(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2008-125075
(P2008-125075A)
(43)公開日　平成20年5月29日(2008.5.29)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 9/32	(2006.01)	H04L	9/00	675A	5B285
G06F 21/20	(2006.01)	G06F	15/00	330A	5J104

審査請求 有　請求項の数 35　ＯＬ　（全 20 頁）

(21)出願番号　特願2007-285466 (P2007-285466)
(22)出願日　平成19年11月1日 (2007.11.1)
(31)優先権主張番号　06124154.3
(32)優先日　平成18年11月15日 (2006.11.15)
(33)優先権主張国　欧州特許庁 (EP)

(71)出願人　500043574
リサーチ　イン　モーション　リミテッド
Ｒｅｓｅａｒｃｈ　Ｉｎ　Ｍｏｔｉｏｎ　Ｌｉｍｉｔｅｄ
カナダ国　エヌ２エル　３ダブリュー８　オンタリオ，　ウォータールー，　フィリップ　ストリート　２９５
２９５　Ｐｈｉｌｌｉｐ　Ｓｔｒｅｅｔ，　Ｗａｔｅｒｌｏｏ，　Ｏｎｔａｒｉｏ　Ｎ２Ｌ　３Ｗ８　Ｃａｎａｄａ
(74)代理人　100078282
弁理士　山本　秀策
(74)代理人　100062409
弁理士　安村　高明

最終頁に続く

(54)【発明の名称】クライアント証明書ベースの安全なセッション認証方法および装置

(57)【要約】
【課題】クライアント証明書ベースの安全なセッション認証方法を提供すること。
【解決手段】クライアントデバイスとサーバとの間でメッセージの認証に基づくクライアント証明書に対する方法であって、該クライアントデバイスと該サーバとの双方は、該クライアント証明書を知っており、該方法は、該クライアント証明書を利用して、キーを生成するステップと、該キーを用いて、該クライアントデバイスと該サーバとの間でメッセージを認証するステップとを包含する、方法。
【選択図】図１

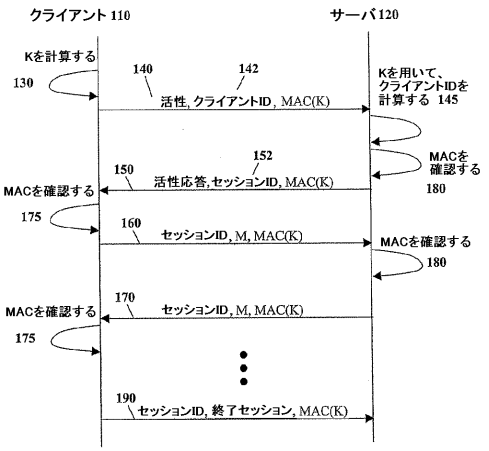

Fig. 1

【特許請求の範囲】
【請求項１】
クライアントデバイスとサーバとの間でメッセージの認証に基づくクライアント証明書に対する方法であって、該クライアントデバイスと該サーバとの双方は、該クライアント証明書を知っており、該方法は、
該クライアント証明書を利用して、キーを生成するステップと、
該キーを用いて、該クライアントデバイスと該サーバとの間でメッセージを認証するステップと
を包含する、方法。
【請求項２】
前記クライアント証明書は、パスワードである、請求項１に記載の方法。
【請求項３】
前記キーは、所望のキー長さが達成されるまで、前記パスワードを繰り返すことによって生成される、請求項１または請求項２に記載の方法。
【請求項４】
前記キーは、前記クライアントデバイスと前記サーバとの双方に知られているハッシュ関数を利用して生成される、請求項１または請求項２に記載の方法。
【請求項５】
前記ハッシュ関数の結果は、所望のキー長さに切頭される、請求項４に記載の方法。
【請求項６】
前記パスワードは、前記キーの前記生成前に、セキュリティトークンと結合される、請求項２に記載の方法、または請求項３～請求項５が請求項２に従属するとき、そのいずれか１項に記載の方法。
【請求項７】
前記セキュリティトークンは、前記クライアントデバイスによって、前記サーバにオフラインで提供される情報を備えており、該情報は、生年月日、出生地、母親の旧姓、および／またはセキュリティ対策のいずれかを備えている、請求項６に記載の方法。
【請求項８】
前記利用するステップは、前記クライアント証明書をセッション識別子と結合して、前記キーを生成すること、および／または前記クライアント証明書を活性化メッセージからのノンスと結合することをさらに包含する、請求項１～請求項７のいずれか１項に記載の方法。
【請求項９】
前記キーの前記生成は、安全な擬似乱数生成器を利用する、請求項１～請求項８のいずれか１項に記載の方法。
【請求項１０】
前記安全な擬似乱数生成器は、前記クライアント証明書をシードとして使用する、請求項９に記載の方法。
【請求項１１】
前記擬似乱数生成器は、前記セキュリティトークンと結合された前記クライアント証明書をシードとして使用する、請求項１０が請求項６に従属するとき、請求項１０に記載の方法。
【請求項１２】
前記擬似乱数生成器は、前記セッション識別子と結合された前記クライアント証明書をシードとして使用するか、あるいは前記ノンスと結合された前記クライアント証明書をシードとして使用する、請求項１０が請求項８に従属するとき、請求項１０に記載の方法。
【請求項１３】
前記キーを用いて、メッセージを認証するステップは、
該キーおよびメッセージを用いて、メッセージ認証コードを生成するステップと、
該メッセージ認証コードを該メッセージに追加して、安全なメッセージを生成するステ

ップと、
該安全なメッセージを送信するステップと
を包含する、請求項１～請求項１２のいずれか１項に記載の方法。
【請求項１４】
前記安全なメッセージを受信すると、前記メッセージ認証コードを再現して、該再現されたメッセージ認証コードを該受信したメッセージ認証コードと比較することよって、該安全なメッセージが、正当かつ不変であると確認される、請求項１３に記載の方法。
【請求項１５】
前記メッセージは、活性化要求メッセージであり、かつクライアント識別子を備えているか、あるいは該メッセージは、活性化返答であり、かつセッション識別子を備えている、請求項１３または請求項１４に記載の方法。
【請求項１６】
前記メッセージは、ＨＴＴＰメッセージであり、前記メッセージ認証コードは、ＨＴＴＰフッターに追加される、請求項１３に記載の方法。
【請求項１７】
前記利用するステップを実行する前に、シーケンス番号を前記メッセージに追加するステップをさらに包含する、請求項１～請求項１６のいずれか１項に記載の方法。
【請求項１８】
前記クライアント証明書を用いて生成された前記キーを利用して、対称キーを交渉するステップをさらに包含する、請求項１～請求項１７のいずれか１項に記載の方法。
【請求項１９】
クライアント証明書に対して適合されるクライアントデバイスであって、該クライアント証明書は、該クライアントデバイスとサーバとの間でのメッセージの認証に基づき、該クライアントデバイスと該サーバとの双方は、該クライアント証明書を知っており、該クライアントデバイスは、
該共有証明書を格納するためのメモリと、
該メモリと通信するプロセッサであって、
該クライアント証明書を利用して、キーを生成することと、
該キーおよびメッセージを用いて、メッセージ認証コードを生成することと、
該メッセージ認証コードを該メッセージに追加して、安全なメッセージを生成すること
を行うように適合されている、プロセッサと、
該安全なメッセージを送信するように適合されている通信サブシステムと
を備える、クライアントデバイス。
【請求項２０】
前記クライアント証明書は、パスワードである、請求項１９に記載のクライアントデバイス。
【請求項２１】
所望のキー長さが達成されるまで、前記パスワードを繰り返すことによって前記キーを生成するように、前記プロセッサは、適合されている、請求項１９または請求項２０に記載のクライアントデバイス。
【請求項２２】
前記クライアントデバイスと前記サーバとの双方に知られているハッシュ関数を利用して、前記キーを生成するように、前記プロセッサは、適合されている、請求項１９または請求項２０に記載のクライアントデバイス。
【請求項２３】
前記ハッシュ関数の結果を、所望のキー長さに切り詰めるように、前記プロセッサは、さらに適合されている、請求項２２に記載のクライアントデバイス。
【請求項２４】
前記キーの生成前に、前記パスワードをセキュリティトークンと結合するように、前記

プロセッサは、さらに適合されている、請求項２０に記載のクライアントデバイス、または請求項２１～請求項２３が請求項２０に従属するとき、そのいずれか１項に記載のクライアントデバイス。

【請求項２５】

前記セキュリティトークンは、前記クライアントデバイスによって、前記サーバにオフラインで提供される情報を備え、該情報は、生年月日、出生地、母親の旧姓、および／またはセキュリティ対策のいずれかを備えている、請求項２４に記載のクライアントデバイス。

【請求項２６】

前記クライアント証明書をセッション識別子と結合して、前記キーを生成するように、あるいは前記クライアント証明書を活性化メッセージからのノンスと結合するように、前記プロセッサは、適合されている、請求項１９～請求項２５のいずれか１項に記載のクライアントデバイス。

【請求項２７】

安全な擬似乱数生成器を利用して、前記キーを生成するように、前記プロセッサは、適合されている、請求項１９～請求項２６のいずれか１項に記載のクライアントデバイス。

【請求項２８】

前記安全な擬似乱数生成器は、前記クライアント証明書をシードとして使用する、請求項２７に記載のクライアントデバイス。

【請求項２９】

前記擬似乱数生成器は、前記セキュリティトークンと結合された前記クライアント証明書をシードとして使用する、請求項２８が請求項２４に従属するとき、請求項２８に記載のクライアントデバイス。

【請求項３０】

前記擬似乱数生成器は、前記セッション識別子と結合された前記クライアント証明書をシードとして使用するか、あるいは前記ノンスと結合された前記クライアント証明書をシードとして使用する、請求項２８が請求項２６に従属するとき、請求項２８に記載のクライアントデバイス。

【請求項３１】

前記メッセージは、活性化要求メッセージであり、かつクライアント識別子を備えているか、あるいは該メッセージは、活性化返答であり、かつセッション識別子を備えている、請求項１９～請求項３０のいずれか１項に記載のクライアントデバイス。

【請求項３２】

シーケンス番号を前記メッセージに追加するように、前記プロセッサは、さらに適合されている、請求項１９～請求項３１のいずれか１項に記載のクライアントデバイス。

【請求項３３】

前記クライアント証明書を用いて生成された前記キーを利用して、対称キーを交渉するように、前記プロセッサは、さらに適合されている、請求項１９～請求項３２のいずれか１項に記載のクライアントデバイス。

【請求項３４】

前記クライアントデバイスは、モバイルデバイスである、請求項１９～請求項３３のいずれか１項に記載のクライアントデバイス。

【請求項３５】

計算デバイスまたはシステムのプロセッサ内で、該計算デバイスまたはシステムに、請求項１～請求項１８のいずれか１項に記載の方法を実行させるプログラムコードを具現化する、コンピュータ読み取り可能な媒体。

【発明の詳細な説明】

【技術分野】

【０００１】

本開示は、一般的に、安全なセッション認証に関し、特に、相当量の計算オーバーヘッ

ドなしに、安全に認証されるセッションの確立に関する。
【背景技術】
【０００２】
クライアント－サーバの環境において、クライアントとサーバとの間の通信は、しばしば、認証される必要がある。特に、しばしば、一つの計算デバイスは、ネットワークを介して、別の計算デバイス（クライアントおよびサーバ）と通信して、特定のサービスにアクセスする。クライアントおよびサーバが真性であること、それによって、アイデンティティおよびデータ保全性を維持することを確実にするために、認証が、要求される。
【０００３】
サーバとクライアントとの間での通信を認証するための幾つかの解決策が、存在する。一つの解決策において、セッションは、シンプルな認証を用いて、認証され得る。今日のインターネット上の安全なウェブサーバの大半は、ＳＳＬ／ＴＬＳ（セキュアソケット層／トランスポート層セキュリティ）を介して、基本認証、またはＨＴＴＰ（ハイパーテキスト転送プロトコル）ポストベースの認証のようなシンプルな認証の一部の形式を用いて、セッションを認証する。次いで、認証されたセッションは、ＨＴＴＰクッキー内のクライアントの中または上に格納されたトークンによって識別される。このスキームは、ＳＳＬ／ＴＬＳを要求するので、複雑である。適切にＳＳＬおよびＴＬＳをサポートするために、クライアントは、比較的強度な暗号化能力を含む必要がある。例えば、公開／秘密キーシステムが、使用され得る。しかしながら、無線データデバイスまたは携帯情報端末（ＰＤＡ）のようなシンプルなクライアント上で、このような強度な暗号化能力を使用することは、そのデバイスによっては、可能でないこともあり得る。さらに、無線環境において使用される場合、この形式の認証を使用することは、チャネルを確立するためだけでも、多数の情報を交換することを要求する。無線デバイスを用いると、無線空間における遅延と、ネットワーク帯域幅、バッテリ寿命、およびデータ送信コストの意味でのコストとは、あまりにも高くつき得る。
【０００４】
代替的な解決策は、よりシンプルな暗号化方法を用いることである。このようなスキームは、ＮＴＬＭ（ウィンドウズ（登録商標）ＮＴ　ＬＡＮマネージャ）認証のようなチャレンジ応答シーケンスを含む。ＮＴＬＭ認証を参照すると、これは、ＴＣＰ（伝送制御プロトコル）接続を認証するチャレンジ応答認証メカニズムに基づくマイクロソフト（登録商標）独自のＨＴＴＰである。ＮＴＬＭ認証された接続を介するＨＴＴＰトラフィックのデータ保全性は、保護されないので、ＨＴＴＰメッセージは、攻撃者によって、変更、削除、または差し込みされ得る。したがって、たとえセッションが認証されても、ＨＴＴＰメッセージに対するデータソース認証は、保証されない。
【０００５】
それゆえ、上述のシンプルな暗号化方法に対して、より安全な解決策が要求される。しかしながら、この解決策が広くインプリメントされることが可能になるためには、この解決策は、どんなに計算量を増やしても増やしすぎるということはない。
【発明の開示】
【課題を解決するための手段】
【０００６】
（概要）
本開示は、クライアントとサーバとの双方によって知られているクライアント証明書を利用することによって、データ保全性が維持される安全なセッション認証の方法および装置を提供することで、上述を克服し得る。特に、本開示は、通信の特定の形式に対して、クライアントとサーバとの双方に既知で共有された秘密を利用する。
【０００７】
一つの実施形態において、クライアントデバイスに対するパスワードは、サーバにも既知であり、これは、共有証明書として使用され得る。
【０００８】

上述の様々な拡張が、とりわけ、セッションの生成、ハッシュキーを生成するためにパスワードと結合される他の既知の情報の使用、共有証明書を展開する（ｅｘｐａｎｄ）ための安全な擬似乱数生成器の使用、アドレッシングリプレイを避けるためのシーケンス番号の使用を含んで記載される。

【０００９】

したがって、本開示は、クライアントとサーバとの間でのメッセージの認証に基づくクライアント証明書のための方法を提供し得、該クライアントと該サーバとの双方は、該クライアント証明書を知っており、該方法は、該クライアント証明書を利用して、キーを生成するステップと、該キーを用いて、該クライアントと該サーバとの間でメッセージを認証するステップとを包含する。

【００１０】

本開示は、クライアント証明書に適合されるクライアントデバイスをさらに提供し得、該クライアント証明書は、該クライアントデバイスとサーバとの間でメッセージの認証に基づき、該クライアントデバイスと該サーバとの双方は、該クライアント証明書を知っており、該クライアントデバイスは、該共有証明書を格納するためのメモリと、該メモリと通信するプロセッサであって、該クライアント証明書を利用して、キーを生成することと、該キーおよびメッセージを用いて、メッセージ認証コードを生成することと、該メッセージ認証コードを該メッセージに追加して、安全なメッセージを生成することとを行うように適合されている、プロセッサと、該安全なメッセージを送信するように適合されている通信サブシステムとを備える。

【００１１】

本発明は、さらに、以下の手段を提供する。

【００１２】

（項目１）

クライアントデバイスとサーバとの間でメッセージの認証に基づくクライアント証明書に対する方法であって、該クライアントデバイスと該サーバとの双方は、該クライアント証明書を知っており、該方法は、

該クライアント証明書を利用して、キーを生成するステップと、

該キーを用いて、該クライアントデバイスと該サーバとの間でメッセージを認証するステップと

を包含する、方法。

【００１３】

（項目２）

上記クライアント証明書は、パスワードである、項目１に記載の方法。

【００１４】

（項目３）

上記キーは、所望のキー長さが達成されるまで、上記パスワードを繰り返すことによって生成される、項目１または項目２に記載の方法。

【００１５】

（項目４）

上記キーは、上記クライアントデバイスと上記サーバとの双方に知られているハッシュ関数を利用して生成される、項目１または項目２に記載の方法。

【００１６】

（項目５）

上記ハッシュ関数の結果は、所望のキー長さに切頭される、項目４に記載の方法。

【００１７】

（項目６）

上記パスワードは、上記キーの上記生成前に、セキュリティトークンと結合される、項目２に記載の方法、または項目３～項目５が項目２に従属するとき、そのいずれか１項に記載の方法。

【００１８】
（項目７）
上記セキュリティトークンは、上記クライアントデバイスによって、上記サーバにオフラインで提供される情報を備えており、該情報は、生年月日、出生地、母親の旧姓、および／またはセキュリティ対策のいずれかを備えている、項目６に記載の方法。
【００１９】
（項目８）
上記利用するステップは、上記クライアント証明書をセッション識別子と結合して、上記キーを生成すること、および／または上記クライアント証明書を活性化メッセージからのノンスと結合することをさらに包含する、項目１～項目７のいずれか１項に記載の方法。
【００２０】
（項目９）
上記キーの上記生成は、安全な擬似乱数生成器を利用する、項目１～項目８のいずれか１項に記載の方法。
【００２１】
（項目１０）
上記安全な擬似乱数生成器は、上記クライアント証明書をシードとして使用する、項目９に記載の方法。
【００２２】
（項目１１）
上記擬似乱数生成器は、上記セキュリティトークンと結合された上記クライアント証明書をシードとして使用する、項目１０が項目６に従属するとき、項目１０に記載の方法。
【００２３】
（項目１２）
上記擬似乱数生成器は、上記セッション識別子と結合された上記クライアント証明書をシードとして使用するか、あるいは上記ノンスと結合された上記クライアント証明書をシードとして使用する、項目１０が項目８に従属するとき、項目１０に記載の方法。
【００２４】
（項目１３）
上記キーを用いて、メッセージを認証するステップは、
該キーおよびメッセージを用いて、メッセージ認証コードを生成するステップと、
該メッセージ認証コードを該メッセージに追加して、安全なメッセージを生成するステップと、
該安全なメッセージを送信するステップと
を包含する、項目１～項目１２のいずれか１項に記載の方法。
【００２５】
（項目１４）
上記安全なメッセージを受信すると、上記メッセージ認証コードを再現して、該再現されたメッセージ認証コードを該受信したメッセージ認証コードと比較することよって、該安全なメッセージが、正当かつ不変であると確認される、項目１３に記載の方法。
【００２６】
（項目１５）
上記メッセージは、活性化要求メッセージであり、かつクライアント識別子を備えているか、あるいは該メッセージは、活性化返答であり、かつセッション識別子を備えている、項目１３または項目１４に記載の方法。
【００２７】
（項目１６）
上記メッセージは、ＨＴＴＰメッセージであり、上記メッセージ認証コードは、ＨＴＴＰフッターに追加される、項目１３に記載の方法。

【００２８】
（項目１７）
上記利用するステップを実行する前に、シーケンス番号を上記メッセージに追加するステップをさらに包含する、項目１～項目１６のいずれか１項に記載の方法。
【００２９】
（項目１８）
上記クライアント証明書を用いて生成された上記キーを利用して、対称キーを交渉するステップをさらに包含する、項目１～項目１７のいずれか１項に記載の方法。
【００３０】
（項目１９）
クライアント証明書に対して適合されるクライアントデバイスであって、該クライアント証明書は、該クライアントデバイスとサーバとの間でのメッセージの認証に基づき、該クライアントデバイスと該サーバとの双方は、該クライアント証明書を知っており、該クライアントデバイスは、
該共有証明書を格納するためのメモリと、
該メモリと通信するプロセッサであって、
該クライアント証明書を利用して、キーを生成することと、
該キーおよびメッセージを用いて、メッセージ認証コードを生成することと、
該メッセージ認証コードを該メッセージに追加して、安全なメッセージを生成すること
を行うように適合されている、プロセッサと、
該安全なメッセージを送信するように適合されている通信サブシステムと
を備える、クライアントデバイス。
【００３１】
（項目２０）
上記クライアント証明書は、パスワードである、項目１９に記載のクライアントデバイス。
【００３２】
（項目２１）
所望のキー長さが達成されるまで、上記パスワードを繰り返すことによって上記キーを生成するように、上記プロセッサは、適合されている、項目１９または項目２０に記載のクライアントデバイス。
【００３３】
（項目２２）
上記クライアントデバイスと上記サーバとの双方に知られているハッシュ関数を利用して、上記キーを生成するように、上記プロセッサは、適合されている、項目１９または項目２０に記載のクライアントデバイス。
【００３４】
（項目２３）
上記ハッシュ関数の結果を、所望のキー長さに切り詰めるように、上記プロセッサは、さらに適合されている、項目２２に記載のクライアントデバイス。
【００３５】
（項目２４）
上記キーの生成前に、上記パスワードをセキュリティトークンと結合するように、上記プロセッサは、さらに適合されている、項目２０に記載のクライアントデバイス、または項目２１～項目２３が項目２０に従属するとき、そのいずれか１項に記載のクライアントデバイス。
【００３６】
（項目２５）
上記セキュリティトークンは、上記クライアントデバイスによって、上記サーバにオフ

ラインで提供される情報を備え、該情報は、生年月日、出生地、母親の旧姓、および／またはセキュリティ対策のいずれかを備えている、項目２４に記載のクライアントデバイス。

【００３７】

（項目２６）

上記クライアント証明書をセッション識別子と結合して、上記キーを生成するように、あるいは上記クライアント証明書を活性化メッセージからのノンスと結合するように、上記プロセッサは、適合されている、項目１９～項目２５のいずれか１項に記載のクライアントデバイス。

【００３８】

（項目２７）

安全な擬似乱数生成器を利用して、上記キーを生成するように、上記プロセッサは、適合されている、項目１９～項目２６のいずれか１項に記載のクライアントデバイス。

【００３９】

（項目２８）

上記安全な擬似乱数生成器は、上記クライアント証明書をシードとして使用する、項目２７に記載のクライアントデバイス。

【００４０】

（項目２９）

上記擬似乱数生成器は、上記セキュリティトークンと結合された上記クライアント証明書をシードとして使用する、項目２８が項目２４に従属するとき、項目２８に記載のクライアントデバイス。

【００４１】

（項目３０）

上記擬似乱数生成器は、上記セッション識別子と結合された上記クライアント証明書をシードとして使用するか、あるいは上記ノンスと結合された上記クライアント証明書をシードとして使用する、項目２８が項目２６に従属するとき、項目２８に記載のクライアントデバイス。

【００４２】

（項目３１）

上記メッセージは、活性化要求メッセージであり、かつクライアント識別子を備えているか、あるいは該メッセージは、活性化返答であり、かつセッション識別子を備えている、項目１９～項目３０のいずれか１項に記載のクライアントデバイス。

【００４３】

（項目３２）

シーケンス番号を上記メッセージに追加するように、上記プロセッサは、さらに適合されている、項目１９～項目３１のいずれか１項に記載のクライアントデバイス。

【００４４】

（項目３３）

上記クライアント証明書を用いて生成された上記キーを利用して、対称キーを交渉するように、上記プロセッサは、さらに適合されている、項目１９～項目３２のいずれか１項に記載のクライアントデバイス。

【００４５】

（項目３４）

上記クライアントデバイスは、モバイルデバイスである、項目１９～項目３３のいずれか１項に記載のクライアントデバイス。

【００４６】

（項目３５）

計算デバイスまたはシステムのプロセッサ内で、該計算デバイスまたはシステムに、項目１～項目１８のいずれか１項に記載の方法を実行させるプログラムコードを具現化する

、コンピュータ読み取り可能な媒体。
【００４７】
（摘要）
クライアントとサーバとの間でメッセージの認証に基づくクライアント証明書に対する方法および装置であって、該クライアントと該サーバとの双方は、該クライアント証明書を知っており、該方法は、該クライアント証明書を利用して、キーを生成するステップと、該キーを用いて、該クライアントと該サーバとの間でメッセージを認証するステップとを有する。
【発明を実施するための最良の形態】
【００４８】
本開示は、図面を参照することによって、より良く理解される。
【００４９】
（好ましい実施形態の説明）
ここで、図１を参照する。図１の例示的な処理において、クライアント１１０は、サーバ１２０と通信する。いずれの方向における通信が、正当であり、データ挿入または変更が発生しないようにするために、本開示は、メッセージテキストを添付された通信を提供し、このメッセージテキストは、この通信の両エンドで複製され得る識別子を有する。
【００５０】
好ましい実施形態において、添付された識別子は、メッセージ認証コード（ＭＡＣ）である。ＭＡＣは、この分野で周知であり、２つの入力を含む。特に、これらの入力は、ＭＡＣが添付されるテキストと、秘密キーとである。両者を組み合わせると、ハッシュが生成されることを可能にし、秘密キーの知識がないと、ハッシュは、複製され得ない。当業者には理解されるように、ランダム値が有効とされないように、ハッシュ値は、一般的に、十分大きい。
【００５１】
様々なＭＡＣアルゴリズムが使用され得る。一つの例は、ＨＭＡＣアルゴリズムである。このようなアルゴリズムは、例えば、
【００５２】
【数１】

$$HMAC_K(m) = h((K \oplus opad) \,||\, h((K \oplus ipad) \,||\, m))$$

であり得る。
【００５３】
ここで、Ｋは、キーであり、ｏｐａｄおよびｉｐａｄは、定数であり、ｍは、メッセージである。Ｈは、安全ハッシュ関数である。
【００５４】
【数２】

$\oplus$

の記号は、ビットごとの排他的論理和（ＸＯＲ）を表し、
【００５５】
【数３】

$||$

の記号は、連結を示す。
【００５６】
「ｈ」が、ＳＨＡ１－アルゴリズムであるように選択される場合、アルゴリズムは、ＳＨＡ１－ＨＭＡＣとなり、これは、シンプルなデバイス上でインプリメントされ得る。
【００５７】
再び、図１を参照すると、クライアント１１０は、セッションが活性化される前に、サ

ーバ１２０と通信したいと願う。ステップ１３０で、クライアント１１０は、キー（Ｋ）を計算する。このキーは、クライアント１１０とサーバ１２０との双方に知られているクライアント証明書に基づく。例えば、キーは、クライアント１１０上のパスワードに基づき得る。このサーバは、既に、このパスワードを有し、したがって、通信チャネルを介して、そのパスワードを送信する必要はない。

【００５８】

当業者には理解されるように、ＭＡＣ関数は、キーが特定の長さであることを要求し得る。したがって、パスワードがキーとして使用され得る前に、パスワードは、様々なアルゴリズムによって修正され、所望の長さのキーを生成する必要があり得る。このような決定論的なアルゴリズムは、当業者には公知であり、様々なアルゴリズムが使用され得る。

【００５９】

一つのこのようなアルゴリズムは、所望のビット数に到達されるまで、コード化されたパスワードストリングを繰り返すことであり得る。他のアルゴリズムは、ＳＨＡ１のような安全なハッシュ関数を用いてパスワードをハッシュして、展開し、特定のビット数を生成して、次いで、不要な任意の過剰のビットを除去する。別のアプローチは、パスワードまたは他のクライアント証明書を、安全な擬似乱数生成器（ＰＲＮＧ）とともに、使用することである。パスワードまたはクライアント証明書を、安全な擬似乱数生成器に対するシードであり得、サーバとクライアントとの双方が、同じ擬似乱数生成器を有する限り、安全なＰＲＮＧによって出力されたビットに要求される数が、キーを構成する。他のアルゴリズムも、当業者には公知である。

【００６０】

他の安全な情報は、パスワードに追加され、エントロピを改善し得る。例えば、クライアントとサーバとの双方に知られている情報の中でも、とりわけ、生年月日、出生都市、母親の旧姓が、パスワードに追加され得、セキュリティトークンの一部として使用され、ＰＲＮＧをシードするため、あるいは安全なハッシュ関数の引数として使用され、キーを生成する。このような追加の安全な情報は、クライアントによってオフラインで提供される。

【００６１】

当業者には理解されるように、安全なハッシュ関数は、可逆的ではない。また、安全なＰＲＮＧによって生成されたランダムバイトのシーケンスが与えられると、ＰＲＮＧによって使用されたシードを計算して、そのシーケンスを生成することは不可能である。したがって、安全なハッシュ関数または安全なＰＲＮＧがキー生成に使用されるとき、所与のセッションに対するキーが危険に晒される場合であっても、パスワードは、即座に回復されない。

【００６２】

理解されるように、パスワードをキーＫに対する所定の長さに展開して、そのパスワード全体を使用することは、パスワードの部分のみを使用することに比べて好ましい。なぜなら、このことは、より安全なキーを提供するからである。

【００６３】

処理は、次いで、ステップ１４０に進む。ステップ１４０で、クライアント１１０は、活性メッセージをサーバ１２０に送信する。活性メッセージは、クライアントＩＤ１４２のようなクライアントを識別するための識別子を含むことが好ましい。このメッセージは、さらに、活性メッセージに対するＭＡＣを含む。当業者には理解されるように、ＭＡＣは、ステップ１３０で計算されたキーとともに、メッセージ情報を含む。

【００６４】

一例において、メッセージは、ＨＴＴＰメッセージであり得る。ユーザが、ＨＴＴＰを介して安全なセッションを確立しようと試みる場合、ＭＡＣは、ＨＴＴＰフッターに追加され得る。しかしながら、この例は、限定するものではなく、他のメッセージタイプも考慮される。

【００６５】

ステップ１４５で、サーバ１２０は、ステップ１４０からのメッセージ内で受信したクライアント識別子に対するキーを計算する。サーバ１２０は、クライアント１１０のクライアント証明書から共通の秘密を知っており、それゆえ、クライアントＩＤを使用して、これらのクライアント証明書を見出し得、クライアント１１０がキーＫを計算するのに使用したのと同じアルゴリズムに基づいて、キーを計算し得る。ステップ１４５で、一度キーが計算されると、このキーは、サーバ１２０上にローカルに格納され得、クライアントＩＤ１４２またはセッション識別子と関連付けられる。これは、クライアント１１０から受信した任意の後続のメッセージに対して再計算する必要を排除するためである。

【００６６】

ステップ１５０で、サーバ１２０は、クライアント１１０に活性応答を、活性応答メッセージに対するセッション識別子１５２およびＭＡＣとともに返信する。ここでも、ＭＡＣは、共有されたキーと、活性応答メッセージのコンテンツとに基づいて計算される。

【００６７】

一度クライアント１１０が、セッション識別子１５２を受信すると、ステップ１６０に示されるように、セッション識別子は、サーバ１２０に送信された後続のメッセージに含まれ得る。同様に、ステップ１７０に示されるように、サーバ１２０からクライアント１１０へのメッセージもまた、セッション識別子を含み得る。

【００６８】

セッションの一部として、活性化メッセージおよび後続のメッセージを含む任意のメッセージは、確認される必要がある。クライアント１１０が、メッセージを受信するとき、メッセージのＭＡＣを確認して、そのメッセージが認証されたことを確証する必要がある。これは、受信されたメッセージを採って、クライアント１１０のキーを用いて、そのメッセージをハッシュすることによって行われる。このハッシュの結果は、サーバ１２０から送信されているＭＡＣと比較される。これは、ステップ１７５として示される。

【００６９】

同様に、サーバ１２０が、クライアント１１０からメッセージを受信するとき、特定のクライアントＩＤに対するキーを用いて、そのメッセージをハッシュして、これをクライアント１１０から送信されたＭＡＣと比較する。これは、ステップ１８０に示されている。

【００７０】

確認ステップ１７５または１８０のいずれかが、それぞれクライアント１１０またはサーバ１２０から送信されているＭＡＣと合致しない結果を生成する場合、このメッセージは、無効なものであると考えられ、成りすまし（ｓｐｏｏｆ）であり得るか、あるいは、何者かによるデータ挿入またはメッセージからのデータ削除の試みであり得る。このメッセージは、無視され得るか、エラーが発信者に返信され得る。

【００７１】

セッションを終了した後、ステップ１９０で、サーバ１２０またはクライアント１１０のいずれかが、相手側にメッセージを送信することによって、セッションを解体し得る。このメッセージは、セッション識別子および終了セッションメッセージを含む。この終了セッションメッセージは、終了セッションに対するＭＡＣ、セッション識別子、およびキーＫをともなう。ステップ１９０で、メッセージが確認される場合、セッションは、終了される。

【００７２】

ここで、図２への参照がなされる。図２は、クライアント１１０とサーバ１２０との間のデータフロー図を示し、図１の実施形態に対する代替の実施形態を提供する。特に、図１の実施形態は、アドレッシングリプレイを妨げないので、システムの設計者が、アドレッシングリプレイ攻撃に関して心配する場合、代わりに、図２の方法が使用される。

【００７３】

当業者には理解されるように、図１の方法を利用するとき、クライアント１１０とサーバ１２０との間での通信を詮索する第三者は、メッセージを傍受し、そのメッセージをサ

ーバ１２０に再送信し得る。図１の方法において、サーバ１２０は、同じ確認１８０を実行し、そのメッセージが有効であることを見出し、適切な応答を送信する。一部の場合において、このようなアドレッシングリプレイ攻撃の発生を許容することは望ましくない。この場合、シーケンス番号が、メッセージの一部として使用され得る。

【００７４】

特に、クライアント１１０は、図１のように、ステップ１３０で、キーＫを計算する。次いで、ステップ２１０で、メッセージが送信され、このメッセージは、活性メッセージ、クライアント識別子１４０、シーケンス番号２４４、およびＭＡＣ２４８を含む。ＭＡＣ２４８は、今やシーケンス番号２４４を含むメッセージに基づいて計算される。シーケンス番号をＭＡＣ計算に含めることで、何者かが、クライアント１１０に成りすまそうと試みるために、異なるシーケンス番号を引き続き挿入することを防ぐ。

【００７５】

サーバ１２０が、ステップ２１０からメッセージを受信するとき、図１の方法のように、ステップ１４５で、サーバ１２０は、クライアントＩＤ１４２に対するキーを計算する。さらに、また、ステップ１８０で、図１と同じように、シーケンス番号も確認する。この処理はまた、ステップ２１５で、シーケンス番号も確認する。このことは、サーバ１２０が、以前に特定のクライアントＩＤから、シーケンス番号を受信したか否かをチェックし、受信した場合は、そのメッセージを無視することを含む。当業者には理解されるように、クライアント１１０が、図２の方法を用いてメッセージを送信するときはいつも、一意的なシーケンス番号が、メッセージとともに送信されるべきである。一意的なシーケンス番号を提供する様々な方法は、当業者には公知である。

【００７６】

ステップ１８０で、ＭＡＣが確認され、ステップ２１５で、シーケンス番号が確認される場合、サーバ１２０は、活性応答メッセージ２２０をクライアント１１０に返信する。この活性応答メッセージは、応答、セッション識別子１５２、シーケンス番号２５４を、ＭＡＣ２５８とともに含む。

【００７７】

図１の方法と同様に、後続のメッセージは、セッション識別子、メッセージ、およびＭＡＣを有するシーケンス番号とともに進み得、ＭＡＣは、これらの全てのために、クライアント１１０とサーバ１２０との双方に知られているキーを用いて計算される。

【００７８】

セッション終了時に、サーバ１２０またはクライアント１１０のいずれかが、終了セッションメッセージを送信することによって、セッションを解体し得る。この終了セッションメッセージは、これらの全てのために、セッション識別子、シーケンス番号、およびＭＡＣを含む。次いで、セッションは、終了される。

【００７９】

パスワードが、キーに対して使用される場合、そのキーが悪いエントロピを有し得るという懸念があり得る。一つの解決策は、所望のパスワード強度レベルを強化することである。例えば、パスワードが最小長さであること、文字と数字との双方を有すること、および共通の単語ではないことを確実にすることなどによってである。例えば、セキュリティエキスパートに許容可能である妥当なキーエントロピを達成するために、パスワード、またはパスワードと他のセキュリティトークンとの結合は、２０バイト以上であり得る。

【００８０】

クライアント１１０およびサーバ１２０によって確立された全てのセッションに対して、キーが同じ状態に留まっていることは、セキュリティの懸念であり得る。解決策として、一意的なキーが、クライアント１１０およびサーバ１２０によって確立されたセッションごとに使用され得る。したがって、一つの方法は、一度セッション識別子が受信されると、キーの一部として、セッション識別子を使用し得る。

【００８１】

図３を参照すると、クライアント１１０は、サーバ１２０と通信する。最初に、ステッ

プ１３０で、キーが計算され、ステップ３１０で、クライアント識別子およびＭＡＣを含む活性メッセージが、サーバに送信される。ステップ１３０で計算されたキーは、パスワードのような共有された秘密に基づく。次いで、サーバは、クライアント識別子に対するキーＫを計算し、ステップ１８０で、ＭＡＣを確認する。その後、ステップ３１５で、本明細書ではＫ２で示される第二のキーが、サーバ１２０によって生成される。Ｋ２は、パスワードのようなクライアント１１０と共有された証明書と、セッションに割り当てられているセッション識別子との結合から導出され得る。共有証明書とセッション識別子との結合に対するアルゴリズムは、クライアント１１０とサーバ１２０との双方に知られている。

【００８２】

ステップ３２０で、サーバ１２０は、認証された応答メッセージをクライアント１１０に返信する。この応答メッセージは、活性応答、セッション識別子１５２を、キーＫ２を用いて形成されたＭＡＣとともに含む。クライアント１１０は、ステップ３２５で、ステップ３２０のメッセージの中で受信したセッション識別子に基づいて、キーＫ２を計算し、キーＫ２を格納する。クライアント１１０は、次いで、サーバ１２０と引き続き通信するために、このキーＫ２を使用する。

【００８３】

理解されるように、図３の方法もまた、メッセージ内のシーケンス番号を利用し得るので、図２の方法と図３の方法とは、組み合わせられ得る。

【００８４】

キー内のセッション識別子の使用は、そのセッションに対する一意的なキーを提供する。

【００８５】

さらなる代替において、より安全な対称キーが、共有されたクライアント証明書に基づいて、キーを利用して、クライアントとサーバとの間で交渉され得、こうして、対称暗号化が可能になる。例えば、クライアントは、サーバにセッション活性化メッセージを送信し得る。サーバは、次いで、共有されたキーを用いて暗号化されている対称キーを用いて応答し得る。代替として、クライアントは、当初のメッセージの中のより安全なキーを送信し得る。なぜなら、サーバとクライアントとの双方は、より安全なキーの復号に使用される共有キーを知っているからである。次いで、対称キーは、クライアントとサーバとの間でのメッセージの認証および／または暗号化に使用され得る。しかしながら、この強化は、対称暗号化／復号能力を要求する。

【００８６】

当業者には理解されるように、上記は、データを送信するために適切な任意のプロトコルを用いて送信され得るが、ＵＤＰのようなデータベースのプロトコルが、無線デバイスにとって好ましい。

【００８７】

したがって、図１、図２、および図３は、ハッシュするためのキーを生成するために、共有された秘密を用いて、クライアントとサーバとの間で通信をする方法を示す。次いで、ハッシュは、このキーを利用し得、メッセージの中に組み込まれ得て、メッセージの正当性を確保し、成りすまし、あるいはメッセージへのデータ挿入またはメッセージからのデータの削除を防止する。知られている証明書は、パスワードのように、クライアントとサーバとの双方に既知のアイテムを含み得る。代替案は、クライアントおよびサーバに知られることになるキーをクライアントとサーバとの双方に追加することを含む。これは、モバイルデバイスが製造されるとき、そのモバイルデバイスのプロビジョニングの間に行われ得るか、あるいは後にプロビジョニングの間に行われ得るかのいずれかである。

【００８８】

上記に基づくと、メッセージ保全性がＭＡＣによって保護されるので、転送の際に、メッセージは、修正され得ない。セッションの所有者のみが、そのセッションに対する有効なメッセージを生成し得ることも、また理解されるべきである。したがって、サーバもま

た、認証される。

【００８９】

クライアント１１０は、サーバ１２０と通信し得る任意のデバイスであり得る。コンピュータのような有線デバイスも利用され得る。しかしながら、本明細書に記載された方法の保護の性質と、軽量な計算要求とのために、本方法は、限られた計算能力を有するデバイス上でもまた使用され得る。このようなデバイスは、例えば、一部の無線デバイスを含み得る。ここで、さらなるメリットは、ハンドシェーキングルーチンのために、限られた通信回数を有することから得られる。本方法が使用され得る一つの例示的なモバイルデバイスが、以下に図４を参照して記載される。これは、限定することを意味するのではなく、例示的な目的で提供される。

【００９０】

図４は、本出願の装置および方法の好ましい実施形態で使用されることの多いモバイルデバイスを示すブロック図である。モバイルデバイス４００は、少なくとも音声およびデータ通信能力を有する双方向無線通信デバイスであることが好ましい。モバイルデバイス４００は、インターネット上の他のコンピュータシステムと通信する能力を有することが好ましい。この無線デバイスは、提供される正確な機能性に依存して、例えば、データメッセージ伝達デバイス、双方向ページャ、無線ｅメールデバイス、データメッセージ伝達能力を有するセルラ電話、無線インターネット機器、あるいはデータ通信デバイスと称され得る。

【００９１】

モバイルデバイス４００は、双方向通信が可能な場合、通信サブシステム４１１を組み込む。通信サブシステム４１１は、受信機４１２と送信機４１４との双方と、１つ以上の関連コンポーネントとを含む。関連コンポーネントは、例えば、好ましくは内蔵または内部のアンテナ素子４１６および４１８、局部発振器（ＬＯ）４１３、デジタル信号プロセッサ（ＤＳＰ）４２０のような処理モジュールである。通信分野の当業者に明らかなように、通信サブシステム４１１の特定の設計は、そのデバイスが動作するように意図される通信ネットワークに依存する。

【００９２】

ネットワークアクセス要求もまた、ネットワーク４１９のタイプに依存しても変化する。一部のＣＤＭＡネットワークにおいて、ネットワークアクセスは、モバイルデバイス４００のクライアントまたはユーザに関連する。ＣＤＭＡモバイルデバイスは、ＣＤＭＡネットワーク上で動作するために、取り外し可能なユーザ識別モジュール（ＲＵＩＭ）またはクライアント識別モジュール（ＳＩＭ）カードを要求し得る。ＳＩＭ／ＲＵＩＭインターフェース４４４は、通常はカードスロットに似ており、この中に、ディスケットまたはＰＣＭＣＩＡカードのように、ＳＩＭ／ＲＵＩＭカードが挿入および排出され得る。ＳＩＭ／ＲＵＩＭカードは、約６４Ｋのメモリを有し得、多数のキー構成４５１と、ＩＤおよびクライアント関連情報のような他の情報４５３を保持し得る。

【００９３】

要求されるネットワーク登録または活性化手順が完了したとき、モバイルデバイス４００は、ネットワーク４１９を介して、通信信号を送受信し得る。図４に示されるように、ネットワーク４１９は、モバイルデバイスと通信する複数の基地局からなり得る。例えば、ハイブリッドＣＤＭＡ　１ｘＥＶＤＯシステムにおいて、ＣＤＭＡ基地局およびＥＶＤＯ基地局は、モバイルデバイスと通信し、そのモバイルデバイスは同時に両者と接続される。ＥＶＤＯ基地局およびＣＤＭＡ　１ｘ基地局は、異なるページングスロットを用いて、モバイルデバイスと通信する。

【００９４】

通信ネットワーク４１９を介してアンテナ４１６によって受信された信号は受信機４１２へ入力され、受信機４１２は、信号増幅、周波数下方変換、フィルタリング、チャネル選択など、および、図４に示される例のシステムにあるアナログデジタル（Ａ／Ｄ）変換などの一般的な受信機の機能を実行し得る。受信信号のＡ／Ｄ変換によって、ＤＳＰ４２

０において実行される復調および復号化などのより複雑な通信機能が可能になる。同様に、送信されるべき信号は、例えば、ＤＳＰ４２０による変調および符号化を含む処理がされ、デジタルアナログ変換、周波数上方変換、フィルタリング、増幅、アンテナ４１８を介した通信ネットワーク４１９上への送信のために、送信機４１４へ入力される。ＤＳＰ４２０は、通信信号を処理するだけでなく、受信機および送信機の制御も提供する。例えば、受信機４１２および送信機４１４における通信信号に付与される利得は、ＤＳＰ４２０内でインプリメントされる自動利得制御アルゴリズムを介して適合するように制御され得る。

【００９５】

モバイルデバイス４００は、デバイスの動作全体を制御するマイクロプロセッサ４３８を含むことが好ましい。少なくともデータおよび音声通信を含む通信機能は、通信サブシステム４１１を介して実行される。また、マイクロプロセッサ４３８は、ディスプレイ４２２、フラッシュメモリ４２４、ランダムアクセスメモリ（ＲＡＭ）４２６、補助入力／出力（Ｉ／Ｏ）サブシステム４２８、シリアルポート４３０、１つ以上のキーボードまたはキーパッド４３２、スピーカ４３４、マイク４３６、短距離通信サブシステムのような他の通信サブシステム４４０、および、一般的に４４２で示される任意の他のデバイスサブシステムなどの追加デバイスサブシステムと相互作用する。シリアルポート４３０は、ＵＳＢポート、または当業者には周知の他のポートを含み得る。

【００９６】

図４に示されるサブシステムの一部は、通信関連の機能を実行するのに対して、他のサブシステムは「常駐」機能またはオンデバイス機能を提供し得る。とりわけ、キーボード４３２およびディスプレイ４２２などの一部のサブシステムは、例えば、通信ネットワークを介する送信のためのテキストメッセージの入力などの通信関連機能と、計算器またはタスクリストのようなデバイス常駐機能との双方のために用いられ得る。

【００９７】

マイクロプロセッサ４３８によって用いられるオペレーティングシステムソフトウェアは、フラッシュメモリ４２４などの持続性ストアに格納されることが好ましい。フラッシュメモリ４２４は、代替として、読み出し専用メモリ（ＲＯＭ）または同様のストレージエレメント（図示せず）であり得る。オペレーティングシステム、特定のデバイスアプリケーション、またはそのパーツが、ＲＡＭ４２６などのような揮発性メモリの中に一時的にロードされ得ることは、当業者には理解される。受信された通信信号もまた、ＲＡＭ４２６の中に格納され得る。

【００９８】

図示されるように、フラッシュメモリ４２４は、コンピュータプログラム４５８と、プログラムデータストレージ４５０、４５２、４５４および４５６との双方の異なるエリアの中に分離され得る。これらの異なるストレージタイプは、これら自身のデータストレージ要求のために、各プログラムがフラッシュメモリ４２４の一部分に割り当てられ得ることを示す。マイクロプロセッサ４３８は、そのオペレーティングシステム機能に加えて、モバイルデバイス上でソフトウェアアプリケーションの実行を可能にすることが好ましい。例えば、少なくともデータおよび音声の通信アプリケーションを含む基本的な動作を制御する所定のアプリケーションのセットは、通常は製造中にモバイルデバイス４００にインストールされる。他のアプリケーションも、引き続き、あるいは動的にインストールされ得る。

【００９９】

好ましいソフトウェアアプリケーションは、モバイルデバイスのユーザに関連するデータ項目を編成および管理する能力を有する個人情報マネージャ（ＰＩＭ）アプリケーションであり得る。ユーザに関連するデータ項目としては、ｅメール、カレンダーイベント、音声メール、約束、タスク項目などが挙げられるが、これらに限定されない。当然、１つ以上のメモリストアは、モバイルデバイス上で利用可能であり、ＰＩＭデータ項目のストレージを容易にする。このようなＰＩＭアプリケーションは、無線ネットワーク４１９を

介してデータ項目を送受信する能力を有することが好ましい。好ましい実施形態において、ＰＩＭデータ項目は、無線ネットワーク４１９を介して、ホストコンピュータシステムに格納または関連付けされたモバイルデバイスユーザの対応データ項目を用いて、途切れなく統合、同期および更新される。さらなるアプリケーションはまた、ネットワーク４１９、補助Ｉ／Ｏサブシステム４２８、シリアルポート４３０、短距離通信サブシステム４４０、または任意の他の適切なサブシステム４４２を介してモバイルデバイス４００上にロードされ得て、マイクロプロセッサ４３８による実行のために、ＲＡＭ４２６、または好ましくは不揮発性ストア（図示せず）内に、ユーザによってインストールされ得る。アプリケーションのインストールにおけるそのような柔軟性は、デバイスの機能性を高め、オンデバイス機能、通信関連機能、またはその双方の強化を提供し得る。例えば、安全な通信アプリケーションによって、モバイルデバイス４００を用いて実行される電子商取引機能および他のそのような金融取引が可能となり得る。

【０１００】

データ通信モードにおいて、テキストメッセージまたはウェブページダウンロードのような受信信号は、通信サブシステム４１１によって処理され、マイクロプロセッサ４３８に入力される。マイクロプロセッサ４３８は、ディスプレイ４２２または代替として補助Ｉ／Ｏデバイス４２８への出力のために、受信信号をさらに処理することが好ましい

モバイルデバイス４００のユーザは、また、例えば、ディスプレイ４２２およびおそらく補助Ｉ／Ｏデバイス４２８と連動するキーボード４３２を用いてｅメールメッセージのようなデータ項目を構成し得る。キーボード４３２は、完全な英数字キーボードまたは電話タイプのキーパッドであることが好ましい。このように構成された項目は、次いで、通信サブシステム４１１を介して通信ネットワーク上に送信され得る。

【０１０１】

音声通信のために、モバイルデバイス４００の動作全体は、類似している。ただし、受信信号は、好ましくはスピーカ４３４への出力であり、送信のための信号は、マイク４３６によって生成されるという点は除く。代替の音声またはオーディオＩ／Ｏサブシステムもまた、例えば、音声メッセージ記録サブシステムなどは、モバイルデバイス４００上でインプリメントされ得る。音声またはオーディオ信号出力は主にスピーカ４３４を介して達成されることが好ましいが、ディスプレイ４２２もまた用いられて、例えば、呼び出し人のアイデンティティの表示、音声呼び出しの継続時間、他の音声呼び出し関連情報を提供し得る。

【０１０２】

図４におけるシリアルポート４３０は、通常、携帯情報端末（ＰＤＡ）タイプのモバイルデバイスでインプリメントされる。このモバイルデバイスが、ユーザのデスクトップコンピュータ（図示せず）と同期することは望ましいことであり得るが、これは、随意のデバイスコンポーネントである。このようなポート４３０によって、ユーザは、外部デバイスまたはソフトウェアプリケーションを介して優先度を設定でき、無線通信ネットワーク以外を介して、モバイルデバイス４００に情報またはソフトウェアのダウンロードを提供することで、モバイルデバイス４００の能力を拡張できる。代替のダウンロード経路は、例えば、直接それゆえ確実で信頼性ある接続を介して、デバイスに暗号化キーをロードし、それによって安全なデバイス通信を可能にするために使用され得る。当業者には理解されるように、シリアルポート４３０は、モバイルデバイスをコンピュータに接続して、モデムとして機能するために、さらに使用され得る。

【０１０３】

短距離通信サブシステムのような他の通信サブシステム４４０は、さらなる随意のコンポーネントであり、モバイルデバイス４００と、異なるシステムまたはデバイスとの間での通信を提供し得る。この異なるシステムまたはデバイスは、必ずしも同様のデバイスである必要はない。例えば、サブシステム４４０は、赤外線デバイス、ならびに関連回路およびコンポーネント、あるいはＢｌｕｅｔｏｏｔｈ™通信モジュールを含み得て、通信に同様に有効化されたシステムおよびデバイスを提供する。

【０１０４】
図４の実施形態は、本明細書の方法をインプリメントするため使用されるデバイスに必ずしも必要でないこともあり得る多数の局面を含む。
【０１０５】
より基本的なデバイスは、プロセッサ、メモリ、および通信サブシステムのみを含み得る。特に、デバイスは、キーＫと、キーＫに基づくＭＡＣとを生成することをプロセッサに要求する。メモリは、パスワードのような共有証明書を格納するために使用され得る。通信サブシステムは、セルラネットワークまたは無線ローカルエリアネットワーク（ＷＬＡＮ）、あるいは有線接続用のモデムまたはケーブル接続と通信するために、無線サブシステムのような無線通信システムを含み得る。図４からの一部の特徴の組み合わせを有して、メモリ、プロセッサ、および通信サブシステムを有する他のデバイスもまた、使用され得る。
【０１０６】
本明細書に記載された実施形態は、本出願の技術のエレメントに対応するエレメントを有する構造、システムまたは方法の例である。この書面による記載によって、当業者は、本出願の技術のエレメントと同様に対応する代替のエレメントを有する実施形態を実施し、使用することが可能となり得る。本出願の技術で意図される範囲は、したがって、本明細書に記載されたような本出願の技術と異ならない他の構造、システムまたは方法を含み、本明細書に記載されたような本出願の技術と実質的でない差を有する他の構造、システムまたは方法をさらに含む。
【図面の簡単な説明】
【０１０７】
【図１】図１は、クライアントとサーバとの間の例示的な通信を示すデータフロー図である。
【図２】図２は、クライアントとサーバとの間の代替の例示的な通信を示すデータフロー図である。
【図３】図３は、クライアントとサーバとの間のさらなる代替の例示的な通信を示すデータフロー図である。
【図４】図４は、上記と関連して使用され得る例示的なモバイルデバイスを示すブロック図である。
【符号の説明】
【０１０８】
１１０　クライアント
１２０　サーバ
１４２　クライアントＩＤ
１５２　セッション識別子
２４８、２５８　ＭＡＣ
２５４　シーケンス番号

【図１】

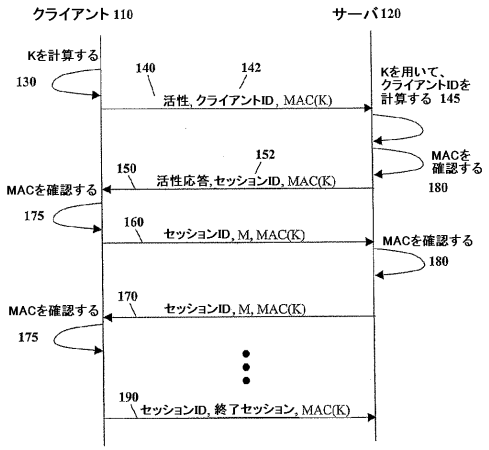

Fig. 1

【図２】

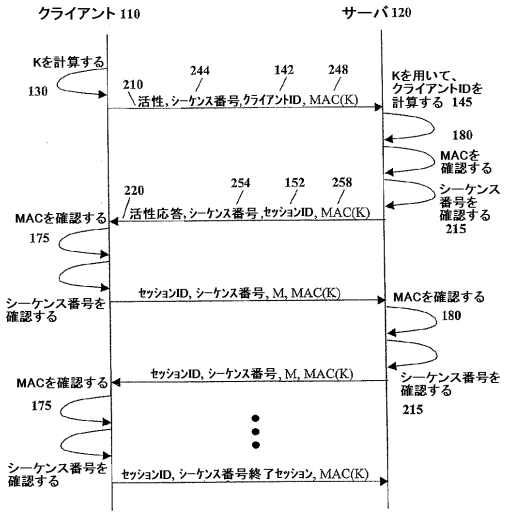

Fig. 2

【図３】

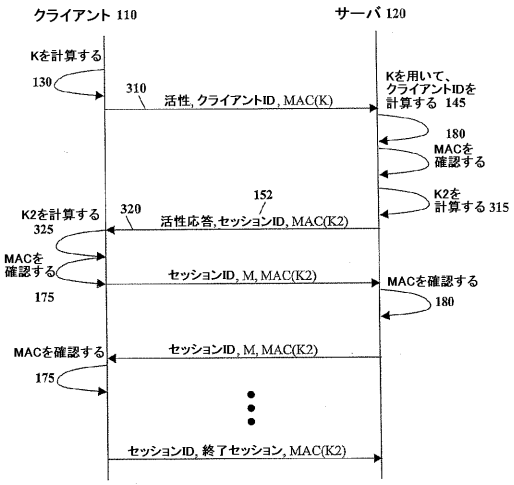

Fig. 3

【図４】

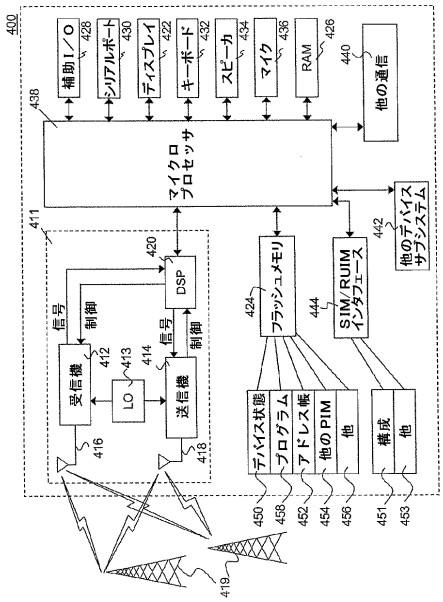

FIG. 4

フロントページの続き

(74)代理人 100113413
弁理士 森下 夏樹
(72)発明者 アレキサンダー シャーキン
カナダ国 エル３エックス ２ジェイ２ オンタリオ, ニューマーケット, ヘドル クレセント ４３０
(72)発明者 マイケル シェンフィールド
カナダ国 エル４シー ３エス９ オンタリオ, リッチモンド ヒル, ストックデール クレセント ３８

Ｆターム(参考) 5B285 AA05 BA01 CA41 CB02 CB35 CB47 CB53 CB76 CB84
5J104 AA07 KA02 KA04 PA07