(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5404501号
(P5404501)
(45)発行日　平成26年2月5日(2014.2.5)　(24)登録日　平成25年11月8日(2013.11.8)

(51)Int.Cl.　　F I
H04L 9/08 (2006.01)　　H04L 9/00 601B
G06F 21/10 (2013.01)　　G06F 21/22 110A
　　H04L 9/00 601F

請求項の数 5　(全 15 頁)

(21)出願番号　特願2010-77989(P2010-77989)
(22)出願日　平成22年3月30日(2010.3.30)
(65)公開番号　特開2011-211537(P2011-211537A)
(43)公開日　平成23年10月20日(2011.10.20)
審査請求日　平成24年2月13日(2012.2.13)

(73)特許権者　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目３番１号
(74)代理人　100147485
弁理士　杉村　憲司
(72)発明者　柏木　巧
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(72)発明者　村井　健二
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内

審査官　青木　重徳

最終頁に続く

(54)【発明の名称】暗号化情報の有効期限延長システム、有効期限延長方法及びプログラム

(57)【特許請求の範囲】
【請求項１】
ポータルサーバを利用した暗号化情報の有効期限を自動的に延長する、暗号化情報の有効期限延長システムであって、
所定の情報端末の利用者に提示するための所定の個人情報に対して共通鍵で暗号化を施すと共に、該共通鍵を公開鍵証明書で暗号化を施して、暗号化個人情報及び暗号化共通鍵を生成するサービスサーバと、
ポータルサーバからの要求に応じて、前記サービスサーバが前記暗号化個人情報及び暗号化共通鍵を生成するのに用いられる公開鍵証明書を、該公開鍵証明書の鍵ペアを構成する秘密鍵とともに生成し、前記公開鍵証明書及び前記秘密鍵を保持して管理する鍵管理サーバと、
前記サービスサーバから前記暗号化個人情報及び暗号化共通鍵を取得し、前記暗号化個人情報及び暗号化共通鍵を生成するのに用いた公開鍵証明書の有効期限を設定して、前記暗号化個人情報及び暗号化共通鍵を個人情報データベース内に保持するポータルサーバと、を備え、
前記ポータルサーバは、
前記個人情報データベースに保持している公開鍵証明書の再発行要求を行う有効期限を定期的に検査する手段と、
該手段によって前記個人情報データベースに保持している公開鍵証明書が前記有効期限に達していると判断した場合に、前記鍵管理サーバに対して、前記暗号化共通鍵を送付し

て前記公開鍵証明書の鍵ペアを構成する秘密鍵で復号させるとともに、新たな公開鍵証明書の生成と、該新たな公開鍵証明書による当該共通鍵の再度の暗号化を実行させて再度の暗号化共通鍵を生成させ、前記新たな公開鍵証明書を前記サービスサーバに送付させるとともに、前記新たな公開鍵証明書及び前記再度の暗号化共通鍵を再取得し、前記新たな公開鍵証明書の有効期限を設定して前記個人情報データベース内に保持する手段と、を備えることを特徴とする、暗号化情報の有効期限延長システム。

【請求項２】

前記ポータルサーバは、

前記情報端末から当該個人情報の閲覧要求を受け付ける手段と、

前記個人情報を復号するために、前記暗号化共通鍵の復号要求を前記鍵管理サーバに送信して、復号した共通鍵を前記鍵管理サーバから取得する手段と、

該共通鍵を用いて、前記個人情報データベース内に格納されている前記暗号化個人情報を復号して前記情報端末に提示する手段と、

を備えることを特徴とする、請求項１に記載の暗号化情報の有効期限延長システム。

【請求項３】

前記ポータルサーバは、前記鍵管理サーバを内部に備えるように構成されていることを特徴とする、請求項１又は２に記載の暗号化情報の有効期限延長システム。

【請求項４】

ポータルサーバを利用した暗号化情報の有効期限を自動的に延長する、暗号化情報の有効期限延長システムにおける、暗号化情報の有効期限延長方法であって、

前記有効期限延長システムは、所定の情報端末の利用者に提示するための所定の個人情報に対して共通鍵で暗号化を施すと共に、該共通鍵を公開鍵証明書で暗号化を施して、暗号化個人情報及び暗号化共通鍵を生成するサービスサーバと、ポータルサーバからの要求に応じて、前記サービスサーバが前記暗号化個人情報及び暗号化共通鍵を生成するのに用いられる公開鍵証明書を、該公開鍵証明書の鍵ペアを構成する秘密鍵とともに生成し、前記公開鍵証明書及び前記秘密鍵を保持して管理する鍵管理サーバと、前記サービスサーバから前記暗号化個人情報及び暗号化共通鍵を取得し、前記暗号化個人情報及び暗号化共通鍵を生成するのに用いた公開鍵証明書の有効期限を設定して、前記暗号化個人情報及び暗号化共通鍵を個人情報データベース内に保持するポータルサーバとを備えており、

前記ポータルサーバの処理手順は、

前記個人情報データベースに保持している公開鍵証明書の再発行要求を行う有効期限を定期的に検査するステップと、

該ステップによって前記個人情報データベースに保持している公開鍵証明書が前記有効期限に達していると判断した場合に、前記鍵管理サーバに対して、前記暗号化共通鍵を送付して前記公開鍵証明書の鍵ペアを構成する秘密鍵で復号させるとともに、新たな公開鍵証明書の生成と、該新たな公開鍵証明書による当該共通鍵の再度の暗号化を実行させて再度の暗号化共通鍵を生成させ、前記新たな公開鍵証明書を前記サービスサーバに送付させるとともに、前記新たな公開鍵証明書及び前記再度の暗号化共通鍵を再取得し、前記新たな公開鍵証明書の有効期限を設定して前記個人情報データベース内に保持するステップと、

を含むことを特徴とする、暗号化情報の有効期限延長方法。

【請求項５】

所定の情報端末の利用者に提示するための所定の個人情報に対して共通鍵で暗号化を施すと共に、該共通鍵を公開鍵証明書で暗号化を施して、暗号化個人情報及び暗号化共通鍵を生成するサービスサーバと、ポータルサーバからの要求に応じて、前記サービスサーバが前記暗号化個人情報及び暗号化共通鍵を生成するのに用いられる公開鍵証明書を、該公開鍵証明書の鍵ペアを構成する秘密鍵とともに生成し、前記公開鍵証明書及び前記秘密鍵を保持して管理する鍵管理サーバと、前記サービスサーバから前記暗号化個人情報及び暗号化共通鍵を取得し、前記暗号化個人情報及び暗号化共通鍵を生成するのに用いた公開鍵証明書の有効期限を設定して、前記暗号化個人情報及び暗号化共通鍵を個人情報データベ

ース内に保持するポータルサーバとを備える有効期限延長システムにおける、前記ポータルサーバとして構成するコンピュータに、
前記個人情報データベースに保持している公開鍵証明書の再発行要求を行う有効期限を定期的に検査するステップと、
該ステップによって前記個人情報データベースに保持している公開鍵証明書が前記有効期限に達していると判断した場合に、前記鍵管理サーバに対して、前記暗号化共通鍵を送付して前記公開鍵証明書の鍵ペアを構成する秘密鍵で復号させるとともに、新たな公開鍵証明書の生成と、該新たな公開鍵証明書による当該共通鍵の再度の暗号化を実行させて再度の暗号化共通鍵を生成させ、前記新たな公開鍵証明書を前記サービスサーバに送付させるとともに、前記新たな公開鍵証明書及び前記再度の暗号化共通鍵を再取得し、前記新たな公開鍵証明書の有効期限を設定して前記個人情報データベース内に保持するステップと、
を実行させるためのプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、公開鍵証明書で暗号化された情報の有効期限の管理技術に関し、特に、暗号化情報の有効期限延長システム、有効期限延長方法及びプログラムに関する。
【背景技術】
【０００２】
従来から、情報の安全な流通を実現する仕組みとして、電子私書箱などのポータルサーバを利用して、情報を利用者のＩＣカードに設定された秘密鍵とペアになる公開鍵証明書にて暗号化し、ポータルサーバ上に保管するシステムが知られている（例えば、非特許文献１参照）。この従来からのシステムでは、図８に示すように、利用者が保存された情報を閲覧する前に暗号に利用した公開鍵証明書の有効期限が切れた場合は、利用者自身がＩＣカードを廃棄または発行元に返却することになるため閲覧不可能となる。
【先行技術文献】
【非特許文献】
【０００３】
【非特許文献１】“電子私書箱（仮称）による社会保障サービス等のＩＴ化に関する検討会報告書、参考資料２、技術検討ワーキンググループ検討案”、平成２０年３月１７日報告、内閣官房情報通信技術（ＩＴ）担当室、［online]、［２０１０年３月１日検索］、インターネット〈http://www.kantei.go.jp/jp/singi/it2/epo-box/dai5/siryou1.pdf〉
【発明の概要】
【発明が解決しようとする課題】
【０００４】
従来からの電子私書箱などのポータルサーバを利用して、情報を利用者のＩＣカードに設定された秘密鍵とペアになる公開鍵証明書にて暗号化し、ポータルサーバ上に保管するシステムは、情報の安全な流通を実現する仕組みとして有益な技術である。
【０００５】
しかしながら、公開鍵証明書で暗号化された情報は、証明書の有効期限が失効すると暗号化された情報を復号するための秘密鍵を廃棄していることがあり、復号して情報を確認できなくなることがある。このため、有効期限が切れる前に新しい公開鍵証明書にて再暗号する仕組みが望まれていた。
【０００６】
本発明は、上述の問題に鑑みて為されたものであり、暗号化情報の有効期限延長システム、有効期限延長方法及びプログラムを提供することにある。
【課題を解決するための手段】
【０００７】
本発明による暗号化情報の有効期限延長システムは、利用者の公開鍵証明書で暗号化さ

れた情報を管理しているポータルサーバと、暗号・復号に利用する鍵を利用者のＩＣカードではなく、サーバ側で生成・管理・演算を行う鍵管理サーバとを備える。公開鍵証明書とペアになる秘密鍵は、鍵管理サーバが備える耐タンパ装置内に格納される。

【０００８】

利用者の公開鍵証明書で暗号化された情報を管理しているポータルサーバは、利用している公開鍵証明書（以下、「旧公開鍵証明書」とも称する）の有効期限が失効する前に、旧公開鍵証明書で暗号化された情報と新しい公開鍵証明書（以下、「新公開鍵証明書」とも称する）の発行要求を鍵管理サーバへ送信する。鍵管理サーバは、新公開鍵証明書を発行すると共に、旧公開鍵証明書で暗号化された情報を旧公開鍵証明書のペアとなる秘密鍵で復号し、新公開鍵証明書にて再暗号し、ポータルサーバに返却する。これにより、暗号化された情報は、常に有効期限内の状態でポータルサーバ上に保管しておくことが可能となる。

【０００９】

即ち、本発明による暗号化情報の有効期限延長システムは、ポータルサーバを利用した暗号化情報の有効期限を自動的に延長する、暗号化情報の有効期限延長システムであって、所定の情報端末の利用者に提示するための所定の個人情報に対して共通鍵で暗号化を施すと共に、該共通鍵を公開鍵証明書で暗号化を施して、暗号化個人情報及び暗号化共通鍵を生成するサービスサーバと、ポータルサーバからの要求に応じて、前記サービスサーバが前記暗号化個人情報及び暗号化共通鍵を生成するのに用いられる公開鍵証明書を、該公開鍵証明書の鍵ペアを構成する秘密鍵とともに生成し、前記公開鍵証明書及び前記秘密鍵を保持して管理する鍵管理サーバと、前記サービスサーバから前記暗号化個人情報及び暗号化共通鍵を取得し、前記暗号化個人情報及び暗号化共通鍵を生成するのに用いた公開鍵証明書の有効期限を設定して、前記暗号化個人情報及び暗号化共通鍵を個人情報データベース内に保持するポータルサーバとを備え、前記ポータルサーバは、前記個人情報データベースに保持している公開鍵証明書の再発行要求を行う有効期限を定期的に検査する手段と、該手段によって前記個人情報データベースに保持している公開鍵証明書が前記有効期限に達していると判断した場合に、前記鍵管理サーバに対して、前記暗号化共通鍵を送付して前記公開鍵証明書の鍵ペアを構成する秘密鍵で復号させるとともに、新たな公開鍵証明書の生成と、該新たな公開鍵証明書による当該共通鍵の再度の暗号化を実行させて再度の暗号化共通鍵を生成させ、前記新たな公開鍵証明書を前記サービスサーバに送付させるとともに、前記新たな公開鍵証明書及び前記再度の暗号化共通鍵を再取得し、前記新たな公開鍵証明書の有効期限を設定して前記個人情報データベース内に保持する手段と、を備えることを特徴とする。

【００１１】

また、本発明による暗号化情報の有効期限延長システムにおいて、前記ポータルサーバは、前記情報端末から当該個人情報の閲覧要求を受け付ける手段と、前記個人情報を復号するために、前記暗号化共通鍵の復号要求を前記鍵管理サーバに送信して、復号した共通鍵を前記鍵管理サーバから取得する手段と、該共通鍵を用いて、前記個人情報データベース内に格納されている前記暗号化個人情報を復号して前記情報端末に提示する手段と、を備えることを特徴とする。

【００１２】

また、本発明による暗号化情報の有効期限延長システムにおいて、前記ポータルサーバは、前記鍵管理サーバを内部に備えるように構成することもできる。

【００１３】

更に、本発明による暗号化情報の有効期限延長方法は、ポータルサーバを利用した暗号化情報の有効期限を自動的に延長する、暗号化情報の有効期限延長システムにおける、暗号化情報の有効期限延長方法であって、前記有効期限延長システムは、所定の情報端末の利用者に提示するための所定の個人情報に対して共通鍵で暗号化を施すと共に、該共通鍵を公開鍵証明書で暗号化を施して、暗号化個人情報及び暗号化共通鍵を生成するサービスサーバと、ポータルサーバからの要求に応じて、前記サービスサーバが前記暗号化個人情

報及び暗号化共通鍵を生成するのに用いられる公開鍵証明書を、該公開鍵証明書の鍵ペアを構成する秘密鍵とともに生成し、前記公開鍵証明書及び前記秘密鍵を保持して管理する鍵管理サーバと、前記サービスサーバから前記暗号化個人情報及び暗号化共通鍵を取得し、前記暗号化個人情報及び暗号化共通鍵を生成するのに用いた公開鍵証明書の有効期限を設定して、前記暗号化個人情報及び暗号化共通鍵を個人情報データベース内に保持するポータルサーバとを備えており、前記ポータルサーバの処理手順は、前記個人情報データベースに保持している公開鍵証明書の再発行要求を行う有効期限を定期的に検査するステップと、該ステップによって前記個人情報データベースに保持している公開鍵証明書が前記有効期限に達していると判断した場合に、前記鍵管理サーバに対して、前記暗号化共通鍵を送付して前記公開鍵証明書の鍵ペアを構成する秘密鍵で復号させるとともに、新たな公開鍵証明書の生成と、該新たな公開鍵証明書による当該共通鍵の再度の暗号化を実行させて再度の暗号化共通鍵を生成させ、前記新たな公開鍵証明書を前記サービスサーバに送付させるとともに、前記新たな公開鍵証明書及び前記再度の暗号化共通鍵を再取得し、前記新たな公開鍵証明書の有効期限を設定して前記個人情報データベース内に保持するステップと、を含むことを特徴とする。

【００１４】

更に、本発明は、所定の情報端末の利用者に提示するための所定の個人情報に対して共通鍵で暗号化を施すと共に、該共通鍵を公開鍵証明書で暗号化を施して、暗号化個人情報及び暗号化共通鍵を生成するサービスサーバと、ポータルサーバからの要求に応じて、前記サービスサーバが前記暗号化個人情報及び暗号化共通鍵を生成するのに用いられる公開鍵証明書を、該公開鍵証明書の鍵ペアを構成する秘密鍵とともに生成し、前記公開鍵証明書及び前記秘密鍵を保持して管理する鍵管理サーバと、前記サービスサーバから前記暗号化個人情報及び暗号化共通鍵を取得し、前記暗号化個人情報及び暗号化共通鍵を生成するのに用いた公開鍵証明書の有効期限を設定して、前記暗号化個人情報及び暗号化共通鍵を個人情報データベース内に保持するポータルサーバとを備える有効期限延長システムにおける、前記ポータルサーバとして構成するコンピュータに、前記個人情報データベースに保持している公開鍵証明書の再発行要求を行う有効期限を定期的に検査するステップと、該ステップによって前記個人情報データベースに保持している公開鍵証明書が前記有効期限に達していると判断した場合に、前記鍵管理サーバに対して、前記暗号化共通鍵を送付して前記公開鍵証明書の鍵ペアを構成する秘密鍵で復号させるとともに、新たな公開鍵証明書の生成と、該新たな公開鍵証明書による当該共通鍵の再度の暗号化を実行させて再度の暗号化共通鍵を生成させ、前記新たな公開鍵証明書を前記サービスサーバに送付させるとともに、前記新たな公開鍵証明書及び前記再度の暗号化共通鍵を再取得し、前記新たな公開鍵証明書の有効期限を設定して前記個人情報データベース内に保持するステップと、を実行させるためのプログラムとして構成される。

【発明の効果】

【００１５】

本発明では、秘密鍵をＩＣカードなどのデバイスではなく、鍵管理サーバにて管理し、ポータルサーバ側にて公開鍵証明書の有効期限を設定し 、ポータルサーバが自ら有効期限を監視して、有効期限に達した契機で有効期限延長のために、旧公開鍵証明書で暗号化した共通鍵を鍵管理サーバに送付し、鍵管理サーバ側でこの暗号化した共通鍵を復号し、新公開鍵証明書を生成するとともに再暗号化して、ポータルサーバに返却するため、常に、利用者は、ポータルサーバの暗号化された情報を閲覧することができるようになる。

【００１６】

また、鍵管理サーバに送付するのは共通鍵のみであるので、個人情報そのものは送付しないため、情報漏えいを抑止することができる。

【００１７】

また、鍵ペアをサーバ側で管理するため、ＩＣカードなどのデバイスに設定する手間や、デバイスを利用者の手元に配送するコストを抑制することが可能になる。

【図面の簡単な説明】

【００１８】
【図１】本発明による一実施例の暗号化情報の有効期限延長システムの概略図である。
【図２】本発明による一実施例の暗号化情報の有効期限延長システムにおける鍵管理サーバのブロック図である。
【図３】本発明による一実施例の暗号化情報の有効期限延長システムにおけるポータルサーバのブロック図である。
【図４】本発明による一実施例の暗号化情報の有効期限延長システムにおけるサービスサーバのブロック図である。
【図５】本発明による一実施例の暗号化情報の有効期限延長システムにおける事前フェーズの動作フロー図である。
【図６】本発明による一実施例の暗号化情報の有効期限延長システムにおける第１の処理シーケンスの動作フロー図である。
【図７】本発明による一実施例の暗号化情報の有効期限延長システムにおける第２の処理シーケンスの動作フロー図である。
【図８】従来からの電子私書箱などのポータルサーバを利用した個人情報を保管するシステムの問題点を説明する図である。
【発明を実施するための形態】
【００１９】
以下、本発明による一実施例の暗号化情報の有効期限延長システムについて説明する。本発明に係る有効期限延長方法及びプログラムは、本実施例の暗号化情報の有効期限延長システムの説明から明らかになる。
【００２０】
〔システム構成〕
図１は、本発明による一実施例の暗号化情報の有効期限延長システムの概略図を示す。本実施例の暗号化情報の有効期限延長システム１は、鍵管理サーバ１１と、ポータルサーバ１２と、サービスサーバ１３と、情報端末１４とを備える。鍵管理サーバ１１、ポータルサーバ１２、サービスサーバ１３、及び情報端末１４の各々は、インターネットやＬＡＮなどのネットワークを介して通信可能に接続される。
【００２１】
（鍵管理サーバ）
図２は、本発明による一実施例の暗号化情報の有効期限延長システムにおける鍵管理サーバのブロック図である。鍵管理サーバ１１は、制御部１１１と、ネットワークとの通信を制御する通信制御部１１２と、耐タンパ装置１１３と、記憶部１１４とを備える。制御部１１１は、公開鍵証明書生成部１１１１と、鍵ペア要求部１１１２と、鍵演算部１１１３とを備える。尚、本発明に係る制御部１１１の各機能を説明するが、鍵管理サーバ１１が備える他の機能を排除することを意図したものではないことに留意する。鍵管理サーバ１１は、コンピュータとして構成することができ、制御部１１１の各機能を実現する処理内容を記述したプログラムを、当該コンピュータの記憶部１１４に格納しておき、当該コンピュータの中央演算処理装置（ＣＰＵ）によってこのプログラムを読み出して実行させることで実現することができる。
【００２２】
耐タンパ装置１１３は、非正規な手段による機密データの読取を防止する機能を有し、非対称鍵ペアの生成及び鍵演算を行う装置であり、公開鍵証明書のペアとなる秘密鍵を管理・保管する秘密鍵保持部１１３１を有する。耐タンパ装置１１３は、耐タンパ性のある装置の例として、ＴＰＭ（Ｔｒｕｓｔｅｄ　Ｐｌａｔｆｏｒｍ　Ｍｏｄｕｌｅ）やＨＳＭ（ＨａｒｄｗａｒｅＳｅｃｕｒｉｔｙＭｏｄｕｌｅ）などがある。
【００２３】
公開鍵証明書生成部１１１１は、耐タンパ装置１１３で生成した公開鍵を用いて公開鍵証明書を生成する機能を有する。尚、本実施例では公開鍵証明書生成部１１１１を具備する例を説明するが、公開鍵証明書の生成自体は、外部の認証局（信用ある第三者機関）で

生成するように構成することもできる。
【００２４】
鍵ペア要求部１１１２は、耐タンパ装置１１３に対して、非対称鍵ペア（秘密鍵、公開鍵）の生成を要求する機能を有する。
【００２５】
鍵演算部１１１３は、耐タンパ装置１１３に対して、鍵演算を要求する機能を有する。
【００２６】
（ポータルサーバ）
図３は、本発明による一実施例の暗号化情報の有効期限延長システムにおけるポータルサーバのブロック図である。ポータルサーバ１２は、制御部１２１と、ネットワークとの通信を制御する通信制御部１２２と、個人情報データベース１２３と、記憶部１２４とを備える。制御部１２１は、公開鍵証明書生成要求部１２１１と、有効期限延長要求部１２１２と、個人情報ＤＢアクセス部１２１３と、有効期限管理部１２１４とを備える。尚、本発明に係る制御部１２１の各機能を説明するが、ポータルサーバ１２が備える他の機能を排除することを意図したものではないことに留意する。ポータルサーバ１２は、コンピュータとして構成することができ、制御部１２１の各機能を実現する処理内容を記述したプログラムを、当該コンピュータの記憶部１２４に格納しておき、当該コンピュータの中央演算処理装置（ＣＰＵ）によってこのプログラムを読み出して実行させることで実現することができる。
【００２７】
公開鍵証明書生成要求部１２１１は、鍵管理サーバ１１に対して、公開鍵証明書の生成を要求する機能を有する。
【００２８】
有効期限延長要求部１２１２は、有効期限管理部１２１４による公開鍵証明書の再発行要求等の要求時期に達したことを確認した際に、有効期限延長の処理を鍵管理サーバ１１に対して要求する機能を有する。
【００２９】
個人情報ＤＢアクセス部１２１３は、個人情報データベース（ＤＢ）１２３にアクセスする機能を有する。有効期限延長を行う際は、旧公開鍵証明書で暗号された情報（暗号化共通鍵や暗号化個人情報）を取得する機能、及び個人情報データベース（ＤＢ）１２３に対して、新公開鍵証明書で暗号された情報（暗号化共通鍵や暗号化個人情報）の保管を行う機能を有する。
【００３０】
有効期限管理部１２１４は、個人情報データベース（ＤＢ）１２３に対して、公開鍵証明書の再発行要求を行う有効期限の設定および設定された要求時期をチェック（検査）する機能を有する。
【００３１】
（サービスサーバ）
図４は、本発明による一実施例の暗号化情報の有効期限延長システムにおけるサービスサーバのブロック図である。サービスサーバ１３は、利用者の公開鍵証明書を用いて情報を暗号化し、ポータルサーバ１２に暗号化した情報を提供するサーバであり、制御部１３１と、ネットワークとの通信を制御する通信制御部１３２と、記憶部１３３とを備える。制御部１３１は、個人情報暗号化部１３１１と、共通鍵暗号化部１３１２とを備える。尚、本発明に係る制御部１３１の各機能を説明するが、サービスサーバ１３が備える他の機能を排除することを意図したものではないことに留意する。サービスサーバ１３は、コンピュータとして構成することができ、制御部１３１の各機能を実現する処理内容を記述したプログラムを、当該コンピュータの記憶部１３３に格納しておき、当該コンピュータの中央演算処理装置（ＣＰＵ）によってこのプログラムを読み出して実行させることで実現することができる。
【００３２】

個人情報暗号化部１３１１は、情報端末１４に提示する利用者個人の個人情報を暗号化するために共通鍵を生成して、生成した共通鍵で当該個人情報を暗号化する機能を有する。尚、「共通鍵」は、暗号化処理と復号処理とで、同一の（共通の）鍵を用いる方式であり、対称鍵とも称される。

【００３３】

共通鍵暗号化部１３１２は、情報端末１４の利用者個人の個人情報の暗号化に用いた共通鍵を公開鍵証明書で暗号化する機能を有する。

【００３４】

サービスサーバ１３の制御部１３１は、個人情報暗号化部１３１１によって暗号化した個人情報（暗号化個人情報）と、共通鍵暗号化部１３１２によって暗号化した共通鍵（暗号化共通鍵）を、通信制御部１３２を介してポータルサーバ１２に送出する機能を有する。

【００３５】

（情報端末）

情報端末１４は、利用者が操作し、ポータルサーバ１２に保管された暗号化情報を閲覧する端末である。

【００３６】

次に、本発明による一実施例の暗号化情報の有効期限延長システムの動作について説明する。先ず、システム動作に伴う事前フェーズとして、事前フェーズＣ１，Ｃ２,Ｃ３について図５を参照して説明する。図５は、本発明による一実施例の暗号化情報の有効期限延長システムにおける事前フェーズの動作フロー図である。

【００３７】

〔システム動作：事前フェーズ〕

（事前フェーズＣ１）

先ず、ポータルサーバ１２は、公開鍵証明書生成要求部１２１１によって、鍵管理サーバ１１に対して、公開鍵証明書（秘密鍵を含む）の生成を要求する（ステップＳ１）。

【００３８】

鍵管理サーバ１１は、鍵ペア要求部１１１２によって、耐タンパ装置１１３に対して、非対称鍵ペア（秘密鍵、公開鍵）の生成を要求して、耐タンパ装置１１３から公開鍵を取得する（ステップＳ２）。

【００３９】

鍵管理サーバ１１は、公開鍵証明書生成部１１１１によって、耐タンパ装置１１３で生成した公開鍵を用いて公開鍵証明書を生成し、ポータルサーバ１２及びサービスサーバ１３に配布する（ステップＳ３）。従って、情報端末１４の利用者個人が利用する公開鍵証明書の発行は鍵管理サーバ１１が行うことなり、ポータルサーバ１２及びサービスサーバ１３へと配布される。

【００４０】

（事前フェーズＣ２）

ポータルサーバ１２は、鍵管理サーバ１１から情報端末１４の利用者個人が利用する公開鍵証明書を受け取ると、有効期限管理部１２１４によって、個人情報データベース（ＤＢ）１２３に対して、公開鍵証明書の再発行要求を行うための有効期限の設定を行い、有効期限を設定した旨を情報端末１４に通知する（ステップＳ４）。尚、有効期限は、利用する公開鍵証明書の有効期限を越えない範囲で、利用者個人がポータルサーバ１２に対して直接設定してもよい。

【００４１】

（事前フェーズＣ３）

一方、サービスサーバ１３は、個人情報暗号化部１３１１によって、情報端末１４に提示する利用者個人の個人情報を暗号化するために共通鍵を生成して、生成した共通鍵で当該個人情報を暗号化する（ステップＳ５）。

【００４２】

続いて、サービスサーバ１３は、共通鍵暗号化部１３１２によって、情報端末１４の利用者個人の個人情報の暗号化に用いた共通鍵を公開鍵証明書で暗号化する（ステップＳ６）。

【００４３】

サービスサーバ１３の制御部１３１は、個人情報暗号化部１３１１によって暗号化した個人情報（暗号化個人情報）と、共通鍵暗号化部１３１２によって暗号化した共通鍵（暗号化共通鍵）を、通信制御部１３２を介してポータルサーバ１２に送出する。

【００４４】

従って、サービスサーバ１３からポータルサーバ１２宛に送付される個人情報は、サービスサーバ１３にて共通鍵を用いて暗号化され、この共通鍵も利用者の公開鍵証明書にて暗号化されたものがセットとなって、ポータルサーバ１２上の個人情報データベース（ＤＢ）１２３に、暗号化されたまま保存される（ステップＳ７）。

【００４５】

上記の各事前フェーズの処理は、情報端末１４に提示する利用者個人の個人情報について任意のタイミングで行われる。

【００４６】

次に、本発明による一実施例の暗号化情報の有効期限延長システムの動作について説明する。

【００４７】

〔システム動作：第１の処理シーケンス〕

図６は、本発明による一実施例の暗号化情報の有効期限延長システムにおける第１の処理シーケンスの動作フロー図である。ポータルサーバ１２は、有効期限管理部１２１４によって、定期的に個人情報データベース（ＤＢ）１２３に設定された公開鍵証明書の有効期限をチェック（検査）する（ステップＳ１１）。

【００４８】

ポータルサーバ１２は、有効期限管理部１２１４によって、有効期限に達したことを確認した場合、個人情報ＤＢアクセス部１２１３によって、個人情報データベース（ＤＢ）１２３に格納していた旧公開鍵証明書で暗号された暗号化共通鍵を取得し（ステップＳ１２）、公開鍵証明書生成要求部１２１１によって、鍵管理サーバ１１に対して、暗号化共通鍵を送付して旧公開鍵証明書の鍵ペアを構成する秘密鍵で復号させるとともに、新たな公開鍵証明書（新公開鍵証明書）の生成を要求するとともに、新公開鍵証明書による共通鍵の暗号化を要求する。

【００４９】

鍵管理サーバ１１は、新公開鍵証明書の生成の要求と、新公開鍵証明書による共通鍵の暗号化の要求を受け付けると、鍵ペア要求部１１１２によって、耐タンパ装置１１３に対して、非対称鍵ペア（秘密鍵、公開鍵）の生成を要求して、耐タンパ装置１１３から公開鍵を取得し、公開鍵証明書生成部１１１１によって、耐タンパ装置１１３で生成した公開鍵を用いて新公開鍵証明書を生成するとともに（ステップＳ１３）、鍵演算部１１１３によって、取得した（旧公開鍵証明書で暗号化された）暗号化共通鍵を旧公開鍵証明書に該当する秘密鍵で復号し（ステップＳ１４）、新公開鍵証明書にて暗号を行い（ステップＳ１５）、制御部１１１の制御によって、新公開鍵証明書と新公開鍵証明書にて暗号化した暗号化共通鍵をポータルサーバ１２に返却するとともに、サービスサーバ１３に送信してサービスサーバ１３に対して公開鍵証明書を更新させる。この際、新公開鍵証明書に対応する秘密鍵は、ポータルサーバ１２には返却せず、鍵管理サーバ１１側で耐タンパ装置１１３内の秘密鍵保持部１１３１にて管理・保管する。

【００５０】

尚、ポータルサーバ１２は、個人情報ＤＢアクセス部１２１３によって、取得した新公開鍵証明書、及び新公開鍵証明書にて暗号化された暗号化個人情報を個人情報データベース（ＤＢ）１２３に保存し（ステップＳ１６）、鍵管理サーバ１１から返却された新公開鍵証明書に記載されている有効期限に合わせて、有効期限管理部１２１４にて管理する期

限を更新する（ステップＳ１７）。
【００５１】
このように、秘密鍵をＩＣカードなどのデバイスではなく、鍵管理サーバ１１にて管理し、ポータルサーバ１２側にて公開鍵証明書の有効期限を設定し 、ポータルサーバ１２が自ら有効期限を監視して、有効期限に達した契機で有効期限延長のために、旧公開鍵証明書で暗号化した共通鍵を鍵管理サーバ１１に送付し、鍵管理サーバ１１側でこの暗号化した共通鍵を復号し、新公開鍵証明書を生成するとともに再暗号化して、ポータルサーバ１２に返却するため、常に、利用者は、ポータルサーバ１２の暗号化された情報を閲覧することができるようになる。
【００５２】
〔システム動作：第２の処理シーケンス〕
図７は、本発明による一実施例の暗号化情報の有効期限延長システムにおける第２の処理シーケンスの動作フロー図である。情報端末１４は、ポータルサーバ１２に保存されている個人情報を閲覧するために、ポータルサーバ１２に閲覧要求を送信する。
【００５３】
ポータルサーバ１２は、個人情報ＤＢアクセス部１２１３によって、要求された個人情報に対応する暗号化共通鍵を個人情報データベース（ＤＢ）１２３から取得し、制御部１２１の制御によって、鍵管理サーバ１１に復号要求を送信する（ステップＳ２１）。
【００５４】
鍵管理サーバ１１は、鍵演算部１１１３によって、耐タンパ装置１１３内の秘密鍵保持部１１３１に格納されている秘密鍵を用いて復号し（ステップＳ２２）、制御部１１１の制御によって、通信制御部１１２を介してＳＳＬなどの安全な通信路を利用して、復号した共通鍵をポータルサーバ１２に返却する。
【００５５】
ポータルサーバ１２は、制御部１２１の制御によって、鍵管理サーバ１１から取得する復号された共通鍵で、サービスサーバ１３から送られていた暗号化個人情報を復号し、情報端末１４に表示させる画面を生成して、情報端末１４に対して表示可能にさせる。
【００５６】
このように、鍵管理サーバ１１に送付するのは共通鍵のみであるので、個人情報そのものは送付しないため、情報漏えいを抑止することができる。
【００５７】
上記の実施例では特定の例について説明したが、鍵管理サーバ１１は、ポータルサーバ１２内に設けることも可能である。また、有効期限の失効のみならず、暗号アルゴリズムの危殆化など、あらゆる公開鍵証明書の更新契機に本発明を適用することも可能である。
【００５８】
包括的には、本発明に係る暗号化情報の有効期限延長システム１は、ポータルサーバ１２を利用した暗号化情報の有効期限を自動的に延長する、暗号化情報の有効期限延長システムとして構成され、所定の情報端末１４の利用者に提示するための所定の個人情報に対して共通鍵で暗号化を施すと共に、該共通鍵を公開鍵証明書で暗号化を施して、暗号化個人情報及び暗号化共通鍵を生成するサービスサーバ１３と、ポータルサーバ１２からの要求に応じて、サービスサーバ１３が暗号化個人情報及び暗号化共通鍵を生成するのに用いられる公開鍵証明書を、該公開鍵証明書の鍵ペアを構成する秘密鍵とともに生成し、これらの公開鍵証明書及び秘密鍵を保持して管理する鍵管理サーバ１１と、サービスサーバ１３から暗号化個人情報及び暗号化共通鍵を取得し、当該暗号化個人情報及び暗号化共通鍵を生成するのに用いた公開鍵証明書の有効期限を設定して、暗号化個人情報及び暗号化共通鍵を個人情報データベース（ＤＢ）１２３内に保持するポータルサーバ１２とを備える。
【００５９】
本発明に係るポータルサーバ１２は、個人情報データベース（ＤＢ）１２３に保持している公開鍵証明書の再発行要求を行う有効期限を定期的に検査する手段と、該手段によっ

て個人情報データベース（ＤＢ）１２３に保持している公開鍵証明書が有効期限に達していると判断した場合に、鍵管理サーバ１１に対して、暗号化共通鍵を送付してこの公開鍵証明書の鍵ペアを構成する秘密鍵で復号させるとともに、新たな公開鍵証明書の生成と、該新たな公開鍵証明書による当該共通鍵の再度の暗号化を実行させて再度の暗号化共通鍵を生成させ、新たな公開鍵証明書をサービスサーバ１３に送付させるとともに、新たな公開鍵証明書及び再度の暗号化共通鍵を取得し、新たな公開鍵証明書の有効期限を設定して個人情報データベース（ＤＢ）１２３内に保持する手段とを備える。

【００６０】

また、ポータルサーバ１２は、情報端末１４から当該個人情報の閲覧要求を受け付ける手段と、個人情報を復号するために、暗号化共通鍵の復号要求を鍵管理サーバ１１に送信して、復号した共通鍵を前記鍵管理サーバから取得する手段と、該共通鍵を用いて、個人情報データベース（ＤＢ）１２３内に格納されている暗号化個人情報を復号して情報端末１４に提示する手段とを備える。

【００６１】

これらの本発明に係る鍵管理サーバ１１、ポータルサーバ１２、及びサービスサーバ１３の各々をコンピュータで構成した場合、各機能を実現する処理内容を記述したプログラムを、当該コンピュータの内部又は外部の記憶部に格納しておき、当該コンピュータの中央演算処理装置（ＣＰＵ）によってこのプログラムを読み出して実行させることで実現することができる。また、このようなプログラムは、例えばＤＶＤ又はＣＤ－ＲＯＭなどの可搬型記録媒体の販売、譲渡、貸与等により流通させることができるほか、そのようなプログラムを、例えばネットワーク上にあるサーバの記憶部に記憶しておき、ネットワークを介してサーバから他のコンピュータにそのプログラムを転送することにより、流通させることができる。また、そのようなプログラムを実行するコンピュータは、例えば、可搬型記録媒体に記録されたプログラム又はサーバから転送されたプログラムを、一旦、自己の記憶部に記憶することができる。また、このプログラムの別の実施態様として、コンピュータが可搬型記録媒体から直接プログラムを読み取り、そのプログラムに従った処理を実行することとしてもよく、更に、このコンピュータにサーバからプログラムが転送される度に、逐次、受け取ったプログラムに従った処理を実行することとしてもよい。従って、本発明は、前述した実施例に限定されるものではなく、その主旨を逸脱しない範囲において種々変更可能である。

【産業上の利用可能性】

【００６２】

本発明によれば、秘密鍵をＩＣカードなどのデバイスではなく、鍵管理サーバにて管理し、ポータルサーバ側にて公開鍵証明書の有効期限を設定し 、ポータルサーバが自ら有効期限を監視して、有効期限に達した契機で有効期限延長のために、旧公開鍵証明書で暗号化した共通鍵を鍵管理サーバに送付し、鍵管理サーバ側でこの暗号化した共通鍵を復号し、新公開鍵証明書を生成するとともに再暗号化して、ポータルサーバに返却するため、常に、利用者に対して情報の閲覧を可能とするので、暗号化情報の有効期限の管理を要する任意の用途に有用である。

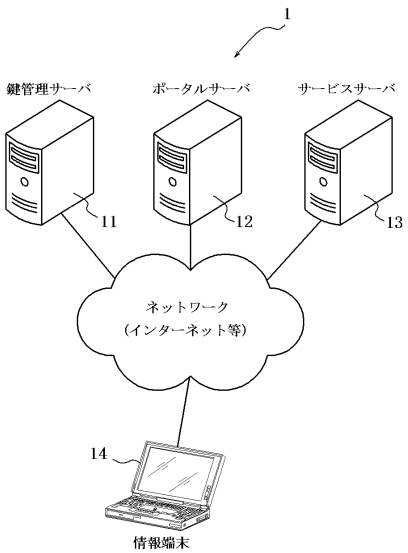
【符号の説明】

【００６３】

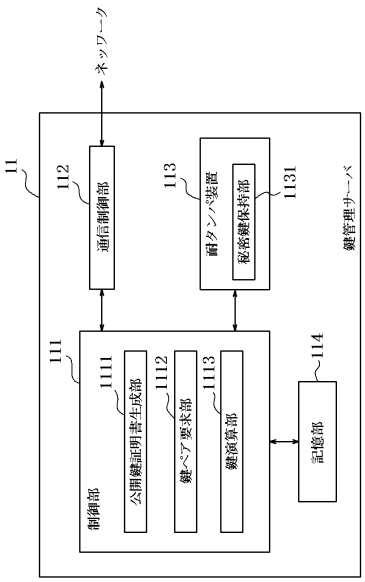
１　暗号化情報の有効期限延長システム
１１　鍵管理サーバ
１２　ポータルサーバ
１３　サービスサーバ
１４　情報端末
１１１　制御部
１１２　通信制御部
１１３　耐タンパ装置
１１４　記憶部

１２１　制御部
１２２　通信制御部
１２３　個人情報データベース
１２４　記憶部
１３１　制御部
１３２　通信制御部
１３３　記憶部
１１１１　公開鍵証明書生成部
１１１２　鍵ペア要求部
１１１３　鍵演算部
１２１１　公開鍵証明書生成要求部
１２１２　有効期限延長要求部
１２１３　個人情報ＤＢアクセス部
１２１４　有効期限管理部
１３１１　個人情報暗号化部
１３１２　共通鍵暗号化部

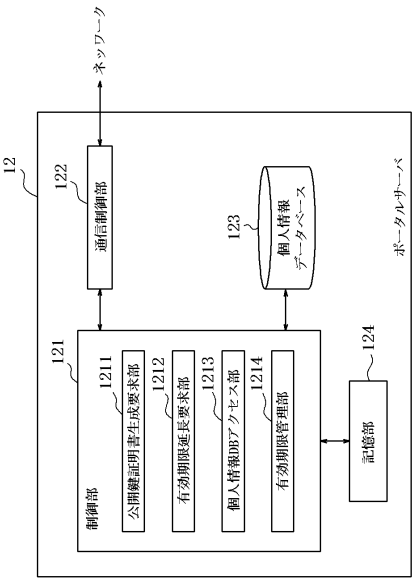
【図１】



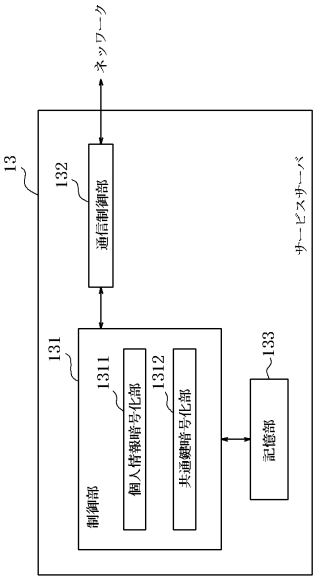
【図２】



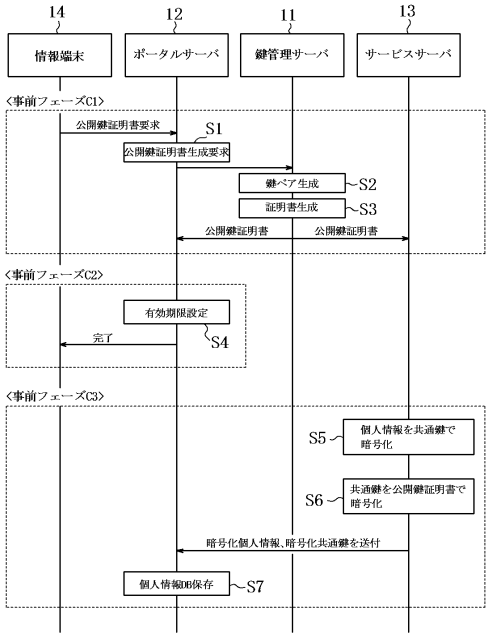
【図３】


ネットワーク
12
122
通信制御部
123
個人情報
データベース
ポータルサーバ
121
制御部
1211
公開鍵証明書生成要求部
1212
有効期限延長要求部
1213
個人情報DBアクセス部
1214
有効期限管理部
124
記憶部

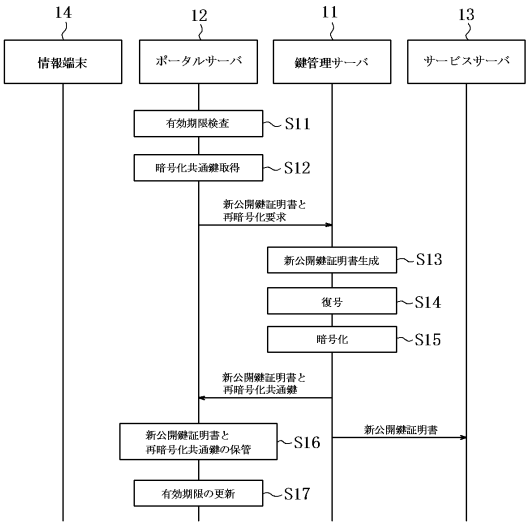
【図４】


ネットワーク
13
132
通信制御部
サービスサーバ
131
制御部
1311
個人情報暗号化部
1312
共通鍵暗号化部
133
記憶部

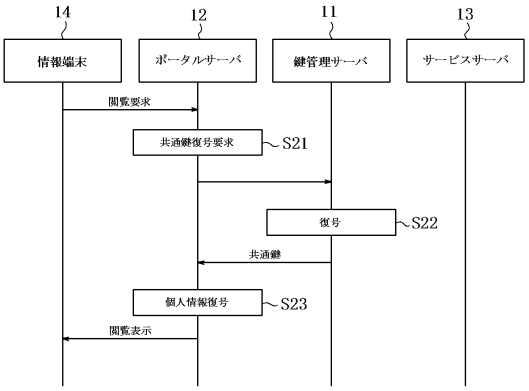
【図５】


14
情報端末
12
ポータルサーバ
11
鍵管理サーバ
13
サービスサーバ
<事前フェーズ(1)>
公開鍵証明書要求
S1
公開鍵証明書生成要求
鍵ペア生成
S2
証明書生成
S3
公開鍵証明書
公開鍵証明書
<事前フェーズ(2)>
有効期限設定
S4
完了
<事前フェーズ(3)>
S5
個人情報を共通鍵で暗号化
S6
共通鍵を公開鍵証明書で暗号化
暗号化個人情報、暗号化共通鍵を送付
個人情報DB保存
S7

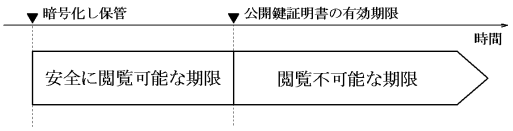
【図６】


14
情報端末
12
ポータルサーバ
11
鍵管理サーバ
13
サービスサーバ
有効期限検査
S11
暗号化共通鍵取得
S12
新公開鍵証明書と
再暗号化要求
新公開鍵証明書生成
S13
復号
S14
暗号化
S15
新公開鍵証明書と
再暗号化共通鍵
新公開鍵証明書と
再暗号化共通鍵の保管
S16
新公開鍵証明書
有効期限の更新
S17

【図７】


14
12
11
13
情報端末
ポータルサーバ
鍵管理サーバ
サービスサーバ
閲覧要求
共通鍵復号要求
S21
復号
S22
共通鍵
個人情報復号
S23
閲覧表示

【図８】


暗号化し保管
公開鍵証明書の有効期限
時間
安全に閲覧可能な期限
閲覧不可能な期限

フロントページの続き

(56)参考文献 特開２００８－２５９１３９（ＪＰ，Ａ）
特開２００７－０１３４８４（ＪＰ，Ａ）
特開２００６－１６６３５４（ＪＰ，Ａ）
特開２００６－０５９２２３（ＪＰ，Ａ）
特開２０１０－１６６２６５（ＪＰ，Ａ）
柏木　巧，川村　浩正，庭野　栄一，小尾　高史，谷内田　益義，李　中淳，本間　祐次，大山　永昭，“電子私書箱で実現するサービスの検討”，２００９年　暗号と情報セキュリティシンポジウム　ＳＣＩＳ２００９　［ＣＤ－ＲＯＭ］，日本，電子情報通信学会情報セキュリティ研究専門委員会，２００９年　1月２０日，３Ｆ４　プライバシー保護，３Ｆ４－３，ｐ．１－６
“電子私書箱（仮称）による社会保障サービス等のＩＴ化に関する検討会【報告書】”，日本，［オンライン］，２００８年　3月１７日，ｐ．ｉ－iii，１－４１，［平成２５年　8月１２日検索］、インターネット，ＵＲＬ，<http://www.kantei.go.jp/jp/singi/it2/epo-box/houkoku1.pdf>

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　　９／０８
Ｇ０６Ｆ　２１／１０