(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2018-525947
(P2018-525947A)
(43)公表日　平成30年9月6日(2018.9.6)

(51)Int.Cl.			F I			テーマコード（参考）
H04L	9/08	(2006.01)	H04L	9/00	601B	5J104
H04L	9/16	(2006.01)	H04L	9/00	643	
G09C	1/00	(2006.01)	G09C	1/00	640E	
H04L	9/32	(2006.01)	H04L	9/00	673B	

審査請求 未請求　予備審査請求 未請求　（全 36 頁）

(21)出願番号　特願2018-510915 (P2018-510915)
(86)(22)出願日　平成28年8月18日 (2016.8.18)
(85)翻訳文提出日　平成30年4月4日 (2018.4.4)
(86)国際出願番号　PCT/CN2016/095858
(87)国際公開番号　WO2017/036310
(87)国際公開日　平成29年3月9日 (2017.3.9)
(31)優先権主張番号　201510549437.5
(32)優先日　平成27年8月31日 (2015.8.31)
(33)優先権主張国　中国 (CN)

(71)出願人　510330264
アリババ・グループ・ホールディング・リミテッド
ＡＬＩＢＡＢＡ　ＧＲＯＵＰ　ＨＯＬＤＩＮＧ　ＬＩＭＩＴＥＤ
英国領，ケイマン諸島，グランド・ケイマン，ジョージ・タウン，ワン・キャピタル・プレイス，フォース・フロア，ピー．オー．ボックス　８４７
(74)代理人　110001243
特許業務法人　谷・阿部特許事務所

最終頁に続く

(54)【発明の名称】確認情報更新方法及び装置

(57)【要約】
本開示は、情報確認方法及び装置を提供する。この方法は、スマート機器とバインドするための第１の要求メッセージを端末機器から受信することであって、第１の要求メッセージが、スマート機器のユニバーサル一意識別子（ＵＵＩＤ：ｕｎｉｖｅｒｓａｌｌｙ　ｕｎｉｑｕｅ　ｉｄｅｎｔｉｆｉｅｒ）を搬送する、該受信すること；ＵＵＩＤと端末機器のユーザ識別子とのバインディング関係を決定し、バインディング関係に対応するセッション乱数を生成すること；ならびにセッション乱数に基づいて、スマート機器の新規確認番号及び新規確認パスワードを生成することを含む。本開示の技術的解決策は、セッション中に確認情報の動的更新を実施することができ、したがって、更新中の確認情報の傍受の難易度が増す。

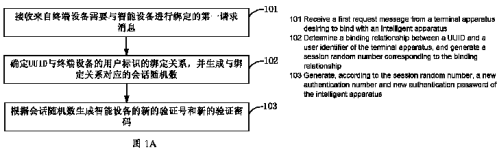


图 1A

【特許請求の範囲】
【請求項１】
サーバに適用される確認情報更新方法であって、
スマート機器とバインドするための第１の要求メッセージを端末機器から受信することであって、前記第１の要求メッセージが、前記スマート機器のユニバーサル一意識別子（ＵＵＩＤ：ｕｎｉｖｅｒｓａｌｌｙ　ｕｎｉｑｕｅ　ｉｄｅｎｔｉｆｉｅｒ）を搬送する、前記受信すること、
前記ＵＵＩＤと前記端末機器のユーザ識別子とのバインディング関係を決定し、前記バインディング関係に対応するセッション乱数を生成すること、ならびに
前記セッション乱数に基づいて、前記スマート機器の新規確認番号及び新規確認パスワードを生成すること
を含む、前記確認情報更新方法。
【請求項２】
前記セッション乱数を前記端末機器に返送して、それにより、前記端末機器が前記セッション乱数を前記スマート機器に転送した後、前記スマート機器は、前記セッション乱数に基づいて、前記スマート機器の新規確認番号及び新規確認パスワードを生成すること
をさらに含む、請求項１に記載の方法。
【請求項３】
前記セッション乱数に基づいて、前記スマート機器の前記新規確認番号及び前記新規確認パスワードを前記生成することが、
前記スマート機器の初期確認番号及び初期確認パスワードを決定すること、
前記初期確認番号及び前記セッション乱数に基づいて、前記スマート機器の前記新規確認番号を生成すること、ならびに
前記初期確認パスワード及び前記セッション乱数に基づいて、前記スマート機器の前記新規確認パスワードを生成すること
を含む、請求項１に記載の方法。
【請求項４】
前記サーバに登録するための第２の要求メッセージを前記スマート機器から受信することであって、前記第２の要求メッセージが、前記スマート機器のアイデンティティ情報及び前記スマート機器の第１の署名値を搬送する、前記受信すること、
前記アイデンティティ情報に対応する初期確認番号及び初期確認パスワードに基づいて、前記スマート機器の第２の署名値を計算すること、
前記第２の署名値が前記第１の署名値と同一である場合、前記ＵＵＩＤを前記スマート機器について生成すること、ならびに
前記ＵＵＩＤを前記スマート機器に返送すること
をさらに含む、請求項１に記載の方法。
【請求項５】
前記第１の署名値は、前記スマート機器が前記スマート機器の前記初期確認番号及び前記初期確認パスワードをランク付けし、文字列を形成した後、ハッシュアルゴリズムを前記文字列に適用する前記スマート機器によって計算される、請求項４に記載の方法。
【請求項６】
再設定するための通知メッセージを前記スマート機器から受信すること、ならびに
前記通知メッセージに基づいて、前記スマート機器の前記新規確認番号及び前記新規確認パスワードを消去すること
をさらに含む、請求項１から５のいずれかに記載の方法。
【請求項７】
端末装置に適用される確認情報更新方法であって、
スマート機器とバインドするための第１の要求メッセージをサーバに送信することであって、前記第１の要求メッセージが、前記スマート機器のユニバーサル一意識別子（ＵＵＩＤ：ｕｎｉｖｅｒｓａｌｌｙ　ｕｎｉｑｕｅ　ｉｄｅｎｔｉｆｉｅｒ）を搬送する、前

記送信すること、
前記第１の要求メッセージに基づいて、前記サーバによって生成されたセッション乱数を受信すること、ならびに
前記セッション乱数を前記スマート機器に送信して、それにより、前記スマート機器が、前記セッション乱数に基づいて、前記スマート機器の新規確認番号及び新規確認パスワードを生成すること
を含む、前記確認情報更新方法。
【請求項８】
前記スマート機器との接続を確立するための第３の要求メッセージを前記スマート機器に送信することであって、前記第３の要求メッセージが、ユーザアカウントを搬送する、前記送信すること、及び
前記スマート機器が前記ユーザアカウントを認証した後、前記第３の要求メッセージに基づいて、前記スマート機器によって返送された前記スマート機器の前記ＵＵＩＤを受信すること
をさらに含む、請求項７に記載の方法。
【請求項９】
前記セッション乱数を前記スマート機器に前記送信することが、
スマートアプリケーション及び前記スマート機器によって確立されたポイントツーポイント通信リンクを使用することによって、前記セッション乱数を前記スマート機器に送信すること、または
前記セッション乱数を前記端末機器のユーザインターフェースに表示して、それにより、前記スマート機器のユーザ入力モジュールが前記ユーザによって入力された前記セッション乱数を取得すること
を含む、請求項７に記載の方法。
【請求項１０】
再設定するための通知メッセージを前記スマート機器から受信すること、ならびに
前記通知メッセージに基づいて、前記スマート機器の前記ＵＵＩＤ及び前記セッション乱数を消去すること
をさらに含む、請求項７から９のいずれかに記載の方法。
【請求項１１】
スマート機器に適用される確認情報更新方法であって、
端末機器によって転送されたセッション乱数をサーバから受信すること、ならびに
前記セッション乱数に基づいて、前記スマート機器の新規確認番号及び新規確認パスワードを生成すること
を含む、前記確認情報更新方法。
【請求項１２】
前記サーバに登録するための第２の要求メッセージを前記サーバに送信することであって、前記第２の要求メッセージが、前記スマート機器のアイデンティティ情報、及び前記スマート機器の第１の署名値を搬送する、前記送信すること、ならびに
前記第２の要求メッセージに基づいて、前記サーバによって生成された前記スマート機器のユニバーサル一意識別子（ＵＵＩＤ：ｕｎｉｖｅｒｓａｌｌｙ　ｕｎｉｑｕｅ　ｉｄｅｎｔｉｆｉｅｒ）を受信すること
をさらに含む、請求項１１に記載の方法。
【請求項１３】
前記セッション乱数に基づいて、前記スマート機器の前記新規確認番号及び前記新規確認パスワードを前記生成することが、
前記スマート機器の初期確認番号及び初期確認パスワードを決定すること、
前記初期確認番号及び前記セッション乱数に基づいて、前記スマート機器の前記新規確認番号を生成すること、ならびに
前記初期確認パスワード及び前記セッション乱数に基づいて、前記スマート機器の前記

新規確認パスワードを生成すること
を含む、請求項１１に記載の方法。
【請求項１４】
再設定するためのボタンがトリガされたことが検出された後、通知メッセージを生成すること、ならびに
前記通知メッセージを前記端末機器及び前記サーバに送信して、それにより、前記サーバが、前記通知メッセージに基づいて、前記スマート機器の前記新規確認番号及び前記新規確認パスワードを消去し、前記端末機器が、前記通知メッセージに基づいて、前記スマート機器の前記ＵＵＩＤ及び前記セッション乱数を消去すること
をさらに含む、請求項１１から１３のいずれかに記載の方法。
【請求項１５】
サーバに適用される確認情報更新装置であって、
スマート機器とバインドするための第１の要求メッセージを端末機器から受信するように構成された第１の受信モジュールであって、前記第１の要求メッセージが、前記スマート機器のユニバーサル一意識別子（ＵＵＩＤ：ｕｎｉｖｅｒｓａｌｌｙ　ｕｎｉｑｕｅ　ｉｄｅｎｔｉｆｉｅｒ）を搬送する、前記第１の受信モジュール、
前記第１の受信モジュールによって受信された前記ＵＵＩＤと前記端末機器のユーザ識別子とのバインディング関係を決定し、前記バインディング関係に対応するセッション乱数を生成するように構成された第１の決定モジュール、ならびに
前記第１の決定モジュールによって決定された前記セッション乱数に基づいて、前記スマート機器の新規確認番号及び新規確認パスワードを生成するように構成された第１の生成モジュール
を備える、前記確認情報更新装置。
【請求項１６】
第１の送信モジュールであって、前記第１の決定モジュールによって決定された前記セッション乱数を前記端末機器に返送するように構成されて、それにより、前記端末機器が前記セッション乱数を前記スマート機器に転送した後、前記スマート機器は、前記セッション乱数に基づいて、前記スマート機器の新規確認番号及び新規確認パスワードを生成する、前記第１の送信モジュール
をさらに備える、請求項１５に記載の装置。
【請求項１７】
前記第１の生成モジュールが、
前記スマート機器の初期確認番号及び初期確認パスワードを決定するように構成された第１の決定ユニット、
前記第１の決定ユニットによって決定された前記初期確認番号、及び前記セッション乱数に基づいて、前記スマート機器の前記新規確認番号を生成するように構成された第１の生成ユニット、ならびに
前記第１の決定ユニットによって決定された前記初期確認パスワード、及び前記セッション乱数に基づいて、前記スマート機器の前記新規確認パスワードを生成するように構成された第２の生成ユニット
を備える、請求項１５に記載の装置。
【請求項１８】
前記サーバに登録するための第２の要求メッセージを前記スマート機器から受信するように構成された第２の受信モジュールであって、前記第２の要求メッセージが、前記スマート機器のアイデンティティ情報、及び前記スマート機器の第１の署名値を搬送する、前記第２の受信モジュール、
前記第２の受信モジュールによって受信された前記第２の要求メッセージにおいて搬送された前記アイデンティティ情報に対応する初期確認番号及び初期確認パスワードに基づいて、前記スマート機器の第２の署名値を計算するように構成された第１の計算モジュール、

前記第１の計算モジュールによって計算された前記第２の署名値が前記第１の署名値と同一である場合、前記ＵＵＩＤを前記スマート機器について生成するように構成された第２の生成モジュール、ならびに
前記第２の生成モジュールによって生成された前記ＵＵＩＤを前記スマート機器に返送するように構成された第２の送信モジュール
をさらに備える、請求項１５に記載の装置。
【請求項１９】
前記第１の署名値は、前記スマート機器が前記スマート機器の前記初期確認番号及び前記初期確認パスワードをランク付けし、文字列を形成した後、ハッシュアルゴリズムを使用する前記スマート機器によって計算される、請求項１８に記載の装置。
【請求項２０】
再設定するための通知メッセージを前記スマート機器から受信するように構成された第３の受信モジュール、ならびに、
前記第３の受信モジュールによって受信された前記通知メッセージに基づいて、前記スマート機器の前記新規確認番号及び前記新規確認パスワードを消去するように構成された第１の消去モジュール
をさらに備える、請求項１５から１９のいずれかに記載の装置。
【請求項２１】
端末機器に適用される確認情報更新装置であって、
スマート機器とバインドするための第１の要求メッセージをサーバに送信するように構成された第３の送信モジュールであって、前記第１の要求メッセージが、前記スマート機器のユニバーサル一意識別子（ＵＵＩＤ：ｕｎｉｖｅｒｓａｌｌｙ　ｕｎｉｑｕｅ　ｉｄｅｎｔｉｆｉｅｒ）を搬送する、前記第３の送信モジュール、
前記第３の送信モジュールによって送信された前記第１の要求メッセージに基づいて、前記サーバによって生成されたセッション乱数を受信するように構成された第４の受信モジュール、ならびに
第４の送信モジュールであって、前記第４の受信モジュールによって受信された前記セッション乱数を前記スマート機器に送信するように構成されて、それにより、前記スマート機器が、前記セッション乱数に基づいて、前記スマート機器の新規確認番号及び新規確認パスワードを生成する、前記第４の送信モジュール
を備える、前記確認情報更新装置。
【請求項２２】
前記スマート機器との接続を確立するための第３の要求メッセージを前記スマート機器に送信するように構成された第５の送信モジュールであって、前記第３の要求メッセージが、ユーザアカウントを搬送する、前記第５の送信モジュール、ならびに
前記スマート機器が、前記第５の送信モジュールによって送信された前記第３の要求メッセージにおいて搬送された前記ユーザアカウントを認証した後、前記第３の要求メッセージに基づいて、前記スマート機器によって返送された前記スマート機器の前記ＵＵＩＤを受信するように構成された第５の受信モジュール
をさらに備える、請求項２１に記載の装置。
【請求項２３】
前記第４の送信モジュールが、
スマートアプリケーションと前記スマート機器との間に確立されたポイントツーポイント通信リンクを使用することによって、前記セッション乱数を前記スマート機器に送信するように構成された送信ユニット、または
表示ユニットであって、前記端末機器のユーザインターフェースに前記セッション乱数を表示するように構成されて、それにより、前記スマート機器のユーザ入力モジュールが、前記ユーザによって入力された前記セッション乱数を取得するように入力する、前記表示ユニット
を備える、請求項２１に記載の装置。

【請求項２４】
再設定するための通知メッセージを前記スマート機器から受信するように構成された第６の受信モジュール、ならびに
前記第６の受信モジュールによって受信された前記通知メッセージに基づいて、前記スマート機器の前記ＵＵＩＤ及び前記セッション乱数を消去するように構成された第２の消去モジュール
をさらに備える、請求項２１または２３に記載の装置。
【請求項２５】
スマート機器に適用される確認情報更新装置であって、
端末機器によって転送されたセッション乱数をサーバから受信するように構成された第７の受信モジュール、ならびに
前記第７の受信モジュールによって受信された前記セッション乱数に基づいて、前記スマート機器の新規確認番号及び新規確認パスワードを生成するように構成された第３の生成モジュール
を備える、前記確認情報更新装置。
【請求項２６】
前記サーバに登録するための第２の要求メッセージを前記サーバに送信するように構成された第６の送信モジュールであって、前記第２の要求メッセージが、前記スマート機器のアイデンティティ情報及びスマート機器の第１の署名値を搬送する、前記第６の送信モジュール、ならびに
前記第２の要求メッセージに基づいて、前記サーバによって生成された前記スマート機器のユニバーサル一意識別子（ＵＵＩＤ：ｕｎｉｖｅｒｓａｌｌｙ　ｕｎｉｑｕｅ　ｉｄｅｎｔｉｆｉｅｒ）を受信するように構成された第８の受信モジュール
をさらに備える、請求項２５に記載の装置。
【請求項２７】
前記第３の生成モジュールが、
前記スマート機器の初期確認番号及び初期確認パスワードを決定するように構成された第２の決定ユニット、
前記第２の決定ユニットによって決定された前記初期確認番号、及び前記セッション乱数に基づいて、前記スマート機器の前記新規確認番号を生成するように構成された第３の生成ユニット、ならびに
前記第２の決定ユニットによって決定された前記初期確認パスワード、及び前記セッション乱数に基づいて、前記スマート機器の前記新規確認パスワードを生成するように構成された第４の生成ユニット
を備える、請求項２５に記載の装置。
【請求項２８】
再設定するためのボタンがトリガされたことが検出された後、通知メッセージを生成するように構成された第４の生成モジュール、ならびに
第７の送信モジュールであって、前記第４の生成モジュールによって生成された前記通知メッセージを前記端末機器及び前記サーバに送信するように構成されて、それにより、前記サーバが、前記通知メッセージに基づいて、前記スマート機器の前記新規確認番号及び前記新規確認パスワードを消去し、前記端末機器が、前記通知メッセージに基づいて、前記スマート機器の前記ＵＵＩＤ及び前記セッション乱数を消去する、前記第７の送信モジュール
をさらに備える、請求項２５から２７のいずれかに記載の装置。
【発明の詳細な説明】
【技術分野】
【０００１】
本開示は、ネットワークセキュリティ技術の分野に関し、より詳細には、確認情報更新方法及び装置に関する。

【背景技術】
【０００２】
スマートホームなどのインターネットオブシングスサービス、及びモバイル健康管理サービスをユーザに提供するためには、複数のスマート機器からの情報を収集する必要があり、この情報には、ユーザの宅内の温度計、湿度計、冷蔵庫、及び照明器具などの宅内機器情報、ならびに血圧、血糖値、心拍数、身長、及び体重などの個人健康情報を含めることができる。従来の技法においては、確認番号（鍵）及び確認パスワード（秘密）が、スマート機器ごとに管理プラットフォームによって割り当てられ、署名値が、その確認番号及び確認パスワードに基づいて計算され、スマート機器のアイデンティティが、管理プラットフォームにおいて、署名値に基づいて認証される。スマート機器が工場から出荷される前に、確認番号と確認パスワードがともに、予め設定され、同一の確認番号及び同一の確認パスワードが、同じタイプのスマート機器に割り当てられるとき、スマート機器は、マスカレードまたは攻撃され易く、したがって、提供されるセキュリティは低くなる。
【発明の概要】
【発明が解決しようとする課題】
【０００３】
上記に鑑みて、本開示は、新奇な技術的解決策を提供し、この解決策により、スマート機器の確認情報が動的に更新されて、更新中の確認情報の傍受の難易度が増す。
【課題を解決するための手段】
【０００４】
上記の目的を達成するために、本開示は、次の技術的解決策を提供する。
【０００５】
本開示の第１の態様によれば、サーバに適用される確認情報更新方法が提供され、この方法は、
スマート機器とバインドするための第１の要求メッセージを端末機器から受信することであって、第１の要求メッセージが、スマート機器のユニバーサル一意識別子（ＵＵＩＤ：ｕｎｉｖｅｒｓａｌｌｙ　ｕｎｉｑｕｅ　ｉｄｅｎｔｉｆｉｅｒ）を搬送する、該受信すること、
ＵＵＩＤと端末機器のユーザ識別子とのバインディング関係を決定し、バインディング関係に対応するセッション乱数を生成すること、ならびに
セッション乱数に基づいて、スマート機器の新規確認番号及び新規確認パスワードを生成すること
を含む。
【０００６】
本開示の第２の態様によれば、端末機器に適用される確認情報更新方法が提供され、この方法は、
スマート機器とバインドするための第１の要求メッセージをサーバに送信することであって、第１の要求メッセージが、スマート機器のＵＵＩＤを搬送する、該送信すること、
第１の要求メッセージに基づいて、サーバによって生成されたセッション乱数を受信すること、ならびに
セッション乱数をスマート機器に送信して、それにより、スマート機器が、セッション乱数に基づいて、スマート機器の新規確認番号及び新規確認パスワードを生成すること
を含む。
【０００７】
本開示の第３の態様によれば、スマート機器に適用される確認情報更新方法が提供され、この方法は、
端末機器によって転送されたセッション乱数をサーバから受信すること、ならびに
セッション乱数に基づいて、スマート機器の新規確認番号及び新規確認パスワードを生成すること
を含む。

【０００８】
本開示の第４の態様によれば、サーバに適用される確認情報更新装置が提供され、この装置は、
スマート機器とバインドするための第１の要求メッセージを端末機器から受信するように構成された第１の受信モジュールであって、第１の要求メッセージが、スマート機器のＵＵＩＤを搬送する、第１の受信モジュール、
第１の受信モジュールによって受信されたＵＵＩＤと端末機器のユーザ識別子とのバインディング関係を決定し、バインディング関係に対応するセッション乱数を生成するように構成された第１の決定モジュール、ならびに
第１の決定モジュールによって決定されたセッション乱数に基づいて、スマート機器の新規確認番号及び新規確認パスワードを生成するように構成された第１の生成モジュールを含む。
【０００９】
本開示の第５の態様によれば、端末機器に適用される確認情報更新装置が提供され、この装置は、
スマート機器とバインドするための第１の要求メッセージをサーバに送信するように構成された第３の送信モジュールであって、第１の要求メッセージが、スマート機器のＵＵＩＤを搬送する、第３の送信モジュール、
第３の送信モジュールによって送信された第１の要求メッセージに基づいて、サーバによって生成されたセッション乱数を受信するように構成された第４の受信モジュール、ならびに
第４の送信モジュールであって、第４の受信モジュールによって受信されたセッション乱数をスマート機器に送信するように構成されて、それにより、スマート機器が、セッション乱数に基づいて、スマート機器の新規確認番号及び新規確認パスワードを生成する、第４の送信モジュール
を含む。
【００１０】
本開示の第６の態様によれば、スマート機器に適用される確認情報更新装置が提供され、この装置は、
端末機器によって転送されたセッション乱数をサーバから受信するように構成された第７の受信モジュール、ならびに
第７の受信モジュールによって受信されたセッション乱数に基づいて、スマート機器の新規確認番号及び新規確認パスワードを生成するように構成された第３の生成モジュールを含む。
【発明の効果】
【００１１】
上記の技術的解決策からわかるように、本開示においては、端末機器が、導入され、セッション乱数が、スマート機器のＵＵＩＤと端末機器のユーザ識別子とのバインディング関係を使用することによって生成され、したがって、スマート機器の確認情報（本開示におけるスマート機器の確認番号及び確認パスワード）の動的更新が実施され、更新中の確認情報の傍受の難易度が増す。スマート機器とサーバの認証及び承認は、セッションにおける確認情報に基づいて実施され、それによって、システムのセキュリティが強化され、インターネットオブシングスにおけるスマート機器のマスカレードまたは攻撃が効果的に防止される。
【図面の簡単な説明】
【００１２】
【図１Ａ】本発明の第１の例示的な実施形態による確認情報更新方法の概略フローチャートである。
【図１Ｂ】本発明の第１の例示的な実施形態によるシナリオ図である。
【図２】本発明の第２の例示的な実施形態による確認情報更新方法の概略フローチャート

である。
【図３】本発明の第３の例示的な実施形態による確認情報更新方法の概略フローチャートである。
【図４】本発明の第４の例示的な実施形態による確認情報更新方法の概略フローチャートである。
【図５】本発明の第５の例示的な実施形態による確認情報更新方法の概略フローチャートである。
【図６】本発明の第６の例示的な実施形態による確認情報更新方法の概略フローチャートである。
【図７】本発明の第７の例示的な実施形態による確認情報更新方法の概略フローチャートである。
【図８】本発明の第８の例示的な実施形態による確認情報更新方法の概略フローチャートである。
【図９】本発明の一例示的な実施形態による確認情報更新方法のシグナル伝達図である。
【図１０】本開示の一例示的な実施形態によるサーバの概略構造図である。
【図１１】本開示の一例示的な実施形態による端末機器の概略構造図である。
【図１２】本開示の一例示的な実施形態によるスマート機器の概略構造図である。
【図１３】本発明の第１の例示的な実施形態による確認情報更新装置の概略構造図である。
【図１４】本発明の第２の例示的な実施形態による確認情報更新装置の概略構造図である。
【図１５】本発明の第３の例示的な実施形態による確認情報更新装置の概略構造図である。
【図１６】本発明の第４の例示的な実施形態による確認情報更新装置の概略構造図である。
【図１７】本発明の第５の例示的な実施形態による確認情報更新装置の概略構造図である。
【図１８】本発明の第６の例示的な実施形態による確認情報更新装置の概略構造図である。
【発明を実施するための形態】
【００１３】
例示的な実施形態を本明細書において詳細に説明し、例示的な実施形態を添付の図面において示している。添付の図面が関係する次の説明においては、異なる添付の図面の中の同じ数字は、特段の指定がない限り、同じまたは類似の要素を示す。次の例示的な実施形態において説明されている実施態様がすべて、本開示と一致する実施態様を表しているとは限らない。これに対して、それらは、別記の特許請求の範囲に詳細に説明されている本開示のいくつかの態様と一致する装置及び方法の単なる例にすぎない。
【００１４】
本開示に使用される用語は、本開示を限定するのではなく、ただ特定の実施形態を説明するのに使用されるにすぎない。本開示及び別記の特許請求の範囲に使用される単数形「１つの（ａ（ｎ））」、「前記（ｓａｉｄ）」、及び「その（ｔｈｅ）」はまた、他の意味が示されている文脈で明確に指定されない限り、複数形も含む。本明細書に使用される用語「及び／または（ａｎｄ／ｏｒ）」は、列挙された１つまたは複数の関連の項目の任意のあるいはすべての可能な組合せを示すこと、及び含むことをさらに理解すべきである。
【００１５】
「第１の（ｆｉｒｓｔ）」、「第２の（ｓｅｃｏｎｄ）」、及び「第３の（ｔｈｉｒｄ）」などの用語は、本開示における様々な種類の情報について説明するのに使用され得るが、これらの種類の情報は、これらの用語に限定すべきでないことを理解すべきである。これらの用語は、同じタイプの情報を互いと区別するためにただ使用されるにすぎない。

たとえば、本開示の範囲から逸脱することなく、第１の情報は、第２の情報とも称されることがあり、同様に、第２の情報は、第１の情報とも称されることがある。文脈に応じて、ここで使用される語「～の場合（ｉｆ）」は、「～のとき（ｗｈｅｎ）」、「～すると（ａｓ）」、または「決定に応答して（ｉｎ　ｒｅｓｐｏｎｓｅ　ｔｏ　ｔｈｅ　ｄｅｔｅｒｍｉｎａｔｉｏｎ）」と説明され得る。

【００１６】

本開示においては、端末機器が、導入され、セッション乱数が、スマート機器のＵＵＩＤと端末機器のユーザ識別子とのバインディング関係を使用することによって生成され、したがって、スマート機器の確認情報（本開示におけるスマート機器の確認番号及び確認パスワード）の動的更新が実施され、更新中の確認情報の傍受の難易度が増す。そのため、スマート機器とサーバの認証及び承認は、セッションにおける確認情報に基づいて実施され、したがって、システムのセキュリティが強化され、インターネットオブシングスにおけるスマート機器のマスカレードまたは攻撃が効果的に防止される。

【００１７】

次の諸実施形態は、本開示をさらに説明するために提供される。

【００１８】

図１Ａは、本発明の第１の例示的な実施形態による確認情報更新方法の概略フローチャートであり、図１Ｂは、本発明の第１の例示的な実施形態によるシナリオ図である。この実施形態は、サーバに適用され、図１Ａに示されているように、次のステップを含む。

【００１９】

ステップ１０１：端末機器から、スマート機器とバインドするための第１の要求メッセージが受信され、第１の要求メッセージは、スマート機器のＵＵＩＤを搬送する。

【００２０】

ステップ１０２：ＵＵＩＤと端末機器のユーザ識別子とのバインディング関係が決定され、バインディング関係に対応するセッション乱数が生成される。

【００２１】

ステップ１０３：セッション乱数に基づいて、スマート機器の新規確認番号及び新規確認パスワードが生成される。

【００２２】

ステップ１０１では、一例示的な実施形態においては、端末機器は、スマートフォン及びタブレットコンピュータなど、アプリケーション（ａｐｐ）またはソフトウェアがインストールされ得る機器とすることができる。スマート機器は、スマート冷蔵庫、スマートＴＶ、及びスマート温度計など、通信機能を有する機器とすることができる。一例示的な実施形態においては、第１の要求メッセージは、スマート機器のユニバーサル一意識別子（ＵＵＩＤ：Ｕｎｉｖｅｒｓａｌｌｙ　Ｕｎｉｑｕｅ　Ｉｄｅｎｔｉｆｉｅｒ）を搬送する、端末機器にインストールされたアプリケーションのユーザインターフェース上のボタンをトリガするユーザによって生成され得る。

【００２３】

ステップ１０２では、サーバへのスマート機器の登録中、スマート機器のＵＵＩＤが生成され得、スマート機器とユーザ識別子とのバインディング関係が記録され得る。したがって、バインディング関係を有するユーザ識別子のみが、スマート機器を管理する許可を得ることが決定され得る。一例示的な実施形態においては、セッション乱数（ｓｅｓｓｉｏｎ＿ｒａｎｄｏｍ）は、疑似ランダムアルゴリズムによって生成され得る。

【００２４】

ステップ１０３では、一例示的な実施形態においては、サーバは、セッション乱数、たとえば、

ｓｅｓｓｉｏｎ＿ｋｅｙ＝ｋｅｙ＋ｓｅｓｓｉｏｎ＿ｒａｎｄｏｍ、

ｓｅｓｓｉｏｎ＿Ｓｅｃｒｅｔ＝Ｈａｓｈ（ｓｅｃｒｅｔ＋ｓｅｓｓｉｏｎ＿ｒａｎｄｏｍ）

に基づいて、新規確認番号及び新規確認パスワードを計算することができ、

ただし、ｓｅｓｓｉｏｎ＿ｒａｎｄｏｍは、セッション乱数を示し、ｓｅｓｓｉｏｎ＿ｋｅｙは、新規確認番号を示し、ｓｅｓｓｉｏｎ＿Ｓｅｃｒｅｔは、新規確認パスワードを示し、ｋｅｙは、スマート機器の初期確認番号を示し、ｓｅｃｒｅｔは、初期確認パスワードを示す。

【００２５】

図１Ｂに示されているように、たとえば、一例示的な説明においては、スマート機器は、スマート冷蔵庫１１であり、端末機器は、スマートフォン１２であり、サーバ１３は、スマート冷蔵庫１１から機器データを取得し、スマートフォン１２上のアプリケーションを通じて、クエリ及び制御などのサービスをスマート冷蔵庫１１に提供する。サーバ１３がスマート冷蔵庫１１を認証する必要があるとき、サーバ１３は、スマート冷蔵庫１１の初期確認番号及び初期確認パスワードを生成する。スマート冷蔵庫１１がサーバ１３に登録する必要があるとき、新規確認番号及び新規確認パスワードが、上記のステップ１０１～ステップ１０３を使用することによって生成される。スマート冷蔵庫１１及びサーバ１３は、後続の認証手順においてその新規確認番号及び新規確認パスワードを使用することによってスマート冷蔵庫１１のアイデンティティを認証し、したがって、不正な機器によるスマート冷蔵庫１１のマスカレードまたは攻撃が防止される。

【００２６】

上記の説明からわかり得るように、本発明の例示的な実施形態においては、端末機器が、導入され、セッション乱数が、スマート機器のＵＵＩＤと端末機器のユーザ識別子とのバインディング関係を使用することによって生成され、したがって、スマート機器の確認情報（本開示におけるスマート機器の確認番号及び確認パスワード）の動的更新が実施され、更新中の確認情報の傍受の難易度が増す。そのため、スマート機器とサーバの認証及び承認は、セッションにおける確認情報に基づいて実施され、したがって、システムのセキュリティが強化され、インターネットオブシングスにおけるスマート機器のマスカレードまたは攻撃が効果的に防止される。その上、スマート機器のＵＵＩＤを取得した後、悪意あるユーザは、ＵＵＩＤが正当なユーザ識別子とバインドされているので、スマート機器をバインドすることができない。

【００２７】

図２は、本発明の第２の例示的な実施形態による確認情報更新方法の概略フローチャートである。この実施形態は、一例として、サーバ側においてセッション乱数の生成を行うことによる例示的な説明を行う。図２に示されているように、この方法は、次のステップを含む。

【００２８】

ステップ２０１：端末機器から、スマート機器とバインドするための第１の要求メッセージが受信され、第１の要求メッセージは、スマート機器のＵＵＩＤを搬送する。

【００２９】

ステップ２０２：ＵＵＩＤと端末機器のユーザ識別子とのバインディング関係が決定され、バインディング関係に対応するセッション乱数が生成される。

【００３０】

ステップ２０３：スマート機器の初期確認番号及び初期確認パスワードが決定される。

【００３１】

ステップ２０４：初期確認番号及びセッション乱数に基づいて、スマート機器の新規確認番号が生成される。

【００３２】

ステップ２０５：初期確認パスワード及びセッション乱数に基づいて、スマート機器の新規確認パスワードが生成される。

【００３３】

ステップ２０６：セッション乱数は、端末機器に返送されて、それにより、端末機器がセッション乱数をスマート機器に転送した後、スマート機器は、セッション乱数に基づいて、スマート機器の新規確認番号及び新規確認パスワードを生成する。

【００３４】
ステップ２０１～ステップ２０２については、上記のステップ１０１～ステップ１０２を参照することができ、これらについては、ここでは詳細に説明しない。
【００３５】
ステップ２０３では、一例示的な実施形態においては、サーバは、スマート機器が工場から出荷され、使用されるようになる前に、スマート機器のモデルごとに初期確認番号及び初期確認パスワード（鍵／秘密ペア）を予め割り当てることができる。割当ては、ハードウェア書込みなどの方式で、スマート機器について実施され得、したがって、サーバの操作と保守の複雑さが低減される。
【００３６】
ステップ２０４及びステップ２０５における新規確認番号及び新規確認パスワードの生成の説明については、図１Ａに示された例示的な実施形態の関連する説明を参照することができ、これらについては、ここでは詳細に説明しない。
【００３７】
ステップ２０６では、一例示的な実施形態においては、スマート機器は、上記のステップ２０４及びステップ２０５のものと同一の生成方法を使用することによって、セッション乱数に基づいて、スマート機器側において新規確認番号及び新規確認パスワードを生成することができる。したがって、同一の新規確認番号及び同一の新規確認パスワードが、スマート機器及びサーバによって別個に生成されることが保証され得、したがって、サーバが、新規確認番号及び新規確認パスワードを使用することによってスマート機器を確認することが容易になる。
【００３８】
この実施形態においては、端末機器は、セッション乱数をスマート機器に転送し、同一の新規確認番号及び同一の新規確認パスワードが、サーバ及びスマート機器によって生成されることが保証され得、したがって、サーバが、新規確認番号及び新規確認パスワードを使用することによってスマート機器を確認することが容易になる。ネットワークを介した新規確認番号及び新規確認パスワードの伝送が回避され、そのため、ネットワークを介した新規確認番号及び新規確認パスワードの漏出のリスクが低減される。
【００３９】
図３は、本発明の第３の例示的な実施形態による確認情報更新方法の概略フローチャートである。この実施形態は、一例として、スマート機器によってサーバからＵＵＩＤの取得を行うことによる例示的な説明を行う。図３に示されているように、この方法は、次のステップを含む。
【００４０】
ステップ３０１：スマート機器から、サーバに登録するための第２の要求メッセージが受信され、第２の要求メッセージは、スマート機器のアイデンティティ情報及びスマート機器の第１の署名値を搬送する。
【００４１】
ステップ３０２：アイデンティティ情報に対応する初期確認番号及び初期確認パスワードに基づいて、スマート機器の第２の署名値が計算される。
【００４２】
ステップ３０３：第２の署名値が第１の署名値と同一である場合、ＵＵＩＤがスマート機器について生成される。
【００４３】
ステップ３０４：ＵＵＩＤは、スマート機器に返送される。
【００４４】
ステップ３０１では、一例示的な実施形態においては、スマート機器のアイデンティティ情報は、スマート機器のＭＡＣ、スマート機器のモデル、スマート機器のチップアイデンティティ（ＩＤ：ｉｄｅｎｔｉｔｙ）、及びスマート機器の初期確認コードを含み得るが、これらに限定されない。一例示的な実施形態では、第１の署名値は、スマート機器が

スマート機器の初期確認番号及び初期確認パスワードをランク付けし、文字列を形成した後、ハッシュアルゴリズムを使用するスマート機器によって計算され得る。初期確認番号及び初期確認パスワードの関連する説明については、図２に示された例示的な実施形態を参照することができ、これらについては、ここでは詳細に説明しない。

【００４５】

ステップ３０２では、一例示的な実施形態においては、第２に署名値もまた、サーバがスマート機器の初期確認番号及び初期確認パスワードをランク付けし、文字列を形成した後、ハッシュアルゴリズムを使用するサーバによって計算され得る。

【００４６】

ステップ３０３では、スマート機器のＵＵＩＤは、ハッシュアルゴリズムを使用することによって生成され得る。スマート機器のＵＵＩＤが一意であることを保証され得る限り、本開示におけるＵＵＩＤを生成するための方法は限定されないことが、当業者には理解され得る。

【００４７】

ステップ３０４では、ＵＵＩＤは、スマート機器に返送され、それにより、スマート機器は、スマート機器と端末機器との後続の対話中、ＵＵＩＤを使用することによって認識され得、したがって、不正な機器によるスマート機器のマスカレードが防止される。

【００４８】

この実施形態においては、第２の署名値が第１の署名値と同一であるとき、一意識別子を有するＵＵＩＤが、スマート機器について生成される。したがって、サーバは、ＵＵＩＤを端末機器のユーザ識別子とバインドし、この２つのバインディング関係を確立することができる。そのため、悪意あるユーザがスマート機器のＵＵＩＤを取得した後、スマート機器はサーバに対してバインドされ得ず、したがって、不正なユーザがスマート機器を制御するのが防止され、悪意ある機器のスマート機器に対する登録攻撃が防止され、システムのセキュリティが向上する。

【００４９】

図４は、本発明の第４の例示的な実施形態による確認情報更新方法の概略フローチャートである。この実施形態は、一例として、スマート機器が再設定された後、サーバにおいてスマート機器の新規確認番号及び新規確認パスワードの消去を行うことによる例示的な説明を行う。

【００５０】

ステップ４０１：スマート機器から、再設定するための通知メッセージが受信される。

【００５１】

ステップ４０２：スマート機器の新規確認番号及び新規確認パスワードが通知メッセージに基づいて消去される。

【００５２】

ステップ４０１では、一例示的な実施形態においては、通知メッセージは、スマート機器が物理ボタンによって再設定された後、生成され得る。

【００５３】

ステップ４０２では、一例示的な実施形態においては、スマート機器の関連情報はすべて、消去され得る。

【００５４】

この実施形態においては、スマート機器の新規確認番号及び新規確認パスワードは、スマート機器が再設定された後に消去されて、それにより、サーバの記憶域が効果的に解放され得、新規確認番号及び新規確認パスワードは、他のスマート機器による不正な使用が防止され得る。

【００５５】

図５は、本発明の第５の例示的な実施形態による確認情報更新方法の概略フローチャートである。この実施形態は、端末機器に適用され得る。端末機器は、スマートフォン及びタブレットコンピュータなど、アプリケーション（ａｐｐ）またはソフトウェアがインス

トールされ得る機器とすることができる。図５に示されているように、この方法は、次のステップを含む。

【００５６】

ステップ５０１：スマート機器とバインドするための第１の要求メッセージがサーバに送信され、第１の要求メッセージは、スマート機器のＵＵＩＤを搬送する。

【００５７】

ステップ５０２：第１の要求メッセージに基づいて、サーバによって生成されたセッション乱数が受信される。

【００５８】

ステップ５０３：セッション乱数は、スマート機器に送信されて、それにより、スマート機器は、セッション乱数に基づいて、スマート機器の新規確認番号及び新規確認パスワードを生成する。

【００５９】

ステップ５０１におけるスマート機器及び第１の要求メッセージの関連する説明については、図１Ａに示された例示的な実施形態を参照することができ、これらについては、ここでは詳細に説明しない。

【００６０】

ステップ５０２におけるセッション乱数を生成する方法については、図１Ａに示された例示的な実施形態を参照することができ、これについては、ここでは詳細に説明しない。

【００６１】

ステップ５０３では、セッション乱数は、スマートアプリケーションとスマート機器との間に確立されたポイントツーポイント通信リンクを使用することによって、スマート機器に送信され、または、セッション乱数は、端末機器のユーザインターフェースに表示されて、それにより、スマート機器のユーザ入力モジュールは、ユーザによって入力されたセッション乱数を取得するように入力する。

【００６２】

上記の説明からわかり得るように、本発明の例示的な実施形態においては、サーバによって生成され、ＵＵＩＤと端末機器のユーザ識別子とのバインディング関係に対応するセッション乱数は、端末機器を通して取得され、セッション乱数は、スマート機器に送信されて、それにより、スマート機器は、セッション乱数に基づいて、スマート機器の新規確認番号及び新規確認パスワードを生成し、したがって、サードパーティを用いることによって確認情報（本開示におけるスマート機器の確認番号及び確認パスワード）の動的更新が実施され、更新中の確認情報の傍受の難易度が増す。そのため、スマート機器とサーバの認証及び承認は、セッションにおける確認情報に基づいて実施され、したがって、システムのセキュリティが強化され、インターネットオブシングスにおけるスマート機器のマスカレードまたは攻撃が効果的に防止される。

【００６３】

図６は、本発明の第６の例示的な実施形態による確認情報更新方法の概略フローチャートである。この実施形態は、一例として、サーバ側においてスマート機器のＵＵＩＤの生成を行うこと、ならびにスマート機器のＵＵＩＤ及びセッション乱数を再設定することによる例示的な説明を行う。図６に示されているように、この方法は、次のステップを含む。

【００６４】

ステップ６０１：スマート機器との接続を確立するための第３の要求メッセージがスマート機器に送信され、第３の要求メッセージは、ユーザアカウントを搬送する。

【００６５】

ステップ６０２：第３の要求メッセージに基づいて、スマート機器がユーザアカウントを認証した後、スマート機器によって返送されたスマート機器のＵＵＩＤが受信される。

【００６６】

ステップ６０３：スマート機器から、再設定するための通知メッセージが受信される。

【００６７】
ステップ６０４：スマート機器のＵＵＩＤ及びセッション乱数が通知メッセージに基づいて消去される。
【００６８】
ステップ６０１では、スマート機器を制御する必要があるとき、ユーザは、ユーザアカウント及びユーザパスワードを使用することによって、端末機器上のスマート機器を制御するためのアプリケーションにログインし、アプリケーションを使用することによって、スマート機器にスマート機器との接続を確立するための第３の要求メッセージを送信することができる。
【００６９】
ステップ６０２では、スマート機器は、ユーザアカウントを認証して、ユーザアカウントが正当なユーザであるかどうかを判定することができる。スマート機器のＵＵＩＤは、ユーザアカウントが正当なユーザである場合、スマート機器のＵＵＩＤを取得するために受信される。スマート機器は、ユーザアカウントが不正なユーザである場合、端末機器へのＵＵＩＤの返送を拒否する。
【００７０】
ステップ６０３及びステップ６０４では、スマート機器の関連情報はすべて、スマート機器が物理ボタンによって再設定された後に生成された通知メッセージを通じて消去され得る。
【００７１】
この実施形態においては、スマート機器のＵＵＩＤは、スマート機器から取得されて、それにより、ＵＵＩＤは、第１の要求メッセージにおいて搬送され得、次いで、サーバは、ＵＵＩＤと端末機器のユーザ識別子とのバインディング関係に対応するセッション乱数を生成し、セッション乱数をスマート機器に送信することができ、したがって、不正なユーザがスマート機器を制御するのが防止され、スマート機器に対する悪意ある機器の登録攻撃が防止され、システムのセキュリティが向上する。スマート機器の新規確認番号及び新規確認パスワードは、スマート機器が再設定された後に消去されて、それにより、サーバの記憶域が効果的に解放され得、新規確認番号及び新規確認パスワードは、他のスマート機器による不正な使用が防止され得る。
【００７２】
図７は、本発明の第７の例示的な実施形態による確認情報更新方法の概略フローチャートである。この実施形態は、スマート機器に適用され得る。スマート機器は、スマート冷蔵庫、スマートＴＶ、及びスマート温度計など、通信機能を有する機器とすることができる。図７に示されているように、この方法は、次のステップを含む。
【００７３】
ステップ７０１：端末機器によって転送されたセッション乱数をサーバから受信される。
【００７４】
ステップ７０２：セッション乱数に基づいて、スマート機器の新規確認番号及び新規確認パスワードが生成される。
【００７５】
一例示的な実施形態においては、セッション乱数を生成し、セッション乱数に基づいて、スマート機器の新規確認番号及び新規確認パスワードを生成する方法については、図１Ａに示された例示的な実施形態を参照することができ、これらについては、ここでは詳細に説明しない。
【００７６】
上記の説明からわかり得るように、本発明の例示的な実施形態においては、端末機器によって転送された、サーバからのセッション乱数が、受信され、スマート機器の新規確認番号及び新規確認パスワードは、セッション乱数に基づいて生成され、したがって、スマート機器の確認情報（本開示におけるスマート機器の確認番号及び確認パスワード）の動

的更新が実施され、更新中の確認情報の傍受の難易度が増す。

【００７７】

図８は、本発明の第８の例示的な実施形態による確認情報更新方法の概略フローチャートである。この実施形態は、一例として、スマート機器側においてセッション乱数の生成を行うことによる例示的な説明を行う。図８に示されているように、この方法は、次のステップを含む。

【００７８】

ステップ８０１：スマート機器の初期確認番号及び初期確認パスワードが決定される。

【００７９】

ステップ８０２：初期確認番号及びセッション乱数に基づいて、スマート機器の新規確認番号が生成される。

【００８０】

ステップ８０３：初期確認パスワード及びセッション乱数に基づいて、スマート機器の新規確認パスワードが生成される。

【００８１】

ステップ８０４：再設定するためのボタンがトリガされた後、通知メッセージが生成される。

【００８２】

ステップ８０５：通知メッセージは、端末機器及びサーバに送信されて、それにより、サーバは、通知メッセージに基づいて、スマート機器の新規確認番号及び新規確認パスワードを消去し、端末機器は、通知メッセージに基づいて、スマート機器のＵＵＩＤ及びセッション乱数を消去する。

【００８３】

ステップ８０１～ステップ８０３の説明については、図２に示された例示的な実施形態の関連する説明を参照することができ、これらについては、ここでは詳細に説明しない。ステップ８０４～ステップ８０５の説明については、図４に示された例示的な実施形態の関連する説明を参照することができ、これらについては、ここでは詳細に説明しない。

【００８４】

この実施形態においては、端末機器は、セッション乱数をスマート機器に転送し、同一の新規確認番号及び同一の新規確認パスワードが、サーバ及びスマート機器によって生成されることが保証され得、したがって、サーバが、新規確認番号及び新規確認パスワードを使用することによってスマート機器を確認することが容易になる。ネットワークを介した新規確認番号及び新規確認パスワードの伝送が回避され、そのため、ネットワークを介した新規確認番号及び新規確認パスワードの漏出のリスクが低減される。スマート機器の新規確認番号及び新規確認パスワードは、スマート機器が再設定された後に消去されて、それにより、サーバの記憶域が効果的に解放され得、新規確認番号及び新規確認パスワードは、他のスマート機器による不正な使用が防止され得る。

【００８５】

図９は、本発明の一例示的な実施形態による確認情報更新方法のシグナル伝達図である。サーバは、スマート機器が工場から出荷され、使用されるようになる前に、スマート機器のモデルごとに初期確認番号及び初期確認パスワード（鍵／秘密ペアとも称される）を予め割り当てる必要がある。割当ては、ハードウェア書込みの方式で、スマート機器ごとに実施され得る。図９に示されているように、この方法は、次のステップを含む。

【００８６】

ステップ９０１：スマート機器は、初期鍵／秘密ペアを使用して機器を登録するために、サーバに第２の要求メッセージを送信する。ここでは、第１の要求メッセージは、スマート機器のＭＡＣ、スマート機器のモデル、スマート機器のチップアイデンティティ（ＩＤ：ｉｄｅｎｔｉｔｙ）、及びスマート機器の初期確認コードを搬送することができる。第１の署名値は、スマート機器の初期確認番号及び初期確認パスワードが辞書順でランク付けされて、文字列が形成された後、ハッシュアルゴリズム（たとえば、ＭＤ５）を使用

することによって計算され得る。
【００８７】
ステップ９０２：第１の要求メッセージを受信した後、サーバは、初期鍵／秘密ペアを使用することによって、第２の署名値を計算し、第２の署名値が、受信した第１の署名値と同一である場合、確認は成功し、一意のＵＵＩＤがスマート機器について生成される。
【００８８】
ステップ９０３：サーバは、生成されたＵＵＩＤをスマート機器に返送する。
【００８９】
ステップ９０４：スマート機器は、ＵＵＩＤを受信し、次いで、ＵＵＩＤをスマート機器にローカルに記憶する。
【００９０】
ステップ９０５：端末機器は、スマート機器との通信接続を確立する。ここでは、端末機器のアプリケーションが、ユーザアカウント及びユーザパスワードを使用することによってログインされ得る。通信接続を確立するための要求が、アプリケーションを使用して、スマート機器に接続しスマート機器のＵＵＩＤを取得するために、スマート機器に送信される。
【００９１】
ステップ９０６：スマート機器は、ＵＵＩＤを端末機器に返送する。
【００９２】
ステップ９０７：端末機器は、スマート機器とバインドするための第１の要求メッセージをサーバに送信する。ここでは、第１の要求メッセージは、バインドされる予定のスマート機器のＵＵＩＤを搬送する。
【００９３】
ステップ９０８：サーバは、ユーザとスマート機器とのバインディング関係を記録し、セッション乱数（ｓｅｓｓｉｏｎ＿ｒａｎｄｏｍ）を生成する。
【００９４】
ステップ９０９：サーバは、セッション乱数を端末機器に返送する。
【００９５】
ステップ９１０：端末機器は、セッション乱数をスマート機器に転送する。ここでは、転送方法は、限定されるものではないが、次を含み得る：第一に、端末機器が、スマート機器とのポイントツーポイント通信リンクを確立することによって、直接、スマート機器にセッション乱数を送信する；第二に、スマート機器がユーザ入力モジュールを有する場合、端末機器は、受信したセッション乱数をユーザに対するアプリケーションのユーザインターフェースにおいて表示し、ユーザは、スマート機器上のユーザ入力モジュールを使用することによってセッション乱数をスマート機器に入力する。
【００９６】
ステップ９１１：スマート機器及びサーバは、同じ計算方法を使用することによって、セッション乱数に基づいて、新規確認番号及び新規確認パスワードを別個に計算する。
【００９７】
次いで、スマート機器のアイデンティティは、スマート機器が再設定されるまで、確認番号及び新規確認パスワードを使用することによって認証される。再設定後、スマート機器とサーバはともに、新規確認番号及び新規確認パスワードを消去することになる。
【００９８】
そのため、悪意ある機器の登録攻撃は、サーバにおいて防止され得る。悪意あるユーザは、スマート機器のＵＵＩＤを取得した後、スマート機器をバインドすることができず、したがって、システムのセキュリティが向上する。
【００９９】
上記の確認情報更新方法に対応して、本開示は、図１０に示されている本開示の一例示的な実施形態によるサーバの概略構造図をさらに提供する。図１１を参照すると、ハードウェアレベルにおいて、サーバは、プロセッサ、内部バス、ネットワークインターフェー

ス、メモリ、及び不揮発性メモリを含み、他のサービスが必要とするハードウェアをさらに含み得ることは確実である。プロセッサは、不揮発性メモリからメモリまで対応するコンピュータプログラムを読み取り、コンピュータプログラムを実行し、したがって、論理レベルにおける確認情報更新装置が形成される。ソフトウェア実施方式に加えて、本開示が、論理機器、またはソフトウェアとハードウェアとの組合せなど、他の実施方式を除外しないことは確実である。言い換えれば、次の処理手順は、限定されるものではないが、様々な論理ユニットによって行われ、また、ハードウェアまたは論理機器によっても行われ得る。

【０１００】

上記の確認情報更新方法に対応して、本開示は、図１１に示されている本開示の一例示的な実施形態による端末機器の概略構造図をさらに提供する。図１１を参照すると、ハードウェアレベルにおいては、端末機器は、プロセッサ、内部バス、ネットワークインターフェース、メモリ、及び不揮発性メモリを含み、他のサービスが必要とするハードウェアをさらに含み得ることは確実である。プロセッサは、不揮発性メモリからメモリまで対応するコンピュータプログラムを読み取り、コンピュータプログラムを実行し、したがって、論理レベルにおける確認情報更新装置が形成される。ソフトウェア実施方式に加えて、本開示が、論理機器、またはソフトウェアとハードウェアとの組合せなど、他の実施方式を除外しないことは確実である。言い換えれば、次の処理手順は、限定されるものではないが、様々な論理ユニットによって行われ、また、ハードウェアまたは論理機器によっても行われ得る。

【０１０１】

上記の確認情報更新方法に対応して、本開示は、図１２に示されている本開示の一例示的な実施形態によるスマート機器の概略構造図をさらに提供する。図１２を参照すると、ハードウェアレベルにおいては、スマート機器は、プロセッサ、内部バス、ネットワークインターフェース、メモリ、及び不揮発性メモリを含み、他のサービスが必要とするハードウェアをさらに含み得ることは確実である。プロセッサは、不揮発性メモリからメモリまで対応するコンピュータプログラムを読み取り、コンピュータプログラムを実行し、したがって、論理レベルにおける確認情報更新装置が形成される。ソフトウェア実施方式に加えて、本開示が、論理機器、またはソフトウェアとハードウェアとの組合せなど、他の実施方式を除外しないことは確実である。言い換えれば、次の処理手順は、限定されるものではないが、様々な論理ユニットによって行われ、また、ハードウェアまたは論理機器によっても行われ得る。

【０１０２】

図１３は、本発明の第１の例示的な実施形態による、サーバに適用され得る確認情報更新装置の概略構造図である。図１３に示されているように、確認情報更新装置は、第１の受信モジュール１３０１、第１の決定モジュール１３０２、及び第１の生成モジュール１３０３を含み得る。

【０１０３】

第１の受信モジュール１３０１は、スマート機器とバインドするための第１の要求メッセージを端末機器から受信するように構成され、第１の要求メッセージは、スマート機器のＵＵＩＤを搬送する。

【０１０４】

第１の決定モジュール１３０２は、第１の受信モジュール１３０１によって受信されたＵＵＩＤと端末機器のユーザ識別子とのバインディング関係を決定し、バインディング関係に対応するセッション乱数を生成するように構成されている。

【０１０５】

第１の生成モジュール１３０３は、第１の決定モジュール１３０２によって決定されたセッション乱数に基づいて、スマート機器の新規確認番号及び新規確認パスワードを生成するように構成されている。

【０１０６】

図１４は、本発明の第２の例示的な実施形態による確認情報更新装置の概略構造図である。図１４に示されているように、図１３に示された例示的な実施形態を基にして、確認情報更新装置は、

第１の送信モジュール１３０４であって、第１の決定モジュール１３０２によって決定されたセッション乱数を端末機器に返送するように構成されて、それにより、端末機器がセッション乱数をスマート機器に転送した後、スマート機器は、セッション乱数に基づいて、スマート機器の新規確認番号及び新規確認パスワードを生成する、第１の送信モジュール１３０４

をさらに含み得る。

【０１０７】

一例示的な実施形態においては、第１の生成モジュール１３０３は、

スマート機器の初期確認番号及び初期確認パスワードを決定するように構成された第１の決定ユニット１３０３１、

第１の決定ユニット１３０３１によって決定された初期確認番号、及びセッション乱数に基づいて、スマート機器の新規確認番号を生成するように構成された第１の生成ユニット１３０３２、ならびに

第１の決定ユニット１３０３１によって決定された初期確認パスワード、及びセッション乱数に基づいて、スマート機器の新規確認パスワードを生成するように構成された第２の生成ユニット１３０３３

を含み得る。

【０１０８】

一例示的な実施形態においては、この装置は、

サーバに登録するための第２の要求メッセージをスマート機器から受信するように構成された第２の受信モジュール１３０５であって、第２の要求メッセージが、スマート機器のアイデンティティ情報、及びスマート機器の第１の署名値を搬送する、第２の受信モジュール１３０５、

第２の受信モジュール１３０５によって受信された第２の要求メッセージにおいて搬送されたアイデンティティ情報に対応する初期確認番号及び初期確認パスワードに基づいて、スマート機器の第２の署名値を計算するように構成された第１の計算モジュール１３０６、

第１の計算モジュール１３０６によって計算された第２の署名値が第１の署名値と同一である場合、ＵＵＩＤをスマート機器について生成するように構成された第２の生成モジュール１３０７、ならびに

第２の生成モジュールによって生成されたＵＵＩＤをスマート機器に返送するように構成された第２の送信モジュール

をさらに含む。

【０１０９】

一例示的な実施形態においては、第１の署名値は、スマート機器がスマート機器の初期確認番号及びスマート機器の初期確認パスワードをランク付けし、文字列を形成した後、ハッシュアルゴリズムを使用するスマート機器によって計算され得る。

【０１１０】

一例示的な実施形態においては、この装置は、

再設定するための通知メッセージをスマート機器から受信するように構成された第３の受信モジュール１３０８、ならびに、

第３の受信モジュール１３０８によって受信された通知メッセージに基づいて、スマート機器の新規確認番号及び新規確認パスワードを消去するように構成された第１の消去モジュール１３０９

をさらに含むことができる。

【０１１１】

図１５は、本発明の第３の例示的な実施形態による、端末機器に適用され得る確認情報

更新装置の概略構造図である。図１５に示されているように、確認情報更新装置は、第３の送信モジュール１５０１、第４の受信モジュール１５０２、及び第４の送信モジュール１５０３を含むことができる。

【０１１２】

第３の送信モジュール１５０１は、スマート機器とバインドするための第１の要求メッセージをサーバに送信するように構成され、第１の要求メッセージは、スマート機器のＵＵＩＤを搬送する。

【０１１３】

第４の受信モジュール１５０２は、第３の送信モジュール１５０１によって送信された第１の要求メッセージに基づいて、サーバによって生成されたセッション乱数を受信するように構成されている。

【０１１４】

第４の送信モジュール１５０３は、第４の受信モジュール１５０２によって受信されたセッション乱数をスマート機器に送信するように構成されて、それにより、スマート機器は、セッション乱数に基づいて、スマート機器の新規確認番号及び新規確認パスワードを生成する。

【０１１５】

図１６は、本発明の第４の例示的な実施形態による確認情報更新装置の概略構造図である。図１６に示されているように、図１５に示された例示的な実施形態を基にして、確認情報更新装置は、

スマート機器との接続を確立するための第３の要求メッセージをスマート機器に送信するように構成された第５の送信モジュール１５０４であって、第３の要求メッセージが、ユーザアカウントを搬送する、第５の送信モジュール１５０４、ならびに

スマート機器が、第５の送信モジュール１５０４によって送信された第３の要求メッセージにおいて搬送されたユーザアカウントを認証した後、第３の要求メッセージに基づいて、スマート機器によって返送されたスマート機器のＵＵＩＤを受信するように構成された第５の受信モジュール１５０５

をさらに含む。

【０１１６】

一例示的な実施形態においては、第４の送信モジュール１５０３は、

スマートアプリケーションとスマート機器との間に確立されたポイントツーポイント通信リンクを使用することによって、セッション乱数をスマート機器に送信するように構成された送信ユニット１５０３１、または

表示ユニット１５０３２であって、端末機器のユーザインターフェースにセッション乱数を表示するように構成されて、それにより、スマート機器のユーザ入力モジュールが、ユーザによって入力されたセッション乱数を取得するように入力する、表示ユニット１５０３２

を含むことができる。

【０１１７】

一例示的な実施形態においては、確認情報更新装置は、

再設定するための通知メッセージをスマート機器から受信するように構成された第６の受信モジュール１５０６、ならびに

第６の受信モジュール１５０６によって受信された通知メッセージに基づいて、スマート機器のＵＵＩＤ及びセッション乱数を消去するように構成された第２の消去モジュール１５０７

をさらに含むことができる。

【０１１８】

図１７は、本発明の第５の例示的な実施形態による、スマート機器に適用され得る確認情報更新装置の概略構造図である。図１７に示されているように、確認情報更新装置は、第７の受信モジュール１７０１、及び第３の生成モジュール１７０２を含むことができる

。
【０１１９】
第７の受信モジュール１７０１は、端末機器によって転送されたセッション乱数をサーバから受信するように構成されている。
【０１２０】
第３の生成モジュール１７０２は、第７の受信モジュール１７０１によって受信されたセッション乱数に基づいて、スマート機器の新規確認番号及び新規確認パスワードを生成するように構成されている。
【０１２１】
図１８は、本発明の第６の例示的な実施形態による確認情報更新装置の概略構造図である。図１８に示されているように、図１７に示された例示的な実施形態を基にして、確認情報更新装置は、
サーバに登録するための第２の要求メッセージをサーバに送信するように構成された第６の送信モジュール１７０３であって、第２の要求メッセージが、スマート機器のアイデンティティ情報及びスマート機器の第１の署名値を搬送する、第６の送信モジュール１７０３、ならびに
第２の要求メッセージに基づいて、サーバによって生成されたスマート機器のＵＵＩＤを受信するように構成された第８の受信モジュール１７０４
をさらに含むことができる。
【０１２２】
一例示的な実施形態においては、第３の生成モジュール１７０２は、
スマート機器の初期確認番号及び初期確認パスワードを決定するように構成された第２の決定ユニット１７０２１、
第２の決定ユニット１７０２１によって決定された初期確認番号、及びセッション乱数に基づいて、スマート機器の新規確認番号を生成するように構成された第３の生成ユニット１７０２２、ならびに
第２の決定ユニット１７０２２によって決定された初期確認パスワード、及びセッション乱数に基づいて、スマート機器の新規確認パスワードを生成するように構成された第４の生成ユニット１７０２３
を含むことができる。
【０１２３】
一例示的な実施形態においては、確認情報更新装置は、
再設定するためのボタンがトリガされたことが検出された後、通知メッセージを生成するように構成された第４の生成モジュール１７０５；
第７の送信モジュール１７０６であって、第４の生成モジュール１７０５によって生成された通知メッセージを端末機器及びサーバに送信するように構成されて、それにより、サーバは、通知メッセージに基づいて、スマート機器の新規確認番号及び新規確認パスワードを消去し、端末機器は、通知メッセージに基づいて、スマート機器のＵＵＩＤ及びセッション乱数を消去する、第７の送信モジュール１７０６
をさらに含むことができる。
【０１２４】
上記の実施形態からわかり得るように、本開示においては、端末機器が、導入され、スマート機器の確認番号及び確認パスワードの動的更新と管理が、スマート機器とサーバとの間の対話機構を用いることによって実施され、したがって、サーバが、更新された確認番号及び確認パスワード（本開示における新規確認番号及び新規確認パスワード）を使用することによって、その後、スマート機器を認証及び承認し得ることが保証され、更新中の確認番号及び確認パスワードの傍受の難易度が増す。それと同時に、スマート機器は、インターネットオブシングスにおける他のスマート機器によるマスカレードまたは攻撃を効果的に防止され得、したがって、ステムのセキュリティがさらに向上する。
【０１２５】

本明細書を考慮し、ここに開示されている本発明を実践後、本開示の他の実施態様解決策を当業者は容易に得ることができる。本開示は、本開示のいずれの変形形態、使用法、または適応変更形態をカバーするように意図され、これらの変形形態、使用法、または適応変更形態は、本開示の一般的原理に従い、技術常識、または本開示に開示されていない本技術分野における従来の技術的手段を含む。本明細書及び諸実施形態は、単なる例示として見なされ、本開示の真の範囲及び趣旨は、次の特許請求の範囲によって定義される。

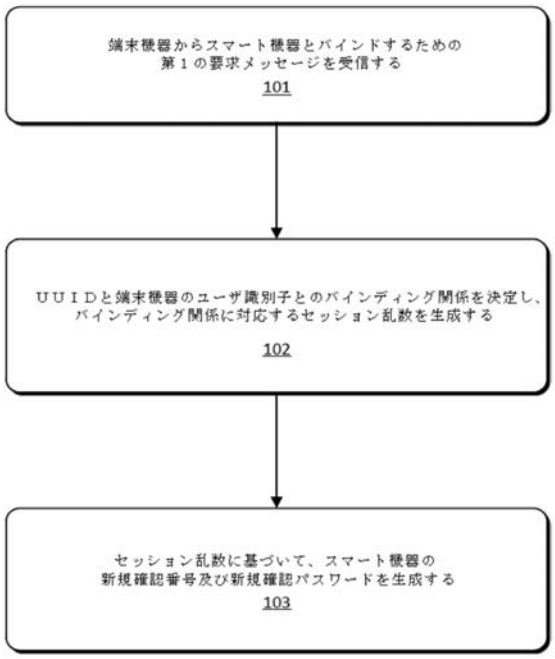
【０１２６】

「含む（ｉｎｃｌｕｄｅ）」、「備える（ｃｏｍｐｒｉｓｅ）」という用語、またはそれらの他の変形形態が、非排他的な包含をカバーするように意図され、それにより、一連の要素を含む工程、方法、商品、または機器が、それらの要素を含むだけでなく、明瞭に記載されていない他の要素も含み、あるいは工程、方法、商品、または機器の固有の要素をさらに含むことにさらに留意されたい。より多くの制限がなくても、「～を含む（ｉｎｃｌｕｄｉｎｇ　ａ／ａｎ．．．）によって定義される要素は、その要素を含む工程、方法、商品、または機器が他の同一の要素をさらに有することを排除しない。

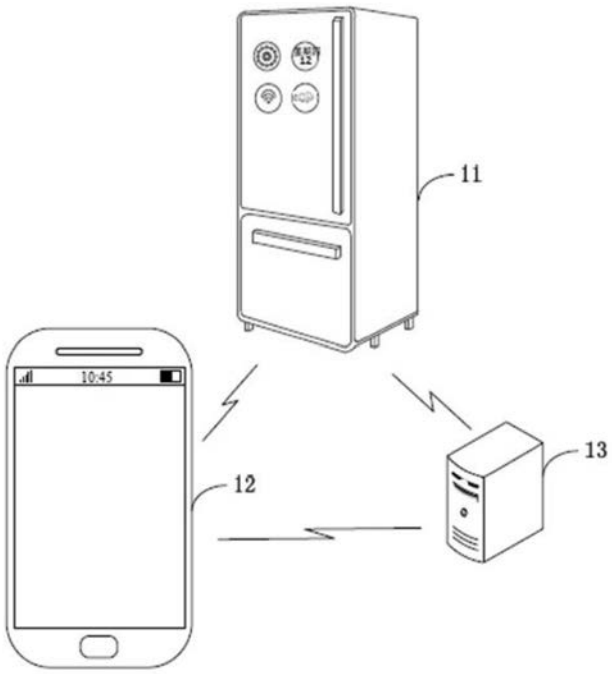
【０１２７】

上記の説明は、本開示の単なる好ましい実施形態にすぎず、本開示を限定するように意図するものではない。本開示の趣旨及び原理内で行われるいずれの修正も、等価な置換も、及び改良も、本開示の保護範囲に入るものとする。

【図１Ａ】



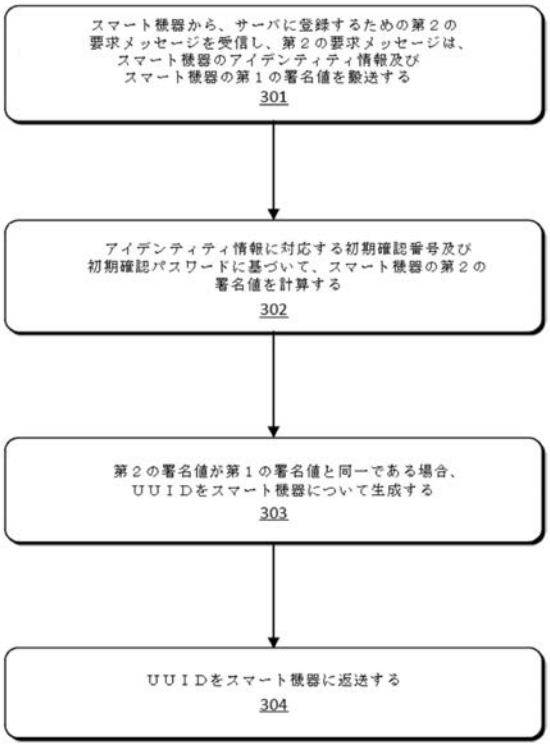
【図１Ｂ】



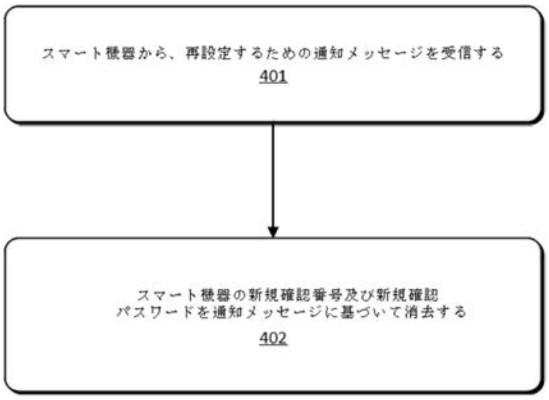
【図２】


端末機器から、スマート機器とバインドするための第１の要求メッセージを受信する
201
ＵＵＩＤと端末機器のユーザ識別子とのバインディング関係を決定し、バインディング関係に対応するセッション乱数を生成する
202
スマート機器の初期確認番号及び初期確認パスワードを決定する
203
初期確認番号及びセッション乱数に基づいて、スマート機器の新規確認番号を生成する
204
初期確認パスワード及びセッション乱数に基づいて、スマート機器の新規確認パスワードを生成する
205
セッション乱数を端末機器に返送して、それにより、端末機器がセッション乱数をスマート機器に転送した後、スマート機器は、セッション乱数に基づいて、スマート機器の新規確認番号及び新規確認パスワードを生成する
206

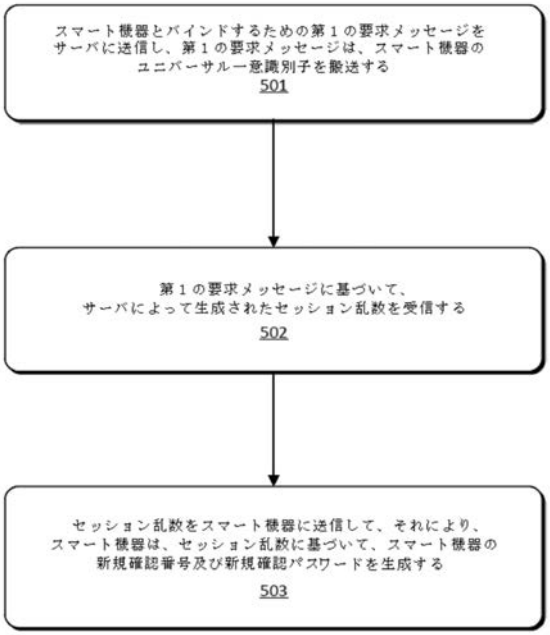
【図３】


スマート機器から、サーバに登録するための第２の要求メッセージを受信し、第２の要求メッセージは、スマート機器のアイデンティティ情報及びスマート機器の第１の署名値を搬送する
301
アイデンティティ情報に対応する初期確認番号及び初期確認パスワードに基づいて、スマート機器の第２の署名値を計算する
302
第２の署名値が第１の署名値と同一である場合、ＵＵＩＤをスマート機器について生成する
303
ＵＵＩＤをスマート機器に返送する
304

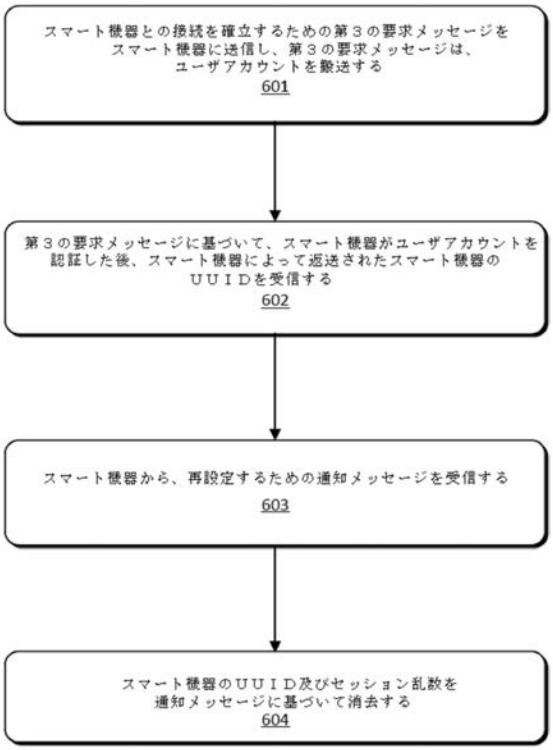
【図４】


スマート機器から、再設定するための通知メッセージを受信する
401
スマート機器の新規確認番号及び新規確認パスワードを通知メッセージに基づいて消去する
402

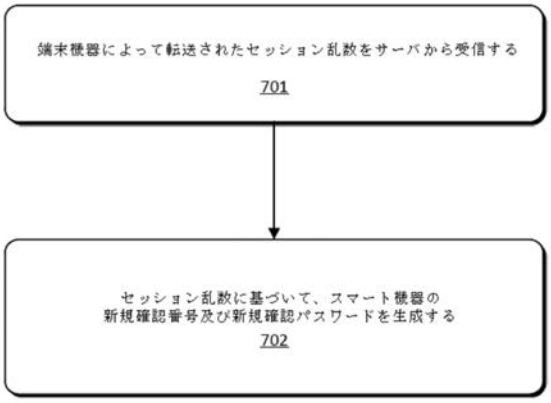
【図５】


スマート機器とバインドするための第１の要求メッセージをサーバに送信し、第１の要求メッセージは、スマート機器のユニバーサル一意識別子を搬送する
501
第１の要求メッセージに基づいて、サーバによって生成されたセッション乱数を受信する
502
セッション乱数をスマート機器に送信して、それにより、スマート機器は、セッション乱数に基づいて、スマート機器の新規確認番号及び新規確認パスワードを生成する
503

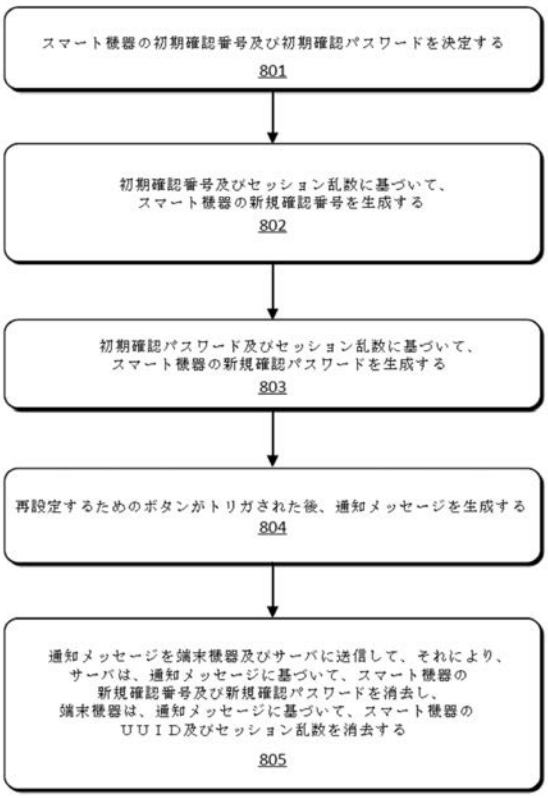
【図６】


スマート機器との接続を確立するための第３の要求メッセージを
スマート機器に送信し、第３の要求メッセージは、
ユーザアカウントを搬送する
601
第３の要求メッセージに基づいて、スマート機器がユーザアカウントを
認証した後、スマート機器によって返送されたスマート機器の
ＵＵＩＤを受信する
602
スマート機器から、再設定するための通知メッセージを受信する
603
スマート機器のＵＵＩＤ及びセッション乱数を
通知メッセージに基づいて消去する
604

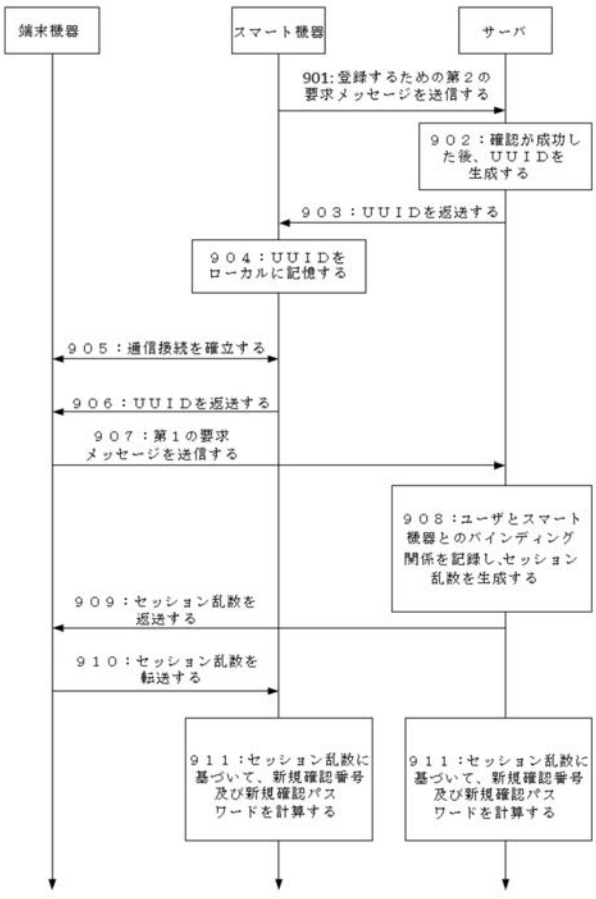
【図７】


端末機器によって転送されたセッション乱数をサーバから受信する
701
セッション乱数に基づいて、スマート機器の
新規確認番号及び新規確認パスワードを生成する
702

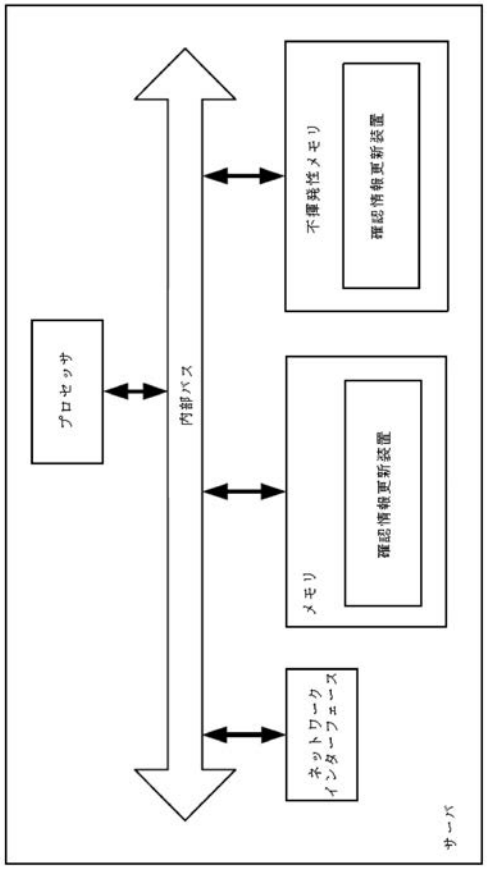
【図８】


スマート機器の初期確認番号及び初期確認パスワードを決定する
801
初期確認番号及びセッション乱数に基づいて、
スマート機器の新規確認番号を生成する
802
初期確認パスワード及びセッション乱数に基づいて、
スマート機器の新規確認パスワードを生成する
803
再設定するためのボタンがトリガされた後、通知メッセージを生成する
804
通知メッセージを端末機器及びサーバに送信して、それにより、
サーバは、通知メッセージに基づいて、スマート機器の
新規確認番号及び新規確認パスワードを消去し、
端末機器は、通知メッセージに基づいて、スマート機器の
ＵＵＩＤ及びセッション乱数を消去する
805

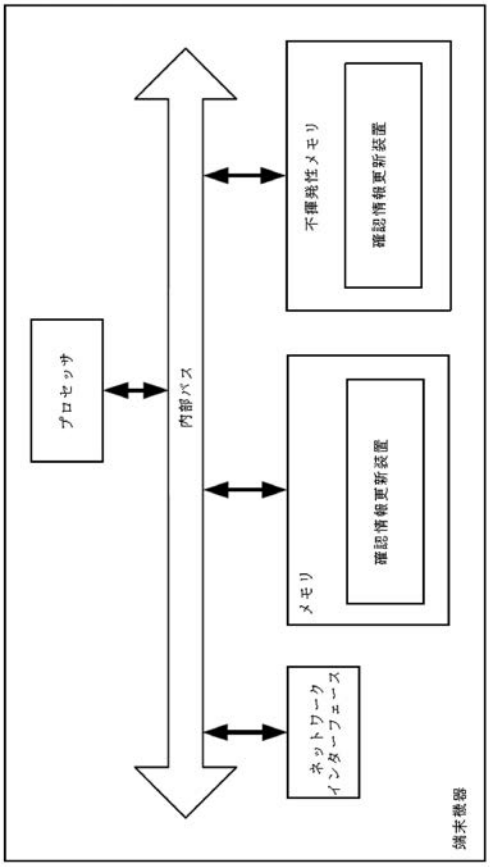
【図９】


端末機器
スマート機器
サーバ
901:登録するための第２の
要求メッセージを送信する
９０２：確認が成功し
た後、ＵＵＩＤを
生成する
９０３：ＵＵＩＤを返送する
９０４：ＵＵＩＤを
ローカルに記憶する
９０５：通信接続を確立する
９０６：ＵＵＩＤを返送する
９０７：第１の要求
メッセージを送信する
９０８：ユーザとスマート
機器とのバインディング
関係を記録し、セッション
乱数を生成する
９０９：セッション乱数を
返送する
９１０：セッション乱数を
転送する
９１１：セッション乱数に
基づいて、新規確認番号
及び新規確認パス
ワードを計算する
９１１：セッション乱数に
基づいて、新規確認番号
及び新規確認パス
ワードを計算する

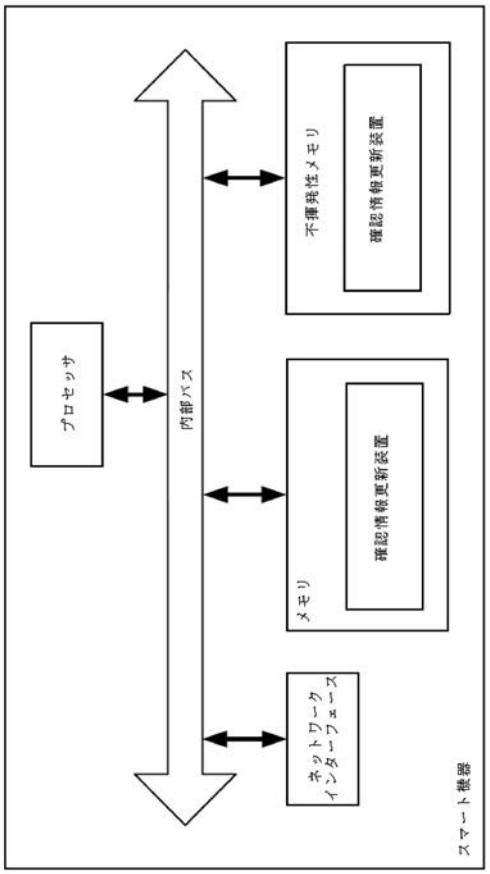
【図１０】



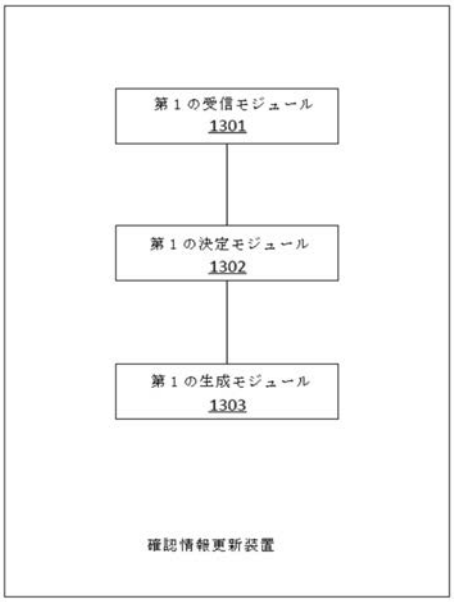
【図１１】



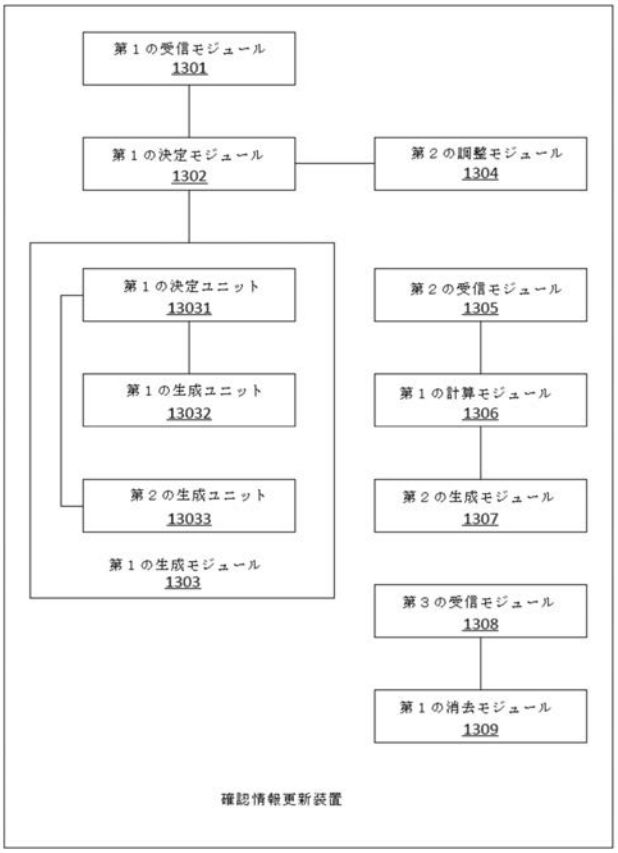
【図１２】



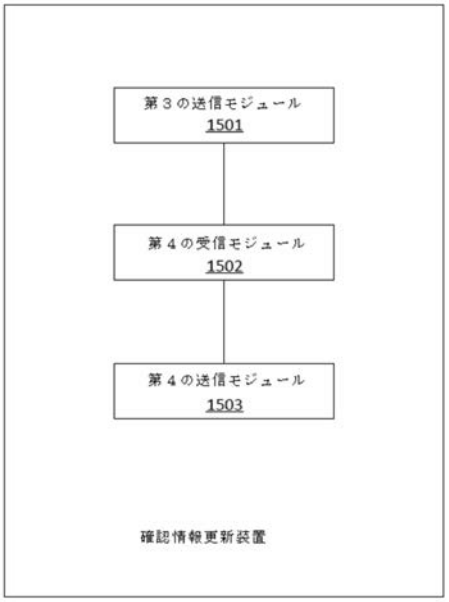
【図１３】



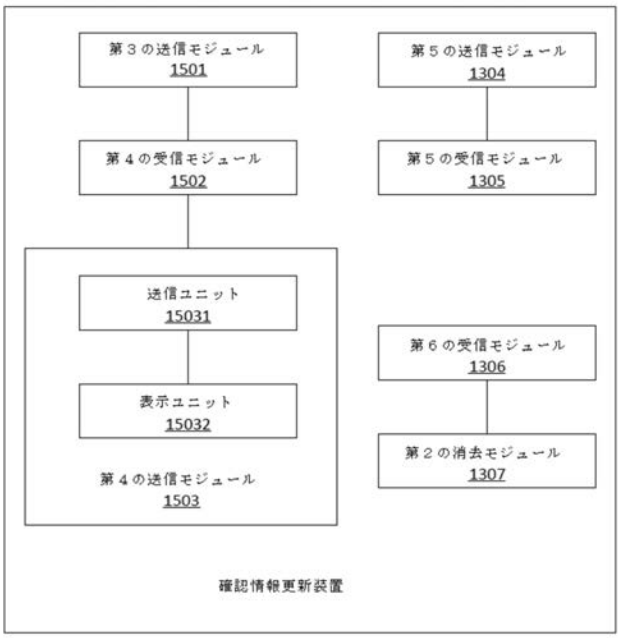
【図１４】



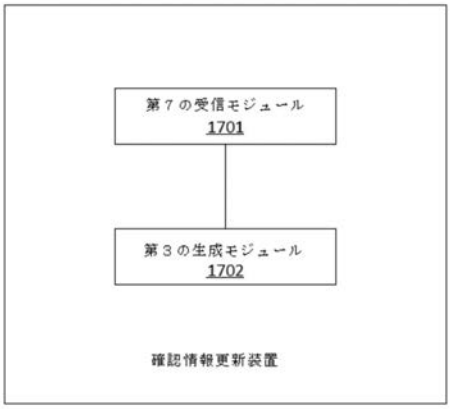
【図１５】



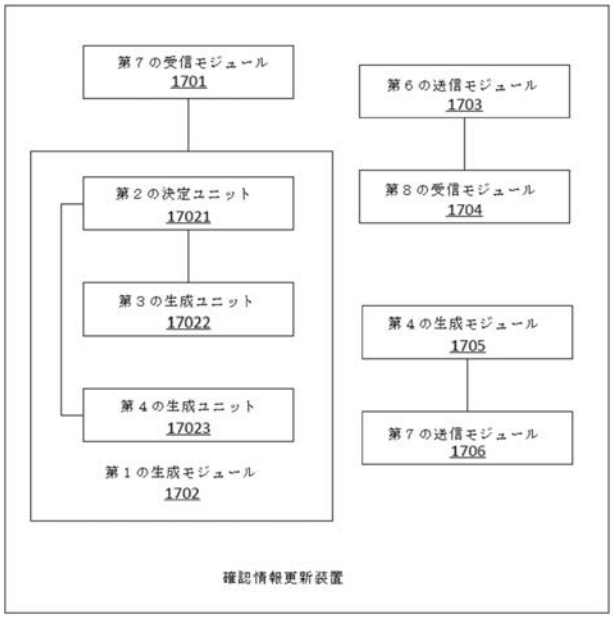
【図１６】



【図１７】



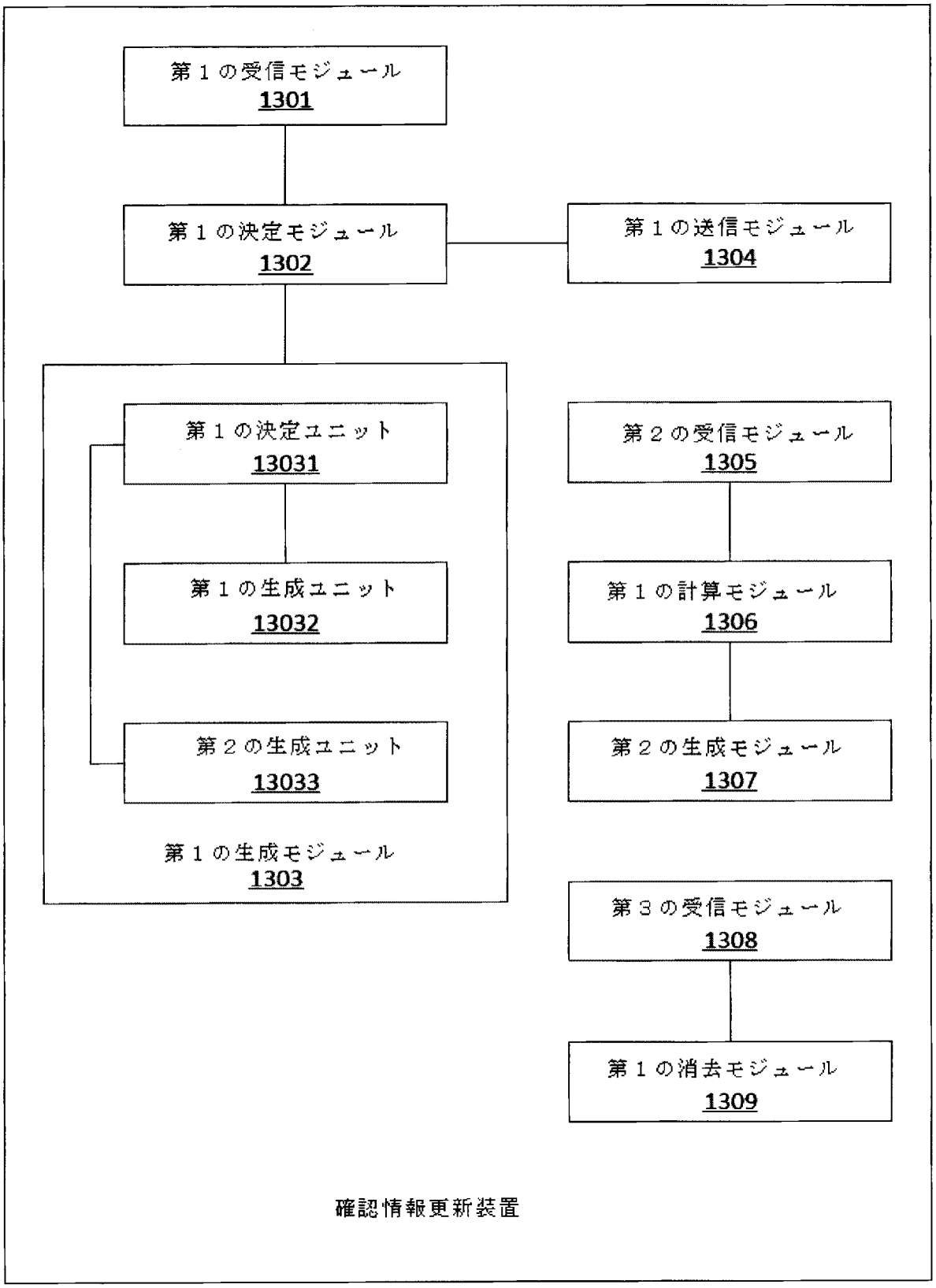
【図１８】



【手続補正書】
【提出日】平成30年7月4日(2018.7.4)
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】００８６
【補正方法】変更
【補正の内容】
【００８６】
ステップ９０１：スマート機器は、初期鍵／秘密ペアを使用して機器を登録するために、サーバに第２の要求メッセージを送信する。ここでは、第2の要求メッセージは、スマート機器のＭＡＣ、スマート機器のモデル、スマート機器のチップアイデンティティ（ＩＤ：ｉｄｅｎｔｉｔｙ）、及びスマート機器の初期確認コードを搬送することができる。第１の署名値は、スマート機器の初期確認番号及び初期確認パスワードが辞書順でランク付けされて、文字列が形成された後、ハッシュアルゴリズム（たとえば、ＭＤ５）を使用することによって計算され得る。
【手続補正２】
【補正対象書類名】明細書
【補正対象項目名】００８７
【補正方法】変更
【補正の内容】
【００８７】
ステップ９０２：第2の要求メッセージを受信した後、サーバは、初期鍵／秘密ペアを使用することによって、第２の署名値を計算し、第２の署名値が、受信した第１の署名値と同一である場合、確認は成功し、一意のＵＵＩＤがスマート機器について生成される。
【手続補正３】

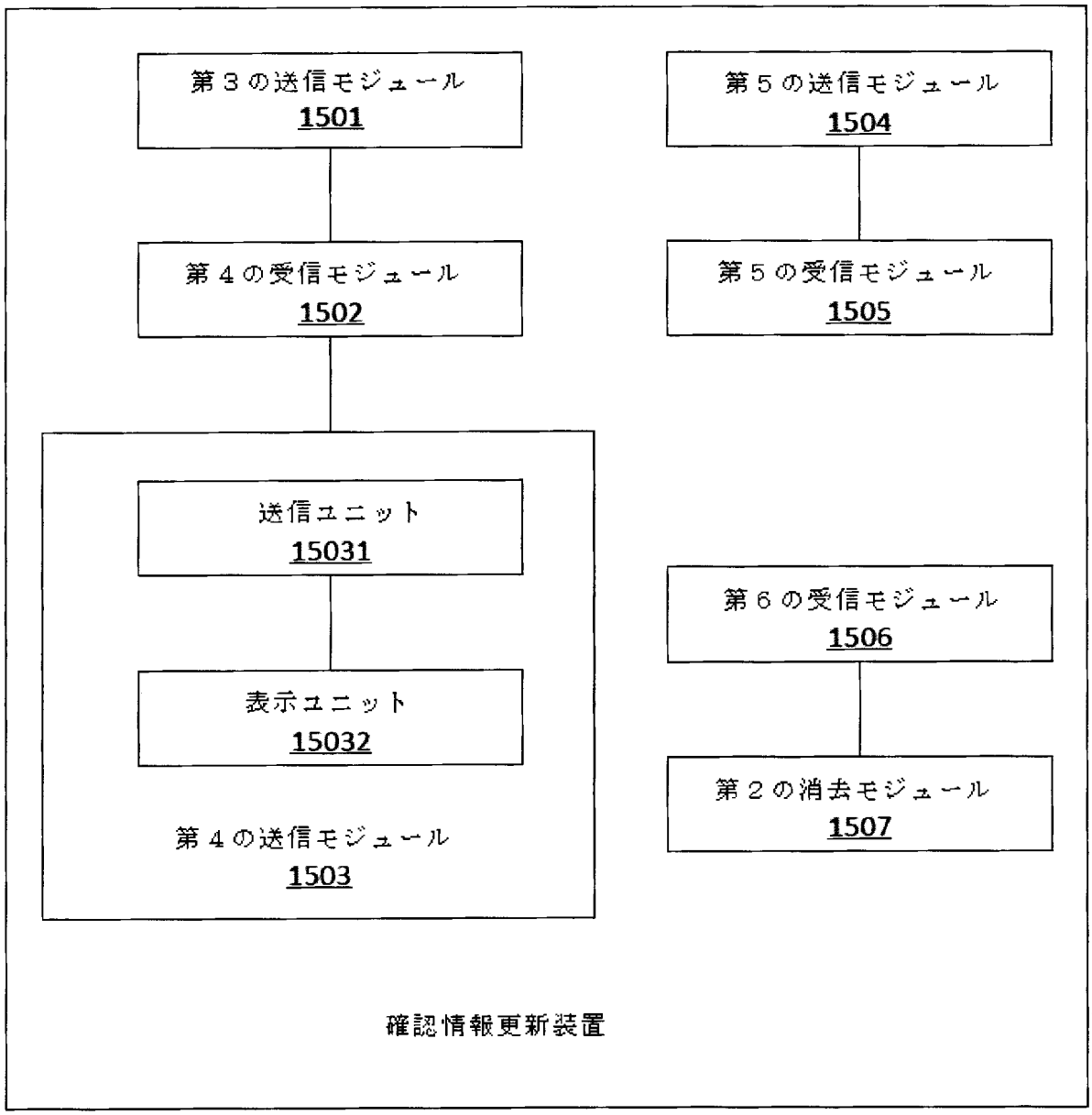
【補正対象書類名】明細書
【補正対象項目名】００９９
【補正方法】変更
【補正の内容】
【００９９】
上記の確認情報更新方法に対応して、本開示は、図１０に示されている本開示の一例示的な実施形態によるサーバの概略構造図をさらに提供する。図１０を参照すると、ハードウェアレベルにおいて、サーバは、プロセッサ、内部バス、ネットワークインターフェース、メモリ、及び不揮発性メモリを含み、他のサービスが必要とするハードウェアをさらに含み得ることは確実である。プロセッサは、不揮発性メモリからメモリまで対応するコンピュータプログラムを読み取り、コンピュータプログラムを実行し、したがって、論理レベルにおける確認情報更新装置が形成される。ソフトウェア実施方式に加えて、本開示が、論理機器、またはソフトウェアとハードウェアとの組合せなど、他の実施方式を除外しないことは確実である。言い換えれば、次の処理手順は、限定されるものではないが、様々な論理ユニットによって行われ、また、ハードウェアまたは論理機器によっても行われ得る。
【手続補正４】
【補正対象書類名】図面
【補正対象項目名】図１４
【補正方法】変更
【補正の内容】

【図１４】



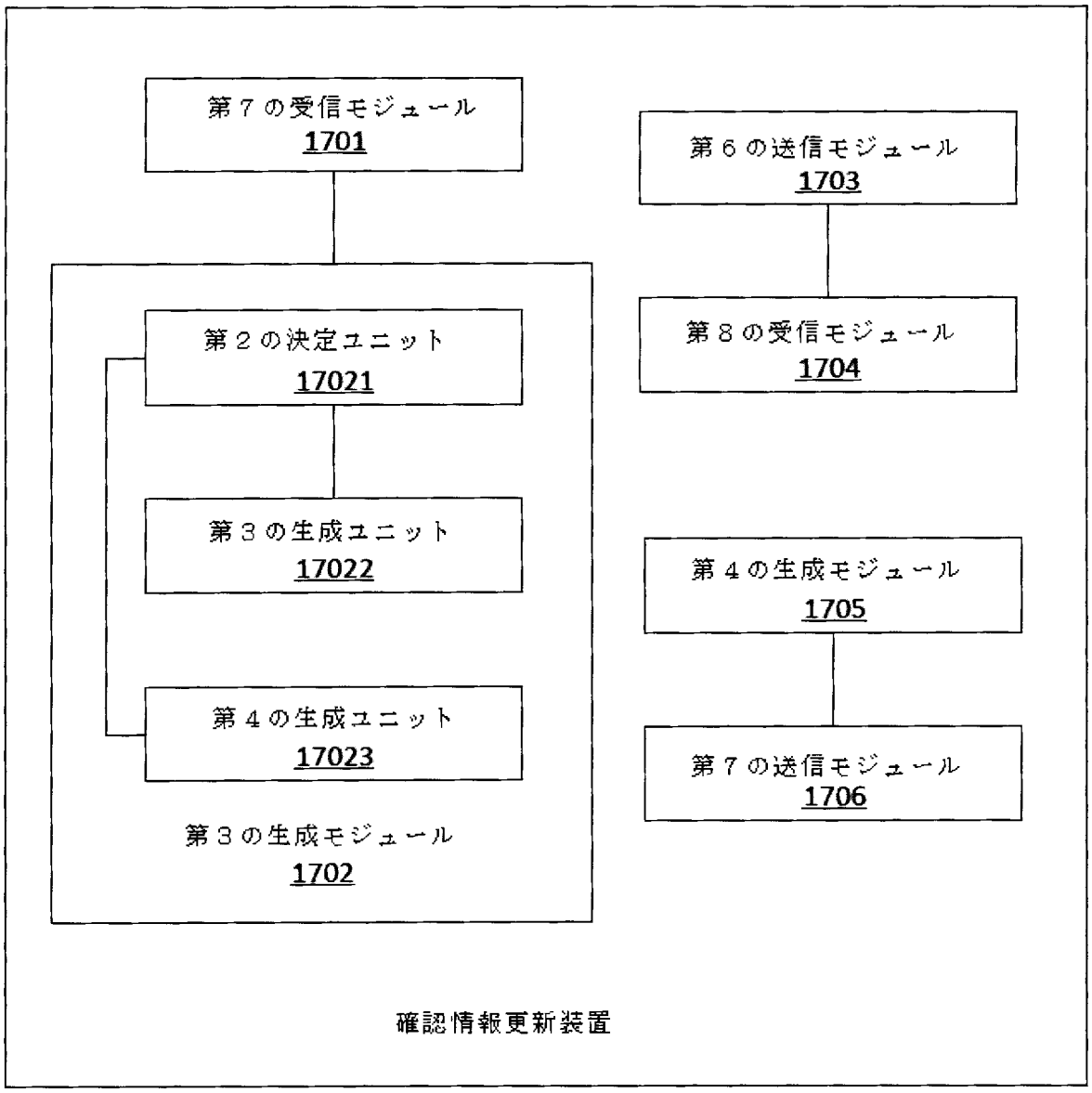
【手続補正５】
【補正対象書類名】図面
【補正対象項目名】図１６
【補正方法】変更
【補正の内容】

【図１６】



【手続補正６】
【補正対象書類名】図面
【補正対象項目名】図１８
【補正方法】変更
【補正の内容】

【図１８】


第７の受信モジュール
1701
第６の送信モジュール
1703
第２の決定ユニット
17021
第８の受信モジュール
1704
第３の生成ユニット
17022
第４の生成モジュール
1705
第４の生成ユニット
17023
第７の送信モジュール
1706
第３の生成モジュール
1702
確認情報更新装置

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2016/095858

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06 (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)

H04L

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

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

Data bases: WPI, EPODOC, CNPAT, CNKI

Key words: universally unique identifier, update, verif+, server, terminal, smart, intelligent, UUID, UID, random number, device, bounding, household appliances

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	CN 104660618 A (LENOVO (BEIJING) CO., LTD.), 27 May 2015 (27.05.2015), description, paragraphs 23-39, and claims 1-7	1-28
Y	CN 103383736 A (INTERMEDIATE FREQUENCY ELECTRONIC CO., LTD.), 06 November 2013 (06.11.2013), description, paragraphs 8-11 and 43-55, claims 1-6, and figure 1	1-28
A	CN 103023917 A (BAIDU ONLINE NETWORK TECHNOLOGY (BEIJING) CO., LTD.), 03 April 2013 (03.04.2013), the whole document	1-28
A	CN 202634464 U (SOUTH CHINA UNIVERSITY OF TECHNOLOGY), 26 December 2012 (26.12.2012), the whole document	1-28
A	US 8205076 B1 (ADOBE SYSTEMS INCORPORATED), 19 June 2012 (19.06.2012), the whole document	1-28

☐ 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
18 October 2016 (18.10.2016)	**07 November 2016 (07.11.2016)**
Name and mailing address of the ISA/CN: State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No.: (86-10) 62019451	Authorized officer **GU, Yizhen** Telephone No.: (86-10) **010-82246963**

Form PCT/ISA/210 (second sheet) (July 2009)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2016/095858

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 104660618 A	27 May 2015	US 2016285644 A1	29 September 2016
CN 103383736 A	06 November 2013	None	
CN 103023917 A	03 April 2013	None	
CN 202634464 U	26 December 2012	None	
US 8205076 B1	19 June 2012	US 8051287 B2	01 November 2011
		US 8245033 B1	14 August 2012
		US 8918644 B2	23 December 2014
		CN 101902453 A	01 December 2010
		US 2015142927 A1	21 May 2015

Form PCT/ISA/210 (patent family annex) (July 2009)

国际检索报告

国际申请号
PCT/CN2016/095858

A. 主题的分类

H04L 29/06(2006.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

H04L

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用）)

数据库：WPI，EPODOC，CNPAT，CNKI；关键词：更新，验证，服务器，终端，智能，通用唯一识别码，随机数，设备，家电，绑定；update，verif+，server，terminal，smart，intelligent，UUID，UID，random number，device，bounding，household appliances.

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
Y	CN 104660618 A (联想北京有限公司) 2015年 5月 27日 (2015-05-27) 说明书第23-39段，权利要求1-7	1-28
Y	CN 103383736 A (中频电子股份有限公司) 2013年 11月 6日 (2013-11-06) 说明书第8-11、43-55段，权利要求1-6，附图1	1-28
A	CN 103023917 A (百度在线网络技术北京有限公司) 2013年 4月 3日 (2013-04-03) 全文	1-28
A	CN 202634464 U (华南理工大学) 2012年 12月 26日 (2012-12-26) 全文	1-28
A	US 8205076 B1 (ADOBE SYSTEMS INCORPORATED) 2012年 6月 19日 (2012-06-19) 全文	1-28

☐ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：

"A" 认为不特别相关的表示了现有技术一般状态的文件

"E" 在国际申请日的当天或之后公布的在先申请或专利

"L" 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

"O" 涉及口头公开、使用、展览或其他方式公开的文件

"P" 公布日先于国际申请日但迟于所要求的优先权日的文件

"T" 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

"X" 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

"Y" 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

"&" 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2016年 10月 18日	2016年 11月 7日
ISA/CN的名称和邮寄地址 中华人民共和国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088 传真号 (86-10)62019451	受权官员 古毅真 电话号码 (86-10)010-82246963

表 PCT/ISA/210 (第2页) (2009年7月)

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2016/095858

检索报告引用的专利文件			公布日（年/月/日）	同族专利			公布日（年/月/日）
CN	104660618	A	2015年 5月 27日	US	2016285644	A1	2016年 9月 29日
CN	103383736	A	2013年 11月 6日		无		
CN	103023917	A	2013年 4月 3日		无		
CN	202634464	U	2012年 12月 26日		无		
US	8205076	B1	2012年 6月 19日	US	8051287	B2	2011年 11月 1日
				US	8245033	B1	2012年 8月 14日
				US	8918644	B2	2014年 12月 23日
				CN	101902453	A	2010年 12月 1日
				US	2015142927	A1	2015年 5月 21日

表 PCT/ISA/210（同族专利附件）（2009年7月）

フロントページの続き

(81)指定国 AP(BW,GH,GM,KE,LR,LS,MW,MZ,NA,RW,SD,SL,ST,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,RU,TJ,TM),EP(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),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,KM,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AO,AT,AU,AZ,BA,BB,BG,BH,BN,BR,BW,BY,BZ,CA,CH,CL,CN,CO,CR,CU,CZ,DE,DK,DM,DO,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,GT,HN,HR,HU,ID,IL,IN,IR,IS,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

(72)発明者 アン チン
中華人民共和国 ３１１１２１ ゼァージアン ハンチョウ ユーハン ディストリクト ウェスト ウェン イー ロード ナンバー９６９ ビルディング ３ ５／エフ アリババ グループ リーガル デパートメント内
(72)発明者 リー コーポン
中華人民共和国 ３１１１２１ ゼァージアン ハンチョウ ユーハン ディストリクト ウェスト ウェン イー ロード ナンバー９６９ ビルディング ３ ５／エフ アリババ グループ リーガル デパートメント内

Ｆターム(参考) 5J104 AA07 AA16 EA23 KA02 NA05 NA36 NA38