【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19年8月9日(2007.8.9)

【公表番号】特表2003-503896(P2003-503896A)
【公表日】平成15年1月28日(2003.1.28)
【出願番号】特願2001-506186(P2001-506186)
【国際特許分類】
Ｈ０４Ｌ　9/08　(2006.01)
Ｈ０４Ｑ　7/38　(2006.01)
Ｈ０４Ｌ　9/32　(2006.01)
【ＦＩ】
Ｈ０４Ｌ　9/00　６０１Ｃ
Ｈ０４Ｂ　7/26　１０９Ｒ
Ｈ０４Ｌ　9/00　６７５Ｚ

【手続補正書】
【提出日】平成19年6月14日(2007.6.14)
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】請求項１０
【補正方法】変更
【補正の内容】
【請求項１０】　通信ノードにおいて暗号キー（７０）を生成する装置であって、前記装置は、
データを格納するために構成されたメモリ（６４）と、
通信リンク（１４）によってデータを送受信するために構成可能なトランシーバ（６６）とを有し、
前記メモリと前記トランシーバ（６６）に接続され、暗号化法のキー（４０）を用いて、外部通信ノードとの通信リンク（１４）により認証処理を実行し（１０２）、前記認証処理中に暗号化オフセットを生成し（１０４）、前記暗号化オフセットを前記メモリ（６４）に格納し（１０６）、その後、少なくとも１つの生成されたランダム入力値（６８）、前記暗号化法のキー（４０）、及び前記暗号化オフセット（５０）からの入力を用いるために構成された暗号化キー発生器（４４′）において、これにより暗号化キー（７０）が論理的に前記認証処理に関連付けられるように前記暗号化キー（７０）を生成する（１０８）ために構成されたプロセッサ（６２）を有することを特徴とする装置。
【手続補正２】
【補正対象書類名】明細書
【補正対象項目名】請求項２０
【補正方法】変更
【補正の内容】
【請求項２０】　通信リンク（１４）を有するシステムであって、
前記通信リンクに接続され、前記通信リンクによってデータを送受信し、暗号化法のキー（４０）を用いて前記通信リンク（１４）により認証処理を実行し、前記認証処理中に暗号化オフセット（５０）を生成し、前記暗号化オフセットを格納し、その後、少なくとも１つの生成されたランダム入力値（６８）、前記暗号化法のキー、及び前記暗号化オフセットとを用いて、暗号化キー（７０）を生成するために構成された第１のノード（１２′）と、
前記通信リンクに接続され、前記通信リンクによってデータを送受信し、前記暗号化法のキー（４０）を用いて前記通信リンク（１４）により前記第１のノードとの前記認証処

理を実行し、前記認証処理中に前記暗号化オフセット（５０）を生成し、前記暗号化オフセットを格納し、その後、少なくとも１つの生成されたランダム入力値（６８）、前記暗号化法のキー（４０）、及び前記暗号化オフセット（５０）からの入力を受信するために構成された暗号化キー発生器（４４′）を用いて、論理的に前記認証処理に関連付けられるように前記暗号化キー（７０）を生成するために構成された第２のノード（１６′）とを有し、

前記暗号化キーが前記第１のノード（１２′）と前記第２のノード（１６′）との両方において同じであることを特徴とするシステム。