(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2012 年 8 月 23 日(23.08.2012)

WIPO | PCT

(10) 国際公開番号
WO 2012/111713 A1

(51) 国際特許分類:
H04L 9/08 (2006.01) *H04L 9/14* (2006.01)

(21) 国際出願番号: PCT/JP2012/053546

(22) 国際出願日: 2012 年 2 月 15 日(15.02.2012)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願 2011-032078 2011 年 2 月 17 日(17.02.2011) JP

(71) 出願人 (米国を除く全ての指定国について): 株式会社 東芝 **(KABUSHIKI KAISHA TOSHIBA)** [JP/JP]; 〒1058001 東京都港区芝浦一丁目１番１号 Tokyo (JP). 東芝ソリューション株式会社 **(TOSHIBA SOLUTIONS CORPORATION)** [JP/JP]; 〒1056691 東京都港区芝浦一丁目１番１号 Tokyo (JP).

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 吉田 琢也 **(YOSHIDA, Takuya)** [JP/JP]. 藤井 吉弘 **(FUJII, Yoshihiro)** [JP/JP].

(74) 代理人: 蔵田 昌俊, 外 **(KURATA, Masatoshi** et al.); 〒1050001 東京都港区虎ノ門１丁目１２番９号 鈴榮特許綜合事務所内 Tokyo (JP).

(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[続葉有]

(54) **Title**: KEY MANAGEMENT SYSTEM

(54) 発明の名称 : 鍵管理システム

[図1]

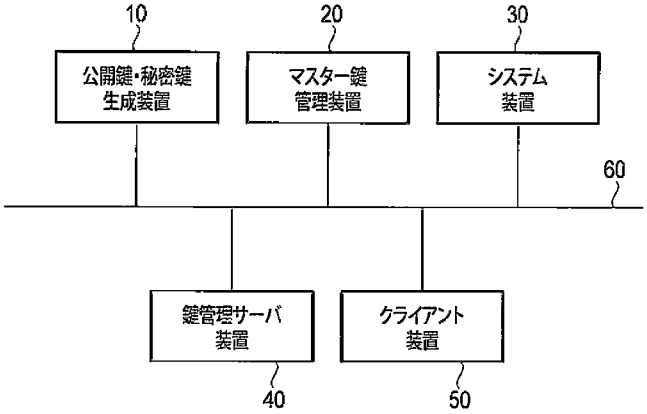


FIG. 1:
10 PUBLIC KEY / PRIVATE KEY GENERATION DEVICE
20 MASTER KEY MANAGEMENT DEVICE
30 SYSTEM DEVICE
40 KEY MANAGEMENT SERVER DEVICE
50 CLIENT DEVICE

(57) **Abstract**: A master key management device includes a re-encryption key generation means which, using a first private key and a third public key stored in a first storage means, generates a re-encryption key used to re-encrypt a second private key, which is encrypted with a first public key stored in a second storage means, into a second private key encrypted with the third public key. A key management server device includes: a receiving means which, in a state in which the master key management device and the key management server device are connected, receives from said master key management device a re-encryption key generated by the re-encryption key generation means; and a third storage means for storing the re-encryption key received by the receiving means. The connection between the master key management device and the key management server device is cut after the re-encryption key is stored in the third storage means.

(57) 要約: マスター鍵管理装置は、第１の記憶手段に記憶されている第１の秘密鍵および３の公開鍵を用いて、第２の記憶手段に記憶されている第１の公開鍵で暗号化された第２の秘密鍵を第３の公開鍵で暗号化された第２の秘密鍵に再暗号化するために用いられる再暗号化鍵を生成する再暗号化鍵生成手段を含む。鍵管理サーバ装置は、マスター鍵管理装置と鍵管理サーバ装置とが接続された状態で再暗号化鍵生成手段によって生成された再暗号化鍵を当該マスター鍵管理装置から受信する受信手段と、受信手段によって受信された再暗号化鍵を記憶する第３の記憶手段とを含む。マスター鍵管理装置と鍵管理サーバ装置との接続は、再暗号化鍵が第３の記憶手段に記憶された後に切断される。

WO 2012/111713 A1

添付公開書類:

— 国際調査報告（条約第 21 条(3)）

明　細　書

発明の名称 ： 鍵管理システム

技術分野

[0001] 本発明の実施形態は、暗号化または復号に用いられる鍵を管理する鍵管理システムに関する。

背景技術

[0002] 一般に、各種システム（装置）のサービスを利用する際に、例えば暗号化、復号および署名等のために鍵が必要な場合がある。従来、このような各種システムで利用される鍵は、それぞれのシステムで独立して管理される場合が多い。

[0003] これに対して近年では、各種システムで利用される鍵を１つの鍵管理サーバ装置（鍵管理装置）で集約して管理し、必要に応じて当該鍵を鍵管理サーバ装置から取得する手法が注目されており、そのような仕組みの製品開発または仕様策定が進められている。

[0004] この鍵管理サーバ装置によれば、当該鍵管理サーバ装置において管理されている鍵が例えばクライアント（装置）に配布され、当該クライアントは、当該鍵を用いることによってシステムのサービスを利用することができるようになる。

[0005] ここで、鍵管理サーバ装置を利用して鍵をクライアントに配布する仕組みにおける鍵管理について説明する。鍵管理サーバ装置は、クライアントからシステムで利用される鍵（例えば、秘密鍵）が要求された場合、例えば要求されたシステムで利用される秘密鍵（以下、システム秘密鍵と表記する）をクライアント向けに暗号化し、当該暗号化されたシステム秘密鍵を当該要求に対する応答に含めて当該クライアントに返す。なお、クライアント向けに暗号化する方法としては、例えば公開鍵暗号による暗号化または鍵共有プロトコルで生成した鍵を利用した共通鍵暗号による暗号化等の方法が考えられる。

[0006] このように鍵管理サーバ装置から暗号化されたシステム秘密鍵が返されると、クライアント側で当該暗号化されたシステム秘密鍵が復号される。これにより、クライアントは、復号されたシステム秘密鍵を用いてシステムのサービスを利用することができる。

[0007] ところで、上記したような近年の鍵管理サーバ装置に全ての鍵を集約する仕様においては、当該鍵管理サーバ装置が全てのシステム秘密鍵を管理することになるが、当該システム秘密鍵が漏洩した場合にはその影響は計り知れない。そのため、鍵管理サーバ装置においては、これまで以上に厳重な鍵管理が求められる。

[0008] その１つの方法として、鍵管理サーバ装置において、システム秘密鍵を例えば鍵管理サーバ装置の鍵（マスター鍵）で全て暗号化して管理することが考えられる。なお、このマスター鍵は、例えば共通鍵暗号における鍵（共通鍵）である。これにより、鍵管理サーバ装置において管理されているシステム秘密鍵が漏洩した場合であっても、当該システム秘密鍵は暗号化されているため、当該システム秘密鍵を保護することができる。

[0009] なお、この場合においてクライアントから鍵が要求されると、鍵管理サーバ装置は、暗号化して管理されているシステム秘密鍵を鍵管理サーバ装置のマスター鍵で一旦復号し、当該復号されたシステム秘密鍵を上記したようにクライアント向けに暗号化して当該クライアントに返す。クライアント側では、上記したように鍵管理サーバ装置から返された暗号化されたシステム秘密鍵が復号される。このようにすることで、より安全にシステム秘密鍵をクライアントに配布することができる。

先行技術文献

特許文献

[0010] 特許文献1：特開２００３－８７２３５号公報

非特許文献

[0011] 非特許文献1：Diffie-Hellman Key Agreement Method, ［Online］, RFC2631, ［平成２３年２月１０日検索］, インターネット＜http://www.ietf.org/r

fc/rfc2631.txt＞

発明の概要

発明が解決しようとする課題

[0012] 上記したようにシステム秘密鍵をクライアントに配布する処理（以下、鍵配布処理と表記する）の過程におけるデータ（例えば、システム秘密鍵およびマスター鍵等）の漏洩は問題となるため、その過程の処理およびデータは厳重に保護されなければならない。このため、上記したような鍵配布処理は、厳重に保護された環境下で行う必要がある。換言すれば、鍵配布処理は、セキュアではない環境下では行うことができない。

[0013] また、全ての鍵（システム秘密鍵等）を鍵管理サーバ装置に集約した場合には、これまで以上に厳重に保護すべき処理および領域（当該鍵を管理するための領域）が多くなるため、それに比例して鍵の管理コストが増大する。

[0014] 特に、鍵管理サーバ装置のマスター鍵が漏洩した場合には、当該鍵管理サーバ装置において管理されている鍵（システム秘密鍵等）が全て復号可能となるため、当該マスター鍵は、例えば秘密分散技術またはパスワードベース暗号化方式等を利用してより厳重に保護することが必要である。

[0015] しかしながら、そのようなマスター鍵の厳重な保護は鍵管理サーバ装置上で行わなければならないため、当該保護方法が複雑になればなるほど鍵管理サーバ装置の運用コストに影響することは明らかである。

[0016] そこで、本発明が解決しようとする課題は、厳重に管理された環境下でなくても、鍵を安全に管理することが可能な鍵管理システムを提供することにある。

課題を解決するための手段

[0017] 実施形態によれば、第１の秘密鍵を記憶する第１の記憶手段を有するマスター鍵管理装置と、前記第１の秘密鍵と対となる第１の公開鍵で暗号化された第２の秘密鍵を記憶する第２の記憶手段を有する鍵管理サーバ装置とを具備する鍵管理システムが提供される。

[0018] 前記マスター鍵管理装置は、前記第１の記憶手段に記憶されている第１の

秘密鍵および第３の公開鍵を用いて、前記第２の記憶手段に記憶されている前記第１の公開鍵で暗号化された第２の秘密鍵を、前記第３の公開鍵で暗号化された第２の秘密鍵に再暗号化するために用いられる再暗号化鍵を生成する再暗号化鍵生成手段を含む。

[0019] 前記鍵管理サーバ装置は、前記マスター鍵管理装置と前記鍵管理サーバ装置とが接続された状態で、前記生成された再暗号化鍵を当該マスター鍵管理装置から受信する受信手段と、前記受信された再暗号化鍵を記憶する第３の記憶手段とを含む。

[0020] 前記マスター鍵管理装置と前記鍵管理サーバ装置との接続は、前記再暗号化鍵が前記第３の記憶手段に記憶された後に切断される。

図面の簡単な説明

[0021] [図1]実施形態に係る鍵管理システムの構成を示すブロック図。

[図2]図１に示す公開鍵・秘密鍵生成装置１０の主として機能構成を示すブロック図。

[図3]図１に示すマスター鍵管理装置２０の主として機能構成を示すブロック図。

[図4]図１に示すシステム装置３０の主として機能構成を示すブロック図。

[図5]図１に示す鍵管理サーバ装置４０の主として機能構成を示すブロック図。

[図6]図１に示すクライアント装置５０の主として機能構成を示すブロック図。

[図7]本実施形態に係る鍵管理システムにおいて用いられる再暗号化技術について説明するための概念図。

[図8]本実施形態に係る鍵管理システムの処理手順を示すフローチャート。

[図9]鍵セットアップ処理の処理手順を示すシーケンスチャート。

[図10]システム秘密鍵セットアップ処理の処理手順を示すシーケンスチャート。

[図11]再暗号化鍵セットアップ処理の処理手順を示すシーケンスチャート。

[図12]鍵配布処理の処理手順を示すシーケンスチャート。

発明を実施するための形態

[0022] 以下、図面を参照して、実施形態について説明する。

[0023] 図１は、本実施形態に係る鍵管理システムの構成を示すブロック図である。鍵管理システムは、公開鍵・秘密鍵生成装置１０、マスター鍵管理装置２０、複数のシステム装置３０、鍵管理サーバ装置４０および複数のクライアント装置５０を備える。なお、図１において、システム装置３０およびクライアント装置５０は、便宜的に１つのみが示されている。

[0024] 本実施形態に係る鍵管理システムは、システム装置３０によって提供されるサービスを利用する際に必要な鍵（当該システム装置３０で利用される鍵）がクライアント装置５０に配布されるような場合において当該鍵を管理する機能を有する。

[0025] 図１に示すように、公開鍵・秘密鍵生成装置１０、マスター鍵管理装置２０、複数のシステム装置３０、鍵管理サーバ装置４０および複数のクライアント装置５０は、例えばネットワーク６０を介して接続されている。また、本実施形態に係る鍵管理システムは、後述するようにマスター鍵管理装置２０をネットワーク６０から切断可能なように構成されている。以下、これらの各装置について説明する。

[0026] なお、公開鍵・秘密鍵生成装置１０、マスター鍵管理装置２０、複数のシステム装置３０、鍵管理サーバ装置４０および複数のクライアント装置５０は、それぞれ装置の各機能を実現するためのハードウェア構成、またはハードウェアとソフトウェアとの組み合わせ構成として実現されている。ソフトウェアは、予め記憶媒体またはネットワークからインストールされ、各装置にその機能を実現させるためのプログラムからなる。

[0027] 図２は、図１に示す公開鍵・秘密鍵生成装置１０の主として機能構成を示すブロック図である。

[0028] 公開鍵・秘密鍵生成装置１０は、通信部１１、公開鍵・秘密鍵生成部１２、パラメータ記憶部１３、一時データ記憶部１４および制御部１５を含む。

[0029] 通信部１１は、ネットワーク６０を介して通信を行う機能部である。通信部１１は、マスター鍵管理装置２０および複数のクライアント装置５０からの鍵生成要求を受信する。なお、鍵生成要求は、各種データを暗号化するための公開鍵および当該公開鍵で暗号化されたデータを復号するための秘密鍵（当該公開鍵と対となる秘密鍵）の生成を要求するものである。

[0030] パラメータ記憶部１２には、公開鍵および秘密鍵を生成するためのパラメータ（鍵生成パラメータ）が予め格納されている。

[0031] 公開鍵・秘密鍵生成部１３は、通信部１１によって受信された鍵生成要求に応じて、公開鍵および秘密鍵（のペア）を生成する。このとき、公開鍵・秘密鍵生成部１３は、パラメータ記憶部１２に記憶されているパラメータを用いて公開鍵および秘密鍵を生成する。

[0032] 以下の説明において、マスター鍵管理装置２０からの鍵生成要求に応じて生成された公開鍵および秘密鍵を当該マスター鍵管理装置２０のマスター公開鍵およびマスター秘密鍵と称する。同様に、各クライアント装置５０からの鍵生成要求に応じて生成された公開鍵および秘密鍵を当該クライアント装置５０のクライアント公開鍵およびクライアント秘密鍵と称する。

[0033] なお、公開鍵・秘密鍵生成部１３によって生成されたマスター公開鍵およびマスター秘密鍵は、当該マスター鍵管理装置２０からの鍵生成要求に対する応答として、通信部１１によって当該マスター鍵管理装置２０に送信される。同様に、公開鍵・秘密鍵生成部１１によって生成されたクライアント公開鍵およびクライアント秘密鍵は、当該クライアント装置５０からの鍵生成要求に対する応答として、通信部１１によって当該クライアント装置５０に送信される。

[0034] 一時データ記憶部１４は、必要に応じて、例えば他装置から受信されたデータ等を一時的に記憶するための機能部である。

[0035] 制御部１５は、通信部１１および公開鍵・秘密鍵生成部１３の処理を含む公開鍵・秘密鍵生成装置１０における処理を制御するための機能部である。

[0036] 図３は、図１に示すマスター鍵管理装置２０の主として機能構成を示すブ

ロック図である。

[0037] マスター鍵管理装置２０は、通信部２１、マスター秘密鍵記憶部２２、一時データ記憶部２３、再暗号化鍵生成部２４および制御部２５を含む。

[0038] 通信部２１は、ネットワーク６０を介して通信を行う機能部である。通信部２１は、例えば公開鍵・秘密鍵生成装置１０（に含まれる通信部１１）によって送信されたマスター鍵管理装置２０のマスター公開鍵およびマスター秘密鍵（つまり、自身の公開鍵および秘密鍵）を受信する。また、通信部２１は、公開鍵要求をクライアント装置５０に対して送信し、当該公開鍵要求の応答として当該クライアント装置５０の公開鍵を受信する。

[0039] マスター秘密鍵記憶部２２には、通信部２１によって受信されたマスター鍵管理装置２０の秘密鍵であるマスター秘密鍵（第１の秘密鍵）が記憶される。なお、通信部２１によって受信されたマスター鍵管理装置２０の公開鍵であるマスター公開鍵（第１の公開鍵）は公開され、例えばマスター鍵管理装置２０において管理される。

[0040] 一時データ記憶部２３は、必要に応じて、例えば他装置から受信されたデータ等を一時的に記憶するための機能部である。一時データ記憶部２３には、例えば通信部２１によって受信されたクライアント装置５０のクライアント公開鍵が記憶される。

[0041] 再暗号化鍵生成部２４は、マスター秘密鍵記憶部２２に記憶されているマスター鍵管理装置２０のマスター秘密鍵および通信部２１によって受信されたクライアント装置５０のクライアント公開鍵（一時データ記憶部２３に記憶されたクライアント装置５０の公開鍵）を用いて再暗号化鍵を生成する。この再暗号化鍵は、マスター鍵管理装置２０の公開鍵で暗号化されたデータを、クライアント装置５０の公開鍵で暗号化されたデータに再暗号化（変換）するために用いられる鍵である。換言すれば、再暗号化鍵は、マスター鍵管理装置２０のマスター秘密鍵で復号できるデータを、クライアント装置５０のクライアント秘密鍵で復号できるデータに再暗号化するための鍵である。

[0042] なお、再暗号化鍵生成部２４によって生成された再暗号化鍵は、通信部２１によって鍵管理サーバ装置５０へ送信される。

[0043] 制御部２５は、通信部２１および再暗号化鍵生成部２４の処理を含むマスター鍵管理装置２０における処理を制御するための機能部である。

[0044] 図４は、図１に示すシステム装置３０の主として機能構成を示すブロック図である。なお、鍵管理システムを構成する複数のシステム装置３０は、それぞれ図４と同様の機能構成を有する。

[0045] システム装置３０は、通信部３１、システム秘密鍵記憶部３２、一時データ記憶部３３、システム秘密鍵暗号化部３４および制御部３５を含む。

[0046] 通信部３１は、ネットワーク６０を介して通信を行う機能部である。通信部３１は、例えばマスター鍵管理装置２０に対してマスター公開鍵要求を送信する。このマスター公開鍵要求は、マスター鍵管理装置２０のマスター公開鍵を要求するものである。通信部３１は、マスター鍵管理装置２０に対して送信されたマスター公開鍵要求に対する応答としてマスター鍵管理装置２０のマスター公開鍵をマスター鍵管理装置２０から受信する。

[0047] システム秘密鍵記憶部３２には、システム装置３０の秘密鍵であるシステム秘密鍵（つまり、自身の秘密鍵）が記憶されている。このシステム秘密鍵記憶部３２に記憶されているシステム秘密鍵は、システム装置３０によって提供されるサービスを利用する際に必要となる鍵である。このシステム秘密鍵は、公開鍵暗号に関する秘密鍵でも、共通鍵暗号に関する秘密鍵でもよく、それ以外の、サービスを利用する際に必要な機密データ（例えばパスワードなど）でもよい。

[0048] 一時データ記憶部３３は、必要に応じて、例えば他装置から受信されたデータ等を一時的に記憶するための機能部である。一時データ記憶部３３には、例えば通信部３１によって受信されたマスター鍵管理装置２０のマスター公開鍵が記憶される。

[0049] システム秘密鍵暗号化部３４は、通信部３１によって受信されたマスター鍵管理装置２０のマスター公開鍵（一時データ記憶部３３に記憶されたマス

ター鍵管理装置２０のマスター公開鍵）を用いて、システム秘密鍵記憶部３２に記憶されているシステム装置３０のシステム秘密鍵を暗号化する。なお、システム秘密鍵暗号化部３４によってマスター鍵管理装置２０のマスター公開鍵で暗号化されたシステム装置３０のシステム秘密鍵は、通信部３１によって鍵管理サーバ装置４０に送信される。

[0050] 制御部３５は、通信部３１およびシステム秘密鍵暗号化部３４の処理を含むシステム装置３０における処理を制御するための機能部である。

[0051] 図５は、図１に示す鍵管理サーバ装置４０の主として機能構成を示すブロック図である。

[0052] 鍵管理サーバ装置４０は、通信部４１、マスター向け暗号化システム秘密鍵記憶部４２、再暗号化鍵記憶部４３、再暗号化部４４および制御部４５を含む。

[0053] 通信部４１は、ネットワーク６０を介して通信を行う機能部である。通信部４１は、システム装置３０（に含まれる通信部３１）によって送信されたマスター鍵管理装置２０の公開鍵で暗号化された当該システム装置３０のシステム秘密鍵であるマスター向け暗号化システム秘密鍵を受信する。また、通信部４１は、マスター鍵管理装置２０（に含まれる通信部２１）によって送信された再暗号化鍵を受信する。

[0054] マスター鍵管理装置２０の公開鍵で暗号化されたシステム装置３０のシステム秘密鍵（第２の秘密鍵）は、マスター向け暗号化システム秘密鍵記憶部４２に記憶される。また、再暗号化鍵は、再暗号化鍵記憶部４３に記憶される。

[0055] 再暗号化部４４は、再暗号化鍵記憶部４３に記憶された再暗号化鍵を用いて、マスター向け暗号化システム秘密鍵記憶部４２に記憶されたマスター向け暗号化システム秘密鍵（つまり、マスター鍵管理装置２０の公開鍵で暗号化されたシステム装置３０の秘密鍵）を、クライアント装置５０のクライアント公開鍵（第３の公開鍵）で暗号化された当該システム装置３０のシステム秘密鍵に再暗号化したクライアント向け暗号化システム秘密鍵を生成する

。つまり、再暗号化部４４によって再暗号化されたシステム装置３０のシステム秘密鍵は、クライアント装置５０のクライアント秘密鍵を用いて復号することができる。

[0056] なお、再暗号化部４４によって再暗号化されたシステム装置３０のシステム秘密鍵は、通信部３１によってクライアント装置５０に送信される。

[0057] 制御部４５は、通信部４１および再暗号化部４４の処理を含む鍵管理サーバ装置４０における処理を制御するための機能部である。

[0058] 図６は、図１に示すクライアント装置５０の主として機能構成を示すブロック図である。

[0059] クライアント装置５０は、通信部５１、クライアント秘密鍵記憶部５２、一時データ記憶部５３、システム秘密鍵復号部５４および制御部５５を含む。

[0060] 通信部５１は、ネットワーク６０を介して通信を行う機能部である。通信部５１は、例えば公開鍵・秘密鍵生成装置１０（に含まれる通信部１１）によって送信されたクライアント装置３０のクライアント公開鍵およびクライアント秘密鍵（つまり、自身の公開鍵および秘密鍵）を受信する。

[0061] また、通信部５１は、鍵管理サーバ装置４０に対してクライアント向け暗号化システム秘密鍵要求を送信する。このクライアント向け暗号化システム秘密鍵要求は、クライアント装置５０（を利用するユーザ）が利用しようとするサービスを提供するシステム装置３０のシステム秘密鍵（当該サービスを利用する際に必要となる鍵）を要求するものである。通信部５１は、鍵管理サーバ装置４０に対して送信されたクライアント向け暗号化システム秘密鍵要求に対する応答として再暗号化されたシステム装置３０の秘密鍵であるクライアント向け暗号化システム秘密鍵を鍵管理サーバ装置４０から受信する。この再暗号化されたシステム装置３０の秘密鍵は、上記したようにクライアント装置５０のクライアント公開鍵（つまり、自身の公開鍵）で暗号化されたシステム装置３０のシステム秘密鍵である。

[0062] クライアント秘密鍵記憶部５２には、通信部５１によって受信されたクラ

イアント装置５０のクライアント秘密鍵（つまり、自身の秘密鍵）が記憶される。なお、通信部５１によって受信されたクライアント装置５０のクライアント公開鍵は公開され、当該クライアント装置５０において管理される。

[0063] 一時データ記憶部５３は、必要に応じて、例えば他装置から受信されたデータ等を一時的に記憶するための記憶部である。一時データ記憶部５３には、例えば通信部５１によって受信された再暗号化されたシステム装置３０のシステム秘密鍵が記憶される。

[0064] システム秘密鍵復号部５４は、クライアント秘密鍵記憶部５２に記憶されたクライアント装置５０のクライアント秘密鍵（第３の秘密鍵）を用いて、通信部５１によって受信された再暗号化されたシステム装置３０のシステム秘密鍵であるクライアント向け暗号化システム秘密鍵（一時データ記憶部５３に記憶された再暗号化されたシステム装置３０の秘密鍵）を復号する。なお、システム秘密鍵復号部５４によって復号されたシステム装置３０のシステム秘密鍵は、一時データ記憶部５３に記憶される。

[0065] クライアント装置５０は、システム秘密鍵復号部５４によって復号されたシステム装置３０のシステム秘密鍵（一時データ記憶部５３に記憶されたシステム装置３０のシステム秘密鍵）を用いて当該システム装置３０によって提供されるサービスを利用することができる。

[0066] 制御部５５は、通信部５１およびシステム秘密鍵復号部５４の処理を含むクライアント装置５０における処理を制御するための機能部である。

[0067] ここで、図７を参照して、本実施形態に係る鍵管理システムにおいて用いられるプロキシ再暗号化技術（Proxy Re-Encryption）の概念について説明する。

[0068] ここでは、便宜的に、機密データ１００を暗号化することによって保護しながら当該機密データ１００をユーザＡおよびＢが復号する場合について説明する。

[0069] まず、機密データ１００は、ユーザＡの公開鍵２０１を用いて暗号化される（ステップＳ１）。これによって、暗号化された機密データ１００（以下

、暗号化機密データ１０１と表記する）が得られる。ユーザＡの公開鍵は、ユーザＡに紐づけられた公開鍵であり、機密データ１００を暗号化するための鍵である。ユーザＡの公開鍵２０１は公開情報であり、当該ユーザＡの公開鍵２０１を利用して誰でもデータを暗号化することができる。

[0070] この暗号化機密データ１０１は、ユーザＡの秘密鍵２０２を用いて復号されることができる（ステップＳ２）。これによって、ユーザＡは、機密データ１００を得ることができる。ユーザＡの秘密鍵２０２は、ユーザＡに紐づけられたユーザＡの公開鍵２０１と対となる鍵であって、当該ユーザＡの公開鍵２０１で暗号化された機密データ１００（つまり、暗号化機密データ１０１）を復号するための鍵である。ユーザＡの秘密鍵は秘密情報であり、当該ユーザＡの秘密鍵２０２を知っている者のみが暗号化機密データ１０１を復号することができる。

[0071] ここで、再暗号化技術によれば、ユーザＡの秘密鍵２０２およびユーザＢの公開鍵３０１を用いて、再暗号化鍵４０１が生成される（ステップＳ３）。再暗号化鍵４０１は、暗号化機密データ１０１を暗号化機密データ１０２に再暗号化（変換）するための鍵である。暗号化機密データ１０２は、ユーザＢの公開鍵（ユーザＢに紐づけられた公開鍵）３０２で暗号化された機密データ１００である。なお、再暗号化鍵４０１の生成には、ユーザＡの秘密鍵を利用するため、ユーザＡの承認が必要である。

[0072] ここでは、ユーザＡの秘密鍵２０２およびユーザＢの公開鍵３０１を用いて再暗号化鍵４０１が生成されるものとして説明したが、これらの鍵２０２および３０１に加えてユーザＡの公開鍵２０１およびユーザＢの秘密鍵３０１を用いて再暗号化か鍵４０１が生成される場合もある。

[0073] 次に、暗号化機密データ１０１は、再暗号化鍵４０１を用いて再暗号化される（ステップＳ４）。これによって、暗号化機密データ１０１は、暗号化機密データ１０２に再暗号化される。なお、再暗号化鍵４０１を用いたとしても暗号化機密データ１０１を復号することはできない（つまり、機密データ１００を得ることはできない）。

[0074] 再暗号化された暗号化機密データ１０２（暗号化機密データ１０１を再暗号化することによって得られた暗号化機密データ１０２）は、ユーザＢの秘密鍵３０２を用いて復号されることができる（ステップＳ５）。これによって、ユーザＢは、機密データ１００を得ることができる。

[0075] 上記したように、再暗号化技術によれば、例えば暗号化機密データ１０１が復号されることなく、当該暗号化機密データ１０１（ユーザＡの公開鍵２０１で暗号化された機密データ１００）を暗号化機密データ１０２（ユーザＢの公開鍵３０１で暗号化された機密データ１００）に再暗号化することが可能となる。

[0076] ここで、上記したプロキシ再暗号化で利用する記号について説明する。

[0077] このプロキシ再暗号化は、公開鍵暗号系に関する概念であり、基本的なモデルは鍵生成、暗号化、復号、再暗号化鍵生成、再暗号化の５つの関数からなる。なお、鍵生成、暗号化、復号については通常の公開鍵暗号と同様である。

[0078] プロキシ再暗号化における鍵生成アルゴリズムＫｅｙＧｅｎは、セキュリティパラメータ1^kを入力とし、公開鍵ｐｋと秘密鍵ｓｋの組（ｐｋ，ｓｋ）を出力する。つまり、ＫｅｙＧｅｎ（1^k）→（ｐｋ，ｓｋ）である。

[0079] プロキシ再暗号化における暗号化アルゴリズムＥｎｃは、対象Ａ（例えば、ユーザＡ）の公開鍵pk_Aと機密データ（平文）ｍを入力とし、当該ユーザＡの公開鍵pk_Aで暗号化された機密データ（暗号化機密データ）C_Aを出力する。つまり、Ｅｎｃ（pk_A，ｍ）→C_Aである。

[0080] プロキシ再暗号化における復号アルゴリズムＤｅｃは、ユーザＡの秘密鍵sk_Aおよび暗号化機密データC_Aを入力とし、機密データｍを出力する。つまり、Ｄｅｃ（sk_A，C_A）→ｍである。

[0081] プロキシ再暗号化における再暗号化鍵生成アルゴリズムＲｅＫｅｙＧｅｎは、例えばユーザＡの公開鍵pk_A、ユーザＡの秘密鍵sk_A、ユーザＢの公開鍵pk_B、ユーザＢの秘密鍵sk_Bを入力とし、再暗号化鍵$rk_{A\to B}$を出力する。つまり、ＲｅＫｅｙＧｅｎ（pk_A，sk_A，pk_B，sk_B）→$rk_{A\to B}$

である。

[0082] プロシキ再暗号化における再暗号アルゴリズムＲｅＥｎｃは、再暗号化鍵$rk_{A\to B}$および暗号化機密データC_Aを入力とし、ユーザＢの公開鍵pk_Bで暗号化された機密データ（暗号化機密データ）C_Bを出力する。つまり、ＲｅＥｎｃ（$rk_{A\to B}$，C_A）→C_Bである。

[0083] 上記した鍵生成、暗号化、復号、再暗号化鍵生成および再暗号化が基本的なモデルであるが、実現方式によっては関数への入力が異なる場合、または上記以外の関数または鍵を含む場合がある。

[0084] 具体的には、再暗号化鍵生成アルゴリズムの入力にsk_Bを必要としないｎｏｎ－ｉｎｔｅｒａｃｔｉｖｅと呼ばれるモデル等がある。

[0085] 更に、再暗号化鍵$rk_{A\to B}$を用いて暗号化機密データC_Aから暗号機密データC_Bの再暗号化を行うことができる一方で、その逆の暗号化機密データC_Bから暗号化機密データC_Aの再暗号化を行うことができないｕｎｉｄｉｒｅｃｔｉｏｎａｌと呼ばれるモデル、および当該再暗号化鍵$rk_{A\to B}$を用いて暗号化機密データC_Aおよび暗号機密データC_Bを相互に再暗号化することができるｂｉｄｉｒｅｃｄｔｉｏｎａｌと呼ばれるモデルもある。なお、ｂｉｄｉｒｅｃｔｉｏｎａｌモデルにおいては、再暗号化鍵$rk_{A\to B}$を$rk_{A\Leftrightarrow B}$と表される場合がある。

[0086] 更に、公開鍵暗号の中でもＩＤベース暗号に基づく方式がある。この場合、マスター鍵生成のための関数Ｓｅｔｕｐが増え、鍵生成ＫｅｙＧｅｎの入力にマスター鍵およびＩＤが追加される。なお、ＩＤベース暗号において、公開鍵ｐｋはＩＤそのものである。

[0087] 以下、本実施形態に係る鍵管理システムの動作について説明する。鍵管理システムにおいては、複数のシステム装置３０のシステム秘密鍵が鍵管理サーバにおいて管理され、当該システム装置３０のシステム秘密鍵が当該システム装置３０によって提供されるサービスを利用しようとするクライアント装置５０に配布される。

[0088] 図８のフローチャートを参照して、本実施形態に係る鍵管理システムの処

理手順について説明する。本実施形態に係る鍵管理システムの処理は、大別すると、図８に示す４つの処理からなる。

[0089] 鍵管理システムにおいては、まず、鍵セットアップ処理が実行される（ステップＳ１１）。この鍵セットアップ処理では、鍵管理システムにおいて用いられるマスター鍵管理装置２０のマスター公開鍵およびマスター秘密鍵と各クライアント装置５０のクライアント公開鍵およびクライアント秘密鍵とがセットアップされる。

[0090] 次に、鍵管理システムにおいては、システム秘密鍵セットアップ処理が実行される（ステップＳ１２）。このシステム秘密鍵セットアップ処理では、各システム装置３０のシステム秘密鍵が鍵管理サーバ装置４０で管理するためにセットアップされる。

[0091] 更に、鍵管理システムにおいては、再暗号化鍵セットアップ処理が実行される（ステップＳ１３）。この再暗号化鍵セットアップ処理では、鍵管理システムにおいて用いられる再暗号化鍵がセットアップされる。

[0092] 上記したステップＳ１１～Ｓ１３の処理が実行されると、鍵管理システムにおいては、鍵配布処理が実行される（ステップＳ１４）。この鍵配布処理では、システム装置３０によって提供されるサービスを利用しようとするクライアント装置５０からの要求に応じて、当該システム装置３０のシステム秘密鍵が、クライアント装置５０のクライアント秘密鍵で復号できるように暗号化された状態で、当該クライアント装置５０に対して配布される。この鍵配布処理によって配布されたシステム装置３０のシステム秘密鍵を用いることによって、クライアント装置５０は、システム装置３０によって提供されるサービスを利用することが可能になる。

[0093] 次に、図９～図１２を用いて、上述した図８に示す各処理（鍵セットアップ処理、システム秘密鍵セットアップ処理、再暗号化鍵セットアップ処理、鍵配布処理）の詳細について説明する。なお、以下では説明を省略しているが、公開鍵・秘密鍵生成装置１０、マスター鍵管理装置２０、各システム装置３０、鍵管理サーバ装置４０および各クライアント装置５０（に含まれる

各部）の処理は、当該各装置に含まれる制御部による制御に応じて行われる。

[0094] まず、図９のシーケンスチャートを参照して、鍵セットアップ処理（図８に示すステップＳ１１の処理）の処理手順について説明する。鍵セットアップ処理は、公開鍵・秘密鍵生成装置１０、マスター鍵管理装置２０および各クライアント装置５０によって実行される。図９においては、便宜的に１つのクライアント装置５０についてのみ説明する。

[0095] マスター鍵管理装置２０に含まれる通信部２１は、公開鍵・秘密鍵生成装置１０に対してマスター鍵生成要求を送信する（ステップＳ２１）。これにより、マスター鍵管理装置２０のマスター公開鍵およびマスター秘密鍵（以下、マスター公開鍵Ｍｐｋおよびマスター秘密鍵Ｍｓｋと表記する）の生成が公開鍵・秘密鍵生成装置１０に対して要求される。

[0096] 公開鍵・秘密鍵生成装置１０に含まれる通信部１１は、マスター鍵管理装置２０（に含まれる通信部２１）から送信されたマスター鍵生成要求を受信する。

[0097] 通信部１１によってマスター鍵管理装置２０からのマスター鍵生成要求が受信されると、公開鍵・秘密鍵生成部１３は、マスター鍵管理装置２０のマスター公開鍵Ｍｐｋおよびマスター秘密鍵Ｍｓｋのペアを生成する（ステップＳ２２）。なお、公開鍵・秘密鍵生成部１３は、パラメータ記憶部１２に記憶されているパラメータを用いてマスター鍵管理装置２０のマスター公開鍵Ｍｐｋおよびマスター秘密鍵Ｍｓｋのペアを生成する。

[0098] 通信部１１は、受信されたマスター鍵管理装置２０からの鍵生成要求に対する応答（マスター鍵生成応答）をマスター鍵管理装置２０に送信する（ステップＳ２３）。なお、このマスター鍵生成応答には、公開鍵・秘密鍵生成部１３によって生成されたマスター鍵管理装置２０のマスター公開鍵Ｍｐｋおよびマスター秘密鍵Ｍｓｋが含まれる。

[0099] 公開鍵・秘密鍵生成装置１０（に含まれる通信部１１）によってマスター鍵生成応答がマスター鍵管理装置２０に対して送信されると、マスター鍵管

理装置２０に含まれる通信部２１は、当該マスター鍵生成応答を受信する。これにより、マスター鍵管理装置２０は、マスター鍵生成応答に含まれるマスター鍵管理装置２０のマスター公開鍵Ｍｐｋおよびマスター秘密鍵Ｍｓｋを取得する。

[0100] マスター鍵管理装置２０において取得されたマスター鍵管理装置２０のマスター秘密鍵Ｍｓｋは、マスター秘密鍵記憶部２２に記憶されて、適切に保管される（ステップＳ２４）。

[0101] 一方、マスター鍵管理装置２０において取得されたマスター鍵管理装置２０のマスター公開鍵Ｍｐｋは、適切な方法で公開される（ステップＳ２５）。

[0102] クライアント装置５０に含まれる通信部５１は、公開鍵・秘密鍵生成装置１０に対してクライアント鍵生成要求を送信する（ステップＳ２６）。これにより、クライアント装置５０のクライアント公開鍵およびクライアント秘密鍵（以下、クライアント公開鍵Ｃｐｋおよびクライアント秘密鍵Ｃｓｋと表記する）の生成が公開鍵・秘密鍵生成装置１０に対して要求される。

[0103] 公開鍵・秘密鍵生成装置１０に含まれる通信部１１は、クライアント装置５０（に含まれる通信部５１）から送信されたクライアント鍵生成要求を受信する。

[0104] 通信部１１によってクライアント装置５０からの鍵生成要求が受信されると、公開鍵・秘密鍵生成部１３は、当該クライアント装置５０のクライアント公開鍵Ｃｐｋおよびクライアント秘密鍵Ｃｓｋのペアを生成する（ステップＳ２７）。なお、公開鍵・秘密鍵生成部１３は、パラメータ記憶部１２に記憶されているパラメータを用いてクライアント装置５０のクライアント公開鍵Ｃｐｋおよびクライアント秘密鍵Ｃｓｋのペアを生成する。

[0105] 通信部１１は、受信されたクライアント装置５０からのクライアント鍵生成要求に対する応答（クライアント鍵生成応答）を当該クライアント装置５０に送信する（ステップＳ２８）。なお、この鍵生成応答には、公開鍵・秘密鍵生成部１３によって生成されたクライアント装置５０のクライアント公

開鍵Ｃｐｋおよびクライアント秘密鍵Ｃｓｋが含まれる。

[0106] 公開鍵・秘密鍵生成装置１０（に含まれる通信部１１）によってクライアント鍵生成応答がクライアント装置５０に対して送信されると、当該クライアント装置５０に含まれる通信部５１は、当該クライアント鍵生成応答を受信する。これにより、クライアント装置５０は、クライアント鍵生成応答に含まれる当該クライアント装置５０のクライアント公開鍵Ｃｐｋおよびクライアント秘密鍵Ｃｓｋを取得する。

[0107] クライアント装置５０において取得された当該クライアント装置５０のクライアント秘密鍵Ｃｓｋは、クライアント秘密鍵記憶部５２に記憶されて、適切に保管される（ステップＳ２９）。

[0108] 一方、クライアント装置５０において取得された当該クライアント装置５０のクライアント公開鍵Ｃｐｋは、適切な方法で公開される（ステップＳ３０）。

[0109] 上記したようにステップＳ２１～Ｓ３０の処理が実行されると、鍵セットアップ処理は終了される。

[0110] 上記したステップＳ２１およびＳ２６において送信されるマスター鍵生成要求およびクライアント鍵生成要求には、当該マスター鍵生成要求およびクライアント鍵生成要求を送信する装置（マスター鍵管理装置２０およびクライアント装置５０）をユニークに特定するためのＩＤ等が含まれていてもよいし、公開鍵・秘密鍵生成装置１０側でユニークなＩＤが割り振られても構わない。

[0111] また、ステップＳ２１およびＳ２６におけるマスター鍵生成要求およびクライアント鍵生成要求、およびステップＳ２３およびＳ２８におけるマスター鍵生成応答およびクライアント鍵生成応答においては、１つのパスだけではなく、例えば鍵共有を行うＴＬＳ　Ｐｒｏｔｏｃｏｌのように複数のメッセージをやり取りして鍵生成を行うような構成であっても構わない。なお、以下に説明する各装置間における各要求および応答においても同様である。

[0112] また、ステップＳ２３およびＳ２８において、マスター公開鍵Ｍｐｋおよ

びマスター秘密鍵Ｍｓｋを含むマスター鍵生成応答、およびクライアント公開鍵Ｃｐｋおよびクライアント秘密鍵Ｃｓｋを含むクライアント鍵生成応答が送信される際には、特にマスター秘密鍵Ｍｓｋおよびクライアント秘密鍵Ｃｓｋを保護する必要がある。これらの秘密鍵の保護を実現するために、例えば２者間（ここでは、公開鍵・秘密鍵生成装置１０およびマスター鍵管理装置２０間、公開鍵・秘密鍵生成装置１０およびクライアント装置５０間）で共通鍵を共有し、当該共通鍵を用いて当該秘密鍵を暗号化して送信するような構成であってもよい。なお、共通鍵とは、共通鍵暗号において用いられる鍵である。

[0113] また、ステップＳ２４およびＳ２９におけるマスター秘密鍵Ｍｓｋおよびクライアント秘密鍵Ｃｓｋの保管方法については明示しないが、例えば予め用意された鍵を用いて暗号化して保管する等であればよい。

[0114] また、ステップＳ２５およびＳ３０におけるマスター公開鍵Ｍｐｋおよびクライアント公開鍵Ｃｐｋの公開方法は、各装置に依存するものであり、例えば公開鍵を管理するサーバに登録する、または本実施形態に係る鍵管理システムの管理者等が管理する等であってもよい。つまり、本実施形態に係る鍵管理システムを構成する各装置が公開鍵を必要なときに取得できるような構成であればよい。なお、以下の説明では、便宜的に、マスター鍵管理装置２０のマスター公開鍵Ｍｐｋはマスター鍵管理装置２０において管理されているものとし、クライアント装置５０のクライアント公開鍵Ｃｐｋは当該クライアント装置５０において管理されているものとする。

[0115] なお、図９においてはステップＳ２１～Ｓ３０の順に処理が実行されるものとして説明したが、ステップＳ２１～Ｓ２５の処理とステップＳ２６～Ｓ３０の処理とは、順番が入れ替えられても構わない。また、ステップＳ２１～Ｓ２５の処理とステップＳ２６～Ｓ３０の処理とは、一連の処理でなくても構わない。例えばステップＳ２１～Ｓ２５の処理が実行され、後でステップＳ２６～Ｓ３０の処理が実行されるような構成であってもよい。

[0116] また、ここでは便宜的に１つのクライアント装置５０についてのみ説明し

たが、図９に示すステップＳ２６～Ｓ３０の処理は、クライアント装置５０の各々について実行される。つまり、鍵セットアップ処理においては、ステップＳ２６～Ｓ３０がクライアント装置５０毎に繰り返されても構わない。

[0117] 次に、図１０のシーケンスチャートを参照して、システム秘密鍵セットアップ処理（図８に示すステップＳ１２の処理）の処理手順について説明する。システム秘密鍵セットアップ処理は、マスター鍵管理装置２０、各システム装置３０および鍵管理サーバ装置４０によって実行される。図９においては、便宜的に１つのシステム装置３０についてのみ説明する。なお、システム装置３０に含まれるシステム秘密鍵記憶部３２には、当該システム装置３０のシステム秘密鍵（以下、システム秘密鍵Ｓｓｋと表記する）が記憶されている。

[0118] まず、システム装置３０に含まれる通信部３１は、マスター鍵管理装置２０に対してマスター公開鍵要求を送信する（ステップＳ４１）。これにより、マスター鍵管理装置２０のマスター公開鍵Ｍｐｋが当該マスター鍵管理装置２０に対して要求される。

[0119] マスター鍵管理装置２０に含まれる通信部２１は、システム装置３０（に含まれる通信部３１）から送信されたマスター公開鍵要求を受信する。

[0120] 通信部２１によってシステム装置３０からのマスター公開鍵要求が受信されると、マスター鍵管理装置２０において管理されているマスター鍵管理装置２０のマスター公開鍵Ｍｐｋが取得される。

[0121] 通信部２１は、受信されたシステム装置３０からのマスター公開鍵要求に対する応答（マスター公開鍵応答）を当該システム装置３０に送信する（ステップＳ４２）。なお、このマスター公開鍵応答には、マスター鍵管理装置２０のマスター公開鍵Ｍｐｋが含まれる。

[0122] マスター鍵管理装置２０（に含まれる通信部２１）によってマスター公開鍵応答がシステム装置３０に対して送信されると、当該システム装置３０に含まれる通信部３１は、当該マスター公開鍵応答を受信する。これにより、システム装置３０は、マスター公開鍵応答に含まれるマスター鍵管理装置２

０のマスター公開鍵Ｍｐｋを取得する。

[0123] 次に、システム秘密鍵暗号化部３４は、システム秘密鍵記憶部３２に記憶されているシステム装置３０のシステム秘密鍵Ｓｓｋを取得する（ステップＳ４３）。ここで、システム装置３０のシステム秘密鍵Ｓｓｋがシステム秘密鍵記憶部３２において例えば暗号化されて保管されているような場合には、適宜復号されることによってシステム装置３０のシステム秘密鍵Ｓｓｋが取得される。

[0124] システム秘密鍵暗号化部３４は、取得されたマスター鍵管理装置２０のマスター公開鍵Ｍｐｋを用いて、ステップＳ４３において取得されたシステム装置３０のシステム秘密鍵Ｓｓｋを暗号化する（ステップＳ４４）。

[0125] 通信部３１は、ステップＳ４４において暗号化されたシステム装置３０のシステム秘密鍵Ｓｓｋであるマスター向け暗号化システム秘密鍵を含む、マスター向け暗号化システム秘密鍵保管要求を、鍵管理サーバ装置４０に対して送信する（ステップＳ４５）。これにより、マスター向け暗号化システム秘密鍵の保管（管理）が鍵管理サーバ装置４０に対して要求される。

[0126] 鍵管理サーバ装置４０に含まれる通信部４１は、システム装置３０（に含まれる通信部３１）から送信されたマスター向け暗号化システム秘密鍵保管要求を受信する。通信部４１によって受信されたマスター向け暗号化システム秘密鍵保管要求に含まれるマスター向け暗号化システム秘密鍵は、当該マスター向け暗号化システム秘密鍵保管要求に応じてマスター向け暗号化システム秘密鍵記憶部４２に記憶されて、保管される（ステップＳ４６）。

[0127] なお、ステップＳ４６の処理が実行されると、マスター向け暗号化システム秘密鍵の保管処理が完了した旨を通知するため、通信部４１は、受信されたマスター向け暗号化システム秘密鍵保管要求に対する応答（マスター向け暗号化システム秘密鍵保管応答）をシステム装置３０に送信する（ステップＳ４７）。

[0128] 上記したようにステップＳ４１～ステップＳ４７の処理が実行されると、システム秘密鍵Ｓｓｋのセットアップ処理は終了される。

[0129] なお、上記したステップＳ４２においてマスター鍵管理装置２０のマスター公開鍵Ｍｐｋを含むマスター公開鍵応答が送信されるが、マスター公開鍵Ｍｐｋは公開される情報であるため、各種秘密鍵の場合ほど厳重にメッセージのやり取りを行う必要はない。なお、以下に説明する処理において各種公開鍵が送信される場合においても同様である。

[0130] また、図１０においては便宜的に１つのシステム装置３０についてのみ説明したが、図１０に示すシステム秘密鍵Ｓｓｋのセットアップ処理は、システム装置３０の各々について実行される。これにより、鍵管理サーバ装置４０に含まれるマスター向け暗号化システム秘密鍵記憶部４２には、マスター鍵管理装置２０のマスター公開鍵Ｍｐｋで暗号化されたシステム装置３０のシステム秘密鍵Ｓｓｋであるマスター向け暗号化システム秘密鍵が、システム装置３０毎に記憶される。つまり、鍵管理サーバ装置４０では、全てのシステム装置３０の秘密鍵Ｓｓｋが暗号化された状態で集約されて管理される。

[0131] 次に、図１１のシーケンスチャートを参照して、再暗号化鍵セットアップ処理（図８に示すステップＳ１３の処理）の処理手順について説明する。再暗号化鍵セットアップ処理は、マスター鍵管理装置２０、鍵管理サーバ装置４０および各クライアント装置５０によって実行される。図１１においては、便宜的に１つのクライアント装置５０についてのみ説明する。

[0132] まず、マスター鍵管理装置２０に含まれる通信部２１は、クライアント装置５０に対してクライアント公開鍵要求を送信する（ステップＳ５１）。これにより、クライアント装置５０のクライアント公開鍵Ｃｐｋが当該クライアント装置５０に対して要求される。

[0133] クライアント装置５０に含まれる通信部５１は、マスター鍵管理装置２０（に含まれる通信部２１）から送信されたクライアント公開鍵要求を受信する。

[0134] 通信部５１によってマスター鍵管理装置２０からのクライアント公開鍵要求が受信されると、クライアント端末５０において管理されているクライア

ント装置５０のクライアント公開鍵Ｃｐｋが取得される。

[0135] 通信部５１は、受信されたマスター鍵管理装置２０からのクライアント公開鍵要求に対する応答（クライアント公開鍵応答）を当該マスター鍵管理装置２０に送信する（ステップＳ５２）。なお、このクライアント公開鍵応答には、クライアント装置５０のクライアント公開鍵Ｃｐｋが含まれる。

[0136] クライアント装置５０（に含まれる通信部５１）によってクライアント公開鍵応答がマスター鍵管理装置２０に送信されると、当該マスター鍵管理装置２０に含まれる通信部２１は、当該クライアント公開鍵応答を受信する。これにより、マスター鍵管理装置２０は、クライアント公開鍵応答に含まれるクライアント装置５０のクライアント公開鍵Ｃｐｋを取得する。

[0137] 次に、再暗号化鍵生成部２４は、マスター秘密鍵記憶部２２に記憶されているマスター鍵管理装置２０のマスター秘密鍵Ｍｓｋを取得する（ステップＳ５３）。マスター鍵管理装置２０のマスター秘密鍵Ｍｓｋがマスター秘密鍵記憶部２２において例えば暗号化された保管されているような場合には、適宜復号されることによってマスター鍵管理装置２０のマスター秘密鍵Ｍｓｋが取得される。

[0138] 再暗号化鍵生成部２４は、取得されたクライアント装置５０のクライアント公開鍵Ｃｐｋおよびマスター鍵管理装置２０のマスター秘密鍵Ｍｓｋを用いて再暗号化鍵（以下、再暗号化鍵M→Ｃｒｅｅと表記する）を生成する（ステップＳ５４）。ここで生成された再暗号化鍵M→Ｃｒｅｅは、マスター鍵管理装置２０のマスター公開鍵Ｍｐｋで暗号化されたデータをクライアント装置５０のクライアント公開鍵Ｃｐｋで暗号化されたデータに再暗号化（変換）するための鍵、つまり、マスター鍵管理装置２０のマスター秘密鍵Ｍｓｋで復号可能なデータ（暗号化データ）をクライアント装置５０のクライアント秘密鍵Ｃｓｋで復号可能なデータ（暗号化データ）に再暗号化するための鍵である。

[0139] 通信部２１は、ステップＳ５４において生成された再暗号化鍵M→Ｃｒｅｅを含む再暗号化鍵保管要求を、鍵管理サーバ装置４０に対して送信する（

ステップＳ５６）。これにより、再暗号化鍵Ｍ→Ｃｒｅｅの保管（管理）が鍵管理サーバ装置４０に対して要求される。

[0140] 鍵管理サーバ装置４０に含まれる通信部４１は、マスター鍵管理装置２０（に含まれる通信部２１）から送信された再暗号化鍵保管要求を受信する。通信部４１によって受信された再暗号化鍵保管要求に含まれる再暗号化鍵Ｍ→Ｃｒｅｅは、当該再暗号化鍵保管要求に応じて再暗号化鍵記憶部４３に記憶されて、保管される（ステップＳ５６）。

[0141] なお、ステップＳ５６の処理が実行されると、再暗号化鍵Ｍ→Ｃｒｅｅの保管処理が完了した旨を通知するため、通信部４１は、受信された再暗号化鍵保管要求に対する応答（再暗号化鍵保管応答）をマスター鍵管理装置２０に送信する（ステップＳ５７）。

[0142] 上記したようにステップＳ５１～ステップＳ５７の処理が実行されると、再暗号化鍵セットアップ処理は終了される。

[0143] なお、上記したステップＳ５５において再暗号化鍵Ｍ→Ｃｒｅｅを含む再暗号化鍵保管要求が送信されるが、再暗号化鍵Ｍ→Ｃｒｅｅのみでは例えばシステム装置３０のシステム秘密鍵Ｓｓｋ等を得ることはできないため、上記した各種公開鍵の場合と同様に、各種秘密鍵の場合ほど厳重にメッセージのやり取りを行う必要はない。

[0144] また、図１１においては便宜的に１つのクライアント装置５０についてのみ説明したが、図１１に示すステップＳ５１～Ｓ５５の処理は、クライアント装置５０の各々について実行される。つまり、再暗号化鍵セットアップ処理においては、ステップＳ５１～Ｓ５５の処理がクライアント装置５０毎に繰り返されても構わない。これにより、鍵管理サーバ装置４０に含まれる再暗号化鍵記憶部４３には、クライアント装置５０毎の再暗号化鍵（クライアント装置５０の各々に対応する再暗号化鍵）Ｍ→Ｃｒｅｅが記憶される。

[0145] 次に、図１２に示すシーケンスチャートを参照して、鍵配布処理（図８に示すステップＳ１４の処理）の処理手順について説明する。鍵配布処理は、鍵管理サーバ装置４０およびシステム装置３０によって提供されるサービス

を利用しようとするクライアント装置５０によって実行される。以下、複数のクライアント装置５０のうちの鍵配布処理を実行するクライアント装置５０を対象クライアント装置５０と称し、複数のシステム装置３０のうちの当該対象クライアント装置５０がサービスを利用とするサービスを提供するシステム装置３０を対象システム装置３０と称する。

[0146] まず、対象クライアント装置５０に含まれる通信部５１は、鍵管理サーバ装置４０に対してクライアント向け暗号化システム秘密鍵要求を送信する（ステップＳ６１）。これにより、対象システム装置３０のシステム秘密鍵Ｓｓｋをクライアント装置５０のクライアント秘密鍵Ｃｓｋで復号できるように暗号化されたデータである、クライアント向け暗号化システム秘密鍵の取得が、鍵管理サーバ装置４０に対して要求される。

[0147] 鍵管理サーバ装置４０に含まれる通信部４１は、対象クライアント装置５０（に含まれる通信部５１）から送信されたクライアント向け暗号化システム秘密鍵要求を受信する。

[0148] 通信部４１によって対象クライアント装置５０からのクライアント向け暗号化システム秘密鍵要求が受信されると、再暗号化部４４は、マスター向け暗号化システム秘密鍵記憶部４２に記憶されている、暗号化された対象システム装置３０のシステム秘密鍵Ｓｓｋを当該クライアント向け暗号化システム秘密鍵要求に応じて取得する（ステップＳ６２）。なお、再暗号化部４４によってマスター向け暗号化システム秘密鍵記憶部４２から取得されたマスター向け暗号化システム秘密鍵は、前述したようにマスター鍵管理装置２０のマスター公開鍵Ｍｓｋで暗号化された対象システム装置３０のシステム秘密鍵Ｓｓｋである。

[0149] 再暗号化部４４は、再暗号化鍵記憶部４３に記憶されている再暗号化鍵Ｍ→Ｃｒｅｅを取得する（ステップＳ６３）。ここで再暗号化部４４によって取得される再暗号化鍵Ｍ→Ｃｒｅｅは、上記したクライアント向け暗号化システム秘密鍵要求の要求元である対象クライアント装置５０に対応する再暗号化鍵Ｍ→Ｃｒｅｅであって、マスター鍵管理装置２０のマスター公開鍵Ｍ

ｐｋで暗号化されたデータを当該クライアント装置５０のクライアント公開鍵Ｃｐｋで暗号化されたデータに再暗号化（変換）するための鍵である。

[0150] 次に、再暗号化部４４は、ステップＳ６３において取得された再暗号化鍵Ｍ→Ｃｒｅｅを用いて、ステップＳ６２において取得されたマスター向け暗号化システム秘密鍵（マスター鍵管理装置２０の公開鍵Ｍｐｋで暗号化された対象システム装置３０の秘密鍵）を再暗号化する（ステップＳ６４）。この場合、マスター鍵管理装置２０のマスター公開鍵Ｍｐｋで暗号化された対象システム装置３０のシステム秘密鍵Ｓｓｋは、クライアント装置５０のクライアント公開鍵Ｃｐｋで暗号化された対象システム装置３０のシステム秘密鍵Ｓｓｋ（つまり、クライアント装置５０のクライアント秘密鍵Ｃｓｋで復号可能なデータ）であるクライアント向け暗号化システム秘密鍵に再暗号化される。なお、マスター鍵管理装置２０のマスター公開鍵Ｍｐｋで暗号化された対象システム装置３０のシステム秘密鍵Ｓｓｋが再暗号化される際に、対象システム装置３０のシステム秘密鍵Ｓｓｋが復号されることはない。

[0151] 通信部４１は、受信されたクライアント向け暗号化システム秘密鍵要求に対する応答（クライアント向け暗号化システム秘密鍵応答）を、当該クライアント向け暗号化システム秘密鍵要求の要求元である対象クライアント装置５０に送信する（ステップＳ６５）。なお、このクライアント向け暗号化システム秘密鍵応答には、再暗号化部４４によって再暗号化されたクライアント向け暗号化システム秘密鍵が含まれる。

[0152] 鍵管理サーバ装置４０（に含まれる通信部４１）によってクライアント向け暗号化システム秘密鍵応答が対象クライアント装置５０に対して送信されると、対象クライアント装置５０に含まれる通信部５１は、当該クライアント向け暗号化システム秘密鍵応答を受信する。これにより、対象クライアント装置５０は、クライアント向け暗号化システム秘密鍵応答に含まれるクライアント向け暗号化システム秘密鍵を取得する。

[0153] 次に、システム秘密鍵復号部５４は、クライアント秘密鍵記憶部５２に記憶されている対象クライアント装置５０のクライアント秘密鍵Ｃｓｋを取得

する（ステップＳ６６）。ここで、対象クライアント装置５０のクライアント秘密鍵Ｃｓｋがクライアント秘密鍵記憶部５２において例えば暗号化された保管されているような場合には、適宜復号されることによって対象クライアント装置５０のクライアント秘密鍵Ｃｓｋが取得される。

[0154] システム秘密鍵復号部５４は、取得されたクライアント向け暗号化システム秘密鍵（対象クライアント装置５０の公開鍵Ｃｐｋで暗号化された対象システム装置３０の秘密鍵）を、対象クライアント装置５０のクライアント秘密鍵Ｃｓｋで復号する（ステップＳ６７）。

[0155] これにより、クライアント装置５０は、対象システム装置（つまり、利用しようとするサービスを提供するシステム装置）３０のシステム秘密鍵Ｓｓｋを取得することができる。クライアント装置５０では、取得された対象システム装置３０のシステム秘密鍵Ｓｓｋを用いて当該対象システム装置３０によって提供されるサービスを利用することができる。

[0156] なお、上記したステップＳ６５において再暗号化された対象システム装置３０のシステム秘密鍵Ｓｓｋを含むクライアント向け暗号化システム秘密鍵応答が送信されるが、当該対象システム装置３０のシステム秘密鍵Ｓｓｋは暗号化された状態であるため、それほど厳重にメッセージのやり取りを行う必要はない。

[0157] ここで、上記したように鍵配布処理は、鍵管理サーバ装置４０およびシステム装置３０のシステム秘密鍵Ｓｓｋを要求するクライアント装置５０（つまり、システム装置３０のシステム秘密鍵の配布先となるクライアント装置５０）によって実行される。つまり、鍵配布処理においては、マスター鍵管理装置２０は必要ない。

[0158] このため、本実施形態においては、鍵配布処理時（つまり、図８に示すステップＳ１１～Ｓ１３の各処理以外の時）にはマスター鍵管理装置２０をネットワー６０から切断されるものとする。より具体的には、マスター鍵管理装置２０において生成された再暗号化鍵Ｍ→Ｃｒｅｅが鍵管理サーバ装置４０の再暗号化鍵記憶部４３に記憶され、再暗号化鍵セットアップ処理が終了

されると、マスター鍵管理装置２０と他の各装置との接続が切断される。これにより、マスター鍵管理装置２０のマスター秘密鍵Ｍｓｋを管理するマスター鍵管理装置２０を完全に隔離することができるため、鍵管理サーバ装置４０で集約して管理されている各システム装置３０のシステム秘密鍵Ｓｓｋを復号可能なマスター鍵管理装置２０のマスター秘密鍵Ｍｓｋをより安全に管理することが可能となる。

[0159] 上記したように本実施形態においては、マスター鍵管理装置２０がマスター鍵管理装置２０のマスター秘密鍵Ｍｓｋおよびクライアント装置５０のクライアント公開鍵Ｃｐｋを用いて再暗号化鍵Ｍ→Ｃｒｅｅを生成し、鍵管理サーバ装置４０がマスター鍵管理装置２０において生成された再暗号化鍵Ｍ→Ｃｒｅｅを管理し、当該マスター鍵管理装置２０と鍵管理サーバ装置４０との接続がその後に切断される構成により、厳重に管理された環境下でなくても、配布される鍵を安全に管理することが可能となる。

[0160] 具体的には、上記したように鍵管理サーバ装置４０で集約して管理されているシステム装置３０のシステム秘密鍵Ｓｓｋを復号可能なマスター鍵管理装置２０のマスター秘密鍵Ｍｓｋを完全に隔離して管理できるため、当該マスター鍵管理装置２０のマスター秘密鍵Ｍｓｋの漏洩を防止することができる。

[0161] また、本実施形態においては、鍵管理サーバ装置４０がシステム装置３０のシステム秘密鍵Ｓｓｋを再暗号化し、クライアント装置５０が当該再暗号化されたシステム装置３０のシステム秘密鍵Ｓｓｋを当該クライアント装置５０のクライアント秘密鍵Ｃｓｋで復号する構成により、各システム装置３０のシステム秘密鍵Ｓｓｋを各クライアント装置５０に配布する処理（鍵配布処理）の過程において一度もシステム装置３０のシステム秘密鍵Ｓｓｋが生のデータとして現れることがないため、鍵管理サーバ装置４０自体を厳重に保護する必要がなく、それほどセキュアではない環境下においても安全に鍵配布処理を行うことができる。

[0162] また、本実施形態においては、再暗号化鍵Ｍ→Ｃｒｅｅの生成を各クライ

アント装置５０からの要求毎に行う必要がなく、当該要求の前に（つまり、鍵配布処理の前の再暗号化鍵セットアップ処理で）作成しておけばよいため、上記したようにマスター鍵管理装置２０と鍵管理サーバ装置４０とが常にオンラインで接続されている必要がない。これにより、本実施形態においては、特別に守るべきデータ（ここでは、マスター鍵管理装置２０のマスター秘密鍵Ｍｓｋ）を管理しているマスター鍵管理装置２０のみを一般にはアクセスできないような高セキュリティ環境に置くというような構成とすることが可能となる。

[0163] また、本実施形態においては、上記したように鍵配布処理を行う鍵管理サーバ装置４０を厳重に保護する必要がないため、当該鍵管理サーバ装置４０の管理コストを減少させ、かつ、鍵管理サーバ装置の構成を見直すことによるコストを減少させることができる。

[0164] 更に、本実施形態においては、上記したように鍵配布処理の過程で例えば鍵管理サーバ装置４０においてシステム装置３０のシステム秘密鍵Ｓｓｋが復号されることがない（つまり、元の鍵データに戻ることはない）ため、例えば鍵配布処理における鍵管理サーバ装置４０の管理者等に対する情報漏洩についても防止することが可能となる。

[0165] 以上説明したように本実施形態においては、鍵管理システムにおいて処理を分割することによって、安全性が高く、なおかつ、自由度の高い柔軟な鍵管理が可能となる。

[0166] なお、本実施形態においては、システム装置３０およびクライアント装置５０を備えるものとして説明したが、一方（例えば、クライアント装置５０）のみが備えられる構成であっても構わない。具体的には、例えばクライアント装置５０のクライアント秘密鍵Ｃｓｋが鍵管理サーバ装置４０で管理され、当該管理されているクライアント装置５０のクライアント秘密鍵Ｃｓｋが各クライアント装置５０の要求に応じて配布されるような構成であっても構わない。

[0167] また、ステップＳ１２のシステムセットアップ処理の実行時以外には、シ

ステム装置３０をネットワーク６０から切り離しておいてもよい。

[0168] また、システム装置３０がシステム秘密鍵記憶部３２の代わりにシステム秘密鍵Ｓｓｋを生成するためのシステム秘密鍵生成部を持つような構成とし、ステップＳ４３のシステム秘密鍵を取得する処理の代わりに、システム秘密鍵生成部でシステム秘密鍵Ｓｓｋを生成するようにしてもよい。

[0169] また、プロキシ再暗号化方式として、ｎｏｎ－ｉｎｔｅｒａｃｔｉｖｅではないもの、ｂｉｄｉｒｅｃｔｉｏｎａｌなものや、ＩＤベースのものなどを利用してもよい。

[0170] また、本実施形態においては公開鍵・秘密鍵生成装置１０を備えるものとして説明したが、当該公開鍵・秘密鍵生成装置１０を備えず、例えばマスター鍵管理装置２０の内部でマスター鍵管理装置２０のマスター公開鍵Ｍｐｋおよびマスター秘密鍵Ｍｓｋが生成され、各クライアント装置５０の内部で当該クライアント装置５０のクライアント公開鍵Ｃｐｋおよびクライアント秘密鍵Ｃｓｋが生成されるような構成であってもよい。

[0171] また、本願発明は、上記実施形態そのままに限定されるものではなく、実施段階ではその要旨を逸脱しない範囲で構成要素を変形して具体化できる。また、上記実施形態に開示されている複数の構成要素の適宜な組合せにより種々の発明を形成できる。例えば、実施形態に示される全構成要素から幾つかの構成要素を削除してもよい。更に、異なる実施形態に亘る構成要素を適宜組合せてもよい。

符号の説明

[0172] １０…公開鍵・秘密鍵生成装置、１１…通信部、１２…パラメータ記憶部、１３…公開鍵・秘密鍵生成部、１４…一時データ記憶部、１５…制御部、２０…マスター鍵管理装置、２１…通信部、２２…マスター秘密鍵記憶部（第１の記憶手段）、２３…一時データ記憶部、２４…再暗号化鍵生成部、２５…制御部、３０…システム装置、３１…通信部、３２…システム秘密鍵記憶部、３３…一時データ記憶部、３４…システム秘密鍵暗号化部、３５…制御部、４０…鍵管理サーバ装置、４１…通信部、４２…マスター向け暗号化

システム秘密鍵記憶部（第２の記憶手段）、４３…再暗号化鍵記憶部（第３の記憶手段）、４４…再暗号化部、４５…制御部、５０…クライアント装置、５１…通信部、５２…クライアント秘密鍵記憶部（第４の記憶手段）、５３…一時データ記憶部、５４…システム秘密鍵復号部、５５…制御部。

請求の範囲

［請求項1］ 第１の秘密鍵を記憶する第１の記憶手段を有するマスター鍵管理装置と、前記第１の秘密鍵と対となる第１の公開鍵で暗号化された第２の秘密鍵を記憶する第２の記憶手段を有する鍵管理サーバ装置とを具備し、

前記マスター鍵管理装置は、

前記第１の記憶手段に記憶されている第１の秘密鍵および第３の公開鍵を用いて、前記第２の記憶手段に記憶されている前記第１の公開鍵で暗号化された第２の秘密鍵を、前記第３の公開鍵で暗号化された第２の秘密鍵に再暗号化するために用いられる再暗号化鍵を生成する再暗号化鍵生成手段を含み、

前記鍵管理サーバ装置は、

前記マスター鍵管理装置と前記鍵管理サーバ装置とが接続された状態で、前記生成された再暗号化鍵を当該マスター鍵管理装置から受信する受信手段と、

前記受信された再暗号化鍵を記憶する第３の記憶手段と

を含み、

前記マスター鍵管理装置と前記鍵管理サーバ装置との接続は、前記再暗号化鍵が前記第３の記憶手段に記憶された後に切断される

ことを特徴とする鍵管理システム。

［請求項2］ 前記第３の公開鍵と対となる第３の秘密鍵を記憶する第４の記憶手段を有するクライアント装置を更に具備し、

前記鍵管理サーバ装置は、

前記第３の記憶手段に記憶された再暗号化鍵を用いて、前記第２の記憶手段に記憶されている前記第１の公開鍵で暗号化された第２の秘密鍵を、前記第３の公開鍵で暗号化された第２の秘密鍵に再暗号化する再暗号化手段を更に含み、

前記クライアント装置は、

前記再暗号化された第２の秘密鍵を、前記第４の記憶手段に記憶されている第３の秘密鍵を用いて復号する復号手段を含む

ことを特徴とする請求項１記載の鍵管理システム。

［請求項3］ 前記第１の秘密鍵および前記第１の公開鍵と、前記第３の秘密鍵および前記第３の公開鍵を生成する鍵生成装置を更に具備し、

前記第１の記憶手段は、前記鍵生成装置によって生成された第１の秘密鍵を記憶し、

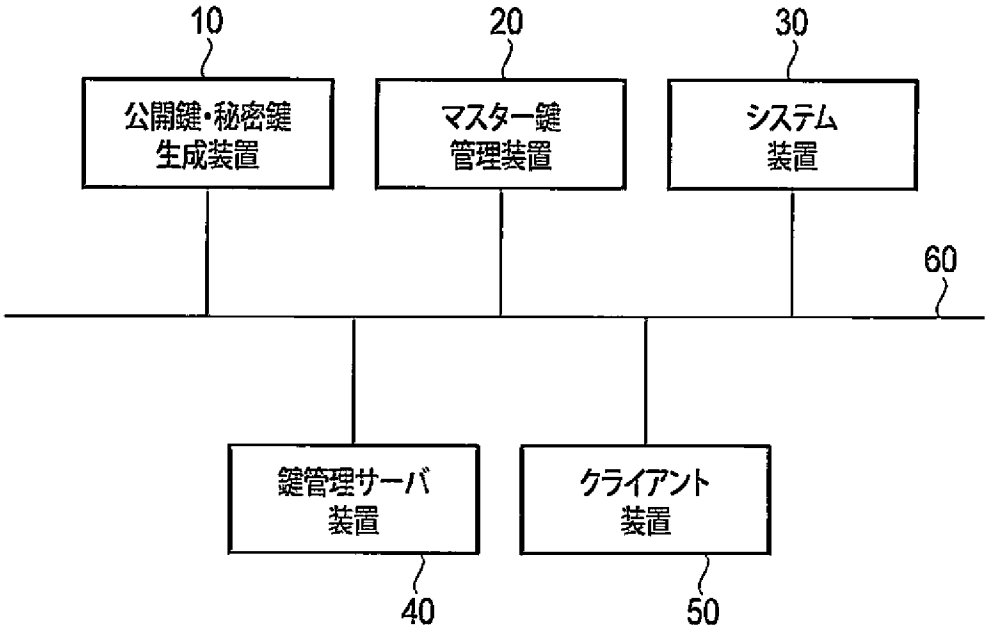
前記第２の記憶手段は、前記鍵生成装置によって生成された第１の公開鍵で暗号化された第２の秘密鍵を記憶し、

前記再暗号化鍵生成手段は、前記鍵生成装置によって生成された第３の公開鍵を用いて前記再暗号化鍵を生成し、

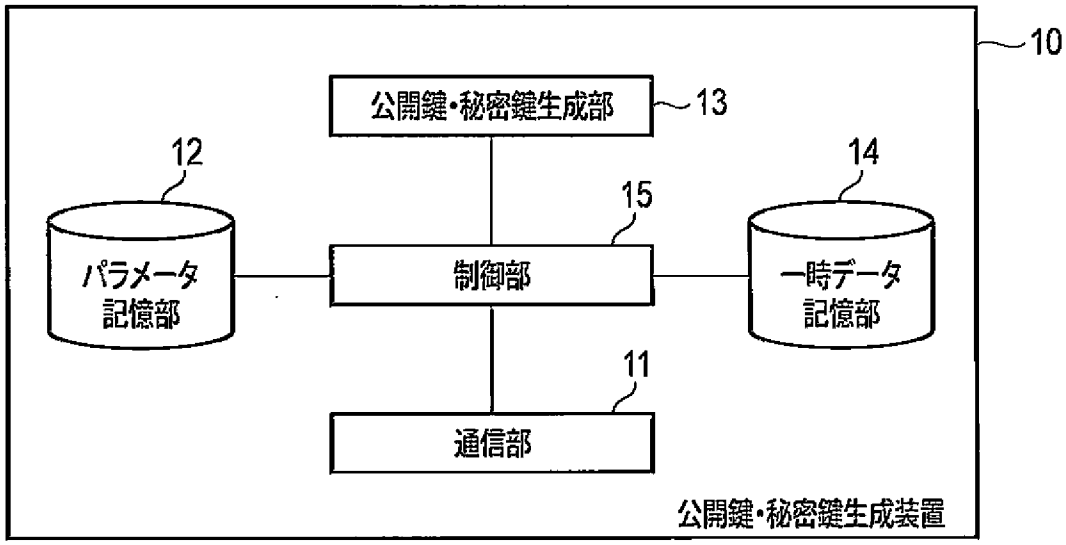
前記第４の記憶手段は、前記鍵生成装置によって生成された第３の秘密鍵を記憶する

ことを特徴とする請求項２記載の鍵管理システム。

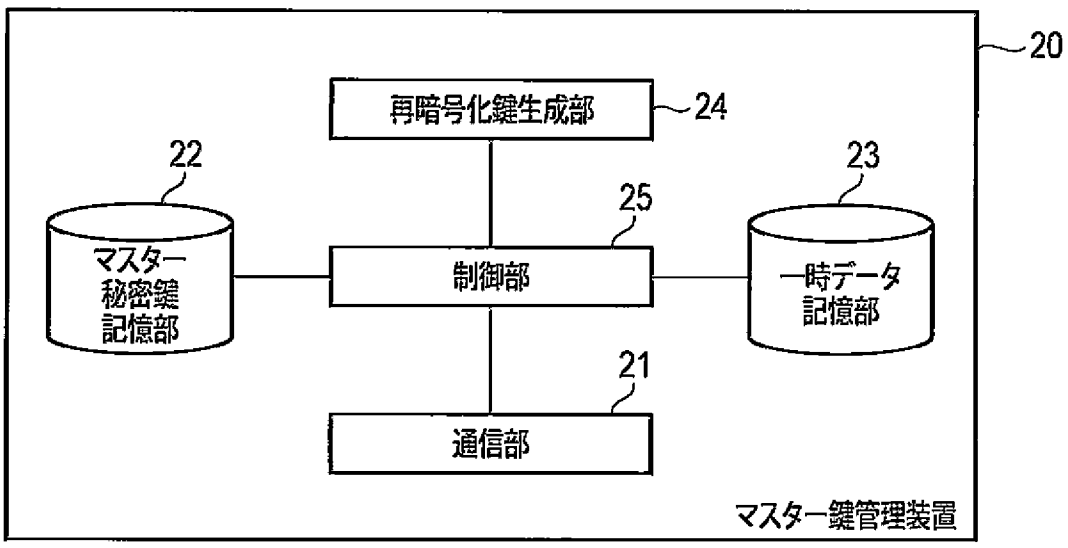
[図1]


10
20
30
公開鍵・秘密鍵
生成装置
マスター鍵
管理装置
システム
装置
60
鍵管理サーバ
装置
クライアント
装置
40
50

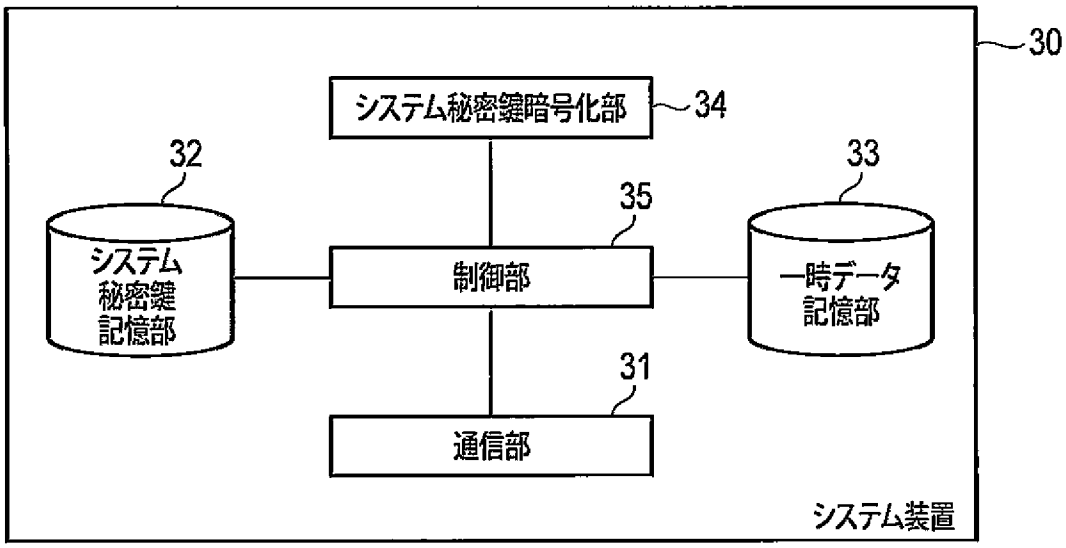
[図2]


10
公開鍵・秘密鍵生成部
13
12
14
15
パラメータ
記憶部
制御部
一時データ
記憶部
11
通信部
公開鍵・秘密鍵生成装置

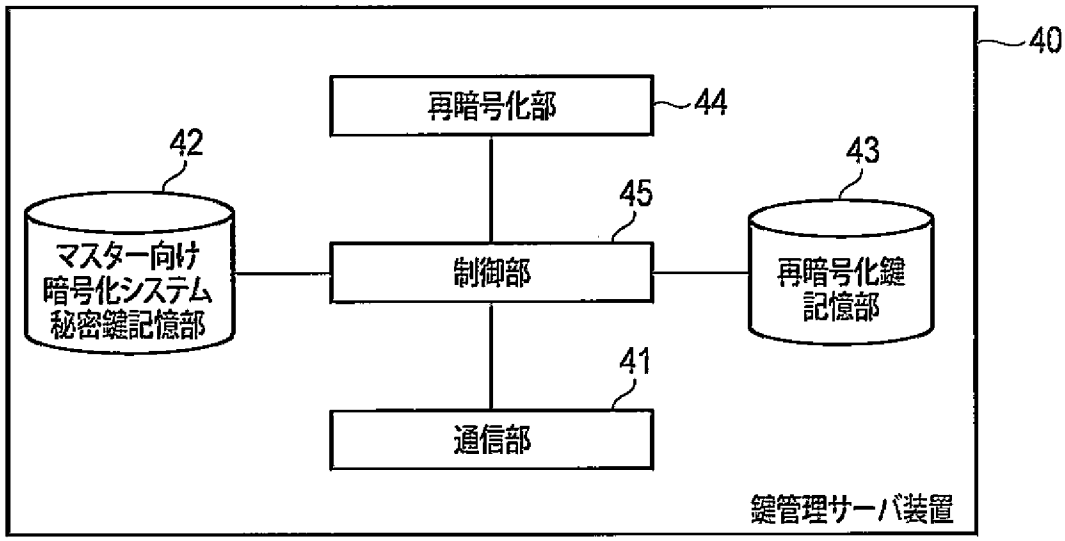
[図3]


20
再暗号化鍵生成部
24
22
23
25
マスター
秘密鍵
記憶部
制御部
一時データ
記憶部
21
通信部
マスター鍵管理装置

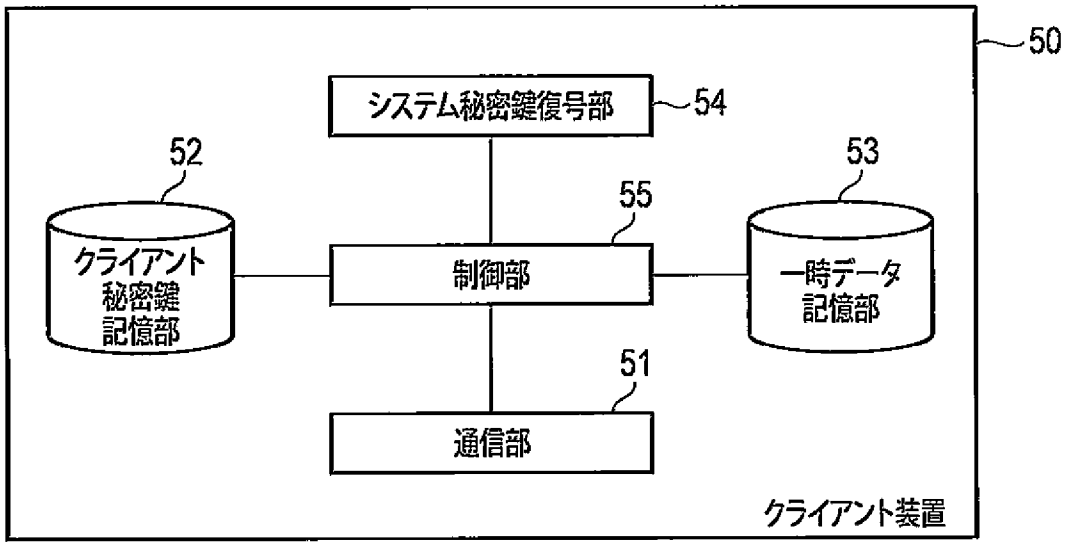
[図4]


30
システム秘密鍵暗号化部
34
32
33
35
システム
秘密鍵
記憶部
制御部
一時データ
記憶部
31
通信部
システム装置

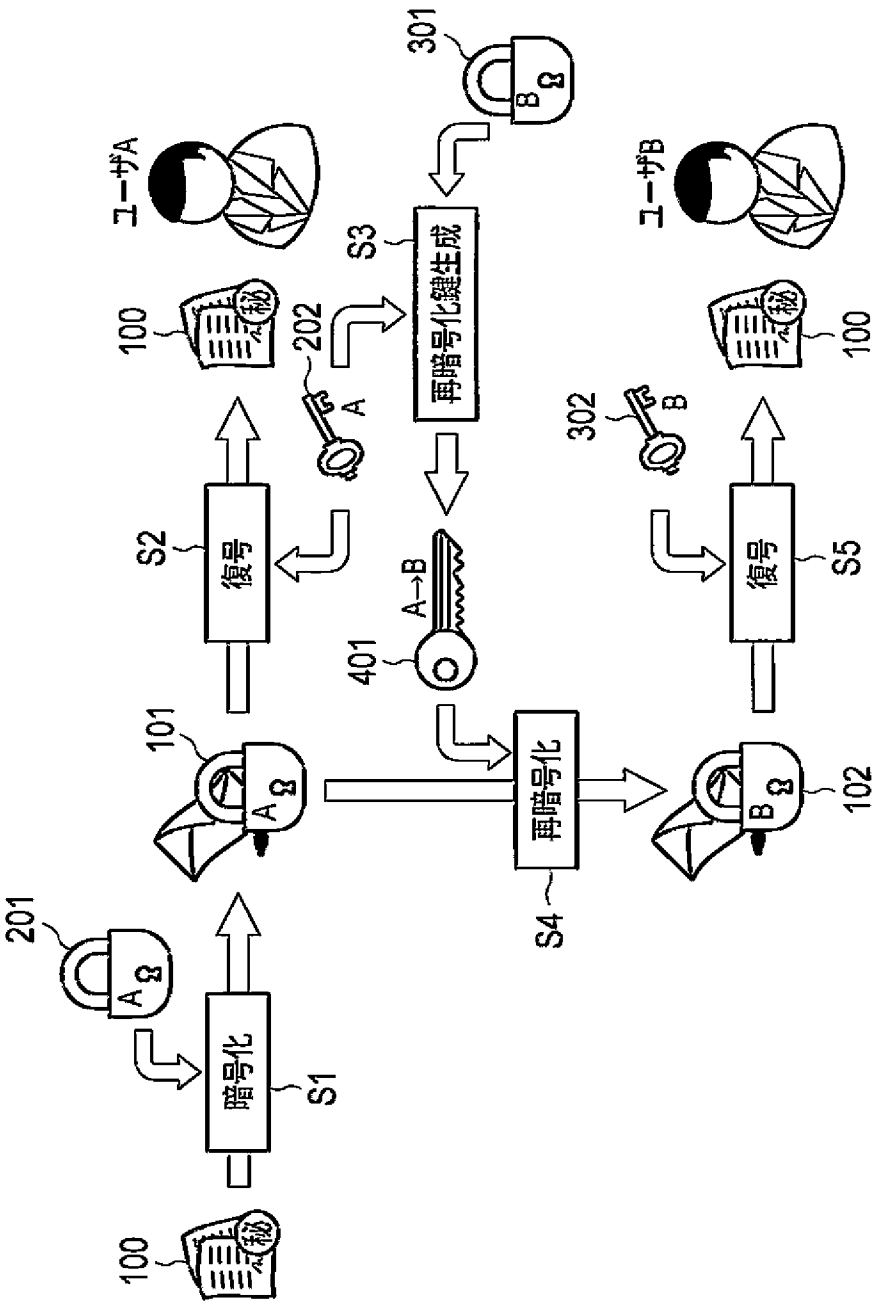
[図5]


40
再暗号化部
44
42
43
45
マスター向け
暗号化システム
秘密鍵記憶部
制御部
再暗号化鍵
記憶部
41
通信部
鍵管理サーバ装置

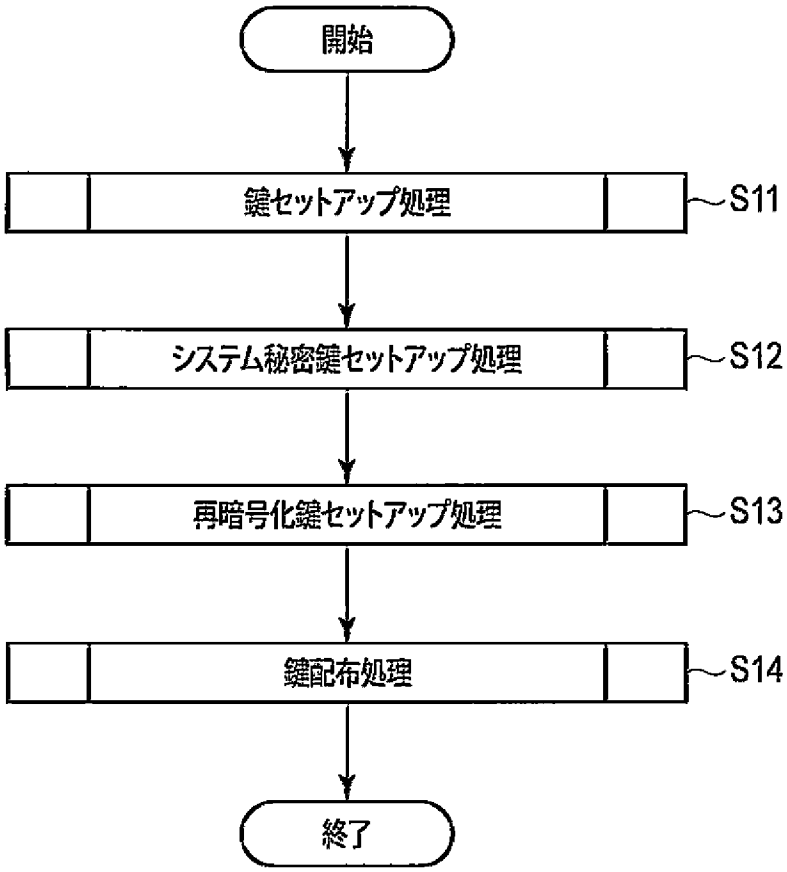
[図6]


50
システム秘密鍵復号部
54
52
53
55
クライアント
秘密鍵
記憶部
制御部
一時データ
記憶部
51
通信部
クライアント装置

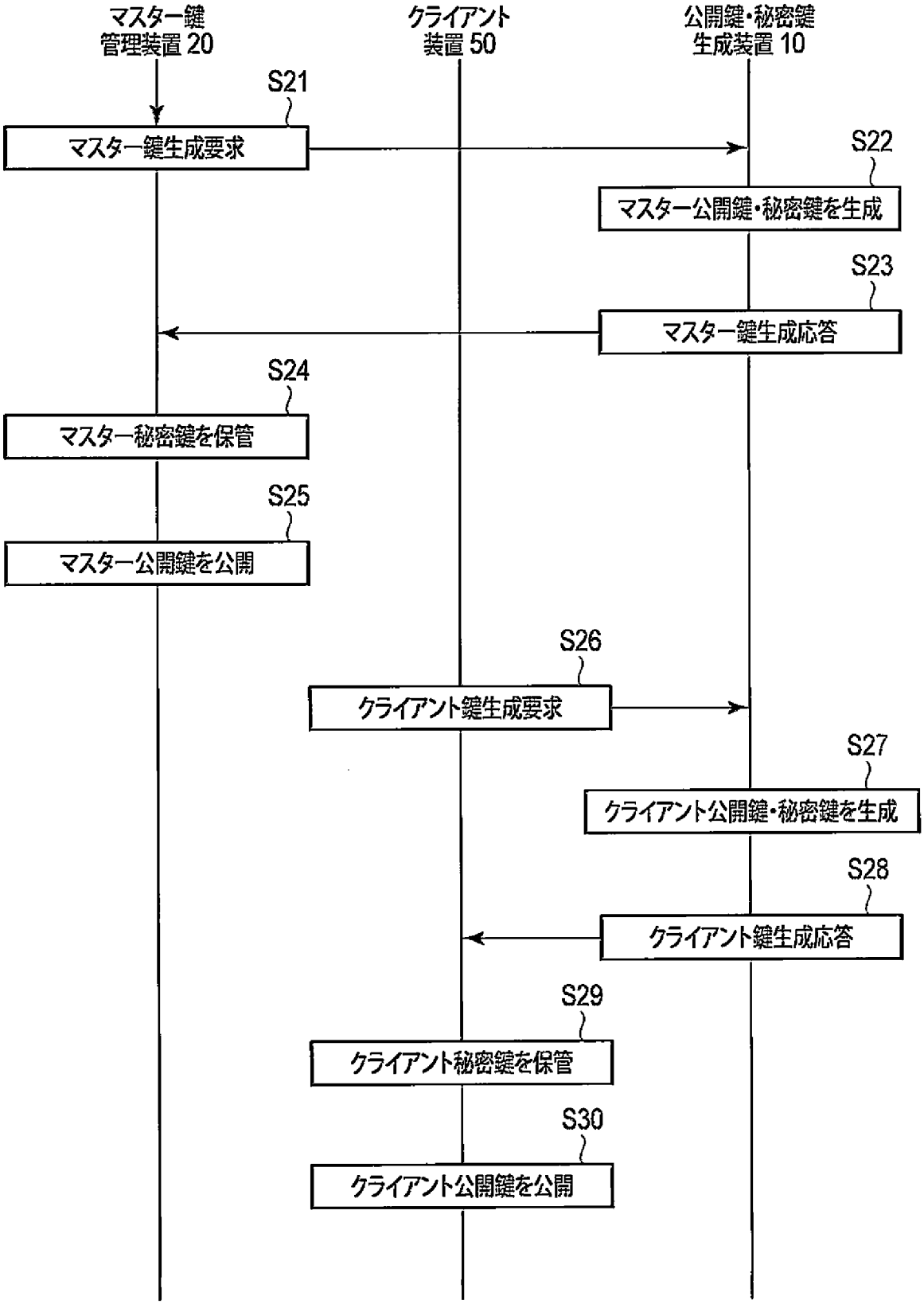
[図7]


301
B
ユーザA
ユーザB
S3
再暗号化鍵生成
100
秘
202
A
302
B
S2
復号
S5
復号
A→B
401
101
A
再暗号化
102
B
S4
201
A
暗号化
S1
100
秘

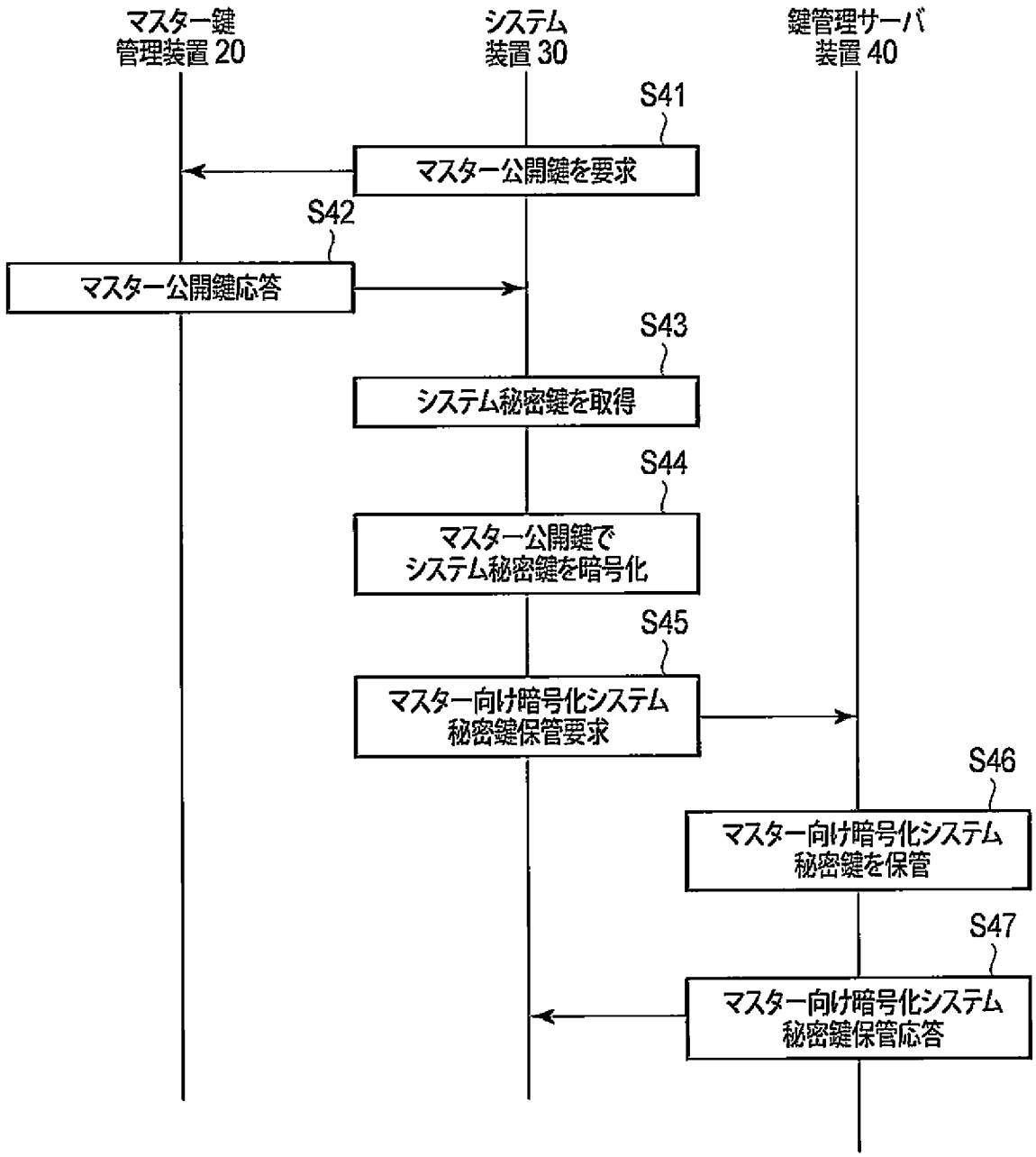
[図8]


開始
鍵セットアップ処理
S11
システム秘密鍵セットアップ処理
S12
再暗号化鍵セットアップ処理
S13
鍵配布処理
S14
終了

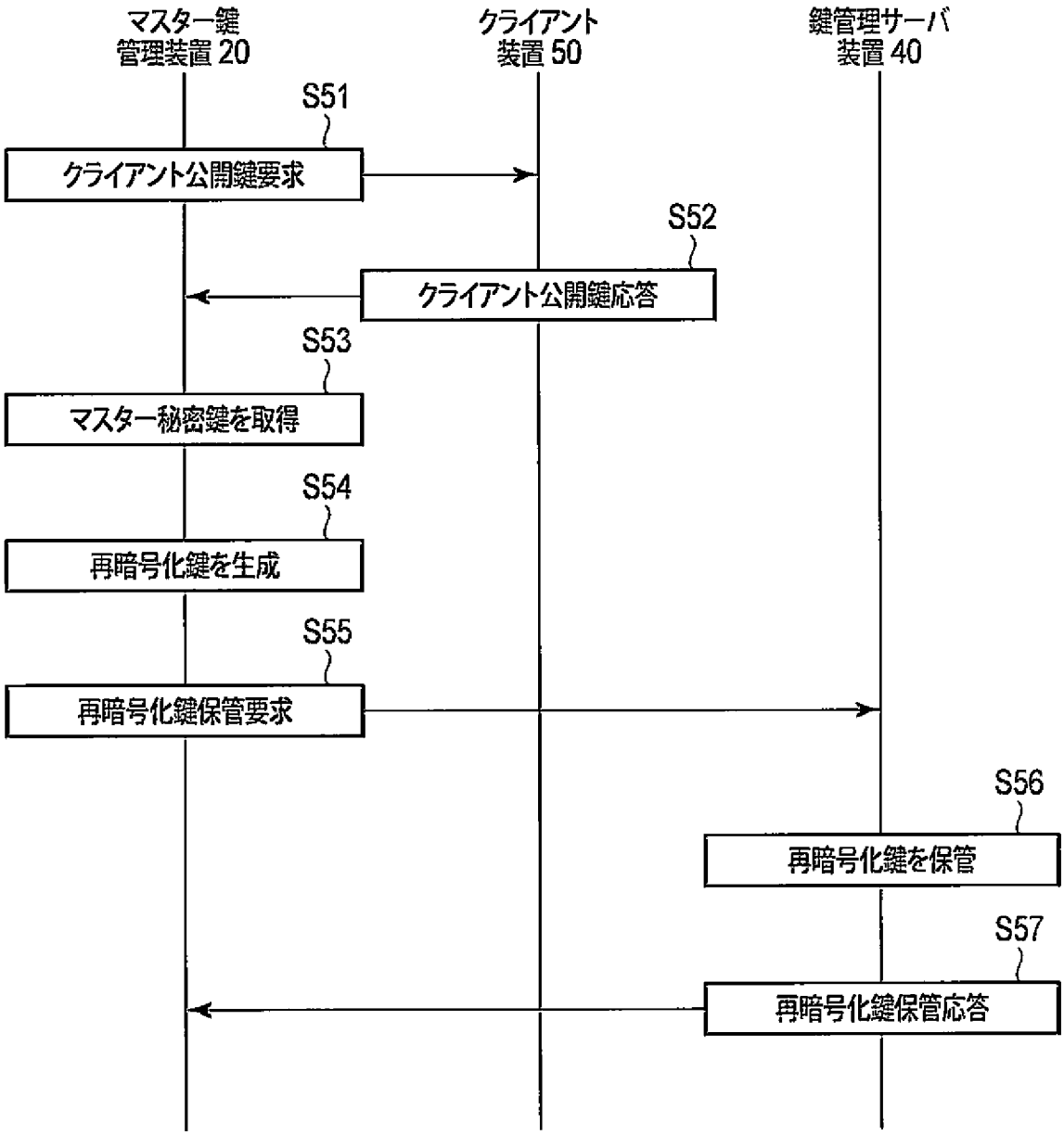
[図9]


マスター鍵
管理装置 20
クライアント
装置 50
公開鍵・秘密鍵
生成装置 10
S21
マスター鍵生成要求
S22
マスター公開鍵・秘密鍵を生成
S23
マスター鍵生成応答
S24
マスター秘密鍵を保管
S25
マスター公開鍵を公開
S26
クライアント鍵生成要求
S27
クライアント公開鍵・秘密鍵を生成
S28
クライアント鍵生成応答
S29
クライアント秘密鍵を保管
S30
クライアント公開鍵を公開

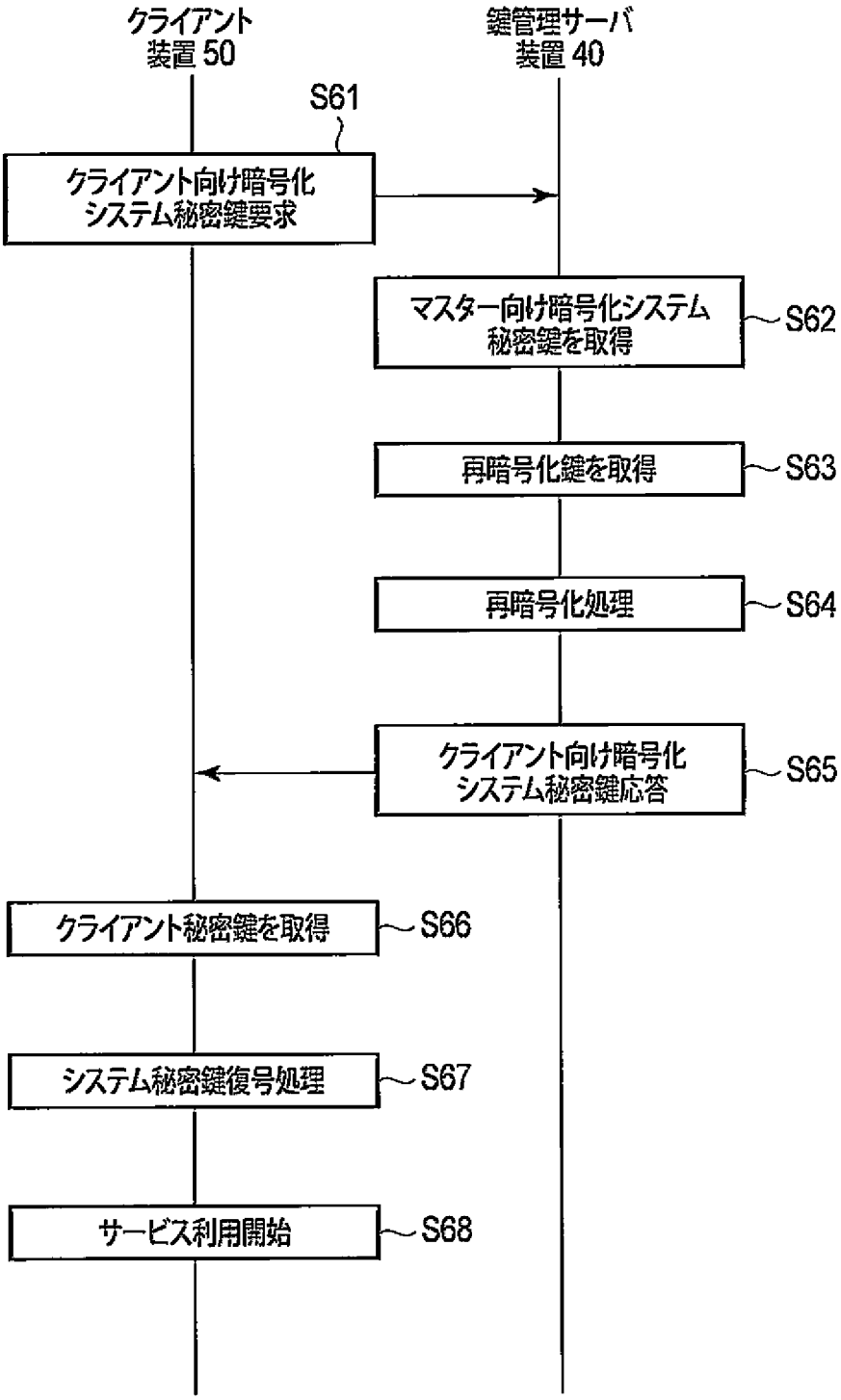
[図10]


マスター鍵
管理装置 20
システム
装置 30
鍵管理サーバ
装置 40
S41
マスター公開鍵を要求
S42
マスター公開鍵応答
S43
システム秘密鍵を取得
S44
マスター公開鍵で
システム秘密鍵を暗号化
S45
マスター向け暗号化システム
秘密鍵保管要求
S46
マスター向け暗号化システム
秘密鍵を保管
S47
マスター向け暗号化システム
秘密鍵保管応答

[図11]


マスター鍵
管理装置 20
クライアント
装置 50
鍵管理サーバ
装置 40
S51
クライアント公開鍵要求
S52
クライアント公開鍵応答
S53
マスター秘密鍵を取得
S54
再暗号化鍵を生成
S55
再暗号化鍵保管要求
S56
再暗号化鍵を保管
S57
再暗号化鍵保管応答

[図12]


クライアント
装置 50
鍵管理サーバ
装置 40
S61
クライアント向け暗号化
システム秘密鍵要求
マスター向け暗号化システム
秘密鍵を取得
S62
再暗号化鍵を取得
S63
再暗号化処理
S64
クライアント向け暗号化
システム秘密鍵応答
S65
クライアント秘密鍵を取得
S66
システム秘密鍵復号処理
S67
サービス利用開始
S68

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2012/053546

A. CLASSIFICATION OF SUBJECT MATTER
H04L9/08(2006.01)i, *H04L9/14*(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L9/08, H04L9/14

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2012
Kokai Jitsuyo Shinan Koho	1971-2012	Toroku Jitsuyo Shinan Koho	1994-2012

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
JSTPlus/JMEDPlus/JST7580(JDreamII), IEEE Xplore

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	Giuseppe Ateniese et al, Improved proxy re-encryption schemes with applications to secure distributed storage, [online], 2005, [retrieval date 14 March 2012 (14.03.2012)], Internet <URL:http://citeseer.ist.psu.edu/viewdoc/summary?doi=10.1.1.100.7790>	1-3
A	Benoit Libert et al, Unidirectional Chosen-Ciphertext Secure Proxy Re-Encryption, [online], 2008, [retrieval date 14 March 2012 (14.03.2012)], Internet <URL:http://hal.inria.fr/inria-00339530/en/>	1-3
A	Benoit Libert et al, Tracing Malicious Proxies in Proxy Re-Encryption, [online], 2008, [retrieval date 14 March 2012 (14.03.2012)], Internet <http://hal.inria.fr/inria-00327353/>	1-3

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
15 March, 2012 (15.03.12)	27 March, 2012 (27.03.12)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2012/053546

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	Jun Shao et al, CCA-Secure Proxy Re-Encryption without Pairings, [online], 2009.03, [retrieval date 14 March 2012 (14.03.2012)], Internet <http://www.iacr.org/archive/pkc2009/pkc2009.html>	1-3
A	Jian Weng et al, Conditional proxy re-encryption secure against chosen-ciphertext attack, ASIACCS '09 Proceedings of the 4th International Symposium on Information, Computer, and Communications Security, 2009.03, p.322-332	1-3
A	Ibraimi, Luan et al, An encryption scheme for a secure policy updating, proceedings of the 2010 International Conference on Security and Cryptography, IEEE, 2010.07, p.1-10	1-3

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２０１２／０５３５４６

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　H04L9/08(2006.01)i, H04L9/14(2006.01)i

Ｂ．　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Int.Cl.　H04L9/08, H04L9/14

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２０１２年
日本国実用新案登録公報	１９９６－２０１２年
日本国登録実用新案公報	１９９４－２０１２年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

JSTPlus/JMEDPlus/JST7580(JDreamII), IEEE Xplore

Ｃ．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求項の番号
A	Giuseppe Ateniese et al, Improved proxy re-encryption schemes with applications to secure distributed storage, [online], 2005, ［平成２４年３月１４日検索］, インターネット <URL:http://citeseer.ist.psu.edu/viewdoc/summary?doi=10.1.1.100.7790>	１－３

☑　Ｃ欄の続きにも文献が列挙されている。

☐　パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの
「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「Ｏ」口頭による開示、使用、展示等に言及する文献
「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「＆」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
１５．０３．２０１２	２７．０３．２０１２

国際調査機関の名称及びあて先
日本国特許庁（ＩＳＡ／ＪＰ）
郵便番号１００－８９１５
東京都千代田区霞が関三丁目４番３号

特許庁審査官（権限のある職員）　５Ｓ　３１４６
松平　英
電話番号　０３－３５８１－１１０１　内線　３５４６

Ｃ（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求項の番号
A	Benoit Libert et al, Unidirectional Chosen-Ciphertext Secure Proxy Re-Encryption, [online], 2008, ［平成２４年３月１４日検索], インターネット <URL:http://hal.inria.fr/inria-00339530/en/>	１－３
A	Benoit Libert et al, Tracing Malicious Proxies in Proxy Re-Encryption, [online], 2008, [平成２４年３月１４日検索], インターネット<http://hal.inria.fr/inria-00327353/>	１－３
A	Jun Shao et al, CCA-Secure Proxy Re-Encryption without Pairings, [online], 2009.03, [平成２４年３月１４日検索], インターネット <http://www.iacr.org/archive/pkc2009/pkc2009.html>	１－３
A	Jian Weng et al, Conditional proxy re-encryption secure against chosen-ciphertext attack, ASIACCS '09 Proceedings of the 4th International Symposium on Information, Computer, and Communications Security, 2009.03, p.322-332	１－３
A	Ibraimi, Luan et al, An encryption scheme for a secure policy updating, proceedings of the 2010 International Conference on Security and Cryptography, IEEE, 2010.07, p.1-10	１－３