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

特許第6773401号
(P6773401)

(45)発行日　令和2年10月21日(2020.10.21)　(24)登録日　令和2年10月5日(2020.10.5)

(51)Int.Cl.		F I		
H04L 9/32	(2006.01)	H04L	9/00	675Z
H04L 9/08	(2006.01)	H04L	9/00	601C
G06F 21/44	(2013.01)	G06F	21/44	350

請求項の数 8　(全 39 頁)

(21)出願番号　特願2015-197851(P2015-197851)
(22)出願日　平成27年10月5日(2015.10.5)
(65)公開番号　特開2017-73609(P2017-73609A)
(43)公開日　平成29年4月13日(2017.4.13)
審査請求日　平成29年6月13日(2017.6.13)
審判番号　不服2019-5244(P2019-5244/J1)
審判請求日　平成31年4月19日(2019.4.19)

(73)特許権者　000233778
任天堂株式会社
京都府京都市南区上鳥羽鉾立町１１番地１
(74)代理人　110001276
特許業務法人　小笠原特許事務所
(74)代理人　100130269
弁理士　石原　盛規
(72)発明者　児島　陽平
京都府京都市南区上鳥羽鉾立町１１番地１
任天堂株式会社内
(72)発明者　黒田　良治
京都府京都市南区上鳥羽鉾立町１１番地１
任天堂株式会社内

最終頁に続く

(54)【発明の名称】周辺機器、無線通信チップ、アプリケーションプログラム、情報処理システム、および情報処理方法

(57)【特許請求の範囲】

【請求項１】

所定の通信機器との間でデータ通信が可能な周辺機器であって、

暗号化通信のための暗号化キーと、前記周辺機器を一意に特定可能な情報である特定情報と、当該特定情報のデジタル署名である署名情報とを、所定の方式で暗号化したうえで認証用のサーバに送信するための第１通信部と、

前記第１通信部で送信した特定情報及び署名情報に基づいて前記認証用のサーバで行なわれた認証処理の結果に基づくデータである第１データを当該認証用のサーバから受信した後、第２データの送信要求を示す要求情報を前記暗号化キーで暗号化し、当該認証用のサーバに送信する第２通信部と、

前記第２通信部で送信した要求情報に応じて前記認証用のサーバから送信される暗号化された前記第２データを受信した後、前記暗号化キーを用いて当該暗号化された第２データを復号化し、当該復号化した第２データを当該認証用サーバに送信する第３通信部と、

前記第３通信部で送信した第２データの正当性が前記認証用のサーバにおいて確認された結果に基づくデータである第３データを当該認証用のサーバから受信した後、当該第３データの受信にかかる処理後に前記暗号化キーを前記認証用のサーバから受信した前記所定の通信機器との間で、当該暗号化キーで暗号化した第４データを送受信する通信処理を実行する通信処理実行部、とを備える、周辺機器。

【請求項２】

前記第２データとして、乱数が用いられる、請求項１に記載の周辺機器。

【請求項３】
前記周辺機器は、
一旦接続が確立した実績のある所定の通信機器と再接続する際に用いる情報であるボンディング情報を、その有効期限を設定したうえで記憶部に記憶する記憶部と
前記所定の通信機器との通信の際に、前記有効期限が経過しているか否かを判定する期限判定部とを更に備え、
前記期限判定部によって前記有効期限を経過していると判定されたとき、前記第１通信部、第２通信部、第３通信部による処理を再度実行した後に、前記通信処理実行部による通信処理を実行する、請求項１または２に記載の周辺機器。
【請求項４】
前記周辺機器は、前記所定の通信機器との間の通信をブルートゥース（登録商標）通信によって行なう、請求項１または２に記載の周辺機器。
【請求項５】
サーバと、所定の通信機器と、当該所定の通信機器との間でデータ通信が可能な周辺機器とを備える情報処理システムであって、
前記周辺機器は、
暗号化通信のための暗号化キーと、前記周辺機器を一意に特定可能な情報である特定情報と、当該特定情報のデジタル署名である署名情報とを、所定の方式で暗号化したうえで前記サーバに送信するための第１通信部と、
前記第１通信部で送信した特定情報及び署名情報に基づいて前記サーバで行なわれた認証処理の結果に基づくデータである第１データを当該サーバから受信した後、第２データの送信要求を示す要求情報を前記暗号化キーで暗号化し、当該サーバに送信する第２通信部と、
前記第２通信部で送信した要求情報に応じて前記サーバから送信される暗号化された前記第２データを受信した後、前記暗号化キーを用いて当該暗号化された第２データを復号化し、当該復号化した第２データを当該サーバに送信する第３通信部と、
前記第３通信部で送信した第２データの正当性が前記サーバにおいて確認された結果に基づくデータである第３データを当該サーバから受信した後、前記所定の通信機器との間で、前記暗号化キーで暗号化した第４データを用いた通信処理を実行する通信処理実行部とを備え、
前記サーバは、前記第１通信部から送信された前記特定情報及び署名情報に基づいて前記周辺機器に関する認証処理を行う認証処理部と、
当該認証処理の結果に基づく前記第１データを前記周辺機器に送信する第１データ送信部と、
前記第２通信部から送信された要求情報に応じて、前記暗号化キーを用いて前記第２データを暗号化して前記周辺機器に送信する第２データ送信部と、
前記第３通信部から送信された前記第２データの正当性を確認し、その結果に基づく前記第３データを前記周辺機器に送信する第３データ送信部と、
前記第３データの送信後、前記第４データの暗号化に用いる前記暗号化キーを前記所定の通信機器に送信する端末用暗号化キー送信部とを備え、
前記周辺機器と前記サーバとの間のデータの送受信は、前記所定の通信機器を経由して行われる、情報処理システム。
【請求項６】
前記周辺機器および前記認証用のサーバの間で行なわれるデータは、暗号化されて送受信される、請求項５に記載の情報処理システム。
【請求項７】
前記周辺機器は、
第５データを共通鍵で暗号化して前記サーバに送信する暗号データ送信部と、
前記サーバで復号化された第５データを当該サーバから受信する復号化データ受信部と、

前記暗号化する前の第５データと、前記復号化データ受信部で受信した第５データが一致するか否かを判定することにより、前記サーバの正当性を判定する判定部とを更に備え、

前記サーバは、前記暗号データ送信部から送られた前記暗号化された第５データを復号化し、送信元の前記周辺機器に当該復号化した第５データを送信するデータ復号化部を更に備える、請求項５に記載の情報処理システム。

【請求項８】

所定の通信機器との間でデータ通信が可能な周辺機器を制御するための情報処理方法であって、

暗号化通信のための暗号化キーと、前記周辺機器を一意に特定可能な情報である特定情報と、当該特定情報のデジタル署名である署名情報とを、所定の方式で暗号化したうえで認証用のサーバに送信するための第１通信ステップと、

前記第１通信ステップで送信した特定情報及び署名情報に基づいて前記認証用のサーバで行なわれた認証処理の結果に基づくデータである第１データを当該認証用のサーバから受信した後、第２データの送信要求を示す要求情報を前記暗号化キーで暗号化し、当該認証用のサーバに送信する第２通信ステップと、

前記第２通信ステップで送信した要求情報に応じて前記認証用のサーバから送信される暗号化された前記第２データを受信した後、前記暗号化キーを用いて当該暗号化された第２データを復号化し、当該復号化した第２データを当該認証用サーバに送信する第３通信ステップと、

前記第３通信ステップで送信した第２データの正当性が前記認証用のサーバにおいて確認された結果に基づくデータである第３データを当該認証用のサーバから受信した後、当該第３データの受信にかかる処理後に前記暗号化キーを前記認証用のサーバから受信した前記所定の通信機器との間で、当該暗号化キーで暗号化した第４データを送受信する通信処理を実行する通信処理実行ステップ、とを有する、情報処理方法。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、例えばスマートデバイス等の通信機器と通信可能な周辺機器に関し、より特定的には、周辺機器の認証処理に関する。

【背景技術】

【０００２】

従来から、スマートフォン等の情報処理機器と、ブルートゥース（Ｂｌｕｅｔｏｏｔｈ：登録商標）などの非接触型のインターフェースを用いて接続可能な周辺機器が知られている（例えば、非特許文献１）。上記ブルートゥースの規格では、機器の種類ごとにプロトコルを定義したプロファイルと呼ばれるものが策定されている。通信しようとする機器同士が同じプロファイルを有していれば、そのプロファイルの機能を利用した通信が可能となっている。例えば、周辺機器がキーボードであれば、ＨＩＤ（Human Interface Device Profile）と呼ばれるプロファイルをお互いに有していれば、両者の間で接続を確立させ、キーボードを用いて情報処理機器へ文字入力等が可能となる。また、例えば周辺機器がヘッドフォンであれば、Ａ２ＤＰ（Advanced Audio Distribution Profile）と呼ばれるプロファイルをお互いに有していれば、両者の間で接続を確立させ、情報処理機器からヘッドフォンに音声を伝送することができる。

【先行技術文献】

【非特許文献】

【０００３】

【非特許文献１】任天堂株式会社、”ニンテンドーワイヤレスキーボードについて”、［online］、［平成２７年５月２０日検索］、インターネット（ＵＲＬ：http://www.nintendo.co.jp/ds/uzpj/keyboard/）

【発明の概要】

【発明が解決しようとする課題】
【０００４】
ところで、従来の技術においては、上記のようなブルートゥースを用いる周辺機器を情報処理機器で用いようとする際に、当該周辺機器を認証するものではなかった。すなわち、上記のようなプロファイルを有していれば、どのような周辺機器でも接続して利用することが可能であった。
【０００５】
それ故に、本発明の目的は、上記のような周辺機器を情報処理機器で用いようとする際に、その周辺機器を認証できるシステム等を提供することである。
【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、例えば以下のような構成例が挙げられる。
【０００７】
構成例の一例は、所定の通信機器との間でデータ通信が可能な周辺機器であって、第１通信部と、第２通信部と、第３通信部と、通信処理実行部、とを備える。第１通信部は、暗号化通信のための暗号化キーと、周辺機器を一意に特定可能な情報である特定情報と、当該特定情報のデジタル署名である署名情報とを認証用のサーバに送信する。第２通信部は、第１送信部で送信した特定情報および署名情報に基づいて認証用のサーバで行なわれた認証処理の結果に基づくデータである第１データを当該認証用のサーバから受信した後、第２データの送信要求を示す要求情報を暗号化キーで暗号化し、当該認証用のサーバに送信する。第３通信部は、第２通信部で送信した要求情報に応じて認証用のサーバから送信される暗号化された第２データを受信した後、暗号化キーを用いて当該暗号化された第２データを復号化し、当該復号化した第２データを当該認証用サーバに送信する。通信処理実行部は、第３通信部で送信した第２データの正当性が認証用のサーバにおいて確認された結果に基づくデータである第３データを当該認証用のサーバから受信した後、所定の通信機器との間で、前記暗号化キーで暗号化した第４データを用いた通信処理を実行する。
【０００８】
上記構成例によれば、所定の通信機器から周辺機器を使用する際に、周辺機器の認証を行ってから、暗号化通信による通信処理を実行することでき、周辺機器の利用の安全性を高めることができる。
【０００９】
更に他の構成例として、第２データとして、乱数が用いられるように構成しても良い。
【００１０】
上記構成例によれば、認証処理の際の安全性をより高めることが可能となる。
【００１１】
更に他の構成例として、周辺機器は、一旦接続が確立した所定の通信機器と再接続する際に用いる情報であるボンディング情報を、その有効期限を設定したうえで記憶部に記憶する記憶部と、所定の通信機器との通信の際に、有効期限が経過しているか否かを判定する期限判定部とを更に備えていてもよい。そして、期限判定部によって有効期限を経過していると判定されたとき、第１送信部、第２送信部、第３送信部による処理を再度実行した後に、通信処理実行部による通信処理を実行するようにしてもよい。
【００１２】
上記構成例によれば、汎用性の高い無線通信規格を利用しつつ、周辺機器の定期的な認証処理も実行することができ、利便性を高めつつ、周辺機器の利用の安全性を確保することもできる。
【００１３】
他の構成例の一例は、ブルートゥース通信が可能な無線通信チップであって、所定の通信機器とのブルートゥース通信が許可される期限である有効期限の情報を記憶する有効期限情報記憶部を備える。更に、有効期限の情報は、日付けを示す情報であってもよいし、

あるいは、有効期限の情報は、所定の回数をカウントするためのカウンタであってもよい。

【００１４】

上記構成例によれば、所定の通信機器との間の通信について、その通信が許可される有効期限を設けることができ、有効期限外となったときに、例えば認証処理等の、通信を許可するための所定の処理を実行させることが可能となる。

【００１５】

他の構成例の一例は、所定の通信機器との間でデータ通信が可能な周辺機器であって、接続部と、ボンディング情報記憶部と、有効期限記憶部と、期限判定部と、再認証部とを備える。接続部は、所定の通信機器と近距離無線通信で接続する。ボンディング情報記憶部は、接続部によって一旦接続が確立した所定の通信機器と再接続する際に用いる情報であるボンディング情報を記憶部に記憶する。有効期限記憶部は、周辺機器と所定の認証用サーバとの間で行なわれた、当該周辺機器を認証するための認証処理の結果に基づき、ボンディング情報の有効期限を示す有効期限情報を記憶部に記憶する。期限判定部は、所定の通信機器との通信の際に、有効期限が経過しているか否かを判定する。再認証部は、有効期限を経過していると判定されたとき、所定の認証用サーバを用いる再度の認証処理を実行する。

【００１６】

上記構成例によれば、ボンディング情報に有効期限を設定することができ、これが有効期限外となったとき、再度の認証処理を行わせることができる。

【００１７】

更に他の構成例として、周辺機器と前記所定の通信機器との間の通信は、ブルートゥース（登録商標）通信によって行なわれるようにしてもよい。

【００１８】

上記構成例によれば、汎用性の高い無線通信規格を利用しつつ、周辺機器の定期的な認証処理も実行することができ、利便性を高めつつ、周辺機器の利用の安全性を確保することができる。

【００１９】

他の構成例の一例は、通信可能に接続された所定の周辺機器を利用する所定の通信機器のコンピュータに実行させるアプリケーションプログラムであって、コンピュータを、要求受信手段と、ＩＤ送信手段と、処理実行手段として機能させる。要求受信手段は、アプリケーションＩＤの送信要求を前記周辺機器から受信する。ＩＤ送信手段は、送信要求に応じて、起動中のアプリケーションプログラムのアプリケーションＩＤを周辺機器に送信する。処理実行手段は、周辺機器におけるアプリケーションＩＤの検証が成功した場合に、当該周辺機器との通信処理を伴う所定の処理を実行する。なお、当該アプリケーションＩＤは、アプリケーション毎に固有のＩＤであってもよい。

【００２０】

上記構成例によれば、周辺機器の利用に際して、当該周辺機器の正当性を確認することができる、また、周辺機器側において、その通信相手となるアプリケーションの正当性確認を行わせることもできる。

【００２１】

他の構成例の一例は、所定のサーバと通信可能に接続された所定の通信機器のコンピュータに実行させるアプリケーションプログラムであって、コンピュータを、要求受信手段と、ＩＤ送信手段と、処理実行手段、として機能させる。要求受信手段は、アプリケーションＩＤの送信要求をサーバから受信する。ＩＤ送信手段は、送信要求に応じて、起動中のアプリケーションプログラムのアプリケーションＩＤをサーバに送信する。処理実行手段は、所定の周辺機器との通信処理を伴う所定の処理を実行する。そして、ＩＤ送信手段によるアプリケーションＩＤの送信の後、サーバにおける当該アプリケーションＩＤの検証が成功した場合に、所定の周辺機器との通信処理を伴う所定の処理の実行が許可される。なお、当該アプリケーションＩＤは、アプリケーション毎に固有のＩＤであってもよい

。

【００２２】

上記構成例によれば、周辺機器の認証処理の際に、周辺機器の通信相手となるアプリケーションの正当性確認を行うことができる。

【００２３】

他の構成例の一例は、所定のサーバと通信可能に接続された所定の通信機器のコンピュータに実行させるアプリケーションプログラムであって、コンピュータを、要求受信手段と、証明書送信手段と、処理実行手段として機能させる。要求受信手段は、クライアント証明書の送信要求をサーバから受信する。証明書送信手段と、送信要求に応じて、所定の通信機器の記憶部に記憶されているクライアント証明書をサーバに送信する。処理実行手段は、所定の周辺機器との通信処理を伴う所定の処理を実行する。そして、証明書送信手段によるクライアント証明書の送信の後、サーバにおける当該クライアント証明書の正当性の検証が成功した場合に、所定の周辺機器との通信処理を伴う所定の処理の実行が許可される。

【００２４】

上記構成例によれば、周辺機器の利用に際して、その周辺機器の通信相手となる通信機器やアプリケーションプログラムの信頼性の高さを確認することができる。

【００２５】

他の構成例の一例は、サーバと、所定の通信機器と、当該所定の通信機器との間でデータ通信が可能な周辺機器とを備える情報処理システムであって、周辺機器は、第１通信部と、第２通信部と、第３通信部と、通信処理実行部とを備える。第１通信部は、暗号化通信のための暗号化キーと、周辺機器を一意に特定可能な情報である特定情報と、当該特定情報のデジタル署名である署名情報とをサーバに送信する。第２通信部は、第１通信部で送信した特定情報及び署名情報に基づいてサーバで行なわれた認証処理の結果に基づくデータである第１データを当該サーバから受信した後、第２データの送信要求を示す要求情報を暗号化キーで暗号化し、当該サーバに送信する。第３通信部は、第２通信部で送信した要求情報に応じてサーバから送信される暗号化された第２データを受信した後、暗号化キーを用いて当該暗号化された第２データを復号化し、当該復号化した第２データを当該サーバに送信する。通信処理実行部は、第３通信部で送信した第２データの正当性がサーバにおいて確認された結果に基づくデータである第３データを当該サーバから受信した後、所定の通信機器との間で、暗号化キーで暗号化した第４データを用いた通信処理を実行する。

また、サーバは、認証処理部と、第１データ送信部と、第２データ送信部と、第３データ送信部とを備える。認証処理部は、第１通信部から送信された特定情報及び署名情報に基づいて周辺機器に関する認証処理を行う。第１データ送信部は、認証処理の結果に基づく第１データを周辺機器に送信する。第２データ送信部は、第２通信部から送信された要求情報に応じて、暗号化キーを用いて第２データを暗号化して周辺機器に送信する。第３データ送信部は、第３通信部から送信された第２データの正当性を確認し、その結果に基づく第３データを周辺機器に送信する。そして、周辺機器とサーバとの間のデータの送受信は、所定の通信機器を経由して行われる。

【００２６】

上記構成例によれば、所定の通信機器から周辺機器を使用する際に、周辺機器の認証を行ってから、暗号化通信による通信処理を実行することでき、周辺機器の利用の安全性を高めることができ、更に、当該周辺機器の汎用性を高めることができる。

【００２７】

更に他の構成例として、周辺機器および認証用のサーバの間で行なわれるデータは、暗号化されて送受信されるよう構成しても良い。また、周辺機器は、第５データを共通鍵で暗号化してサーバに送信する暗号データ送信部と、サーバで復号化された第５データを当該サーバから受信する復号化データ受信部と、暗号化する前の第５データと、復号化データ受信部で受信した第５データが一致するか否かを判定することにより、サーバの正当性

を判定する判定部とを更に備え、サーバは、暗号データ送信部から送られた暗号化された第５データを復号化し、送信元の周辺機器に当該復号化した第５データを送信するデータ復号化部を更に備える構成としても良い。

【００２８】

上記構成例によれば、周辺機器の認証処理について、より安全な認証処理を行うことができる。

【発明の効果】

【００２９】

本実施形態によれば、周辺機器を使用する際に、当該周辺機器の認証処理を行い、認証されてから使用を許可することが可能となる。これにより、周辺機器の利用に際しての安全性を高めることができる。

【図面の簡単な説明】

【００３０】

【図１】本実施形態における認証システム全体を示す模式図
【図２】認証サーバ１００のハードウェア構成を示す模式図
【図３】スマートデバイス２００のハードウェア構成を示す模式図
【図４】周辺機器３００のハードウェア構成を示す模式図
【図５】認証サーバ１００の記憶部１０２に記憶されるデータを示す図
【図６】アプリテーブル１１４の構成の一例
【図７】周辺機器３００の不揮発メモリ３０３に記憶されるデータを示す図
【図８】拡張ボンディング情報３１６のデータ構成の一例
【図９】スマートデバイス２００の記憶部２０４に記憶されるデータを示す図
【図１０】第１の実施形態における認証処理の概要を説明するための図
【図１１】第１の実施形態における第１フェーズ処理の詳細を示すフローチャート
【図１２】第１の実施形態における第２フェーズ処理の詳細を示すフローチャート
【図１３】第１の実施形態における第３フェーズ処理の詳細を示すフローチャート
【図１４】第１の実施形態における第４フェーズ処理の詳細を示すフローチャート
【図１５】第１の実施形態における第４フェーズ処理の詳細を示すフローチャート
【図１６】第１の実施形態における第５フェーズ処理の詳細を示すフローチャート
【図１７】第１の実施形態における第６フェーズ処理の詳細を示すフローチャート
【図１８】第２の実施形態にかかる周辺機器４００のハードウェア構成を示す模式図
【図１９】第２の実施形態において認証サーバ１００の記憶部１０２に記憶されるデータを示す図
【図２０】周辺機器４００のセキュアメモリ４０５に記憶されるデータを示す図
【図２１】周辺機器４００の不揮発メモリ４０３に記憶されるデータを示す図
【図２２】第２の実施形態における認証処理の概要を説明するための図
【図２３】第２の実施形態における第２フェーズ処理の詳細を示すフローチャート
【図２４】第２の実施形態における第３フェーズ処理の詳細を示すフローチャート
【図２５】第２の実施形態における第４フェーズ処理の詳細を示すフローチャート
【図２６】第２の実施形態における第５フェーズ処理の詳細を示すフローチャート
【図２７】第２の実施形態における第５フェーズ処理の詳細を示すフローチャート
【図２８】第２の実施形態における第６フェーズ処理の詳細を示すフローチャート
【図２９】第２の実施形態における第７フェーズ処理の詳細を示すフローチャート

【発明を実施するための形態】

【００３１】

以下、本発明の実施形態について説明する。

【００３２】

まず、本実施形態では、次のような利用の態様を想定している。まず、所定のサーバとの通信が可能な通信機器、具体的にはスマートフォンなどのスマートデバイスがあるとする。更に、当該スマートデバイスで利用可能な周辺機器があるとする。この周辺機器は、

ブルートゥース（Ｂｌｕｅｔｏｏｔｈ：登録商標）技術でスマートデバイスと接続可能であるとする。換言すれば、周辺機器はブルートゥースデバイスであるとする。また、当該スマートデバイスには、所定のアプリケーションがインストールされる。そして、上記周辺機器と連携させながら当該アプリケーションをユーザが利用する、というような場合を想定する。例えば、上記周辺機器は、体調管理やフィットネスに関する機器であって、上記アプリケーションは、ユーザが当該周辺機器を利用した健康管理やトレーニング等を行うことが可能なアプリケーションである。以下では、当該アプリケーションのことを「専用アプリ」と呼ぶ。

【００３３】

上記のような専用アプリの利用に際しては、まず、上記周辺機器をスマートデバイスと接続して、当該アプリケーションから利用可能な状態とする必要がある。ここで、当該周辺機器に関しては、粗悪品等による使用感の低下等の防止や、所定の規格を満たすことによる安全性の確保（安全規格を満たさない周辺機器による事故防止等）という観点から、いわゆる「正規品・純正品」や「動作確認済み」のものを利用することが好ましい。例えば上記専用アプリのメーカで動作確認がとれた周辺機器や、あるいは、上記専用アプリのメーカによって開発・販売されている周辺機器である。特に、専用アプリのメーカによって開発・販売されている周辺機器（いわゆる純正品）であれば、使用に際しての安全性は高いものと考えられる。

【００３４】

このような観点から、本実施形態では、上記のような利用態様に際し、周辺機器として上記専用アプリのメーカによる「純正品」を利用する場合を想定する。例えば、メーカが、上記周辺機器および専用アプリをセットで提供するような場合を考える。そして、本実施形態で説明する技術は、上記専用アプリを利用する際に、当該専用アプリと連携して使用する上記のような周辺機器の正当性（例えば純正品であるか）を認証するための技術に関するものである。すなわち、専用アプリの実行開始に先立って、上記周辺機器が純正品であるか否かをチェックするという処理（周辺機器の認証処理）が本実施形態では行なわれる。

【００３５】

ここで、上記のような周辺機器の認証処理を行なう場合、一般に、スマートデバイス上において認証処理を行うことが考えられる。しかし、昨今では、スマートデバイスは多種多様な機種が存在しており、また、汎用的なデバイスであるともいえる。そのため、どのユーザがどのようなスマートデバイスを利用しているかを専用アプリのメーカ側で把握したり、予測したりすることは困難であるという側面がある。また、上記専用アプリが改ざんされたり、あるいは、他のアプリを介在させたりすることで周辺機器の認証が回避されるリスクも想定される。例えば、純正品ではない周辺機器が存在するとして、上記専用アプリが何らかの形で改ざんされる等し、上記のような認証処理が行なわれずに、純正品ではない周辺機器が用いられてしまうことも考えられる。

【００３６】

そこで、本実施形態では、上記のような周辺機器の認証処理を、スマードデバイス側では行なわないようにしている。具体的には、認証用のサーバ（以下、認証サーバ）を用意し、スマートデバイス（専用アプリ）が中継する形で、周辺機器とサーバとの間における認証処理を行ない、周辺機器を専用アプリから利用可能な状態とするものである。また、本実施形態では、更に、専用アプリ自体の正当性をチェックする処理も実行される。

【００３７】

なお、以下の説明では、「認証」という用語と「検証」という用語を用いる。以下の説明では、「認証」は、周辺機器の正当性を確認することを意図し、後述する一連のプロセスが該当する。すなわち、後述の一連の処理が「認証処理」に該当する。一方、「検証」は、後述の一連の認証プロセスにおいて適宜行なわれる処理を意図し、主にこの認証プロセスの間にやりとりされるデータの正当性をチェックする処理である。例えば受信した「証明書」の送信主体が、正しい送信主体であるのかの確証を得るために行なわれる処理で

ある。
【００３８】
（第１の実施形態）
以下、第１の実施形態を説明する。まず、第１の実施形態で想定する周辺機器認証システムの全体像について説明する。図１は、本実施形態における認証システム全体を示す模式図である。図１では、認証サーバ１００、スマートデバイス２００、スマートデバイス用周辺機器３００（以下、単に周辺機器と呼ぶ）が示されている。認証サーバ１００は、インターネットに接続されている。スマートデバイス２００もインターネットに接続されている。認証サーバ１００およびスマートデバイス２００は、インターネットを介して通信可能となっている。また、スマートデバイス２００と周辺機器３００は、上記のようにブルートゥース技術を用いて無線接続されている。そのため、スマートデバイス２００と周辺機器３００との間は、基本的にはブルートゥース規格に沿った無線通信が行なわれる。
【００３９】
次に、認証サーバ１００、スマートデバイス２００、周辺機器３００のハードウェア構成について説明する。図２は、認証サーバ１００のハードウェア構成を示す模式図である。認証サーバ１００は、処理部１０１、記憶部１０２、通信部１０３を備える。処理部１０１は、所定のプロセッサ等であり、本実施形態にかかる認証処理におけるサーバ側での各種情報処理を実行する。記憶部１０２は、当該処理で用いる各種データ（データベース等）が記憶される。通信部１０３は、処理部１０１の制御に基づき、インターネットに接続し、上記スマートデバイス２００と通信を行なう。また、図示は省略するが、認証サーバ１００には、サーバとしての機能を果たすためのその他の各種コンポーネントも含まれている。
【００４０】
次に、図３は、スマートデバイス２００のハードウェア構成を示す模式図である。スマートデバイス２００は、例えばスマートフォンやタブレット端末等の情報機器である。スマートデバイス２００は、処理部２０１、第１通信部２０２、第２通信部２０３、記憶部２０４、入力部２０５等を備える。処理部２０１は、専用アプリの実行等の、各種情報処理を実行する。第１通信部２０２は、処理部２０１の制御に基づいて、インターネットに接続し、通信する機能を有する。本実施形態では、第１通信部２０２は、無線ＬＡＮ機能を有する無線モジュールであるとする。第１通信部２０２は、処理部２０１による制御に基づき、インターネットを介して上記認証サーバ１００との間で各種データの送受信を行う。第２通信部２０３は、周辺機器３００と通信するための機能を有する。本実施形態では、第２通信部２０３は、ブルートゥースモジュールであるとする。第２通信部２０３は、処理部２０１による制御に基づき、ブルートゥース技術を用いて周辺機器３００との通信を行う。記憶部２０４は、例えばフラッシュメモリであり、アプリケーションプログラムや各種データ等が記憶される。入力部２０５は、スマートデバイスに対するユーザからの入力を受け付けるためのものであり、タッチパネルや各種のボタン等である。表示部２０６は、各種情報処理の結果等を表示するための画面である。
【００４１】
次に、図４は、周辺機器３００のハードウェア構成を示す模式図である。周辺機器３００は、通信部３０１を備える。また、図示は省略するが、操作ボタンや各種センサ等、専用アプリの実行において必要な各種ハードウェアコンポーネントも備えている。通信部３０１は、例えば通信チップ（より具体的には、ブルートゥースチップやブルートゥースモジュール）であり、スマートデバイス２００と近距離無線通信を行なうための機能を有する。通信部３０１は、マイコン３０２、不揮発メモリ３０３、ＲＡＭ３０４を有する。不揮発メモリ３０３には、後述するような処理を実行するためのプログラムやデータが記憶されている。当該プログラムはマイコン３０２によって実行されることになる。ＲＡＭ３０４には、後述の処理において必要な各種データが適宜記憶される。
【００４２】

次に、本実施形態で実行される認証処理の処理概要について説明する。本実施形態では、概ね次のような動作の流れを想定している。まず、ユーザが専用アプリをスマートデバイス２００にインストールし、起動を行なう。このときは、初回起動となるため、周辺機器の認証処理が実行される。詳細は後述するが、この認証処理の最初に、まず、スマートデバイス２００と周辺機器３００との間で無線接続が確立され、両者の間で通信可能な状態とされる。この時点では、両者の間で最低限の通信ができる状態であり、専用アプリから周辺機器が利用できるかどうかはまだ不明な状態である（つまり、周辺機器３００はまだ認証されていない状態である）。その後、スマートデバイス２００を中継するような形で周辺機器３００と認証サーバ１００との間で各種データの送受信等が行なわれることによって、認証処理が進行する。そのため、認証処理の実行に際しては、スマートデバイス２００はインターネット通信（認証サーバ１００との通信）が可能な状態であることが必要となる。認証処理の結果、周辺機器３００が正常に認証されたときは、所定の情報（後述のボンディング情報等）が周辺機器３００の不揮発メモリ３０３に記憶される。認証処理が終われば、専用アプリから周辺機器３００が利用可能（両者の暗号化通信が可能）となる。そして、周辺機器３００が通常起動し、専用アプリによる、当該周辺機器３００を利用した所定の処理が実行される。

【００４３】

周辺機器３００が一旦正常に認証されれば、専用アプリの次回起動時は、周辺機器３００において上記不揮発メモリ３０３に記憶された所定の情報に基づく簡易的なチェック処理が実行される。これは、周辺機器３００側から見た通信相手である専用アプリ（スマートデバイス２００）の正当性を検証するための簡易的な処理である。そして、検証に成功すれば、周辺機器３００が通常起動される。つまり、周辺機器３００が一旦正常に認証されれば、基本的は上記認証サーバ１００を用いた認証処理を省略することが可能となっている。これにより、ユーザの利便性を高めることができる。

【００４４】

また、本実施形態では、周辺機器３００の正常認証時に不揮発メモリ３０３に記憶される所定の情報について、有効期限を設ける構成とする。そして、この期限が経過した場合は、認証サーバ１００を用いる再度の認証処理が必要となる。つまり、本実施形態では、純正品の周辺機器３００を用いていても、定期的に認証処理の実行を要求するという構成を採っている。

【００４５】

上記のような処理を行うことで、本実施形態では、周辺機器３００の正当性や安全性の確認と、ユーザの利便性の確保とを両立することが可能となっている。

【００４６】

次に、本実施形態における認証処理の動作をより詳細に説明する。まず、本処理において用いられる各種データに関して説明する。

【００４７】

図５は、認証サーバ１００の記憶部１０２に記憶されるデータを示す図である。記憶部１０２には、Ｖｆ＿Ｋｅｙ１１１、Ｐｖｔ＿Ｋｅｙ１１２、データベース１１３等が記憶されている。Ｖｆ＿Ｋｅｙ１１１は、後述するデジタル署名であるＢＴ＿Ｓｉｇｎの検証用の検証鍵（Ｖｅｒｉｆｉｃａｔｉｏｎ　Ｋｅｙ）である。Ｐｖｔ＿Ｋｅｙ１１２は、暗号化方式のひとつである公開鍵方式における「秘密鍵」であり、後述の周辺機器３００において記憶されているＰｕｂ＿Ｋｅｙ３１３と対になるものである。

【００４８】

データベース１１３は、純正品の周辺機器３００に関するデータベースである。データベース１１３には、複数のアプリテーブル１１４が含まれている。このアプリテーブル１１４については、１つの専用アプリに対して１つのアプリテーブル１１４が用意される。例えば、周辺機器３００を用いる専用アプリとして、アプリＡ、アプリＢ、アプリＣの３つのアプリがあるとする（それぞれのアプリで実現される機能は異なるものとする）。この場合は、アプリテーブル１１４としては３つのテーブルが用意される。すなわち、アプ

リＡ用のアプリテーブル１１４と、アプリＢ用のアプリテーブル１１４と、アプリＣ用のアプリテーブル１１４である。

【００４９】

図６に、アプリテーブル１１４の構成の一例を示す。アプリテーブル１１４は、ＢＴ＿Ａｄｄｒ１１５、ユーザＩＤ１１６、ＰＷＤ１１７等の項目を有する。ＢＴ＿Ａｄｄｒ１１５は、周辺機器３００を一意に識別するためのデータである。本実施例では、周辺機器３００がブルートゥースデバイスである場合を例として説明しているため、ブルートゥースデバイスに固有のアドレス（ＢＤデバイスアドレスやＢＤアドレスと呼ばれることもある）を当該ＢＴ＿Ａｄｄｒ１１５として利用している。ここで、当該ＢＴ＿Ａｄｄｒ１１５のデータ登録に関して補足説明する。まず、周辺機器３００が製造された際に、各周辺機器３００の上記固有のアドレスが所定のリストとして記録される。換言すれば、製造された全ての周辺機器３００の上記固有のアドレスのリストが用意されることになる。そして、当該リストに基づいて（例えば当該リストからデータをインポートする等）、ＢＴ＿Ａｄｄｒ１１５のデータが登録される。このようにして生成されたアプリテーブル１１４は、いわば、ＢＴ＿Ａｄｄｒ１１５のホワイトリストとしての役割も有する。

【００５０】

次に、ユーザＩＤ１１６、および、ＰＷＤ１１７は、ユーザアカウントの情報である。後述するが、本実施例では、上記専用アプリの利用に際して、ユーザアカウント情報を要求する。例えば、専用アプリの初回起動時には、ユーザアカウント作成のための処理が実行される。当該ユーザＩＤ１１６とＰＷＤ１１７は、このアカウント作成処理でユーザに入力されたユーザＩＤとパスワードを示すデータである。つまり、このアカウント作成処理において、当該データベース１１３に登録される。

【００５１】

なお、本実施形態では、説明の便宜上、１つのＢＴ＿Ａｄｄｒ１１５（１台の周辺機器３００）に対して、１人分のユーザＩＤ／パスワードが登録可能であるとして説明する。但し、他の実施形態では、１つのＢＴ＿Ａｄｄｒ１１５に対して複数人分のユーザＩＤ／パスワードが登録可能なように構成しても良い。例えば、１台の周辺機器を家族がそれぞれ所有するスマートデバイス（専用アプリ）から利用することが想定される場合、このような構成としても良い。

【００５２】

次に、周辺機器３００に記憶されるデータについて説明する。図７は、周辺機器３００の不揮発メモリ３０３に記憶されるデータを示す図である。不揮発メモリ３０３には、ＢＴ＿Ａｄｄｒ３１１、ＢＴ＿Ｓｉｇｎ３１２、Ｐｕｂ＿Ｋｅｙ３１３、ボンディング情報３１４、ＡＰＰ＿ＩＤ３１７、ＢＴ＿Ｋｅｙ３１８等が記憶される。

【００５３】

ＢＴ＿Ａｄｄｒ３１１は、その周辺機器３００に固有のアドレスであり、製造時に決定されるアドレスである。換言すれば、その周辺機器３００を一意に識別するための機器識別情報ともいえる。また、当該ＢＴ＿Ａｄｄｒ３１１は、上記データベース１１３のアプリテーブル１１４に記憶されるＢＴ＿Ａｄｄｒ１１５として登録されるデータでもある。なお、以下の説明においては、ＢＴ＿Ａｄｄｒ３１１および上記ＢＴ＿Ａｄｄｒ１１５に関して、「周辺機器３００に固有のアドレス」を示す意図で、単にＢＴ＿Ａｄｄｒと呼ぶこともある。

【００５４】

ＢＴ＿Ｓｉｇｎ３１２は、その周辺機器３００の製造時に生成され、記憶（書き込み）されるデジタル署名である。具体的には、上記ＢＴ＿Ａｄｄｒ３１１を、署名鍵Ｓｉｇｎ＿Ｋｅｙ（図示せず）を用いて暗号化したものが、ＢＴ＿Ｓｉｇｎ３１２として、不揮発メモリ３０３に記憶される。なお、この署名鍵Ｓｉｇｎ＿Ｋｅｙは、上記認証サーバに記憶されているＶｆ＿Ｋｅｙ１１１と対になるものである。

【００５５】

Ｐｕｂ＿Ｋｅｙ３１３は、暗号化通信における公開鍵（パブリックキー）であり、上記

認証サーバ１００で記憶されているＰｖｔ＿Ｋｅｙ１１２と対になるものである。

【００５６】

なお、ＢＴ＿Ａｄｄｒ３１１、ＢＴ＿Ｓｉｇｎ３１２、Ｐｕｂ＿Ｋｅｙ３１３については、周辺機器３００の製造時に不揮発メモリ３０３に書き込まれる。つまり、ユーザが周辺機器３００を購入等した時点で、これらのデータは既に周辺機器３００に記憶されている状態となっている。一方、以下に説明するボンディング情報３１４、ＡＰＰ＿ＩＤ３１７、ＢＴ＿Ｋｅｙ３１８は、本実施形態にかかる認証処理等を経て、最終的に周辺機器３００に記憶されるものである。

【００５７】

ボンディング情報３１４は、スマートデバイス２００と周辺機器３００との接続の組み合わせに関する情報である。ここで、本実施形態では、「ボンディング」とは、スマートデバイス２００と周辺機器３００とで接続情報を共有することを意味するものとする。このような接続情報がボンディング情報であり、スマートデバイス２００と周辺機器３００との再接続時の手続きを簡略化するために利用される。例えば、ある周辺機器３００と、あるスマートデバイス２００とが互いに一度も接続したことがない状態から、ユーザが所定の接続確立操作を行うことで、両者の間で接続が確立したとき（接続の実績ができたとき）、お互いの情報（固有アドレス等の接続相手の情報）を交換して記憶しておく。次回接続時には、この情報に基づくことで、ユーザによる所定の接続確立操作を行うことなく、自動的に再度の接続確立が可能となる。このような自動的な再度の接続のための情報がボンディング情報である。なお、以下の説明では、このような接続情報が記憶されていない状態のことを「未ボンディング」、ボンディング情報が記憶済みの状態のことを「ボンディング済み」と呼ぶこともある。

【００５８】

本実施形態では、当該ボンディング情報３１４には、基本ボンディング情報３１５と拡張ボンディング情報３１６とが含まれている。基本ボンディング情報３１５は、ブルートゥース規格に基づいた所定のデータであり、接続相手のアドレスや識別情報等が含まれている。また、当該基本ボンディング情報３１５が設定されているときは、「ボンディング済み」であり、設定されていないときは「未ボンディング」でると判定することが可能である。

【００５９】

拡張ボンディング情報３１６は、本実施形態において使用される独自の拡張データである。具体的には、ボンディング情報３１４（基本ボンディング情報３１５）に「有効期限」を設定するためのデータが含まれている。図８に、当該拡張ボンディング情報３１６のデータ構成の一例を示す。拡張ボンディング情報３１６には、期限切れフラグ３１９、期限カウンタ３２０等が含まれている。期限切れフラグ３１９は、ボンディング情報３１４が有効期限内であるか、期限切れであるかを示すフラグである。本実施形態では、Ｔｒｕｅの場合は期限切れであることを示し、Ｆａｌｓｅの場合は有効期限内であることを示す。また、期限カウンタ３２０は、有効期限を示すデータであり、また、カウントするためのカウンタである。例えば、ボンディング情報３１４の有効期限が「６０日」であるとする。この場合、例えばボンディング情報３１４更新されたタイミングで、当該期限カウンタに「６０」という値が設定されるようにする。そして、周辺機器３００のマイコン３０２は、１日単位で当該期限カウンタ３２０を１ずつカウントダウンする処理を行ない、有効期限が終了した場合（当該カウンタが０になったとき）、上記期限切れフラグ３１９にＴｒｕｅを設定する処理を行なう。このような拡張ボンディング情報３１６は、換言すれば、スマートデバイス２００（専用アプリ）と周辺機器３００との接続が許可されるか否かを示すための情報であるともいえる。

【００６０】

なお、他の実施例では、上述した「未ボンディング」であるか「ボンディング済み」であるかを示すフラグを、当該拡張ボンディング情報３１６に持たせるようにしてもよい。そして、このフラグを用いてボンディング済みか否かを判定するような構成としても良い

。
【００６１】
図７に戻り、ＡＰＰ＿ＩＤ３１７は、専用アプリを識別するためのアプリケーションＩＤである。本実施形態では、このデータは主に専用アプリの正当性の確認等のために用いられる。また、一旦周辺機器が正常に認証された後、専用アプリが再度起動された際、認証サーバを用いた認証処理を省略するために、このデータを利用したチェック処理が行なわれる。
【００６２】
ＢＴ＿Ｋｅｙ３１８は、周辺機器３００とスマートデバイス２００（専用アプリ）との間で暗号化通信を行なう際に「鍵」として用いられるデータである。これは、後述の認証処理の過程で生成される。周辺機器が正常に認証された後、周辺機器３００とスマートデバイス２００（専用アプリ）との間では、当該ＢＴ＿Ｋｅｙ３１８で各種データを暗号化したうえで送受信が行なわれる。
【００６３】
また、図示は省略するが、周辺機器３００のＲＡＭ３０４には、後述の認証処理において必要となる各種データが適宜生成されて記憶される。
【００６４】
次に、スマートデバイス２００の記憶部２０４に記憶されるデータについて説明する。図９は、スマートデバイス２００の記憶部２０４に記憶されるデータを示す図である。記憶部２０４には、専用アプリプログラム２１１と、ＡＰＰ＿ＩＤ２１２と、ボンディング情報２１３と、クライアント証明書２１４と、ＢＴ＿Ｋｅｙ２１５等が記憶される。
【００６５】
専用アプリプログラム２１１は、後述する認証処理のうち、スマートデバイス側での処理を実行するためのプログラムである。ＡＰＰ＿ＩＤ２１２は、当該専用アプリプログラムに対応するアプリケーションＩＤである。なお、認証処理が正常に行われたことを前提とすれば、上記周辺機器３００に記憶されているＡＰＰ＿ＩＤ３１７は当該ＡＰＰ＿ＩＤ２１２と同じものとなる。以下の説明では、ＡＰＰ＿ＩＤ３１７およびＡＰＰ＿ＩＤ２１２を総称し、「アプリケーションＩＤ」の意味で単にＡＰＰ＿ＩＤと記載することもある。
【００６６】
ボンディング情報２１３は、スマートデバイス２００と周辺機器３００との接続の組み合わせに関する情報である。上記周辺機器３００におけるボンディング情報３１４と対になる関係である。その構成としては、上記周辺機器３００におけるボンディング情報３１４のデータ構成のうち、拡張ボンディング情報３１６を省いた構成（つまり、実質的に基本ボンディング情報３１５のみ）となる。
【００６７】
クライアント証明書２１４は、認証サーバ１００への正当なアクセス権を有すること等を証明するためのデータである（いわゆるアクセスコントロールのために用いられるデータである）。専用アプリのユーザアカウントの登録の際に生成されるデータである（認証局も兼ねた認証サーバ１００から発行される）。また、当該クライアント証明書２１４には、いわゆるクライアント公開鍵およびクライアント秘密鍵も含まれている。この鍵を用いることで、スマートデバイス２００と通信相手（認証サーバ１００）との間での暗号化通信が可能となる。
【００６８】
ＢＴ＿Ｋｅｙ２１５は、周辺機器３００とスマートデバイス２００（専用アプリ）との間で暗号化通信を行なうための鍵となるデータである。認証処理が正常終了すれば、最終的に、当該データが記憶されていることになる。そして、その内容は、上記ＢＴ＿Ｋｅｙ３１８と同じ内容である。なお、以下の説明では、ＢＴ＿Ｋｅｙ３１８、ＢＴ＿Ｋｅｙ２１５（更には、認証サーバ１００で一時的に記憶されるＢＴ＿Ｋｅｙ）が同じ内容であることに鑑み、暗号化通信用の「鍵」という意図で、総称してＢＴ＿Ｋｅｙと呼ぶこともあ

る。
【００６９】
　また、図示は省略するが、本実施形態の処理で必要なその他のデータも適宜記憶部２０４に記憶される。
【００７０】
　次に、本実施形態にかかる認証処理の流れについて説明する。なお、説明の便宜上、以下では当該認証処理をいくつかの「フェーズ」に分けて説明する。まず、図１０を用いて、本実施形態にかかる認証処理のフローの全体像と、各フェーズで行なわれる処理の概略を説明する。その後、各フェーズにおける処理の詳細を説明する。図１０では、左から認証サーバ１００、スマートデバイス２００、周辺機器３００の順でそれぞれにおける処理のフェーズを示している。各フェーズは縦方向に時系列で並べている。横方向の矢印は、データの送受信が行なわれることを示す。
【００７１】
　まず、第１フェーズ処理での処理概要について説明する。このフェーズの処理は、スマートデバイス２００と周辺機器３００との間で行なわれる処理である。主に、スマートデバイス２００（専用アプリ）と周辺機器３００との間の接続確立の処理と、認証サーバ１００との通信を伴う認証処理の必要性を判定する処理が実行される。認証サーバ１００との通信を伴う認証処理が不要と判断された場合は、周辺機器側にて、通信相手であるスマートデバイス２００（専用アプリ）の正当性を検証するための比較的簡易な検証処理が行なわれる。検証に成功すれば、当該プロセスにかかる認証処理が終了し、周辺機器３００が通常起動することになる。
【００７２】
　次に、第２フェーズ処理の概要について説明する。このフェーズの処理は、認証サーバ１００、スマートデバイス２００、周辺機器３００の３者間で行なわれる。主に、このフェーズでは、上記ＢＴ＿Ｋｅｙ３１８の生成処理や、認証サーバ側における周辺機器３００や専用アプリの正当性を検証する処理が実行される。
【００７３】
　次に、第３フェーズ処理の概要について説明する。このフェーズの処理は、認証サーバ１００とスマートデバイス２００との間で行なわれる。主に、スマートデバイス２００（専用アプリ）から認証サーバ１００にクライアント証明書を送信し、認証サーバ１００側で当該クライアント証明書を検証する処理が実行される。つまり、クライアント証明書に基づいて、スマートデバイス２００のアクセス権限の正当性（認証サーバ１００へのアクセスが許可される端末であるか否か）をチェックする処理が実行される。なお、専用アプリの初回起動時は、クライアント証明書がまだ作成されていない（ユーザアカウントがまだ作成されていない）ため、ユーザアカウントの作成処理が行なわれる（その結果、クライアント証明書も作成される）。
【００７４】
　次に、第４フェーズ処理の概要を説明する。このフェーズの処理は、認証サーバ１００、スマートデバイス２００、周辺機器３００の３者間で行なわれる。但し、スマートデバイス２００は主に中継役であり、実質的には認証サーバ１００と周辺機器３００との間でのやりとりとなる。このフェーズでは、以降のフェーズで行なわれる暗号化通信に先立って、認証サーバ１００と周辺機器３００との間で、信頼できる通信相手であるかをお互いに確認するための処理が行なわれる。
【００７５】
　次に、第５フェーズ処理の概要を説明する。このフェーズの処理も、認証サーバ１００、スマートデバイス２００、周辺機器３００の３者間で行なわれるが、スマートデバイス２００は主に中継役であり、実質的には認証サーバ１００と周辺機器３００との間でのやりとりとなる。このフェーズの処理では、主に、次回以降の認証処理を省略できるようにするためのデータを、認証サーバ１００から周辺機器３００に暗号化して送信する処理等が実行される。

【００７６】
次に、第６フェーズ処理の概要について説明する。このフェーズの処理は、認証サーバ１００とスマートデバイス２００との間で行なわれる。このフェーズでは、認証サーバ１００からスマートデバイス２００（専用アプリ）に、周辺機器３００との間で暗号化通信を行なう際の「鍵」データ（上記ＢＴ＿Ｋｅｙ）を送信する処理が実行される。
【００７７】
以下、各フェーズの処理の詳細を説明する。ここで、以下の説明においては、図面（フローチャート）で示される各処理について参照符号を付している。この参照符号については、以下の命名規則に沿うものとする。すなわち、”フェーズ番号略称”－”実行主体略称”－”ステップ番号”、という命名規則に沿って付すものとする。フェーズ番号略称は、例えばフェーズ１は”Ｐｈ１”と示す。実行主体略称は、認証サーバを”ＳＶ”、スマートデバイスを”ＳＤ”、周辺機器を”ＰＰ”とする。ステップ番号は、”Ｓｎ（ｎは整数）”とする。例えば、フェーズ１において周辺機器で行なわれる一つ目の処理の場合は、「Ｐｈ１－ＰＰ－Ｓ１」のように示す。
【００７８】
なお、当該処理の開始に際しては、周辺機器３００が通電しており、正常に利用可能な状態であって、また、スマートデバイス２００もインターネット通信が可能な状態（認証サーバ１００と通信可能な状態）であるものとする。このよう状態で、スマートデバイス２００において上記専用アプリが起動されると、以下に説明する処理が開始される。
【００７９】
また、以下の説明において、各処理の実行主体は、認証サーバ１００は処理部１０１が実行主体となり、スマートデバイス２００は処理部２０１が実行主体となり、周辺機器３００はマイコン３０２が実行主体であるものとする。

【００８０】
まず、第１フェーズ処理の詳細について説明する。図１１は、第１フェーズ処理の詳細を示すフローチャートである。図１１における左側のフローがスマートデバイス（専用アプリ）側の処理、右側のフローが周辺機器３００側の処理の流れを示している。上記のように、この処理では、主にスマートデバイス２００と周辺機器３００との間の接続の確立と、認証処理の必要性を判定する処理が実行される。認証処理が不要と判断された場合は、その時点で当該プロセスにかかる認証処理が終了し、周辺機器３００が通常起動することになる。まず、専用アプリが起動されると、周辺機器３００とスマートデバイスとの間の接続を確立するための処理が実行される（Ｐｈ１－ＳＤ－Ｓ１およびＰｈ１－ＰＰ－Ｓ１）。この接続の確立処理は、ブルートゥース規格に沿った手法で行なわれる。
【００８１】
なお、本実施形態では、専用アプリの起動時にスマートデバイス２００と周辺機器３００との接続を確立させる例を示しているが、他の実施例では、専用アプリの起動前に、スマートデバイス２００と周辺機器３００との接続の確立を済ませておくようにしてもよい（例えばシステム側の制御で接続確立だけが行なわれる等）。この場合でも、両者の接続が確立しているだけであり、まだ専用アプリから周辺機器３００が使用できるかどうかは不明な状態である。
【００８２】
スマートデバイス２００と周辺機器３００との間で接続が確立されれば、次に、ボンディング情報をチェックする処理が実行される（Ｐｈ１－ＳＤ－Ｓ２およびＰｈ１－ＰＰ－Ｓ２）。具体的には、まず、「ボンディング済み」であるか「未ボンディング」であるかの判定が行なわれる。これは、スマートデバイス２００では、ボンディング情報２１３を参照することで、周辺機器３００では、ボンディング情報３１４を参照することで判定される（例えば、通信相手のＢＴ＿Ａｄｄｒが記憶されているか否か等で判定可能）。そして、それぞれでの判定結果を互いに送受信することで、「ボンディング済み」か「未ボンディング」かが判定される。この結果、「ボンディング済み」と判定された場合は、更に

、ボンディング情報３１４の有効期限が終了しているか否かの判定も実行される。これは、周辺機器３００において、拡張ボンディング情報３１６の期限切れフラグ３１９を参照することで判定される。そして、その結果を示すデータが周辺機器３００からスマートデバイス２００に送信されることで、スマートデバイス側でも有効期限が終了しているか否かを把握することが可能である。

【００８３】

上記のボンディング情報をチェックの結果、「未ボンディング」の場合、あるいは、「ボンディング済み」ではあるがその有効期限が終了していると判定された場合は、以下の処理はスキップされて、後述の第２フェーズ処理へと処理が進められる。

【００８４】

一方、「ボンディング済み」であり且つその有効期限内である場合は、次のような処理が実行される。まず、周辺機器３００からスマートデバイス２００に対して、ＡＰＰ_ＩＤ２１２の送信要求が送られる（Ｐｈ１－ＰＰ－Ｓ３）。この要求を受けたスマートデバイス２００では、ＡＰＰ＿ＩＤ２１２が記憶部から読み出され、これが周辺機器３００に返信される（Ｐｈ１－ＳＤ－Ｓ３）。次に、周辺機器３００において、返信されてきたＡＰＰ＿ＩＤ２１２を検証する処理が実行される（Ｐｈ１－ＰＰ－Ｓ４）。この検証処理は、次のようにして行なわれる。すなわち、周辺機器３００において、不揮発メモリ３０３に記憶されているＡＰＰ＿ＩＤ３１７と、返信されてきたＡＰＰ＿ＩＤ２１２が一致するか否かを判定し、一致すれば、検証成功と判定する。なお、不揮発メモリ３０３に記憶されているＡＰＰ＿ＩＤ３１７は、この後説明する処理の過程で（換言すれば、認証処理が正常終了した場合に）当該不揮発メモリ３０３に記憶されたものである。

【００８５】

上記のＡＰＰ＿ＩＤの検証の結果、検証が成功すれば、認証サーバ１００を用いた認証処理が不要であると判断されることになる。その結果、この時点で本実施形態にかかる認証処理は終了し、周辺機器３００が通常起動することになる。

【００８６】

一方、周辺機器３００側におけるＡＰＰ＿ＩＤの検証が失敗した場合は、認証サーバ１００を用いた認証処理を行なうための処理が実行される。具体的には、ボンディング情報３１４の期限切れフラグ３１９にＴｒｕｅを設定する処理が実行される。つまり、強制的にボンディング情報を有効期限切れの状態とする処理が実行される。その後、上記ボンディング情報のチェック処理（Ｐｈ１－ＳＤ－Ｓ２およびＰｈ１－ＰＰ－Ｓ２）に戻るような制御が行なわれる。その結果、ボンディング情報の有効期限切れと判定され、フェーズ２の処理へと進むことになる。

【００８７】

なお、周辺機器３００側におけるＡＰＰ＿ＩＤの検証が失敗する場合としては、初回起動時や所定期間接続していないことによるボンディングの有効期限の経過の他、周辺機器３００に記憶されているＡＰＰ＿ＩＤ２１２とは異なるＡＰＰ＿ＩＤがスマートデバイス２００から返信された場合もあり得る。例えば専用アプリＡ、専用アプリＢという２種類の異なる専用アプリがある場合において、専用アプリＡを起動して認証処理を一旦行なったとする。その結果、専用アプリＡのＡＰＰ＿ＩＤが周辺機器３００に記憶される状態となる。その後、専用アプリＢを起動して当該周辺機器３００に接続しにいった場合に、このような異なるＡＰＰ＿ＩＤが周辺機器３００に送られてくることになる。このような場合、上記のように強制的にボンディング情報を有効期限切れの状態として、改めて専用アプリＢを用いた認証処理が実行されることになる。その結果、周辺機器３００には、専用アプリＢのＡＰＰ＿ＩＤが記憶されることになる。

【００８８】

また、例えば、仮に専用アプリ以外のアプリから当該接続確立済みの周辺機器３００にアクセスし、当該周辺機器３００の機能を利用しようとしたような場合も、上記のようなＡＰＰ＿ＩＤのチェック処理の結果、実質的に利用できないという結果になる。例えば、周辺機器３００からのＡＰＰ_ＩＤ２１２の送信要求に対して、専用アプリ以外のアプリ

では、この要求に応えられない場合や、上記のように、周辺機器３００の不揮発メモリ３０３に記憶されているＡＰＰ＿ＩＤ３１７とは一致しないＡＰＰ＿ＩＤ２１２が送られる場合である。

【００８９】

また、例えば周辺機器３００が純正品ではないような場合は、上記ボンディング情報のチェック処理の後、周辺機器３００からのＡＰＰ＿ＩＤ２１２の送信要求がスマートデバイス２００側に送られてこないと考えられる。そのため、例えば、専用アプリにおいて、上記ボンディング情報のチェック処理の後、所定時間経過しても周辺機器側からＡＰＰ＿ＩＤの送信要求が来ない場合（タイムアウトした場合）、認証失敗と判断して、失敗時を想定した所定の処理を実行するようにしてもよい。

【００９０】

次に、第２フェーズ処理の詳細について説明する。図１２は、第２フェーズ処理の詳細を示すフローチャートである。図１２では、左側のフローが認証サーバ１００側の処理、中央のフローがスマートデバイス（専用アプリ）側の処理、右側のフローが周辺機器３００側の処理の流れを示している。このフェーズでは、ＢＴ＿Ｋｅｙ３１８の生成処理や、認証サーバ１００側における周辺機器３００や専用アプリの正当性を検証する処理が実行される。

【００９１】

まず、周辺機器３００において、ＢＴ＿Ｋｅｙ３１８を生成する処理が実行される（Ｐｈ２－ＰＰ－Ｓ１）。具体的には、ＢＴ＿Ａｄｄｒ３１１および所定の乱数（後述の第１乱数ＲＡＮＤ１や第２乱数ＲＡＮＤ２とは異なる乱数である）を用い、所定の処理によってＢＴ＿Ｋｅｙ３１８が生成され、不揮発メモリ３０３に記憶される。この所定の処理としては、例えば、いわゆるＡＥＳ（Advanced Encryption Standard）のアルゴリズムを用いてＢＴ＿Ｋｅｙ３１８を生成する処理がある。

【００９２】

次に、周辺機器３００において、第１乱数ＲＡＮＤ１を生成する処理が実行される。そして、当該ＲＡＮＤ１を上記ＢＴ＿Ｋｅｙ３１８を用いて暗号化する処理が実行される（Ｐｈ２－ＰＰ－Ｓ２）。なお、ここでいう「乱数」には、「真性乱数」の他、「疑似乱数」も含むものとする。また、ＢＴ＿Ｋｅｙ３１８がＡＥＳ鍵であるため、ＲＡＮＤ１はＡＥＳ方式で暗号化されることになる。

【００９３】

次に、周辺機器３００において、不揮発メモリ３０３から読み出したＢＴ＿Ａｄｄｒ３１１およびＢＴ＿Ｓｉｇｎ３１２と、上記生成したＢＴ＿Ｋｅｙ３１８および、ＢＴ＿Ｋｅｙ３１８で暗号化された第１乱数ＲＡＮＤ１を、Ｐｕｂ＿Ｋｅｙ３１３で暗号化する処理が実行される（Ｐｈ２－ＰＰ－Ｓ３）。

【００９４】

続いて、周辺機器３００において、上記暗号化されたＢＴ＿Ａｄｄｒ３１１、ＢＴ＿Ｓｉｇｎ３１２、ＢＴ＿Ｋｅｙ３１８、および第１乱数ＲＡＮＤ１を、その送信宛先を認証サーバ１００に設定して、スマートデバイス２００に送信する処理が実行される（Ｐｈ２－ＰＰ－Ｓ４）。

【００９５】

次に、スマートデバイス２００において、上記送信宛先を判別し、周辺機器３００から受信したデータを認証サーバ１００に送信する（中継する）処理が実行される（Ｐｈ２－ＳＤ－Ｓ１）。つまり、スマートデバイス２００を経由して、周辺機器３００から認証サーバ１００へ上記暗号化されたＢＴ＿Ａｄｄｒ３１１、ＢＴ＿Ｓｉｇｎ３１２、ＢＴ＿Ｋｅｙ３１３、および第１乱数ＲＡＮＤ１が送信されることになる。

【００９６】

次に、認証サーバ１００において、スマートデバイス２００から送られてきた上記各データを受信し、記憶部１０２に記憶する処理が実行される（Ｐｈ２－ＳＶ－Ｓ１）。

【００９７】

次に、認証サーバ１００において、スマートデバイス２００（専用アプリ）に対して、「ＡＰＰ＿ＩＤ２１２の送信要求」を送る処理が実行される（Ｐｈ２－ＳＶ－Ｓ２）。この要求を受けたスマートデバイス２００では、ＡＰＰ＿ＩＤ２１２を記憶部２０４から読み出し、これを認証サーバ１００に返信する処理が実行される（Ｐｈ２－ＳＤ－Ｓ２）。次に、認証サーバ１００において、返信されてきたＡＰＰ＿ＩＤ２１２を検証する処理が実行される（Ｐｈ２－ＳＶ－Ｓ３）。この検証処理は、次のようにして行なわれる。すなわち、認証サーバ１００において、返信されてきたＡＰＰ＿ＩＤ２１２と同じ名前のアプリテーブル１１４をデータベース１１３から検索する。その結果、見つからない場合は、現在通信相手となっている専用アプリは正規の専用アプリではない可能性があると判断される。その結果、検証は失敗したとして、検証失敗時を想定した所定の処理が実行される（例えば、所定のエラーメッセージをスマートデバイスに送信する等）。本実施形態にかかる認証処理も、この時点で終了することになる。

【００９８】

一方、アプリテーブル１１４が検索できた場合（ＡＰＰ＿ＩＤ２１２の検証に成功したことになる）は、認証サーバ１００において、次に、上記スマートデバイス２００から受信した暗号化データを復号化する処理が実行される（Ｐｈ２－ＳＶ－Ｓ４）。具体的には、認証サーバ１００において、Ｐｖｔ＿Ｋｅｙ１１２を用いて上記暗号化データをそれぞれ復号化する処理が実行される。なお、第１乱数ＲＡＮＤ１に関しては、ＢＴ＿Ｋｅｙ３１８で暗号化されたうえで、更にＰｕｂ＿Ｋｅｙ３１３で暗号化されて送信されている（つまり２重で暗号化されている）。そのため、この復号化の時点では、ＢＴ＿Ｋｅｙ３１８によりまだ暗号化されている状態のものが得られることになる。

【００９９】

次に、認証サーバ１００において、上記復号化処理で得られたＢＴ＿Ｓｉｇｎ３１２を検証する処理が実行される（Ｐｈ２－ＳＶ－Ｓ５）。具体的には、認証サーバ１００において、ＢＴ＿Ｓｉｇｎ３１２をＶｆ＿Ｋｅｙ１１１で検証する処理が実行される。これにより、ＢＴ＿Ａｄｄｒ３１１が通信路の途中で改ざんされていないか、通信相手となる周辺機器３００が純正品であるかどうか、についてチェックすることができる。検証の結果、検証に失敗した場合は、検証失敗時を想定した所定の処理が実行され、本実施形態にかかる認証処理も、この時点で終了する。

【０１００】

一方、ＢＴ＿Ｓｉｇｎ３１２の検証に成功した場合は、次に、認証サーバ１００において、上記復号化で得られたＢＴ＿Ａｄｄｒ３１１を検証する処理が実行される（Ｐｈ２－ＳＶ－Ｓ６）。具体的には、認証サーバ１００において、上記検索されたアプリテーブル１１４から、上記周辺機器３００から得られたＢＴ＿Ａｄｄｒ３１１と一致するＢＴ＿Ａｄｄｒ１１５を検索する処理が実行される。その結果、見つからない場合は、周辺機器３００が純正品ではない可能性があるとして、検証は失敗したと判定される。そして、検証失敗時を想定した所定の処理が実行される。一方、一致するＢＴ＿Ａｄｄｒ１１５が見つかった場合は、検証に成功したと判定される。このとき、図示は省略するが、ＢＴ＿Ａｄｄｒの検証に成功した旨を示す所定のメッセージを認証サーバ１００から（スマートデバイス２００経由で）周辺機器３００に送信するようにしてもよい（つまり、この時点で検証成功を通知してもよい）。そして、認証処理のプロセスは、次に説明する第３フェーズ処理へ進められる。

【０１０１】

次に、第３フェーズ処理の詳細を説明する。図１３は、第３フェーズ処理の詳細を示すフローチャートである。図１３では、左側のフローが認証サーバ１００側の処理、右側のフローがスマートデバイス（専用アプリ）側の処理の流れを示している。このフェーズでは、主にスマートデバイス２００のクライアント証明書を検証するための処理が実行される。つまり、認証サーバ１００からみて、通信相手となるスマートデバイス２００が信頼できる通信相手であるか否かをチェックする処理が実行される。

【０１０２】

図１３において、まず、認証サーバ１００からスマートデバイス２００に対して、クライアント証明書要求を送信する処理が実行される（Ｐｈ３－ＳＶ－Ｓ１）。この要求を受けたスマートデバイス２００では、まず、要求されたクライアント証明書２１４を有しているか（記憶されているか）否かの判定が行なわれる（Ｐｈ３－ＳＤ－Ｓ１）。その結果、クライアント証明書２１４を有していない場合は（Ｐｈ３－ＳＤ－Ｓ１でＮＯ）、ユーザアカウントの作成処理が実行される（Ｐｈ３－ＳＤ－Ｓ２）。例えば、専用アプリを使用するためのユーザＩＤとパスワードを登録するための画面が表示され、これに対してユーザが任意のユーザＩＤとパスワードを入力する。これが認証サーバ１００に送信され、専用アプリのユーザとして、適宜アプリテーブル１１４に登録される。その後、既知の手法を用いてクライアント証明書が生成され（当該生成に際しての認証局は、例えば認証サーバ１００となる）、これがクライアント証明書２１４として記憶部２０４に記憶される。

【０１０３】

一方、既にクライアント証明書２１４を既に有している場合は（Ｐｈ３－ＳＤ－Ｓ１でＹＥＳ）、上記のアカウント作成処理は行なわれない。

【０１０４】

次に、スマートデバイス２００において、クライアント証明書２１４を認証サーバ１００に返信する処理が実行される（Ｐｈ３－ＳＤ－Ｓ３）。続いて、認証サーバ１００において、既知の手法を用いて、クライアント証明書２１４を検証する処理が実行される（Ｐｈ３－ＳＶ－Ｓ２）。例えば、クライアント証明書２１４に含まれる署名（クライアント証明書を発行したサーバがクライアント公開鍵につけた署名）を、当該クライアント証明書発行サーバの公開鍵を用いて検証する処理が実行される。クライアント証明書の検証が成功すれば、次の第４フェーズの処理へと進む。

【０１０５】

次に、第４フェーズ処理の詳細について説明する。図１４および図１５は、第４フェーズ処理の詳細を示すフローチャートである。図１４および図１５では、左側のフローが認証サーバ１００側の処理、中央のフローがスマートデバイス（専用アプリ）側の処理、右側のフローが周辺機器３００側の処理の流れを示している。このフェーズでは、主に認証サーバ１００と周辺機器３００との間で、お互いに信頼できる通信相手であるかを確認するための処理が行なわれる。

【０１０６】

まず、周辺機器側から見て、認証サーバ１００が、暗号化通信する相手として信頼できる相手であるか否か（認証サーバ１００の暗号化通信相手としての正当性）をチェックする処理が実行される。具体的には、まず、認証サーバ１００において、上記第２フェーズ処理（上記Ｐｈ２－ＳＶ－Ｓ４の処理）で得られた第１乱数ＲＡＮＤ１（その時点ではまだＢＴ＿Ｋｅｙ３１８で暗号化されている状態である）を、同じく第２フェーズ処理で得られたＢＴ＿Ｋｅｙを用いて復号化する処理が実行される。その結果、暗号化されていない第１乱数ＲＡＮＤ１が得られる。そして、当該ＲＡＮＤ１をスマートデバイス２００（を経由して周辺機器３００）に送信する処理が実行される（Ｐｈ４－ＳＶ－Ｓ１）。つまり、送信宛先としては周辺機器３００を設定して、スマートデバイス２００に送信する。

【０１０７】

次に、スマートデバイス２００では、上記宛先を判別することで、認証サーバ１００から受信した当該データを周辺機器３００に送信する処理が実行される（Ｐｈ４－ＳＤ－Ｓ１）。

【０１０８】

次に、周辺機器３００において、スマートデバイス２００経由で認証サーバから送られてきたＲＡＮＤ１と、自身が生成したＲＡＮＤ１（上記Ｐｈ２-ＰＰ-Ｓ２参照）とが一致するか否かを確認する処理が実行される（Ｐｈ４－ＰＰ－Ｓ１）。一致しなかった場合は、認証サーバ１００の正当性が確認できなかったとして、確認失敗時を想定した所定の処理が実行される。一方、一致した場合は、次に、周辺機器３００において、第１乱数ＲＡ

ＮＤ１を用いた確認処理が完了した旨を示す所定のメッセージを生成する。ここで、当該所定のメッセージは、周辺機器３００から認証サーバ１００に対する、後述の第２乱数ＲＡＮＤ２の送信依頼（発行依頼）のメッセージという性質も有する。そして、周辺機器３００において、当該所定のメッセージをＢＴ＿Ｋｅｙ３１８で暗号化する処理が実行される。そして、当該暗号化されたメッセージを、その送信宛先を認証サーバ１００に設定したうえで、スマートデバイス２００に送信する処理が実行される（Ｐｈ４－ＰＰ－Ｓ２）。スマートデバイス２００では、周辺機器３００から受信した当該メッセージを認証サーバ１００に送信する処理が実行される（Ｐｈ４－ＳＤ－Ｓ２）。

【０１０９】

次に、認証サーバ１００において、スマートデバイス２００から中継されてきた上記の暗号化メッセージを受信し、これを第２フェーズ処理で得られたＢＴ＿Ｋｅｙで復号化する処理が実行される（Ｐｈ４－ＳＶ－Ｓ２）。これにより、認証サーバ１００では、周辺機器３００における上記認証サーバ１００の暗号化通信相手としての正当性をチェックする処理が完了したことが把握できる。そして、次に、認証サーバ１００から見て、周辺機器３００が暗号化通信の相手として信頼できる相手であるか否か（周辺機器３００の暗号化通信相手としての正当性）をチェックする処理が実行される。

【０１１０】

まず、認証サーバ１００において、第２乱数ＲＡＮＤ２が生成される。そして、上記第２フェーズ処理で得られたＢＴ＿Ｋｅｙによって当該ＲＡＮＤ２が暗号化される。更に、その送信宛先を周辺機器３００に設定したうえで、当該暗号化された第２乱数ＲＡＮＤ２（以下、暗号化ＲＡＮＤ２）をスマートデバイス２００に送信する処理が実行される（Ｐｈ４－ＳＶ－Ｓ３）。スマートデバイス２００では、上記宛先を判別することで、認証サーバ１００から受信した当該暗号化ＲＡＮＤ２を周辺機器３００に送信する処理が実行される（Ｐｈ４－ＳＤ－Ｓ３）。

【０１１１】

次に、周辺機器３００において、受信した暗号化ＲＡＮＤ２をＢＴ＿Ｋｅｙ３１８で復号化する処理が実行される。そして、復号化したＲＡＮＤ２を、その送信宛先を認証サーバ１００に設定したうえで、スマートデバイス２００に送信する処理が実行される（Ｐｈ４－ＰＰ－Ｓ３）。スマートデバイス２００では、周辺機器３００から受信した当該ＲＡＮＤ２を認証サーバ１００に送信する処理が実行される（Ｐｈ４－ＳＤ－Ｓ４）。

【０１１２】

次に、認証サーバ１００において、スマートデバイス２００から受信した第２乱数ＲＡＮＤ２と、先ほど生成した第２乱数ＲＡＮＤ２とが一致しているか否かを確認する処理が実行される（Ｐｈ４－ＳＶ-Ｓ４）。一致しなかった場合は、周辺機器３００の正当性が確認できなかったとして、確認失敗時を想定した所定の処理が実行される。一方、一致した場合は、認証サーバ１００と周辺機器３００との間でお互いに暗号化通信相手として信頼できることが確認されたことになる。そのため、次の第５フェーズ処理へと進む。

【０１１３】

次に、第５フェーズ処理の詳細について説明する。図１６は、第５フェーズ処理の詳細を示すフローチャートである。図１６では、左側のフローが認証サーバ１００側の処理、中央のフローがスマートデバイス（専用アプリ）側の処理、右側のフローが周辺機器３００側の処理の流れを示している。このフェーズでは、ＡＰＰ＿ＩＤ３１７を周辺機器に登録あるいは更新する処理等が実行される（その結果、例えば専用アプリの次回起動時には、このＡＰＰ＿ＩＤ３１７が、上記第１フェーズ処理において用いられることになる）。

【０１１４】

まず、認証サーバ１００において、上記第２フェーズ処理でスマートデバイスから得られたＡＰＰ＿ＩＤを、おなじく第２フェーズ処理で周辺機器３００から得たＢＴ＿Ｋｅｙで暗号化する処理が実行される。そして、当該暗号化されたＡＰＰ＿ＩＤ（以下、暗号化ＡＰＰ＿ＩＤ）をスマートデバイス２００経由で周辺機器３００に送信する処理が実行される（Ｐｈ５－ＳＶ－Ｓ１）。スマートデバイス２００では、認証サーバ１００から受信

した暗号化ＡＰＰ＿ＩＤを周辺機器３００に送信する処理が実行される（Ｐｈ５－ＳＤ－Ｓ１）。

【０１１５】

周辺機器３００では、受信した暗号化ＡＰＰ＿ＩＤを、ＢＴ＿Ｋｅｙ３１８で復号化する処理が実行される。そして、不揮発メモリ３０３に記憶されているＡＰＰ＿ＩＤ３１７を当該復号化したＡＰＰ＿ＩＤで更新する処理が実行される。また、不揮発メモリ３０３にＡＰＰ＿ＩＤ３１７がまだ記憶されていない場合は（初回起動時の場合等）、これが新たに記憶される。これにより、最新のＡＰＰ＿ＩＤ３１７が周辺機器３００に記憶されることになる。例えば、専用アプリがバージョンアップしたような場合に、ＡＰＰ＿ＩＤも新しいものが割り当てられるとする。この場合、最新バージョンのＡＰＰ＿ＩＤが周辺機器３００に記憶されることで、古いバージョンの専用アプリからは当該周辺機器３００が利用できないことになる（なお、このような場合、上記第１フェーズ処理において、専用アプリのバージョンアップを促すようなメッセージをスマートデバイス２００側に表示するような構成としても良い）。

【０１１６】

次に、周辺機器３００において、次回以降に専用アプリを起動した際に認証サーバ１００を用いた認証処理が不要な状態となるようにボンディング情報３１４を更新するための処理が実行される。すなわち、基本ボンディング情報３１５の内容を適宜更新すると共に、拡張ボンディング情報３１６における期限切れフラグ３１９をＦａｌｓｅに更新する処理も実行される。また、期限カウンタ３２０にも、有効期限をカウントするための値が適宜設定される。周辺機器３００においては、認証処理はこれで終了する。

【０１１７】

次に、第６フェーズ処理の詳細について説明する。図１７は、第６フェーズ処理の詳細を示すフローチャートである。図１７では、左側のフローが認証サーバ１００側の処理、右側のフローがスマートデバイス（専用アプリ）側の処理の流れを示している。この処理では、暗号化通信のための鍵であるＢＴ＿Ｋｅｙを認証サーバ１００からスマートデバイス２００に渡す処理が実行される。すなわち、まず、認証サーバ１００において、上記第２フェーズ処理で周辺機器３００から得たＢＴ＿Ｋｅｙをクライアント公開鍵で暗号化する処理が実行される。当該クライアント公開鍵は、上記第３フェーズ処理で得られたクライアント証明書に含まれているものである。そして、認証サーバ１００において、当該暗号化されたＢＴ＿Ｋｅｙをスマートデバイス２００に送信する処理が実行される（Ｐｈ６-ＳＶ-Ｓ１）。

【０１１８】

次に、スマートデバイス２００において、当該暗号化されたＢＴ＿Ｋｅｙが受信される。そして、スマートデバイス２００がクライアント証明書の発行を受ける際に生成された秘密鍵（上記クライアント公開鍵と対になる鍵）を用いて、当該ＢＴ＿Ｋｅｙyを復号化する処理が実行される（Ｐｈ６-ＳＤ-Ｓ１）。そして、スマートデバイス２００において、当該復号化されたＢＴ＿ＫｅｙがＢＴ＿Ｋｅｙ２１５として記憶部２０４に記憶される。

【０１１９】

以上で、認証サーバ１００およびスマートデバイス２００における認証処理も終了する。この後は、周辺機器３００が通常起動し、専用アプリと周辺機器３００との間の通信については、上記ＢＴ＿Ｋｅｙによる暗号化が行なわれることになる。このＢＴ＿Ｋｅｙによる暗号化は、次に上記のような認証処理が行なわれるまで実行される（つまり、次に認証処理が行なわれるまでは、当該ＢＴ＿Ｋｅｙが暗号化のために用いられる）。更に、本実施形態では、ブルートゥース規格に基づく暗号化（例えばＬＴＫ：Ｌｏｎｇ　Ｔｅｒｍ　Ｋｅｙ等）も行なわれる。例えば、専用アプリで用いる各種データそのものはＢＴ＿Ｋｅｙで暗号化される。このデータが、送受信に適したパケットに含まれ、このパケット自体を、ブルートゥース規格に基づいて暗号化して送受信する。つまり、専用アプリと周辺機器３００間の通信については、ＢＴ＿Ｋｅｙによる暗号化とブルートゥース規格による

暗号化の２重の暗号化が行なわれた状態となる。そのため、仮に、ブルートゥース規格による暗号化に関して盗聴されたとしても、ＢＴ＿Ｋｅｙによる暗号化が有効であるため、データの盗聴をより強固に防止することが可能となる。

【０１２０】

このように、本実施形態では、スマートデバイスと通信可能な周辺機器の認証を行なうものである。そして、その認証処理に際して、認証サーバ１００を利用している。更に、周辺機器３００と認証サーバ１００との間にスマートデバイスを介在させる構成ではあるが、当該スマートデバイスには直接的な認証処理を行なわせないようにしている。これにより、周辺機器３００は、専用アプリがインストールされていればどのようなスマートデバイスが用いられても、セキュアな環境下での認証処理を実行することが可能となる。

【０１２１】

また、本実施形態では、周辺機器に記憶される上記ボンディング情報に有効期限を設けるようにしている。これにより、有効期限内はユーザの利便性を高めることができ、また、有効期限切れのタイミングで再度の認証処理を実行させることができる。つまり、ユーザの利便性と、周辺機器や専用アプリの正当性のチェックとの両立を図ることができる。

【０１２２】

（第２の実施形態）

次に、第２の実施形態について説明する。第２の実施形態では、上記周辺機器におけるデータ記憶部として、いわゆるセキュアメモリ（セキュア領域を有するメモリ）を利用した場合を説明する。当該セキュアメモリに記憶されたデータは、上記マイコン３０２のような、周辺機器内部のコンポーネントからのアクセスしかできないように構成されている。周辺機器の外部からは、当該セキュアメモリに記憶されているデータにはアクセスできない。例えば、当該周辺機器と無線あるいは有線接続された他の情報処理機器からは、当該セキュアメモリに記憶されているデータにはアクセスできない。

【０１２３】

第２の実施形態にかかる認証システムの全体像は、上記第１の実施形態における図１で示したシステム構成と基本的には同様である。また、ハードウェア構成については、認証サーバ１００、スマートデバイス２００については、上記第１の実施形態におけるものと同様である。そのため、これらについての詳細な説明は省略する。一方、周辺機器に関しては、上記のようなセキュアメモリが設けられている点が異なる。

【０１２４】

図１８は、第２の実施形態にかかる周辺機器４００のハードウェア構成を示す模式図である。周辺機器４００は、通信部４０１を備える。また、図示は省略するが、操作ボタンや各種センサ等、専用アプリの実行において必要な各種ハードウェアコンポーネントも備えている。通信部４０１は、例えば通信チップであり、スマートデバイス２００と無線通信を行なうための機能を有する。通信部４０１は、マイコン４０２、不揮発メモリ４０３、ＲＡＭ４０４、セキュアメモリ４０５、を有する。不揮発メモリ４０３には、後述するような処理を実行するためのプログラムやデータが記憶されている。当該プログラムはマイコン４０２によって実行されることになる。ＲＡＭ４０４には、後述の処理において必要な各種データが適宜記憶される。セキュアメモリ４０５は、上記のようにそのアクセスに制限が設けられているメモリである。本実施形態では、当該セキュアメモリ４０５に記憶されているデータにはマイコン４０２しかアクセスできないものとする。

【０１２５】

次に、第２の実施形態で実行される認証処理の処理概要について説明する。基本的には、第２の実施形態では、上記第１の実施形態と同じ目的の処理が実行される。そのため、認証処理の一部は、上記第１の実施形態と共通している。その一方で、認証処理の過程で用いるデータの一部が上記セキュアメモリ４０５に記憶される。当該セキュアメモリ４０５に記憶されているデータについては、その信頼性が高いものであるといえる。そのため、第２の実施形態では、その信頼性の高さに基づき、認証処理の一部を上記第１の実施形態と異なる処理としている。

【０１２６】
次に、第２の実施形態の処理で用いられる各種データに関して説明する。まず、認証サーバ１００に記憶されるデータについて説明する。図１９は、認証サーバ１００の記憶部１０２に記憶されるデータを示す図である。記憶部１０２には、ＢＴ＿Ｓｉｇｎ＿Ｐｕｂｋｅｙ５０１と、ＡＳ＿Ｓｅｃｋｅｙ５０２と、ＡＳ＿Ｃｅｒｔｉｆｉｃａｔｅ５０３と、アプリＩＤリスト５０６とが記憶されている。更に、記憶部１０２には、ＡＳ＿Ｓｉｇｎ＿Ｓｅｃｋｅｙ５０７と、ＢＴ＿Ｓｉｇｎ＿Ｓｅｃｋｅｙ５０８とが記憶されている。
【０１２７】
ＢＴ＿Ｓｉｇｎ＿Ｐｕｂｋｅｙ５０１は、後述する周辺機器４００に記憶されるＢＴ＿Ｃｅｒｔｉｆｉｃａｔｅ６０３を検証するための鍵データである。また、後述のＢＴ＿Ｓｉｇｎ＿Ｓｅｃｋｅｙ５０８（秘密鍵）と対になる公開鍵でもある。
【０１２８】
ＡＳ＿Ｓｅｃｋｅｙ５０２は、認証サーバ１００の秘密鍵である。ＡＳ＿Ｃｅｒｔｉｆｉｃａｔｅ５０３は、認証サーバ１００の証明書データである。当該ＡＳ＿Ｃｅｒｔｉｆｉｃａｔｅ５０３は、ＡＳ＿Ｐｕｂｋｅｙ５０４とＳｉｇｎａｔｕｒｅ５０５とで構成されている。ＡＳ＿Ｐｕｂｋｅｙ５０４は、上記ＡＳ＿Ｓｅｃｋｅｙ５０２と対の関係になる公開鍵である。Ｓｉｇｎａｔｕｒｅ５０５は、いわゆるデジタル署名である。具体的には、ＡＳ＿Ｐｕｂｋｅｙ５０４のハッシュを計算し、これを後述のＡＳ＿Ｓｉｇｎ＿Ｓｅｃｋｅｙ５０７を用いて暗号化したものである。つまり、ＡＳ＿Ｃｅｒｔｉｆｉｃａｔｅ５０３は、暗号化前のＡＳ＿Ｐｕｂｋｅｙ５０４と、暗号化されたＡＳ＿Ｐｕｂｋｅｙ５０４（＝Ｓｉｇｎａｔｕｒｅ５０５）とから構成されていることになる。
【０１２９】
アプリＩＤリスト５０６は、専用アプリのアプリケーションＩＤのリストデータである。複数の専用アプリがリリースされている場合、各専用アプリの最新バーションのアプリケーションＩＤが当該リストに格納されている。
【０１３０】
ＡＳ＿Ｓｉｇｎ＿Ｓｅｃｋｅｙ５０７、および、ＢＴ＿Ｓｉｇｎ＿Ｓｅｃｋｅｙ５０８は、認証サーバ１００をいわゆる「認証局」として機能させるためのデータである。本実施形態では、説明の便宜上、これらデータを認証サーバ１００に記憶させた例を示しているが、他の実施形態では、別途「認証局」としての役割を果たすサーバ等を設けてもよい。この場合、当該「認証局」となる機器の方にＡＳ＿Ｓｉｇｎ＿Ｓｅｃｋｅｙ５０７、および、ＢＴ＿Ｓｉｇｎ＿Ｓｅｃｋｅｙ５０８を記憶させておけばよい。
【０１３１】
ＡＳ＿Ｓｉｇｎ＿Ｓｅｃｋｅｙ５０７は、認証サーバの署名鍵である。すなわち、上記ＡＳ＿Ｃｅｒｔｉｆｉｃａｔｅ５０３のＳｉｇｎａｔｕｒｅ５０５を生成するために用いられる署名鍵である。また、ＢＴ＿Ｓｉｇｎ＿Ｓｅｃｋｅｙ５０８は、周辺機器４００の署名鍵である。後述する上記ＢＴ＿Ｃｅｒｔｉｆｉｃａｔｅ６０３のＳｉｇｎａｔｕｒｅ６０５を生成するために用いられる署名鍵である。
【０１３２】
次に、周辺機器４００に記憶されるデータについて説明する。図２０および図２１は、周辺機器４００に記憶されるデータを示す図である。まず、図２０を用いて、セキュアメモリ４０５に記憶されるデータについて説明する。セキュアメモリ４０５には、ＡＳ＿Ｓｉｇｎ＿Ｐｕｂｋｅｙ６０１と、ＢＴ＿Ｓｅｃｋｅｙ６０２と、ＢＴ＿Ｃｅｒｔｉｆｉｃａｔｅ６０３とが記憶されている。これらのデータについては、セキュアメモリ４０５に記憶されるため、その信頼度が高い（改ざんの危険性が低い等）データであるといえる。
【０１３３】
ＡＳ＿Ｓｉｇｎ＿Ｐｕｂｋｅｙ６０１は、認証サーバ１００の証明書、すなわち、上記ＡＳ＿Ｃｅｒｔｉｆｉｃａｔｅ５０３を検証するための鍵データである。また、上記ＡＳ＿Ｓｉｇｎ＿Ｓｅｃｋｅｙ５０７（秘密鍵）と対になる公開鍵でもある。ＢＴ＿Ｓｅｃｋｅｙ６０２は、周辺機器４００の秘密鍵である。ＢＴ＿Ｃｅｒｔｉｆｉｃａｔｅ６０３は

、周辺機器４００の証明書データである。当該ＢＴ＿Ｃｅｒｔｉｆｉｃａｔｅ６０３は、ＢＴ＿Ｐｕｂｋｅｙ６０４とＳｉｇｎａｔｕｒｅ６０５とで構成されている。ＢＴ＿Ｐｕｂｋｅｙ６０４は、上記ＢＴ＿Ｓｅｃｋｅｙ６０２と対の関係になる公開鍵である。Ｓｉｇｎａｔｕｒｅ６０５は、デジタル署名であり、ＢＴ＿Ｐｕｂｋｅｙ６０４のハッシュを計算し、これを上記ＢＴ＿Ｓｉｇｎ＿Ｓｅｃｋｅｙ５０８を用いて暗号化したものである。つまり、ＢＴ＿Ｃｅｒｔｉｆｉｃａｔｅ６０３は、暗号化前のＢＴ＿Ｐｕｂｋｅｙ６０４と、暗号化されたＢＴ＿Ｐｕｂｋｅｙ６０４（＝Ｓｉｇｎａｔｕｒｅ６０５）とから構成されていることになる。

【０１３４】

次に、図２１を用いて、周辺機器４００の不揮発メモリ４０３に記憶されるデータについて説明する。不揮発メモリ４０３には、ボンディング情報７０１と、ＡＰＰ＿ＩＤ７０４と、ＢＴ＿Ｋｅｙ７０５等が記憶されている。これらのデータの内容については、上述の第１の実施形態におけるボンディング情報３１４、ＡＰＰ＿ＩＤ３１７、ＢＴ＿Ｋｅｙ３１８と同じであるため、ここでは説明を省略する。

【０１３５】

なお、第２の実施形態でのスマートデバイス２００で記憶されるデータについては、基本的に、上述の第１の実施形態と同じものが記憶される（上記図９参照）。そのため、当該スマートデバイス２００で記憶されるデータについても、その詳細な説明は省略するが、専用アプリプログラム２１１については、以下に説明する処理を実行するためのプログラムが記憶される。すなわち、実現される機能としては第１の実施形態のものとは少し異なる専用アプリプログラム２１１が記憶されることになる。

【０１３６】

次に、第２の実施形態にかかる認証処理の流れについて説明する。説明の便宜上、以下では当該認証処理をいくつかの「フェーズ」に分けて説明する。まず、図２２を用いて、第２の実施形態にかかる認証処理のフローの全体像と、各フェーズで行なわれる処理の概略を説明する。その後、各フェーズにおける処理の詳細を説明する。

【０１３７】

図２２では、左から認証サーバ１００、スマートデバイス２００、周辺機器４００の順でそれぞれにおける処理のフェーズを示している。各フェーズは縦方向に時系列で並べている。横方向の矢印は、データの送受信が行なわれることを示す。

【０１３８】

まず、第１フェーズ処理の概要について説明する。当該処理では、上述の第１の実施形態における第１フェーズ処理を同様の処理が行なわれる。すなわち、スマートデバイス２００（専用アプリ）と周辺機器４００との間の接続確立の処理と、認証サーバ１００との通信を伴う認証処理の必要性を判定する処理等が実行される。

【０１３９】

次に、第２フェーズ処理の概要について説明する。このフェーズの処理は、認証サーバ１００、スマートデバイス２００、周辺機器４００の３者間で行なわれる。主に、このフェーズでは、上記周辺機器４００の証明書を認証サーバ１００で検証することで、周辺機器の正当性を判断する処理が実行される。

【０１４０】

次に、第３フェーズ処理の概要について説明する。このフェーズの処理は、認証サーバ１００とスマートデバイス２００との間で行なわれる。このフェーズでは、主に、認証サーバ１００において、専用アプリのアプリケーションＩＤをチェックする処理や、クライアント証明書を検証する処理が実行される。

【０１４１】

次に、第４フェーズ処理の概要について説明する。このフェーズの処理は、認証サーバ１００、スマートデバイス２００、周辺機器４００の３者間で行なわれるが、スマートデバイス２００は主に中継役であり、実質的には認証サーバ１００と周辺機器４００との間でのやりとりとなる。このフェーズでは、主に認証サーバ１００の証明書を周辺機器４０

０側で検証する処理が実行される。
【０１４２】
次に、第５フェーズの処理の概要について説明する。このフェーズの処理は、認証サーバ１００、スマートデバイス２００、周辺機器４００の３者間で行なわれる。但し、ここでもスマートデバイス２００は主に中継役であり、実質的には認証サーバ１００と周辺機器４００との間でのやりとりとなる。このフェーズでは、主に、認証サーバ１００と周辺機器４００との間で、暗号化通信の共通鍵を生成するために必要なデータ（後述の第１乱数ＲＡＮＤ１および第２乱数ＲＡＮＤ２）を交換する処理が行なわれる。
【０１４３】
次に、第６フェーズの処理の概要について説明する。このフェーズでは、主に、認証サーバ１００において暗号化通信に用いる共通鍵を生成し、スマートデバイス２００へ送信する処理と、周辺機器４００側でも当該共通鍵を生成する処理が行なわれる。
【０１４４】
次に、第７フェーズの処理の概要について説明する。このフェーズでは、主に、次回以降の認証処理を省略できるようにするため設定処理が実行される。
【０１４５】
以下、各フェーズの処理の詳細を説明する。以下の説明においては、図面（フローチャート）で示される各処理について参照符号を付している。この参照符号の命名規則は、上記第１の実施形態に準ずるが、ステップ番号については第１の実施形態との区別のため、３桁の数字で示す。
【０１４６】
また、上記第１の実施形態の場合と同様に、当該処理の開始に際しては、周辺機器４００が通電しており、また、スマートデバイス２００もインターネット通信が可能な状態（認証サーバ１００と通信可能な状態）であるものとする。このよう状態で、スマートデバイス２００において上記専用アプリが起動されると、以下に説明する処理が開始される。
【０１４７】
また、各処理の実行主体は、上記第１の実施形態と同様に、認証サーバ１００は処理部１０１が実行主体となり、スマートデバイス２００は処理部２０１が実行主体となり、周辺機器４００はマイコン４０２が実行主体であるものとする。
【０１４８】
まず、第２の実施形態における第１フェーズ処理について説明する。このフェーズの処理は、上記第１の実施形態における第１フェーズと同様の処理が実行される。すなわち、スマートデバイス２００と周辺機器４００との間の接続の確立と、認証サーバ１００を用いた認証処理の必要性を判定する処理等が実行される。認証サーバ１００を用いた認証処理が不要と判断されれば、周辺機器３００が通常起動する。認証サーバ１００を用いた認証処理が必要と判断されれば、以下の第２フェーズ処理に進むことになる。当該第１フェーズでの処理内容は、上記図１１を用いて説明した上記第１の実施形態における第１フェーズと同様であるため、ここではその詳細な説明は省略する。
【０１４９】
次に、第２の実施形態における第２フェーズ処理の詳細について説明する。図２３は、当該第２の実施形態にかかる第２フェーズ処理の詳細を示すフローチャートである。このフェーズでは、認証サーバ１００において周辺機器４００の正当性を確認するための処理が実行される。まず、周辺機器４００において、セキュアメモリ４０５からＢＴ＿Ｃｅｒｔｉｆｉｃａｔｅ６０３が読み出される。そして、当該読み出されたＢＴ＿Ｃｅｒｔｉｆｉｃａｔｅ６０３をスマートデバイス２００に送信する処理が実行される（Ｐｈ２-ＰＰ-Ｓ１０１）。次に、スマートデバイス２００において、周辺機器４００から受信したＢＴ＿Ｃｅｒｔｉｆｉｃａｔｅ６０３を認証サーバ１００に送信する処理が実行される（Ｐｈ２-ＳＤ-Ｓ１０１）。
【０１５０】
次に、認証サーバ１００において、スマートデバイス２００から受信したＢＴ＿Ｃｅｒ

ｔｉｆｉｃａｔｅ６０３を、ＢＴ＿Ｓｉｇｎ＿Ｐｕｂｋｅｙ５０１を用いて検証する処理が実行される。具体的には、ＢＴ＿Ｃｅｒｔｉｆｉｃａｔｅ６０３に含まれているＳｉｇｎａｔｕｒｅ６０５を復号化し、当該Ｓｉｇｎａｔｕｒｅ６０５を復号化した値とＢＴ＿Ｐｕｂｋｅｙ６０４のハッシュ値と一致するか否かを判断する。一致すれば、検証に成功したことになる。また、当該ＢＴ＿Ｃｅｒｔｉｆｉｃａｔｅ６０３は、後の処理で用いられるため、記憶部１０２に記憶される。一方、一致しなければ、検証に失敗したことになる。この場合は、検証失敗時を想定した所定の処理が実行され、本実施形態にかかる認証処理も、この時点で終了する。

【０１５１】

次に、第３フェーズ処理の詳細について説明する。ここでは、主に、スマートデバイス２００についての検証を行なう処理が実行される。図２４は、第２の実施形態にかかる第３フェーズ処理の詳細を示すフローチャートである。まず、認証サーバ１００において、スマートデバイス２００（専用アプリ）に対し、当該専用アプリに対応しているＡＰＰ＿ＩＤ２１２の送信要求を送る処理が実行される。この要求を受けたスマートデバイス２００では、ＡＰＰ＿ＩＤ２１２を記憶部２０４から読み出し、これを認証サーバ１００に返信する処理が実行される（Ｐｈ２－ＳＤ－Ｓ１０２）。

【０１５２】

次に、認証サーバ１００において、スマートデバイス２００から送られてきたＡＰＰ＿ＩＤ２１２を検証する処理が実行される（Ｐｈ２－ＳＶ－Ｓ３）。この検証処理は、次のようにして行なわれる。すなわち、認証サーバ１００において、返信されてきたＡＰＰ＿ＩＤ２１２をアプリＩＤリスト５０６から検索する処理が実行される。その結果、見つからない場合は、現在通信相手となっている専用アプリは正規の専用アプリではない可能性があると判断される。その結果、検証は失敗したとして、検証失敗時を想定した所定の処理が実行される（例えば、所定のエラーメッセージをスマートデバイスに送信する等）。本実施形態にかかる認証処理も、この時点で終了することになる。

【０１５３】

一方、アプリＩＤリスト５０６を検索した結果、ＡＰＰ＿ＩＤ２１２が見つかった場合（検証に成功した場合）は、次に、認証サーバ１００において、スマートデバイス２００に対して、クライアント証明書要求を送信する処理が実行される（Ｐｈ３－ＳＶ-Ｓ１０１）。この要求を受けたスマートデバイス２００では、まず、クライアント証明書２１４を既に有している否かの判定が行なわれる（Ｐｈ３－ＳＤ－Ｓ１０２）。その結果、クライアント証明書２１４を有していない場合は（Ｐｈ３－ＳＤ－Ｓ１０２でＮＯ）、ユーザアカウントの作成処理が実行される（Ｐｈ３－ＳＤ－Ｓ１０３）。この処理は、上記第１の実施形態における第３フェーズ処理でのアカウント作成処理を同様である。そのため、詳細な説明は省略する。

【０１５４】

一方、既にクライアント証明書２１４を有している場合は（Ｐｈ３－ＳＤ－Ｓ１０２でＹＥＳ）、上記のアカウント作成処理は行なわれない。

【０１５５】

次に、スマートデバイス２００において、クライアント証明書２１４を認証サーバ１００に返信する処理が実行される（Ｐｈ３－ＳＤ－Ｓ１０４）。続いて、認証サーバ１００において、クライアント証明書２１４を検証する処理が実行される（Ｐｈ３－ＳＶ－Ｓ１０４）。当該検証処理は、上記第１の実施形態の第３フェーズ処理でのクライアント証明書検証処理と同様の処理が行なわれる。クライアント証明書の検証が成功すれば、次の第４フェーズの処理へと進む。

【０１５６】

次に、第４フェーズ処理の詳細について説明する。このフェーズでは、周辺機器４００側で認証サーバ１００について検証する処理が実行される。図２５は、第２の実施形態における第４フェーズ処理の詳細を示すフローチャートである。まず、認証サーバ１００において、ＡＳ＿Ｃｅｒｔｉｆｉｃａｔｅ５０３（認証サーバ証明書）を記憶部１０２から

読み出し、これをスマートデバイス２００に送信する処理が実行される。次に、スマートデバイス２００において、認証サーバ１００から受信したＡＳ＿Ｃｅｒｔｉｆｉｃａｔｅ５０３を周辺機器４００に送信する処理が実行される（Ｐｈ４-ＳＤ-Ｓ１０１）。つまり、スマートデバイス２００を中継して、認証サーバ１００から周辺機器４００にＡＳ＿Ｃｅｒｔｉｆｉｃａｔｅ５０３が送信されることになる。

【０１５７】

次に、周辺機器４００において、スマートデバイス２００から受信したＡＳ＿Ｃｅｒｔｉｆｉｃａｔｅ５０３を、セキュアメモリ４０５に記憶されているＡＳ＿Ｓｉｇｎ＿Ｐｕｂｋｅｙ６０１を用いて検証する処理が実行される。具体的には、ＡＳ＿Ｃｅｒｔｉｆｉｃａｔｅ５０３の署名、すなわちＳｉｇｎａｔｕｒｅ５０５を検証する処理が実行される。その結果、検証に失敗した場合は、検証失敗時を想定した所定の処理が実行され、第２の実施形態にかかる認証処理も、この時点で終了する。一方、検証に成功すれば、次の第５フェーズの処理へと進む。

【０１５８】

次に、第５フェーズ処理の詳細について説明する。図２６および図２７は、第２の実施形態における第５フェーズ処理の詳細を示すフローチャートである。図２６および図２７では、左側のフローが認証サーバ１００側の処理、中央のフローがスマートデバイス（専用アプリ）側の処理、右側のフローが周辺機器４００側の処理の流れを示している。このフェーズでは、主に認証サーバ１００と周辺機器４００との間で、第１乱数ＲＡＮＤ１と第２乱数ＲＡＮＤ２を交換するための処理が実行される。これらの乱数は、専用アプリと周辺機器４００間の暗号化通信のために利用される共通鍵を作成するためのデータでもある。換言すれば、当該共通鍵の「種」となるデータとも言える。

【０１５９】

まず周辺機器４００において、第１乱数ＲＡＮＤ１が生成される。そして、当該第１乱数ＲＡＮＤ１を、上記受信したＡＳ＿Ｃｅｒｔｉｆｉｃａｔｅ５０３に含まれているＡＳ＿Ｐｕｂｋｅｙ５０４を用いて暗号化する処理が実行される（Ｐｈ５－ＰＰ－Ｓ１０１）。

【０１６０】

次に、周辺機器４００において、ＢＴ＿Ｃｅｒｔｉｆｉｃａｔｅ６０３に含まれているＢＴ＿Ｐｕｂｋｅｙ６０４を、ＡＳ＿Ｐｕｂｋｅｙ５０４で暗号化する処理が実行される（Ｐｈ５－ＰＰ－Ｓ１０２）。当該ＡＳ＿Ｐｕｂｋｅｙ５０４は、上記第４フェーズ処理において認証サーバ１００から送られてきたＡＳ＿Ｃｅｒｔｉｆｉｃａｔｅ５０３に含まれているものが用いられる。

【０１６１】

次に、周辺機器４００において、上記暗号化した第１乱数ＲＡＮＤ１、および、暗号化したＢＴ＿Ｐｕｂｋｅｙ６０４を、スマードデバイス２００に送信する処理が実行される（Ｐｈ５－ＰＰ－Ｓ１０３）。スマートデバイス２００では、これを認証サーバ１００に送信する処理が実行される（Ｐｈ５－ＳＤ－Ｓ１０１）。つまり、暗号化された第１乱数ＲＡＮＤ１、および、ＢＴ＿Ｐｕｂｋｅｙ６０４がスマートデバイス２００を経由して周辺機器４００から認証サーバ１００に送信されることになる。

【０１６２】

次に、認証サーバ１００では、受信したＢＴ＿Ｐｕｂｋｅｙ６０４を検証する処理が実行される（Ｐｈ５－ＳＶ－Ｓ１０１）。具体的には、受信したＢＴ＿Ｐｕｂｋｅｙ６０４をＡＳ＿Ｓｅｃｋｅｙ５０２で復号化する。そして、上記第２フェーズ処理において周辺機器４００から取得したＢＴ＿Ｐｕｂｋｅｙ６０４（上記Ｐｈ２－ＳＶ－Ｓ１０１参照）と一致するか否かを判定する処理が行なわれる。一致すれば、検証は成功となり、不一致の場合は検証に失敗したことになる。当該検証の結果、検証に失敗した場合は、検証失敗時を想定した所定の処理が実行され、本実施形態にかかる認証処理も、この時点で終了する。

【０１６３】

一方、検証に成功した場合は、次に、認証サーバ１００において、第２乱数ＲＡＮＤ２が生成される。そして、ＢＴ＿Ｐｕｂｋｅｙ６０４を用いて（上記第２フェーズ処理において取得したものでも、上記検証処理に成功したものでも、いずれを用いても良い）、当該第２乱数ＲＡＮＤ２を暗号化する処理する処理が実行される（Ｐｈ５－ＳＶ－Ｓ１０２）。

【０１６４】

次に、認証サーバ１００において、上記受信した第１乱数ＲＡＮＤ１と記憶部に記憶されているＡＳ＿Ｐｕｂｋｅｙ５０４とを、上記同様にＢＴ＿Ｐｕｂｋｅｙ６０４で暗号化する処理が実行される（Ｐｈ５－ＳＶ－Ｓ１０３）。

【０１６５】

次に、認証サーバ１００において、上記暗号化したＡＳ＿Ｐｕｂｋｅｙ５０４、第１乱数ＲＡＮＤ１、および第２乱数ＲＡＮＤ２をスマートデバイス２００に送信する処理が実行される（Ｐｈ５－ＳＶ－Ｓ１０４）。スマートデバイス２００では、これを周辺機器４００に送信する処理が実行される（Ｐｈ５－ＳＤ－Ｓ１０２）。

【０１６６】

次に、周辺機器４００では、スマートデバイス２００経由で認証サーバ１００から送られてきた上記暗号化された各データを、ＢＴ＿Ｓｅｃｋｅｙ６０２で復号化する処理が実行される。更に、復号化した第１乱数ＲＡＮＤ１、および、ＡＳ＿Ｐｕｂｋｅｙ５０４を検証する処理が実行される（Ｐｈ５－ＰＰ－Ｓ１０４）。すなわち、認証サーバ１００から送られてきた第１乱数ＲＡＮＤ１、および、ＡＳ＿Ｐｕｂｋｅｙ５０４が、自身が送信したものと一致するか否かを判定することで、検証が行われる。この検証に失敗した場合は、検証失敗時を想定した所定の処理が実行される。当該検証に成功した場合は、次の第６フェーズ処理へと進む。

【０１６７】

なお、当該第５フェーズ処理において、周辺機器からＢＴ＿Ｐｕｂｋｅｙ６０４を認証サーバ１００に送信しているのは、ＢＴ＿Ｐｕｂｋｅｙ６０４が、いわば「発信元証明書」のような役目を有するためである。つまり、ＢＴ＿Ｐｕｂｋｅｙ６０４は、その周辺機器４００のみが知っている情報であり、かつ、セキュアメモリ４０５に記憶されているため、改ざん等の可能性も低い。そのため、発信元の証明としての信頼性は極めて高いといえる。換言すれば、セキュアメモリ４０５に記憶されている、周辺機器を特定可能な情報を用いて、認証サーバ１００での検証を行なっている。そのため、他の実施形態では、ＢＴ＿Ｐｕｂｋｅｙ６０４の代わりに、例えばＢＴ＿Ｃｅｒｔｉｆｉｃａｔｅ６０３全体を用いるようにしてもよい。

【０１６８】

また、他の実施形態では、上記第５フェーズ処理において、第１乱数ＲＡＮＤ１については周辺機器４００で生成せずに、認証サーバ１００で生成するようにしても良い。例えば、上記Ｐｈ５－ＳＶ-Ｓ１０２の処理で、認証サーバ１００で第１乱数ＲＡＮＤ１と第２乱数ＲＡＮＤ２の双方を生成し、これらをＢＴ＿Ｐｕｂｋｅｙ６０４で暗号化して周辺機器４００に送信するようにしても良い。

【０１６９】

次に、第６フェーズ処理の詳細について説明する。このフェーズでは、スマートデバイス２００および周辺機器４００との間の暗号化通信に用いられる共通鍵Ｃｏｍ＿ｋｅｙを準備（生成）するための処理が実行される。図２８は、第２の実施形態における第６フェーズ処理の詳細を示すフローチャートである。図２８では、左側のフローが認証サーバ１００側の処理、中央のフローがスマートデバイス（専用アプリ）側の処理、右側のフローが周辺機器４００側の処理の流れを示している。

【０１７０】

まず、認証サーバ１００において、上記第１乱数ＲＡＮＤ１および第２乱数ＲＡＮＤ２を用いて、共通鍵Ｃｏｍ＿ｋｅｙを生成する処理が実行される（Ｐｈ６－ＳＶ－Ｓ１０１）。次に、認証サーバ１００において、当該共通鍵Ｃｏｍ＿ｋｅｙを、クライアント公開

鍵で暗号化する処理が実行されるこのクライアント公開鍵は、上記クライアント証明書に含まれているものが用いられる。そして、暗号化された共通鍵Ｃｏｍ＿ｋｅｙをスマートデバイス２００に送信する処理が実行される（Ｐｈ６－ＳＶ－Ｓ１０２）。

【０１７１】

スマートデバイス２００においては、受信した共通鍵Ｃｏｍ＿ｋｅｙを、自身が有するクライアント秘密鍵（クライアント証明書に含まれているもの）を用いて復号化する処理が実行される（Ｐｈ６－ＳＤ－Ｓ１０１）。更に、復号化した共通鍵Ｃｏｍ＿ｋｅｙを記憶部２０４に記憶する処理も実行される。これにより、スマートデバイス２００で、周辺機器４００との暗号化通信に必要な共通鍵を入手できたことになる。

【０１７２】

一方、周辺機器４００においては、上記第１乱数ＲＡＮＤ１および第２乱数ＲＡＮＤ２を用いて、共通鍵Ｃｏｍ＿ｋｅｙを生成する処理が実行される（Ｐｈ６－ＰＰ－Ｓ１０１）。これらの乱数は、認証サーバ１００で用いられているものと同じものであるため、結果として、認証サーバ１００で生成されたものと同じ共通鍵Ｃｏｍ＿ｋｅｙが生成されることになる。以上で、第６フェーズの処理は終了する。

【０１７３】

次に、第７フェーズの処理の詳細を説明する。このフェーズでは、主に、次回以降の認証処理を省略できるようにするため設定処理等が実行される。図２９は、第２の実施形態における第７フェーズ処理の詳細を示すフローチャートである。まず、認証サーバ１００において、上記第３フェー処理でスマートデバイス２００から得たＡＰＰ＿ＩＤを上記共通鍵Ｃｏｍ＿ｋｅｙで暗号化し、ＡＳ＿Ｓｅｃｋｅｙ５０２を用いて署名する処理が実行される。そして、当該暗号化したＡＰＰ＿ＩＤをスマートデバイス２００に送信する処理が実行される（Ｐｈ７－ＳＶ－Ｓ１０１）。スマートデバイス２００では、当該受信したデータを周辺機器４００に送信する処理が実行される（Ｐｈ７－ＳＤ－Ｓ１０１）。

【０１７４】

次に、周辺機器４００において、スマートデバイス２００経由で認証サーバ１００から送られてきた上記暗号化された共通鍵Ｃｏｍ＿ｋｅｙを受信する処理が実行される。更に、上記署名を検証する処理が実行される。検証に成功すれば、上記暗号化されたＡＰＰ＿ＩＤを共通鍵Ｃｏｍ＿ｋｅｙで復号化する処理が実行される。そして、これで得られたＡＰＰ＿ＩＤで既存のＡＰＰ＿ＩＤ７０４を更新する（あるいは新規に格納する）処理が実行される（Ｐｈ７－ＰＰ－Ｓ１０１）。

【０１７５】

次に、周辺機器４００において、ボンディング情報７０１を更新する処理が実行される（Ｐｈ７－ＳＶ－Ｓ１０２）。この処理は、上記第１の実施形態の第５フェーズ処理におけるボンディング情報の更新処理を同様である。そのため、ここでは詳細な説明は省略する。

【０１７６】

以上で、第２の実施形態にかかる認証処理は正常終了したことになる。この後は、専用アプリと周辺機器４００との間の通信については、共通鍵Ｃｏｍ＿ｋｅｙを用いた暗号化が行なわれる。更に、第１の実施形態と同様、ブルートゥース規格に基づく暗号化も行なわれる。つまり、２重の暗号化によって両者の間の通信が行なわれることになる。

【０１７７】

このように、第２の実施形態では、周辺機器４００側にセキュアメモリ４０５を有する構成としている。そして、このセキュアメモリ４０５に鍵や証明書のデータを記憶する構成としている。換言すれば、上記共通鍵Ｃｏｍ＿ｋｅｙの生成にために利用される情報がセキュアメモリ４０５に記憶されていることになる。このような構成により、上記第１の実施形態に比べて、認証サーバの運用コストを低減することが可能となる。例えば、第１の実施形態では、認証サーバ１００の運用において、データベース１１３（特に、ＢＴ＿Ａｄｄｒ）の更新が必要となるが、第２の実施形態では、この更新の手間が不要となる。また、周辺機器の製造工程におけるコストを削減することも可能となる。例えば、第１の

実施形態では、周辺機器の製造工程において署名（ＢＴ＿Ｓｉｇｎ）を書き込む工程が必要となるが、第２の実施形態であれば、この工程が不要となる。

【０１７８】

なお、上述した実施形態では、認証サーバ１００と周辺機器３００（第２の実施形態では周辺機器４００）との間の通信をスマートデバイス２００が中継する構成を例として説明した。他の実施形態では、スマートデバイス２００を介さずに、周辺機器３００と認証サーバ１００とで通信を行ない、認証処理を行なうようにしても良い。例えば、周辺機器３００に無線ＬＡＮ機能を実装し、上記認証用サーバ１００と通信可能なように構成する。例えば、認証用サーバ１００と接続するためのサーバのアドレス等、所定の設定を不揮発メモリ３０３に記憶させておく。また、周辺機器自体に、簡易なユーザインターフェース（小さな液晶画面と数個の操作ボタン等）を備えておくよう構成する。ユーザは、周辺機器３００の当該ユーザインターフェースを操作して、自宅内に設置されている所定のアクセスポイントに接続するような所定の設定操作を行う。そして、周辺機器３００の初回起動時に、スマートデバイス２００を介さずに認証サーバ１００との通信を行ない、認証処理を行なうようにしてもよい（なお、この場合は、アクセスポイントという通信機器を介する構成ともいえる）。換言すれば、スマートデバイス（専用アプリ）との接続に先立って認証処理を行ない、ＡＰＰ＿ＩＤ３１７を周辺機器３００に記憶させることになる。このような場合、例えば、認証サーバ１００のデータベースの持ち方として、ＢＴ＿Ａｄｄｒ１１５を主キーとしたテーブルを有するように構成しておく（いわゆるホワイトリストに相当する）。周辺機器３００からは、ＢＴ＿Ｋｅｙ３１８、ＢＴ＿Ａｄｄｒ３１１、ＢＴ＿Ｓｉｇｎ３１２、第１乱数ＲＡＮＤ１を暗号化して認証用サーバ１００に（スマートデバイスを介さずに）送信する。認証用サーバ１００では、これらのデータに基づく検証を行なう。周辺機器３００の正当性が確認できれば、最終的に認証用サーバ１００からＡＰＰ＿ＩＤが周辺機器３００に送信される。そして、これを受信した周辺機器３００において、ＡＰＰ＿ＩＤ３１７の更新やボンディング情報３１４の更新を行なうような構成としても良い。

【０１７９】

また、認証処理が実行されるタイミングについては、周辺機器３００の初回起動時に限らず、例えば、専用アプリの起動をトリガとして、周辺機器３００と認証サーバ１００との間で認証処理を行なうような構成としても良い。専用アプリから周辺機器に接続要求が行なわれたときに、周辺機器３００においてボンディング情報の有無や有効期限のチェックを行ない、その後、認証処理が必要な場合は、周辺機器３００と認証サーバ１００との間で、スマートデバイス２００を介さない認証処理が行なわれるような構成としても良い。

【０１８０】

また、有効期限の判定に関して、上記実施例では、期限カウンタ３２０を用い、一日単位でカウントダウンする例を示した。この他、例えば、ボンディング情報３１４更新されたタイミングで、所定のカウンタに所定の値（例えば１００）を設定し、周辺機器３００とスマートデバイス２００が接続されるたびに当該カウンタを１ずつ減らすような処理を行うようにしても良い（いわば、接続回数をカウントしている）。そして、周辺機器３００とスマートデバイス２００との接続時に当該カウンタが０であるか否かを判定するようにして、０であれば、上記のような認証処理の実行を要求するような構成としてもよい。このようなカウンタも、上記有効期限を示す情報であるといえる。

【０１８１】

また、認証処理を実行するタイミングに関しては、以下のようなタイミングで行われるように構成しても良い。例えば、スマートデバイスがインターネットにオンライン接続されている状態（つまり、認証サーバと通信可能な状態）であれば、周辺機器が当該スマートデバイスに接続されるたびに、上記の認証サーバを用いた認証処理を実行するようにしても良い。また、例えば、上記専用アプリがセーブデータを保存するような構成となっている場合に、当該セーブデータが消去されたときは、（その後に周辺機器と接続されたと

きの）上記認証サーバを用いた認証処理の実行を必須とするような構成としてもよい。

【０１８２】

また、周辺機器３００に、携帯電話回線網に接続できる機能を備えるように構成し、上記のようなスマートデバイス２００を介さずに、認証サーバ１００とで通信を行うような構成としてもよい。この場合は、上記のようなユーザによる自宅のアクセスポイントへの接続設定作業は不要となる。

【０１８３】

また、上記説明でも少し触れていたが、認証サーバ１００に記憶されるアプリテーブル１１４に関して、他の実施形態では、１つのＢＴ＿Ａｄｄｒに対して複数人分のユーザＩＤ／パスワードが登録可能なように構成しても良い。そして、このような場合、次のような制御を行なうようにしても良い。認証サーバ１００において、１つの（同一の）ＢＴ＿Ａｄｄｒ１１５に対して登録されているユーザＩＤ１１６の数が、所定数を越えたか否かを判定する。その結果、ユーザＩＤ１１６の数が所定数を越えている場合は、該当するＢＴ＿Ａｄｄｒ１１５に対応する周辺機器３００の使用を許可しないような制御を行なっても良い。例えば、当該ＢＴ＿Ａｄｄｒ１１５を有する周辺機器３００からの認証の要求が来ても、認証処理を行なわないようにする。このように構成することで、例えば、１つのＢＴ＿Ａｄｄｒ１１５に対して、不自然に多くのユーザＩＤが登録されているような場合、ＢＴ＿Ａｄｄｒ３１１、ＢＴ＿Ｓｉｇｎ３１２、Ｐｕｂ＿ｋｅｙ３１３が不正にコピーされている（すなわち純正品でない周辺機器が存在している）可能性もあるが、このような場合の被害拡大を防止することが可能となる。

【０１８４】

また、上述の例では、周辺機器３００において、ＡＰＰ＿ＩＤは一つ分しか記憶しない例を挙げていた。これに限らず、他の実施形態では、周辺機器３００において複数のＡＰＰ＿ＩＤが記憶可能なように構成しても良い。例えば、周辺機器３００に対応する専用アプリＡ、専用アプリＢ、専用アプリＣの３種類の専用アプリがあると想定する。このような場合、それぞれのアプリの初回起動時をトリガとして、それぞれのアプリで認証処理が行なわれ、その結果、３つの異なるＡＰＰ＿ＩＤが周辺機器に記憶されるような構成としても良い、そして、上記第１フェーズの処理において、周辺機器３００側では、専用アプリから送信されてきたＡＰＰ＿ＩＤが、自身の記憶している複数のＡＰＰ＿ＩＤのいずれかと一致するか否かを判定するように構成すれば良い。

【０１８５】

また、上記の例では、スマートフォン等のスマートデバイス上で専用アプリを実行し、この専用アプリから周辺機器３００を利用するという例を挙げた。このスマートデバイスに関しては、他の実施形態では、パーソナルコンピュータ等の通信機器であってもよい。また、例えば、通信機能を備えた家電製品という形での通信機器であってもよい。

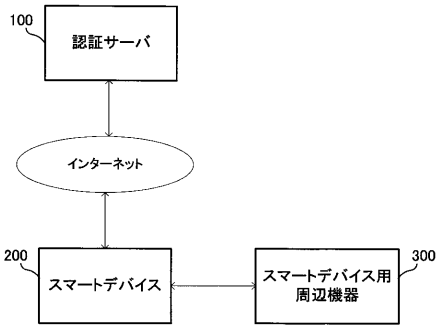
【符号の説明】

【０１８６】

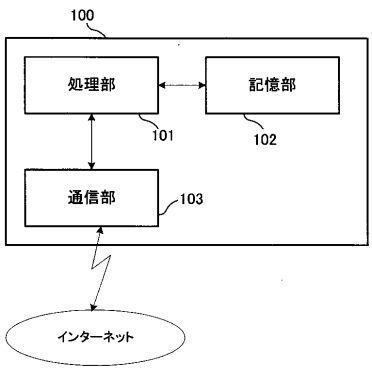
１００　認証サーバ
１０１　処理部
１０２　記憶部
１０３　通信部
２００　スマートデバイス
２０１　処理部
２０２　第１通信部
２０３　第２通信部
２０４　記憶部
２０５　入力部
２０６　表示部
３００　周辺装置
３０１　通信部

３０２　マイコン
３０３　不揮発メモリ
３０４　ＲＡＭ
４００　周辺装置
４０１　通信部
４０２　マイコン
４０３　不揮発メモリ
４０４　ＲＡＭ
４０５　セキュアメモリ

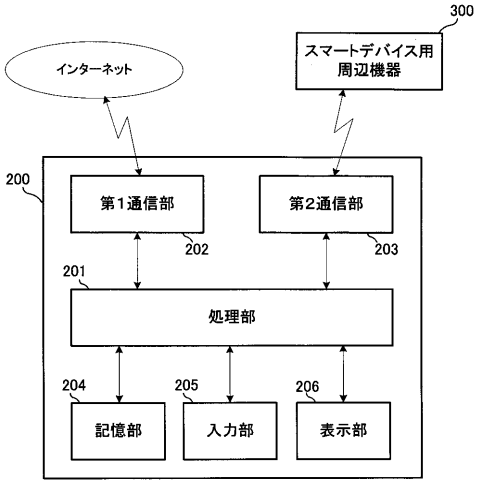
【図１】



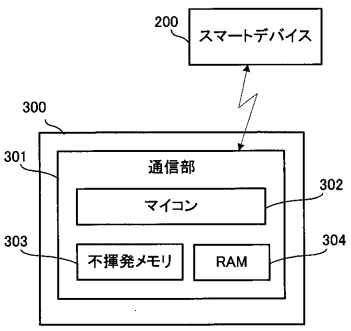
【図２】



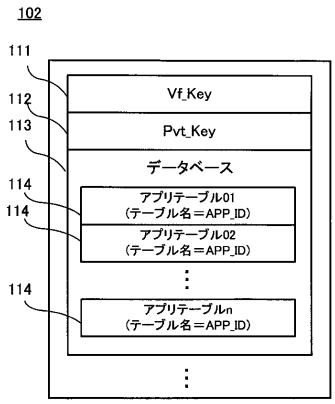
【図３】



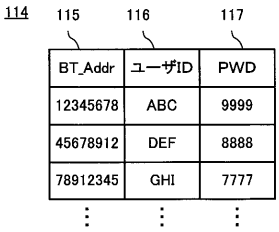
【図４】



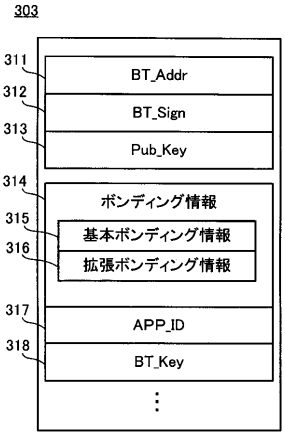
【図５】



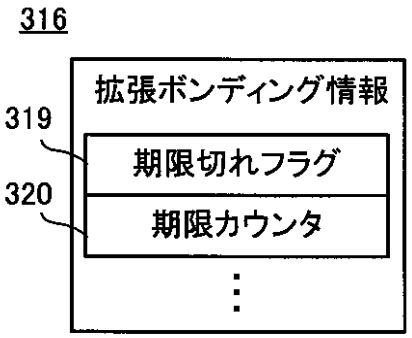
【図６】



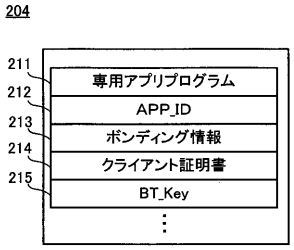
【図７】



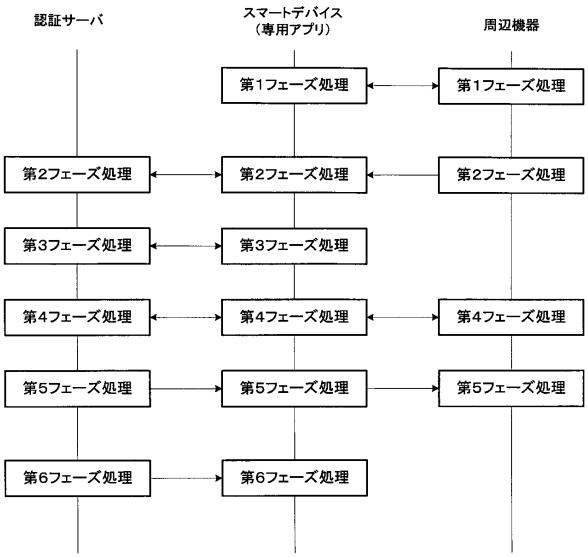
【図８】



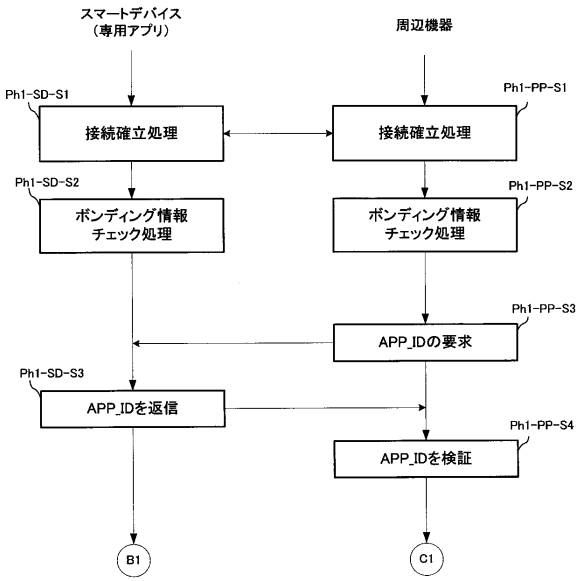
【図９】



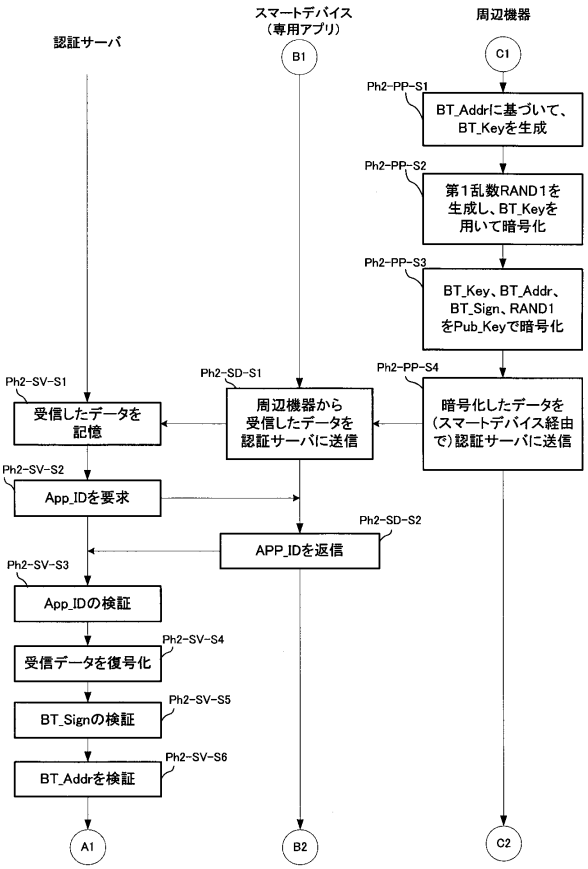
【図１０】



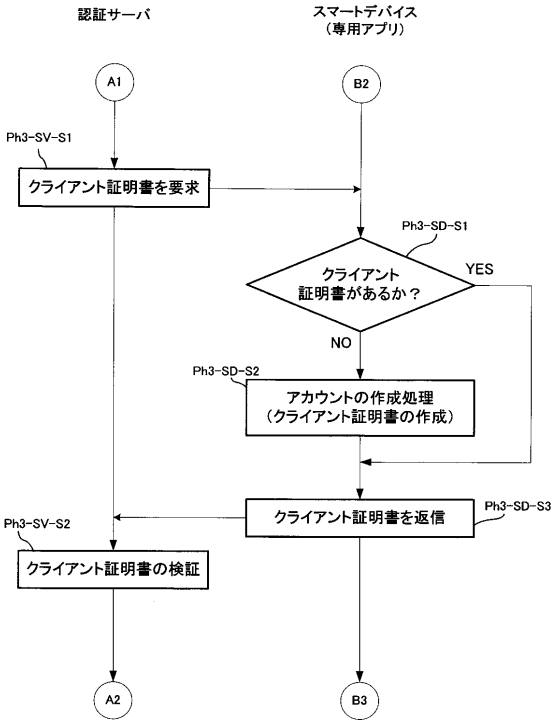
【図１１】



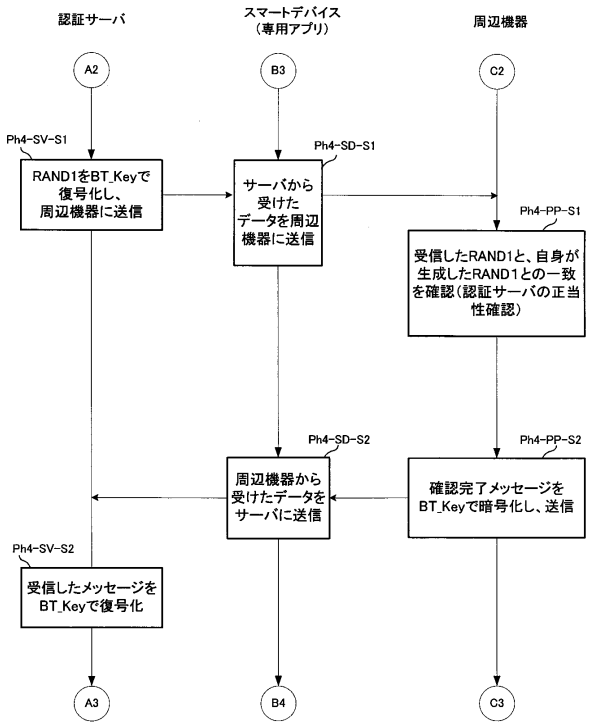
【図１２】



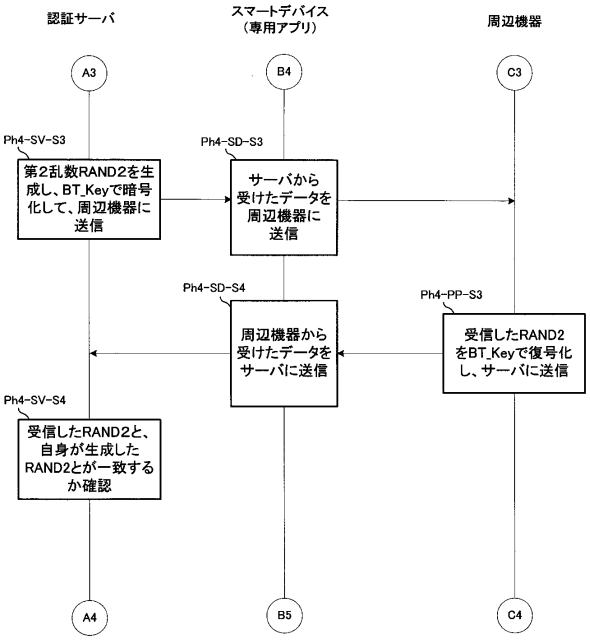
【図１３】



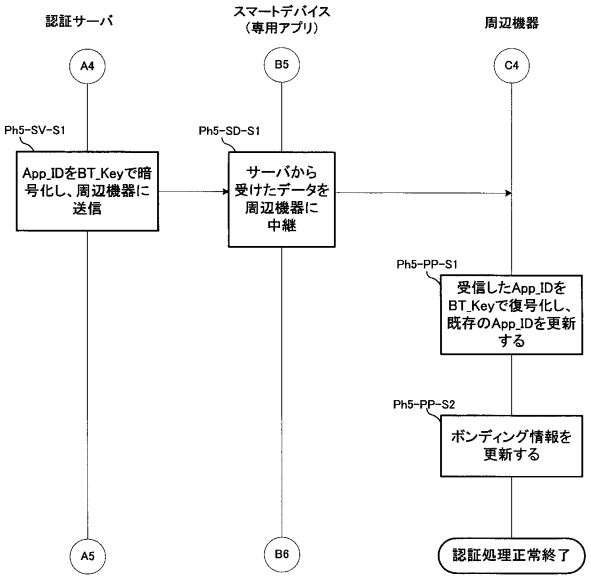
【図１４】



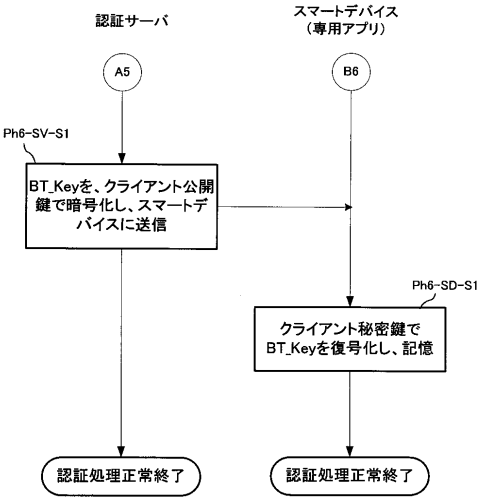
【図１５】



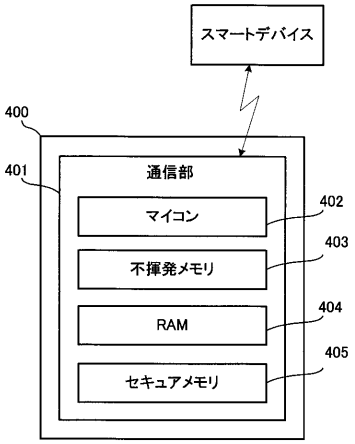
【図１６】



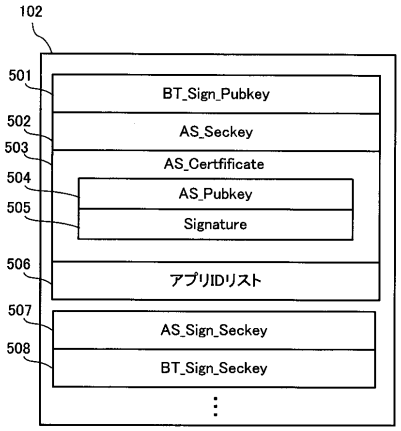
【図１７】



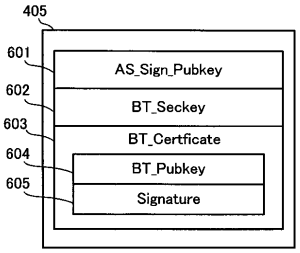
【図１８】



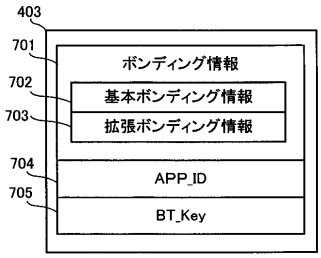
【図１９】



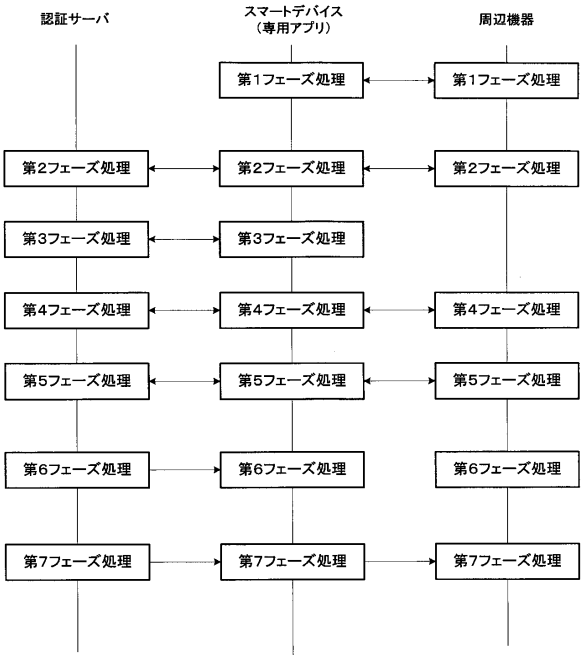
【図２０】



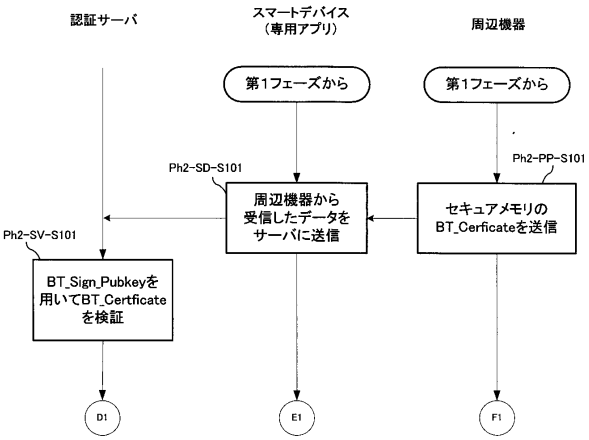
【図２１】



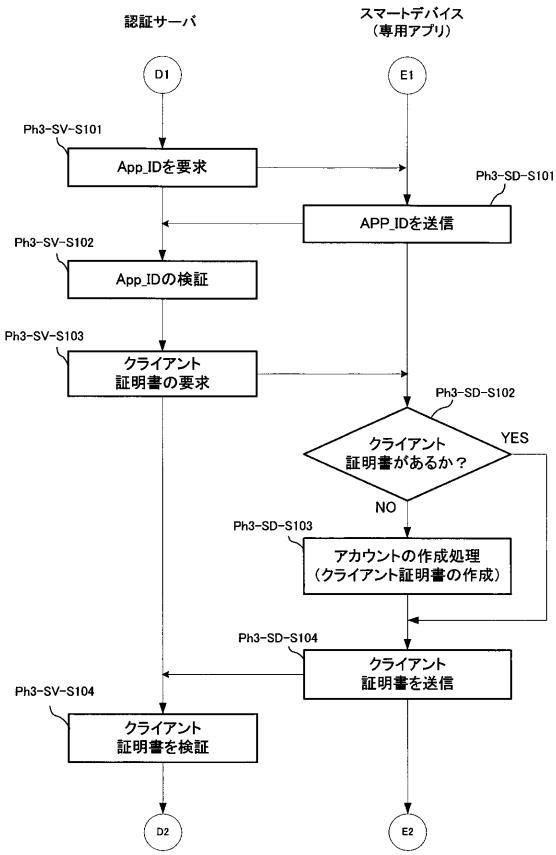
【図２２】



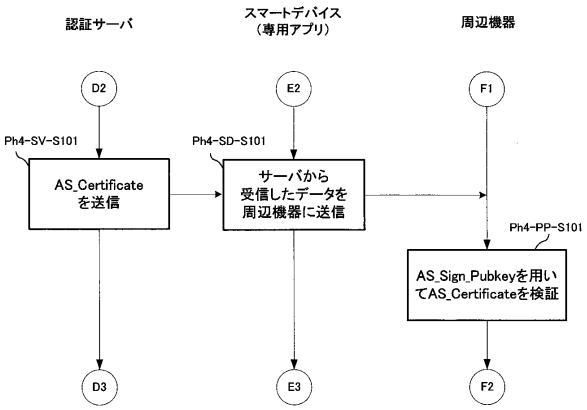
【図２３】



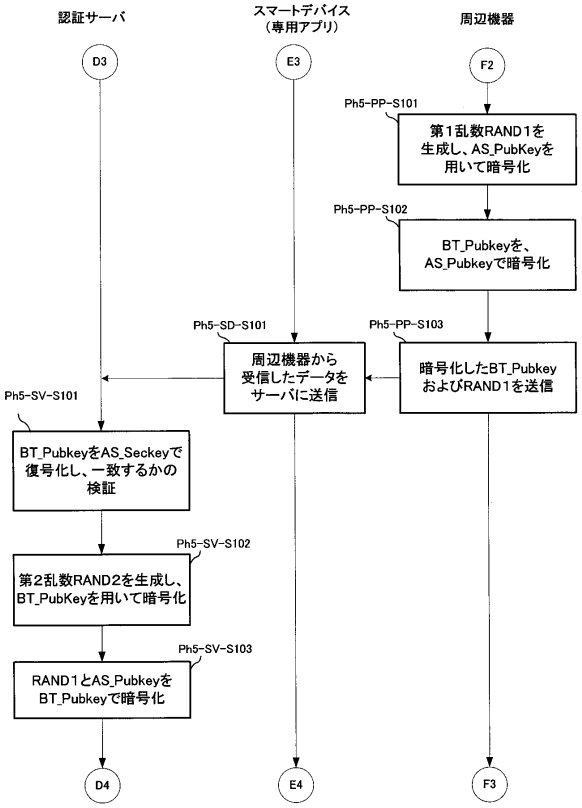
【図２４】



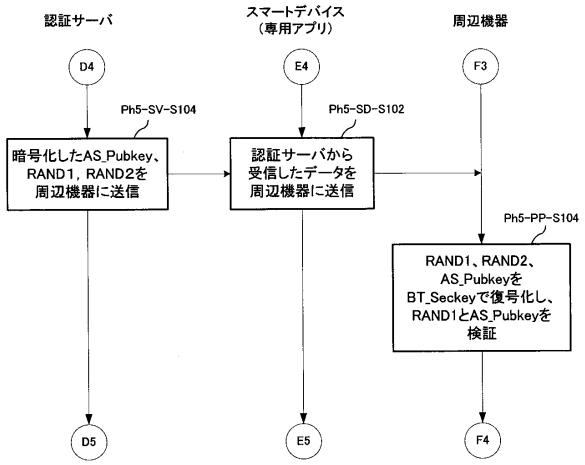
【図２５】



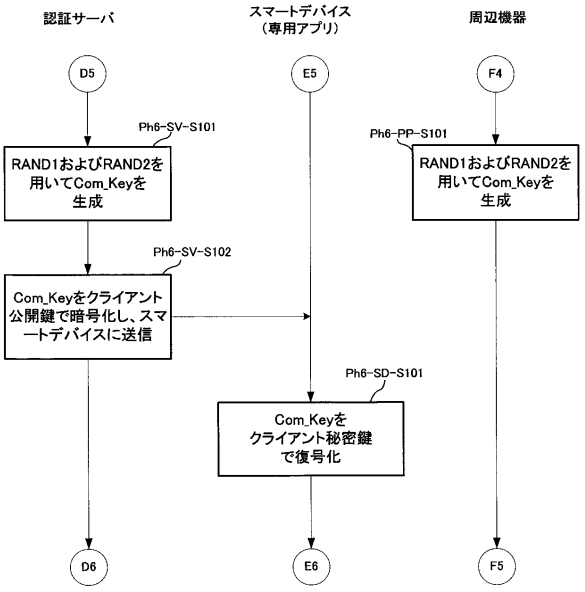
【図２６】



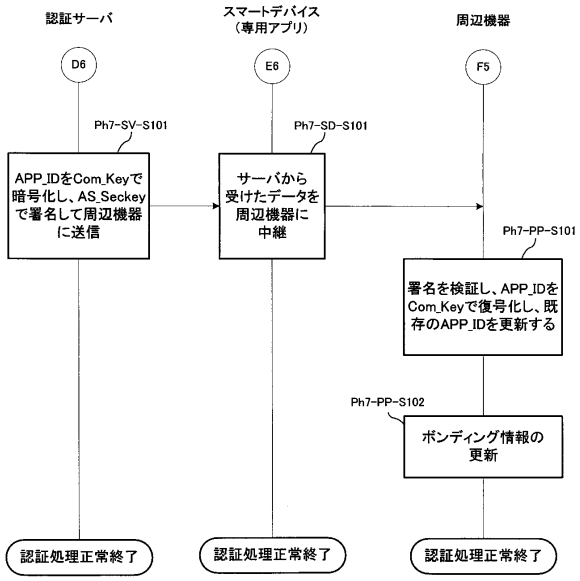
【図２７】



【図２８】



【図２９】


認証サーバ
スマートデバイス
（専用アプリ）
周辺機器
D6
E6
F5
Ph7-SV-S101
Ph7-SD-S101
APP_IDをCom_Keyで暗号化し、AS_Seckeyで署名して周辺機器に送信
サーバから受けたデータを周辺機器に中継
Ph7-PP-S101
署名を検証し、APP_IDをCom_Keyで復号化し、既存のAPP_IDを更新する
Ph7-PP-S102
ボンディング情報の更新
認証処理正常終了
認証処理正常終了
認証処理正常終了

フロントページの続き

(72)発明者　白井　達広
京都府京都市南区上鳥羽鉾立町１１番地１　任天堂株式会社内
(72)発明者　和田　純平
京都府京都市南区上鳥羽鉾立町１１番地１　任天堂株式会社内

合議体
審判長　田中　秀人
審判官　石井　茂和
審判官　山崎　慎一

(56)参考文献　特開２０１５－１２２７０４（ＪＰ，Ａ）
特開２０１５－１４６５６７（ＪＰ，Ａ）
特開２０１２－５１２６１７（ＪＰ，Ａ）
特開２００４－１３９２９５（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
H04L 9/32,H04L 9/08,G06F21/44