(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2007-538470
(P2007-538470A)
(43)公表日　平成19年12月27日(2007.12.27)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 12/56	***(2006.01)***	H04L	12/56	H	5K030
H04L 12/66	***(2006.01)***	H04L	12/56	A	5K067
H04Q 7/38	***(2006.01)***	H04L	12/66	E	
		H04B	7/26	109A	
		H04B	7/26	109R	

審査請求 未請求　予備審査請求 有　（全 15 頁）

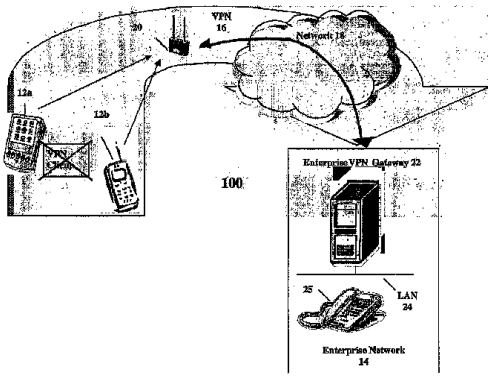
(21)出願番号　特願2007-527294 (P2007-527294)
(86)(22)出願日　平成17年5月10日 (2005.5.10)
(85)翻訳文提出日　平成18年11月16日 (2006.11.16)
(86)国際出願番号　PCT/US2005/016378
(87)国際公開番号　WO2005/117392
(87)国際公開日　平成17年12月8日 (2005.12.8)
(31)優先権主張番号　60/571,742
(32)優先日　平成16年5月17日 (2004.5.17)
(33)優先権主張国　米国 (US)

(71)出願人　501263810
トムソン　ライセンシング
Ｔｈｏｍｓｏｎ　Ｌｉｃｅｎｓｉｎｇ
フランス国，　エフ－９２１００　ブローニュ　ビヤンクール，　ケ　アルフォンス　ル　ガロ，　４６番地
４６　Ｑｕａｉ　Ａ．　Ｌｅ　Ｇａｌｌｏ，　Ｆ－９２１００　Ｂｏｕｌｏｇｎｅ－Ｂｉｌｌａｎｃｏｕｒｔ，　Ｆｒａｎｃｅ
(74)代理人　100070150
弁理士　伊東　忠彦
(74)代理人　100091214
弁理士　大貫　進介
(74)代理人　100107766
弁理士　伊東　忠重

最終頁に続く

(54)【発明の名称】ＶＰＮクライアントのないポータブル装置の仮想プライベートネットワークへのアクセスを管理する方法

(57)【要約】
有利には、ポータブル通信装置（１２ａ、１２ｂ）は、ＶＰＮクライアント（２６）の必要なく、仮想プライベートネットワーク（１６）リンクを通じて企業ネットワーク（１４）にアクセスすることができる。通信を実現するために、ポータブル通信装置は、１つ以上の周知のセキュア無線プロトコルを使用して、無線アクセスポイント（２０）と通信リンクを確立する。無線アクセスポイントは、ＶＰＮ（１６）を通じて企業ネットワークと通信リンクを確立し、接続をブリッジして、ポータブル計算装置と企業ネットワークとの間のエンド・ツー・エンド・リンクを提供する。



【特許請求の範囲】
【請求項１】
ポータブル通信装置と企業ネットワークとの間で接続を確立する方法であって、
ポータブル通信装置から企業ネットワークにアクセスする要求を無線アクセスポイントで受信するステップと、
前記ポータブル通信装置が何の企業ネットワークにアクセスしようとしているかを前記無線アクセスポイントで決定するステップと、
前記ポータブル通信装置との無線通信リンクを生成するために無線アクセス認証プロトコルを使用して、前記無線アクセスポイントで前記ポータブル通信装置を認証するステップと、
前記ポータブル通信装置によりアクセスされる前記企業ネットワークへの仮想プライベートネットワーク接続を確立し、前記ポータブル通信装置と前記企業ネットワークとの間で前記アクセスポイントを介して接続を提供するステップと、
前記無線通信リンクと仮想プライベート通信接続とをブリッジするステップと
を有する方法。
【請求項２】
請求項１に記載の方法であって、
前記決定するステップは、
前記企業ネットワークにアクセスしようとする前記ポータブル通信装置から識別証明書を受信するステップと、
前記識別証明書から前記企業ネットワークを特定するステップと
を更に有する方法。
【請求項３】
請求項１に記載の方法であって、
前記決定するステップは、
前記企業ネットワークにアクセスしようとする前記ポータブル通信装置からネットワーク識別情報を受信するステップと、
前記ネットワーク識別情報から前記企業ネットワークを特定するステップと
を更に有する方法。
【請求項４】
請求項１に記載の方法であって、
前記認証するステップは、前記企業ネットワークに問い合わせて、前記ポータブル通信装置の証明書を確認するステップを更に有する方法。
【請求項５】
請求項１に記載の方法であって、
前記認証するステップは、ｔｅｍｐｏｒａｌ ｋｅｙ ｉｎｔｅｇｒｉｔｙ ｐｒｏｔｏｃｏｌ、ｗｉ－ｆｉ ｐｒｏｔｅｃｔｅｄ Ａｃｃｅｓｓ ｐｒｏｔｏｃｏｌ又はａｄｖａｎｃｅｄ ｅｎｃｒｙｐｔｉｏｎ ｓｔａｎｄａｒｄ ｐｒｏｔｏｃｏｌのうち１つを使用して、前記ポータブル通信装置を認証することを更に有する方法。
【請求項６】
ポータブル通信装置が企業ネットワークにアクセスするように動作する方法であって、
無線アクセスポイントにより受信するためのアクセス要求を前記ポータブル通信装置から送信するステップと、
前記無線アクセスポイントにより受信するためにアクセスされる前記企業ネットワークの識別情報の指示を前記ポータブル通信装置により供給するステップと、
前記ポータブル通信装置から前記無線アクセスポイントに認証情報を提供し、前記無線アクセスポイントが前記ポータブル通信装置と無線通信リンクを確立することを可能にし、前記無線アクセスポイントが前記企業ネットワークとＶＰＮ接続を確立することを可能にし、これによって、無線アクセスポイントが前記ＶＰＮ接続と無線通信リンクとをブリッジすることができるステップと

を有する方法。
【請求項７】
ポータブル通信装置と企業ネットワークとの間で接続を確立する装置であって、
ポータブル通信装置から企業ネットワークにアクセスする要求を無線アクセスポイントで受信する手段と
前記ポータブル通信装置が何の企業ネットワークにアクセスしようとしているかを前記無線アクセスポイントで決定する手段と、
前記ポータブル通信装置との無線通信リンクを生成するために無線アクセス認証プロトコルを使用して、前記無線アクセスポイントで前記ポータブル通信装置を認証する手段と、
前記ポータブル通信装置によりアクセスされる前記企業ネットワークへの仮想プライベートネットワーク接続を確立し、前記ポータブル通信装置と前記企業ネットワークとの間で前記アクセスポイントを介して接続を提供する手段と、
前記無線通信リンクと仮想プライベート通信接続とをブリッジする手段と
を有する装置。
【請求項８】
請求項７に記載の装置であって、
前記決定する手段は、
前記企業ネットワークにアクセスしようとする前記ポータブル通信装置からネットワーク識別情報を受信する手段と、
前記ネットワーク識別情報から前記企業ネットワークを特定する手段と
を更に有する装置。
【請求項９】
請求項７に記載の装置であって、
前記決定する手段は、
前記企業ネットワークにアクセスしようとする前記ポータブル通信装置からネットワーク識別情報を受信する手段と、
前記ネットワーク識別情報から前記企業ネットワークを特定する手段と
を更に有する装置。
【発明の詳細な説明】
【技術分野】
【０００１】
この出願は、２００４年５月１７日に出願された米国仮特許出願第６０／５７１７４２号の３５Ｕ．Ｓ．Ｃ．１１９（ｅ）の優先権を主張する。この内容が取り込まれる。
【０００２】
本発明は無線装置とネットワークとの間の安全な接続を管理する技術に関する。
【背景技術】
【０００３】
多くの人は、日々の仕事で１つ以上のポータブル通信装置をますます利用している。このようなポータブル装置は、ラップトップコンピュータと、携帯情報端末（ＰＤＡ）と、無線電話とを有する。これらのポータブル通信装置は、無線接続を介して通信ネットワークにアクセスする機能を提供する。無線電話及びいくつかの形式のＰＤＡは、ユーザが公衆無線電話ネットワークにアクセスすることを可能にする。典型的には、今日の公衆無線電話ネットワークは、ＴＤＭＡ（Ｔｉｍｅ Ｄｉｖｉｓｉｏｎ Ｍｕｌｔｉｐｌｅ Ａｃｃｅｓｓ）、ＣＤＭＡ（Ｃｏｄｅ Ｄｉｖｉｓｉｏｎ Ｍｕｌｔｉｐｌｅ Ａｃｃｅｓｓ）、ＧＳＭ（Ｇｌｏｂａｌ Ｓｔａｎｄａｒｄ ｆｏｒ Ｍｏｂｉｌｅ）及び第３世代セルラ電話標準のような複数の周知の無線標準のうち１つを利用する。多数のラップトップコンピュータは、ＩＥＥＥ８０２．１１ｉ標準を利用する公衆ネットワークを通じて無線接続を提供する。多数のユーザにとって、公衆無線ネットワークへのアクセスは、企業ネットワーク（通信の対象の宛先）への次のアクセスを可能にする。

【０００４】
これまでは、ほとんどの企業ネットワークは、ユーザのアクセスを可能にするために、１つ以上の公衆ネットワークとの専用回線接続に依存している。専用回線接続は高いセキュリティを提供するが、高いコストになる。インターネットの出現で、現在では公衆ネットワークは、公衆ネットワーク内で仮想プライベートネットワーク（ＶＰＮ：Ｖｉｒｔｕａｌ　Ｐｒｉｖａｔｅ　Ｎｅｔｗｏｒｋ）を生成する機能を企業ネットワークのオペレータに提供している。このようなＶＰＮは、プライベート専用回線ネットワークの相当物をシミュレートするために仮想接続を使用するが、低減したコストで行う。
【０００５】
所定の公衆ネットワーク内では、複数のＶＰＮは共通の通信パスを共有することができる。従って、意図しない受信者が特定の企業ネットワーク宛へのデータにアクセスすることができないことを確保するために、セキュリティが重要になる。様々なセキュリティ技術がＶＰＮネットワークに存在する。このような技術は、対称鍵及び公衆鍵暗号化を含み、しばしば異なる暗号化技術を利用する。いくつかのＶＰＮは、ＩＰＳＥＣ（Ｉｎｔｅｒｎｅｔ　Ｐｒｏｔｏｃｏｌ　Ｓｅｃｕｒｉｔｙ　Ｐｒｏｔｏｃｏｌ）を利用する。ポータブル通信装置がＶＰＮを介して企業ネットワークへのエンド・ツー・エンド接続を確立することを可能にするために、通信装置はＶＰＮクライアントを有さなければならない。ＶＰＮクライアントは、様々なセキュリティプロトコルを実装するために必要なハードウェア及び／又はソフトウェアの形式を取る。ラップトップコンピュータのようないくつかのポータブル通信装置はＶＰＮクライアントを組み込む機能を有するが、無線電話及びＰＤＡのような多数の小型装置は有さない。従って、このような小型ポータブル通信装置は、ＶＰＮを通じて企業ネットワークへの接続を容易に確立することができない。
【発明の開示】
【発明が解決しようとする課題】
【０００６】
従って、ポータブル通信装置がＶＰＮを通じて少なくとも部分的に企業ネットワークと接続を確立することを可能にする技術についてのニーズが存在する。
【課題を解決するための手段】
【０００７】
要約すれば、本発明の好ましい実施例によれば、ポータブル通信装置と企業ネットワークとの間で接続を確立する方法が提供される。この方法は、企業ネットワークへのアクセスのためにポータブル通信装置による要求の無線アクセスポイントでの受信で開始する。アクセス要求に応じて、無線アクセスポイントは、ポータブル通信装置がアクセスしようとする企業ネットワークの識別情報を決定する。無線アクセスポイントは、無線認証プロトコルを使用してポータブル通信装置を認証する。ポータブル通信装置の認証の成功時に、無線アクセスポイントは、特定された企業ネットワークと仮想プライベートネットワークを確立し、ポータブル通信装置と企業ネットワークとの間の通信を促進する。このように、無線アクセスポイントは、ポータブル装置とアクセスポイントとの間で無線ＬＡＮセキュリティ機構を利用して接続を確立し、アクセスポイントと企業ネットワークとの間でＶＰＮ接続を確立する。
【発明を実施するための最良の形態】
【０００８】
ポータブル通信装置でＶＰＮクライアントの必要なく、ＶＰＮを通じて部分的にポータブル通信装置と企業ネットワークとの間で通信を促進するための本発明の技術を最も良く理解するために、従来技術の簡単な説明が有用になる。
【０００９】
図１は、ポータブル通信装置１２（ラップトップコンピュータ、無線電話又はＰＤＡ等）が仮想プライベートネットワーク（ＶＰＮ）１６を介して企業ネットワーク１４とエンド・ツー・エンド通信リンクを確立する従来技術の通信ネットワーク１０のブロック概略図を示している。ＶＰＮ１６は、公衆ネットワーク１８及び無線アクセスポイント２０を

通じて企業ネットワーク１４とポータブル通信装置１２との間に広がる。単一のエンティティとして図示されているが、無線アクセスポイント２０は、無線ネットワークの一部を有してもよい（図示せず）。図示の実施例では、企業ネットワーク１４は、ローカルエリアネットワーク２４に結合された企業ゲートウェイサーバ２０を有する。

【００１０】

ポータブル通信装置１２がＶＰＮ１６を通じて企業ネットワーク１４とエンド・ツー・エンド通信リンクを確立するために、ポータブル通信装置１２は、ＶＰＮクライアント２６を有さなければならない。ＶＰＮクライアント２６は、１つ以上のプログラム及び関連データの形式を取り、場合によってはポータブル通信装置１２が適用可能なセキュリティプロトコルを考慮してＶＰＮ１６とインタフェース接続することを可能にする１つ以上のハードウェア要素（図示）の形式を取る。ラップトップコンピュータのようないくつかの通信装置はＶＰＮクライアント２２を組み込む機能を有するが、無線電話装置のように小さいリソースを有する他のポータブル通信装置はこのような機能を有さない。従って、限られたリソースを有するポータブル通信装置は、ＶＰＮ１６を通じて企業ネットワーク１４と通信リンクを確立する機能を欠いている。

【００１１】

図２は、装置１２ａ及び１２ｂのようなポータブル通信装置が仮想プライベートネットワーク（ＶＰＮ）１６を通じて少なくとも部分的に企業ネットワーク１４と通信を確立するための本発明の好ましい実施例による通信ネットワーク１００のブロック概略図を示している。図２のネットワーク１００は、図１のネットワーク１０と同じ多数の要素を有するため、同じ数字は同じ要素を示す。

【００１２】

図２のネットワーク１００は、１つの重要な点で図１のネットワーク１０と異なる。ポータブル通信装置１２がＶＰＮクライアント２６を有する図１のネットワーク１０と異なり、図２のネットワーク１００のポータブル通信装置１２ａ及び１２ｂはＶＰＮクライアントを有さない。図１のようにＶＰＮ１６を通じて企業ネットワーク１４とエンド・ツー・エンド通信リンクを確立するのではなく、まず、各ポータブル通信装置１２ａ及び１２ｂは、複数の周知の無線通信プロトコルのうち１つを使用して、無線アクセスポイント２０と通信リンクを確立する。従って、例えばポータブル通信装置１２ａ及び１２ｂの一方が無線電話又はＰＤＡを有する場合、その装置と無線アクセスポイント２０との間の通信は、典型的には複数の周知の無線電話通信プロトコル（ＣＤＭＡ、ＴＤＭＡ、ＧＳＭ、３Ｇ等）のうちいずれかを使用して生じる。構成に応じて、ポータブル通信装置１２ａ及び１２ｂのうち一方又は双方は、ＩＥＥＥ８０２．１１ｉプロトコルを使用して無線アクセスポイント２０と通信してもよい。これらの前述のもの以外の無線プロトコルを介した通信が生じてもよい。

【００１３】

ポータブル通信装置１２ａ及び１２ｂの１つが無線アクセスポイント２０と通信リンクを確立すると、無線アクセスポイントは、ポータブル通信装置が認証を可能にするためにアクセスしようとする企業ネットワークを特定しようとする。無線アクセスポイント２０は、２つの方法のうち少なくとも一方で企業ネットワーク１４を特定する。例えば、ポータブル通信装置のユーザに関連する証明書が企業ネットワーク１４を特定してもよい。例えば、ユーザの証明書はユーザ名（すなわちｂｏｂ＠ｔｈｏｍｓｏｎ．ｎｅｔ）を有し、ユーザ名のドメイン部分が企業ネットワークを特定する。ユーザはまた、アクセスしようとする企業ネットワーク１４を具体的に特定してもよい。

【００１４】

無線アクセスポイント２０は、ユーザの証明書を確認することができる企業ネットワーク１４に問い合わせることにより、ポータブル通信装置のユーザを認証する。このような認証は、無線アクセスポイント２０とポータブル通信装置との間でＩＥＥＥ８０２．１１ｉ通信プロトコルを使用して生じてもよい。無線アクセスポイント２０と企業ネットワーク１４との間で、ＲＡＤＩＵＳ通信プロトコルが使用されてもよい。認証の成功時に、無

線アクセスポイント２０は、無線ＬＡＮセキュリティ機構（例えばＴＫＩＰ（Ｔｅｍｐｏｒａｌ Ｋｅｙ Ｉｎｔｅｇｒｉｔｙ ｐｒｏｔｏｃｏｌ）、ＷＰＡ（Ｗｉ－Ｆｉ Ｐｒｏｔｅｃｔｅｄ Ａｃｃｅｓｓ）又はＡＥＳ（Ａｄｖａｎｃｅｄ Ｅｎｃｒｙｐｔｉｏｎ ｓｔａｎｄａｒｄ））を使用してポータブル通信装置１２ａ及び１２ｂのうち１つと安全なセッションを構築する。

【００１５】

無線アクセスポイント２０はまた、ＩＰＳＥＣ等を通じた通常のＶＰＮモデルを使用して、ポータブル通信装置の代わりに自分と企業ネットワーク１４との間でＶＰＮを構築する。無線アクセスポイント２０は、これらの２つの安全な接続をブリッジし、ポータブル装置と企業ネットワートの間でエンド・ツー・エンド接続を構築する。無線アクセスポイント２０と企業ネットワーク１４との間のＶＰＮ接続は、単一のＶＰＮセッションとして予め構築されてもよい点に留意すべきである。無線アクセスポイント２０は、企業ネットワーク１４の信頼を有していなければならないため、中間のネットワークが信頼を受ける必要のない図１のエンド・ツー・エンドＶＰＮの対策に比べて更なるレベルの複雑性を導入する。

【００１６】

前記では、ポータブル通信装置がＶＰＮクライアントを有する必要なく、通信装置が企業ネットワークと確立することを可能にする技術について説明した。

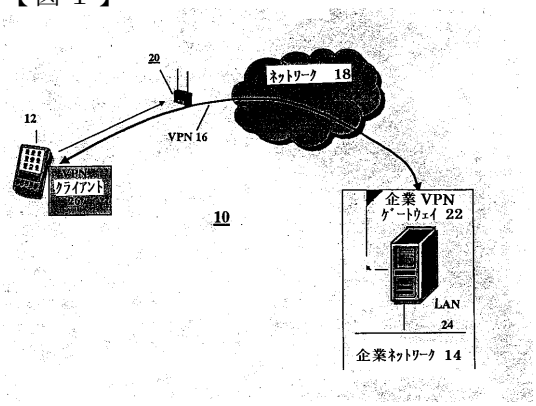
【図面の簡単な説明】

【００１７】

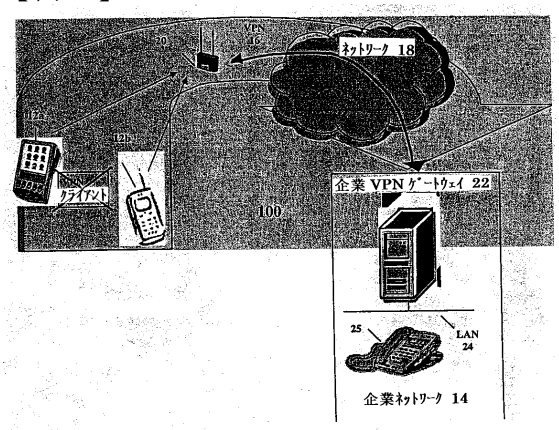
【図１】ポータブル通信装置がエンド・ツー・エンドＶＰＮ接続を通じて企業ネットワークと通信するＶＰＮクライアントを有する場合の従来技術による無線ネットワークのブロック概略図

【図２】ポータブル通信装置がＶＰＮクライアントを有する必要なく、ポータブル通信装置がＶＰＮ接続を通じて部分的に企業ネットワークと通信する場合の本発明による無線ネットワークのブロック概略図

【図１】



【図２】



【手続補正書】
【提出日】平成18年1月12日(2006.1.12)
【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】
仮想プライベートネットワーク（VPN）クライアントのないポータブル通信装置と企業ネットワークとの間で接続を確立する方法であって、
ポータブル通信装置から企業ネットワークにアクセスする要求を無線アクセスポイントで受信するステップと、
前記ポータブル通信装置が何の企業ネットワークにアクセスしようとしているかを前記無線アクセスポイントで決定するステップと、
前記ポータブル通信装置との無線通信リンクを生成するために無線アクセス認証プロトコルを使用して、前記無線アクセスポイントで前記VPNクライアントのないポータブル通信装置を認証するステップと、
前記VPNクライアントのないポータブル通信装置によりアクセスされる前記企業ネットワークへの仮想プライベートネットワーク接続を確立し、前記ポータブル通信装置と前記企業ネットワークとの間で前記アクセスポイントを介して接続を提供するステップと、
前記無線通信リンクと仮想プライベート通信接続とをブリッジするステップと
を有する方法。
【請求項２】
請求項１に記載の方法であって、

前記決定するステップは、
前記企業ネットワークにアクセスしようとする前記ポータブル通信装置から識別証明書を受信するステップと、
前記識別証明書から前記企業ネットワークを特定するステップと
を更に有する方法。
【請求項３】
請求項１に記載の方法であって、
前記決定するステップは、
前記企業ネットワークにアクセスしようとする前記ポータブル通信装置からネットワーク識別情報を受信するステップと、
前記ネットワーク識別情報から前記企業ネットワークを特定するステップと
を更に有する方法。
【請求項４】
請求項１に記載の方法であって、
前記認証するステップは、前記企業ネットワークに問い合わせて、前記ポータブル通信装置の証明書を確認するステップを更に有する方法。
【請求項５】
請求項１に記載の方法であって、
前記認証するステップは、temporal key integrity protocol、wi-fi protected Access protocol又はadvanced encryption standard protocolのうち１つを使用して、前記ポータブル通信装置を認証することを更に有する方法。
【請求項６】
仮想プライベートネットワーク（VPN）クライアントのないポータブル通信装置が企業ネットワークにアクセスするように動作する方法であって、
無線アクセスポイントにより受信するためのアクセス要求を前記ポータブル通信装置から送信するステップと、
前記無線アクセスポイントにより受信するためにアクセスされる前記企業ネットワークの識別情報の指示を前記ポータブル通信装置により供給するステップと、
前記VPNクライアントのないポータブル通信装置から前記無線アクセスポイントに認証情報を提供し、前記無線アクセスポイントが前記ポータブル通信装置と無線通信リンクを確立することを可能にし、前記無線アクセスポイントが前記企業ネットワークとVPN接続を確立することを可能にし、これによって、無線アクセスポイントが前記VPN接続と無線通信リンクとをブリッジすることができるステップと
を有する方法。
【請求項７】
仮想プライベートネットワーク（VPN）クライアントのないポータブル通信装置と企業ネットワークとの間で接続を確立する装置であって、
ポータブル通信装置から企業ネットワークにアクセスする要求を無線アクセスポイントで受信する手段と
前記ポータブル通信装置が何の企業ネットワークにアクセスしようとしているかを前記無線アクセスポイントで決定する手段と、
前記ポータブル通信装置との無線通信リンクを生成するために無線アクセス認証プロトコルを使用して、前記無線アクセスポイントで前記VPNクライアントのないポータブル通信装置を認証する手段と、
前記VPNクライアントのないポータブル通信装置によりアクセスされる前記企業ネットワークへの仮想プライベートネットワーク接続を確立し、前記ポータブル通信装置と前記企業ネットワークとの間で前記アクセスポイントを介して接続を提供する手段と、
前記無線通信リンクと仮想プライベート通信接続とをブリッジする手段と
を有する装置。
【請求項８】

請求項７に記載の装置であって、
前記決定する手段は、
前記企業ネットワークにアクセスしようとする前記ポータブル通信装置からネットワーク識別情報を受信する手段と、
前記ネットワーク識別情報から前記企業ネットワークを特定する手段と
を更に有する装置。
【請求項９】
請求項７に記載の装置であって、
前記決定する手段は、
前記企業ネットワークにアクセスしようとする前記ポータブル通信装置からネットワーク識別情報を受信する手段と、
前記ネットワーク識別情報から前記企業ネットワークを特定する手段と
を更に有する装置。
【手続補正書】
【提出日】平成18年12月27日(2006.12.27)
【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】
ネットワーククライアントのないポータブル通信装置とネットワークとの間で接続を確立する方法であって、
ポータブル通信装置からネットワークにアクセスする要求を無線アクセスポイントで受信するステップと、
前記ポータブル通信装置が何のネットワークにアクセスしようとしているかを前記無線アクセスポイントで決定するステップと、
前記ポータブル通信装置との無線通信リンクを生成するために無線アクセス認証プロトコルを使用して、前記無線アクセスポイントで前記ネットワーククライアントのないポータブル通信装置を認証するステップと、
前記ネットワーククライアントのないポータブル通信装置によりアクセスされる前記ネットワークへの仮想プライベートネットワーク接続を確立し、前記ポータブル通信装置と前記ネットワークとの間で前記アクセスポイントを介して接続を提供するステップと、
前記無線通信リンクと仮想プライベート通信接続とをブリッジするステップと
を有する方法。
【請求項２】
請求項１に記載の方法であって、
前記決定するステップは、
前記ネットワークにアクセスしようとする前記ポータブル通信装置から識別証明書を受信するステップと、
前記識別証明書から前記ネットワークを特定するステップと
を更に有する方法。
【請求項３】
請求項１に記載の方法であって、
前記決定するステップは、
前記ネットワークにアクセスしようとする前記ポータブル通信装置からネットワーク識別情報を受信するステップと、
前記ネットワーク識別情報から前記ネットワークを特定するステップと
を更に有する方法。

【請求項４】
請求項１に記載の方法であって、
前記認証するステップは、前記ネットワークに問い合わせて、前記ポータブル通信装置の証明書を確認するステップを更に有する方法。
【請求項５】
請求項１に記載の方法であって、
前記認証するステップは、temporal key integrity protocol、wi-fi protected Access protocol又はadvanced encryption standard protocolのうち１つを使用して、前記ポータブル通信装置を認証することを更に有する方法。
【請求項６】
ネットワーククライアントのないポータブル通信装置がネットワークにアクセスするように動作する方法であって、
無線アクセスポイントにより受信するためのアクセス要求を前記ポータブル通信装置から送信するステップと、
前記無線アクセスポイントにより受信するためにアクセスされる前記ネットワークの識別情報の指示を前記ポータブル通信装置により供給するステップと、
前記ネットワーククライアントのないポータブル通信装置から前記無線アクセスポイントに認証情報を提供し、前記無線アクセスポイントが前記ポータブル通信装置と無線通信リンクを確立することを可能にし、前記無線アクセスポイントが前記ネットワークとVPN接続を確立することを可能にし、これによって、無線アクセスポイントが前記VPN接続と無線通信リンクとをブリッジすることができるステップと
を有する方法。
【請求項７】
ネットワーククライアントのないポータブル通信装置とネットワークとの間で接続を確立する装置であって、
ポータブル通信装置からネットワークにアクセスする要求を無線アクセスポイントで受信する手段と
前記ポータブル通信装置が何のネットワークにアクセスしようとしているかを前記無線アクセスポイントで決定する手段と、
前記ポータブル通信装置との無線通信リンクを生成するために無線アクセス認証プロトコルを使用して、前記無線アクセスポイントで前記ネットワーククライアントのないポータブル通信装置を認証する手段と、
前記ネットワーククライアントのないポータブル通信装置によりアクセスされる前記ネットワークへの仮想プライベートネットワーク接続を確立し、前記ポータブル通信装置と前記ネットワークとの間で前記アクセスポイントを介して接続を提供する手段と、
前記無線通信リンクと仮想プライベート通信接続とをブリッジする手段と
を有する装置。
【請求項８】
請求項７に記載の装置であって、
前記決定する手段は、
前記ネットワークにアクセスしようとする前記ポータブル通信装置からネットワーク識別情報を受信する手段と、
前記ネットワーク識別情報から前記ネットワークを特定する手段と
を更に有する装置。
【請求項９】
請求項７に記載の装置であって、
前記決定する手段は、
前記ネットワークにアクセスしようとする前記ポータブル通信装置からネットワーク識別情報を受信する手段と、
前記ネットワーク識別情報から前記ネットワークを特定する手段と

を更に有する装置。

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US2005/016378

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L29/06 H04L12/56

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 03/029916 A (BLUESOCKET, INC) 10 April 2003 (2003-04-10) paragraph '0002! - paragraph '0073!; figure 1A	1-10
A	PAT R CALHOUN US ROBOTICS ACCESS CORP ELLIS WONG BAY NETWORKS ET AL: "Virtual Tunneling Protocol (VTP)" IETF STANDARD-WORKING-DRAFT, INTERNET ENGINEERING TASK FORCE, IETF, CH, July 1996 (1996-07), pages 1-62, XP015011451 ISSN: 0000-0004 paragraph '001.! - paragraph '002.!	1-10

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
8 August 2005	16/08/2005

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Günther, S

Form PCT/ISA/210 (second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US2005/016378

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2002/090089 A1 (BRANIGAN STEVEN ET AL) 11 July 2002 (2002-07-11) paragraph '0008! - paragraph '0024!; figure 3	1-10
A	WO 02/17558 A (ETUNNELS INC; MEHARG, GERSHAM; POIER, M., SKYE; PANKRATOV, ALEXENDRE) 28 February 2002 (2002-02-28) page 4, line 1 - page 13, line 27; figures 2,4	1-10
A	FEIL H ED - INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS: "802.11 wireless network policy recommendation for usage within unclassified government networks" 2003 IEEE MILITARY COMMUNICATIONS CONFERENCE. MILCOM 2003. BOSTON, MA, OCT. 13 - 16, 2003, IEEE MILITARY COMMUNICATIONS CONFERENCE, NEW YORK, NY : IEEE, US, vol. VOL. 2 OF 2, 13 October 2003 (2003-10-13), pages 832-838, XP010698595 ISBN: 0-7803-8140-8 paragraph '2.2.! - paragraph '5.4.!; tables 5-1	1-10
A	WO 03/007561 A (SSH COMMUNICATIONS SECURITY CORP; YLOENEN, TATU) 23 January 2003 (2003-01-23) page 3, line 11 - page 7, line 23; figure 1	1-10

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/US2005/016378

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 03029916 A	10-04-2003	WO 03029916 A2	10-04-2003
		US 2003087629 A1	08-05-2003
US 2002090089 A1	11-07-2002	JP 2002281045 A	27-09-2002
WO 0217558 A	28-02-2002	AU 8162201 A	04-03-2002
		WO 0217558 A2	28-02-2002
		US 2002124090 A1	05-09-2002
		CA 2323221 A1	18-02-2002
WO 03007561 A	23-01-2003	WO 03007561 A1	23-01-2003

Form PCT/ISA/210 (patent family annex) (January 2004)

フロントページの続き

(81)指定国 AP(BW,GH,GM,KE,LS,MW,MZ,NA,SD,SL,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,MD,RU,TJ,TM),EP(AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HU,IE,IS,IT,LT,LU,MC,NL,PL,PT,RO,SE,SI,SK,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AT,AU,AZ,BA,BB,BG,BR,BW,BY,BZ,CA,CH,CN,CO,CR,CU,CZ,DE,DK,DM,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,HR,HU,ID,IL,IN,IS,JP,KE,KG,KM,KP,KR,KZ,LC,LK,LR,LS,LT,LU,LV,MA,MD,MG,MK,MN,MW,MX,MZ,NA,NG,NI,NO,NZ,OM,PG,PH,PL,PT,RO,RU,SC,SD,SE,SG,SK,SL,SM,SY,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC,VN,YU,ZA,ZM,ZW

(74)代理人 100135105
弁理士 渡邊 直満
(72)発明者 ジェルラン，オリヴィエ
フランス国，７８５９０ ノワシー－ル－ロワ，シュマン・デ・ノワイエ，１２－２
(72)発明者 ジャン，ジュンビアオ
アメリカ合衆国，ニュージャージー州 ０８８０７，ブリッジウォーター，ジェンナ・ドライヴ ２０
(72)発明者 ラマスワミー，クマール
アメリカ合衆国，ニュージャージー州 ０８５４０，プリンストン，セイアー・ドライヴ ７１

Ｆターム(参考) 5K030 GA15 HA08 HB11 HC01 HC09 HD03 HD06 JL01 JT09 KA04
KA05 KA06 LB01 LD19 MD07
5K067 AA33 BB21 DD34 EE02 EE10 EE16 HH17 HH24