

【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】令和3年12月9日(2021.12.9)

【公開番号】特開2020-88742(P2020-88742A)

【公開日】令和2年6月4日(2020.6.4)

【年通号数】公開・登録公報2020-022

【出願番号】特願2018-223974(P2018-223974)

【国際特許分類】

H 04 W 76/19 (2018.01)

H 04 W 4/00 (2018.01)

H 04 W 12/04 (2021.01)

【F I】

H 04 W	76/19	
H 04 W	4/00	1 1 0
H 04 W	12/04	

【手続補正書】

【提出日】令和3年10月29日(2021.10.29)

【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】

通信装置であって、

Wi-Fi DPP (Device Provisioning Protocol)

規格に従って通信パラメータを取得する第1の取得手段と、

前記第1の取得手段により取得された前記通信パラメータを用いて、第1の他の通信装置とDPPに準拠したNetwork Introduction処理を実行することにより、暗号鍵を取得する第2の取得手段と、

前記Network Introduction処理を実行することにより取得された前記暗号鍵を用いて、前記第1の他の通信装置との接続処理を実行する接続手段と、

前記第1の他の通信装置との再接続においては、前記Network Introduction処理による前記暗号鍵の取得を省略して前記第1の他の通信装置と接続する再接続手段と、

を備えることを特徴とする通信装置。

【請求項2】

前記第1の取得手段は、DPPにおけるコンフィギュレータとして動作する第2の他の通信装置から、前記通信パラメータを取得することを特徴とする請求項1に記載の通信装置。

【請求項3】

前記接続手段は、AuthenticationパケットまたはAssociation Requestを前記第1の他の通信装置へ送信することにより、前記第1の他の通信装置との前記接続処理を開始することを特徴とする請求項1または2に記載の通信装置。

【請求項4】

前記接続手段は、前記第1の他の通信装置との間で4-Way Handshakeを実行することを特徴とする請求項1から3のいずれか1項に記載の通信装置。

【請求項 5】

接続の対象となっている前記第1の他の通信装置に関する接続履歴が存在するかを判定する判定手段をさらに備え、

前記判定手段により前記接続履歴が存在すると判定された場合に、前記再接続手段は、前記Network Introduction処理による前記暗号鍵の取得を省略して前記第1の他の通信装置と接続することを特徴とする請求項1から4のいずれか1項に記載の通信装置。

【請求項 6】

前記接続履歴は、前記第1の他の通信装置のMACアドレスを含むことを特徴とする請求項5に記載の通信装置。

【請求項 7】

前記第1の他の通信装置を検索する検索手段をさらに備え、

前記再接続手段は、前記検索手段において前記第1の他の通信装置から受信したBeaconもしくはProbe Responseに付加されている情報に基づいて前記接続履歴が存在するか否かを判定することを特徴とする請求項5または6に記載の通信装置。

【請求項 8】

前記第1の他の通信装置から受信したBeaconもしくはProbe ResponseにPMKIDが付加されている場合に、前記接続履歴が存在すると判定することを特徴とする請求項7に記載の通信装置。

【請求項 9】

前記再接続手段は、前記暗号鍵を示す情報が付加されたAssociation Requestを送信することを特徴とする請求項1から8のいずれか1項に記載の通信装置。

【請求項 10】

前記再接続手段による前記第1の他の通信装置との接続に失敗した場合、前記第1の他の通信装置と前記Network Introduction処理を実行する実行手段をさらに備えることを特徴とする請求項1から9のいずれか1項に記載の通信装置。

【請求項 11】

前記第1の他の通信装置は、IEEE802.11シリーズ規格に準拠したアクセスポイントであることを特徴とする請求項1から10のいずれか1項に記載の通信装置。

【請求項 12】

前記暗号鍵は、PMK(Pairwise Master Key)であることを特徴とする請求項1から11のいずれか1項に記載の通信装置。

【請求項 13】

通信装置であって、

他の通信装置とDPPに準拠したNetwork Introduction処理を実行することにより、暗号鍵を取得する取得手段と、

前記Network Introduction処理を実行することにより取得された前記暗号鍵を用いて、前記他の通信装置と接続する接続手段と、

前記暗号鍵を特定する情報が付加された要求信号を前記他の通信装置から受信した場合、前記Network Introduction処理を省略して、前記他の通信装置と接続する再接続手段と、

を備えることを特徴とする通信装置。

【請求項 14】

前記接続手段は、前記他の通信装置と4-Way Handshakeを実行することによって、前記他の通信装置と接続することを特徴とする請求項13に記載の通信装置。

【請求項 15】

前記暗号鍵を特定する情報を付加したBeacon信号を送信する送信手段をさらに備えることを特徴とする請求項13または14に記載の通信装置。

【請求項 16】

Beacon信号に対応するプローブリクエストを受信した場合に、前記プローブリクエストに対して、前記暗号鍵を特定する情報を付加したプロープレスポンスを送信する送信手段をさらに備えることを特徴とする請求項13または14に記載の通信装置。

【請求項17】

前記通信装置は、IEEE802.11シリーズ規格に準拠したアクセスポイントであることを特徴とする請求項13から16のいずれか1項に記載の通信装置。

【請求項18】

通信装置の制御方法であって、

Wi-Fi DPP (Device Provisioning Protocol)
規格に従って通信パラメータを取得する第1の取得工程と、

前記第1の取得工程において取得された前記通信パラメータを用いて、第1の他の通信装置とDPPに準拠したNetwork Introduction処理を実行することにより、暗号鍵を取得する第2の取得工程と、

前記Network Introduction処理を実行することにより取得された前記暗号鍵を用いて、前記第1の他の通信装置との接続処理を実行する接続工程と、

前記第1の他の通信装置との再接続においては、前記Network Introduction処理による前記暗号鍵の取得を省略して前記第1の他の通信装置と接続する再接続工程と、

を備えることを特徴とする制御方法。

【請求項19】

通信装置の制御方法であって、

他の通信装置とDPPに準拠したNetwork Introduction処理を実行することにより、暗号鍵を取得する取得工程と、

前記Network Introduction処理を実行することにより取得された前記暗号鍵を用いて、前記他の通信装置と接続する接続工程と、

前記暗号鍵を特定する情報が付加された要求信号を前記他の通信装置から受信した場合、前記Network Introduction処理を省略して、前記他の通信装置と接続する再接続工程と、

を備えることを特徴とする制御方法。

【請求項20】

請求項1から17のいずれか1項に記載された通信装置の各手段としてコンピュータを機能させるためのプログラム。

【手続補正2】

【補正対象書類名】明細書

【補正対象項目名】0007

【補正方法】変更

【補正の内容】

【0007】

本発明の一態様による通信装置は以下の構成を備える。すなわち、

Wi-Fi DPP (Device Provisioning Protocol)
規格に従って通信パラメータを取得する第1の取得手段と、

前記第1の取得手段により取得された前記通信パラメータを用いて、第1の他の通信装置とDPPに準拠したNetwork Introduction処理を実行することにより、暗号鍵を取得する第2の取得手段と、

前記Network Introduction処理を実行することにより取得された前記暗号鍵を用いて、前記第1の他の通信装置との接続処理を実行する接続手段と、

前記第1の他の通信装置との再接続においては、前記Network Introduction処理による前記暗号鍵の取得を省略して前記第1の他の通信装置と接続する再接続手段と、を備える。