

【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 6 部門第 3 区分
 【発行日】平成 26 年 9 月 4 日 (2014.9.4)

【公表番号】特表 2014-509760 (P2014-509760A)
 【公表日】平成 26 年 4 月 21 日 (2014.4.21)
 【年通号数】公開・登録公報 2014-020
 【出願番号】特願 2013-558147 (P2013-558147)
 【国際特許分類】

G 0 6 F 21/31 (2013.01)

G 0 9 C 1/00 (2006.01)

【F I】

G 0 6 F 21/20 1 3 1 A

G 0 9 C 1/00 6 4 0 E

【手続補正書】
 【提出日】平成 26 年 7 月 17 日 (2014.7.17)
 【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】

第 1 の通信プロトコルと第 2 の通信プロトコルとにそれぞれしたがって動作する第 1 のサブネットワークと第 2 のサブネットワークとを有するハイブリッドネットワークであって、前記第 1 の通信プロトコルと前記第 2 の通信プロトコルとは異なり、ホームプラグプロトコルと、無線ローカルエリアネットワーク (WLAN) プロトコルとから選択され、前記ハイブリッドネットワークは、第 1 のデバイスを含み、前記第 1 のデバイスは、

前記第 1 の通信プロトコルの第 1 のネットワークインターフェースと、

第 1 のプロセッサと、

前記第 1 のプロセッサに結合され、第 1 のコンピュータ実行可能な命令を記憶した、第 1 のメモリと

を備え、前記第 1 のコンピュータ実行可能な命令は、前記第 1 のプロセッサによって実行されると、前記第 1 のデバイスに、

ユーザからマスターパスフレーズを受信することと、

前記マスターパスフレーズを前記第 1 の通信プロトコルに準拠した第 1 のパスワードに変換することであって、前記第 1 の通信プロトコルに応答して、前記マスターパスフレーズの文字を選択的に、切り捨て、追加し、または置換して、前記第 1 のパスワードを生成することによって変換することと、

前記第 1 のパスワードを使用して、前記第 1 のサブネットワークに対し前記第 1 のデバイスを認証することと、

前記第 1 のパスワードをハッシュして、前記第 1 の通信プロトコルに準拠した第 1 の鍵を導出することと、

前記第 1 の鍵を使用して、前記第 1 のデバイスを前記第 1 のサブネットワークに参加させることと

を行わせる、ハイブリッドネットワーク。

【請求項 2】

前記第 2 の通信プロトコルの第 2 のネットワークインターフェースと、

第 2 のプロセッサと、

前記第 2 のプロセッサに結合され、第 2 のコンピュータ実行可能な命令を記憶した、第 2 のメモリと

を備える第 2 のデバイスをさらに含み、前記第 2 のコンピュータ実行可能な命令は、前記第 2 のプロセッサによって実行されると、前記第 2 のデバイスに、

前記ユーザから前記マスターパスフレーズを受信することと、

前記マスターパスフレーズを前記第 2 の通信プロトコルに準拠した第 2 のパスワードに変換することであって、前記第 2 の通信プロトコルに応答して、前記マスターパスフレーズの文字を選択的に、切り捨て、追加し、または置換して、前記第 2 のパスワードを生成することによって変換することと、

前記第 2 のパスワードを使用して、前記第 2 のサブネットワークに対し前記第 2 のデバイスを認証することと、

前記第 2 のパスワードをハッシュして、前記第 2 の通信プロトコルに準拠した第 2 の鍵を導出することと、

前記第 2 のパスワードを使用して、前記第 2 のデバイスを前記第 2 のサブネットワークに参加させることと

を行わせる、請求項 1 に記載のハイブリッドネットワーク。

【請求項 3】

前記第 1 のメモリは、追加のコンピュータ実行可能な命令を記憶し、前記追加のコンピュータ実行可能な命令は、前記第 1 のプロセッサによって実行されると、前記第 1 のデバイスに、

前記第 1 のデバイスから、前記第 1 または第 2 の通信プロトコルのネットワークインターフェースを有する第 3 のデバイスに、前記マスターパスフレーズを送信すること

を行わせる、請求項 1 に記載のハイブリッドネットワーク。

【請求項 4】

第 1 の通信プロトコルと第 2 の通信プロトコルとにそれぞれしたがって動作する第 1 のサブネットワークと第 2 のサブネットワークとを有するハイブリッドネットワークに複数のデバイスを追加するための方法であって、前記第 1 の通信プロトコルと前記第 2 の通信プロトコルとは異なり、ホームプラグプロトコルと、無線ローカルエリアネットワーク (WLAN) プロトコルとから選択され、

第 1 のデバイスにマスターパスフレーズを入力することと、ここで、前記第 1 のデバイスは、前記第 1 の通信プロトコルの第 1 のネットワークインターフェースを備える、

前記第 1 のデバイスにおいて第 1 の変換演算を使用して前記マスターパスフレーズを変換して、前記第 1 の通信プロトコルに準拠した第 1 のパスワードを生成することと、ここで、前記第 1 の変換演算は、前記第 1 の通信プロトコルに応答して、前記マスターパスフレーズの文字を選択的に、切り捨て、追加し、または置換して、前記第 1 のパスワードを生成することを含み、

前記第 1 のパスワードを使用して、前記第 1 のサブネットワークに対し前記第 1 のデバイスを認証することと、

前記第 1 のパスワードをハッシュして、前記第 1 の通信プロトコルに準拠した第 1 の鍵を導出することと、

前記第 1 の鍵を使用して、前記第 1 のデバイスを前記第 1 のサブネットワークに参加させることと

を備える方法。

【請求項 5】

前記第 1 のデバイスから第 3 のデバイスに、暗号化されたメッセージにおいて前記マスターパスフレーズを送信すること

をさらに備える、請求項 4 に記載の方法。

【請求項 6】

第 2 のデバイスにマスターパスフレーズを入力することと、ここで、前記第 2 のデバイスは、前記第 2 の通信プロトコルの第 2 のネットワークインターフェースを備える、

前記第 2 のデバイスにおいて第 2 の変換演算を使用して前記マスターパスフレーズを変換して、前記第 2 の通信プロトコルに準拠した第 2 のパスワードを生成することと、ここで、前記第 2 の変換演算は、前記第 2 の通信プロトコルに応答して、前記マスターパスフレーズの文字を選択的に、切り捨て、追加し、または置換して、前記第 2 のパスワードを生成することを含み、

前記第 2 のパスワードを使用して、前記第 2 のサブネットワークに対し前記第 2 のデバイスを認証することと、

前記第 2 のパスワードをハッシュして、前記第 2 の通信プロトコルに準拠した第 2 の鍵を導出することと、

前記第 2 の鍵を使用して、前記第 2 のデバイスを前記第 2 のサブネットワークに参加させることと

をさらに備える、請求項 4 に記載の方法。

【請求項 7】

前記第 1 のデバイスから、前記第 1 および第 2 の通信プロトコルのネットワークインターフェースを有する第 3 のデバイスに、前記マスターパスフレーズを送信すること

をさらに備え、前記第 3 のデバイスは、前記第 3 のデバイスにおいて、前記第 2 の変換演算を使用して前記マスターパスフレーズを変換し、前記第 2 のパスワードを生成するためのものである、請求項 6 に記載の方法。

【請求項 8】

前記第 3 のデバイスは、

前記第 2 のパスワードをハッシュして、前記第 2 の鍵を導出し、

前記第 2 の鍵を使用して、前記第 3 のデバイスを前記ハイブリッドネットワークに参加させる

ためのものである、請求項 7 に記載の方法。

【請求項 9】

前記ハイブリッドネットワークの既存のメンバーである第 3 のデバイスにおいて、前記第 3 のデバイスを前記ハイブリッドネットワークに参加させるために以前に使用された第 3 のパスワードを選択することと、

前記第 3 のデバイスにおいて逆変換演算を使用して、前記第 3 のパスワードから前記マスターパスフレーズを導出することと

をさらに備える、請求項 4 に記載の方法。

【請求項 10】

前記第 1 の通信プロトコルのネットワークインターフェースを有する第 3 のデバイスにおいて、前記変換演算を実行しない第 4 のデバイスに代わり、前記マスターパスフレーズを導出すること

をさらに備える、請求項 4 に記載の方法。

【請求項 11】

第 1 の通信プロトコルと第 2 の通信プロトコルとにそれぞれしたがって動作する第 1 のサブネットワークと第 2 のサブネットワークとを有するハイブリッドネットワークに複数のデバイスを追加するためのシステムであって、前記第 1 の通信プロトコルと前記第 2 の通信プロトコルとは異なり、ホームプラグプロトコルと、無線ローカルエリアネットワーク (WLAN) プロトコルとから選択され、

第 1 のデバイスにマスターパスフレーズを入力する手段と、ここで、前記第 1 のデバイスは、前記第 1 の通信プロトコルの第 1 のネットワークインターフェースを備える、

前記第 1 のデバイスにおいて第 1 の変換演算を使用して前記マスターパスフレーズを変換して、前記第 1 の通信プロトコルに準拠した第 1 のパスワードを生成する手段と、ここで、前記第 1 の変換演算は、前記第 1 の通信プロトコルに応答して、前記マスターパスフレーズの文字を選択的に、切り捨て、追加し、または置換して、前記第 1 のパスワードを生成するためのものであり、

前記第 1 のパスワードを使用して、前記第 1 のサブネットワークに対し前記第 1 のデバ

イスを認証する手段と、

前記第 1 のパスワードをハッシュして、前記第 1 の通信プロトコルに準拠した第 1 の鍵を導出する手段と、

前記第 1 の鍵を使用して、前記第 1 のデバイスを前記第 1 のサブネットワークに参加させる手段と

を備えるシステム。

【請求項 1 2】

前記第 1 のデバイスから第 3 のデバイスに、暗号化されたメッセージにおいて前記マスターパスフレーズを送信する手段

をさらに備える、請求項 1 1 に記載のシステム。

【請求項 1 3】

第 2 のデバイスにマスターパスフレーズを入力する手段と、ここで、前記第 2 のデバイスは、前記第 2 の通信プロトコルの第 2 のネットワークインターフェースを備える、

前記第 2 のデバイスにおいて第 2 の変換演算を使用して前記マスターパスフレーズを変換して、前記第 2 の通信プロトコルに準拠した第 2 のパスワードを生成する手段と、ここで、前記第 2 の変換演算は、前記第 2 の通信プロトコルに応答して、前記マスターパスフレーズの文字を選択的に、切り捨て、追加し、または置換して、前記第 2 のパスワードを生成するためのものであり、

前記第 2 のパスワードを使用して、前記第 2 のサブネットワークに対し前記第 2 のデバイスを認証する手段と、

前記第 2 のパスワードをハッシュして、前記第 2 の通信プロトコルに準拠した第 2 の鍵を導出する手段と、

前記第 2 の鍵を使用して、前記第 2 のデバイスを前記第 2 のサブネットワークに参加させる手段と

をさらに備える、請求項 1 1 に記載のシステム。

【請求項 1 4】

前記第 1 のデバイスから、前記第 1 および第 2 の通信プロトコルのネットワークインターフェースを有する第 3 のデバイスに、前記マスターパスフレーズを送信する手段

をさらに備え、前記第 3 のデバイスは、前記第 3 のデバイスにおいて、前記第 2 の変換演算を使用して前記マスターパスフレーズを変換し、前記第 2 のパスワードを生成するためのものである、請求項 1 3 に記載のシステム。

【請求項 1 5】

前記第 3 のデバイスは、

前記第 2 のパスワードをハッシュして、前記第 2 の鍵を導出し、

前記第 2 の鍵を使用して、前記第 3 のデバイスを前記ハイブリッドネットワークに参加させる

ためのものである、請求項 1 4 に記載のシステム。

【請求項 1 6】

前記ハイブリッドネットワークの既存のメンバーである第 3 のデバイスにおいて、前記第 3 のデバイスを前記ハイブリッドネットワークに参加させるために以前に使用された第 3 のパスワードを選択する手段と、

前記第 3 のデバイスにおいて逆変換演算を使用して、前記第 3 のパスワードから前記マスターパスフレーズを導出する手段と

をさらに備える、請求項 1 1 に記載のシステム。

【請求項 1 7】

前記第 1 の通信プロトコルのネットワークインターフェースを有する第 3 のデバイスにおいて、前記変換演算を実行しない第 4 のデバイスに代わり、前記マスターパスフレーズを導出する手段

をさらに備える、請求項 1 1 に記載のシステム。