(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6921066号
(P6921066)
(45)発行日　令和3年8月18日(2021.8.18)　(24)登録日　令和3年7月29日(2021.7.29)

(51)Int.Cl.　　F I
G06F 21/41 (2013.01)　　G06F 21/41
G06F 21/32 (2013.01)　　G06F 21/32
H04L 9/32 (2006.01)　　H04L 9/00　673A

請求項の数 18　(全 23 頁)

(21)出願番号　特願2018-521402(P2018-521402)
(86)(22)出願日　平成28年10月18日(2016.10.18)
(65)公表番号　特表2019-502189(P2019-502189A)
(43)公表日　平成31年1月24日(2019.1.24)
(86)国際出願番号　PCT/CN2016/102323
(87)国際公開番号　WO2017/071496
(87)国際公開日　平成29年5月4日(2017.5.4)
審査請求日　令和1年10月15日(2019.10.15)
(31)優先権主張番号　201510702527.3
(32)優先日　平成27年10月26日(2015.10.26)
(33)優先権主張国・地域又は機関
中国(CN)

(73)特許権者　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】セッション識別子同期を実現する方法及びデバイス

(57)【特許請求の範囲】
【請求項１】
セッション識別子同期を実現する方法であって、端末に適用され、
サーバにアプリケーションプログラムへのログインを求める第１の要求を開始することであって、前記第１の要求は、第１のセッション識別子を含み、前記第１のセッション識別子は、前記アプリケーションプログラムのログインアカウント及び元のパスワードから生成され、前記元のパスワードは、前記ログインアカウントの修正前のログインパスワードである、ことと、
前記第１のセッション識別子が無効であると前記サーバによって決定された場合、前記端末のユーザに対する有効性検証を行うことと、取得した検証結果を前記サーバに送信して、前記サーバが、前記検証結果に対するチェックを行うことを可能にすることと、
前記サーバによって前記検証結果が検証及び承認された場合、第２のセッション識別子を前記サーバから受信し、前記第２のセッション識別子を前記端末に記憶することと
を含み、前記第２のセッション識別子は、前記ログインアカウントと新しいパスワードから生成され、前記新しいパスワードは、前記ログインアカウントの修正後のログインパスワードである、前記方法。
【請求項２】
前記方法は、
前記検証結果に対応する検証文字列の乱数を、ハッシュアルゴリズムを通して、生成することと、

前記検証文字列及び前記乱数を前記サーバの対称秘密鍵を用いて暗号化して、暗号化された検証結果を取得することと、
をさらに含む、請求項１に記載の方法。
【請求項３】
前記方法は、
前記端末の公開鍵及びプライベート鍵を非対称暗号化アルゴリズムに基づいて生成することと、
前記端末の前記公開鍵を前記サーバに送信することと、
前記端末の前記公開鍵を用いて暗号化された前記サーバの対称秘密鍵を前記サーバから受信することと、
前記暗号化された対称秘密鍵を前記端末の前記プライベート鍵を用いて解読して、前記サーバの前記対称秘密鍵を取得することと、
をさらに含む、請求項２に記載の方法。
【請求項４】
前記端末の前記ユーザに対する前記有効性検証を行うことは、
前記端末の前記ユーザの生物学的特性を前記アプリケーションプログラムのログインインタフェースでバイオメトリックセンサを用いて収集することと、
前記生物学的特性に対する検証を行うことと、
前記生物学的特性が前記検証に合格した場合、前記端末の前記ユーザは正規ユーザであると決定することと、
前記生物学的特性が前記検証に合格しなかった場合、前記ログインアカウント及び前記ログインパスワードを用いて前記アプリケーションプログラムにログインするように前記アプリケーションプログラムの前記ログインインタフェースでプロンプトを提供することと、を含む、請求項１に記載の方法。
【請求項５】
前記方法は、
前記第２のセッション識別子が有効期間内にあるか否かを決定することと、
前記第２のセッション識別子が前記有効期間内にある場合、前記アプリケーションプログラムは前記第２のセッション識別子を用いてログインされると決定することと、
前記第２のセッション識別子が前記有効期間を過ぎている場合、前記ログインアカウント及び前記ログインアカウントの有効なログインパスワードを用いて前記アプリケーションプログラムにログインするように前記ユーザにプロンプトすることと、
をさらに含む、請求項１～４のいずれか１項に記載の方法。
【請求項６】
セッション識別子同期を実現する方法であって、サーバに適用され、
アプリケーションプログラムへのログインを求める第１の要求が端末で開始される時、前記第１の要求に含まれた第１のセッション識別子の有効性を検証することであって、前記第１のセッション識別子は、前記アプリケーションプログラムのログインアカウント及び元のパスワードから生成され、前記元のパスワードは、前記ログインアカウントの修正前のログインパスワードである、ことと、
前記第１のセッション識別子が無効であると決定された場合、前記端末のユーザに対する有効性検証を行うように前記端末に命令することと、
前記ユーザの前記有効性検証の検証結果を前記端末から受信することと、
前記検証結果が前記サーバによって検証、承認された場合、第２のセッション識別子を前記端末に送信することであって、前記第２のセッション識別子は、前記ログインアカウントと新しいパスワードから生成され、前記新しいパスワードは、前記ログインアカウントの修正後のログインパスワードである、前記方法。
【請求項７】
前記方法は、
前記検証結果が、前記サーバの対称秘密鍵を用いて前記端末によって暗号化されている

場合、暗号化された検証結果を前記サーバの前記対称秘密鍵を用いて解読して、前記検証結果に対応する検証文字列及び乱数を取得することと、
前記検証文字列と前記乱数に対する検証を行うことと、
前記検証文字列と前記乱数が前記検証に合格した場合、前記第２のセッション識別子を前記端末に送信することと、
をさらに含む、請求項６に記載の方法。
【請求項８】
前記方法は、
前記サーバの前記対称秘密鍵を対称暗号化アルゴリズムに基づいて生成することと、
前記対称秘密鍵を前記端末の公開鍵を用いて暗号化することと、
前記暗号化された対称秘密鍵を前記端末に送信して、前記端末が、前記暗号化された対称秘密鍵を前記公開鍵に対応するプライベート鍵を用いて暗号化して、前記サーバの前記対称秘密鍵を取得するのを可能にすることと、
をさらに含む、請求項７に記載の方法。
【請求項９】
前記方法は、
前記第２のセッション識別子が有効期間内であるか否かを決定することと、
前記第２のセッション識別子が前記有効期間内である場合、前記ユーザが、前記第２のセッション識別子を通して前記アプリケーションプログラムにログインするのを可能にすることと、
前記第２のセッション識別子が前記有効期間を過ぎている場合、前記ユーザが、前記第２のセッション識別子を通して前記アプリケーションプログラムにログインするのを禁止することと、
をさらに含む、請求項６～８のいずれか１項に記載の方法。
【請求項１０】
セッション識別子同期を実現する装置であって、
サーバにアプリケーションプログラムへのログインを求める第１の要求を開始するために使用される第１の送信モジュールであって、前記第１の要求は、第１のセッション識別子を含み、前記第１のセッション識別子は、前記アプリケーションプログラムのログインアカウント及び元のパスワードから生成され、前記元のパスワードは、前記ログインアカウントの修正前のログインパスワードである、前記第１の送信モジュールと、
前記第１の送信モジュールによって送信された前記第１のセッション識別子が無効であると前記サーバによって決定された場合、端末のユーザに対する有効性検証を行うために使用され、取得した検証結果を前記サーバに送信して、前記サーバが前記検証結果に対するチェックを行うのを可能にするために使用される第１の検証モジュールと、
前記第１の検証モジュールによって取得された前記検証結果が、前記サーバによって検証、承認された場合、第２のセッション識別子を前記サーバから受信して、前記第２のセッション識別子を前記端末に記憶するために使用される第１の受信モジュールと
を含み、前記第２のセッション識別子は、前記ログインアカウント及び新しいパスワードから生成され、前記新しいパスワードは、前記ログインアカウントの修正後のログインパスワードである、前記装置。
【請求項１１】
前記装置は、
前記第１の検証モジュールによって取得された前記検証結果に対応する検証文字列の乱数を生成するために使用される第１の生成モジュールと、
前記第１の検証モジュールによって取得された前記検証文字列と、前記第１の生成モジュールによって生成された前記乱数とを前記サーバの対称秘密鍵を用いて暗号化して、暗号化された検証結果を取得するために使用される第１の暗号化モジュールと、
をさらに含む、請求項１０に記載の装置。
【請求項１２】

前記装置は、
前記端末の公開鍵及びプライベート鍵を、非対称暗号化アルゴリズムを用いて、生成するために使用される第２の生成モジュールと、
前記第２の生成モジュールによって生成された前記端末の前記公開鍵を前記サーバに送信するために使用される第２の送信モジュールと、
前記第２の送信モジュールによって送信された前記端末の前記公開鍵を用いて暗号化された前記サーバの前記対称秘密鍵を前記サーバから受信するために使用される第２の受信モジュールと、
前記暗号化された対称秘密鍵を前記第２の生成モジュールによって生成された前記端末の前記プライベート鍵を用いて解読して、前記サーバの前記対称秘密鍵を取得するために使用される第１の解読モジュールと
をさらに含む、請求項１１に記載の装置。
【請求項１３】
前記第１の検証モジュールは、
前記アプリケーションプログラムのログインインタフェースでバイオメトリックセンサを通して前記端末のユーザの生物学的特性を収集するために使用される特性収集ユニットと、
前記特性収集ユニットによって収集された前記生物学的特性に対する検証を行うために使用される検証ユニットと、
前記生物学的特性が前記検証ユニットの前記検証に合格すると、前記端末の前記ユーザは正規ユーザであると決定するために使用される第１の決定ユニットと、
前記ログインアカウント及び前記ログインパスワードを用いて前記アプリケーションプログラムにログインするように前記アプリケーションプログラムの前記ログインインタフェースでプロンプトを提供するために使用されるプロンプトユニットと
を含む、請求項１０に記載の装置。
【請求項１４】
前記装置は、
前記第１の受信モジュールによって受信された前記第２のセッション識別子が有効期間内であるか否かを決定するために使用される第１の決定モジュールと、
前記第２のセッション識別子が前記有効期間内であると前記第１の決定モジュールが決定した場合、前記第２のセッション識別子が前記アプリケーションプログラムにログインするために使用されると決定するために使用される第２の決定モジュールと、
前記第２のセッション識別子が前記有効期間を過ぎていると前記第１の決定モジュール１２０が決定した場合、前記ログインアカウント及び前記ログインアカウントの有効なログインパスワードを用いて前記アプリケーションプログラムにログインするように前記ユーザにプロンプトするために使用されるプロンプトモジュールと
をさらに含む、請求項１０～１３のいずれか１項に記載の装置。
【請求項１５】
セッション識別子同期を実現する装置であって、
アプリケーションプログラムへのログインを求める第１の要求が端末で開始されると、前記第１の要求に含まれる第１のセッション識別子の有効性を検証するために使用される第２の検証モジュールであって、前記第１のセッション識別子は、前記アプリケーションプログラムのログインアカウント及び元のパスワードから生成され、前記元のパスワードは、前記ログインアカウントの修正前のログインパスワードである、前記第２の検証モジュールと、
前記第１のセッション識別子が無効であると、無効になる前記第２の検証モジュールによって検証された場合、前記端末のユーザに対する有効性検証を行うように前記端末に命令するために使用されるコマンドモジュールと、
前記コマンドモジュールの命令に従って前記端末によって行われた前記ユーザの前記有効性検証の検証結果を受信するために使用される第３の受信モジュールと、

前記第３の受信モジュールによって受信された前記検証結果が、サーバによって検証及び承認された場合、第２のセッション識別子を前記端末に送信するために使用される第３の送信モジュールと

を含み、前記第２のセッション識別子は、前記ログインアカウント及び新しいパスワードから生成され、前記新しいパスワードは、前記ログインアカウントの修正後のログインパスワードである、前記装置。

【請求項１６】

前記装置は、

前記第３の受信モジュールによって取得された前記検証結果が前記サーバの対称秘密鍵を用いて前記端末によって暗号化されている場合、暗号化された検証結果を前記サーバの前記対称秘密鍵を用いて解読して、前記検証結果に対応する検証文字列と乱数を取得するために使用される第２の解読モジュールと、

前記第２の解読モジュールによる解読後に取得された前記検証文字列及び前記乱数に対して検証を行うために使用される第３の検証モジュールと

をさらに含み、前記第３の送信モジュールは、前記検証文字列及び前記乱数が前記検証に合格した場合、前記第２のセッション識別子を前記端末に送信する、

請求項１５に記載の装置。

【請求項１７】

前記装置は、

対称暗号化アルゴリズムに基づいて前記サーバの前記対称秘密鍵を生成して前記第２の解読モジュールが、前記暗号化された検証結果を前記サーバの前記対称秘密鍵を用いて解読することを可能にするために使用される第３の生成モジュールと、

前記第３の生成モジュールによって生成された前記対称秘密鍵を前記端末の公開鍵を用いて暗号化するために使用される第２の暗号化モジュールと、

前記第２の暗号化モジュールによって暗号化された前記対称秘密鍵を前記端末に送信して、前記端末が、前記公開鍵に対応するプライベート鍵を用いて、暗号化された前記対称秘密鍵を解読して、前記サーバの前記対称秘密鍵を取得するために使用される第４の送信モジュールと、

をさらに含む、請求項１６に記載の装置。

【請求項１８】

前記装置は、

前記第３の送信モジュールによって送信された前記第２のセッション識別子が有効期間内であるか否かを決定するために使用される第３の決定モジュールと、

前記第２のセッション識別子が前記有効期間内であると前記第３の決定モジュールが決定する場合、前記ユーザが前記第２のセッション識別子を用いて前記アプリケーションプログラムにログインするのを可能にするために使用される第１の制御モジュールと、

前記第２のセッション識別子が前記有効期間を過ぎていると前記第３の決定モジュール１４０が決定する場合、前記ユーザが前記第２のセッション識別子を用いて前記アプリケーションプログラムにログインするのを禁止するために使用される第２の制御モジュールと、

をさらに含む、請求項１５～１７のいずれか１項に記載の装置。

【発明の詳細な説明】

【技術分野】

【０００１】

本出願は、「Ｍｅｔｈｏｄ ａｎｄ Ｄｅｖｉｃｅ ｆｏｒ Ｒｅａｌｉｚｉｎｇ Ｓｅｓｓｉｏｎ Ｉｄｅｎｔｉｆｉｅｒ Ｓｙｎｃｈｒｏｎｉｚａｔｉｏｎ」と題する２０１５年１０月２６日出願の中国特許出願番号２０１５１０７０２５２７．３号の優先権を主張し、同出願は参照によりその全体が本明細書に組み込まれる。

【０００２】

本発明は、ネットワークセキュリティの技術分野に関し、詳細には、セッション識別子

同期を実現する方法及び装置に関する。
【背景技術】
【０００３】
埋め込み技術及び端末技術の絶え間ない発展に伴って、ますます多くの端末装置が、人々の日々の職業生活に適用されるようになっている。端末装置にインストールされるアプリケーションプログラムもＷｉｎｄｏｗｓ、Ｌｉｎｕｘ、Ａｎｄｒｏｉｄ、ｉＯＳ等の異なるオペレーティングシステムで使用されるのに適した多数の異なる種類のバージョンを用いて設計されている。ユーザが、異なる端末装置のアプリケーションプログラムに、そのアカウントを用いてアクセスする時、アカウントの本人確認の問題が発生する。ユーザが、本人確認情報を繰り返し入力するのを防ぐために、多くのアプリケーションプログラムが、パスワード記録機能を組み込んでいる。しかしながら、ユーザが、アプリケーションプログラムに関連付けられたパスワードを端末装置の１つでリセットした後、ユーザが、他の端末装置を通してアプリケーションプログラムにログインする必要がある時、他の端末装置に以前に記録されたパスワードが無効になっているので、ユーザは、そのアプリケーションプログラムに新しいパスワードを入力する必要がある。あるシナリオにおいては、他の端末装置を通して新しいパスワードを入力することは、ユーザにとって都合が良くない場合がある。例えば、他の業務を行っているユーザにとって、両手がふさがっている時、新しいパスワードを端末装置に入力することは、あるセキュリティリスクを生み出す。
【発明の概要】
【０００４】
従って、本出願が提供する新しい技術的解決法は、ユーザが、新しいパスワードを再入力する必要無く、他の端末でアプリケーションプログラムにログインするのを可能にでき、また、アプリケーションプログラムのログインセキュリティを保証できる。
【０００５】
上記目的を達成するために、本開示は、以下の技術的解決法を提供する。
【０００６】
本出願の第１の態様に従って、パスワード同期を実現する方法を提供する。方法は、サーバにアプリケーションプログラムへのログインを求める第１の要求を開始することであって、第１の要求は、第１のセッション識別子を含み、第１のセッション識別子は、アプリケーションプログラムのログインアカウント及び元のパスワードから生成され、元のパスワードは、ログインアカウントに対応する修正前のログインパスワードである、第１の要求を開始することと、第１のセッション識別子が無効であるとサーバによって決定された場合、端末のユーザに対する有効性検証を行い、取得した検証結果をサーバに送信して、サーバが検証結果に対するチェックを行うのを可能にすることと、検証結果がサーバによって検証、承認された場合、第２のセッション識別子をサーバから受信し、第２のセッション識別子を端末に記憶することを含み、第２のセッション識別子は、ログインアカウント及び新しいパスワードから生成され、新しいパスワードは、ログインアカウントに対応する修正後のログインパスワードである。
【０００７】
本出願の第２の態様に従って、パスワード同期を実現する方法を提供する。方法は、アプリケーションプログラムへのログインを求める第１の要求が端末において開始される時、第１の要求に含まれる第１のセッション識別子の有効性を検証することであって、第１のセッション識別子は、アプリケーションプログラムのログインアカウント及び元のパスワードから生成され、元のパスワードは、ログインアカウントに対応する修正前のログインパスワードである、第１のセッション識別子の有効性を検証することと、第１のセッション識別子が無効であると検証された場合、端末のユーザに対する有効性検証を行うように端末に命令することと、ユーザの有効性検証の検証結果を端末から受信することと、検証結果がサーバにより検証、承認された場合、第２のセッション識別子を端末に送信することを含み、第２のセッション識別子は、ログインアカウント及び新しいパスワードから

生成され、新しいパスワードは、ログインアカウントに対応する修正後のログインパスワードである。

【０００８】

本出願の第３の態様に従って、パスワード同期を実現する装置を提供する。装置は、サーバにアプリケーションプログラムへのログインを求める第１の要求を開始するために使用される第１の送信モジュールであって、第１の要求は、第１のセッション識別子を含み、第１のセッション識別子は、アプリケーションプログラムのログインアカウント及び元のパスワードから生成され、元のパスワードは、ログインアカウントに対応する修正前のログインパスワードである、第１の送信モジュールと、第１の送信モジュールによって送信された第１のセッション識別子が無効であるとサーバによって決定された場合、端末のユーザに対する有効性検証を行うために使用され、取得した検証結果をサーバに送信して、サーバが検証結果に対するチェックを行うのを可能にするために使用される第１の検証モジュールと、第１の検証モジュールによって取得された検証結果が、サーバによって検証、承認された場合、第２のセッション識別子をサーバから受信して、第２のセッション識別子を端末に記憶するために使用される第１の受信モジュールとを含み、第２のセッション識別子は、ログインアカウント及び新しいパスワードから生成され、新しいパスワードは、ログインアカウントに対応する修正後のログインパスワードである。

【０００９】

本出願の第４の態様に従って、パスワード同期を実現する装置を提供する。装置は、アプリケーションプログラムへのログインを求める第１の要求が端末において開始されると、第１の要求に含まれる第１のセッション識別子の有効性を検証するために使用される第２の検証モジュールであって、第１のセッション識別子は、アプリケーションプログラムのログインアカウント及び元のパスワードから生成され、元のパスワードは、ログインアカウントに対応する修正前のログインパスワードである、第２の検証モジュールと、第１のセッション識別子が第２の検証モジュールによって無効であると検証された場合、端末のユーザに対する有効性検証を行うように端末に命令するために使用されるコマンドモジュールと、コマンドモジュールの命令に従って端末によって行われたユーザの有効性検証の検証結果を受信するために使用される第３の受信モジュールと、第３の受信モジュールによって受信された検証結果がサーバによって検証、承認された場合、第２のセッション識別子を端末に送信するために使用される第３の送信モジュールとを含み、第２のセッション識別子は、ログインアカウント及び新しいパスワードから生成され、新しいパスワードは、ログインアカウントに対応する修正後のログインパスワードである。

【００１０】

上記技術的解決法から分かるように、本出願は、ユーザが第２のセッション識別子を通してアプリケーションプログラムにログインするのを可能にすることができ、それによって、端末を使用するユーザが、アプリケーションプログラムにログインするために新しいパスワードを再入力するのを回避し、アプリケーションプログラムへのユーザのログイン体験を大きく向上させる。多数のユーザが、アプリケーションプログラムに関連付けられたログインパスワードをリセットする必要がある時、ユーザの正当性の検証に関するサーバのワークロードは、ユーザの有効性検証を端末側で行うことにより軽減され、従って、サーバのリソースの浪費が避けられる。

【図面の簡単な説明】

【００１１】

【図１】アプリケーションプログラムに関連付けられたログインパスワードを第１の端末を通して修正するプロセスを示すフローチャートである。

【図２】本発明の実施形態による、セッション識別子同期を実現する第１の例示の方法を示すフローチャートである。

【図３Ａ】本発明の実施形態による、セッション識別子同期を実現する第２の例示の方法を示すフローチャートである。

【図３Ｂ】図３Ａの端末とサーバの間の鍵の同期の仕方を示すフローチャートである。

【図４】本発明の実施形態による、セッション識別子同期を実現する第３の例示の方法を示すフローチャートである。
【図５】本発明の実施形態による、セッション識別子同期を実現する第４の例示の方法を示すフローチャートである。
【図６】本発明の別の実施形態による、セッション識別子同期を実現する第１の例示の方法を示すフローチャートである。
【図７】本発明の別の実施形態による、セッション識別子同期を実現する第２の例示の方法を示すフローチャートである。
【図８】本発明の別の実施形態による、セッション識別子同期を実現する第３の例示の方法を示すフローチャートである。
【図９】本発明の例示の実施形態による、端末の概略構造図である。
【図１０】本発明の例示の実施形態による、サーバの概略構造図である。
【図１１】本発明の実施形態による、セッション識別子同期を実現する第１の例示の装置の概略構造図である。
【図１２】本発明の実施形態による、セッション識別子同期を実現する第２の例示の装置の概略構造図である。
【図１３】本発明の実施形態による、セッション識別子同期を実現する第３の例示の装置の概略構造図である。
【図１４】本発明の実施形態による、セッション識別子同期を実現する第４の例示の装置の概略構造図である。
【発明を実施するための形態】
【００１２】
例示の実施形態を、添付の図面で例を表して、ここに詳細に記載する。添付図面は以下の記載に関する時、異なる添付図面中の同じ参照番号は、別段の記載のない限り、同じまたは類似の要素を表す。以下の例示の実施形態で記載する実施態様は、本出願に一致する実施態様の全てではなく一部のみを表し、請求項で詳細に記載する本出願の態様に一致する方法及び装置の例である。
【００１３】
本出願で使用される用語は、単に、特定の実施形態を記載する目的で使用され、本出願を制限する意図はない。本出願及び添付の請求項で使用される単数形「ａ　ｔｙｐｅ（ある種類）」「ｓａｉｄ（前記）」及び「ｔｈｅ（前記）」は、文脈上明らかに別の意味でない限り、複数形を含むことを意図している。明細書で使用される「及び／または」という語は、列挙される１つまたは複数の関連する項目の任意または全ての可能な組み合わせを指し、それらを含む。
【００１４】
「第１」、「第２」及び「第３」等の語は、本出願において、様々な種類の情報を記載するために使用されてよいが、これらの情報は、これらの語に制限されないことは理解されたい。これらの語は、単に、同じ種類の情報の間の区別に使用される。例えば、本出願の範囲を逸脱することなく、第１の情報は、第２の情報と呼ぶこともできる。同様に、第２の情報は、第１の情報と呼ぶこともできる。文脈に応じて、本明細書で使用される「ｉｆ」という句は、「ｉｎ　ａｎ　ｅｖｅｎｔ　ｔｈａｔ（の場合）」「ｗｈｅｎ（時）」または「ｉｎ　ｒｅｓｐｏｎｓｅ　ｔｏ（に応答して）」と解釈されてよい。
【００１５】
図１は、アプリケーションプログラムに関連付けられたログインパスワードを第１の端末を通して修正するプロセスを示すフローチャートである。元のパスワードが修正される前に、第１の端末及び第２の端末は両方とも、パスワードを記録する機能を通して、アプリケーションプログラムにログインする度にログインパスワードを入力する必要性を回避している。ユーザが、アプリケーションプログラムの元のパスワードを第１の端末を通して修正する場合、第２の端末は依然として、記録された元のパスワードを使用してアプリケーションプログラムにログインし、ログインパスワードは修正されているので、ログイ

ンに失敗する。図１に示すように、以下のステップが含まれる。

【００１６】

ステップ１０１において、第１の端末は、パスワード修正要求をサーバに送信し、パスワード修正に必要な情報、例えば、ログインアカウント、元のパスワード、及び、新しいパスワード等をサーバに提供する。

【００１７】

ステップ１０２において、サーバは、提供された情報に対するチェックを行い、元のパスワードが正確か否かを検証する。元のパスワードが不正確な場合、ステップ１０１が再び行われて、パスワード修正要求を第１の端末を通してサーバに再送するようにユーザに命令する。元のパスワードが正確な場合、ステップ１０３が行われる。

【００１８】

ステップ１０３において、サーバは、新しいパスワードをバックエンドデータベースに記憶し、ログインアカウント及び新しいパスワードに基づいて新しいセッション識別子を生成し、ログインアカウント及び元のパスワードに基づいて生成された元のセッション識別子を無効に設定する。

【００１９】

ステップ１０４において、新しいセッション識別子が、第１の端末に返信される。

【００２０】

ステップ１０５において、第１の端末は、サーバが返信した新しいセッション識別子を受信し、新しいセッション識別子を第１の端末のローカルなセキュアスペースに記憶して、第１の端末のアプリケーションプログラムのパスワード修正のプロセスを完了する。

【００２１】

ステップ１０６において、サーバがパスワードを修正した後、第２の端末が、元のセッション識別子を用いてサーバにログイン要求を開始する。ここで、第２の端末は、アプリケーションプログラムに最初に第２の端末でログインした後、パスワード記録方法を通して元のセッション識別子を第２の端末に記録している。

【００２２】

ステップ１０７において、サーバは、第２の端末の元のセッション識別子に対する検証を行い、使用されている元のセッション識別子が無効になっていることを決定し、第２の端末にパスワードの再入力を求める要求を返信する。この状況において、第２の端末は、再度、修正された新しいパスワードを入力する必要がある。ユーザの両手がふさがっている時、第２の端末を通して新しいパスワードを入力することは、あるセキュリティリスクを生じ得る。

【００２３】

従って、本出願は、ログインパスワードが第１の端末で修正された後、以下の実施形態を使用して、第２の端末が、新しいパスワードを入力する必要無く、サーバにログインするのを可能にし、それによって、ユーザがアプリケーションプログラムに第２の端末を通してログインする必要がある時、アプリケーションプログラムを提供するサーバにログインするために新しいパスワードの入力が必要であるという既存技術の欠点を解決する。

【００２４】

本出願をさらに詳細に記載するために以下の実施形態を提供する。

【００２５】

図２は、本発明の実施形態による、セッション識別子同期を実現する第１の例示の方法を示すフローチャートである。方法が適用される端末は、図１に示す第２の端末である。図２に示すように、以下のステップが含まれる。

【００２６】

ステップ２０１：サーバにアプリケーションプログラムへのログインを求める第１の要求が開始される。第１の要求は、第１のセッション識別子を含み、第１のセッション識別子は、アプリケーションプログラムのログインアカウント及び元のパスワードから生成され、元のパスワードは、ログインアカウントに対応する修正前のログインパスワードであ

る。

【００２７】

ある実施形態においては、アプリケーションプログラムに最初にログインする時、端末は、パスワード記録方法を通して第１のセッション識別子に対応する文字列をサーバに送信でき、第１のセッション識別子を第１の端末にローカルに記録できる。アプリケーションプログラムに再度、ログインする時、端末は、記録された第１のセッション識別子を用いてアプリケーションプログラムにログインできるので、ユーザがログインパスワードを再入力する動作を回避できる。ある実施形態においては、第１のセッション識別子を生成する方法は、サーバによって決定できる。第１のセッション識別子は、ユーザのログインアカウント及び元のパスワードに基づいて、ｍｄ５またはｓｈａ１等のハッシュアルゴリズムを用いて生成できる。例えば、ログインアカウント及び元のパスワードであるｚｈａｎｇｘｉａｏ及びｚｘ０９８と、ログインタイムスタンプ２０１５１０２６に基づいて、第１のセッション識別子（３ＥＣ３ＥＤ３８１Ｂ９ＣＦ４３５９Ｆ４Ｃ１ＣＢ０２ＣＤＦ６４）が、ｍｄ５アルゴリズムを通して、ログインアカウント、元のパスワード、及び、タイムスタンプにＭＤ５アルゴリズムの列計算を行うことによって取得される。

【００２８】

ステップ２０２：第１のセッション識別子が無効であるとサーバが決定した場合、端末のユーザに対する有効性検証が行われ、取得した検証結果がサーバに送信されて、サーバが検証結果に対するチェックを行うのを可能にする。

【００２９】

ある実施形態においては、有効性検証は、端末のユーザの生物学的特性を用いて行われてよい。例えば、端末にローカルの有効性検証が、ユーザの指紋、虹彩、顔等の生物学的特性を用いてユーザに対して行われてよい。ある実施形態においては、端末が検証結果をサーバに送信する前に、検証結果及び検証結果に対応する乱数が、サーバの対称秘密鍵を用いて暗号化できる。暗号化された検証結果がサーバに送信されるので、検証結果が、送信プロセス中に違法に傍受されたり、操作されたりしないことを保証し、端末とサーバ間で送信される検証結果のセキュリティを保証する。

【００３０】

ステップ２０３：検証結果がサーバによって承認された場合、サーバから来る第２のセッション識別子が、端末で受信及び記憶される。第２のセッション識別子は、ログインアカウント及び新しいパスワードから生成され、新しいパスワードは、ログインアカウントに対応する修正後のログインパスワードである。

【００３１】

ある実施形態においては、第２のセッション識別子が、送信プロセス中に違法に傍受及び操作されるのを防ぐために、第２のセッション識別子は、端末の公開鍵を用いて暗号化できる。暗号化された第２のセッション識別子を受信後、端末は、暗号化された第２のセッション識別子を端末のプライベート鍵を用いて解読して、第２のセッション識別子を取得する。ある実施形態においては、第２のセッション識別子を生成する方法は、第１のセッション識別子を生成する上記方法を参照できる。例えば、図１に示す実施形態で第１の端末を用いて、ユーザがログインパスワードをｚｈａｎｇｘｉａｏに変更した後、第２のセッション識別子（２ＥＦ４３０３３８ＤＦ５６Ａ６ＦＥ４０８１９ＣＢＦ７５９８２Ａ９）が、第１のセッション識別子に対するのと同じハッシュ計算を用いて取得される。

【００３２】

ステップ２０１～ステップ２０３を通して、ユーザは、第２のセッション識別子を用いてアプリケーションプログラムにログインでき、端末を使用するユーザは、アプリケーションプログラムにログインするために新しいパスワードを再入力しなくてよく、それによって、ユーザのアプリケーションプログラムのログイン体験を大きく向上させる。

【００３３】

図３Ａは、本発明の実施形態による、セッション識別子同期を実現する第２の例示の方法を示すフローチャートである。図３Ｂは、図３Ａの端末とサーバとの間の鍵の同期の仕

方を示すフローチャートである。図３Ａに示すように、以下のステップが含まれる。

【００３４】

ステップ３０１：検証結果に対応する検証文字列の乱数は、ハッシュ計算を用いて生成される。

【００３５】

ある実施形態においては、端末及びサーバは、同じハッシュアルゴリズムに同意して、端末及びサーバが、ハッシュアルゴリズムに基づいて同じ乱数を生成できることを保証してよい。ある実施形態においては、検証結果の検証文字列は、例えば、「００１」及び「０００」であってよく、「００１」は、検証に合格したことを表し、「０００」は、検証に失敗したことを表す。

【００３６】

ステップ３０２：検証文字列及び乱数は、サーバの対称秘密鍵を用いて暗号化されて、暗号化された検証結果を取得する。

【００３７】

ある実施形態においては、端末がサーバの対称秘密鍵をどのように取得するかは、図３Ｂに示すプロセスを参照できる。図３Ｂに示すように、サーバと端末の間の鍵の同期は以下のステップを含む。

【００３８】

ステップ３１１：端末の公開鍵及びプライベート鍵は、非対称暗号化アルゴリズムに基づいて生成される。

【００３９】

ある実施形態においては、非対称暗号化アルゴリズムは、例えば、ＲＳＡ、ナップザックアルゴリズム、Ｅｌｇａｍａ１、Ｄ－Ｈ、楕円曲線暗号化アルゴリズム（ＥＣＣ）等であってよい。本実施形態は、公開鍵及びプライベート鍵が非対称暗号化アルゴリズムに基づいて生成できることを条件として、非対称暗号化アルゴリズムにいかなる制限も設けない。

【００４０】

ステップ３１２：端末の公開鍵がサーバに送信される。

【００４１】

ステップ３１３：端末の公開鍵を用いて暗号化されたサーバの対称秘密鍵が受信される。

【００４２】

ある実施形態においては、サーバは、サーバの対称秘密鍵を生成し、端末の公開鍵を用いて対称秘密鍵を暗号化し、暗号化された対称秘密鍵を端末に送信する。さらに、サーバは、対称秘密鍵を用いて修正された新しいパスワードも暗号化及び記憶してよく、それによって、図１に示す第１の端末を通してユーザによって修正された新しいパスワードの漏洩によるリスクを回避する。

【００４３】

ステップ３１４：暗号化された対称秘密鍵は、端末のプライベート鍵を用いて解読されて、サーバの対称秘密鍵を取得する。

【００４４】

ステップ３１１～ステップ３１４を通して、サーバは、端末の公開鍵を取得することができ、端末は、サーバの対称鍵を取得でき、それによって、サーバの対称秘密鍵と端末のプライベート鍵との間の鍵同期のプロセスを実現する。

【００４５】

本実施形態においては、検証結果の機密性は、対称暗号化技術を通して保証でき、不法なユーザによる検証結果の改ざんを防止できる。乱数の使用によって、暗号化されたデータの再使用を防止できる。

【００４６】

図４は、本発明の実施形態による、セッション識別子同期を実現する第３の例示の方法

を示すフローチャートである。本実施形態は、説明のために、端末がローカルでどのようにユーザの有効性検証を行うかの例を使用する。図４に示すように、以下のステップが含まれる。

【００４７】

ステップ４０１：端末のユーザの生物学的特性が、アプリケーションプログラムのログインインタフェースにおいてバイオメトリックセンサを通して収集される。

【００４８】

ある実施形態においては、生物学的特性は、ユーザの指紋、虹彩、または、顔等の生物学的特性であってよい。生物学的特性が指紋である場合、アプリケーションプログラムの現在のログインインタフェースは、ユーザの指紋を取得でき、それによって、ユーザは、アプリケーションプログラムによって現在表示されているログインインタフェースを出なくてよい。これによって、ログインインタフェースで直接、指紋認証の動作を行い、ユーザに対する有効性検証をローカルで行う手順を簡単にする。

【００４９】

ステップ４０２：生物学的特性に対する検証が行われて、検証に合格するか否かを決定する。生物学的特性が検証に合格した場合、ステップ４０３が行われる。生物学的特性が検証に合格しなかった場合、ステップ４０４が行われる。

【００５０】

ステップ４０３：生物学的特性が検証に合格した場合、端末のユーザは、不法なユーザであると確証される。

【００５１】

ある実施形態においては、生物学的特性の検証については、既存の技術の関連する記載を参照し得るので、本実施形態において詳細は記載しない。

【００５２】

ステップ４０４：生物学的特性が検証に合格しなかった場合、アプリケーションプログラムのログインインタフェースは、ログインアカウント及びログインパスワードを使用してアプリケーションプログラムにログインするようにプロンプトする。

【００５３】

本実施形態においては、同じアプリケーションプログラムの多数のユーザが、複数の端末のうちの１つの端末を通してログインパスワードをリセットし、且つ、他の端末を通してアプリケーションプログラムにログインする時、本実施形態は、ローカルの本人確認機構を通してサーバのワークロードを最適化でき、サーバが、攻撃者からの分散型サービス妨害（ＤＤＯＳ）の攻撃を受けるのを防止できる。

【００５４】

図５は、本発明の実施形態による、セッション識別子同期を実現する第４の例示の方法を示すフローチャートである。端末が、上記実施形態を通して第２のセッション識別子を取得及び記憶した後、サーバは、第２のセッション識別子の有効期間をユーザログインのセキュリティを保証するように設定できる。よって、ユーザがアプリケーションプログラムへのログインに割り当てられる時間は、第２のセッション識別子の有効期間を通して制限される。図５に示すように、以下のステップが含まれる。

【００５５】

ステップ５０１：第２のセッション識別子が有効期間内であるか否かについて決定が行われ、第２のセッション識別子が有効期間内である場合、ステップ５０２が行われ、第２のセッション識別子が有効期間外である場合、ステップ５０３が行われる。

【００５６】

ステップ５０２：第２のセッション識別子が有効期間内である場合、アプリケーションプログラムは第２のセッション識別子を用いてログインされる。

【００５７】

ステップ５０３：第２のセッション識別子が有効期間外である場合、ユーザは、ログインアカウント及びログインアカウントの有効なパスワードを用いてアプリケーションプロ

グラムにログインするようにプロンプトされる。

【００５８】

ある実施形態においては、有効期間は、サーバから取得できる。例えば、ユーザは、第１の端末を通して新しいパスワードをリセットする。サーバが新しいパスワードから第２のセッション識別子を生成する時刻は、２０１５年１０月１０日１２：１２で、有効期間は１ヶ月である。端末は、第２のセッション識別子の生成時刻及び有効期間をサーバから取得できる。従って、ユーザが第２のセッション識別子を用いてアプリケーションプログラムに直接ログインできるか否かに関して第２のセッション識別子に基づいて決定を行うことができる。第２のセッション識別子が１ヶ月を過ぎた場合、アプリケーションプログラムのログインインタフェースは、ログインアカウント及びログインアカウントの有効なログインパスワードがアプリケーションプログラムへのログインに必要であることをユーザにプロンプトできる。

【００５９】

本実施形態においては、ユーザのログイン行動が、第２のセッション識別子の有効期間を通して制限され、それによって、不法なユーザが、第２のセッション識別子取得後、不法にアプリケーションプログラムにログインするのを防止し、アプリケーションプログラムのユーザログインのセキュリティを保証する。

【００６０】

図６は、本発明の別の実施形態による、セッション識別子同期を実現する第１の例示の方法を示すフローチャートである。図１に示す実施形態と一致するように、方法をサーバに適用する例を説明のために使用する。図６に示すように、以下のステップが含まれる。

【００６１】

ステップ６０１：アプリケーションプログラムにログインする第１の要求が、端末によって開始されると、第１の要求に含まれる第１のセッション識別子の有効性に対する検証が行われる。第１のセッション識別子は、アプリケーションプログラムに関連付けられたログインアカウント及び元のパスワードから生成され、元のパスワードは、ログインアカウントに対応する修正前のログインパスワードである。

【００６２】

ある実施形態においては、第１のセッション識別子は、サーバに記憶された有効なセッション識別子と比較できる。第１のセッション識別子が、記憶された有効なセッション識別子と同じ場合、第１のセッション識別子は、有効であると決定される。第１のセッション識別子が記憶された有効なセッション識別子と同じでない場合、第１のセッション識別子は無効であると決定される。

【００６３】

ステップ６０２：第１のセッション識別子が無効であると検証された場合、端末のユーザに対する有効性検証を行うように端末に命令する。

【００６４】

ある実施形態においては、端末のユーザの有効性検証を行う方法は、上記実施形態の関連する記載を参照できるので、ここに繰り返し記載しない。

【００６５】

ステップ６０３：ユーザの有効性検証の検証結果が、端末から受信される。

【００６６】

ある実施形態においては、検証結果及び検証結果に対応する乱数が、端末が検証結果をサーバに送信する前に、サーバの対称秘密鍵を用いて暗号化される場合、暗号化された検証結果がサーバに送信される。この場合、サーバは、さらに、対称秘密鍵を用いて、暗号化された検証結果を復号化する必要がある。

【００６７】

ステップ６０４：検証結果がサーバによって検証及び承認された場合、第２のセッション識別子が端末に送信される。第２のセッション識別子は、ログインアカウント及び新しいパスワードから生成され、新しいパスワードは、ログインアカウントに対応する修正後

のログインパスワードである。

【００６８】

ステップ６０１～ステップ６０４を通して、正規ユーザは、サーバへのログインを許可されてよい。さらに、正規ユーザは、第２のセッション識別子を取得できる。これによって、正規ユーザが、端末を使用する時、アプリケーションプログラムにログインするために新しいパスワードを再入力することを防ぎ、従って、アプリケーションプログラムへのユーザログインの体験を大きく向上させる。多数のユーザが、アプリケーションプログラムのログインパスワードをリセットする必要があった後、ユーザの有効性検証に関するサーバのワークロードは、ユーザに対する有効性検証を端末側で行うことによって低減でき、それによって、サーバのリソースの浪費を回避する。

【００６９】

図７は、本発明の別の実施形態による、セッション識別子同期を実現する第２の例示の方法を示すフローチャートである。図７に示すように、以下のステップが含まれる。

【００７０】

ステップ７０１：検証結果が、サーバの対称秘密鍵を用いて、端末によって暗号化されている場合、暗号化された検証結果は、サーバの対称秘密鍵を用いて解読されて、検証結果に対応する検証文字列及び乱数を取得する。

【００７１】

ステップ７０２：検証文字列及び乱数に対して検証が行われ、検証文字列及び乱数が検証に合格すると、第２のセッション識別子が端末に送信される。

【００７２】

ある実施形態においては、端末及びサーバは、同じハッシュアルゴリズムに同意して、端末及びサーバが、ハッシュアルゴリズムに基づいて同じ乱数を生成できることを保証し、それによって乱数を用いた二重検証を行うことができる。ある実施形態においては、検証結果の検証文字列は、例えば、「００１」及び「０００」であってよく、「００１」は、検証に合格したことを表し、「０００」は、検証に失敗したことを表す。ある実施形態においては、第２のセッション識別子は、端末の公開鍵を用いて暗号化でき、それによって、送信プロセス中、第２のセッション識別子のセキュリティを保証する。

【００７３】

端末がサーバの対称鍵をどのように取得するかと、サーバが端末の公開鍵をどのように取得するかに関する詳細は、図３Ｂの上記の説明を参照できるので、ここに繰り返し記載しない。

【００７４】

本実施形態においては、検証結果の機密性は、対称暗号化技術を通して保証でき、不法なユーザによる検証結果の改ざんを防止できる。乱数の使用によって、暗号化されたデータの再使用を防止できる。

【００７５】

図８は、本発明の別の実施形態による、セッション識別子同期を実現する第３の例示の方法を示すフローチャートである。サーバが上記の実施形態を用いて第２のセッション識別子を生成した後、サーバは、ユーザログインのセキュリティを保証するために、第２のセッション識別子の有効期間を設定できる。よって、ユーザがアプリケーションプログラムにログインするために割り当てられた時間は、第２のセッション識別子の有効期間を通して制限される。図８に示すように、以下のステップが含まれる。

【００７６】

ステップ８０１：第２のセッション識別子が有効期間内であるか否かの決定が行われ、第２のセッション識別子が有効期間内である場合、ステップ８０２が行われ、第２のセッション識別子が有効期間外である場合、ステップ８０３が行われる。

【００７７】

ステップ８０２：第２のセッション識別子が有効期間内である場合、ユーザは、第２のセッション識別子を用いてアプリケーションプログラムにログインするのを許可される。

【００７８】
ステップ８０３：第２のセッション識別子が有効期間外である場合、ユーザは、第２のセッション識別子を用いてアプリケーションプログラムにログインするのを許可されない。
【００７９】
ある実施形態においては、サーバは、ユーザが設定した割り当て時間に基づいて、第２のセッション識別子の有効期間を決定できる。例えば、ユーザは、第１の端末を通して新しいパスワードをリセットし、有効期間は１ヶ月である。サーバが新しいパスワードから第２のセッション識別子を生成する時刻は、２０１５年１０月１０日１２：１２で、サーバは、第２のセッション識別子の終了時刻は、２０１５年１１月１０日１２：１２と決定できる。ユーザは、この割り当て期間内は第２のセッション識別子を用いて、アプリケーションプログラムに直接ログインできる。割当期間が過ぎると、ユーザは、第２のセッション識別子を用いてアプリケーションプログラムにログインすることは許可されない。
【００８０】
本実施形態において、ユーザのログイン行動は、第２のセッション識別子の有効期間を通して制限され、それによって、不法なユーザが、第２のセッション識別子を取得した後、アプリケーションプログラムに不法にログインするのを防止し、アプリケーションプログラムのユーザログインのセキュリティを保証する。
【００８１】
例示のシナリオとして、ユーザが、携帯電話を用いて、アプリケーションプログラムのログインパスワードをリセットした後、ユーザが、アプリケーションプログラムに車載端末を通してログインする場合、車載端末は、ユーザがログインパスワードをリセットする前の無効な第１のセッション識別子を記録している。サーバは、第１のセッション識別子を無効に設定しているので、ユーザは、車載端末を通してアプリケーションプログラムにログインできない。ユーザは運転中なので、新しいパスワードを入力するのは不都合である。ユーザのバイオメトリック検証を行う上記の実施形態を用いて、ユーザが車載端末の正規ユーザであると決定されると、第２のセッション識別子が、サーバから車載端末を通して取得できる。よって、アプリケーションプログラムは、第２のセッション識別子を用いてログインされ、従って、ユーザの運転中のリスクを軽減できる。
【００８２】
セッション識別子同期を実現する上記の方法に関して、本出願は、図９に示すように、本出願の例示の実施形態による、端末の概略構造図をさらに開示する。図９を参照すると、端末は、ハードウェアレベルで、プロセッサ、内部バス、ネットワークインタフェース、メモリ、及び、不揮発性記憶装置を含む。他のサービスに必要なハードウェアも含まれてよいことは明らかである。プロセッサは、実行のため、また、論理レベルでセッション識別子同期を実現する装置を形成するために、不揮発性記憶装置からメモリに、対応するコンピュータ命令を読み出す。ソフトウェア実施態様以外に、本出願は、論理構成要素、または、ソフトウェアとハードウェアの組み合わせ等の他の実施態様を除外しないことは明らかである。言い換えると、以下の処理手順の実行エンティティ（複数可）は、様々な論理ユニットに制限されず、またハードウェアまたは論理構成要素であってもよい。
【００８３】
セッション識別子同期を実現する上記方法に関して、本出願は、図１０に示すように、本出願の例示の実施形態による、サーバの概略構造図をさらに開示する。図１０を参照すると、サーバは、ハードウェアレベルで、プロセッサ、内部バス、ネットワークインタフェース、メモリ、及び、不揮発性記憶装置を含む。他のサービスに必要なハードウェアも含まれてよいことは明らかである。プロセッサは、実行のため、また、論理レベルでセッション識別子同期を実現する装置を形成するために、不揮発性記憶装置からメモリに、対応するコンピュータ命令を読み出す。ソフトウェア実施態様以外に、本出願は、論理構成要素、または、ソフトウェア及びハードウェアの組み合わせ等の他の実施態様を除外しないことは明らかである。言い換えると、以下の処理手順の実行エンティティ（複数可）は

、様々な論理ユニットに制限されず、ハードウェアまたは論理構成要素であってもよい。
【００８４】
図１１は、本発明の実施形態による、セッション識別子同期を実現する第１の例示の装置の概略構造図を示す。図１１に示すように、セッション識別子同期を実現する装置は、第１の送信モジュール１１１、第１の検証モジュール１１２、及び、第１の受信モジュール１１３を含んでよい。
【００８５】
第１の送信モジュール１１１は、サーバにアプリケーションプログラムへのログインを求める第１の要求を開始するために使用される。第１の要求は、第１のセッション識別子を含み、第１のセッション識別子は、アプリケーションプログラムのログインアカウント及び元のパスワードから生成され、元のパスワードは、ログインアカウントに対応する修正前のログインパスワードである。
【００８６】
第１の送信モジュール１１１によって送信された第１のセッション識別子が、サーバによって無効であると決定された場合、第１の検証モジュール１１２は、端末のユーザに対する有効性検証を行うために、また、取得した検証結果をサーバに送信して、サーバが、検証結果をチェックするのを可能にするために使用される。
【００８７】
第１の検証モジュール１１２によって取得された検証結果が、サーバによって検証及び承認された場合、第１の受信モジュール１１３は、第２のセッション識別子をサーバから受信し、第２のセッション識別子を端末に記憶するために使用される。第２のセッション識別子は、ログインアカウント及び新しいパスワードから生成され、新しいパスワードは、ログインアカウントに対応する修正後のログインパスワードである。
【００８８】
図１２は、本発明の実施形態による、セッション識別子同期を実現する第２の例示の装置の概略構造図を示す。一実施形態においては、図１１に示す実施形態に基づいて、図１２に示す装置は、第１の検証モジュール１１２によって取得された検証結果に対応する検証文字列の乱数を生成するために使用される第１の生成モジュール１１４と、第１の検証結果によって取得された検証文字列及び第１の生成モジュール１１４によって生成された乱数をサーバの対称秘密鍵を用いて暗号化して、暗号化された検証結果を取得するために使用される第１の暗号化モジュール１１５とをさらに含んでよい。
【００８９】
一実施形態においては、装置は、端末の公開鍵及びプライベート鍵を非対称暗号化アルゴリズムを用いて生成するために使用される第２の生成モジュール１１６と、第２の生成モジュール１１６によって生成された端末の公開鍵をサーバに送信するために使用される第２の送信モジュール１１７と、第２の送信モジュール１１７によって送信された端末の公開鍵を用いて暗号化されたサーバの対称秘密鍵をサーバから受信するために使用される第２の受信モジュール１１８と、暗号化された対称秘密鍵を第２の生成モジュール１１８によって生成された端末のプライベート鍵を用いて解読して、サーバの対称秘密鍵を取得するために使用される第１の解読モジュール１１９とをさらに含んでよい。
【００９０】
ある実施形態においては、第１の検証モジュール１１２は、アプリケーションプログラムのログインインタフェースでバイオメトリックセンサを通して端末のユーザの生物学的特性を収集するために使用される特性収集ユニット１１２１と、特性収集ユニット１１２１によって収集される生物学的特性に対する検証を行うために使用される検証ユニット１１２２と、生物学的特性が検証ユニット１１２２の検証に合格すると、端末のユーザは正規ユーザであると決定するために使用される第１の決定ユニットと、ログインアカウント及びログインパスワードを用いてアプリケーションプログラムにログインするようにアプリケーションプログラムのログインインタフェースでプロンプトを提供するために使用されるプロンプトユニット１１２３とを含んでよい。

【００９１】
ある実施形態においては、装置は、第１の受信モジュール１１３によって受信された第２のセッション識別子が有効期間内であるか否かを決定するために使用される第１の決定モジュール１２０と、第２のセッション識別子が有効期間内であると第１の決定モジュール１２０が決定した場合、第２のセッション識別子がアプリケーションプログラムにログインするために使用されると決定するために使用される第２の決定モジュール１２１と、第２のセッション識別子が有効期間を過ぎていると第１の決定モジュール１２０が決定した場合、ログインアカウント及びログインアカウントの有効なログインパスワードを用いてアプリケーションプログラムにログインするようにユーザにプロンプトするために使用されるプロンプトモジュール１２２とをさらに含んでよい。

【００９２】
図１３は、本発明の実施形態による、セッション識別子同期を実現する第３の例示の装置の概略構造図を示す。図１３に示すように、セッション識別子同期を実現する装置は、第２の検証モジュール１３１、コマンドモジュール１３２、第３の受信モジュール１３３、及び、第３の送信モジュール１３４を含んでよい。

【００９３】
第２の検証モジュール１３１は、アプリケーションプログラムへのログインを求める第１の要求が端末で開始されると、第１の要求に含まれる第１のセッション識別子の有効性を検証するために使用され、第１のセッション識別子は、アプリケーションプログラムのログインアカウント及び元のパスワードから生成され、元のパスワードは、ログインアカウントに対応する修正前のログインパスワードである。

【００９４】
第１のセッション識別子が無効であると第２の検証モジュール１３１によって検証された場合、コマンドモジュール１３２は、端末のユーザに対する有効性検証を行うように端末に命令するために使用される。

【００９５】
第３の受信モジュール１３３は、コマンドモジュール１３２の命令に従って端末によって行われたユーザの有効性検証の検証結果を受信するために使用される。

【００９６】
第３の送信モジュール１３４は、第３の受信モジュール１３４によって受信された検証結果が、サーバによって検証及び承認された場合、第２のセッション識別子を端末に送信するために使用される。第２のセッション識別子は、ログインアカウント及び新しいパスワードから生成され、新しいパスワードは、ログインアカウントに対応する修正後のログインパスワードである。

【００９７】
図１４は、本発明の実施形態による、セッション識別子同期を実現する第４の例示の装置の概略構造図を示す。一実施形態においては、図１３に示す実施形態に基づいて、図１４に示す装置は、第３の受信モジュール１３３によって取得された検証結果が、サーバの対称秘密鍵を用いて端末によって暗号化されている場合、暗号化された検証結果をサーバの対称秘密鍵を用いて解読して、検証結果に対応する検証文字列と乱数を取得するために使用される第２の解読モジュール１３５と、第２の解読モジュール１３５によって解読された後、取得された検証文字列と乱数に対する検証を行うために使用される第３の検証モジュール１３６とをさらに含んでよい。検証文字列及び乱数が検証に合格した場合、第３の送信モジュール１３４は、第２のセッション識別子を端末に送信するステップを行う。

【００９８】
ある実施形態においては、装置は、対称暗号化アルゴリズムに基づいてサーバの対称秘密鍵を生成して、第２の解読モジュール１３５が、サーバの対称秘密鍵を用いて暗号化された検証結果を解読できるようにするために使用される第３の生成モジュール１３７と、第３の生成モジュール１３７によって生成された対称秘密鍵を端末の公開鍵を用いて暗号化するために使用される第２の暗号化モジュール１３８と、第２の暗号化モジュール１３

８によって暗号化された対称秘密鍵を端末に送信して、端末が、公開鍵に対応するプライベート鍵を用いて、暗号化された対称秘密鍵を解読して、サーバの対称鍵を取得するのを可能にするために使用される第４の送信モジュール１３９とをさらに含んでよい。

【００９９】

ある実施形態においては、装置は、第３の送信モジュール１３４によって送信された第２のセッション識別子が有効期間内であるか否かを決定するために使用される第３の決定モジュール１４０と、第２のセッション識別子が有効期間内であると第３の決定モジュール１４０が決定した場合、ユーザが第２のセッション識別子を用いてアプリケーションプログラムにログインすることを可能にするために使用される第１の制御モジュール１４１と、第２のセッション識別子が有効期間を過ぎていると第３の決定モジュール１４０が決定した場合、ユーザが第２のセッション識別子を用いてアプリケーションプログラムにログインするのを禁止するために使用される第２の制御モジュール１４２とをさらに含んでよい。

【０１００】

上記の実施形態から分かるように、ユーザが第１の端末でアプリケーションプログラムのログインパスワードを修正した後、ユーザが第２の端末を通してアプリケーションプログラムにログインすると、この同じユーザは、第１の端末とは異なる第２の端末のアプリケーションプログラムへのログインを許可され得る、従って、アプリケーションプログラムにログインするために修正されたログインパスワードを入力するという方法を回避する。よって、ユーザ体験は向上し、ログインのセキュリティが保証される。

【０１０１】

当業者は、明細書を考慮し、本明細書に開示される発明を実施すると、本出願の他の実施態様を容易に考え付くことができる。本出願は、任意の修正、使用、または、適応的な変更を含むことを意図している。これらの修正、使用、または、適応的な変更は、本出願の一般的原理に従い、また、本出願に記載されていない本技術分野における周知の知識または一般的な技術手段を含む。明細書及び実施形態は、例示としてのみ見なされる。本出願の実際の範囲及び精神は、添付の請求項によって示される。

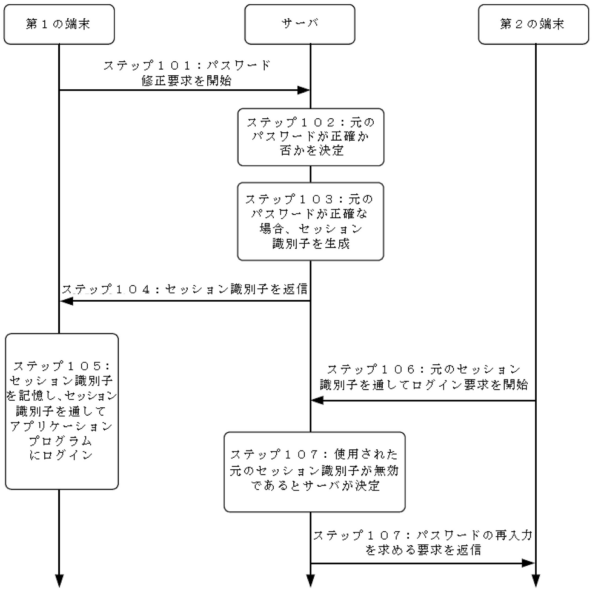
【０１０２】

「ｉｎｃｌｕｄｅ（含む）」、「ｃｏｎｔａｉｎ（含む）」という語、または、任意の他の変形は、排他的ではなく含むことを意図することにも注意されたい。よって、一連の要素を含むプロセス、方法、製品、または、デバイスは、これらの要素を含むだけでなく、明示的に列挙されていない他の要素も含む、または、プロセス、方法、製品、または、デバイスに本来備わる要素をさらに含んでよい。さらなる制限なく、「ｉｎｃｌｕｄｉｎｇ　ａ・・・（を含む）」という句によって規定される要素は、この要素を含むプロセス、方法、製品、または、デバイスの同じ要素をさらに追加することを除外しない。

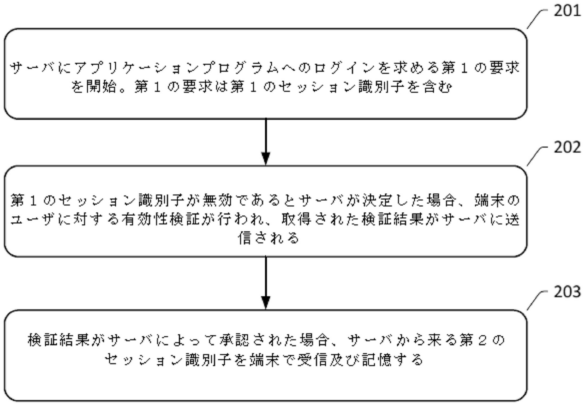
【０１０３】

上記の説明は、本出願の好ましい実施形態のみを指し、本出願への制限として使用されない。本出願の精神及び原理で行われた修正、同等の置き換え、改良等はいずれも、全て本出願の保護の範囲に含まれるものとする。

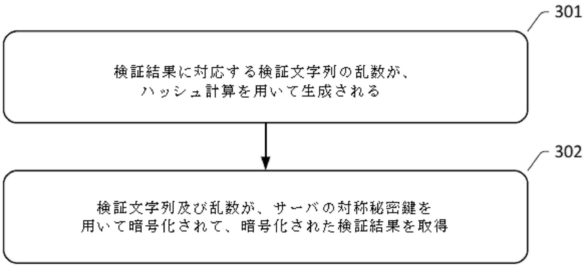
【図１】



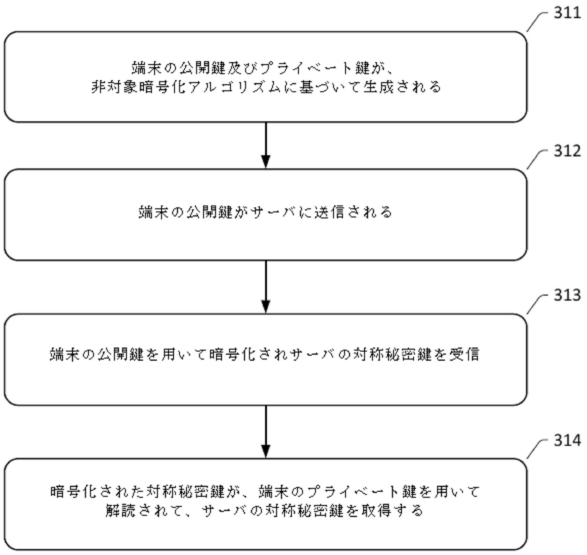
【図２】



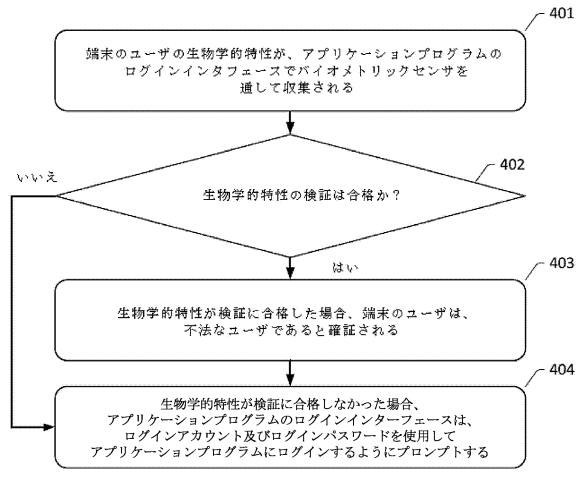
【図３Ａ】



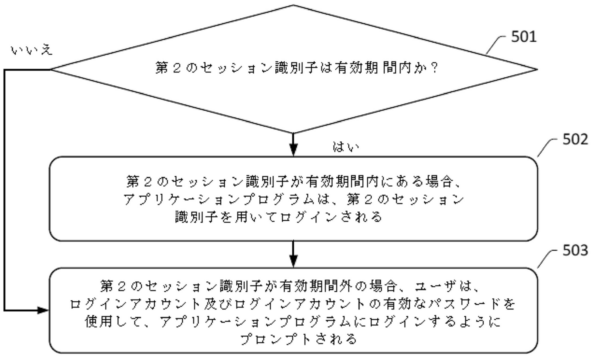
【図３Ｂ】



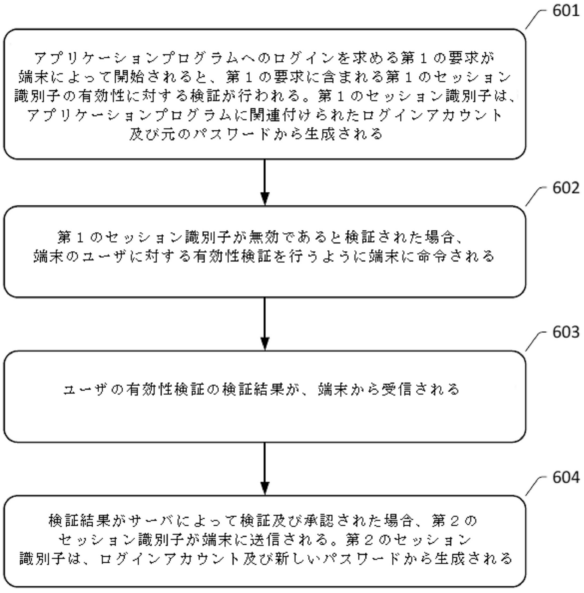
【図４】



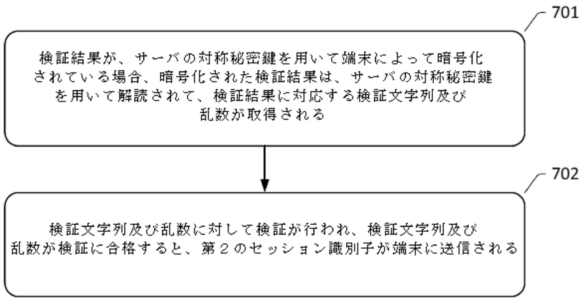
【図５】


501
第２のセッション識別子は有効期間内か？
いいえ
はい
502
第２のセッション識別子が有効期間内にある場合、
アプリケーションプログラムは、第２のセッション
識別子を用いてログインされる
503
第２のセッション識別子が有効期間外の場合、ユーザは、
ログインアカウント及びログインアカウントの有効なパスワードを
使用して、アプリケーションプログラムにログインするように
プロンプトされる

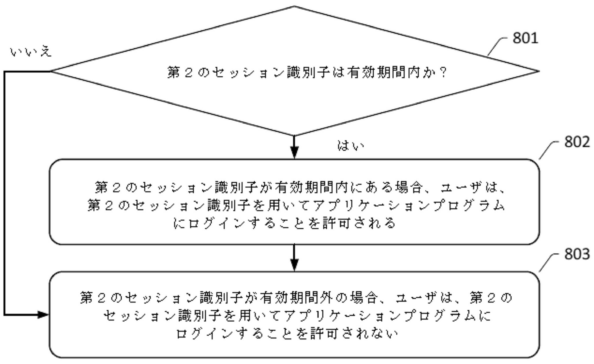
【図６】


601
アプリケーションプログラムへのログインを求める第１の要求が
端末によって開始されると、第１の要求に含まれる第１のセッション
識別子の有効性に対する検証が行われる。第１のセッション識別子は、
アプリケーションプログラムに関連付けられたログインアカウント
及び元のパスワードから生成される
602
第１のセッション識別子が無効であると検証された場合、
端末のユーザに対する有効性検証を行うように端末に命令される
603
ユーザの有効性検証の検証結果が、端末から受信される
604
検証結果がサーバによって検証及び承認された場合、第２の
セッション識別子が端末に送信される。第２のセッション
識別子は、ログインアカウント及び新しいパスワードから生成される

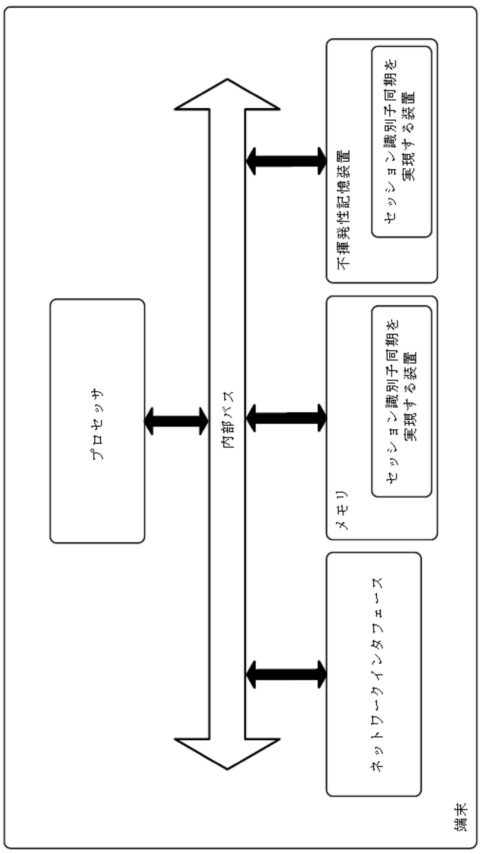
【図７】


701
検証結果が、サーバの対称秘密鍵を用いて端末によって暗号化
されている場合、暗号化された検証結果は、サーバの対称秘密鍵
を用いて解読されて、検証結果に対応する検証文字列及び
乱数が取得される
702
検証文字列及び乱数に対して検証が行われ、検証文字列及び
乱数が検証に合格すると、第２のセッション識別子が端末に送信される

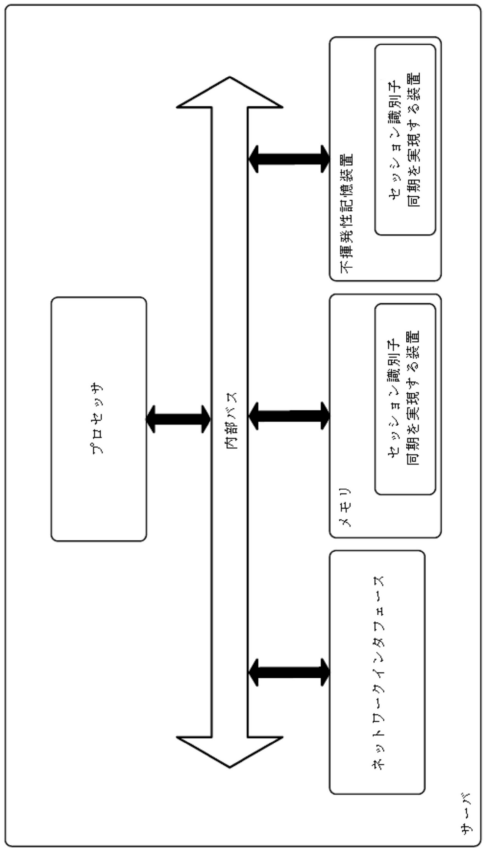
【図８】


801
第２のセッション識別子は有効期間内か？
いいえ
はい
802
第２のセッション識別子が有効期間内にある場合、ユーザは、
第２のセッション識別子を用いてアプリケーションプログラム
にログインすることを許可される
803
第２のセッション識別子が有効期間外の場合、ユーザは、第２の
セッション識別子を用いてアプリケーションプログラムに
ログインすることを許可されない

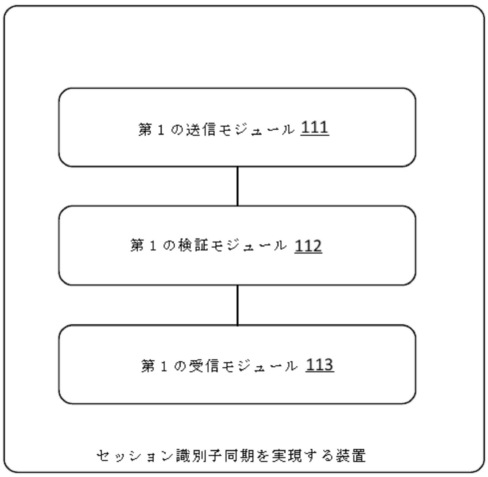
【図９】


プロセッサ
内部バス
不揮発性記憶装置
セッション識別子同期を
実現する装置
メモリ
セッション識別子同期を
実現する装置
ネットワークインタフェース
端末

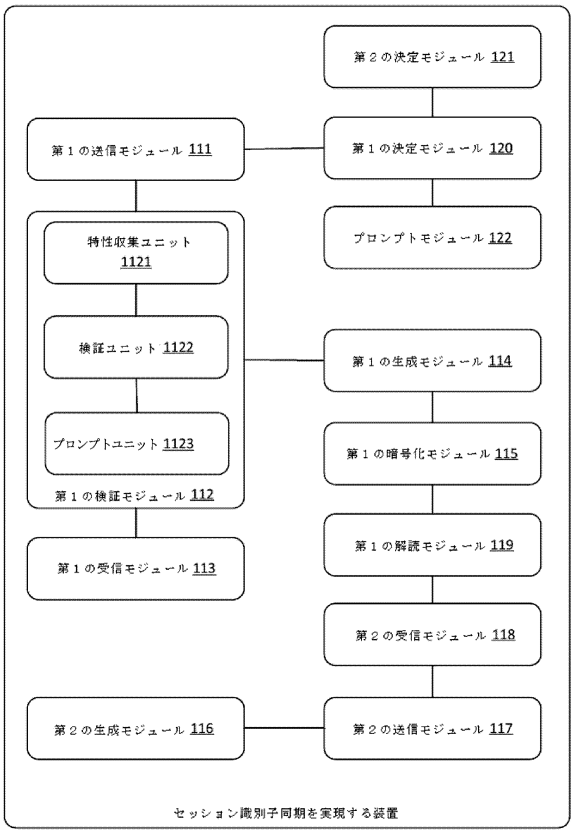
【図１０】



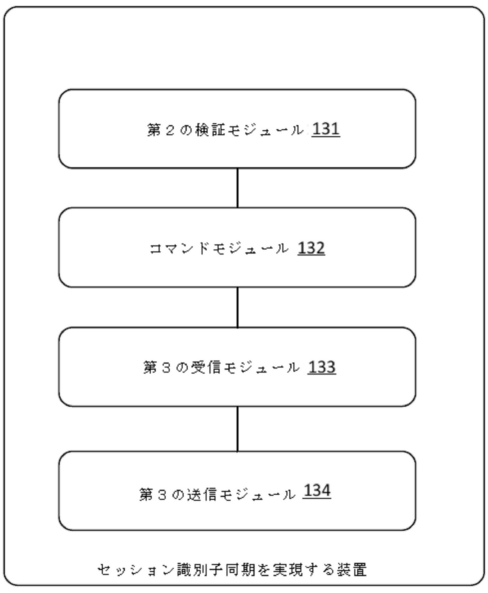
【図１１】



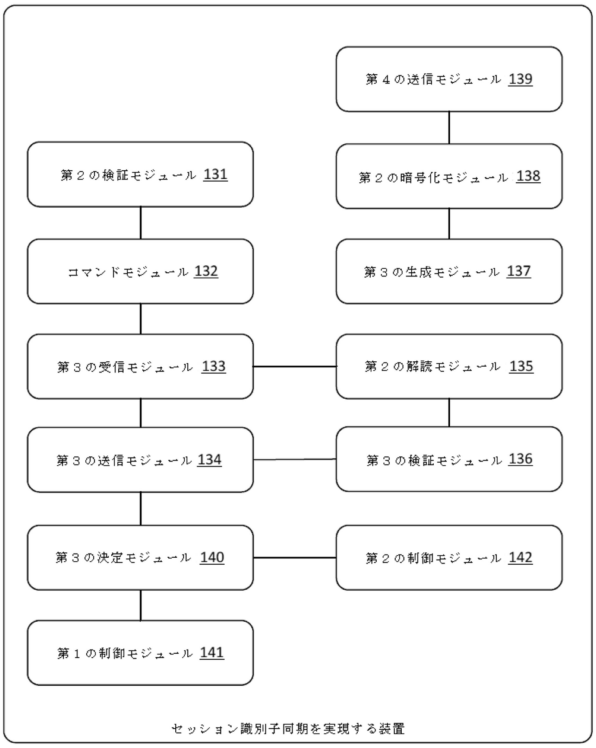
【図１２】



【図１３】



【図１４】


第４の送信モジュール 139
第２の検証モジュール 131
第２の暗号化モジュール 138
コマンドモジュール 132
第３の生成モジュール 137
第３の受信モジュール 133
第２の解読モジュール 135
第３の送信モジュール 134
第３の検証モジュール 136
第３の決定モジュール 140
第２の制御モジュール 142
第１の制御モジュール 141
セッション識別子同期を実現する装置

フロントページの続き

(72)発明者　チアン　ファン
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　チャオ　ドワン
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

審査官　平井　誠

(56)参考文献　特開２００７－３２８４８２（ＪＰ，Ａ）
特開２０１２－１９１２７０（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／００－８８
Ｈ０４Ｌ　９／３２