(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2009-43196
(P2009-43196A)
(43)公開日　平成21年2月26日(2009.2.26)

| (51)Int.Cl. | | F I | | | テーマコード（参考） |
|---|---|---|---|---|---|
| G06Q 20/00 | (2006.01) | G06F | 17/60 | 416 | 5J104 |
| G06Q 40/00 | (2006.01) | G06F | 17/60 | 242 | |
| G06Q 10/00 | (2006.01) | G06F | 17/60 | 512 | |
| G09C 1/00 | (2006.01) | G09C | 1/00 | 660A | |

審査請求 未請求　請求項の数 5　ＯＬ　（全 14 頁）

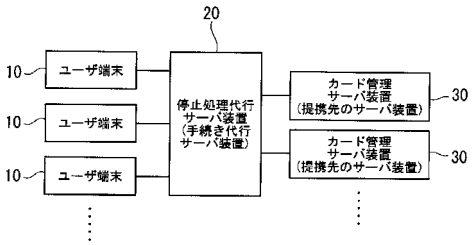
(21)出願番号　特願2007-210369 (P2007-210369)
(22)出願日　平成19年8月10日 (2007.8.10)

(71)出願人　505022563
株式会社ＩＣＯＮ
神奈川県横浜市神奈川区金港町５番地３６
(74)代理人　100110559
弁理士　友野　英三
(72)発明者　土屋　敏子
神奈川県横浜市神奈川区金港町５番地３６
株式会社ＩＣＯＮ内

Ｆターム(参考)　5J104 AA07 AA12 AA16 EA04 EA15
EA22 JA03 KA01 KA04 NA02
NA27 NA35 NA37 NA38

(54)【発明の名称】手続き代行サーバ装置、停止処理代行サーバ装置、停止処理代行方法及びプログラム

(57)【要約】
【課題】暗号鍵が漏れる可能性をなくした手続き代行サーバ装置、停止処理代行サーバ装置、方法及びプログラムを提供することにある。また、それとともに管理している全ての情報が漏洩することを防止することを目的とする。
【解決手段】手続き代行サーバ装置、停止処理代行サーバ装置、停止処理代行方法及びプログラムは、ユーザのカード情報を暗号化する際に用いる第２の暗号鍵を暗号化する。また、第２の暗号鍵を暗号化する際に用いる第１の暗号鍵は、管理データベースに保持せず、動的に生成するものとする。さらに、第２の暗号鍵及び第１の暗号鍵はユーザ毎に固有のものとする。
【選択図】図１



【特許請求の範囲】
【請求項１】
ユーザの属性情報を基に当該ユーザに固有の第１の暗号鍵を動的に生成する鍵生成処理部と、
前記ユーザのカードに関するカード情報を保持する管理データベースと、
ユーザの認証処理を行なう認証部と、
前記認証部による前記ユーザ認証処理の結果に基づき、ユーザ端末から当該ユーザのカードに関するカード情報と第２の暗号鍵とを受信し、前記カード情報を前記第２の暗号鍵を用いて暗号化して前記管理データベースに書き込むとともに、当該ユーザの属性情報を基に前記鍵生成処理部が生成した前記第１の暗号鍵を用いて前記第２の暗号鍵を暗号化して前記管理データベースに書き込む管理データ登録部と、
前記認証部による前記ユーザ認証処理の結果に基づき、ユーザ端末から、停止するカードを特定する情報を受信し、この特定されたカードに関する前記カード情報を前記管理データベースから読み出し、当該カード情報を、前記管理データベースから読み出した当該ユーザの前記第２の暗号鍵および前記鍵生成処理部が当該ユーザの属性情報を基に生成した第１の暗号鍵とともにカード管理サーバ装置に送信する停止サービス処理部と
を備えることを特徴とする停止処理代行サーバ装置。
【請求項２】
請求項１に記載の停止処理代行サーバ装置と、
前記停止処理代行サーバ装置から、前記カード情報と前記第２の暗号鍵と前記第１の暗号鍵とを受信し、前記第１の暗号鍵を用いて前記第２の暗号鍵を復号化し、復号化された前記第２の暗号鍵を用いて前記カード情報を復号化し、復号化された前記カード情報を用いて当該カードの使用停止のための処理を実行するカード管理サーバ装置と、
を含んで構成されるカード停止処理システム。
【請求項３】
ユーザのカードに関するカード情報を保持するデータベースを備える停止処理サービス装置を用いた停止処理代行方法であって、
ユーザの属性情報を基に当該ユーザに固有の第１の暗号鍵を動的に生成するステップと、
ユーザの認証処理を行なうステップと、
前記ユーザ認証処理の結果に基づき、ユーザ端末から当該ユーザのカードに関するカード情報と第２の暗号鍵とを受信し、前記カード情報を前記第２の暗号鍵を用いて暗号化して前記管理データベースに書き込むとともに、当該ユーザの属性情報を基に生成した前記第１の暗号鍵を用いて前記第２の暗号鍵を暗号化して前記管理データベースに書き込むステップと、
前記ユーザ認証処理の結果に基づき、ユーザ端末から、停止するカードを特定する情報を受信し、この特定されたカードに関する前記カード情報を前記管理データベースから読み出し、当該カード情報を、前記管理データベースから読み出した当該ユーザの前記第２の暗号鍵および当該ユーザの属性情報を基に生成した第１の暗号鍵とともにカード管理サーバ装置に送信するステップと
を有する停止処理代行方法。
【請求項４】
ユーザのカードに関するカード情報を保持する管理データベースを備えるコンピュータに、
ユーザの属性情報を基に当該ユーザに固有の第１の暗号鍵を動的に生成するステップと、
ユーザの認証処理を行なうステップと、
前記ユーザ認証処理の結果に基づき、ユーザ端末から当該ユーザのカードに関するカード情報と第２の暗号鍵とを受信し、前記カード情報を前記第２の暗号鍵を用いて暗号化して前記管理データベースに書き込むとともに、当該ユーザの属性情報を基に生成した前記

第１の暗号鍵を用いて前記第２の暗号鍵を暗号化して前記管理データベースに書き込むステップと、
前記ユーザ認証処理の結果に基づき、ユーザ端末から、停止するカードを特定する情報を受信し、この特定されたカードに関する前記カード情報を前記管理データベースから読み出し、当該カード情報を、前記管理データベースから読み出した当該ユーザの前記第２の暗号鍵および当該ユーザの属性情報を基に生成した第１の暗号鍵とともにカード管理サーバ装置に送信するステップと
を実行させるためのプログラム。
【請求項５】
ユーザの属性情報を基に当該ユーザに固有の第１の暗号鍵を動的に生成する鍵生成処理部と、
前記ユーザのための代行サービスに関する代行サービス情報を保持する管理データベースと、
ユーザの認証処理を行なう認証部と、
前記認証部による前記ユーザ認証処理の結果に基づき、ユーザ端末から当該ユーザのための代行サービスに関する代行サービス情報と第２の暗号鍵とを受信し、前記代行サービス情報を前記第２の暗号鍵を用いて暗号化して前記管理データベースに書き込むとともに、当該ユーザの属性情報を基に前記鍵生成処理部が生成した前記第１の暗号鍵を用いて前記第２の暗号鍵を暗号化して前記管理データベースに書き込む管理データ登録部と、
前記認証部による前記ユーザ認証処理の結果に基づき、ユーザ端末から、前記代行サービスに関する手続きを特定する情報を受信し、この特定された手続きの情報を前記管理データベースから読み出し、当該手続きの情報を、前記管理データベースから読み出した当該ユーザの前記第２の暗号鍵および前記鍵生成処理部が当該ユーザの属性情報を基に生成した第１の暗号鍵とともに提携先の管理サーバ装置に送信する手続きサービス処理部と
を備えることを特徴とする手続き代行サーバ装置。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、手続き代行サーバ装置、停止処理代行サーバ装置、停止処理代行方法及びプログラムに関する。
【背景技術】
【０００２】
従来は、キャッシュカードやクレジットカードを紛失してカードの停止を行う際、利用者が各金融機関やクレジットカード会社に個別に連絡をしてカード停止処理を行っており、手間が掛かっていた。
また、特許文献１に開示された代行サービスによれば、ユーザの個人情報及びユーザが契約しているサービス内容等の情報は暗号化され、代行サーバ装置に記憶される。このため、ユーザの個人情報及びユーザが契約しているサービス内容等の情報は第三者に知られることはない。
【特許文献１】特開２００２－０５６１９８号公報
【発明の開示】
【発明が解決しようとする課題】
【０００３】
しかしながら、特許文献１に開示されたシステムにおいては、ユーザの個人情報及びユーザが契約しているサービス内容等の情報を暗号化する際に用いた暗号鍵を保持しておく必要があり、暗号鍵が第三者に盗み見られる危険性がある。
また、暗号鍵が破られた場合には、代行サーバ装置に保持している全てのユーザの情報が漏洩する危険性がある。
本発明は上記の点に鑑みてなされたものであり、その目的は、暗号鍵が漏れる可能性をなくした停止処理代行サーバ装置、方法及びプログラムを提供することにある。また、そ

れとともに管理している全ての情報が漏洩することを防止することを目的とする。
【課題を解決するための手段】
【０００４】
（１）本発明は上記の課題を解決するためになされたものであり、本発明の一態様は、ユーザの属性情報を基に当該ユーザに固有の第１の暗号鍵を動的に生成する鍵生成処理部と、前記ユーザのカードに関するカード情報を保持する管理データベースと、ユーザの認証処理を行なう認証部と、前記認証部による前記ユーザ認証処理の結果に基づき、ユーザ端末から当該ユーザのカードに関するカード情報と第２の暗号鍵とを受信し、前記カード情報を前記第２の暗号鍵を用いて暗号化して前記管理データベースに書き込むとともに、当該ユーザの属性情報を基に前記鍵生成処理部が生成した前記第１の暗号鍵を用いて前記第２の暗号鍵を暗号化して前記管理データベースに書き込む管理データ登録部と、前記認証部による前記ユーザ認証処理の結果に基づき、ユーザ端末から、停止するカードを特定する情報を受信し、この特定されたカードに関する前記カード情報を前記管理データベースから読み出し、当該カード情報を、前記管理データベースから読み出した当該ユーザの前記第２の暗号鍵および前記鍵生成処理部が当該ユーザの属性情報を基に生成した第１の暗号鍵とともにカード管理サーバ装置に送信する停止サービス処理部とを備えることを特徴とする停止処理代行サーバ装置である。
【０００５】
（２）また、本発明の一態様は、前記停止処理代行サーバ装置と、前記停止処理代行サーバ装置から、前記カード情報と前記第２の暗号鍵と前記第１の暗号鍵とを受信し、前記第１の暗号鍵を用いて前記第２の暗号鍵を復号化し、復号化された前記第２の暗号鍵を用いて前記カード情報を復号化し、復号化された前記カード情報を用いて当該カードの使用停止のための処理を実行するカード管理サーバ装置と、を含んで構成されるカード停止処理システムである。
【０００６】
（３）また、本発明の一態様は、ユーザのカードに関するカード情報を保持するデータベースを備える停止処理サービス装置を用いた停止処理代行方法であって、ユーザの属性情報を基に当該ユーザに固有の第１の暗号鍵を動的に生成するステップと、前記ユーザのカードに関するカード情報を前記管理データベースに保持するステップと、ユーザの認証処理を行なうステップと、前記ユーザ認証処理の結果に基づき、ユーザ端末から当該ユーザのカードに関するカード情報と第２の暗号鍵とを受信し、前記カード情報を前記第２の暗号鍵を用いて暗号化して管理データベースに書き込むとともに、当該ユーザの属性情報を基に生成した前記第１の暗号鍵を用いて前記第２の暗号鍵を暗号化して前記管理データベースに書き込むステップと、前記ユーザ認証処理の結果に基づき、ユーザ端末から、停止するカードを特定する情報を受信し、この特定されたカードに関する前記カード情報を前記管理データベースから読み出し、当該カード情報を、前記管理データベースから読み出した当該ユーザの前記第２の暗号鍵および当該ユーザの属性情報を基に生成した第１の暗号鍵とともにカード管理サーバ装置に送信するステップとを有する停止処理代行方法である。
【０００７】
（４）また、本発明の一態様は、ユーザのカードに関するカード情報を保持する管理データベースを備えるコンピュータに、ユーザの属性情報を基に当該ユーザに固有の第１の暗号鍵を動的に生成するステップと、ユーザの認証処理を行なうステップと、前記ユーザ認証処理の結果に基づき、ユーザ端末から当該ユーザのカードに関するカード情報と第２の暗号鍵とを受信し、前記カード情報を前記第２の暗号鍵を用いて暗号化して管理データベースに書き込むとともに、当該ユーザの属性情報を基に生成した前記第１の暗号鍵を用いて前記第２の暗号鍵を暗号化して前記管理データベースに書き込むステップと、前記ユーザ認証処理の結果に基づき、ユーザ端末から、停止するカードを特定する情報を受信し、この特定されたカードに関する前記カード情報を前記管理データベースから読み出し、当該カード情報を、前記管理データベースから読み出した当該ユーザの前記第２の暗号鍵

および当該ユーザの属性情報を基に生成した第１の暗号鍵とともにカード管理サーバ装置に送信するステップとを実行させるためのプログラムである。

【０００８】

（５）また、本発明の一態様は、ユーザの属性情報を基に当該ユーザに固有の第１の暗号鍵を動的に生成する鍵生成処理部と、前記ユーザのための代行サービスに関する代行サービス情報を保持する管理データベースと、ユーザの認証処理を行なう認証部と、前記認証部による前記ユーザ認証処理の結果に基づき、ユーザ端末から当該ユーザのための代行サービスに関する代行サービス情報と第２の暗号鍵とを受信し、前記代行サービス情報を前記第２の暗号鍵を用いて暗号化して前記管理データベースに書き込むとともに、当該ユーザの属性情報を基に前記鍵生成処理部が生成した前記第１の暗号鍵を用いて前記第２の暗号鍵を暗号化して前記管理データベースに書き込む管理データ登録部と、前記認証部による前記ユーザ認証処理の結果に基づき、ユーザ端末から、前記代行サービスに関する手続きを特定する情報を受信し、この特定された手続きの情報を前記管理データベースから読み出し、当該手続きの情報を、前記管理データベースから読み出した当該ユーザの前記第２の暗号鍵および前記鍵生成処理部が当該ユーザの属性情報を基に生成した第１の暗号鍵とともに提携先の管理サーバ装置に送信する手続きサービス処理部とを備えることを特徴とする手続き代行サーバ装置である。

【発明の効果】

【０００９】

本発明によれば、停止処理代行サーバ、手続き代行サーバにより複数の異なる金融機関やクレジットカード会社のカードを一括して停止するため、ユーザの手間が減少する。

また、本発明によれば、ユーザのカード情報を暗号化する際に用いる第２の暗号鍵を暗号化する。よって、暗号鍵自身の安全性が高まる。また、第２の暗号鍵を暗号化する際に用いる第１の暗号鍵は、管理データベースに保持せず、動的に生成するものとする。さらに、第２の暗号鍵及び第１の暗号鍵はユーザ毎に固有のものとするので、全てのユーザのカード情報が一度に漏洩することを防止できる。

【発明を実施するための最良の形態】

【００１０】

以下、図面を参照しながら本発明の実施形態について詳しく説明する。

図１は、本実施形態による停止処理代行サービスシステム（手続き代行サービスシステム）の構成図である。停止処理代行サービスシステムは、ユーザ端末１０と、停止処理代行サーバ装置２０（手続き代行サーバ装置）と、カード管理サーバ装置３０（提携先のサーバ装置）と、を含んで構成される。

停止処理代行サービスを提供する代行業者は、停止処理代行サーバ装置２０を設け、カード管理サーバ装置３０を設けた複数の金融機関やクレジットカード会社と提携する。停止処理代行サービスを利用するユーザの操作によりユーザ端末１０は、停止したい銀行カードやクレジットカードを複数選択して停止要求を停止処理代行サーバ装置２０へ送信する。当該停止要求を受け取った停止処理代行サーバ装置２０は、各金融機関やクレジットカード会社のカード管理サーバ装置３０へ選択されたカードの停止要求を送信する。当該停止要求を受け取ったカード管理サーバ装置３０は、該当するカードの停止処理を行う。これによりユーザは複数の異なる金融機関やクレジットカード会社の銀行カードやクレジットカードを一括して停止することができる。

【００１１】

ユーザ端末１０は、ユーザが使用するパーソナルコンピュータ、携帯電話端末、ＰＤＡ（Ｐｅｒｓｏｎａｌ　Ｄｉｇｉｔａｌ　Ａｓｓｉｓｔａｎｔｓ）などの端末であって、インターネットや携帯電話網などのネットワークにより停止処理代行サーバ装置２０と接続される。

郵送にて停止処理代行サービスへの初期登録を行ったユーザの操作によりユーザ端末１０はユーザＩＤとパスワードを停止処理代行サーバ２０へ送信し、停止処理代行サービスへログインする。ユーザ端末１０は、ログインすると以下に記す操作が可能になる。

ユーザの操作によりユーザ端末１０は停止処理代行サービスを利用したい銀行カードやクレジットカードのカード情報と当該カード情報を暗号化するための暗号鍵（データ用）とを停止処理代行サーバ装置２０へ送信し、サービス登録を行う。

ユーザが銀行カードやクレジットカードを紛失して、そのカードを停止したい場合には、ユーザの操作によりユーザ端末１０は予め登録してある銀行カードやクレジットカードを選択して停止要求を停止処理代行サーバ装置２０へ送信し、停止処理代行サービスを利用する。

【００１２】

カード管理サーバ装置３０は、ユーザに対してカードを発行する金融機関やクレジットカード会社などが設けるサーバ装置である。カード管理サーバ装置３０は、インターネットなどのネットワークにより停止処理代行サーバ装置２０と接続される。

カード管理サーバ装置３０は、停止処理代行サーバ装置２０から停止要求と共に受信した後述するカード情報、後述する暗号鍵（データ用）、後述する暗号鍵（鍵用）を取得する。カード管理サーバ装置３０は、当該受信した情報を用いてカード情報を復号化する。復号化の詳しい処理の流れは後述する。カード管理サーバ装置３０は、当該復号化したカード情報を基にカードの停止処理を行う。

【００１３】

停止処理代行サーバ装置２０は、停止処理代行サービスを提供するサーバ装置である。

図２は、本実施形態にかかる停止処理代行サーバ装置２０の機能構成を示すブロック図である。停止処理代行サーバ装置２０は、通信インタフェース部２１と、制御部２２と、認証部２３と、管理データ登録部２４と、停止サービス処理部２５（手続きサービス処理部）と、鍵生成処理部２６と、管理データベース２７と、を含んで構成される。

【００１４】

通信インタフェース部２１は、ユーザ端末１０またはカード管理サーバ３０との間で通信を実行する。

制御部２２は、停止処理代行サーバ装置２０の処理動作を統括して制御する。

【００１５】

管理データベース２７は、ユーザの属性情報及びユーザのカードに関するカード情報を保持する。

【００１６】

認証部２３は、ユーザの認証処理を行なう。

認証部２３は、通信インタフェース部２１を通じてユーザ端末１０から通知されたユーザＩＤとパスワードを取得する。次に認証部２３は、当該ユーザＩＤと属性情報テーブルに記憶されたユーザＩＤを照合し、一致したユーザＩＤに関連付けて記憶されるパスワードと通知されたパスワードとを照合し、一致するか否かの判定を行う。認証部２３は、一致すると判定された場合、ユーザ認証成功とする。認証部２３は、通知されたユーザＩＤと一致したユーザＩＤがない場合あるいはパスワードが一致しない場合は、ユーザ認証失敗とする。

制御部２２は、認証部２３におけるユーザ認証が成功した場合は停止処理サービスをユーザへ提供し、ユーザ認証が失敗した場合は停止処理サービスをユーザへ提供しない。

【００１７】

管理データ登録部２４は、認証部２３による前記ユーザ認証処理の結果に基づき、ユーザ端末１０から当該ユーザのカードに関するカード情報と第２の暗号鍵とを受信し、当該カード情報を第２の暗号鍵を用いて暗号化して管理データベース２７に書き込むとともに、当該ユーザの属性情報を基に鍵生成処理部２６が生成した第１の暗号鍵を用いて前記第２の暗号鍵を暗号化して管理データベース２７に書き込む。

管理データ登録部２４は、ユーザ端末１０がサービス登録をする際にユーザ端末１０から通知されたカード情報と暗号鍵（データ用）を取得し、管理データベース２７へ記憶する。その際、管理データ登録部２４は、カード情報の銀行番号、支店番号、口座種別、口座番号、クレジットカード番号、カード有効期限、暗証番号、カード名義、は通知された

暗号鍵（データ用）を用いて暗号化する。また、管理データ登録部２４は、この暗号鍵（データ用）を後述する鍵生成処理部２６によって生成された暗号鍵（鍵用）を用いて暗号化し、属性情報テーブルへ記憶する。

【００１８】

停止サービス処理部２５は、認証部２３によるユーザ認証処理の結果に基づき、ユーザ端末から、停止するカードを特定する情報を受信し、この特定されたカードに関するカード情報を管理データベース２７から読み出し、当該カード情報を、管理データベース２７から読み出した当該ユーザの前記第２の暗号鍵および鍵生成処理部２６が当該ユーザの属性情報を基に生成した第１の暗号鍵とともにカード管理サーバ装置に送信する。つまり、ユーザ端末から手続きを特定する情報を受信し、特定された手続きに関する手続き情報を管理データベース２７から読み出し、当該手続き情報を、管理データベース２７から読み出した当該ユーザの前記第２の暗号鍵および鍵生成処理部２６が当該ユーザの属性情報を基に生成した第１の暗号鍵とともに提携先のサーバ装置に送信する

停止サービス処理部２５は、ユーザ端末１０から停止要求が送信されてきた際に、通信インタフェース部２１を通じてユーザ端末１０から通知されたユーザＩＤとカードＩＤを取得する。次に停止サービス処理部２５は、通知されたユーザＩＤとカードＩＤとカード情報テーブルに記憶されたユーザＩＤとカードＩＤを照合し、一致するユーザＩＤとカードＩＤに関連付けて記憶された暗号化されているカード情報を取得する。その後停止サービス処理部２５は、通知されたユーザＩＤと属性情報テーブルに記憶されたユーザＩＤを照合し、一致するユーザＩＤに関連付けて記憶された暗号化されている暗号鍵（データ用）を取得する。最後に停止サービス処理部２５は、後述する鍵生成処理部２６によって生成された暗号鍵（鍵用）を取得する。停止サービス処理部２５は、取得したカード情報、暗号鍵（データ用）及び暗号鍵（鍵用）を通知されたカードＩＤに対応する金融機関あるいはクレジットカード会社のカード管理サーバ装置３０へ通信インタフェース部２１を通じて送信する。

【００１９】

鍵生成処理部２６は、属性情報テーブルに記憶する暗号鍵（データ用）を暗号化する際に使用する暗号鍵（鍵用）を生成する。

鍵生成処理部２６は、属性情報テーブルに記憶されたユーザＩＤとパスワードを取得する。そして、これらのユーザＩＤとパスワードを鍵生成用の関数に入力して、出力結果を暗号鍵（鍵用）とする。

鍵生成処理部２６は、ユーザの属性情報を基に当該ユーザに固有の第１の暗号鍵を動的に生成する。

【００２０】

図３は管理データベース２７に記憶される属性情報テーブルの構成とデータ例を示す概略図である。属性情報テーブルは、住所、氏名、パスワード、暗号鍵（データ用）、をユーザＩＤ毎に関連付けて保持する。ここで、ユーザＩＤはユーザを一意に特定する番号である。住所はユーザの住所である。氏名はユーザの氏名である。パスワードは後述する認証部２３にて行われるユーザ認証に使用されるパスワードである。暗号鍵は後述するカード情報を暗号化するための暗号鍵（データ用）である。図示するデータ例では、一行目は、ユーザＩＤが「０００１」、住所が「○○県××市」、氏名が「Ｙ田Ｔ郎」、パスワードが「＊＊＊＊＊」、暗号鍵が「＆％＃＄」となっており、二行目は、ユーザＩＤが「０００２」、住所が「△△県□□市」、氏名が「Ｕ田Ｓ子」、パスワードが「＊＊＊＊＊」、暗号鍵が「％？＋｝」となっている。

なお、属性情報テーブル内では、ユーザＩＤ、住所、氏名、パスワード等は、暗号化されて保持されている。また、暗号鍵（データ用）は後述する暗号鍵（鍵用）を用いて暗号化されている。

【００２１】

図４は管理データベース２７に記憶されるカード情報テーブルの構成とデータ例を示す概略図である。カード情報テーブルは、銀行番号、支店番号、口座種別、口座番号、クレ

ジットカード番号、カード有効期限、暗証番号、カード名義、をユーザＩＤと口座ＩＤに関連付けて保持する（これらが、カード情報）。ユーザＩＤと口座ＩＤとの複合が、カード情報テーブルの主キーである。銀行番号は停止処理サービスを利用する銀行カードの銀行の番号である。支店番号は前記銀行カードの支店番号である。口座種別は前記銀行カードの口座種別である。口座番号は前記銀行カードの番号である。クレジットカード番号は停止処理サービスを利用するクレジットカードの番号である。カード有効期限は前記クレジットカードの有効期限である。暗証番号は前記銀行カードまたは前記クレジットカードの暗証番号である。カード名義は前記銀行カードまたは前記クレジットカードのカード名義人の氏名である。図示するデータ例では、一行目はユーザＩＤが「０００１」、口座ＩＤが「０１」、銀行番号が「－」、支店番号が「－」、口座種別が「－」、口座番号が「－」クレジットカード番号が「１２３４－５６７８－８９０１－２３４５」、カード有効期限が「２００７／０９」、暗証番号が「＊＊＊＊＊」、カード名義が「Ｙ田Ｔ郎」となっており、二行目は、ユーザＩＤが「０００１」、口座ＩＤが「０２」、銀行番号が「２２５」、支店番号が「００１」、口座種別が「普通」、口座番号が「１２３４５６７」、クレジットカード番号が「－」、カード有効期限が「－」、暗証番号が「＊＊＊＊＊」、カード名義が「Ｙ田Ｔ郎」となっている。

また、銀行番号、支店番号、口座種別、口座番号、クレジットカード番号、カード有効期限、暗証番号、カード名義、は属性情報テーブルに記憶された暗号鍵を用いて暗号化されている。

【００２２】

図５は、暗号鍵（データ用）（第２の暗号鍵）を暗号化する際の処理を示す図である。まず、鍵生成処理部２６は鍵生成用の関数を用いて暗号鍵（鍵用）を生成する。この関数はユーザＩＤとパスワードを入力とし（ユーザＩＤとパスワードがユーザの属性情報）、暗号鍵（鍵用）（第１の暗号鍵）を出力する。この関数は、入力値から出力値を人が類推するのは困難であり、かつ、出力値から入力値を計算することは困難であるハッシュ関数等の関数を用いる。鍵生成処理部２６は、ハッシュ関数等の関数によって得られる値を用いて演算により出力値を得る。次に、暗号化処理５１は前記生成された暗号鍵（鍵用）と暗号鍵（データ用）を入力とし、暗号化された暗号鍵（データ用）を出力する。

なお、パスワードが変更された場合には、上記の関数によって生成される暗号鍵（鍵用）も変更される。そのため、パスワードが変更された場合には、鍵生成処理部２６が新たな暗号鍵（鍵用）を生成すると共に、既に旧・暗号鍵（鍵用）で暗号化されている暗号鍵（データ用）がある場合には、それを一旦復号化したうえで、新たな暗号鍵（鍵用）で再度暗号化するようにする。

【００２３】

図６は、暗号鍵（データ用）を復号化する際の処理を示す図である。復号化処理６０は暗号鍵（鍵用）と暗号化された暗号鍵（データ用）を入力とし、復号化された暗号鍵（データ用）を出力する。復号化に使用する暗号鍵（鍵用）は、鍵生成処理部２６にて、ユーザＩＤとパスワードを使用して生成されたものである。

【００２４】

図７は、カード情報を暗号化する際の処理を示す図である。暗号化処理７０は暗号鍵（データ用）とカード情報である管理データを入力とし、暗号化された管理データを出力する。暗号鍵（データ用）は、前述した暗号化処理５１により暗号化されて属性情報テーブルに記憶されており、使用する際には前述した復号化処理６０により復号化して使用される。

【００２５】

図８は、カード情報を復号化する際の処理を示す図である。復号化処理８０は暗号鍵（データ用）と暗号化された管理データを入力とし、復号化された管理データを出力する。暗号鍵（データ用）は、前述した暗号化処理５１により暗号化されて属性情報テーブルに記憶されており、使用する際には前述した復号化処理６０により復号化して使用される。

【００２６】

図９は、サービス登録の手順を示すシーケンス図である。前提条件として、ユーザは、代行業者へサービス利用申請を本人確認資料と共に送付しており、代行業者は、ユーザへ郵送にて仮ユーザＩＤ及び仮パスワードを発行している。

ユーザ端末１０は、発行された仮ユーザＩＤ及び仮パスワードを停止処理代行サーバ装置２０へ送信する（ステップＳ９０１）。当該データを受信した停止処理代行サーバ装置２０は、認証部２３にてユーザ認証を行い（ステップＳ９０２）、ユーザ認証が成功すると、管理データ登録部２４にてユーザの属性情報を管理データベース２７へ記憶する（ステップＳ９０３）。その際、ユーザの属性情報が既に記憶されていないかをチェックする。次に停止処理代行サーバ装置２０は、ユーザＩＤ及びパスワードの入力フォームをユーザ端末１０へ送信する（ステップＳ９０４）。ユーザ端末１０は、入力フォームへ入力されたユーザＩＤとパスワードを停止処理代行サーバ装置２０へ送信する。停止処理代行サーバ装置２０は、ユーザ端末１０から受信したユーザＩＤとパスワードをユーザ固有のユーザＩＤとパスワードとして決定する（ステップＳ９０６）。停止処理代行サーバ２０は、当該ユーザＩＤと当該パスワードを属性情報テーブルへ記憶し（ステップＳ９０７）、管理データ入力フォームをユーザ端末１０へ送信する（ステップＳ９０８）。ユーザ端末１０は、この管理データ入力フォームに入力されたカード情報とこのカード情報を暗号化するための暗号鍵（データ用）を停止処理代行サーバ装置２０へ送信する（ステップＳ９０９）。停止処理代行サーバ装置２０は、管理データ登録部２４にて受信したカード情報を受信した暗号鍵（データ用）を用いて暗号化し、暗号鍵（データ用）を鍵生成部２６にて生成した暗号鍵（鍵用）を用いて暗号化し、この暗号化したカード情報と暗号鍵（データ用）を管理データベース２７へ記憶する（ステップＳ９１０）。

【００２７】

図１０は、停止処理代行サーバ２０の上記ステップＳ９０８の処理に基づきユーザ端末１０が表示する管理データ入力フォームの例である。入力フォームには、ユーザＩＤが表示されており、ユーザは複数の銀行カード及びクレジットカードの情報を入力することができる。銀行カードの情報は、銀行番号、支店番号、口座種別、口座番号、名義、暗証番号である。また、クレジットカードの情報は、カード番号、期限、名義、暗証番号である。

【００２８】

図１１は、停止処理の依頼の手順を示すシーケンス図である。ユーザ端末１０は、ユーザＩＤとパスワードを停止処理代行サーバ装置２０へ送信する（ステップＳ１１０）。このデータを受信した代行サーバ装置２０は認証部２３にてユーザ認証を行い（ステップＳ１１１）、ユーザ認証が成功するとサービス選択フォームをユーザ端末１０へ送信する（ステップＳ１１２）。ユーザは、サービス選択フォームでは、停止サービスかデータメンテナンスかを選択可能である。ユーザ端末１０は、選択した情報を停止処理代行サーバ装置２０へ送信する（ステップＳ１１３）。停止処理代行サーバ装置２０は、データメンテナンスが選択された場合には、上述したサービス登録を行う（ステップＳ１１９）。ストップサービスが選択された場合は、停止処理代行サーバ装置２０は、実行認証画面をユーザ端末１０へ送信する（ステップＳ１１６）。ユーザ端末１０は、実行認証画面に入力したデータを停止処理代行サーバ装置２０へ送信する（ステップＳ１１７）。停止処理代行サーバ装置２０は、停止サービス処理部２５にて選択されたカードのカード情報を取り出し、該当する提携会社のカード管理サーバ装置３０へカード情報、暗号鍵（データ用）、暗号鍵（鍵用）を送信する（ステップＳ１１８）。

【００２９】

図１２は、停止処理代行サーバ２０の上記ステップＳ１１６の処理に基づきユーザ端末１０が表示する実行認証画面の例である。実行認証画面には、ユーザＩＤと、停止を実行するボタンと、カード停止操作と登録したカードが複数選択できるチェックボックスと、が表示される。情報カード停止操作を選択した場合には、登録済みの全てのカードの停止をする。また、個別に停止をするカードを複数選択することもできる。停止を実行するボタンを押すと、ユーザ端末１０は、入力したデータを停止処理代行サーバ２０へ送信する

。

【００３０】

図１３は、停止処理代行サーバ装置２０とカード管理サーバ装置３０間の停止処理の手順を示すシーケンス図である。停止処理代行サーバ装置２０は、暗号化された暗号鍵（データ用）と、暗号鍵（データ用）を復号化する暗号鍵（鍵用）と、暗号化されたカード情報である管理データと、をカード管理サーバ装置３０へ送信する（ステップＳ１３０）。この情報を受け取った（ステップＳ１３１）カード管理サーバ装置３０は、管理データを復号化する（ステップＳ１３２、ステップＳ１３７）。既存システムがカード管理サーバ装置３０と連動している場合は、カード管理サーバ装置３０は、既存システムへ停止命令を送信する（ステップＳ１３３）。そうでない場合は、カード管理サーバ装置３０は、オペレータの画面へ復号化したカード情報を表示する（ステップＳ１３７）。オペレータは既存システムにて停止作業を行う（ステップＳ１３８）。既存システムでの停止作業が終了したら、既存システムもしくはオペレータは、カード管理サーバ装置３０へ通知する（ステップＳ１３４、ステップＳ１３９）。通知を受けたカード管理サーバ装置３０は、終了した旨を停止処理代行サーバ装置２０へ通知する（ステップＳ１３５）。停止処理代行サーバ装置２０は、終了を確認すると、ユーザ端末１０へ停止処理終了がしたことを通知する（ステップＳ１３６）。

【００３１】

このように、本実施形態によれば、停止処理代行サーバにより複数の異なる金融機関やクレジットカード会社のカードを一括して停止することができる。また、停止処理代行サーバ装置２０は、カード情報を暗号化する際に使用する暗号鍵（データ用）を別の暗号鍵（鍵用）で暗号化している。よって、暗号鍵自身の安全性が高まる。また、暗号鍵（鍵用）は、ユーザＩＤとパスワードを使用して動的に生成しているため、ユーザに固有であり、管理データベース２７へ保持する必要はない。これにより、全てのユーザのカード情報が一度に漏洩することを防止できる。

【００３２】

また、ユーザ端末１０と停止処理代行サーバ装置２０とカード管理サーバ装置３０の各部の機能を実現するためのプログラムをコンピュータ読み取り可能な記録媒体に記録して、この記録媒体に記録されたプログラムをコンピュータシステムに読み込ませ、実行することにより、

停止処理を行ってもよい。なお、ここでいう「コンピュータシステム」とは、ＯＳや周辺機器等のハードウェアを含むものであってもよい。

また、「コンピュータシステム」は、ＷＷＷシステムを利用している場合であれば、ホームページ提供環境（あるいは表示環境）も含むものとする。また、「コンピュータ読み取り可能な記録媒体」とは、フレキシブルディスク、光磁気ディスク、ＲＯＭ、フラッシュメモリ等の書き込み可能な不揮発性メモリ、ＣＤ－ＲＯＭ等の可搬媒体、コンピュータシステムに内蔵されるハードディスク等の記憶装置のことをいう。

【００３３】

さらに「コンピュータ読み取り可能な記録媒体」とは、インターネット等のネットワークや電話回線等の通信回線を介してプログラムが送信された場合のサーバやクライアントとなるコンピュータシステム内部の揮発性メモリ（例えばＤＲＡＭ（Dynamic Random Access Memory））のように、一定時間プログラムを保持しているものも含むものとする。

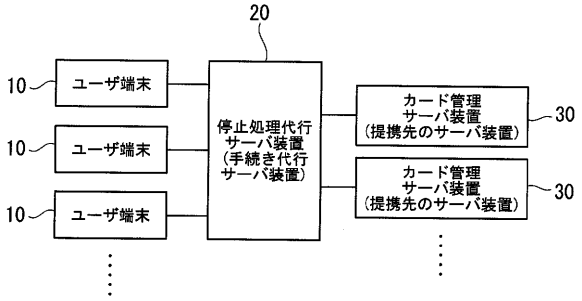
また、上記プログラムは、このプログラムを記憶装置等に格納したコンピュータシステムから、伝送媒体を介して、あるいは、伝送媒体中の伝送波により他のコンピュータシステムに伝送されてもよい。ここで、プログラムを伝送する「伝送媒体」は、インターネット等のネットワーク（通信網）や電話回線等の通信回線（通信線）のように情報を伝送する機能を有する媒体のことをいう。

また、上記プログラムは、前述した機能の一部を実現するためのものであっても良い。さらに、前述した機能をコンピュータシステムにすでに記録されているプログラムとの組み合わせで実現できるもの、いわゆる差分ファイル（差分プログラム）であっても良い。

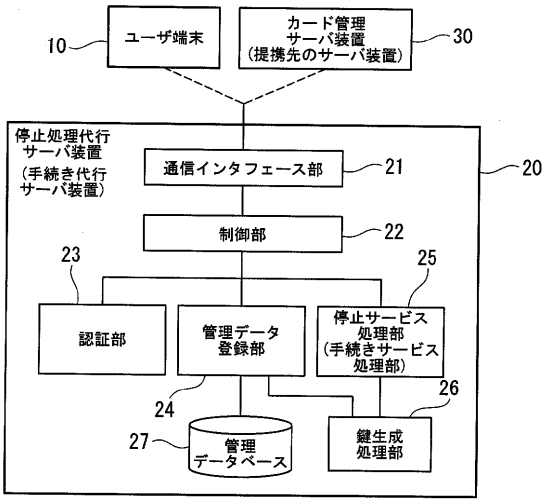
【００３４】
以上、図面を参照してこの発明の一実施形態について詳しく説明してきたが、具体的な構成は上述のものに限られることはなく、この発明の要旨を逸脱しない範囲内において様々な設計変更等をすることが可能である。
例えば、ガス、電気、水道、決済、予約などのシステムの代行サービスにおけるデータ管理にも適用が可能である。
つまり、ガス、電気、水道、決済、予約や、その他、生活における活動、ビジネスにおける活動、経済活動において、ユーザの利便性を向上させるために、ユーザの属性情報を基に当該ユーザに固有の第１の暗号鍵を動的に生成する鍵生成処理部と、前記ユーザのための代行サービスに関する代行サービス情報を保持する管理データベースと、ユーザの認証処理を行なう認証部と、前記認証部による前記ユーザ認証処理の結果に基づき、ユーザ端末から当該ユーザのための代行サービスに関する代行サービス情報と第２の暗号鍵とを受信し、前記代行サービス情報を前記第２の暗号鍵を用いて暗号化して前記管理データベースに書き込むとともに、当該ユーザの属性情報を基に前記鍵生成処理部が生成した前記第１の暗号鍵を用いて前記第２の暗号鍵を暗号化して前記管理データベースに書き込む管理データ登録部と、前記認証部による前記ユーザ認証処理の結果に基づき、ユーザ端末から、前記代行サービスに関する手続きを特定する情報を受信し、この特定された手続きの情報を前記管理データベースから読み出し、当該手続きの情報を、前記管理データベースから読み出した当該ユーザの前記第２の暗号鍵および前記鍵生成処理部が当該ユーザの属性情報を基に生成した第１の暗号鍵とともに提携先の管理サーバ装置に送信する手続きサービス処理部とを備えることを特徴とする手続き代行サーバ装置を設けるようにしても良い。
【図面の簡単な説明】
【００３５】
【図１】本発明の一本実施形態による停止処理代行サービスシステム（手続き代行サービスシステム）の構成図である。
【図２】本実施形態における停止処理代行サーバ装置（手続き代行サーバ装置）の構成を示すブロック図である。
【図３】本実施形態における管理データベースに記憶される属性情報テーブルの構成とデータ例を示す概略図である。
【図４】本実施形態における管理データベースに記憶されるカード情報テーブルの構成とデータ例を示す概略図である。
【図５】本実施形態における暗号鍵（データ用）を暗号化する際の処理を示す図である。
【図６】本実施形態における暗号鍵（データ用）を復号化する際の処理を示す図である。
【図７】本実施形態におけるカード情報を暗号化する際の処理を示す図である。
【図８】本実施形態におけるカード情報を復号化する際の処理を示す図である。
【図９】本実施形態におけるサービス登録の手順を示すシーケンス図である。
【図１０】本実施形態におけるユーザ端末が表示する管理データ入力フォームの例である。
【図１１】本実施形態における停止処理（手続きサービス処理）の依頼の手順を示すシーケンス図である。
【図１２】本実施形態におけるユーザ端末が表示する実行認証画面の例である。
【図１３】本実施形態における停止処理代行サーバ装置（手続き代行サーバ装置）とカード管理サーバ装置（提携先のサーバ装置）間の停止処理（手続きサービス処理）の手順を示すシーケンス図である。
【符号の説明】
【００３６】
１０…ユーザ端末　２０…停止処理代行サーバ装置（手続き代行サーバ装置）　３０…カード管理サーバ装置（提携先のサーバ装置）　２１…通信インタフェース部　２２…制御部　２３…認証部　２４…管理データ登録部　２５…停止サービス処理部（手続きサー

いす処理部）　２６…鍵生成処理部　２７…管理データベース　５０…関数　５１…暗号化処理　６０…復号化処理　７０…暗号化処理　８０…復号化処理

【図１】




【図２】



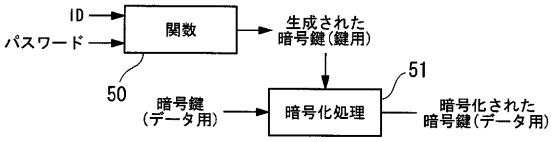

【図３】

| ユーザID | 住所 | 氏名 | パスワード | 暗号鍵 |
|---|---|---|---|---|
| 0001 | ○○県××市 | Ｙ田　Ｔ郎 | ***** | &%#$ |
| 0002 | △△県□□市 | Ｕ田　Ｓ子 | ***** | %?*] |
| … | … | … | … | … |

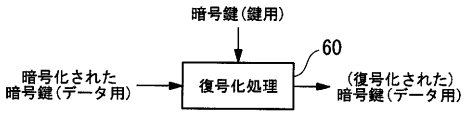
【図４】

| ユーザID | 口座ID | 銀行番号 | 支店番号 | 口座種別 | 口座番号 | クレジットカード番号 | カード有効期限 | 暗証番号 | カード名義 |
|---|---|---|---|---|---|---|---|---|---|
| 0001 | 01 | — | — | — | — | 1234-5678-8901-2345 | 2007/09 | ***** | Y田 T郎 |
| 0001 | 02 | 225 | 001 | 普通 | 1234567 | — | — | ***** | Y田 T郎 |
| … | … | … | … | … | … | … | … | … | … |

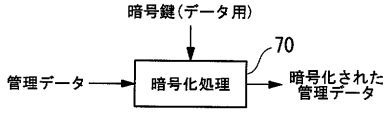
【図５】




【図６】

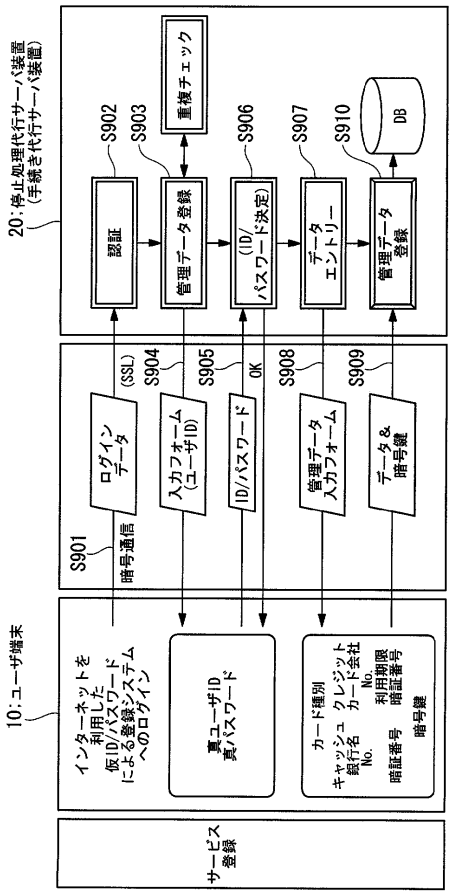



【図７】

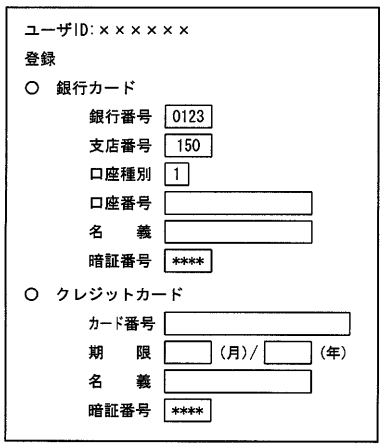



【図８】

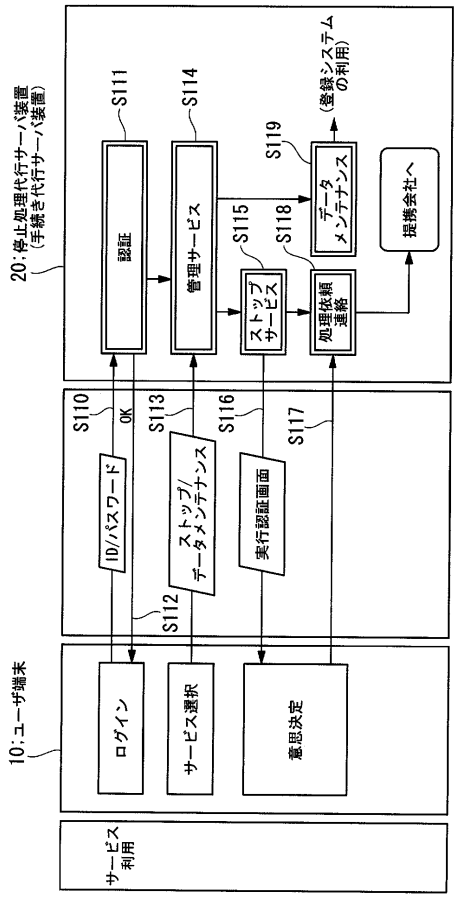

【図９】



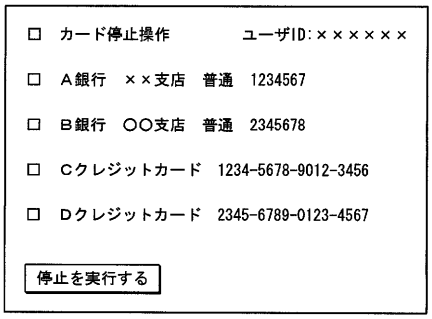

【図１０】



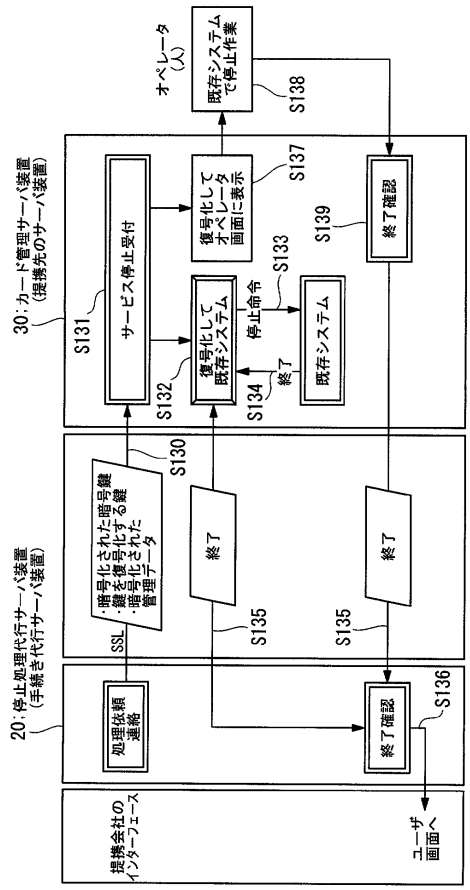
【図１１】


10:ユーザ端末
20:停止処理代行サーバ装置
(手続き代行サーバ装置)
サービス利用
ログイン
サービス選択
意思決定
ID/パスワード
ストップ/データメンテナンス
実行認証画面
認証
管理サービス
ストップサービス
処理依頼連絡
データメンテナンス
提携会社へ
(登録システムの利用)
S110
S111
S112
S113
S114
S115
S116
S117
S118
S119
OK

【図１２】


□ カード停止操作 ユーザID:××××××
□ A銀行 ××支店 普通 1234567
□ B銀行 ○○支店 普通 2345678
□ Cクレジットカード 1234-5678-9012-3456
□ Dクレジットカード 2345-6789-0123-4567
停止を実行する

【図１３】


20:停止処理代行サーバ装置
(手続き代行サーバ装置)
30:カード管理サーバ装置
(提携先のサーバ装置)
オペレータ(人)
提携会社のインターフェース
ユーザ画面へ
処理依頼連絡
SSL
暗号化された暗号鍵
鍵を復号化する鍵
暗号化されたデータ
終了
サービス停止受付
復号化して既存システム
停止命令
終了
既存システム
復号化してオペレータ画面に表示
既存システムで停止作業
終了確認
S130
S131
S132
S133
S134
S135
S136
S137
S138
S139