

【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18年8月3日(2006.8.3)

【公表番号】特表2005-529525(P2005-529525A)

【公表日】平成17年9月29日(2005.9.29)

【年通号数】公開・登録公報2005-038

【出願番号】特願2004-512049(P2004-512049)

【国際特許分類】

H 0 4 L 9/32 (2006.01)

【F I】

H 0 4 L 9/00 6 7 5 B

【手続補正書】

【提出日】平成18年5月17日(2006.5.17)

【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】

相互接続機能を有する無線LANにおいて前記無線LANと第2のネットワークとの間の相互接続のための方法であって、

第1の鍵を受信するステップと、

プローカーからネットワークへの認可証と第2の鍵を含むユーザへの認可証を受信するステップと、

第3の鍵を得るために、前記第1の鍵を用いて前記プローカーからネットワークへの認可証を認証するステップと、

前記第2の鍵を得るために、前記第3の鍵を用いて前記ネットワークからユーザへの認可証を認証するステップと、

セッション鍵を生成し、前記第2の鍵を用いて前記セッション鍵を暗号化し、前記暗号化されたセッション鍵を送信するステップと、

前記セッション鍵を用いて通信するステップと、
を含む、前記方法。

【請求項2】

前記ネットワークからユーザへの認可証は、前記ユーザの相互接続サービスに加入しているかどうかを示す加入レベルを更に含み、前記セッション鍵を送信するステップが、前記加入レベルに応答して行われる、請求項1に記載の方法。

【請求項3】

前記ネットワークからユーザへの認可証は、前記ネットワークからユーザへの認可証の有効期限を更に含み、更に、前記方法が、前記ネットワークからユーザへの認可証の期限が終了しているかどうかを判定するために、前記有効期限をチェックするステップを含む、請求項1に記載の方法。

【請求項4】

第4鍵を用いて署名され、前記セッション鍵を含む無線LANからユーザへの認可証を生成するステップを更に含み、前記ステップにより、前記無線LANは認証することが可能である、請求項1に記載の方法。

【請求項5】

相互接続機能を有する無線LANにおける無線LANと第2のネットワークとの間の相

互接続のための方法であって、

プローカー公開鍵を受信するステップと、

ネットワーク秘密鍵を用いて署名され、プローカーからネットワークへの認可証とユーザ公開鍵を含むネットワークからユーザへの認可証を受信するステップとを含み、前記プローカーからネットワークへの認可証は、プローカー秘密鍵を用いて署名され、ネットワーク公開鍵を含み、

前記プローカー公開鍵を用いて前記プローカーから前記ネットワークへの認可証を認証し、前記ネットワーク公開鍵を得るステップと、

前記ネットワーク公開鍵を用いて前記ネットワークからユーザへの認可証を認証し、前記ユーザ公開鍵を得るステップと、

セッション鍵を生成し、前記ユーザ公開鍵を用いて前記セッション鍵を暗号化し、前記暗号化されたセッション鍵を送信するステップと、

前記セッション鍵を用いて通信するステップと、
を含む、前記方法。

【請求項 6】

前記ネットワークからユーザへの認可証は、前記ユーザが相互接続サービスに加入しているかどうかを示す前記ユーザの加入レベルを更に含み、前記セッション鍵を送信するステップが、前記加入レベルに応答して行われる、請求項 5 に記載の方法。

【請求項 7】

前記ネットワークからユーザへの認可証は、前記ネットワークからユーザへの認可証の有効期限を更に含み、更に、前記方法が前記ネットワークからユーザへの認可証の期限が終了しているかどうかを判定するために前記有効期限をチェックするステップを含む、請求項 5 に記載の方法。

【請求項 8】

前記ユーザの装置に前記無線 LAN を認証する機能を与えるステップを更に含む、請求項 5 に記載の方法。

【請求項 9】

前記ユーザの装置に前記無線 LAN を認証する機能を与えるステップは、

前記プローカー秘密鍵を用いて署名され、無線 LAN 秘密鍵を含むプローカーから無線 LAN への認可証を受信するステップと、

無線 LAN 秘密鍵を用いて署名され、前記暗号化されたセッション鍵を含む無線 LAN からユーザへの認可証を生成するステップと、

前記無線 LAN からユーザへの認可証を送信するステップと、
を更に含む、請求項 8 に記載の方法。

【請求項 10】

ネットワークに加入しているユーザの装置を用いて無線 LANとの通信を行うための方法であって、

前記ネットワークが、前記無線 LAN と相互接続契約をしており、

前記方法は、

ユーザの装置への認可証を前記ネットワークから受信するステップを含み、前記ネットワークからユーザの装置への認可証は、ネットワーク秘密鍵を用いて署名され、プローカーからネットワークへの認可証とユーザ公開鍵とを含み、

前記無線 LAN に対して前記ネットワークからユーザの装置への認可証を送信するステップを含み、前記無線 LAN は、プローカー公開鍵を用いて前記ユーザ公開鍵を得ることが可能であり、

前記ユーザの公開鍵を用いて暗号化されたセッション鍵を受信するステップと、

ユーザ秘密鍵を用いて前記セッション鍵を復号化するステップと、

前記セッション鍵を用いて通信するステップと、
を含む、前記方法。

【請求項 11】

前記第2のネットワークからユーザの装置への認可証は、前記ユーザが相互接続サービスに加入しているかどうかを示す加入レベルを更に含む、請求項10に記載の方法。

【請求項12】

前記ネットワークからユーザの装置への認可証が、前記ネットワークからユーザへの認可証の有効期限を含み、前記有効期限が満了していない場合、前記送信ステップが行われる、請求項10に記載の方法。

【請求項13】

前記受信ステップが、前記ブローカー秘密鍵により署名され、前記セッション鍵を含む無線LANからユーザへの認可証を受信するステップを含み、更に、前記ブローカー公開鍵を受信し、前記ブローカー公開鍵を用いて前記無線LANからユーザへの認可証を認証し、前記セッション鍵を得るステップを含む、請求項10に記載の方法。

【請求項14】

相互接続関係を有する複数のネットワークにおいてユーザの認証を行うためのブローカーに基づくシステムであって、

相互接続機能を有する無線LANと、

第2のネットワークと、

前記無線LANおよび前記第2のネットワークと通信可能なブローカーとを含み、前記ブローカーは、ブローカー公開鍵を前記無線LANに送信する手段と、ブローカー秘密鍵を用いて署名され、第2のネットワーク公開鍵を含むブローカーから第2のネットワークへの認可証を前記第2のネットワークに送信する手段とを含み、

前記第2のネットワークは、ユーザの装置に対し、第2のネットワーク秘密鍵を用いて署名され、前記ブローカーから第2のネットワークへの認可証と前記ユーザ公開鍵とを含む第2のネットワークからユーザへの認可証を送信する手段を含み、

前記無線LANは、前記ブローカーから第2のネットワークへの認可証を認証し、前記第2のネットワーク公開鍵を得る手段と、前記第2のネットワークからユーザへの認可証を認証し、前記ユーザ公開鍵を得る手段と、セッション鍵を生成し、前記ユーザ公開鍵を用いて前記セッション鍵を暗号化する手段と、

を含む、前記ブローカーに基づくシステム。

【請求項15】

前記無線LANが、無線LAN秘密鍵を用いて署名され、前記暗号化されたセッション鍵を含む無線LANからユーザへの認可証を送信する手段を更に含む、請求項14に記載のシステム。

【請求項16】

ブローカーからネットワーク認可証を含むユーザ認可証に対するネットワークを受信する手段と、

セッション鍵を受信する手段と、

前記セッション鍵を使用して通信する手段と
を含む、携帯型装置。

【請求項17】

第1のネットワークがユーザ認可証に対する前記ネットワークを受信し、前記セッション鍵を生成し、更に、前記第1のネットワークが、相互接続機能を有する無線LANである、請求項16に記載の携帯型装置。

【請求項18】

前記ユーザ認可証に対する第2のネットワークが、前記第2のネットワークによって転送され、前記第2のネットワークは、セルラー・ネットワークである、請求項16に記載の携帯型装置。