

【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22年4月15日(2010.4.15)

【公開番号】特開2006-14182(P2006-14182A)

【公開日】平成18年1月12日(2006.1.12)

【年通号数】公開・登録公報2006-002

【出願番号】特願2004-191542(P2004-191542)

【国際特許分類】

H 04 L 9/08 (2006.01)

【F I】

H 04 L 9/00 6 0 1 B

H 04 L 9/00 6 0 1 F

【手続補正書】

【提出日】平成22年2月26日(2010.2.26)

【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】

データ処理装置であって、

公開鍵及び秘密鍵のペアの初期値を格納する格納手段と、

前記格納手段に格納された公開鍵及び秘密鍵のペアの初期値とは異なる新たな公開鍵及び秘密鍵のペアを生成することなく、前記格納手段に格納された前記公開鍵及び秘密鍵のペアの初期値を用いて外部の端末と暗号通信を行う通信手段とを有することを特徴とするデータ処理装置。

【請求項2】

前記通信手段は、暗号通信によって、前記新たな公開鍵及び秘密鍵のペアを前記外部の端末から受信することを特徴とする請求項1に記載のデータ処理装置。

【請求項3】

前記外部の端末から送られてくるパスワードまたはダイジェスト認証の正当性を判定する正当性判定手段と、

前記正当性判定手段の判定結果に基づいて、管理者権限が付与されたユーザによる公開鍵及び秘密鍵のペアのインストールを許可するインストール許可手段とを有し、

前記格納手段に格納された公開鍵及び秘密鍵のペアの初期値を用いて暗号通信を行って、前記外部の端末から前記新たな公開鍵及び秘密鍵のペアをインストール可能としたことを特徴とする請求項1に記載のデータ処理装置。

【請求項4】

ユーザからの指示により前記データ処理装置内で前記公開鍵及び秘密鍵のペアの初期値を作成する作成手段を有し、

前記作成手段により作成した公開鍵及び秘密鍵のペアの初期値を使用した暗号通信により、前記外部の端末から前記新たな公開鍵及び秘密鍵のペアをインストール可能としたことを特徴とする請求項1～3の何れか1項に記載のデータ処理装置。

【請求項5】

前記格納手段に格納された公開鍵及び秘密鍵のペアの初期値の内容を表示装置に表示する第1の表示手段を有することを特徴とする請求項1～4の何れか1項に記載のデータ処理装置。

【請求項 6】

前記作成手段により作成した公開鍵の初期値を表示装置に表示する第2の表示手段を有することを特徴とする請求項4に記載のデータ処理装置。

【請求項 7】

前記外部の端末からインストールされた新たな公開鍵の値及び公開鍵証明書の内容を表示装置に表示する第3の表示手段を有することを特徴とする請求項2～6の何れか1項に記載のデータ処理装置。

【請求項 8】

前記格納手段に格納された公開鍵の初期値を前記外部の端末に送信する公開鍵送信手段と、

前記公開鍵送信手段により送信された公開鍵の初期値で暗号化された鍵を受信する第1の鍵受信手段と、

前記第1の鍵受信手段により受信された鍵で復号可能に暗号化された前記新たな公開鍵及び秘密鍵のペアを受信する第2の鍵受信手段と、

前記第2の鍵受信手段により受信された暗号化された前記新たな公開鍵及び秘密鍵のペアを、前記第1の鍵受信手段により受信された鍵で復号化する復号化手段とを有することを特徴とする請求項1～7の何れか1項に記載のデータ処理装置。

【請求項 9】

データ処理装置であって、

公開鍵証明書の初期値を格納する格納手段と、

前記格納手段に格納された公開鍵証明書の初期値とは異なる新たな公開鍵証明書を生成することなく、前記格納手段に格納された前記公開鍵証明書の初期値を用いて外部の端末と暗号通信を行う通信手段とを有することを特徴とするデータ処理装置。

【請求項 10】

データ処理装置を用いた暗号通信方法であって、

前記データ処理装置の記憶装置に記憶されている公開鍵及び秘密鍵のペアの初期値または公開鍵証明書の初期値を用いて外部の端末と暗号通信を行う通信工程を有し、

前記格納手段に格納された公開鍵及び秘密鍵のペアの初期値または公開鍵証明書の初期値とは異なる新たな公開鍵及び秘密鍵のペアまたは公開鍵証明書を生成することなく、前記通信工程は暗号通信を行うことを特徴とする暗号通信方法。

【請求項 11】

前記通信工程は、暗号通信によって、前記新たな公開鍵及び秘密鍵のペアを前記外部の端末から受信することを特徴とする請求項1～10に記載の暗号通信方法。

【請求項 12】

データ処理装置において暗号通信をコンピュータに実行させるコンピュータプログラムであって、

前記データ処理装置の記憶装置に記憶されている公開鍵及び秘密鍵のペアの初期値または公開鍵証明書の初期値を用いて外部の端末と通信を行う通信工程を前記コンピュータに実行させ、

前記格納手段に格納された公開鍵及び秘密鍵のペアの初期値または公開鍵証明書の初期値とは異なる新たな公開鍵及び秘密鍵のペアまたは公開鍵証明書を生成することなく前記通信工程をコンピュータに実行させることを特徴とするコンピュータプログラム。

【請求項 13】

前記通信工程は、暗号通信によって、公開鍵及び秘密鍵のペアを前記外部の端末から受信することを特徴とする請求項1～12に記載のコンピュータプログラム。

【手続補正2】

【補正対象書類名】明細書

【補正対象項目名】0011

【補正方法】変更

【補正の内容】

【0011】

本発明のデータ処理装置は、データ処理装置であって、公開鍵及び秘密鍵のペアの初期値を格納する格納手段と、前記格納手段に格納された公開鍵及び秘密鍵のペアの初期値とは異なる新たな公開鍵及び秘密鍵のペアを生成することなく、前記格納手段に格納された前記公開鍵及び秘密鍵のペアの初期値を用いて外部の端末と暗号通信を行う通信手段とを有することを特徴としている。

また、本発明のデータ処理装置の他の特徴とするところは、データ処理装置であって、公開鍵証明書の初期値を格納する格納手段と、前記格納手段に格納された公開鍵証明書の初期値とは異なる新たな公開鍵証明書を生成することなく、前記格納手段に格納された前記公開鍵証明書の初期値を用いて外部の端末と暗号通信を行う通信手段とを有することを特徴としている。

【手続補正3】

【補正対象書類名】明細書

【補正対象項目名】0012

【補正方法】変更

【補正の内容】

【0012】

本発明のデータ処理方法は、データ処理装置を用いた暗号通信方法であって、前記データ処理装置の記憶装置に記憶されている公開鍵及び秘密鍵のペアの初期値または公開鍵証明書の初期値を用いて外部の端末と暗号通信を行う通信工程を有し、前記格納手段に格納された公開鍵及び秘密鍵のペアの初期値または公開鍵証明書の初期値とは異なる新たな公開鍵及び秘密鍵のペアまたは公開鍵証明書を生成することなく、前記通信工程は暗号通信を行うことを特徴としている。

【手続補正4】

【補正対象書類名】明細書

【補正対象項目名】0013

【補正方法】変更

【補正の内容】

【0013】

本発明のコンピュータプログラムは、データ処理装置において暗号通信をコンピュータに実行させるコンピュータプログラムであって、前記データ処理装置の記憶装置に記憶されている公開鍵及び秘密鍵のペアの初期値または公開鍵証明書の初期値を用いて外部の端末と通信を行う通信工程を前記コンピュータに実行させ、前記格納手段に格納された公開鍵及び秘密鍵のペアの初期値または公開鍵証明書の初期値とは異なる新たな公開鍵及び秘密鍵のペアまたは公開鍵証明書を生成することなく前記通信工程をコンピュータに実行することを特徴とする。