

【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17年7月7日(2005.7.7)

【公開番号】特開2002-281045(P2002-281045A)

【公開日】平成14年9月27日(2002.9.27)

【出願番号】特願2002-602(P2002-602)

【国際特許分類第7版】

H 04 L 12/28

H 04 L 12/66

H 04 Q 7/38

【F I】

H 04 L 12/28 3 0 0 Z

H 04 L 12/66 E

H 04 B 7/26 1 0 9 S

【手続補正書】

【提出日】平成16年11月2日(2004.11.2)

【手続補正1】

【補正対象書類名】明細書

【補正対象項目名】特許請求の範囲

【補正方法】変更

【補正の内容】

【特許請求の範囲】

【請求項1】

(A) 無線ネットワークアクセスポイント(112)に接続されたサーバ(102)と、

(B) 前記サーバ(102)にアクセス可能で、無線ネットワーククライアント(114)を認証検査する際に用いられるユーザデータベース(108)と、
からなり、

前記サーバ(A)は、

(A1) 無線ネットワークアクセスポイント(112)を介しサーバ(102)への接続を確立する無線ネットワーククライアント(114)に対する認証検査を実行し、

(A2) 前記クライアントの認証結果に基づいて、接続セッションを確立し、

(A3) 前記クライアントの認証結果に基づいて、接続セッションの間有効な有線ネットワークアドレスを前記クライアントに与え、

(A4) 無線ネットワークアクセスポイントとの通信を暗号化し、

(A5) 前記クライアントの認証結果に基づいて、前記クライアントへの接続セッションの間有効な暗号化キーを提供する

ことを特徴とする無線ネットワーククライアントに対し認証されたアクセスを提供する有線ネットワーク。

【請求項2】

(C) 前記サーバ(102)と前記有線ネットワーク上の資源(108)との間の接続を提供するネットワークハブ(106)

をさらに有することを特徴とする請求項1記載の有線ネットワーク。

【請求項3】

(D) 前記サーバと前記有線ネットワーク上の資源との間の接続を提供し、かつ別の有線ネットワークへの接続を提供するルータ

をさらに有することを特徴とする請求項1記載の有線ネットワーク。

【請求項4】

無線ネットワークのクライアントと有線ネットワークのクライアントの間のセキュリティを有する認証された通信を提供する無線ネットワークにおいて、

(A) 無線ネットワーク(104)と有線ネットワーク(100)との間の入口として動作するサーバー(102)との接続を確立するために動作する無線ネットワークアクセスポイント(112)と、

(B) 前記無線ネットワークアクセスポイントとの接続を確立するために動作する複数の無線ネットワーククライアント(114)と、

からなり、

前記無線ネットワークアクセスポイント(A)は、

(A1) 前記サーバとの通信を実行し、

(A2) 前記クライアントからの認証情報を受領し、この認証情報をサーバに転送して、サーバから暗号化キーを受領してこの暗号化キーを各クライアントに転送し、

前記各無線ネットワーククライアント(B)は、

(B1) アクセスポイントを介しサーバと暗号化された通信を実行し、認証情報を前記無線ネットワークアクセスポイントに送り、アドレス情報と暗号化するための暗号化データを前記無線ネットワークアクセスポイントを介して、アクセスポイントから受領して有線ネットワークと通信し、

(B2) アドレスと暗号化情報を受領すると、アクセスポイントを介し有線ネットワークとの間でデータの暗号化された転送を行う

ことを特徴とする無線ネットワークのクライアントと有線ネットワークのクライアントの間のセキュリティを有する認証された通信を提供する無線ネットワーク。

【請求項5】

(C) 無線ネットワークアクセスポイントと複数の別のネットワークアクセスポイントと接続されたハブ(216)、

をさらに有し、

各別のネットワークアクセスポイントは、複数の別の無線ネットワーククライアントと、無線ネットワークアクセスポイントと、別のネットワークアクセスポイントと通信し、ネットワークハブを介してサーバと通信を確立する

ことを特徴とする請求項4記載の無線ネットワーク。

【請求項6】

無線ネットワーククライアントと有線ネットワークとの間のセキュリティを有する通信を実行する方法において、

(A) 有線ネットワークに接続されたSBサーバと、無線ネットワークアクセスポイントとの間に接続を確立するステップと、

(B) 前記SBサーバと、前記無線ネットワークアクセスポイントを介して前記SBサーバと通信するネットワーククライアントとの間に接続を確立するステップと、

(C) 前記SBサーバと無線ネットワーククライアントとの間で暗号化キーを交換するステップと、

(D) 前記無線ネットワーククライアントに対し認証検査を実行するステップと、

(E) 認証が不許可の場合、有線ネットワークへの接続を拒否するステップと、

(F) 認証が許可の場合、有線ネットワークへの接続を受け入れるステップと、

(G) 一時的な有線ネットワークアドレスとユニークなセッション暗号化キーを無線ネットワーククライアントに与えるステップと、

(H) 無線ネットワーククライアントによるリクエストに応答して、有線ネットワーク資源へのアクセスを与えるステップと

を有することを特徴とする無線ネットワーククライアントと有線ネットワークとの間のセキュリティを有する通信をする方法。

【請求項7】

前記(E)ステップは、拒否をログインするステップが伴い、

前記(F)ステップは、受け入れをログインするステップが伴う

ことを特徴とする請求項 6 記載の方法。

【請求項 8】

前記(G)ステップは、アドレスを与えるためのダイナミックホスト制御プロトコールを用いて行われる

ことを特徴とする請求項 6 記載の方法。

【請求項 9】

前記(D)ステップは、無線ネットワークと S B サーバとの間で認証情報を転送するステップを含み、

前記認証情報は、公開キー暗号化方式を用いて暗号化される
ことを特徴とする請求項 8 記載の方法。

【請求項 10】

前記(G)ステップは、前記ユニークなセッション暗号化キーを公開キー暗号化方式を用いて暗号化するステップを含む

ことを特徴とする請求項 9 記載の方法。