

【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 06 F 21/31 (2013.01)

G 09 C 1/00 (2006.01)

【F I】

G 06 F 21/20 1 3 1 A

G 09 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12】**

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11に記載のシステム。

**【請求項13】**

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11に記載のシステム。

**【請求項14】**

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13に記載のシステム。

**【請求項15】**

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14に記載のシステム。

**【請求項16】**

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11に記載のシステム。

**【請求項17】**

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11に記載のシステム。