【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第７部門第３区分
【発行日】令和2年12月10日(2020.12.10)

【公開番号】特開2018-110378(P2018-110378A)
【公開日】平成30年7月12日(2018.7.12)
【年通号数】公開・登録公報2018-026
【出願番号】特願2017-212587(P2017-212587)
【国際特許分類】
Ｈ０４Ｌ　9/32　(2006.01)
Ｈ０４Ｌ　9/08　(2006.01)
Ｇ０６Ｆ　21/44　(2013.01)
【ＦＩ】
Ｈ０４Ｌ　9/00　６７３Ａ
Ｈ０４Ｌ　9/00　６７５Ａ
Ｈ０４Ｌ　9/00　６０１Ｂ
Ｇ０６Ｆ　21/44

【手続補正書】
【提出日】令和2年10月27日(2020.10.27)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【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、
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し、前記導出時に有効である、前記方法。
【請求項２】
前記アクセス・ポイントは、ＷｉＦｉアクセス・ポイントであり、
前記方法は、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、
前記第１の鍵は、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３】
前記第３の鍵は、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４】
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、前記第３の鍵は、前記アクセス・ポイントによって管理される無線ネットワークにパケットを送信するのに用いられる、請求項１に記載の方法。
【請求項５】
記憶済みの一次的な入力は、ネットワークにおける通常ユーザによって使用されるパスフレーズであり、記憶済みの二次的な入力は、前記ネットワークにおけるゲストによって使用される、請求項１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、
前記記憶済みの一次的な入力と前記記憶済みの少なくとも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、
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し、前記導出時に有効である、前記アクセス・ポイント。
【請求項７】
前記アクセス・ポイントは、ＷｉＦｉアクセス・ポイントであり、
前記送信する手段は、第２のノンスを前記クライアントに送信するように更に構成されており、
前記アクセス・ポイントは、前記第１の鍵を前記第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８】
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９】
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７に記載のアクセス・ポイント。
【請求項１０】
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、前記第３の鍵は、前記アクセス・ポイントによって管理される無線ネットワークにパ

ケットを送信するのに用いられる、請求項６に記載のアクセス・ポイント。
【請求項１１】
記憶済みの一次的な入力は、ネットワークにおける通常ユーザによって使用されるパスフレーズであり、記憶済みの二次的な入力は、前記ネットワークにおけるゲストによって使用される、請求項６に記載のアクセス・ポイント。
【請求項１２】
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。
【手続補正２】
【補正対象書類名】明細書
【補正対象項目名】００６８
【補正方法】変更
【補正の内容】
【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。
なお、上述の実施形態の一部又は全部は、以下の付記のように記載され得るが、以下には限定されない。
（付記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。
（付記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、付記１に記載の方法。
（付記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、付記１に記載の方法。
（付記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、付記１に記載の方法。
（付記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、付記２に記載の方法。
（付記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。
（付記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、付記６に記載のアクセス・ポイント。
（付記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、付記６に記載のアクセス・ポイント。
（付記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、付記６に記載のアクセス・ポイント。
（付記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、付記８に記載のアクセス・ポイント。
（付記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、付記７に記載のアクセス・ポイント。
（付記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。
（付記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。
（付記１４）
付記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。