(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
2010 年 4 月 15 日(15.04.2010)

PCT

(10) 国際公開番号
WO 2010/041442 A1

(51) 国際特許分類:
H04L 9/08 (2006.01) *G09C 1/00* (2006.01)
G06F 12/00 (2006.01) *H04L 9/14* (2006.01)

(21) 国際出願番号: PCT/JP2009/005217

(22) 国際出願日: 2009 年 10 月 7 日(07.10.2009)

(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 2008-263680 2008 年 10 月 10 日(10.10.2008) JP

(71) 出願人 (米国を除く全ての指定国について): パナソニック株式会社 (PANASONIC CORPORATION) [JP/JP]; 〒5718501 大阪府門真市大字門真１００６番地 Osaka (JP).

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 伊藤孝幸 (ITO, Takayuki). 松島秀樹 (MATSUSHIMA, Hideki). 高山久 (TAKAYAMA, Hisashi). 芳賀智之 (HAGA, Tomoyuki).

(74) 代理人: 中島司朗, 外 (NAKAJIMA, Shiro et al.); 〒5310072 大阪府大阪市北区豊崎三丁目２番１号淀川５番館６Ｆ Osaka (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, JP, 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, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

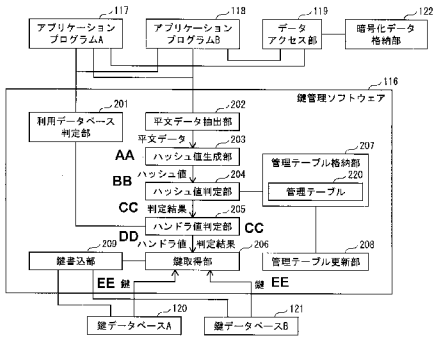
(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL,

[続葉有]

(54) **Title**: INFORMATION PROCESSING DEVICE, METHOD, PROGRAM, AND INTEGRATED CIRCUIT

(54) 発明の名称 : 情報処理装置、方法、プログラム及び集積回路

[図2]



116 key management software
117 application program A
118 application program B
119 data access unit
120 key database A
121 key database B
122 encrypted data storage unit
201 in-use database decision unit
202 plaintext data extraction unit
203 hash value generation unit
204 hash value decision unit
205 handler value decision unit
206 key acquisition unit
207 management table storage unit
208 management table update unit
209 key writing unit
220 management table
AA plaintext data
BB hash value
CC decision result
DD handler value
EE key

(57) **Abstract**: Provided is a high-speed data synchronizing process in which the number of key decodings is reduced when a plurality of key databases are used to synchronize the same data, because the keys of another key database, which was preset, are used to update the data managed in the other databases. Key management software (116) for managing a key database A (120) and a key database B (121), which have tree structures, determines whether or not synchronization is needed when the encryption of data from a high-level application is requested. The keys in the other key database, which was preset, are used, and the encrypted data are synchronized. Thus, repeated loads of the encrypted keys to an encryption unit (114) are eliminated, and data is encrypted at high speed.

(57) 要約: 複数の鍵データベースを用いて同一のデータを同期する際に、あらかじめ設定された別鍵データベースの鍵を利用して、別データベースで管理するデータを更新するため、鍵の復号回数を削減することによって、高速なデータ同期処理を提供することを目的とする。木構造の鍵データベースＡ１２０と鍵データベースＢ１２１を管理する鍵管理ソフトウェア１１６が、上位アプリからのデータの暗号化要求の際に、同期すべきか否かを判定し、あらかじめ設定された別鍵データベースの鍵を利用し、暗号化データの同期を行う。これにより、暗復号処理部１１４へ暗号化された鍵のロード回数を削除し、高速なデータの暗復号を行う。

WO 2010/041442 A1

NO, PL, PT, RO, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, 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 ： 情報処理装置、方法、プログラム及び集積回路

技術分野

[0001] 本発明は、複数の暗復号システムにおいてデータを共有する技術に関する。

背景技術

[0002] 近年、Ｐｅｒｓｏｎａｌ　Ｃｏｍｐｕｔｅｒ（ＰＣ）や携帯電話などの情報処理装置に格納された個人情報などのデータの盗難が問題となっている。

[0003] このようなデータの盗難は、コンピュータウイルスなどの悪意のあるプログラムによって行われることがある。悪意のあるプログラムは、対象とする情報処理装置で動作する他のプログラムの不具合などを利用して、当該情報処理装置に入り込んで不正に動作し、当該情報処理装置の記憶部に格納されているデータを読み取り、ネットワークを介して、読み取ったデータを攻撃者などに送付する。

[0004] このようなデータの盗難を防ぐために、データを暗号化することによってデータを保護することができる。データ暗号化技術として、ファイルシステムを用いた暗号処理によって実現する技術や、ファイルシステムに依存しない技術が存在する。

[0005] 特許文献１には、ファイルに対応するファイル鍵を用いて、ファイルを暗号化する技術が開示されている。これにより、ファイルごとに異なる鍵で暗号化を行うことが可能である。

[0006] また、非特許文献１には、ファイルシステムに依存しない技術として、Ｔｒｕｓｔｅｄ　Ｃｏｍｐｕｔｉｎｇ　Ｇｒｕｏｐ（ＴＣＧ）において、データの暗号化を行うＰｒｏｔｅｃｔｅｄ　Ｓｔｏｒａｇｅという仕様が公開されている。以下に、非特許文献１において開示されている暗復号処理モジュールについて説明する。

[0007] この暗復号処理モジュールを実現するための鍵管理ソフトウェアは、鍵デ

ータベースを有し、鍵データベースは、この暗復号処理モジュールで用いられる鍵を木構造により管理する。鍵データベースは、暗復号処理モジュールの外部の記憶装置に存在する。鍵データベースの木構造は、説明を簡単にするために、３階層から構成され、１個のルート、２個の中間ノード、４個のリーフから構成されるとする。前記ルートの直下には、２個の中間ノードが接続し、２個の中間ノードの直下には、それぞれ、２個のリーフが接続している。ルートには、ルート鍵が割り当てられる。第１及び第２の中間ノードには、それぞれ、ルート鍵を用いて暗号化された鍵Ａ及びルート鍵を用いて暗号化された鍵Ｂが格納される。第１の中間ノードの直下に接続する２個のリーフには、それぞれ、第１の中間ノードの鍵Ａを用いて暗号化された鍵Ｃ及び暗号化された鍵Ｄが格納される。第２の中間ノードの直下に接続する２個のリーフには、それぞれ、第２の中間ノードの鍵Ｂを用いて暗号化された鍵Ｅ及び暗号化された鍵Ｆが格納される。ここで、鍵Ｃ、鍵Ｄ、鍵Ｅ及び鍵Ｆは、それぞれ、データを暗号化又は復号するために使用される鍵である。

[0008] 前記暗復号処理モジュールは、不揮発性メモリ、暗復号エンジン及び鍵格納部から構成されている。また、前記暗復号処理モジュールは、外部からの処理データの盗み取り及び改竄ができないように耐タンパ化されている。不揮発性メモリは、前記ルート鍵を格納している。ルート鍵は、公開鍵暗号方式の秘密鍵（私有鍵）や、共通鍵暗号方式の秘密鍵である。暗復号エンジンは、暗号化された鍵の復号、鍵の暗号化、暗号化されたデータの復号及びデータの暗号化を行う。鍵格納部は、暗復号エンジンが使用する鍵を格納する。

[0009] このように、ルート鍵は、耐タンパ化された暗復号処理モジュールの内部に格納されることにより、保護されている。一方、その他の鍵Ａ、鍵Ｂ、鍵Ｃ、鍵Ｄ、鍵Ｅ及び鍵Ｆは、暗復号処理モジュールの外部の記憶装置において、暗号化されることにより、保護されている。

[0010] 鍵管理ソフトウェアは、暗復号処理モジュールの外部のアプリケーションプログラムから鍵Ｃの取得を要求されると、鍵Ｃに対応するリーフの親であ

る中間ノードに格納された暗号化鍵Ｂを鍵管理データベースから取得し、暗号化鍵Ｂを暗復号処理モジュールへ出力する。暗復号処理モジュールは、暗復号エンジンにより、暗号化鍵Ｂをルート鍵を用いて復号して鍵Ｂを生成する。次に、鍵管理ソフトウェアは、鍵Ｃに対応するリーフに格納された暗号化鍵Ｃを鍵管理データベースから取得し、暗号化鍵Ｃを暗復号処理モジュールへ出力する。暗復号処理モジュールは、暗復号エンジンにより、暗号化鍵Ｃを鍵Ｂを用いて復号し、復号して得られた鍵Ｃを鍵格納部に格納する。次に、鍵管理ソフトウェアは、暗復号処理モジュールから鍵のロード終了を示す通知を受け取る。これで鍵の暗復号処理モジュールへのロード処理が終了する。

[0011] 暗復号処理モジュールの鍵格納部に鍵Ｃが格納された後に、鍵管理ソフトウェアは、アプリケーションプログラムからデータの暗号化又は復号を要求され、鍵管理ソフトウェアは、アプリケーションプログラムから受け取ったデータを、暗復号処理モジュールへ出力し、鍵Ｃを用いて暗号化又は復号を行うように、暗復号処理モジュールに依頼する。暗復号処理モジュールは、受け取ったデータを、暗復号エンジンにより、鍵格納部に格納された鍵Ｃを用いて、暗号化又は復号し、暗号文又は復号文を出力する。鍵管理ソフトウェアは、暗復号処理モジュールから受け取った暗号文又は復号文を、アプリケーションプログラムに出力する。これで、暗復号処理が終了する。

[0012] 以上説明したように、鍵データベース及び暗復号処理モジュールを用いることで、平文の鍵（ルート鍵）は、常に耐タンパ化された暗復号処理モジュールの内部に格納されて使用することが可能となる。そのため、平文の鍵の盗み取りを防ぐ事が可能となる。

先行技術文献

特許文献

[0013] 特許文献1：日本国特表２００６－５１０９５８号公報

非特許文献

[0014] 非特許文献1：ＴＣＧ Ｓｐｅｃｉｆｉｃａｔｉｏｎ Ａｒｃｈｉｔｅｃｔｕ

ｒｅ Ｏｖｅｒｖｉｅｗ Ｓｐｅｃｉｆｉｃａｔｉｏｎ Ｒｅｖｉｓｉｏｎ １．３ ２８ｔｈ Ｍａｒｃｈ ２００７

発明の概要

発明が解決しようとする課題

[0015] ここで、非特許文献１により開示された方法により、１個の暗復号処理モジュールと、異なる木構造により構成された２個の鍵データベースとを用いる場合を想定する。

[0016] 例えば、情報処理装置が、音楽を配信する音楽配信システム及び映画を配信する映画配信システムを利用して、音楽及び映画の供給を受ける場合に、音楽配信システムと、映画配信システムとは、異なる音楽配信業者と映画配信業者とにより運営されているので、それぞれのシステムで用いられる鍵データベースが異なるものとなることは多い。

[0017] このような場合において、それぞれの鍵データベースにより、１個の共有データを暗号化した暗号化共有データを保持しているとする。

[0018] このとき、共有データの更新が発生すると、まず、第１の鍵データベースにおいて、ルート鍵を用いて、中間ノードの暗号化鍵を復号し、得られた鍵を用いて、リーフの暗号化鍵を復号し、得られた鍵を用いて、更新された共有データを暗号化して、保持する。次に、第１の鍵データベースの場合と同様に、第２の鍵データベースにおいて、ルート鍵を用いて、中間ノードの暗号化鍵を復号し、得られた鍵を用いて、リーフの暗号化鍵を復号し、得られた鍵を用いて、更新された共有データを暗号化して、保持する。

[0019] このように、異なる木構造の２個の鍵データベースを用いて、１個の共有データを暗号化して保持する場合には、それぞれの鍵データベースにおいて、ルートからリーフへの方向の鍵の復号処理が発生する。このため、情報処理装置の負荷が大きくなるという問題がある。

[0020] 上記の問題を解決するために、本発明は、複数の暗復号システムにおいて同一のデータをそれぞれ暗号化して保持する場合において、処理の負荷が大きくならないようにすることができる情報処理装置、方法、プログラム及び

集積回路を提供することを目的とする。

課題を解決するための手段

[0021] 上記目的を達成するために、本発明の一実施態様である情報処理装置は、それぞれデータを暗号化して保管する複数の暗復号システムを有する情報処理装置であって、一の暗復号システムにおける暗号化の対象データを取得するデータ取得手段と、前記対象データが、他の暗復号システムにおいて暗号化されて保管されているか否かを判断する判断手段と、保管されていると判断する場合に、他の暗復号システムにおいて保管されている暗号化データの鍵を取得する鍵取得手段と、前記一の暗復号システムにおいて用いられる鍵記憶手段と、前記一の暗復号システムにおいて、前記対象データに対応付けて、取得した前記鍵を前記鍵記憶手段に書き込む鍵書込手段とを備えることを特徴とする。

発明の効果

[0022] このように構成されているので、他の暗復号システムの鍵を、一の暗復号システムから直接復号することができる。これにより、他の暗復号システムにおいて前記鍵を取得する手間が省け、情報処理装置の負荷が大きくならないようにすることができる。

図面の簡単な説明

[0023] [図1]本発明の実施の形態１の情報処理装置１０のハードウェア構成を示すブロック図である。

[図2]情報処理装置１０のソフトウェア構成を示すブロック図である。

[図3]鍵データベースＡ１２０及び鍵データベースＢ１２１の木構造を示す。

[図4]ノード情報構造体１５０のデータ構造の一例を示す。

[図5]ノード情報構造体１６０のデータ構造の一例を示す。

[図6]管理テーブル２２０のデータ構造の一例を示す。

[図7]暗復号処理部１１４への鍵のロードの動作を示すフローチャートである。

[図8]データの暗復号の動作を示すフローチャートである。

[図9]共有しているデータＢを同期して更新する動作を示すフローチャートである。

[図10]管理テーブル２２０の更新の動作を示すフローチャートである。図１１へ続く。

[図11]管理テーブル２２０の更新の動作を示すフローチャートである。図１２へ続く。

[図12]管理テーブル２２０の更新の動作を示すフローチャートである。図１１から続く。

[図13]鍵の取得の動作を示すフローチャートである。

[図14]共有データの更新の動作を示すフローチャートである。

[図15]本発明の実施の形態２の情報処理装置１０が備える暗復号処理部２６０の構成を示すブロック図である。

[図16]本発明の実施の形態３の情報処理装置１０が備える暗復号処理部２７０の構成を示すブロック図である。

[図17]鍵テーブル２７４のデータ構造の一例を示す。

[図18]鍵テーブル２７４の別のデータ構造の一例を示す。

[図19]鍵格納部３３０のデータ構造の一例を示す。

[図20]ブロック管理テーブル３３１のデータ構造の一例を示す。

[図21]変形例としての鍵データベースＡ２８３及び鍵データベースＢ２８４の木構造の一例を示す。

[図22]変形例としての管理テーブルの管理情報３００のデータ構造の一例を示す。

[図23]変形例としての鍵管理ソフトウェアによる管理テーブルの更新処理を示すフローチャートである。

[図24]変形例としての、暗号化データのハッシュ値を用いる場合の管理テーブル３２０の一例を示す。

[図25]変形例として同期すべきデータの鍵の取得を示すフローチャートである。

[図26]変形例として共有データを同期するよう指示された場合に、他の暗復号システムが管理する共有データの更新処理を示すフローチャートである。

[図27]変形例として、暗号化された共有データの更新の指示が外部から供給される情報処理装置のソフトウェア構成を示す。

[図28]変形例として、暗号化された共有データの更新の指示が外部から供給された際のデータ同期処理を示すフローチャートである。

発明を実施するための形態

[0024] 請求項１に記載の態様である情報処理装置は、それぞれデータを暗号化して保管する複数の暗復号システムを有する情報処理装置であって、一の暗復号システムにおける暗号化の対象データを取得するデータ取得手段と、前記対象データが、他の暗復号システムにおいて暗号化されて保管されているか否かを判断する判断手段と、保管されていると判断する場合に、他の暗復号システムにおいて保管されている暗号化データの鍵を取得する鍵取得手段と、前記一の暗復号システムにおいて用いられる鍵記憶手段と、前記一の暗復号システムにおいて、前記対象データに対応付けて、取得した前記鍵を前記鍵記憶手段に書き込む鍵書込手段とを備えることを特徴とする。

[0025] また、請求項２に記載の態様である情報処理装置は、それぞれデータを暗号化して記憶する第１暗復号システム及び第２暗復号システムを有する情報処理装置であって、前記第１暗復号システムにおける暗号化の対象データを取得するデータ取得手段と、前記対象データを暗号化して生成した暗号化データが、前記第２暗復号システムにおいて記憶されているか否かを判断する判断手段と、記憶されていると判断する場合に、前記第２暗復号システムにおいて前記暗号化データを暗号化するために用いられる第２鍵を取得する鍵取得手段と、前記第１暗復号システムにおいて用いられる第１鍵記憶手段と、前記第１暗復号システムにおいて、前記対象データを暗号化するために用いられる第１鍵を用いて、取得した前記第２鍵を暗号化して暗号化第２鍵を生成する暗復号化手段と、前記第１暗復号システムにおいて、前記対象データに対応付けて、生成した前記暗号化第２鍵を前記第１鍵記憶手段に書き込

む鍵書込手段とを備えることを特徴とする。

[0026] また、請求項３に記載の態様の前記情報処理装置は、さらに、前記第２暗復号システムにおいて、前記暗号化データとして、前記第２鍵を用いて前記対象データを暗号化して生成した第２暗号化対象データを記憶している第２データ格納手段を備え、前記判断手段は、前記暗号化データとしての前記第２暗号化対象データが、前記第２データ格納手段に記憶されているか否かを判断する。

[0027] また、請求項４に記載の態様の前記情報処理装置において、前記暗復号化手段は、さらに、前記第１暗復号システムにおいて、前記第１鍵を用いて前記対象データを暗号化して第１暗号化対象データを生成し、前記情報処理装置は、さらに、前記第１暗復号システムにおける第１データ格納手段と、生成した前記第１暗号化対象データを前記第１データ格納手段に書き込むデータ書込手段とを備える。

[0028] また、請求項５に記載の態様の前記情報処理装置は、さらに、前記対象データに対応付けて、前記第２暗復号システムにおいて前記暗号化データが記憶されている位置を示す位置情報を含む管理テーブルを記憶しているテーブル記憶手段を備え、前記判断手段は、前記対象データに対応する位置情報が前記管理テーブルに記憶されているか否かを判断することにより、前記暗号化データが前記第２暗号化手段において記憶されているか否かを判断する。

[0029] また、請求項６に記載の態様の前記情報処理装置において、前記データ取得手段は、さらに、前記対象データの更新の指示を取得し、前記判断手段は、さらに、前記指示に係る前記対象データを暗号化して生成した暗号化データが、前記第２暗復号システムにおいて記憶されているか否かを判断し、前記鍵取得手段は、さらに、記憶されていると判断する場合に、前記第１鍵記憶手段から前記暗号化第２鍵を取得し、前記暗復号化手段は、さらに、取得した前記暗号化第２鍵を復号して第２鍵を生成し、生成した第２鍵を用いて、前記対象データの更新により得られた更新データを暗号化して第２暗号化更新データを生成し、前記データ書込手段は、さらに、生成した前記第２暗

号化更新データを、前記第２データ格納手段に記憶されている前記第２暗号化対象データに上書きする。

[0030] また、請求項７に記載の態様の前記情報処理装置において、前記暗復号化手段は、前記第１鍵に対応する復号鍵を用いて、前記暗号化第２鍵を復号する。

[0031] また、請求項８に記載の態様の前記情報処理装置において、前記管理テーブルは、前記対象データに対応付けて、さらに、前記第１鍵に対応する復号鍵が記憶されている位置を示す鍵位置情報を含み、前記暗復号手段は、前記鍵位置情報により示される位置から取得した前記復号鍵を用いる。

[0032] また、請求項９に記載の態様の前記情報処理装置において、前記暗復号化手段は、さらに、前記第１鍵を用いて、前記更新データを暗号化して第１暗号化更新データを生成し、前記データ書込手段は、さらに、生成した前記第１暗号化更新データを、前記第１データ格納手段に記憶されている前記第１暗号化対象データに上書きする。

[0033] また、請求項１０に記載の態様の前記情報処理装置において、前記データ書込手段は、前記第１暗号化更新データを前記第１データ格納手段に記憶されている前記第１暗号化対象データに上書きした後、同期指示を受け取った場合に、前記第２暗号化更新データを、前記第２データ格納手段に記憶されている前記第２暗号化対象データに上書きする。

[0034] また、請求項１１に記載の態様の前記情報処理装置において、前記管理テーブルに含まれる前記位置情報は、前記第２データ格納手段において前記第２暗号化対象データが記憶されている位置を示し、前記データ書込手段は、前記位置情報により示される位置において、前記第２暗号化更新データを書き込む。

[0035] また、請求項１２に記載の態様の前記情報処理装置において、前記暗復号化手段は、さらに、前記第１データ格納手段に記憶されている前記第１暗号化対象データを復号して、対象データを生成し、生成した対象データを基にして得られた更新データを暗号化する。

[0036] また、請求項１３に記載の態様の前記情報処理装置において、前記管理テーブルは、前記対象データの要約値と前記位置情報とを対応付けて含み、前記判断手段は、前記対象データからその要約値を算出し、得られた要約値に対応する前記位置情報が前記管理テーブルに記憶されているか否かを判断する。

[0037] また、請求項１４に記載の態様の前記情報処理装置において、前記管理テーブルは、前記第１暗号化対象データの要約値と前記位置情報とを対応付けて含み、前記判断手段は、第１データ格納手段に記憶されている前記第１暗号化対象データからその要約値を算出し、得られた要約値に対応する前記位置情報が前記管理テーブルに記憶されているか否かを判断する。

[0038] また、請求項１５に記載の態様の前記情報処理装置において、前記情報処理装置は、さらに、前記第２暗復号システムにおいて用いられる第２鍵記憶手段を備え、前記データ取得手段は、さらに、前記第２暗復号システムにおける暗号化の対象データを取得し、前記判断手段は、さらに、前記対象データを暗号化して生成した暗号化データが、前記第１暗復号システムにおいて記憶されているか否かを判断し、前記鍵取得手段は、さらに、記憶されていると判断する場合に、前記第１暗復号システムにおいて前記暗号化データを暗号化するために用いられる第１鍵を取得し、前記暗復号化手段は、さらに、前記第２暗復号システムにおいて、前記対象データを暗号化するために用いられる第２鍵を用いて、取得した前記第１鍵を暗号化して暗号化第１鍵を生成し、前記鍵書込手段は、さらに、前記第２暗復号システムにおいて、前記対象データに対応付けて、生成した前記暗号化第１鍵を前記第２鍵記憶手段に書き込む。

[0039] また、請求項１６に記載の態様の前記情報処理装置において、前記暗復号化手段は、さらに、前記第２暗復号システムにおいて、前記第２鍵を用いて前記対象データを暗号化して第２暗号化対象データを生成し、前記情報処理装置は、さらに、前記第２暗復号システムにおける第２データ格納手段と、生成した前記第２暗号化対象データを前記第２データ格納手段に書き込むデ

ータ書込手段とを備える。

[0040] また、請求項１７に記載の態様の前記情報処理装置において、前記データ取得手段は、さらに、前記対象データの更新の指示を取得し、前記判断手段は、さらに、前記指示に係る前記対象データを暗号化して生成した暗号化データが、前記第１暗復号システムにおいて記憶されているか否かを判断し、前記鍵取得手段は、さらに、記憶されていると判断する場合に、前記第２鍵記憶手段から前記暗号化第１鍵を取得し、前記暗復号化手段は、さらに、取得した前記暗号化第１鍵を復号して第１鍵を生成し、生成した第１鍵を用いて、前記対象データの更新により得られた更新データを暗号化して第１暗号化更新データを生成し、前記データ書込手段は、さらに、生成した前記第１暗号化更新データを、前記第１データ格納手段に記憶されている前記第１暗号化対象データに上書きする。

[0041] また、請求項１８に記載の態様の前記情報処理装置において、前記第１鍵記憶手段は、第１暗復号システムにおいて、鍵を階層構造により管理し、階層構造の各鍵の下位には、当該鍵を用いて復号できるように暗号化された鍵が割り当てられており、鍵書込手段は、前記暗号化第２鍵を、前記第２鍵の下位に割り当てて書き込む。

[0042] また、請求項１９に記載の態様の前記情報処理装置において、前記情報処理装置は、さらに、第１暗復号システムにおける暗号化データを利用するアプリケーションプログラムに従って動作するプロセッサを備えており、前記アプリケーションプログラムは、暗号化の対象データを出力する命令を含み、前記プロセッサは、前記データ取得手段に対して、暗号化の対象データを出力する。

[0043] また、請求項２０に記載の態様の前記情報処理装置において、前記情報処理装置は、さらに、前記第１暗復号システムにおいて復号された鍵を、前記第１暗復号システム用であることを示す第１タイプ情報と対応付けて保持し、前記第２暗復号システムにおいて復号された鍵を、前記第２暗復号システム用であることを示す第２タイプ情報と対応付けて保持する鍵格納手段を備

え、前記暗復号化手段は、前記第１暗復号システムにおいては、前記第１タイプ情報と対応付けられた鍵を用いて復号を行い、前記暗復号化手段は、前記第２暗復号システムにおいては、前記第２タイプ情報と対応付けられた鍵を用いて暗号化を行い、前記情報処理装置は、さらに、前記第１暗復号システムにおける復号の結果、前記第１タイプ情報と対応付けられて前記鍵格納手段に保持された鍵について、前記第１タイプ情報を前記第２暗復号システム用であることを示す前記第２タイプ情報に書き換えることで、前記鍵を用いた前記更新データの暗号化を前記第２暗復号システムにおいて行わせる制御手段を備える。

[0044] また、請求項２１に記載の態様の前記情報処理装置において、前記鍵格納手段は、所定の容量を持つ複数のブロックから構成されており、保持する鍵それぞれがどのブロックに格納されているかを示すブロック情報を、前記保持する鍵それぞれと対応付けて保持している。

[0045] また、請求項２２に記載の態様の前記情報処理装置において、前記暗復号化手段は、制御部と、前記第１暗復号システム用の前記第１鍵を保持する鍵格納部と、前記鍵格納部に保持されている前記第１鍵を用いて、暗号化する暗復号エンジン部とを備え、前記制御部は、前記第１鍵を取得して前記鍵格納部に保持させるにあたって、前記鍵格納部の空き領域が不足している場合に、前記鍵格納部が既に保持している一の鍵を、前記暗復号エンジン部により、暗号化して前記鍵格納部の外に退避し、前記鍵格納部において、退避対象の前記鍵が保持されていた領域に取得した前記第１鍵を上書きし、前記第１暗復号システムにおける前記第１鍵を用いた暗号化が完了した後、退避した前記暗号化鍵を、前記暗復号エンジン部により、復号して前記第１鍵が保持されている領域に上書きする。

[0046] また、請求項２３に記載の態様の方法は、それぞれデータを暗号化して記憶する第１暗復号システム及び第２暗復号システムを有し、前記第１暗復号システムにおいて用いられる第１鍵記憶手段を備える情報処理装置において用いられる方法であって、前記第１暗復号システムにおける暗号化の対象デ

ータを取得するデータ取得ステップと、前記対象データを暗号化して生成した暗号化データが、前記第２暗復号システムにおいて記憶されているか否かを判断する判断ステップと、記憶されていると判断する場合に、前記第２暗復号システムにおいて前記暗号化データを暗号化するために用いられる第２鍵を取得する鍵取得ステップと、前記第１暗復号システムにおいて、前記対象データを暗号化するために用いられる第１鍵を用いて、取得した前記第２鍵を暗号化して暗号化第２鍵を生成する暗復号化ステップと、前記第１暗復号システムにおいて、前記対象データに対応付けて、生成した前記暗号化第２鍵を前記第１鍵記憶手段に書き込む鍵書込ステップとを備えることを特徴とする。

[0047] また、請求項２４に記載の態様のコンピュータプログラムは、それぞれデータを暗号化して記憶する第１暗復号システム及び第２暗復号システムを有し、前記第１暗復号システムにおいて用いられる第１鍵記憶手段を備える情報処理装置において用いられるコンピュータプログラムであって、コンピュータである前記情報処理装置に、前記第１暗復号システムにおける暗号化の対象データを取得するデータ取得ステップと、前記対象データを暗号化して生成した暗号化データが、前記第２暗復号システムにおいて記憶されているか否かを判断する判断ステップと、記憶されていると判断する場合に、前記第２暗復号システムにおいて前記暗号化データを暗号化するために用いられる第２鍵を取得する鍵取得ステップと、前記第１暗復号システムにおいて、前記対象データを暗号化するために用いられる第１鍵を用いて、取得した前記第２鍵を暗号化して暗号化第２鍵を生成する暗復号化ステップと、前記第１暗復号システムにおいて、前記対象データに対応付けて、生成した前記暗号化第２鍵を前記第１鍵記憶手段に書き込む鍵書込ステップとを実行させるためのコンピュータプログラムであることを特徴とする。

[0048] また、請求項２５に記載の態様の前記コンピュータプログラムは、コンピュータ読み取り可能な記録媒体に記録されている。

[0049] また、請求項２６に記載の態様の集積回路は、それぞれデータを暗号化し

て記憶する第１暗復号システム及び第２暗復号システムを有する集積回路であって、前記第１暗復号システムにおける暗号化の対象データを取得するデータ取得手段と、前記対象データを暗号化して生成した暗号化データが、前記第２暗復号システムにおいて記憶されているか否かを判断する判断手段と、記憶されていると判断する場合に、前記第２暗復号システムにおいて前記暗号化データを暗号化するために用いられる第２鍵を取得する鍵取得手段と、前記第１暗復号システムにおいて用いられる第１鍵記憶手段と、前記第１暗復号システムにおいて、前記対象データを暗号化するために用いられる第１鍵を用いて、取得した前記第２鍵を暗号化して暗号化第２鍵を生成する暗復号化手段と、前記第１暗復号システムにおいて、前記対象データに対応付けて、生成した前記暗号化第２鍵を前記第１鍵記憶手段に書き込む鍵書込手段とを備えることを特徴とする。

[0050] 以下に、本発明の実施の形態について、図面を参照しながら説明を行う。

[0051] １．実施の形態１

本発明に係る１の実施の形態としての情報処理装置１０について説明する。

[0052] （情報処理装置１０の概要）

情報処理装置１０においては、第１の暗復号システム及び第２の暗復号システムがそれぞれ独立して動作し、第１及び第２の暗復号システム間で、１個のデータを共有して利用する。第１及び第２の暗復号システムは、異なる暗復号システムであり、それぞれ、鍵データベース及び暗号化されたデータから構成される。

[0053] 一例として、情報処理装置１０は、音楽を配信する音楽配信システム及び映画を配信する映画配信システムを利用し、音楽配信システムから音楽の供給を受け、映画配信システムから映画の供給を受ける。音楽配信システムと、映画配信システムとは、異なる音楽配信業者と映画配信業者とにより運営されている。第１の暗復号システムは、音楽配信システムのための暗復号システムであり、第２の暗復号システムは、映画配信システムのための暗復号

システムである。第１及び第２の暗復号システムにおいて、共有するデータの一例は、情報処理装置１０の利用者の住所である。

[0054] （住所を共有する場合）

ここでは、一例として、住所を共有する場合について説明する。

[0055] なお、映画配信システムにおける第２の暗復号システムにおいて、既に利用者の暗号化された住所が保持されているものとする。具体的には、情報処理装置１０は、第２の暗復号システムのためのサブ暗号化データ格納部を備えており、このサブ暗号化データ格納部は、第２の暗復号システムの第２鍵を用いて、対象データである住所を暗号化して生成した第２暗号化対象データつまり暗号化された住所を記憶しているものとする。しかし、第１の暗復号システムにおいては、まだ利用者の暗号化された住所を保持していないものとする。

[0056] 情報処理装置１０は、音楽配信システムにおける第１の暗復号システムにおいて、利用者の住所を暗号化して保持するために、暗号化の対象データである利用者の住所を取得する。次に、対象データである住所を暗号化して生成した暗号化データ（暗号化された住所）が、第２の暗復号システムにおいて記憶されているか否かを判断する。具体的には、情報処理装置１０は、第２暗号化対象データ（暗号化された住所）が、第２の暗復号システムのためサブ暗号化データ格納部に記憶されているか否かを判断する。次に、暗号化データ（暗号化された住所）が第２の暗復号システムにおいて記憶されていると判断する場合に、第２の暗復号システムにおいて前記暗号化データ（暗号化された住所）を暗号化するために用いられている第２鍵を、第２の暗復号システムから取得する。ここで、情報処理装置１０は、第１の暗復号システムにおいて用いられる鍵データベースＡを保持している。情報処理装置１０は、第１の暗復号システムにおいて、前記対象データ（利用者の住所）を暗号化するために用いられる第１鍵を用いて、取得した前記第２鍵を暗号化して暗号化第２鍵を生成し、第１の暗復号システムの鍵データベースＡにおいて、前記対象データ（利用者の住所）に対応付けて、生成した前記暗号化

第２鍵を鍵データベースＡに書き込む。

[0057] また、情報処理装置１０は、第１の暗復号システムにおいて、前記第１鍵を用いて前記対象データ（利用者の住所）を暗号化して第１暗号化対象データ（暗号化された住所）を生成する。情報処理装置１０は、第１暗号化対象データ（暗号化された住所）を記憶するためのサブ暗号化データ格納部を備えており、第１の暗復号システムのためのサブ暗号化データ格納部に、生成した前記第１暗号化対象データ（暗号化された住所）を書き込む。

[0058] 以上により、第１の暗復号システムにおいて、暗号化された住所を保持することにより、第１の暗復号システムと第２の暗復号システムにおいて、住所を共有することになる。さらに、第１の暗復号システムにおいては、住所に対応付けて、第２の暗復号システムにおいて住所の暗号化に用いられた第２鍵を、第１の暗復号システムにおいて、暗号化して保持することとなる。

[0059] （共有している住所を更新する場合）

次に、一例として、情報処理装置１０の利用者が、第１の暗復号システムと第２の暗復号システムにおいて、共有している対象データである住所を更新する場合について説明する。

[0060] 情報処理装置１０は、第１の暗復号システムにおいて、対象データである住所の更新の指示を取得する。情報処理装置１０は、上記と同様にして、さらに、前記指示に係る前記対象データ（旧住所）を暗号化して生成した暗号化データ（暗号化された旧住所）が、第２の暗復号システムにおいて記憶されているか否かを判断する。記憶されていると判断する場合に、鍵データベースＡから前記暗号化第２鍵を取得し、取得した前記暗号化第２鍵を復号して第２鍵を生成し、生成した第２鍵を用いて、前記対象データ（旧住所）の更新により得られた更新データ（新住所）を暗号化して第２暗号化更新データ（暗号化された新住所）を生成し、生成した前記第２暗号化更新データ（暗号化された新住所）を、第２の暗号化システムのためのサブ暗号化データ格納部に記憶されている前記第２暗号化対象データ（暗号化された旧住所）に上書きする。

[0061] また、情報処理装置１０は、第１の暗復号システムにおいて、前記第１鍵を用いて、更新データ（新住所）を暗号化して第１暗号化更新データ（暗号化された新住所）を生成し、生成した前記第１暗号化更新データ（暗号化された新住所）を、第１の暗号化システムのためのサブ暗号化データ格納部に記憶されている前記第１暗号化対象データ（暗号化された旧住所）に上書きする。

[0062] 以上により、第２の暗復号システムに依存することなく、第１の暗復号システムのみで、第２の暗復号システムにおいて用いられている第２鍵を知ることができる。

[0063] １．１　情報処理装置１０のハードウェア構成

情報処理装置１０は、図１に示すように、ＣＰＵ１１１、第１記憶部１１２、第２記憶部１１３、暗復号処理部１１４、バス１１５及び入出力部（図示していない）から構成される。ＣＰＵ１１１、第１記憶部１１２、第２記憶部１１３、暗復号処理部１１４及び入出力部は、バス１１５を介して互いに接続されている。

[0064] 以下、情報処理装置１０の各構成要素の詳細について説明する。

[0065] ＣＰＵ１１１は、マイクロプロセッサであって、第１記憶部１１２に格納されているプログラム等に含まれる命令コードを読み出し、解読し、実行することにより、情報処理装置１０全体の動作を制御する。

[0066] 第１記憶部１１２は、揮発性の半導体メモリにより構成され、鍵管理ソフトウェア１１６、アプリケーションプログラムＡ１１７、アプリケーションプログラムＢ１１８、データアクセス部１１９、鍵データベースＡ１２０及び鍵データベースＢ１２１を格納している。

[0067] 第２記憶部１１３は、ハードディスクユニットから構成され、暗号化データ格納部１２２を有している。暗号化データ格納部１２２は、サブ暗号化データ格納部１２２ａ及びサブ暗号化データ格納部１２２ｂから構成されている。暗号化データ格納部１２２は、アプリケーションプログラムＡ１１７やアプリケーションプログラムＢ１１８などで使用する暗号化されたデータを

格納する。サブ暗号化データ格納部１２２ａは、アプリケーションプログラムＡ１１７で使用する暗号化されたデータを格納する。サブ暗号化データ格納部１２２ｂは、アプリケーションプログラムＢ１１８で使用する暗号化されたデータを格納する。

[0068] 暗復号処理部１１４は、不揮発性メモリ部１２３、暗復号エンジン部１２４、鍵データベースＢ用鍵格納部１２５及び鍵データベースＡ用鍵格納部１２６から構成されており、暗復号処理部１１４は、暗復号処理部１１４の外部からの処理データの盗み取り及び改竄ができないように耐タンパ化されている。

[0069] 不揮発性メモリ部１２３は、外部電源から電力が供給されない場合でも、記憶しているデータが失われない不揮発性の半導体メモリから構成されている。不揮発性メモリ部１２３は、鍵データベースＡ用のルート鍵１２７と鍵データベースＢ用のルート鍵１２８を格納している。

[0070] 鍵データベースＡ用のルート鍵１２７及び鍵データベースＢ用のルート鍵１２８は、公開鍵暗号方式（public key cryptosystem、非対称暗号方式asymmetric key cryptosystemとも呼ぶ。）の秘密鍵（私有鍵）や、共通鍵暗号方式（secret key cryptosystem、対称暗号方式symmetric key cryptosystemとも呼ぶ）の秘密鍵である。また、鍵データベースＡ用のルート鍵１２７及び鍵データベースＢ用のルート鍵１２８は、それぞれ、鍵データベースＡ及び鍵データベースＢのルートに対応する鍵である。鍵データベースＡ用のルート鍵１２７及び鍵データベースＢ用のルート鍵１２８は、鍵データベースＡ及び鍵データベースＢの他のすべてのノードの鍵の復号に用いる鍵であるので、第１記憶部１１２上の鍵データベースＡ１２０や鍵データベースＢ１２１ではなく、耐タンパ化された暗復号処理部１１４により管理され、保持されている。なお、鍵データベースＡ１２０及び鍵データベースＢ１２１に含まれる鍵の全てを耐タンパ化された暗復号処理部１１４の不揮発性メモリ部１２３に記録すると、暗復号処理部１１４に求められる記録容量が大きくなってしまうため、他の全てのノードの鍵を復号する際に必要となるルート鍵

だけを耐タンパ化された暗復号処理部１１４の不揮発性メモリ部１２３において保護している。

[0071] 暗復号エンジン部１２４は、暗号化された鍵の復号、鍵の暗号化、暗号化されたデータの復号及びデータの暗号化を行う。暗復号においては、公開鍵暗号方式であるＲＳＡ暗号や共通鍵暗号方式であるＡＥＳ暗号などの暗号アルゴリズムなどを用いる。

[0072] 鍵データベースＢ用鍵格納部１２５は、暗復号エンジン部１２４を利用する際に、鍵データベースＢ１２１で管理された鍵を格納する。

[0073] 鍵データベースＡ用鍵格納部１２６は、暗復号エンジン部１２４を利用する際に、鍵データベースＡ１２０で管理された鍵を格納する。

[0074] なお、鍵データベースＡ１２０、鍵データベースＡ用鍵格納部１２６、鍵データベースＡ用のルート鍵１２７及びサブ暗号化データ格納部１２２ａは、第１の暗復号システムを構成し、鍵データベースＢ１２１、鍵データベースＡ用鍵格納部１２５、鍵データベースＢ用のルート鍵１２８及びサブ暗号化データ格納部１２２ｂは、第２の暗復号システムを構成している。

[0075] １．２ 情報処理装置１０のソフトウェア構成

情報処理装置１０のソフトウェア構成について、図２を用いて説明する。

[0076] 情報処理装置１０では、アプリケーションプログラムＡ１１７及びアプリケーションプログラムＢ１１８は、それぞれ、鍵管理ソフトウェア１１６を介して、鍵データベースＡ１２０及び鍵データベースＢ１２１にアクセスし、データアクセス部１１９を介して、暗号化データ格納部１２２にアクセスする。なお、情報処理装置１０においては、図示していないＯＳ、デバイスドライバ、そのほかのアプリケーションプログラムも動作する。

[0077] なお、以下に説明するように、アプリケーションプログラムＡ１１７とアプリケーションプログラムＢ１１８とは、データＢを共有している。

[0078] （１）鍵データベースＡ１２０及び鍵データベースＢ１２１

ここでは、鍵データベースＡ１２０及び鍵データベースＢ１２１について説明する。

（鍵データベースＡ１２０）

鍵データベースＡ１２０は、ｎ分木である木構造を用いて、鍵を管理するデータベースであり、アプリケーションプログラムＡ１１７により利用される。鍵データベースＡ１２０により用いる木構造の一例を図３に示す。

[0079] 鍵データベースＡ１２０の木構造は、一例として、図３に示すように、４階層から構成され、１個のルート１３２、２個の中間ノード１３３及び１３４、４個のリーフ１３５～１３８及び１個のリーフ２３９から構成されている。ルート１３２の直下には、２個の中間ノード１３３及び１３４が接続し、中間ノード１３３の直下には、２個のリーフ１３５及び１３６が接続し、中間ノード１３４の直下には、２個のリーフ１３７及び１３８が接続している。また、リーフ１３８の直下には、１個のリーフ２３９が接続している。

[0080] ルート１３２には、鍵データベースＡ用のルート鍵１２７が割り当てられている。上述したように、ルート鍵１２７は、鍵データベースＡ１２０内ではなく、暗復号処理部１１４の不揮発性メモリ部１２３に格納されている。

[0081] 中間ノード１３３及び１３４には、それぞれ、鍵Ａ及び鍵Ｂが割り当てられ、リーフ１３５、１３６、１３７、１３８、２３９には、それぞれ、鍵Ｃ、鍵Ｄ、鍵Ｅ、鍵Ｆ及び鍵Ｉが割り当てられている。

[0082] 中間ノード１３３には、ルート鍵１２７を用いて暗号化された鍵Ａが格納され、中間ノード１３４には、ルート鍵１２７を用いて暗号化された鍵Ｂが格納される。リーフ１３５には、中間ノード１３３の鍵Ａを用いて暗号化された鍵Ｃが格納され、リーフ１３６には、中間ノード１３３の鍵Ａを用いて暗号化された鍵Ｄが格納され、リーフ１３７には、中間ノード１３４の鍵Ｂを用いて暗号化された鍵Ｅが格納され、リーフ１３８には、中間ノード１３４の鍵Ｂを用いて暗号化された鍵Ｆが格納されている。ここで、鍵Ｃ、鍵Ｄ、鍵Ｅ及び鍵Ｆは、それぞれ、データを暗号化又は復号するために使用される鍵である。

[0083] リーフ２３９には、後述する鍵データベースＢ１２１のリーフ１４２の鍵Ｉが暗号化されて格納されている。ここで、リーフ２３９に格納されている

暗号化された鍵Ｉは、リーフ１３８の鍵Ｆを用いて暗号化されたものである。

[0084] なお、一例として、図３に示すように、暗号化されたデータＡ（１４６）は、リーフ１３６に割り当てられた鍵Ｄを用いて、データＡを暗号化して生成したものであり、暗号化されたデータＢ（１４７）は、データＢをリーフ１３８に割り当てられた鍵Ｆを用いて暗号化して生成したものである。

[0085] 鍵データベースＡ１２０は、第１記憶部１１２において、複数のノード情報構造体を記憶しており、これらの複数のノード情報構造体により木構造を構成している。複数のノード情報構造体は、鍵データベースＡ１２０のルート、複数の中間ノード及び複数のリーフのそれぞれに対応しており、鍵データベースＡ１２０において鍵を管理するために使用される。図４に、鍵データベースＡ１２０のノード情報構造体１５０のデータ構造の一例を示す。

[0086] ノード情報構造体１５０は、図４に示すように、鍵長１５１、鍵１５２、親ノード識別子１５３、鍵ハンドラ値１５４、データハンドラ値１５５、データ１５６及びその他の付属情報１５７から構成される。

[0087] 鍵長１５１のフィールドには、暗復号を行う場合に使用する鍵の長さが格納される。格納される値はビット長やバイト長などの数値でもよい。さらに、予め決められている鍵の長さに対応する識別子でもよい。

[0088] 鍵１５２のフィールドには、暗復号を行う場合に使用する鍵を暗号化して生成した暗号化鍵が格納される。また、鍵１５２のフィールドには、暗号化鍵の存在する位置を示す位置情報が格納されてもよい。ただし、ルートに対応する鍵は、ノード情報構造体の鍵１５２のフィールドには格納されない。また、鍵１５２のフィールドに格納される暗号化鍵は、親ノード識別子１５３で指定されているノード番号により定まる中間ノード又はルートの鍵（各ノードの親ノードの鍵）を使用して暗号化されたものである。

[0089] 親ノード識別子１５３のフィールドには、当該ノード情報構造体１５０に対応するノードの親ノードを指定する識別子が格納される。また、親ノード識別子１５３のフィールドには、親ノードの位置を示す位置情報が格納され

るとしてもよい。さらに、予め決められている識別子や動的に生成した識別子を格納してもよい。これらの識別子は、親ノードを指定する。

[0090] 鍵ハンドラ値１５４のフィールドには、当該ノードに割り当てられた暗号化鍵が存在する位置を示す位置情報が格納される。暗号化鍵が存在しない場合には、ＮＵＬＬが格納される。

[0091] データハンドラ値１５５のフィールドには、当該ノード情報構造体１５０に対応する鍵を用いて暗号化されたデータが存在する場合に、当該暗号化データの生成の基になった平文データの存在する位置を示す位置情報が格納される。このような暗号化データが存在しない場合には、ＮＵＬＬが格納される。

[0092] データ１５６のフィールドには、ノード情報構造体１５０を用いてデータを格納する際に、暗号化されたデータが格納される。

[0093] その他の付属情報１５７は、他に各ノードが必要とする情報を格納するフィールドである。

[0094] 一例として、リーフ２３９のノード情報構造体の鍵のフィールドには、後述する鍵データベースＢ１２１のリーフ１４２に対応する鍵Ｉが暗号化されて格納されており、リーフ２３９のノード情報構造体の親ノード識別子には、リーフ１３８を識別する識別子（ノード番号）が格納されている。なお、リーフ１４２は、鍵データベースＢ１２１において、データＢを暗号化する鍵を格納するリーフである。

[0095] 以上説明したように、鍵データベースＡは、第１の暗復号システムにおいて、鍵を階層構造により管理している。階層構造の各鍵の下位には、当該鍵を用いて復号できるように暗号化された鍵が割り当てられている。

（鍵データベースＢ１２１）

鍵データベースＢ１２１は、ｎ分木である木構造を用いて、鍵を管理するデータベースであり、アプリケーションプログラムＢ１１８により利用される。鍵データベースＢ１２１により用いる木構造の一例を図３に示す。

[0096] 鍵データベースＢ１２１の木構造は、一例として、図３に示すように、４

階層から構成され、１個のルート１３９、２個の中間ノード１４０及び１４１、４個のリーフ１４２～１４５、及び１個のリーフ２４７から構成されている。ルート１３９の直下には、２個の中間ノード１４０及び１４１が接続し、中間ノード１４０の直下には、２個のリーフ１４２及び１４３が接続し、中間ノード１４１の直下には、２個のリーフ１４４及び１４５が接続している。また、リーフ１４２の直下には、リーフ２４７が接続している。

[0097] ルート１３９には、鍵データベースＢ用のルート鍵１２８が割り当てられている。上述したように、ルート鍵１２８は、鍵データベースＢ１２１内ではなく、暗復号処理部１１４の不揮発性メモリ部１２３に格納されている。

[0098] 中間ノード１４０及び１４１には、それぞれ、鍵Ｇ及び鍵Ｈが割り当てられ、リーフ１４２、１４３、１４４、１４５、２４７には、それぞれ、鍵Ｉ、鍵Ｊ、鍵Ｋ、鍵Ｌ及び鍵Ｆが割り当てられている。

[0099] 中間ノード１４０には、ルート鍵１２８を用いて暗号化された鍵Ｇが格納され、中間ノード１４１には、ルート鍵１２８を用いて暗号化された鍵Ｈが格納される。リーフ１４２には、中間ノード１４０の鍵Ｇを用いて暗号化された鍵Ｉが格納され、リーフ１４３には、中間ノード１４０の鍵Ｇを用いて暗号化された鍵Ｊが格納され、リーフ１４４には、中間ノード１４１の鍵Ｈを用いて暗号化された鍵Ｋが格納され、リーフ１４５には、中間ノード１４１の鍵Ｈを用いて暗号化された鍵Ｌが格納されている。ここで、鍵Ｉ、鍵Ｊ、鍵Ｋ及び鍵Ｌは、それぞれ、データを暗号化又は復号するために使用される鍵である。

[0100] リーフ２４７には、鍵データベースＡ１２０のリーフ１３８の鍵Ｆが暗号化されて格納されている。ここで、リーフ２４７に格納されている暗号化された鍵Ｆは、リーフ１４２の鍵Ｉを用いて暗号化されたものである。

[0101] なお、一例として、図３に示すように、暗号化されたデータＢ（１４８）は、リーフ１４２に割り当てられた鍵Ｉを用いて、データＢを暗号化して生成したものである。

[0102] ここで、図３に示す暗号化されたデータＢ（１４７）と、暗号化されたデ

ータＢ（１４８）とは、暗号化の基になるデータＢが共通している。つまり、アプリケーションプログラムＡ１１７とアプリケーションプログラムＢ１１８とは、データＢを共有している。

[0103] 鍵データベースＢ１２１は、第１記憶部１１２において、複数のノード情報構造体を記憶しており、これらの複数のノード情報構造体により木構造を構成している。複数のノード情報構造体は、鍵データベースＢ１２１のルート、複数の中間ノード及び複数のリーフのそれぞれに対応しており、鍵データベースＢ１２１において鍵を管理するために使用される。図５に、鍵データベースＢ１２１のノード情報構造体１６０のデータ構造の一例を示す。

[0104] ノード情報構造体１６０は、図５に示すように、暗号種別１６１、鍵長１６２、鍵やデータを格納した場所のリンク先情報１６３、親ノード識別子１６４、鍵ハンドラ値１６５、データハンドラ値及びその他の付属情報１６７から構成される。

[0105] 図５に示すノード情報構造体１６０は、図４に示すノード情報構造体１５０に含まれる鍵１５２及びデータ１５６に代えて、暗号種別１６１及びリンク先情報１６３を含む。その他の構成要素については、ここでは、説明を省略する。

[0106] 暗号種別１６１のフィールドには、ＲＳＡ暗号や楕円暗号などの公開鍵暗号方式や、ＡＥＳ暗号や３ＤＥＳ暗号などの共通鍵暗号方式の暗号アルゴリズムの名称や、前述の暗号アルゴリズムに対応する識別子が格納される。なお、公開鍵方式の場合には、本フィールドには、親ノードに割り当てられた公開鍵で暗号化された秘密鍵と、公開鍵が格納される。

[0107] リンク先情報１６３のフィールドには、暗復号に利用する鍵のファイルや、暗号化されたデータのファイルが存在する場所を指し示す情報が格納される。

[0108] 一例として、リーフ２４７のノード情報構造体のリンク先情報により示される位置には、鍵データベースＡ１２０のリーフ１３８に割り当てられた鍵Ｆが暗号化されて格納されており、リーフ２４７のノード情報構造体の親ノ

ード識別子には、リーフ１４２を識別する識別子（ノード番号）が格納されている。なお、リーフ１３８は、鍵データベースＡ１２０において、データＢを暗号化する鍵を格納するリーフである。

[0109] 以上説明したように、鍵データベースＢは、第２の暗復号システムにおいて、鍵を階層構造により管理している。階層構造の各鍵の下位には、当該鍵を用いて復号できるように暗号化された鍵が割り当てられている。

[0110] （２）暗号化データ格納部１２２

暗号化データ格納部１２２は、暗号化されたデータを格納する。暗号化データ格納部１２２は、サブ暗号化データ格納部１２２ａ及びサブ暗号化データ格納部１２２ｂから構成されている。

[0111] サブ暗号化データ格納部１２２ａは、一例として、リーフ１３６の鍵Ｄを用いて暗号化されたデータＡ（１４６）及びリーフ１３８の鍵Ｆを用いて暗号化されたデータＢ（１４７）を格納している。また、サブ暗号化データ格納部１２２ｂは、リーフ１４２の鍵Ｉを用いて暗号化されたデータＢ（１４８）を格納している。

[0112] ここで、図３に示す暗号化されたデータＢ（１４７）と、暗号化されたデータＢ（１４８）とは、暗号化の基になるデータＢが共通している。つまり、アプリケーションプログラムＡ１１７とアプリケーションプログラムＢ１１８とは、データＢを共有している。

[0113] （３）アプリケーションプログラムＡ１１７、アプリケーションプログラムＢ１１８及びデータアクセス部１１９

アプリケーションプログラムＡ１１７は、鍵データベースＡ１２０によって管理された鍵を用いて、暗号化データ格納部１２２に格納される暗号化データを利用するソフトウェアである。アプリケーションプログラムＡ１１７は、第１の暗復号システムに対するデータ処理を要求するコンピュータ命令を含んでいる。例えば、第１の暗復号システムに対するデータの新規の登録（暗号化して記憶）、参照（復号して参照）、更新（復号して更新し、再度暗号化して記憶）、削除などである。また、暗号化の対象データを出力する

命令を含む。

[0114] アプリケーションプログラムＢ１１８は、鍵データベースＢ１２１によって管理された鍵を用いて、暗号化データ格納部１２２に格納される暗号化データを利用するソフトウェアである。アプリケーションプログラムＢ１１８は、第２の暗復号システムに対するデータ処理を要求するコンピュータ命令を含んでいる。例えば、第２の暗復号システムに対するデータの新規の登録（暗号化して記憶）、参照（復号して参照）、更新（復号して更新し、再度暗号化して記憶）、削除などである。また、暗号化の対象データを出力する命令を含む。

[0115] データアクセス部１１９は、暗号化データ格納部１２２にアクセスし、暗号化データを読み出し、更新し、又は書き込むためのソフトウェアである。

[0116] （４）鍵管理ソフトウェア１１６

鍵管理ソフトウェア１１６は、図２に示すように、利用データベース判定部２０１、平文データ抽出部２０２、ハッシュ値生成部２０３、ハッシュ値判定部２０４、ハンドラ値判定部２０５、鍵取得部２０６、管理テーブル格納部２０７、管理テーブル更新部２０８及び鍵書込部２０９から構成されている。ここで、ハッシュ値生成部２０３、ハッシュ値判定部２０４及び管理テーブル格納部２０７は、一の暗復号システムにおける暗号化の対象データが、他の暗復号システムにおいて暗号化されて保管されているか否かを判断する判断部を構成している。鍵取得部２０６は、この判断部により、保管されていると判断する場合に、他の暗復号システムにおいて保管されている暗号化データの鍵を取得する。鍵書込部２０９は、前記一の暗復号システムにおいて、前記対象データに対応付けて、取得した前記鍵を鍵データベースＡ１２０（又は鍵データベースＢ１２１）に書き込む。

（管理テーブル格納部２０７）

管理テーブル格納部２０７は、図６に示す管理テーブル２２０を保持している。

[0117] 管理テーブル２２０は、暗号化データ格納部１２２に存在する複数の暗号

化データのそれぞれが、鍵データベースＡ１２０と鍵データベースＢ１２１の鍵を用いて、どのように管理されているかを示す。管理テーブル２２０は、暗号化されたデータで管理するデータから生成したハッシュ値をエントリとして構成される。

[0118] 管理テーブル２２０は、図６に示すように、複数の管理情報から構成されている。複数の管理情報は、それぞれ、暗号化データ格納部１２２に格納されている複数の暗号化データに対応している。各管理情報は、ハッシュ値、第１データハンドラ値、第２データハンドラ値、第１鍵ハンドラ値及び第２鍵ハンドラ値から構成されている。

[0119] ハッシュ値は、対応する暗号化データの基になった平文データから生成されたハッシュ値である。

[0120] 第１データハンドラ値は、当該管理情報のハッシュ値の生成の基になった平文データであって、鍵データベースＡのリーフに割り当てられた暗号化データの基になった平文データのデータハンドラ値である。平文データのデータハンドラ値は、当該平文データが存在する位置を示す位置情報である。この第１データハンドラ値は、図４のノード情報構造体１５０のデータハンドラ値１５５に対応する。平文データが、鍵データベースＡ１２０により管理されていない場合には、第１データハンドラ値は、ＮＵＬＬ値である。

[0121] 第２データハンドラ値は、当該管理情報のハッシュ値の生成の基になった平文データであって、鍵データベースＢのリーフに割り当てられた暗号化データの基になった平文データのデータハンドラ値である。平文データのデータハンドラ値は、当該平文データが存在する位置を示す位置情報である。この第２データハンドラ値は、図５のノード情報構造体１６０のデータハンドラ値１６６に対応する。平文データが、鍵データベースＢ１２１により管理されていない場合には、第２データハンドラ値は、ＮＵＬＬ値である。

[0122] 第１鍵ハンドラ値は、当該管理情報のハッシュ値の生成の基になった平文データを暗号化する鍵のハンドラ値である。言い換えると、対応する暗号化データが、鍵データベースＡ１２０により管理されている場合において、当

該暗号化データを暗号化するために用いられた鍵を暗号化して生成した暗号化鍵が、鍵データベースＡ１２０のどこに存在しているかを示す位置データである。対応する暗号化データが、鍵データベースＡ１２０により管理されていない場合には、第１鍵ハンドラ値は、ＮＵＬＬ値である。この第１鍵ハンドラ値は、図４のノード情報構造体の鍵ハンドラ値１５４に対応する。

[0123] 第２鍵ハンドラ値は、当該管理情報のハッシュ値の生成の基になった平文データを暗号化する鍵のハンドラ値である。言い換えると、対応する暗号化データが、鍵データベースＢ１２１により管理されている場合において、当該暗号化データを暗号化するために用いられた鍵を暗号化して生成した暗号化鍵が、鍵データベースＢ１２１のどこに存在しているかを示す位置データである。対応する暗号化データが、鍵データベースＢ１２１により管理されていない場合には、第２鍵ハンドラ値は、ＮＵＬＬ値である。この第２鍵ハンドラ値は、図５のノード情報構造体１６０の鍵ハンドラ値１６５に対応する。

（鍵管理ソフトウェア１１６のその他の構成要素）

利用データベース判定部２０１は、要求元のアプリケーションプログラムから、ノード情報構造体を受け取り、受け取ったノード情報構造体を用いて、要求元のアプリケーションプログラムが、鍵データベースＡ１２０又は鍵データベースＢ１２１のどちらかを利用するかを判断する。受け取ったノード情報構造体が図４に示すノード情報構造体１５０である場合には、鍵データベースＡ１２０を利用すると決定する。受け取ったノード情報構造体が図５に示すノード情報構造体１６０である場合には、鍵データベースＢ１２１を利用すると決定する。次に、データベースの判定結果をハンドラ値判定部２０５へ出力する。

[0124] 平文データ抽出部２０２は、要求元のアプリケーションプログラムからノード情報構造体を取得し、取得したノード情報構造体からデータハンドラ値を抽出し、抽出したデータハンドラ値がＮＵＬＬでない場合には、抽出したデータハンドラ値により示される位置から平文データを取得し、取得した平

文データをハッシュ値生成部２０３へ出力する。このように、平文データ抽出部２０２は、一の暗復号システムにおける暗号化の対象データを取得するデータ取得部である。

[0125] ハッシュ値生成部２０３は、平文データ抽出部２０２から平文データを受け取り、受け取った平文データから、一意のハッシュ値（要約値）を生成する。たとえば、一方向性関数（ＳＨＡ１アルゴリズムなど）を利用して、一意なハッシュ値を生成し、生成したハッシュ値をハッシュ値判定部２０４へ出力する。

[0126] ハッシュ値判定部２０４は、ハッシュ値生成部２０３からハッシュ値を受け取り、管理テーブル格納部２０７が管理している管理テーブル２２０に格納されているハッシュ値を参照し、管理テーブル２２０にハッシュ値生成部２０３により生成されたハッシュ値と一致するハッシュ値が存在するか否かを判定する。判定結果をハンドラ値判定部２０５へ出力する。また、一致するハッシュ値が存在する場合に、そのハッシュ値を含む管理情報を管理テーブル２２０から読み出し、読み出した管理情報をハンドラ値判定部２０５へ出力する。

[0127] ハンドラ値判定部２０５は、利用データベース判定部２０１からデータベースの判定結果を受け取る。また、ハッシュ値判定部２０４から判定結果を受け取る。一致するハッシュ値が存在する場合に、そのハッシュ値を含む管理情報を受け取る。受け取った判定結果が一致するハッシュ値が存在することを示す場合に、受け取った管理情報に含まれる管理情報に含まれる第１鍵ハンドラ値又は第２鍵ハンドラ値がＮＵＬＬか否か判定する。

[0128] 第１鍵ハンドラ値及び第２鍵ハンドラ値のうちのどちらについて判定するかについては、利用データベース判定部２０１から受け取ったデータベースの判定結果を用いる。つまり、データベースの判定結果が、鍵データベースＡの利用を示す場合には、鍵データベースＡのリーフの鍵ハンドラ値である第１鍵ハンドラ値について判定する。一方、データベースの判定結果が、鍵データベースＢの利用を示す場合には、鍵データベースＢのリーフの鍵ハン

ドラ値である第２鍵ハンドラ値について判定する。次に、その判定結果を鍵取得部２０６へ出力する。判定結果がＮＵＬＬでないことを示す場合に、さらに、データベースの判定結果が、鍵データベースＡの利用を示す場合には、第１鍵ハンドラ値を鍵取得部２０６へ出力する。データベースの判定結果が、鍵データベースＢの利用を示す場合には、第２鍵ハンドラ値を鍵取得部２０６へ出力する。

[0129] 鍵取得部２０６は、ハンドラ値判定部２０５から判定結果を受け取る。受け取った判定結果がＮＵＬＬでないことを示す場合には、さらに、鍵ハンドラ値を受け取る。次に、迂路取った鍵ハンドラ値により示される位置から、暗号化鍵を取得し、取得した暗号化鍵を暗復号処理部１１４の暗復号エンジン部１２４へ出力する。

[0130] 鍵書込部２０９は、鍵データベースＡ１２０又は鍵データベースＢ１２１のノード情報構造体を更新する。また、新たにノード情報構造体を生成し、生成したノード情報構造体を鍵データベースＡ１２０又は鍵データベースＢ１２１に追加して書き込む。また、鍵書込部２０９は、暗号化鍵を、当該鍵の下位に割り当てて書き込む。

[0131] 管理テーブル更新部２０８は、管理テーブル格納部２０７が管理している管理テーブルを更新する。

[0132] １．３　情報処理装置１０の動作説明

ここでは、情報処理装置１０の動作について説明する。

[0133] （１）暗復号処理部１１４への鍵のロードの動作及びデータの暗復号の動作

（ａ）暗復号処理部１１４への鍵のロードの動作について、図７に示すフローチャートを用いて説明する。

[0134] 鍵管理ソフトウェア１１６は、一例として、アプリケーションプログラムＡ１１７から図３に示す鍵Ａのロードを要求される（Ｓ４００）。

[0135] 次に、鍵管理ソフトウェア１１６は、鍵データベースＡ１２０から、指定された鍵Ａに対応するノードに格納されている暗号化鍵Ａを取得し、取得し

た暗号化鍵Ａを暗復号処理部１１４へ出力する（Ｓ４０１）。

[0136] 次に、暗復号処理部１１４は、鍵管理ソフトウェア１１６から暗号化鍵Ａを受け取り、暗復号エンジン部１２４により、暗号化鍵Ａを、不揮発性メモリ部１２３に格納されているルート鍵１２７を用いて復号し、得られた鍵Ａを鍵データベースＡ用鍵格納部１２６に格納する（Ｓ４０２）。

[0137] 次に、鍵管理ソフトウェア１１６は、暗復号処理部１１４から鍵Ａのロード終了を示す通知を受け取る（Ｓ４０３）。

[0138] 以上により、暗復号処理部１１４への鍵のロード処理が終了する。

[0139] 鍵Ｃ、鍵Ｄなどの暗復号処理部１１４へのロードについても上記と同様の動作により可能である。例えば、暗号化鍵Ｃを基にして鍵Ｃを暗復号処理部１１４へロードする場合には、上記のステップＳ４００～Ｓ４０３に従って鍵Ａをロードした後に、上記のステップＳ４００～Ｓ４０３と同様の動作をさせる。その場合に、特に、上記ステップＳ４０１において、鍵管理ソフトウェア１１６は、鍵データベースＡ１２０から暗号化鍵Ｃを取得し、ステップＳ４０２において、暗復号処理部１１４は、鍵データベースＡ用鍵格納部１２６に格納されている鍵Ａを用いて、暗号化鍵Ｃを復号すればよい。鍵Ｄのロード処理についても同様である。

[0140] このように、図３に示す鍵Ｃを暗復号処理部１１４へロードするためには、次のようにすればよい。

[0141] （ｉ）上記のステップＳ４００～Ｓ４０３に従って、鍵Ａをロードする。

[0142] （ｉｉ）鍵Ａがロードされた後に、上記に説明したように、ステップＳ４００～Ｓ４０３と同様にして、鍵Ｃをロードする。

[0143] また、図３の鍵データベースＡ１２０のリーフ２３９の鍵Ｉを暗復号処理部１１４へロードするためには、次のようにすればよい。

[0144] （ｉ）上記のステップＳ４００～Ｓ４０３と同様にして、鍵Ｂをロードする。

[0145] （ｉｉ）鍵Ｂがロードされた後に、上記のステップＳ４００～Ｓ４０３と同様にして、鍵Ｆをロードする。この場合、上記ステップＳ４０１において、

鍵管理ソフトウェア１１６は、鍵データベースＡ１２０から暗号化鍵Ｆを取得し、ステップＳ４０２において、暗復号処理部１１４は、鍵データベースＡ用鍵格納部１２６に格納されている鍵Ｂを用いて、暗号化鍵Ｆを復号する。

[0146] （iii）鍵Ｆがロードされた後に、上記のステップＳ４００～Ｓ４０３と同様にして、鍵Ｉをロードする。この場合、上記ステップＳ４０１において、鍵管理ソフトウェア１１６は、鍵データベースＡ１２０から暗号化鍵Ｉを取得し、ステップＳ４０２において、暗復号処理部１１４は、鍵データベースＡ用鍵格納部１２６に格納されている鍵Ｆを用いて、暗号化鍵Ｉを復号する。

[0147] また、アプリケーションプログラムＢ１１８から鍵のロードを要求される場合についても、上記と同様に動作させればよい。

[0148] （ｂ）次に、データの暗復号の動作について、図８に示すフローチャートを用いて説明する。ここでは、図３に示す暗号化されたデータＢ（１４７）を復号する場合を例として説明する。なお、鍵データベースＡ用鍵格納部１２６には、鍵Ｆが格納されているものとする。

[0149] 鍵Ｆが鍵データベースＡ用鍵格納部１２６に格納された後に、鍵管理ソフトウェア１１６は、アプリケーションプログラムＡ１１７から暗号化されたデータＢ（１４７）の復号処理を要求される（Ｓ４１０）。

[0150] 次に、鍵管理ソフトウェア１１６は、アプリケーションプログラムＡ１１７から暗号化されたデータＢ（１４７）を受け取り、暗号化されたデータＢ（１４７）を暗復号処理部１１４へ出力し、鍵Ｆを用いて復号を行うように、暗復号処理部１１４に依頼する（Ｓ４１１）。

[0151] 次に、暗復号処理部１１４は、暗号化されたデータＢ（１４７）を受け取り、受け取った暗号化されたデータＢ（１４７）を、暗復号エンジン部１２４により、鍵データベースＡ用鍵格納部１２６に格納された鍵Ｆを用いて復号し、データＢを出力する（Ｓ４１２）。

[0152] 次に、鍵管理ソフトウェア１１６は、暗復号処理部１１４からデータＢを

受け取り、データＢをアプリケーションプログラムＡ１１７へ出力し、復号の完了をアプリケーションプログラムＡ１１７に通知する（Ｓ４１３）。

[0153] 以上により、復号処理を終了する。

[0154] なお、データを暗号化する場合にも、上記と同様にすればよい。この場合、ステップ４１２において、暗復号エンジン部１２４は、鍵格納部に格納された鍵を用いてデータを暗号化すればよい。

[0155] （２）データの同期更新処理

上述したように、アプリケーションプログラムＡ１１７とアプリケーションプログラムＢ１１８とは、データＢを共有している。ここでは、共有しているデータＢを同期して更新する際の情報処理装置１０の動作について、図９に示すフローチャートを用いて説明する。

[0156] アプリケーションプログラムＡ１１７が、アプリケーションプログラムＢ１１８と共有しているデータＢを更新する際に、情報処理装置１０は、次のように動作する。

[0157] アプリケーションプログラムＡ１１７は、上述したように、鍵管理ソフトウェア１１６と鍵データベースＡ１２０を用いて、鍵データベースＡ１２０のルートからデータＢに対応するリーフ１３８までのそれぞれのノードに格納された暗号化鍵を順番に復号させる（Ｓ２０１）。

[0158] 次に、アプリケーションプログラムＡ１１７は、更新されたデータＢを、ステップＳ２０１で取得した鍵Ｆで暗号化するように、鍵管理ソフトウェア１１６に依頼し、鍵管理ソフトウェア１１６は、管理テーブル２２０を更新する（Ｓ２０２）。なお、このステップのさらに詳細な内容については、図１０～図１２を用いて後述する。

[0159] 次に、鍵管理ソフトウェア１１６は、管理テーブル２２０を用いて、暗号化の対象のデータ（更新する前のデータＢ）が、鍵データベースＡ１２０と鍵データベースＢ１２１とで共有しているデータであるか否かを判断する（Ｓ２０３）。共有しているデータであるか否かは、次のようにして行う。つまり、鍵管理ソフトウェア１１６は、更新する前のデータＢのハッシュ値を

ハッシュ値生成部２０３に生成させ、ハッシュ値判定部２０４に生成したハッシュ値と同じハッシュ値を含む管理情報が管理テーブル２２０に存在するか否かを判定させ、存在する場合に、ハンドラ値判定部２０５による判定は、次の通りとなる。

[0160] ハンドラ値判定部２０５は、この管理情報に含まれる第１鍵ハンドラ値及び第２鍵ハンドラ値のうち、指定された側の暗復号システムとは異なるもう一方の側の暗復号システムの鍵ハンドラ値が、ＮＵＬＬでない場合には、第１の暗復号システム及び第２の暗復号システムにおいて、共有していると決定する。この場合、ステップＳ２０４へ制御を移す。

[0161] 一方、ハンドラ値判定部２０５は、この管理情報に含まれる第１鍵ハンドラ値及び第２鍵ハンドラ値のうち、指定された側の暗復号システムとは異なるもう一方の側の暗復号システムの鍵ハンドラ値が、ＮＵＬＬである場合には、第１の暗復号システム及び第２の暗復号システムにおいて、共有していないと決定する。この場合、ステップＳ２０６へ制御を移す。

[0162] 次に、鍵管理ソフトウェア１１６は、データＢの同期処理で利用する鍵を取得する。つまり、相手側の鍵を取得する（Ｓ２０４）。なお、このステップの詳細な内容については、図１３を用いて後述する。

[0163] 次に、鍵管理ソフトウェア１１６は、相手側の共有するデータを同期して更新する（Ｓ２０５）。なお、このステップの詳細な内容については、図１４を用いて後述する。

[0164] 次に、鍵管理ソフトウェア１１６は、上記に述べたようにして、自身の更新されたデータＢを暗号化し、暗号化された更新データＢをサブ暗号化データ格納部１２２ａに上書きで書き込む（ステップＳ２０６）。次に、処理を終了する。

[0165] なお、上記の説明では、アプリケーションプログラムＡ１１７が、共有データを更新することとして説明を行ったが、アプリケーションプログラムＢ１１８も、同様な方法で、共有データを更新することができる。

[0166] ここで、ステップＳ２０３における判定結果及びその後の処理を整理する

と次のようになる。なお、ここでは、第１鍵ハンドラ値は、指定された側の暗復号システムの鍵ハンドラ値であり、第２鍵ハンドラ値は、もう一方の側の暗復号システムの鍵ハンドラ値であるとしている。

[0167] （ｉ）ステップＳ２０３において、第１鍵ハンドラ値と第２鍵ハンドラ値の両方が、ＮＵＬＬでない場合と判断された場合

この場合には、第１の暗復号システム及び第２の暗復号システムの両方が、対象のデータを有している。

[0168] 第２の暗復号システムにおける暗号化データの鍵を取得し、取得した鍵を第１の暗復号システムで暗号化し、第１の暗復号システムで暗号化鍵を記憶する。また、第２の暗復号システムにおいて、更新データを暗号化して暗号化更新データを生成し、生成した暗号化更新データにより暗号化データを上書きする。さらに、第１の暗復号システムにおいて、更新データを暗号化して暗号化更新データを生成し、生成した暗号化更新データにより暗号化データを上書きする。

[0169] （ｉｉ）ステップＳ２０３において、第１鍵ハンドラ値がＮＵＬＬであり、第２鍵ハンドラ値がＮＵＬＬでないと判断された場合

この場合には、第１の暗復号システムは、対象のデータを有しておらず、第２の暗復号システムは、対象のデータを有している。

[0170] 第２の暗復号システムにおける暗号化データの鍵を取得し、取得した鍵を第１の暗復号システムで暗号化し、第１の暗復号システムで暗号化鍵を記憶する。また、第２の暗復号システムにおいて、更新データを暗号化して暗号化更新データを生成し、生成した暗号化更新データにより暗号化データを上書きする。さらに、第１の暗復号システムにおいて、更新データを暗号化して暗号化更新データを生成し、生成した暗号化更新データを書き込む。

[0171] （ｉｉｉ）ステップＳ２０３において、第１鍵ハンドラ値がＮＵＬＬでなく、第２鍵ハンドラ値がＮＵＬＬであると判断された場合

この場合には、第１の暗復号システムは、対象のデータを有しており、第２の暗復号システムは、対象のデータを有していない。

[0172] 第１の暗復号システムにおいて、更新データを暗号化して暗号化更新データを生成し、生成した暗号化更新データにより暗号化データを上書きする。

[0173] 第２の暗復号システムにおける処理はない。

[0174] （iv）ステップＳ２０３において、第１鍵ハンドラ値がＮＵＬＬであり、第２鍵ハンドラ値もＮＵＬＬであると判断された場合

この場合には、第１の暗復号システムは、対象のデータを有しておらず、第２の暗復号システムも、対象のデータを有していない。

[0175] 第１の暗復号システムにおいて、更新データを暗号化して暗号化更新データを生成し、生成した暗号化更新データを書き込む。

[0176] このケースでは、データの更新ではなく、新規のデータの書き込みである。

[0177] 第２の暗復号システムにおける処理はない。

（３）管理テーブル２２０の更新

ここでは、管理テーブル２２０の更新の動作について、図１０～図１２に示すフローチャートを用いて説明する。なお、ここで説明する管理テーブル２２０の更新の動作は、図９のステップＳ２０２の詳細である。

[0178] 利用データベース判定部２０１は、アプリケーションプログラム（アプリケーションプログラムＡ１１７又はアプリケーションプログラムＢ１１８）から入力されたコマンドを用いて、入力されたデータ（ノード情報構造体）が、鍵データベースＡ用であるのか、又は鍵データベースＢ用であるのかを判定する（Ｓ２１１）。アプリケーションプログラムは、鍵データベースＡ１２０で管理された鍵やデータを利用する場合には、鍵データベースＡ１２０用のコマンドとノード情報構造体１５０を利用し、鍵データベースＢ１２１で管理され鍵やデータを利用する場合には、鍵データベースＢ１２１用のコマンドとノード情報構造体１６０を利用する。そのため、利用データベース判定部２０１は、アプリケーションプログラムから入力されたコマンドを参照して、入力されたデータつまりノード情報構造体がノード情報構造体１５０であるか、又はノード情報構造体１６０であるかを判定することにより

、鍵データベースＡ１２０用であるのか、又は鍵データベースＢ１２１用であるのかを判定することが可能である。

[0179] 鍵データベースＡ１２０用である場合、平文データ抽出部２０２は、ノード情報構造体１５０から平文データとデータハンドラ値とを抽出する（Ｓ２１２）。また、鍵データベースＢ１２１用である場合、平文データ抽出部２０２は、ノード情報構造体１６０からデータハンドラ値を抽出し、ノード情報構造体１６０のリンク先情報により定まる位置から平文データを抽出する（Ｓ２１３）。

[0180] 次に、ハッシュ値生成部２０３は、抽出された平文データからハッシュ値を生成する（Ｓ２１４）。

[0181] 次に、ハッシュ値判定部２０４は、管理テーブル２２０に格納された管理情報に含まれる平文データのハッシュ値のうち、ステップＳ２１４で生成されたハッシュ値とが一致するものが存在するか否かを判断する。具体的には、次のようにする。

[0182] ハッシュ値判定部２０４は、管理テーブル２２０内で管理情報のエントリ番号を示す変数Ｎに初期値０を代入する（Ｓ２１５）。ここで、管理テーブル２２０のエントリ番号とは、管理テーブル２２０に含まれる管理情報を一意に識別する識別情報である。

[0183] 次に、ハッシュ値判定部２０４は、Ｎ番目の管理情報内のハッシュ値が、ステップＳ２１４で生成したハッシュ値と一致するか否かを確認する（Ｓ２１６）。一致しない場合（Ｓ２１６でＮＯ）、Ｎが管理テーブル２２０の終端の管理情報のエントリ番号でなければ（Ｓ２１８でＮＯ）、Ｎに１を加算し（Ｓ２２０）、ステップＳ２１６へ戻る。

[0184] Ｎが管理テーブル２２０の終端の管理情報のエントリ番号であれば（Ｓ２１８でＹＥＳ）、Ｓ２１９へ制御を移す。

[0185] Ｎ番目の管理情報内のハッシュ値が、ステップＳ２１４で生成したハッシュ値と一致すれば（Ｓ２１６でＹＥＳ）、管理テーブル２２０の同一の管理情報内の一方のデータハンドラ値がＮＵＬＬか否かを判断する（Ｓ２１７）

。具体的には、ハンドラ値判定部２０５は、ステップＳ２１４で生成したハッシュ値と一致する値が格納されている管理テーブル２２０の管理情報を参照し、その管理情報内の第１及び第２データハンドラ値を参照する。もし、第１及び第２データハンドラ値のうち、アプリケーションプログラムにより指定された鍵データベースとは異なるもう一方の鍵データベース用のデータハンドラ値がＮＵＬＬ（空）ならば、もう一方の鍵データベースでは、他のアプリケーションプログラムから暗号化依頼されているデータを共有していないということを示す。また、もし、アプリケーションプログラムにより指定された鍵データベースとは異なるもう一方の鍵データベース用のデータハンドラ値がＮＵＬＬ（空）でないならば、他のアプリケーションプログラムから暗号化依頼されているデータを共有していることを示す。したがって、一方のデータハンドラ値がＮＵＬＬ（空）ならば、ステップＳ２１９に制御を移す（Ｓ２１７でＹＥＳ）。また、一方のデータハンドラ値のフィールドがＮＵＬＬ（空）でないならば、ステップＳ２２１に制御を移す（Ｓ２１７でＮＯ）。

[0186] ハッシュ値判定部２０４が、管理テーブルに、ステップＳ２１４で生成したハッシュ値が存在しないと判定した場合には（Ｓ２１８でＹＥＳ）、又は、管理テーブル２２０の同一の管理情報内の一方のデータハンドラ値がＮＵＬＬであると判断した場合（Ｓ２１７でＹＥＳ）、管理テーブル更新部２０８は、管理テーブル２２０に新たな管理情報を追加し、その管理情報の各フィールドに、ステップＳ２１４で生成したハッシュ値及びノード情報構造体のデータハンドラ値を格納する（Ｓ２１９）。次に、当該処理は終了する。

[0187] 次に、管理テーブル更新部２０８は、管理テーブル２２０の管理情報において、指定された鍵データベースに対応するデータハンドラ値のフィールドに、アプリケーションプログラムから受け取ったノード情報構造体から抽出したデータハンドラ値を格納する（Ｓ２２１）。たとえば、アプリケーションプログラムＡ１１７が、鍵データベースＡ１２０を用いて、暗号化処理を要求した場合には、アプリケーションプログラムＡ１１７から受け取ったノ

ード情報構造体から抽出したデータハンドラ値が、管理テーブル２２０の管理情報内の鍵データベースＡに対応するデータハンドラ値のフィールドに格納される。

[0188] 次に、鍵取得部２０６は、アプリケーションプログラムから受け取ったノード情報構造体により示され、データハンドラ値に対応するデータを暗号化するように指定された鍵を、異なる鍵データベース用鍵格納部に転送する（Ｓ２２２）。例えば、アプリケーションプログラムＡ１１７から指示された場合には、指定された鍵を鍵データベースＢ用鍵格納部１２５に転送する。また、アプリケーションプログラムＢ１１８から指示された場合には、指定された鍵を鍵データベースＡ用鍵格納部１２６に転送する。

[0189] 次に、鍵取得部２０６は、指定された鍵データベースとは異なる鍵データベース用の鍵格納部に、データＢの親ノードに対応する鍵ハンドラにより示される鍵がロードされているか否か確認する（Ｓ２２３）。例えば、アプリケーションプログラムＡ１１７から指示された場合には、データＢの親ノードに対応する鍵ハンドラにより示される鍵が鍵データベースＢ用鍵格納部１２５にロードされているか否かを確認する。また、アプリケーションプログラムＢ１１８から指示された場合には、データＢの親ノードに対応する鍵ハンドラにより示される鍵が鍵データベースＡ用鍵格納部１２６にロードされているか否かを確認する。

[0190] もし、対応する鍵がロードされているならば（Ｓ２２３でＹＥＳ）、改めてロードする必要がないため、ステップＳ２２５へ制御を移す。もし、対応する鍵がロードされていないならば（Ｓ２２３でＮＯ）、鍵取得部２０６は、異なる鍵データベースのルートからデータＢの親ノードまでの暗号化鍵を取得し、暗号化鍵の復号化を繰り返して、データＢを暗号化する鍵を取得する（Ｓ２２４）。

[0191] 次に、鍵取得部２０６は、データＢの暗号化のために取得した鍵を、データハンドラ値に対応するデータを暗号化するように指定された鍵を用いて、つまり、ステップＳ２２２で転送した鍵を用いて暗号化して暗号化鍵を生成

する。次に、指定された鍵データベースが鍵データベースＡの場合には、生成した暗号化鍵を、データＢのノード情報構造体１５０の鍵のフィールドに格納することにより、鍵データベースＡを更新する。また、指定された鍵データベースが鍵データベースＢの場合には、生成した暗号化鍵を、データＢのノード情報構造体１６０のリンク先情報のフィールドに、暗号化鍵が格納された位置を示す情報を格納することにより、鍵データベースＢを更新する（Ｓ２２５）。次に、処理を終了する。

[0192] このような操作によって、データＢと、データＢのノードに対応する鍵ハンドラの鍵とが、同じノード（リーフ）で管理されることになる。

[0193] （４）鍵の取得の動作

鍵の取得の動作について、図１３に示すフローチャートを用いて説明する。なお、ここで説明する鍵の取得の動作は、図９のステップＳ２０４の詳細である。

[0194] ハッシュ値生成部２０３は、抽出された平文データからハッシュ値を生成する（Ｓ２３１）。

[0195] 次に、ハッシュ値判定部２０４は、管理テーブル２２０に格納されている管理情報内のハッシュ値と、ステップＳ２３１で生成されたハッシュ値とが一致するものが存在するか否かを判断する。具体的には、次のようにして行う。

[0196] ハッシュ値判定部２０４は、管理テーブル２２０内で管理情報のエントリ番号を示す変数Ｎに初期値０を代入する（Ｓ２３２）。次に、Ｎ番目の管理情報のハッシュ値が、ステップＳ２３１で生成したハッシュ値と一致するか否かを確認する（Ｓ２３３）。一致しない場合（Ｓ２３３でＮＯ）、Ｎが管理テーブル２２０の終端の管理情報のエントリ番号でなければ（Ｓ２３８でＮＯ）、Ｎに１を加算し（Ｓ２３９）、ステップＳ２３３へ戻る。

[0197] Ｎが管理テーブル２２０の終端の管理情報のエントリ番号であれば（Ｓ２３８でＹＥＳ）、処理を終了する。

[0198] 一致する場合（Ｓ２３３でＹＥＳ）、ハンドラ値判定部２０５は、ステッ

プＳ２３１で生成したハッシュ値と一致する値が格納されている管理テーブル２２０の管理情報を参照し、その管理情報内の第１データハンドラ値及び第２データハンドラ値を参照する。すなわち、鍵データベースＡのリーフのデータハンドラ値と、鍵データベースＢのリーフのデータハンドラ値とを参照する。もし、第１及び第２データハンドラ値が全てＮＵＬＬ（空）でないならば、もう一方の鍵データベースでも、アプリケーションプログラムから暗号化依頼されているデータを共有していることを示す。また、もし、第１及び第２データハンドラ値の少なくとも一方がＮＵＬＬ（空）ならば、もう一方の鍵データベースでは、アプリケーションプログラムから暗号化依頼されているデータを共有していないことを示す。したがって、第１及び第２データハンドラ値の少なくとも一方がＮＵＬＬ（空）ならば（Ｓ２３４でＮＯ）、処理を終了する。

[0199] また、第１及び第２データハンドラ値のフィールドが全てＮＵＬＬ（空）でないならば（Ｓ２３４でＹＥＳ）、ハンドラ値判定部２０５は、管理テーブル２２０の前記管理情報から、指定された鍵管理データベースに対応する鍵ハンドラ値を取得する（Ｓ２３５）。

[0200] 次に、鍵取得部２０６は、ステップＳ２３５で取得した鍵ハンドラ値に対応する暗号化された鍵を取得し、暗号化鍵を暗復号処理部１１４を用いて復号し、取得した鍵を暗復号処理部１１４の鍵データベースＡ用鍵格納部１２６に鍵をロードする（Ｓ２３６）。また、ステップＳ２３６における復号処理で用いる鍵は、共有データの暗号化の際に利用する鍵と同一のため、ステップＳ２３６を行う時点で、暗復号処理部１１４にロードされている。

[0201] 次に、処理を終了する。

[0202] （５）共有データの更新の動作

共有データの更新の動作について、図１４に示すフローチャートを用いて説明する。なお、ここで説明する共有データの更新の動作は、図９のステップＳ２０５の詳細である。

[0203] データアクセス部１１９は、図１３に示す鍵の取得の動作において取得し

た鍵を、異なる鍵データベース用鍵格納部に転送する（Ｓ２４１）。

[0204] 次に、データアクセス部１１９は、異なる鍵データベース用のノード情報構造体を生成し、生成したノード情報構造体の各フィールドに値を格納し、修正されたデータを異なる鍵データベースに格納する（Ｓ２４２）。

[0205] 次に、暗復号エンジン部１２４は、データアクセス部１１９の指示により、ステップＳ２４１で転送した鍵を用いて、更新データを暗号化する（Ｓ２４３）。

[0206] そして、共有データのハッシュ値を参照して、管理テーブル２２０の対応する管理情報を抽出し、抽出した管理情報において、異なる鍵データベースのデータハンドラ値に格納されている値を参照して、共有データのノードを特定する。次に、異なる鍵データベースで管理されている共有データのノードの暗号化データを、暗号化された更新データにより、上書きすることによって、リンクを更新する（Ｓ２４４）。次に、処理を終了する。

[0207] なお、共有データのハッシュ値はステップＳ２１２やＳ２１３ですでに生成した値を利用してもよいし、新たに生成してもよい。また、別の更新方法として、鍵データベース及び暗号化されたデータの各ノードの位置情報を管理する情報が存在するならば、その位置情報を新たなノード情報構造が格納されている位置を指し示すように変更することでもよい。

[0208] 以上により、本実施の形態の情報処理装置１０は、鍵データベースＢ側が格納している鍵を、鍵データベースＡを含む暗復号システムから直接復号することができる。これにより、鍵を鍵データベースＢの木構造をたどって取得する手間が省け、更新されたデータを高速に同期させることができる。

[0209] また、同様の態様にすることより、本実施の形態の情報処理装置は、鍵データベースＡ側が格納している鍵を、鍵データベースＢを含む暗復号システムから直接復号することができる。これにより、鍵を鍵データベースＡの木構造をたどって取得する手間が省け、更新されたデータを高速に同期させることができる。

[0210] また、本実施の形態の情報処理装置は、共有データの更新時には、共有デ

ータノードを特定してそのノードを更新する。そのため、共有データの更新を行う際に、誤って異なるノードのデータを破壊することを防げる。また、共有データを特定された位置に上書きするため、古い共有データを確実に破棄することができる。

[0211] ２．実施の形態２

本発明に係る別の実施の形態としての情報処理装置１０が備える暗復号処理部２６０について説明する。

[0212] 実施の形態２の情報処理装置１０は、実施の形態１の情報処理装置１０が備える暗復号処理部１１４に代えて、図１５に示す暗復号処理部２６０を備えている。暗復号処理部２６０は、実施の形態１の暗復号処理部１１４と類似する構成を有している。ここでは、暗復号処理部１１４との相違点を中心として説明する。

[0213] 暗復号処理部２６０は、実施の形態１の暗復号処理部１１４が有する不揮発性メモリ部１２３、暗復号エンジン部１２４、鍵データベースＢ用鍵格納部１２５及び鍵データベースＡ用鍵格納部１２６に加えて、さらに、同期専用鍵格納部２６５を備えている。

[0214] また、実施の形態２では、実施の形態１のステップＳ２２２とＳ２４１において、鍵データベースＢ用鍵格納部１２５又は鍵データベースＡ用鍵格納部１２６への転送に代えて、鍵を同期専用鍵格納部２６５に転送して利用する。

[0215] すなわち、鍵取得部２０６は、アプリケーションプログラムから受け取ったノード情報構造体により示され、データハンドラ値に対応するデータを暗号化するように指定された鍵を、同期専用鍵格納部２６５に転送する（Ｓ２２２）。

[0216] また、データアクセス部１１９は、図１３に示す鍵の取得の動作において取得した鍵を、同期専用鍵格納部２６５に転送する（Ｓ２４１）。

[0217] このように、同期専用鍵格納部２６５を備えることによって、データ同期処理において、実施の形態１の鍵データベースＡ用鍵格納部１２６及び鍵デ

ータベースＢ用鍵格納部１２５を利用する必要がない。したがって、データ同期処理時に、鍵データベースＡ用鍵格納部１２６や鍵データベースＢ用鍵格納部１２５に格納されている鍵を破棄する必要がない。

[0218] ３．実施の形態３

本発明に係る別の実施の形態としての情報処理装置１０が備える暗復号処理部２７０について説明する。

[0219] 実施の形態３の情報処理装置１０は、実施の形態１の情報処理装置１０が備える暗復号処理部１１４に代えて、図１６に示す暗復号処理部２７０を備えている。暗復号処理部２７０は、実施の形態１の暗復号処理部１１４と類似する構成を有している。ここでは、暗復号処理部１１４との相違点を中心として説明する。

[0220] 暗復号処理部２７０は、実施の形態１の暗復号処理部１１４が有する不揮発性メモリ部１２３及び暗復号エンジン部１２４に加えて、さらに、共用鍵格納部２７３を備えている。暗復号処理部２７０は、鍵データベースＡ用鍵格納部１２６及び鍵データベースＢ用鍵格納部１２５を備えていない。共用鍵格納部２７３は、鍵データベースＡ用鍵格納部１２６及び鍵データベースＢ用鍵格納部１２５に相当する。

[0221] 共用鍵格納部２７３は、図１６に示すように、鍵テーブル２７４を格納している。

[0222] 鍵テーブル２７４は、図１７に示すように、複数の鍵情報を含む。各鍵情報は、タイプ及び鍵から構成されている。タイプは、利用する鍵データベースを示す。つまり、鍵データベースＡ用であるか又は鍵データベースＢ用であるかを示す。鍵のフィールドには、上述した鍵が格納される。

[0223] 実施の形態３の情報処理装置１０では、実施の形態１のステップＳ２２２とＳ２４１において、鍵を転送する代わりに、鍵テーブル２７４において、利用するデータベースのタイプを変更する。

[0224] データベースのタイプの変更の一例を、図１７及び図１８を用いて説明する。ここで、図１７に示す例では、鍵データベースＢにおいて、共有データ

は、鍵データベースＢの鍵である“０ｘＡＡ　０ｘＢＢ　…　０ｘ１１”で暗号化されているものとする。

[0225] まず、実施の形態１で説明した方法を用いて、鍵データベースＡで管理されている、鍵データベースＢの鍵“０ｘＡＡ　０ｘＢＢ　…　０ｘ１１”を、共用鍵格納部２７３にロードする。この時点では、鍵データベースＢの鍵“０ｘＡＡ　０ｘＢＢ　…　０ｘ１１”は、鍵データベースＡで管理されているため、図１７の鍵テーブル２７４において、データベースのタイプは、“データベースＡ用”２７５である。

[0226] 次に、鍵管理ソフトウェア１１６が、暗復号処理部２７０に対して、ロードした鍵“０ｘＡＡ　０ｘＢＢ　…　０ｘ１１”を、鍵データベースＢ用に変更するよう指定する。暗復号処理部２７０は、共用鍵格納部２７３の鍵テーブル２７４において、ロードした鍵“０ｘＡＡ　０ｘＢＢ　…　０ｘ１１”を、鍵データベースＢ用に変更する（図１８）。図１８の鍵テーブル２７４において、データベースのタイプは、“データベースＢ用”２７６となる。

[0227] そして、鍵管理ソフトウェア１１６は、実施の形態１で説明した方法を用いて、共有データを更新（同期）する。

[0228] その後、鍵管理ソフトウェア１１６が、暗復号処理部２７０に対して、ロードした鍵“０ｘＡＡ　０ｘＢＢ　…　０ｘ１１”を、鍵データベースＡ用に変更するよう指定する。暗復号処理部２７０は、共用鍵格納部２７３の鍵テーブル２７４において、ロードした鍵“０ｘＡＡ　０ｘＢＢ　…　０ｘ１１”を、鍵データベースＡ用に変更する（図１７）。図１７の鍵テーブル２７４において、データベースのタイプは、“データベースＡ用”２７５となる。

[0229] このように、共用鍵格納部２７３を備え、鍵テーブル２７４を用いることによって、データ同期処理において、鍵の転送が不要になる。また、鍵データベースＡと鍵データベースＢとで鍵を共用するので鍵の格納に必要な領域のサイズを小さくすることができる。

[0230] なお、共有データの更新（同期）の後に、鍵データベースのタイプを変更するように指定しないでもよい。

[0231] また、共有データの更新（同期）の後に、暗復号処理部２７０は、利用した鍵を破棄してもよい。

[0232] ４．その他変形例

（１）上記の各実施の形態では、鍵データベースＡ１２０及び鍵データベースＢ１２１は、半導体メモリである第１記憶部１１２に格納されているが、ハードディスクユニットから構成される第２記憶部１１３に格納されているとしてもよい。

[0233] （２）上記の各実施の形態では、暗復号処理部１１４を、ハードウェア装置で実現していたが、ソフトウェアで実現してもよい。さらに、暗復号処理部１１４を実現するソフトウェアは、安全なソフトウェア実行環境で実行されてもよい。

[0234] （３）上記の各実施の形態において、ステップＳ２２２とステップＳ２４１において、鍵転送された後に、各鍵格納部から破棄すべき鍵を、ルート鍵で暗号化して、一時的に暗復号処理部の不揮発性メモリに格納し、同期処理終了後に、再度、暗復号処理部内部の揮発性メモリにロードしてもよい。なお、同期処理の間は、暗復号処理部に対する、新たな処理要求を受け付けないことで、各鍵格納部内部の場所などの情報を変更しないこととする。

[0235] この場合に、暗復号化処理部は、制御部と、第１の暗復号システム用の前記第１鍵を保持する第１鍵格納部と、第２の暗復号システム用の前記第２鍵を保持する第１鍵格納部と、前記第１及び第２鍵格納部に保持されている前記第１鍵及び第２鍵を用いて、暗号化する暗復号エンジン部とを備える。前記制御部は、前記第１鍵を取得して前記第１鍵格納部に保持させるにあたって、前記第１鍵格納部の空き領域が不足しているか否かを判断し、前記第１鍵格納部の空き領域が不足している場合に、前記第１鍵格納部が既に保持している一の鍵を、前記暗復号エンジン部により、暗号化して前記第１鍵格納部の外に退避し、前記第１鍵格納部において、退避対象の前記鍵が保持され

ていた領域に、取得した前記第１鍵を上書きし、前記第１暗復号システムにおける前記第１鍵を用いた暗号化が完了した後、退避した前記暗号化鍵を、前記暗復号エンジン部により、復号して前記第１鍵が保持されている領域に上書きする。

[0236] （４）上記の各実施の形態において、各鍵格納部を固定長サイズのブロック単位で管理し、鍵の長さに応じて、複数ブロックを用いて鍵を格納してもよい。その場合には、ブロック管理用のブロック管理テーブルを用いて、各鍵格納部を管理してもよい。

[0237] 各鍵格納部を固定長サイズのブロック単位で管理する場合の一例を図１９に示す。図１９に示す鍵格納部３３０は、固定長サイズの１０個のブロックから構成されており、鍵は、ブロック単位で管理される。

[0238] 鍵格納部を固定長サイズのブロック単位で管理する場合のブロック管理テーブルの一例を図２０に示す。図２０に示すブロック管理テーブル３３１は、鍵格納部３３０のどのブロックが、どの鍵データベースの鍵を格納するため利用されているかを示す。ブロック管理テーブル３３１は、鍵データベースのタイプ及び利用するブロック番号からなる組を複数個含んで構成されており、データベースのタイプと利用するブロック番号の対応関係の表を構成している。

[0239] ブロック管理テーブル３３１は、鍵格納部３３０のブロック＃１及びブロック＃２に格納された２個のデータを連結してできた連結体が鍵データベースＡ用の一つの鍵であり、ブロック＃３及びブロック＃４に格納された２個のデータを連結してできた連結体が鍵データベースＡ用の一つの鍵であり、ブロック＃５、ブロック＃６、ブロック＃７及びブロック＃８に格納された４個のデータを連結してできた連結体が鍵データベースＢ用の一つの鍵であり、ブロック＃９に格納されたデータが鍵データベースＢ用の一つの鍵であり、ブロック＃１０に格納されたデータが鍵データベースＢ用の一つの鍵であることを示す。

[0240] この構成によると、鍵を保持する領域をブロック単位で効率的に管理する

ことができる。

[0241] 以上説明したように、情報処理装置は、第１の暗復号システムにおいて復号された鍵を、第１の暗復号システム用であることを示す第１タイプ情報と対応付けて保持し、第２の暗復号システムにおいて復号された鍵を、第２の暗復号システム用であることを示す第２タイプ情報と対応付けて保持する鍵格納部（図１９に示す）を備えている。

[0242] 暗復号化処理部は、第１の暗復号システムにおいては、前記第１タイプ情報と対応付けられた鍵を用いて復号を行い、第２の暗復号システムにおいては、前記第２タイプ情報と対応付けられた鍵を用いて暗号化を行う。

[0243] 情報処理装置は、さらに、第１の暗復号システムにおける復号の結果、第１タイプ情報と対応付けられて、鍵格納部に保持された鍵について、第１タイプ情報を第２の暗復号システム用であることを示す第２タイプ情報に書き換えることで、前記鍵を用いた前記更新データの暗号化を第２の暗復号システムにおいて行わせる制御手段を備える。

[0244] また、鍵格納部は、所定の容量を持つ複数のブロックから構成されており、保持する鍵それぞれがどのブロックに格納されているかを示すブロック情報を、前記保持する鍵それぞれと対応付けて保持している。

[0245] （５）上記の各実施の形態において、管理テーブルの各管理情報を、当該管理情報に対応するリーフの鍵で暗号化して保持してもよい。その場合には、管理テーブルは、管理情報ごとに分割され、各管理情報は、リーフにより管理される。

[0246] 管理テーブルを、管理情報ごとに分割してリーフで管理する場合の一例を図２１に示す。アプリケーションプログラムＡ２８０、アプリケーションプログラムＢ２８１、鍵データベースＡ２８３及び鍵データベースＢ２８４は、実施の形態１のアプリケーションプログラムＡ１１７、アプリケーションプログラムＢ１１８、鍵データベースＡ１２０及び鍵データベースＢ１２１と同一である。鍵管理ソフトウェア２８２は、鍵データベースＡ２８３及び鍵データベースＢ２８４を用いて、後述の方法を用いて、管理する。

[0247] 管理テーブルの各管理情報は、当該管理情報に対応するデータを暗号化する鍵が割り当てられているノードの鍵で暗号化される。図２１に示す一例では、共有されるデータＢについては、鍵データベースＡ２８３において、データＢを暗号化する鍵が割り当てられているノード２８７（リーフ－４）の鍵を用いて、データＢに対応する管理情報が暗号化されて、格納される（２８９）。同様に、共有されるデータＢについては、鍵データベースＢ２８４において、データＢを暗号化する鍵が割り当てられているノード２９３（リーフ－５）の鍵で、データＢに対応する管理情報が暗号化されて、格納される（２９５）。

[0248] 図２１のデータＢに対応する管理テーブルの管理情報３００を図２２に一例として示す。管理情報３００を構成する要素は、図６に示す管理テーブル２２０の管理情報を構成する要素と同一である。

[0249] 共有データを暗号化するためのリーフの鍵は、共有データの更新時に必ず探索される。管理テーブルには、他の鍵データベースで管理されているリーフの鍵によって暗号化された共有データの位置が記録される。そのため、この管理テーブルにそのようなリーフの鍵を対応付けることで、同期処理時に更新すべき共有データの位置の探索を簡便化することができる。

[0250] 以上説明したように、管理テーブルは、暗号化データの要約値と各ハンドラ値（位置情報）とを対応付けて含む。判断部は、暗号化データ格納部に記憶されている暗号化データからその要約値を算出し、得られた要約値に対応する各ハンドラ値（位置情報）が管理テーブルに記憶されているか否かを判断する。

[0251] （６）上記の各実施の形態において、管理テーブルの各管理情報を、暗復号処理部に格納されているルート鍵を用いて暗号化して保持してもよい。

[0252] （７）上記の各実施の形態では、アプリケーションプログラムが、データを暗号化する際に、鍵管理ソフトウェアが管理テーブルを更新しているが、鍵管理ソフトウェアは、それ以外のタイミングで管理テーブルを更新してもよい。

[0253] 図２３は、アプリケーションプログラム（アプリケーションプログラムＡ又はアプリケーションプログラムＢ）がデータを復号する際に、鍵管理ソフトウェアによる管理テーブルの更新処理を示すフローチャートである。

[0254] アプリケーションプログラム（ここでは、一例として、アプリケーションプログラムＡ）は、データＢを復号するように、鍵管理ソフトウェアに要求する（Ｓ５００）。

[0255] 次に、鍵管理ソフトウェアは、復号を要求されたデータＢを格納しているノード情報構造体から平文データを取得する（Ｓ５０１）。

[0256] 鍵管理ソフトウェアは、アプリケーションプログラムから使用するように指定された鍵データベースとは異なる鍵データベース用のノード情報構造体に、取得した平文データを格納する（Ｓ５０２）。

[0257] 鍵管理ソフトウェアは、暗復号エンジン部に対して、ステップＳ５０２で平文データを格納したノード情報構造体を、アプリケーションプログラムから使用するように指定された鍵データベースとは異なる鍵データベースの全てのリーフの鍵で暗号化するように指示し、暗復号エンジン部は、平文データを格納したノード情報構造体を暗号化する（Ｓ５０３）。

[0258] 鍵管理ソフトウェアは、ステップＳ５０３で暗号化したノード情報構造体を、アプリケーションプログラムから使用するように指定された鍵データベースとは異なる鍵データベースで暗号化されて管理されているデータと一致するか否かを判断する（Ｓ５０４）。一致するならば（Ｓ５０４でＹＥＳ）、そのデータは共有データであると判断し、管理テーブルを更新し（Ｓ５０５）、管理テーブルの更新を終了する。

[0259] また、ステップＳ５０４で一致しないと判断された場合には（Ｓ５０３でＮＯ）、管理テーブルの更新を終了する。

[0260] なお、ステップＳ５０４における一致するか否かを判断する際には、暗号化データのハッシュ値を用いて比較してもよい。また、暗号化データのハッシュ値を管理テーブルの平文データのハッシュ値のフィールドに格納してもよい。

[0261] 図２４に、共有データの特定の際に、暗号化データのハッシュ値を用いる場合の管理テーブル３２０の一例を示す。図２４の管理テーブル３２０と図６の管理テーブル２２０との違いは、ハッシュ値を生成する対象が、管理テーブル３２０では暗号化データであるのに対して、管理テーブル２２０では平文データであることである。それ以外の管理テーブルのフィールドは、同一である。

[0262] 図２５に、図２４に示す管理テーブル３２０を用いて、共有データを特定し、同期すべきデータの鍵を取得するフローチャートを示す。

[0263] 図２５に示すフローチャートと、実施の形態１で説明した鍵取得のフローチャート（図１３）との違いは、実施の形態１の鍵取得では、ステップＳ２３１において平文データからハッシュ値を生成していることに対して、図２５のフローチャートでは、ステップＳ２３１ａにおいて暗号化データからハッシュ値を生成することである。

[0264] 図２５のステップＳ２３２以降の処理は、図１３のステップＳ２３２以降の処理と同一である。

[0265] （８）上記の各実施の形態において、鍵管理ソフトウェアや管理テーブルを、安全なソフトウェア実行環境で実行及び管理してもよい。安全なソフトウェア実行環境を実現する技術として、正当なソフトウェアのみを起動する技術であるセキュアブートを用いてもよい。さらに、別の方法で安全なソフトウェア実行環境を構築してもよい。

[0266] （９）上記の各実施の形態では、ノード情報構造体に含まれる暗号種別として、楕円曲線暗号方式やＮＴＲＵ暗号方式を指定してもよい。さらに、ノード情報構造体に含まれる鍵長として、鍵のビット長の指定以外に、あらかじめ定義された定義情報で、鍵長を指定してもよい。また、暗復号エンジン部は、楕円曲線暗号方式やＮＴＲＵ暗号方式の暗復号を実現してもよい。

[0267] （１０）上記の各実施の形態では、ノード情報構造体において、鍵ハンドラ値のフィールドとデータハンドラ値のフィールドとを異なるフィールドを用いて実現したが、同一のフィールドを用いて実現してもよい。

[0268] 例えば、対応する鍵とデータとが存在する位置を示すために、同一の番号を用い、ノード情報構造体において、当該番号を格納する１個のフィールドのみを設けてもよい。この番号の一例は、鍵データベースの木構造のノードを識別する識別情報である。

[0269] この場合に、各鍵データベースにおいて、領域を確保し、この領域に鍵ハンドラ値とデータハンドラ値とを組にして格納する。この領域において、この組の記憶されている位置を前記の番号により識別するようにする。

[0270] また、この場合に、各鍵データベースにおいて、鍵ハンドラ値領域を確保し、この鍵ハンドラ値領域に鍵ハンドラ値を格納する。この鍵ハンドラ値領域において、この鍵ハンドラ値が記憶されている位置を前記の番号により識別するようにする。また、各鍵データベースにおいて、データハンドラ値領域を確保し、このデータハンドラ値領域にデータハンドラ値を格納する。このデータハンドラ値領域において、このデータハンドラ値が記憶されている位置を前記の番号により識別するようにする。

[0271] （１１）上記の各実施の形態では、ハッシュ値をＳＨＡ－１アルゴリズムを用いて生成するとしたが、それ以外の方法を用いてもよい。たとえば、SHA-2（SHA-224、SHA-256、SHA-384、SHA-512）アルゴリズムやＭＤ５（Message Digest 5）アルゴリズムなどでもよい。

[0272] （１２）上記の各実施の形態では、情報処理装置は、一方の暗復号システムが管理する共有データが更新されると、そのたびに他の暗復号システムが管理する共有データを更新している。しかし、これに限られるものではなく、共有データを同期するよう指示された場合に、他の暗復号システムが管理する共有データを更新するとしてもよい。これにより、他の暗復号システム側で共有データが必要になった時にだけ、その共有データを更新することができるので、更新処理を行う回数を少なくすることができる。

[0273] 図２６に、共有データを同期するよう指示された場合に、他の暗復号システムが管理する共有データの更新処理のフローチャートを示す。

[0274] 図２６に示すフローチャートと、実施の形態１で説明したデータ同期のフ

ローチャート（図９）との違いは、図２６で示すフローチャートにおいて、ステップＳ５１１において、同期指示があるか否かを判断する判断ステップが追加されたことである。

[0275] ステップＳ５１１において、同期指示がある場合には、ステップＳ２０１に制御を移す。ステップＳ２０１以降の処理は、図９のステップＳ２０１以降の処理と同一である。

[0276] また、ステップＳ５１１において、同期指示が無い場合には、ステップＳ２０６に制御を移し、ステップＳ２０６において、自身の更新データＢを暗号化し、次に、処理を終了する。

[0277] また、ステップＳ５１１における同期指示の判断では、鍵管理ソフトウェアで管理するフラグの値や、鍵管理ソフトウェアへのデータ暗復号回数や、鍵管理ソフトウェアの利用時間などを用いて判断してもよい。

[0278] また、データアクセス部１１９は、第１の暗復号システムにおいて暗号された更新データを、サブ暗号化データ格納部１２２ａに記憶されている暗号化データに上書きする。その後、同期指示を受け取った場合に、データアクセス部１１９は、第２の暗復号システムにおいて暗号化された更新データを、サブ暗号化データ格納部１２２ｂに記憶されている暗号化データに上書きする。

[0279] （１３）上記の各実施の形態では、情報処理装置における共有データの更新の詳細については触れていないが、共有データの更新を、暗号化された共有データを復号してから行うとしてもよい。例えば、コンテンツの利用回数を示す情報のような累積的に変化するような共有データを管理することができる。利用回数が暗号化されて第１の暗復号システム及び第２の暗復号システムにおいて保持されている。第１の暗復号システムにおいてコンテンツを利用する際に、暗号化された利用回数を復号し、利用回数を得、得られ利用回数から「１」を減じる。次に、「１」を減じた利用回数を再度暗号化する。このとき、第２の暗復号システムにおいて保持されている暗号化利用回数に、新たな暗号化利用回数を上書きする。

[0280] また、暗号化された共有データの更新の指示が外部から供給されるとしてもよい。つまり、共有データを更新して得られた更新データが、外部から供給されるとしてもよい。この場合、第１の暗復号システムにおいて、更新データを暗号化して、暗号化更新データを保持し、第２の暗復号システムにおいても、更新データを暗号化して、暗号化更新データを保持する。

[0281] 暗号化された共有データの更新の指示が外部から供給される情報処理装置のソフトウェア構成を図２７に示す。

[0282] アプリケーションプログラムＡ１１７、アプリケーションプログラムＢ１１８、鍵データベースＡ１２０、鍵データベースＢ１２１及び暗号化データ格納部１２２は、実施の形態１のアプリケーションプログラムＡ１１７、アプリケーションプログラムＢ１１８、鍵データベースＡ１２０、鍵データベースＢ１２１及び暗号化データ格納部１２２と同一である。

[0283] 鍵管理ソフトウェア１１６ａは、図２７に示すように、鍵管理ソフトウェア１１６が有する利用データベース判定部２０１、平文データ抽出部２０２、ハッシュ値生成部２０３、ハッシュ値判定部２０４、ハンドラ値判定部２０５、鍵取得部２０６、管理テーブル格納部２０７、管理テーブル更新部２０８及び鍵書込部２０９に加えて、さらに、データ状態変更部３２４を含む。

[0284] データ状態変更部３２４は、暗号化データ格納部１２２に格納されているデータの状態を管理及び変更する。

[0285] 暗号化された共有データの更新の指示が外部から供給された際のデータ同期処理について、図２８に示すフローチャートを用いて説明する。

[0286] 鍵管理ソフトウェア１１６ａのデータ状態変更部３２４は、暗号化データ格納部１２２に格納されている暗号化データＢを復号して、平文データを取得し、アプリケーションプログラムＡ１１７から指定された変更を平文データに反映して、更新データＢを作成する（Ｓ５２１）。

[0287] 例えば、アプリケーションプログラムＡ１１７は、鍵データベースＡ１２０のリーフに割り当てられた鍵で暗号化されているデータＢに対して、累積

的な変更として、１を減算するように、鍵管理ソフトウェア１１６ａに指示した場合、データ状態変更部３２４は、鍵データベースＡ１２０を用いて、暗号化データＢを復号して平文データを取得し、平文データから１を減算する。そして、減算された結果のデータを更新データＢとする。

[0288] ステップＳ２０１以降の処理は、図９のステップＳ２０１以降の処理と同一である。

[0289] なお、図２８のステップＳ２０５において、鍵管理ソフトウェア１１６ａは、暗号化された更新データＢにより、相手側の暗号化データＢを更新する。

[0290] （１４）上記の実施の形態で述べた構成要素については、その一部または全てを実現可能な範囲でソフトウェアとして実装してもよい。この場合、集積回路上に乗せなくてはならないハードウェアの量を抑えることができるので、より集積度を向上させることができる。

[0291] （１５）上記の各実施の形態では、アプリケーションプログラムＡが鍵データベースＡを用い、アプリケーションプログラムＢが鍵データベースＢを用い、また、不揮発性メモリ部１２３には、鍵データベースＡ用のルート鍵及び鍵データベースＢ用のルート鍵が記憶され、暗復号処理部には、鍵データベースＡ用鍵格納部及び鍵データベースＢ用鍵格納部が存在するとしているが、これには限定されない。

[0292] 情報処理装置には、ｎ（ｎは、３以上の正整数）個のアプリケーションプログラムが記憶され、ｎ個の鍵データベースが保持され、ｎ個のアプリケーションプログラムは、それぞれ、ｎ個の鍵データベースに対応し、アプリケーションプログラムは、対応する鍵データベースを用い、不揮発性メモリ部１２３には、ｎ個の鍵データベース用のルート鍵が記憶され、暗復号処理部には、ｎ個の鍵データベース用の鍵格納部が存在し、暗号化データ格納部は、ｎ個のサブ暗号化データ格納部を備えるとしてもよい。

[0293] この場合に、情報処理装置は、それぞれデータを暗号化して保管するｎ個の暗復号システムを有し、この情報処理装置は、ｎ個の暗復号システムのう

ちのいずれか一の暗復号システムにおける暗号化の対象データを取得するデータ取得部と、前記対象データが、他の暗復号システムにおいて暗号化されて保管されているか否かを判断する判断部と、保管されていると判断する場合に、他の暗復号システムにおいて保管されている暗号化データの鍵を取得する鍵取得部と、前記一の暗復号システムにおいて用いられる鍵データベース（鍵記憶手段）と、前記一の暗復号システムにおいて、前記対象データに対応付けて、取得した前記鍵を前記鍵データベースに書き込む鍵書込部とを備えるとしてもよい。

[0294] （１６）本発明の第１の態様に係る情報処理装置は、第１システムと第２システムとが動作する情報処理装置であって、前記第１システムと前記第２システムとは、データを暗号化して管理する互いに独立したシステムであり、前記情報処理装置は、前記第１システムと前記第２システムとの間で共有される共有データを前記第１システム用の鍵である第１暗号鍵で暗号化した暗号化共有データを格納する第１データ格納部と、前記共有データを前記第２システム用の鍵である第２暗号鍵で暗号化した暗号化共有データを格納する第２データ格納部と、前記第１システム用の鍵として、前記第１暗号鍵を用いて暗号化された前記第２暗号鍵を格納する第１鍵格納部と、前記第１システムと前記第２システムとを制御する制御部とを備え、前記制御部は、前記第１データ格納部に格納されている暗号化共有データの更新が指示されると、更新された共有データを前記第１暗号鍵で暗号化して前記第１データ格納部に記録し、前記暗号化された第２暗号鍵を前記第１暗号鍵に対応する第１復号鍵を用いて復号して前記第２暗号鍵を生成するよう、前記第１システムを制御し、前記第１システムで生成された第２暗号鍵で前記更新された共有データを暗号化して前記第２データ格納部に記録することで前記暗号化共有データを更新するよう、前記第２システムを制御するものである。

[0295] これによると、本態様の情報処理装置は、更新された共有データを前記第１暗号鍵で暗号化して前記第１データ格納部に記録し、前記暗号化された第２暗号鍵を前記第１暗号鍵に対応する第１復号鍵を用いて復号して前記第２

暗号鍵を生成するよう、前記第１システムを制御し、前記第１システムで生成された第２暗号鍵で前記更新された共有データを暗号化して前記第２データ格納部に記録する。これにより、本態様の情報処理装置は、第２のシステムの持つ第２暗号鍵を、第１のシステムから直接復号することができる。これにより、第２のシステムに第２暗号鍵を取得する手間が省け、更新されたデータを高速に同期させることができる。

[0296] また、本発明の第２の態様に係る情報処理装置において、前記制御部は、更に、前記第２データ格納部における前記暗号化共有データの位置を特定し、前記第２暗号鍵で前記更新された共有データを前記特定された位置に上書きするよう前記第２システムを制御するものである。

[0297] これによると、暗号化共有データの位置を特定するため、暗号化共有データの更新を行う際に、誤って異なるデータを破壊することを防げる。また、共有データを特定された位置に上書きするため、古い共有データを確実に破棄することができる。

[0298] また、本発明の第３の態様に係る情報処理装置は、さらに、暗号化された前記共有データの前記第２データ格納部における位置を示す情報を、前記第１復号鍵と対応付けて管理する共有データ管理部を備え、前記制御部は、前記第１復号鍵に対応付けられた前記情報を基に、前記第２データ格納部における前記暗号化共有データの所在を特定し、前記位置に前記第２更新データを上書きするよう、前記第２システムを制御するものである。

[0299] これによると、共有データの第２データ格納部における位置を示す情報を、第１復号鍵と対応付けて管理する。第１復号鍵は、共有データの更新時に必ず探索される情報である。本態様では、暗号化共有データの位置、すなわち、更新すべき共有データの位置をそのような第１復号鍵に対応付けているため、共有データの位置の探索を簡便化することができる。

[0300] また、本発明の第４の態様に係る情報処理装置は、さらに、暗号化された前記共有データの前記第２データ格納部における位置を示す情報を、前記共有データの要約値と対応付けて管理する共有データ管理部を備え、前記制御

部は、前記第１データ格納部に格納されている暗号化共有データを前記第１復号鍵を用いて復号し、復号により得た共有データについての要約値を計算し、前記要約値を用いて前記共有データ管理部の管理する情報を参照することで、前記第２データ格納部における前記暗号化共有データの位置を特定し、前記位置に前記第２更新データを上書きするよう、前記第２システムを制御するものである。

[0301] これによると、第２データ格納部における位置を示す情報を、前記共有データの要約値として対応づけて管理する。共有データの要約値はデータサイズを小さくすることができるため、小さなサイズのデータで管理することができる。また、共有データの要約値と対応付けて管理するため、共有データが改竄されている場合は正しい要約値が得られなくなり、共有データの位置も特定できない。これにより、不正な読み出しを防止することができる。

[0302] また、本発明の第５の態様に係る情報処理装置は、さらに、暗号化された前記共有データの前記第２データ格納部における位置を示す情報を、前記第１データ格納部に格納されている暗号化共有データの要約値と対応付けて管理する共有データ管理部を備え、制御部は、前記第１データ格納部に格納されている前記暗号化共有データの要約値を計算し、前記要約値を用いて前記共有データ管理部の管理する情報を参照することで、前記第２データ格納部における前記暗号化共有データの位置を特定し、前記位置に前記第２更新データを上書きするよう、前記第２システムを制御するものである。

[0303] これによると、第２データ格納部における位置を示す情報を、前記第１データ格納部に格納されている暗号化共有データの要約値として対応づけて管理する。暗号化共有データの要約値はデータサイズを小さくすることができるため、小さなサイズのデータで管理することができる。また、暗号化共有データの要約値と対応付けて管理するため、暗号化共有データが改竄されている場合は正しい要約値が得られなくなり、暗号化共有データの位置を特定できない。これにより、不正な読み出しを防止することができる。

[0304] また、本発明の第６の態様に係る情報処理装置は、更に、前記第２システ

ム用の鍵として、前記第２暗号鍵を用いて暗号化された前記第１暗号鍵を格納する第２鍵格納部を備え、前記制御部は、更に、前記第２データ格納部に格納されている暗号化共有データの更新が指示されると、更新された共有データを前記第２暗号鍵で暗号化して前記第２データ格納部に記録し、前記暗号化された第１暗号鍵を前記第２暗号鍵に対応する第２復号鍵を用いて復号して前記第１暗号鍵を生成するよう、前記第２システムを制御し、前記第２システムで生成された第１暗号鍵で前記更新された共有データを暗号化して前記第１データ格納部に記録することで前記暗号化共有データを更新するよう、前記第１システムを制御するものである。

[0305] これによると、第２システムに対しても、共有データの同期を行うことができる。

[0306] また、本発明の第７の態様に係る情報処理装置において、前記制御部は、前記第１データ格納部に格納されている暗号化共有データの更新が指示されると、さらに、前記第１データ格納部に格納されている暗号化共有データを、前記第１復号鍵を用いて復号し、前記復号された共有データを前記更新された共有データに更新するよう、前記第１システムを制御するものである。

[0307] これによると、共有データを復号してから更新することができる。これにより、例えば、コンテンツの利用回数を示す情報のような累積的に変化するような共有データを管理することができる。

[0308] また、本発明の第８の態様に係る情報処理装置において、前記制御部は、前記第１データ格納部に格納されている暗号化共有データが更新された後、前記第１システムと前記第２システムとの間で前記共有データを同期するよう指示された場合に、前記第１システムで生成された第２暗号鍵で前記更新された共有データを暗号化して前記第２データ格納部に記録し、前記暗号化共有データを更新するよう、前記第２システムを制御するものである。

[0309] これによると、前記第１データ格納部に格納されている暗号化共有データが更新された後、前記第１システムと前記第２システムとの間で前記共有データを同期するよう指示された場合に、第２システムの共有データを更新す

る。これにより、第２システムで更新された共有データが必要になった時にだけ、第２システムの共有データを更新することができるので、更新処理を行う回数を削減することができる。

[0310] また、本発明の第９の態様に係る情報処理装置は、更に、前記第１復号鍵を含む前記第１システム用の鍵を階層構造で管理する階層管理部を備え、前記階層構造において、各鍵の下位には前記各鍵を用いて復号できるよう暗号化された鍵が割り当てられており、前記階層管理部は、暗号化された前記第２暗号鍵を前記第１復号鍵の下位に対応付けて管理するものである。

[0311] これによると、第１システムは、木構造等の階層構造で管理された鍵データベースを利用することができる。

[0312] また、本発明の第１０の態様に係る情報処理装置は、さらに、前記第１システムが管理するデータを利用するソフトウェアを動作させる動作部を備え、前記制御部は、前記データ格納部に格納されている暗号化共有データの更新の指示を前記ソフトウェアから受け付けるものである。

[0313] これによると、第１システムをアプリケーションから利用することができる。

[0314] また、本発明の第１１の態様に係る情報処理装置は、更に、前記第１システムが復号した鍵を、前記第１システム向けであることを示す情報と対応付けて保持し、前記第２システムが復号した鍵を、前記第２システム向けであることを示す情報と対応付けて保持する保持部を備え、前記第１システムは、前記第１システム向けであることを示す情報と対応付けられた鍵を用いて復号を行い、前記第２システムは、前記第２システム向けであることを示す情報と対応付けられた鍵を用いて暗号化を行い、前記制御部は、前記第１システムによる復号の結果、前記第１システム向けであることを示す情報と対応付けられて前記保持手段に保持された第２暗号鍵について、前記情報を前記第２システム向けであることを示す情報に書き換えることで、前記第２暗号鍵を用いた前記更新された共有データの暗号化を前記第２システムに行わせるものである。

[0315] これによると、制御部は、前記第１システムによる復号の結果、前記第１システム向けであることを示す情報と対応付けられて前記保持手段に保持された第２暗号鍵について、前記情報を前記第２システム向けであることを示す情報に書き換えることで、前記第２暗号鍵を用いた前記更新された共有データの暗号化を前記第２システムに行わせる。したがって、暗復号に用いる鍵の格納に必要な領域のサイズを小さくすることができる。また、暗復号に用いる鍵を復号化した状態で保持しつづけるため、鍵の復号回数を削減することができる。

[0316] また、本発明の第１２の態様に係る情報処理装置において、前記保持部は、所定の容量を持つ複数のブロックから構成されており、保持する鍵それぞれがどのブロックに格納されているかを示す情報を、前記保持する鍵それぞれと対応付けて保持するものである。

[0317] この構成によると、鍵を保持する領域をブロック単位で効率的に管理することができる。

[0318] また、本発明の第１３の態様に係る情報処理装置において、前記情報処理装置は、更に、前記第２システム向けの鍵を保持する保持部を備え、前記第２システムは、前記保持部の保持する鍵を用いて暗号化を行い、前記制御部は、前記第２暗号鍵を前記保持部に保持させることで、前記第２システムに前記更新後の共有データの暗号化を行わせ、前記第２暗号鍵を前記保持部に保持させるにあたって、前記保持部の空き領域が不足している場合には、前記保持部が既に保持している鍵を暗号化して前記保持部の外に退避し、退避した前記鍵が保持されていた領域に前記第２暗号鍵を上書きし、前記第２システムによる前記第２更新データの生成が完了した後、退避した前記鍵を復号して前記第２暗号鍵が保持されている領域に上書きするものである。

[0319] この構成によると、制御部は、第２暗号鍵を前記保持部に保持させるにあたって、前記保持部の空き領域が不足している場合には、前記保持部が既に保持している鍵を暗号化して前記保持部の外に退避し、退避した前記鍵が保持されていた領域に前記第２暗号鍵を上

書きし、前記第２システムによる前記第２更新データの生成が完了した後、退避した前記鍵を復号して前記第２暗号鍵が保持されている領域に上書きする。したがって、保持部に十分な空き領域がない場合であっても、共有データの更新ができる。また、保持部外に鍵を対比する際には暗号化を行うので、保持部の外で鍵を奪うなどの攻撃から鍵を保護することができる。

[0320] また、本発明の第１４の態様に係る情報処理方法は、第１システムと第２システムとが動作する情報処理装置で用いられる情報処理方法であって、前記第１システムと前記第２システムとは、データを暗号化して管理する互いに独立したシステムであり、前記情報処理装置は、前記第１システムと前記第２システムとの間で共有される共有データを前記第１システム用の鍵である第１暗号鍵で暗号化した暗号化共有データを格納する第１データ格納部と、前記共有データを前記第２システム用の鍵である第２暗号鍵で暗号化した暗号化共有データを格納する第２データ格納部と、前記第１システム用の鍵として、前記第１暗号鍵を用いて暗号化された前記第２暗号鍵を格納する第１鍵格納部とを備え、前記情報処理方法は、前記第１データ格納部に格納されている暗号化共有データの更新が指示されると、更新された共有データを前記第１暗号鍵で暗号化して前記第１データ格納部に記録し、前記暗号化された第２暗号鍵を前記第１暗号鍵に対応する第１復号鍵を用いて復号して前記第２暗号鍵を生成するよう、前記第１システムを制御し、前記第１システムで生成された第２暗号鍵で前記更新された共有データを暗号化して前記第２データ格納部に記録することで前記暗号化共有データを更新するよう、前記第２システムを制御するものである。

[0321] また、本発明の第１５の態様に係る情報処理プログラムは、第１システムと第２システムとが動作する情報処理装置で用いられる情報処理プログラムであって、前記第１システムと前記第２システムとは、データを暗号化して管理する互いに独立したシステムであり、前記情報処理装置は、前記第１システムと前記第２システムとの間で共有される共有データを前記第１システム用の鍵である第１暗号鍵で暗号化した暗号化共有データを格納する第１デ

一タ格納部と、前記共有データを前記第２システム用の鍵である第２暗号鍵で暗号化した暗号化共有データを格納する第２データ格納部と、前記第１システム用の鍵として、前記第１暗号鍵を用いて暗号化された前記第２暗号鍵を格納する第１鍵格納部とを備え、前記情報処理プログラムは、前記第１データ格納部に格納されている暗号化共有データの更新が指示されると、更新された共有データを前記第１暗号鍵で暗号化して前記第１データ格納部に記録し、前記暗号化された第２暗号鍵を前記第１暗号鍵に対応する第１復号鍵を用いて復号して前記第２暗号鍵を生成するよう、前記第１システムを制御し、前記第１システムで生成された第２暗号鍵で前記更新された共有データを暗号化して前記第２データ格納部に記録することで前記暗号化共有データを更新するよう、前記第２システムを制御するものである。

[0322] 本発明の第１６の態様に係る情報処理プログラムは、コンピュータ読み取り可能な記録媒体に記録されているものである。

[0323] 本発明の第１７の態様に係る情報処理集積回路は、第１システムと第２システムとが動作する情報処理装置で用いられる集積回路であって、前記第１システムと前記第２システムとは、データを暗号化して管理する互いに独立したシステムであり、前記情報処理装置は、前記第１システムと前記第２システムとの間で共有される共有データを前記第１システム用の鍵である第１暗号鍵で暗号化した暗号化共有データを格納する第１データ格納部と、前記共有データを前記第２システム用の鍵である第２暗号鍵で暗号化した暗号化共有データを格納する第２データ格納部と、前記第１システム用の鍵として、前記第１暗号鍵を用いて暗号化された前記第２暗号鍵を格納する第１鍵格納部とを備え、前記集積回路は、前記第１データ格納部に格納されている暗号化共有データの更新が指示されると、更新された共有データを前記第１暗号鍵で暗号化して前記第１データ格納部に記録し、前記暗
号化された第２暗号鍵を前記第１暗号鍵に対応する第１復号鍵を用いて復号して前記第２暗号鍵を生成するよう、前記第１システムを制御し、前記第１システムで生成された第２暗号鍵で前記更新された共有データを暗号化して

前記第２データ格納部に記録することで前記暗号化共有データを更新するよう、前記第２システムを制御するものである。

[0324] また、本発明の一の実施態様である情報処理装置は、第１システムと第２システムとが動作する情報処理装置であって、前記第１システムと前記第２システムとの間で共有される共有データを前記第１システム用の鍵である第１暗号鍵で暗号化した暗号化共有データを格納する第１データ格納部と、前記共有データを前記第２システム用の鍵である第２暗号鍵で暗号化した暗号化共有データを格納する第２データ格納部と、前記第１システム用の鍵として、前記第１暗号鍵を用いて暗号化された前記第２暗号鍵を格納する第１鍵格納部と、前記第１システムと前記第２システムとを制御する制御部とを備え、前記制御部は、前記第１データ格納部に格納されている暗号化共有データの更新が指示されると、更新された共有データを前記第１暗号鍵で暗号化して前記第１データ格納部に記録し、前記暗号化された第２暗号鍵を前記第１暗号鍵に対応する第１復号鍵を用いて復号して前記第２暗号鍵を生成するよう、前記第１システムを制御し、前記第１システムで生成された第２暗号鍵で前記更新された共有データを暗号化して前記第２データ格納部に記録することを特徴とする。

[0325] このような構成により、本発明に関する情報処理装置は、更新された共有データを前記第１暗号鍵で暗号化して前記第１データ格納部に記録し、前記暗号化された第２暗号鍵を前記第１暗号鍵に対応する第１復号鍵を用いて復号して前記第２暗号鍵を生成するよう、前記第１システムを制御し、前記第１システムで生成された第２暗号鍵で前記更新された共有データを暗号化して前記第２データ格納部に記録する。この構成により、本発明に関する情報処理装置は、第２のシステムの持つ第２暗号鍵を、第１のシステムから直接復号することができる。これにより、第２のシステムに第２暗号鍵を取得する手間が省け、更新されたデータを高速に同期させることができる。

[0326] （１７）上記の実施の形態で述べた構成要素については、１個のシステムＬＳＩ（Ｌａｒｇｅ　Ｓｃａｌｅ　Ｉｎｔｅｇｒａｔｉｏｎ：大規模集積回

路）から構成されているとしてもよい。システムＬＳＩは、複数の構成部を１個のチップ上に集積して製造された超多機能ＬＳＩであり、具体的には、マイクロプロセッサ、ＲＯＭ、ＲＡＭなどを含んで構成されるコンピュータシステムである。前記ＲＡＭには、コンピュータプログラムが記憶されている。前記マイクロプロセッサが、前記コンピュータプログラムにしたがって動作することにより、システムＬＳＩは、その機能を達成する。

[0327] また、上記の各装置を構成する構成要素の各部は、個別に１チップ化されていても良いし、一部又は全てを含むように１チップ化されてもよい。この場合、上記の構成要素をソフトウェアで実装するよりも処理を高速化することができる。

[0328] （１８）システムＬＳＩは集積度の違いにより、ＩＣ、ＬＳＩ、スーパーＬＳＩ、ウルトラＬＳＩと呼称されることもあるが、システムＬＳＩを上記のいずれの集積度で実現した場合も本発明に含まれることは言うまでもない。また、ＬＳＩ製造後に、プログラムすることが可能なＦＰＧＡ（Ｆｉｅｌｄ Ｐｒｏｇｒａｍｍａｂｌｅ Ｇａｔｅ Ａｒｒａｙ）や、ＬＳＩ内部の回路セルの接続や設定を再構成可能なリコンフィギュラブル・プロセッサを利用しても良い。

[0329] さらには、半導体技術の進歩または派生する別技術によりＬＳＩに置き換わる集積回路化の技術が登場すれば、当然、その技術を用いて構成要素の集積化を行ってもよい。バイオ技術の適応等が可能性としてありえる。

[0330] （１９）上記の各装置を構成する構成要素の一部または全部は、各装置に脱着可能なＩＣカードまたは単体のモジュールから構成されているとしてもよい。前記ＩＣカードまたは前記モジュールは、マイクロプロセッサ、ＲＯＭ、ＲＡＭなどから構成されるコンピュータシステムである。前記ＩＣカードまたは前記モジュールは、上記の超多機能ＬＳＩを含むとしてもよい。マイクロプロセッサが、コンピュータプログラムにしたがって動作することにより、前記ＩＣカードまたは前記モジュールは、その機能を達成する。このＩＣカードまたはこのモジュールは、耐タンパ性を有するとしてもよい。

[0331] （２０）また、本発明は、前記コンピュータプログラムまたは前記デジタル信号をコンピュータ読み取り可能な記録媒体、例えば、フレキシブルディスク、ハードディスク、ＣＤ－ＲＯＭ、ＭＯ、ＤＶＤ、ＤＶＤ－ＲＯＭ、ＤＶＤ－ＲＡＭ、ＢＤ（Ｂｌｕ－ｒａｙＤｉｓｃ）、半導体メモリなどに記録したものとしてもよい。また、これらの記録媒体に
記録されている前記デジタル信号であるとしてもよい。

[0332] また、本発明は、前記コンピュータプログラムまたは前記デジタル信号を、電気通信回線、無線または有線通信回線、インターネットを代表とするネットワーク、データ放送等を経由して伝送するものとしてもよい。

[0333] また、本発明は、マイクロプロセッサとメモリを備えたコンピュータシステムであって、前記メモリは、上記コンピュータプログラムを記憶しており、前記マイクロプロセッサは、前記コンピュータプログラムにしたがって動作するとしてもよい。

[0334] また、前記プログラムまたは前記デジタル信号を前記記録媒体に記録して移送することにより、または前記プログラムまたは前記デジタル信号を前記ネットワーク等を経由して移送することにより、独立した他のコンピュータシステムにより実施するとしてもよい。

[0335] （２１）これらの実施の形態および変形例の組合せであってもよい。

産業上の利用可能性

[0336] 本発明にかかる複数の木構造の鍵データベースの鍵で保護されたデータを管理する鍵管理ソフトウェアにおける、鍵使用の高速化手法は、２つの鍵データベースを用いて同一のデータを同期する際に、あらかじめ設定された別鍵データベースの鍵を利用して、別データベースで管理するデータを更新するため、鍵の復号回数を削減するという効果を有する。そのため、高速なデータ同期を行う機器等の分野で特に有効である。

符号の説明

[0337] １０ 情報処理装置

１１１ ＣＰＵ

１１２　第１記憶部

１１３　第２記憶部

１１４　暗復号処理部

１１５　バス

１１６　鍵管理ソフトウェア

１１７　アプリケーションプログラムＡ

１１８　アプリケーションプログラムＢ

１１９　データアクセス部

１２０　鍵データベースＡ

１２１　鍵データベースＢ

１２２　暗号化データ格納部

１２３　不揮発性メモリ部

１２４　暗復号エンジン部

１２５　鍵データベースＢ用鍵格納部

１２６　鍵データベースＡ用鍵格納部

２０１　利用データベース判定部

２０２　平文データ抽出部

２０３　ハッシュ値生成部

２０４　ハッシュ値判定部

２０５　ハンドラ値判定部

２０６　鍵取得部

２０７　管理テーブル格納部

２０８　管理テーブル更新部

請求の範囲

[請求項1] それぞれデータを暗号化して保管する複数の暗復号システムを有する情報処理装置であって、

一の暗復号システムにおける暗号化の対象データを取得するデータ取得手段と、

前記対象データが、他の暗復号システムにおいて暗号化されて保管されているか否かを判断する判断手段と、

保管されていると判断する場合に、他の暗復号システムにおいて保管されている暗号化データの鍵を取得する鍵取得手段と、

前記一の暗復号システムにおいて用いられる鍵記憶手段と、

前記一の暗復号システムにおいて、前記対象データに対応付けて、取得した前記鍵を前記鍵記憶手段に書き込む鍵書込手段と

を備えることを特徴とする情報処理装置。

[請求項2] それぞれデータを暗号化して記憶する第１暗復号システム及び第２暗復号システムを有する情報処理装置であって、

前記第１暗復号システムにおける暗号化の対象データを取得するデータ取得手段と、

前記対象データを暗号化して生成した暗号化データが、前記第２暗復号システムにおいて記憶されているか否かを判断する判断手段と、

記憶されていると判断する場合に、前記第２暗復号システムにおいて前記暗号化データを暗号化するために用いられる第２鍵を取得する鍵取得手段と、

前記第１暗復号システムにおいて用いられる第１鍵記憶手段と、

前記第１暗復号システムにおいて、前記対象データを暗号化するために用いられる第１鍵を用いて、取得した前記第２鍵を暗号化して暗号化第２鍵を生成する暗復号化手段と、

前記第１暗復号システムにおいて、前記対象データに対応付けて、生成した前記暗号化第２鍵を前記第１鍵記憶手段に書き込む鍵書込手

段と

を備えることを特徴とする情報処理装置。

[請求項3] 前記情報処理装置は、さらに、前記第２暗復号システムにおいて、前記暗号化データとして、前記第２鍵を用いて前記対象データを暗号化して生成した第２暗号化対象データを記憶している第２データ格納手段を備え、

前記判断手段は、前記暗号化データとしての前記第２暗号化対象データが、前記第２データ格納手段に記憶されているか否かを判断することを特徴とする請求項２に記載の情報処理装置。

[請求項4] 前記暗復号化手段は、さらに、前記第１暗復号システムにおいて、前記第１鍵を用いて前記対象データを暗号化して第１暗号化対象データを生成し、

前記情報処理装置は、さらに、

前記第１暗復号システムにおける第１データ格納手段と、

生成した前記第１暗号化対象データを前記第１データ格納手段に書き込むデータ書込手段と

を備えることを特徴とする請求項３に記載の情報処理装置。

[請求項5] 前記情報処理装置は、さらに、

前記対象データに対応付けて、前記第２暗復号システムにおいて前記暗号化データが記憶されている位置を示す位置情報を含む管理テーブルを記憶しているテーブル記憶手段を備え、

前記判断手段は、前記対象データに対応する位置情報が前記管理テーブルに記憶されているか否かを判断することにより、前記暗号化データが前記第２暗号化手段において記憶されているか否かを判断することを特徴とする請求項４に記載の情報処理装置。

[請求項6] 前記データ取得手段は、さらに、前記対象データの更新の指示を取得し、

前記判断手段は、さらに、前記指示に係る前記対象データを暗号化

して生成した暗号化データが、前記第２暗復号システムにおいて記憶されているか否かを判断し、

前記鍵取得手段は、さらに、記憶されていると判断する場合に、前記第１鍵記憶手段から前記暗号化第２鍵を取得し、

前記暗復号化手段は、さらに、取得した前記暗号化第２鍵を復号して第２鍵を生成し、生成した第２鍵を用いて、前記対象データの更新により得られた更新データを暗号化して第２暗号化更新データを生成し、

前記データ書込手段は、さらに、生成した前記第２暗号化更新データを、前記第２データ格納手段に記憶されている前記第２暗号化対象データに上書きする

ことを特徴とする請求項５に記載の情報処理装置。

[請求項7] 前記暗復号化手段は、前記第１鍵に対応する復号鍵を用いて、前記暗号化第２鍵を復号する

ことを特徴とする請求項６に記載の情報処理装置。

[請求項8] 前記管理テーブルは、前記対象データに対応付けて、さらに、前記第１鍵に対応する復号鍵が記憶されている位置を示す鍵位置情報を含み、

前記暗復号手段は、前記鍵位置情報により示される位置から取得した前記復号鍵を用いる

ことを特徴とする請求項７に記載の情報処理装置。

[請求項9] 前記暗復号化手段は、さらに、前記第１鍵を用いて、前記更新データを暗号化して第１暗号化更新データを生成し、

前記データ書込手段は、さらに、生成した前記第１暗号化更新データを、前記第１データ格納手段に記憶されている前記第１暗号化対象データに上書きする

ことを特徴とする請求項６に記載の情報処理装置。

[請求項10] 前記データ書込手段は、前記第１暗号化更新データを前記第１デー

タ格納手段に記憶されている前記第１暗号化対象データに上書きした後、同期指示を受け取った場合に、前記第２暗号化更新データを、前記第２データ格納手段に記憶されている前記第２暗号化対象データに上書きする

ことを特徴とする請求項９に記載の情報処理装置。

[請求項11] 前記管理テーブルに含まれる前記位置情報は、前記第２データ格納手段において前記第２暗号化対象データが記憶されている位置を示し、

前記データ書込手段は、前記位置情報により示される位置において、前記第２暗号化更新データを書き込む

ことを特徴とする請求項９に記載の情報処理装置。

[請求項12] 前記暗復号化手段は、さらに、前記第１データ格納手段に記憶されている前記第１暗号化対象データを復号して、対象データを生成し、生成した対象データを基にして得られた更新データを暗号化する

ことを特徴とする請求項６に記載の情報処理装置。

[請求項13] 前記管理テーブルは、前記対象データの要約値と前記位置情報とを対応付けて含み、

前記判断手段は、前記対象データからその要約値を算出し、得られた要約値に対応する前記位置情報が前記管理テーブルに記憶されているか否かを判断する

ことを特徴とする請求項５に記載の情報処理装置。

[請求項14] 前記管理テーブルは、前記第１暗号化対象データの要約値と前記位置情報とを対応付けて含み、

前記判断手段は、第１データ格納手段に記憶されている前記第１暗号化対象データからその要約値を算出し、得られた要約値に対応する前記位置情報が前記管理テーブルに記憶されているか否かを判断する

ことを特徴とする請求項５に記載の情報処理装置。

[請求項15] 前記情報処理装置は、さらに、前記第２暗復号システムにおいて用

いられる第２鍵記憶手段を備え、

前記データ取得手段は、さらに、前記第２暗復号システムにおける暗号化の対象データを取得し、

前記判断手段は、さらに、前記対象データを暗号化して生成した暗号化データが、前記第１暗復号システムにおいて記憶されているか否かを判断し、

前記鍵取得手段は、さらに、記憶されていると判断する場合に、前記第１暗復号システムにおいて前記暗号化データを暗号化するために用いられる第１鍵を取得し、

前記暗復号化手段は、さらに、前記第２暗復号システムにおいて、前記対象データを暗号化するために用いられる第２鍵を用いて、取得した前記第１鍵を暗号化して暗号化第１鍵を生成し、

前記鍵書込手段は、さらに、前記第２暗復号システムにおいて、前記対象データに対応付けて、生成した前記暗号化第１鍵を前記第２鍵記憶手段に書き込む

ことを特徴とする請求項２に記載の情報処理装置。

[請求項16] 前記暗復号化手段は、さらに、前記第２暗復号システムにおいて、前記第２鍵を用いて前記対象データを暗号化して第２暗号化対象データを生成し、

前記情報処理装置は、さらに、

前記第２暗復号システムにおける第２データ格納手段と、

生成した前記第２暗号化対象データを前記第２データ格納手段に書き込むデータ書込手段と

を備えることを特徴とする請求項１５に記載の情報処理装置。

[請求項17] 前記データ取得手段は、さらに、前記対象データの更新の指示を取得し、

前記判断手段は、さらに、前記指示に係る前記対象データを暗号化して生成した暗号化データが、前記第１暗復号システムにおいて記憶

されているか否かを判断し、

前記鍵取得手段は、さらに、記憶されていると判断する場合に、前記第２鍵記憶手段から前記暗号化第１鍵を取得し、

前記暗復号化手段は、さらに、取得した前記暗号化第１鍵を復号して第１鍵を生成し、生成した第１鍵を用いて、前記対象データの更新により得られた更新データを暗号化して第１暗号化更新データを生成し、

前記データ書込手段は、さらに、生成した前記第１暗号化更新データを、前記第１データ格納手段に記憶されている前記第１暗号化対象データに上書きする

ことを特徴とする請求項１６に記載の情報処理装置。

[請求項18] 前記第１鍵記憶手段は、第１暗復号システムにおいて、鍵を階層構造により管理し、階層構造の各鍵の下位には、当該鍵を用いて復号できるように暗号化された鍵が割り当てられており、

鍵書込手段は、前記暗号化第２鍵を、前記第２鍵の下位に割り当てて書き込む

ことを特徴とする請求項２に記載の情報処理装置。

[請求項19] 前記情報処理装置は、さらに、第１暗復号システムにおける暗号化データを利用するアプリケーションプログラムに従って動作するプロセッサを備えており、

前記アプリケーションプログラムは、暗号化の対象データを出力する命令を含み、

前記プロセッサは、前記データ取得手段に対して、暗号化の対象データを出力する

ことを特徴とする請求項２に記載の情報処理装置。

[請求項20] 前記情報処理装置は、さらに、前記第１暗復号システムにおいて復号された鍵を、前記第１暗復号システム用であることを示す第１タイプ情報と対応付けて保持し、前記第２暗復号システムにおいて復号さ

れた鍵を、前記第２暗復号システム用であることを示す第２タイプ情報と対応付けて保持する鍵格納手段を備え、

前記暗復号化手段は、前記第１暗復号システムにおいては、前記第１タイプ情報と対応付けられた鍵を用いて復号を行い、

前記暗復号化手段は、前記第２暗復号システムにおいては、前記第２タイプ情報と対応付けられた鍵を用いて暗号化を行い、

前記情報処理装置は、さらに、前記第１暗復号システムにおける復号の結果、前記第１タイプ情報と対応付けられて前記鍵格納手段に保持された鍵について、前記第１タイプ情報を前記第２暗復号システム用であることを示す前記第２タイプ情報に書き換えることで、前記鍵を用いた前記更新データの暗号化を前記第２暗復号システムにおいて行わせる制御手段を備える

ことを特徴とする請求項２に記載の情報処理装置。

[請求項21] 前記鍵格納手段は、所定の容量を持つ複数のブロックから構成されており、保持する鍵それぞれがどのブロックに格納されているかを示すブロック情報を、前記保持する鍵それぞれと対応付けて保持している

ことを特徴とする請求項２０に記載の情報処理装置。

[請求項22] 前記暗復号化手段は、

制御部と、

前記第１暗復号システム用の前記第１鍵を保持する鍵格納部と、

前記鍵格納部に保持されている前記第１鍵を用いて、暗号化する暗復号エンジン部とを備え、

前記制御部は、前記第１鍵を取得して前記鍵格納部に保持させるにあたって、前記鍵格納部の空き領域が不足している場合に、前記鍵格納部が既に保持している一の鍵を、前記暗復号エンジン部により、暗号化して前記鍵格納部の外に退避し、前記鍵格納部において、退避対象の前記鍵が保持されていた領域に取得した前記第１鍵を上書きし、

前記第１暗復号システムにおける前記第１鍵を用いた暗号化が完了した後、退避した前記暗号化鍵を、前記暗復号エンジン部により、復号して前記第１鍵が保持されている領域に上書きする

ことを特徴とする請求項２に記載の情報処理装置。

[請求項23] それぞれデータを暗号化して記憶する第１暗復号システム及び第２暗復号システムを有し、前記第１暗復号システムにおいて用いられる第１鍵記憶手段を備える情報処理装置において用いられる方法であって、

前記第１暗復号システムにおける暗号化の対象データを取得するデータ取得ステップと、

前記対象データを暗号化して生成した暗号化データが、前記第２暗復号システムにおいて記憶されているか否かを判断する判断ステップと、

記憶されていると判断する場合に、前記第２暗復号システムにおいて前記暗号化データを暗号化するために用いられる第２鍵を取得する鍵取得ステップと、

前記第１暗復号システムにおいて、前記対象データを暗号化するために用いられる第１鍵を用いて、取得した前記第２鍵を暗号化して暗号化第２鍵を生成する暗復号化ステップと、

前記第１暗復号システムにおいて、前記対象データに対応付けて、生成した前記暗号化第２鍵を前記第１鍵記憶手段に書き込む鍵書込ステップと

を備えることを特徴とする方法。

[請求項24] それぞれデータを暗号化して記憶する第１暗復号システム及び第２暗復号システムを有し、前記第１暗復号システムにおいて用いられる第１鍵記憶手段を備える情報処理装置において用いられるコンピュータプログラムであって、

コンピュータである前記情報処理装置に、

前記第１暗復号システムにおける暗号化の対象データを取得するデータ取得ステップと、

前記対象データを暗号化して生成した暗号化データが、前記第２暗復号システムにおいて記憶されているか否かを判断する判断ステップと、

記憶されていると判断する場合に、前記第２暗復号システムにおいて前記暗号化データを暗号化するために用いられる第２鍵を取得する鍵取得ステップと、

前記第１暗復号システムにおいて、前記対象データを暗号化するために用いられる第１鍵を用いて、取得した前記第２鍵を暗号化して暗号化第２鍵を生成する暗復号化ステップと、

前記第１暗復号システムにおいて、前記対象データに対応付けて、生成した前記暗号化第２鍵を前記第１鍵記憶手段に書き込む鍵書込ステップと

を実行させるためのコンピュータプログラム。

[請求項25] 前記コンピュータプログラムは、コンピュータ読み取り可能な記録媒体に記録されていることを特徴とする請求項２４に記載のコンピュータプログラム。

[請求項26] それぞれデータを暗号化して記憶する第１暗復号システム及び第２暗復号システムを有する集積回路であって、

前記第１暗復号システムにおける暗号化の対象データを取得するデータ取得手段と、

前記対象データを暗号化して生成した暗号化データが、前記第２暗復号システムにおいて記憶されているか否かを判断する判断手段と、

記憶されていると判断する場合に、前記第２暗復号システムにおいて前記暗号化データを暗号化するために用いられる第２鍵を取得する鍵取得手段と、

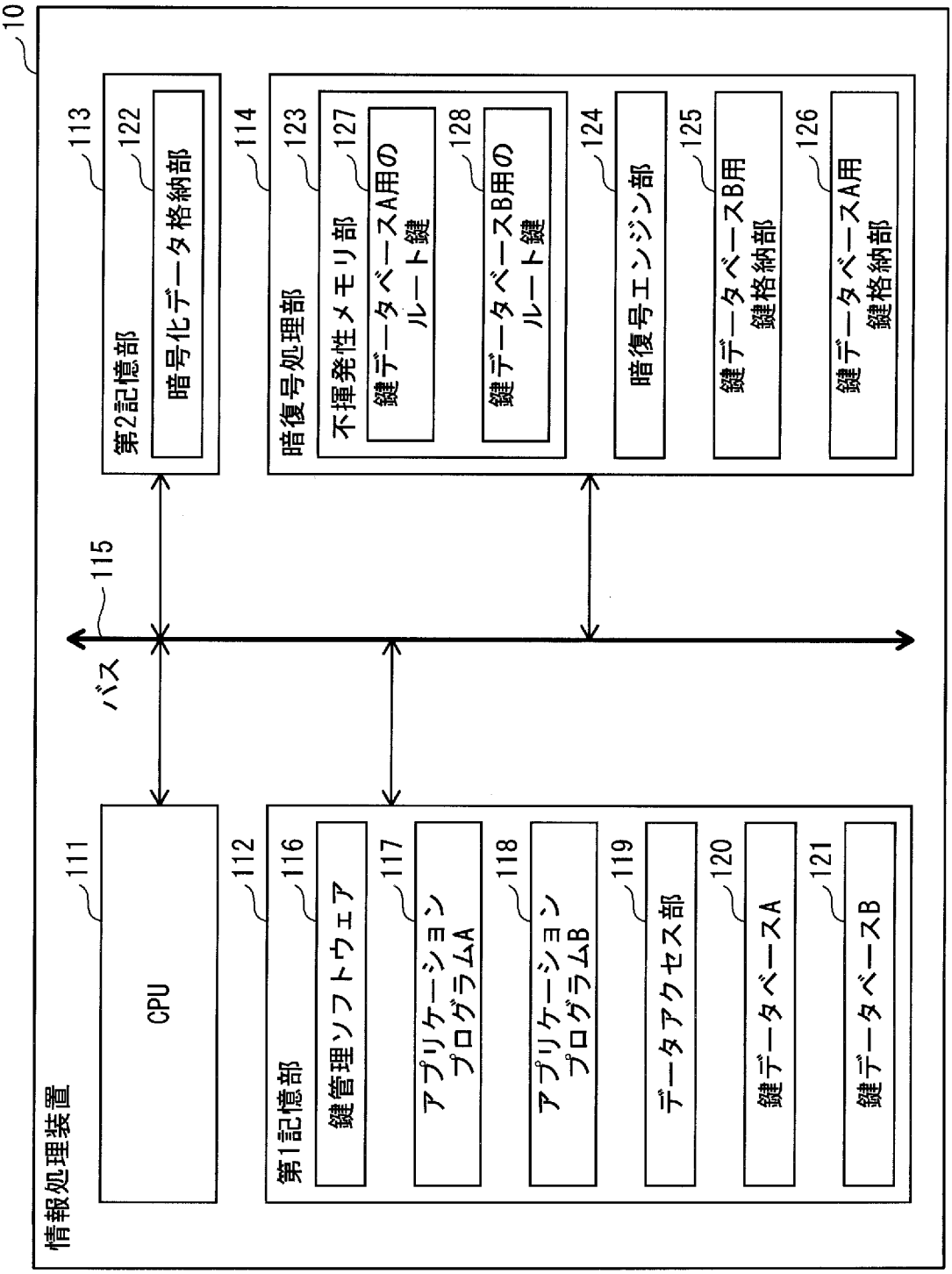
前記第１暗復号システムにおいて用いられる第１鍵記憶手段と、

前記第１暗復号システムにおいて、前記対象データを暗号化するために用いられる第１鍵を用いて、取得した前記第２鍵を暗号化して暗号化第２鍵を生成する暗復号化手段と、

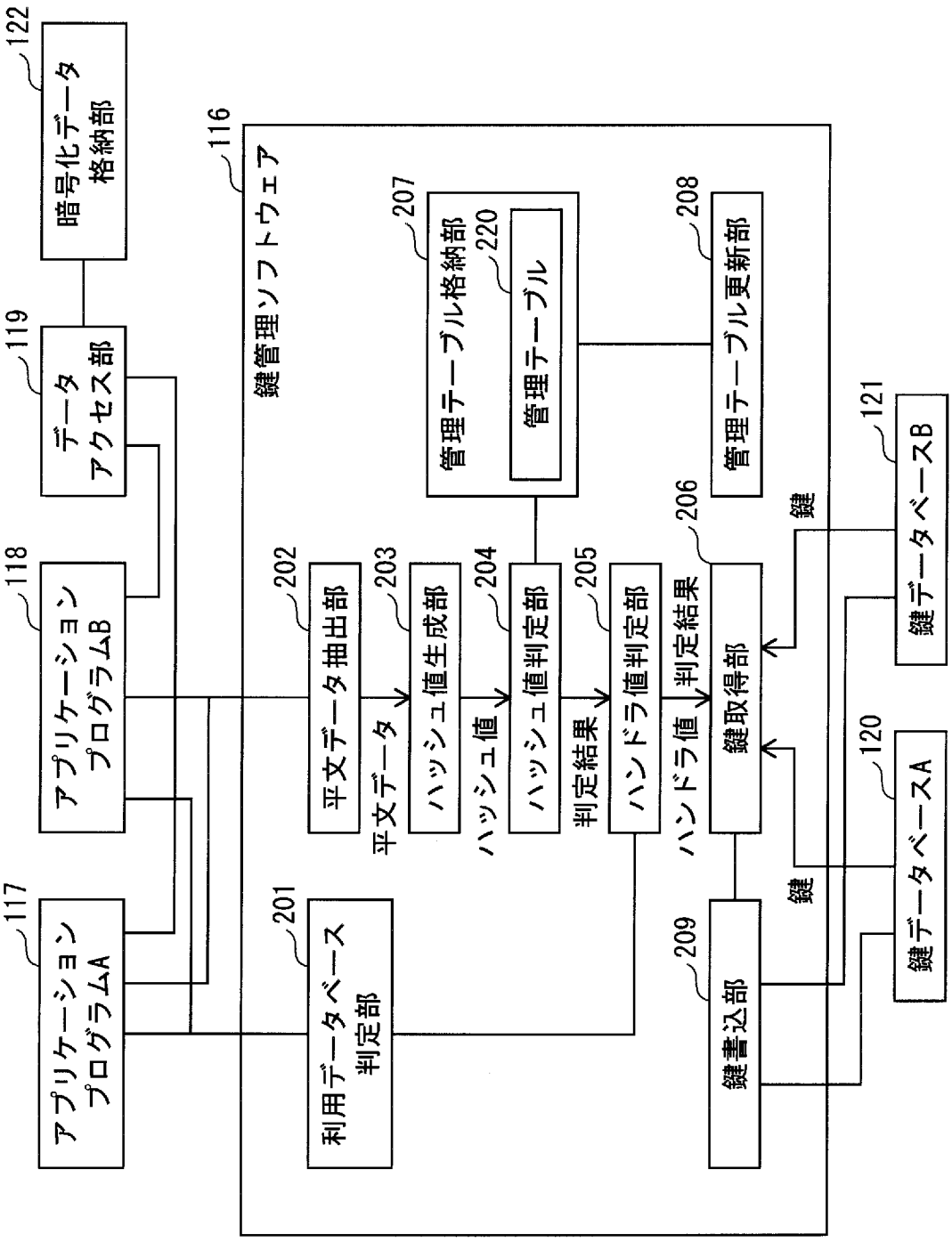
前記第１暗復号システムにおいて、前記対象データに対応付けて、生成した前記暗号化第２鍵を前記第１鍵記憶手段に書き込む鍵書込手段と

を備えることを特徴とする集積回路。

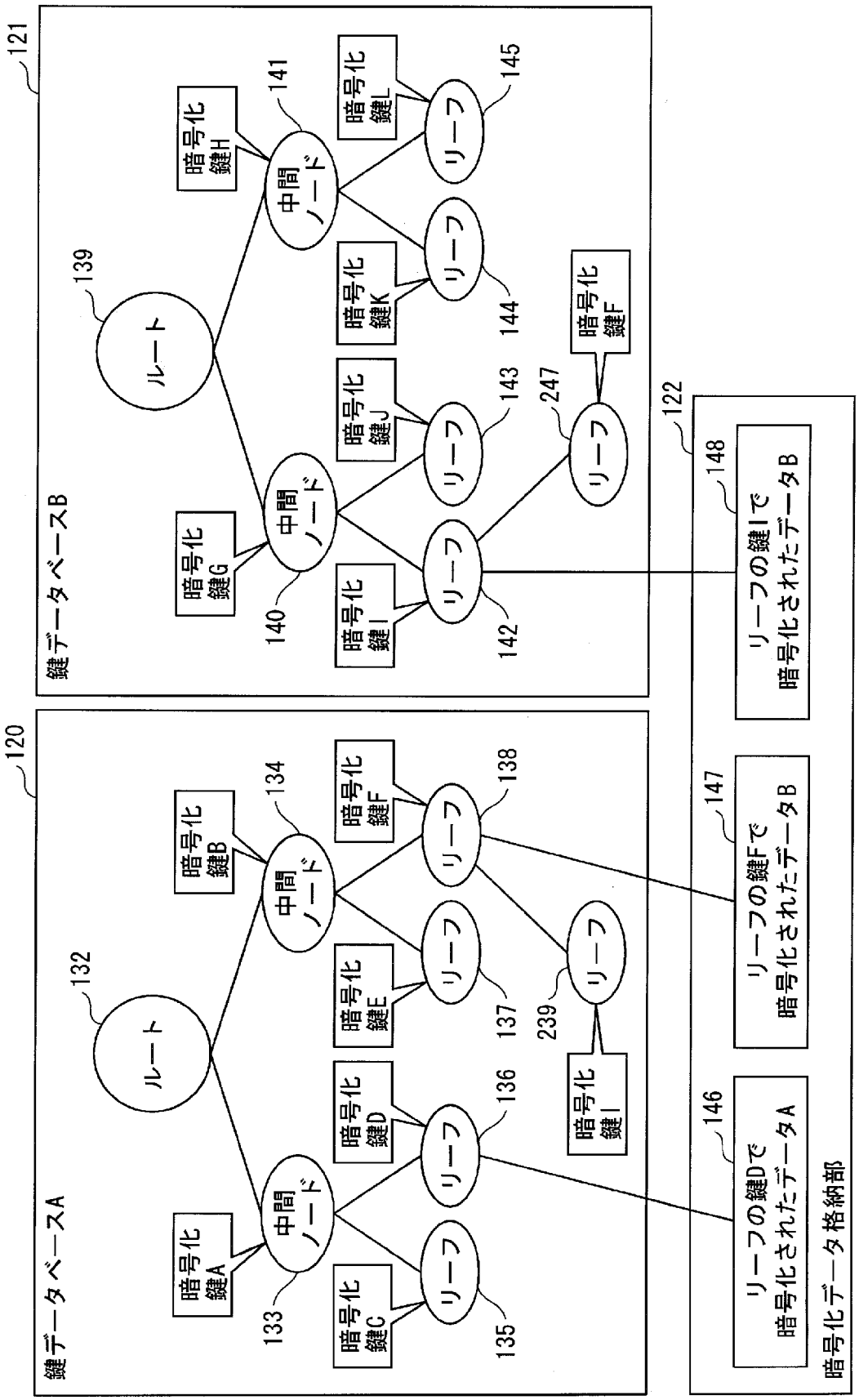
[図1]


10
情報処理装置
CPU
111
第1記憶部
112
鍵管理ソフトウェア
116
アプリケーション
プログラムA
117
アプリケーション
プログラムB
118
データアクセス部
119
鍵データベースA
120
鍵データベースB
121
バス
115
第2記憶部
113
暗号化データ格納部
122
暗復号処理部
114
不揮発性メモリ部
123
鍵データベースA用の
ルート鍵
127
鍵データベースB用の
ルート鍵
128
暗復号エンジン部
124
鍵データベースB用
鍵格納部
125
鍵データベースA用
鍵格納部
126

[図2]


122
暗号化データ格納部
116
鍵管理ソフトウェア
119
データアクセス部
207
管理テーブル格納部
220
管理テーブル
208
管理テーブル更新部
118
アプリケーションプログラムB
202
平文データ抽出部
203
ハッシュ値生成部
204
ハッシュ値判定部
205
ハンドラ値判定部
206
鍵取得部
121
鍵データベースB
117
アプリケーションプログラムA
201
利用データベース判定部
209
鍵書込部
120
鍵データベースA
平文データ
ハッシュ値
判定結果
ハンドラ値
判定結果
鍵
鍵

[図3]


鍵データベースA
120
ルート
132
中間ノード
133
中間ノード
134
リーフ
135
リーフ
136
リーフ
137
リーフ
138
暗号化鍵A
暗号化鍵B
暗号化鍵C
暗号化鍵D
暗号化鍵E
暗号化鍵F
暗号化鍵I
239
鍵データベースB
121
ルート
139
中間ノード
140
中間ノード
141
リーフ
142
リーフ
143
リーフ
144
リーフ
145
247
暗号化鍵G
暗号化鍵H
暗号化鍵I
暗号化鍵J
暗号化鍵K
暗号化鍵L
暗号化鍵F
暗号化データ格納部
122
リーフの鍵Dで暗号化されたデータA
146
リーフの鍵Fで暗号化されたデータB
147
リーフの鍵Iで暗号化されたデータB
148

[図4]

鍵データベースAのノード情報構造体 150

151	鍵長	2048ビット
152	鍵	0xFF 0xFE ... 0x00
153	親ノード識別子	ノード番号
154	鍵ハンドラ値	0xFF 0xFE ... 0x00
155	データハンドラ値	NULL
156	データ	0xAA 0xBB ... 0x1F
157	その他の付属情報	フラグ設定済み

[図5]

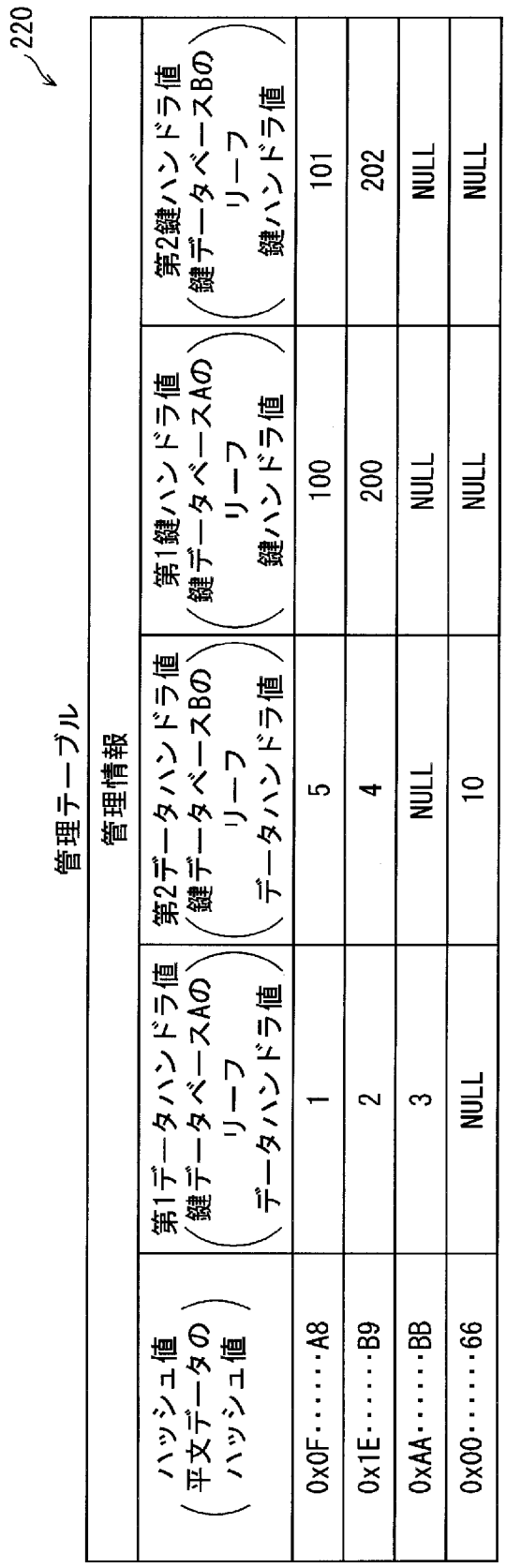
鍵データベースBのノード情報構造体 160

161	暗号種別	RSA暗号
162	鍵長	2048ビット
163	リンク先情報	鍵やデータを格納した場所のリンク先情報
164	親ノード識別子	ノード番号
165	鍵ハンドラ値	NULL
166	データハンドラ値	0x11 0x22 ... 0x00
167	その他の付属情報	フラグ設定済み

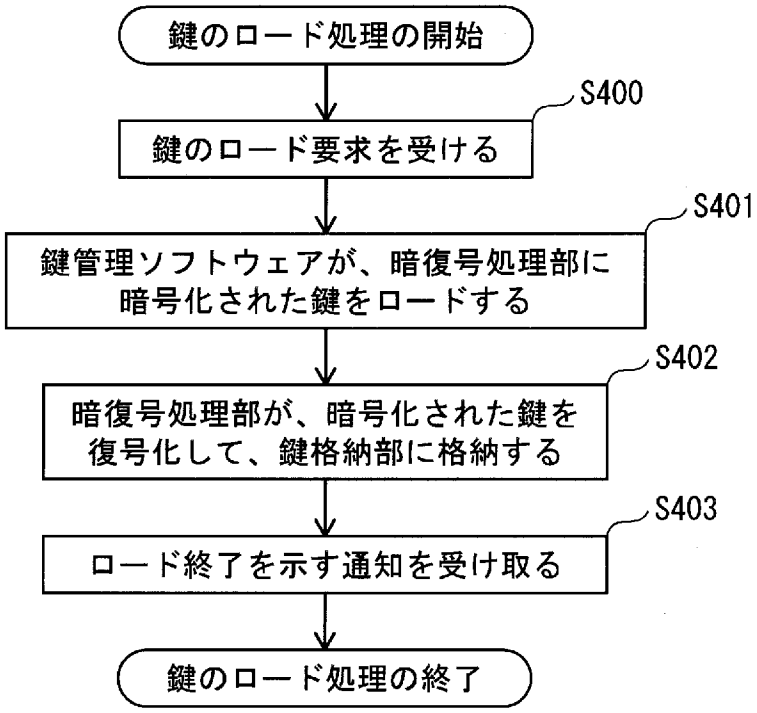
168

鍵、
または
データ

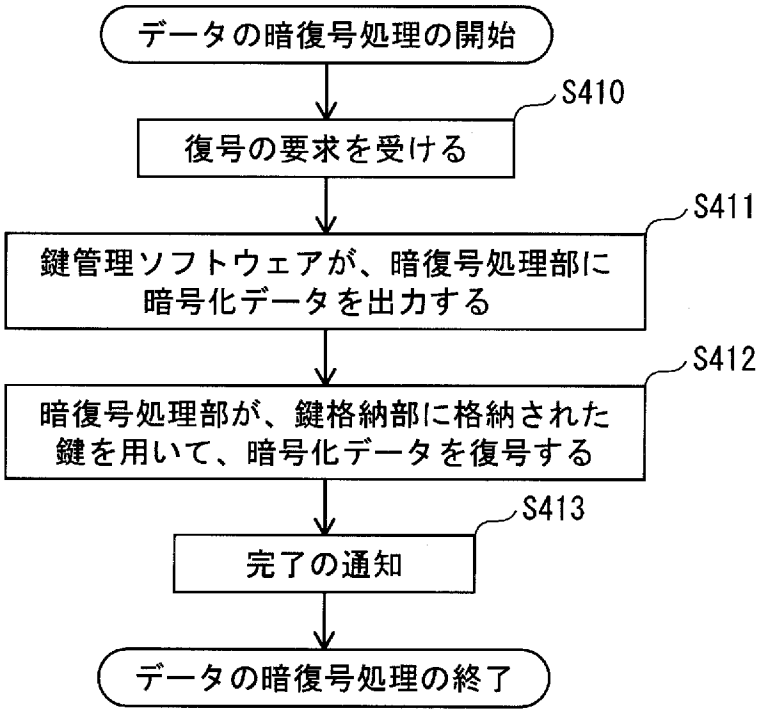
[図6]


220
管理テーブル
管理情報
ハッシュ値
(平文データのハッシュ値)
第1データハンドラ値
(鍵データベースAのリーフデータハンドラ値)
第2データハンドラ値
(鍵データベースBのリーフデータハンドラ値)
第1鍵ハンドラ値
(鍵データベースAのリーフ鍵ハンドラ値)
第2鍵ハンドラ値
(鍵データベースBのリーフ鍵ハンドラ値)
0x0F……A8
1
5
100
101
0x1E……B9
2
4
200
202
0xAA……BB
3
NULL
NULL
NULL
0x00……66
NULL
10
NULL
NULL

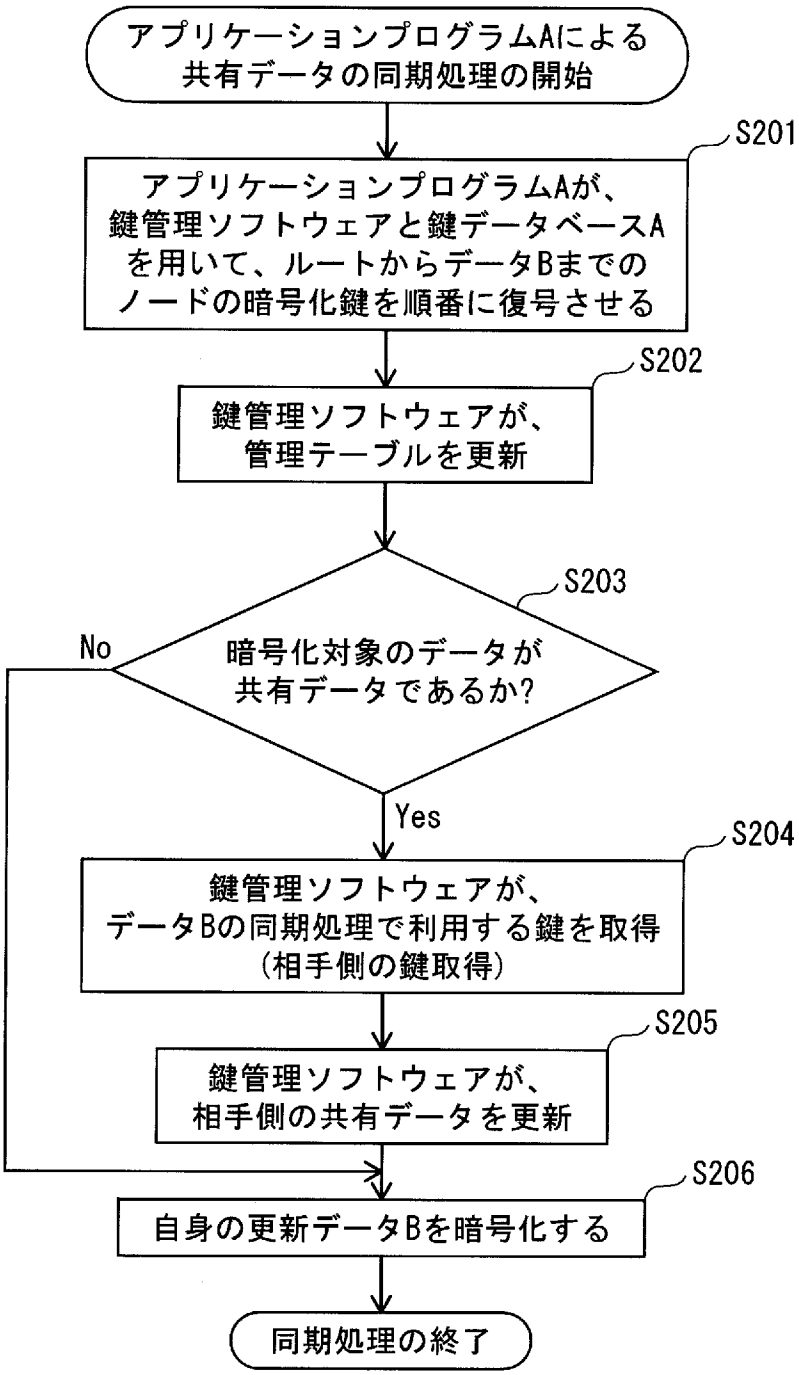
[図7]


鍵のロード処理の開始
S400
鍵のロード要求を受ける
S401
鍵管理ソフトウェアが、暗復号処理部に
暗号化された鍵をロードする
S402
暗復号処理部が、暗号化された鍵を
復号化して、鍵格納部に格納する
S403
ロード終了を示す通知を受け取る
鍵のロード処理の終了

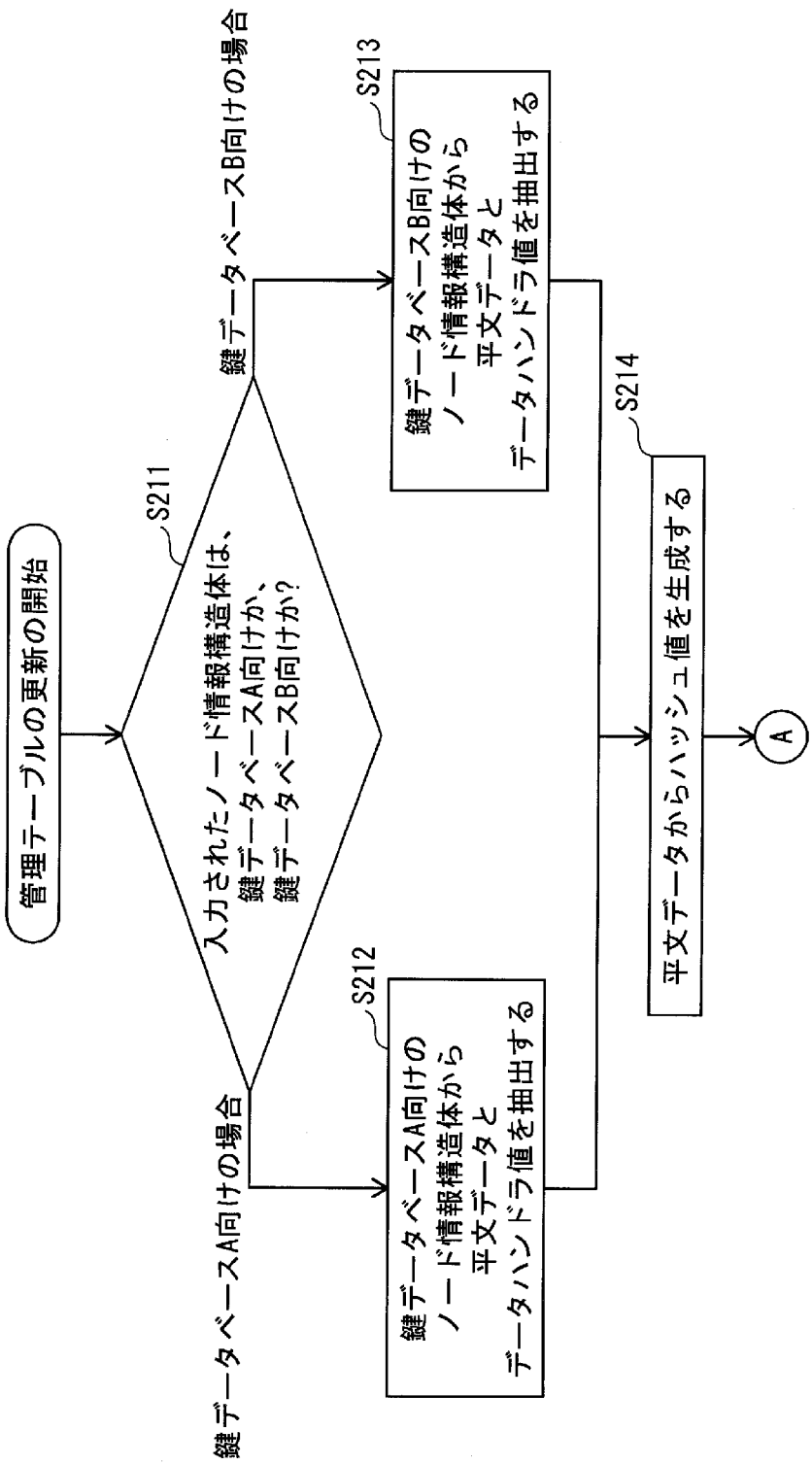
[図8]


データの暗復号処理の開始
S410
復号の要求を受ける
S411
鍵管理ソフトウェアが、暗復号処理部に
暗号化データを出力する
S412
暗復号処理部が、鍵格納部に格納された
鍵を用いて、暗号化データを復号する
S413
完了の通知
データの暗復号処理の終了

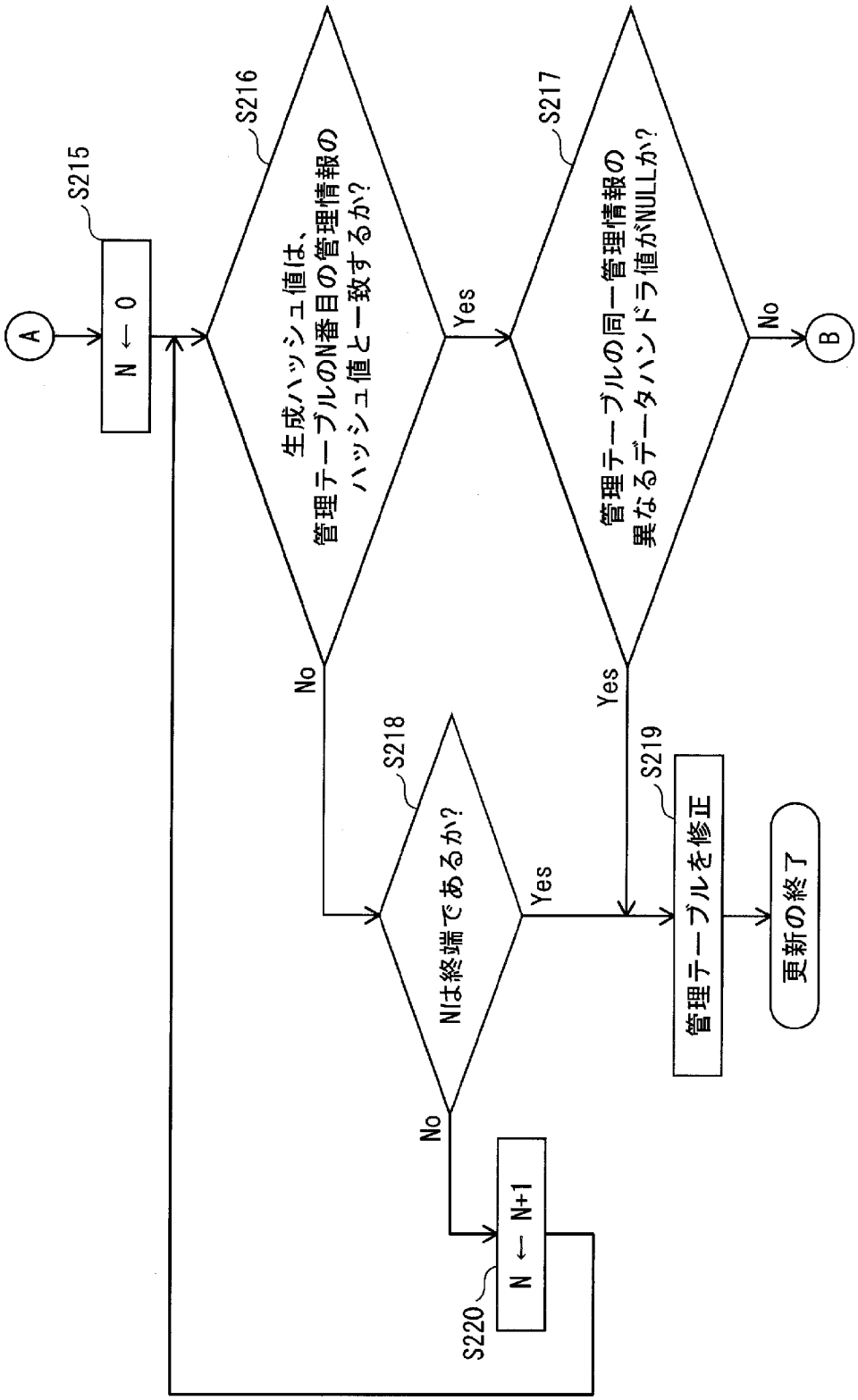
[図9]


アプリケーションプログラムAによる
共有データの同期処理の開始
S201
アプリケーションプログラムAが、
鍵管理ソフトウェアと鍵データベースA
を用いて、ルートからデータBまでの
ノードの暗号化鍵を順番に復号させる
S202
鍵管理ソフトウェアが、
管理テーブルを更新
S203
暗号化対象のデータが
共有データであるか?
No
Yes
S204
鍵管理ソフトウェアが、
データBの同期処理で利用する鍵を取得
(相手側の鍵取得)
S205
鍵管理ソフトウェアが、
相手側の共有データを更新
S206
自身の更新データBを暗号化する
同期処理の終了

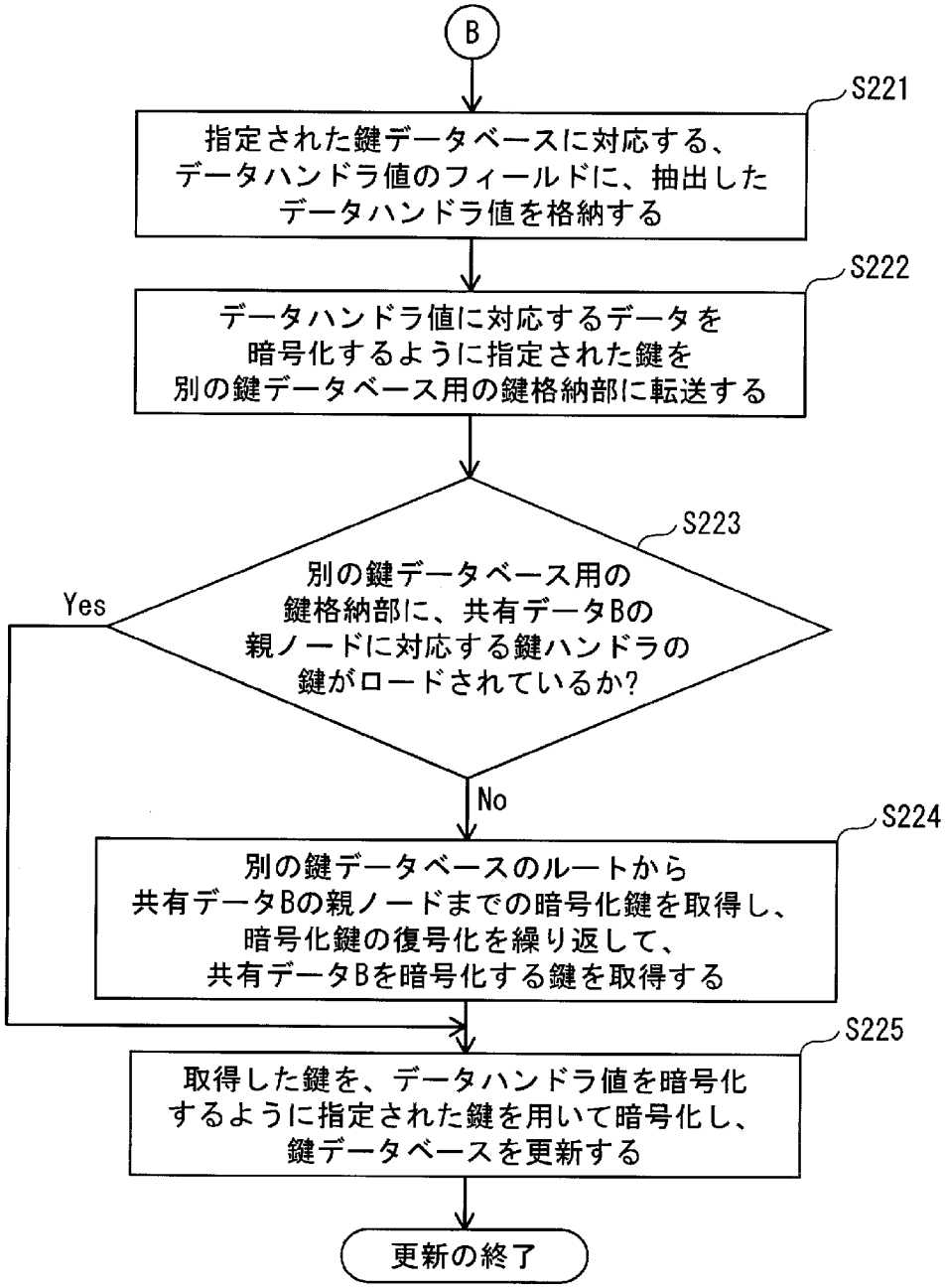
[図10]


管理テーブルの更新の開始
S211
入力されたノード情報構造体は、
鍵データベースA向けか、
鍵データベースB向けか?
鍵データベースA向けの場合
鍵データベースB向けの場合
S212
鍵データベースA向けの
ノード情報構造体から
平文データと
データハンドラ値を抽出する
S213
鍵データベースB向けの
ノード情報構造体から
平文データと
データハンドラ値を抽出する
S214
平文データからハッシュ値を生成する
A

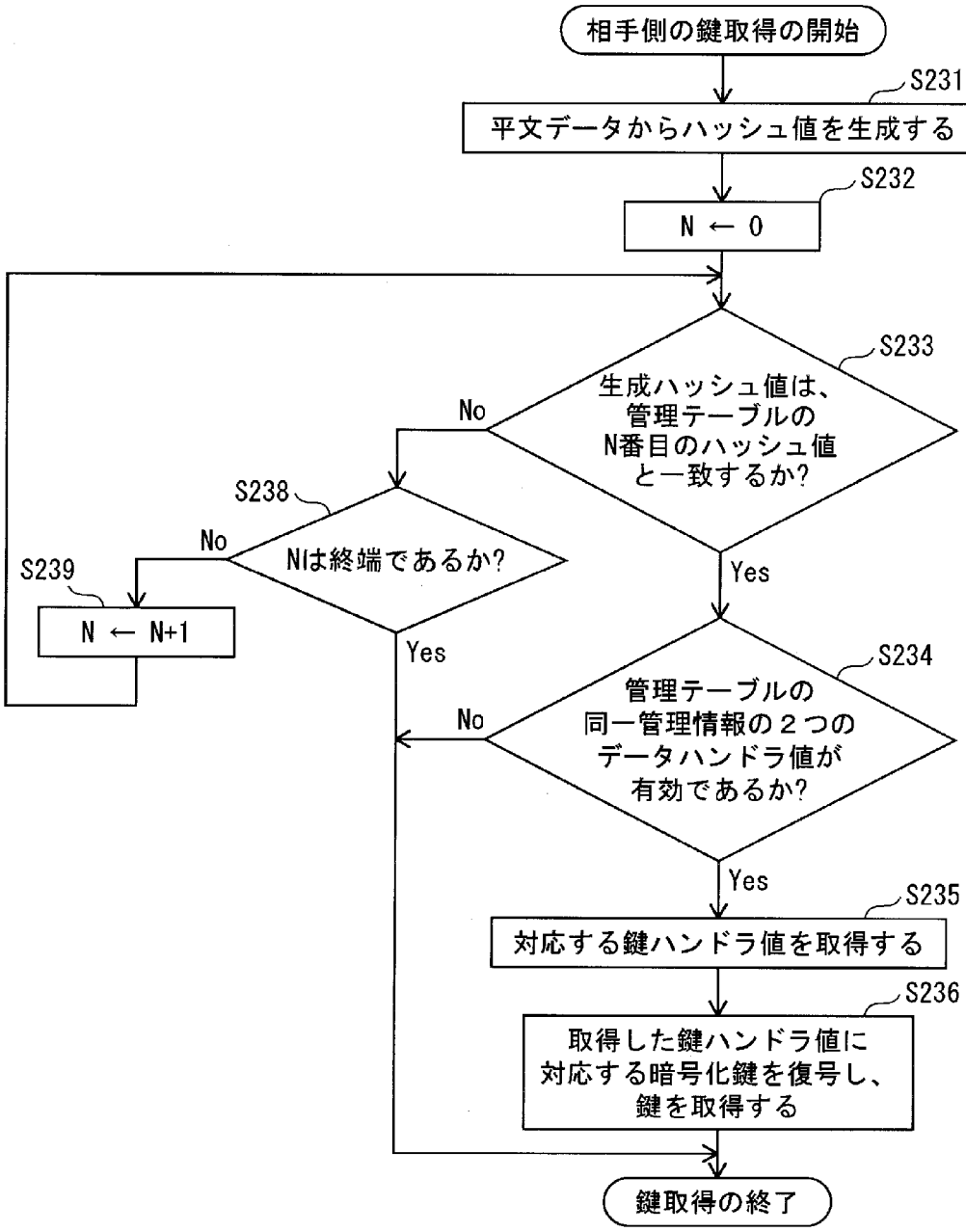
[図11]


A
S215
N ← 0
S216
生成ハッシュ値は、
管理テーブルのN番目の管理情報の
ハッシュ値と一致するか?
Yes
No
S217
管理テーブルの同一管理情報の
異なるデータハンドラ値がNULLか?
Yes
No
B
S218
Nは終端であるか?
Yes
No
S219
管理テーブルを修正
更新の終了
S220
N ← N+1

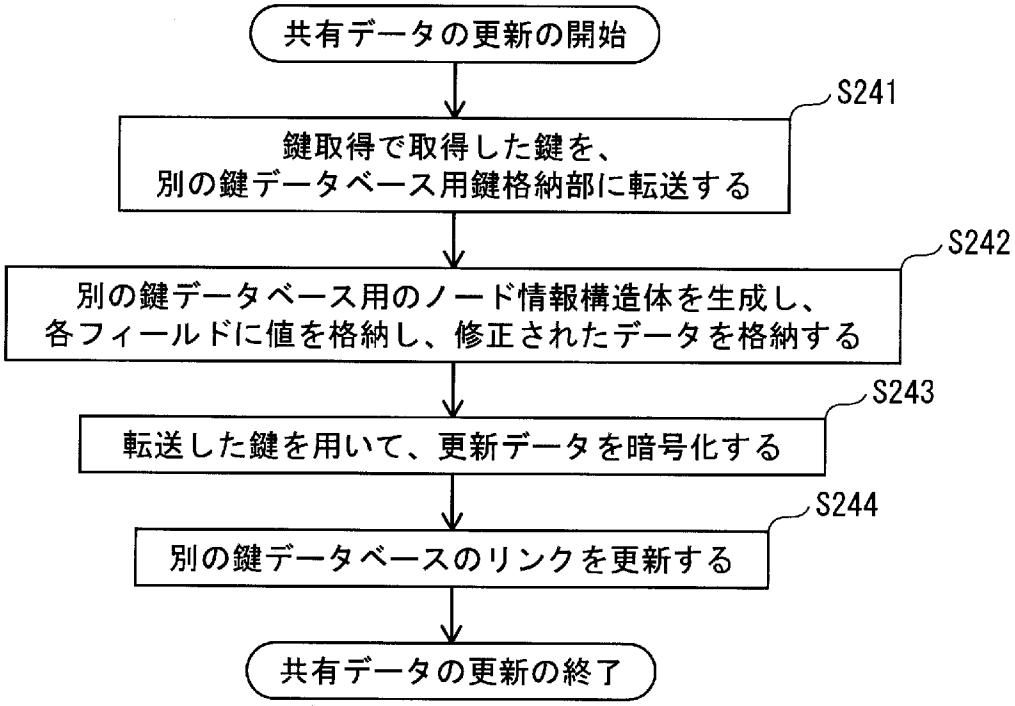
[図12]


B
S221
指定された鍵データベースに対応する、
データハンドラ値のフィールドに、抽出した
データハンドラ値を格納する
S222
データハンドラ値に対応するデータを
暗号化するように指定された鍵を
別の鍵データベース用の鍵格納部に転送する
S223
別の鍵データベース用の
鍵格納部に、共有データBの
親ノードに対応する鍵ハンドラの
鍵がロードされているか?
Yes
No
S224
別の鍵データベースのルートから
共有データBの親ノードまでの暗号化鍵を取得し、
暗号化鍵の復号化を繰り返して、
共有データBを暗号化する鍵を取得する
S225
取得した鍵を、データハンドラ値を暗号化
するように指定された鍵を用いて暗号化し、
鍵データベースを更新する
更新の終了

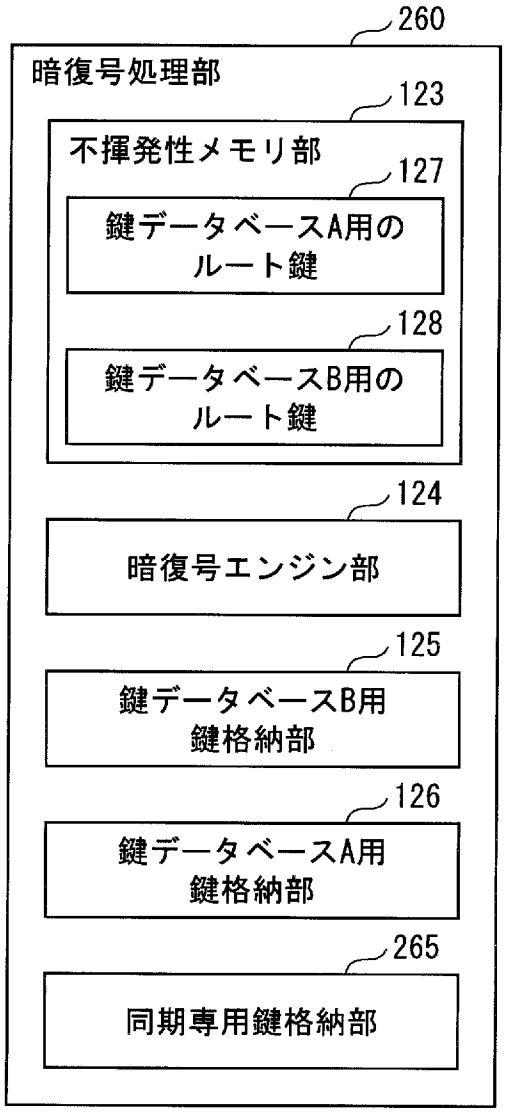
[図13]


相手側の鍵取得の開始
S231
平文データからハッシュ値を生成する
S232
N ← 0
S233
生成ハッシュ値は、
管理テーブルの
N番目のハッシュ値
と一致するか?
No
Yes
S238
Nは終端であるか?
No
Yes
S239
N ← N+1
S234
管理テーブルの
同一管理情報の２つの
データハンドラ値が
有効であるか?
No
Yes
S235
対応する鍵ハンドラ値を取得する
S236
取得した鍵ハンドラ値に
対応する暗号化鍵を復号し、
鍵を取得する
鍵取得の終了

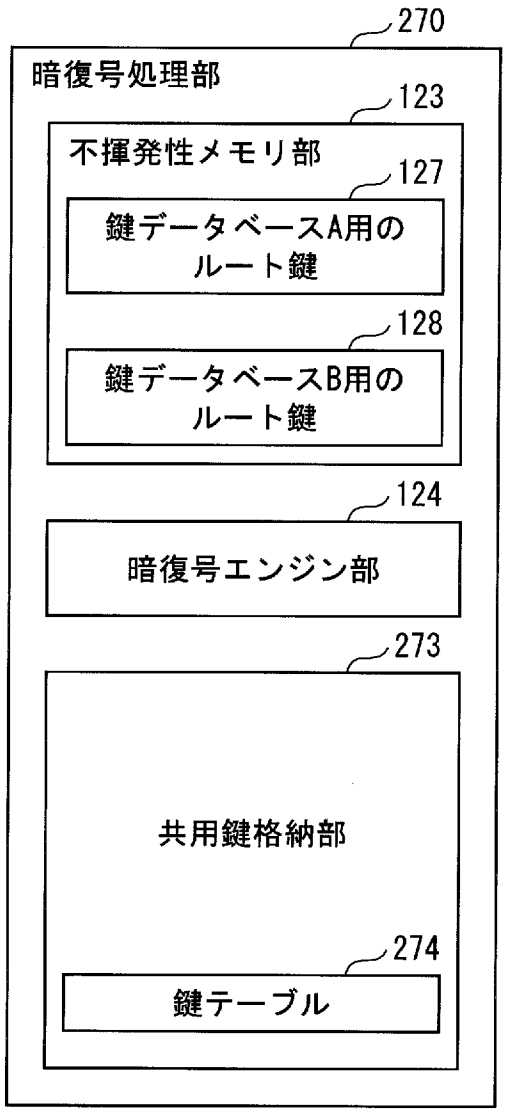
[図14]


共有データの更新の開始
S241
鍵取得で取得した鍵を、
別の鍵データベース用鍵格納部に転送する
S242
別の鍵データベース用のノード情報構造体を生成し、
各フィールドに値を格納し、修正されたデータを格納する
S243
転送した鍵を用いて、更新データを暗号化する
S244
別の鍵データベースのリンクを更新する
共有データの更新の終了

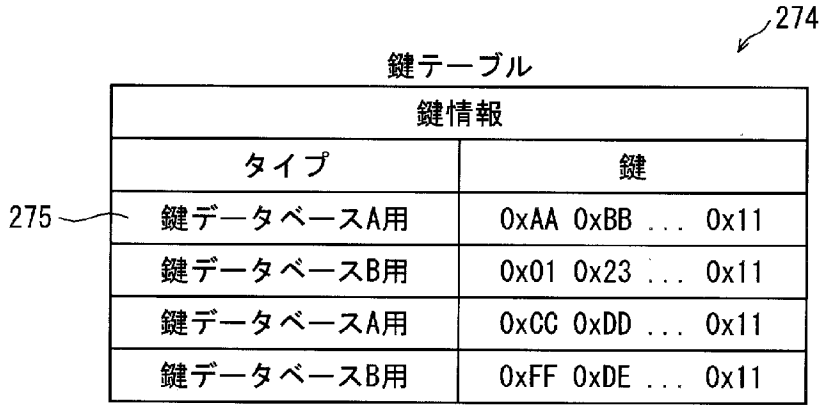
[図15]


260
暗復号処理部
123
不揮発性メモリ部
127
鍵データベースA用の
ルート鍵
128
鍵データベースB用の
ルート鍵
124
暗復号エンジン部
125
鍵データベースB用
鍵格納部
126
鍵データベースA用
鍵格納部
265
同期専用鍵格納部

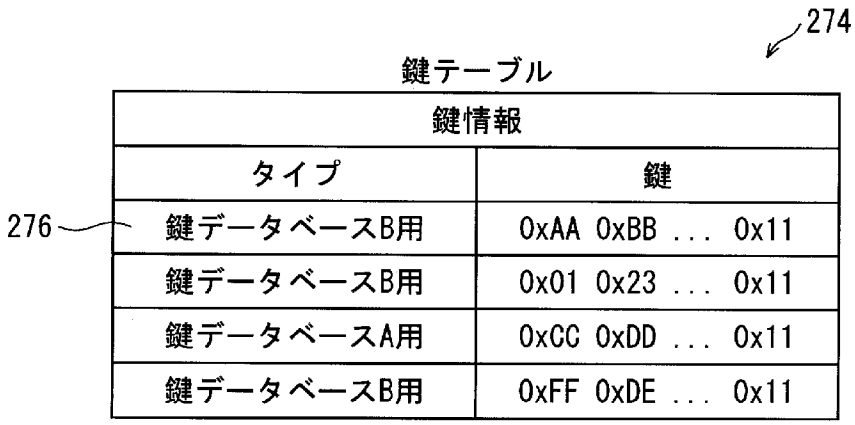
[図16]


270
暗復号処理部
123
不揮発性メモリ部
127
鍵データベースA用の
ルート鍵
128
鍵データベースB用の
ルート鍵
124
暗復号エンジン部
273
共用鍵格納部
274
鍵テーブル

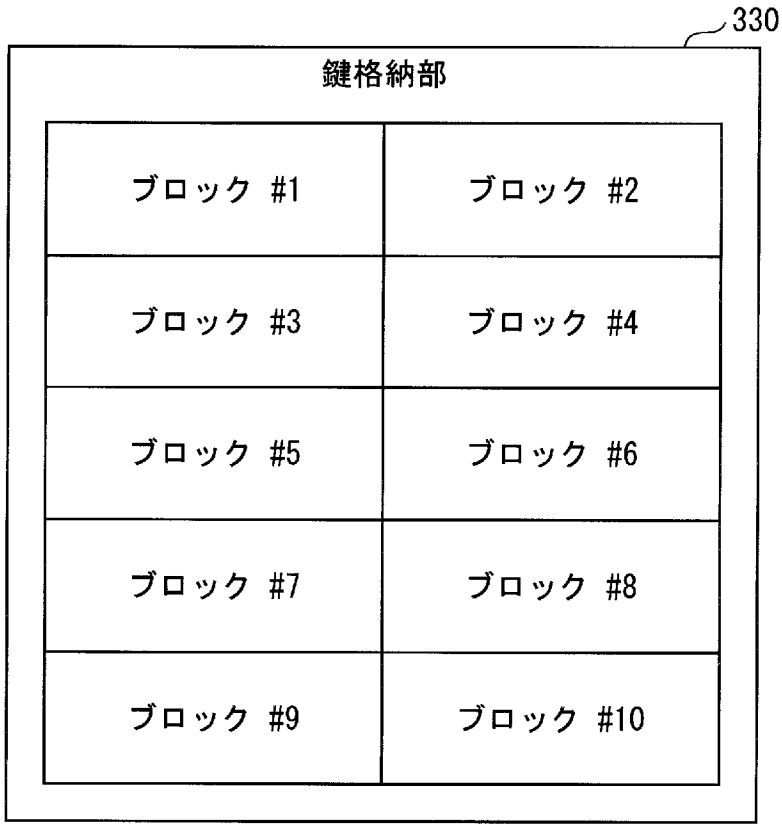
[図17]


274
鍵テーブル
鍵情報
タイプ
鍵
275
鍵データベースA用
0xAA 0xBB ... 0x11
鍵データベースB用
0x01 0x23 ... 0x11
鍵データベースA用
0xCC 0xDD ... 0x11
鍵データベースB用
0xFF 0xDE ... 0x11

[図18]


274
鍵テーブル
鍵情報
タイプ
鍵
276
鍵データベースB用
0xAA 0xBB ... 0x11
鍵データベースB用
0x01 0x23 ... 0x11
鍵データベースA用
0xCC 0xDD ... 0x11
鍵データベースB用
0xFF 0xDE ... 0x11

[図19]

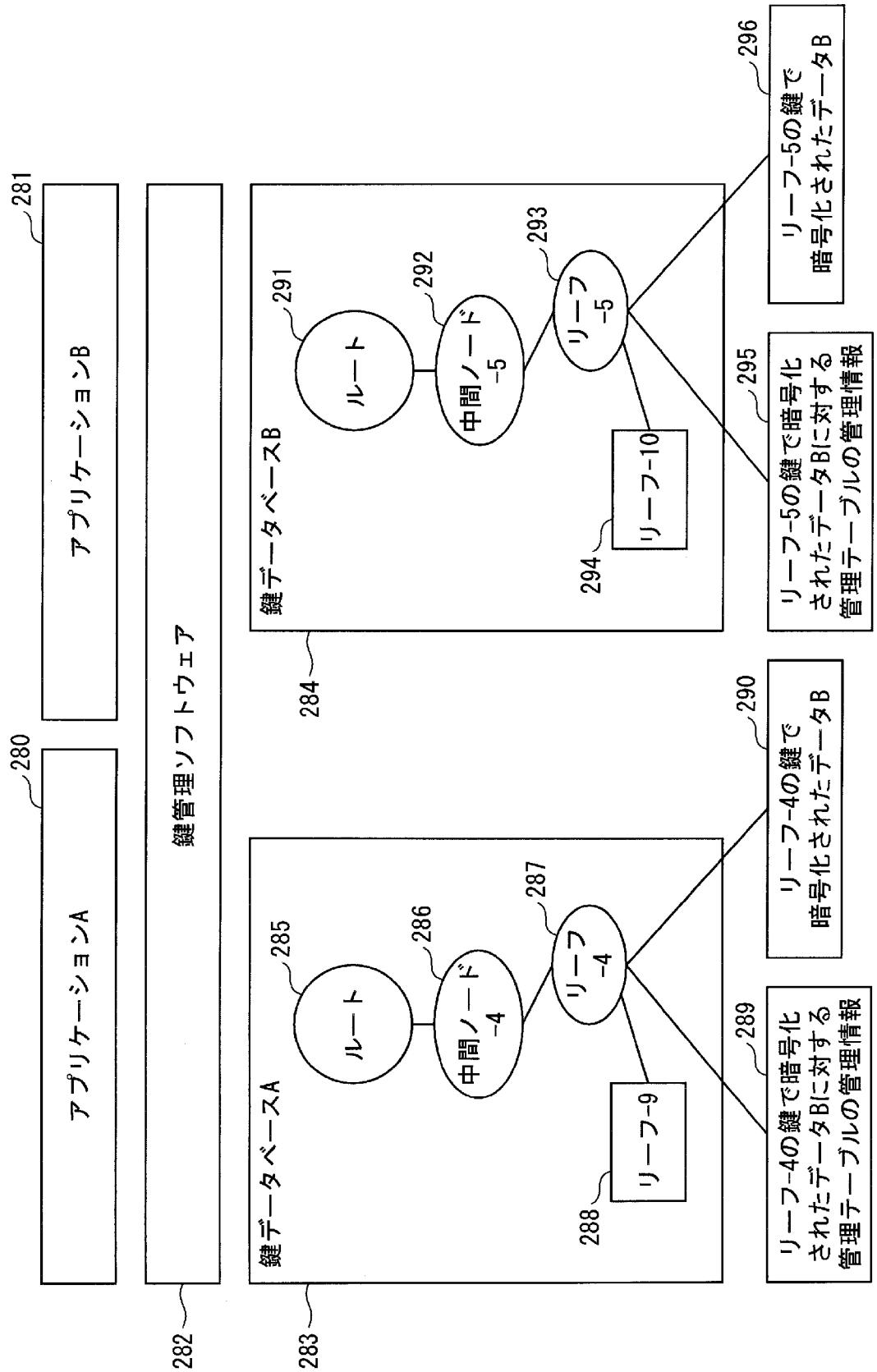


[図20]

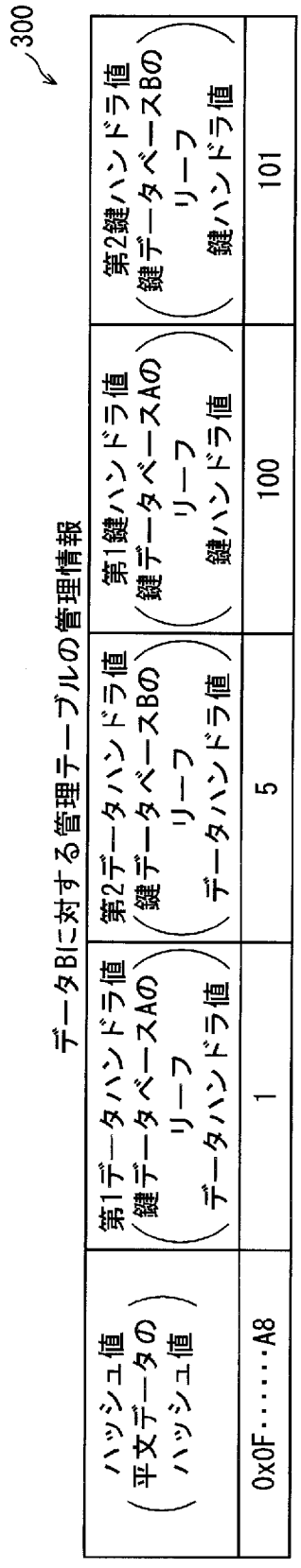
ブロック管理テーブル 331

鍵データベースのタイプ	利用するブロック番号
鍵データベースA用	#1、#2
鍵データベースA用	#3、#4
鍵データベースB用	#5、#6、#7、#8
鍵データベースB用	#9
鍵データベースB用	#10

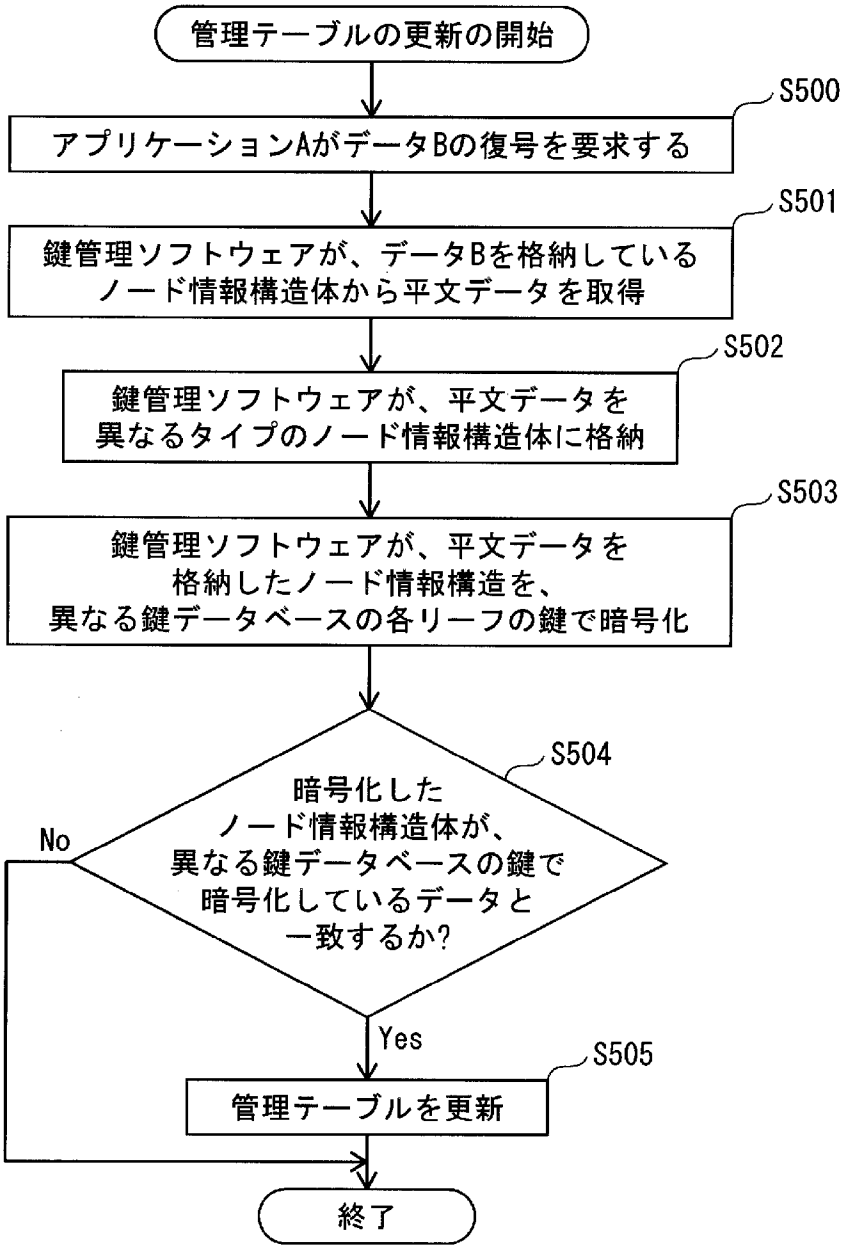
[図21]


281
アプリケーションB
280
アプリケーションA
鍵管理ソフトウェア
282
283
鍵データベースA
285
ルート
286
中間ノード-4
287
リーフ-4
288
リーフ-9
289
リーフ-4の鍵で暗号化されたデータBに対する管理情報
290
リーフ-4の鍵で暗号化されたデータB
284
鍵データベースB
291
ルート
292
中間ノード-5
293
リーフ-5
294
リーフ-10
295
リーフ-5の鍵で暗号化されたデータBに対する管理テーブルの管理情報
296
リーフ-5の鍵で暗号化されたデータB

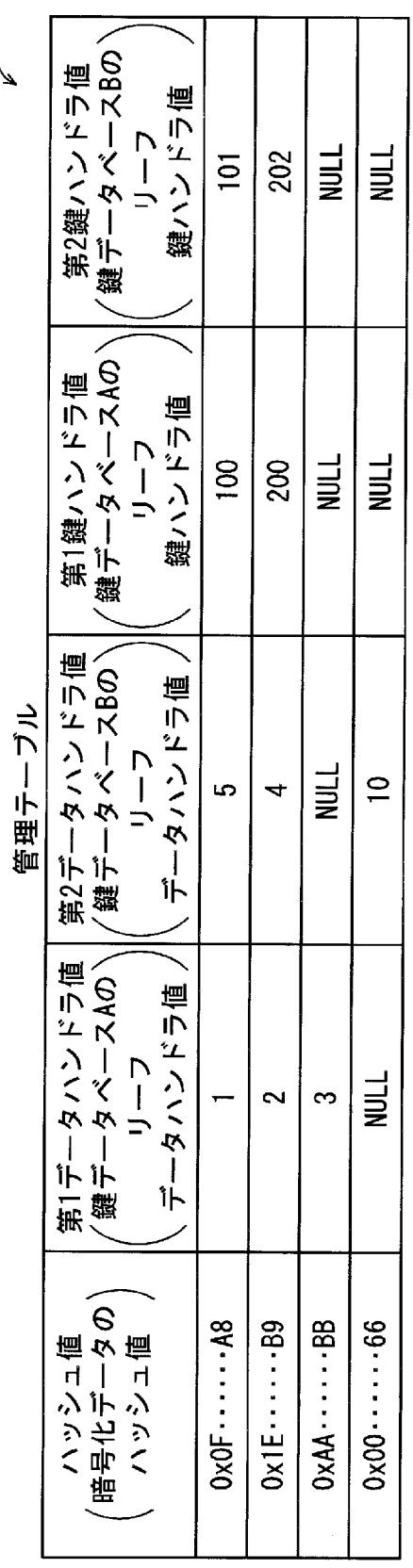
[図22]


300
データBIに対する管理テーブルの管理情報
ハッシュ値
（平文データのハッシュ値）
第1データハンドラ値
（鍵データベースAのリーフデータハンドラ値）
第2データハンドラ値
（鍵データベースBのリーフデータハンドラ値）
第1鍵ハンドラ値
（鍵データベースAのリーフ鍵ハンドラ値）
第2鍵ハンドラ値
（鍵データベースBのリーフ鍵ハンドラ値）
0x0F……A8
1
5
100
101

[図23]

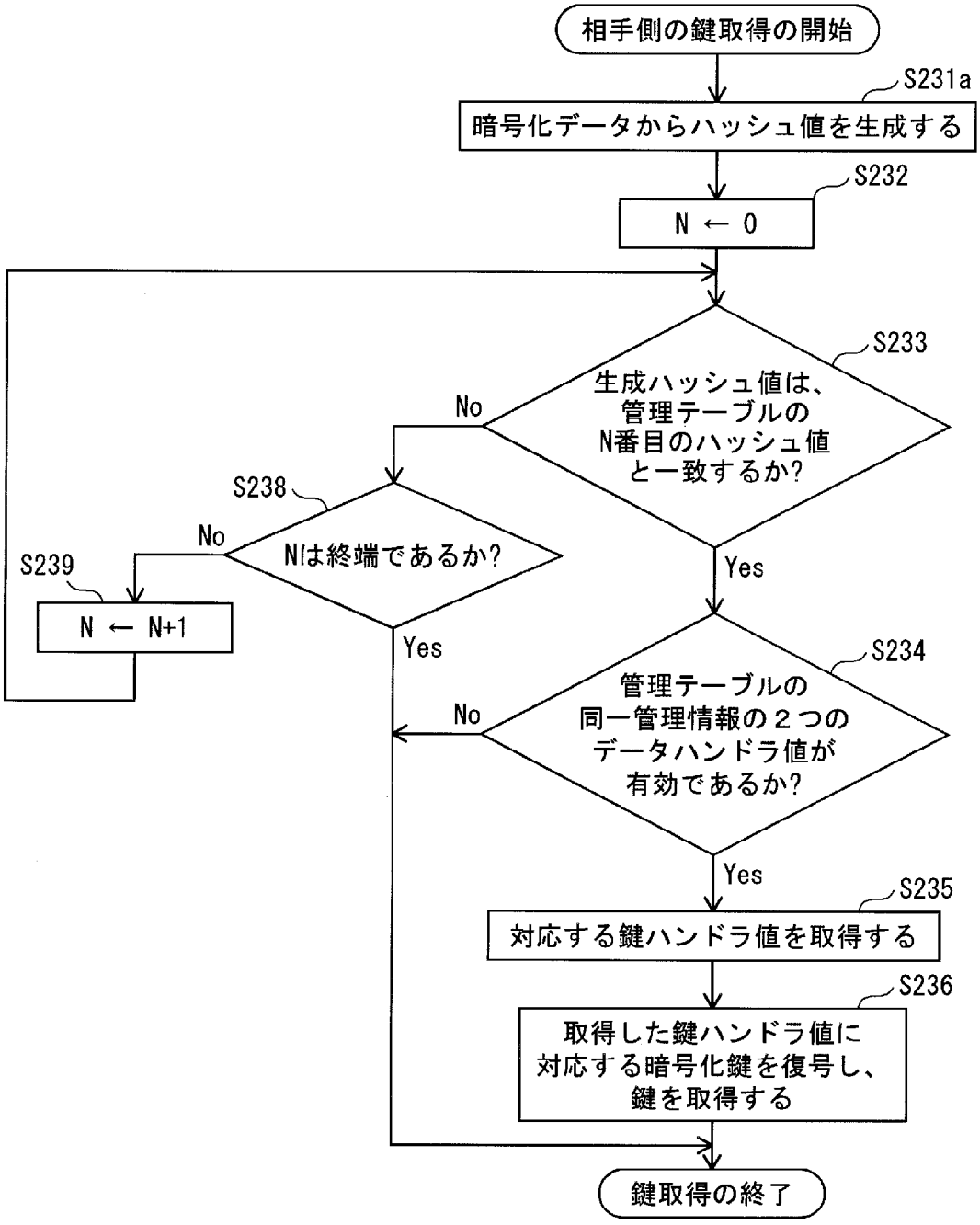

管理テーブルの更新の開始
S500
アプリケーションAがデータBの復号を要求する
S501
鍵管理ソフトウェアが、データBを格納している
ノード情報構造体から平文データを取得
S502
鍵管理ソフトウェアが、平文データを
異なるタイプのノード情報構造体に格納
S503
鍵管理ソフトウェアが、平文データを
格納したノード情報構造を、
異なる鍵データベースの各リーフの鍵で暗号化
S504
暗号化した
ノード情報構造体が、
異なる鍵データベースの鍵で
暗号化しているデータと
一致するか?
No
Yes
S505
管理テーブルを更新
終了

[図24]

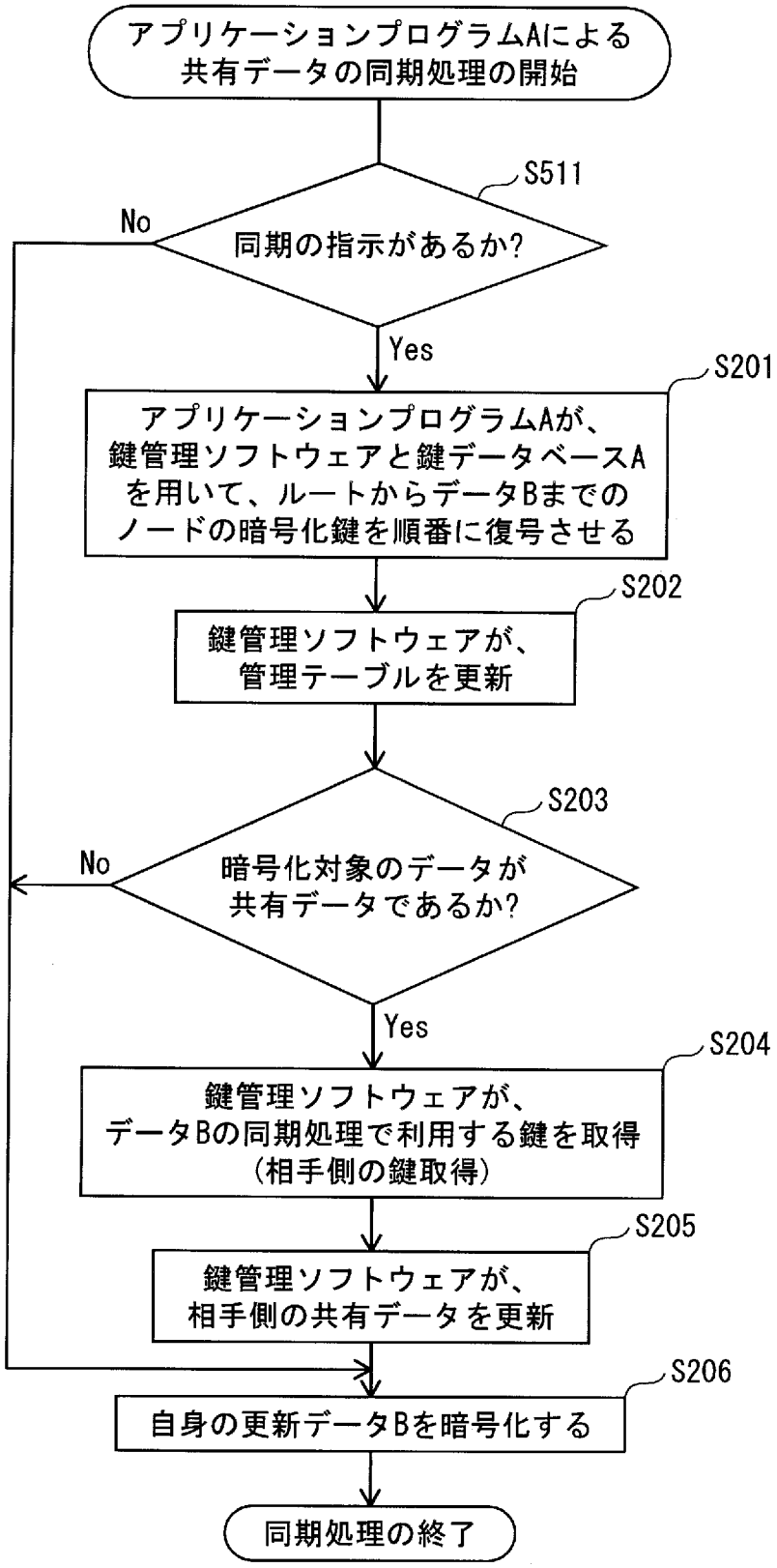


ハッシュ値（暗号化データのハッシュ値）	第1データハンドラ値（鍵データベースAのリーフデータハンドラ値）	第2データハンドラ値（鍵データベースBのリーフデータハンドラ値）	第1鍵ハンドラ値（鍵データベースAのリーフ鍵ハンドラ値）	第2鍵ハンドラ値（鍵データベースBのリーフ鍵ハンドラ値）
0x0F……A8	1	5	100	101
0x1E……B9	2	4	200	202
0xAA……BB	3	NULL	NULL	NULL
0x00……66	NULL	10	NULL	NULL

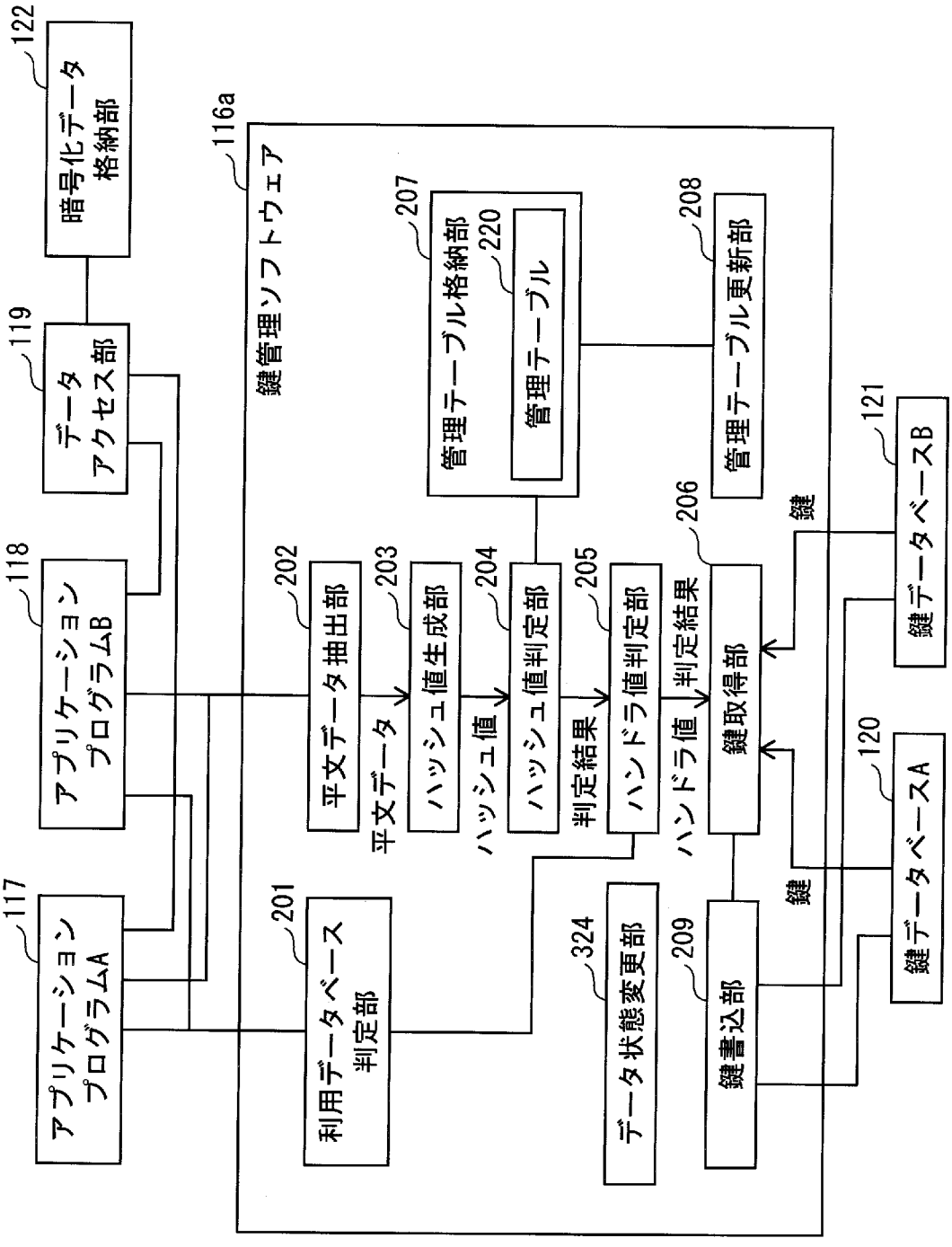
[図25]


相手側の鍵取得の開始
S231a
暗号化データからハッシュ値を生成する
S232
N ← 0
S233
生成ハッシュ値は、
管理テーブルの
N番目のハッシュ値
と一致するか?
No
Yes
S238
Nは終端であるか?
No
Yes
S239
N ← N+1
S234
管理テーブルの
同一管理情報の２つの
データハンドラ値が
有効であるか?
No
Yes
S235
対応する鍵ハンドラ値を取得する
S236
取得した鍵ハンドラ値に
対応する暗号化鍵を復号し、
鍵を取得する
鍵取得の終了

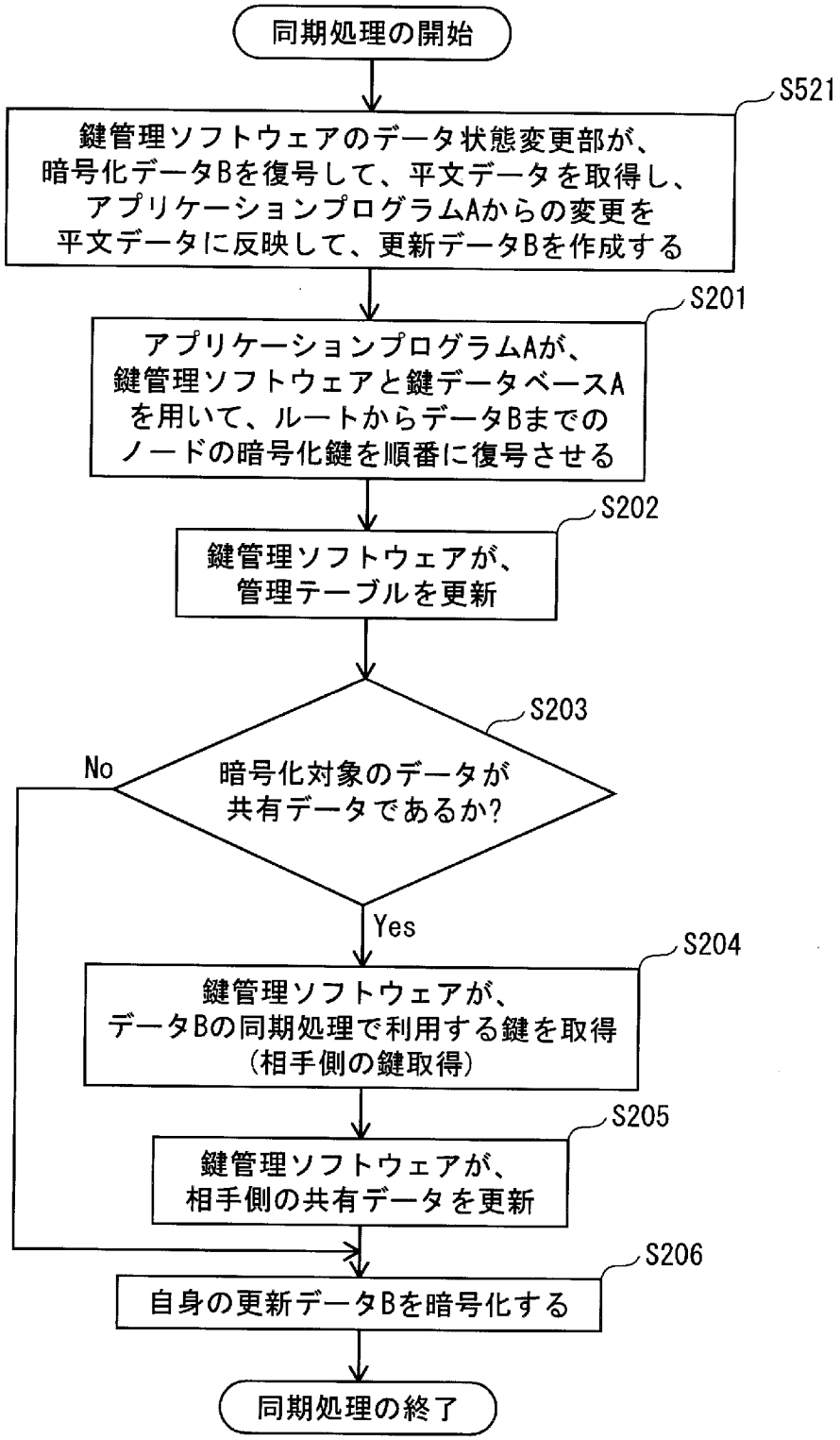
[図26]


アプリケーションプログラムAによる
共有データの同期処理の開始
S511
同期の指示があるか?
No
Yes
S201
アプリケーションプログラムAが、
鍵管理ソフトウェアと鍵データベースA
を用いて、ルートからデータBまでの
ノードの暗号化鍵を順番に復号させる
S202
鍵管理ソフトウェアが、
管理テーブルを更新
S203
暗号化対象のデータが
共有データであるか?
No
Yes
S204
鍵管理ソフトウェアが、
データBの同期処理で利用する鍵を取得
(相手側の鍵取得)
S205
鍵管理ソフトウェアが、
相手側の共有データを更新
S206
自身の更新データBを暗号化する
同期処理の終了

[図27]


122
暗号化データ格納部
116a
鍵管理ソフトウェア
119
データアクセス部
118
アプリケーションプログラムB
117
アプリケーションプログラムA
202
平文データ抽出部
203
ハッシュ値生成部
204
ハッシュ値判定部
205
ハンドラ値判定部
206
鍵取得部
207
管理テーブル格納部
220
管理テーブル
208
管理テーブル更新部
201
利用データベース判定部
324
データ状態変更部
209
鍵書込部
121
鍵データベースB
120
鍵データベースA
平文データ
ハッシュ値
判定結果
ハンドラ値
判定結果
鍵
鍵

[図28]


同期処理の開始
S521
鍵管理ソフトウェアのデータ状態変更部が、
暗号化データBを復号して、平文データを取得し、
アプリケーションプログラムAからの変更を
平文データに反映して、更新データBを作成する
S201
アプリケーションプログラムAが、
鍵管理ソフトウェアと鍵データベースA
を用いて、ルートからデータBまでの
ノードの暗号化鍵を順番に復号させる
S202
鍵管理ソフトウェアが、
管理テーブルを更新
S203
暗号化対象のデータが
共有データであるか?
No
Yes
S204
鍵管理ソフトウェアが、
データBの同期処理で利用する鍵を取得
(相手側の鍵取得)
S205
鍵管理ソフトウェアが、
相手側の共有データを更新
S206
自身の更新データBを暗号化する
同期処理の終了

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2009/005217

A. CLASSIFICATION OF SUBJECT MATTER
H04L9/08(2006.01)i, *G06F12/00*(2006.01)i, *G09C1/00*(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, G06F12/00, G09C1/00, 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	1996-2010
Kokai Jitsuyo Shinan Koho	1971-2010	Toroku Jitsuyo Shinan Koho	1994-2010

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 2000-98885 A (Sony Corp.), 07 April 2000 (07.04.2000), entire text; all drawings & US 7506367 B1	1-26
A	JP 2000-305853 A (Victor Company Of Japan, Ltd.), 02 November 2000 (02.11.2000), entire text; all drawings & US 6745166 B1 & EP 1047062 A2 & CN 1271907 A	1-26

☒ 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
05 January, 2010 (05.01.10)	19 January, 2010 (19.01.10)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2009/005217

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2006-155606 A (Microsoft Corp.), 15 June 2006 (15.06.2006), paragraphs [0044] to [0047] & US 2006/0117018 A1 & EP 1662408 A1 & CA 2524421 A & KR 10-2006-0060549 A & CN 1783081 A & BRA PI0505047 & ZA 200508765 A	1-26
A	JP 2006-227839 A (Hitachi, Ltd.), 31 August 2006 (31.08.2006), entire text; all drawings & US 2006/0182281 A1	1-26

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２００９／００５２１７

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, G06F12/00(2006.01)i, G09C1/00(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, G06F12/00, G09C1/00, 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	１９７１－２０１０年
日本国実用新案登録公報	１９９６－２０１０年
日本国登録実用新案公報	１９９４－２０１０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 2000-98885 A (ソニー株式会社) 2000.04.07, 全文, 全図 & US 7506367 B1	１－２６
A	JP 2000-305853 A (日本ビクター株式会社) 2000.11.02, 全文, 全図 & US 6745166 B1 & EP 1047062 A2 & CN 1271907 A	１－２６

☑　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 ０５．０１．２０１０	国際調査報告の発送日 １９．０１．２０１０
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　４２２９ 青木　重徳 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	JP 2006-155606 A (マイクロソフト　コーポレーション) 2006.06.15, 段落【００４４】－【００４７】 & US 2006/0117018 A1 & EP 1662408 A1 & CA 2524421 A & KR 10-2006-0060549 A & CN 1783081 A & BRA PI0505047 & ZA 200508765 A	１－２６
Ａ	JP 2006-227839 A (株式会社日立製作所) 2006.08.31, 全文, 全図 & US 2006/0182281 A1	１－２６