

【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8月25日(2005.8.25)

【公開番号】特開2003-304236(P2003-304236A)

【公開日】平成15年10月24日(2003.10.24)

【出願番号】特願2003-35883(P2003-35883)

【国際特許分類第7版】

H 04 L 9/14

H 04 L 9/08

H 04 L 9/32

H 04 L 12/28

【F I】

H 04 L 9/00 6 4 1

H 04 L 12/28 3 0 0 Z

H 04 L 9/00 6 0 1 B

H 04 L 9/00 6 7 5 Z

【手続補正書】

【提出日】平成17年2月16日(2005.2.16)

【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】

無線網におけるセキュリティを向上させるための方法であって、

少なくとも一つ新たなキーが一つ生成されるべきかを示す時間期間を決定するステップと、

複数のキーをコントローラ内にロードするステップであって、このキーの数が無線網に接続されたデバイスが所定の数の前記時間期間に再認証されるのをミスしてもまだ無線網上で安全に通信することができるようセットされるようなステップと、

前記キーを前記コントローラから前記デバイスに通信するステップとを含むことを特徴とする方法。

【請求項2】

前記方法がさらに前記複数のキーの内の一つをローカル送信キーとして選択するステップを含み；

前記キーをデバイスに通信するステップがさらに前記複数のキーの内のある特定のキーが前記デバイスに対する送信キーとされるべきことを前記デバイスに伝えるステップを含み、この特定のキーが前記ローカル送信キーとは異なるように選択されることを特徴とする請求項1記載の方法。

【請求項3】

前記コントローラが混合モードにて動作し；

複数のキーをロードする前記ステップが；

固定キーをロードするステップ；及び

少なくとも一つの追加のキーをロードするステップを含み、前記複数のキーが前記固定キーと前記少なくとも一つ追加のキーとからなり；

前記複数のキーの内の一つをローカル送信キーとして選択するステップが前記固定キーを前記ローカル送信キーとして選択するステップからなることを特徴とする請求項2記載

の方法。

【請求項 4】

前記少なくとも一つのキーが一つのキーとされ、前記時間期間の所定の数が1とされることを特徴とする請求項3記載の方法。

【請求項 5】

前記コントローラが標準モードにて動作し；

前記複数のキーをロードするステップが少なくとも三つのキーをロードすることからなり、この方法がさらに：

前記複数のキーの内の一つをローカル送信キーとして選択するステップ；及び

その他のキーをローカル受信キーとして選択するステップを含み；

前記複数のキーを送信するステップが前記少なくとも三つのキーを前記デバイスに通信することから成ることを特徴とする請求項1記載の方法。

【請求項 6】

前記少なくとも三つのキーが三つのキーとされ、前記時間期間の所定の数が1とされることを特徴とする請求項5記載の方法。

【請求項 7】

前記方法がさらに：

各時間期間の度に、少なくとも一つの新たなキーを決定するステップ；及び

前記複数のキーが所定の数のキーに達しているときは、前記少なくとも一つの新たなキーに前記複数のキーの一つを取り替え、達していないときは、前記少なくとも一つの新たなキーを前記複数のキーに追加するステップを含むことを特徴とする請求項1記載の方法。

【請求項 8】

前記方法がさらに、各時間期間に対して、前記複数のキーの内の一つをローカル送信キーとして選択するステップを含み、現在の時間期間に対するローカル送信キーが直前の時間期間に対するローカル送信キーとは異なるように選択されることを特徴とする請求項1記載の方法。

【請求項 9】

無線網におけるセキュリティを向上させるための方法であって、

少なくとも一つ新たなキーがいつ生成されるべきかを示す時間期間をロードするステップと、

複数のキーをロードするステップと、

前記複数のキーの内の一つをローカル送信キーとして選択するステップ、

その他のキーを受信キーとして選択するステップとからなり、前記方法はさらに、

各時間期間において：

(1) 少なくとも一つのキーを生成するステップ；及び

(2) 前記少なくとも一つの新たなキーを用いて、前記少なくとも一つのキーの各々に、前記複数のキーの一つのキーを置換するステップを遂行するステップとを含み、前記少なくとも一つの新たなキーと置換されなかったキーによって新たな複数のキーが構成され、さらに各時間期間において：

(3) 前記新たな複数のキーの一つのキーをローカル送信キーとして選択するステップがを遂行するステップを含み、現在の時間期間に対するローカル送信キーが直前の時間期間に対するローカル送信キーとは異なるように選択されることを特徴とする方法。

【請求項 10】

無線網へのアクセスを制御するための装置であって、

コンピュータにて読み出し可能なコードを格納するメモリ；及び

前記メモリに接続されたプロセッサを備え、該プロセッサが前記コンピュータにて読み出し可能なコードを実装するように構成され、前記コンピュータにて読み出し可能なコードが：

少なくとも一つ新たなキーがいつ生成されるべきかを示す時間期間を決定し、

複数のキーをロードするように構成され、このキーの数が無線網に接続されたデバイスが所定数の前記時間期間に再認証されるのをミスしてもまだ無線網上で安全に通信することができるようにセットされ；前記コンピュータにて読み出し可能なコードがさらに、前記キーを前記コントローラから前記デバイスに通信するように構成されることを特徴とする装置。