(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
2015 年 1 月 15 日(15.01.2015)

WIPO | PCT

(10) 国際公開番号
WO 2015/004706 A1

(51) 国際特許分類:
G09C 1/00 (2006.01) *H04L 9/08* (2006.01)
G06F 21/62 (2013.01)

(21) 国際出願番号: PCT/JP2013/068595

(22) 国際出願日: 2013 年 7 月 8 日(08.07.2013)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(71) 出願人: 株式会社日立製作所 **(HITACHI, LTD.)** [JP/JP]; 〒1008280 東京都千代田区丸の内一丁目６番６号 Tokyo (JP).

(72) 発明者: 菅野 慎一郎 **(KANNO, Shinichiro)**; 〒2500872 神奈川県小田原市中里３２２番２号 株式会社日立製作所 ＩＴプラットフォーム事業本部内 Kanagawa (JP). 大崎 伸之 **(OSAKI, Nobuyuki)**; 〒2500872 神奈川県小田原市中里３２２番２号 株式会社日立製作所 ＩＴプラットフォーム事業本部内 Kanagawa (JP).

(74) 代理人: 特許業務法人ウィルフォート国際特許事務所 **(WILLFORT INTERNATIONAL)**; 〒1010052 東京都千代田区神田小川町三丁目３番地 神田小川町トーセイビルＩＩ ７階 Tokyo (JP).

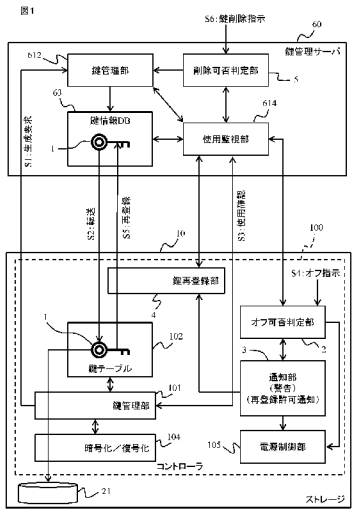
(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, 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, RU, TJ, TM), ヨーロッパ

[続葉有]

(54) **Title**: STORAGE DEVICE AND CONTROL METHOD FOR STORAGE DEVICE

(54) 発明の名称 : ストレージ装置およびストレージ装置の制御方法



2 Off advisability determination unit
3 Notification unit (alarm) (re-registration permission notification)
4 Key re-registration unit
5 Deletion advisability determination unit
10 Storage
60 Key management server
63 Key information DB
100 Controller
101 Key management unit
102 Key table
104 Encoding/decoding
105 Power supply control unit
612 Key management unit
614 Usage monitoring unit
S1 Generation request
S2 Transfer
S3 Usage confirmation
S4 Off instruction
S5 Re-registration
S6 Key deletion instruction

(57) Abstract: In order to store in a management server key information that is being used and to enable loss of key information to be suppressed, a storage device (10) is connected so as to be able to communicate with a management server (60) managing key information (1). The storage device comprises a memory device (21) and a controller (100) controlling the memory device. The controller is configured so as to use the key information and encrypt data input to and output from the memory device. When an instruction is given to stop operation, the controller determines whether or not key information used by the controller is managed by the management server, stops operation if a determination is made that the key information is managed by the management server, and does not stop operation if a determination is made that the key information is not managed by the management server.

(57) 要約: 使用中の鍵情報を管理サーバに保管させて、鍵情報の消失を抑制できるようにすること。 ストレージ装置１０は、鍵情報１を管理する管理サーバ６０と通信可能に接続される。ストレージ装置は、記憶装置２１と、記憶装置を制御するコントローラ１００とを備える。コントローラは、記憶装置に入出力するデータを鍵情報を用いて暗号化処理するようになっている。コントローラは、動作停止が指示されると、当該コントローラで使用している鍵情報が管理サーバで管理されているか判定し、鍵情報が管理サーバで管理されていると判定した場合は動作を停止し、鍵情報が管理サーバで管理されていないと判定した場合は動作を停止しない。

WO 2015/004706 A1

(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, KM, ML, MR, NE, SN, TD, TG).

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 ： ストレージ装置およびストレージ装置の制御方法

技術分野

[0001] 本発明は、ストレージ装置およびストレージ装置の制御方法に関する。

背景技術

[0002] データの秘密を守るために、暗号化機能を有するストレージ装置が利用されている。暗号化機能を有するストレージ装置は、暗号鍵を用いてデータを暗号化し、記憶装置に保存する。もしも暗号鍵を消失すると、暗号化データを復号できなくなるため、事実上そのデータを消失したに等しい。一方、暗号鍵とその暗号鍵を用いて暗号化されたデータとをストレージ装置に格納することは、セキュリティの観点から好ましくない。もしもストレージ装置全体を盗まれると、暗号化されたデータが解読されてしまい、情報が漏洩するおそれがあるためである。

[0003] そこで、暗号鍵をストレージ装置とは物理的に別の管理サーバに格納し、ストレージ装置はそれが必要になったときに管理サーバから暗号鍵を取得して使用する技術が提案されている（特許文献１）。

先行技術文献

特許文献

[0004] 特許文献1：米国特許第８，０１０，８１０号

発明の概要

発明が解決しようとする課題

[0005] 特許文献１に記載の従来技術では、ストレージ装置の使用する暗号鍵を鍵管理用のサーバに格納し、ストレージ装置と管理サーバとが連携することで暗号鍵を使用できるようにしている。

[0006] しかし、管理サーバは、ストレージ装置から独立して別個に管理するため、ストレージ装置の状態とは無関係に、暗号鍵を削除することも可能である。従って、ストレージ装置が停止状態の場合において、管理サーバで管理し

ている暗号鍵を誤って削除してしまうと、ストレージ装置を起動できなくなったり、あるいは、ストレージ装置内の暗号化されたデータを使用できなくなったりする。従って、従来技術では、ストレージ装置で使用する暗号鍵の保管の信頼性が低い。

[0007] 本発明は、上記の問題に鑑みてなされたもので、その目的は、信頼性を向上できるようにしたストレージ装置およびストレージ装置の制御方法を提供することにある。本発明の他の目的は、使用中の鍵情報を管理サーバに保管させて、鍵情報の消失を抑制できるようにしたストレージ装置およびストレージ装置の制御方法を提供することにある。

課題を解決するための手段

[0008] 本発明の一つの観点に係るストレージ装置は、鍵情報を管理する管理サーバと通信可能に接続されるストレージ装置であって、記憶装置と、記憶装置を制御するコントローラとを備え、コントローラは、記憶装置に入出力するデータを鍵情報を用いて暗号化処理するようになっており、動作停止が指示されると、当該コントローラで使用している鍵情報が管理サーバで管理されているか判定し、鍵情報が管理サーバで管理されていると判定した場合は動作を停止し、鍵情報が管理サーバで管理されていないと判定した場合は動作を停止しない。

[0009] コントローラは、鍵情報が管理サーバで管理されていないと判定した場合に、その旨の通知を出力してもよい。

[0010] コントローラは、鍵情報が管理サーバで管理されていないと判定した場合に、管理サーバに鍵情報を登録するか確認するための通知を出力してもよい。

[0011] コントローラは、管理サーバへの鍵情報の登録が許可された場合に、鍵情報を管理サーバに送信して登録させてもよい。

図面の簡単な説明

[0012] [図1]本発明の実施形態の概要を示す説明図。

[図2]ストレージ装置を含む情報処理システムのハードウェア構成図。

[図3]ストレージ装置を含む情報処理システムの機能ブロック図。

[図4]鍵管理サーバに格納されている、鍵情報の構成例を示す説明図。

[図5]鍵管理サーバに格納されている、装置情報の構成例を示す説明図。

[図6]ストレージ装置に格納されている、鍵情報を取得するための鍵番号を管理する情報の構成例を示す説明図。

[図7]ストレージ装置に格納されている、鍵テーブルの構成例を示す説明図。

[図8]ストレージ装置に格納されている、鍵管理サーバに接続するための設定情報の構成例を示す説明図。

[図9]鍵情報を新規作成する処理を示すフローチャート。

[図10]鍵管理サーバがストレージ装置での鍵情報の使用状態を確認する処理を示すフローチャート。

[図11]ストレージ装置での鍵情報の使用状態を、ストレージ装置から鍵管理サーバに通知する処理を示すフローチャート。

[図12]ストレージ装置で使用中の鍵情報を鍵管理サーバに送信して登録させる処理を示すフローチャート。

[図13]ストレージ装置で使用中の鍵情報を鍵管理サーバに送信して登録させる処理の他の例を示すフローチャート。

[図14]ストレージ装置の停止が指示された場合の処理を示すフローチャート。

[図15]鍵情報の削除が指示された鍵管理サーバの処理を示すフローチャート。

[図16]第２実施例に係り、ストレージ装置の停止が指示された場合の処理を示すフローチャート。

[図17]図１６に続くフローチャート。

[図18]第３実施例に係り、ストレージ装置の停止が指示された場合の処理を示すフローチャート。

[図19]第４実施例に係り、ストレージ装置および鍵管理サーバの動作を決定するためのポリシーを設定する処理を示すフローチャート。

[図20]第５実施例に係り、鍵管理サーバに鍵情報の削除を指示した場合の処理を示すフローチャート。

[図21]第６実施例に係り、鍵管理情報の削除が指示された鍵管理サーバの処理を示すフローチャート。

発明を実施するための形態

[0013] 以下、添付図面を参照して本発明の実施形態について説明する。ただし、本実施形態は本発明を実現するための一例に過ぎず、本発明の技術的範囲を限定するものではないことに注意すべきである。本実施形態で開示される複数の特徴は、様々に組み合わせることができる。

[0014] 本実施形態の処理動作の説明では、「コンピュータプログラム」を動作主体（主語）として説明することがある。コンピュータプログラムは、マイクロプロセッサによって実行される。従って、プロセッサを動作主体として読み替えても良い。

[0015] 本実施形態では、一方の装置で使用する鍵情報を、一方の装置とは別に設けられた他方の装置で管理する情報処理システムにおいて、保管の必要が有る限り、他方の装置に鍵情報を保持させる。本実施形態では、他方の装置が鍵情報を保持していない場合、一方の装置を停止させないことにより、鍵情報の消失を防止する。また、本実施形態では、他方の装置が鍵情報を保持していない場合、一方の装置で一時的に記憶されている鍵情報を他方の装置に送信して保持させる。

[0016] 図１は、本実施形態の概要を示す説明図である。より詳細な構成は図２以降の図面を参照しながら後述する。図１は、本実施形態の理解のために用いられるもので、本発明の範囲を図１に記載の構成に限定する意図はない。図１に示す構成の一部を欠いた構成、図１に示す構成に新たな部材または機能を追加した構成も、本発明の範囲に含まれる。

[0017] 情報処理システムは、鍵管理サーバ６０と、鍵管理サーバ６０で管理される鍵情報（以下、鍵または暗号鍵とも呼ぶ）を用いてデータを暗号化処理するストレージ装置１０とを含む。鍵管理サーバ６０とストレージ装置１０と

は、複数ずつ設けることができる。

[0018] ストレージ装置１０は、コントローラ１００と、コントローラ１００により制御される記憶装置２１を備える。後述のように、ストレージ装置１０は、図外のホストコンピュータ３０からの要求に応じて、データを記憶装置２１に入出力する。本実施例では、暗号化処理とは、鍵を用いて平文データを暗号データに変換する暗号化と、鍵を用いて暗号化データを復号する復号化との両方を含む。

[0019] 記憶装置２１は、ハードディスクドライブ、フラッシュメモリデバイスなどの物理的記憶装置から構成されており、一つまたは複数の物理的記憶装置の有する物理的記憶領域から、所定サイズまたは可変サイズの論理的記憶装置が生成される。論理的記憶装置は、論理ボリュームとも呼ばれる。ここでは、論理的記憶装置２１を例に挙げて説明するが、記憶装置２１は物理的記憶装置であってもよい。記憶装置２１を論理ボリューム２１と呼ぶこともある。暗号化されたデータ（暗号データとも呼ぶ）を記憶する記憶装置２１は、平文データを記憶する記憶装置と区別するために、暗号化記憶装置と呼ぶことがある。

[0020] ストレージ装置１０の使用する鍵情報としての鍵（暗号鍵）は、セキュリティを確保するために、鍵を管理するための専用装置として構成される鍵管理サーバ６０で生成され、鍵管理サーバ６０で管理される。ストレージ装置１０は、例えば、装置の起動時や暗号化記憶装置２１にデータを入出力する場合など、鍵を必要な場合に、鍵管理サーバ６０から鍵を取得して使用する。ストレージ装置１０の電源をオフして動作を停止すると、ストレージ装置１０内の鍵は消失する。従って、ストレージ装置１０のみを取り外して持ち去っても、ストレージ装置１０内に鍵は存在しないため、暗号化記憶装置のデータ漏洩を防止できる。

[0021] 鍵の生成と登録について説明する。ストレージ装置１０内で鍵を管理する鍵管理部１０１は、鍵管理サーバ６０内で鍵を管理する鍵管理部６１２に対して、鍵の生成を要求する（Ｓ１）。

[0022] サーバ側の鍵管理部６１２は、新たな鍵１を生成して、鍵情報格納部６３に登録する。その新たな鍵１は、鍵管理サーバ６０からストレージ装置１０に転送されて、ストレージ装置１０の鍵テーブル１０２に格納される（Ｓ２）。鍵テーブル１０２は、揮発性メモリの領域に記憶されているため、ストレージ装置１０の電源がオフして停止すると、消失する。

[0023] 暗号化／復号化部１０４（以下、暗号化処理部１０４とも呼ぶ）は、鍵管理部１０１を介して鍵テーブル１０２から鍵１を受領し、その鍵１を用いて暗号化記憶装置２１にデータを入出力する。暗号化処理部１０４は、ストレージ装置１０に電源が供給されている間、鍵テーブル１０２に一時的に記憶されている鍵１を用いて、データを暗号化したり、暗号化されたデータを復号したりする。

[0024] 鍵管理サーバ６０の使用監視部６１４は、ストレージ装置１０における鍵の使用状況を監視する（Ｓ３）。使用監視部６１４は、所定タイミングで、または、一定周期で、ストレージ装置１０内で使用している鍵を確認することができる。

[0025] ストレージ装置１０は、２４時間３６５日の連続運転も可能であるが、例えば、保守作業、情報処理システムの構成変更などの理由から、停止する場合もある。ストレージ管理者などがストレージ装置１０に電源オフを指示すると（Ｓ４）、電源オフの可否を判定するオフ可否判定部２は、ストレージ装置１０で使用している全ての鍵が鍵管理サーバ６０で管理されているか確認する。鍵が管理されているとは、その鍵が鍵情報格納部６３に格納されていることを意味する。

[0026] オフ可否判定部２は、鍵管理サーバ６０がストレージ装置１０で使用している全ての鍵を管理していると判断すると、ストレージ装置１０の電源を制御する電源制御部１０５に電源オフを指示する。この指示を受けた電源制御部１０５は、マイクロプロセッサやメモリ、記憶装置２１等への電源供給を停止する。

[0027] これに対し、オフ可否判定部２は、ストレージ装置１０で使用している全

ての鍵のうちいずれか一つでも鍵管理サーバ６０で管理されていないと判断すると、通知部３を介して警告を出力する。

[0028] その警告には、例えば、ストレージ装置１０で使用している鍵のうち幾つかの鍵が鍵管理サーバ６０に記憶されていないのに、ストレージ装置１０が停止されようとしていることを示す情報が含まれる。その警告は、例えば、ストレージ管理者の使用する管理端末５０（図２参照）に表示したり、または、ストレージ管理者の所持する携帯端末（携帯電話を含む）に表示したりできる。その警告は、テキストメッセージだけでなく、音声メッセージとして構成されてもよい。

[0029] 通知部３は、警告に代えて、または警告と一緒に、鍵の再登録についての許可を求める通知を出力することもできる。鍵の再登録とは、ストレージ装置１０で使用している鍵の少なくとも一部を鍵管理サーバ６０に送信して記憶させることを意味する。ストレージ管理者は、再登録の許可を求める通知を受領すると、ストレージ装置１０に対して、鍵管理サーバ６０への鍵の再登録を許可する。

[0030] 鍵を再登録する鍵再登録部４は、鍵テーブル１０２に記憶されている鍵のうち登録対象の鍵を鍵管理サーバ６０に送信し、鍵情報格納部６３に記憶させる（Ｓ５）。ここで、オフ可否判定部２、通知部３、鍵再登録部４は、後述するフローチャート（図１２、図１３、図１４、図１６）中の、一つまたは複数のステップとして現れる。

[0031] サーバ管理者は、鍵管理サーバ６０で管理している鍵の一部または全部の削除を指示することができる（Ｓ６）。鍵管理サーバ６０とストレージ装置１０とはそれぞれ別々の装置として構成されており、互いに離れた場所に設置されている。また、セキュリティ性および信頼性の観点から、複数の鍵管理サーバ６０と複数のストレージ装置１０とが多対多で対応付けられることがある。従って、或る鍵管理サーバ６０を管理するサーバ管理者は、その鍵管理サーバ６０で鍵を管理している全てのストレージ装置１０について熟知しているとは限らず、誤った削除指示を鍵管理サーバ６０に与えるおそれが

ある。

[0032] 鍵管理サーバ６０の削除可否判定部５は、削除指示が適切であるか否かを判定するものであり、鍵の削除について示す後述のフローチャート（図１５、図２０、図２１）中の、一つまたは複数のステップとして現れる。削除可否判定部５は、削除対象の鍵の使用状態に基づいて、その鍵の削除が適切か否か判定する。削除可否判定部５が削除してもよいと判定した場合、鍵管理部６１２は鍵情報格納部６３から対象の鍵を削除する。

[0033] このように構成される本実施形態では、ストレージ装置１０の使用している鍵１が失われる可能性がある場合に、鍵１が失われる可能性を抑制する。例えば、鍵管理サーバ６０がストレージ装置１０で使用している鍵１を保持していない場合において、ストレージ装置１０の電源オフが指示された場合は、電源をオフしない。この場合、ストレージ装置１０内の鍵１を鍵管理サーバ６０に送信して再登録した後に、ストレージ装置１０の電源をオフする。

[0034] 従って、本実施形態によれば、ストレージ装置１０で使用している鍵が情報処理システム内で失われてしまうのを未然に阻止することができ、信頼性を高めることができる。また、本実施形態によれば、ストレージ装置１０のみが保持する鍵を鍵管理サーバ６０に送信して再登録することができるため、使い勝手が向上する。

[0035] 換言すれば、本実施形態では、保管する必要がある限り、その鍵を鍵管理サーバ６０に保管させるため、鍵管理サーバ６０とストレージ装置１０とが別々に設けられている情報処理システム（ストレージシステム）のセキュリティ性および信頼性を向上できる。

実施例 １

[0036] 図１～図１５を用いて第１実施例を説明する。図１は、ストレージ装置１０を含むストレージシステムのハードウェア構成を示すブロック図である。ストレージシステムは、例えば、少なくとも一つのストレージ装置１０と、少なくとも一つのディスク搭載ユニット２０と、少なくとも一つのホストコ

ンピュータ（以下、ホスト）３０と、少なくとも一つの管理端末５０と、少なくとも一つの鍵管理サーバ６０とを備える。ストレージシステムは、さらに外部ストレージ装置４０を含んでもよい。

[0037] 本実施例では、複数のストレージ装置１０が設けられており、各ストレージ装置１０にはそれぞれ管理端末５０が接続されている。複数のストレージ装置１０は、複数の鍵管理サーバ６０に対応付けることができるようになっている。

[0038] 先に接続構成を説明すると、ホスト３０とストレージ装置１０とは、データ入出力用のネットワークＣＮ１を介して接続されている。ストレージ装置１０と外部ストレージ装置４０とは、外部接続用の通信ネットワークＣＮ２を介して接続されている。管理端末５０および鍵管理サーバ６０とストレージ装置１０とは管理用通信ネットワークＣＮ３を介して接続されている。ストレージ装置１０のコントローラ１００とディスク搭載ユニット２０とは、ディスク入出力用のネットワークＣＮ４を介して接続されている。

[0039] 通信ネットワークＣＮ１、ＣＮ２、ＣＮ３は、例えば、ＦＣ－ＳＡＮ（Fibre Channel - Storage Area Network）、ＩＰ－ＳＡＮ（Internet Protocol - Storage Area Network）を用いることができる。通信ネットワークＣＮ３は、例えば、ＬＡＮ（Local Area Network）等のＩＰ（Internet Protocol）ネットワークを用いることができる。各通信ネットワークＣＮ１～ＣＮ４の全部または一部を共通の通信ネットワークとして構成してもよい。

[0040] ストレージ装置１０は、コントローラ１００を有する。コントローラ１００は、ホスト３０からのコマンドを処理し、それらコマンドに応じてディスク搭載ユニット２０内の記憶装置２１にデータを入出力する。コントローラ１００は、コマンドの処理結果をコマンド発行元のホスト３０に返す。さらに、コントローラ１００は、暗号化処理に使用している鍵の消失を防止すべく、コントローラ１００への電源オフ指示の可否を判定したり、鍵管理サーバ６０からの問合せに応答したりする。図２では、一つのコントローラ１００を示しているが、負荷分散や冗長性実現のために、一つのストレージ装置

１０内に複数のコントローラ１００を設けてもよい。

[0041] ディスク搭載ユニット２０は、複数の記憶装置２１を有する。記憶装置２１は、一つまたは複数の物理的記憶装置を利用して生成される論理的な記憶装置である。物理的記憶装置としては、例えば、ハードディスクデバイス、半導体メモリデバイス、光ディスクデバイス、光磁気ディスクデバイス等のデータを読み書き可能な種々の装置を挙げることができる。ハードディスクデバイスとしては、例えば、ＦＣ（Fibre Channel）ディスク、ＳＣＳＩ（Small Computer System Interface）ディスク、ＳＡＴＡディスク、ＡＴＡ（AT Attachment）ディスク、ＳＡＳ（Serial Attached SCSI）ディスク等がある。

[0042] さらに例えば、フラッシュメモリ、ＦｅＲＡＭ（Ferroelectric Random Access Memory）、ＭＲＡＭ（MagnetoresistiveRandom Access Memory）、相変化メモリ（Ovonic Unified Memory）、ＲＲＡＭ（登録商標）、ＲｅＲＡＭ（Resistive Random Access Memory）等の種々の記憶装置を用いることもできる。さらに、例えば、フラッシュメモリデバイスとハードディスクデバイスのように、種類の異なる記憶装置を混在させる構成でもよい。

[0043] 例えば、複数の物理的記憶装置の物理的記憶領域をＲＡＩＤ（Redundant Arrays of Inexpensive Disks）グループとして管理し、ＲＡＩＤグループとして仮想化された物理的記憶領域から所定サイズまたは可変サイズの記憶領域を切り出すことで、論理的な記憶装置２１（論理ボリューム２１）を得ることができる。記憶装置２１は、コントローラ１００の通信ポートを介してホスト３０に対応付けられ、そのホスト３０により使用される。

[0044] ディスク搭載ユニット２０は、コントローラ１００を収容する筐体内に設けられてもよいし、コントローラ１００を収容する筐体とは別の筐体に設けられてもよい。なお、ストレージ装置１０は、後述のように外部のストレージ装置４０の有する記憶装置４１も利用できるため、必ずしもストレージ装置として構成される必要はない。例えば、装置４１は、暗号化処理用のアプライアンス装置として構成してもよいし、スイッチ装置として構成してもよ

い。

[0045] 外部ストレージ装置４０は、ストレージ装置１０により利用される装置である。利用元の装置であるストレージ装置１０から見て外部に存在するため、外部ストレージ装置４０と呼ぶ。外部ストレージ装置４０の有する論理的記憶装置４１の記憶空間は、ストレージ装置１０のコントローラ１００の制御する仮想的な記憶装置の記憶空間にマッピングされている。図２では外部ストレージ装置４０を一つだけ示すが、ストレージ装置１０は複数の外部ストレージ装置４０を利用することができる。

[0046] コントローラ１００は、仮想的な記憶装置をホスト３０に提供し、ホスト３０からのライトデータを外部ストレージ装置４０の記憶装置４１に書き込む。コントローラ１００は、ホスト３０からのリードコマンドを受領すると、外部ストレージ装置４０の記憶装置４１からデータを読み出し、そのデータをホスト３０に送信する。このように、ストレージ装置１０は、外部ストレージ装置４０の有する記憶装置４１を、あたかもストレージ装置１０の記憶装置２１であるかのようにして、ホスト３０に提供する。

[0047] ホスト３０は、ストレージ装置１０にデータを書き込んだり、ストレージ装置１０からデータを読み出したりするコンピュータであり、例えばサーバのように構成される。ホスト３０は、図外のクライアント装置にデータ処理サービスを提供することもできる。

[0048] 管理端末５０は、ストレージ装置１０を操作するためのコンピュータ端末である。システム管理者は、管理端末５０を介してストレージ装置１０に指示を与えたり、ストレージ装置１０の状態を管理端末５０の画面に表示させたりすることができる。管理端末５０は、システム管理者（ストレージ管理者）が指示や情報などを入力するための入力装置と、システム管理者に情報を提供するための出力装置とを備える。入力装置としては、例えば、キーボード、タッチパネル、ポインティングデバイス、音声入力装置、視線検出装置、動作検出装置、脳波検出装置などがある。出力装置としては、例えば、ディスプレイ、プリンタ、音声合成装置などがある。

[0049] 鍵管理サーバ６０は、ストレージ装置１０の使用する暗号鍵を管理するためのコンピュータである。鍵管理サーバ６０は、別に設けられる操作用コンピュータ（図示せず）と接続されている。システム管理者（サーバ管理者）は、操作用コンピュータを用いて、鍵管理サーバ６０に指示を与えることができる。なお、ストレージ管理者とサーバ管理者とが共通する場合などでは、管理端末５０で、鍵管理サーバ６０とストレージ装置１０の両方を操作できる構成としてもよい。

[0050] 鍵管理サーバ６０は、マイクロプロセッサ、メモリ、補助記憶装置、通信インターフェース、ユーザインターフェースなどを備えており、メモリや補助記憶装置には所定のコンピュータプログラムが格納されている。マイクロプロセッサが所定のコンピュータプログラムを読み込んで実行することで、鍵を生成したり、保管したり、削除したり（無効化したり）、ストレージ装置１０での鍵の使用状態を監視したりするための所定の処理が実現する。鍵管理サーバ６０の実現する機能については、図３で後述する。

[0051] ストレージ装置１０のコントローラ１００について説明する。ストレージ装置１０を制御するコントローラ１００は、例えば、フロントエンドインターフェース１１と、バックエンドインターフェース１２と、メモリパッケージ１３と、マイクロプロセッサパッケージ１４と、スイッチ１５と、サービスプロセッサ１６を備えている。

[0052] フロントエンドインターフェース１１は、ホスト３０や外部ストレージ装置４０との通信を担当する装置である。フロントエンドインターフェース１１は、複数の通信インターフェース１１１を備えている。それら通信インターフェース１１１は、通信ネットワークを介してホスト３０や外部ストレージ装置４０に接続されている。通信の冗長性を実現すべく、一つのホスト３０が複数の通信インターフェース１１１と通信できるように構成してもよい。同様に、一つの外部ストレージ装置４０が複数の通信インターフェース１１１と通信できるように構成してもよい。

[0053] バックエンドインターフェース１２は、各記憶装置２１との通信を担当す

る装置であり、複数の通信インターフェース１２１を備える。それら通信インターフェース１１１は、記憶装置２１を形成する物理的記憶装置の通信ポートに接続されている。冗長性を実現するために、バックエンドインターフェース１２は、複数の異なる経路から物理的記憶装置にアクセスできるようになっている。

[0054] メモリパッケージ１３は、共有メモリ１３１とキャッシュメモリ１３２を備える。共有メモリ１３１は、制御情報や管理情報などを格納する。キャッシュメモリ１３２は、ホスト３０から書き込まれたデータや記憶装置２１から読み出したデータなどを一時的に記憶する。また、キャッシュメモリ１３２には、ストレージ装置１０で使用する鍵情報も記憶される。

[0055] マイクロプロセッサパッケージ１４は、複数のマイクロプロセッサ１４１と、ローカルメモリ１４２を備える。ローカルメモリ１４２には、例えば、共有メモリ１３１に格納されている情報のうち必要な情報や、コンピュータプログラムなどが記憶されている。フロントエンドインターフェース１１がホスト３０からのコマンドを受領すると、複数のマイクロプロセッサ１４１のうちコマンド受領に気づいたいずれか一つのマイクロプロセッサ１４１が、そのコマンドを処理する。コマンドを処理したマイクロプロセッサ１４１は、処理結果をフロントエンドインターフェース１１を介してホスト３０に返す。

[0056] サービスプロセッサ（図中、ＳＶＰ）１６は、ストレージ装置１０の構成変更などを管理するための装置である。サービスプロセッサ１６は、例えば、ストレージ装置１０の状態を管理端末５０や鍵管理サーバ６０に出力したり、管理端末５０からの入力に応じてストレージ装置１０の構成を変更したり、鍵管理サーバ６０と通信したりする。

[0057] 図３は、ストレージシステムの機能構成を示すブロック図である。図中、鍵管理サーバ６０をサーバ６０または管理サーバ６０と、ストレージ装置１０をストレージ１０と略記することがある。

[0058] 鍵管理サーバ６０は、例えば、情報管理部６１、装置情報格納部６２、鍵

情報格納部６３、閲覧／編集部６４、連携部６５を備える。

[0059] 情報管理部６１は、鍵情報や鍵情報を使用する装置１０の情報を管理するための機能であり、ソフトウェアモジュールとして構成される。

[0060] 装置情報格納部６２は、装置情報を格納する記憶領域である。装置情報とは、鍵情報を使用する装置（本実施例ではストレージ装置１０）についての情報であり、データベースとして管理されている。

[0061] 鍵情報格納部６３は、暗号化処理に使用する鍵情報（鍵と略記する場合がある）を格納するための記憶領域である。鍵情報格納部６３には、複数の鍵情報を格納できる。それら鍵情報には鍵番号が対応付けられており、鍵番号を指定して検索などを行うようになっている。

[0062] 閲覧／編集部６４は、システム管理者（サーバ管理者）が鍵管理サーバ６０の構成情報を閲覧したり、設定操作したりするための機能である。

[0063] 連携部６５は、外部装置（本実施例ではストレージ装置１０）と通信するための機能である。連携部６５は、外部装置から接続された場合の認証、および、外部装置に接続する場合の認証も行う。

[0064] 情報管理部６１は、例えば、装置情報管理部６１０と、装置情報検索部６１１と、鍵管理部６１２と、鍵検索部６１３と、使用監視部６１４を備える。図中では、装置情報管理部６１０を管理部６１０と、装置情報検索部６１１を検索部６１１と略記する。

[0065] 装置情報管理部６１０は、装置情報格納部６２に格納する装置情報を管理する。装置情報管理部６１０は、装置情報格納部６２に装置情報を格納したり、装置情報格納部６２に格納されている装置情報を削除したりする。装置情報検索部６１１は、装置情報格納部６２に格納されている装置情報を検索する。

[0066] 鍵管理部６１２は、鍵情報格納部６３に格納する鍵情報を管理する。鍵検索部６１３は、鍵情報格納部６３に格納されている鍵情報を検索する。

[0067] 使用監視部６１４は、装置情報格納部６２に格納されている装置情報で特定される装置が、鍵情報格納部６３に格納されている鍵情報を使用している

かを監視する。

[0068] サービスプロセッサ１６は、管理端末５０と共に、ストレージ装置１０を管理するための装置として機能する。以下、サービスプロセッサをＳＶＰと略記する。図３などで示すＳＶＰ１６は、鍵管理サーバ６０と通信したり、鍵情報をコントローラ１００に設定したりする。

[0069] ＳＶＰ１６は、例えば、連携部１６１、使用通知部１６２、接続設定部１６３、接続設定格納部１６４、鍵情報設定部１６５、構成設定部１６６、電源管理部１６７、ユーザインターフェース部１６８（以下、ＵＩ部１６８）を備える。

[0070] 連携部１６１は、鍵管理サーバ６０と通信するための機能である。連携部１６１は、鍵管理サーバ６０から接続された場合の認証、および、鍵管理サーバ６０に接続する場合の認証も行う。

[0071] 使用通知部１６２は、ストレージ装置１０での鍵の使用状態を鍵管理サーバ６０に通知する機能である。使用状態には、鍵の使用された時刻（例えば、年月日時分秒の形式で示される時刻）を含めることができる。

[0072] 接続設定部１６３は、鍵管理サーバ６０に接続するための情報を接続設定格納部１６４に保存するための機能である。鍵管理サーバ６０に接続するための情報としては、例えば、ＩＰアドレスや認証情報である。接続設定格納部１６４は、鍵管理サーバ６０に接続するための接続設定情報を保存する記憶領域である。

[0073] 鍵情報設定部１６５は、鍵情報をストレージ装置１０に設定する機能である。構成設定部１６６は、ストレージ装置１０の構成を設定する機能である。構成設定としては、例えば、記憶装置２１の生成および削除、記憶装置２１の暗号化指定、記憶装置２１とホスト３０との対応付けなどがある。

[0074] ＵＩ部１６８は、管理端末５０の有する入力装置および出力装置を用いて、システム管理者（ストレージ管理者）がストレージ装置１０に指示を与えたり、ストレージ装置１０の構成を設定変更したりするための機能である。

[0075] ストレージ装置１０の持つ機能のうち暗号鍵に関する機能を説明する。ス

トレージ装置１０は、暗号鍵に関して、例えば、鍵管理部１０１、鍵テーブル１０２、番号格納部１０３、暗号化／復号化部（暗号化処理部）１０４、記憶装置２１Ａ、２１Ｂを有する。

[0076] 鍵管理部１０１は、ストレージ装置１０で使用する鍵情報を管理したり、検索したりする機能である。鍵情報の管理と鍵情報の検索とを別々の機能として設けてもよい。鍵管理部１０１は、例えばマイクロプロセッサ１４１により実現される。

[0077] 鍵テーブル１０２は、ストレージ装置１０で使用する鍵情報を記憶する。鍵テーブル１０２は、例えばキャッシュメモリ１３２に記憶される。

[0078] 鍵番号格納部１０３は、鍵に対応付けられている鍵番号を格納する記憶領域である。ストレージ装置１０は、鍵管理サーバ６０に鍵番号を示して鍵を要求する。鍵番号格納部１０３は、メモリパッケージ１３の有する記憶領域のうち、不揮発性の記憶領域に設けられている。ストレージ装置１０を再起動した場合に、鍵番号格納部１０３に記憶されている鍵番号に基づいて、鍵管理サーバ６０から鍵を取得する必要があるためである。従って、メモリパッケージ１３に代えて、複数の記憶装置２１のうちの所定の記憶装置２１に、鍵番号を格納する構成でもよい。なお、図中では、鍵番号を番号と略記する。

[0079] 暗号化／復号化部１０４（暗号化処理部１０４）は、鍵を用いてデータを暗号化したり、鍵を用いてデータを復号したりする機能である。暗号化／復号化部１０４は、例えば、バックエンドインターフェース１２に設けられる。

[0080] 電源制御部１０５は、ストレージ装置１０の電源装置（図示せず）の動作を制御する機能である。電源制御部１０５は、ＳＶＰ１６の電源管理部１６７からの指示により、ストレージ装置１０の電源をオフして動作を停止する。電源制御部１０５は、例えば、マイクロプロセッサ１４１により実現される。

[0081] 図３では、使用形態の異なる２種類の記憶装置２１を示している。一方の

記憶装置２１は、暗号化が指定されている暗号化記憶装置２１Ａである。他方の記憶装置２１Ｂは、暗号化が指定されていない通常の記憶装置２１Ｂである。

[0082] 図４は、鍵情報格納部６３に格納される鍵情報の構成例を示す。鍵情報は、鍵毎に、例えば、番号、作成日時、鍵の種別、装置番号、鍵使用状況管理、使用状況最終確認日時、使用有無、鍵データを対応付けて管理する。

[0083] 番号とは、鍵を一意に特定するための識別情報である。作成日時とは、鍵を作成した日時を示す情報である。鍵の種別とは、鍵の種類を示す情報である。装置番号とは、鍵を使用する装置（ストレージ装置）を一意に特定するための識別情報である。鍵使用状況管理とは、鍵の使用状況を管理するか否かを決定するための情報である。使用状況最終確認日時とは、鍵の使用状況を確認した最新日時を示す情報である。使用有無とは、鍵を使用しているか否かを示す情報である。鍵データとは、鍵のデータである。

[0084] 図５は、装置情報格納部６２に格納される装置情報の構成例を示す。装置情報は、装置毎に、例えば、番号、ストレージに接続するための情報、ストレージから接続されるときの情報、ストレージ情報、ストレージへの最終接続情報を対応付けて管理する。

[0085] 番号とは、ストレージ装置１０を一意に特定するための識別情報である。ストレージに接続するための情報とは、鍵管理サーバ６０がストレージ装置１０に接続するために必要な情報であり、例えばＩＰアドレス、ポート番号、クライアント証明書、サーバ証明書などである。ストレージから接続されるときの情報とは、ストレージ装置１０が鍵管理サーバ６０に接続するときに使用する情報であり、例えばクライアント証明書やサーバ証明書である。ストレージ情報とは、ストレージ装置１０についての情報であり、例えば、機種、製造番号である。ストレージへの最終接続日時とは、鍵管理サーバ６０がストレージ装置１０に最後にアクセスした日時、つまり、最新のアクセス日時を示す情報である。

[0086] 図６は、鍵番号格納部１０３に格納されている鍵番号情報の構成例を示す

。鍵番号情報は、ストレージ装置１０が鍵管理サーバ６０から暗号鍵を取得するための番号である。鍵番号情報は、鍵毎に、例えば、ストレージ内鍵番号、鍵管理サーバ番号、鍵管理サーバ内での鍵番号、設定日時、最終確認日時を対応付けて管理する。

[0087] ここで、ストレージ内鍵番号とは、ストレージ装置１０内で鍵を管理するための識別情報である。ストレージ側鍵番号とも呼ぶ。鍵管理サーバ番号とは、鍵管理サーバ６０がストレージ装置１０に接続する場合に使用する情報であり、ストレージ装置１０が鍵管理サーバ６０を識別するための情報である。鍵管理サーバ内での鍵番号とは、鍵管理サーバ６０が鍵を管理するための識別情報である。サーバ側鍵番号とも呼ぶ。設定日時とは、ストレージ装置１０が鍵管理サーバ６０から鍵を取得してストレージ装置１０に設定した日時を示す情報である。最終確認日時とは、鍵管理サーバ６０が鍵の存在を確認した最終日時（つまり最新日時）を示す情報である。

[0088] 図７は、鍵テーブル１０２の構成例を示す説明図である。鍵テーブル１０２は、鍵毎に、例えば、ストレージ内鍵番号と、鍵データとを対応付けて管理する。

[0089] ここで、ストレージ内鍵番号とは、ストレージ装置１０内で鍵を管理するための識別情報である。鍵データとは、鍵番号で特定される鍵のデータである。

[0090] 図８は、接続設定格納部１６４に格納されている、鍵管理サーバへ接続するための設定情報の構成例を示す。接続設定情報は、鍵管理サーバ毎に、例えば、番号と、鍵管理サーバに接続するための情報と、鍵管理サーバから接続されるときの情報とを対応付けて管理する。

[0091] 番号とは、鍵管理サーバ６０を一意に特定するための識別情報である。鍵管理サーバに接続するための情報とは、ストレージ装置１０が鍵管理サーバ６０に接続するときに使用する情報であり、例えば、ＩＰアドレス、通信ポート番号、クライアント証明書、サーバ証明書がある。鍵管理サーバから接続されるときの情報とは、鍵管理サーバ６０がストレージ装置１０に接続す

るときに使用する情報であり、例えば、クライアント証明書、サーバ証明書がある。

[0092] 図９は、暗号鍵を新規に作成する処理を示すフローチャートである。システム管理者は、管理端末５０に表示されるＵＩ部１６８から、ＳＶＰ１６の鍵情報設定部１６５に鍵の生成を要求する（Ｓ１１）。鍵の生成要求は、鍵情報設定部１６５から連携部１６１に送信され（Ｓ１２）、連携部１６１から鍵管理サーバ６０の連携部６５に通信ネットワークＣＮ３を経由して送信される（Ｓ１３）。鍵の生成要求には、要求元のストレージ装置１０を識別するための情報などが含まれている。

[0093] 連携部６５は、鍵の生成要求を鍵管理部６１２に送る（Ｓ１４）。鍵管理部６１２は、装置情報管理部６１０に対して、鍵の生成を要求するストレージ装置１０が鍵管理サーバ６０に接続した日時（最終接続日時）の更新を要求する（Ｓ１５）。この要求を受けた装置情報管理部６１０は、装置情報格納部６２内のデータベースにアクセスして、装置情報を更新する（Ｓ１６）。

[0094] 一方、鍵管理部６１２は、新たな鍵を生成し（Ｓ１７）、その鍵を鍵情報格納部６３内のデータベースに登録する（Ｓ１８）。鍵管理部６１２は、生成した鍵を連携部６５に送る（Ｓ１９）。その鍵は、連携部６５から通信ネットワークＣＮ３を介してストレージ装置１０の連携部１６１に送られる（Ｓ２０）。

[0095] 連携部１６１は、鍵管理サーバ６０から取得した鍵を鍵情報設定部１６５に送る（Ｓ２１）鍵情報設定部１６５は、鍵管理部１０１に引き渡す（Ｓ２２）。鍵管理部１０１は、新規に作成された鍵をストレージ装置１０内で管理するための鍵番号を生成し、その鍵番号を鍵番号格納部１０３内のデータベースに登録する（Ｓ２３）。さらに、鍵管理部１０１は、鍵管理サーバ６０で新規に生成された鍵のデータ（鍵情報）を鍵テーブル１０２に登録する（Ｓ２４）。

[0096] このように、ストレージ装置１０が新たな鍵を必要とする場合、ストレー

ジ装置１０から鍵管理サーバ６０に鍵の生成が要求され、鍵管理サーバ６０で生成された鍵はストレージ装置１０に送信され、ストレージ装置１０に設定される。

[0097] 図１０は、鍵管理サーバ６０がストレージ装置１０での鍵の使用状態を確認する処理を示すフローチャートである。

[0098] 鍵管理サーバ６０の使用監視部６１４は、装置情報管理部６１０を介して装置情報検索部６１１に、装置情報（ストレージ装置の情報）の一覧を要求する（Ｓ３１）。一つの鍵管理サーバ６０は、複数のストレージ装置１０を管理することができる。

[0099] 装置情報検索部６１１は、装置情報格納部６２内のデータベースに記憶されている装置情報を検索することで、装置情報の一覧を取得し（Ｓ３１）、その一覧を使用監視部６１４に送る（Ｓ３３）。

[0100] 使用監視部６１４は、鍵管理サーバ６０で管理しているストレージ装置１０の一覧を装置情報検索部６１１から受領すると、その一覧に記載されている全てのストレージ装置１０に対して、使用中の鍵の鍵番号を問い合わせる（Ｓ３４）。鍵番号の問合せは、連携部６５から通信ネットワークＣＮ３を介して各ストレージ装置１０の連携部１６１に送信される。鍵管理サーバ６０とのやり取りはＳＶＰ１６が担当するが、ストレージ装置１０とＳＶＰ１６とを特に区別しなくともよい。

[0101] ＳＶＰ１６の連携部１６１は、使用監視部６１４から受領した鍵番号の問合せを、使用通知部１６２を介してストレージ装置１０の鍵管理部１０１（検索もできるため、図中では鍵検索と表示）に引き渡す。鍵管理部１０１は、ストレージ装置１０の鍵番号格納部１０３に格納されたデータベースを検索することで、使用している鍵の番号の一覧を取得する（Ｓ３５）。

[0102] 鍵管理サーバ６０の使用監視部６１４は、ストレージ装置１０で使用している鍵番号の一覧を、使用通知部１６２、連携部１６１、通信ネットワークＣＮ３、連携部６５を介して受領する（Ｓ３６）。使用監視部６１４は、鍵管理部６１２に対して、ストレージ装置１０から取得した鍵番号についての

使用状況の最終確認日時を更新するよう、要求する（Ｓ３７）。

[0103] 鍵管理部６１２は、鍵情報格納部６３内のデータベースに格納されている鍵情報について、最終確認日時を更新する（Ｓ３８）。使用状況の最終確認日時が更新された旨は、鍵管理部６１２から使用監視部６１４に通知される。

[0104] このように、鍵管理サーバ６０は、管理下にある各ストレージ装置１０で使用中の鍵番号をＳＶＰ１６を介して全て取得し、鍵情報格納部６３に格納されている鍵情報内の最終確認日時を更新することができる。

[0105] 図１１は、ストレージ装置１０（ＳＶＰ１６）から鍵管理サーバ６０に対して、ストレージ装置１０で使用中の鍵番号を通知する処理を示すフローチャートである。

[0106] ＳＶＰ１６の使用通知部１６２は、ストレージ装置１０の鍵管理部１０１に対し、使用中の鍵を問い合わせる（Ｓ４１）。鍵管理部１０１は、鍵番号格納部１０３に格納されているデータベースを検索することで、使用中の鍵番号の一覧と、鍵を管理している鍵管理サーバ６０のサーバ番号の一覧とを取得する（Ｓ４２）。

[0107] 使用通知部１６２は、鍵番号の一覧と、鍵を管理している鍵管理サーバ６０の番号の一覧とを取得すると（Ｓ４３）、各鍵番号に対応する鍵を管理している鍵管理サーバ毎に、鍵を保持しているか否か問い合わせる。

[0108] 使用通知部１６２は、連携部１６１に対して、鍵管理サーバ６０が鍵を保持しているか調べるよう要求する（Ｓ４４）。連携部１６１は、接続設定格納部１６４に格納されているデータベースを検索することで（Ｓ４５）、鍵管理サーバ６０に接続するための情報を取得する（Ｓ４６）。

[0109] 連携部１６１は、接続設定格納部１６４から取得した接続設定情報を用いて、鍵管理サーバ６０に接続し、鍵管理サーバ６０の連携部６５に対して、ストレージ装置１０で使用中の鍵番号の一覧を通知する（Ｓ４７）。連携部６５は、その鍵番号一覧を使用監視部６１４に渡す。連携部６５から使用監視部６１４に渡される情報には、鍵番号一覧の送信元であるストレージ装置

１０を特定するための情報が含まれている。

[0110] 鍵管理サーバ６０の使用監視部６１４は、装置情報管理部６１０に対して、ストレージ装置１０と接続した日時を更新するよう要求する（Ｓ４８）。装置情報管理部６１０は、装置情報格納部６２に格納されているデータベース内の装置情報について、ストレージ装置との最終接続日時を更新する（Ｓ４９）。なお、本実施例において、日時を更新するとは、現在時刻に更新することを意味する。

[0111] 使用監視部６１４は、鍵管理部６１２に対して、鍵の使用状況の最終確認日時を更新するよう要求する（Ｓ５０）。鍵管理部６１２は、鍵情報格納部６３に格納されているデータベース内の鍵情報について、使用状況の最終確認日時を更新する（Ｓ５１）。使用監視部６１４は、ストレージ装置１０から受領した鍵番号のうち、鍵情報格納部６３に格納されていない未登録の鍵番号を発見した場合、その未登録の鍵番号をＳＶＰ１６の使用通知部１６２に返信する（Ｓ５２）。

[0112] このように、鍵管理サーバ６０からの確認を待たずに、ストレージ装置１０から鍵管理サーバ６０に対して、ストレージ装置１０で使用中の鍵を管理しているか（保持しているか）を確認することができる。そして、鍵管理サーバ６０は、未登録の鍵を発見した場合に、その旨をストレージ装置１０に通知することができる。

[0113] ストレージ装置１０は、ストレージ装置１０で使用している鍵のうち鍵管理サーバ６０で管理されていない鍵が存在することに気づくと、その鍵を鍵管理サーバ６０に登録させることができる。鍵管理サーバ６０で管理されていた鍵がサーバ管理者の誤操作などで削除された場合でも、ストレージ装置１０から鍵を鍵管理サーバ６０に再登録することができるようになっている。なお、以下の説明では、鍵を鍵管理サーバに登録することを、鍵を鍵管理サーバに再登録する、と表現する場合がある。

[0114] 図１２は、ストレージ装置１０が鍵管理サーバ６０に鍵を登録する処理を示すフローチャートである。

[0115] ＳＶＰ１６の使用通知部１６２は、ストレージ装置１０の鍵管理部１０１に対しサーバ側の鍵番号を明示して、登録対象の鍵データの取得を要求する（Ｓ６１）。鍵管理部１０１に明示する鍵番号は、例えば、図１１のステップＳ５２で鍵管理サーバ６０から通知された未登録の鍵番号（鍵管理サーバ内での鍵番号）である。

[0116] 鍵管理部１０１は、使用通知部１６２から受信したサーバ側鍵番号に基づいて、鍵番号格納部１０３に格納されたデータベースを検索することで、ストレージ装置内での鍵番号（ストレージ側鍵番号、または装置側鍵番号）と、それに対応する鍵管理サーバ６０のサーバ番号とを取得する（Ｓ６２）。鍵管理部１０１は、ストレージ側鍵番号に基づいて鍵テーブル１０２を検索し、ストレージ側鍵番号に対応する鍵データを取得し（Ｓ６３）、その鍵データを使用通知部１６２に送信する（Ｓ６４）。

[0117] 使用通知部１６２は、連携部１６１に対して、鍵管理サーバ６０に鍵を登録するよう要求する（Ｓ６５）。この要求には、ステップＳ８４で取得した登録先の鍵管理サーバを特定するためのサーバ番号が含まれている。

[0118] 連携部１６１は、接続設定格納部１６４に格納されたデータベースに対し、鍵の登録先である鍵管理サーバ６０に接続するための情報を問合せ（Ｓ６６）、登録先の鍵管理サーバ６０に接続するための情報を取得する（Ｓ６７）。連携部１６１は、ステップＳ６７で取得した情報を用いて鍵管理サーバ６０に接続し、鍵の再登録を要求する（Ｓ６８）。この再登録要求には、ストレージ側鍵番号と鍵データが含まれている。

[0119] 鍵管理サーバ６０の連携部６５は、ストレージ装置１０のＳＶＰ１６から受領した再登録要求を使用監視部６１４に渡す。使用監視部６１４は、装置情報管理部６１０に対して、ストレージ装置に接続した最終日時の更新を要求する（Ｓ６９）。装置情報管理部６１０は、装置情報格納部６２に格納されているデータベースの装置情報のうち、再登録を要求するストレージ装置に関する装置情報の最終接続日時を更新する（Ｓ７０）。

[0120] 使用監視部６１４は、鍵管理部６１２に対して、鍵の再登録を要求する（

Ｓ７１）。鍵管理部６１２は、鍵情報格納部６３に格納されたデータベースに、ストレージ装置１０から要求された鍵データを登録し（Ｓ７２）、その鍵データに新たに設定されたサーバ側鍵番号を使用通知部１６２に通知する（Ｓ７３）。

[0121] 使用通知部１６２は、ストレージ装置１０の鍵管理部１０１に対して、ステップＳ７３で受領したサーバ側鍵番号の登録を要求する（Ｓ７４）。鍵管理部１０１は、鍵番号格納部１０３に格納されているデータベースに、サーバ番号などと共にサーバ側鍵番号を登録する（Ｓ７５）。

[0122] 図１３は、鍵管理サーバが、再登録の必要な鍵を見つけて鍵情報格納部６３に登録する処理を示すフローチャートである。

[0123] ＳＶＰ１６の使用通知部１６２は、ストレージ装置１０の鍵管理部１０１に対して、ストレージ装置１０で使用している鍵のデータおよび鍵番号を要求する（Ｓ８１）。鍵管理部１０１は、鍵番号格納部１０３に格納されているデータベースを検索し、鍵番号を全て取得する（Ｓ８２）。さらに、鍵管理部１０１は、使用している鍵のデータを鍵テーブル１０２から取得する（Ｓ８３）。鍵管理部１０１は、鍵データおよび鍵番号の一覧を、使用通知部１６２に送る（Ｓ８４）。

[0124] 使用通知部１６２は、連携部１６１に対して、ストレージ装置１０で使用している鍵について鍵管理サーバ６０に通知するよう要求する（Ｓ８５）。連携部１６１は、接続設定格納部１６４に対して、通知先の鍵管理サーバ６０に接続するために使用する情報を問い合わせて（Ｓ８６）、取得する（Ｓ８７）。連携部１６１は、ステップＳ８７で取得した情報を用いて鍵管理サーバ６０に接続し、ストレージ装置１０で使用している鍵の存在と、未登録の鍵を見つけた場合の再登録とを、連携部６５に要求する（Ｓ８８）。この要求には、サーバ側鍵番号および鍵データの一覧が含まれている。

[0125] 鍵管理サーバ６０の使用監視部６１４は、使用通知部１６２からの要求を連携部６５を介して受領すると、装置情報管理部６１０に対して、ストレージ装置１０の最終接続日時の更新を要求する（Ｓ８９）。装置情報管理部６

１０は、装置情報格納部６２に格納されているデータベース内の装置情報のうち、再登録を要求してきたストレージ装置１０に関する装置情報の最終接続日時を更新する（Ｓ９０）。

[0126] 使用監視部６１４は、鍵管理部６１２に対して、鍵の使用状況の最終確認日時を更新するよう要求する（Ｓ９１）。鍵管理部６１２は、鍵情報格納部６３に格納されているデータベース内の鍵情報のうち、再登録要求の発行元のストレージ装置１０に関する鍵情報の最終確認日時を更新する（Ｓ９２）。

[0127] さらに、鍵管理部６１２は、ストレージ装置１０から受領したサーバ側鍵番号のうち、鍵情報格納部６３に登録されていないサーバ側鍵番号を検出すると、そのサーバ側鍵番号に対応する鍵データを鍵情報格納部６３に格納する（Ｓ９３）。鍵管理部６１２は、登録した鍵データに設定されるサーバ側鍵番号を、使用監視部６１４、連携部６５、連携部１６１などを介して、ＳＶＰ１６の使用通知部１６２に通知する（Ｓ９４）。

[0128] 使用通知部１６２は、ストレージ装置１０の鍵管理部１０１に対して、サーバ側鍵番号を登録するよう要求する（Ｓ９５）。鍵管理部１０１は、鍵番号格納部１０３に格納されているデータベースにサーバ側鍵番号を登録する（Ｓ９６）。

[0129] このようにして、ストレージ装置１０で使用している鍵の鍵番号および鍵データを全て鍵管理サーバ６０に送信し、鍵管理サーバ６０が未登録の鍵を検出して登録するように構成することもできる。

[0130] 図１１および図１２に示すフローチャートでは、ストレージ装置１０が、鍵管理サーバ６０に登録されていない鍵を検出し、未登録の鍵データを鍵管理サーバ６０に送信して登録させる。従って、未登録の鍵を検出するまでの処理時間と、未登録の鍵を登録するための処理時間とがかかる。その一方、ストレージ装置１０から鍵管理サーバ６０には、未登録の鍵についてのみ鍵番号および鍵データを送信すればよいため、通信ネットワークＣＮ３の通信負荷を軽減することができる。

[0131] これに対し、図１２に示すフローチャートでは、ストレージ装置１０は全ての鍵についての情報を鍵管理サーバ６０に送りつけ、鍵管理サーバ６０が未登録の鍵を検出して再登録するようになっている。従って、未登録の鍵を比較的簡単に鍵管理サーバ６０に登録することができる。一方、ストレージ装置１０から鍵管理サーバ６０に全ての鍵の鍵番号および鍵データを送信するため、通信ネットワークＣＮ３の通信負荷が増大する。

[0132] 図１４は、ストレージ装置１０の電源オフ（動作停止）が指示された場合の処理を示すフローチャートである。

[0133] システム管理者（ストレージ管理者）は、管理端末５０からＳＶＰ１６の電源管理部１６７に対して、電源オフを指示することができる。電源オフとは、ストレージ装置１０内の各パッケージ１１、１２、１３，１４、１５への電源装置からの給電を停止することを意味する。なお、電源をオフした場合でも、メモリパッケージ１３内の不揮発性記憶領域を内蔵電池でバックアップしたり、再起動信号などを受け付けるために必要な回路に最低限の給電を行ったりしてもよい。

[0134] 電源管理部１６７は、電源オフ指示を受領すると、使用通知部１６２に対して、ストレージ装置１０で使用している鍵が鍵管理サーバ６０に登録されているかチェックするよう要求する（Ｓ１０１）。

[0135] 使用通知部１６２は、ストレージ装置１０の鍵管理部１０１に、ストレージ装置１０で使用している鍵について、そのサーバ側鍵番号および鍵管理サーバ６０のサーバ番号の一覧を問い合わせる（Ｓ１０２）。

[0136] 鍵管理部１０１は、鍵番号格納部１０３に格納されているデータベースから、ストレージ装置１０で使用している鍵についての、サーバ側鍵番号と鍵管理サーバ６０のサーバ番号とを取得する（Ｓ１０３）。

[0137] 使用通知部１６２は、サーバ側鍵番号およびサーバ番号を鍵管理部１０１から受け取ると（Ｓ１０４）、連携部１６１に対して、ストレージ装置１０で使用している鍵について鍵管理サーバ６０に通知するよう要求する（Ｓ１０５）。連携部１６１は、接続設定格納部１６４に対して、通知先の鍵管理

サーバ６０に接続するために使用する情報を問い合わせて（Ｓ１０６）、取得する（Ｓ１０７）。連携部１６１は、ステップＳ１０７で取得した情報を用いて鍵管理サーバ６０に接続し、ストレージ装置１０で使用している鍵について通知する（Ｓ１０８）。

[0138] 鍵管理サーバ６０の使用監視部６１４は、ＳＶＰ１６からの通知を連携部６５を介して受領すると、装置情報管理部６１０に対して、ストレージ装置１０の最終確認日時を更新するよう要求する（Ｓ１０９）。装置情報管理部６１０は、装置情報格納部６２に格納されている装置情報のうち、通知元のストレージ装置１０に対応する装置情報の最終確認日時を更新する（Ｓ１１０）。

[0139] 使用監視部６１４は、鍵の使用状況の最終確認日時を更新するよう鍵管理部６１２に要求する（Ｓ１１１）。鍵管理部６１２は、鍵情報格納部６３に格納されているデータベース内の鍵情報のうち、ＳＶＰ１６から通知されたサーバ側鍵番号に対応する鍵情報の使用状況の最終確認日時を更新する（Ｓ１１２）。鍵管理部６１２は、ＳＶＰ１６から通知されたサーバ側鍵番号のうち、鍵情報格納部６３のデータベースに登録されていないサーバ側鍵番号を検出した場合は、その未登録のサーバ側鍵番号をＳＶＰ１６の電源管理部１６７に返信する（Ｓ１１３）。

[0140] 電源管理部１６７は、ストレージ装置１０で使用している鍵の全てが鍵管理サーバ６０で管理されているか判定する。電源管理部１６７は、全ての鍵管理サーバ６０で管理されていると判定した場合、ストレージ装置１０の電源制御部１０５に対して、電源オフを指示する（Ｓ１１４）。電源制御部１０５は、その指示に従ってストレージ装置１０の各パッケージへの給電を停止するための停止シーケンスを開始する。

[0141] これに対し、電源管理部１６７は、ストレージ装置１０で使用している鍵のうちいずれか一つでも鍵管理サーバ６０に管理されていないと判定すると、その旨を知らせるための警告を管理端末５０の画面に出力する（Ｓ１１５）。

[0142] この場合、電源管理部１６７は、電源制御部１０５に電源オフを指示しない。さらに、電源管理部１６７は、警告出力に続けて、または警告出力と共に、鍵管理サーバ６０に管理されていない未登録の鍵を鍵管理サーバ６０に再登録するための処理（図１２参照）を自動的に実行することができる。電源管理部１６７は、システム管理者による鍵の再登録についての許可が管理端末５０から入力された場合に、鍵を鍵管理サーバ６０に再登録する処理を実行してもよい。

[0143] このように、ストレージ装置１０の電源オフが指示された場合、ストレージ装置１０で使用している鍵の全てを鍵管理サーバ６０で管理しているか確認し、いずれか一つの鍵でも鍵管理サーバ６０で管理していないと判定したときは、電源をオフしない。ストレージ装置１０で使用する全ての鍵が鍵管理サーバ６０に管理されていることを確認した場合に、ストレージ装置１０の電源をオフにする。

[0144] 従って、ストレージ装置１０で使用している鍵がストレージシステムから消失するのを未然に防止して、信頼性および安全性を向上できる。また、鍵管理サーバ６０で管理されていない未登録の鍵が検出された場合は、その旨をシステム管理者に通知することができるため、システム管理者の管理作業の効率および使い勝手が向上する。さらに、未登録の鍵を検出した場合は、自動的にまたは手動で、未登録の鍵を鍵管理サーバ６０に登録することができる。従って、管理作業の効率および使い勝手がさらに向上する。

[0145] 図１５は、鍵管理サーバ６０に対して鍵の削除が指示された場合の処理を示すフローチャートである。

[0146] システム管理者（サーバ管理者）は、鍵管理サーバ６０の閲覧／編集部６４を用いて、鍵の削除を指示することができる（Ｓ１２１）。閲覧／編集部６４は、鍵管理部６１２に対して、鍵の使用状況を問い合わせる（Ｓ１２２）。鍵管理部６１２は、鍵情報格納部６３に格納されたデータベースから、削除対象として指定された鍵の使用状況を最後に確認した最終確認日時を取得する（Ｓ１２３）。

[0147] 閲覧／編集部６４は、削除対象の鍵の使用状況の最終確認日時に基づき、その鍵が、予め設定された所定時間以上、存在が確認されていないか判定する（Ｓ１２４）。換言すれば、閲覧／編集部６４は、削除対象の鍵が所定の削除禁止期間以上、使用されていないか判定する。

[0148] 閲覧／編集部６４は、削除対象の鍵が所定時間以上、その存在が確認されていないと判定すると、鍵管理部６１２にその鍵の削除を指示する（Ｓ１２５）。所定時間以上その存在を確認していない鍵は、使用されていないと判断できるためである。そこで、鍵管理部６１２は、指定された鍵の情報を鍵情報格納部６３のデータベースから削除する（Ｓ１２６）。これに対し、閲覧／編集部６４は、削除対象の鍵が所定時間内に存在が確認されていると判定すると、鍵管理部６１２に削除を指示しない。

[0149] このように、システム管理者が鍵管理サーバ６０に鍵の削除を指示した場合、その鍵がストレージ装置１０で使用されているか判定し、使用していると判定したときは削除せず、使用していないと判定したときは削除する。これにより、ストレージ装置１０で使用されている鍵がシステム管理者の誤操作などで削除されるのを防止できる。

[0150] このように構成される本実施例によれば、鍵が必要とされる限り、その鍵を鍵管理サーバ６０で管理させ続けることができる。本実施例では、ストレージ装置１０の電源をオフする前に、使用中の全ての鍵が鍵管理サーバ６０で管理されているか確認し、確認できたときに電源をオフする。未登録の鍵（管理されていない鍵）を検出すると、ストレージ装置の電源をオフせず、未登録の鍵を鍵管理サーバ６０に送って再登録させる。従って、本実施例によれば、ストレージ装置１０とは別の鍵管理サーバ６０で鍵を管理し、かつ、使用中の鍵の喪失を防止するため、セキュリティ性、信頼性、管理作業の効率および使い勝手を向上することができる。

[0151] さらに本実施例によれば、鍵管理サーバ６０は、ストレージ装置１０で使用されている鍵を削除しないため、信頼性、管理作業の安全性を向上できる。

実施例 2

[0152] 図１６、図１７を用いて第２実施例を説明する。本実施例を含む以下の各実施例は、第１実施例の変形例に相当するため、第１実施例との相違を中心に説明する。本実施例では、通信不能な鍵管理サーバが有る場合に、他の鍵管理サーバにストレージ装置で使用している鍵を登録する。

[0153] 図１６は、ストレージ装置１０の電源オフ（動作停止）が指示された場合の処理を示すフローチャートである。

[0154] 電源管理部１６７は、電源オフ指示を受領すると、使用通知部１６２に対して、ストレージ装置１０で使用している鍵が鍵管理サーバ６０に登録されているかチェックするよう要求する（Ｓ１３１）。

[0155] 使用通知部１６２は、ストレージ装置１０の鍵管理部１０１に、ストレージ装置１０で使用している鍵について、そのサーバ側鍵番号と鍵管理サーバ６０のサーバ番号とを問い合わせる（Ｓ１３２）。

[0156] 鍵管理部１０１は、鍵番号格納部１０３に格納されているデータベースから、ストレージ装置１０で使用している鍵についての、サーバ側鍵番号および鍵管理サーバ６０のサーバ番号の一覧を取得する（Ｓ１３３）。さらに、鍵管理部１０１は、鍵テーブル１０２から、使用している鍵のデータを取得する（Ｓ１３４）。

[0157] 使用通知部１６２は、サーバ側鍵番号およびサーバ番号の一覧と全ての鍵データとを鍵管理部１０１から受け取ると（Ｓ１３５）、連携部１６１に対して、ストレージ装置１０で使用している鍵について鍵管理サーバ６０に通知するよう要求する（Ｓ１３６）。連携部１６１は、接続設定格納部１６４に対して、通知先の鍵管理サーバ６０に接続するために使用する情報を問い合わせて、取得する（Ｓ１３７）。

[0158] 連携部１６１は、ステップＳ１３７で取得した情報を用いて鍵管理サーバ６０に接続し、ストレージ装置１０で使用している鍵について通知しようとするが、その通信に失敗したとする（Ｓ１３８）。つまり、ストレージ装置１０のＳＶＰ１６は、本来の通知先である鍵管理サーバ６０に接続できなか

ったと仮定する。例えば、通知先の鍵管理サーバ６０が保守作業または障害などで停止している場合、その鍵管理サーバ６０にストレージ装置１０で使用している鍵について通知することはできない。

[0159] 連携部１６１は、所定の鍵管理サーバ（通知先の鍵管理サーバ）６０への通知に失敗すると、他の鍵管理サーバ６０を通知先として選択し、選択した他の鍵管理サーバ６０に接続するための情報を接続設定格納部１６４から取得する（Ｓ１３９）。連携部１６１は、他の鍵管理サーバ６０に接続して、鍵の登録を要求する（Ｓ１４０）。

[0160] 他の鍵管理サーバ６０の連携部６５が鍵の登録要求を受領すると、鍵管理部６１２は、受信した鍵データを鍵情報格納部６３のデータベースに格納する（Ｓ１４１）。鍵管理部６１２は、鍵情報格納部６３に登録した鍵データのそれぞれに新たなサーバ側鍵番号を付与し、それらサーバ側鍵番号をＳＶＰ１６に返信する（Ｓ１４２）。電源管理部１６７は、サーバ側鍵番号を使用通知部１６２を介して受領する。

[0161] なお、図示は省略するが、他の鍵管理サーバ６０の装置情報管理部６１０は、鍵データの送信元であるストレージ装置１０の情報を、装置情報格納部６２のデータベースに登録する。

[0162] 図１７に移る。電源管理部１６７は、ストレージ装置１０の鍵管理部１０１に対して、サーバ側鍵番号と他の鍵管理サーバ６０のサーバ番号とを送り、鍵番号格納部１０３のデータベースを更新するよう要求する。鍵管理部１０１は、鍵番号格納部１０３のデータベースを更新する（Ｓ１４４）。

[0163] 電源管理部１６７は、ストレージ装置１０で使用している鍵が他の鍵管理サーバ６０に登録されたことを確認すると、電源制御部１０５に対して電源をオフするよう指示する（Ｓ１４５）。電源制御部１０５は、その指示に従ってストレージ装置１０の各パッケージへの給電を停止するための停止シーケンスを開始する。

[0164] このように構成される本実施例も第１実施例と同様の作用効果を得ることができる。さらに、本実施例では、本来の鍵管理サーバ６０を利用できない

場合に、他の鍵管理サーバ６０にストレージ装置１０で使用している鍵を登録する。従って、ストレージシステムの信頼性、堅牢性がさらに向上する。

実施例 3

[0165] 図１８を用いて第３実施例を説明する。本実施例では、ストレージ装置１０の電源オフが指示された場合に、ストレージ装置１０内の情報で電源オフの可否を判定する。

[0166] 図１８は、ストレージ装置１０に電源オフが指示された場合の処理を示すフローチャートである。ＳＶＰ１６の電源管理部１６７は、ＵＩ部１６８を介してシステム管理者から電源オフが指示されると、ストレージ装置１０の鍵管理部１０１に対して、鍵管理サーバ６０が鍵の使用状況を最後に確認した日時を転送するよう要求する（Ｓ１５１）。鍵管理部１０１は、鍵番号格納部１０３に格納されたデータベースから、鍵管理サーバ６０が鍵の使用状況を最後に確認した日時を取得し（Ｓ１５２）、その確認日時リストを電源管理部１６７に返信する。

[0167] 電源管理部１６７は、鍵管理サーバ６０による鍵の使用状況の最終確認日時のリストに基づいて、ストレージ装置１０で使用している全ての鍵が所定時間内に確認されているか判定する（Ｓ１５３）。

[0168] 電源管理部１６７は、ストレージ装置１０で管理している全ての鍵の存在が所定時間内に鍵管理サーバ６０により確認されていると判定すると、電源制御部１０５に電源オフを指示する（Ｓ１５４）。鍵管理サーバ６０は、所定時間内に全ての鍵の存在を確認しているため、鍵管理サーバ６０は全ての鍵を管理していると推定することができる。

[0169] これに対し、電源管理部１６７は、ストレージ装置１０で管理している鍵のうちいずれか一つでも、その存在が所定時間以上鍵管理サーバ６０により確認されていない鍵があると判定すると、警告を通知する（Ｓ１５５）。鍵管理サーバ６０が所定時間以上その存在を確認していない鍵は、鍵管理サーバ６０に管理されていない、つまり、鍵管理サーバ６０に登録されていないと判定できる。そこで、電源管理部１６７は、システム管理者（ストレージ

管理者）に、鍵管理サーバ６０で管理されておらず、ストレージ装置１０にのみ保持されている鍵が有ることを通知する。電源管理部１６７は、電源制御部１０５に電源オフを指示しない。

[0170] この後、システム管理者からの手動指示により、または自動的に、上述した鍵の再登録処理を行うことで、ストレージ装置１０で使用している全ての鍵が鍵管理サーバ６０に登録される。全ての鍵を鍵管理サーバ６０で保持したことを確認した後に、電源管理部１６７は電源制御部１０５にストレージ装置１０の電源をオフするよう指示する。

[0171] このように構成される本実施例も第１実施例と同様の作用効果を奏する。さらに、本実施例では、ストレージ装置１０の電源をオフする際に、ストレージ装置１０内で保持されている情報（鍵の使用状況の最終確認日時）に基づいて、電源オフの可否を判定することができる。従って、本実施例によれば、全ての鍵を管理しているか否かを鍵管理サーバ６０に問い合わせる必要がなく、ストレージ装置１０のみで電源オフの可否を判定し、電源をオフすることができる。この結果、ストレージシステムの信頼性を維持しつつ、より簡易な方法でストレージ装置１０の電源をオフすることができ、使い勝手が向上する。

実施例 4

[0172] 図１９を用いて第４実施例を説明する。本実施例では、鍵の管理について、ストレージ装置１０の動作、および鍵管理サーバ６０の動作を事前に設定する。鍵管理サーバ６０とストレージ装置１０とは物理的に別々の装置として構成され、物理的に離れて設置されているため、暗号鍵に関する信頼性を向上するための動作をそれぞれ別々に設定することができる。

[0173] 図１９に示すポリシー設定処理には、ストレージ装置１０の動作を規定するためのストレージ側ポリシーの設定（Ｓ１６１～Ｓ１６４）と、鍵管理サーバ６０の動作を規定するためのサーバ側ポリシーの設定（Ｓ１６５～Ｓ１６７）とが示されている。

[0174] ストレージ側ポリシーの設定について先に説明する。ストレージ装置１０

へのポリシー設定は、システム管理者（ストレージ管理者）が管理端末５０からＵＩ部１６８を介して行うことができる。

[0175] ストレージ装置１０のＳＶＰ１６は、ストレージ装置１０が主導して鍵管理サーバ６０に鍵を再登録することが許可されたか判定する（Ｓ１６１）。ストレージ装置１０が主導する鍵の再登録処理とは、例えば、図１２で述べたように、鍵管理サーバ６０で管理していない未登録の鍵を、ストレージ装置１０から鍵管理サーバ６０に送信して登録させる処理である。

[0176] ＳＶＰ１６は、ストレージ装置１０の主導による鍵の再登録処理が許可されたと判定すると（Ｓ１６１：ＹＥＳ）、使用通知部１６２対して、鍵管理サーバ６０への鍵の再登録を許可する（Ｓ１６２）。

[0177] 次に、ＳＶＰ１６は、使用通知部１６２に対して、本来の鍵管理サーバ６０への鍵登録ができない場合に、他の鍵管理サーバ６０への鍵の登録を許可する（Ｓ１６３）。この処理については図１６で述べた。

[0178] 最後に、ＳＶＰ１６は、ストレージ装置１０で使用している全ての鍵のうちいずれか一つでも鍵管理サーバ６０が管理していない場合、ストレージ装置１０の電源をオフしないよう、電源管理部１６７に設定する（Ｓ１６４）。なお、ＳＶＰ１６は、ストレージ装置１０から鍵管理サーバ６０への鍵の再登録が許可されていない場合（Ｓ１６１：ＮＯ）、ステップＳ１６２、Ｓ１６３をスキップし、ステップＳ１６４に移る。

[0179] サーバ側ポリシーの設定を説明する。システム管理者（サーバ管理者）は、図外の端末を用いて、鍵管理サーバ６０の動作を設定することができる。

[0180] 鍵管理サーバ６０は、ストレージ装置１０が使用している鍵を鍵管理サーバ６０の主導で登録することが許可されたか判定する（Ｓ１６５）。鍵管理サーバ６０の主導による鍵の再登録処理とは、例えば、図１３で述べた処理である。鍵管理サーバ６０は、ストレージ装置１０から全ての鍵のデータを事前に受領し、その中から未登録の鍵だけ鍵管理サーバ６０に登録する。

[0181] 鍵管理サーバ６０は、鍵管理サーバ６０による鍵の再登録が許可されたと判定すると（Ｓ１６５：ＹＥＳ）、使用監視部６１４に鍵の再登録を許可す

る（Ｓ１６６）。そして、鍵管理サーバ６０は、ストレージ装置１０で使用中の鍵の削除が指示された場合は、その削除指示を行わないよう設定する（Ｓ１６７）。なお、ステップＳ１６５でＮＯと判定された場合は、ステップＳ１６６をスキップして、Ｓ１６７に移る。

[0182] このように構成される本実施例も第１実施例と同様の作用効果を奏する。さらに、本実施例では、ストレージ装置１０と鍵管理サーバ６０の、鍵の管理に関する動作を、例えば必要性や使用目的などに応じて設定することができる。このため、本実施例では、使い勝手がさらに向上する。

実施例 5

[0183] 図２０を用いて第５実施例を説明する。本実施例では、鍵管理サーバ６０で管理している鍵の削除が指示された場合に、削除対象の鍵の使用状況をストレージ装置１０に問い合わせる。

[0184] システム管理者（サーバ管理者）が閲覧／編集部６４を介して鍵の削除を指示すると（Ｓ１７１）、鍵管理部６１２は連携部６５を介して、ストレージ装置１０に対し、削除対象の鍵について問い合わせる（Ｓ１７２）。

[0185] ストレージ装置１０の鍵管理部１０１は、鍵管理サーバ６０からの問合せを連携部１６１および使用通知部１６２などを介して受領すると、鍵番号格納部１０３のデータベースから、削除対象の鍵についての、サーバ側鍵番号と使用状況の最終確認時刻とを取得する（Ｓ１７３）。

[0186] 鍵管理サーバ６０の鍵管理部６１２は、ストレージ装置１０の鍵管理部１０１から、削除対象の鍵についてのサーバ側鍵番号および最終確認日時を取得する際に、通信が正常に行われたか判定する（Ｓ１７４）。

[0187] 鍵管理サーバ６０の鍵管理部６１２は、ストレージ装置１０との通信が正常ではないと判定すると（Ｓ１７４：ＮＯ）、鍵の削除を禁止する（Ｓ１７７）。

[0188] 鍵管理部６１２は、ストレージ装置１０との通信が正常な場合（Ｓ１７４：ＹＥＳ）、削除対象の鍵の最終確認日時に基づいて、その鍵の存在を所定時間内に確認したか判定する（Ｓ１７５）。鍵管理部６１２は、削除対象の

鍵の存在を所定時間以上確認していないと判定すると（Ｓ１７５：ＮＯ）、その鍵を鍵情報格納部６３のデータベースから削除する（Ｓ１７６）。

[0189] このように構成される本実施例も第１実施例と同様の作用効果を奏する。さらに本実施例では、鍵を削除する場合に、ストレージ装置１０での最新の使用状況を確認するため、図１５に示す処理よりも安全に鍵を削除することができる。

実施例 6

[0190] 図２１を用いて第６実施例を説明する。本実施例では、鍵の寿命を予め設定しておき、削除が指示されたときには、ストレージ装置１０での使用状況と鍵の寿命との両方を考慮する。

[0191] 図２１は、鍵管理サーバ６０で管理している鍵の削除が指示された場合の処理を示すフローチャートである。

[0192] システム管理者（サーバ管理者）は、鍵管理サーバ６０の閲覧／編集部６４を用いて、鍵の削除を指示する（Ｓ１８１）。閲覧／編集部６４は、鍵管理部６１２に対して、鍵の使用状況を問い合わせる（Ｓ１８２）。鍵管理部６１２は、鍵情報格納部６３に格納されたデータベースから、削除対象として指定された鍵の使用状況を最後に確認した最終確認日時を取得する（Ｓ１８３）。

[0193] 閲覧／編集部６４は、削除対象の鍵の使用状況の最終確認日時に基づき、その鍵が、予め設定された所定時間以上、存在が確認されていないか判定する（Ｓ１８４）。さらに、閲覧／編集部６４は、削除対象の鍵に設定されている寿命が切れているか確認する（Ｓ１８５）。鍵管理サーバ６０は、鍵を生成するときに、その鍵の有効期間を示す寿命を設定することができる。

[0194] 閲覧／編集部６４は、削除対象の鍵の存在が所定時間以上確認されておらず、かつ、その鍵の寿命が切れていると判定すると、鍵管理部６１２にその鍵の削除を指示する（Ｓ１８６）。鍵管理部６１２は、指定された鍵の情報を鍵情報格納部６３のデータベースから削除する（Ｓ１８７）。閲覧／編集部６４は、削除対象の鍵の存在が所定時間内に確認されている場合、または

、鍵の寿命が残っている場合のいずれかの場合、鍵管理部６１２に削除を指示しない。

[0195] このように構成される本実施例も第１実施例と同様の作用効果を奏する。さらに本実施例では、鍵の寿命（有効期間）も考慮して削除するため、より安全に鍵を削除することができる。

[0196] なお、本発明は、上述した各実施例に限定されない。当業者であれば、本発明の範囲内で、種々の追加や変更等を行うことができる。例えば、上述された本発明の技術的特徴は、適宜結合させて実施することができる。

[0197] 例えば、本発明は以下のように情報処理システムまたはストレージシステムとして表現することもできる。

[0198] 表現１．

鍵情報を管理する第１装置と、

前記第１装置と双方向通信可能に接続され、前記管理装置で管理される前記鍵情報を使用する第２装置とを備える情報処理システムであって、

前記第２装置は、

前記第１装置から前記鍵情報を取得し、

前記鍵情報を揮発性記憶領域に記憶し、

前記鍵情報を用いて所定のデータ処理を行い、

動作停止が指示された場合は、前記鍵情報が前記第１装置で管理されているかを判定し、

前記鍵情報が前記第１装置で管理されていると判定した場合は動作を停止し、

前記鍵情報が前記第１装置で管理されていないと判定した場合は動作を停止しない、情報処理システム。

表現２．

前記第２装置は、前記鍵情報が前記第１装置で管理されていないと判定した場合に、その旨の通知を出力する、

表現１に情報処理システム。

表現３．

前記第２装置は、前記鍵情報が前記第１装置で管理されていないと判定した場合に、前記鍵情報を前記第１装置に送信して登録させる、

表現１または２のいずれかに記載の情報処理システム。

符号の説明

[0199] １：鍵、１０：ストレージ装置、２１：記憶装置、３０：ホストコンピュータ、５０：管理端末、６０：鍵管理サーバ

請求の範囲

[請求項1] 鍵情報を管理する管理サーバと通信可能に接続されるストレージ装置であって、

記憶装置と、

前記記憶装置を制御するコントローラとを備え、

前記コントローラは、

前記記憶装置に入出力するデータを前記鍵情報を用いて暗号化処理するようになっており、

動作停止が指示されると、当該コントローラで使用している鍵情報が前記管理サーバで管理されているか判定し、

前記鍵情報が前記管理サーバで管理されていると判定した場合は動作を停止し、前記鍵情報が前記管理サーバで管理されていないと判定した場合は動作を停止しない、

ストレージ装置。

[請求項2] 前記コントローラは、前記鍵情報が前記管理サーバで管理されていないと判定した場合に、その旨の通知を出力する、

請求項１に記載のストレージ装置。

[請求項3] 前記コントローラは、前記鍵情報が前記管理サーバで管理されていないと判定した場合に、前記管理サーバに前記鍵情報を登録するか確認するための通知を出力する、

請求項２に記載のストレージ装置。

[請求項4] 前記コントローラは、前記管理サーバへの前記鍵情報の登録が許可された場合に、前記鍵情報を前記管理サーバに送信して登録させる、

請求項３に記載のストレージ装置。

[請求項5] 前記コントローラは、前記鍵情報が前記管理サーバで管理されていないと判定した場合に、前記鍵情報を前記管理サーバに送信して登録させる、
請求項１に記載のストレージ装置。

[請求項6] 前記コントローラは、前記鍵情報を前記管理サーバが登録したことを確認してから、動作を停止する、
請求項５に記載のストレージ装置。

[請求項7] 前記コントローラは、前記管理サーバで管理されていないと判定した前記鍵情報を含む全ての鍵情報を前記管理サーバに送信することで、前記管理サーバにより、前記全ての鍵情報のうち前記管理サーバで管理していない前記鍵情報のみを当該管理サーバに登録させ、前記管理サーバが前記鍵情報を登録したことを確認してから動作を停止する、
請求項６に記載のストレージ装置。

[請求項8] 前記コントローラは、前記鍵情報を前記管理サーバに送信して登録させることができなかった場合に、予め設定されている他の管理サーバを選択し、選択した前記他の管理サーバに全ての鍵情報を送信して登録させ、前記他の管理サーバが前記全ての鍵情報を登録したことを確認してから動作を停止する、
請求項７に記載のストレージ装置。

[請求項9] 前記コントローラは、当該コントローラで使用している鍵情報を前記管理サーバが確認したときの時刻を示す鍵確認情報を保持しており、前記鍵確認情報に記録された確認時刻と現在時刻との差異が所定時間内である鍵情報は前記管理サーバで管理されていると判定し、動作

を停止する、
請求項１に記載のストレージ装置。

[請求項10] 前記コントローラは、前記管理サーバで管理している鍵情報のいずれかの削除が当該管理サーバに対して指示された場合に、前記コントローラで使用している鍵情報を前記管理サーバが削除しないように、前記コントローラが使用している鍵情報に関する情報を前記管理サーバに送信する、
請求項１に記載のストレージ装置。

[請求項11] 鍵情報を管理する管理サーバと通信可能に接続されるストレージ装置を制御するための方法であって、
記憶装置に入出力するデータを鍵情報を用いて暗号化処理し、
動作停止が指示されたか判定し、
前記動作停止が指示されたと判定した場合は、前記ストレージ装置で使用している鍵情報が前記管理サーバで管理されているか判定し、
前記鍵情報が前記管理サーバで管理されていると判定した場合は動作を停止し、前記鍵情報が前記管理サーバで管理されていないと判定した場合は動作を停止しない、
ストレージ装置の制御方法。

[請求項12] 前記鍵情報が前記管理サーバで管理されていないと判定した場合は、動作を停止せず、かつ、前記鍵情報が前記管理サーバで管理されていない旨の通知を出力する、
請求項１１に記載のストレージ装置の制御方法。

[請求項13] 前記通知には、前記管理サーバに前記鍵情報を登録するか確認するための通知も含まれている、

請求項１２に記載のストレージ装置の制御方法。

［請求項14］　前記鍵情報が前記管理サーバで管理されていないと判定した場合は、前記鍵情報を前記管理サーバに送信して登録させる、
請求項１１に記載のストレージ装置の制御方法。

[図1]

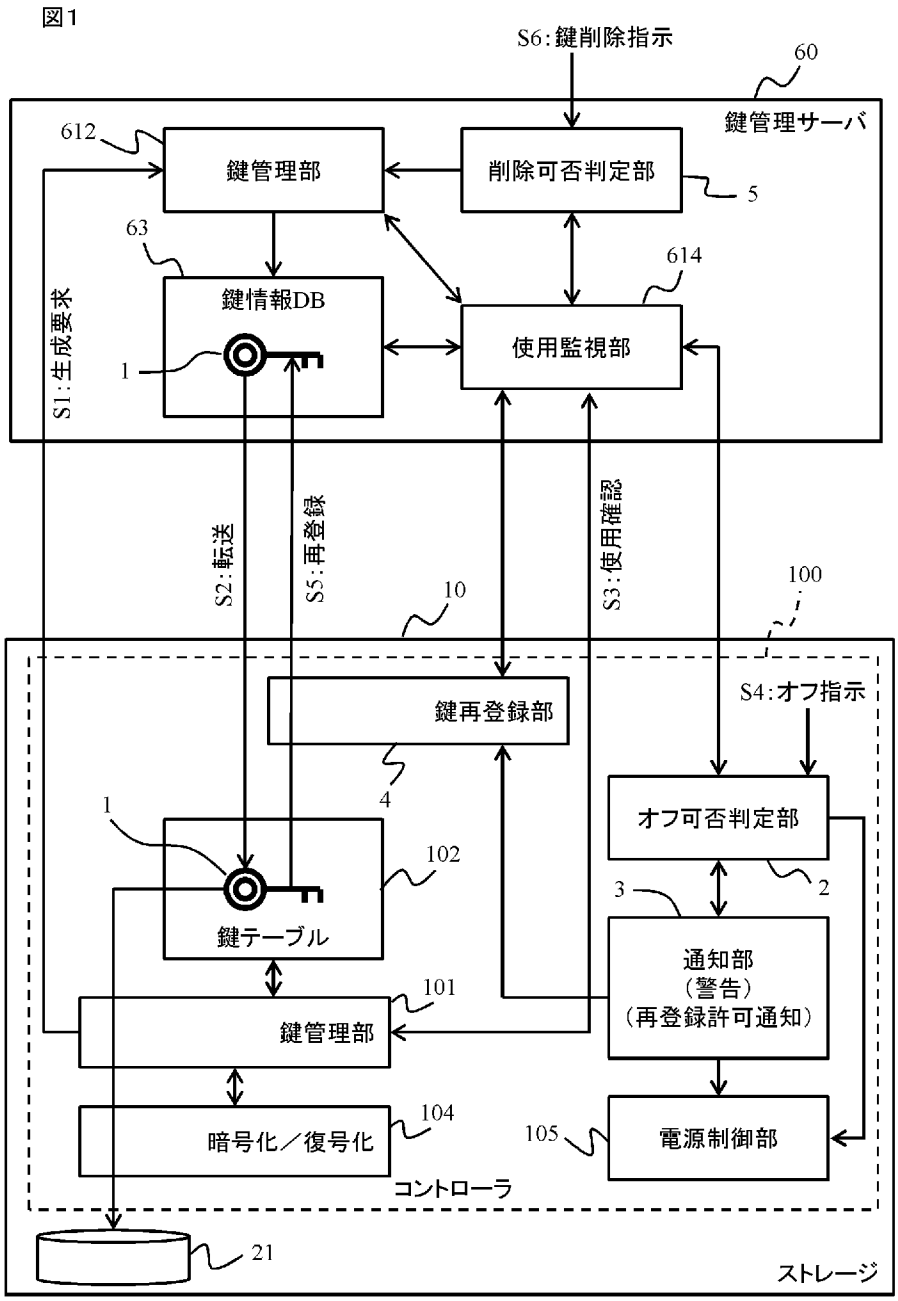
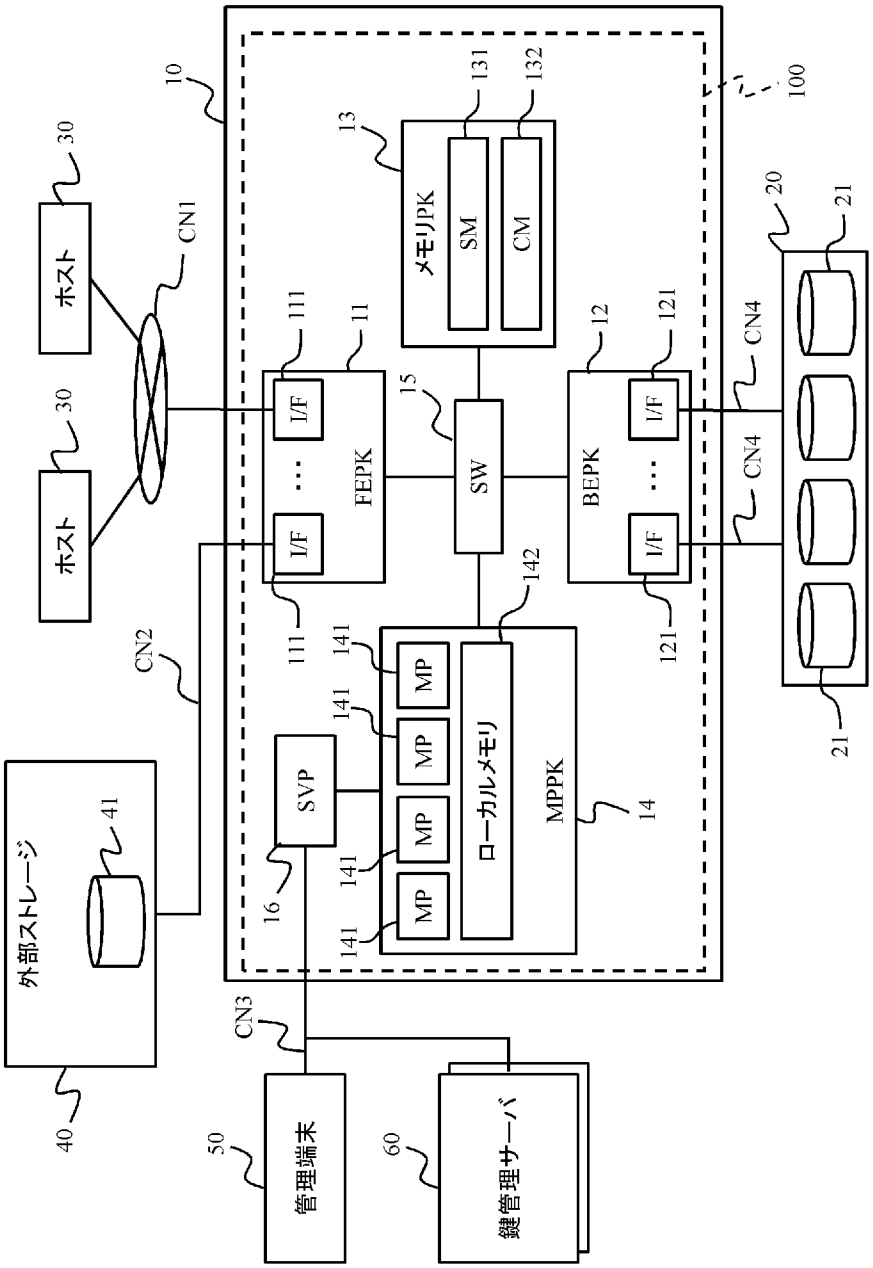


図1
S6:鍵削除指示
60
鍵管理サーバ
612
鍵管理部
削除可否判定部
5
63
鍵情報DB
614
使用監視部
1
S1:生成要求
S2:転送
S5:再登録
S3:使用確認
10
100
S4:オフ指示
鍵再登録部
4
1
102
オフ可否判定部
2
3
鍵テーブル
通知部
(警告)
(再登録許可通知)
101
鍵管理部
104
暗号化／復号化
105
電源制御部
コントローラ
21
ストレージ

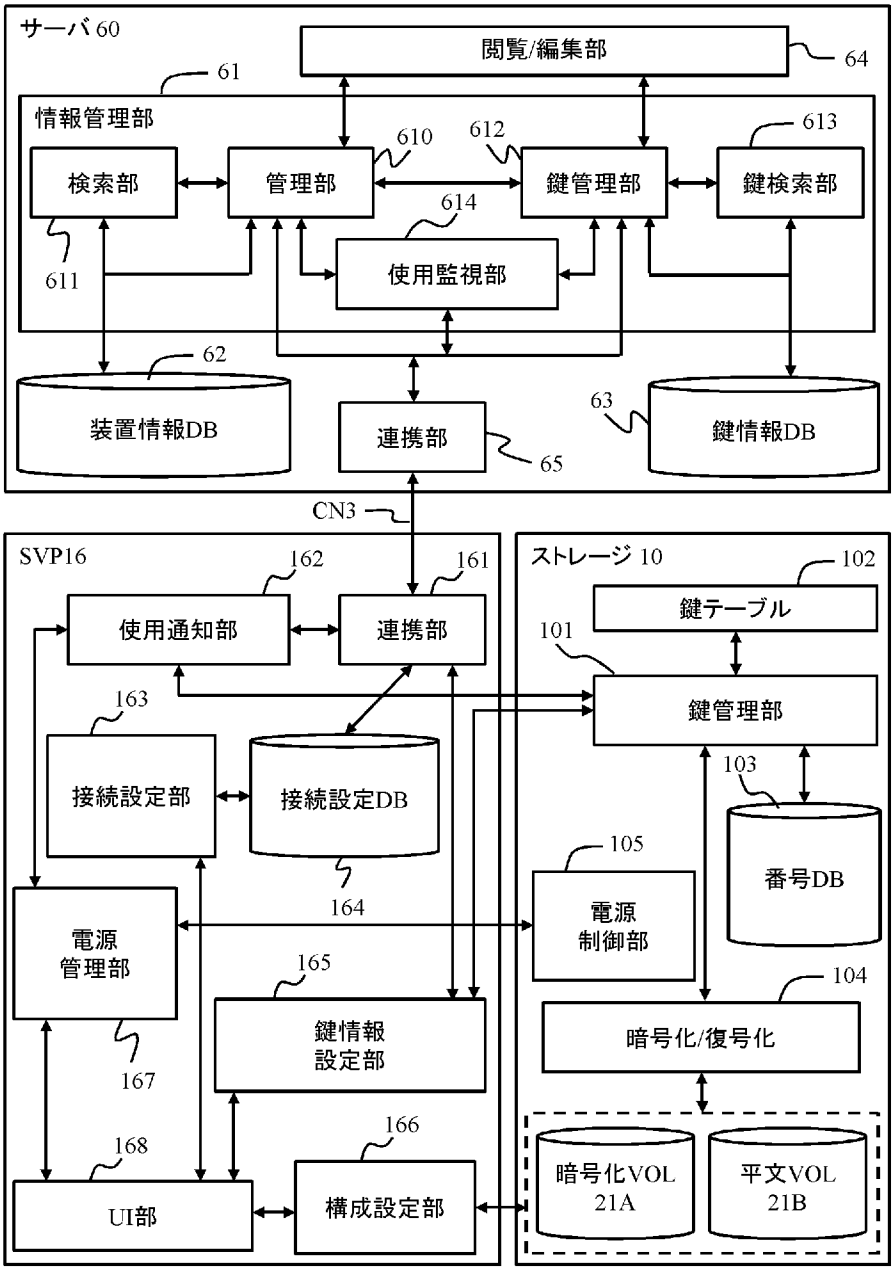
[図2]

図2


10
100
30
ホスト
30
ホスト
CN1
13
メモリPK
131
SM
132
CM
111
11
I/F
FEPK
I/F
15
SW
12
121
I/F
BEPK
I/F
CN4
CN4
20
21
21
142
111
121
CN2
141
MP
141
MP
141
MP
141
MP
SVP
16
ローカルメモリ
MPPK
14
外部ストレージ
41
40
CN3
50
管理端末
60
鍵管理サーバ

[図3]

図3


サーバ 60
閲覧/編集部
64
61
情報管理部
610
612
613
検索部
管理部
鍵管理部
鍵検索部
614
611
使用監視部
62
63
装置情報DB
連携部
65
鍵情報DB
CN3
SVP16
162
161
ストレージ 10
102
使用通知部
連携部
鍵テーブル
101
鍵管理部
163
103
接続設定部
接続設定DB
番号DB
105
164
電源
管理部
電源
制御部
165
104
鍵情報
設定部
暗号化/復号化
167
166
168
暗号化VOL
21A
平文VOL
21B
UI部
構成設定部

[図4]

図4

鍵情報 63	
番号	Key201
作成日時	2013/02/02 10:45:32.555
鍵の種別	Symmetric Key
装置番号	Storage401
鍵使用状況管理	Yes
使用状況最終確認日時	2013/02/10 15:15:43.321
使用有無	Yes
鍵データ	87289738647896874923...8748914786178

[図5]

図5

装置情報 62	
番号	Storage401
ストレージに接続するための情報	IP:10.231.54.22 ポート:8080 クライアント証明書:bd867826499.....2837648992 サーバ証明書：de27836766412385.....456474534343
ストレージから接続されるときの情報	クライアント証明書:ad689239816.....9786567191 サーバ証明書:2378466347869....32746472389
ストレージ情報	機種:RAID800 製造番号:10387
ストレージへの最終接続日時	2013/02/10 15:15:43.321

[図6]

図6

鍵番号情報 103	
ストレージ内鍵番号	Internal_Key1
鍵管理サーバ番号	KeyStore_111
鍵管理サーバ内での鍵番号	Key201
設定日時	2013/02/02 10:45:32.555
最終確認日時	2013/02/10 15:15:43.321

[図7]

図7

鍵テーブル 102	
ストレージ内鍵番号	Internal_Key1
鍵データ	87289738647896874923...8748914786178

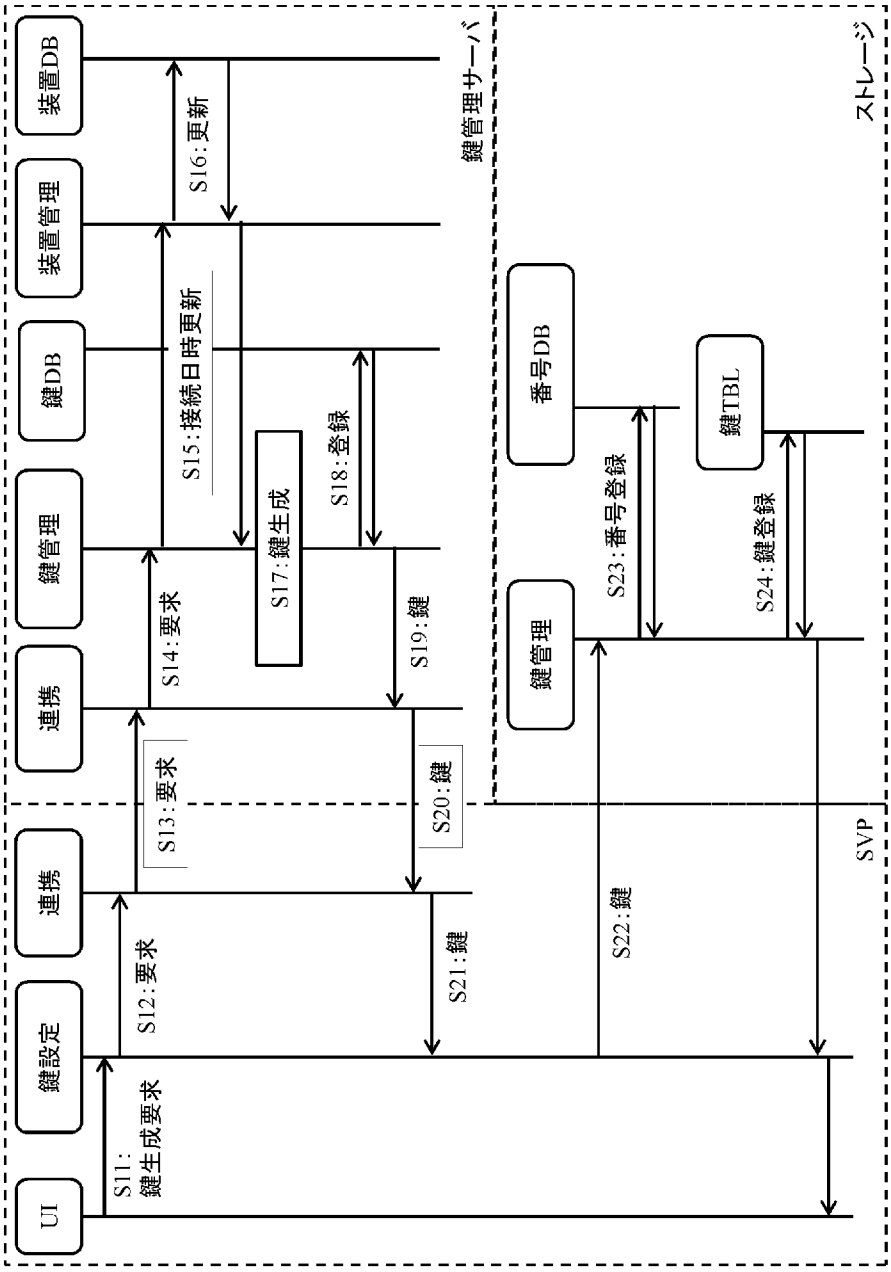
[図8]

図8

鍵管理サーバへの接続設定情報 164	
番号	KeyStore_111
鍵管理サーバに接続するための情報	IP:10.231.54.1 ポート:5636 クライアント証明書: ad689239816.....9786567191 サーバ証明書:2378466347869....32746472389
鍵管理サーバから接続されるときの情報	クライアント証明書:bd867826499.....2837648992 サーバ証明書：dc27836766412385.....456474534343

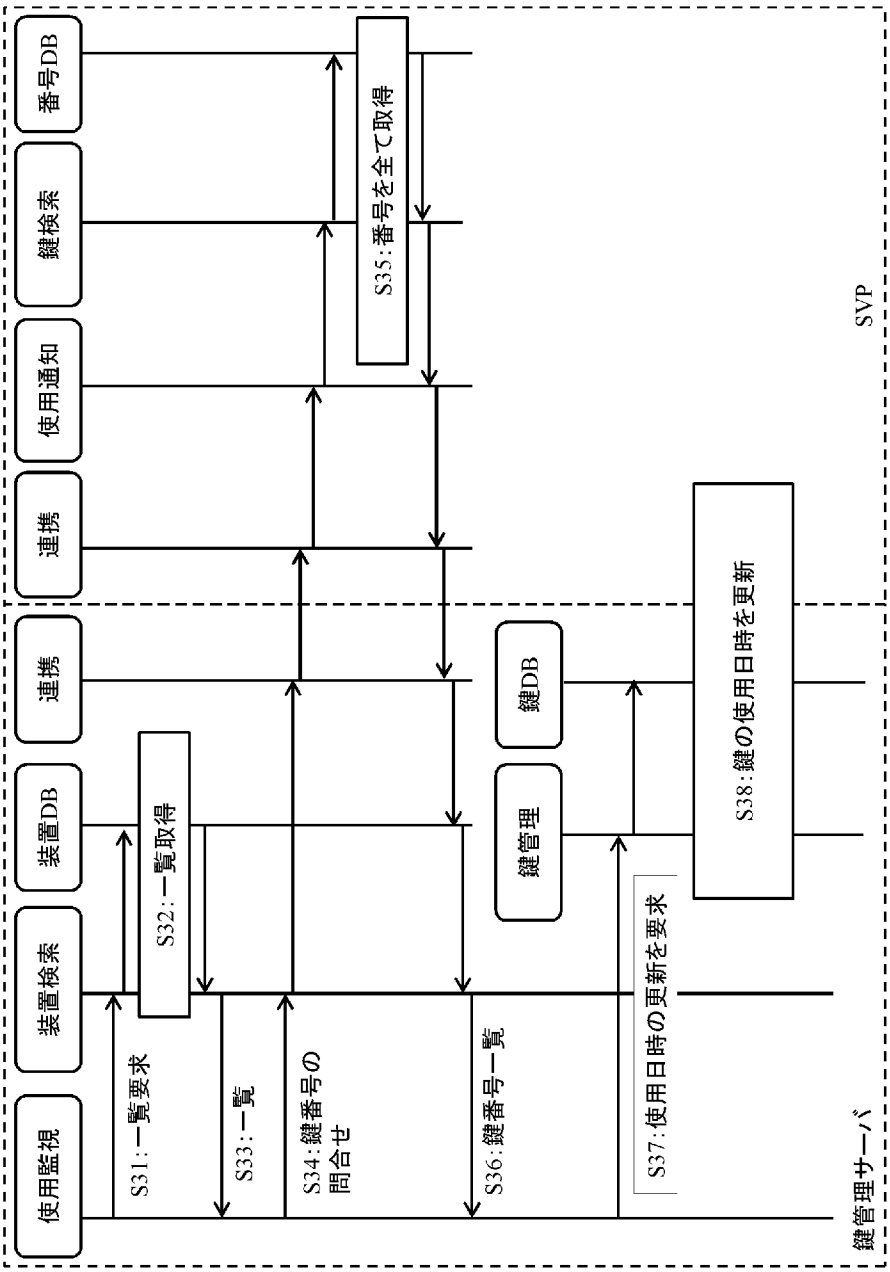
[図9]

図9


UI
鍵設定
連携
連携
鍵管理
鍵DB
装置管理
装置DB
鍵管理サーバ
鍵管理
番号DB
鍵TBL
ストレージ
SVP
S11:
鍵生成要求
S12:要求
S13:要求
S14:要求
S15:接続日時更新
S16:更新
S17:鍵生成
S18:登録
S19:鍵
S20:鍵
S21:鍵
S22:鍵
S23:番号登録
S24:鍵登録

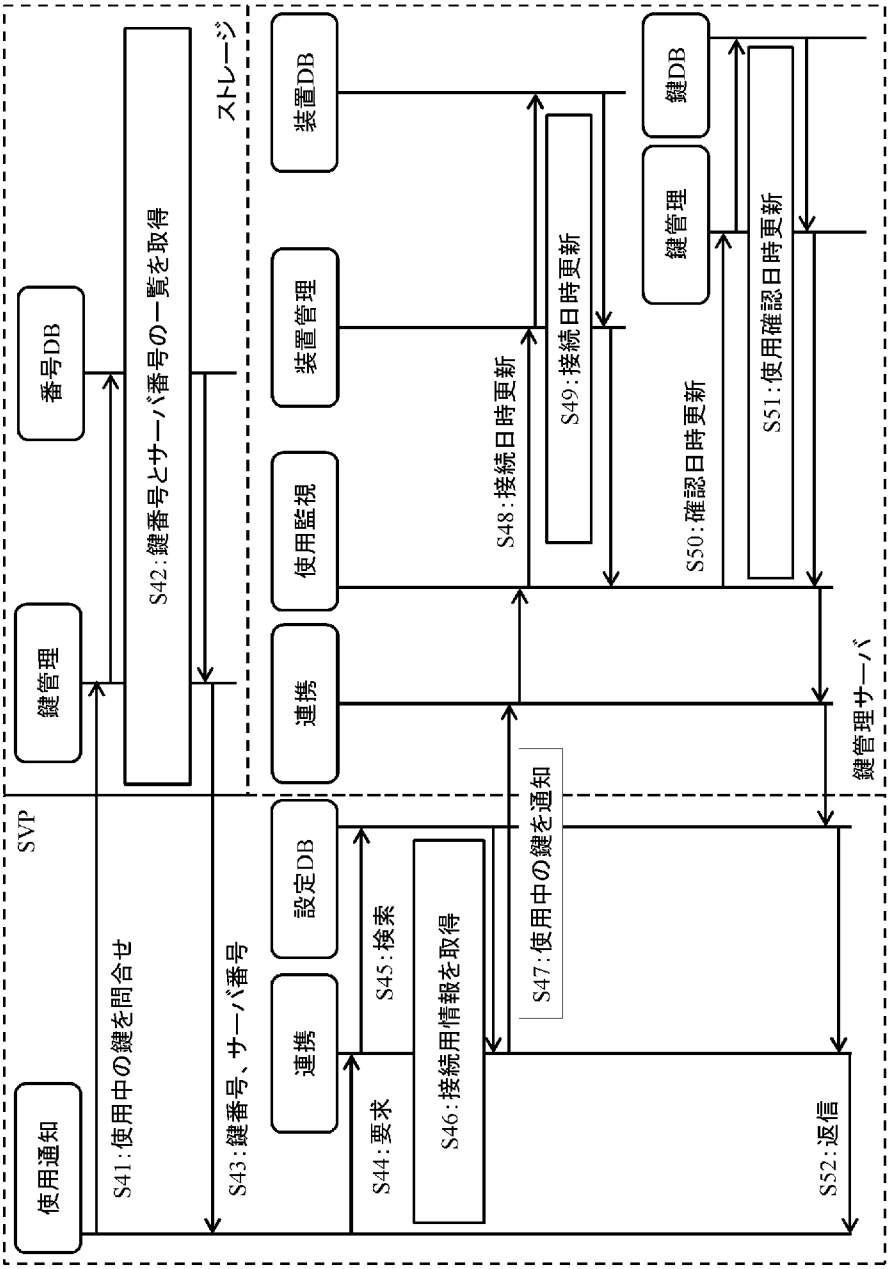
[図10]

図10


使用監視
装置検索
装置DB
連携
使用通知
鍵検索
番号DB
連携
鍵管理
鍵DB
S31:一覧要求
S32:一覧取得
S33:一覧
S34:鍵番号の問合せ
S35:番号を全て取得
S36:鍵番号一覧
S37:使用日時の更新を要求
S38:鍵の使用日時を更新
鍵管理サーバ
SVP

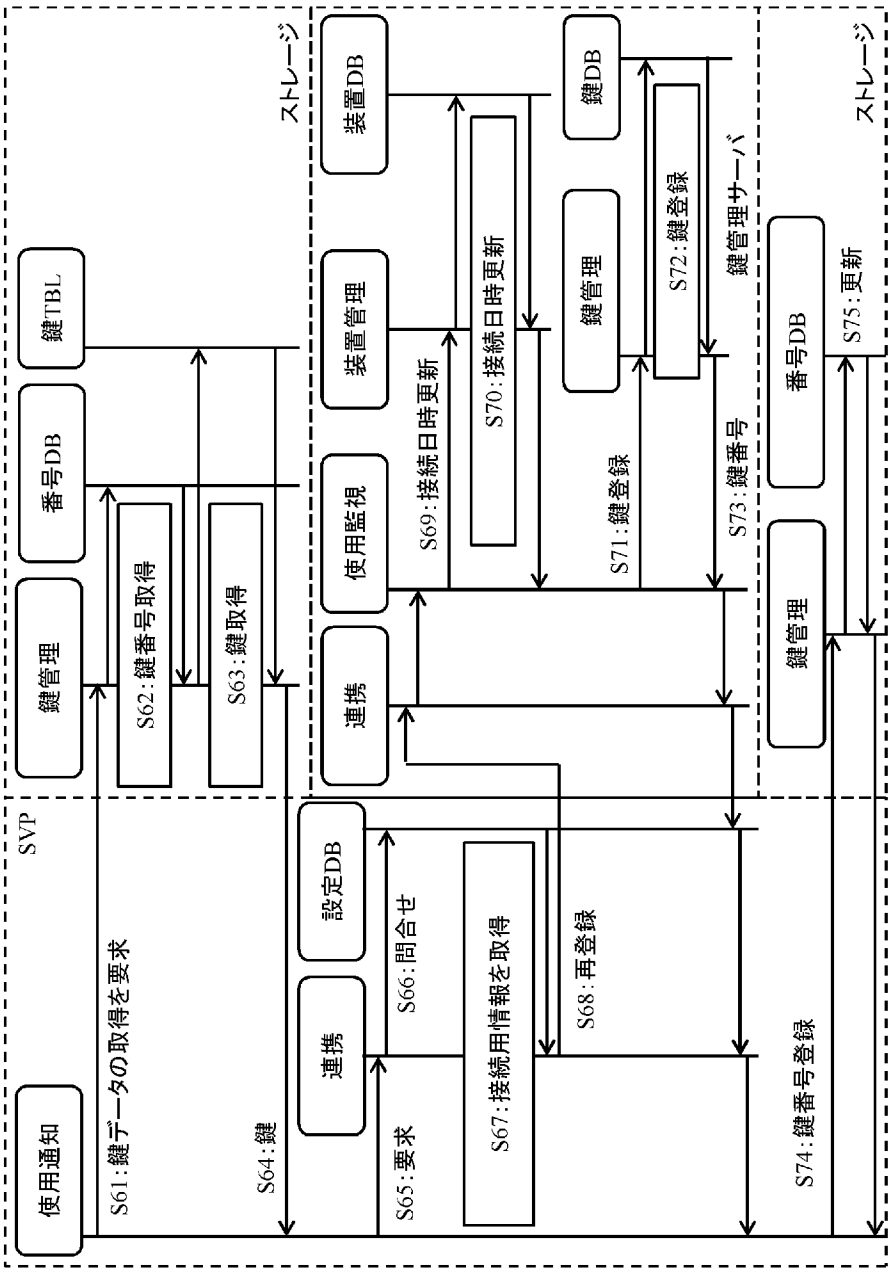
[図11]

図11


SVP
使用通知
鍵管理
番号DB
ストレージ
S42:鍵番号とサーバ番号の一覧を取得
S41:使用中の鍵を問合せ
S43:鍵番号、サーバ番号
連携
設定DB
S44:要求
S45:検索
S46:接続用情報を取得
S47:使用中の鍵を通知
S52:返信
鍵管理サーバ
連携
使用監視
装置管理
装置DB
S48:接続日時更新
S49:接続日時更新
鍵管理
鍵DB
S50:確認日時更新
S51:使用確認日時更新

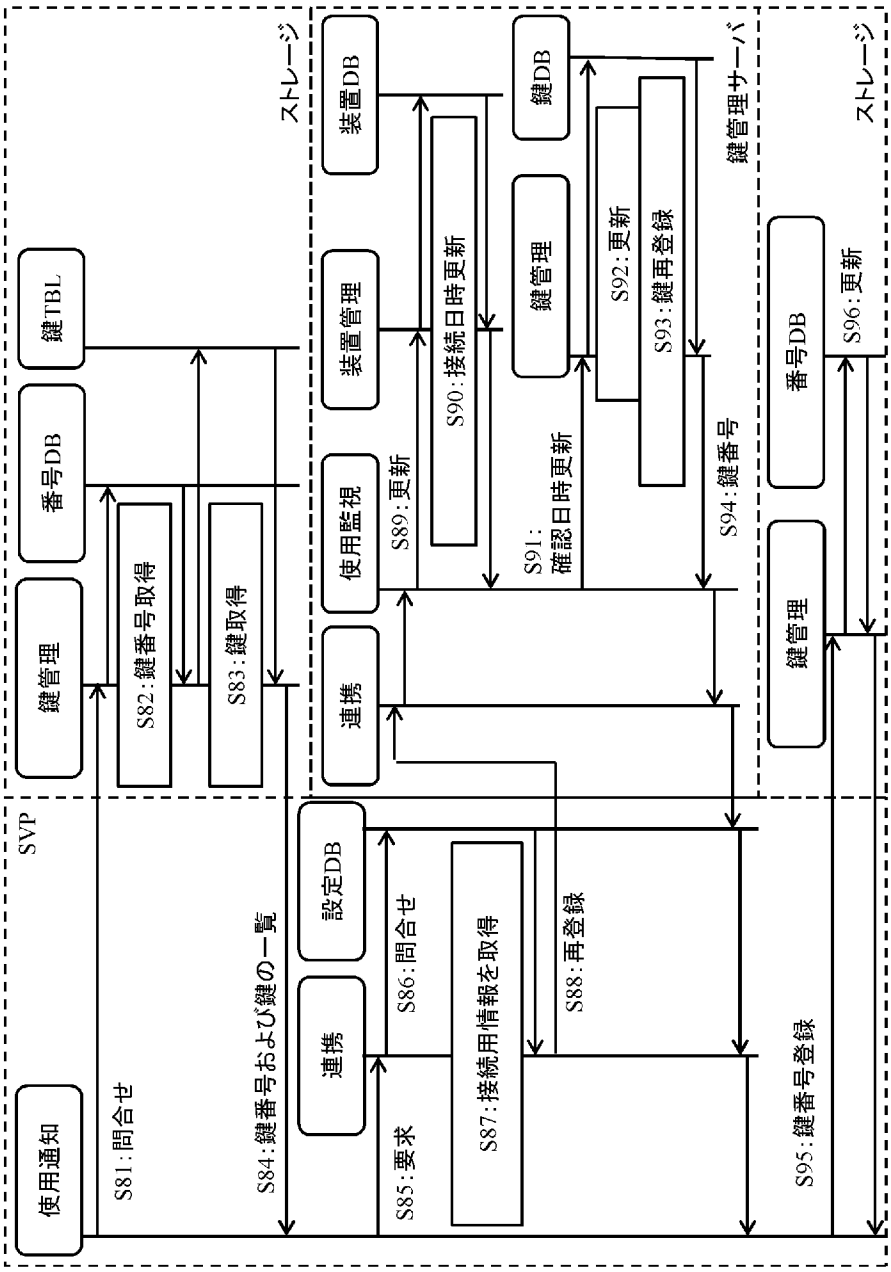
[図12]

図12


SVP
使用通知
鍵管理
鍵TBL
番号DB
ストレージ
S61:鍵データの取得を要求
S62:鍵番号取得
S63:鍵取得
S64:鍵
連携
設定DB
S65:要求
S66:問合せ
S67:接続用情報を取得
使用監視
装置管理
装置DB
S68:再登録
連携
S69:接続日時更新
S70:接続日時更新
鍵管理
鍵DB
S71:鍵登録
S72:鍵登録
鍵管理サーバ
S73:鍵番号
鍵管理
番号DB
ストレージ
S74:鍵番号登録
S75:更新

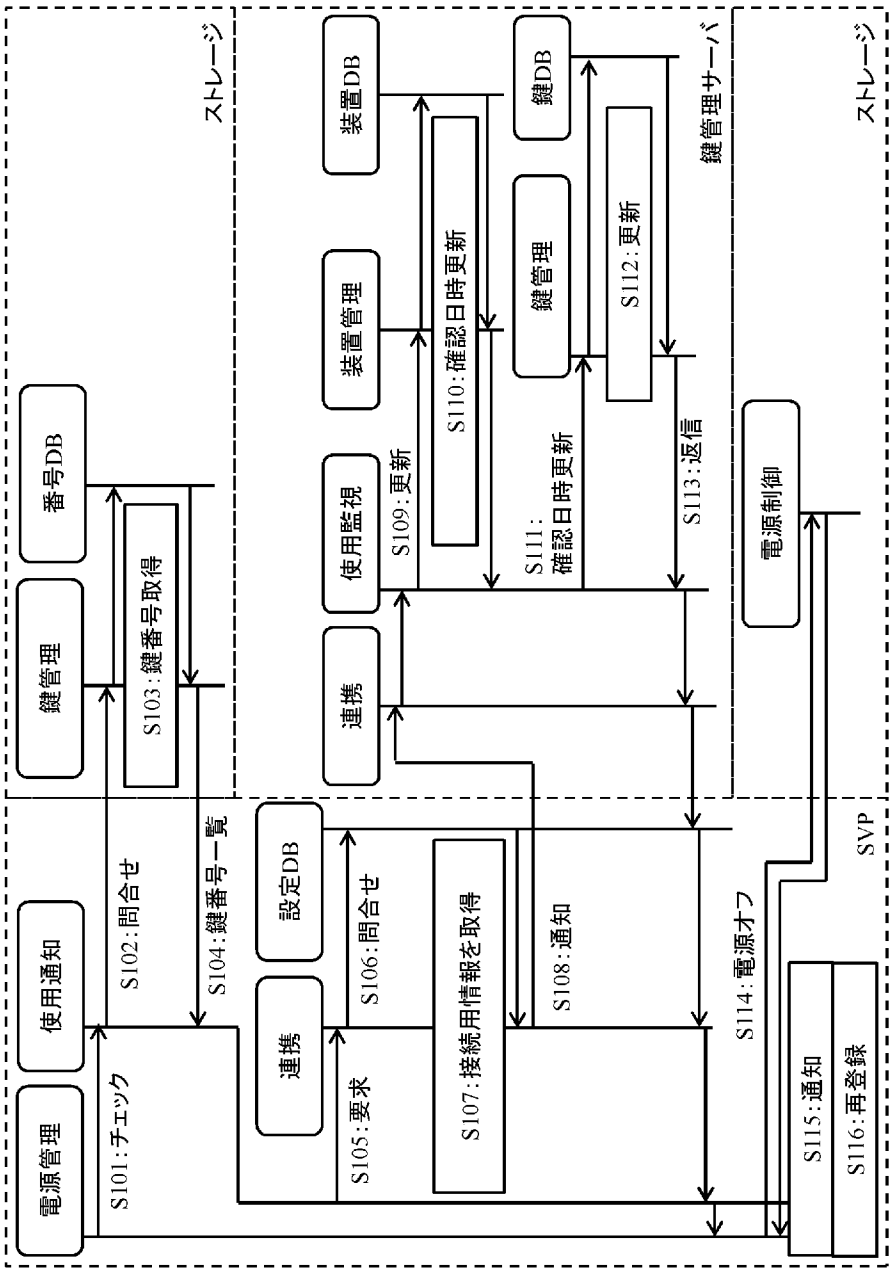
[図13]

図13


SVP
使用通知
連携
設定DB
ストレージ
鍵管理
鍵TBL
番号DB
鍵管理サーバ
連携
使用監視
装置管理
装置DB
鍵管理
鍵DB
番号DB
ストレージ
S81:問合せ
S82:鍵番号取得
S83:鍵取得
S84:鍵番号および鍵の一覧
S85:要求
S86:問合せ
S87:接続用情報を取得
S88:再登録
S89:更新
S90:接続日時更新
S91:
確認日時更新
S92:更新
S93:鍵再登録
S94:鍵番号
S95:鍵番号登録
S96:更新

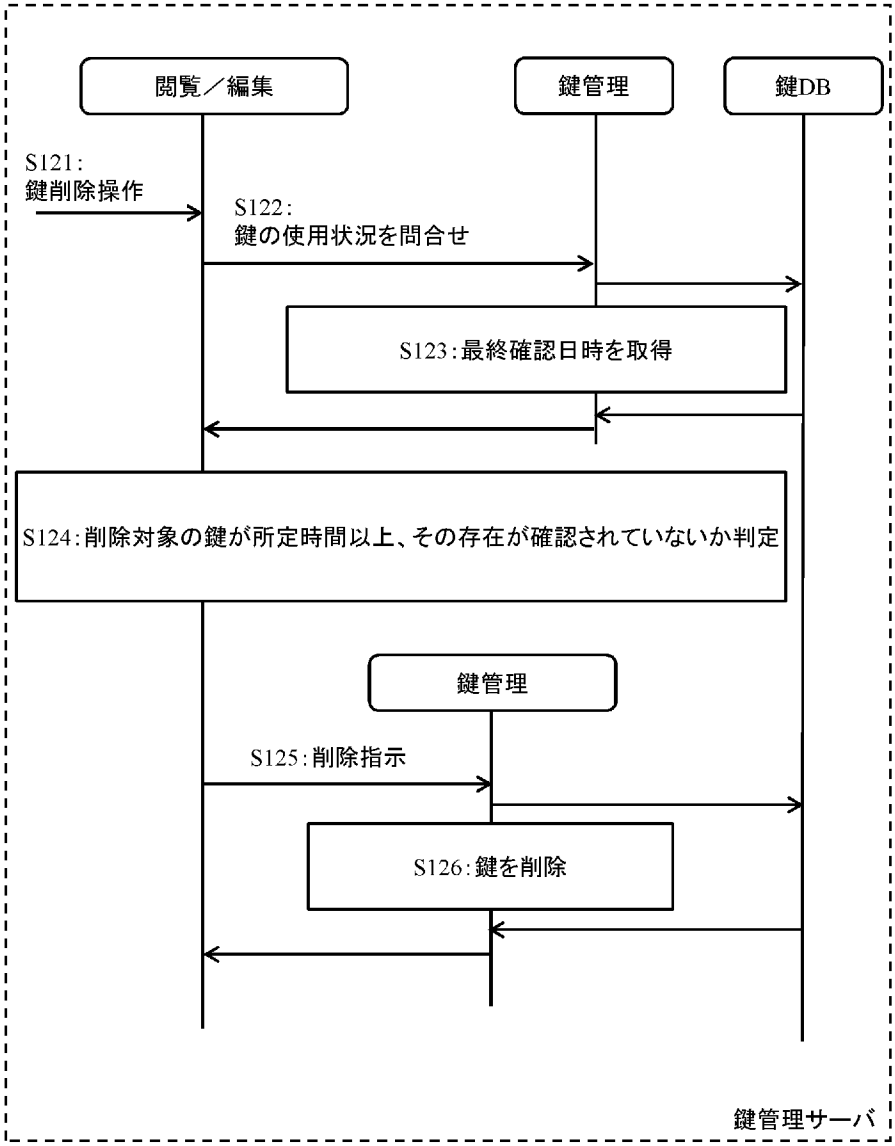
[図14]

図14


ストレージ
番号DB
鍵管理
S103:鍵番号取得
装置DB
装置管理
使用監視
連携
S109:更新
S110:確認日時更新
鍵DB
鍵管理
S111:
確認日時更新
S112:更新
S113:返信
鍵管理サーバ
電源制御
ストレージ
電源管理
使用通知
S101:チェック
S102:問合せ
S104:鍵番号一覧
連携
設定DB
S105:要求
S106:問合せ
S107:接続用情報を取得
S108:通知
S114:電源オフ
SVP
S115:通知
S116:再登録

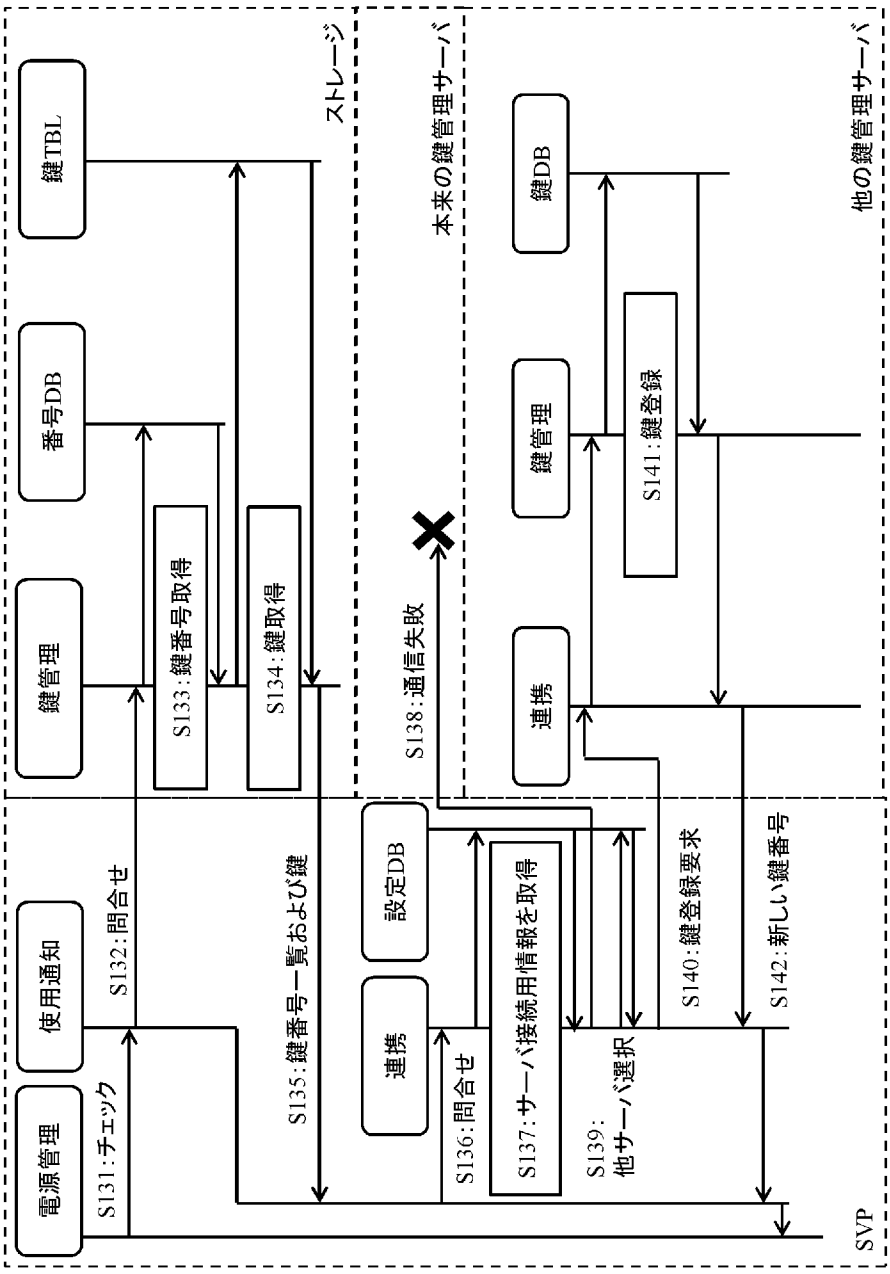
[図15]

図15


閲覧／編集
鍵管理
鍵DB
S121:
鍵削除操作
S122:
鍵の使用状況を問合せ
S123:最終確認日時を取得
S124:削除対象の鍵が所定時間以上、その存在が確認されていないか判定
鍵管理
S125:削除指示
S126:鍵を削除
鍵管理サーバ

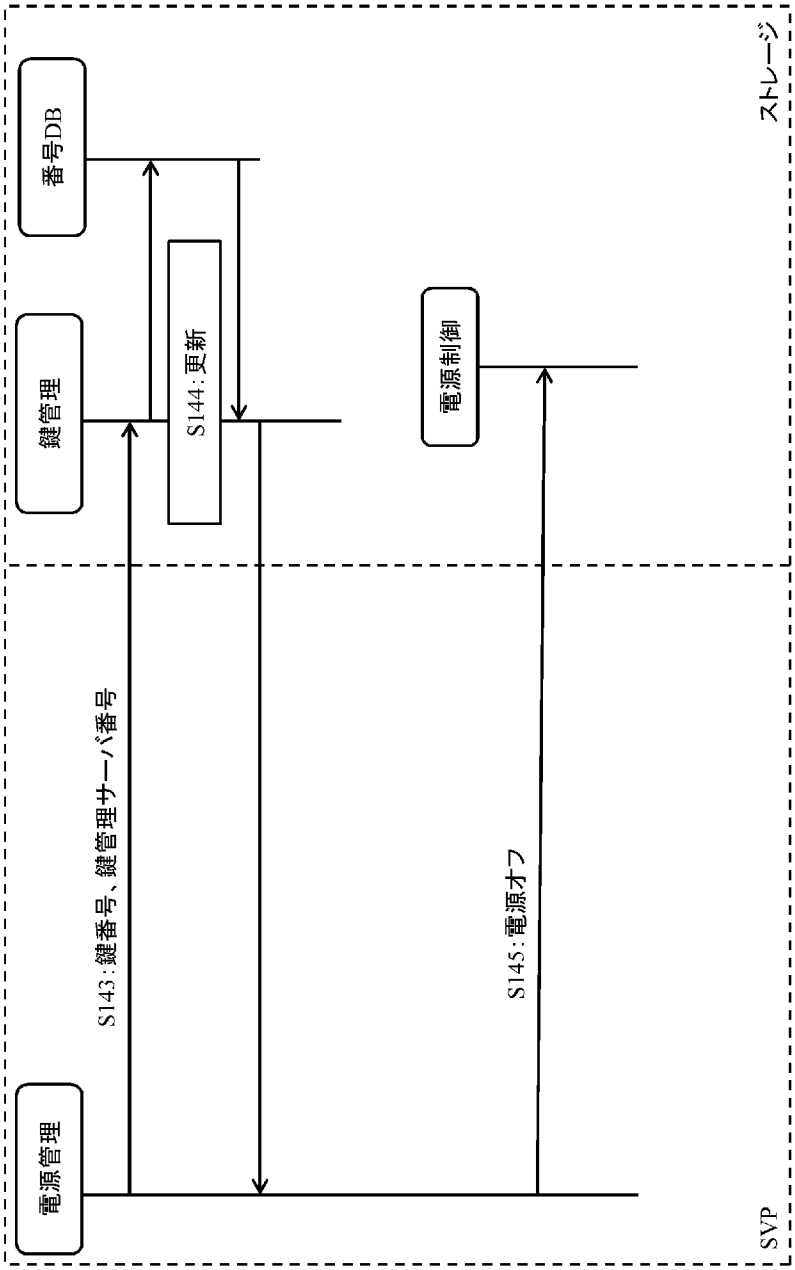
[図16]

図16


ストレージ
本来の鍵管理サーバ
他の鍵管理サーバ
鍵TBL
番号DB
鍵管理
S133:鍵番号取得
S134:鍵取得
S138:通信失敗
鍵DB
鍵管理
連携
S141:鍵登録
電源管理
使用通知
S131:チェック
S132:問合せ
S135:鍵番号一覧および鍵
設定DB
連携
S136:問合せ
S137:サーバ接続用情報を取得
S139:
他サーバ選択
S140:鍵登録要求
S142:新しい鍵番号
SVP

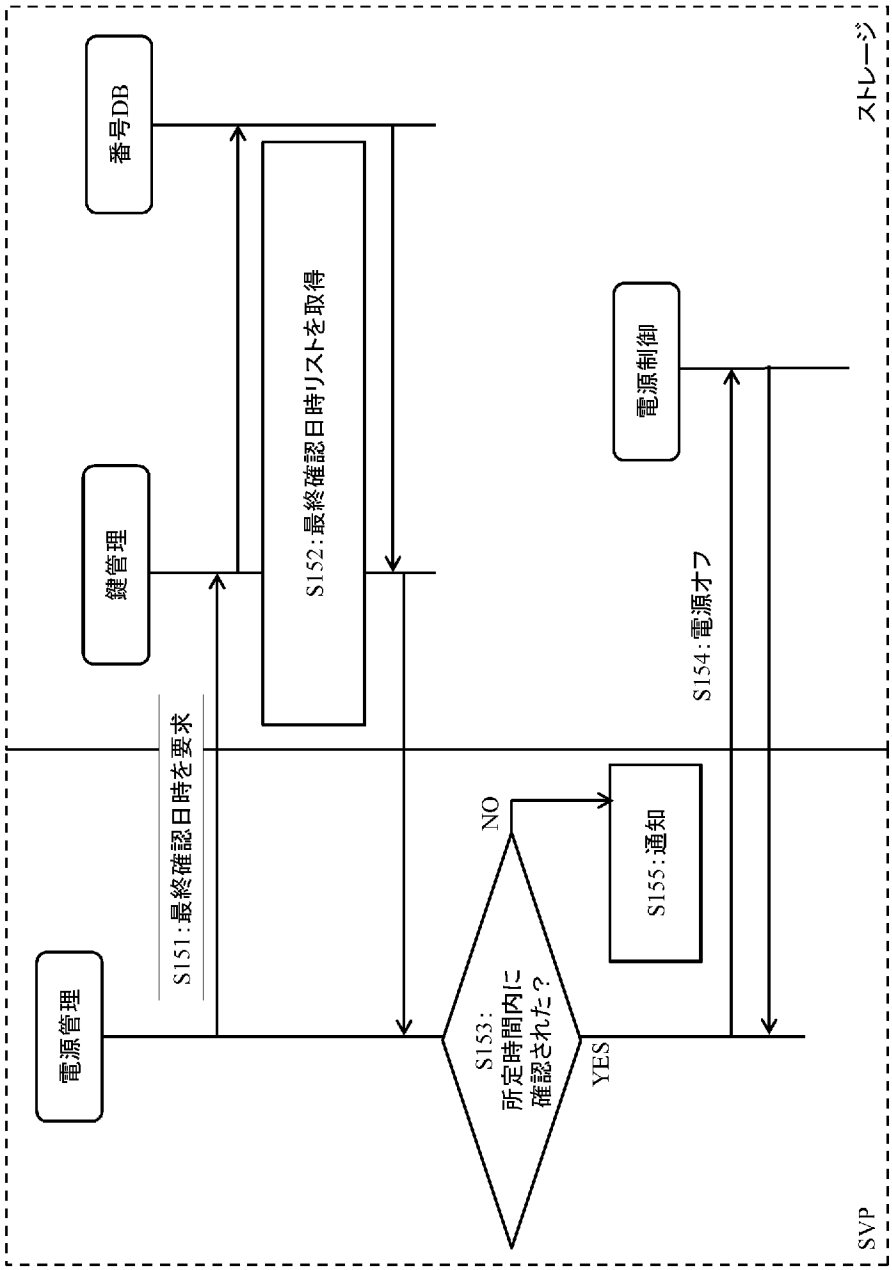
[図17]

図17


ストレージ
番号DB
鍵管理
S144:更新
電源制御
S143:鍵番号、鍵管理サーバ番号
S145:電源オフ
電源管理
SVP

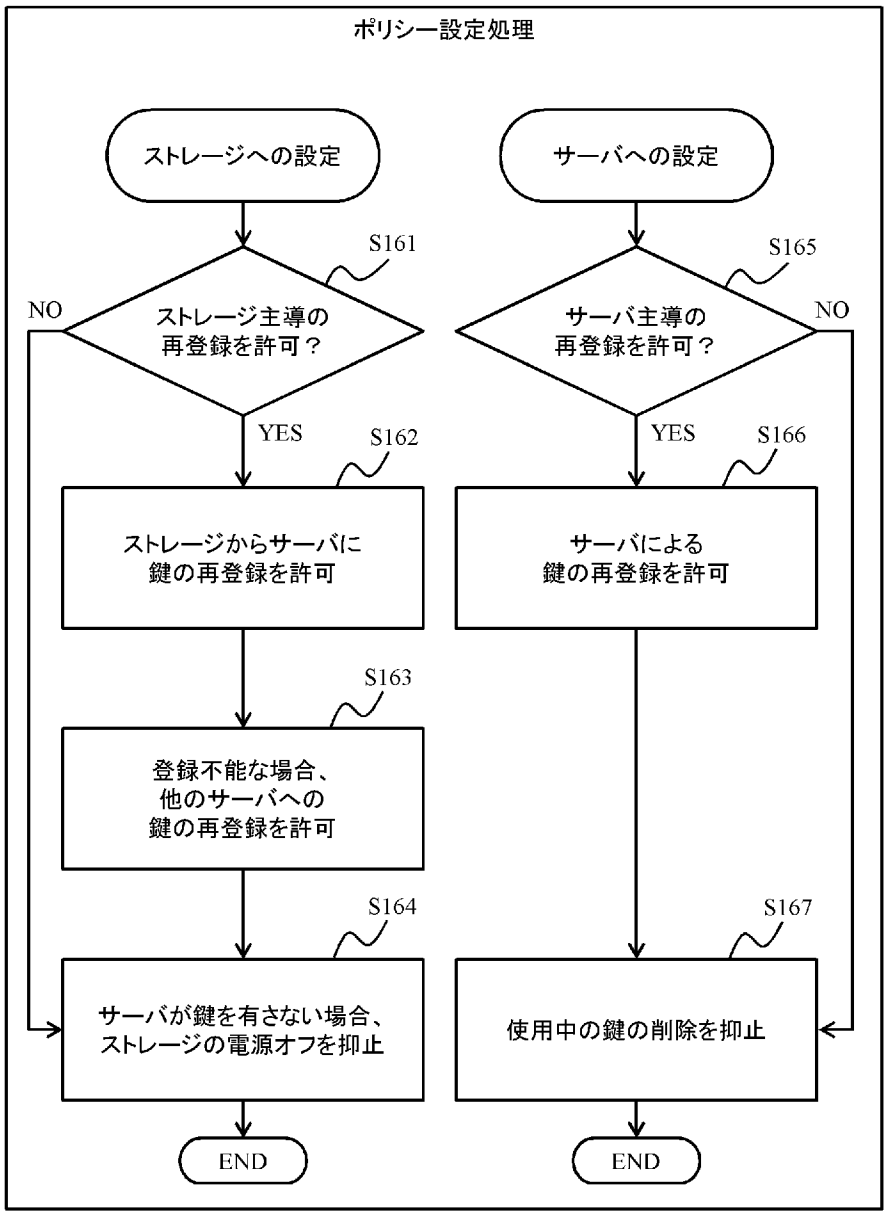
[図18]

図18


ストレージ
番号DB
鍵管理
電源制御
S152:最終確認日時リストを取得
S151:最終確認日時を要求
S154:電源オフ
電源管理
NO
S153:
所定時間内に
確認された？
S155:通知
YES
SVP

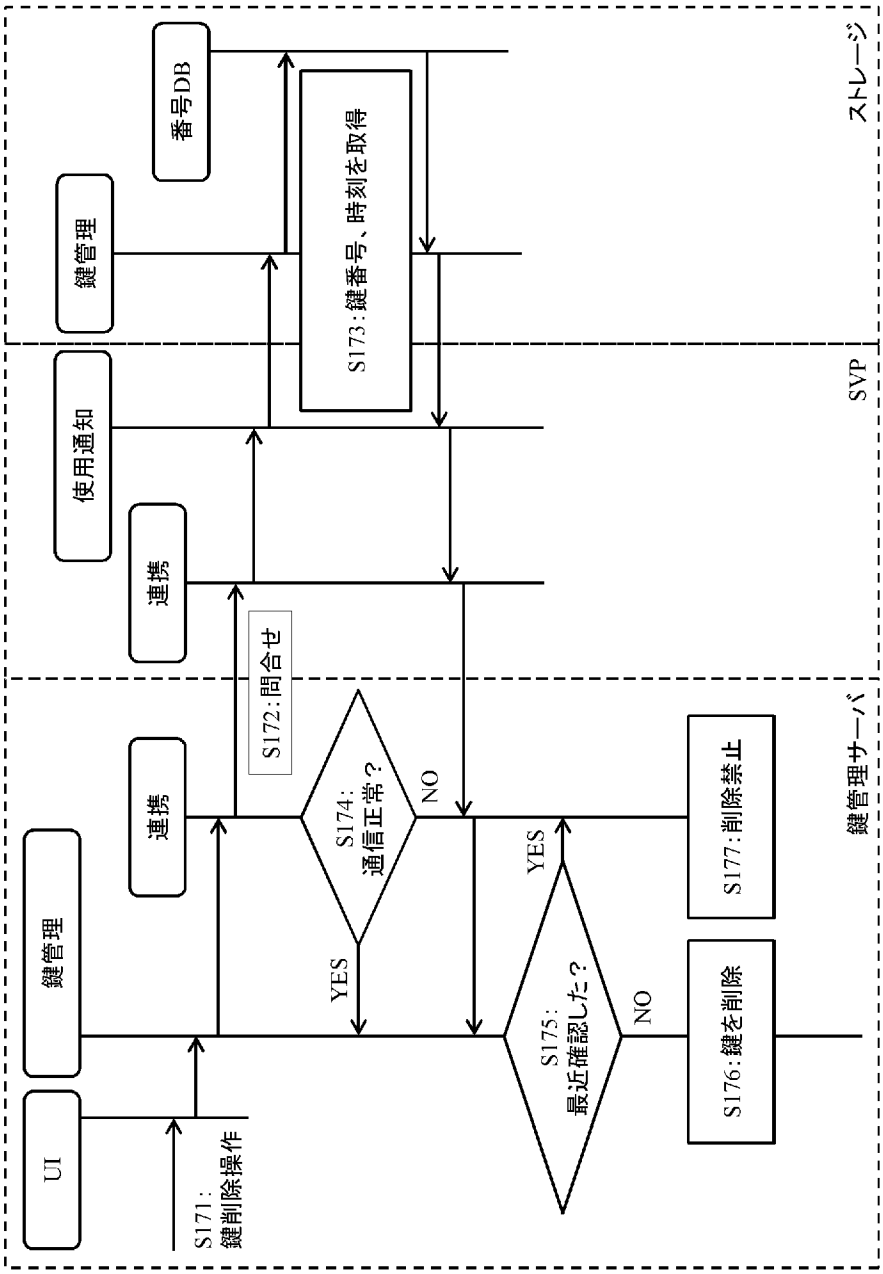
[図19]

図19


ポリシー設定処理
ストレージへの設定
サーバへの設定
S161
S165
ストレージ主導の
再登録を許可？
サーバ主導の
再登録を許可？
NO
NO
YES
YES
S162
S166
ストレージからサーバに
鍵の再登録を許可
サーバによる
鍵の再登録を許可
S163
登録不能な場合、
他のサーバへの
鍵の再登録を許可
S164
S167
サーバが鍵を有さない場合、
ストレージの電源オフを抑止
使用中の鍵の削除を抑止
END
END

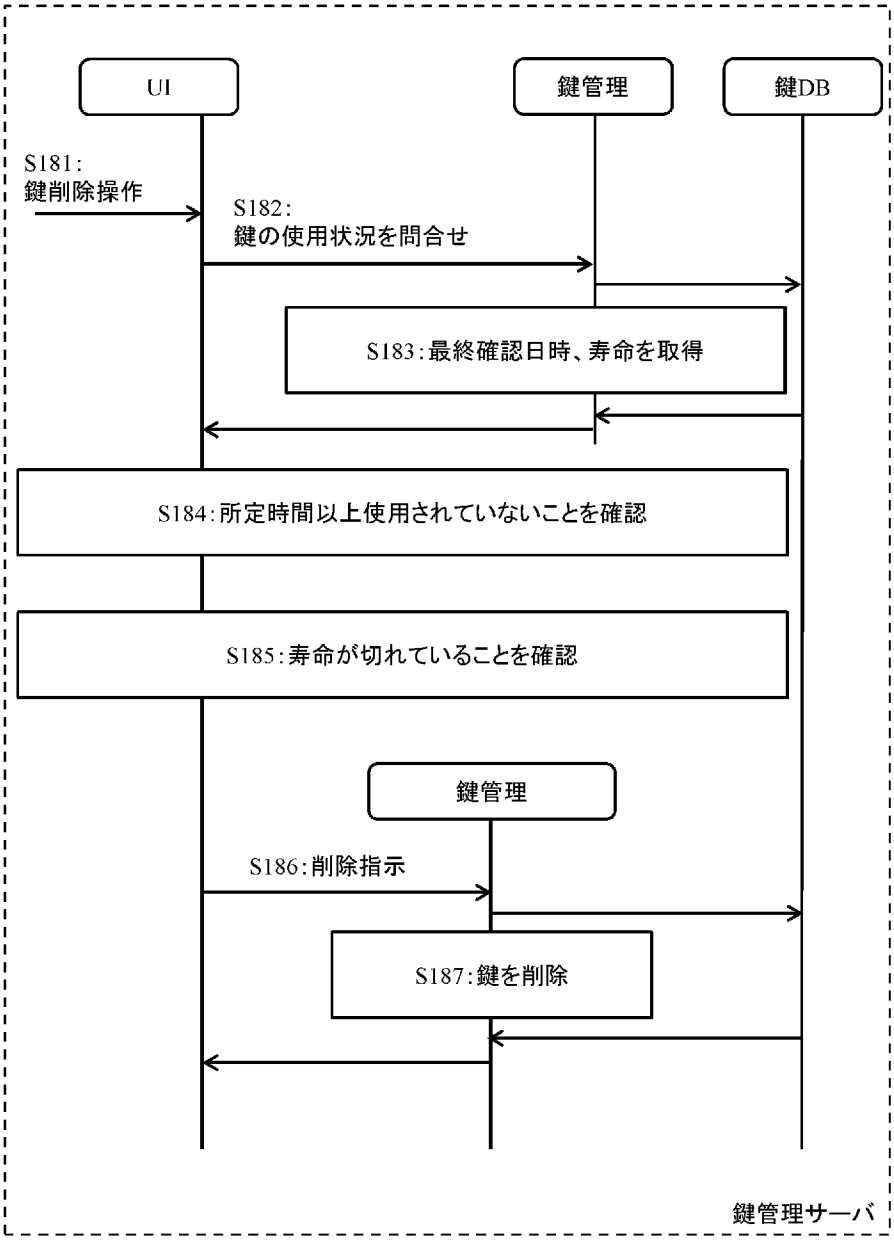
[図20]

図20


ストレージ
SVP
鍵管理サーバ
番号DB
鍵管理
使用通知
連携
S173:鍵番号、時刻を取得
連携
S172:問合せ
S174:
通信正常？
NO
YES
鍵管理
UI
S171:
鍵削除操作
YES
S175:
最近確認した？
NO
S177:削除禁止
S176:鍵を削除

[図21]

図21


UI
鍵管理
鍵DB
S181:
鍵削除操作
S182:
鍵の使用状況を問合せ
S183:最終確認日時、寿命を取得
S184:所定時間以上使用されていないことを確認
S185:寿命が切れていることを確認
鍵管理
S186:削除指示
S187:鍵を削除
鍵管理サーバ

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2013/068595

A. CLASSIFICATION OF SUBJECT MATTER
G09C1/00(2006.01)i, *G06F21/62*(2013.01)i, *H04L9/08*(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)
G09C1/00, G06F21/62, H04L9/08

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	1996-2013
Kokai Jitsuyo Shinan Koho	1971-2013	Toroku Jitsuyo Shinan Koho	1994-2013

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2009-98719 A (Hitachi, Ltd.), 07 May 2009 (07.05.2009), entire text; all drawings & US 2010/0031058 A1	1-14
A	JP 2008-278469 A (Quantum Corp.), 13 November 2008 (13.11.2008), entire text; all drawings & US 2008/0219449 A1 & EP 1967979 A2	1-14
A	JP 2007-157049 A (Hitachi, Ltd.), 21 June 2007 (21.06.2007), entire text; all drawings & US 2007/0136606 A1	1-14

☐ 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
03 September, 2013 (03.09.13)	10 September, 2013 (10.09.13)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２０１３／０６８５９５

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　G09C1/00(2006.01)i, G06F21/62(2013.01)i, H04L9/08(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.　G09C1/00, G06F21/62, H04L9/08

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　１９７１－２０１３年
日本国実用新案登録公報　１９９６－２０１３年
日本国登録実用新案公報　１９９４－２０１３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）

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	JP 2009-98719 A (株式会社日立製作所) 2009.05.07, 全文, 全図 & US 2010/0031058 A1	1-14
A	JP 2008-278469 A (クウォンタム・コーポレイション) 2008.11.13, 全文, 全図 & US 2008/0219449 A1 & EP 1967979 A2	1-14
A	JP 2007-157049 A (株式会社日立製作所) 2007.06.21, 全文, 全図 & US 2007/0136606 A1	1-14

☐　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
０３．０９．２０１３	１０．０９．２０１３

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　９４６９
石田　信行
電話番号　０３－３５８１－１１０１　内線　３５４６