

【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】平成24年12月20日 (2012.12.20)

【公表番号】特表2012-507963(P2012-507963A)

【公表日】平成24年3月29日 (2012.3.29)

【年通号数】公開・登録公報2012-013

【出願番号】特願2011-534868(P2011-534868)

【国際特許分類】

H 0 4 W 12/04 (2009.01)

【F I】

H 0 4 Q 7/00 1 8 2

【手続補正書】

【提出日】平成24年11月5日 (2012.11.5)

【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・ポイントとして構成されているデバイスを動作させる方法であって、前記アクセス・ポイントには複数の事前共有鍵が供給されており、

少なくとも 1 つのクライアント・デバイスからの前記アクセス・ポイントへの接続要求を受けるステップであって、前記要求が、鍵を用いて発生した部分を含む、ステップと、

前記部分が、前記アクセス / ポイントに供給された前記複数の事前共有鍵の内 1 つの鍵を用いて発生した情報と一致するか否か判断するステップであって、前記複数の事前共有鍵は、異なる複雑さを有する複数の事前共有鍵を含み、前記複数の事前共有鍵のうち少なくとも 1 つの鍵の複雑さは、前記少なくとも 1 つの鍵の寿命に依存する、ステップと、

前記部分の情報が、前記複数の事前共有鍵からの鍵を用いて発生した情報と一致したと判断した場合、前記接続を許可するステップと、

前記部分の情報が、前記複数の事前共有鍵からの鍵を用いて発生した情報と一致しないと判断した場合、前記接続を許可しないステップと、
を備えている、方法。

【請求項 2】

請求項 1 記載の方法において、前記複数の事前共有鍵が、長期事前共有鍵および短期事前共有鍵の内少なくとも 1 つを含む、方法。

【請求項 3】

請求項 1 記載の方法であって、更に、前記複数の事前共有鍵から選択した事前共有鍵を除去する要求に応答して、

前記選択した事前共有鍵を前記複数の事前共有鍵から除去するステップと、

前記少なくとも 1 つのクライアント・デバイスが前記選択した事前共有鍵を用いているか否か判断するステップと、

前記少なくとも 1 つのクライアント・デバイスが前記選択した事前共有鍵を用いていると判断した場合、前記少なくとも 1 つのクライアント・デバイスを切断するステップと、
を備えている、方法。

【請求項 4】

請求項 3 記載の方法において、前記選択した事前共有鍵を除去する要求が、ユーザーによってユーザー・インターフェースを通じて行われる、方法。

【請求項 5】

請求項 3 記載の方法において、

前記複数の事前共有鍵の鍵には、存続時間値が関連付けられており、

前記選択した事前共有鍵を除去する要求が、前記選択した事前共有鍵の存続時間が満了したという判断に応答して発生される、方法。

【請求項 6】

請求項 1 記載の方法において、前記要求を受けるステップが、W P A または W P A 2 プロトコルにしたがって前記要求を受けるステップを含む、方法。

【請求項 7】

請求項 6 記載の方法であって、更に、

前記接続が許可された場合、前記 W P A または W P A 2 プロトコル にしたがって、別のメッセージを送るステップを備えている、方法。

【請求項 8】

請求項 1 記載の方法であって、更に、前記少なくとも 1 つのクライアント・デバイスが、前記アクセス・ポイントに接続されている複数のクライアント・デバイスを含む場合、前記複数のクライアントの内前記少なくとも 1 つと関連付けられている前記事前共有鍵を除去するステップと、

前記複数のクライアント・デバイスの内他のものへの接続を分断せずに、前記複数のクライアントの内前記少なくとも 1 つへの接続を選択的に遮断するステップと、
を備えている、方法。

【請求項 9】

請求項 8 記載の方法において、前記事前共有鍵を除去するステップが、事前共有鍵の寿命が満了したときおよび / または前記少なくとも 1 つのクライアント・デバイスによって用いられている前記事前共有鍵が前記複数の事前共有鍵から除去されたときに、前記事前共有鍵を除去するステップを含む、方法。

【請求項 10】

請求項 1 記載の方法であって、更に、前記事前共有鍵が、前記複数の事前共有鍵からの鍵と一致したと判断した場合、前記少なくとも 1 つのクライアント・デバイスにグループ鍵を発生するステップを備えている、方法。

【請求項 11】

アクセス・ポイントとして構成されている装置であって、

クライアント・デバイスに事前共有鍵を供給する際のユーザー許容度に基づいて選択される異なる複雑さを有する複数の事前共有鍵を、ユーザー入力に応答して受け取るように構成されたインターフェースであって、前記複数の事前共有鍵は、ユーザーフレンドリーなフォーマットの少なくとも 1 つの事前共有鍵を含み、前記ユーザーフレンドリーなフォーマットは、ユーザーによる少なくとも 1 つの事前共有鍵の入力を容易にする、インターフェースと、

前記複数の事前共有鍵を格納するように構成されているコンピューター・メモリーと、
少なくとも 1 つのクライアント・デバイスからの、前記アクセス・ポイントへの接続要求を受けるように構成されているインターフェースであって、前記要求が、鍵を用いて発生した情報を含む、インターフェースと、

制御ロジックと、

を備えており、前記制御ロジックが、

前記鍵を用いて発生した情報が、前記複数の事前共有鍵からの 1 つの鍵を用いて発生した情報と一致するか否か判断し、

前記鍵を用いて発生した情報が、前記複数の事前共有鍵からの 1 つの鍵を用いて発生した情報と一致すると判断した場合、前記接続を許可し、

前記鍵を用いて発生した情報が、前記複数の事前共有鍵からの 1 つの鍵を用いて発生した情報と一致しないと判断した場合、前記接続を許可しない、
ように構成されている、装置。

【請求項 1 2】

請求項 1 1 記載の装置において、前記コンピューター・メモリーが、更に、
前記アクセス・ポイントに接続されているクライアント・デバイスに関する情報を格納するように構成されている複数のデータ構造を備えており、前記複数のデータ構造の内各データ構造が、クライアント・デバイスの識別子、および前記クライアント・デバイスによって用いられる事前共有鍵を格納する、装置。

【請求項 1 3】

請求項 1 1 記載の装置において、
前記鍵を用いて発生した情報が、前記要求を構成するメッセージの署名を含み、
前記鍵を用いて発生した情報が、前記複数の事前共有鍵からの 1 つの鍵を用いて発生した情報と一致するか否か判断する際に、前記複数の事前共有鍵からの鍵を用いて発生した情報を用いて、前記メッセージの署名を計算する、装置。

【請求項 1 4】

請求項 1 1 記載の装置において、前記制御ロジックが、前記複数の事前共有鍵から選択した事前共有鍵を除去する要求に応答して、
前記選択した鍵を、前記複数の事前共有鍵から除去し、
前記少なくとも 1 つのクライアント・デバイスが前記選択した事前共有鍵を用いているか否か判断し、
前記少なくとも 1 つのクライアント・デバイスが前記選択した事前共有鍵を用いていると判断した場合、前記少なくとも 1 つのクライアント・デバイスの切断を命令する、ように構成されている、装置。

【請求項 1 5】

請求項 1 1 記載の装置において、前記アクセス・ポイントが、Wi-Fi 対応デバイスを備えており、前記少なくとも 1 つのクライアント/デバイスが、Wi-Fi 対応クライアント・デバイスを備えている、装置。