(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2018-110378
(P2018-110378A)
(43)公開日　平成30年7月12日(2018.7.12)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 9/32	(2006.01)	H04L	9/00	673A	5J104
H04L 9/08	(2006.01)	H04L	9/00	675A	
G06F 21/44	(2013.01)	H04L	9/00	601B	
		G06F	21/44		

審査請求 未請求　請求項の数 14　ＯＬ　外国語出願　（全 17 頁）

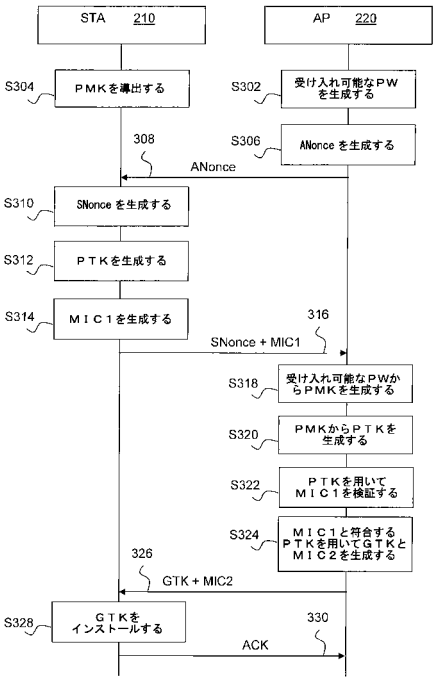
(21)出願番号　特願2017-212587 (P2017-212587)
(22)出願日　平成29年11月2日 (2017.11.2)
(31)優先権主張番号　16306445.4
(32)優先日　平成28年11月4日 (2016.11.4)
(33)優先権主張国　欧州特許庁 (EP)
(31)優先権主張番号　17305661.5
(32)優先日　平成29年6月6日 (2017.6.6)
(33)優先権主張国　欧州特許庁 (EP)

(71)出願人　501263810
トムソン　ライセンシング
Ｔｈｏｍｓｏｎ　Ｌｉｃｅｎｓｉｎｇ
フランス国，　９２１３０　イツシー　レ　ムーリノー，　ル　ジヤンヌ　ダルク，　１－５
１－５，　ｒｕｅ　Ｊｅａｎｎｅ　ｄ’Ａｒｃ，　９２１３０　ＩＳＳＹ　ＬＥＳ　ＭＯＵＬＩＮＥＡＵＸ，　Ｆｒａｎｃｅ
(74)代理人　100107766
弁理士　伊東　忠重
(74)代理人　100070150
弁理士　伊東　忠彦
(74)代理人　100091214
弁理士　大貫　進介

最終頁に続く

(54)【発明の名称】クライアント装置の認証のための装置と方法

(57)【要約】　（修正有）
【課題】無線通信ネットワークにおける共有秘密鍵の入力に関するタイピング誤りの問題を解決する。
【解決手段】アクセス・ポイント２２０が、クライアント２１０から第１のノンスと、クライアント２１０に入力されているか、或いは、クライアント２１０に入力されたパスフレーズから導出されている第２の鍵から導出された第１の鍵を用いて算定された第１のノンスについての第１の暗号ハッシュとを受信し、第２の鍵とパスフレーズとの一方である記憶済みの一次的な入力と導出時に有効な少なくとも１つの記憶済みの二次的な入力との各々から第１の鍵を導出し、各々の導出された第１の鍵を用いて第１の暗号ハッシュを検証して第１の暗号ハッシュと符合する１つの導出された第１の鍵を検出し、第１の暗号ハッシュと符合する１つの導出された第１の鍵を用いて第３の鍵と第２の暗号ハッシュを生成し、第３の鍵と第２の暗号ハッシュをクライアントに送信する。
【選択図】図３



【特許請求の範囲】
【請求項１】
アクセス・ポイントにおけるクライアント認証のための方法であって、アクセス・ポイントにおいて、
受信手段によって、クライアントから第１のノンスと該第１のノンスについての第１の暗号ハッシュとを受信するステップであり、前記第１の暗号ハッシュが第１の鍵を用いて算定されており、該第１の鍵が第２の鍵から導出されており、該第２の鍵が前記クライアントに入力されているか、或いは、前記クライアントに入力されたパスフレーズから導出されている、該受信するステップと、
導出手段によって、記憶済みの一次的な入力と導出時に有効な少なくとも１つの記憶済みの二次的な入力との各々から第１の鍵を導出するステップであり、前記記憶済みの一次的な入力と前記少なくとも１つの記憶済みの二次的な入力が、各々、第２の鍵とパスフレーズとの一方である、該導出するステップと、
検証手段によって、各々の前記導出された第１の鍵を用いて前記第１の暗号ハッシュを検証して、前記第１の暗号ハッシュと符合する１つの前記導出された第１の鍵を検出するステップと、
生成手段によって、前記第１の暗号ハッシュと符合する前記１つの前記導出された第１の鍵を用いて第３の鍵と第２の暗号ハッシュを生成するステップと、
送信手段によって、前記第３の鍵と前記第２の暗号ハッシュを前記クライアントに送信するステップと、
を備えている前記方法。
【請求項２】
各々の前記記憶済みの二次的な入力が、明確に定められた限定された有効期間を有するか、或いは、各々の前記記憶済みの二次的な入力が、少なくとも１つのタイピング誤りを有する前記一次的な入力に対応する、請求項１に記載の方法。
【請求項３】
前記アクセス・ポイントがＷｉＦｉアクセス・ポイントであり、前記方法が前記送信手段によって第２のノンスを前記クライアントに送信するステップを更に備えており、前記第１の鍵が前記第１のノンスと前記第２のノンスとから更に導出される、請求項１に記載の方法。
【請求項４】
前記第３の鍵が、前記第１の暗号ハッシュと符合する前記１つの前記導出された第１の鍵から生成された暗号鍵を用いて暗号化されて、送信される、請求項１に記載の方法。
【請求項５】
記憶済みの二次的な入力が無効になった時に更新手段によって前記第３の鍵を新しくするステップを更に備えている、請求項２に記載の方法。
【請求項６】
アクセス・ポイントであって、
クライアントから第１のノンスと該第１のノンスについての第１の暗号ハッシュとを受信する手段であり、前記第１の暗号ハッシュが第１の鍵を用いて算定されており、該第１の鍵が第２の鍵から導出されており、該第２の鍵が前記クライアントに入力されているか、或いは、前記クライアントに入力されたパスフレーズから導出されている、該受信する手段と、
前記クライアントに第３の鍵と第２の暗号ハッシュを送信する手段と、
一次的な入力と少なくとも１つの二次的な入力とを記憶するように構成されたメモリであり、前記一次的な入力と前記少なくとも１つの二次的な入力が、各々、第２の鍵とパスフレーズとの一方である、該メモリと、
前記記憶された一次的な入力と導出時に有効な前記記憶された少なくとも１つの二次的な入力との各々から第１の鍵を導出する手段と、
各々の前記導出された第１の鍵を用いて前記第１の暗号ハッシュを検証して、前記第１

の暗号ハッシュと符合する１つの前記導出された第１の鍵を検出する手段と、
前記第１の暗号ハッシュと符合する前記１つの前記導出された第１の鍵を用いて前記第３の鍵と前記第２の暗号ハッシュを生成する手段と、
を備えている前記アクセス・ポイント。
【請求項７】
各々の前記記憶された二次的な入力が、明確に定められた限定された有効期間を有するか、或いは、各々の前記記憶された二次的な入力が、少なくとも１つのタイピング誤りを有する前記一次的な入力に対応する、請求項６に記載のアクセス・ポイント。
【請求項８】
前記アクセス・ポイントがＷｉＦｉアクセス・ポイントであり、前記送信する手段が、更に、第２のノンスを前記クライアントに送信するように構成されており、前記アクセス・ポイントが、前記第１の鍵を更に前記第１のノンスと前記第２のノンスとから導出する手段を更に備えている、請求項６に記載のアクセス・ポイント。
【請求項９】
前記第３の鍵を、前記クライアントに送信する前に、前記第１の暗号ハッシュと符合する前記１つの前記導出された第１の鍵から生成された暗号鍵を用いて暗号化する手段を更に備えている、請求項６に記載のアクセス・ポイント。
【請求項１０】
前記導出する手段が、更に、第１の鍵を、記憶された二次的な入力から、該記憶された二次的な入力についての有効期間にのみ、導出するように構成されている、請求項８に記載のアクセス・ポイント。
【請求項１１】
記憶された二次的な入力が無効になった時に前記第３の鍵を新しくする手段を更に備えている、請求項７に記載のアクセス・ポイント。
【請求項１２】
Ｗｉ-Ｆｉ　Ｐｒｏｔｅｃｔｅｄ　Ａｃｃｅｓｓ　２　Ｅｎｔｅｒｐｒｉｓｅの認証装置においてクライアント装置を認証するための方法であって、
送信手段によって、前記クライアント装置にセッション識別子と第１のチャレンジを送信するステップと、
受信手段によって、前記クライアント装置から、ユーザ・ネーム、第２のチャレンジ、及び、前記第１のチャレンジと前記第２のチャレンジと前記セッション識別子とパスフレーズとについての暗号ハッシュ、を受信するステップと、
検証手段によって、有効な記憶済みの一次的なパスフレーズ、或いは、少なくとも１つの有効な記憶済みの二次的なパスフレーズが、前記暗号ハッシュと符合するか否かを検証するステップであり、各々の前記記憶済みの二次的なパスフレーズが、明確に定められた限定された有効期間において有効であるか、或いは、各々の前記記憶済みの二次的な入力が、少なくとも１つのタイピング誤りを有する前記一次的な入力に対応する、該検証するステップと、
あるパスフレーズが前記暗号ハッシュと符合する場合に、
前記送信手段によって、前記クライアント装置に、認証が成功したことを示すメッセージを送信するステップと、
ハンドシェイク実施手段によって、前記クライアント装置と共にハンドシェイクを実施して、鍵を採用するステップと、
を備えている前記方法。
【請求項１３】
Ｗｉ-Ｆｉ　Ｐｒｏｔｅｃｔｅｄ　Ａｃｃｅｓｓ　２　Ｅｎｔｅｒｐｒｉｓｅの認証装置であって、
クライアント装置にセッション識別子と第１のチャレンジを送信する手段と、
前記クライアント装置から、ユーザ・ネーム、第２のチャレンジ、及び、前記第１のチャレンジと前記第２のチャレンジと前記セッション識別子とパスフレーズとについての暗

号ハッシュ、を受信する手段と、
有効な記憶済みの一次的なパスフレーズ、或いは、少なくとも１つの有効な記憶済みの二次的なパスフレーズが、前記暗号ハッシュと符合するか否かを検証する手段であり、各々の前記記憶済みの二次的なパスフレーズが、明確に定められた限定された有効期間において有効であるか、或いは、各々の前記記憶済みの二次的な入力が、少なくとも１つのタイピング誤りを有する前記一次的な入力に対応する、該検証する手段と、
あるパスフレーズが前記暗号ハッシュと符合する場合に、
通信インタフェースを介して、前記クライアント装置に、認証が成功したことを示すメッセージを送信する手段と、
前記クライアント装置と共にハンドシェイクを実施して鍵を採用する手段と、
を備えている前記認証装置。
【請求項１４】
請求項１に記載の方法のステップを実施するための、プロセッサによって実行可能なプログラム・コード命令を備えているコンピュータ・プログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本開示は、概してネットワーク・セキュリティに関し、詳しくはネットワークにおけるクライアント装置の認証（authentication）に関する。
【背景技術】
【０００２】
この節は、読者に種々の技術の態様を紹介することを意図しているが、これらの態様は、後述する、及び／又は、特許請求の範囲の請求項に記載する本開示の種々の態様に関係することもある。この解説は、本開示の種々の態様についてのより良い理解を容易にする背景情報を読者に提供することに役立つと信じる。従って、この解説は、この観点で読まれるべきであり、従来技術についての容認として読まれるべきではないことを理解されたい。
【０００３】
無線通信において、いわゆるアクセス・ポイントへのアクセスを認証済みクライアント装置のみに限定することが望ましい場合が多い。ここでは、最も広く普及している無線ネットワーキング技術であるＷｉＦｉを、非限定的な説明用の例として、用いる。
【０００４】
クライアント装置を認証するための第１の解決手段は証明書（certificates）を使用することであるが、この証明書は複雑なインストールと管理を必要とするので、この解決手段は、多くの場合、適していない。
【０００５】
第２の解決手段は、ユーザがクライアント装置に入力した共有秘密鍵 (shared secret)を用いることであるが、これは、共有秘密鍵をアクセス・ポイントに知らせる必要がある。
【０００６】
第２の解決手段は、例えば、Ｗｉ－Ｆｉ プロテクテッド・アクセス(ＷＰＡ：Ｗｉ-Ｆｉ Ｐｒｏｔｅｃｔｅｄ Ａｃｃｅｓｓ)パーソナル（Ｐｅｒｓｏｎａｌ）（また、ＷＰＡ-ＰＳＫ （Ｐｒｅ-Ｓｈａｒｅｄ Ｋｅｙ)としても知られている）において広く用いられており、そのセカンド・バージョンは、ＷＰＡ２ パーソナル（Ｐｅｒｓｏｎａｌ）と呼ばれており、規格ＩＥＥＥ８０２.１１ｉに記述されており、図１に例示されている。
【０００７】
ステップＳ１０２とＳ１０４において、クライアント装置ＳＴＡとアクセス・ポイントＡＰは、互い独立して、共有パスフレーズと、サービスセットＩＤ(ＳＳＩＤ：Ｓｅｒｖｉｃｅ Ｓｅｔ Ｉｄｅｎｔｉｆｉｅｒ)と呼ばれるネットワーク識別子と、ＳＳＩＤの長さと、を入力として取り入れるＰａｓｓｗｏｒｄ-Ｂａｓｅｄ Ｋｅｙ Ｄｅｒｉｖａ

ｔｉｏｎ Ｆｕｎｃｔｉｏｎ２（ＰＢＫＤＦ２）と呼ばれる鍵導出機能を用いてＰａｉｒｗｉｓｅ Ｍａｓｔｅｒ Ｋｅｙ（ＰＭＫ)を導出する。或いは、その代わりに、ＰＭＫは、一連の６４個の１６進数字として入力できる。

【０００８】

ステップＳ１０６において、ＡＰは、乱数（即ち、ノンス（nonce））ＡＮｏｎｃｅを生成して、これをメッセージ１０８に入れてＳＴＡに送る。

【０００９】

ＳＴＡは、ステップＳ１１０において乱数（即ち、ノンス）ＳＮｏｎｃｅを生成し、ステップＳ１１２においてノンスと、ＰＭＫと、クライアント装置ＳＴＡ及びアクセス・ポイントＡＰのＭｅｄｉａ Ａｃｃｅｓｓ Ｃｏｎｔｒｏｌ（ＭＡＣ：媒体アクセス制御）アドレスと、からＰａｉｒｗｉｓｅ Ｔｒａｎｓｉｅｎｔ Ｋｅｙ（ＰＴＫ)を生成する。次に、ＳＴＡは、ステップＳ１１４において、ＳＮｏｎｃｅについてのＭｅｓｓａｇｅ Ｉｎｔｅｇｒｉｔｙ Ｃｏｄｅ（ＭＩＣ）を生成し、このＭＩＣは、ＳＮｏｎｃｅの鍵付き暗号ハッシュ（ＨＭＡＣ-ＳＨＡ１又はＡＥＳ-ＣＭＡＣ）である。ＭＩＣは、鍵として１２８ビットのＰＴＫを用いる。次に、ＳＴＡは、ＳＮｏｎｃｅとＭＩＣをメッセージ１１６に入れてＡＰに送る。

【００１０】

ＡＰは、ＳＮｏｎｃｅとＭＩＣを受信すると、ステップＳ１１８において、ＳＴＡがステップＳ１１２において行った同じやり方で、ＰＴＫを導出する。ステップＳ１２０において、ＡＰは、ＭＩＣが正しいことを検証する。この時点で、ＳＴＡとＡＰは、認証されて、同じＰＴＫを相互に導出している。

【００１１】

ＡＰは、（ＰＴＫのビット１２８～２５６を用いて暗号化された）第２のＭＩＣを用いて保護されたＧｒｏｕｐ Ｔｅｍｐｏｒａｌ Ｋｅｙ（ＧＴＫ）とシーケンス番号とを含むメッセージ１２２をＳＴＡに送る。ＳＴＡは、メッセージ１２２を受信すると、ステップＳ１２４においてＧＴＫをインストールし、次に、これを用いてパケットをＡＰによって管理される無線ネットワークに送ることができる。最終的に、ＳＴＡは、肯定応答１２６をＡＰに送る。

【００１２】

もう１つの実行可能な解決手段はＷＰＡ-Ｅｎｔｅｒｐｒｉｓｅであり、これは、異なる態様で機能してＥｘｔｅｎｓｉｂｌｅ Ａｕｔｈｅｎｔｉｃａｔｉｏｎ Ｐｒｏｔｏｃｏｌ（ＥＡＰ)を提供する。多数のＥＡＰプロトコルの中で最も一般的なものは、Ｐｒｏｔｅｃｔｅｄ Ｅｘｔｅｎｓｉｂｌｅ Ａｕｔｈｅｎｔｉｃａｔｉｏｎ Ｐｒｏｔｏｃｏｌ（ＰＥＡＰ)、Ｔｒａｎｓｐｏｒｔ Ｌａｙｅｒ Ｓｅｃｕｒｉｔｙ（ＴＬＳ)、及び、Ｔｕｎｎｅｌｌｅｄ Ｔｒａｎｓｐｏｒｔ Ｌａｙｅｒ Ｓｅｃｕｒｉｔｙ（ＴＴＬＳ）である。これらの中で、ＴＬＳがクライアントとサーバの両方において証明書を必要とする一方で、ＴＴＬＳとＰＥＡＰは、共に、証明書がサーバ上に在り且つパスワードがクライアントによって入力される点で、非常に類似している。

【００１３】

一例として、ＰＥＡＰは、Ｍｉｃｒｏｓｏｆｔ's Ｃｈａｌｌｅｎｇｅ Ｈａｎｄｓｈａｋｅ Ａｕｔｈｅｎｔｉｃａｔｉｏｎ Ｐｒｏｔｏｃｏｌ, ｖｅｒｓｉｏｎ ２（ＭＳ-ＣＨＡＰ ｖ２)を用いて、次のようにパスワードを交換する。クライアントと認証装置（ＲＡＤＩＵＳサーバ）は、ＡＰまでのトンネルを設定する。認証装置はセッションＩＤと第１のチャレンジ（challenge）をクライアントに送り、クライアントは、ユーザ・ネーム、第２のチャレンジ、チャレンジのハッシュ、セッションＩＤ、及び、ユーザのパスワードのＭＤ４ハッシュを用いて返答する。ＲＡＤＩＵＳサーバは、ハッシュを検査して、適宜、成功又は失敗について返答し、そして、クライアントを受け入れるようにＡＰに知らせ、これによって、ＡＰは、クライアントと共に４ウェイ・ハンドシェイク（4-way handshake）を開始して、共有鍵を採用する。

【００１４】

共有される秘密鍵とパスワードとについての問題は、特に、ＷｉＦｉによくあることであるが、受容できるレベルのセキュリティを確保するために、入力すべきデータが長い又は複雑である場合に、それらを入力することが、エラー（誤り）に陥りやすい作業になることである。この問題を緩和する試みにおいて、プロテクテッド・セットアップ(ＷＰＳ：Ｗｉ-Ｆｉ　Ｐｒｏｔｅｃｔｅｄ　Ｓｅｔｕｐ)を用いることが提案されている。しかしながら、ｉＯＳ機器のような多くの機器はＷＰＳをサポートしておらず、ＷＰＳの一部の実施はセキュリティの問題に悩まされており、従って、それらの使用が限定されている。

【００１５】

「Ｐａｓｓｗｏｒｄ　Ｔｙｐｏｓ　ａｎｄ　Ｈｏｗ　ｔｏ　Ｃｏｒｒｅｃｔ　Ｔｈｅｍ　Ｓｅｃｕｒｅｌｙ（パスワードのタイプミスとそれらをセキュリティ上安全に補正する方法）」において、Ｃｈａｔｔｅｒｊｅｅ氏その他が、パスワードのタイプミス（即ち、タイピング誤り）に寛容な認証方法を提案している。この論文は、ある形式的な評価を提示しているが、何ら実施形態を提示することなく、即ち、そのような手法を既存の認証プロトコルに組み込む方法を提示することなく、単に理論的な解決手段のみを提案している。

【００１６】

その他のタイプミスに寛容な解決手段が、例えば、欧州特許出願公開第２９４７５９１号明細書（ＥＰ２９４７５９１、特許文献１）、欧州特許出願公開第２８７６５６９号明細書（ＥＰ２８７６５６９、特許文献２）、欧州特許出願公開第３０６７８１１号明細書（ＥＰ３０６７８１１、特許文献３）、米国特許出願公開第２０１５／０３６３５８８号明細書（ＵＳ２０１５／０３６３５８８、特許文献４）及び米国特許出願公開第２０１５／０３６３５９３号明細書（ＵＳ２０１５/０３６３５９３、特許文献５）に記載されているが、これらの全てはクライアント装置の修正を必要とし、また、米国特許９２８０６５７号明細書（ＵＳ９２８０６５７、特許文献６）にも記載されているが、そこでは、サーバが、入力された誤りのパスワードの後に続く正しいパスワードを受け入れるように構成されている。従って、これらの従来の解決手段は、欠点を有する。

【先行技術文献】

【特許文献】

【００１７】

【特許文献１】欧州特許出願公開第２９４７５９１号明細書
【特許文献２】欧州特許出願公開第２８７６５６９号明細書
【特許文献３】欧州特許出願公開第３０６７８１１号明細書
【特許文献４】米国特許出願公開第２０１５／０３６３５８８号明細書
【特許文献５】米国特許出願公開第２０１５／０３６３５９３号明細書
【特許文献６】米国特許９２８０６５７号明細書

【００１８】

ＷｉＦｉのような技術に基づくネットワークにおける共有される秘密鍵とパスワードとについての別の問題は、単一の共有される秘密鍵又はパスワードが用いられることである。例えば、ゲストにネットワークへのアクセス権を与える場合、これは、いずれにせよ、ゲストにネットワーク・パスワードを与えることによって行われる。これは、ゲストが、ネットワーク・パスワードが変更されるまでネットワークにアクセスし続けることができることを意味し、このことは、ネットワーク・パスワードの変更がネットワークにアクセスすべき全ての装置上のパスワードの変更を必要とするので、不都合なことである。

【００１９】

他方、ゲートウェイが、第２のＳＳＩＤを用いてゲストに例えばインターネットへのアクセス権を与えてもよいが、第２のＳＳＩＤが第１のＳＳＩＤとは異なるので、これを用いて第１のＳＳＩＤのネットワークにアクセスすることはできない。

【００２０】

別の一解決手段はワンタイム・パスワードの使用であるが、これらは、一般的に、ユーザが使用しているネットワークと同じネットワークへのアクセス権をゲストに与えない。

【００２１】
無線通信ネットワークにおける共有秘密鍵の入力に関する従来の問題の少なくとも一部を解決する解決手段を得ることが望まれていることが理解されるであろう。
【発明の概要】
【００２２】
第１の態様において、本原理は、アクセス・ポイントにおけるクライアント認証のための方法に向けられている。アクセス・ポイントの少なくとも１つのハードウェア・プロセッサが、クライアントから第１のノンスとこの第１のノンスについての第１の暗号ハッシュとを受信し、この場合、第１の暗号ハッシュは第１の鍵を用いて算定されており、この第１の鍵は第２の鍵から導出されており、この第２の鍵はクライアントに入力されているか、或いは、クライアントに入力されたパスフレーズから導出されている、次に、記憶済みの一次的な入力と導出時に有効な少なくとも１つの記憶済みの二次的な入力との各々から第１の鍵を導出し、この場合、記憶済みの一次的な入力と少なくとも１つの記憶済みの二次的な入力は、各々、第２の鍵とパスフレーズとの一方であり、次に、各々の導出された第１の鍵を用いて第１の暗号ハッシュを検証して第１の暗号ハッシュと符合する１つの導出された第１の鍵を検出し、第１の暗号ハッシュと符合する１つの導出された第１の鍵を用いて第３の鍵と第２の暗号ハッシュを生成し、第３の鍵と第２の暗号ハッシュをクライアントに送信する。
【００２３】
第１の態様の種々の具体的実例には、下記のことが含まれている。
○各々の記憶済みの二次的な入力は、明確に定められた限定された有効期間を有するか、或いは、少なくとも１つのタイピング誤りを有する一次的な入力に対応すること。第３の鍵は、記憶済みの二次的な入力が無効になった時に、新しくすることができること。
○アクセス・ポイントは、ＷｉＦｉアクセス・ポイントであり、第２のノンスもクライアントに送信すること、及び、第１の鍵は、第１のノンスと第２のノンスとから更に導出されること。
○第３の鍵は、第１の暗号ハッシュと符合する１つの導出された第１の鍵から生成された暗号鍵を用いて暗号化されて、送信されること。
【００２４】
第２の態様において、本原理はアクセス・ポイントに向けられており、このアクセス・ポイントは、一方で、クライアントから第１のノンスとこの第１のノンスについての第１の暗号ハッシュとを受信するように構成された通信インタフェースであり、この場合、第１の暗号ハッシュは第１の鍵を用いて算定されており、第１の鍵は第２の鍵から導出されており、第２の鍵はクライアントに入力されているか、或いは、クライアントに入力されたパスフレーズから導出されており、他方で、クライアントに第３の鍵と第２の暗号ハッシュを送信するようにも構成されたこの通信インタフェースと、一次的な入力と少なくとも１つの二次的な入力とを記憶するように構成されたメモリであり、この場合、一次的な入力と少なくとも１つの二次的な入力は、各々、第２の鍵とパスフレーズとの一方である、このメモリと、記憶された一次的な入力と導出時に有効な記憶された少なくとも１つの二次的な入力との各々から第１の鍵を導出し、各々の導出された第１の鍵を用いて第１の暗号ハッシュを検証して第１の暗号ハッシュと符合する１つの導出された第１の鍵を検出し、第１の暗号ハッシュと符合する１つの導出された第１の鍵を用いて第３の鍵と第２の暗号ハッシュを生成するように構成された少なくとも１つのハードウェア・プロセッサと、を備えている。
【００２５】
第２の態様の種々の具体的実例には、下記のことが含まれている。
○各々の記憶済みの二次的な入力は、明確に定められた限定された有効期間を有するか、或いは、少なくとも１つのタイピング誤りを有する一次的な入力に対応すること。第３の鍵は、記憶済みの二次的な入力が無効になった時に、新しくすることができること。
○アクセス・ポイントはＷｉＦｉアクセス・ポイントであり、通信インタフェースは、更

に、第２のノンスをクライアントに送信するように構成されており、少なくとも１つのハードウェア・プロセッサは、更に、第１の鍵を第１のノンスと第２のノンスとから導出するように構成されていること。また、少なくとも１つのハードウェア・プロセッサは、更に、第１の鍵を、記憶された二次的な入力から、この記憶された二次的な入力についての有効期間にのみ、導出するように構成できること。
○少なくとも１つのハードウェア・プロセッサは、更に、第３の鍵を、クライアントに送信する前に、第１の暗号ハッシュと符合する１つの導出された第１の鍵から生成された暗号鍵を用いて暗号化するように構成されていること。
【００２６】
第３の態様において、本原理は、Ｗｉ-Ｆｉ　Ｐｒｏｔｅｃｔｅｄ　Ａｃｃｅｓｓ　２　Ｅｎｔｅｒｐｒｉｓｅの認証装置においてクライアント装置を認証するための方法に向けられており、この認証は、クライアント装置にセッション識別子と第１のチャレンジを送信するステップと、クライアント装置から、ユーザ・ネーム、第２のチャレンジ、及び、第１のチャレンジと第２のチャレンジとセッション識別子とパスフレーズとについての暗号ハッシュ、を受信するステップと、有効な記憶済みの一次的なパスフレーズ、或いは、少なくとも１つの有効な記憶済みの二次的なパスフレーズが、暗号ハッシュと符合するか否かを検証するステップであり、各々の記憶済みの二次的なパスフレーズが、明確に定められた限定された有効期間において有効であるか、或いは、各々の記憶済みの二次的な入力が、少なくとも１つのタイピング誤りを有する一次的な入力に対応する、この検証ステップと、あるパスフレーズが暗号ハッシュと符合する場合に、クライアント装置に、認証が成功したことを示すメッセージを送信するステップと、クライアント装置と共にハンドシェイクを実施して、鍵を採用するステップと、によって行われる。
【００２７】
第４の態様において、本原理は、Ｗｉ-Ｆｉ　Ｐｒｏｔｅｃｔｅｄ　Ａｃｃｅｓｓ　２　Ｅｎｔｅｒｐｒｉｓｅの認証装置に向けられており、この認証装置は、クライアント装置にセッション識別子と第１のチャレンジを送信し、クライアント装置から、ユーザ・ネーム、第２のチャレンジ、及び、第１のチャレンジと第２のチャレンジとセッション識別子とパスフレーズとについての暗号ハッシュ、を受信するように構成された通信インタフェースと、有効な記憶済みの一次的なパスフレーズ、或いは、少なくとも１つの有効な記憶済みの二次的なパスフレーズが暗号ハッシュと符合するか否かを検証し、この場合、各々の記憶済みの二次的なパスフレーズは、明確に定められた限定された有効期間において有効であるか、或いは、各々の記憶済みの二次的な入力は、少なくとも１つのタイピング誤りを有する一次的な入力に対応しており、あるパスフレーズが暗号ハッシュと符合する場合に、通信インタフェースを介して、クライアント装置に、認証が成功したことを示すメッセージを送信し、クライアント装置と共にハンドシェイクを実施して鍵を採用するように構成された少なくとも１つのハードウェア・プロセッサと、を備えている。
【００２８】
第５の態様において、本原理は、コンピュータ・プログラムに向けられており、このコンピュータ・プログラムは、第１の態様の任意の具体的実例による方法のステップを実施するための、プロセッサによって実行可能なプログラム・コード命令を備えている。
【図面の簡単な説明】
【００２９】
次に、下記の添付図面を参照しつつ、本原理の好ましい特徴を、非限定的な例として、説明する。
【図１】従来のＷｉ-Ｆｉ　Ｐｒｏｔｅｃｔｅｄ　Ａｃｃｅｓｓ（ＷＰＡ）　Ｐｅｒｓｏｎａｌのプロトコルを例示する図である。
【図２】本原理の第１の実施態様による代表的なシステムを例示する図である。
【図３】本原理の一実施態様による代表的な装置挿入方法を例示する図である。
【図４】本原理の更なる一実施態様による代表的な装置挿入方法を例示する図である。
【発明を実施するための形態】

【００３０】
図２は、本原理の第１の実施形態による代表的なシステム２００を例示している。システム２００は、クライアント装置（ＳＴＡ）２１０と、ゲートウェイのようなアクセス・ポイント（ＡＰ）２２０とを備えている。アクセス・ポイント２２０は、ローカル・ネットワーク２４０とインターネットのような外部ネットワーク２５０とのインタフェースとなるように構成されており、この外部ネットワークを介して、別のネットワーク（図示せず）内の装置との接続が可能である。この代表的なシステムにおいて、ローカル・ネットワーク２４０は、ＷｉＦｉネットワークである。
【００３１】
クライアント装置２１０とアクセス・ポイント２２０は、それぞれ、少なくとも１つのハードウェア処理部（「プロセッサ」）２１１、２２１と、メモリ２１２、２２２と、他の装置と通信するように構成された、この例ではＷｉＦｉインタフェースである少なくとも１つの通信インタフェース２１３、２２３と、を備えている。当業者であれば、例示された装置が明快さの理由で非常に単純化されており、且つ、実際の装置が内部接続線や電源などのようなものを備えていることが分かるであろう。非一時的記憶媒体２６０には、プロセッサによって実行されると、後述の如くアクセス・ポイント２２０の機能を実施する命令が記憶されている。
【００３２】
クライアント装置２１０は、ローカル・ネットワーク２４０に接続でき、ユーザ・インタフェース２１４を更に備えている。クライアント装置は、例えば、ノートパソコン、スマートフォン又はタブレットであってもよい。
【００３３】
アクセス・ポイント２２０は、ローカル・ネットワーク２４０と外部ネットワーク２５０とのインタフェースとなるような従来のアクセス・ポイントの機能を実施するように構成されている。複数のクライアント装置が、ローカル・ネットワーク２４０に、或いは、ローカル・ネットワーク２４０を介して、接続されてもよく、或いは、アクセス・ポイント２２０としての１つのローカル・ネットワークが、例えば、それぞれ孤立したサブネットの形態を取る複数のローカル・ネットワークを提供してもよい。一般的に、ネットワーク・キーのような共有ネットワーク秘密鍵を知っていることを証明する任意の装置には、ローカル・ネットワーク２４０へのアクセス権が与えられる。
【００３４】
外部ネットワーク２５０を用いて、場合によっては他のアクセス・ポイント（図示せず）を介して、サーバと他の装置とに接続できる。
【００３５】
図３には、本原理の一実施形態による代表的な装置挿入方法が例示されている。
【００３６】
ステップＳ３０２において、アクセス・ポイント（「ＡＰ」）２２０のプロセッサ２２１は、アクセス・ポイント２２０の構成における１つの主要パスフレーズ組から、限定された１組の、誤りが有るが受け入れ可能なパスフレーズを生成し、この１組には主要パスフレーズも含まれている。換言すれば、プロセッサ２２１は、オリジナルの正しいパスフレーズと、少なくとも１つの誤りを含む複数の異形のパスフレーズと、を含む１組のパスフレーズを生成して記憶する。導入される誤りは例えば下記のような共通の誤りに対応することが望ましい（３２文字のパスフレーズについて、オリジナルのパスフレーズを含む異形体の数が括弧内に示されている）。
○任意のランダムな位置の１文字を削除する（３３）
○大文字使用を逆にする（２）
○４文字毎にスペースを付加する（９）
○Ｉ（ｉの大文字）をｌ（Ｌの小文字）に置き換える（２）
○０（ゼロ）をＯに置き換える（２）
○１文字（任意の１つの文字）を４つの最も近いもの（4 closest）のうちの１つに置

き換える（４*３２＋１＝１２９）
○１文字又は２文字（任意の２つの文字）を４つの最も近いもの（4 closest）のうちの１つに置き換える
【数１】

$$\left(\binom{32}{2} * 4 + 32 * 4 + 1 = 2113\right)$$

○これらのうちの任意の組み合わせ（異形体数の積は５０２０４８８）
尚、このような誤りの任意の組み合わせを受け入れても、せいぜい２３ビットのエントロピが取り除かれるだけである。若し文字が、工場で設定されるパスフレーズにおいて一般的である１６進法表記（０～９、Ａ～Ｆ）であれば、オリジナルのエントロピは、３２*４＝１２８ビットである。従って、これら全ての誤りを受け入れても、多数のケースにおいて依然として十分な（少なくとも）１０５ビットのエントロピが残される。
【００３７】
一変形実施形態において、アクセス・ポイント（「ＡＰ」）２２０のプロセッサ２２１は、主要なデフォルトのパスフレーズと少なくとも１つの有効な二次的なパスフレーズとを含む１組の受け入れ可能なパスフレーズを生成する。主要なパスフレーズは、一般的に、ネットワークの正規のユーザによって用いられ、例えば、ネットワークのユーザ又は管理者によって変更されるまで有効なパスフレーズである。二次的なパスフレーズは、例えば、ネットワークにおいてゲストによって用いられ、その有効性は、一般的に、時間的に限定されるが、取り消されるまで同じく有効であり得る。
【００３８】
この一変形実施形態において、プロセッサ２２１は、各々が１日間だけ有効な二次的なパスフレーズを生成するように構成できる。従って、１組の受け入れ可能なパスフレーズには、主要なパスフレーズと当日間だけ有効な二次的なパスフレーズとが含まれる。例えば、毎日、プロセッサは、例えば、反復一方向ハッシングを用いて、当日とそれに続くＮ日とについての二次的なパスフレーズを生成できる。これらの二次的なパスフレーズは、ＡＰのユーザ・インタフェース（図示せず）内に表示でき、或いは、主要なパスフレーズを用いて接続しているユーザの装置に送られて、そのＵＩ２１４上に又は専用アプリケーションを実施している装置上に表示できる。プロセッサ２２１に複数の二次的なパスフレーズを生成させることによって、ゲストに対して、一度に、複数日の期間のアクセス権を与えることができる。
【００３９】
この一変形実施形態の具体的実例において、アクセス・ポイントは、「ゲストＷＰＳボタン」を備えている。このボタンは、その日のパスフレーズが（デフォルトのパスフレーズの代わりに）クライアントに強制されることを除いて、ＷＰＳと同じメカニズムを実施する。
【００４０】
この一変形実施形態のこの具体的実例において、ユーザは、ゲスト装置上のＷｉＦｉ Ｐｒｏｔｅｃｔｅｄ Ｓｅｔｕｐボタンを作動させて、ＡＰ２２０上のＷｉＦｉ Ｐｒｏｔｅｃｔｅｄ Ｓｅｔｕｐボタンを作動させる。それによって、ＡＰとゲスト装置はディフィー・ヘルマン（Ｄｉｆｆｉｅ-Ｈｅｌｌｍａｎ）鍵交換を行い、その後、ＡＰはゲスト装置にその日のパスフレーズを送り、ゲスト装置はネットワークへの接続時にそのパスフレーズを使用し、その後、ＡＰは前述の如く認証を実施する。
【００４１】
図１に示された従来のプロトコルとの顕著な違いとして、アクセス・ポイント２２０は、必ずしも最初にＰＭＫを導出せずに、クライアント装置（「ＳＴＡ」）２１０からＳＮｏｎｃｅ＋ＭＩＣを受信するまで待つことができる。尚、プロトコルは、クライアント装

置２１０については不変である。
【００４２】
ステップＳ３０４において、クライアント装置２１０は、入力パスフレーズと、Ｓｅｒｖｉｃｅ Ｓｅｔ Ｉｄｅｎｔｉｆｉｅｒ (ＳＳＩＤ)と呼ばれるネットワーク識別子と、ＳＳＩＤの長さと、を入力として取り入れる鍵導出機能（この例では、ＰＢＫＤＦ２）を用いてＰａｉｒｗｉｓｅ Ｍａｓｔｅｒ Ｋｅｙ (ＰＭＫ)を導出する。或いは、その代わりに、ＰＭＫは、一連の６４個の１６進数字として入力できる。
【００４３】
ステップＳ３０６において、アクセス・ポイント２２０は、乱数ＡＮｏｎｃｅを生成して、これをメッセージ３０８に入れてクライアント装置２１０に送る。
【００４４】
クライアント装置２１０は、ステップＳ３１０において別の乱数ＳＮｏｎｃｅを生成し、ステップＳ３１２においてノンスと、ＰＭＫと、クライアント装置２１０及びアクセス・ポイント２２０のＭｅｄｉａ Ａｃｃｅｓｓ Ｃｏｎｔｒｏｌ (ＭＡＣ)アドレスと、からＰａｉｒｗｉｓｅ Ｔｒａｎｓｉｅｎｔ Ｋｅｙ (ＰＴＫ)を生成する。次に、クライアント装置２１０は、ステップＳ３１４において、ＳＮｏｎｃｅについてのＭｅｓｓａｇｅ Ｉｎｔｅｇｒｉｔｙ Ｃｏｄｅ (ＭＩＣ) 、即ち、図３におけるＭＩＣ１を生成し、このＭＩＣ１は、ＳＮｏｎｃｅの鍵付き暗号ハッシュ（ＨＭＡＣ-ＳＨＡ１又はＡＥＳ-ＣＭＡＣ）である。ＭＩＣは、鍵として１２８ビットのＰＴＫを用いる。次に、クライアント装置２１０は、ＳＮｏｎｃｅとＭＩＣ１をメッセージ３１６に入れてアクセス・ポイント２２０に送る。
【００４５】
アクセス・ポイント２２０は、ＳＮｏｎｃｅとＭＩＣ１を受信すると、ステップＳ３１８において１組の受け入れ可能なパスフレーズ内の各々のパスフレーズからＰＭＫを導出する。これらの生成されたＰＭＫは、この１組の受け入れ可能なパスフレーズの代わりに、又は、この１組の受け入れ可能なパスフレーズに加えて、記憶できる。或いは、その代わりに、ＰＭＫが一連の６４個の１６進数字として入力されるケースでは、アクセス・ポイント２２０は、正しいＰＭＫから受け入れ可能なＰＭＫを導出して記憶する。尚、このステップは、予め、例えばステップＳ３０２の直後に、実施できる。
【００４６】
ステップＳ３２０において、アクセス・ポイント２２０は、クライアント装置２１０がステップＳ３１２で行った同じ生成方法を用いて、ステップＳ３１８で生成された各々のＰＭＫについてＰＴＫを生成する。
【００４７】
ステップＳ３２２において、アクセス・ポイント２２０は、ＭＩＣ１がステップＳ３２０で生成された何れかのＰＴＫについて正しいことを検証する。若しあるＰＴＫがＭＩＣ１のこの（正しいという）検証を可能にするならば、そのＰＴＫは現行のＰＴＫとして設定される。この時点で、アクセス・ポイント２２０とクライアント装置２１０は、認証されて、（主要な又は二次的なパスフレーズから）同じＰＴＫを相互に導出している。尚、若しＭＩＣのこの（正しいという）検証を可能にするＰＴＫが無ければ、正にあたかも図１に例示された従来の方法において正しくないパスフレーズが入力された如く、クライアント装置２１０は認証されない。
【００４８】
アクセス・ポイント２２０は、ステップＳ３２４において、（ＰＴＫのビット１２８～２５６を用いて暗号化された）第２のＭＩＣ、即ち、図３におけるＭＩＣ２を用いて保護されたＧｒｏｕｐ Ｔｅｍｐｏｒａｌ Ｋｅｙ (ＧＴＫ)とシーケンス番号を生成して、これらをメッセージ３２６に入れてクライアント装置２１０に送る。クライアント装置２１０は、メッセージ３２６を受信すると、ステップＳ３２８においてＧＴＫをインストールし、次に、これを用いてパケットをアクセス・ポイント２２０によって管理される無線ネットワークに送ることができる。最終的に、クライアント装置２１０は、肯定応答３３

０をアクセス・ポイント２２０に送る。
【００４９】
以上のことから理解できるように、アクセス・ポイント２２０は、１組の受け入れ可能なパスフレーズにおいて、受信したＭＩＣ、即ち、ＭＩＣ１が有効となるパスフレーズを検出しようとする。そのようなパスフレーズが検出されると、クライアントを認証することができ、そのパスフレーズは、交換の残り（即ち、ＰＴＫの導出、ＧＴＫの暗号化、及び、メッセージの送信）についての基礎として使用される。
【００５０】
アクセス・ポイントは、（ＭＡＣアドレスによって識別される）所与のクライアント装置が使用するＰＭＫを記憶していることが望ましい。換言すれば、アクセス・ポイントは、ＭＩＣの（正しいという）検証を可能にしたＰＴＫがＰＭＫから生成された際のそのＰＭＫを記憶している。このようにして、クライアント装置が次に接続するときに、アクセス・ポイントは、この記憶しているＰＭＫを取り出すことができ、これによって、再接続の際に、推測されるパスフレーズの数を低減できる。
【００５１】
時間限定されたパスフレーズについての一変形実施形態において、アクセス・ポイント２２０は、もはや有効でない二次的な鍵を取り消すこと、例えば、１日間の鍵を、その有効性を有する日が終わったときに、取り消すことが望ましい。
【００５２】
二次的な鍵の取り消しについての簡単な手法は、二次的な鍵が期限切れになる度に、アクセス・ポイント２２０がＧＴＫを新しくすることである。ＧＴＫは、ＩＥＥＥ ８０２.１１ｉにおいて定義されている、所謂、グループ・キー・ハンドシェイク・メカニズム（Ｇｒｏｕｐ Ｋｅｙ ｈａｎｄｓｈａｋｅ ｍｅｃｈａｎｉｓｍ）を用いて、新しくできる。勿論、その他の適切なメカニズムも用いてもよい。
【００５３】
二次的な鍵の取り消しについての更に入念な手法は、アクセス・ポイント２２０が、二次的な鍵がゲスト装置によって用いられたことがあるか否かを常に把握することである。二次的な鍵が用いられたことがない場合には、その二次的な鍵が期限切れになったときにＧＴＫを新しくする必要はない。ＧＴＫは、期限切れの二次的な鍵がその二次的な鍵の有効期間中に用いられた場合にのみ、例えばグループ・キー・ハンドシェイク・メカニズムによって、新しくされる。
【００５４】
本原理は、パスワードに基づくＷＰＡ２ Ｅｎｔｅｒｐｒｉｓｅ（ＰＥＡＰ／ＥＡＰ-ＴＴＬＳ)のケースにも適用される。ＷｉＦｉに関しては、１組の受け入れ可能なパスワードを試用して、認証が成功であるか否かを判定する。
【００５５】
図４は、本原理の更なる一実施形態による代表的な装置挿入方法を例示している。
【００５６】
図４は、図２におけるクライアント装置と同一であり得るクライアント装置２１０を例示している。この図は、認証装置２３０も示しており、この認証装置２３０には、簡潔さの理由で例示されていないが、少なくとも１つのハードウェア処理装置（「プロセッサ」）と、メモリと、他の装置と通信するように構成された少なくとも１つの通信インタフェースとが含まれている。
【００５７】
ステップＳ４０２において、クライアント装置２１０は、アクセス・ポイント（図２における２２０）を介して、例えばＲＡＤＩＵＳサーバのような認証装置２３０と共に、Ｔｒａｎｓｐｏｒｔ Ｌｅｖｅｌ Ｓｅｃｕｒｉｔｙ（ＴＬＳ）トンネルを設定する。認証装置２３０は、セッションＩＤ （ＳＩｄ)とチャレンジ（ＡＣｈ）とをメッセージ４０４に入れてクライアント装置２１０に送る。クライアント装置２１０は、ステップＳ４０６において、ユーザ・ネーム（Ｕｓｅｒｎａｍｅ）、チャレンジ（ＳＣｈ）、及び、チャレ

ンジ（ＡＣｈ、ＳＣｈ）とセッションＩＤ(ＳＩｄ)とユーザ・パスワードとのＭＤ４ハッシュ、を有するメッセージ４０８を生成する。このメッセージ４０８は、認証装置２３０に送られる。ここまでは、この方法は、従来の方法に対応している。

【００５８】

ステップＳ４１０において、認証装置２３０は、ユーザについての１組の受け入れ可能なユーザ・パスワードにおける何れかのユーザ・パスワードがハッシュＨと符合するか否か、換言すれば、チャレンジ（ＡＣｈ、ＳＣｈ）と、セッションＩＤ（ＳＩｄ）と、１組の受け入れ可能なユーザ・パスワードにおけるユーザ・パスワードとの算定されたＭＤ４ハッシュが、メッセージ４０８において受信されたハッシュＨと同じであるか否か、を検査する。

【００５９】

認証装置２３０は、次に、メッセージ４１２をクライアント装置２１０に送る。もしハッシュＨと符合するパスワードが上述の１組内に無ければ、メッセージ４１２は失敗を示し、クライアント装置２１０は認証されず、この方法は終了する。他方、もしハッシュＨと符合するパスワードが有れば、メッセージ４１２は成功を示し、クライアント装置２１０は認証される。次に、クライアント装置２１０と認証装置は、ステップＳ４１４において、従来の４ウェイ・ハンドシェイクを開始して１つの鍵を採用する。

【００６０】

理解されるであろうが、本原理は、既存のクライアントと共に有効に機能し、実施形態により、アクセス・ポイント又はＲＡＤＩＵＳサーバにおいてのみに修正を必要とするだけである。更に、オリジナルのパスフレーズ又はパスワードが上述の１組の一部分であるので、本方法は、バックワード・コンパチブル（backward compatible）である（後方互換性を有する）。

【００６１】

図に示された要素は、ハードウェア、ソフトウェア又はそれらの組み合わせの種々の形態で実施してもよいことを理解されたい。これらの要素は、１つ又は複数の適切にプログラムされた汎用装置上のハードウェアとソフトウェアとの組み合わせの形態で実施されることが望ましく、その装置には、プロセッサ、メモリ及び入出力インタフェースが含まれ得る。

【００６２】

本説明は、本開示の原理を例示している。従って、当業者であれば、ここに明示的に記載されていない、或いは、示されていないが、本開示の原理を具現化し、その権利範囲内に含まれる種々の構成を考案できることが理解されるであろう。

【００６３】

ここに列挙された全ての例と条件を表す用語とは、技術を推進させるために本発明者によって提供された本開示の原理と概念とを読者が理解するのを手助けする教育的な目的を意図するものであり、本開示の原理と概念は、このような具体的に列挙された例と条件とには限定されないと解釈されるべきである。

【００６４】

更に、本開示の原理、態様及び実施形態、並びに、その具体的な例をここに列挙した全ての記載は、その構造的な等価物及び機能的な等価物の両方を包含するように意図されている。また、そのような等価物は、既知の等価物、及び、将来開発される等価物、即ち、構造に関わらず同じ機能を果たすように開発された任意の要素、を含むことが意図されている。

【００６５】

従って、例えば、ここに提示されたブロック図が、本開示の原理を具現化する例示的な回路の概念的な図を表していることが当業者に理解されるであろう。同様に、任意のフローチャート、流れ図、状態遷移図、擬似コードなどが種々の処理を表しており、それらの種々の処理が、コンピュータ可読媒体において実質的に表されてもよく、従って、コンピュータ又はプロセッサによって実行されてもよく、その際、そのようなコンピュータ又は

プロセッサが明示的に示されているか否かに関わらず、実行されてもよいことが理解されるであろう。

【００６６】

図に示された種々の要素の機能は、適切なソフトウェアと共同してソフトウェアを実行できるハードウェアのみならず、専用ハードウェアを用いて提供されてもよい。それらの機能は、プロセッサによって提供される場合、単一の専用プロセッサによって、或いは、単一の共用プロセッサによって、或いは、一部が共用されてもよい複数の個別のプロセッサによって、提供されてもよい。更に、「プロセッサ」又は「コントローラ」という用語の明示的な使用は、ソフトウェアを実行できるハードウェアを排他的に意味すると解釈されるべきではなく、無制限に、デジタル信号プロセッサ（ＤＳＰ）のハードウェア、ソフトウェアを記憶するリード・オンリ・メモリ（ＲＯＭ）、ランダム・アクセス・メモリ（ＲＡＭ）、及び、不揮発性記憶装置を暗示的に含むことがある。

【００６７】

従来型である、及び／又は、特別仕様であるその他のハードウェアも含まれてもよい。同様に、図に示されたあらゆるスイッチは、単に概念的なものである。それらの機能は、プログラム・ロジックの動作を介して、専用ロジックを介して、プログラム制御と専用ロジックとのインタラクションを介して、或いは、手作業によっても、実施されてもよく、個々の技術は、状況からより具体的に理解される如く、実施者によって選択可能である。

【００６８】

ここに記載された特許請求の範囲の請求項において、規定された機能を実施する手段として表現された任意の素子は、その機能を実施する任意の様式、例えば、ａ)その機能を実施する回路素子の組み合わせ、或いは、ｂ） 任意の形態のソフトウェア、従って、ファームウェア、マイクロコードなどを含むソフトウェアであって、そのソフトウェアを実行してその機能を実施する適切な回路と組み合わされるソフトウェア、を含む任意の様式を包含するように意図されている。このような請求項によって規定される本開示の本質は、列挙された種々の手段によって提供される機能が、請求項によって規定される態様で組み合わされて統合されることに在る。従って、それらの機能を提供し得るあらゆる手段は、ここに示された手段と等価であると認められる。

【図１】

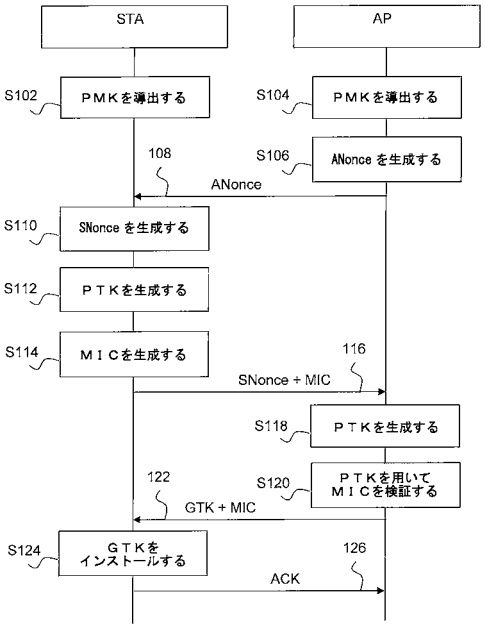
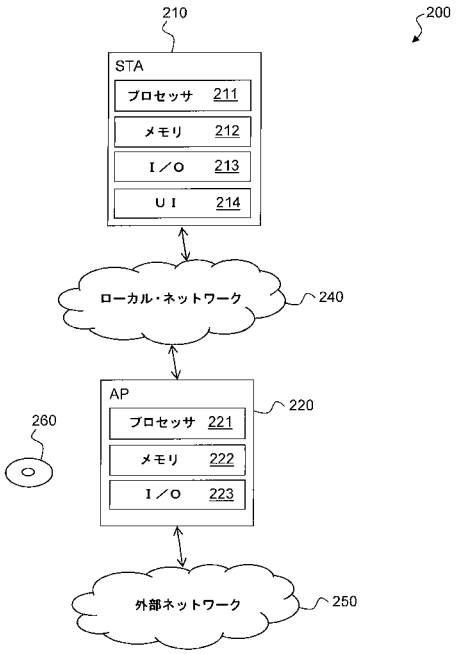
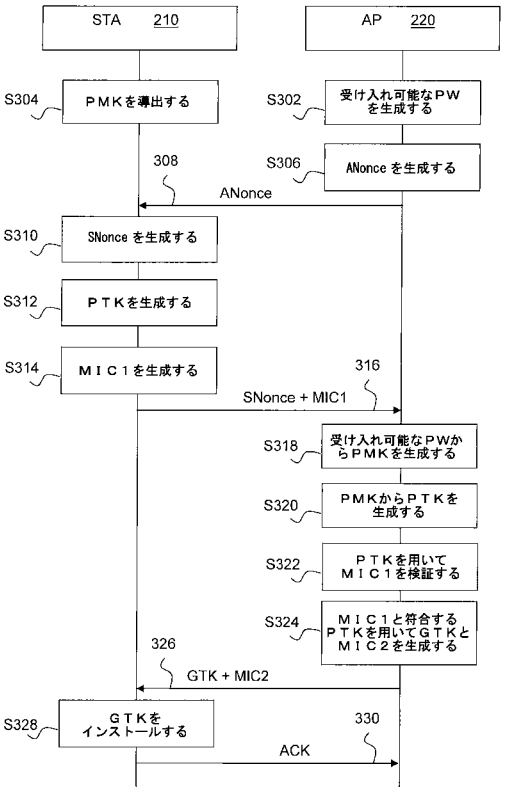


図１（従来技術）

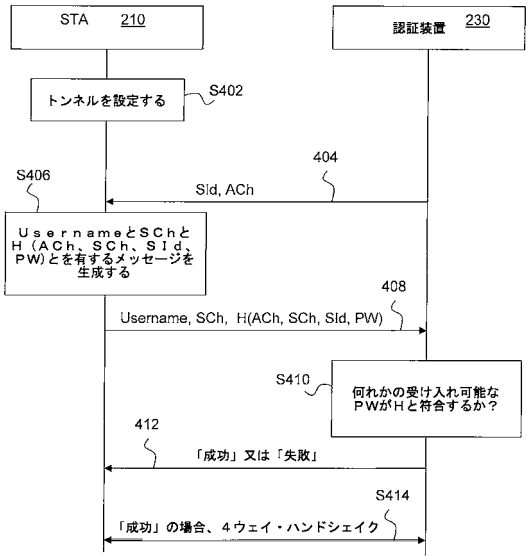
【図２】



【図３】



【図４】



フロントページの続き

(74)代理人 100134094
弁理士 倉持 誠
(74)代理人 100123629
弁理士 吹田 礼子
(72)発明者 ル・スクアネツク, ニコラス
フランス国 エフ－３５５７６ セソン セビニエ セーエス １７６ １６ ゼドアーセー・デ・シヤン・ブラン アベニユー・デ・シヤン・ブラン ９７５ テクニカラー・アール・アンド・デイー フランス
(72)発明者 ノイマン, クリストフ
フランス国 エフ－３５５７６ セソン セビニエ セーエス １７６ １６ ゼドアーセー・デ・シヤン・ブラン アベニユー・デ・シヤン・ブラン ９７５ テクニカラー・アール・アンド・デイー フランス
(72)発明者 ヒーン, オリビエ
フランス国 エフ－３５５７６ セソン セビニエ セーエス １７６ １６ ゼドアーセー・デ・シヤン・ブラン アベニユー・デ・シヤン・ブラン ９７５ テクニカラー・アール・アンド・デイー フランス

Ｆターム(参考) 5J104 AA07 AA08 AA16 EA03 EA16 KA02 KA03 KA06 LA01 NA02
NA05 NA37 NA38 PA01

【外国語明細書】
2018110378000001.pdf