(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第3955025号
(P3955025)
(45)発行日　平成19年8月8日(2007.8.8)　(24)登録日　平成19年5月11日(2007.5.11)

(51)Int.Cl.		F I		
H04L 12/66	(2006.01)	H04L	12/66	B
H04L 12/56	(2006.01)	H04L	12/56	H
H04Q 7/22	(2006.01)	H04Q	7/04	A
H04Q 7/24	(2006.01)	H04B	7/26	109R
H04Q 7/26	(2006.01)			

請求項の数 13　(全 22 頁)　最終頁に続く

(21)出願番号　特願2004-8507(P2004-8507)
(22)出願日　平成16年1月15日(2004.1.15)
(65)公開番号　特開2005-204086(P2005-204086A)
(43)公開日　平成17年7月28日(2005.7.28)
審査請求日　平成17年2月17日(2005.2.17)

(73)特許権者　000005821
松下電器産業株式会社
大阪府門真市大字門真１００６番地
(74)代理人　100105050
弁理士　鷲田　公一
(72)発明者　岩間　智大
神奈川県横浜市港北区綱島東四丁目３番１号　パナソニックモバイルコミュニケーションズ株式会社内
(72)発明者　金子　友晴
神奈川県横浜市港北区綱島東四丁目３番１号　パナソニックモバイルコミュニケーションズ株式会社内

最終頁に続く

(54)【発明の名称】移動無線端末装置、仮想私設網中継装置及び接続認証サーバ

(57)【特許請求の範囲】

【請求項１】

公衆網と私設網と公衆無線ＬＡＮシステムとを具備し、前記公衆網を介して前記私設網に設置された網中継装置とＩＰsecトンネルを確立し移動無線端末装置との間でＩＰsecトンネルを確立して前記移動無線端末装置の前記公衆無線ＬＡＮシステムから前記私設網への接続を中継する仮想私設網中継装置と、前記公衆無線ＬＡＮシステムに設置され前記移動無線端末装置の前記公衆無線ＬＡＮシステムへの接続を認証する接続認証サーバと、前記移動無線端末装置と前記接続認証サーバとの間で行われる公衆無線ＬＡＮの接続認証手順を中継する無線ＬＡＮアクセスポイントと、を具備する移動無線通信システムにおける移動無線端末装置であって、

前記接続認証サーバに対して前記公衆無線ＬＡＮシステムへの接続認証処理を行う認証処理部と、前記公衆無線ＬＡＮシステムへの接続が許可された時に前記接続認証サーバから前記仮想私設網中継装置のＩＰアドレスを取得するアドレス取得部と、前記移動無線端末装置のＩＰアドレスを前記接続認証サーバに通知するアドレス通知部と、前記仮想私設網中継装置のＩＰアドレスを用いて前記仮想私設網中継装置とＩＰsec鍵交換を行うＩＰsec鍵交換部と、を具備する移動無線端末装置。

【請求項２】

公衆網と私設網と公衆無線ＬＡＮシステムとを具備し、前記公衆網を介して前記私設網に設置された網中継装置とＩＰsecトンネルを確立し移動無線端末装置との間でＩＰsecトンネルを確立して前記移動無線端末装置の前記公衆無線ＬＡＮシステムから前記私設網へ

の接続を中継する仮想私設網中継装置と、前記公衆無線ＬＡＮシステムに設置され前記移動無線端末装置の前記公衆無線ＬＡＮシステムへの接続を認証する接続認証サーバと、前記移動無線端末装置と前記接続認証サーバとの間で行われる公衆無線ＬＡＮの接続認証手順を中継する無線ＬＡＮアクセスポイントと、を具備する移動無線通信システムにおける移動無線端末装置であって、

前記接続認証サーバに対して前記公衆無線ＬＡＮシステムへの接続認証処理を行う認証処理部と、前記公衆無線ＬＡＮシステムへの接続が許可された時に前記接続認証サーバから前記仮想私設網中継装置との間で行うＩＰsec鍵交換に用いるＩＰsec事前共有秘密鍵を取得するＩＰsec共有鍵取得部と、前記ＩＰsec事前共有秘密鍵を用いて前記仮想私設網中継装置とＩＰsec鍵交換を行うＩＰsec鍵交換部と、を具備する移動無線端末装置。

【請求項３】

公衆網と私設網と公衆無線ＬＡＮシステムとを具備し、前記公衆網を介して前記私設網に設置された網中継装置とＩＰsecトンネルを確立し移動無線端末装置との間でＩＰsecトンネルを確立して前記移動無線端末装置の前記公衆無線ＬＡＮシステムから前記私設網への接続を中継する仮想私設網中継装置と、前記移動無線端末装置の移動制御を行うホームエージェントと、前記公衆無線ＬＡＮシステムに設置され前記移動無線端末装置の前記公衆無線ＬＡＮシステムへの接続を認証する接続認証サーバと、前記移動無線端末装置と前記接続認証サーバとの間で行われる公衆無線ＬＡＮの接続認証手順を中継する無線ＬＡＮアクセスポイントと、を具備する移動無線通信システムにおける移動無線端末装置であって、

前記接続認証サーバに対して前記公衆無線ＬＡＮシステムへの接続認証処理を行う認証処理部と、前記公衆無線ＬＡＮシステムへの接続が許可された時に前記接続認証サーバから前記ホームエージェントとの間で行うモバイルＩＰ登録に用いる事前共有秘密鍵を取得するＭＩＰ共有鍵取得部と、前記事前共有秘密鍵を用いて前記ホームエージェントへモバイルＩＰ登録を行うＭＩＰ登録部と、を具備する移動無線端末装置。

【請求項４】

公衆網と私設網と公衆無線ＬＡＮシステムとを具備し、前記公衆網を介して前記私設網に設置された網中継装置とＩＰsecトンネルを確立し移動無線端末装置との間でＩＰsecトンネルを確立して前記移動無線端末装置の前記公衆無線ＬＡＮシステムから前記私設網への接続を中継する仮想私設網中継装置と、前記移動無線端末装置の移動制御を行うホームエージェントと、前記公衆無線ＬＡＮシステムに設置され前記移動無線端末装置の前記公衆無線ＬＡＮシステムへの接続を認証する接続認証サーバと、前記移動無線端末装置と前記接続認証サーバとの間で行われる公衆無線ＬＡＮの接続認証手順を中継する無線ＬＡＮアクセスポイントと、を具備する移動無線通信システムにおける移動無線端末装置であって、

前記接続認証サーバに対して前記公衆無線ＬＡＮシステムへの接続認証処理を行う認証処理部と、前記公衆無線ＬＡＮシステムへの接続が許可された時に前記接続認証サーバから前記仮想私設網中継装置のＩＰアドレスを取得するアドレス取得部と、前記移動無線端末装置のＩＰアドレスを前記接続認証サーバに通知するアドレス通知部と、前記接続認証サーバから前記仮想私設網中継装置との間で行うＩＰsec鍵交換に用いるＩＰsec事前共有秘密鍵を取得するＩＰsec共有鍵取得部と、前記接続認証サーバから前記ホームエージェントとの間で行うモバイルＩＰ登録に用いるＭＩＰ事前共有秘密鍵を取得するＭＩＰ共有鍵取得部と、前記仮想私設網中継装置のＩＰアドレスと前記ＩＰsec事前共有秘密鍵を用いて前記仮想私設網中継装置とＩＰsec鍵交換を行うＩＰsec鍵交換部と、前記ＭＩＰ事前共有秘密鍵を用いて前記ホームエージェントへモバイルＩＰ登録を行うＭＩＰ登録部と、を具備する移動無線端末装置。

【請求項５】

公衆網と私設網と公衆無線ＬＡＮシステムとを具備し、前記公衆網を介して前記私設網に設置された網中継装置とＩＰsecトンネルを確立し移動無線端末装置との間でＩＰsecトンネルを確立して前記移動無線端末装置の前記公衆無線ＬＡＮシステムから前記私設網へ

の接続を中継する仮想私設網中継装置と、前記公衆無線ＬＡＮシステムに設置され前記移動無線端末装置の前記公衆無線ＬＡＮシステムへの接続を認証する接続認証サーバと、前記移動無線端末装置と前記接続認証サーバとの間で行われる公衆無線ＬＡＮの接続認証手順を中継する無線ＬＡＮアクセスポイントと、を具備する移動無線通信システムにおける仮想私設網中継装置であって、

前記接続認証サーバから前記移動無線端末装置のＩＰアドレスを受信するアドレス取得部と、前記移動無線端末装置のＩＰアドレスを用いて前記移動無線端末装置とＩＰsec鍵交換を行うＩＰsec鍵交換部と、を具備する仮想私設網中継装置。

【請求項６】

公衆網と私設網と公衆無線ＬＡＮシステムとを具備し、前記公衆網を介して前記私設網に設置された網中継装置とＩＰsecトンネルを確立し移動無線端末装置との間でＩＰsecトンネルを確立して前記移動無線端末装置の前記公衆無線ＬＡＮシステムから前記私設網への接続を中継する仮想私設網中継装置と、前記公衆無線ＬＡＮシステムに設置され前記移動無線端末装置の前記公衆無線ＬＡＮシステムへの接続を認証する接続認証サーバと、前記移動無線端末装置と前記接続認証サーバとの間で行われる公衆無線ＬＡＮの接続認証手順を中継する無線ＬＡＮアクセスポイントと、を具備する移動無線通信システムにおける仮想私設網中継装置であって、

前記接続認証サーバから前記移動無線端末装置との間で行うＩＰsec鍵交換に用いる事前共有秘密鍵を受信するＩＰsec共有鍵取得部と、前記事前共有秘密鍵を用いて前記移動無線端末装置とＩＰsec鍵交換を行うＩＰsec鍵交換部と、を具備する仮想私設網中継装置。

【請求項７】

公衆網と私設網と公衆無線ＬＡＮシステムとを具備し、前記公衆網を介して前記私設網に設置された網中継装置とＩＰsecトンネルを確立し移動無線端末装置との間でＩＰsecトンネルを確立して前記移動無線端末装置の前記公衆無線ＬＡＮシステムから前記私設網への接続を中継する仮想私設網中継装置と、前記公衆無線ＬＡＮシステムに設置され前記移動無線端末装置の前記公衆無線ＬＡＮシステムへの接続を認証する接続認証サーバと、前記移動無線端末装置と前記接続認証サーバとの間で行われる公衆無線ＬＡＮの接続認証手順を中継する無線ＬＡＮアクセスポイントと、を具備する移動無線通信システムにおける仮想私設網中継装置であって、

前記接続認証サーバから前記移動無線端末装置のＩＰアドレスを受信するアドレス取得部と、前記接続認証サーバから前記移動無線端末装置との間で行うＩＰsec鍵交換に用いる事前共有秘密鍵を受信するＩＰsec共有鍵取得部と、前記移動無線端末装置のＩＰアドレスと前記事前共有秘密鍵を用いて前記移動無線端末装置とＩＰsec鍵交換を行うＩＰsec鍵交換部と、を具備する仮想私設網中継装置。

【請求項８】

公衆網と私設網と公衆無線ＬＡＮシステムとを具備し、前記公衆網を介して前記私設網に設置された網中継装置とＩＰsecトンネルを確立し移動無線端末装置との間でＩＰsecトンネルを確立して前記移動無線端末装置の前記公衆無線ＬＡＮシステムから前記私設網への接続を中継する仮想私設網中継装置と、前記公衆無線ＬＡＮシステムに設置され前記移動無線端末装置の前記公衆無線ＬＡＮシステムへの接続を認証する接続認証サーバと、前記移動無線端末装置と前記接続認証サーバとの間で行われる公衆無線ＬＡＮの接続認証手順を中継する無線ＬＡＮアクセスポイントと、を具備する移動無線通信システムにおける接続認証サーバであって、

前記移動無線端末装置の前記公衆無線ＬＡＮシステムへの接続認証を行う認証処理部と、前記移動無線端末装置の前記公衆無線ＬＡＮシステムへの接続を許可する時に前記移動無線端末装置のＩＰアドレスを前記移動無線端末装置から受信するアドレス取得部と、前記仮想私設網中継装置のＩＰアドレスを前記移動無線端末装置に通知し、かつ、前記移動無線端末装置のＩＰアドレスを前記仮想私設網中継装置に通知するアドレス通知部と、を具備する接続認証サーバ。

【請求項９】
公衆網と私設網と公衆無線ＬＡＮシステムとを具備し、前記公衆網を介して前記私設網に設置された網中継装置とＩＰsecトンネルを確立し移動無線端末装置との間でＩＰsecトンネルを確立して前記移動無線端末装置の前記公衆無線ＬＡＮシステムから前記私設網への接続を中継する仮想私設網中継装置と、前記公衆無線ＬＡＮシステムに設置され前記移動無線端末装置の前記公衆無線ＬＡＮシステムへの接続を認証する接続認証サーバと、前記移動無線端末装置と前記接続認証サーバとの間で行われる公衆無線ＬＡＮの接続認証手順を中継する無線ＬＡＮアクセスポイントと、を具備する移動無線通信システムにおける接続認証サーバであって、
前記移動無線端末装置の前記公衆無線ＬＡＮシステムへの接続認証を行う認証処理部と、前記移動無線端末装置の公衆無線ＬＡＮシステムへの接続を許可する時に前記移動無線端末装置と前記仮想私設網中継装置との間で行うＩＰsec鍵交換に用いる事前共有秘密鍵を前記移動無線端末装置と前記仮想私設網中継装置にそれぞれ配布するＩＰsec共有鍵配布部と、を具備する接続認証サーバ。
【請求項１０】
公衆網と私設網と公衆無線ＬＡＮシステムとを具備し、前記公衆網を介して前記私設網に設置された網中継装置とＩＰsecトンネルを確立し移動無線端末装置との間でＩＰsecトンネルを確立して前記移動無線端末装置の前記公衆無線ＬＡＮシステムから前記私設網への接続を中継する仮想私設網中継装置と、前記移動無線端末装置の移動制御を行うホームエージェントと、前記公衆無線ＬＡＮシステムに設置され前記移動無線端末装置の前記公衆無線ＬＡＮシステムへの接続を認証する接続認証サーバと、前記移動無線端末装置と前記接続認証サーバとの間で行われる公衆無線ＬＡＮの接続認証手順を中継する無線ＬＡＮアクセスポイントと、を具備する移動無線通信システムにおける接続認証サーバであって、
前記移動無線端末装置の前記公衆無線ＬＡＮシステムへの接続認証を行う認証処理部と、前記移動無線端末装置の公衆無線ＬＡＮシステムへの接続を許可する時に前記移動無線端末装置と前記ホームエージェントとの間で行うモバイルＩＰ登録に用いる事前共有秘密鍵を前記移動無線端末装置と前記ホームエージェントにそれぞれ配布するＭＩＰ共有鍵配布部と、を具備する接続認証サーバ。
【請求項１１】
公衆網と私設網と公衆無線ＬＡＮシステムとを具備し、前記公衆網を介して前記私設網に設置された網中継装置とＩＰsecトンネルを確立し移動無線端末装置との間でＩＰsecトンネルを確立して前記移動無線端末装置の前記公衆無線ＬＡＮシステムから前記私設網への接続を中継する仮想私設網中継装置と、前記移動無線端末装置の移動制御を行うホームエージェントと、前記公衆無線ＬＡＮシステムに設置され前記移動無線端末装置の前記公衆無線ＬＡＮシステムへの接続を認証する接続認証サーバと、前記移動無線端末装置と前記接続認証サーバとの間で行われる公衆無線ＬＡＮの接続認証手順を中継する無線ＬＡＮアクセスポイントと、を具備する移動無線通信システムにおける接続認証サーバであって、
前記移動無線端末装置の前記公衆無線ＬＡＮシステムへの接続認証を行う認証処理部と、前記移動無線端末装置の公衆無線ＬＡＮシステムへの接続を許可する時に前記移動無線端末装置のＩＰアドレスを前記移動無線端末装置から受信するアドレス取得部と、前記仮想私設網中継装置のＩＰアドレスを前記移動無線端末装置に通知し、かつ、前記移動無線端末装置のＩＰアドレスを前記仮想私設網中継装置に通知するアドレス通知部と、前記移動無線端末装置と前記仮想私設網中継装置との間で行うＩＰsec鍵交換に用いるＩＰsec事前共有秘密鍵を前記移動無線端末装置と前記仮想私設網中継装置にそれぞれ配布するＩＰsec共有鍵配布部と、前記移動無線端末装置と前記ホームエージェントとの間で行うモバイルＩＰ登録に用いるＭＩＰ事前共有秘密鍵を前記移動無線端末装置と前記ホームエージェントにそれぞれ配布するＭＩＰ共有鍵配布部と、を具備する接続認証サーバ。
【請求項１２】

公衆網と私設網と公衆無線ＬＡＮシステムとを具備し、前記公衆網を介して前記私設網に設置された網中継装置とＩＰsecトンネルを確立し移動無線端末装置との間でＩＰsecトンネルを確立して前記移動無線端末装置の前記公衆無線ＬＡＮシステムから前記私設網への接続を中継する仮想私設網中継装置と、前記移動無線端末装置の移動制御を行うホームエージェントと、前記公衆無線ＬＡＮシステムに設置され前記移動無線端末装置の前記公衆無線ＬＡＮシステムへの接続を認証する接続認証サーバと、前記移動無線端末装置と前記接続認証サーバとの間で行われる公衆無線ＬＡＮの接続認証手順を中継する無線ＬＡＮアクセスポイントと、を具備する移動無線通信システムにおける無線ＬＡＮアクセスポイントであって、

前記移動無線端末装置と前記接続認証サーバとの間で行われる公衆無線ＬＡＮの接続認証手順において確立した安全な通信路を用いて、前記接続認証サーバから送信されるＩＰアドレスとＩＰsec事前共有鍵、Mobile ＩＰ事前共有鍵を前記移動無線端末装置に送信し、かつ、前記移動無線端末装置から送信されるＩＰアドレスを前記接続認証サーバへ送信する認証中継部と、を具備する無線ＬＡＮアクセスポイント。

【請求項１３】

公衆網と私設網と公衆無線ＬＡＮシステムとを具備し、前記公衆網を介して前記私設網に設置された網中継装置とＩＰsecトンネルを確立し移動無線端末装置との間でＩＰsecトンネルを確立して前記移動無線端末装置の前記公衆無線ＬＡＮシステムから前記私設網への接続を中継する仮想私設網中継装置と、前記移動無線端末装置の移動制御を行うホームエージェントと、前記公衆無線ＬＡＮシステムに設置され前記移動無線端末装置の前記公衆無線ＬＡＮシステムへの接続を認証する接続認証サーバと、前記移動無線端末装置と前記接続認証サーバとの間で行われる公衆無線ＬＡＮの接続認証手順を中継する無線ＬＡＮアクセスポイントと、を具備する移動無線通信システムにおけるホームエージェントであって、

前記接続認証サーバから前記移動無線端末装置のモバイルＩＰ登録に用いる事前共有秘密鍵を受信するＭＩＰ共有鍵取得部と、前記事前共有秘密鍵を用いて前記移動無線端末装置からのモバイルＩＰ登録を処理するＭＩＰ処理部と、を具備するホームエージェント。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、公衆無線ＬＡＮシステムなどの公衆網から私設網へアクセスするようなモバイルＶＰＮ接続環境において、セキュリティの高い通信路を確立するための移動無線端末装置、仮想私設網中継装置及び接続認証サーバに関する。

【背景技術】

【０００２】

公衆網から私設網への接続において、セキュアな通信路を確立するためにＩＰsec技術がＩＥＴＦにより標準化されている。ＩＰv6では、このＩＰsec技術をサポートすることが必須とされている。移動無線端末装置が公衆網と私設網を自由に移動可能なモバイル環境にＩＰsecを適用し、移動無線端末装置が公衆網から私設網へ接続することを想定する。この場合、移動無線端末装置は移動先の公衆網で使用可能なＩＰアドレスが移動の度にＤＨＣＰ（Dynamic Host Configuration Protocol）などにより割り当てられる。即ち、移動無線端末装置の移動先によりＩＰアドレスが変化することになる。

【０００３】

このため、私設網に設置されたＩＰsecトンネルの確立先であるセキュリティゲートウェイでは、各移動先でのＩＰアドレスが既知である必要があるため、移動無線端末装置のＩＰアドレスを用いたＩＰsec鍵交換を実施することが困難となるから、メインモードによるＩＰsecトンネルの確立が事実上不可能となる。従って、アグレッシブモードによるＩＰsecトンネルの確立が必要となるため、ＩＰsecユーザＩＤ（ＩＳＡＫＡＭＰＩＤペイロード）がネットワークを暗号化されない状態で流れることになるから、セキュリティの低下を招く。

【０００４】
また、ＩＰsecでは、ＩＰsecトンネルを確立する双方において相互認証を行うための事前共有秘密鍵方式をサポートすることが必須となっている。しかし、一つの事前共有秘密鍵を使用し続けることによるセキュリティの低下が懸念される。そこで、事前共有秘密鍵を定期に変更しセキュリティを保つことが考えられるが、ユーザ及び管理者の双方の負担が大きくなる。
【０００５】
これまで、ＩＰsecの認証に用いる事前共有秘密鍵を動的に配布するためのプロトコルとして、ＩＥＴＦ（Internet Engineering Task Force）においてＰＩＣ（Pre-IKE Credential Provisioning Protocol）が提案されている（非特許文献１参照）。
【０００６】
ＰＩＣは、ＩＰsecでも利用されているＩＳＡＫＭＰ（Internet Security Association and Key Management Protocol）を用いて移動無線端末装置と認証サーバとの間に安全な通信路を確立し、ＰＩＣにおける認証に必要とされる認証情報を交換して認証を行う。この認証が成功すると、認証サーバはクレデンシャルと呼ばれるその後のＩＰsecの認証で利用する認証情報（例えば、事前共有秘密鍵及び公開鍵証明書）を移動無線端末装置に発行する。
【非特許文献１】“PIC, A Pre-IKE Credential Provisioning Protocol”、draft-ietf-ipsra-pic-06.txt、http://www.ietf.org/internet-drafts/draft-ietf-ipsra-pic-06.txt
【発明の開示】
【発明が解決しようとする課題】
【０００７】
移動無線端末装置が公衆無線ＬＡＮシステムなどの公衆網おいて、社内ネットワークなどの私設網に接続する場合に、移動無線端末装置はＩＰsecを用いて私設網とセキュアな通信路、即ちＩＰsecトンネルを確立することが考えられる。
【０００８】
しかし、この場合に、移動無線端末装置が公衆網と私設網を自由に移動可能なモバイル環境にＩＰsecを適用した場合には、移動無線端末装置のＩＰアドレスが移動の度に変化するため、ＩＰsecメインモードによるＩＰsec鍵交換が困難である。このため、アグレッシブモードのＩＰsec鍵交換によるトンネルの確立が余儀なくされ、ＩＰsecユーザＩＤがネットワークを暗号化されない状態で流れることとなりセキュリティの低下を招くことになるという問題がある。
【０００９】
また、ＩＰsecメインモードの鍵交換によるトンネルを確立するためには、移動無線端末装置の移動先でのＩＰアドレスが既知である必要がある。しかし、公衆無線ＬＡＮシステムなどの公衆網においてはＤＨＣＰによりＩＰアドレスが割り当てられることが多いため、移動無線端末装置のＩＰアドレスを予め知ることは難しい。仮に移動無線端末装置の公衆無線ＬＡＮシステムにおけるＩＰアドレスが既知である場合でも、公衆無線ＬＡＮシステムにおける各ＩＰアドレスに対してセキュリティポリシーを記述しておく必要があるため、セキュリティゲートウェイの性能が劣化し、また、管理者の管理の負担となるという問題がある。
【００１０】
また、ＩＰsecトンネルを確立する際の相互認証方式として、事前共有秘密鍵方式を適用した場合に、一つの事前共有鍵を使用し続けることは、時間と共にセキュリティが低下していくという問題がある。さらに、定期的に事前共有鍵を変更することが考えられるが、この場合には利用者と管理者の双方の負担となるという問題がある。
【００１１】
前記問題を解決するために、ＩＰsecの認証に用いる事前共有秘密鍵を動的に配布するプロトコルとしてＰＩＣが提案されている。しかし、ＰＩＣを利用するためには、既存の

装置にＰＩＣプロトコル機能を新たに追加する必要があるという問題がある。さらに、ＩＰsecトンネル確立手順にＰＩＣを適用した場合に、ＰＩＣによる移動無線端末装置と接続認証サーバとの間でＩＳＡＫＭＰ通信路の確立と、移動無線端末装置とセキュリティゲートウェイとの間でのＩＳＡＫＭＰ通信路の確立という移動無線端末装置にとって２度のＩＳＡＫＭＰによる通信路を確立することになるため、手順が冗長であるから、ＩＰsecトンネルの確立に要する時間が長くなるという問題がある。

【００１２】

本発明は、かかる点に鑑みてなされたものであり、セキュリティの低下を防ぐことができ、ユーザ及び管理者の特別な作業を必要とせず、かつ、モバイルＶＰＮ接続環境におけるＩＰsecトンネルの確立に要する時間を短縮することができる移動無線端末装置、仮想私設網中継装置及び接続認証サーバを提供することを目的とする。

【課題を解決するための手段】

【００１５】

本発明の移動無線端末装置は、公衆網と私設網と公衆無線ＬＡＮシステムとを具備し、前記公衆網を介して前記私設網に設置された網中継装置とＩＰsecトンネルを確立し移動無線端末装置との間でＩＰsecトンネルを確立して前記移動無線端末装置の前記公衆無線ＬＡＮシステムから前記私設網への接続を中継する仮想私設網中継装置と、前記公衆無線ＬＡＮシステムに設置され前記移動無線端末装置の前記公衆無線ＬＡＮシステムへの接続を認証する接続認証サーバと、前記移動無線端末装置と前記接続認証サーバとの間で行われる公衆無線ＬＡＮの接続認証手順を中継する無線ＬＡＮアクセスポイントと、を具備する移動無線通信システムにおける移動無線端末装置であって、前記接続認証サーバに対して前記公衆無線ＬＡＮシステムへの接続認証処理を行う認証処理部と、前記公衆無線ＬＡＮシステムへの接続が許可された時に前記接続認証サーバから前記仮想私設網中継装置のＩＰアドレスを取得するアドレス取得部と、前記移動無線端末装置のＩＰアドレスを前記接続認証サーバに通知するアドレス通知部と、前記仮想私設網中継装置のＩＰアドレスを用いて前記仮想私設網中継装置とＩＰsec鍵交換を行うＩＰsec鍵交換部と、を具備する構成を採る。

【００１６】

この構成によれば、移動無線端末装置は仮想私設網中継装置のＩＰアドレスを取得することができ、かつ、仮想私設網中継装置は移動無線端末装置のＩＰアドレスを取得することができるため、移動無線端末装置と仮想私設網中継装置とはそれぞれのＩＰアドレスを用いてＩＰsecメインモードによる鍵交換を開始することができるから、セキュリティの低下を防ぐことができ、かつ、ユーザ及び管理者の特別な作業を必要としない。また、この構成によれば、移動無線端末装置と接続認証サーバにおいて接続認証手順により確立されたセキュアな通信路を用いてＩＰアドレスを送信することにより、ＩＰアドレスを配布するためのセキュアな通信路を改めて確立する必要がないため、モバイルＶＰＮ接続環境におけるＩＰsecトンネルの確立に要する時間を短縮することができる。

【００１７】

本発明の移動無線端末装置は、公衆網と私設網と公衆無線ＬＡＮシステムとを具備し、前記公衆網を介して前記私設網に設置された網中継装置とＩＰsecトンネルを確立し移動無線端末装置との間でＩＰsecトンネルを確立して前記移動無線端末装置の前記公衆無線ＬＡＮシステムから前記私設網への接続を中継する仮想私設網中継装置と、前記公衆無線ＬＡＮシステムに設置され前記移動無線端末装置の前記公衆無線ＬＡＮシステムへの接続を認証する接続認証サーバと、前記移動無線端末装置と前記接続認証サーバとの間で行われる公衆無線ＬＡＮの接続認証手順を中継する無線ＬＡＮアクセスポイントと、を具備する移動無線通信システムにおける移動無線端末装置であって、前記接続認証サーバに対して前記公衆無線ＬＡＮシステムへの接続認証処理を行う認証処理部と、前記公衆無線ＬＡＮシステムへの接続が許可された時に前記接続認証サーバから前記仮想私設網中継装置との間で行うＩＰsec鍵交換に用いるＩＰsec事前共有秘密鍵を取得するＩＰsec共有鍵取得部と、前記ＩＰsec事前共有秘密鍵を用いて前記仮想私設網中継装置とＩＰsec鍵交換を行

うＩＰsec鍵交換部と、を具備する構成を採る。

【００１８】

この構成によれば、移動無線端末装置と仮想私設網中継装置が同一のＩＰsec事前共有秘密鍵を取得することが可能であり、かつ、移動無線端末装置の公衆無線ＬＡＮシステムへの接続の度にＩＰsec事前共有秘密鍵を更新することができるため、セキュリティの低下を防ぐことができ、かつ、ユーザ及び管理者の特別な作業を必要としない。また、この構成によれば、移動無線端末装置と接続認証サーバにおいて接続認証手順により確立されたセキュアな通信路を用いてＩＰsec事前共有秘密鍵を送信することにより、ＩＰsec事前共有秘密鍵を配布するためのセキュアな通信路を改めて確立する必要がないため、モバイルＶＰＮ接続環境におけるＩＰsecトンネルの確立に要する時間を短縮することができる。

【００１９】

本発明の移動無線端末装置は、公衆網と私設網と公衆無線ＬＡＮシステムとを具備し、前記公衆網を介して前記私設網に設置された網中継装置とＩＰsecトンネルを確立し移動無線端末装置との間でＩＰsecトンネルを確立して前記移動無線端末装置の前記公衆無線ＬＡＮシステムから前記私設網への接続を中継する仮想私設網中継装置と、前記移動無線端末装置の移動制御を行うホームエージェントと、前記公衆無線ＬＡＮシステムに設置され前記移動無線端末装置の前記公衆無線ＬＡＮシステムへの接続を認証する接続認証サーバと、前記移動無線端末装置と前記接続認証サーバとの間で行われる公衆無線ＬＡＮの接続認証手順を中継する無線ＬＡＮアクセスポイントと、を具備する移動無線通信システムにおける移動無線端末装置であって、前記接続認証サーバに対して前記公衆無線ＬＡＮシステムへの接続認証処理を行う認証処理部と、前記公衆無線ＬＡＮシステムへの接続が許可された時に前記接続認証サーバから前記ホームエージェントとの間で行うモバイルＩＰ登録に用いる事前共有秘密鍵を取得するＭＩＰ共有鍵取得部と、前記事前共有秘密鍵を用いて前記ホームエージェントへモバイルＩＰ登録を行うＭＩＰ登録部と、を具備する構成を採る。

【００２０】

この構成によれば、移動無線端末装置とホームエージェントが同一のＭＩＰ事前共有秘密鍵を取得することが可能であり、かつ、移動無線端末装置の公衆無線ＬＡＮシステムへの接続の度にＭＩＰ事前共有秘密鍵を更新することができるため、セキュリティの低下を防ぐことが可能であり、かつ、ユーザ及び管理者の特別な作業を必要としない。また、移動無線端末装置と接続認証サーバにおいて接続認証手順により確立されたセキュアな通信路を用いてＭＩＰ事前共有秘密鍵を送信することにより、ＭＩＰ事前共有秘密鍵を配布するためのセキュアな通信路を改めて確立する必要がないため、モバイルＶＰＮ接続環境におけるＩＰsecトンネルの確立に要する時間を短縮することができる。

【００２１】

本発明の移動無線端末装置は、公衆網と私設網と公衆無線ＬＡＮシステムとを具備し、前記公衆網を介して前記私設網に設置された網中継装置とＩＰsecトンネルを確立し移動無線端末装置との間でＩＰsecトンネルを確立して前記移動無線端末装置の前記公衆無線ＬＡＮシステムから前記私設網への接続を中継する仮想私設網中継装置と、前記移動無線端末装置の移動制御を行うホームエージェントと、前記公衆無線ＬＡＮシステムに設置され前記移動無線端末装置の前記公衆無線ＬＡＮシステムへの接続を認証する接続認証サーバと、前記移動無線端末装置と前記接続認証サーバとの間で行われる公衆無線ＬＡＮの接続認証手順を中継する無線ＬＡＮアクセスポイントと、を具備する移動無線通信システムにおける移動無線端末装置であって、前記接続認証サーバに対して前記公衆無線ＬＡＮシステムへの接続認証処理を行う認証処理部と、前記公衆無線ＬＡＮシステムへの接続が許可された時に前記接続認証サーバから前記仮想私設網中継装置のＩＰアドレスを取得するアドレス取得部と、前記移動無線端末装置のＩＰアドレスを前記接続認証サーバに通知するアドレス通知部と、前記接続認証サーバから前記仮想私設網中継装置との間で行うＩＰsec鍵交換に用いるＩＰsec事前共有秘密鍵を取得するＩＰsec共有鍵取得部と、前記接続

認証サーバから前記ホームエージェントとの間で行うモバイルＩＰ登録に用いるＭＩＰ事前共有秘密鍵を取得するＭＩＰ共有鍵取得部と、前記仮想私設網中継装置のＩＰアドレスと前記ＩＰsec事前共有秘密鍵を用いて前記仮想私設網中継装置とＩＰsec鍵交換を行うＩＰsec鍵交換部と、前記ＭＩＰ事前共有秘密鍵を用いて前記ホームエージェントへモバイルＩＰ登録を行うＭＩＰ登録部と、を具備する構成を採る。

【００２２】

この構成によれば、移動無線端末装置は仮想私設網中継装置のＩＰアドレスを取得することができ、かつ、仮想私設網中継装置は移動無線端末装置のＩＰアドレスを取得することができるため、それぞれのＩＰアドレスを用いてＩＰsecメインモードによる鍵交換を開始することができ、かつ、移動無線端末装置と仮想私設網中継装置とは同一のＩＰsec事前共有秘密鍵を取得することが可能であるため移動無線端末装置の公衆無線ＬＡＮシステムへの接続の度にＩＰsec事前共有秘密鍵を更新することができる。さらに、この構成によれば、移動無線端末装置とホームエージェントとは同一のＭＩＰ事前共有秘密鍵を取得することが可能であり、かつ、移動無線端末装置の公衆無線ＬＡＮシステムへの接続の度にＭＩＰ事前共有秘密鍵を更新することができる。これにより、セキュリティの低下を防ぐことが可能であり、かつ、ユーザ及び管理者の特別な作業を必要としない。

【００２３】

さらに、この構成によれば、移動無線端末装置と接続認証サーバにおいて接続認証手順により確立されたセキュアな通信路を用いてＩＰアドレスとＩＰsec事前共有秘密鍵とＭＩＰ事前共有秘密鍵を送信することにより、これらを配布するためのセキュアな通信路を改めて確立する必要がないため、モバイルＶＰＮ接続環境におけるＩＰsecトンネルの確立に要する時間を短縮することができる。

【００２４】

本発明の仮想私設網中継装置は、公衆網と私設網と公衆無線ＬＡＮシステムとを具備し、前記公衆網を介して前記私設網に設置された網中継装置とＩＰsecトンネルを確立し移動無線端末装置との間でＩＰsecトンネルを確立して前記移動無線端末装置の前記公衆無線ＬＡＮシステムから前記私設網への接続を中継する仮想私設網中継装置と、前記公衆無線ＬＡＮシステムに設置され前記移動無線端末装置の前記公衆無線ＬＡＮシステムへの接続を認証する接続認証サーバと、前記移動無線端末装置と前記接続認証サーバとの間で行われる公衆無線ＬＡＮの接続認証手順を中継する無線ＬＡＮアクセスポイントと、を具備する移動無線通信システムにおける仮想私設網中継装置であって、前記接続認証サーバから前記移動無線端末装置のＩＰアドレスを受信するアドレス取得部と、前記移動無線端末装置のＩＰアドレスを用いて前記移動無線端末装置とＩＰsec鍵交換を行うＩＰsec鍵交換部と、を具備する構成を採る。

【００２５】

この構成によれば、仮想私設網中継装置は移動無線端末装置のＩＰアドレスを取得することができるため、そのＩＰアドレスを用いてＩＰsecメインモードによる鍵交換を開始することができるから、セキュリティの低下を防ぐことが可能であり、ユーザ及び管理者の特別な作業を必要とせず、かつ、モバイルＶＰＮ接続環境におけるＩＰsecトンネルの確立に要する時間を短縮することができる。

【００２６】

本発明の仮想私設網中継装置は、公衆網と私設網と公衆無線ＬＡＮシステムとを具備し、前記公衆網を介して前記私設網に設置された網中継装置とＩＰsecトンネルを確立し移動無線端末装置との間でＩＰsecトンネルを確立して前記移動無線端末装置の前記公衆無線ＬＡＮシステムから前記私設網への接続を中継する仮想私設網中継装置と、前記公衆無線ＬＡＮシステムに設置され前記移動無線端末装置の前記公衆無線ＬＡＮシステムへの接続を認証する接続認証サーバと、前記移動無線端末装置と前記接続認証サーバとの間で行われる公衆無線ＬＡＮの接続認証手順を中継する無線ＬＡＮアクセスポイントと、を具備する移動無線通信システムにおける仮想私設網中継装置であって、前記接続認証サーバから前記移動無線端末装置との間で行うＩＰsec鍵交換に用いる事前共有秘密鍵を受信する

ＩＰsec共有鍵取得部と、前記事前共有秘密鍵を用いて前記移動無線端末装置とＩＰsec鍵交換を行うＩＰsec鍵交換部と、を具備する構成を採る。

【００２７】

この構成によれば、移動無線端末装置と仮想私設網中継装置とは同一のＩＰsec事前共有秘密鍵を取得することが可能であり、かつ、移動無線端末装置の公衆無線ＬＡＮシステムへの接続の度にＩＰsec事前共有秘密鍵を更新することができるため、セキュリティの低下を防ぐことが可能であり、ユーザ及び管理者の特別な作業を必要とせず、かつ、モバイルＶＰＮ接続環境におけるＩＰsecトンネルの確立に要する時間を短縮することができる。

【００２８】

本発明の仮想私設網中継装置は、公衆網と私設網と公衆無線ＬＡＮシステムとを具備し、前記公衆網を介して前記私設網に設置された網中継装置とＩＰsecトンネルを確立し移動無線端末装置との間でＩＰsecトンネルを確立して前記移動無線端末装置の前記公衆無線ＬＡＮシステムから前記私設網への接続を中継する仮想私設網中継装置と、前記公衆無線ＬＡＮシステムに設置され前記移動無線端末装置の前記公衆無線ＬＡＮシステムへの接続を認証する接続認証サーバと、前記移動無線端末装置と前記接続認証サーバとの間で行われる公衆無線ＬＡＮの接続認証手順を中継する無線ＬＡＮアクセスポイントと、を具備する移動無線通信システムにおける仮想私設網中継装置であって、前記接続認証サーバから前記移動無線端末装置のＩＰアドレスを受信するアドレス取得部と、前記接続認証サーバから前記移動無線端末装置との間で行うＩＰsec鍵交換に用いる事前共有秘密鍵を受信するＩＰsec共有鍵取得部と、前記移動無線端末装置のＩＰアドレスと前記事前共有秘密鍵を用いて前記移動無線端末装置とＩＰsec鍵交換を行うＩＰsec鍵交換部と、を具備する構成を採る。

【００２９】

この構成によれば、仮想私設網中継装置は移動無線端末装置のＩＰアドレスを取得することができるため、そのＩＰアドレスを用いてＩＰsecメインモードによる鍵交換を開始することができる。また、この構成によれば、移動無線端末装置と仮想私設網中継装置とは同一のＩＰsec事前共有秘密鍵を取得することが可能であり、かつ、移動無線端末装置の公衆無線ＬＡＮシステムへの接続の度にＩＰsec事前共有秘密鍵を更新することができる。これにより、セキュリティの低下を防ぐことが可能であり、ユーザ及び管理者の特別な作業を必要とせず、かつ、モバイルＶＰＮ接続環境におけるＩＰsecトンネルの確立に要する時間を短縮することができる。

【００３０】

本発明の接続認証サーバは、公衆網と私設網と公衆無線ＬＡＮシステムとを具備し、前記公衆網を介して前記私設網に設置された網中継装置とＩＰsecトンネルを確立し移動無線端末装置との間でＩＰsecトンネルを確立して前記移動無線端末装置の前記公衆無線ＬＡＮシステムから前記私設網への接続を中継する仮想私設網中継装置と、前記公衆無線ＬＡＮシステムに設置され前記移動無線端末装置の前記公衆無線ＬＡＮシステムへの接続を認証する接続認証サーバと、前記移動無線端末装置と前記接続認証サーバとの間で行われる公衆無線ＬＡＮの接続認証手順を中継する無線ＬＡＮアクセスポイントと、を具備する移動無線通信システムにおける接続認証サーバであって、前記移動無線端末装置の前記公衆無線ＬＡＮシステムへの接続認証を行う認証処理部と、前記移動無線端末装置の前記公衆無線ＬＡＮシステムへの接続を許可する時に前記移動無線端末装置のＩＰアドレスを前記移動無線端末装置から受信するアドレス取得部と、前記仮想私設網中継装置のＩＰアドレスを前記移動無線端末装置に通知し、かつ、前記移動無線端末装置のＩＰアドレスを前記仮想私設網中継装置に通知するアドレス通知部と、を具備する構成を採る。

【００３１】

この構成によれば、移動無線端末装置は仮想私設網中継装置のＩＰアドレスを取得することができ、かつ、仮想私設網中継装置は移動無線端末装置のＩＰアドレスを取得することができるため、移動無線端末装置と仮想私設網中継装置とはそれぞれのＩＰアドレスを

用いてＩＰsecメインモードによる鍵交換を開始することができるから、セキュリティの低下を防ぐことが可能であり、かつ、ユーザ及び管理者の特別な作業を必要としない。また、この構成によれば、移動無線端末装置と接続認証サーバにおいて接続認証手順により確立されたセキュアな通信路を用いてＩＰアドレスを送信することにより、ＩＰアドレスを配布するためのセキュアな通信路を改めて確立する必要がないため、モバイルＶＰＮ接続環境におけるＩＰsecトンネルの確立に要する時間を短縮することができる。

【００３２】

本発明の接続認証サーバは、公衆網と私設網と公衆無線ＬＡＮシステムとを具備し、前記公衆網を介して前記私設網に設置された網中継装置とＩＰsecトンネルを確立し移動無線端末装置との間でＩＰsecトンネルを確立して前記移動無線端末装置の前記公衆無線ＬＡＮシステムから前記私設網への接続を中継する仮想私設網中継装置と、前記公衆無線ＬＡＮシステムに設置され前記移動無線端末装置の前記公衆無線ＬＡＮシステムへの接続を認証する接続認証サーバと、前記移動無線端末装置と前記接続認証サーバとの間で行われる公衆無線ＬＡＮの接続認証手順を中継する無線ＬＡＮアクセスポイントと、を具備する移動無線通信システムにおける接続認証サーバであって、前記移動無線端末装置の前記公衆無線ＬＡＮシステムへの接続認証を行う認証処理部と、前記移動無線端末装置の公衆無線ＬＡＮシステムへの接続を許可する時に前記移動無線端末装置と前記仮想私設網中継装置との間で行うＩＰsec鍵交換に用いる事前共有秘密鍵を前記移動無線端末装置と前記仮想私設網中継装置にそれぞれ配布するＩＰsec共有鍵配布部と、を具備する構成を採る。

【００３３】

この構成によれば、移動無線端末装置と仮想私設網中継装置とは同一のＩＰsec事前共有秘密鍵を取得することが可能であり、かつ、移動無線端末装置の公衆無線ＬＡＮシステムへの接続の度にＩＰsec事前共有秘密鍵を更新することができるため、セキュリティの低下を防ぐことが可能であり、かつ、ユーザ及び管理者の特別な作業を必要としない。また、この構成によれば、移動無線端末装置と接続認証サーバにおいて接続認証手順により確立されたセキュアな通信路を用いてＩＰsec事前共有秘密鍵を送信することにより、ＩＰsec事前共有秘密鍵を配布するためのセキュアな通信路を改めて確立する必要がないため、モバイルＶＰＮ接続環境におけるＩＰsecトンネルの確立に要する時間を短縮することができる。

【００３４】

本発明の接続認証サーバは、公衆網と私設網と公衆無線ＬＡＮシステムとを具備し、前記公衆網を介して前記私設網に設置された網中継装置とＩＰsecトンネルを確立し移動無線端末装置との間でＩＰsecトンネルを確立して前記移動無線端末装置の前記公衆無線ＬＡＮシステムから前記私設網への接続を中継する仮想私設網中継装置と、前記移動無線端末装置の移動制御を行うホームエージェントと、前記公衆無線ＬＡＮシステムに設置され前記移動無線端末装置の前記公衆無線ＬＡＮシステムへの接続を認証する接続認証サーバと、前記移動無線端末装置と前記接続認証サーバとの間で行われる公衆無線ＬＡＮの接続認証手順を中継する無線ＬＡＮアクセスポイントと、を具備する移動無線通信システムにおける接続認証サーバであって、前記移動無線端末装置の前記公衆無線ＬＡＮシステムへの接続認証を行う認証処理部と、前記移動無線端末装置の公衆無線ＬＡＮシステムへの接続を許可する時に前記移動無線端末装置と前記ホームエージェントとの間で行うモバイルＩＰ登録に用いる事前共有秘密鍵を前記移動無線端末装置と前記ホームエージェントにそれぞれ配布するＭＩＰ共有鍵配布部と、を具備する構成を採る。

【００３５】

この構成によれば、移動無線端末装置とホームエージェントとは同一のＭＩＰ事前共有秘密鍵を取得することが可能であり、かつ、移動無線端末装置の公衆無線ＬＡＮシステムへの接続の度にＭＩＰ事前共有秘密鍵を更新することができるため、セキュリティの低下を防ぐことが可能であり、かつ、ユーザ及び管理者の特別な作業を必要としない。また、この構成によれば、移動無線端末装置と接続認証サーバにおいて接続認証手順により確立されたセキュアな通信路を用いてＭＩＰ事前共有秘密鍵を送信することにより、ＭＩＰ事

前共有秘密鍵を配布するためのセキュアな通信路を改めて確立する必要がないため、モバイルＶＰＮ接続環境におけるＩＰsecトンネルの確立に要する時間を短縮することができる。

【００３６】

本発明の接続認証サーバは、公衆網と私設網と公衆無線ＬＡＮシステムとを具備し、前記公衆網を介して前記私設網に設置された網中継装置とＩＰsecトンネルを確立し移動無線端末装置との間でＩＰsecトンネルを確立して前記移動無線端末装置の前記公衆無線ＬＡＮシステムから前記私設網への接続を中継する仮想私設網中継装置と、前記移動無線端末装置の移動制御を行うホームエージェントと、前記公衆無線ＬＡＮシステムに設置され前記移動無線端末装置の前記公衆無線ＬＡＮシステムへの接続を認証する接続認証サーバと、前記移動無線端末装置と前記接続認証サーバとの間で行われる公衆無線ＬＡＮの接続認証手順を中継する無線ＬＡＮアクセスポイントと、を具備する移動無線通信システムにおける接続認証サーバであって、前記移動無線端末装置の前記公衆無線ＬＡＮシステムへの接続認証を行う認証処理部と、前記移動無線端末装置の公衆無線ＬＡＮシステムへの接続を許可する時に前記移動無線端末装置のＩＰアドレスを前記移動無線端末装置から受信するアドレス取得部と、前記仮想私設網中継装置のＩＰアドレスを前記移動無線端末装置に通知し、かつ、前記移動無線端末装置のＩＰアドレスを前記仮想私設網中継装置に通知するアドレス通知部と、前記移動無線端末装置と前記仮想私設網中継装置との間で行うＩＰsec鍵交換に用いるＩＰsec事前共有秘密鍵を前記移動無線端末装置と前記仮想私設網中継装置にそれぞれ配布するＩＰsec共有鍵配布部と、前記移動無線端末装置と前記ホームエージェントとの間で行うモバイルＩＰ登録に用いるＭＩＰ事前共有秘密鍵を前記移動無線端末装置と前記ホームエージェントにそれぞれ配布するＭＩＰ共有鍵配布部と、を具備する構成を採る。

【００３７】

この構成によれば、移動無線端末装置は仮想私設網中継装置のＩＰアドレスを取得することができ、かつ、仮想私設網中継装置は移動無線端末装置のＩＰアドレスを取得することができるため、移動無線端末装置と仮想私設網中継装置とはそれぞれのＩＰアドレスを用いてＩＰsecメインモードによるトンネル確立を開始することができる。また、この構成によれば、移動無線端末装置と仮想私設網中継装置とは同一のＩＰsec事前共有秘密鍵を取得することが可能であり、かつ、移動無線端末装置の公衆無線ＬＡＮシステムへの接続の度にＩＰsec事前共有秘密鍵を更新することができる。さらに、この構成によれば、移動無線端末装置とホームエージェントが同一のＭＩＰ事前共有秘密鍵を取得することが可能であり、かつ、移動無線端末装置の公衆無線ＬＡＮシステムへの接続の度にＭＩＰ事前共有秘密鍵を更新することができる。これにより、セキュリティの低下を防ぐことが可能であり、かつ、ユーザ及び管理者の特別な作業を必要としない。

【００３８】

またさらに、この構成によれば、移動無線端末装置と接続認証サーバにおいて接続認証手順により確立されたセキュアな通信路を用いてＩＰアドレスとＩＰsec事前共有秘密鍵とＭＩＰ事前共有秘密鍵を送信することにより、これらを配布するためのセキュアな通信路を改めて確立する必要がないため、モバイルＶＰＮ接続環境におけるＩＰsecトンネルの確立に要する時間を短縮することができる。

【００３９】

本発明の無線ＬＡＮアクセスポイントは、公衆網と私設網と公衆無線ＬＡＮシステムとを具備し、前記公衆網を介して前記私設網に設置された網中継装置とＩＰsecトンネルを確立し移動無線端末装置との間でＩＰsecトンネルを確立して前記移動無線端末装置の前記公衆無線ＬＡＮシステムから前記私設網への接続を中継する仮想私設網中継装置と、前記移動無線端末装置の移動制御を行うホームエージェントと、前記公衆無線ＬＡＮシステムに設置され前記移動無線端末装置の前記公衆無線ＬＡＮシステムへの接続を認証する接続認証サーバと、前記移動無線端末装置と前記接続認証サーバとの間で行われる公衆無線ＬＡＮの接続認証手順を中継する無線ＬＡＮアクセスポイントと、を具備する移動無線通

信システムにおける無線ＬＡＮアクセスポイントであって、前記移動無線端末装置と前記接続認証サーバとの間で行われる公衆無線ＬＡＮの接続認証手順において確立した安全な通信路を用いて、前記接続認証サーバから送信されるＩＰアドレスとＩＰsec事前共有鍵、Mobile ＩＰ事前共有鍵を前記移動無線端末装置に送信し、かつ、前記移動無線端末装置から送信されるＩＰアドレスを前記接続認証サーバへ送信する認証中継部と、を具備する構成を採る。

【００４０】

この構成によれば、移動無線端末装置が仮想私設網中継装置のＩＰアドレスを取得することができ、かつ、仮想私設網中継装置は移動無線端末装置のＩＰアドレスを取得することができるため、移動無線端末装置と仮想私設網中継装置とはそれぞれのＩＰアドレスを用いてＩＰsecメインモードによる鍵交換を開始することができる。また、この構成によれば、移動無線端末装置と仮想私設網中継装置とは同一のＩＰsec事前共有秘密鍵を取得することが可能であり、かつ、移動無線端末装置の公衆無線ＬＡＮシステムへの接続の度にＩＰsec事前共有秘密鍵を更新することができる。これにより、セキュリティの低下を防ぐことが可能であり、かつ、ユーザ及び管理者の特別な作業を必要としない。

【００４１】

さらに、この構成によれば、移動無線端末装置と接続認証サーバにおいて接続認証手順により確立されたセキュアな通信路を用いてＩＰアドレスとＩＰsec事前共有秘密鍵とＭＩＰ事前共有秘密鍵を送信することにより、これらを配布するためのセキュアな通信路を改めて確立する必要がないため、モバイルＶＰＮ接続環境におけるＩＰsecトンネルの確立に要する時間を短縮することができる。

【００４２】

本発明のホームエージェントは、公衆網と私設網と公衆無線ＬＡＮシステムとを具備し、前記公衆網を介して前記私設網に設置された網中継装置とＩＰsecトンネルを確立し移動無線端末装置との間でＩＰsecトンネルを確立して前記移動無線端末装置の前記公衆無線ＬＡＮシステムから前記私設網への接続を中継する仮想私設網中継装置と、前記移動無線端末装置の移動制御を行うホームエージェントと、前記公衆無線ＬＡＮシステムに設置され前記移動無線端末装置の前記公衆無線ＬＡＮシステムへの接続を認証する接続認証サーバと、前記移動無線端末装置と前記接続認証サーバとの間で行われる公衆無線ＬＡＮの接続認証手順を中継する無線ＬＡＮアクセスポイントと、を具備する移動無線通信システムにおけるホームエージェントであって、前記接続認証サーバから前記移動無線端末装置のモバイルＩＰ登録に用いる事前共有秘密鍵を受信するＭＩＰ共有鍵取得部と、前記事前共有秘密鍵を用いて前記移動無線端末装置からのモバイルＩＰ登録を処理するＭＩＰ処理部と、を具備する構成を採る。

【００４３】

この構成によれば、ホームエージェントはＭＩＰ事前共有秘密鍵を取得することが可能であり、かつ、移動無線端末装置の公衆無線ＬＡＮシステムへの接続の度にＭＩＰ事前共有秘密鍵を更新することができるため、セキュリティの低下を防ぐことが可能であり、ユーザ及び管理者の特別な作業を必要とせず、かつ、モバイルＶＰＮ接続環境におけるＩＰsecトンネルの確立に要する時間を短縮することができる。

【発明の効果】

【００４４】

以上説明したように、本発明によれば、セキュリティの低下を防ぐことが可能であり、ユーザ及び管理者の特別な作業を必要とせず、かつ、モバイルＶＰＮ接続環境におけるＩＰsecトンネルの確立に要する時間を短縮することができる。

【発明を実施するための最良の形態】

【００４５】

本発明の骨子は、移動無線端末装置が公衆無線ＬＡＮシステムから公衆網を介して私設網に接続する時に移動無線端末装置と接続認証サーバとの間で行う接続認証手順において確立した暗号化通信路を用いて、移動無線端末装置と仮想私設網中継装置のＩＰアドレス

を互いに通知する。

【００４６】

以下、本発明の実施の形態について図面を参照して詳細に説明する。

（一実施の形態）

図１に示すように、本発明の一実施の形態に係る移動無線通信システム１００は、公衆網１０１、私設網１０２、公衆無線ＬＡＮシステム１０３、網中継装置１０４、仮想私設網中継装置１０５及びホームエージェント１０６を具備している。公衆無線ＬＡＮシステム１０３は、公衆無線ＬＡＮ１０７、接続認証サーバ１０８、無線ＬＡＮアクセスポイント１０９及び複数の移動無線端末装置１１０（１つのみが図示されている）を具備している。

【００４７】

仮想私設網中継装置１０５は、私設網１０２に設置された網中継装置１０４と公衆網１０１を介してＩＰsecトンネルを静的に確立しており、仮想私設網中継装置１０５と私設網１０２との間のセキュアな通信を実現している。また、仮想私設網中継装置１０５は、公衆無線ＬＡＮシステム１０３に存在する移動無線端末装置１１０との間でＩＰsecトンネルを確立し、移動無線端末装置１１０の公衆無線ＬＡＮシステム１０３から私設網１０２への接続を中継する。なお、仮想私設網中継装置１０５と移動無線端末装置１１０とのＩＰsecトンネルは、移動無線端末装置１１０の公衆無線ＬＡＮシステム１０３への接続の度に動的に確立し、また、移動無線端末装置１１０からの私設網１０２への接続要求の度に動的に確立する。

【００４８】

接続認証サーバ１０８は、移動無線端末装置１１０の公衆無線ＬＡＮ１０７への接続認証を行う。この時に、無線ＬＡＮアクセスポイント１０９は、移動無線端末装置１１０と接続認証サーバ１０８との間で行われる接続認証手順を中継する役割を果たす。

【００４９】

図２は、本発明の一実施の形態に係る移動無線端末装置１１０の構成を示すブロック図である。図３は、本発明の一実施の形態に係る仮想私設網中継装置１０５の構成を示すブロック図である。図４は、本発明の一実施の形態に係る接続認証サーバ１０８の構成を示すブロック図である。図５は、本発明の一実施の形態に係る無線ＬＡＮアクセスポイント１０９の構成を示すブロック図である。図６は、本発明の一実施の形態に係るホームエージェント１０６の構成を示すブロック図である。

【００５０】

図２に示すように、移動無線端末装置１１０は、認証処理部２０１、アドレス通知部２０２、アドレス取得部２０３、ＩＰsec共有鍵取得部２０４、ＩＰsec鍵交換部２０５、ＭＩＰ共有鍵取得部２０６及びＭＩＰ登録部２０７を具備している。なお、移動無線端末装置１１０は、移動無線通信を行う装置（図示せず）を具備している。

【００５１】

図３に示すように、仮想私設網中継装置１０５は、アドレス取得部３０１、ＩＰsec共有鍵取得部３０２及びＩＰsec鍵交換部３０３を具備している。図４に示すように、接続認証サーバ１０８は、認証処理部４０１、アドレス通知部４０２、アドレス取得部４０３、ＩＰsec共有鍵配布部４０４及びＭＩＰ共有鍵配布部４０５を具備している。図５に示すように、無線ＬＡＮアクセスポイント１０９は、認証中継部５０１を具備している。図６に示すように、ホームエージェント１０６は、ＭＩＰ共有鍵取得部６０１及びＭＩＰ処理部６０２を具備している。

【００５２】

次に、公衆無線ＬＡＮシステム１０３に存在する移動無線端末装置１１０が私設網１０２に接続する場合の手順を例にとって説明する。

【００５３】

移動無線端末装置１１０が公衆無線ＬＡＮシステム１０３の通信範囲内に存在する時に、移動無線端末装置１１０の認証処理部２０１は、公衆無線ＬＡＮシステム１０３に接続

するために、無線ＬＡＮアクセスポイント１０９の認証中継部５０１を介して接続認証サーバ１０８の認証処理部４０１へ接続要求を送信する。公衆無線ＬＡＮシステム１０３へ接続するためのプロトコルとして、ＩＥＥＥ（the Institute of Electrical and Electronics Engineers）で規定されている８０２.１xなどが挙げられる。

【００５４】

以下、説明の簡単のため、８０２.１xを用いた場合の手順を説明する。８０２.１xの枠組みでは、移動無線端末装置１１０と無線ＬＡＮアクセスポイント１０９との間では、ＥＡＰ（Extensible Authentication Protocol）プロトコルが適用される。また、無線ＬＡＮアクセスポイント１０９と接続認証サーバ１０８との間では、ＲＡＤＩＵＳ（Remote Authentication Dial In User Service）プロトコルなどが適用される。無線ＬＡＮアクセスポイント１０９は、前記両者のプロトコルを中継するブリッジ機能を有する。

【００５５】

接続認証サーバ１０８の認証処理部４０１は、最初に、移動無線端末装置１１０の認証処理部２０１から送信されてくる接続要求の認証を行う。この認証は、ＥＡＰ－ＭＤ５、ＥＡＰ－ＴＬＳ、ＥＡＰ－ＬＥＡＰ又はＰＥＡＰといった種々の認証方式より行われる。ここでは説明の簡単のため、ＥＡＰ－ＴＬＳを適用した場合の手順を説明する。ＥＡＰ－ＴＬＳでは、移動無線端末装置１１０と接続認証サーバ１０８との間で電子証明書を交換することにより、相互の認証を行う。

【００５６】

また、同時に、移動無線端末装置１１０と接続認証サーバ１０８は、乱数を交換して擬似乱数関数などによる演算処理を行うことにより、相互に共通のマスターシークレットを保持する。移動無線端末装置１１０と接続認証サーバ１０８は、前記マスターシークレットからＰＭＫ（Pairwise Master Key）を生成する。そして、接続認証サーバ１０８において移動無線端末装置１１０の認証が成功した場合、移動無線端末装置１１０と接続認証サーバ１０８は前記マスターシークレットを用いて、接続認証サーバ１０８と移動無線端末装置１１０との間の通信路を暗号化する。

【００５７】

この時、無線ＬＡＮアクセスポイント１０９の認証中継部５０１は前記通信路を中継する役割を果たすため、移動無線端末装置１１０と接続認証サーバ１０８の秘匿通信が可能となる。即ち、移動無線端末装置１１０の認証処理部２０１と無線ＬＡＮアクセスポイント１０９の認証中継部５０１と接続認証サーバ１０８の認証処理部４０１との間でセキュアな通信路が確立されたことになる。以後、特別な断りがない限り、移動無線端末装置１１０と無線ＬＡＮアクセスポイント１０９と接続認証サーバ１０８との通信は、このセキュアな通信路を用いて行う。

【００５８】

そして、接続認証サーバ１０８は、この暗号化されたセキュアな通信路を用いて無線ＬＡＮアクセスポイント１０９にＰＭＫを送信する。これにより、移動無線端末装置１１０と無線ＬＡＮアクセスポイント１０９は、共有するＰＭＫからＷＥＰキーを生成し、公衆無線ＬＡＮシステム１０３における無線通信区間通信路をＷＥＰキーにより暗号化する。（図７のステップＳＴ１）。

【００５９】

次に、移動無線端末装置１１０と接続認証サーバ１０８との間で共有するマスターシークレットにより暗号化された通信路を用いて、移動無線端末装置１１０と仮想私設網中継装置１０５のＩＰアドレスを交換する。接続認証サーバ１０８のアドレス通知部４０２は、無線ＬＡＮアクセスポイント１０９の認証中継部５０１を中継して移動無線端末装置１１０のアドレス取得部２０３へ仮想私設網中継装置１０５のＩＰアドレスを送信する（図７のステップＳＴ２）。

【００６０】

なお、接続認証サーバ１０８は仮想私設網中継装置１０５のＩＰアドレスを予め保持しておくことなどが考えられる。仮想私設網中継装置１０５のＩＰアドレスを受信した移動

無線端末装置１１０のアドレス取得部２０３は、アドレス通知部２０２へ信号を送る。そして、その信号を受信したアドレス通知部２０２は、自身に割り当てられたＩＰアドレスを無線ＬＡＮアクセスポイント１０９の認証中継部５０１を介して接続認証サーバ１０８のアドレス取得部４０３へ送信する（図７のステップＳＴ３）。

【００６１】

また、接続認証サーバ１０８と移動無線端末装置１１０とがＩＰアドレスを送受信するために、ＥＡＰプロトコルとＥＡＰＯＬプロトコルは拡張される。接続認証サーバ１０８の認証処理部４０１と無線ＬＡＮアクセスポイント１０９の認証中継部５０１とがＩＰアドレスを送受信するために、ＥＡＰプロトコルのメッセージタイプにＥＡＰ－ＩＰＡＤＤＲが新たに定義される。そして、接続認証サーバ１０８の認証処理部４０１は、無線ＬＡＮアクセスポイント１０９の認証中継部５０１へＲＡＤＩＵＳプロトコルのvendor specificフィールドの属性値としてＩＰアドレスを送信する。

【００６２】

一方、移動無線端末装置１１０の認証処理部２０１と無線ＬＡＮアクセスポイント１０９の認証中継部５０１とがＩＰアドレスを送受信するために、図８に示すＥＡＰＯＬプロトコルのパケットタイプにＥＡＰＯＬ－ＩＰＡＤＤＲが新たに定義され、属性値としてＩＰアドレスを通知するためのａｄｄｒフォーマット（図９）は追加される。このＥＡＰＯＬ－ＩＰＡＤＤＲメッセージの受信は、移動無線端末装置１１０にとっては仮想私設網中継装置１０５のＩＰアドレスの受信を示し、無線ＬＡＮアクセスポイント１０９にとっては移動無線端末装置１１０のＩＰアドレスの受信をそれぞれ示す。

【００６３】

そして、接続認証サーバ１０８のアドレス通知部４０２は、移動無線端末装置１１０のＩＰアドレスを仮想私設網中継装置１０５のアドレス取得部３０１へ送信する（図７のステップＳＴ４）。

【００６４】

以上の手順により、移動無線端末装置１１０と仮想私設網中継装置１０５は相互のＩＰアドレスを取得することができる。そして、移動無線端末装置１１０のＩＰsec鍵交換部２０５と仮想私設網中継装置１０５のＩＰsec鍵交換部３０３は、取得したＩＰアドレスを用いて、ＩＰsecメインモードによる鍵交換を開始することができる。

【００６５】

さらに、接続認証サーバ１０８は、移動無線端末装置１１０と接続認証サーバ１０８との間で共有するマスターシークレットにより暗号化された通信路を用いて、移動無線端末装置１１０と仮想私設網中継装置１０５との間で行われるＩＰsecトンネル確立時に用いるＩＰsec事前共有秘密鍵を、移動無線端末装置１１０と仮想私設網中継装置１０５とに配布する。接続認証サーバ１０８の認証中継部４０１は、無線ＬＡＮアクセスポイント１０９の認証中継部５０１にＩＰsec事前共有秘密鍵を送信する。このＩＰsec事前共有秘密鍵を受信した無線ＬＡＮアクセスポイント１０９の認証中継部５０１は、ＩＰsec事前共有秘密鍵をそのまま移動無線端末装置１１０の認証処理部２０１へ送信する（図７のステップＳＴ４）。

【００６６】

なお、接続認証サーバ１０８の認証処理部４０１から移動無線端末装置１１０の認証処理部２０１へＩＰsec事前共有秘密鍵を送信するために、ＥＡＰプロトコルとＥＡＰＯＬプロトコルは拡張される。接続認証サーバ１０８の認証処理部４０１が無線ＬＡＮアクセスポイント１０９の認証中継部５０１へＩＰsec事前共有秘密鍵を送信するために、ＥＡＰプロトコルのメッセージタイプにＥＡＰ-ＩＰSECKEYを新たに定義する。そして、ＲＡＤＩＵＳプロトコルのvendor specificフィールドの属性値としてＩＰsec事前共有秘密鍵を送信する。一方、無線ＬＡＮアクセスポイント１０９の認証中継部５０１から移動無線端末装置１１０の認証処理部２０１へＩＰsec事前共有秘密鍵を送信するためにＥＡＰＯＬプロトコルの鍵配布メッセージを用いる。この時、key descriptionフォーマットのdescriptor typeをＩＰsecとして、keyフィールドを用いてＩＰsec事前共有秘密鍵を通知す

る。
【００６７】
そして、接続認証サーバ１０８のＩＰsec共有鍵配布部４０４は、移動無線端末装置１１０に送信したＩＰsec事前共有秘密鍵と同一のＩＰsec事前共有秘密鍵を仮想私設網中継装置１０５のＩＰsec共有鍵取得部３０２へ送信する。
【００６８】
なお、接続認証サーバ１０８から仮想私設網中継装置１０５への通信路は、ＩＰsecトンネルを静的に確立し、ＩＰsec事前共有秘密鍵が盗聴されないセキュアな通信路を実現する。さらに、接続認証サーバ１０８で保持するＩＰsec事前共有秘密鍵は、接続認証サーバ１０８が動的に生成することも可能であるし、また、別の鍵生成サーバなどから受信することなどが可能である。
【００６９】
以上の手順により、移動無線端末装置１１０と仮想私設網中継装置１０５とは同一のＩＰsec事前共有秘密鍵を共有する。移動無線端末装置１１０のＩＰsec鍵交換部２０５と仮想私設網中継装置１０５のＩＰsec鍵交換部３０３は、共有したＩＰsec事前共有秘密鍵を用いて、ＩＰsecメインモードによる鍵交換を開始する。仮想私設網中継装置１０５のＩＰsec鍵交換部３０３は、移動無線端末装置１１０のＩＰsec鍵交換部２０５からの認証要求に記載のＩＰsec事前共有秘密鍵とＩＰアドレスとユーザＩＤが仮想私設網中継装置１０５で保持するＩＰsec事前共有秘密鍵とＩＰアドレスとユーザＩＤと一致する場合に、移動無線端末装置１１０の認証を許可してＩＰsecトンネルを確立する。
【００７０】
また、接続認証サーバ１０８は、移動無線端末装置１１０と接続認証サーバ１０８との間で共有するマスターシークレットにより暗号化された通信路を用いて、移動無線端末装置１１０がホームエージェント１０６への登録に用いるＭＩＰ事前共有秘密鍵を移動無線端末装置１１０へ送信する。接続認証サーバ１０８の認証処理部４０１は、ＭＩＰ事前共有秘密鍵を無線ＬＡＮアクセスポイント１０９の認証中継部５０１に送信する。このＭＩＰ事前共有秘密鍵を受信した無線ＬＡＮアクセスポイント１０９の認証中継部５０１は、ＭＩＰ事前共有秘密鍵を移動無線端末装置１１０の認証処理部２０１へ送信する。
【００７１】
なお、接続認証サーバ１０８の認証処理部４０１が移動無線端末装置１１０の認証処理部２０１へＭＩＰ事前共有秘密鍵を送信するために、ＥＡＰプロトコルとＥＡＰＯＬプロトコルは拡張される。接続認証サーバ１０８の認証処理部４０１が無線ＬＡＮアクセスポイント１０９の認証中継部５０１へＭＩＰ事前共有秘密鍵を送信するために、ＥＡＰプロトコルのメッセージタイプにＥＡＰ－ＭＩＰＫＥＹは新たに定義される。そして、続認証サーバ１０８の認証処理部４０１は、無線ＬＡＮアクセスポイント１０９の認証中継部５０１へＲＡＤＩＵＳプロトコルのvendor specificフィールドの属性値としてＭＩＰ事前共有秘密鍵を送信する。
【００７２】
一方、無線ＬＡＮアクセスポイント１０９の認証中継部５０１が移動無線端末装置１１０の認証処理部２０１へＭＩＰ事前共有秘密鍵を送信するためにＥＡＰＯＬプロトコルの鍵配布メッセージが用いられる。この時、key descriptionフォーマットのdescriptor typeをＭＩＰとして、keyフィールドを用いてＭＩＰ事前共有秘密鍵が通知される。
【００７３】
そして、接続認証サーバ１０８のＭＩＰ共有鍵配布部４０５は、移動無線端末装置１１０に送信したＭＩＰ事前共有秘密鍵と同一のＭＩＰ事前共有秘密鍵と移動無線端末装置１１０のＩＰアドレスをホームエージェント１０６のＭＩＰ共有鍵取得部６０１へ送信する（図７のステップＳＴ５）。
【００７４】
なお、接続認証サーバ１０８からホームエージェント１０６への通信路は、ＩＰsecトンネルを静的に確立し、ＭＩＰ事前共有秘密鍵が盗聴されないセキュアな通信路を実現す

る。さらに、接続認証サーバ１０８で保持するＭＩＰ事前共有秘密鍵は、接続認証サーバ１０８が動的に生成することも可能であるし、また、別の鍵生成サーバなどから受信することなどが可能である。

【００７５】

以上の手順により、移動無線端末装置１１０とホームエージェント１０６は、同一のＭＩＰ事前共有秘密鍵を共有する。移動無線端末装置１１０のＭＩＰ登録部２０７は、ＭＩＰ事前共有鍵を用いてホームエージェント１０６のＭＩＰ処理部６０２に対してモバイルＩＰ登録（Binding Update）を行う。ホームエージェント１０６のＭＩＰ処理部６０２は、移動無線端末装置１１０のＭＩＰ登録部２０７からのモバイルＩＰ登録メッセージの認証フィールドに記載のＭＩＰ事前共有秘密鍵とＳＰＩがホームエージェント１０６で保持するＭＩＰ事前共有秘密鍵とＳＰＩと一致する場合に、移動無線端末装置１１０のモバイルＩＰ登録の認証を許可する。なお、既に移動無線端末装置１１０と仮想私設網中継装置１０５との間にはＩＰsecトンネルが確立されているため、移動無線端末装置１１０とホームエージェント１０６との通信路はセキュアである。

【００７６】

このように、本発明の一実施の形態によれば、移動無線端末装置１１０が公衆無線ＬＡＮシステム１０３などの公衆網から私設網へ接続するようなモバイルＶＰＮ接続環境において、ＩＰsecメインモードによるＩＰsecトンネルを確立することが可能となる。また、本発明の一実施の形態によれば、移動無線端末装置１１０の公衆無線ＬＡＮシステム１０３へのアクセスの度にＩＰsec事前共有鍵とＭＩＰ事前共有鍵を動的に更新することができる。したがって、本発明の一実施の形態によれば、セキュリティの低下を防ぐことができ、ユーザ及び管理者の特別な作業を必要とせず、かつ、モバイルＶＰＮ接続環境におけるＩＰsecトンネルの確立に要する時間を短縮することができる。

【産業上の利用可能性】

【００７７】

本発明は、移動無線端末装置が公衆無線ＬＡＮシステムから公衆網を介して私設網へアクセスするモバイルＶＰＮ環境を提供する移動無線通信システムとして好適である。

【図面の簡単な説明】

【００７８】

【図１】本発明の一実施の形態に係る移動無線通信システムの構成を示す図

【図２】本発明の一実施の形態に係る移動無線端末装置の構成を示すブロック図

【図３】本発明の一実施の形態に係る仮想私設網中継装置の構成を示すブロック図

【図４】本発明の一実施の形態に係る接続認証サーバの構成を示すブロック図

【図５】本発明の一実施の形態に係る無線アクセスポイントの構成を示すブロック図

【図６】本発明の一実施の形態に係るホームエージェントの構成を示すブロック図

【図７】本発明の一実施の形態に係る移動無線通信システムを説明するためのシーケンス図

【図８】本発明の一実施の形態に係る移動無線通信システムに用いられるＥＡＰＯＬメッセージフォーマットを説明するための図

【図９】本発明の一実施の形態に係る移動無線通信システムに用いられるaddrメッセージフォーマットを説明するための図

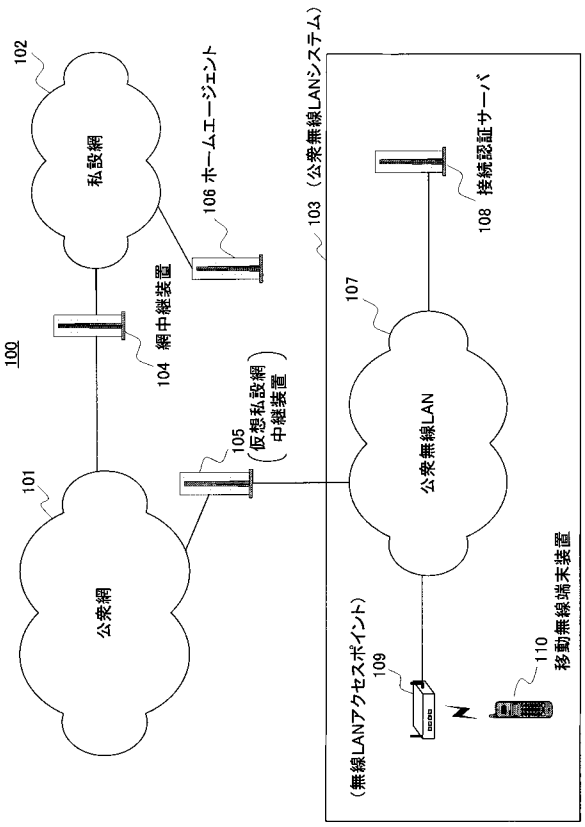
【符号の説明】

【００７９】

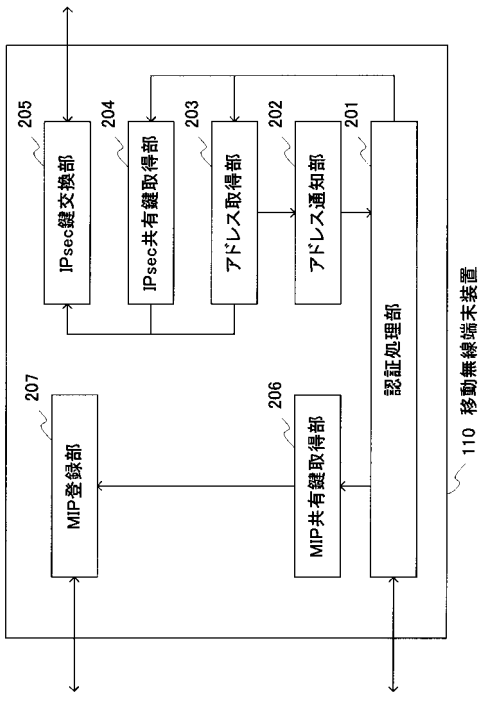
１００　移動無線通信システム
１０１　公衆網
１０２　私設網
１０３　公衆無線ＬＡＮシステム
１０４　網中継装置
１０５　仮想私設網中継装置
１０６　ホームエージェント

１０７　公衆無線ＬＡＮ
１０８　接続認証サーバ
１０９　無線ＬＡＮアクセスポイント
１１０　移動無線端末装置
２０１　認証処理部
２０２　アドレス通知部
２０３　アドレス取得部
２０４　ＩＰsec共有鍵取得部
２０５　ＩＰsec鍵交換部
２０６　ＭＩＰ共有鍵取得部
２０７　ＭＩＰ登録部
３０１　アドレス取得部
３０２　ＩＰsec共有鍵取得部
３０３　ＩＰsec鍵交換部
４０１　認証処理部
４０２　アドレス通知部
４０３　アドレス取得部
４０４　ＩＰsec共有鍵配布部
４０５　ＭＩＰ共有鍵配布部
５０１　認証中継部
６０１　ＭＩＰ共有鍵取得部
６０２　ＭＩＰ処理部

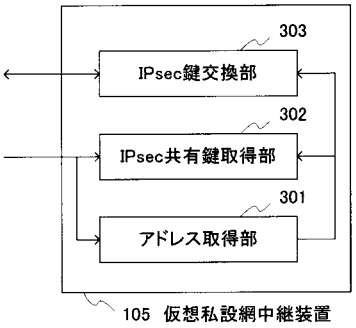
【図１】



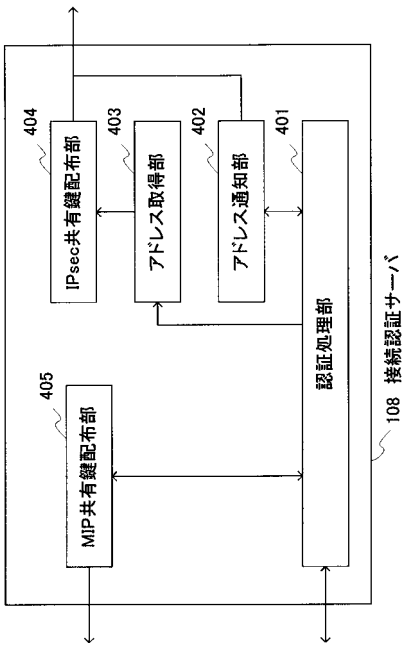
【図２】



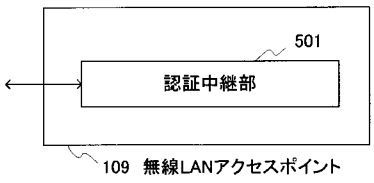
【図３】


303
IPsec鍵交換部
302
IPsec共有鍵取得部
301
アドレス取得部
105 仮想私設網中継装置

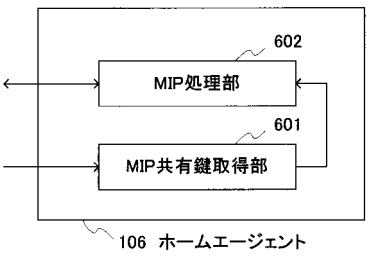
【図４】


404
IPsec共有鍵配布部
403
アドレス取得部
402
アドレス通知部
401
認証処理部
405
MIP共有鍵配布部
108 接続認証サーバ

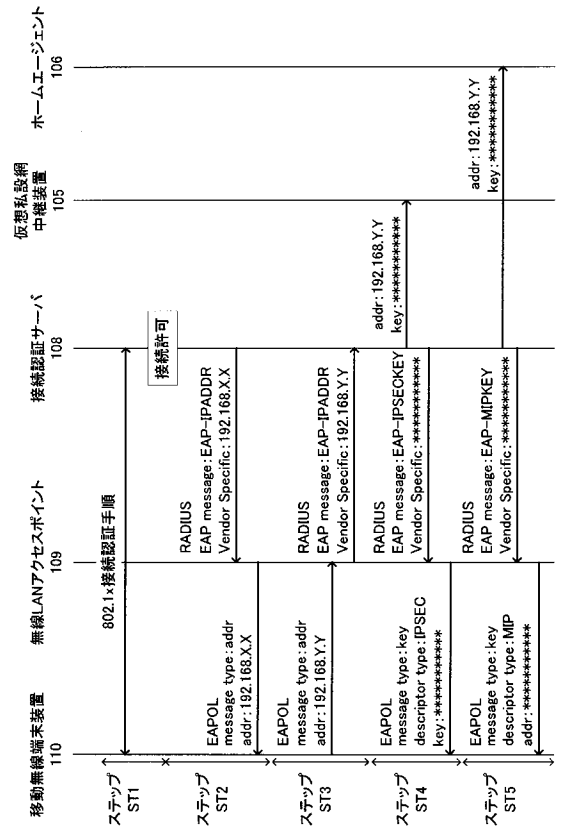
【図５】


501
認証中継部
109 無線LANアクセスポイント

【図６】


602
MIP処理部
601
MIP共有鍵取得部
106 ホームエージェント

【図７】



【図８】

PAE Ethernet Type
Protocol Version
Packet Type
Packet Body Length
Packet Body

EAPOLメッセージフォーマット

【図９】

Description Type
Length
IP Address

addrメッセージフォーマット

フロントページの続き

(51)Int.Cl. F I

H04Q 7/30 (2006.01)
H04Q 7/38 (2006.01)

(72)発明者 石井 義一
神奈川県横浜市港北区綱島東四丁目３番１号 パナソニックモバイルコミュニケーションズ株式会社内

審査官 清水 稔

(56)参考文献 特開２００１－１７７５１４（ＪＰ，Ａ）
Feder, P.M. Lee, N.Y. Martin-Leon, S. , A seamless mobile VPN data solution for UMTS and WLAN users , 3G Mobile Communication Technologies, 2003. 3G 2003. 4th International Conference on (Conf. Publ. No. 494) , ２００３年 ６月２７日, p.210 - 216

(58)調査した分野(Int.Cl., ＤＢ名)
Ｈ０４Ｌ １２／６６
Ｈ０４Ｌ １２／５６
Ｈ０４Ｑ ７／２２
Ｈ０４Ｑ ７／２４
Ｈ０４Ｑ ７／２６
Ｈ０４Ｑ ７／３０
Ｈ０４Ｑ ７／３８