【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20年5月15日(2008.5.15)

【公開番号】特開2005-295570(P2005-295570A)
【公開日】平成17年10月20日(2005.10.20)
【年通号数】公開・登録公報2005-041
【出願番号】特願2005-108017(P2005-108017)
【国際特許分類】
*Ｈ０４Ｌ　9/08　(2006.01)*
【ＦＩ】
Ｈ０４Ｌ　9/00　６０１Ｃ
Ｈ０４Ｌ　9/00　６０１Ｅ

【手続補正書】
【提出日】平成20年4月1日(2008.4.1)
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】００２８
【補正方法】変更
【補正の内容】
【００２８】
この実施形態では、サーバローミングアプリケーション２２８は、ローミングクライアントアプリケーション３０４と通信ネットワーク２１２を介して、ローミングクライアント３０２から要求を受信して、データベース２２６からそれに記憶されている暗号化プライベートデータを取り出す。サーバローミングアプリケーション２２８は、受信された要求に応答し、ローミングユーザ３０６を認証するためにウェブサーバ２０４によって実行することができる。この実施形態では、サーバ２０４は、入力フォーム（図示しない）を介してローミングユーザ３０６に認証パスワードを要求する。
【手続補正２】
【補正対象書類名】明細書
【補正対象項目名】００２９
【補正方法】変更
【補正の内容】
【００２９】
上記で図２を参照して説明したやり方と実質的に同じように、サーバローミングアプリケーション２２８は、クライアントから受け取ったある形態の認証パスワードを照合して、ローミングユーザ３０６が、データベースから暗号化データを取り出す権限があるかどうかを判定する。認証パスワードが有効であると認められない場合、サーバローミングアプリケーション２２８は、データベース２２６に記憶された暗号化プライベートデータへのローミングクライアント３０２によるアクセスを拒否する。一方、認証パスワードが有効であると認められた場合、サーバローミングアプリケーション２２８は、参照符号３１０で示すように、データベース２２６から暗号化データを取り出し、参照符号３１１で示すように、その暗号化データをローミングクライアント３０２に転送する。ローミングクライアントアプリケーション３０４は、受け取った暗号化プライベートデータに応答して、ユーザに暗号化パスワード（図示しない）を要求し、ラッピングキーＫ１を生成し、暗号解読アルゴリズム３１２を実行する。この場合、暗号解読アルゴリズム３１２は、受け取った暗号化プライベートデータを、ローミングクライアント３０２で生成されたラッピングキー２３０の関数として解読して、ホームクライアント２０２に関連付けられたプライベートキーを取得する。その後、ローミングクライアントアプリケーション３０４は、

取得したプライベートキーを、ローミングクライアント３０２に関連付けられたメモリ３１４に記憶することができる。