(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2005-295570
(P2005-295570A)
(43)公開日　平成17年10月20日(2005.10.20)

(51)Int.Cl.[7]	F I			テーマコード（参考）
H04L 9/08	H04L	9/00	601C	5J104
	H04L	9/00	601E	

審査請求 未請求　請求項の数 32　ＯＬ　外国語出願　（全 28 頁）

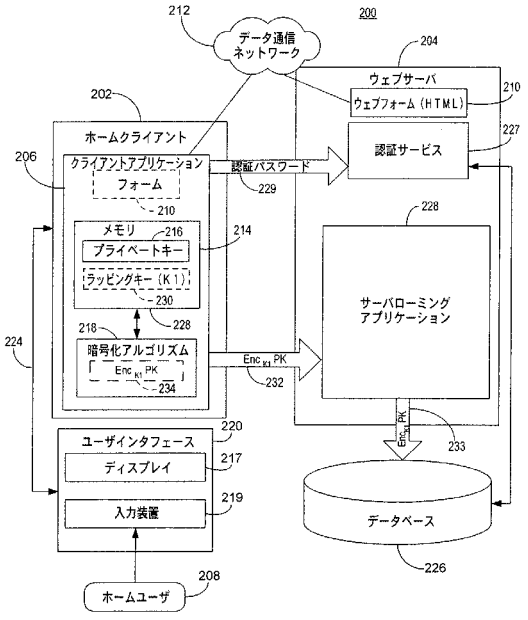
(21)出願番号　特願2005-108017 (P2005-108017)
(22)出願日　平成17年4月4日 (2005.4.4)
(31)優先権主張番号　10/816,756
(32)優先日　平成16年4月2日 (2004.4.2)
(33)優先権主張国　米国 (US)

(71)出願人　500046438
マイクロソフト　コーポレーション
アメリカ合衆国　ワシントン州　９８０５２－６３９９　レッドモンド　ワン　マイクロソフト　ウェイ
(74)代理人　100077481
弁理士　谷　義一
(74)代理人　100088915
弁理士　阿部　和夫
(72)発明者　アダム　バック
アメリカ合衆国　９８０５２　ワシントン州　レッドモンド　ワン　マイクロソフト　ウェイ　マイクロソフト　コーポレーション内

最終頁に続く

(54)【発明の名称】プライベートデータを露出せずに通信ネットワークを介してパスワードで保護されたプライベートデータを回復する方法およびシステム

(57)【要約】
【課題】　通信ネットワークを介して接続した第１のクライアントコンピュータから第２のクライアントコンピュータにプライベートデータを安全に移動するシステムと方法を提供する。
【解決手段】　第１のクライアントコンピュータのユーザが、ホームクライアントアプリケーションを実行し移動するプライベートデータを指示する。ホームクライアントアプリケーションは、パスワードに応答して第１の鍵を生成し、指示されたプライベートデータを第１の鍵の関数として暗号化する。サーバは、暗号化されたプライベートデータを受け取り、記憶する。第２のコンピュータのユーザがローミングクライアントアプリケーションを実行し、サーバから暗号化されたプライベートデータの転送を要求する。ローミングクライアントアプリケーションは、パスワードに応答して第１の鍵を生成し、サーバから転送された暗号化プライベートデータを解読してプライベートデータを得る。
【選択図】　図２



【特許請求の範囲】
【請求項１】
データ通信ネットワークに接続されたコンピュータ間でプライベートデータを通信する方法であって、
ネットワークサーバと第１のクライアントとが前記データ通信ネットワークに接続され、該サーバにとって未知のラッピングキーの関数として該第１のクライアントによって暗号化されたプライベートデータを該ネットワークサーバで受信することと、
前記受信された暗号化プライベートデータを前記サーバで記憶することと、
前記暗号化されたプライベートデータに対する第２のクライアントからの要求を前記サーバで受信することと、
前記受信された要求に応答して、前記ラッピングキーの関数として解読するために、前記暗号化されたプライベートデータを前記サーバから前記第２のクライアントに転送することと
を含むことを特徴とする方法。
【請求項２】
前記暗号化されたプライベートデータを受信することは、暗号化されたプライベートキーを受信することを含み、該暗号化されたプライベートキーは、前記第１のクライアントに関連付けられ、かつ前記ラッピングキーの関数として暗号化されたプライベートキーを表し、該ラッピングキーは、該第１のクライアントのユーザから受け取られる暗号化パスワードに応答して前記第１のクライアントで生成されることを特徴とする請求項１に記載の方法。
【請求項３】
前記暗号化されたプライベートキーを前記ラッピングキーの関数として前記第２のクライアントで解読することをさらに含み、該ラッピングキーは、前記第２のクライアントのユーザから受け取られる前記暗号化パスワードに応答して前記第２のクライアントで生成されることを特徴とする請求項２に記載の方法。
【請求項４】
前記サーバに未知の回復キーの関数として前記第１のクライアントによって暗号化された前記ラッピングキーを前記サーバで受信することであって、該回復キーは、前記ユーザによって選択された回復のオプションに応答して該第１のクライアントで生成されることと、
前記ラッピングキーの関数として前記第１のクライアントによって暗号化された前記回復キーを前記サーバで受信することと
をさらに含むことを特徴とする請求項２に記載の方法。
【請求項５】
暗号化されたプライベートデータが前記第１のクライアントから受信されるのに応答して前記サーバでバックアップキーを生成することと、
前記生成されたバックアップキーを前記サーバに関連付けられたデータベースに記憶することと、
前記第１のクライアントの前記ユーザから受信される回復の要求に応答して、前記記憶されたバックアップキーを取り出すことと、
前記受信された回復要求に応答して、前記バックアップキーを前記サーバから前記データ通信ネットワークを介して前記第１のクライアントに転送することであって、前記第１のクライアントは、前記転送されたバックアップキーの関数として暗号化された前記回復キーを表すバックアップ用の暗号化された回復キーを生成して前記第１のクライアントに記憶し、前記バックアップキーは前記サーバに既知であることと
をさらに含むことを特徴とする請求項４に記載の方法。
【請求項６】
前記受信された回復要求に応答して、前記暗号化されたプライベートキーと前記暗号化されたラッピングキーを前記サーバから前記第１のクライアントに転送することをさらに

備え、該第１のクライアントに記憶された前記バックアップ用の暗号化された回復キーが、前記転送されたバックアップキーの関数として該第１のクライアントで解読されて前記回復キーを取得し、前記暗号化されたラッピングキーが、前記取得された回復キーの関数として前記第１のクライアントで解読されて前記ラッピングキーを取得し、前記暗号化されたプライベートキーが、前記取得されたラッピングキーの関数として前記第１のクライアントで解読されて前記プライベートキーを取得することを特徴とする請求項５に記載の方法。

【請求項７】

前記第２のクライアントのユーザから受信されたバックアップ要求に応答して、前記暗号化された回復キーと前記転送されたバックアップキーを前記第２のクライアントに転送することをさらに備え、該転送された暗号化回復キーが、該第２のクライアントで生成された前記ラッピングキーの関数として該第２のクライアントで解読されて前記回復キーを取得し、該第２のクライアントが、前記転送されたバックアップキーの関数として、前記取得した回復キーを暗号化して前記バックアップ用の暗号化された回復キーを生成し、前記第２のクライアントに関連付けられたメモリに記憶することを特徴とする請求項５に記載の方法。

【請求項８】

前記第２のクライアントのユーザから受け取られた回復要求に応答して、前記サーバに関連付けられた前記データベースから前記記憶されたバックアップキーを取り出すことと、

前記受け取られた回復要求に応答して前記バックアップキーを前記サーバから前記第２のクライアントに転送することと

をさらに含むことを特徴とする請求項５に記載の方法。

【請求項９】

前記第２のクライアントから前記データ通信ネットワークを介して受信された回復要求に応答して、前記暗号化されたプライベートキーと前記暗号化されたラッピングキーを前記サーバから前記第２のクライアントに転送することをさらに含み、該第２のクライアントに記憶された前記バックアップ用の暗号化された回復キーが、前記転送されたバックアップキーの関数として該第２のクライアントで解読されて前記回復キーを取得し、該暗号化されたラッピングキーが、該取得された回復キーの関数として該第２のクライアントで解読され、該暗号化されたプライベートキーが、該取得されたラッピングキーの関数として該第２のクライアントで解読されて前記プライベートキーを取得することを特徴とする請求項５に記載の方法。

【請求項１０】

前記第２のクライアントは、前記データ通信ネットワークに接続されたローミングクライアントコンピュータであることを特徴とする請求項１に記載の方法。

【請求項１１】

請求項１に記載の方法を行うコンピュータ実行可能命令を有することを特徴とする１つまたは複数のコンピュータ可読媒体。

【請求項１２】

データ通信ネットワークでプライベートデータを通信するシステムであって、

当該サーバに未知のラッピングキーの関数として第１のクライアントによって暗号化されたプライベートデータを受信するサーバであって、前記サーバと前記第１のクライアントは、前記データ通信ネットワークに接続されるサーバと、

前記サーバに関連付けられたデータベースであって、前記サーバは、前記受信した暗号化プライベートデータを前記データベースに記憶し、第２のクライアントから受信される暗号化プライベートデータに対する要求に応答して、ラッピングキーの関数として解読するために、前記記憶された暗号化プライベートデータを、同じく前記データ通信ネットワークに接続された前記第２のクライアントに転送するように構成されるデータベースと

を含むことを特徴とするシステム。

【請求項１３】
前記暗号化されたプライベートデータは、前記前記第１のクライアントに関連付けられ、前記ラッピングキーの関数として暗号化されたプライベートキーからなり、前記ラッピングキーは、前記第１のクライアントのユーザから受け取られる暗号化パスワードに応答して前記第１のクライアントで生成されることを特徴とする請求項１２に記載のシステム。
【請求項１４】
前記第１のクライアントは、前記第１のクライアントで前記ラッピングキーを生成し、前記生成したラッピングキーの関数として前記プライベートデータを暗号化し、前記第１のクライアントに記憶される回復キーを生成するように構成されることを特徴とする請求項１３に記載のシステム。
【請求項１５】
前記第２のクライアントは、前記第２のクライアントコンピュータで前記ラッピングキーを生成し、前記第２のクライアントで生成された前記ラッピングキーの関数として、前記転送された暗号化プライベートデータを解読するように構成され、前記ラッピングキーは、前記第２のクライアントのユーザから受け取られる暗号化パスワードに応答して前記第２のクライアントコンピュータで生成されることを特徴とする請求項１３に記載のシステム。
【請求項１６】
サーバアプリケーションを実施するコンピュータ可読命令をさらに備え、前記サーバは、前記第１のクライアントコンピュータのユーザから受け取られた記憶要求に応答して前記サーバアプリケーションを実行して、前記受信した暗号化データを前記データベースに記憶し、前記データベースに記憶するバックアップキーを生成し、前記生成したバックアップキーを前記第１のクライアントコンピュータに転送し、前記バックアップキーが前記第１のクライアントコンピュータによって使用されて、前記第１のクライアントコンピュータに記憶する第２の暗号化された回復キーを生成することを特徴とする請求項１５に記載のシステム。
【請求項１７】
前記バックアップキーは、前記第１のクライアントから暗号化されたプライベートデータを受信するのに応答して前記サーバによって無作為に生成されることを特徴とする請求項１６に記載のシステム。
【請求項１８】
前記受信される暗号化プライベートデータは、前記ラッピングキーの関数として暗号化された、前記第１のクライアントに関連付けられたプライベートキーを表す暗号化されたプライベートキーと、前記回復キーの関数として暗号化された前記ラッピングキーを表す暗号化ラッピングキーと、前記ラッピングキーの関数として暗号化された前記回復キーを表す第１の暗号化された回復キーとを含むことを特徴とする請求項１７に記載のシステム。
【請求項１９】
前記サーバはさらに、前記第２のクライアントから受け取られるバックアップ要求に応答して、前記第１の暗号化された回復キーと前記バックアップキーとを前記第２のクライアントに転送するように構成され、前記バックアップ要求は、定義されたバックアップパスワードを含み、前記転送された第１の暗号化回復キーが、前記第２のクライアントコンピュータで生成された前記ラッピングキーの関数として前記第２のクライアントで解読されて前記回復キーを取得し、前記取得された回復キーが前記転送されたバックアップキーの関数として暗号化されて、前記第２のクライアントコンピュータに関連付けられたメモリに記憶する前記第２の暗号化回復キーを生成することを特徴とする請求項１８に記載のシステム。
【請求項２０】
前記サーバはさらに、前記第２のクライアントコンピュータから受け取られる回復要求

に応答して、前記暗号化されたプライベートキー、前記生成されたバックアップキー、および前記暗号化されたラッピングキーを前記第２のクライアントコンピュータに転送するように構成され、前記第２のクライアントコンピュータに関連付けられた前記メモリに記憶された前記第２の暗号化された回復キーが、前記転送されたバックアップキーの関数として前記第２のクライアントで解読されて前記回復キーを取得し、前記転送された暗号化ラッピングキーが、前記取得された回復キーの関数として前記第２のクライアントで解読されて前記ラッピングキーを取得し、前記転送された暗号化プライベートキーが、前記取得されたラッピングキーの関数として前記第２のクライアントで解読されて前記プライベートキーを取得することを特徴とする請求項１９に記載のシステム。

【請求項２１】

データ通信ネットワークに接続されたコンピュータ間でプライベートデータを通信するコンピュータ実行可能命令を備えるコンピュータ可読媒体であって、

ネットワークサーバに未知のラッピングキーの関数として第１のクライアントによって暗号化されたプライベートデータを前記サーバで受信する第１の受信命令であって、前記サーバと前記第１のクライアントは、前記データ通信ネットワークに接続される第１の受信命令と、

前記受信された暗号化プライベートデータを前記サーバに記憶する記憶命令と、

前記暗号化されたプライベートデータに対する第２のクライアントからの要求を前記サーバで受信する第２の受信命令と、

前記受信された要求に応答して、前記ラッピングキーの関数として解読するために前記暗号化されたプライベートデータを前記サーバから前記第２のクライアントに転送する転送命令とを備えることを特徴とするコンピュータ可読媒体。

【請求項２２】

前記第１の受信命令は、前記第１のクライアントに関連付けられ、前記ラッピングキーの関数として暗号化されたプライベートキーを表す暗号化されたプライベートキー（$E_{K_1}PK$）を受信する命令を含み、前記ラッピングキーは、前記第１のクライアントのユーザから受け取られる暗号化パスワードに応答して前記第１のクライアントで生成されることを特徴とする請求項２１に記載のコンピュータ可読媒体。

【請求項２３】

前記転送命令は、前記暗号化されたプライベートキーを転送する命令を含み、前記暗号化されたプライベートキーは、前記ラッピングキーの関数として前記第２のクライアントで解読され、前記ラッピングキーは、前記第２のクライアントのユーザから受け取られた前記暗号化パスワードに応答して前記第２のクライアントで生成されることを特徴とする請求項２２に記載のコンピュータ可読媒体。

【請求項２４】

前記第１の受信命令はさらに、前記サーバに未知の回復キーの関数として前記第１のクライアントによって暗号化された前記ラッピングキーを前記サーバで受信する命令であって、前記回復キーは、前記第１のクライアントを介して前記ユーザによって選択される回復のオプションに応答して前記第１のクライアントで生成される命令と、前記ラッピングキーの関数として前記第１のクライアントによって暗号化された前記回復キーを前記サーバで受信する命令とを含むことを特徴とする請求項２２に記載のコンピュータ可読媒体。

【請求項２５】

データ通信ネットワークに接続されたコンピュータ間でプライベートデータを通信する方法であって、

暗号化されたプライベートデータに対するローミングクライアントからの要求をサーバで受信することであって、該要求は、認証パスワードのダイジェストまたはハッシュ値を含み、前記サーバと前記ローミングクライアントは、前記データ通信ネットワークに接続されていることと、

前記ローミングクライアントから受信されたある形態の前記認証パスワードが有効であるかどうかを判定することと、

前記ある形態の前記認証パスワードが有効である場合、前記サーバに未知の暗号化パスワードの関数として以前に暗号化されたプライベートデータを取り出すことと、
前記ラッピングキーの関数として解読するために、前記取り出した暗号化プライベートデータを前記サーバから前記ローミングクライアントに転送することと
を含むことを特徴とする方法。
【請求項２６】
前記暗号化されたプライベートデータを取り出すことは、暗号化されたプライベートキーを取り出すことを含み、前記暗号化されたプライベートキーは、前記ホームクライアントに関連付けられ、前記ラッピングキーの関数として暗号化されたプライベートキーを表し、前記ラッピングキーは、前記ホームクライアントのユーザから受け取られる暗号化パスワードに応答して前記ホームクライアントで生成されることを特徴とする請求項２５に記載の方法。
【請求項２７】
前記転送された暗号化プライベートキーを前記ラッピングキーの関数として前記ローミングクライアントで解読することをさらに含み、前記ラッピングキーは、前記ローミングクライアントのユーザから受け取られる前記暗号化パスワードに応答して前記ローミングクライアントで生成されることを特徴とする請求項２６に記載の方法。
【請求項２８】
前記サーバに未知の回復キーの関数として前記ホームクライアントで暗号化された前記ラッピングキーを取り出すことであって、前記回復キーは、前記ホームクライアントを介して前記ユーザによって選択された回復のオプションに応答して前記ホームクライアントで生成されることと、
前記ラッピングキーの関数として前記ホームクライアントによって暗号化された前記回復キーを取り出すことと、
前記暗号化された回復キーを、前記ローミングクライアントで生成された前記ラッピングキーの関数として前記ローミングクライアントで解読して、前記回復キーを取得することと、
前記ローミングクライアントのユーザから受け取られるバックアップ要求に応答して、記憶されたバックアップキーを取り出すことであって、前記バックアップキーは、前記ホームクライアントから暗号化されたプライベートデータを受信するのに応答して前記サーバで生成されることと、
前記受信された回復要求に応答して、セキュリティが保護された方式で前記バックアップキーを前記サーバから前記データ通信ネットワークを介して前記ローミングクライアントに転送することであって、前記ローミングクライアントは、前記取り出されたバックアップキーの関数として前記取得された回復キーを暗号化することと、
前記転送されたバックアップキーの関数として暗号化された前記回復キーを表すバックアップ用の暗号化回復キーを前記ローミングクライアントに記憶することと
を含むことを特徴とする請求項２７に記載の方法。
【請求項２９】
前記ローミングクライアントのユーザから受け取られる回復要求に応答して前記記憶されたバックアップキーを取り出すことであって、前記バックアップキーは、前記ホームクライアントから暗号化されたプライベートデータを受信するのに応答して前記サーバで生成されることと、
前記受信された回復要求に応答して、セキュリティが保護された方式で前記バックアップキーを前記サーバから前記データ通信ネットワークを介して前記ローミングクライアントに転送することであって、前記ローミングクライアントは、前記バックアップ用の暗号化回復キーを解読して前記回復キーを取得することと
をさらに含むことを特徴とする請求項２８に記載の方法。
【請求項３０】
前記受信された回復要求に応答して前記暗号化されたプライベートキーと前記暗号化さ

れたラッピングキーを前記サーバから前記ローミングクライアントに転送することをさらに含み、前記暗号化されたラッピングキーが、前記取得された回復キーの関数として前記ローミングクライアントで解読されて前記ラッピングキーを取得し、前記暗号化されたプライベートキーが前記取得されたラッピングキーの関数として前記ローミングクライアントで解読されて前記プライベートキーを取得することを特徴とする請求項２９に記載の方法。

【請求項３１】

データ構造が記憶されたコンピュータ可読媒体であって、該データ構造は、

プライベートデータを含む第１のデータフィールドと、

ユーザから受け取られた入力データストリームを表す鍵データを含む第２のデータフィールドと、

前記鍵データの関数として前記プライベートデータを暗号化し、前記暗号化されたプライベートデータを記憶装置の中心位置に転送するための第３の機能フィールドと

を備えることを特徴とするコンピュータ可読媒体。

【請求項３２】

前記暗号化されたプライベートデータは、暗号化されたプライベートキーを含み、前記暗号化されたプライベートキーは、ホームクライアントに関連付けられ、ラッピングキーの関数として暗号化されたプライベートキーを表し、前記ラッピングキーは、前記ホームクライアントのユーザから受け取られた暗号化パスワードに応答して前記ホームクライアントで生成されることを特徴とする請求項３１に記載のコンピュータ可読媒体。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、コンピュータネットワーク環境の分野に関する。詳細には、本発明は、通信ネットワークを介してつながれた１つまたは複数のクライアントコンピュータ間を巡ることが可能なプライベートデータ（非公開データ、秘密データともいう）をバックアップおよび回復するシステムおよび方法に関する。

【背景技術】

【０００２】

インターネットサイトなどのウェブサービスは、非常に多くの場合、情報、プロダクト、サービスなどをユーザに提供する。しかし、ユーザとウェブサービス双方にとっての大きな問題は、特に機密性のある情報を送信する際のインターネットの安全性（セキュリティ）である。情報の安全性は、多くの場合、暗号化方式を通じてユーザおよび／またはウェブサービスに提供される。例えば、公開鍵基盤（ＰＫＩ）と公開鍵暗号システムが、通信の安全性のための良く知られた鍵管理サービスである。プライベートキー（秘密鍵、私有鍵、非公開鍵ともいう）は秘密性を保つために安全に記憶しなければならないので、上記のサービスは、通常、１台のコンピュータでしか利用することができない。したがって、プライベートキーをローミングし、バックアップを作成し、回復できることが望ましい。

【発明の開示】

【発明が解決しようとする課題】

【０００３】

既存のプライベートキー（秘密鍵）ローミングプロトコルは、ユーザが主要（プライマリ）パスワードを思い出せないときに、終端間のセキュリティ上の問題とデータの回復に対応することができない。したがって、ユーザデータとユーザ通信の機密性、秘密性、完全性、および真正性に対応しながら、非公開のユーザデータをローミングするシステムが望まれる。

【課題を解決するための手段】

【０００４】

本発明は、通信ネットワークを介してつながれた１つまたは複数のクライアント間での

秘密性のある情報の改良されたローミングに関する。詳細には、本発明は、サーバが秘密情報の知識を得ることなく、あるいは秘密情報を受け取ることなく、サーバにリンクされたクライアント間で秘密情報（プライベートキーなど）をローミングする能力をユーザに提供する。さらに、本発明は、ユーザがそのプライベートキーの暗号化に関連付けられたパスワードを思い出せない場合でも、クライアントで解読するために、暗号化されたバージョンのプライベートキーをサーバから取り出す能力をユーザに与える。クライアント間で秘密情報をローミングし、そのような情報をサーバに隠す能力をユーザに与えることにより、ネットワークの安全性が大幅に強化され、したがって、悪意あるユーザが、セキュリティの保護された通信を妨害する能力は著しく低下する。

【０００５】

本発明の一態様によれば、データ通信ネットワークに接続されたコンピュータ間でプライベートデータを通信する方法が提供される。この方法は、サーバにとって未知のラッピングキーの関数として第１のクライアントによって暗号化されたプライベートデータをネットワークサーバで受け取ることを含む。サーバと第１のクライアントは、データ通信ネットワークに接続されている。この方法はさらに、受け取った暗号化プライベートデータをサーバで記憶することを含む。この方法は、暗号化されたプライベートデータに対する第２のクライアントからの要求をサーバで受け取ることも含む。この方法はさらに、受け取られた要求に応答して、ラッピングキーの関数として解読するために、暗号化されたプライベートデータをサーバから第２のクライアントに転送することも含む。

【０００６】

本発明の別の態様によれば、データ通信ネットワーク上でプライベートデータを通信するシステムが提供される。サーバが、サーバに未知のラッピングキーの関数として第１のクライアントによって暗号化されたプライベートデータを受け取る。サーバと第１のクライアントは、データ通信ネットワークに接続されている。サーバにデータベースが関連付けられる。サーバは、受け取った暗号化プライベートデータをそのデータベースに記憶するように構成される。サーバは、第２のクライアントから受け取られた暗号化されたプライベートデータに対する要求に応答して、ラッピングキーの関数として解読するために、記憶された暗号化プライベートデータを、データ通信ネットワークに接続された第２のクライアントに転送するようにも構成される。

【０００７】

本発明の別の態様によれば、データ通信ネットワークに接続されたコンピュータ間でプライベートデータを通信するコンピュータ実行可能命令を有するコンピュータ可読媒体が提供される。第１の受信命令は、サーバに未知のラッピングキーの関数として第１のクライアントによって暗号化されたプライベートデータをネットワークサーバで受け取る。サーバと第１のクライアントは、データ通信ネットワークに接続されている。記憶命令は、受け取った暗号化プライベートデータをサーバに記憶する。第２の受信命令は、暗号化されたプライベートデータに対する第２のクライアントからの要求をサーバで受信する。転送命令は、受け取られた要求に応答して、ラッピングキーの関数として解読するために、暗号化されたプライベートデータをサーバから第２のクライアントに転送する。

【０００８】

本発明のさらに別の態様によれば、データ通信ネットワークに接続されたコンピュータ間でプライベートデータを通信する方法が提供される。この方法は、暗号化されたプライベートデータに対するローミングクライアントからの要求をサーバで受信することを含む。この要求は、認証パスワードのダイジェストあるいはハッシュ値を含む。サーバとローミングクライアントは、データ通信ネットワークに接続されている。この方法はさらに、ローミングクライアントから受け取られたある形態の認証パスワードが有効であるかどうかを判定することを含む。この方法はさらに、ある形態の認証パスワードが有効である場合、暗号化されたプライベートデータを取り出すことを含み、プライベートデータは、サーバに未知の暗号化パスワードの関数としてあらかじめ暗号化されている。この方法はさらに、ラッピングキーの関数として解読するために、取り出された暗号化プライベートデ

ータをサーバからローミングクライアントに転送することを含む。
【０００９】
本発明の別の態様によれば、データ構造が記憶されたコンピュータ可読媒体が提供される。第１のデータフィールドは、プライベートデータを含む。第２のデータフィールドは、ユーザから受け取られた入力データストリームを表す鍵データを含む。第３の機能フィールドは、鍵データの関数としてプライベートデータを暗号化し、暗号化されたプライベートデータを記憶装置の中心位置に転送する。
【００１０】
これに代えて、本発明は、各種の他の方法および装置を備えることができる。
【００１１】
以下で、この他の特徴が部分的には明らかになり、部分的には指摘される。
【００１２】
すべての図面を通じて、同じ参照符号は、同じ部分を示す。
【発明を実施するための最良の形態】
【００１３】
さて、図１を参照すると、ホームあるいはローカルクライアントコンピュータ１０２がデータ通信ネットワーク１０４に接続されている。この例では、ネットワーク１０４は、インターネット（あるいはワールドワイドウェブ）である。ただし、本発明の教示は、どのようなデータ通信ネットワークにも適用することができる。複数のローミングあるいはリモートクライアントコンピュータ１０６および１０８もネットワーク１０４に接続されている。そして、ホームクライアントコンピュータ１０２は、ネットワーク１０４を介してローミングクライアントコンピュータ１０６および１０８と通信することができる。信頼できない第３者はコンピュータ１０２への制限のないアクセス権あるいは容易な物理的アクセス権を持たないので、ホームクライアントコンピュータ１０２は、そのユーザが信頼に対する根拠を有するコンピュータを表す。ローミングクライアントコンピュータ１０６および１０８は、第３者により所有され、物理的に制御されるため、ユーザの信頼がより制限されたコンピュータを表す。ネットワーク１０４に接続された認証サーバ１１０が、認証サーバ１１０と、ホームクライアントコンピュータ１０２と、ローミングクライアントコンピュータ１０６および１０８との間の通信を可能にする。「認証サーバ」と称するが、図１の実施形態の認証サーバ１１０は、単に、ユーザを認証することができるもので、ウェブブラウザおよび他のウェブサーバと対話することが可能なウェブサーバである。
【００１４】
この例では、データは、情報を安全に交換するために一般にインターネットで使用されるプロトコルであるＳＳＬ（セキュアソケットレイヤ：セキュリティ規格の１つ）を使用して、認証サーバ１１０、クライアントコンピュータシステム１０２、およびローミングクライアントコンピュータ１０６と１０８間で安全に通信される。より具体的には、ＳＳＬを使用して公開鍵の暗号化を実施することができる。当業者には知られるように、公開鍵の暗号化には、プライベートキー（秘密鍵、私有鍵、非公開鍵ともいう）を有する者（あるいはコンピュータ）だけがその情報を復号できるような方式で情報を符号化することが必要となる。現在使用されるコンピュータ暗号化システムには、対称鍵暗号化（共通鍵暗号化ともいう）と公開鍵暗号化がある。
【００１５】
対称鍵暗号化では、各コンピュータがプライベートキー（コード）を有し、それを使用して情報のパケットを暗号化した後、そのパケットがネットワークを介して別のコンピュータに送信される。対称鍵では、各コンピュータに鍵をインストールすることができるように、通信相手のコンピュータを知っていることが必要となる。このタイプの暗号化を成功させるには、双方のコンピュータが、情報を復号するために暗号（secret code）を知らなければならない。
【００１６】

公開鍵暗号化では、プライベートキー（秘密鍵）と公開鍵の組み合わせが情報の符号化と復号化に使用される。例えば、特定の送信元コンピュータ（ホームクライアント）が、公開鍵／プライベートキーの対を有するローミングクライアント（移動するクライアント）に、安全に情報を送信する。送信元コンピュータは、情報に関して行われる数学的操作でローミングクライアントの公開鍵を利用して暗号化されたメッセージを生成し、自身のプライベートキーでそのメッセージに署名してメッセージの完全性（integrity）をアサートする（有効な状態にする）ことができる。送信元コンピュータは、自身の公開鍵をローミングクライアントに提供するが、プライベートキー（秘密鍵）は、送信元のコンピュータに非公開（すなわち秘密）のままにされる。暗号化メッセージを復号するには、受信者は、自身のプライベートキーを使用しなければならず、送信者から提供された公開鍵を使用してそのメッセージ上の署名を照合する。したがって、ホームクライアント１０２のユーザである受信者が、ローミングクライアント１０６および１０８を介して暗号化メッセージを復号する能力を望む場合には、ユーザは、プライベートキーをそれらのローミングクライアントに転送しなければならない。

【００１７】

認証サーバ１１０は、認証データベース１１２が接続され、クライアントコンピュータシステム１０２のユーザ（およびネットワーク上の他のユーザ）を認証するのに必要な情報と、ホームクライアントコンピュータまたはローミングクライアントコンピュータのユーザがデータベースに暗号データを記憶する、かつ／またはデータベース１１２から暗号データを受け取る権限を有するかどうかを判定するのに必要な情報を保持する。

【００１８】

次に、図２を参照すると、ブロック図により、本発明の一実施形態による、ホームクライアント２０２（例えばホームクライアントコンピュータ１０２）とウェブサーバ２０４（例えば認証サーバ１１０）の間で暗号化されたプライベートデータを通信するシステム２００を示す。

【００１９】

ホームクライアントアプリケーション２０６は、ホームユーザ２０８が、プライベートデータを暗号化し、その暗号化したプライベートデータを通信ネットワーク２１２（例えばネットワーク１０４）を介してウェブサーバ２０４に転送することを可能にする。ホームクライアントアプリケーション２０６は、ホームクライアント２０２によって実行することができ、プライベートデータの暗号化と、その暗号化したプライベートデータのウェブサーバ２０４への転送を開始させるユーザ入力に応答する。この実施形態では、ホームクライアントアプリケーション２０６は、図１を参照して上述したような公開鍵の暗号化プロセスで使用されるプライベートキー２１６を記憶するメモリ２１４を包含する。ホームクライアントアプリケーション２０６は、プライベートデータに数学的操作を行ってそれを暗号化されたプライベートデータに変換する暗号化アルゴリズム２１８を含む。より具体的には、鍵データと併せて暗号化アルゴリズム２１８を使用してプライベートデータを変換する。当業者によく知られているように、いくつかの暗号化アルゴリズム（３ＤＥＳやＨＭＡＣ－ＲＣ４など）を使用して、暗号鍵（encryption key）を知らないで内容を復号することがほぼ不可能となるように、データを暗号化することができる。

【００２０】

ホームクライアント２０２のユーザ２０８は、１つまたは複数のローミングクライアント（例えば、ローミングクライアント１０６、１０８）を介して安全にウェブサービスと通信するために、プライベートキー２１６をローミング（移動）する能力を望む場合がある。しかし、そのようにプライベートキー２１６をローミングすると、プライベートキー２１６が悪意のある者に傍受されてしまう可能性がある。その結果、その特定のプライベートキー２１６で安全に（セキュリティを確保して）データを復号する、あるいはデータに署名するユーザ２０８の能力が、著しく損なわれる可能性がある。

【００２１】

ホームクライアント２０２に結び付けられたユーザインタフェース（ＵＩ）２２０によ

り、ユーザ２０８は、ウェブブラウザ２０４と対話することができる。ＵＩ２２０は、例えば、データおよび／または入力フォームを表示するコンピュータモニタなどのディスプレイ２１７と、入力フォーム（図示せず）にデータを入力するためのキーボードまたはポインティングデバイス（マウス、トラックボール、ペン、タッチパッドなど）などの入力装置２１９とを含むことができる。すなわち、ＵＩ２１４により、ユーザ２０８は、暗号化するホームクライアント２１０上のデータを選択し、暗号化したデータを、記憶するためにホームクライアント２０２からウェブサーバ２０４に転送する要求を提出することができる。

【００２２】

データベース２２６（データベース１１０など）がウェブサーバ２０４に接続され、暗号化されたプライベートデータをデータベース２２６に記憶することを求めるホームクライアント２０２（ならびにネットワーク上の他のユーザ）からの要求を検証するのに必要な情報を保持する。データベース２１０は認証サーバ（ウェブサーバ）２０４と別個になっているが、本発明の他の実施形態では、データベース２２６はウェブサーバ２０４の中に含めることができることを理解されたい。

【００２３】

一実施形態では、ウェブサーバ２０４は、サーバ２０４へのアクセスを要求するユーザ２０８を認証する認証サービス２２７を実行するログインサーバである。そのような実施形態では、ウェブサーバ２０４は、ウェブサーバ２０４によって提供されるウェブサービスへのユーザアクセスを許可する前に、参照符号２２９で示すように初めに認証パスワードなどの認証情報をユーザ２０８に要求する。

【００２４】

さらに図２を参照すると、ホームクライアント２０２は、ホームクライアントアプリケーション２０６を使用して、暗号化されたプライベートキーをサーバ２０４に記憶することを求める。その前に、ホームクライアントアプリケーション２０６は、サーバ２０４に対してユーザ２０８を認証する／権限を付与する必要がある。この実施形態では、ユーザ２０８から提供される認証パスワードを使用してサーバ２０４に対してユーザ２０８を認証する。

【００２５】

安全に（セキュリティを確保して）プライベートデータを転送し、記憶するために、ホームクライアントアプリケーション２０６は、暗号化パスワードなどの入力データをユーザ２０８に要求する。ホームクライアントアプリケーション２０６とＵＩ２２０は、ユーザ２０８が暗号化パスワードを入力できるようにしている。ホームクライアントアプリケーション２０６は、ユーザ２０８によって入力された暗号化パスワードに応答してラッピングキーＫ１　２３０を生成し、そのキーでプライベートデータを暗号化する。この実施形態では、ラッピングキーＫ１は、プライベートキーを暗号化する（例えば、ハッシュ値を生成する）ために使用される対称鍵である。ホームクライアントアプリケーション２０６は、参照符号２３２で示すように、暗号化されたプライベートデータをサーバのローミングアプリケーション２２８に転送する。認証パスワードと暗号化パスワードは、ユーザデータの秘密性を保護するために別個のパスワードとして図解している。しかし、それらのパスワードは１つのパスワードとしてもよいことは理解されよう。また、ウェブサーバ２０４は、スマートカード（メモリ内蔵カード）、ワンタイムパスワード（使い捨てパスワード）、バイオメトリクス（生体測定）など、異なる認証機構を用いてユーザ２０８を認証できることも理解されよう。

【００２６】

サーバ２０４によって実行されるサーバローミングアプリケーション２２８（すなわち、ウェブサービス）は、参照符号２３３で示すように、受け取った暗号化プライベートデータをデータベース２２６に記憶する。この例では、プライベートデータは、メモリ２１４に記憶されたプライベートキー２１６であり、このプライベートキーは、生成されたラッピングキー２３０の関数として暗号化アルゴリズム２１８により暗号化されて、暗号化

されたプライベートキーE_{K1}ＰＫ２３４を生成する。注意すべき点として、生成されたラッピングキーとプライベートキー２１６は、ウェブサーバ２０４にとって未知のままにされていることである。さらに、サーバは、ラッピングキー２３０の生成に使用される暗号化パスワードを所有していないので、サーバローミングアプリケーションは、暗号化されたプライベートデータ２３４を解読することができない。

【００２７】

次に、図３を参照すると、本発明の一実施形態によるローミングクライアント３０２とウェブサーバ２０４間で暗号化プライベートデータを通信するシステム３００をブロック図で示す。

【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、図２Ａに示すような入力フォーム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。

【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３０８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（３０８は図３では誤って図示されている）。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。

【００３０】

次に、図４を参照すると、ブロック図により、本発明の別の好ましい実施形態による、ホームクライアントコンピュータ２０２とサーバ２０４間で暗号化されたプライベートデータと回復データを通信するシステム４００を示す。

【００３１】

この実施形態では、ホームユーザ２０８は、データをＵＩ２２０を使用して、暗号化パスワードを思い出させないときでさえも、サーバ２０４に記憶された暗号化プライベート回復することができる回復のオプションを選択する。この実施形態では、上記で図２を参照して述べたように、ローミングクライアントアプリケーション２０６は、暗号化パスワードの関数としてラッピングキーＫ１を生成するのに加えて、回復キー要求に応答して、新しい暗号鍵（すなわち回復キーＫ２）を無作為に生成する。例えば、ユーザ２０８は、フォーム（図示せず）に暗号化パスワードを入力した後、例えば、メッセージ「暗号化パスワードなしでプライベートデータの回復を可能にする」を表示するダイアログボックスとともにユーザに提示される「ＹＥＳ」ボタンを、マウスを使用してクリックする。ホームクライアントアプリケーション２０６は、ユーザによる「ＹＥＳ」の選択に応答して、

回復キーＫ２を無作為に生成する。注意すべき点として、Ｋ２は、どのような形でも暗号化パスワードに結び付けられない。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認証パスワードを検証して承認することによりユーザ２０８を認証する。認証パスワードが有効であることが確認されると、ユーザ２０８は、暗号化されたプライベートデータをサーバ２０４に転送することが許可され、このプライベートデータは、それぞれ４１８、４２０、４２２で示すように、ラッピングキーE_{K1}ＰＫ２３４で暗号化されたプライベートキー、回復キーE_{K2}Ｋ１　４１４で暗号化されたラッピングキー、および、ラッピングキーE_{K1}Ｋ２　４１６で暗号化された回復キーを含む。サーバローミングアプリケーション２２８は、受け取った暗号化プライベートデータに応答して、それぞれ４２１、４２２、４２３で表すように、E_{K1}ＰＫと、E_{K2}Ｋ１と、E_{K1}Ｋ２をデータベース２２６に記憶する。さらに、サーバローミングアプリケーション２２８は、ホームクライアント２０２から受け取った暗号化データに応答して、参照符号４２５で表すように、データベース２２６に記憶するためのバックアップキーＫ３　４２４を無作為に生成し、４２６で示すように、生成したバックアップキー４２４をホームクライアント２０２に転送する。Ｋ３の転送は、セキュリティ機能が確保されたチャネル（secure channel）（例えば、ＳＳＬ（secure socket layer）上で）を介して行われることに留意されたい。セキュアチャネルがないと、値が変更される可能性があり、それゆえ回復キーが容易に発見されてしまう。ホームクライアントアプリケーション２０６は、受け取ったバックアップキー４２４に応答して、第２の暗号化された回復キーE_{K3}Ｋ２　４２８を生成し、これをホームクライアント２０２に関連付けられたメモリ２１４および／またはディスクに記憶する。

【００３２】

この実施形態では、暗号化アルゴリズム２１８を使用して、暗号化されたプライベートキー２３４、暗号化されたラッピングキー４１４、第１の暗号化された回復キー４１６、および第２の暗号化された回復キー４２８を生成する。暗号化されたプライベートキー２３４は、ラッピングキーの関数として暗号化されたプライベートキーに相当し、暗号化されたラッピングキー４１４は、回復キーＫ２の関数として暗号化されたラッピングキーに相当し、第１の暗号化された回復キー４１６は、ラッピングキーＫ１の関数として暗号化された回復キー４０８に相当し、第２の暗号化された回復キー４２８は、バックアップキー４２４の関数として暗号化された回復キー４０８に相当する。本明細書では同じ暗号化アルゴリズムを使用するものとして本発明を説明しているが、異なる暗号化鍵のそれぞれを生成するために異なる暗号化アルゴリズムを使用できることが意図されている。

【００３３】

次に、図５を参照すると、ブロック図により、本発明の一実施形態による、サーバ２０４からローミングクライアント３０２に回復データを転送するシステム５００を示す。

【００３４】

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、遠隔の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とを介して、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からバックアップデータを取り出す。この例では、バックアップデータは、第１の暗号化された回復キー４１６とバックアップキー４２４である。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検証し承認することによりユーザ２０８を認証する。認証パスワードが有効であると確認された場合、サーバローミングアプリケーション２２８は、それぞれ参照符号５０６、５０８で示すように、データベース２２６から第１の暗号化された回復キー４１６とバックアップキー４２４を取り出し、それぞれ参照符号５１０、５１２で示すように、E_{K1}Ｋ２とＫ３をローミングクライアントアプリケーション３０４に転送する。一方、認証パスワードが有効と認められない場合には、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へのアクセスを拒否する。

【００３５】

ローミングクライアントアプリケーション３０４は、受け取った第１の暗号化回復キー

４１６に応答して、ユーザに暗号化パスワード５０４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、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、受け取った第１の暗号化された回復キー４１６を解読して、ホームクライアントコンピュータ２０２に関連付けられた回復キー４０８を取得する。ローミングクライアントアプリケーション３０４は、受け取ったバックアップキー４２４に応答して暗号化アルゴリズム２１８を実行する。この場合、暗号化アルゴリズム２１８は、受け取ったバックアップキー４２４の関数として、取得した回復キー４０８を暗号化して、第２の暗号化された回復キー４２８を生成する。その後、ローミングクライアントアプリケーション３０４は、第２の暗号化された回復キー４２８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とディスクに記憶する。メモリ３１４に記憶された第２の暗号化された回復キー４２８、サーバから得たバックアップキー４２４および暗号化されたラッピングキーを得た結果、ローミングクライアント３０２は、ラッピングキーＫ１を生成するために使用されたパスワード（すなわち、暗号化パスワード）の知識を持たずに、データベース２２６に記憶された暗号化プライベートキー２３４を回復し、解読することができる。

【００３６】

次に、図６を参照すると、ブロック図により、本発明の一実施形態による、暗号化パスワードの知識を持たずに、ローミングクライアント３０２でウェブサーバ２０４から暗号化されたプライベートデータを回復するシステム６００を示す。

【００３７】

この実施形態では、すでに上記のバックアッププロセスがローミングクライアント３０２で行われ、ローミングクライアント３０２は、メモリ３１４に第２の暗号化された回復キー４２８を有する。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とを介してローミングクライアント３０２からの要求を受信して、データベース２２６から、プライベートキー２１６などの暗号化された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、クライアントから受け取った認証パスワードの有効性を検証し承認することによりユーザ３０２を認証する。ユーザの認証が成功すると、サーバアプリケーションは、暗号化されたプライベートデータ２１６をローミングクライアントアプリケーション３０４に転送する。図３および図５を参照して上記で説明したように、ローミングクライアントアプリケーション３０４は、暗号化されたプライベートデータに応答して、ラッピングキーＫ１を生成するためにローミングユーザ３０６に暗号化パスワードを要求する。

【００３８】

ユーザ３０６が暗号化パスワードを覚えていない場合、ユーザは例えばＵＩを使用して、「暗号化パスワードを入力せずにプライベートデータを回復する」というメッセージを表示する別のダイアログボックス（図示せず）とともにユーザに提示される「ＹＥＳ」の選択肢を選択する。サーバローミングアプリケーション２２８は、回復要求に応答して、それぞれ参照符号６０４、６０６、６０８で示すように、データベース２２６からバックアップキー４２４、暗号化されたプライベートキー２３４、および暗号化されたラッピングキー４１４を取り出し、それぞれ参照符号６１０、６１２、６１４で示すように、取り出したＫ３、E_{K1}ＰＫ、E_{K2}Ｋ１をローミングクライアントアプリケーション３０４に転送する。

【００３９】

ローミングクライアントアプリケーション３０４は、受け取ったバックアップキー４２４、暗号化されたプライベートキー２３４、および暗号化されたラッピングキー４１４に応答して、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、受け取ったバックアップキー４２４の関数として、それまでメモリに記憶されていた（図５参照）第２の暗号化回復キー４２８を解読して、ホームクライアント２０２に関連付けられた回復キー４０８を取得する。暗号解読アルゴリズム３１２は、次に、取得した回復キー４０８の関数として、受け取った暗号化ラッピングキー４１４を解読して、

ラッピングキー２３０を得る。暗号解読アルゴリズム３１２は次いで、取得したラッピングキー２３０の関数として、受け取った暗号化プライベートキー２３４を解読して、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２１６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ＰＫを、ローミングクライアント３０２に関連付けられたメモリ２１４に記憶する。

【００４０】

次に、図７を参照して、例示的なフローチャートにより、本発明の一実施形態による、ホームクライアントコンピュータとサーバ間でプライベートデータを通信してローミングクライアントコンピュータによるプライベートデータの回復（再生、リカバリー）を容易にする方法を説明する。７０２で、ホームクライアントコンピュータのユーザが、ホームクライアントアプリケーションを実行し、暗号化してサーバに転送すべき、ホームクライアントコンピュータに関連付けられたメモリに記憶されているプライベートデータ（プライベートキー）を指示する。７０４で、ホームクライアントアプリケーションは、ユーザに暗号化パスワードを要求する。７０６で、ユーザから受け取られた暗号化パスワードの関数としてラッピングキーが生成される。７０８で、指示されたプライベートデータが、生成されたラッピングキーの関数として暗号化される。７１０で、ホームクライアントアプリケーションは、暗号化されたデータを、サーバローミングアプリケーションを実行するサーバに転送する。７１２で、サーバアプリケーションは、転送された暗号化プライベートデータに応答し、暗号化されたプライベートデータが、サーバにリンクされたデータベースに記憶される。

【００４１】

次に、図８を参照して、例示的なフローチャートにより、本発明の一実施形態による、サーバからローミングクライアントコンピュータに暗号化されたプライベートデータを転送する方法を説明する。

【００４２】

８０２で、ローミングクライアントアプリケーションを実行するローミングクライアントコンピュータのユーザが、サーバローミングアプリケーションを実行するサーバからの暗号化されたプライベートデータの転送を要求する。この例では、ユーザは、上記で図７を参照して説明したような方法で、サーバにリンクされたデータベースにあらかじめ記憶されている暗号化されたプライベートキーE_{K1}ＰＫの転送を要求する。８０４で、ローミングクライアントアプリケーションは、ユーザに暗号化パスワードを要求する。８０６で、ユーザから受け取った暗号化パスワードの関数として、ローミングクライアントアプリケーションによりラッピングキーが生成される。認証サービスが、初めに、パスワードの照合などの何らかの認証機構を使用してユーザを認証する。認証に通らなかった場合８０８、サーバローミングアプリケーションは、８０９で、要求される暗号化データへのユーザアクセスを拒否する。認証が成功した場合８０８、サーバローミングアプリケーションは、データベースから要求される暗号化プライベートキーE_{K1}ＰＫを取り出し、８１０で、取り出した暗号化プライベートキーをローミングクライアントコンピュータに転送する。８１２で、ローミングクライアントアプリケーションは、生成されたラッピングキー２３０の関数として、受け取った暗号化プライベートキーE_{K1}ＰＫを解読してプライベートキーＰＫを得る。

【００４３】

次に、図９Ａおよび図９Ｂを参照して、例示的なフローチャートにより、本発明の一実施形態による、ホームクライアントコンピュータとサーバ間でプライベートデータと回復データを通信する方法を説明する。

【００４４】

９０２で、ホームクライアントコンピュータのユーザがローミングクライアントアプリケーションを実行し、暗号化すべき、ホームクライアントコンピュータのメモリに記憶されたプライベートデータを指示し、その指示したプライベートデータをサーバに転送する要求を提出する。要求が上記で図８を参照して記述したように認証されると、サーバは、

９０４でローミングサーバアプリケーションを実行する。サーバローミングアプリケーションは、９０６で、その特定のホームクライアントからの要求に応答してＳＲＡ（サーバローミングアプリケーション）が実行されるのが初めてであるかどうかを判定する。サーバローミングアプリケーションが９０６で初めての実行であると判定するか、または、そのユーザについてバックアップキーＫ３がデータベースに見つからないと判定した場合、サーバローミングアプリケーションは、９０８でランダムなバックアップキーＫ３を生成する。９１０で、サーバローミングアプリケーションは、バックアップキーＫ３をデータベースに記憶し、９１２で、回復データを暗号化する際に使用するためにバックアップキーＫ３をホームクライアントアプリケーションに提供する。サーバローミングアプリケーションは、９０６で実行されるのが初めてではないと判定した場合、９０９でデータベースからバックアップキーを取り出し、９１２で、回復データを暗号化する際に使用するためにバックアップキーＫ３をホームクライアントアプリケーションに提供する。

【００４５】

次に、図９Ｂを参照すると、ホームクライアントアプリケーションは、９１４で、ユーザから提供された暗号化パスワードの関数としてラッピングキーＫ１を生成する。ホームクライアントアプリケーションは、９１６で、回復キーＫ２がホームクライアントコンピュータに記憶されているかどうかを判定する。９１６で回復キーＫ２がホームクライアントに関連付けられたメモリに記憶されていないとホームクライアントアプリケーションが判定し、第１の暗号化された回復キーE_{K1}Ｋ２がサーバに存在しない場合には、ホームクライアントアプリケーションは、９１８でランダムな回復キーＫ２を生成する。例えば、ホームクライアントアプリケーションが実行されるのが初めてである場合は、回復キーは、ホームクライアントコンピュータには存在しない。９１６で回復キーＫ２がホームクライアントに関連付けられたメモリに記憶されているとホームクライアントアプリケーションが判断した場合には、ホームクライアントアプリケーションは、９２０でメモリから回復キーＫ２を取り出す。９２２で、ホームクライアントアプリケーションは、暗号化されたプライベートキー、暗号化されたラッピングキーＫ１、第１の暗号化された回復キー、および第２の暗号化された回復キーを生成する。暗号化されたプライベートキーは、生成されたラッピングキーＫ１の関数として暗号化されたプライベートキーＰＫに相当する。暗号化されたラッピングキーE_{K2}Ｋ１は、回復キーＫ２の関数として暗号化されたラッピングキーＫ１に相当する。第１の暗号化された回復キーE_{K1}Ｋ２は、ラッピングキーＫ１の関数として暗号化された回復キーＫ２に相当する。第２の暗号化された回復キーE_{K3}Ｋ２は、サーバから転送されたバックアップキーＫ３の関数として暗号化された回復キーＫ２に相当する。９２４で、ホームクライアントアプリケーションは、第２の暗号化された回復キーE_{K3}Ｋ２を、ホームクライアントコンピュータに関連付けられたメモリに記憶する。９２６で、ホームクライアントアプリケーションは、暗号化されたプライベートキー、暗号化されたラッピングキー、第１の暗号化された回復キー、および第１の暗号化された回復キーをサーバに転送する。再度図９Ａを参照すると、９２８で、サーバローミングアプリケーションは、転送された暗号化プライベートキー、暗号化されたラッピングキー、および第１の暗号化回復キーを受信し、データベースに記憶する。

【００４６】

次に、図１０を参照すると、回復データをサーバからローミングクライアントに転送して、ローミングクライアントが暗号化パスワードなしでプライベートデータを回復できるようにする方法を例示的フローチャートで示す。１００２で、ローミングサーバアプリケーションを実行するサーバが、ローミングクライアントアプリケーションを実行するローミングクライアントのユーザから、認証パスワードと、回復データをローミング、あるいはバックアップを作成する要求とを受け取る。ローミングクライアントアプリケーションは、１００４で、認証されたユーザから提供された暗号化パスワードに応答してラッピングキーＫ１を生成する。１００６で、バックアップＫ３および第１の暗号化された回復キーE_{K1}Ｋ２が、ローミングサーバアプリケーションからローミングクライアントアプリケーションに転送される。ローミングクライアントアプリケーションは、１００８で、生

成されたラッピングキーＫ１の関数として、受け取った第１の暗号化された回復キーE_{K_1}Ｋ２を解読してＫ２を得る。１０１０で、クライアントアプリケーションは、受け取ったバックアップキーＫ３の関数として、取得した回復キーＫ２を暗号化して、第２の暗号化された回復キーE_{K_3}Ｋ２を生成する。１０１２で、ローミングクライアントアプリケーションは、生成した第２の暗号化回復キーを、ローミングクライアントコンピュータに関連付けられたメモリに記憶する。

【００４７】

次に、図１１を参照すると、例示的なフローチャートで、ローミングクライアントで暗号化パスワードなしでサーバからのプライベートデータを回復する方法を示す。１１０２で、サーバは、ローミングクライアントアプリケーションを実行するローミングクライアントから認証パスワードと、暗号化されたプライベートキーを暗号化パスワードなしで転送する要求とを受け取る。１１０４で、ローミングサーバアプリケーションは、データベースからバックアップキー、暗号化されたラッピングキーE_{K_2}Ｋ１、および暗号化されたプライベートキーE_{K_1}ＰＫを取り出す。１１０６で、ローミングサーバアプリケーションは、取り出したバックアップキー、暗号化されたラッピングキー、および暗号化されたプライベートキーをローミングクライアントに転送する。ローミングクライアントアプリケーションは、１１０８で、取り出されたバックアップキーＫ３の関数として、あらかじめローミングクライアント（図１０参照）に記憶されていた第２の暗号化された回復キーE_{K_3}Ｋ２を解読して、回復キーＫ２を得る。１１１０で、ローミングクライアントアプリケーションは、取得した回復キーＫ２の関数として、暗号化されたラッピングキーE_{K_2}Ｋ１を解読して、ラッピングキーＫ１を得る。ローミングクライアントアプリケーションは、１１１２で、取得したラッピングキーの関数として、暗号化されたプライベートキーを解読する。

【００４８】

とりわけ、クライアントでＫ２を生成し、それを決してサーバに公開しないことにより、サーバが暗号化パスワードキーＫ１と回復キーＫ２を一切知ることなく、サーバでその両方のバックアップを作成することができる。同時に、クライアントは２つの鍵の少なくとも１つが分かる、すなわち、ユーザが暗号化パスワードＫ１を入力するか、またはＫ２がクライアントにあらかじめ記憶されているので、クライアントは、プライベートデータを復元するため、またバックアップを行うためにもE_{k_1}Ｋ２とE_{k_2}Ｋ１を使用することができる。

【００４９】

図１２に、コンピュータ１３０の形態の汎用コンピューティングデバイスの一例を示す。本発明の一実施形態では、コンピュータ１３０のようなコンピュータが、図示されてここで説明した他の図で使用するのに適する。コンピュータ１３０は、１つまたは複数のプロセッサあるいは処理装置１３２とシステムメモリ１３４を有する。本図の実施形態では、システムバス１３６は、システムメモリ１３４を含む各種のシステム構成要素をプロセッサ１３２に接続する。バス１３６は、各種のバスアーキテクチャを使用した、メモリバスあるいはメモリコントローラ、ペリフェラルバス、アクセラレーテッドグラフィックポート、およびプロセッサバスまたはローカルバスを含む数種のバス構造の１つまたは複数を表す。限定ではなく例示として、そのようなアーキテクチャには、ＩＳＡ（Ｉｎｄｕｓｔｒｙ Ｓｔａｎｄａｒｄ Ａｒｃｈｉｔｅｃｔｕｒｅ：業界標準アーキテクチャ）バス、ＭＣＡ（Ｍｉｃｒｏ Ｃｈａｎｎｅｌ Ａｒｃｈｉｔｅｃｔｕｒｅ：マイクロチャネルアーキテクチャ）バス、ＥＩＳＡ（Ｅｎｈａｎｃｅｄ ＩＳＡ：３２ビットの拡張スロットバスの共通規格）バス、ＶＥＳＡ（Ｖｉｄｅｏ Ｅｌｅｃｔｒｏｎｉｃｓ Ｓｔａｎｄａｒｄｓ Ａｓｓｏｃｉａｔｉｏｎ：ビデオ電子標準規格）ローカルバス、およびメザニンバスとも称されるＰＣＩ（Ｐｅｒｉｐｈｅｒａｌ Ｃｏｍｐｏｎｅｎｔ Ｉｎｔｅｒｃｏｎｎｅｃｔ：周辺構成要素相互接続）バスがある。

【００５０】

コンピュータ１３０は通例、少なくとも何らかの形態のコンピュータ可読媒体を備える

。コンピュータ可読媒体は、揮発性および不揮発性の媒体、取り外し可能および取り外し不能の媒体を含み、コンピュータ１３０によるアクセスが可能な任意の利用可能媒体でよい。限定ではなく例示として、コンピュータ可読媒体は、コンピュータ記憶媒体と通信媒体からなる。コンピュータ記憶媒体は、コンピュータ可読命令、データ構造、プログラムモジュール、または他のデータなどの情報を記憶するための方式または技術として実施された、揮発性および不揮発性、取り外し可能および取り外し不能の媒体を含む。例えば、コンピュータ記憶媒体には、ＲＡＭ、ＲＯＭ、ＥＥＰＲＯＭ、フラッシュメモリ、または他のメモリ技術、ＣＤ－ＲＯＭ、デジタル多用途ディスク（ＤＶＤ）、あるいは他の光ディスク記憶、磁気カセット、磁気テープ、磁気ディスク記憶、または他の磁気記憶装置、あるいは、所望の情報を記憶するために使用することができ、コンピュータ１３０によるアクセスが可能な他の媒体が含まれる。通信媒体は通例、コンピュータ可読命令、データ構造、プログラムモジュール、または他のデータを、搬送波などの変調データ信号や他のトランスポート機構として実施し、任意の情報伝達媒体を含む。当業者は、信号中に情報を符号化するような方式で特性の１つまたは複数を設定または変化させた変調データ信号に精通していよう。有線ネットワークや直接配線接続などの有線媒体と、音波、ＲＦ、赤外線、および他の無線媒体などの無線媒体は、通信媒体の例である。上記の媒体の組み合わせもコンピュータ可読媒体の範囲に含まれる。

【００５１】

システムメモリ１３４は、取り外し可能および／または取り外し不能メモリ、揮発性および／または不揮発性メモリの形態のコンピュータ記憶媒体を含む。図の実施形態では、システムメモリ１３４は、読み取り専用メモリ（ＲＯＭ）１３８とランダムアクセスメモリ（ＲＡＭ）１４０を含む。起動時などにコンピュータ１３０中の要素間の情報転送を助ける基本ルーチンを含んだ基本入出力システム１４２（ＢＩＯＳ）は、通例、ＲＯＭ１３８に記憶される。ＲＡＭ１４０は、通例、処理装置１３２から即座にアクセスできる、かつ／または処理装置１３２によって現在操作されているデータおよび／またはプログラムモジュールを保持する。限定ではなく例として、図１２にはオペレーティングシステム１４４、アプリケーションプログラム１４６、他のプログラムモジュール１４８、およびプログラムデータ１５０を示す。

【００５２】

コンピュータ１３０は、他の取り外し可能／取り外し不能、揮発性／不揮発性のコンピュータ記憶媒体も含むことができる。例えば、図１２には、取り外し不能、不揮発性の磁気媒体の読み書きを行うハードディスクドライブ１５４を示す。図１２には、取り外し可能、不揮発性の磁気ディスク１５８の読み書きを行う磁気ディスクドライブ１５６と、ＣＤ－ＲＯＭや他の光学媒体などの取り外し可能、不揮発性の光ディスク１６２の読み書きを行う光ディスクドライブ１６０も示す。例示的動作環境で使用することができるこの他の取り外し可能／取り外し不能、揮発性／不揮発性のコンピュータ記憶媒体には、これらに限定しないが、磁気テープカセット、フラッシュメモリカード、デジタル多用途ディスク、デジタルビデオテープ、固体素子ＲＡＭ、固体素子ＲＯＭなどがある。ハードディスクドライブ１５４、磁気ディスクドライブ１５６、および光ディスクドライブ１６０は、通例、インタフェース１６６などの不揮発性メモリインタフェースでシステムバス１３６に接続される。

【００５３】

上記で説明し、図１２に示すこれらのドライブあるいはその他の大容量記憶装置とそれに関連付けられたコンピュータ記憶媒体は、コンピュータ可読命令、データ構造、プログラムモジュール、および他のデータの記憶をコンピュータ１３０に提供する。図１２では、例えば、ハードディスクドライブ１５４にオペレーティングシステム１７０、アプリケーションプログラム１７２、他のプログラムモジュール１７４、およびプログラムデータ１７６が記憶されている。これらのコンポーネントは、オペレーティングシステム１４４、アプリケーションプログラム１４６、他のプログラムモジュール１４８、およびプログラムデータ１５０と同じでも異なってもよいことに留意されたい。ここでは、オペレーテ

ィングシステム１７０、アプリケーションプログラム１７２、他のプログラムモジュール１７４、およびプログラムデータ１７６には、それらが少なくとも異なるコピーであることを表すために異なる参照符号を付している。

【００５４】

ユーザは、キーボード１８０およびポインティングデバイス１８２（マウス、トラックボール、ペン、タッチパッドなど）などの入力装置またはユーザインタフェース選択装置（user interface selection device）を通じてコンピュータ１３０にコマンドと情報を入力することができる。他の入力装置（図示せず）には、マイクロフォン、ジョイスティック、ゲームパッド、衛星受信アンテナ、スキャナなどがある。これらおよび他の入力装置は、システムバス１３６に接続されたユーザ入力インタフェース１８４を通じて処理装置１３２に接続されるが、パラレルポート、ゲームポート、ユニバーサルシリアルバス（ＵＳＢ）など他のインタフェースおよびバス構造で接続してもよい。モニタ１８８あるいは他のタイプの表示装置も、ビデオインタフェース１９０などのインタフェースを介してシステムバス１３６に接続される。モニタ１８８に加えて、コンピュータは多くの場合、プリンタやスピーカなどの他の周辺出力装置（図示せず）を含み、それらは、出力周辺インタフェース（図示せず）を通じて接続することができる。

【００５５】

コンピュータ１３０は、ローミングクライアント１９４などの１つまたは複数のローミングクライアントとの論理接続を使用するネットワーク環境で動作することができる。ローミングクライアント１９４は、パーソナルコンピュータ、サーバ、ルータ、ネットワークＰＣ、ピアデバイス(peer device)、あるいは他の一般的なネットワークノードであり、通例は、コンピュータ１３０との関連で上述した要素の多くまたはすべてを含む。図１２に示す論理接続には、ローカルエリアネットワーク（ＬＡＮ）１９６とワイドエリアネットワーク（ＷＡＮ）１９８が含まれるが、他のネットワークを含むことも可能である。このようなネットワーキング環境は、オフィス、企業内のコンピュータネットワーク、イントラネット、および世界規模のコンピュータネットワーク（インターネットなど）に一般的に見られる。

【００５６】

ローカルエリアネットワーク環境で使用される場合、コンピュータ１３０は、ネットワークインタフェースあるいはアダプタ１８６を通じてＬＡＮ１９６に接続される。ワイドエリアネットワーク環境で使用される場合、コンピュータ１３０は通例、インターネットなどのＷＡＮ１９８を通じて通信を確立するためのモデム１７８あるいは他の手段を含む。モデム１７８は、内蔵型でも外付け型でもよく、ユーザ入力インタフェース１８４または他の適切な機構を介してシステムバス１３６に接続される。ネットワーク環境では、コンピュータ１３０との関連で図示するプログラムモジュールまたはその一部は、遠隔のメモリ記憶装置（図示せず）に記憶することができる。限定ではなく例として、図１２では、リモートアプリケーションプログラム１９２がメモリデバイスにある。図のネットワーク接続は典型的なものであり、コンピュータ間に通信リンクを確立する他の手段を使用してよいことは認識されよう。

【００５７】

一般に、コンピュータ１３０のデータプロセッサは、異なる時にコンピュータの各種のコンピュータ可読記憶媒体に記憶される命令によってプログラムされる。プログラムとオペレーティングシステムは、通例、フロッピー（登録商標）ディスクやＣＤ－ＲＯＭなどで配布される。そこから、コンピュータの２次メモリにインストールあるいはロードされる。実行時には、少なくとも一部分がコンピュータの主要電子メモリにロードされる。ここに記載される本発明は、そのような媒体がマイクロプロセッサまたは他のデータプロセッサと併せて上記のステップを実施する命令またはプログラムを含む場合は、上記および他の各種タイプのコンピュータ可読記憶媒体を含む。本発明は、ここに記載される方法および技術に従ってプログラムされた場合はコンピュータ自体も含む。

【００５８】

説明のために、オペレーティングシステムなどのプログラムおよび他の実行可能プログラムコンポーネントは、本明細書では別個のブロックとして図示する。しかし、そのようなプログラムとコンポーネントは、様々な時にコンピュータの異なる記憶コンポーネントに存在し、コンピュータのデータプロセッサによって実行されることが認識されよう。

【００５９】

コンピュータ１３０を含む典型的なコンピューティングシステム環境との関連で説明したが、本発明は、多数の他の汎用または特殊目的のコンピューティングシステム環境または構成で動作する。このコンピューティングシステム環境は、本発明の使用または機能の範囲についての限定を示唆するものではない。さらに、このコンピューティングシステム環境は、例示的動作環境に図示する構成要素の１つまたは組み合わせに関連する依存性または必要性を有するものとも解釈すべきでない。本発明とともに使用するのに適する可能性のある、よく知られるコンピューティングシステム、環境、および／または構成の例には、これらに限定しないが、パーソナルコンピュータ、サーバコンピュータ、ハンドヘルドまたはラップトップデバイス、マルチプロセッサシステム、マイクロプロセッサを利用したシステム、セットトップボックス、プログラム可能な家庭電化プロダクト、ネットワークＰＣ、ミニコンピュータ、メインフレームコンピュータ、上記のシステムまたはデバイスを含む分散コンピューティング環境などがある。

【００６０】

本発明は、１つまたは複数のコンピュータあるいは他のデバイスによって実行されるプログラムモジュールなどのコンピュータ実行可能命令との一般的関連で説明することができる。一般に、プログラムモジュールには、これに限定しないが、特定のタスクを行うか、特定の抽象データ型を実施するルーチン、プログラム、オブジェクト、コンポーネント、およびデータ構造が含まれる。本発明は、通信ネットワークで結ばれた遠隔の処理デバイスによってタスクが行われる分散コンピューティング環境で実施することもできる。分散コンピューティング環境では、プログラムモジュールは、メモリ記憶装置を含むローカルクライアントとローミングクライアント両方の記憶媒体に置くことができる。

【００６１】

動作の際、コンピュータ１３０は、図７～図１１に示すようなコンピュータ実行可能命令を実行して、プライベートデータを暗号化および転送し、かつ／またはプライベートデータを取り出し、解読する。

【００６２】

本発明またはその実施形態の要素を紹介する際、冠詞「ａ」、「ａｎ」、「ｔｈｅ」、および「ｓａｉｄ」は、その要素が１つまたは複数あることを意味するものとする。用語「～を備える」、「～を含む」、および「～を有する」は、包含的な意味とし、記載される要素以外に追加的な要素があってよいことを意味する。

【００６３】

上記に鑑みて、本発明のいくつかの目的が達成され、他の有利な結果が得られることが理解されよう。

【００６４】

本発明の特許請求の範囲から逸脱せずに構成および方法に各種の変更を加えることができるので、上記の説明に含まれ、添付図面に図示されるすべての事項は、限定的な意味ではなく例示的に解釈されたい。

【図面の簡単な説明】

【００６５】

【図１】本発明を利用することができる例示的なネットワーク環境を示すブロック図である。

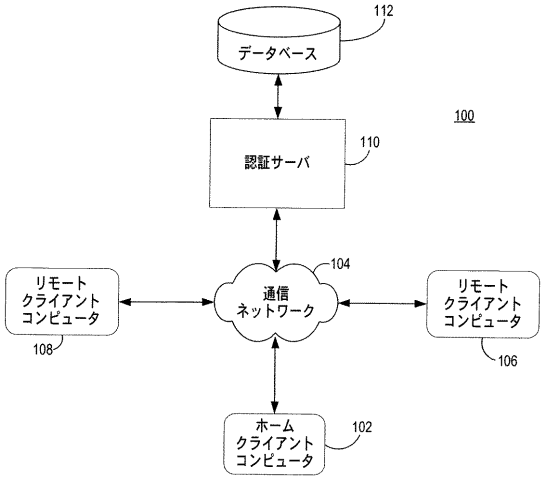
【図２】本発明の一実施形態によるホームクライアントとサーバ間で暗号化されたプライベートデータを通信するシステムを表すブロック図である。

【図３】本発明の一実施形態によるローミングクライアントコンピュータとサーバ間で暗号化されたプライベートデータを通信するシステムを表すブロック図である。

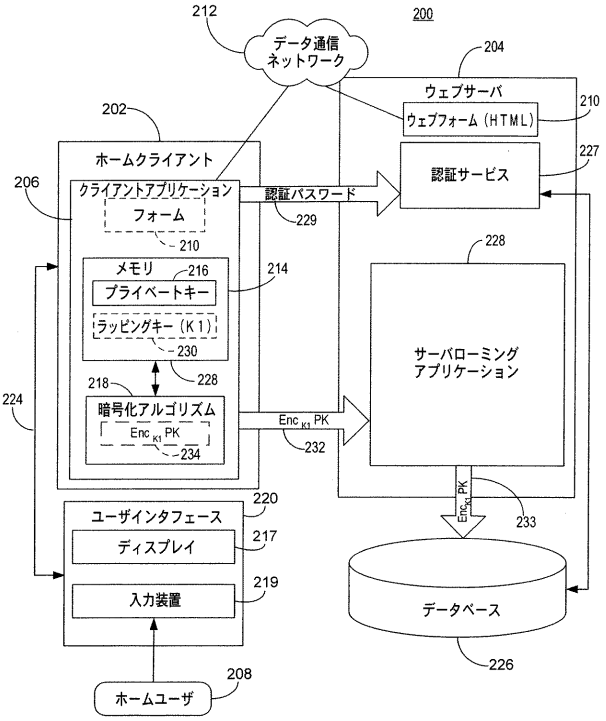
【図４】本発明の一実施形態によるホームクライアントとサーバ間で暗号化されたプライベートデータと回復データを通信するシステムを表すブロック図である。
【図５】本発明の一実施形態によるサーバからローミングクライアントに回復データを通信するシステムを表すブロック図である。
【図６】本発明の一実施形態による暗号化パスワードなしでサーバからローミングクライアントに暗号化されたプライベートデータを回復するシステムを表すブロック図である。
【図７】本発明の一実施形態によるホームクライアントとサーバ間でプライベートデータを通信する方法を説明する例示的なフローチャートである。
【図８】本発明の一実施形態によるサーバからローミングクライアントに暗号化されたプライベートデータを通信する方法を説明する例示的なフローチャートである。
【図９Ａ】本発明の一実施形態によるサーバとホームクライアント間で暗号化されたプライベートデータと回復データを通信する方法を説明する例示的なフローチャートである。
【図９Ｂ】本発明の一実施形態によるサーバとホームクライアント間で暗号化されたプライベートデータと回復データを通信する方法を説明する例示的なフローチャートである。
【図１０】本発明の一実施形態によるサーバとローミングクライアント間で回復データを通信する方法を説明する例示的フローチャートである。
【図１１】本発明の一実施形態による暗号化パスワードなしでサーバからローミングクライアントに暗号化されたプライベートデータを回復する方法を説明する例示的フローチャートである。
【図１２】本発明を実施することが可能な適切なコンピューティングシステム環境の一例を示すブロック図である。
【符号の説明】
【００６６】
１０２　ホームクライアントコンピュータ
１０４　通信ネットワーク
１０６、１０８　リモートクライアントコンピュータ
１１０　認証サーバ
１１２　データベース
１３２　処理装置
１３４　システムメモリ
１３６　システムバス
１４４、１７０　オペレーティングシステム
１４６、１７２　アプリケーションプログラム
１４８、１７４　他のプログラムモジュール
１５０、１７６　プログラムデータ
１６６　不揮発性メモリインタフェース
１８４　ユーザ入力インタフェース
１８６　ネットワークインタフェース
１９０　ビデオインタフェース
１９２　リモートアプリケーションプログラム
１９６　ローカルエリアネットワーク
１９８　ワイドエリアネットワーク
２０２　ホームクライアント
２０４　ウェブサーバ
２０６　クライアントアプリケーション
２０８　ホームユーザ
２１０　ウェブフォーム（ＨＴＭＬ）
２１２　データ通信ネットワーク
２１４　メモリ
２１５　認証サービス

２１６　プライベートキー（ＰＫ）
２１７　ディスプレイ
２１８　暗号化アルゴリズム
２１９　入力装置
２２０　ユーザインタフェース
２２６　データベース
２２７　認証サービス
２２８　サーバローミングＰＫＩアプリケーション
２２９　認証パスワード
２３０　ラッピングキー（Ｋ１）
２３２，２３３　プライベートデータ
２３４　プライベートキー
３０２　ローミングクライアント
３０４　ローミングクライアントアプリケーション
３０６　ローミングユーザ
３１０，３１１　暗号化データ
３１２　暗号解読アルゴリズム
４０８　回復キー（Ｋ２）
４１４　ラッピングキー
４１６　第１の暗号化された回復キー
４２１，４２２，４２３，４２５　書き込みデータ
４２４　バックアップキー（Ｋ３）
４２６　転送データ
４２８　第２の暗号化された回復キー
５０６，５０８，６０４，６０６，６０８　取り出したデータ
５１０，５１２，６１０，６１２，６１４　転送データ

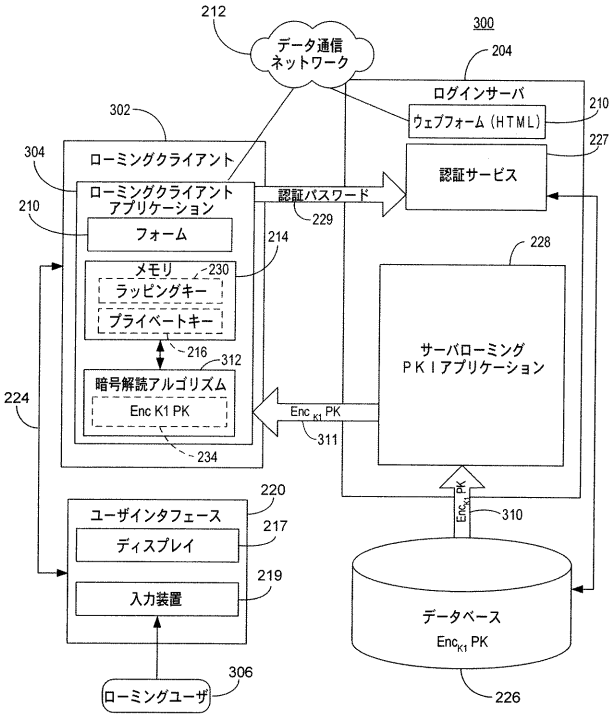
【図１】


データベース
112
認証サーバ
110
100
通信
ネットワーク
104
リモート
クライアント
コンピュータ
108
リモート
クライアント
コンピュータ
106
ホーム
クライアント
コンピュータ
102

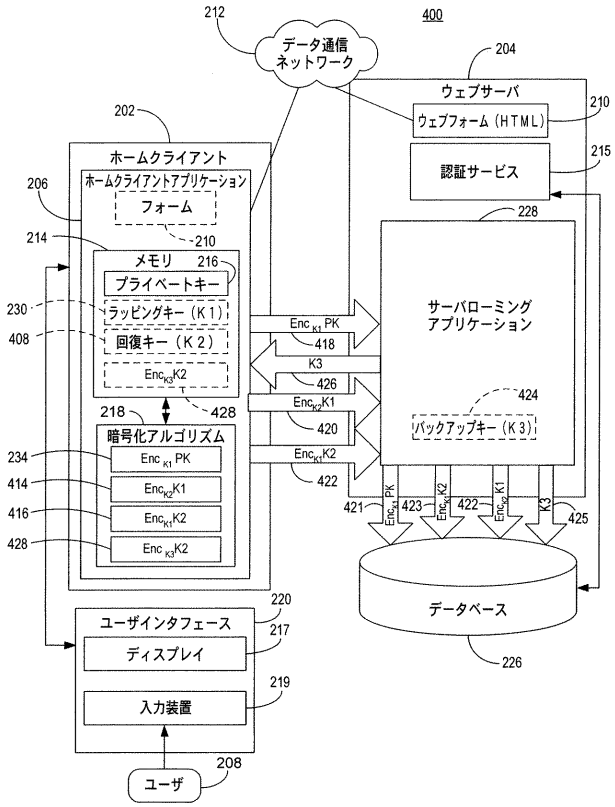
【図２】


212
データ通信
ネットワーク
200
204
ウェブサーバ
ウェブフォーム（HTML）
210
202
ホームクライアント
206
クライアントアプリケーション
フォーム
210
認証パスワード
229
認証サービス
227
メモリ
216
プライベートキー
ラッピングキー（K1）
230
214
228
サーバローミング
アプリケーション
218
暗号化アルゴリズム
Enc K1 PK
234
224
Enc K1 PK
232
Enc K1 PK
233
220
ユーザインタフェース
ディスプレイ
217
219
入力装置
データベース
226
ホームユーザ
208

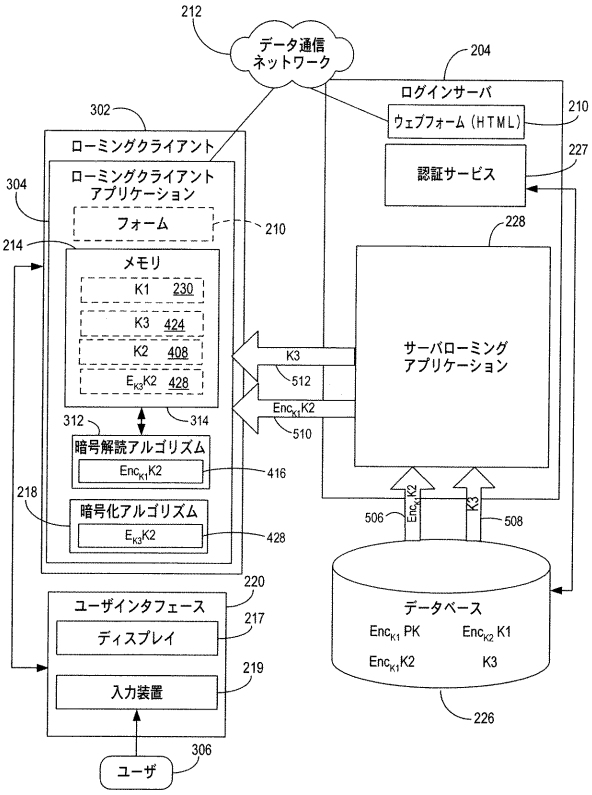
【図３】


212
データ通信
ネットワーク
300
204
ログインサーバ
ウェブフォーム（HTML）
210
227
302
ローミングクライアント
304
ローミングクライアント
アプリケーション
210
フォーム
認証パスワード
229
認証サービス
214
228
メモリ
230
ラッピングキー
プライベートキー
216
312
サーバローミング
PKIアプリケーション
暗号解読アルゴリズム
Enc K1 PK
224
Enc K1 PK
311
234
220
ユーザインタフェース
ディスプレイ
217
219
入力装置
Enc K1 PK
310
データベース
Enc K1 PK
226
ローミングユーザ
306

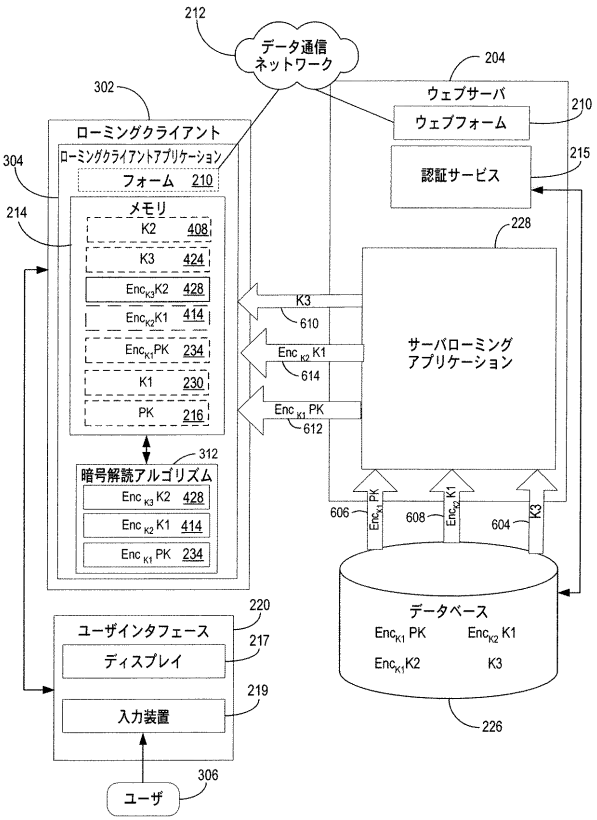
【図４】


212
データ通信
ネットワーク
400
204
ウェブサーバ
ウェブフォーム（HTML）
210
202
ホームクライアント
ホームクライアントアプリケーション
206
フォーム
210
認証サービス
215
214
228
メモリ
216
プライベートキー
230
ラッピングキー（K1）
408
回復キー（K2）
Enc K2
218
428
サーバローミング
アプリケーション
暗号化アルゴリズム
Enc K1 PK
234
Enc K2 K1
414
Enc K1 K2
416
Enc K3 K2
428
Enc K1 PK
418
K3
426
Enc K2 K1
420
Enc K1 K2
422
424
バックアップキー（K3）
421
423
422
425
データベース
226
220
ユーザインタフェース
ディスプレイ
217
219
入力装置
ユーザ
208

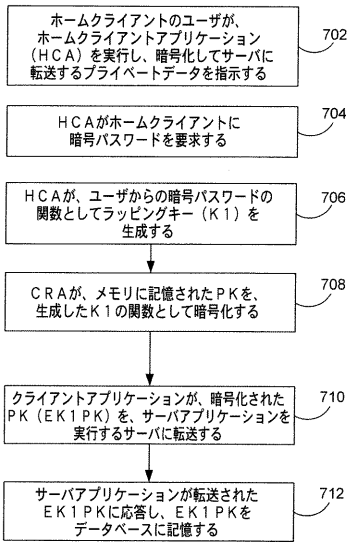
【図５】


212
データ通信ネットワーク
204
ログインサーバ
ウェブフォーム（HTML）
210
302
ローミングクライアント
ローミングクライアントアプリケーション
フォーム
210
304
214
メモリ
K1 230
K3 424
K2 408
$E_{K3}K2$ 428
227
認証サービス
228
サーバローミングアプリケーション
K3
512
$Enc_{K1}K2$
510
312
314
暗号解読アルゴリズム
$Enc_{K1}K2$
416
218
暗号化アルゴリズム
$E_{K3}K2$
428
506
$Enc_{K2}K2$
K3
508
220
ユーザインタフェース
ディスプレイ
217
入力装置
219
データベース
$Enc_{K1}PK$
$Enc_{K2}K1$
$Enc_{K1}K2$
K3
226
306
ユーザ

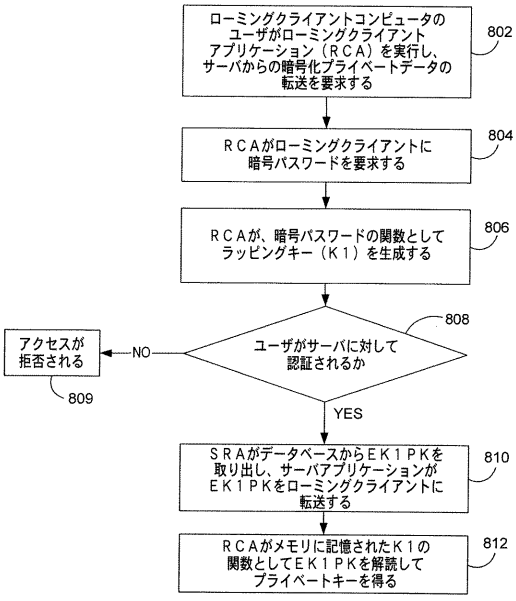
【図６】


212
データ通信ネットワーク
204
ウェブサーバ
ウェブフォーム
210
302
ローミングクライアント
ローミングクライアントアプリケーション
フォーム 210
304
214
メモリ
K2 408
K3 424
$Enc_{K3}K2$ 428
$Enc_{K2}K1$ 414
$Enc_{K1}PK$ 234
K1 230
PK 216
215
認証サービス
228
サーバローミングアプリケーション
K3
610
$Enc_{K2}K1$
614
$Enc_{K1}PK$
612
312
暗号解読アルゴリズム
$Enc_{K3}K2$ 428
$Enc_{K2}K1$ 414
$Enc_{K1}PK$ 234
606
$Enc_{K1}PK$
608
$Enc_{K2}K1$
604
K3
220
ユーザインタフェース
ディスプレイ
217
入力装置
219
データベース
$Enc_{K1}PK$
$Enc_{K2}K1$
$Enc_{K1}K2$
K3
226
306
ユーザ

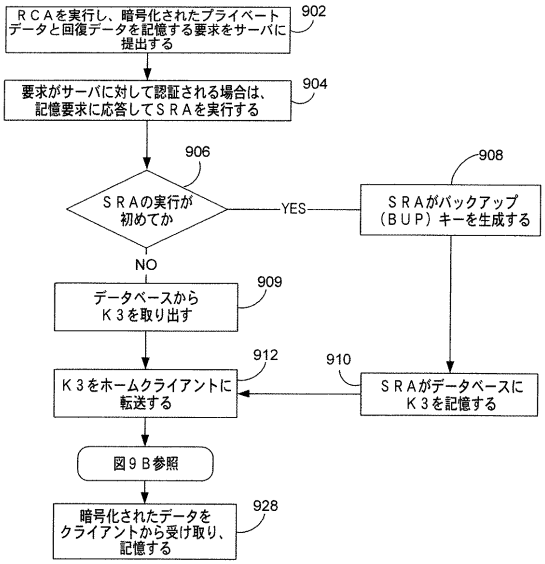
【図７】


ホームクライアントのユーザが、ホームクライアントアプリケーション（ＨＣＡ）を実行し、暗号化してサーバに転送するプライベートデータを指示する
702
ＨＣＡがホームクライアントに暗号パスワードを要求する
704
ＨＣＡが、ユーザからの暗号パスワードの関数としてラッピングキー（Ｋ１）を生成する
706
ＣＲＡが、メモリに記憶されたＰＫを、生成したＫ１の関数として暗号化する
708
クライアントアプリケーションが、暗号化されたＰＫ（ＥＫ１ＰＫ）を、サーバアプリケーションを実行するサーバに転送する
710
サーバアプリケーションが転送されたＥＫ１ＰＫに応答し、ＥＫ１ＰＫをデータベースに記憶する
712

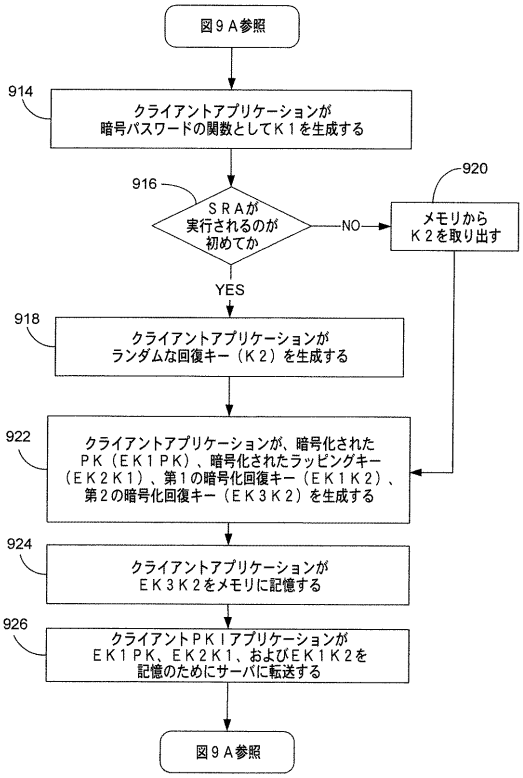
【図８】


ローミングクライアントコンピュータのユーザがローミングクライアントアプリケーション（ＲＣＡ）を実行し、サーバからの暗号化プライベートデータの転送を要求する
802
ＲＣＡがローミングクライアントに暗号パスワードを要求する
804
ＲＣＡが、暗号パスワードの関数としてラッピングキー（Ｋ１）を生成する
806
ユーザがサーバに対して認証されるか
808
NO
アクセスが拒否される
809
YES
ＳＲＡがデータベースからＥＫ１ＰＫを取り出し、サーバアプリケーションがＥＫ１ＰＫをローミングクライアントに転送する
810
ＲＣＡがメモリに記憶されたＫ１の関数としてＥＫ１ＰＫを解読してプライベートキーを得る
812

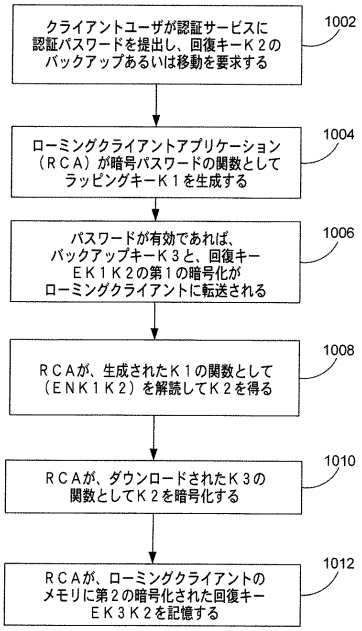
【図９Ａ】



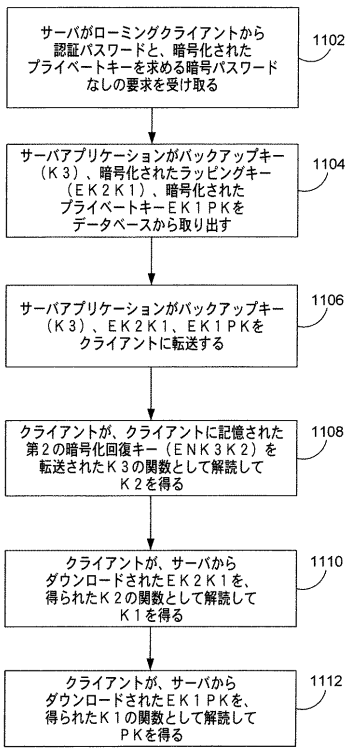
【図９Ｂ】



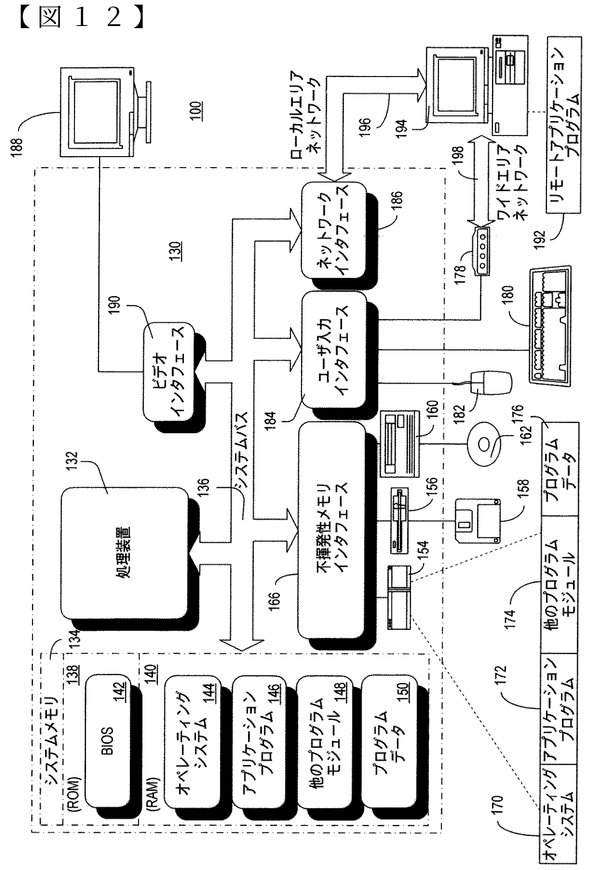
【図１０】



【図１１】



【図１２】


100
130
システムメモリ
(ROM)
138
BIOS
142
(RAM)
140
オペレーティングシステム
144
アプリケーションプログラム
146
他のプログラムモジュール
148
プログラムデータ
150
134
処理装置
132
136
システムバス
166
不揮発性メモリインタフェース
154
156
158
160
162
184
ユーザ入力インタフェース
182
180
178
190
ビデオインタフェース
188
186
ネットワークインタフェース
ローカルエリアネットワーク
196
194
198
ワイドエリアネットワーク
192
リモートアプリケーションプログラム
170
オペレーティングシステム
172
アプリケーションプログラム
174
他のプログラムモジュール
176
プログラムデータ

フロントページの続き

(72)発明者　バシカラン　ダルマラジヤン
アメリカ合衆国　９８０５２　ワシントン州　レッドモンド　ワン　マイクロソフト　ウェイ　マイクロソフト　コーポレーション内
(72)発明者　ダフィナ　イワノワ　トンシュバ
アメリカ合衆国　９８０５２　ワシントン州　レッドモンド　ワン　マイクロソフト　ウェイ　マイクロソフト　コーポレーション内
(72)発明者　コック　ワイ　チャン
アメリカ合衆国　９８０５２　ワシントン州　レッドモンド　ワン　マイクロソフト　ウェイ　マイクロソフト　コーポレーション内
(72)発明者　ラフル　シュリカント　ネワスカル
アメリカ合衆国　９８０５２　ワシントン州　レッドモンド　ワン　マイクロソフト　ウェイ　マイクロソフト　コーポレーション内

Ｆターム(参考) 5J104 AA16　EA23　PA07

【外国語明細書】
2005295570000001.pdf