証状態が第１状態である前記レコードがある場合、前記セッション識別子を更新することとを含み、前記第１状態は、前記通信インターフェースが、前記認証開始要求に対する認証開始応答を前記機器に送信した後、前記機器から前記認証開始応答に対する応答を未だ受信していない状態であることを特徴とする。

【発明の効果】

【０００９】

本発明によれば、認証開始要求に応じて、セッション管理テーブルを編集することにより、リソースの消費量を削減し、堅牢性を向上することができる認証装置、認証システム及び認証方法を提供することができる。

【図面の簡単な説明】

【００１０】

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

【図２】図２は、本発明の実施の形態に係る認証システムが備える機器制御装置の基本的な構成を説明するブロック図である。

【図３】図３は、本発明の実施の形態に係る認証システムに用いるセッション管理テーブルの基本的なデータ構成を説明する表である。

【図４】図４は、本発明の実施の形態に係る認証システムに用いる認証状態を説明する表である。

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

【図６】図６は、本発明の実施の形態に係る認証システムの動作例を説明するシーケンス図である。

【図７】図７は、本発明の実施の形態に係る認証システムに用いるセッション管理テーブルを説明する表である。

【図８】図８は、本発明の実施の形態に係る認証システムの動作例を説明するシーケンス図である。

【図９】図９は、認証状態をレコードに含まないセッション管理テーブルを説明する表である。

【図１０】図１０は、本発明の実施の形態に係る認証システムに用いるセッション管理テーブルを説明する表である。

【図１１】図１１は、本発明の実施の形態に係る認証システムに用いるセッション管理テーブルを説明する表である。

【図１２】図１２は、本発明の実施の形態に係る認証システムが備える機器制御装置の動作例を説明するフローチャートである。

【図１３】図１３は、本発明の実施の形態に係る認証システムが備える機器制御装置の動作例を説明するフローチャートである。

【図１４】図１４は、本発明の実施の形態に係る認証システムの動作例を説明するシーケンス図である。

【図１５】図１５は、本発明の実施の形態に係る認証システムに用いるセッション管理テーブルを説明する表である。

【図１６】図１６は、本発明の実施の形態に係る認証システムに用いるセッション管理テーブルを説明する表である。

【発明を実施するための形態】

【００１１】

次に、図面を参照して、実施の形態を説明する。以下の図面の記載において、同一又は

類似の部分には同一又は類似の符号を付し、重複する説明を省略している。

【００１２】

（認証システム）

本実施の形態に係る認証システムは、図１に示すように、機器制御装置１と、機器２とを備える。機器制御装置１は、ブロードバンドルータ４を介して機器２と通信可能に接続される。機器制御装置１は、ブロードバンドルータ４を介さずに機器２と直接的に通信可能に接続されるようにしてもよい。機器２の数は、単数であっても複数であってもよい。ブロードバンドルータ４は、機器制御装置１と機器２との間の通信や機器制御装置１及び機器２とインターネット５との間の通信を中継する。機器制御装置１、機器２及びブロードバンドルータ４の相互間の通信は、有線通信であっても無線通信であってもよい。

【００１３】

機器制御装置１は、例えば、機器２の使用電力量、発電余剰電力量等を管理するホームエネルギーマネジメントシステム（ＨＥＭＳ）におけるコントローラである。例えば、機器制御装置１は、機器２との認証処理が成功することにより機器２を登録し、登録された機器とＨＥＭＳを構成する。機器制御装置１は、認証処理の開始を要求するメッセージである認証開始要求に応じて、認証開始要求を送信した通信機器との認証処理を行う認証装置である。

【００１４】

図２に示すように、機器制御装置１は、処理装置１０と、処理装置１０による制御に応じて他の機器と通信する通信インターフェース（Ｉ／Ｆ）１１と、プログラムや各種データ等の情報を記憶する記憶装置１２とを備える。通信Ｉ／Ｆ１１が行う通信は、無線通信であっても有線通信であってもよい。記憶装置１２は、セッション管理テーブル１２１と、認証情報１２２と、登録情報１２３とを記憶する。

【００１５】

図３に示すように、セッション管理テーブル１２１は、機器識別子（機器ＩＤ）と、セッション識別子（セッションＩＤ）と、セッションにおける段階を示す認証状態とを、セッション毎のレコードとして有する。

【００１６】

機器ＩＤは、認証開始要求を送信した機器２を識別する送信元識別子である。機器ＩＤは、例えば、認証開始要求に含まれる認証開始要求の送信元アドレスである。セッションＩＤは、認証開始要求に対応する、機器２とのセッションを識別する識別子である。セッションＩＤは、例えば、受信した認証開始要求毎に付される一連番号である。認証状態は、セッションＩＤ毎の、機器２とのセッションにおける段階を示す。

【００１７】

図４に示すように、認証状態は、例えば、ＲＦＣ５１９１に規定されるネットワークアクセス認証プロトコル（ＰＡＮＡ）におけるフェーズに一部が対応する。なお、ＰＡＮＡにおける状態遷移については、ＲＦＣ５６０９に規定される。

【００１８】

認証情報１２２は、機器２との認証処理に必要な情報である。認証情報１２２は、機器制御装置１自身の秘密鍵及び公開鍵証明書を含む。公開鍵証明書は、公開鍵証明書のバージョン、発行者、有効期間の開始時、有効期間の終了時（有効期限）、証明書ＩＤ（識別子）、機器制御装置１の公開鍵、認証局の署名を含む。公開鍵証明書の公開鍵は、機器制御装置１の秘密鍵に対応する。公開鍵証明書の署名は、認証局の秘密鍵を用いて作成される。公開鍵証明書は、認証局により発行され、機器制御装置１の製造時に記憶装置１２に記憶される。

【００１９】

登録情報１２３は、既に登録された機器２に関する情報である。登録情報１２３は、既に登録された機器２を識別する機器ＩＤ、各機器２の公開鍵証明書を識別する証明書ＩＤ、共有鍵（事前共有鍵：ＰＳＫ）、グループ鍵、セッション鍵、セッション有効期間を含む。共有鍵は、機器制御装置１と各機器２との間でそれぞれ共有される。グループ鍵は、

機器制御装置１が各機器２に一斉送信する情報の暗号化及び復号化に用いられる。同一のグループに属する機器２は、同一のグループ鍵を機器制御装置１と共有する。セッション鍵は、機器制御装置１と各機器２との間のユニキャスト通信の暗号化及び復号化に用いられる。セッション有効期間は、機器制御装置１と各機器２との間で設定される、セッションが有効である期間である。

【００２０】

処理装置１０は、セッション管理部１０１と、認証処理部１０２と、暗号処理部１０３とを論理構造として有する。処理装置１０は、例えば、中央演算装置（ＣＰＵ）等を含む集積回路からなる。処理装置１０が、予めインストールされたコンピュータプログラムを実行することにより、セッション管理部１０１、認証処理部１０２及び暗号処理部１０３が構成される。

【００２１】

セッション管理部１０１は、通信Ｉ／Ｆ１１が認証開始要求を受信することに応じて、セッション管理テーブル１２１を編集することにより、認証開始要求に対応するセッションを管理する。認証処理部１０２は、認証情報１２２を用いて、機器２と相互認証する。認証処理部１０２は、認証処理が成功することに応じて、認証された機器２に関する情報を登録情報１２３として登録する。暗号処理部１０３は、登録情報１２３に登録された機器２との通信における暗号化及び復号化を行う。

【００２２】

機器２は、例えば、エアコン、冷蔵庫、照明装置等の負荷機器、太陽電池、蓄電池等の電源機器、スマートメータ等からそれぞれ構成される。機器２は、機器制御装置１との認証処理が成功することにより機器制御装置１に登録される。機器２は、機器制御装置１に登録されることによりＨＥＭＳに加入し、機器制御装置１と暗号化通信を行う通信機器である。

【００２３】

図５に示すように、機器２は、処理装置２０と、処理装置２０の制御に応じて機器制御装置１と通信する通信Ｉ／Ｆ２１と、プログラムや各種データを記憶する記憶装置２２とを備える。通信Ｉ／Ｆ２１が行う通信は、無線通信であっても有線通信であってもよい。記憶装置２２は、認証情報２２１と、登録情報２２２とを記憶する。

【００２４】

認証情報２２１は、機器制御装置１との認証処理に必要な情報である。認証情報２２１は、機器２自身の秘密鍵及び公開鍵証明書を含む。公開鍵証明書の公開鍵は、機器２の秘密鍵に対応する。公開鍵証明書の署名は、認証局の秘密鍵を用いて作成される。公開鍵証明書は、認証局により発行され、機器２の製造時に記憶装置２２に記憶される。

【００２５】

登録情報２２２は、機器２自身が登録される機器制御装置１に関する情報である。登録情報２２２は、機器２自身が登録される機器制御装置１を識別する機器制御装置ＩＤ、機器制御装置１の公開鍵証明書を識別する証明書ＩＤ、共有鍵、グループ鍵、セッション鍵、セッション有効期間を含む。共有鍵は、機器制御装置１と各機器２との間で共有される。グループ鍵は、機器制御装置１が機器２に対して一斉送信する情報の暗号化及び復号化に用いられる。セッション鍵は、機器制御装置１との間のユニキャスト通信の暗号化及び復号化に用いられる。

【００２６】

処理装置２０は、認証処理部２０１と、暗号処理部２０２とを論理構造として有する。処理装置２０は、例えば、中央演算装置（ＣＰＵ）等を含む集積回路からなる。処理装置２０が、予めインストールされたコンピュータプログラムを実行することにより、認証処理部２０１及び暗号処理部２０２が構成される。

【００２７】

認証処理部２０１は、認証情報２２１を用いて、機器制御装置１と相互認証する。機器２は、機器制御装置１との認証処理が成功したことに応じて、機器制御装置１に登録され

る。暗号処理部２０２は、登録された機器制御装置１との通信における暗号化及び復号化を行う。

【００２８】

（認証方法）

図６のシーケンス図を参照して、本実施の形態に係る認証システムにおける認証方法の一例を説明する。

【００２９】

先ず、ステップＳ１において、機器２の認証処理部２０１は、例えばユーザの操作に応じて、通信Ｉ／Ｆ１１を介して、認証処理の開始を要求するメッセージである認証開始要求を機器制御装置１に送信する。例えば、認証開始要求は、ＰＡＮＡにおけるＰＣＩ（ＰＡＮＡ－Ｃｌｉｅｎｔ－Ｉｎｉｔｉａｔｉｏｎ）メッセージである。認証開始要求は、機器２の機器ＩＤを含む。

【００３０】

機器制御装置１の通信Ｉ／Ｆ１１は、機器２から送信された認証開始要求を受信する。セッション管理部１０１は、認証開始要求の受信に応じて、セッション管理テーブル１２１において、認証開始要求に含まれる機器ＩＤを検索する。認証開始要求に含まれる機器ＩＤを含むレコードがない場合、セッション管理部１０１は、機器ＩＤと、新たなセッションＩＤと、第１状態（ＰｒｅＡｕｔｈ）を示す認証状態とが、新たなレコードとしてセッション管理テーブル１２１に追加する。

【００３１】

例えば、認証開始要求を送信した機器２－１を示す機器ＩＤを含むレコードがセッション管理テーブル１２１にないとする。この場合、セッション管理部１０１は、図３に示すように、機器ＩＤ「２－１」、認証状態「ＰｒｅＡｕｔｈ」及び新たなセッションＩＤ「９」を、新たなレコードとしてセッション管理テーブル１２１に追加する。

【００３２】

第１状態（ＰｒｅＡｕｔｈ）は、機器制御装置１の通信Ｉ／Ｆ１１が、認証開始要求に対する認証開始応答を機器２に送信した後に機器２から送信される、認証開始応答に対する応答を未だ受信していない状態を意味する。例えば、第１状態は、図４を示すように、ＰＡＮＡにおける認証フェーズ（Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　Ｐｈａｓｅ）のうち、認証開始要求の受信から認証処理が開始されるまでの状態である。

【００３３】

ステップＳ２において、機器制御装置１の認証処理部１０２は、認証開始要求に応じて、認証開始応答を機器２に送信する。例えば、認証開始応答は、ＰＡＮＡにおけるＰＡＲ（ＰＡＮＡ－Ａｕｔｈ－Ｒｅｑｕｅｓｔ）（ｐ）メッセージである。ｐはシーケンス番号である。認証開始応答は、機器制御装置１が使用可能な認証アルゴリズムの種類、公開鍵証明書を含む。

【００３４】

ステップＳ３において、機器２の認証処理部２０１は、認証開始応答に対する応答を機器制御装置１に送信する。例えば、認証開始応答に対する応答は、ＰＡＮＡにおけるＰＡＮ（ＰＡＮＡ－Ａｕｔｈ－Ａｎｓｗｅｒ）（ｐ）メッセージである。認証開始応答に対する応答は、認証開始応答に含まれる認証アルゴリズムの種類のうち、以降の認証処理において使用する種類、公開鍵証明書を含む。

【００３５】

通信Ｉ／Ｆ１１がＰＡＮ（ｐ）メッセージを受信することにより、認証処理部１０２は、機器２との認証処理を開始する。セッション管理部１０１は、認証処理が開始されたことに応じて、対応するレコードの認証状態を第２状態（Ａｕｔｈ）に変更する。第２状態は、図４を示すように、ＰＡＮＡにおける認証フェーズ（Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　Ｐｈａｓｅ）のうち、認証処理が開始されてから完了するまでの状態である。機器２との認証処理は、例えば、ＰＡＮＡによりサポートされるＥＡＰ（Ｅｘｔｅｎｓｉｂｌｅ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　Ｐｒｏｔｏｃｏｌ）等の認証プロトコルにより行われる

。
【００３６】
ステップＳ４において、認証処理部１０２は、ＰＡＲ（ｐ＋１）メッセージを機器２に送信する。ＰＡＲ（ｐ＋１）メッセージは、例えば、ＥＡＰペイロードデータとして、機器２のＩＤを要求するＩＤ要求、ノンス等を含む。
【００３７】
ステップＳ５において、認証処理部２０１は、ＰＡＲ（ｐ＋１）メッセージに応じて、ＰＡＮ（ｐ＋１）メッセージを機器制御装置１に送信する。ＰＡＮ（ｐ＋１）は、例えば、ＥＡＰペイロードデータとして、ＩＤ要求に対する応答である機器２のＩＤ、ノンス等を含む。
【００３８】
ステップＳ６－ステップＳ９において、機器制御装置１及び機器２は、例えば、ＥＡＰ－ＰＳＫ認証メソッドにより、認証処理を行う。機器制御装置１及び機器２が、公開鍵証明書の検証、共有鍵の生成等を行った後、機器制御装置１は、セッション鍵、グループ鍵、セッション有効期間等のセッション情報を生成する。
【００３９】
ステップＳ１０において、認証処理部１０２は、暗号化したセッション情報を含むＰＡＲ（ｐ＋４）メッセージを機器２に送信する。ステップＳ１１において、認証処理部２０１は、ＰＡＲ（ｐ＋４）メッセージに含まれるセッション情報を復号化して、認証処理が完了したことを示すＰＡＮ（ｐ＋４）メッセージを機器制御装置１に送信する。
【００４０】
通信Ｉ／Ｆ１１がＰＡＮ（ｐ＋４）メッセージを受信することにより、認証処理部１０２は、機器２との認証処理が成功したとして、認証処理を完了する。セッション管理部１０１は、認証処理が成功したことに応じて、図７に示すように、対応するレコードの認証状態を第３状態（Ａｃｃｅｓｓ）に変更する。第３状態は、図４を示すように、ＰＡＮＡにおけるアクセスフェーズ（Ａｃｃｅｓｓ　Ｐｈａｓｅ）に対応する。
【００４１】
ステップＳ１２において、暗号処理部１０３は、シーケンス番号更新通知等を含むメッセージを、セッション鍵を用いて暗号化し、機器２に送信する。ステップＳ１３において、暗号処理部２０２は、例えば、ＥＣＨＯＮＥＴ　Ｌｉｔｅ（登録商標）におけるインスタンスリスト通知を、セッション鍵を用いて暗号化し、機器制御装置１に送信する。
【００４２】
例えば、図８のシーケンス図に示すように、機器制御装置１が、認証処理前の状態（第１状態）において、機器２－１からの認証開始要求を複数回受信したとする。これは、例えば、機器制御装置１と機器２との間の電波状態が悪い場合や、機器２－１に成りすました不正機器３が認証開始要求を送信している場合に起こり得る。
【００４３】
図９に示すように、ＲＦＣ５６０９に規定の状態遷移では、図８のステップＳ１０１，Ｓ１０３，Ｓ１０５において送信された認証開始要求毎に、セッションＩＤが割り当てられ、セッション管理テーブルにおいて不要なレコードが増加してしまう。更に、図８のステップＳ１１０において、最後に送信された認証開始要求に対応する認証処理が完了した場合であっても、セッションＩＤ「１１」以外の、同一機器ＩＤのレコードが残留してしまい、リソースの不要な消費を招いてしまう。更に、これにより、正当な機器２から認証開始要求に応じた手続きを継続できなくなる可能性がある。
【００４４】
そこで、本実施の形態では、セッション管理部１０１が、セッション管理テーブル１２１において、機器ＩＤが認証開始要求を送信した機器２を示し、且つ、認証状態が第１状態であるレコードがある場合、セッションＩＤを更新する。
【００４５】
例えば、図８に示す例では、ステップＳ１０３において送信された認証開始要求を通信

Ｉ／Ｆ１１が受信する。このとき、図１０に示すように、セッション管理部１０１は、機器ＩＤが認証開始要求を送信した機器２－１を示し、且つ、認証状態が第１状態（ＰｒｅＡｕｔｈ）であるレコードを検索し、検索されたレコードのセッションＩＤ「９」を「１０」に更新する。

【００４６】

同様に、図８のステップＳ１０５において送信された認証開始要求を通信Ｉ／Ｆ１１が受信する。セッション管理部１０１は、機器ＩＤが認証開始要求を送信した機器２－１を示し、且つ、認証状態が第１状態（ＰｒｅＡｕｔｈ）であるレコードを検索し、検索されたレコードのセッションＩＤ「１０」を「１１」に更新する。

【００４７】

このように、本実施の形態に係る認証システムによれば、セッション管理部１０１が、通信Ｉ／Ｆ１１が受信した認証開始要求に応じて、セッション管理テーブル１２１を編集することにより、リソースの消費を低減し、堅牢性を向上することができる。

【００４８】

なお、図８のステップＳ１１０において通信Ｉ／Ｆ１１がＰＡＮ（ｐ＋４）メッセージを受信することにより、認証処理部１０２は、機器２との認証処理が成功したとして、認証処理を完了する。セッション管理部１０１は、認証処理が成功したことに応じて、図１１に示すように、対応するレコードの認証状態を第３状態（Ａｃｃｅｓｓ）に変更する。また、図８の他のステップの説明は、図６についての説明と実質的に同様であるため省略する。

【００４９】

（機器制御装置の動作）

図１２のフローチャートを用いて、機器制御装置１の、認証開始要求を受信してから認証処理が開始されるまでの動作の一例を説明する。

【００５０】

先ず、ステップＳ２１において、通信Ｉ／Ｆ１１は、機器２から送信された認証開始要求を受信する。セッション管理部１０１は、ステップＳ２１において受信された認証開始要求に含まれる機器ＩＤを取得する。

【００５１】

ステップＳ２２において、セッション管理部１０１は、セッション管理テーブル１２１において、取得した機器ＩＤを含むレコード、すなわち、ステップＳ２１において受信した認証開始要求に対応するレコードを検索する。

【００５２】

ステップＳ２３において、セッション管理部１０１は、取得した機器ＩＤが既にセッション管理テーブル１２１において記録されているか否かを判定する。セッション管理部１０１は、取得した機器ＩＤを含むレコードがある場合、ステップＳ２４に処理を進め、取得した機器ＩＤを含むレコードがない場合、ステップＳ２８に処理を進める。

【００５３】

ステップＳ２４において、セッション管理部１０１は、認証開始要求に対応するレコードの認証状態が、第３状態（Ａｃｃｅｓｓ）であるか否かを判定する。認証状態が第３状態である場合、ステップＳ２８に処理を進め、認証状態が第３状態でない場合、ステップＳ２５に処理を進める。

【００５４】

ステップＳ２５において、セッション管理部１０１は、認証開始要求に対応するレコードの認証状態が、第１状態（ＰｒｅＡｕｔｈ）であるか否かを判定する。認証状態が第１状態である場合、ステップＳ２６に処理を進め、認証状態が第１状態でない場合、ステップＳ２７に処理を進める。

【００５５】

ステップＳ２６において、セッション管理部１０１は、セッション管理テーブル１２１において、認証開始要求に対応するレコードのセッションＩＤを更新し、ステップＳ２９

に処理を進める。
【００５６】
ステップＳ２７において、セッション管理部１０１は、ステップＳ２１において受信された認証開始要求を破棄し、処理を終了する。
【００５７】
ステップＳ２８において、セッション管理部１０１は、認証開始要求に含まれる機器ＩＤと、認証状態である第１状態（ＰｒｅＡｕｔｈ）と、新たなセッションＩＤとを、新たなレコードとしてセッション管理テーブル１２１に追加する。
【００５８】
ステップＳ２９において、認証処理部１０２は、ステップＳ２１において受信された認証開始要求を受け入れて、認証処理を開始する。
【００５９】
図１３のフローチャートを用いて、機器制御装置１の、認証処理が完了時の動作の一例を説明する。
【００６０】
ステップＳ３１において、通信Ｉ／Ｆ１１は、認証処理が成功した機器２から、認証が完了したことを示すＰＡＮ（ｐ＋４）メッセージ（認証完了メッセージ）を受信する。
【００６１】
ステップＳ３２において、セッション管理部１０１は、セッション管理テーブル１２１において、認証開始要求に含まれる機器ＩＤを含むレコード、すなわち、認証開始要求に対応するレコードを検索する。
【００６２】
ステップＳ３３において、セッション管理部１０１は、セッション管理テーブル１２１において、認証開始要求に対応するレコードが複数あるか否かを判定する。複数のレコードがある場合、ステップＳ３４に処理を進め、複数のレコードがない場合、ステップＳ３５に処理を進める。
【００６３】
ステップＳ３４において、セッション管理部１０１は、認証開始要求に対応する複数のレコードのうち、認証状態が第２状態（Ａｕｔｈ）以外のレコードを、１つのみ残すように削除する。
【００６４】
ステップＳ３５において、セッション管理部１０１は、セッション管理テーブル１２１において、認証開始要求に対応するレコードの認証状態を第３状態（Ａｃｃｅｓｓ）に変更し、処理を終了する。
【００６５】
（認証システムの他の動作例）
図１４のシーケンス図を用いて、既に認証処理が成功し、機器制御装置１に登録されている機器２－１及び２－２のうち、機器２－１が再起動する場合の認証システムの動作例を説明する。
【００６６】
ステップＳ２０１において、暗号処理部１０３は、例えば、グループ鍵を用いて暗号されたメッセージをマルチキャスト送信する。この状態（第３状態）で、ステップＳ２０２において、機器２－１は、電源遮断等により、再起動する。
【００６７】
ステップＳ２０３において、機器２－１の認証処理部２０１は、例えばユーザの操作に応じて、認証開始要求を機器制御装置１に送信する。機器制御装置１の通信Ｉ／Ｆ１１は、機器２から送信された認証開始要求を受信する。
【００６８】
セッション管理部１０１は、認証開始要求の受信に応じて、セッション管理テーブル１２１において、認証開始要求に含まれる機器ＩＤを検索する。機器２－１は既に登録済み

のため、認証開始要求に含まれる機器ＩＤを含むレコードの認証状態は、第３状態（Ａｃｃｅｓｓ）である。よって、セッション管理部１０１は、図１５に示すように、機器ＩＤ「２－１」と、認証状態である第１状態（ＰｒｅＡｕｔｈ）と、新たなセッションＩＤ「１０」とを、新たなレコードとしてセッション管理テーブル１２１に追加する。

【００６９】

ステップＳ２０８において、認証処理部２０１は、認証処理が完了したことを示すＰＡＮ（ｐ＋４）メッセージを機器制御装置１に送信する。この時点で、図１５に示すように、セッション管理テーブル１２１において、認証開始要求に対応する２つのレコードがある。

【００７０】

図１６に示すように、セッション管理部１０１は、認証開始要求に対応する複数のレコードのうち、認証状態が第２状態（Ａｕｔｈ）以外のレコードを、１つのみ残すように削除する。また、セッション管理部１０１は、セッション管理テーブル１２１において、認証開始要求に対応するレコードの認証状態を第３状態（Ａｃｃｅｓｓ）に変更し、処理を終了する。

【００７１】

本実施の形態に係る認証システムによれば、認証開始要求に応じて、セッション管理テーブル１２１において、機器ＩＤが認証開始要求を送信した機器２を示し、且つ、認証状態が第１状態であるレコードがある場合、セッションＩＤが更新される。よって、機器制御装置１は、同一の機器ＩＤを含む複数の認証開始要求を受信する場合であっても、認証開始要求に応じて、セッション管理テーブル１２１を編集することにより、リソースの消費を低減し、堅牢性を向上することができる。更に、記憶域を従来構成と比べて削減することができるため、製造コストを低減することができる。

【００７２】

例えば、機器制御装置１、機器２等の認証機能が組み込まれた通信機器においては、一般的に記憶装置の記憶域が制限される。機器制御装置１の記憶域が不足すると、セッション管理テーブル１２１において新たなレコードを追加できず、認証処理が適正に行われない可能性がある。本実施の形態に認証システムによれば、記憶域が制限される場合であっても、認証開始要求に応じて、セッション管理テーブル１２１を編集することにより、リソースの消費を低減し、堅牢性を向上することができる。

【００７３】

また、本実施の形態に係るに認証システムによれば、セッション管理テーブル１２１において、機器ＩＤが認証開始要求を送信した機器２を示し、且つ、認証状態が第１状態であるレコードがある場合、認証開始要求を受け入れ、認証処理の開始を許可する。これにより、同一の機器ＩＤを含む複数の認証開始要求を受信する場合であっても、セッション管理テーブル１２１において第１状態のレコードが追加されることがなくなり、リソースの消費を低減し、堅牢性を向上することができる。

【００７４】

また、本実施の形態に係るに認証システムによれば、セッション管理テーブル１２１において、機器ＩＤが認証開始要求を送信した機器２を示し、且つ、認証状態が第２状態であるレコードがある場合、認証開始要求を破棄し、認証処理の開始を禁止する。これにより、不正な機器から送信された認証開始要求を受信する場合であっても、機器２との認証処理が中断されず、リソースの消費を低減し、堅牢性を向上することができる。

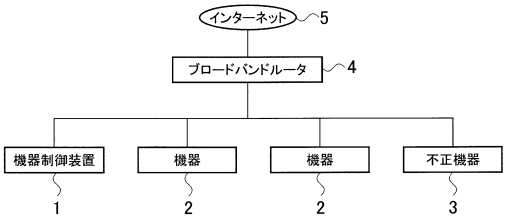
【００７５】

また、本実施の形態に係るに認証システムによれば、セッション管理テーブル１２１において、機器ＩＤが認証開始要求を送信した機器２を示し、且つ、認証状態が第３状態であるレコードがある場合、認証開始要求を受け入れ、認証処理の開始を許可する。これにより、登録済みの機器２が再起動される場合であっても、速やかに復帰することができる。

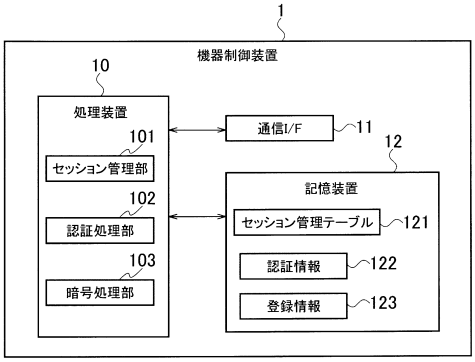
【００７６】

（その他の実施の形態）
上記のように、実施の形態を記載したが、この開示の一部をなす論述及び図面は本発明を限定するものであると理解すべきではない。この開示から当業者には様々な代替実施の形態、実施例及び運用技術が明らかとなろう。
【００７７】
例えば、既に述べた実施の形態において、ＰＡＮＡにおける再認証フェーズ（Ｒｅ－Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　Ｐｈａｓｅ）（図４参照）は、認証フェーズと同様に、第２状態として扱うことができる。再認証フェーズは、セッション有効期間延長のためにセッション情報の更新をするフェーズである。
【００７８】
また、既に述べた実施の形態において、機器制御装置１及び機器２を構成する処理装置や記憶装置は、その論理構造により、単一のハードウェアに記憶されてもよく、別個のハードウェアに記憶されてもよい。
【００７９】
上記の他、上記の実施の形態において説明される各構成を任意に応用した構成等、本発明はここでは記載していない様々な実施の形態等を含むことは勿論である。したがって、本発明の技術的範囲は上記の説明から妥当な特許請求の範囲に係る発明特定事項によってのみ定められるものである。
【符号の説明】
【００８０】
１　機器制御装置（認証装置）
２，２－１，２－２　機器
１０，２０　処理装置
１１，２１　通信インターフェース（Ｉ／Ｆ）
１２，２２　記憶装置
１０１　セッション管理部
１２１　セッション管理テーブル

【図１】



【図２】



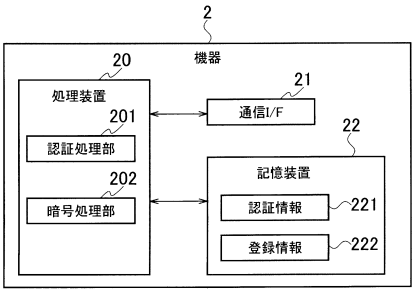
【図３】

セッション管理テーブル			121
機器ID	認証状態	セッションID	
2-1	PreAuth	9	
2-2	Access	8	

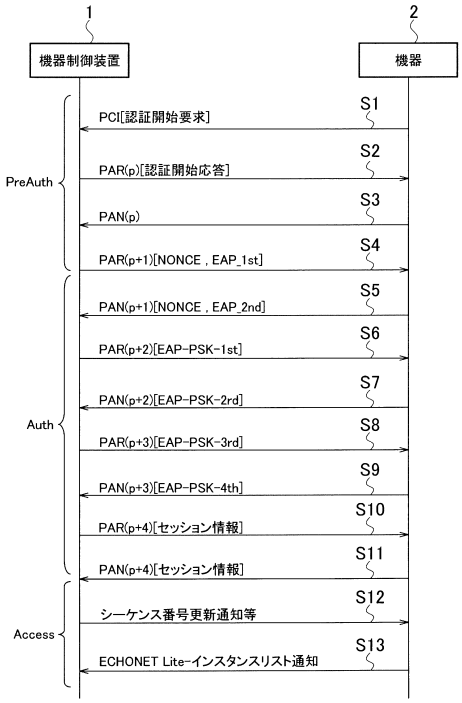
【図４】

認証状態	説明	PANAにおけるフェーズ	同一機器IDからの認証開始要求
PreAuth	認証開始要求から認証処理前の状態	Authentication Phase (PCI～PAR[EAP_1st])	受入
Auth	認証処理中の状態	Authentication Phase (PAR[EAP_1st]～PAN[C-bit])	拒否
Access	暗号通信可能な状態	Access Phase (PAN[C-bit]～PAR[A-bit])	受入
ReAuth	鍵更新処理中の状態	Re-authentication phase (PAR[A-bit]～PAN[C-bit])	拒否

【図５】



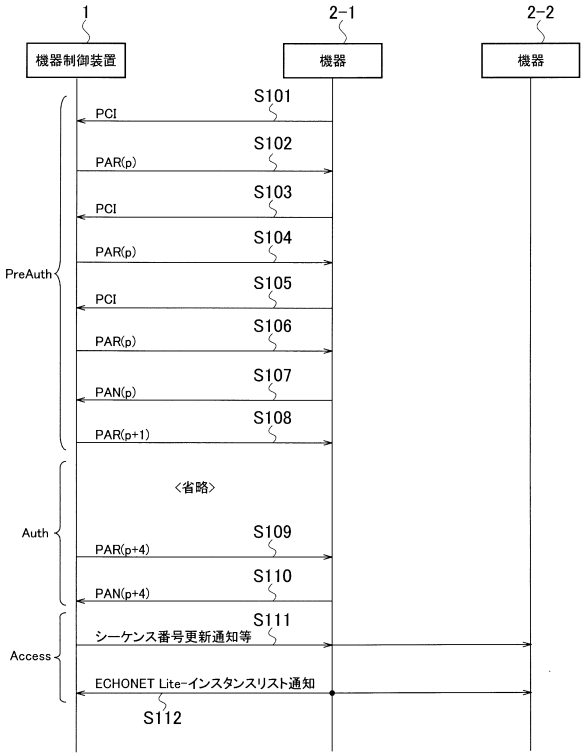
【図６】



【図７】

セッション管理テーブル			121
機器ID	認証状態	セッションID	
2-1	Access	9	
2-2	Access	8	

【図８】



【図９】

セッション管理テーブル	
機器ID	セッションID
2-1	9
2-2	8
2-1	10
2-1	11

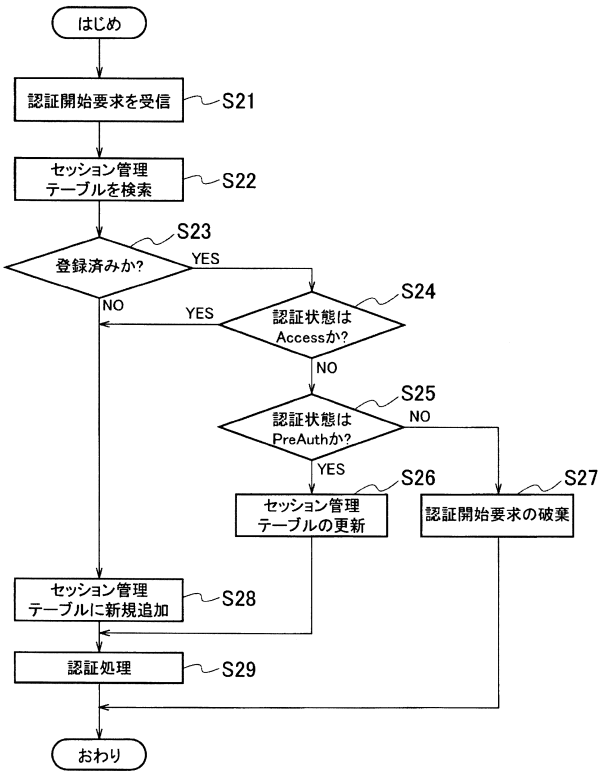
【図１０】

セッション管理テーブル			121
機器ID	認証状態	セッションID	
2-1	PreAuth	9→10→11	
2-2	Access	8	

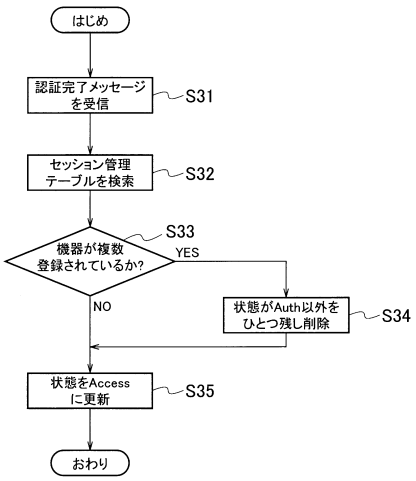
【図１１】

セッション管理テーブル			121
機器ID	認証状態	セッションID	
2-1	Access	11	
2-2	Access	8	

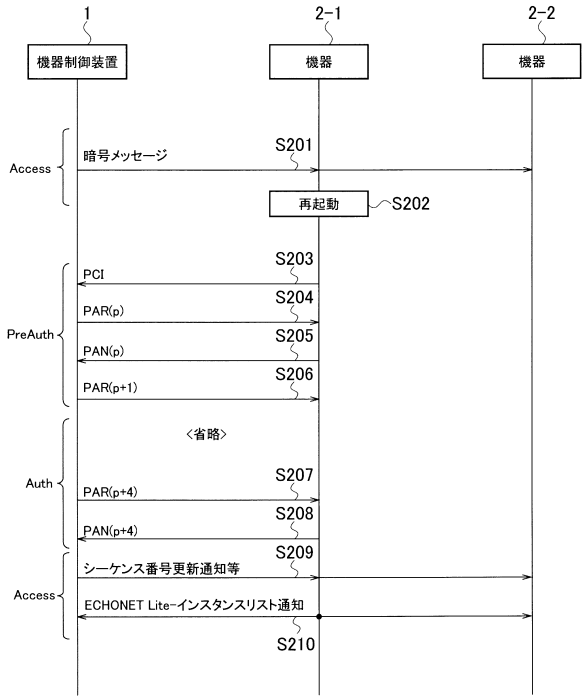
【図１２】



【図１３】



【図１４】



【図１５】

セッション管理テーブル 121

機器ID	認証状態	セッションID
2-1	Access	9
2-2	Access	8
2-1	PreAuth	10

【図１６】

セッション管理テーブル 121

機器ID	認証状態	セッションID
~~2-1~~	~~Access~~	~~9~~
2-2	Access	8
2-1	Access	10

フロントページの続き

審査官　宮司　卓佳

(56)参考文献　特開２０１１－０１００４５（ＪＰ，Ａ）
特開２０１１－２１１３０７（ＪＰ，Ａ）
特表２０１４－５１８０２２（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／４４
Ｇ０６Ｆ　１５／００
Ｈ０４Ｌ　９／０８
Ｈ０４Ｌ　９／３２