(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5506810号
(P5506810)
(45)発行日　平成26年5月28日(2014.5.28)　(24)登録日　平成26年3月28日(2014.3.28)

(51)Int.Cl.　F I
H04W 12/04 (2009.01)　H04W 12/04

請求項の数 15　(全 24 頁)

(21)出願番号	特願2011-534868 (P2011-534868)
(86)(22)出願日	平成21年11月3日 (2009.11.3)
(65)公表番号	特表2012-507963 (P2012-507963A)
(43)公表日	平成24年3月29日 (2012.3.29)
(86)国際出願番号	PCT/US2009/063044
(87)国際公開番号	WO2010/053889
(87)国際公開日	平成22年5月14日 (2010.5.14)
審査請求日	平成24年11月5日 (2012.11.5)
(31)優先権主張番号	61/111,240
(32)優先日	平成20年11月4日 (2008.11.4)
(33)優先権主張国	米国 (US)
(31)優先権主張番号	12/359,987
(32)優先日	平成21年1月26日 (2009.1.26)
(33)優先権主張国	米国 (US)

(73)特許権者　500046438
マイクロソフト　コーポレーション
アメリカ合衆国　ワシントン州　９８０５２－６３９９　レッドモンド　ワン　マイクロソフト　ウェイ
(74)代理人　100140109
弁理士　小野　新次郎
(74)代理人　100075270
弁理士　小林　泰
(74)代理人　100080137
弁理士　千葉　昭男
(74)代理人　100096013
弁理士　富田　博行
(74)代理人　100153028
弁理士　上田　忠

最終頁に続く

(54)【発明の名称】アクセス・ポイントにおける多数の事前共有キーのサポート

(57)【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、
前記複数の事前挙有鍵の鍵には、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、ＷＰＡまたはＷＰＡ２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ＷＰＡまたはＷＰＡ２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１２】
請求項１１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１３】
請求項１１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１４】
請求項１１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１５】
請求項１１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。
【発明の詳細な説明】
【背景技術】
【０００１】
[0001] 今日では、種々のコンピューター・デバイスがワイヤレスで通信することができる。例えば、パーソナル・コンピューター、パーソナル・デジタル・アシスタント、セルラー・フォン、プリンター、スキャナー、およびその他というような移動体コンピューティングデバイスは、ワイヤレス・ネットワーキングに対するＩＥＥＥ８０２．１１規格を用いるワイヤレス・ローカル・エリア・ネットワーク（ＷＬＡＮ）を通じて通信することができる。ワイヤレス・ネットワークにアクセスするためには、コンピューター・デバイス、またはその他のクライアント・デバイスは、ワイヤレスで、アクセス・ポイント（ＡＰ）として構成されているデバイスと「連携」すればよく、次いで、アクセス・ポイントが、クライアント・デバイスに、システムまたはネットワーク・リソースへのアクセスを与える。ＡＰは、特別にネットワーク・アクセスを与えるように構成された専用デバイスとして実現することができ、あるいは他の機能を実行するコンピューターをプログラミングすることによって実現することもできる。コンピューターをプログラミングすること

によって実現する場合、アクセス・ポイントを「ソフトＡＰ」と呼ぶこともできる。ソフトＡＰがアクセスを与えることができるリソースは、例えば、「ハードＡＰ」と同様、ネットワークに接続されている他のデバイスを含むことができ、場合によって、ソフトＡＰとしての機能を果たすコンピューター内にあるアプリケーションまたはその他のエレメントを含むこともできる。

【０００２】

[0002] 安全な通信を可能にするために、クライアント・デバイスおよびＡＰは互いに秘密データを交換することによって、相互認証する。交換が成功すると、ＡＰは、クライアント・デバイスがネットワークに接続することを許可する。秘密情報は、事前共有鍵(pre-shared key)であってもよい。事前共有鍵を用いる場合、ＡＰおよび連携するワイヤレス・クライアント・デバイスには、認証に用いられる同一の事前共有鍵が与えられる。

【０００３】

[0003] 例えば、ＷＰＡおよびＷＰＡ２認証および鍵交換プロトコルによれば、ネットワークにアクセスしようとするとき、クライアント・デバイスは、その事前共有鍵で発生した情報を、ＡＰに提供する。ＡＰが、その事前共有鍵のコピーを用いてその情報を検証することができると、クライアントは認証されたことになる。事前共有鍵は、データの暗号化および解読のため、ならびに他の目的のために一時セッション鍵を得るためにも用いることができる。

【０００４】

[0004] 従来では、事前共有鍵が用いられる場合、ＡＰはクライアント・デバイスと連携するために、１つの事前共有鍵を用いる。つまり、同じＡＰと連携するクライアント・デバイスは全て、同じ事前共有鍵を共有することになる。

【発明の概要】

【発明が解決しようとする課題】

【０００５】

[0005] 本発明者は、ワイヤレス・ネットワークの役割が変化する可能性があること、そしてアクセス・ポイントが多数の共有鍵をサポートし、ネットワーク・アクセスまたはシステム・アクセスをしようとしているデバイス毎に自動的にしかるべき事前共有鍵を特定することができることによって、ユーザーの期待に一層よく応える運用を提供できることを認識し理解している。

【課題を解決するための手段】

【０００６】

[0006] 多数の異なるタイプのデバイスから接続要求を受けるアクセス・ポイントにおいて、クライアント・デバイスは、事前共有鍵（ＰＳＫ）に関して異なる要件を有し、更にデバイスに複雑な鍵をプロビジョニングするに際して異なるユーザー許容度(user tolerance)を有することがある。つまり、アクセス・ポイントにおける多数の事前共有鍵は、その寿命や複雑さが異なる場合がある。具体的な一例として、プリンターおよびその他の据置型クライアント・デバイスは、ＡＰとの長期接続を維持することができる。これらのデバイスには極希にしか事前共有鍵がプロビジョニングされないと考えられるので、ユーザーに多大な負担をかけることなく、セキュリティを維持するために複雑な鍵を用いることができる。対照的に、パーソナル・デジタル・アシスタントおよびその他の移動体デバイスは、ＡＰとの短期接続しか必要としないこともあり、この接続は、ユーザーが移動体デバイスにタイプ入力した鍵を用いて開始するのであってもよい。このような接続には、余り複雑でない鍵を用いるとよい。何故なら、短い接続の間この鍵が用いられても、ネットワークのセキュリティを脅かす危険性は殆どないからである。用いる鍵が複雑でない程、デバイスにプロビジョニングする際のユーザーの負担は軽減される。

【０００７】

[0007] 異なる期間の鍵をサポートするために、本発明の一部の実施形態によるアクセス・ポイントは、他のＰＳＫを用いているかもしれない他のクライアント・デバイスを切断することなく、一部のＰＳＫを除去するように構成することができる。このように、短

期ＰＳＫは、ＡＰとの長期接続を有するデバイスを混乱させることなく、短期ＰＳＫを除去することができる。

【０００８】

[0008] ＡＰと連携するクライアント・デバイスとの間における通信を促進するために、本発明の実施形態では、多数の事前共有鍵（ＰＳＫ）をサポートするようにＡＰを構成するステップを備えている。ＡＰと連携されている各クライアント・デバイスには、これら多数のＰＳＫの内１つをプロビジョニングすることができる。このように、本発明の一部の実施形態によれば、１つよりも多いクライアント・デバイスが１つのＰＳＫを共有することができつつ、ＡＰはなおも１つよりも多いＰＳＫを所与の時点においてサポートして、その連携するクライアント・デバイスを認証する。クライアント・デバイスがＡＰを通じてネットワークにアクセスしようとすると、ＡＰは、多数のＰＳＫの内どのＰＳＫを用いてこのクライアント・デバイスを認証すべきか決定する。ＡＰおよびクライアント・デバイスは、これらのＰＳＫをＷＬＡＮ上の通信に用いることができる。ＷＬＡＮは、例えば、ＩＥＥＥ８０２．１１規格を用いるＷｉ－Ｆｉ（登録商標）技術である。

【０００９】

[0009] 本発明の一部の実施形態では、１つのＡＰと連携されているクライアント・デバイスをグループに纏めることができ、同じグループに属するデバイスがＰＳＫを共有する。１つのグループを形成するクライアント・デバイスによって用いられるＰＳＫを除去すると、このグループに属するデバイスによるネットワークへのアクセスが終了するが、異なるＰＳＫを用いる他のグループに属するクライアント・デバイスによるネットワーク・アクセスは影響を受けない。

【００１０】

[0010] ＡＰに多数のＰＳＫをプロビジョニングすることによって、異なるタイプのＰＳＫをサポートするようにＡＰを構成することが可能になる。例えば、異なる寿命および複雑さのＰＳＫを、ＡＰによって所与の時点において用いることもできる。ＰＳＫの中には、短くて人間のユーザーによる入力に適したものもある。ＰＳＫの中には、頻繁に変化するものもあり、一過性のネットワーク・アクセスをサポートすることができるものもある。他のＰＳＫは、長期接続に対してセキュリティを強化するために、長くすることができる。

【００１１】

[0011] 以上の説明は、非限定的な本発明の摘要である。本発明は、添付した特許請求の範囲によって定義されるものとする。

【図面の簡単な説明】

【００１２】

[0012] 添付図面は、同じ倍率で描かれることを意図していない。図面において、同じコンポーネントまたはほぼ同じコンポーネントが種々の図において示される場合、これを同様の参照番号で表すこととする。明確化の目的上、各図においてあらゆるコンポーネントに番号が付されていない場合もある。

【図１】図１は、本発明の一部の実施形態を実現することができるコンピューティング環境の概略図である。

【図２】図２は、本発明の一部の実施形態によるアクセス・ポイントとして構成されたデバイス内におけるコンポーネントのブロック図である。

【図３】図３は、本発明の一部の実施形態にしたがって、アクセス・ポイントを動作させるプロセスのフローチャートである。

【図４】図４は、本発明の一部の実施形態にしたがって、アクセス・ポイントにプロビジョニングされた事前共有鍵を除去するプロセスのフローチャートである。

【図５Ａ】図５Ａは、本発明の一部の実施形態にしたがってアクセス・ポイントに事前共有鍵をプロビジョニングするプロセスの間に用いられるユーザー・インターフェースの概略図である。

【図５Ｂ】図５Ｂは、本発明の一部の実施形態にしたがってアクセス・ポイントに事前共

有鍵をプロビジョニングするプロセスの間に用いられるユーザー・インターフェースの概略図である。
【図５Ｃ】図５Ｃは、本発明の一部の実施形態にしたがってアクセス・ポイントに事前共有鍵をプロビジョニングするプロセスの間に用いられるユーザー・インターフェースの概略図である。
【図６】図６は、本発明の一部の実施形態による、Wi-Fi Protected Access 2（ＷＰＡ２）プロトコルを用いた、アクセス・ポイントとクライアント・デバイスとの間における鍵交換プロセスを示す概略図である。
【図７】図７は、本発明の一部の実施形態による、Wi-Fi保護アクセス（ＷＰＡ：Wi-Fi Protected Access）プロトコルを用いた、アクセス・ポイントとクライアント・デバイスとの間における鍵交換プロセスを示す概略図である。
【発明を実施するための形態】
【００１３】
[0020] ワイヤレス通信では、アクセス・ポイント（ＡＰ）として構成されたデバイスと、クライアント・デバイスとが相互に、ある種の秘密情報を用いて、互いに認証する。この情報は、事前共有鍵（ＰＳＫ）を含むことができる。
【００１４】
[0021] クライアント・デバイスが、ＰＳＫに関して異なる要件を有し、更にデバイスに複雑な鍵をプロビジョニングするに際して異なるユーザー許容度を有する可能性があることを本発明者らは認識し理解している。つまり、クライアント・デバイスのユーザーが異なるタイプのＰＳＫをＡＰアクセスのために用いることを可能にすることによって、ユーザー体験を向上させることができる。例えば、異なる鍵毎に、ＡＰへの所与の接続に適した寿命および複雑さを有することができる。例えば、ＰＳＫが、一時的に用いられ、ユーザーに親しみやすい短期鍵であり、クライアント・デバイスのユーザーによって容易にタイプ入力できるものであることもある。短期鍵は、例えば、短期間だけＡＰを通じてインターネットにアクセスすることが許可されたラップトップまたはＰＤＡユーザーが用いるとよい。余り複雑でない鍵を用いることによって、ＡＰアクセスのためにクライアントにプロビジョニングする際のユーザー負担は軽減され、鍵は短期間の後期限切れになるので、セキュリティ上の懸念も低い。別の例として、ＰＳＫは、もっと複雑で長い寿命を有する長期鍵であってもよい。例えば、据置型のプリンターまたはスキャナーは、ＡＰと長期間の通信を維持することもあり、したがって、ユーザーが入力するのが一層困難になることもあり得る長期鍵を利用するとよい。
【００１５】
[0022] 更に、本発明者らは、多数の事前共有鍵（ＰＳＫ）をサポートするようにＡＰを構成することによって、ＡＰの動作、およびＡＰと連携するクライアント・デバイスとの間の通信を容易にすることができることも認識し理解している。ＡＰに多数のＰＳＫをプロビジョニングすることによって、連携するクライアント・デバイスをＡＰから選択的に切断することが可能になる。つまり、ＡＰがサポートする複数のＰＳＫから１つのＰＳＫを除去し、そのＰＳＫを用いてＡＰと認証したクライアント・デバイスを切断しても、ＡＰにアクセスするために異なるＰＳＫを用いている残りのクライアント・デバイスは切断されない。
【００１６】
[0023] 更に、２つ以上のデバイスがグループを形成し、このグループ内ではデバイスがＰＳＫを共有するとき、このＰＳＫを除去すると、このグループの中にあるデバイスによるネットワークへのアクセスは終了するが、異なるＰＳＫを用いている他のグループ（１つまたは複数）の中にあるクライアント・デバイスによるネットワーク・アクセスには影響を及ぼさない。
【００１７】
[0024] 異なる寿命の鍵をサポートするために、本発明の一部の実施形態によるＡＰは、このＡＰと長期接続を有するかもしれない他のクライアント・デバイスを切断すること

なく、一部のＰＳＫを除去するように構成することができる。つまり、あるＰＳＫの寿命が満了したときに、このＰＳＫをＡＰから選択的に除去する。

【００１８】

[0025] 本発明の一部の実施形態は、ＡＰとして構成されているデバイスを動作させる方法を提供する。このＡＰには多数のＰＳＫがプロビジョニングされている。クライアント・デバイスがＡＰに接続しようとすると、ＡＰは、このクライアント・デバイスから接続要求を受ける。この要求は、クライアント・デバイス上に格納されている鍵に基づいて暗号化、署名、またはそれ以外の処理がなされている情報を含むことができる。ＡＰは、このクライアント・デバイスがこの情報を発生するために有効な事前格納鍵にアクセスできるか否か判断し、アクセスできる場合、多数のサポートされているＰＳＫの内どのＰＳＫが用いられたのか判断することができる。この判断を行うために、ＡＰは、接続要求の一部としてクライアント・デバイスから受け取った情報を、ＡＰにプロビジョニングされている多数のＰＳＫからのＰＫＳに基づいて発生した同様の情報と比較することができる。

【００１９】

[0026] ＡＰには、適した方法であればいずれを用いてでも、複数のＰＳＫをプロビジョニングすることができる。例えば、各ＰＳＫを格納するために、ＡＰはプログラミング・インターフェースを通じてコールを受けることができる。これは、アプリケーション・プログラムによって、またはユーザー・インターフェースによって、ユーザー入力に応答して、または他のいずれかの適した方法でコールすることができる。

【００２０】

[0027] 本発明の一部の実施形態によれば、ＡＰは、このＡＰに格納されている多数のＰＳＫから、選択したＰＳＫを除去する。ＡＰは、ＡＰＩへのコール、ユーザー・インターフェースを通じたユーザー入力、ＰＳＫの寿命満了、およびその他のイベントの結果、ＰＳＫを除去することができる。ＰＳＫを除去する際、ＡＰは、ＡＰに接続されているいずれかのクライアント・デバイスが、接続を形成するために、この選択したＰＳＫを用いていたか否か判断することができる。このようなデバイスが発見されると、ＡＰは、異なるＰＳＫを用いてＡＰと認証したクライアント・デバイスを切断せずに、これらを切断することができる。ＡＰは、１つ又は複数のＡＰＩをサポートすることができ、これらのＡＰＩを通じて、ＡＰは鍵を除去することを要求することができる。このような要求は、ユーザー入力に応答してユーザー・インターフェースを通じて、または適した方法であれば他のいずれによってでも、アプリケーション・プログラムによって発生することができる。

【００２１】

[0028] 更に、ＰＫＳの除去は、ＡＰ自体の中にある制御エレメントによって誘起することもできる。例えば、あるＰＳＫの寿命が満了したときに、ＡＰに格納されている多数のＰＳＫから、このＰＳＫを選択して除去することができる。ＡＰに接続されているいずれかのクライアント・デバイスが、この選択されたＰＳＫを用いている場合、ＡＰは、ＡＰと認証するために異なるＰＳＫを用いたクライアント・デバイスを切断せずに、これらのクライアント・デバイスを切断することができる。

【００２２】

[0029] 図１は、多数のコンピューティングデバイスが、アクセス・ポイントとして構成されているデバイス１０２と、ワイヤレス・ネットワーク１０４を用いて通信する、ネットワーク状コンピューティング環境１００を示す。ネットワーク１０４は、例えば、ワイヤレス・ローカル・エリア・ネットワーク（ＷＬＡＮ）とすることができる。デバイス１０２は、例えば、「ソフトＡＰ」として構成されているコンピューターとすることができる。しかしながら、ＡＰは、ハードウェアＡＰであってもよく、またはクライアント・デバイスがワイヤレス・プロトコルにしたがってリソースにアクセスすることを許可するプロトコルを実行するように構成されているその他のワイヤレス・デバイスであってもよい。例えば、ＡＰは、ＩＥＥＥ８０２．１１規格によってサポートされているＷｉ－Ｆｉ

（登録商標）技術を用いて動作することができる。

【００２３】

[0030] 図示した例では、４つのクライアント・デバイス、スキャナー１０６、プリンター１０８、ラップトップ１１０、およびＰＤＡ１１２が、図示のように、アクセス・ポイント１０２とワイヤレスで通信する。これらのデバイスは、移動式、据置型でもよく、移動動作モードおよび据置動作モード双方を実現することもできる。４つのコンピューティングデバイスを示したが、いずれの数またはタイプのコンピューティングデバイスでも、本発明の実施形態によるアクセス・ポイントと通信することができ、４つのデバイスは簡略化のために示したに過ぎない。

【００２４】

[0031] ここでは、ＡＰは、多数のＰＳＫをサポートするように構成されている。クライアント・デバイス１０６、１０８、１１０、および１１２は、ＡＰ１０２と連携されており、各々１つのＰＳＫを格納する。つまり、この例では、デバイス１０６、１０８、１１０、および１１２の各々は、それぞれのＰＳＫを含む。これらのＰＳＫは、ブロック１０７、１０９、１１１、および１１３にそれぞれ模式的に示されている。例えば、スキャナー１０６およびプリンター１０８は、双方共、鍵１を含み、ラップトップ１１０は鍵２を含み、ＰＤＡ１１２は鍵３を含む。このように、スキャナー１０６およびプリンター１０８は鍵１と呼ばれるＰＳＫを共有するが、ラップトップ１１０およびＰＤＡ１１２は異なるＰＳＫを含む。これは、ＡＰ１０２が所与の時点においてその連携するクライアント・デバイスを認証するために、１つよりも多いＰＳＫをサポートすることを例示する。

【００２５】

[0032] ＡＰと連携するクライアント・デバイスをグループに纏めることができ、同じグループに属するデバイスは１つの鍵を共有する。図１は、スキャナー１０６およびプリンター１０８が同じＰＳＫを有することを示す。つまり、これらのデバイスはグループを形成することができる。一部の実施形態によれば、１つのグループを形成するクライアント・デバイスによって用いられているＰＳＫを除去すると、そのグループの中にあるデバイスによるネットワーク・アクセスは終了するが、異なるＰＳＫを用いている他のグループの中にあるクライアント・デバイスによるネットワーク・アクセスには影響を及ぼさない。

【００２６】

[0033] ＡＰと連携するクライアント・デバイスは、ＰＳＫに関して異なる要件を有することや、クライアント・デバイスに複雑な鍵をプロビジョニングする際には異なるユーザー許容度を有することもある。つまり、ＡＰにおける多数のＰＳＫは、異なる寿命や複雑さを有することもある。例えば、図１に示すスキャナー１０６およびプリンター１０８は、据置型デバイスであり、ＡＰ１０２と長期の接続を維持する可能性がある。これらのデバイスには希にＰＳＫがプロビジョニングされるだけに過ぎないと考えられるので、複雑な鍵、または「強い」鍵を用いて、ユーザーに負担をかけずに、セキュリティを維持することができる。対照的に、ラップトップ１１０およびＰＤＡ１１２のような移動体デバイスは、ＡＰ１０２に対して短期の接続しか必要としない場合もあり、この接続は、ユーザーが鍵を移動体デバイスにタイプ入力することによって開始されることもある。このような短期接続では、余り複雑でなく、ユーザーにとって使いやすい鍵、即ち、「容易な」鍵を用いるとよい。何故なら、不正者がこの鍵を識別したり、あるいは不正な目的にそれを用いることができるようになる前に、この短期鍵を除去できれば、ネットワーク・セキュリティを損なう危険性は低いからである。しかも、余り複雑でない鍵を用いることによって、デバイスにプロビジョニングする際のユーザーの負担は軽減する。これは、移動体デバイスがネットワークに接続する度にＰＳＫを思い出して手作業で入力しなければならないこともあるユーザーにとっては、便利であると考えられる。

【００２７】

[0034] このように、鍵１、２、および３の各々は、異なるタイプであってもよい。タイプは、鍵の寿命の期間、鍵の複雑さ、またはその他の特性を反映することができる。例

えば、鍵１、２、および３は、各々、異なる「存続時間」（ＴＴＬ：time-to-live）特性を有することができる。しかしながら、ＴＴＬは鍵の寿命を追跡する手法の一例に過ぎず、寿命は他の適した方法であればいずれによってでも定義できることは、認められてしかるべきである。

【００２８】

[0035] 本発明の一部の実施形態によれば、クライアント・デバイスがＡＰを通じてネットワークにアクセスしようとすると、ＡＰは、このクライアント・デバイスを認証するために、多数のサポートしているＰＳＫの内どのＰＳＫを用いるべきか判断する。図１に示すように、ＡＰ１０２は、このＡＰがサポートするＰＳＫを含むストレージ１１４を含むか、または何らかの方法でストレージ１１４に関連付けられている。この例では、ＡＰ１０２は、鍵１、２、および３と模式的に示す３つのＰＳＫをサポートすることができるように示されている。しかしながら、本発明の実施形態はこれに関して限定されないので、ＡＰ１０２はいかなる数の異なるタイプのＰＳＫでもサポートすることができる。更に、ストレージ１１４は、クライアント・デバイス１０６、１０８、１１０、および１１２に格納されているＰＳＫの全てを含むように示されているが、クライアント・デバイスは、ＡＰ１０２がサポートしていないＰＳＫを有してもよいことを言うまでもない。また、ＡＰ１０２は、連携するクライアント・デバイスのいずれにも格納されていないＰＳＫを格納することもできる。

【００２９】

[0036] 図２は、本発明の一実施形態によるＡＰ１０２として構成されているコンピューター内におけるコンポーネント例を含むシステム２００を示す。ＡＰ１０２は、１つ又は複数のクライアント・デバイス２１０とネットワーク・インターフェース２０８を通じてワイヤレスで通信する。ネットワーク・インターフェース２０８は、ＡＰ１０２の中にある他のコンポーネントによって制御される。ＡＰ１０２は、コンピューティングデバイス２０４を通じて、その構成を設定することができる。コンピューティングデバイス２０４は、デスクトップ、ラップトップ、ＰＤＡ、あるいはアプリケーション・プログラムを実行し、ユーザー入力に応答する、または制御機能を実行することができる他の何らかのデバイスというようなデバイスであれば、いずれでも可能である。尚、コンピューティングデバイス２０４がＡＰ１０２を含んでもよく、このような場合、ＡＰ１０２は、コンピューティングデバイス２０４内においてソフトＡＰの機能を提供することは、認められてしかるべきである。ＡＰ１０２がソフトＡＰである場合、図２におけるコンポーネントの一部は、コンピューター記憶媒体におけるコンピューター・ソフトウェアとして実現することができ、またはプロセッサー（図示せず）によって実行することができる。しかしながら、ＡＰ１０２は、「ハード」ＡＰにおけるファームウェアを含む、適した方法であればいずれでも実現することができる。

【００３０】

[0037] 図示した例では、ＡＰ１０２は、ＰＳＫを追加および除去するためのインターフェースを含む。これらは、一例として、鍵追加ＡＰＩ２１２および鍵除去ＡＰ２１４として示されている。２つのＡＰＩが示されているが、ＡＰ１０２内においてＰＳＫを管理するためには、いずれの数またはタイプのＡＰＩでも用いることができる。ＡＰ１０２によってサポートされているＰＳＫの追加および除去、ならびにクライアント・デバイスがＡＰ１０２とＰＳＫを共有しているか否かの判断というような、ＡＰ１０２の他の機能は、制御ロジック２１６によって設けることができる。尚、制御ロジック２１６は、本発明の一部の実施形態にしたがってＡＰ１０２の動作を制御するのに適したコンポーネントであれば、いずれの数でも含むことができることは認められてしかるべきである。

【００３１】

[0038] ＡＰ１０２にプロビジョニングされたＰＳＫは、ＡＰ１０２のコンピューター・メモリーの中にあるＰＳＫストア２１８に格納されている。図示した実施形態では、このメモリーは不揮発性であるが、適したメモリーであればいずれでも用いることができる。

【００３２】
[0039] ＰＳＫに関する情報は、適した方法であればいずれでも編成することができる。ここでは、ＰＳＫストア２１８は、鍵テーブル２２０を含む。このテーブル２２０は、ＡＰ１０２に現在格納されているＰＳＫについての情報を維持する。尚、ＰＳＫストア２１８は、他の適したコンポーネント（１つまたは複数）を含んでもよいことは認められてしかるべきである。例えば、鍵追加ＡＰＩ２１２のコールによってＡＰ１０２にプロビジョニングされたＰＳＫを、ＰＳＫストアに格納する。
【００３３】
[0040] 尚、鍵テーブル２２０は、鍵の数、および格納することができる付随データに制限を設けることができることは、注記してしかるべきである。このような実施形態では、鍵テーブル２２０が格納できるＰＳＫの数に対する限度に達していない限り、ＰＳＫを鍵テーブル２２０に追加することができる。逆に、ＰＳＫをリストとしてまたはメモリー構造として格納し、任意の数の鍵を受け入れるように拡大することもでき、実施形態によっては、ＰＳＫの数に制限を設けないようにしてもよいことは認められてしかるべきである。
【００３４】
[0041] 例えば、鍵除去ＡＰＩ２１４を通じて命令を受け取ったときにＰＳＫをＡＰ１０２から除去する場合、このＰＳＫはＰＳＫストア２１８から除去される。
[0042] 図２に示すように、鍵テーブル２２０に格納されているｎ個の鍵の各々は、それぞれの期間を有する。この期間は、一例として、存続時間（ＴＴＬ）として示されている。尚、鍵の期間は、適した方法であれば他のいずれでも定義できることは認められてしかるべきである。先に論じたように、ＰＳＫは異なる期間を有することができ、それぞれのＴＴＬの満了時にＰＳＫを除去することができる。ＴＴＬの満了時におけるＰＳＫの除去は、鍵除去ＡＰＩ２１４によって管理することができる。
【００３５】
[0043] あるいは、ＴＴＬの満了時における鍵の除去は、制御ロジック２１６または他のいずれかの適したコンポーネントによって誘起させることもできる。図示した実施形態では、除去がＡＰＩ２１４によるコマンドによって誘起されたか、または制御ロジック２１６によって発行されたトリガによって誘起されたかには係わらず、鍵を除去するときの処理は同一である。しかしながら、実施形態によっては、ＰＳＫを除去するトリガに応じて、異なる処理を実行することもできる。尚、鍵テーブル２２０は、ＰＳＫと関連のある他の情報を格納することもでき、ＴＴＬを含む列は簡略化のために示されていることは、認められてしかるべきである。
【００３６】
[0044] クライアント・デバイスがＡＰまたはＡＰ上のアプリケーションを通じてネットワークにアクセスしようとすると、例えば、制御ロジック２１６のような、ＡＰの内部にある適したコンポーネントが、多数のサポートされているＰＳＫの内どのＰＳＫを用いてクライアント・デバイスとの接続を形成すべきか判断する。例えば、図１に示した例では、ＡＰＩ１０２では格納されている鍵１と表記されているＰＳＫを用いて、鍵１を用いるラップトップ１１０との接続を形成することができると、ＡＰ１０２は判断することができる。
【００３７】
[0045] ラップトップ１１０がＡＰ１０２との接続を形成するとき、この接続を形成するために用いられる鍵をＡＰ１０２に記録することができる。更に、ＡＰ１０２は接続ストア２２２を含む。接続ストア２２２は、一例として２２４Ａ～２２４Ｃとして示すデータ構造を格納する。各データ構造は、ＡＰ１０２がサポートする接続と関連のあるデータを含む。例えば、データ構造２２４Ａは、ＡＰ１０２と、例えば、図１に示したデバイス１０６、１０８、１１０、および１１２の内のいずれかとの間における接続についてのデータを含む。データ構造２２４Ａは、適した欄であればいずれでも含むことができる。つまり、データ構造２２４Ａは、接続を確立する相手となるクライアント・デバイスの識別

子を含む。この識別子は、ここではクライアントＩＤ２２６として示されている。また、データ構造は、ＡＰ１０２とクライアント・デバイスとの間で共有されている鍵を示す欄ＰＳＫ２２８も含む。ＰＳＫは、セッション鍵のような他の情報を得るために用いることができ、更にＡＰ１０２とクライアント・デバイスとの間の鍵交換中におけるデータ暗号化および解読にも用いることができる。このようにして得られた情報も、格納することができる。このように、接続ストア２２２は、セッション鍵２３０、および任意のグループ鍵２３２を所与の接続毎に格納することができる。尚、接続に関する他の情報もデータ構造２２４Ａに記録することができ、４つのエレメント２２６～２３２は、例示の目的で示したに過ぎないことは、認められてしかるべきである。

【００３８】

[0046] データ構造２２４Ｂおよび２２４Ｃは、ＡＰ１０２と連携するクライアント・デバイスとの間における他の接続についての同様の情報を含む。例えば、データ構造２２４Ａは、図１に示したＡＰ１０２とスキャナー１０６との間の接続についての情報を格納することができ、一方データ構造２２４Ｂおよび２２４Ｃは、それぞれ、ＡＰ１０２とラップトップ１１０およびＰＤＡ１１２との間の接続についての情報を含むことができる。接続ストア２２２は、３つのデータ構造のみを含むように示されているが、ＡＰ１０２に接続されているクライアント・デバイス毎にデータ構造を接続ストア２２２に格納することもできることは認められてしかるべきである。クライアント・デバイスが接続を形成すると、制御ロジック２１６がデータ構造を接続ストア２２２に追加することができる。クライアント・デバイスがＡＰ１０２から切断されると、それぞれのデータ構造を接続ストア２２２から除去することができる。

【００３９】

[0047] 先に論じたように、本発明の実施形態は、多数のＰＳＫをプロビジョニングされているＡＰを動作させる方法を提供する。クライアント・デバイスがリソースにアクセスしようとすると、ＡＰは、このクライアント・デバイスからＡＰへの接続要求を受ける。この要求の少なくとも一部は、クライアント・デバイスにプロビジョニングされた鍵を用いて作成されている。次いで、ＡＰは、この要求がＰＳＫの１つを用いて作成されたのか否か判断する。そうである場合、クライアント・デバイスを接続し、認証し、特定したＰＳＫに基づいて接続を確立することができる。そうでない場合、クライアントは認証されず、接続も確立されない。図示した実施形態では、ＡＰは、要求に含まれている情報が、ＡＰにプロビジョニングされたＰＳＫからの鍵を用いて発生することができる情報と一致するか否か判断することによって、クライアント・デバイスがＡＰのＰＳＫの内の１つを有するか否か判断する。一致があった場合、ＡＰは接続を許可する。そうでない場合、接続は許可されない。

【００４０】

[0048] 図３は、本発明の一部の実施形態にしたがってアクセス・ポイントを動作させるプロセスのフローチャートである。プロセス３００は、デバイスがＡＰ（例えば、ＡＰ１０２）として構成されたとき、または他のいずれかの適した時点において開始する。ブロック３０２において、ＡＰに複数のＰＳＫをプロビジョニングすることができる。ＡＰにＰＳＫをプロビジョニングするには、適した方法であればいずれでも用いることができる。例えば、各鍵を追加するために、ＡＰは、プログラミング・インターフェース（例えば、鍵追加ＡＰＩ２１２）によるコールを受けて、ＡＰに格納されている鍵を特定することができる。このようなＡＰＩによるコールは、ユーザー・インターフェースを通じてまたは他のいずれかの適した方法によって受け取られた入力に応答して発生することができる。

【００４１】

[0049] ＰＳＫ毎に値を規定することに加えて、ＰＳＫのプロビジョニングは、鍵の期間または鍵の他の特性を指定することを含むこともできる。このような情報は、鍵自体として同じＡＰＩを通じて提供することができ、または他のいずれかの適した方法でも提供することができる。先に論じたように、クライアント・デバイスは、ＰＳＫに関して異な

る要件を有することもある。つまり、本発明の実施形態は、異なる寿命および複雑さのＰＳＫの使用を提案する。一実施形態では、ＰＳＫは２５６ビットの数値、または８から６３ビット長のパスフレーズ(passfrase)であってもよい。しかしながら、本発明の実施形態はこの点において限定されることはなく、適した長さおよびフォーマットであればいずれのＰＳＫでも利用可能であることは、認められてしかるべきである。ＰＳＫは、異なる寿命および複雑さを有することができ、クライアント・デバイスに鍵をプロビジョニングするユーザー許容度に基づいて、寿命および複雑さを選択することができる。つまり、ＰＳＫは、一時的に用いられ（例えば、短いＴＴＬを有する）、クライアント・デバイスのユーザーによる鍵の容易な入力を可能にする、ユーザーに使いやすいフォーマットを有する短期鍵とすることができる。短期鍵は、一連の英数字キャラクタから成るパスワードであってもよい。短期鍵は、例えば、ＡＰを通じて短期間だけインターネットにアクセスすることを許可されているラップトップ・ユーザーによって用いられるとよい。また、ＰＳＫは、短期鍵よりも複雑で長い寿命の期間を有する（例えば、長いＴＴＬを有する）長期鍵であってもよい。この長期鍵は、ＡＰとの長期通信を維持するクライアント・デバイスに与えるとよい。例えば、据置型プリンターは、ＡＰとの長期通信を維持する場合があり、したがって長期鍵を利用するとよい。長期鍵は、ユーザーが入力するにはより難しいと考えられる。

【００４２】

[0050] プロビジョニングされた鍵は、後にＡＰＩが使用するために、格納することができる。ＡＰＩによる使用は、ＡＰがリブートされた後の使用を含む。ＡＰにプロビジョニングされたＰＳＫは、例えば、図２に示したＰＳＫストア２１８に格納することができる。各ＰＳＫは、それに関連付けられたＴＴＬ、およびＰＳＫストア２１８に格納されている他の特性も有することができる。尚、ＡＰには、適した時点であればいつでも、多数のＰＳＫをプロビジョニングすることができることは、認められてしかるべきである。例えば、異なるＰＳＫを異なる時点にＡＰにプロビジョニングすることもできる。

【００４３】

[0051] ブロック３０４において、ＡＰは（例えば、図２に示したネットワーク・インターフェース２０８を通じて）、クライアント・デバイスから、ＡＰへの接続要求を受ける。この要求は、いずれの時点でも送ることができ、既知の接続フォーマットであっても、または適したフォーマットであれば他のいずれでもよい。また、要求されたネットワーク・アクセスは、いずれの所望の目的のためであってもよい。例えば、クライアント・デバイスは、ＡＰを通じてネットワーク上のリソースにアクセスするために接続を要求することができる。また、クライアント・デバイスは、ＡＰ上にあるアプリケーションにアクセスする要求を送ることもできる。尚、本発明の実施形態はこの点において限定されないので、クライアント・デバイスは、他の目的のために、ＡＰへの接続要求を送ってもよいことは、認められてしかるべきである。この要求の一部は、クライアント・デバイスに格納されている鍵を用いて作成することもできる。

【００４４】

[0052] 判断ブロック３０６において、ＡＰ（例えば、制御ロジック２１６）は、ＡＰにプロビジョニングされた複数のＰＳＫからの各ＰＳＫについて、鍵を用いて作成された要求の一部が、複数のＰＳＫからのＰＳＫを用いて発生した情報と一致する情報を含むか否か判断する。鍵を用いて作成された要求の一部は、例えば、この要求を構成するメッセージの署名であってもよい。ＷＰＡおよびＷＰＡ２プロトコルでは、この署名は、クライアント・デバイスによって計算されるメッセージ・インテグリティ・コード（ＭＩＣ：message integrity code）とすることができる。これについては、以下で更に詳しく説明する。しかしながら、鍵から得られたいずれの情報でも、クライアントがＰＳＫを有することを示すことができる。この情報は、署名され、暗号化され、ハッシュされるか、またはこの鍵を用いて他の方法で処理されるか、あるいは他の鍵またはこの鍵を用いて発生したコードを用いて処理されてもよい。

【００４５】

[0053] 情報が一致したと判断した場合、本プロセスは分岐してブロック３０８に進み、ここで、クライアント・デバイスとＡＰとの間の接続が許可される。次いで、本プロセスは終了することができる。接続を許可することの一部として、ＡＰは、当技術分野において周知のようにＡＰが要求に応答するのと同じ方法で、この要求に応答すればよいが、ＡＰの応答は、クライアント・デバイスからの要求の中にある情報を照合した後に選択されたＰＳＫに基づいてもよく、追加の処理は、セッション鍵、グループ鍵、または特定されたＰＳＫに基づく他の情報の発生を含むことができる。また、接続の許可は、先に論じたように、接続ストア２２２にデータ構造を作成することを含んでもよい。

【００４６】

[0054] 情報が一致しないと判断した場合、本プロセスはブロック３１０に進み、ここで、接続を拒否し、クライアント・デバイスはリソースにアクセスすることを許可されない。次いで、本プロセスは終了する。尚、クライアント・デバイスから他の接続要求を受けたときも、図３に示すように、プロセス３００はブロック３０４に戻ってもよいことは言うまでもない。

【００４７】

[0055] 本発明の一部の実施形態によれば、ＰＳＫがクライアント・デバイスの１つ又は複数と関連付けられていても、このＰＳＫをＡＰから除去することができる。この除去は、例えば、ユーザーまたはアプリケーションが鍵の除去を要求したときに開始することができる。選択された鍵を除去する要求は、ユーザーによってＡＰ上のユーザー・インターフェースを通じて実行することができ、あるいはＡＰの構成を設定するために用いられたデバイスを通じて実行することもできる。

【００４８】

[0056] 更に、ＰＳＫは、その寿命が満了したときに、無効にすることができる。鍵が無効にされると、このＰＳＫを用いている１つ又は複数のクライアント・デバイス間の接続を選択的に遮断することができる。ＡＰに接続されており、ＡＰと異なるＰＳＫを共有している他のクライアント・デバイスは、ＡＰから切断されることはない。

【００４９】

[0057] 図４は、本発明の一実施形態にしたがって、アクセス・ポイントにプロビジョニングされた事前共有鍵を除去するプロセス４００を示す。このプロセスは、適した時点であればいつでも開始することができ、例えば、図２に示した鍵除去ＡＰＩ２１４のようなプログラミング・インターフェース、および／またはいずれかのＰＳＫがそのＴＴＬを超過しているか否かについての周期的なチェックを誘起する制御ロジック２１６内にあるタイミング・コンポーネントの状態の連続的監視の一部であってもよい。判断ブロック４０２において、本プロセスは、選択されたＰＳＫを除去することをＡＰ（例えば、ＡＰ１０２）に命令するユーザー入力を受け取ったか否か判断する。ＡＰまたはこのＡＰの構成を設定したデバイス（例えば、コンピューティングデバイス２０４）は、ユーザー・インターフェースを有することがあり、このインターフェースを、ユーザー入力を受け取るために用いることができる。

【００５０】

[0058] 選択されたＰＳＫを除去することを命令するユーザー入力が与えられたと判断したとき、本プロセスは分岐してブロック４０６に進み、ここでＰＳＫを除去する。先に論じたように、選択されたＰＳＫをＰＳＫストア２１８から除去することができる。このようにして、除去されたＰＳＫに基づく接続は、今後行われないようにすることができる。

【００５１】

[0059] 逆に、判断ブロック４０２において、ユーザー入力が与えられなかったと判断した場合、本プロセスはブロック４０４に進み、ここで、選択されたＰＳＫに付随する存続時間（ＴＴＬ）が満了したか否か判断する。ＴＴＬが満了している場合、本プロセスはブロック４０６に進み、ここで、選択されたＰＳＫを除去する。ＴＴＬが満了していない場合、本プロセスは、図４に示すように、開始に戻り、ＡＰＩ２１４を通じて入力が受け

取られるまで、または選択されたＰＳＫが除去されるまで、本プロセスはループ状に継続する。選択されたＰＳＫを除去することをＡＰに命令するユーザー入力が与えられたか否か判断するステップ、および選択されたＰＳＫに付随するＴＴＬが満了したか否か判断するステップは、２つの連続するステップとして示されているが、本発明はこの点について限定されないので、これらの動作は、いずれの順序で実行しても、同時に実行しても、またはいつの時点で実行してもよいことは認められてしかるべきである。更に、図４は、図示の簡略化のために、ステップの順次実行を示すことも認められてしかるべきである。図４に示す１つ又は複数の動作は、図示した動作の一部が同時にまたは別の時点で現れることができるように、別の計算スレッドで実行するとよい。例えば、ＰＳＫに付随するＴＴＬが満了したときに鍵を除去する動作は、ＡＰＩによるコールを処理する動作とは別の計算スレッドにおいて実行するとよい。

【００５２】

[0060] ブロック４０８において、ＡＰは、選択されたＰＳＫを用いているクライアント・デバイスを検索する。何のイベントがＡＰＩにＰＳＫを除去させたかには係わらず、ＰＳＫの除去は、除去されたＰＳＫ内において形成されていたあらゆる接続を終了することも含むとよい。したがって、図２に示した実施形態において、接続ストア２２２において検索することによって、このようなデバイスを特定することができる。しかしながら、接続をＰＳＫに関連付けるのに適したメカニズムであればいずれでも用いることができる。

【００５３】

[0061] 判断ブロック４１０において、１つ又は複数のクライアントが、選択されたＰＳＫを用いているか否か判断する。このようなデバイスが発見された場合、本プロセスはブロック４１２に進み、ここで、これらのクライアント・デバイスをＡＰから切断する。何故なら、これらが用いている鍵が除去されたからである。更に、切断された接続毎に、接続ストア２２２に格納されている構造２２４Ａ～２２４Ｃの内の１つというような、その接続と関連付けられているそれぞれのデータ構造を、接続ストア２２２から除去する。

【００５４】

[0062] 本発明の実施形態によれば、除去されるために選択されたＰＳＫを用いていたクライアント・デバイスのみが、ＰＳＫの除去時に切断される。ＡＰとの認証のために異なるＰＳＫを用いている他のクライアント・デバイスは、ＡＰに接続されたままとなっている。

【００５５】

[0063] 選択されたＰＳＫを用いているクライアント・デバイスが見つからなかった場合、本プロセスは終了することができる。しかしながら、プロセス４００は、図４に示すように、ＡＰにプロビジョニングされた鍵毎に繰り返すこともできる。

【００５６】

[0064] 本発明の一部の実施形態によれば、ＡＰ上にあるユーザー・インターフェースを通じて、またはＡＰの構成を設定するために用いたデバイス（例えば、コンピューティングデバイス２０４）を通じて、複数のＰＳＫをＡＰにプロビジョニングする。しかしながら、適したプロビジョニング・メカニズムであればいずれでも用いることができる。図５Ａから図５Ｃは、本発明の一実施形態による、ＰＳＫのプロビジョニングのためのユーザー・インターフェースの一例を示す。図５Ａは、ユーザー・インターフェース５００を含む。このユーザー・インターフェース５００は、鍵追加エレメント（例えば、プッシュ・ダウン・ボタンまたは他のエレメント）、およびユーザーが鍵の値を入力することができる欄５０４を含む。また、ユーザー・インターフェース５００は、ユーザーが鍵の中から１つを選択できることを示す鍵タイプ選択エレメント５０６（例えば、プッシュ・ダウン・ボタンまたは他のエレメント）を含む。図示した実施形態では、２つの鍵タイプ、即ち、長期および短期鍵タイプ、がサポートされている。各タイプでは、いくつの鍵でも許容することができる。しかしながら、実施形態によっては、ＡＰが各タイプ毎に１つの鍵しかサポートできない場合もある。つまり、ドロップ・ダウン・メニュー５０８において

一例として示すように、ユーザーは、入力した鍵が短期鍵かまたは長期鍵か選択することができる。

【００５７】

[0065] 図５Ｂは、ドロップ・ダウン・メニュー４０８において、図５Ｂではエレメント５１２として示されている「短期鍵」選択肢を選択することによって、ユーザーが短期鍵を選択したときのユーザー・インターフェースを示す。同様に、図５Ｃは、ドロップ・ダウン・メニュー４０８において、図５Ｃではエレメント５１６として示されている「長期鍵」選択肢を選択することによって、ユーザーが長期鍵を選択したことを示す。実施形態によっては、長期鍵は、ユーザーによるタイプ入力ではなく、自動的に発生するとよい場合もある。

【００５８】

[0066] 選択された鍵のタイプには関係なく、ユーザーは、適した入力デバイスを通じて、鍵の値も入力することができる。図５Ｂおよび図５Ｃは、欄５１０に入力された短期鍵に対する値、または欄５１４に入力された長期鍵に対する値を示す。図５Ｂおよび図５Ｃは、模式的に、短期鍵５１０が長期鍵５１６よりも短く、ユーザーによる入力が長期鍵５１６よりも簡単に行えることを示す。図５Ａ～図５Ｃは２つのタイプの鍵を示すが、２つよりも多いタイプの鍵を採用してもよいことは認められてしかるべきである。何故なら、本発明はこの点において限定されないからである。更に、ユーザー・インターフェース５００は、適したコンポーネントであれば他のいずれでも含むことができ、他のいかなる情報であっても、いかなるテキスト・フォーマットおよび視覚フォーマットでも表示することができる。例えば、他のコンポーネントをユーザー・インターフェースに含ませて、鍵の特性を定義する入力を受け取ることができる。先に示したように鍵が入力されると、図２に示したＰＳＫストア２１８における鍵テーブル２２０のような、鍵テーブルにこの鍵を格納することができる。尚、鍵テーブル２２０は、エントリ数に限度を有する場合もあることは注記してしかるべきである。

【００５９】

[0067] 先に論じたように、既知のプロトコルにしたがってＰＳＫを用いることができる。例えば、ＰＳＫは、データの暗号化および解読のため、ならびにその他の目的のために、一時的セッション鍵を派生させるために用いることができる。更に、ＡＰにおいて多数のＰＳＫをサポートすることに対する変更以外に、これらのプロトコルは、当技術分野において周知のように実施することができる。図６および図７は、本発明の一部の実施形態にしたがって、ＡＰにプロビジョニングされたＰＳＫを用いる鍵交換メカニズムの２つの例を示す。

【００６０】

[0068] コンピューター・デバイスは、ＩＥＥＥ８０２．１１規格に基づくＷｉ－Ｆｉ（登録商標）技術を増々用いつつある。Ｗｉ－Ｆｉ（登録商標）ネットワークは、Ｗｉ－Ｆｉ保護アクセス（ＷＰＡおよびＷＰＡ２）プロトコルを利用することができる。これらのプロトコルは、所与の時点におけるＡＰによる認証および鍵交換に、１つの事前共有鍵を用いる。尚、ＷＰＡおよびＷＰＡ２の認証および鍵交換プロトコルは、本明細書では一例として記載されるに過ぎず、適した認証および鍵交換プロトコルであれば他のいずれでも、ＡＰおよびクライアント・デバイスによって用いることができることは、認められてしかるべきである。図６は、本発明の一部の実施形態にしたがって、Ｗｉ－Ｆｉ保護アクセス２（ＷＰＡ２）プロトコルを用いた、ＡＰとクライアント・デバイスとの間における鍵交換プロセスを示す。図６は、クライアント・デバイス６００側、即ち、要求側(supplicant)で実行されるプロセスと、ＡＰ６０２側、即ち、認証側(authenticator)で実行されるプロセスとを示す。クライアント・デバイス６００は、例えば、図１に示したデバイスの内のいずれでもよい。この例におけるクライアント６００内部での処理は、ＡＰが１つの事前格納鍵しかサポートしない場合の鍵交換と同一であることに、当業者であれば気がつくであろう。

【００６１】

[0069] 本プロセスは、この例ではＷｉ－Ｆｉクライアント・デバイスまたは要求側と呼ぶことができるクライアント・デバイスが、ＡＰ６０２に接続要求を送った後に開始するが、このプロセスは、適したイベントであればいずれによって誘起されてもよい。先に論じたように、本プロセスは、メッセージの作成を含み、このメッセージの一部は、クライアント・デバイスに格納されている鍵に基づく。次に、ＡＰは、それにプロビジョニングされた多数のＰＳＫの内どれを、クライアント・デバイスを認証するために用いることができるか判断する。そのＰＳＫは、以下で説明するように、鍵交換に用いることができる。

【００６２】

[0070] ＷＰ２プロトコルでは、鍵交換は、ＬＡＮ上拡張可能認証プロトコル（ＥＡＰＯＬ：Extensible Authentication Protocol over LANs）－ＫＥＹメッセージを用いて実行される。ブロック６０４において、ＡＰ６０２はメッセージ１EAPOL_KEY(ANonce, Unicast)を送る。このメッセージは、ブロック６０６において、クライアント・デバイス６００によって受信される。Unicastパラメータは、メッセージ１がクライアント・デバイス６００のみに送られることを示す。ANonceは、認証側Nonceを示し、この例では、ＷＰＡ２プロトコルを用いてＡＰ６０２において発生された、いずれかの適したフォーマットのランダム・データである。

【００６３】

[0071] クライアント６００は、メッセージ１をブロック６０６において受信する。図示した鍵交換のために、クライアント・デバイス６００は、SNonce（要求側Nonce）を発生する。これも、いずれかの適したフォーマットのランダム・データである。

【００６４】

[0072] ブロック６０８において、クライアント・デバイス６００は、それに格納されている鍵を用いて、ANonceおよびSNonceからペア一時鍵(Pairwise Transient Key)を計算する。ブロック６１０において、クライアント６００は、ＰＴＫを用いてメッセージ２EAPOL_KEY(SNonse, Unicast, MIC)を送る。Unicastパラメータは、メッセージ２がＡＰ６０２のみに送られることを示す。ＷＰＡ２プロトコルによって実施されるメッセージ完全性コード（ＭＩＣ：message integrity code）は、データ・パケットの有害な変更を検出することによって、データ・パケット完全性を保護する鍵付きハッシング関数(keyed hashing function)である。ＭＩＣは、例えば、暗号化および送信される前の非暗号化生データ全体から計算された８ビット値とすることができる。しかしながら、本発明の実施形態はこの点において限定されないので、ＭＩＣは、適したフォーマットおよび長さであればいずれでもよい。ここでは、ＰＴＫを用いてＭＩＣを発生する。一方、ＰＴＫは、クライアント６００に格納されている鍵に基づいて発生する。つまり、ＭＩＣを含むメッセージ２の一部は、クライアント６００の格納されている鍵に基づく。この格納されている鍵のコピーを有する他のデバイスも、同様に、ＭＩＣの同じ値を発生することができる。しかしながら、クライアントに格納されている鍵のコピーを有していないデバイスは、ＭＩＣに対して同じ値を容易に発生することはできない。

【００６５】

[0073] ブロック６１２において、ＡＰ６０２はメッセージ２を受信する。ブロック６１４において、ＡＰ６０２は、ＡＰ６０２に格納されている多数のＰＳＫの内１つを用いて、ANoceおよびSNonceからＰＴＫを計算する。次いで、ブロック６１６において、計算したＰＴＫを用いて、当技術分野では周知のように、ＭＩＣの有効性を判断する。このような有効性判断は、ＡＰ６０２において発生したＭＩＣを、メッセージ２において受信したそれと比較することによって行うことができる。ＡＰ６０２によって用いられている事前格納鍵がクライアント６００によって用いられている鍵と同一である場合、ＭＩＣは一致するはずである。判断ブロック６１８において、ＡＰ６０２は（例えば、図２に示した制御ロジック２１６のようなコンポーネントを用いて）、クライアント・デバイス６００から受け取ったＭＩＣが、ＡＰ６０２によって計算されたＡＰと一致するか否か判断する。ＭＩＣがＰＴＫと一致しないと判断した場合、本プロセスは分岐して判断ブロック６１

９に進み、ここで、本プロセスは、別のＰＳＫが比較のために残っているか否かに基づいて、分岐を行う。他のＰＳＫがない場合、クライアント６００によって用いられている鍵に一致するものがないことを意味し、本プロセスは分岐してブロック６２０に進み、ここで鍵交換プロセスを中断し、クライアント・デバイス６００は、要求したリソースにアクセスすることを許可されず、ＡＰ６０２から切断される。

【００６６】

[0074] 図６に示すように、ブロック６１４からブロック６１８において実行される動作は、ＡＰ６０２において格納されている多数のＰＳＫの各々について繰り返される。したがって、１つのＰＳＫで一致が生じない場合、本プロセスはブロック６１９からブロック６１４に戻る。つまり、ＡＰは、多数のＰＳＫがある場合、その内のどれが、クライアント・デバイスに格納されている鍵と一致するのか判断する。

【００６７】

[0075] ＭＩＣ同士が一致したと判断した場合、これは、ＡＰ６０２が、クライアント・デバイス６００によって用いられる鍵と一致するＰＳＫを発見したことを示す。したがって、クライアント・デバイス６００とＡＰ６０２との間における接続が許可され、クライアント・デバイスはリソースにアクセスすることが許可される。この状況では、本プロセスは分岐してブロック６２２に進む。また、クライアント・デバイス６００のＰＳＫ、および関連する情報は、ＡＰ６０２に記録することができる。例えば、図２に示したデータ構造２２４Ａ～２２４Ｃの内の１つのようなデータ構造が作成され、接続ストア２２２に記録される。

【００６８】

[0076] 鍵交換プロセスを完了するために、ＰＴＫをクライアント・デバイスにインストールする必要がある。このため、ブロック６２２において、ＡＰ６０２は、メッセージ３EAPOL_KEY（InstallＰＴＫ、Unicast、MIC、EncryptedＧＴＫ）を送り、クライアント６００にＰＴＫをインストールすることを命令する。ＧＴＫは、ＷＰＡ２プロトコルによるグループ毎一時鍵を意味し、クライアント・デバイス６００に合わせて任意に作成することができる。ＧＴＫは、ＰＳＫを用いて発生され、クライアント６００を、デバイスのグループの１メンバーとして識別するために用いることができる。ＡＰ６０２は、ＧＴＫを暗号化し、暗号化したＧＴＫをクライアント・デバイス６００に、メッセージ３の一部として送る。クライアント・デバイス６００は、ブロック６２４においてメッセージ３を受信し、ブロック６２６において、ＡＰ６０２に承認をメッセージ４EAPOL_KEY(Unicast, MIC)として送る。このメッセージ４は、ブロック６２８においてＡＰ６０２によって受信される。次いで、本プロセスは終了することができる。

【００６９】

[0077] 図７は、本発明の一部の実施形態による、Ｗｉ－Ｆｉ保護アクセス（ＷＰＡ）を用いた、ＡＰとクライアント・デバイスとの間における鍵交換プロセスを示す。ＷＰＡ２プロトコルにおけると同様、鍵交換は、ＬＡＮ上拡張可能認証プロトコル（ＥＡＰＯＬ）－KEYメッセージを用いて行われる。図７は、クライアント・デバイス７００およびＡＰ７０２において実行されるプロセスを示す。クライアント・デバイス７００は、例えば、図１に示したデバイスの内いずれでもよい。同様に、ＡＰ７０２は、図１および図２に示したＡＰ１０２とすればよい。

【００７０】

[0078] 本プロセスは、Ｗｉ－Ｆｉクライアント・デバイス７００、即ち、要求側がＡＰ７０２に接続して、ネットワークまたは他のリソースへのＡＰ７０２を通じてアクセスを要求した後に開始することができる。先に論じたように、クライアント・デバイス７００は、その鍵を用いて、ＡＰ７０２へのメッセージを作成し、次いで、ＡＰ７０２は、それにプロビジョンされた多数のＰＳＫの内いずれかを、クライアント・デバイス７００を認証するために用いることができるか否か判断する。ＰＳＫは、以下で述べるように、鍵交換に用いることができる。

【００７１】

[0079] ブロック７０４において、ＡＰ７０２はメッセージ１EAPOL_KEY(ANonce, Unicast)を送り、ブロック７０６において、クライアント・デバイス７００がこのメッセージ１を受信する。Unicastパラメータは、メッセージ１がクライアント・デバイス７００のみに送られることを示す。ANonceは、認証側Nonceを示し、この例では、ＷＰＡプロトコルを用いてＡＰ７０２において発生した、いずれかの適したフォーマットのランダム・データである。この例では、クライアント・デバイス７００はSNonce(要求側Nonce）を発生するが、これも、いずれかの適したフォーマットのランダム・データである。

【００７２】

[0080] ブロック７０８において、クライアント・デバイス７００は、それに格納されている鍵を用いて、ANonceおよびSNonceからペア一時鍵（ＰＴＫ）を計算し、ブロック７１０において、メッセージ２EAPOL_KEY(SNonce, Unicast, MIC, SSN IE)を送る。このメッセージは、ブロック７１２において、ＡＰ７０２によって受信される。Unicastパラメータは、メッセージ２がＡＰ７０２のみに送られることを示す。SSN IEは、ＷＰＡプロトコルにしたがって定義された、メッセージ２における安全情報エレメント(Secure Information Element)である。メッセージ完全性コード（ＭＩＣ）は、前述のように定義され、クライアント・デバイス７００に格納されている鍵に基づいて発生した情報を含む。

【００７３】

[0081] ブロック７１４において、ＡＰ７０２は、ＡＰ７０２にプロビジョニングされた多数のＰＳＫの内１つを用いて、ANonceおよびSNonceからＰＴＫを計算する。次いで、ブロック７１６において、計算したＰＴＫを用いて、当技術分野で周知のように、ＭＩＣの有効性を判断する。このような有効性判断は、ＡＰ７０２が発生したＭＩＣを、メッセージ２において受信したＭＩＣと比較することによって実行することができる。ＡＰ７０２によって用いられる事前格納鍵が、クライアント７００によって用いられる鍵と同一である場合、ＭＩＣ同士が一致するはずである。更に、判断ブロック７１８において、ＡＰ７０２は（例えば、図２に示した制御ロジック２１６のようなコンポーネントを用いて）、クライアント・デバイス７００から受信したＭＩＣが、ＡＰ７０２によって計算されたＭＩＣと一致するか否か判断する。

【００７４】

[0082] ＭＩＣがＰＴＫと一致しないと判断した場合、本プロセスはブロック７１９からブロック７１４に戻り、別のＰＳＫを検査する。一致するＰＳＫがない場合、本プロセスは先に進み、鍵交換プロセスを中断し、クライアント・デバイス７００は、要求したリソースにアクセスすることを許可されず、ＡＰ７０２から切断される。図７に示すように、ブロック７１４～７１８において実行される動作は、一致するＰＳＫが発見されるまで、またはＡＰ７０２に格納されている多数のＰＳＫの全てが評価され終わるまで繰り返される。こうして、ＡＰは、多数のＰＳＫがあるのであればその内のどれが、クライアント・デバイスに格納されている鍵と一致するのか判断する。

【００７５】

[0083] ＡＰ７０２によって発生されたＭＩＣが、クライアントによって発生されたＭＩＣと一致すると判断した場合、本プロセスは分岐して７２２に進む。この時点で、クライアント・デバイス７００のＰＳＫはＡＰ７０２に記録される。例えば、図２に示したデータ構造２２４Ａ～２２４Ｃの内の１つというようなデータ構造が作成され、接続ストア２２２に記録される。ブロック７２２において、ＡＰ７０２は、メッセージ３EAPOL_KEY(InstallＰＴＫ、Unicast, MIC, SSN IE)を送り、クライアント・デバイス７００にＰＴＫをインストールすることを命令する。クライアント・デバイス７００は、ブロック７２５においてメッセージ３を受信し、ＰＴＫをインストールし、ブロック７２６においてＡＰ７０２に承認をメッセージ４EAPOL_KEY(Unicast, MIC)として送り、ＰＴＫがインストールされたことを示す。メッセージ４は、ブロック７２８においてＡＰ７０２によって受信される。この時点で、ペア一時鍵の交換が完了し、クライアント・デバイス７００およびＡＰ７０２は互いに認証される。

【００７６】

[0084] ＩＥＥＥ８０２．１１規格は、例えば、ビデオ・データの配信において有用となり得るマルチキャスト・メッセージをサポートする。ＷＰＡプロトコルは、マルチキャスト・メッセージに発生されるグループ一時鍵をサポートする。この鍵は、ＰＴＫのようなペア一時鍵とは異なる。

【００７７】

[0085] このように、クライアント・デバイス７００とＡＰ７０２との間において確立された安全な接続を、ＡＰ７０２が、ＡＰ７０２において発生されＱＰＡプロトコルによって実現されたグループ一時鍵（ＧＴＫ）を含むメッセージを送るために用いることができる。ＡＰ７０２は、ＧＴＫを暗号化し、暗号化したＧＴＫをクライアント・デバイス７００に、メッセージ５EAPOL_KEY(EncryptedGTK, GNonce, Group, MIC)の一部として送る。GNonceは、グループ一時鍵発生のために発生されたランダム・データであるGroup Nonceのことであり、一方Groupパラメータは、メッセージ５が、クライアント・デバイス７００が属するデバイス・グループに送られるマルチキャスト・メッセージであることを指定する。ブロック７３２において、クライアント・デバイス７００はメッセージ５を受信し、ＧＴＫをインストールする。ブロック７３４において、クライアント・デバイス７００は、ＡＰ７０２に承認メッセージ６EAPOLEKY(Group, MIC)を送り、暗号化したＧＴＫがクライアント・デバイス７００にインストールされたことを示す。これによって、クライアント・デバイス７００とＡＰ７０２との間における鍵交換プロセスが完了する。

【００７８】

[0086] 以上、本発明の少なくとも１つの実施形態の様々な態様について説明したが、種々の変更、修正、および改良が当業者には想起されることは認められてしかるべきである。

【００７９】

[0087] このような変更、修正、および改良は、本開示の一部であることと意図しており、更に本発明の主旨および範囲に該当することも意図している。したがって、以上の説明および図面は、単なる一例である。

【００８０】

[0088] 本発明の前述の実施形態は、多数の方法のいずれでも実現することができる。例えば、実施形態は、ハードウェア、ソフトウェア、またはその組み合わせを用いて実現することができる。ソフトウェアで実現する場合、ソフトウェア・コードをいずれかの適したプロセッサーまたはプロセッサーの集合体において実行することができる。プロセッサーの集合体は、１つのコンピューター内に設けられているか否かには係わらない。

【００８１】

[0089] 更に、コンピューターは、ラック設置コンピューター、デスクトップ・コンピューター、ラップトップ・コンピューター、またはタブレット・コンピューターというような、多数の形態の内いずれにおいても具体化できることは認められてしかるべきである。加えて、コンピューターとは一般に見なされないが適した処理能力を有するデバイスに、コンピューターを埋め込むこともできる。このようなデバイスには、パーソナル・デジタル・アシスタント（ＰＤＡ）、スマート・フォン、あるいは適した携帯用または固定電子デバイスであればそのいずれもが含まれる。

【００８２】

[0090] また、コンピューターは１つ又は複数の入力および出力デバイスも有することができる。これらのデバイスは、とりわけ、ユーザー・インターフェースを提示するために用いることができる。ユーザー・インターフェースを設けるために用いることができる出力デバイスの例には、プリンター、または出力の視覚的提示のための表示画面、および出力の聴覚的提示のためのスピーカーまたはその他の音響発生デバイスが含まれる。ユーザー・インターフェースに用いることができる入力デバイスの例には、キーボード、ならびに、マウスのようなポインティング・デバイス、タッチ・パッド、およびデジタル化タブレットが含まれる。別の例として、コンピューターは、音声認識を通じて、または他の可聴フォーマットで、入力情報を受けることもできる。

【００８３】
[0091] このようなコンポーネントは、ローカル・エリア・ネットワーク、あるいは企業ネットワークまたはインターネットというようなワイド・エリア・ネットワークを含む１つ又は複数のネットワークによって，いずれかの適した形態で相互接続することができる。このようなネットワークは、いずれかの適した技術に基づくことができ、いずれかの適したプロトコルにしたがって動作することができ、ワイヤレス・ネットワーク、有線ネットワーク、または光ファイバ・ネットワークを含むことができる。
【００８４】
[0092] また、本明細書において概要を説明した種々の方法またはプロセスをソフトウェアとしてコード化することもでき、種々のオペレーティング・システムまたはプラットフォームのいずれか１つを採用する１つ又は複数のプロセッサー上で実行可能である。加えて、このようなソフトウェアは、多数の適したプログラミング言語および／またはプログラミング・ツールまたはスクリプティング・ツールの内いずれを用いても書くことができ、実行可能機械語コードまたは中間コードとしてコンパイルし、フレームワークまたは仮想マシン上で実行することもできる。
【００８５】
[0093] これに関して、本発明をコンピューター読み取り可能媒体（または多数のコンピューター読み取り可能媒体）(例えば、コンピューター・メモリー、１つ又は複数のフロッピ・ディスク、コンパクト・ディスク、光ディスク、磁気テープ、フラッシュ・メモリー、フィールド・プログラマブル・ゲート・アレイまたは他の半導体デバイス内における回路構成、あるいはその他の有形コンピューター記憶媒体）として具体化することができる。このコンピューター読み取り可能媒体には１つ又は複数のプログラムがエンコードされており、１つ又は複数のコンピューターまたは他のプロセッサー上で実行すると、先に論じた本発明の種々の実施形態を実現する方法を実行する。１つまたは複数のコンピューター読み取り可能媒体は、そこに格納されている１つまたは複数のプログラムを１つ又は複数の異なるコンピューターまたは他のプロセッサーにロードして、先に論じた本発明の種々の態様を実現することができるように、移転可能にすることができる。
【００８６】
[0094] 「プログラム」または「ソフトウェア」という用語は、本明細書では、先に論じた本発明の種々の態様を実現するためにコンピューターまたは他のプロセッサーをプログラミングするために採用することができる、あらゆるタイプのコンピューター・コードまたは１組のコンピューター実行可能命令を指すように、包括的な意味で用いられるものとする。加えて、本発明の一態様によれば、実行したときに本発明の方法を実行する１つ又は複数のコンピューター・プログラムは、１つのコンピューターまたはプロセッサー上に常駐する必要はなく、多数の異なるコンピューターまたはプロセッサー間においてモジュール様式で分散して、本発明の種々の態様を実現することもできる。
【００８７】
[0095] コンピューター実行可能命令は、プログラム・モジュールのような多くの形態にすることができ、１つ又は複数のコンピューターまたは他のデバイスによって実行することができる。一般に、プログラム・モジュールは、ルーチン、プログラム、オブジェクト、コンポーネント、データ構造などを含み、特定のタスクを実行するか、または特定の抽象データ・タイプを実現する。通例、プログラム・モジュールの機能は、種々の実施形態において、所望に応じて組み合わせることまたは分散することができる。
【００８８】
[0096] また、データ構造は適した形態であればいずれでもコンピューター読み取り可能媒体に格納することができる。図示の簡略化のために、データ構造は、データ構造における位置に関する欄を有するように示すことができる。このような関係は、同様に、これらの欄にストレージを割り当て、コンピューター読み取り可能媒体における位置が欄間の関係を伝えるようにすることによっても達成することができる。しかしながら、データ構造の欄における情報間に関係を確立するためには、適したメカニズムであればいずれでも

用いることができる。適したメカニズムには、データ・エレメント間に関係を確立するポインタ、タグ、またはその他のメカニズムの使用が含まれる。

【００８９】

[0097] 本発明の種々の態様は、単独で用いることも、組み合わせて用いることも、または以上で説明した実施形態においては具体的に論じられなかった種々の構成で用いることもでき、したがって、以上の説明において明記され図面において図示されたコンポーネントの詳細や構成に、その適用が限定されるのではない。例えば、一実施形態において記載された態様を、他の実施形態において記載された態様と、いかようにでも組み合わせることができる。

【００９０】

[0098] また、本発明は、方法として具体化することができ、その一例が紹介されている。この方法の一部として実行される動作(act)は、いずれかの適した方法で順序付けることができる。したがって、図示したのとは異なる順序で動作が実行される実施形態を構築することもできる。例示的な実施形態では、順次動作として示されているが、一部の動作を同時に実行することを含むことができる。

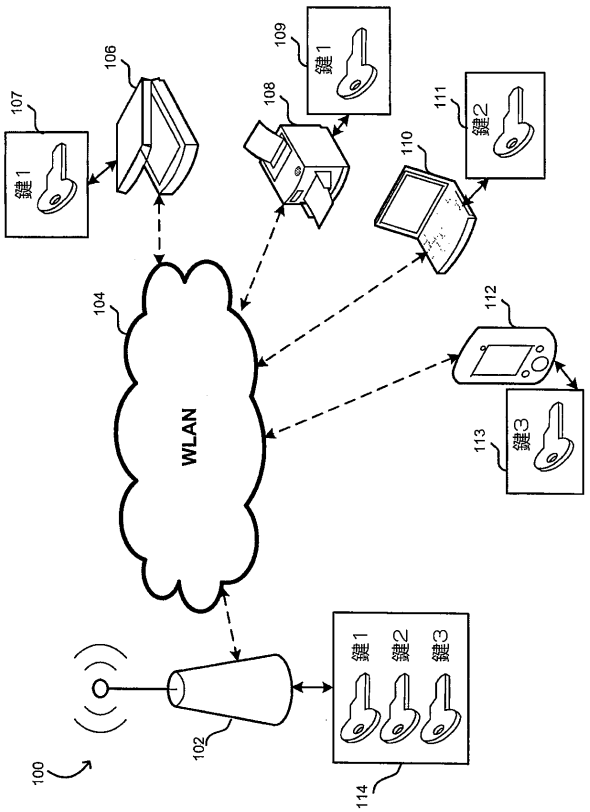
【００９１】

[0099] 「第１」、「第２」、「第３」等というような序数を特許請求の範囲において請求項の要素を修飾するために用いる場合、それ自体によって、なんら優先順位、優位性、１つの請求項の要素の他方に対する順序、方法の動作が実行される時間的順序を暗示することはなく、請求項の要素を区別するために、単に、ある名称を有する請求項の要素を、同じ名称(序数語を除く）を有する他のエレメントと区別するための標識として用いられるに過ぎない。

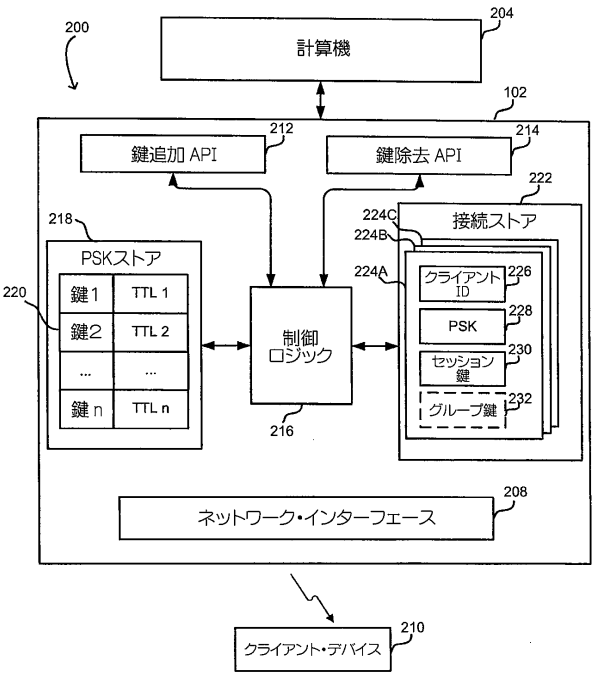
【００９２】

[0100] また、本明細書において用いた言葉使いや用語は、説明を目的としており、限定と見なしてはならない。「含む」(including)、「備えている」(comprising)、または「有する」(having)、「内蔵する」(containing)、「伴う」(involving)、およびその変形は、本明細書では、その後に羅列される項目およびその同等物、ならびに追加項目を包含することを意味するものとする。

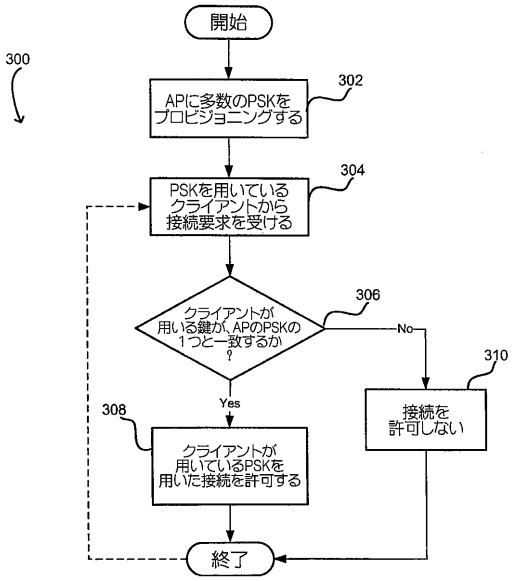
【図１】


鍵1
鍵2
鍵3
WLAN
100
102
104
106
107
108
109
110
111
112
113
114

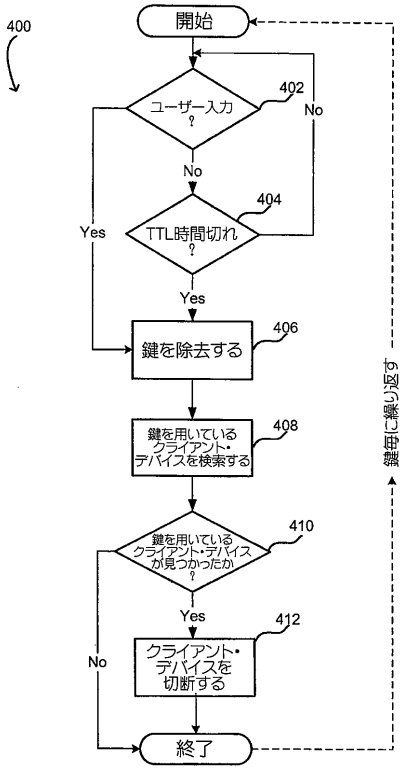
【図２】


200
計算機
204
102
鍵追加 API
212
鍵除去 API
214
222
接続ストア
224C
224B
224A
218
PSKストア
220
鍵1
TTL 1
鍵2
TTL 2
...
...
鍵 n
TTL n
制御
ロジック
216
クライアント ID
226
PSK
228
セッション 鍵
230
グループ鍵
232
ネットワーク・インターフェース
208
クライアント・デバイス
210

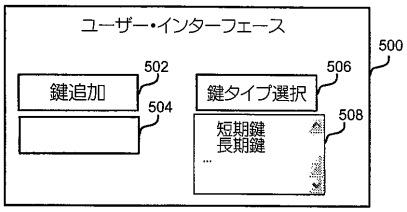
【図３】


300
開始
APに多数のPSKを プロビジョニングする
302
PSKを用いている クライアントから 接続要求を受ける
304
クライアントが 用いる鍵が、APのPSKの 1つと一致するか ?
306
No
Yes
接続を 許可しない
310
308
クライアントが 用いているPSKを 用いた接続を許可する
終了

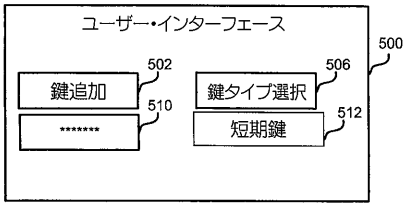
【図４】


400
開始
ユーザー入力 ?
402
No
Yes
TTL時間切れ ?
404
Yes
No
鍵を除去する
406
鍵を用いている クライアント・ デバイスを検索する
408
鍵を用いている クライアント・デバイス が見つかったか ?
410
Yes
No
クライアント・ デバイスを 切断する
412
終了
鍵毎に繰り返す

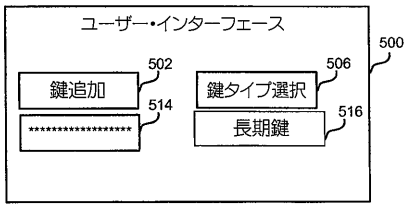
【図５Ａ】



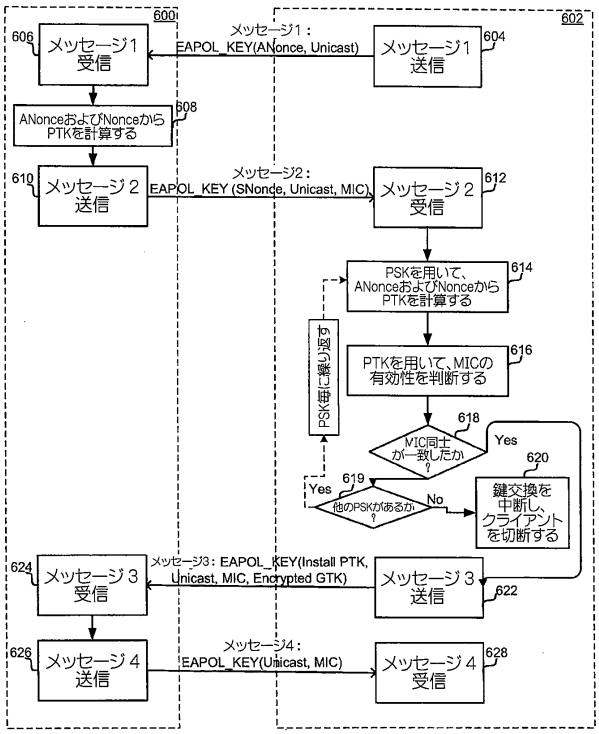
【図５Ｂ】



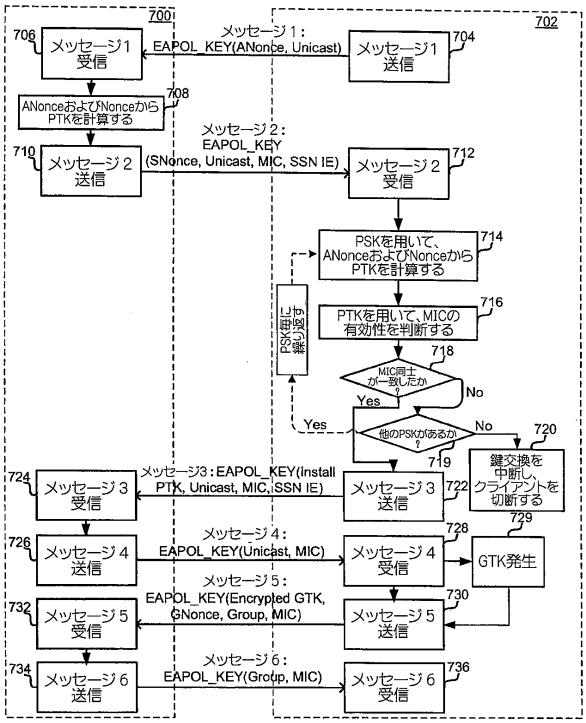
【図５Ｃ】



【図６】



【図７】



フロントページの続き

(72)発明者　シェン，ホイ
アメリカ合衆国ワシントン州９８０５２－６３９９，レッドモンド，ワン・マイクロソフト・ウェイ，マイクロソフト　コーポレーション，エルシーエイ－インターナショナル・パテンツ
(72)発明者　ジャン，ショーン
アメリカ合衆国ワシントン州９８０５２－６３９９，レッドモンド，ワン・マイクロソフト・ウェイ，マイクロソフト　コーポレーション，エルシーエイ－インターナショナル・パテンツ
(72)発明者　バナジー，アニルバン
アメリカ合衆国ワシントン州９８０５２－６３９９，レッドモンド，ワン・マイクロソフト・ウェイ，マイクロソフト　コーポレーション，エルシーエイ－インターナショナル・パテンツ
(72)発明者　リウ，ホン
アメリカ合衆国ワシントン州９８０５２－６３９９，レッドモンド，ワン・マイクロソフト・ウェイ，マイクロソフト　コーポレーション，エルシーエイ－インターナショナル・パテンツ
(72)発明者　マンダナ，タルーン
アメリカ合衆国ワシントン州９８０５２－６３９９，レッドモンド，ワン・マイクロソフト・ウェイ，マイクロソフト　コーポレーション，エルシーエイ－インターナショナル・パテンツ

審査官　重田　尚郎

(56)参考文献　特表２００８－５３７３８１（ＪＰ，Ａ）
米国特許出願公開第２００４／０２４０４１２（ＵＳ，Ａ１）
特開２００４－２５４２８６（ＪＰ，Ａ）
特表２００４－５３５６２７（ＪＰ，Ａ）
特開２００７－１１０４８７（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｗ　　４／００－９９／００