(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
2024年7月4日(04.07.2024)

WIPO | PCT

(10) 国際公開番号
WO 2024/142555 A1

(51) 国際特許分類:
G06F 21/60 (2013.01) *G06F 21/78* (2013.01)

(21) 国際出願番号： PCT/JP2023/037435

(22) 国際出願日： 2023年10月16日(16.10.2023)

(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 2022-208965 2022年12月26日(26.12.2022) JP
特願 2023-100945 2023年6月20日(20.06.2023) JP

(71) 出願人：パナソニックＩＰマネジメント株式会社(**PANASONIC INTELLECTUAL PROPERTY MANAGEMENT CO., LTD.**) [JP/JP]；〒5710057 大阪府門真市元町２２番６号 Osaka (JP).

(72) 発明者：高橋 克直(**TAKAHASHI, Katsunao**). 北御門 昌紀(**KITAMIKADO, Masanori**).

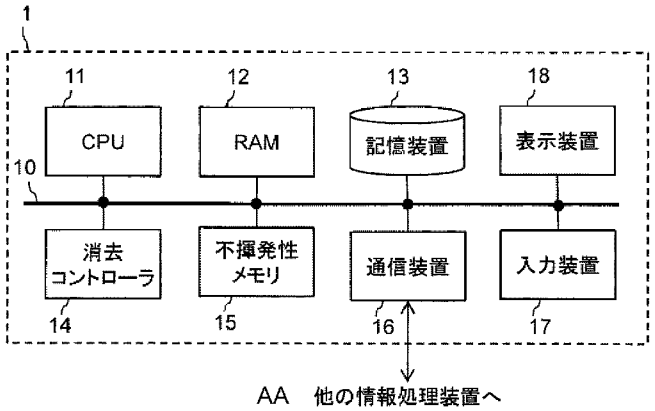
(74) 代理人：山尾 憲人，外(**YAMAO, Norihito** et al.)；〒5300017 大阪府大阪市北区角田町８番１号 大阪梅田ツインタワーズ・ノース 青山特許事務所 Osaka (JP).

(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, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, MG, MK, MN, MU, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, 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, CV, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SC, SD, SL, ST, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, RU, TJ, TM), ヨーロッパ (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS,

(54) **Title:** INFORMATION PROCESSING APPARATUS

(54) 発明の名称： 情報処理装置



13 Storage device
14 Deletion controller
15 Nonvolatile memory
16 Communication device
17 Input device
18 Display device
AA To other information processing apparatus

(57) **Abstract:** In the present invention, a deletion controller (14) acquires a first hash value obtained by calculating on the basis of data to be stored or having been stored in a designated position in a storage region. The deletion controller (14) controls a storage device (13) to change a first encryption key stored in a nonvolatile memory (23) into a second encryption key. The deletion controller (14) calculates a second hash value on the basis of data read out from the designated position in the storage region. The deletion controller (14) outputs, when the second hash value is different from the first hash value, a verification result indicating that deletion of the data stored in the storage device (13) has succeeded. The deletion controller (14) outputs, when the second hash value coincides with the first hash value, a verification result indicating that the deletion of the data stored in the storage device (13) has failed.

WO 2024/142555 A1

［続葉有］

IT, LT, LU, LV, MC, ME, 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：

一　国際調査報告（条約第21条(3)）

(57) 要約：消去コントローラ（１４）は、記憶領域の指定された位置に格納されるべき又は格納されたデータに基づいて計算された第１のハッシュ値を取得する。消去コントローラ（１４）は、不揮発性メモリ（２３）に格納された第１の暗号鍵を第２の暗号鍵に変更するように記憶装置（１３）を制御する。消去コントローラ（１４）は、記憶領域の指定された位置から読み出されたデータに基づいて第２のハッシュ値を計算する。消去コントローラ（１４）は、第２のハッシュ値が第１のハッシュ値とは異なる場合、記憶装置（１３）に格納されたデータの消去に成功したことを示す検証結果を出力する。消去コントローラ（１４）は、第２のハッシュ値が第１のハッシュ値に一致する場合、記憶装置（１３）に格納されたデータの消去に失敗したことを示す検証結果を出力する。

明　細　書

発明の名称 ： 情報処理装置

技術分野

[0001]　本開示は、情報処理装置、情報処理方法、情報処理システム、及びプログラムに関する。

背景技術

[0002]　パーソナルコンピュータなどの情報処理装置を廃棄する場合、機密データの漏洩を防ぐために、記憶装置に格納されたデータを消去し（又は等価的に、データにアクセス不能にし）、データが確実に消去されたことを検証することが求められる。例えば、特許文献１及び非特許文献１は、データ消去を検証する方法を開示している。

先行技術文献

特許文献

[0003] 特許文献1：特許第７０９６８２９号公報

非特許文献

[0004] 非特許文献1：Richard Kissel et al., ”Guidelines for Media Sanitization”, NIST Special Publication 800-88, Revision 1, National Institute of Standards and Technology, December 2014［令和４年１２月１日検索］, インターネット＜ＵＲＬ：http://dx.doi.org/10.6028/NIST.SP.800-88r1＞

発明の概要

発明が解決しようとする課題

[0005]　従来、データの消去に成功したか否かを検証するためには、消去後に記憶装置に格納されている現在のデータ（例えば、元データに上書きされたパターンデータ又はランダムデータ）が、消去前に記憶装置に格納されていた元データと比較される。この場合、大量のデータを比較するために、情報処理装置に大きな負荷がかかる。従って、データの消去に成功したか否かを従来よりも小さな負荷で検証することが求められる。

[0006] 本開示は、記憶装置に格納されたデータの消去に成功したか否かを従来よりも小さな負荷で検証することができる情報処理装置、情報処理方法、情報処理システム、及びプログラムを提供する。

課題を解決するための手段

[0007] 本開示の一態様に係る情報処理装置は、

格納されるデータの自己暗号化機能を有する記憶装置と、

前記記憶装置に格納されたデータの消去を制御する消去コントローラとを備え、

前記記憶装置は、

記憶領域を有する記憶媒体と、

暗号鍵を格納した不揮発性メモリと、

入力されたデータを前記記憶領域に書き込み、前記記憶領域から読み出されたデータを出力し、前記記憶領域に書き込まれるデータの少なくとも一部を前記暗号鍵を用いて暗号化し、前記記憶領域から読み出されたデータの少なくとも一部を前記暗号鍵を用いて復号する入出力コントローラとを備え、

前記消去コントローラは、

前記不揮発性メモリに第１の暗号鍵が格納されている場合、前記記憶領域の指定された位置に格納されるべきデータに基づいて、又は、前記記憶領域の指定された位置に格納されているデータに基づいて計算された第１のハッシュ値を取得し、

前記不揮発性メモリに格納された前記第１の暗号鍵を第２の暗号鍵に変更するように前記記憶装置を制御し、

前記不揮発性メモリに前記第２の暗号鍵が格納されている場合、前記記憶領域の前記指定された位置から読み出されたデータに基づいて第２のハッシュ値を計算し、

前記第２のハッシュ値が前記第１のハッシュ値とは異なる場合、前記記憶装置に格納されたデータの消去に成功したことを示す検証結果を出力し、

前記第２のハッシュ値が前記第１のハッシュ値に一致する場合、前記記憶

装置に格納されたデータの消去に失敗したことを示す検証結果を出力する。

発明の効果

[0008] 本開示の一態様に係る情報処理装置によれば、記憶装置に格納されたデータの消去に成功したか否かを従来よりも小さな負荷で検証することができる。

図面の簡単な説明

[0009] [図1]第１の実施形態に係る情報処理装置１の構成を示すブロック図である。

[図2]図１の記憶装置１３の構成を示すブロック図である。

[図3]図２のフラッシュメモリ２４の論理ブロック３１を示す概略図であって、データの消去を検証するために比較される論理ブロック３１の配置の一例を示す図である。

[図4]比較例１に係る消去処理を示すフローチャートである。

[図5]比較例２に係る消去処理を示すフローチャートである。

[図6]図１の消去コントローラ１４によって実行される実施例１に係る消去処理を示すフローチャートである。

[図7]比較例１、比較例２、及び実施例１に係る検証方法を比較する表である。

[図8]図２のフラッシュメモリ２４の論理ブロック３１を示す概略図であって、データの消去を検証するために比較される論理ブロック３１の配置の第１の変形例を示す図である。

[図9]図２のフラッシュメモリ２４の論理ブロック３１を示す概略図であって、データの消去を検証するために比較される論理ブロック３１の配置の第２の変形例を示す図である。

[図10]図１の消去コントローラ１４によって実行される実施例２に係る消去処理を示すフローチャートである。

[図11]図１の消去コントローラ１４によって実行される実施例３に係る消去処理を示すフローチャートである。

[図12]図２のフラッシュメモリ２４の論理ブロック３１を示す概略図であっ

て、データの消去を検証するためにすべての論理ブロック３１が比較される場合を示す図である。

[図13]図２のフラッシュメモリ２４の論理ブロック３１を示す概略図であって、データの消去を検証するために部分領域２４ｂ－１，２４ｂ－２のそれぞれに含まれる論理ブロック３１が比較される場合を示す図である。

[図14]図２のフラッシュメモリ２４の論理ブロック３１を示す概略図であって、データの消去を検証するために部分領域２４ｃ－１～２４ｃ－４のそれぞれに含まれる論理ブロック３１が比較される場合を示す図である。

[図15]図２のフラッシュメモリ２４の論理ブロック３１を示す概略図であって、データの消去を検証するために部分領域２４ｄ－１～２４ｄ－８のそれぞれに含まれる論理ブロック３１が比較される場合を示す図である。

[図16]第１の実施形態の変形例に係る情報処理装置１Ａの構成を示すブロック図である。

[図17]第２の実施形態に係る情報処理装置１によって実行される消去処理を示すフローチャートである。

[図18]図１７の前処理（ステップＳ１０１）のサブルーチンを示すフローチャートである。

[図19]図１７の鍵変更処理（ステップＳ１０２）のサブルーチンを示すフローチャートである。

[図20]図１７の検証処理（ステップＳ１０３）のサブルーチンを示すフローチャートである。

[図21]図１７の消去処理を実行することによって図１の表示装置１８に表示される、データ消去の進捗度を示す画像の一例を示す図である。

[図22]図１７の消去処理を実行することによって図１の表示装置１８に表示される、データ消去の進捗度を示す画像の他の一例を示す図である。

[図23]図１７の検証処理の第１の変形例を示すフローチャートである。

[図24]図１７の検証処理の第２の変形例を示すフローチャートである。

[図25]図１７の検証処理の第３の変形例を示すフローチャートである。

[図26]第３の実施形態に係る情報処理装置１及びサーバ装置を含む情報処理システムの構成を示すブロック図である。

[図27]図２６のサーバ装置２の構成を示すブロック図である。

[図28]図２６のサーバ装置２によって実行される消去処理を示すフローチャートである。

[図29]図２６の情報処理装置１によって実行される消去処理を示すフローチャートである。

[図30]図２６のサーバ装置２によって実行される消去処理の変形例を示すフローチャートである。

[図31]図２６の情報処理装置１によって実行される消去処理の変形例を示すフローチャートである。

[図32]図３１の前処理（ステップＳ２３１）のサブルーチンを示すフローチャートである。

[図33]図３１の鍵変更処理（ステップＳ２３２）のサブルーチンを示すフローチャートである。

[図34]図３１の検証処理（ステップＳ２３３）のサブルーチン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

[0010] 以下、適宜図面を参照しながら、実施形態を詳細に説明する。但し、必要以上に詳細な説明は省略する場合がある。例えば、既によく知られた事項の詳細説明や実質的に同一の構成に対する重複説明を省略する場合がある。これは、以下の説明が不必要に冗長になるのを避け、当業者の理解を容易にするためである。

[0011] なお、発明者（ら）は、当業者が本開示を十分に理解するために添付図面および以下の説明を提供するのであって、これらによって特許請求の範囲に記載の主題を限定することを意図するものではない。

[0012] ［第１の実施形態］

［第１の実施形態の構成］

図１は、第１の実施形態に係る情報処理装置１の構成を示すブロック図である。情報処理装置１は、バス１０、中央処理装置（ＣＰＵ）１１、ランダムアクセスメモリ（ＲＡＭ）１２、記憶装置１３、消去コントローラ１４、不揮発性メモリ１５、通信装置１６、入力装置１７、及び表示装置１８を備える。

[0013] ＣＰＵ１１は、情報処理装置１全体の動作を制御する。

[0014] ＲＡＭ１２は、情報処理装置１の動作に必要なプログラム及びデータを一時的に記憶する。

[0015] 記憶装置１３は、オペレーティングシステム、アプリケーションプログラム、及びユーザデータを含むデータを格納する。記憶装置１３は、格納されるデータの自己暗号化機能を有する自己暗号化ドライブ（Self-Encrypting Drive：ＳＥＤ）であり、例えば、自己暗号化機能を有するソリッドステートドライブ（ＳＳＤ）である。

[0016] 消去コントローラ１４は、図６等を参照して後述する消去処理を実行することで、記憶装置１３に格納されたデータの消去を制御する。本開示では、「消去」とは、記憶装置１３に格納された少なくとも一部のデータにアクセス不能にすることを意味する。消去コントローラ１４は、例えば、マイクロプロセッサを含む。

[0017] 不揮発性メモリ１５は、消去処理の実行に必要なプログラム及びデータを格納する。不揮発性メモリ１５は、例えば、フラッシュメモリなどの不揮発性記憶媒体を含む。

[0018] 消去処理のためのプログラムは、ＵＥＦＩ（Unified Extensible Firmware Interface）又はＢＩＯＳ（Basic Input/Output System）プログラムのような情報処理装置１のファームウェアプログラムに組み込まれてもよい。この場合、消去処理のためのプログラムは、ＵＥＦＩ又はＢＩＯＳプログラムと同じ記憶媒体に格納されてもよく、ＵＥＦＩ又はＢＩＯＳプログラムと同じマイクロプロセッサによって実行されてもよい。

[0019] 通信装置１６は、ローカルエリアネットワーク（ＬＡＮ）などの通信回線

を介して、外部の他の情報処理装置と通信可能に接続される。

[0020] 入力装置１７は、情報処理装置１の動作を制御するユーザ入力を受ける。入力装置１７は、例えば、キーボード及びポインティングデバイスを含む。

[0021] 表示装置１８は、情報処理装置１の状態に関連する情報、例えば、記憶装置１３に格納されたデータの消去に関連する情報を表示する。

[0022] ＣＰＵ１１、ＲＡＭ１２、記憶装置１３、消去コントローラ１４、不揮発性メモリ１５、通信装置１６、入力装置１７、及び表示装置１８は、バス１０を介して互いに接続される。

[0023] 情報処理装置１は、例えば、パーソナルコンピュータである。

[0024] 図２は、図１の記憶装置１３の構成を示すブロック図である。記憶装置１３は、入出力コントローラ２１、ランダムアクセスメモリ（ＲＡＭ）２２、不揮発性メモリ２３、及びフラッシュメモリ２４を備える。入出力コントローラ２１は、記憶装置１３に対するデータの書き込み及び読み出しを制御する。ＲＡＭ２２は、記憶装置１３に対して書き込まれるデータ及び読み出されるデータを一時的に格納するバッファメモリである。不揮発性メモリ２３は、記憶装置１３のファームウェアプログラム（ＦＷ）と、暗号鍵とを格納する。フラッシュメモリ２４は、記憶領域を有する不揮発性の記憶媒体である。入出力コントローラ２１は、不揮発性メモリ２３に格納されたファームウェアプログラムを実行することで、記憶装置１３の動作を制御する。入出力コントローラ２１は、入力されたデータをフラッシュメモリ２４の記憶領域に書き込み、記憶領域から読み出されたデータを出力する。

[0025] 前述したように、記憶装置１３は自己暗号化機能を有する。記憶装置１３は、フラッシュメモリ２４の記憶領域全体に格納されるデータを暗号化及び復号してもよく、記憶領域の一部に格納されるデータのみを暗号化及び復号してもよい。入出力コントローラ２１は、フラッシュメモリ２４の記憶領域に書き込まれるデータの少なくとも一部を不揮発性メモリ２３に格納された暗号鍵を用いて暗号化する。また、入出力コントローラ２１は、フラッシュメモリ２４の記憶領域から読み出されたデータの少なくとも一部を暗号鍵を

用いて復号する。入出力コントローラ２１は、データの暗号化及び復号のために、ハードウェア、ソフトウェア、又はそれらの組み合わせを用いてもよい。

[0026] このような記憶装置１３を備えたことにより、情報処理装置１は、オペレーティングシステム及びアプリケーションプログラムによらずに、記憶装置１３に格納されるデータを暗号化及び復号することができる。

[0027] 自己暗号化機能を有する記憶装置１３では、暗号鍵を変更すると、変更前の暗号鍵によって暗号化されてフラッシュメモリ２４の記憶領域に格納されたデータは、変更後の暗号鍵を用いて復号できなくなる。従って、記憶装置１３の暗号鍵を変更することにより、記憶装置１３に格納された元データにアクセス不能になり、等価的に、記憶装置１３に格納された元データを消去（暗号的消去）することができる。入出力コントローラ２１は、消去コントローラ１４の制御下で、不揮発性メモリ２３に格納された暗号鍵を変更する。暗号鍵は、例えば、入出力コントローラ２１が記憶装置１３のファームウェアに含まれるｒｅｖｅｒｔコマンドを実行することにより変更されてもよい。

[0028] 前述したように、記憶領域の一部の領域に格納されるデータのみを暗号化及び復号する場合、暗号化及び復号されないデータは、暗号鍵を変更してもアクセス不能にならず、従って、消去されない。データの消去に成功したか否かを検証するためには、消去コントローラ１４は、暗号鍵の変更後に記憶装置１３に格納されている現在のデータを、暗号鍵の変更前に記憶装置１３に格納されていた元データと比較する。現在のデータが元データと異なる場合、消去コントローラ１４はデータの消去に成功したと判断し、現在のデータが元データに一致する場合、消去コントローラ１４はデータの消去に失敗したと判断する。

[0029] 図３は、図２のフラッシュメモリ２４の論理ブロック３１を示す概略図であって、データの消去を検証するために比較される論理ブロック３１の配置の一例を示す図である。フラッシュメモリ２４の記憶領域は、複数の論理ブ

ロック３１を含む。各論理ブロック３１は、記憶領域を論理的に分割した部分領域である。例えば、１ＴＢの記憶領域は、１００ＭＢのサイズをそれぞれ有する１００００個の論理ブロック３１に分割されてもよい。消去コントローラ１４は、データの消去に成功したか否かを検証するために、暗号鍵の変更前及び変更後のデータを、記憶領域全体について比較してもよく、記憶領域の一部（例えば、記憶領域全体の１０％に相当する１０００個の論理ブロック３１）について比較してもよい。後者の場合、比較される論理ブロック３１は、所定の規則に従って指定されてもよく（例えば、図３のハッチングされた論理ブロック３１）、ランダムに指定されてもよい。

[0030] 図３等では、フラッシュメモリ２４の記憶領域を２次元的に示すが、記憶領域は連続した一連のメモリ空間と考えてもよい。

[0031] ［比較例］

ここで、図４及び図５を参照して、従来技術に係るデータ消去の検証について説明する。説明のため、図１の情報処理装置１が、図４及び図５に示す消去処理を実行する場合を想定する。

[0032] 図４は、比較例１に係る消去処理を示すフローチャートである。図４は、非特許文献１に開示されたデータ消去の検証方法を示す。

[0033] 図４他の消去処理は、例えば、ＢＩＯＳ又はＵＥＦＩプログラムを介して記憶装置１３に格納されたデータの消去が指示されたときに開始される。

[0034] ステップＳ１において、消去コントローラ１４は、例えば図３に示すように指定された論理ブロック３１の元データを読み出す。ここで、「元データ」は、変更前の暗号鍵が不揮発性メモリ２３に格納されている場合に、記憶領域の指定された論理ブロック３１から読み出されたデータを示す。この論理ブロック３１が暗号化及び復号の対象である場合、消去コントローラ１４は、変更前の暗号鍵を用いて復号されたデータを取得する。一方、この論理ブロック３１が暗号化及び復号の対象ではない場合、消去コントローラ１４は、論理ブロック３１から読み出されたデータを復号せずにそのまま取得する。一般に、例えば、ＲＡＭ１２が数ＧＢ～数十ＧＢのサイズを有し、記憶

装置１３が１ＴＢの記憶領域を有し、記憶領域の１０％、すなわち１００ＧＢのデータを読み出す場合、そのすべてをＲＡＭ１２に保持することはできない。従って、ステップＳ２において、消去コントローラ１４は、元データを一時的に退避するため、元データを外部の情報処理装置に送信する。

[0035] ステップＳ３において、消去コントローラ１４は、不揮発性メモリ２３に格納された暗号鍵を変更する。本明細書では、変更前の暗号鍵を「第１の暗号鍵」とも呼び、変更後の暗号鍵を「第２の暗号鍵」とも呼ぶ。

[0036] ステップＳ４において、消去コントローラ１４は、ステップＳ１の場合と同じ指定された論理ブロック３１の現在のデータを読み出す。ここで、「現在のデータ」は、変更後の暗号鍵が不揮発性メモリ２３に格納されている場合に、記憶領域の指定された論理ブロック３１から読み出されたデータを示す。この論理ブロック３１が暗号化及び復号の対象である場合、消去コントローラ１４は、変更後の暗号鍵を用いて復号されたデータを取得する。一方、この論理ブロック３１が暗号化及び復号の対象ではない場合、消去コントローラ１４は、論理ブロック３１から読み出されたデータを復号せずにそのまま取得する。

[0037] ステップＳ５において、消去コントローラ１４は、外部の情報処理装置から、一時的に退避した元データを受信する。

[0038] ステップＳ６において、消去コントローラ１４は、現在のデータが元データと異なるか否かを判断し、ＹＥＳのときはステップＳ７に進み、ＮＯのときはステップＳ８に進む。ここで、現在のデータ及び元データは論理ブロック３１ごとに比較されるので、数ＧＢ～数十ＧＢのサイズを有するＲＡＭ１２を用いて実行可能である。

[0039] ステップＳ７において、消去コントローラ１４は、データの消去に成功したことを示す検証結果を表示装置１８に出力する。また、ステップＳ８において、消去コントローラ１４は、データの消去に失敗したことを示す検証結果を表示装置１８に出力する。

[0040] 図４の処理によれば、ＲＡＭ１２に格納できない大量のデータを比較する

ので、データを一時的に退避するために外部の情報処理装置が必要とされる。従って、外部の情報処理装置を必要とせず、情報処理装置１のみで実行可能なデータ消去の検証方法が求められる。

[0041] 図５は、比較例２に係る消去処理を示すフローチャートである。図５は、特許文献１に開示されたデータ消去の検証方法を示す。

[0042] ステップＳ１１において、消去コントローラ１４は、例えば図３に示すように指定された論理ブロック３１に既知のパターンデータを書き込む。パターンデータは、例えば、すべて１からなるビット列、すべて０からなるビット列、ランダムなビット列、などを含む。パターンデータは、不揮発性メモリ１５に予め格納されている。パターンデータは、変更前の暗号鍵を用いて暗号化されて記憶領域の指定された論理ブロック３１に書き込まれる。

[0043] ステップＳ１２において、消去コントローラ１４は、不揮発性メモリ２３に格納された暗号鍵を変更する。

[0044] ステップＳ１３において、消去コントローラ１４は、ステップＳ１１の場合と同じ指定された論理ブロック３１の現在のデータを読み出す。

[0045] ステップＳ１４において、消去コントローラ１４は、現在のデータがパターンデータと異なるか否かを判断し、ＹＥＳのときはステップＳ１５に進み、ＮＯのときはステップＳ１６に進む。

[0046] ステップＳ１５において、消去コントローラ１４は、データの消去に成功したことを示す検証結果を表示装置１８に出力する。また、ステップＳ１６において、消去コントローラ１４は、データの消去に失敗したことを示す検証結果を表示装置１８に出力する。

[0047] パターンデータは、上述したように、変更前の暗号鍵が不揮発性メモリ２３に格納されている場合に、記憶領域の指定された論理ブロック３１に書き込まれる。従って、パターンデータは、実質的に、図４の処理の「元データ」、すなわち、変更前の暗号鍵が不揮発性メモリ２３に格納されている場合に、記憶領域の指定された論理ブロック３１から読み出されたデータに対応する。

[0048] 図５の処理によれば、既知のパターンデータを用いることにより、外部の情報処理装置を必要とせず、情報処理装置１のみで実行可能である。しかしながら、図５の処理は、図４の処理と同様に、大量のデータを比較するために、情報処理装置１に大きな負荷がかかる。従って、データの消去に成功したか否かをより小さな負荷で検証できる消去処理が求められる。

[0049] 次いで、データの消去に成功したか否かをより小さな負荷で検証できる、実施形態に係る消去処理について説明する。

[0050] ［実施例１］

図６は、図１の消去コントローラ１４によって実行される実施例１に係る消去処理を示すフローチャートである。

[0051] ステップＳ２１において、消去コントローラ１４は、例えば図３に示すように指定された論理ブロック３１に既知のパターンデータを書き込む。不揮発性メモリ１５は、パターンデータを格納するとともに、任意のハッシュ関数を用いて計算されたパターンデータのハッシュ値を予め格納している。ハッシュ関数は、例えば、ＳＨＡ－２５６などのＳＨＡ－２関数であってもよい。ＳＨＡ－２５６関数は、最長で$2^{(64-1)}$ビットまでの任意長のデータから、２５６ビット（３２バイト）のハッシュ値を生成する。

[0052] ステップＳ２２において、消去コントローラ１４は、不揮発性メモリ２３に格納された暗号鍵を変更する。

[0053] ステップＳ２３において、消去コントローラ１４は、ステップＳ２１の場合と同じ指定された論理ブロック３１の現在のデータを読み出す。次いで、ステップＳ２４において、消去コントローラ１４は、パターンデータのハッシュ値を計算するために用いたハッシュ関数と同じハッシュ関数を用いて、現在のデータのハッシュ値を計算する。

[0054] ステップＳ２５において、消去コントローラ１４は、パターンデータのハッシュ値を不揮発性メモリ１５から読み出す。

[0055] ステップＳ２６において、消去コントローラ１４は、現在のデータのハッシュ値がパターンデータのハッシュ値とは異なるか否かを判断し、ＹＥＳの

ときはステップＳ２７に進み、ＮＯのときはステップＳ２８に進む。

[0056] 異なるデータのハッシュ値が衝突する可能性がある。ただし、比較されるすべての論理ブロック３１においてパターンデータのハッシュ値及び現在のデータのハッシュ値が衝突する可能性は極めて低いと考えられる。従って、例えば１０００個の論理ブロック３１においてハッシュ値を比較する場合、数個の論理ブロック３１においてハッシュ値が一致していても、消去コントローラ１４は、データの消去に成功したと判断してもよい。また、半分以上の論理ブロック３１においてハッシュ値が異なる場合、消去コントローラ１４は、データの消去に成功したと判断してもよい。

[0057] また、互いに近接したいくつかの論理ブロック３１においてパターンデータのハッシュ値及び現在のデータのハッシュ値が一致する場合、消去コントローラ１４は、データの消去に失敗したと判断してもよい。この場合、これらの論理ブロック３１を含む領域が暗号化及び復号の対象ではないと考えられる。

[0058] ステップＳ２７において、消去コントローラ１４は、データの消去に成功したことを示す検証結果を表示装置１８に出力する。また、ステップＳ２８において、消去コントローラ１４は、データの消去に失敗したことを示す検証結果を表示装置１８に出力する。

[0059] 図７は、比較例１、比較例２、及び実施例１に係る検証方法を比較する表である。記憶装置１３が１ＴＢの記憶領域を有し、１ＴＢの記憶領域が１００ＭＢのサイズをそれぞれ有する１００００個の論理ブロック３１に分割される場合を想定する。また、記憶領域の１０％、すなわち、１０００個の論理ブロック３１の合計１００ＧＢのデータを読み出して検証する場合を想定する。比較例１によれば、１００ＧＢのデータを外部の情報処理装置に一時的に退避する必要がある。また、比較例１及び比較例２によれば、暗号鍵の変更前及び変更後の１００ＧＢのデータを互いに比較する必要がある。一方、実施例１によれば、ＳＨＡ－２５６関数を用いる場合、各論理ブロック３１のデータは、３２バイトのハッシュ値によって表される。従って、実施例

１によれば、データを外部の情報処理装置に一時的に退避することは不要であり、また、暗号鍵の変更前及び変更後のデータとして、合計３２ＫＢのデータを比較するだけでよい。このように、実施例１によれば、データの消去に成功したか否かを小さな負荷で検証することができる。

[0060] 記憶領域の１０％のデータを読み出して検証する場合、１０個ごとに１つの論理ブロック３１のデータを指定してもよい。また、記憶領域のうちの５％のデータを読み出して検証する場合、２０個ごとに１つの論理ブロック３１のデータを指定してもよい。記憶領域が１００００個の論理ブロック３１に分割され、記憶領域の１０％、すなわち、１０００個の論理ブロック３１のデータを読み出して検証する場合、データのハッシュ値は合計３２ＫＢのサイズを有する。また、記憶領域が１０００個の論理ブロック３１に分割され、記憶領域の１０％、すなわち、１００個の論理ブロック３１のデータを読み出して検証する場合、データのハッシュ値は合計３２００バイトのサイズを有する。また、記憶領域が１００００個の論理ブロック３１に分割され、記憶領域の５％、すなわち、５００個の論理ブロック３１のデータを読み出して検証する場合、データのハッシュ値は合計１６ＫＢのサイズを有する。また、記憶領域が１０００個の論理ブロック３１に分割され、記憶領域の５％、すなわち、５０個の論理ブロック３１のデータを読み出して検証する場合、データのハッシュ値は合計１６００バイトのサイズを有する。いずれの場合でも、比較されるデータのサイズは、比較例１及び比較例２の場合よりもずっと小さくなる。

[0061] 比較する論理ブロック３１をランダムに指定する場合、論理ブロック３１のアドレスをさらに記憶する必要がある。記憶領域が１００００個又は１０００個の論理ブロック３１に分割される場合、各論理ブロック３１のアドレス（０～９９９９又は０～９９９）は２バイトで表される。従って、１０００個、５００個、１００個、又は５０個の論理ブロック３１のデータを読み出して検証する場合、記憶されるアドレスの合計サイズは、２０００バイト、１０００バイト、２００バイト、又は１００バイトになる。いずれの場合

でも、記憶されるアドレスのサイズは比較的小さい。

[0062] 図８は、図２のフラッシュメモリ２４の論理ブロック３１を示す概略図であって、データの消去を検証するために比較される論理ブロック３１の配置の第１の変形例を示す図である。記憶領域は、記憶領域を論理的に分割した複数の部分領域であって、論理的に連続した複数の論理ブロック３１をそれぞれ含む複数の部分領域２４ａ－１～２４ａ－２を含んでもよい。図８の例では、部分領域２４ａ－１は、部分領域２４ａ－２の論理アドレスよりも小さな論理アドレスを有する。消去コントローラ１４は、複数の部分領域２４ａ－１～２４ａ－２のそれぞれに関して、当該部分領域に含まれる複数の論理ブロック３１のうち、部分領域ごとに異なる割合の論理ブロック３１を指定してもよい（例えば、図８のハッチングされた論理ブロック３１）。ハッシュ値は、指定された複数の論理ブロック３１に格納されたデータに基づいて計算される。情報処理装置１の重要なファイル（例えば、情報処理装置１へのログインパスワードなどの機密データ）は、小さい論理アドレスを有する論理ブロック３１に格納されている可能性が高いと考えられる。従って、消去コントローラ１４は、部分領域２４ａ－１において、部分領域２４ａ－２における割合よりも多くの割合の論理ブロック３１を指定してもよい。図８に示すように論理ブロック３１を指定することにより、情報処理装置１の重要なファイルを含むと考えられる領域に格納されたデータの消去をより確実に検証することができる。

[0063] 記憶装置１３の記憶領域は、２つの部分領域２４ａ－１～２４ａ－２に限らず、３つ以上の部分領域に分割されてもよい。

[0064] 図９は、図２のフラッシュメモリ２４の論理ブロック３１を示す概略図であって、データの消去を検証するために比較される論理ブロック３１の配置の第２の変形例を示す図である。消去コントローラ１４は、論理的に互いに隣接する複数の論理ブロック３１を指定してもよい（例えば、図９のハッチングされた論理ブロック３１）。ハッシュ値は、論理的に互いに隣接する複数の論理ブロック３１に格納されたデータに基づいて計算される。ハッシュ

値は、論理的に互いに隣接する２つの論理ブロック３１に格納されたデータの論理積、論理和、又は排他的論理和に基づいて計算されてもよい。図９に示すように論理ブロック３１を指定することにより、ハッシュ値の衝突を回避できる場合がある。

[0065] ［実施例２］

図１０は、図１の消去コントローラ１４によって実行される実施例２に係る消去処理を示すフローチャートである。

[0066] ステップＳ３１において、消去コントローラ１４は、例えば図３、図８、又は図９に示すように指定された論理ブロック３１の元データを読み出す。次いで、ステップＳ３２において、消去コントローラ１４は、元データのハッシュ値を計算する。論理ブロック３１ごとに１つのハッシュ値が計算されてもよく、予め決められた個数の論理ブロック３１ごとに１つのハッシュ値が計算されてもよい。後者の場合、ＲＡＭ１２において、読み出されたデータを格納するためのバッファメモリが設けられる。バッファメモリは、例えば、論理ブロック３１の１０倍のサイズを有する。消去コントローラ１４は、読み出されたデータを順次にバッファメモリに書き込み、バッファメモリがフルになったとき、データのハッシュ値を計算する。図１０の処理の実行中（特に、暗号鍵の変更前後）に情報処理装置１の電源はオフされないので、計算されたハッシュ値はＲＡＭ１２に保持されてもよい。また、計算されたハッシュ値は不揮発性メモリ１５に保持されてもよい。

[0067] ステップＳ３３において、消去コントローラ１４は、不揮発性メモリ２３に格納された暗号鍵を変更する。

[0068] ステップＳ３４において、消去コントローラ１４は、ステップＳ３１の場合と同じ指定された論理ブロック３１の現在のデータを読み出す。次いで、ステップＳ３５において、消去コントローラ１４は、元データのハッシュ値を計算するために用いたハッシュ関数と同じハッシュ関数を用いて、現在のデータのハッシュ値を計算する。元データのハッシュ値を計算する場合と同様に、論理ブロック３１ごとに１つのハッシュ値が計算されてもよく、予め

決められた個数の論理ブロック３１ごとに１つのハッシュ値が計算されてもよい。これにより、同じ１つ又は複数の論理ブロック３１について、元データのハッシュ値が計算され（ステップＳ３２）、現在のデータのハッシュ値が計算される（ステップＳ３５）。

[0069] ステップＳ３６において、消去コントローラ１４は、現在のデータのハッシュ値が元データのハッシュ値とは異なるか否かを判断し、ＹＥＳのときはステップＳ３７に進み、ＮＯのときはステップＳ３８に進む。

[0070] 前述したように、異なるデータのハッシュ値が衝突する可能性がある。ただし、比較されるすべての論理ブロック３１において元データのハッシュ値及び現在のデータのハッシュ値が衝突する可能性は極めて低いと考えられる。従って、例えば１０００個の論理ブロック３１においてハッシュ値を比較する場合、数個の論理ブロック３１においてハッシュ値が一致していても、消去コントローラ１４は、データの消去に成功したと判断してもよい。また、半分以上の論理ブロック３１においてハッシュ値が異なる場合、消去コントローラ１４は、データの消去に成功したと判断してもよい。

[0071] また、互いに近接したいくつかの論理ブロック３１において元データのハッシュ値及び現在のデータのハッシュ値が一致する場合、消去コントローラ１４は、データの消去に失敗したと判断してもよい。この場合、これらの論理ブロック３１を含む領域が暗号化及び復号の対象ではないと考えられる。

[0072] ステップＳ３７において、消去コントローラ１４は、データの消去に成功したことを示す検証結果を表示装置１８に出力する。また、ステップＳ３８において、消去コントローラ１４は、データの消去に失敗したことを示す検証結果を表示装置１８に出力する。

[0073] 実施例２によれば、実施例１と同様に、データを外部の情報処理装置に一時的に退避することは不要であり、また、暗号鍵の変更前及び変更後のデータとして、ハッシュ値を比較するだけでよい。このように、実施例２によれば、データの消去に成功したか否かを小さな負荷で検証することができる。

[0074] 一般に、ソリッドステートドライブでは、データの書き込みはデータの読

み出しよりも時間がかかる。図１０の処理によれば、パターンデータを記憶装置１３に書き込む必要がないので、図６の場合よりも処理時間を短縮することができる。

[0075] また、複数の論理ブロック３１ごとに１つのハッシュ値を計算する場合、論理ブロック３１ごとに１つのハッシュ値を計算する場合よりも、計算量が低減されて処理速度が向上し、また、計算されたハッシュ値を格納するために必要な記憶容量が削減される。

[0076] ［実施例３］

図１１は、図１の消去コントローラ１４によって実行される実施例３に係る消去処理を示すフローチャートである。

[0077] ステップＳ４１において、消去コントローラ１４は、記憶領域の全体及び部分の元データを読み出す。記憶領域は、記憶領域を互いに異なる複数のサイズで論理的に分割した複数の部分領域を含む。元データは、記憶領域の全体及び複数のサイズを有する複数の部分領域のそれぞれに関して読み出される。ステップＳ４２において、消去コントローラ１４は、記憶領域の全体及び複数のサイズを有する複数の部分領域のそれぞれに関して、当該領域に格納された元データのハッシュ値を計算する。

[0078] 図１２は、図２のフラッシュメモリ２４の論理ブロック３１を示す概略図であって、データの消去を検証するためにすべての論理ブロック３１が比較される場合を示す図である。図１３は、図２のフラッシュメモリ２４の論理ブロック３１を示す概略図であって、データの消去を検証するために部分領域２４ｂ－１，２４ｂ－２のそれぞれに含まれる論理ブロック３１が比較される場合を示す図である。図１４は、図２のフラッシュメモリ２４の論理ブロック３１を示す概略図であって、データの消去を検証するために部分領域２４ｃ－１～２４ｃ－４のそれぞれに含まれる論理ブロック３１が比較される場合を示す図である。図１５は、図２のフラッシュメモリ２４の論理ブロック３１を示す概略図であって、データの消去を検証するために部分領域２４ｄ－１～２４ｄ－８のそれぞれに含まれる論理ブロック３１が比較される

場合を示す図である。図１２の場合、記憶領域の全体で１つのハッシュ値が計算される。図１３の場合、記憶領域の全体が２つの部分領域２４ｂ－１，２４ｂ－２に分割され、部分領域２４ｂ－１，２４ｂ－２のそれぞれについて１つのハッシュ値が計算される。図１４の場合、記憶領域の全体が４つの部分領域２４ｃ－１～２４ｃ－４に分割され、部分領域２４ｃ－１～２４ｃ－４のそれぞれについて１つのハッシュ値が計算される。図１５の場合、記憶領域の全体が８つの部分領域２４ｄ－１～２４ｄ－８に分割され、部分領域２４ｄ－１～２４ｄ－８のそれぞれについて１つのハッシュ値が計算される。図１２～図１５と同様に、より細分化された部分領域のそれぞれについてハッシュ値が計算されてもよい。

[0079] 図１１のステップＳ４３において、消去コントローラ１４は、不揮発性メモリ２３に格納された暗号鍵を変更する。

[0080] ステップＳ４４において、消去コントローラ１４は、記憶領域の現在のデータを読み出す。次いで、ステップＳ４５において、消去コントローラ１４は、記憶領域の全体の現在のデータのハッシュ値を計算する。

[0081] ステップＳ４６において、消去コントローラ１４は、現在のデータのハッシュ値が、ステップＳ４２において計算された対応する元データのハッシュ値と異なるか否かを判断し、ＹＥＳのときはステップＳ４９に進み、ＮＯのときはステップＳ４７に進む。

[0082] ステップＳ４７において、消去コントローラ１４は、ステップＳ４２において計算された元データのすべてのハッシュ値に対して比較したか否かを判断し、ＹＥＳのときはステップＳ５０に進み、ＮＯのときはステップＳ４８に進む。

[0083] ステップＳ４８において、消去コントローラ１４は、記憶領域を分割した各部分領域の現在のデータのハッシュ値を計算する。ステップＳ４８を最初に実行する場合、消去コントローラ１４は、記憶領域を２つに分割した部分領域２４ｂ－１，２４ｂ－２のそれぞれについて現在のデータのハッシュ値を計算する。ステップＳ４８を２回目に実行する場合、消去コントローラ１

４は、記憶領域を４つに分割した部分領域２４ｃ－１～２４ｃ－４のそれぞれについて現在のデータのハッシュ値を計算する。以後、消去コントローラ１４は、ステップＳ４６又はＳ４７においてＹＥＳと判断されるまでステップＳ４８を同様に繰り返し、部分領域の現在のデータのハッシュ値を計算する。

[0084] ステップＳ４９において、消去コントローラ１４は、データの消去に成功したことを示す検証結果を表示装置１８に出力する。また、ステップＳ５０において、消去コントローラ１４は、データの消去に失敗したことを示す検証結果を表示装置１８に出力する。

[0085] 図１１の処理によれば、ある部分領域において元データのハッシュ値及び現在のデータのハッシュ値が衝突しても、より小さな部分領域のハッシュ値を比較することにより、ハッシュ値の衝突を回避できる場合がある。

[0086] ［第１の実施形態の変形例］

図１６は、第１の実施形態の変形例に係る情報処理装置１Ａの構成を示すブロック図である。情報処理装置１Ａは、図１の情報処理装置１の各構成要素に加えて、外部装置に接続するための装置インターフェース（Ｉ／Ｆ）１９をさらに備える。装置インターフェース１９は、例えば、ＵＳＢである。図１６の例では、装置インターフェース１９は、ＵＳＢメモリ、ソリッドステートドライブ、ハードディスクドライブなどの外部記憶装置４１に接続される。

[0087] 図６他を参照して説明される消去処理のためのプログラムは、不揮発性メモリ１５に格納されることに代えて、外部記憶装置４１に格納されてもよい。この場合、消去コントローラ１４は、消去処理のためのプログラムを外部記憶装置４１から読み出して実行する。また、消去処理のためのプログラムは、複数の部分に分割され、一部が不揮発性メモリ１５に格納され、他の一部が外部記憶装置４１に格納されてもよい。この場合、外部記憶装置４１に格納されたプログラム部分を実行することにより、不揮発性メモリ１５に格納されたプログラム部分が呼び出されて実行される。

[0088] 例えば、情報処理装置１Ａが実施例２に係る消去処理を実行する場合、計算された元データのハッシュ値は、ＲＡＭ１２又は不揮発性メモリ１５に格納されることに代えて、外部記憶装置４１に格納されてもよい。ハッシュ値から元データを推測することは困難であるので、外部記憶装置４１を紛失した場合又は盗難にあった場合であっても、機密データが漏洩する可能性は低い。

[0089] 計算された元データのハッシュ値は、通信装置１６を介して接続された外部の情報処理装置に送信されて格納されてもよい。また、情報処理装置１，１Ａは、ＣＤ、ＤＶＤなどの記憶媒体のためのドライブ装置をさらに備えてもよく、この場合、計算された元データのハッシュ値は、ＣＤ、ＤＶＤなどに格納されてもよい。

[0090] ［第１の実施形態の効果等］

第１の実施形態に係る情報処理装置１は、格納されるデータの自己暗号化機能を有する記憶装置１３と、記憶装置１３に格納されたデータの消去を制御する消去コントローラ１４とを備える。記憶装置１３は、記憶領域を有する記憶媒体と、暗号鍵を格納した不揮発性メモリ２３と、入力されたデータを記憶領域に書き込み、記憶領域から読み出されたデータを出力し、記憶領域に書き込まれるデータの少なくとも一部を暗号鍵を用いて暗号化し、記憶領域から読み出されたデータの少なくとも一部を暗号鍵を用いて復号する入出力コントローラ２１とを備える。消去コントローラ１４は、不揮発性メモリ２３に第１の暗号鍵が格納されている場合、記憶領域の指定された位置に格納されるべきデータに基づいて、又は、記憶領域の指定された位置に格納されているデータに基づいて計算された第１のハッシュ値を取得する。消去コントローラ１４は、不揮発性メモリ２３に格納された第１の暗号鍵を第２の暗号鍵に変更するように記憶装置１３を制御する。消去コントローラ１４は、不揮発性メモリ２３に第２の暗号鍵が格納されている場合、記憶領域の指定された位置から読み出されたデータに基づいて第２のハッシュ値を計算する。消去コントローラ１４は、第２のハッシュ値が第１のハッシュ値とは

異なる場合、記憶装置１３に格納されたデータの消去に成功したことを示す検証結果を出力する。消去コントローラ１４は、第２のハッシュ値が第１のハッシュ値に一致する場合、記憶装置１３に格納されたデータの消去に失敗したことを示す検証結果を出力する。

[0091] これにより、記憶装置１３に格納されたデータの消去に成功したか否かを従来よりも小さな負荷で検証することができる。

[0092] 第１の実施形態に係る情報処理装置１によれば、消去コントローラ１４は、予め決められたパターンデータを記憶領域の指定された位置に格納するように記憶装置１３を制御してもよい。この場合、第１のハッシュ値は、パターンデータに基づいて計算される。

[0093] これにより、データを外部の情報処理装置に一時的に退避することなく、データ消去を検証することができる。

[0094] 第１の実施形態に係る情報処理装置１によれば、消去コントローラ１４は、記憶領域の指定された位置から読み出されたデータに基づいて、第１のハッシュ値を計算してもよい。

[0095] これにより、データを外部の情報処理装置に一時的に退避することなく、データ消去を検証することができる。

[0096] 第１の実施形態に係る情報処理装置１によれば、記憶領域は複数のブロックを含んでもよい。この場合、第１及び第２のハッシュ値は、予め決められた個数のブロックごとに、当該ブロックに格納されたデータに基づいて計算される。

[0097] これにより、論理ブロック３１ごとに１つのハッシュ値を計算する場合よりも、計算量が低減されて処理速度が向上し、また、計算されたハッシュ値を格納するために必要な記憶容量が削減される。

[0098] 第１の実施形態に係る情報処理装置１によれば、記憶領域は、記憶領域を論理的に分割した複数の部分領域であって、論理的に連続した複数のブロックをそれぞれ含む複数の部分領域を含んでもよい。この場合、消去コントローラ１４は、複数の部分領域のそれぞれに関して、当該部分領域に含まれる

複数の論理ブロックのうち、部分領域ごとに異なる割合の論理ブロックを指定する。第１及び第２のハッシュ値は、指定された複数のブロックに格納されたデータに基づいて計算される。

[0099] これにより、情報処理装置１の重要なファイルを含むと考えられる領域に格納されたデータの消去をより確実に検証することができる。

[0100] 第１の実施形態に係る情報処理装置１によれば、記憶領域は複数のブロックを含んでもよい。この場合、第１及び第２のハッシュ値は、論理的に互いに隣接する複数のブロックに格納されたデータに基づいて計算される。

[0101] これにより、ハッシュ値の衝突を回避できる場合がある。

[0102] 第１の実施形態に係る情報処理装置１によれば、記憶領域は、記憶領域を互いに異なる複数のサイズで論理的に分割した複数の部分領域を含んでもよい。この場合、第１のハッシュ値は、複数のサイズを有する複数の部分領域のそれぞれに関して、当該部分領域に格納されたデータに基づいて計算される。消去コントローラ１４は、複数のサイズのうち第１のサイズを有する複数の部分領域のそれぞれに関して、当該部分領域に格納されたデータに基づいて第２のハッシュ値を計算する。消去コントローラ１４は、第１のサイズを有する部分領域に関して第２のハッシュ値が第１のハッシュ値とは異なる場合、記憶装置１３に格納されたデータの消去に成功したことを示す検証結果を出力する。消去コントローラ１４は、第１のサイズを有する部分領域に関して第２のハッシュ値が第１のハッシュ値に一致する場合、複数のサイズのうち、第１のサイズよりも小さい第２のサイズを有する複数の部分領域のそれぞれに関して、当該部分領域に格納されたデータに基づいて第２のハッシュ値を計算する。消去コントローラ１４は、第２のサイズを有する部分領域に関して第２のハッシュ値が第１のハッシュ値とは異なる場合、記憶装置１３に格納されたデータの消去に成功したことを示す検証結果を出力する。

[0103] これにより、ある部分領域において元データのハッシュ値及び現在のデータのハッシュ値が衝突しても、より小さな部分領域のハッシュ値を比較することにより、ハッシュ値の衝突を回避できる場合がある。

[0104] 第１の実施形態に係る情報処理装置１は、検証結果を出力する表示装置１８を備えてもよい。

[0105] これにより、記憶装置１３に格納されたデータの消去に成功したか否かを把握することができる。

[0106] 第１の実施形態に係る情報処理方法は、自己暗号化機能を有する記憶装置１３に格納されたデータの消去を制御する。記憶装置１３は、記憶領域を有する記憶媒体と、暗号鍵を格納した不揮発性メモリ２３と、入力されたデータを記憶領域に書き込み、記憶領域から読み出されたデータを出力し、記憶領域に書き込まれるデータの少なくとも一部を暗号鍵を用いて暗号化し、記憶領域から読み出されたデータの少なくとも一部を暗号鍵を用いて復号する入出力コントローラ２１とを備える。情報処理方法は、不揮発性メモリ２３に第１の暗号鍵が格納されている場合、記憶領域の指定された位置に格納されるべきデータに基づいて、又は、記憶領域の指定された位置に格納されているデータに基づいて計算された第１のハッシュ値を取得するステップを含む。情報処理方法は、不揮発性メモリ２３に格納された第１の暗号鍵を第２の暗号鍵に変更するように記憶装置１３を制御するステップを含む。情報処理方法は、不揮発性メモリ２３に第２の暗号鍵が格納されている場合、記憶領域の指定された位置から読み出されたデータに基づいて第２のハッシュ値を計算するステップを含む。情報処理方法は、第２のハッシュ値が第１のハッシュ値とは異なる場合、記憶装置１３に格納されたデータの消去に成功したことを示す検証結果を出力するステップを含む。情報処理方法は、第２のハッシュ値が第１のハッシュ値に一致する場合、記憶装置１３に格納されたデータの消去に失敗したことを示す検証結果を出力するステップを含む。

[0107] これにより、記憶装置１３に格納されたデータの消去に成功したか否かを従来よりも小さな負荷で検証することができる。

[0108] 第１の実施形態に係るプログラムは、情報処理装置１に実装されたプロセッサによって実行される命令を含む。情報処理装置１は、格納されるデータの自己暗号化機能を有する記憶装置１３をさらに備える。記憶装置１３は、

記憶領域を有する記憶媒体と、暗号鍵を格納した不揮発性メモリ２３と、入力されたデータを記憶領域に書き込み、記憶領域から読み出されたデータを出力し、記憶領域に書き込まれるデータの少なくとも一部を暗号鍵を用いて暗号化し、記憶領域から読み出されたデータの少なくとも一部を暗号鍵を用いて復号する入出力コントローラとを備える。命令は、プロセッサに、不揮発性メモリ２３に第１の暗号鍵が格納されている場合、記憶領域の指定された位置に格納されるべきデータに基づいて、又は、記憶領域の指定された位置に格納されているデータに基づいて計算された第１のハッシュ値を取得することを含む。命令は、プロセッサに、不揮発性メモリ２３に格納された第１の暗号鍵を第２の暗号鍵に変更するように記憶装置１３を制御することを含む。命令は、プロセッサに、不揮発性メモリ２３に第２の暗号鍵が格納されている場合、記憶領域の指定された位置から読み出されたデータに基づいて第２のハッシュ値を計算することを含む。命令は、プロセッサに、第２のハッシュ値が第１のハッシュ値とは異なる場合、記憶装置１３に格納されたデータの消去に成功したことを示す検証結果を出力することを含む。命令は、プロセッサに、第２のハッシュ値が第１のハッシュ値に一致する場合、記憶装置１３に格納されたデータの消去に失敗したことを示す検証結果を出力することを実行させる。

[0109] これにより、記憶装置１３に格納されたデータの消去に成功したか否かを従来よりも小さな負荷で検証することができる。

[0110] ［第２の実施形態］

第２の実施形態では、第１の実施形態の消去処理（図１０を参照）を実行しながら、データ消去の進捗度を表示する場合について説明する。

[0111] 図１７は、第２の実施形態に係る情報処理装置１によって実行される消去処理を示すフローチャートである。第２の実施形態に係る情報処理装置１は、第１の実施形態の場合と同様に構成される。図１７の消去処理は、図１の消去コントローラ１４によって実行される。

[0112] ステップＳ１０１において、消去コントローラ１４は前処理を実行し、指

定された論理ブロック３１の元データのハッシュ値を計算する。

[0113] ステップＳ１０２において、消去コントローラ１４は鍵変更処理を実行し、不揮発性メモリ２３に格納された暗号鍵を変更する。

[0114] ステップＳ１０３において、消去コントローラ１４は検証処理を実行し、現在のデータのハッシュ値が元データのハッシュ値とは異なるか否か、すなわち、データの消去に成功したか否かを判断する。

[0115] 図１８は、図１７の前処理（ステップＳ１０１）のサブルーチンを示すフローチャートである。

[0116] ステップＳ１１１において、消去コントローラ１４は、パラメータｉ１を１に初期化する。パラメータｉ１は、例えば図３、図８、又は図９に示すように指定された複数の論理ブロック３１のいずれかを示す。図１８の例では、Ｎ１個の論理ブロック３１が指定される。

[0117] ステップＳ１１２において、消去コントローラ１４は、指定された論理ブロック３１のうち、ｉ１番目の論理ブロック３１の元データを読み出す。次いで、ステップＳ１１３において、消去コントローラ１４は、元データのハッシュ値を計算する。ステップＳ１１２～Ｓ１１３は、指定された論理ブロック３１のうちの１つに対して実行していることを除いて、図１０のステップＳ３１～Ｓ３２と同様である。

[0118] ステップＳ１１４において、消去コントローラ１４は、元データのハッシュ値と、ｉ１番目の論理ブロック３１のアドレスとを、ＲＡＭ１２又は不揮発性メモリ１５（又は、図１６の外部記憶装置４１）に格納する。

[0119] ステップＳ１１５において、消去コントローラ１４は、ステップＳ１１２～Ｓ１１４の処理を実行済みである論理ブロック３１の個数を、所定のフォーマットで表示装置１８に出力する。

[0120] ステップＳ１１６において、消去コントローラ１４は、パラメータｉ１がしきい値Ｎ１を超えたか否かを判断し、ＹＥＳのときは図１７のステップＳ１０２に進み、ＮＯのときはステップＳ１１７に進む。

[0121] ステップＳ１１７において、消去コントローラ１４は、パラメータｉ１を

１だけインクリメントし、ステップＳ１１２～Ｓ１１６を繰り返す。

[0122] 図１９は、図１７の鍵変更処理（ステップＳ１０２）のサブルーチンを示すフローチャートである。

[0123] ステップＳ１２１において、消去コントローラ１４は、不揮発性メモリ２３に格納された暗号鍵を変更する。ステップＳ１２１は、図１０のステップＳ３３と同様である。

[0124] ステップＳ１２２において、消去コントローラ１４は、暗号鍵の変更が完了したことを、所定のフォーマットで表示装置１８に出力する。

[0125] 図２０は、図１７の検証処理（ステップＳ１０３）のサブルーチンを示すフローチャートである。

[0126] ステップＳ１３１において、消去コントローラ１４は、パラメータｉ２を１に初期化する。パラメータｉ２は、図１８の前処理において指定されたＮ１個の論理ブロック３１のいずれかを示す。

[0127] ステップＳ１３２において、消去コントローラ１４は、ＲＡＭ１２又は不揮発性メモリ１５（又は、図１６の外部記憶装置４１）に格納された元データのハッシュ値及びアドレスを読み出す。このアドレスに基づいて、前処理においてハッシュ値が計算された論理ブロック３１が特定される。

[0128] ステップＳ１３３において、消去コントローラ１４は、ステップＳ１３２で読み出されたアドレスにより特定される論理ブロック３１のうち、ｉ２番目の論理ブロック３１の現在のデータを読み出す。次いで、ステップＳ１３４において、消去コントローラ１４は、現在のデータのハッシュ値を計算する。ステップＳ１３３～Ｓ１３４は、指定された論理ブロック３１のうちの１つに対して実行していることを除いて、図１０のステップＳ３４～Ｓ３５と同様である。

[0129] ステップＳ１３５において、消去コントローラ１４は、現在のデータのハッシュ値が元データのハッシュ値とは異なるか否かを判断し、ＹＥＳのときはステップＳ１３６に進み、ＮＯのときはステップＳ１４０に進む。ステップＳ１３５は、指定された論理ブロック３１のうちの１つに対して実行して

いることを除いて、図１０のステップＳ３６と同様である。

[0130] ステップＳ１３６において、消去コントローラ１４は、検証された論理ブロック３１、すなわち、現在のデータのハッシュ値が元データのハッシュ値と異なるか否かを判断した論理ブロック３１の個数を、所定のフォーマットで表示装置１８に出力する。

[0131] ステップＳ１３７において、消去コントローラ１４は、パラメータｉ２がしきい値Ｎ１を超えたか否かを判断し、ＹＥＳのときはステップＳ１３９に進み、ＮＯのときはステップＳ１３８に進む。

[0132] ステップＳ１３８において、消去コントローラ１４は、パラメータｉ２を１だけインクリメントし、ステップＳ１３２～Ｓ１３７を繰り返す。

[0133] ステップＳ１３９において、消去コントローラ１４は、データの消去に成功したことを示す検証結果を表示装置１８に出力する。ステップＳ１４０において、消去コントローラ１４は、データの消去に失敗したことを示す検証結果を表示装置１８に出力する。

[0134] 図２１は、図１７の消去処理を実行することによって図１の表示装置１８に表示される、データ消去の進捗度を示す画像の一例を示す図である。図２１（ａ）は、前処理の進捗度を示す画像である。前処理の進捗度は、例えば、指定された論理ブロック３１の個数に対する処理された論理ブロック３１の個数の割合、すなわち、ｉ１／Ｎ１を示すプログレスバーによって表される。図２１（ｂ）は、鍵変更処理の進捗度を示す画像である。鍵変更処理の進捗度は、例えば、暗号鍵の変更が完了したか否かを示すプログレスバーによって表される。図２１（ｃ）は、検証処理の進捗度を示す画像である。検証処理の進捗度は、例えば、指定された論理ブロック３１の個数に対する検証された論理ブロック３１の個数の割合、すなわち、ｉ２／Ｎ１を示すプログレスバーによって表される。

[0135] 図２２は、図１７の消去処理を実行することによって図１の表示装置１８に表示される、データ消去の進捗度を示す画像の他の一例を示す図である。図２１に示す３つのプログレスバーを１つにまとめて表示してもよい。

[0136] データ消去の進捗度は、図２１及び図２２のような画像として表示されることに代えて、下記のようなテキストとして表示されてもよい。

[0137] 前処理： ａ１

鍵変更処理：ａ２

検証処理： ａ３

[0138] ここで、ａ１は、指定されたブロックの個数Ｎ１から開始して、パラメータｉ１が増大するにつれて減少する（ａ１＝Ｎ１－ｉ１）。ａ２は、暗号鍵が変更される前に「１」になり、暗号鍵が変更された後に「０」になる。ａ３は、指定されたブロックの個数Ｎ１から開始して、パラメータｉ２が増大するにつれて減少する（ａ３＝Ｎ１－ｉ２）。

[0139] また、データ消去の進捗度は、下記のようなテキストとして表示されてもよい。

[0140] 前処理： ｂ１／Ｎ１

鍵変更処理：ｂ２

検証処理： ｂ３／Ｎ１

[0141] ここで、ｂ１＝ｉ１である。ｂ２は、暗号鍵が変更される前に「０」になり、暗号鍵が変更された後に「１」になる。また、ｂ３＝ｉ２である。

[0142] また、データ消去の進捗度は、「ｃ」としてまとめて表示されてもよく、ここで、ｃ＝ａ１＋ａ２＋ａ３である。また、データ消去の進捗度は、「ｄ／Ｎ」としてまとめて表示されてもよく、ここで、ｄ＝ｂ１＋ｂ２＋ｂ３，Ｎ＝Ｎ１×２＋１である。

[0143] 前述したように、複数の論理ブロック３１ごとに１つのハッシュ値を計算する場合、データ消去の進捗度は、１つのハッシュ値に対応する論理ブロック３１のグループを単位として、論理ブロック３１のグループの個数又は割合に基づいて、画像又はテキストとして表示されてもよい。

[0144] 図２０の検証処理では、１つの論理ブロック３１において現在のデータのハッシュ値が元データのハッシュ値に一致する場合、データの消去に失敗したと判断される。しかしながら、前述したように、指定された論理ブロック

３１のうちの一部においてハッシュ値が一致していても、消去コントローラ１４は、データの消去に成功したと判断してもよい。次に、図２３～図２５を参照して、このようなハッシュ値の衝突を許容する検証処理の変形例について説明する。

[0145] 図２３は、図１７の検証処理の第１の変形例を示すフローチャートである。図２３の処理は、図２０の各ステップに加えて、ステップＳ１４１～Ｓ１４３を含む。

[0146] ステップＳ１４１において、消去コントローラ１４は、パラメータｊ１を０に初期化する。パラメータｊ１を用いて、現在のデータのハッシュ値が元データのハッシュ値に一致した論理ブロック３１の個数がカウントされる。

[0147] ステップＳ１３５において現在のデータのハッシュ値が元データのハッシュ値に一致すると判断したとき、処理はステップＳ１４２に進む。ステップＳ１４２において、消去コントローラ１４は、パラメータｊ１を１だけインクリメントする。

[0148] ステップＳ１４３において、消去コントローラ１４は、パラメータｊ１がしきい値Ｔｈ１を超えたか否かを判断し、ＹＥＳのときはステップＳ１４０に進み、ＮＯのときはステップＳ１３６に進む。

[0149] 図２３の検証処理によれば、しきい値Ｔｈ１以下の個数の論理ブロック３１においてハッシュ値の衝突が発生しても、他の論理ブロック３１においてハッシュ値が異なるならば、データの消去に成功したと判断することができる。

[0150] 図２４は、図１７の検証処理の第２の変形例を示すフローチャートである。図２４の処理は、図２０の各ステップに加えて、ステップＳ１５１～Ｓ１５６を含む。

[0151] ステップＳ１５１において、消去コントローラ１４は、パラメータｊ２を０に初期化する。パラメータｊ２を用いて、指定された論理ブロック３１のうち、互いに近接したいくつかの論理ブロック３１において連続して発生するハッシュ値の衝突の回数がカウントされる。

[0152] ステップＳ１３５において現在のデータのハッシュ値が元データのハッシュ値と異なると判断したとき、処理はステップＳ１５２に進み、そうでないとき、処理はステップＳ１５３に進む。ステップＳ１５２において、消去コントローラ１４はパラメータｊ２を１だけデクリメントする。ステップＳ１５３において、消去コントローラ１４は、パラメータｊ２を１だけインクリメントする。

[0153] ステップＳ１５４において、消去コントローラ１４は、パラメータｊ２が０より小さいか否かを判断し、ＹＥＳのときはステップＳ１５５に進み、ＮＯのときはステップＳ１５６に進む。ステップＳ１５５において、消去コントローラ１４は、パラメータｊ２を０に再初期化する。

[0154] ステップＳ１５６において、消去コントローラ１４は、パラメータｊ２がしきい値Ｔｈ２を超えたか否かを判断し、ＹＥＳのときはステップＳ１４０に進み、ＮＯのときはステップＳ１３６に進む。

[0155] 図２４の検証処理によれば、ハッシュ値の一致又は不一致に応じて、パラメータｊ２が増大又は減少する。従って、指定された論理ブロック３１のうち、互いに近接したいくつかの論理ブロック３１においてハッシュ値の衝突が連続して発生する場合、パラメータｊ２は増大する。この場合、これらの論理ブロック３１を含む記憶領域は、暗号化の対象ではなく、データが平文のまま格納されていると考えられる。一方、指定された論理ブロック３１のうち、互いに近接したいくつかの論理ブロック３１においてハッシュ値の一致及び不一致がほぼ交替して発生する場合、パラメータｊ２は増大しない。この場合、ハッシュ値の衝突は偶然であると考えられる。

[0156] 図２５は、図１７の検証処理の第３の変形例を示すフローチャートである。図２５の処理は、図２０の各ステップに加えて、ステップＳ１６１～Ｓ１６９を含む。

[0157] ステップＳ１３５において現在のデータのハッシュ値が元データのハッシュ値に一致すると判断したとき、処理はステップＳ１６１に進む。ステップＳ１６１において、消去コントローラ１４は、ハッシュ値の衝突が発生した

論理ブロック３１のアドレスを、ＲＡＭ１２又は不揮発性メモリ１５（又は、図１６の外部記憶装置４１）に格納する。

[0158] ステップＳ１３７においてパラメータｉ２がしきい値Ｎ１を超えたとき、処理はステップＳ１６２に進む。ステップＳ１６２において、消去コントローラ１４は、パラメータｉ３，ｉ４をそれぞれ１に初期化し、パラメータｊ３を０に初期化する。図２５の検証処理では、指定された論理ブロック３１のうち、互いに近接した所定個数の論理ブロック３１のグループにおいてハッシュ値の衝突の回数がカウントされる。パラメータｉ３は、論理ブロック３１のグループの位置を示す。パラメータｉ４は、あるグループに含まれる論理ブロック３１のいずれかを示す。図２５の例では、各グループはＮ４個の論理ブロック３１を含み、グループの位置は、指定された論理ブロック３１のうちで、Ｎ３＝Ｎ１－Ｎ４通りにシフトする。パラメータｊ３を用いて、あるグループにおけるハッシュ値の衝突の回数がカウントされる。

[0159] ステップＳ１６３において、消去コントローラ１４は、ステップＳ１６１において格納されたアドレスに基づいて、ｉ３＋ｉ４番目の論理ブロック３１において、現在のデータのハッシュ値が元データのハッシュ値に一致するか否かを判断し、ＹＥＳのときはステップＳ１６４に進み、ＮＯのときはステップＳ１６５に進む。ステップＳ１６４において、消去コントローラ１４は、パラメータｊ３を１だけインクリメントする。

[0160] ステップＳ１６５において、消去コントローラ１４は、パラメータｉ４がしきい値Ｎ４を超えたか否か、すなわち、現在のグループに含まれるすべての論理ブロック３１を処理したか否かを判断し、ＹＥＳのときはステップＳ１６７に進み、ＮＯのときはステップＳ１６６に進む。

[0161] ステップＳ１６６において、消去コントローラ１４は、パラメータｉ４を１だけインクリメントし、ステップＳ１６３～Ｓ１６５を繰り返す。

[0162] ステップＳ１６７において、消去コントローラ１４は、パラメータｊ３がしきい値Ｔｈ３を超えたか否かを判断し、ＹＥＳのときはステップＳ１４０に進み、ＮＯのときはステップＳ１６８に進む。

[0163] ステップＳ１６８において、消去コントローラ１４は、パラメータｉ３がしきい値Ｎ３を超えたか否か、すなわち、論理ブロック３１のグループをすべての位置にシフトさせたか否かを判断し、ＹＥＳのときはステップＳ１３９に進み、ＮＯのときはステップＳ１６９に進む。

[0164] ステップＳ１６９において、消去コントローラ１４は、パラメータｉ３を１だけインクリメントし、ステップＳ１６３～Ｓ１６８を繰り返す。

[0165] 図２５の処理によれば、互いに近接した所定個数の論理ブロック３１のグループにおいてハッシュ値の衝突が繰り返し発生する場合、これらの論理ブロック３１を含む記憶領域は、暗号化の対象ではなく、データが平文のまま格納されていると考えられる。

[0166] ステップＳ１６７のしきい値Ｔｈ３は、例えば、グループに含まれる論理ブロック３１の個数Ｎ３に近い値に設定されてもよい。また、ステップＳ１６８において、消去コントローラ１４はｊ３／Ｎ３を計算してもよく、この場合、しきい値Ｔｈ３は、例えば、１に近い値に設定されてもよい。

[0167] ［第２の実施形態の効果等］

第２の実施形態に係る情報処理装置１によれば、消去コントローラ１４は、記憶装置１３に格納されたデータの消去の進捗度を表示装置１８に出力してもよい。

[0168] これにより、データ消去の進捗度を把握することができる。

[0169] ［第３の実施形態］

図２６は、第３の実施形態に係る情報処理装置１及びサーバ装置を含む情報処理システムの構成を示すブロック図である。図２６の情報処理システムは、複数の情報処理装置１－１～１－３、サーバ装置２、及び通信回線３を含む。各情報処理装置１－１～１－３は、図１の情報処理装置１と同様に構成される。サーバ装置２は、通信回線３を介して各情報処理装置１－１～１－３に接続される。

[0170] 本明細書では、情報処理装置１－１～１－３をまとめて「情報処理装置１」を呼ぶ。

[0171] 図２７は、図２６のサーバ装置２の構成を示すブロック図である。サーバ装置２は、バス１２０、ＣＰＵ１２１、ＲＡＭ１２２、記憶装置１２３、通信装置１２６、入力装置１２７、及び表示装置１２８を備える。ＣＰＵ１２１は、サーバ装置２全体の動作を制御し、また、各情報処理装置１の記憶装置１３に格納されたデータの消去を管理する。ＲＡＭ１２２は、サーバ装置２の動作に必要なプログラム及びデータを一時的に記憶する。記憶装置１２３は、サーバ装置２の動作に必要なプログラムを格納する不揮発性記憶媒体である。通信装置１２６は、通信回線３を介して各情報処理装置１と通信可能に接続される。入力装置１２７は、サーバ装置２の動作を制御するユーザ入力を受ける。入力装置１２７は、例えば、キーボード及びポインティングデバイスを含む。表示装置１２８は、各情報処理装置１の記憶装置１３に格納されたデータの消去に関連する情報を表示する。ＣＰＵ１２１、ＲＡＭ１２２、記憶装置１２３、通信装置１２６、入力装置１２７、及び表示装置１２８は、バス１２０を介して互いに接続される。

[0172] 図２８は、図２６のサーバ装置２によって実行される消去処理を示すフローチャートである。図２９は、図２６の情報処理装置１によって実行される消去処理を示すフローチャートである。

[0173] 図２８のステップＳ２０１において、サーバ装置２のＣＰＵ１２１は、データの消去を指示する制御信号を情報処理装置１に送信する。

[0174] 図２９のステップＳ２１１において、情報処理装置１の消去コントローラ１４は、データの消去を指示する制御信号をサーバ装置２から受信する。次いで、消去コントローラ１４は、制御信号に従って、ステップＳ２１２～Ｓ２１９を実行する。ステップＳ２１２～Ｓ２１７は、図１０のステップＳ３１～Ｓ３６と同様である。ステップＳ２１７において現在のデータのハッシュ値が元データのハッシュ値と異なると判断したとき、処理はステップＳ２１８に進み、そうでないとき、処理はステップＳ２１９に進む。ステップＳ２１８において、消去コントローラ１４は、データの消去に成功したことを示す検証結果を含む通知信号をサーバ装置２に送信する。ステップＳ２１９

において、消去コントローラ１４は、データの消去に失敗したことを示す検証結果を含む通知信号をサーバ装置２に送信する。

[0175] 図２８のステップＳ２０２において、サーバ装置２のＣＰＵ１２１は、検証結果を示す通知信号を情報処理装置１から受信する。ステップＳ２０３において、ＣＰＵ１２１は、検証結果を表示装置１２８に出力する。

[0176] 図２８及び図２９の処理によれば、複数の情報処理装置１の記憶装置１３に格納されたデータの消去をサーバ装置２によって集中的に制御することができ、また、データの消去に成功したか否かを小さな負荷で検証することができる。

[0177] また、図３０～図３４を参照して説明するように、データ消去の進捗度をサーバ装置２の表示装置１２８に出力してもよい。

[0178] 図３０は、図２６のサーバ装置２によって実行される消去処理の変形例を示すフローチャートである。図３１は、図２６の情報処理装置１によって実行される消去処理の変形例を示すフローチャートである。図３０の処理は、図２８のステップＳ２０２に代えてステップＳ２２１～Ｓ２２３を含む。図３１の処理は、図２９のステップＳ２１２～Ｓ２１９に代えて、ステップＳ２３１～Ｓ２３３を含む。

[0179] 図３０のステップＳ２０１において、サーバ装置２のＣＰＵ１２１は、データの消去を指示する制御信号を情報処理装置１に送信する。

[0180] 図３１のステップＳ２１１において、情報処理装置１の消去コントローラ１４は、データの消去を指示する制御信号をサーバ装置２から受信する。次いで、消去コントローラ１４は、制御信号に従って、ステップＳ２３１～Ｓ２３３を実行する。ステップＳ２３１～Ｓ２３３は、データ消去の進捗度及び検証結果を情報処理装置１の表示装置１８に出力することに代えてサーバ装置２に送信することを除いて、図１７のステップＳ１０１～Ｓ１０３と同様である。

[0181] 図３２は、図３１の前処理（ステップＳ２３１）のサブルーチンを示すフローチャートである。図３２の処理は、図１８のステップＳ１１５に代えて

ステップＳ１１５Ａを含む。ステップＳ１１５Ａにおいて、消去コントローラ１４は、データ消去の進捗度として、ステップＳ１１２～Ｓ１１４の処理を実行済みである論理ブロック３１の個数を含む通知信号をサーバ装置２に送信する。

[0182] 図３３は、図３１の鍵変更処理（ステップＳ２３２）のサブルーチンを示すフローチャートである。図３３の処理は、図１９のステップＳ１２２に代えてステップＳ１２２Ａを含む。ステップＳ１２２Ａにおいて、消去コントローラ１４は、データ消去の進捗度として、暗号鍵の変更が完了したことを示す通知信号をサーバ装置２に送信する。

[0183] 図３４は、図３１の検証処理（ステップＳ２３３）のサブルーチンを示すフローチャートである。図３４の処理は、図２０のステップＳ１３６，Ｓ１３９，Ｓ１４０に代えて、ステップＳ１３６Ａ，Ｓ１３９Ａ，Ｓ１４０Ａを含む。ステップＳ１３６Ａにおいて、消去コントローラ１４は、データ消去の進捗度として、検証された論理ブロック３１の個数を含む通知信号をサーバ装置２に送信する。ステップＳ１３９Ａにおいて、消去コントローラ１４は、データの消去に成功したことを示す検証結果を含む通知信号をサーバ装置２に送信する。ステップＳ１４０Ａにおいて、消去コントローラ１４は、データの消去に失敗したことを示す検証結果を含む通知信号をサーバ装置２に送信する。

[0184] 図３０のステップＳ２２１において、サーバ装置２のＣＰＵ１２１は、データ消去の進捗度を含む通知信号を情報処理装置１から受信する。ステップＳ２２２において、ＣＰＵ１２１は、情報処理装置１の表示装置１８に出力する場合と同様に、データ消去の進捗度を所定のフォーマットで表示装置１２８に出力する。ステップＳ２２３において、ＣＰＵ１２１は、データ消去が完了したか否か、すなわち、検証結果を示す通知信号を情報処理装置１から受信したか否かを判断し、ＹＥＳのときはステップＳ２０３に進み、ＮＯのときはステップＳ２２１に戻る。ステップＳ２０３において、ＣＰＵ１２１は、検証結果を表示装置１２８に出力する。

[0185] 図３０～図３４の処理によれば、複数の情報処理装置１の記憶装置１３に格納されたデータの消去の進捗度をサーバ装置２において把握することができる。

[0186] ［第３の実施形態の効果等］

第３の実施形態に係る情報処理システム１００は、第１の実施形態に係る情報処理装置１と、情報処理装置１に通信回線を介して接続されたサーバ装置２とを備える。消去コントローラ１４は、サーバ装置２から受信された制御信号に従って、記憶装置１３に格納されたデータの消去を制御する。

[0187] これにより、記憶装置１３に格納されたデータの消去に成功したか否かを従来よりも小さな負荷で検証することができる。

[0188] 第３の実施形態に係る情報処理システム１００は、消去コントローラ１４は、検証結果を含む第１の通知信号をサーバ装置２に送信してもよい。サーバ装置２は、検証結果を出力する表示装置１２８を備えてもよい。

[0189] これにより、記憶装置１３に格納されたデータの消去に成功したか否かを把握することができる。

[0190] 第３の実施形態に係る情報処理システム１００は、消去コントローラ１４は、記憶装置１３に格納されたデータの消去の進捗度を含む第２の通知信号をサーバ装置２に送信してもよい。この場合、表示装置１２８は進捗度を表示する。

[0191] これにより、データ消去の進捗度を把握することができる。

[0192] ［他の実施形態］

以上のように、本出願において開示する技術の例示として、実施形態を説明した。しかしながら、本開示における技術は、これに限定されず、適宜、変更、置き換え、付加、省略などを行った実施形態にも適用可能である。また、上記実施形態で説明した各構成要素を組み合わせて、新たな実施形態とすることも可能である。

[0193] そこで、以下、他の実施形態を例示する。

[0194] 記憶装置１３は、ソリッドステートドライブに限らず、自己暗号化機能を

有するハードディスクドライブ（ＨＤＤ）などの不揮発性記憶媒体であってもよい。

[0195] 検証結果は、表示装置１８に出力されることに限らず、通信装置１６を介して外部の情報処理装置に出力されてもよい。

[0196] 記憶領域の論理的な先頭には重要なデータが格納されるので、消去コントローラ１４は、記憶領域の先頭の３２バイトを常に指定してもよい。

[0197] 消去コントローラ１４は、ハッシュ値を計算する際に、データにソルト（予め決められたキーワード）を付加してもよい。

[0198] 消去コントローラ１４は、論理ブロック３１のサイズを、例えば１／１０にシュリンクしてもよい。

[0199] 図１７～図２５、図３０～図３４では、実施例２に係る消去処理（図１０を参照）を実行しながら、データ消去の進捗度を表示する場合について説明した。それに代わって、実施例１に係る消去処理（図６を参照）又は実施例３に係る消去処理（図１１を参照）を実行しながら、データ消去の進捗度を同様に表示してもよい。

[0200] 以上のように、本開示における技術の例示として、実施形態を説明した。そのために、添付図面および詳細な説明を提供した。

[0201] したがって、添付図面および詳細な説明に記載された構成要素の中には、課題解決のために必須な構成要素だけでなく、上記技術を例示するために、課題解決のためには必須でない構成要素も含まれ得る。そのため、それらの必須ではない構成要素が添付図面や詳細な説明に記載されていることをもって、直ちに、それらの必須ではない構成要素が必須であるとの認定をするべきではない。

[0202] また、上述の実施形態は、本開示における技術を例示するためのものであるから、特許請求の範囲またはその均等の範囲において種々の変更、置き換え、付加、省略などを行うことができる。

[0203] ［実施形態のまとめ］

本開示の第１の態様に係る情報処理装置は、

格納されるデータの自己暗号化機能を有する記憶装置と、

前記記憶装置に格納されたデータの消去を制御する消去コントローラとを備え、

前記記憶装置は、

記憶領域を有する記憶媒体と、

暗号鍵を格納した不揮発性メモリと、

入力されたデータを前記記憶領域に書き込み、前記記憶領域から読み出されたデータを出力し、前記記憶領域に書き込まれるデータの少なくとも一部を前記暗号鍵を用いて暗号化し、前記記憶領域から読み出されたデータの少なくとも一部を前記暗号鍵を用いて復号する入出力コントローラとを備え、

前記消去コントローラは、

前記不揮発性メモリに第１の暗号鍵が格納されている場合、前記記憶領域の指定された位置に格納されるべきデータに基づいて、又は、前記記憶領域の指定された位置に格納されているデータに基づいて計算された第１のハッシュ値を取得し、

前記不揮発性メモリに格納された前記第１の暗号鍵を第２の暗号鍵に変更するように前記記憶装置を制御し、

前記不揮発性メモリに前記第２の暗号鍵が格納されている場合、前記記憶領域の前記指定された位置から読み出されたデータに基づいて第２のハッシュ値を計算し、

前記第２のハッシュ値が前記第１のハッシュ値とは異なる場合、前記記憶装置に格納されたデータの消去に成功したことを示す検証結果を出力し、

前記第２のハッシュ値が前記第１のハッシュ値に一致する場合、前記記憶装置に格納されたデータの消去に失敗したことを示す検証結果を出力する。

[0204] 本開示の第２の態様に係る情報処理装置は、第１の態様に係る情報処理装置において、

前記消去コントローラは、予め決められたパターンデータを前記記憶領域の前記指定された位置に格納するように前記記憶装置を制御し、

前記第１のハッシュ値は、前記パターンデータに基づいて計算される。

[0205] 本開示の第３の態様に係る情報処理装置は、第１の態様に係る情報処理装置において、

前記消去コントローラは、前記記憶領域の前記指定された位置から読み出されたデータに基づいて、前記第１のハッシュ値を計算する。

[0206] 本開示の第４の態様に係る情報処理装置は、第３の態様に係る情報処理装置において、

前記記憶領域は複数のブロックを含み、

前記第１及び第２のハッシュ値は、予め決められた個数のブロックごとに、当該ブロックに格納されたデータに基づいて計算される。

[0207] 本開示の第５の態様に係る情報処理装置は、第１～第４のうちの１つの態様に係る情報処理装置において、

前記記憶領域は、前記記憶領域を論理的に分割した複数の部分領域であって、論理的に連続した複数のブロックをそれぞれ含む複数の部分領域を含み、

前記消去コントローラは、前記複数の部分領域のそれぞれに関して、当該部分領域に含まれる複数のブロックのうち、前記部分領域ごとに異なる割合のブロックを指定し、

前記第１及び第２のハッシュ値は、前記指定された複数のブロックに格納されたデータに基づいて計算される。

[0208] 本開示の第６の態様に係る情報処理装置は、第１～第４のうちの１つの態様に係る情報処理装置において、

前記記憶領域は複数のブロックを含み、

前記第１及び第２のハッシュ値は、論理的に互いに隣接する複数のブロックに格納されたデータに基づいて計算される。

[0209] 本開示の第７の態様に係る情報処理装置は、第１の態様に係る情報処理装置において、

前記記憶領域は、前記記憶領域を互いに異なる複数のサイズで論理的に分

割した複数の部分領域を含み、

前記第１のハッシュ値は、前記複数のサイズを有する前記複数の部分領域のそれぞれに関して、当該部分領域に格納されたデータに基づいて計算され、

前記消去コントローラは、

前記複数のサイズのうち第１のサイズを有する複数の部分領域のそれぞれに関して、当該部分領域に格納されたデータに基づいて前記第２のハッシュ値を計算し、

前記第１のサイズを有する部分領域に関して前記第２のハッシュ値が前記第１のハッシュ値とは異なる場合、前記記憶装置に格納されたデータの消去に成功したことを示す検証結果を出力し、

前記第１のサイズを有する部分領域に関して前記第２のハッシュ値が前記第１のハッシュ値に一致する場合、前記複数のサイズのうち、前記第１のサイズよりも小さい第２のサイズを有する複数の部分領域のそれぞれに関して、当該部分領域に格納されたデータに基づいて前記第２のハッシュ値を計算し、

前記第２のサイズを有する部分領域に関して前記第２のハッシュ値が前記第１のハッシュ値とは異なる場合、前記記憶装置に格納されたデータの消去に成功したことを示す検証結果を出力する。

[0210] 本開示の第８の態様に係る情報処理装置によれば、第１～第７のうちの１つの態様に係る情報処理装置において、

前記検証結果を出力する第１の表示装置を備える。

[0211] 本開示の第９の態様に係る情報処理装置は、第８の態様に係る情報処理装置において、

前記消去コントローラは、前記記憶装置に格納されたデータの消去の進捗度を前記第１の表示装置に出力する。

[0212] 本開示の第１０の態様に係る情報処理システムは、

第１～第９のうちの１つの態様に係る情報処理装置と、

前記情報処理装置に通信回線を介して接続されたサーバ装置とを備え、

前記消去コントローラは、前記サーバ装置から受信された制御信号に従って、前記記憶装置に格納されたデータの消去を制御する。

[0213] 本開示の第１１の態様に係る情報処理システムによれば、第１０の態様に係る情報処理システムにおいて、

前記消去コントローラは、前記検証結果を含む第１の通知信号を前記サーバ装置に送信し、

前記サーバ装置は、前記検証結果を出力する第２の表示装置を備える。

[0214] 本開示の第１２の態様に係る情報処理システムによれば、第１１の態様に係る情報処理システムにおいて、

前記消去コントローラは、前記記憶装置に格納されたデータの消去の進捗度を含む第２の通知信号を前記サーバ装置に送信し、

前記第２の表示装置は前記進捗度を表示する。

[0215] 本開示の第１３の態様に係る情報処理方法は、

自己暗号化機能を有する記憶装置に格納されたデータの消去を制御する情報処理方法であって、

前記記憶装置は、

記憶領域を有する記憶媒体と、

暗号鍵を格納した不揮発性メモリと、

入力されたデータを前記記憶領域に書き込み、前記記憶領域から読み出されたデータを出力し、前記記憶領域に書き込まれるデータの少なくとも一部を前記暗号鍵を用いて暗号化し、前記記憶領域から読み出されたデータの少なくとも一部を前記暗号鍵を用いて復号する入出力コントローラとを備え、

前記情報処理方法は、

前記不揮発性メモリに第１の暗号鍵が格納されている場合、前記記憶領域の指定された位置に格納されるべきデータに基づいて、又は、前記記憶領域の指定された位置に格納されているデータに基づいて計算された第１のハッシュ値を取得するステップと、

前記不揮発性メモリに格納された前記第１の暗号鍵を第２の暗号鍵に変更するように前記記憶装置を制御するステップと、

前記不揮発性メモリに前記第２の暗号鍵が格納されている場合、前記記憶領域の前記指定された位置から読み出されたデータに基づいて第２のハッシュ値を計算するステップと、

前記第２のハッシュ値が前記第１のハッシュ値とは異なる場合、前記記憶装置に格納されたデータの消去に成功したことを示す検証結果を出力するステップと、

前記第２のハッシュ値が前記第１のハッシュ値に一致する場合、前記記憶装置に格納されたデータの消去に失敗したことを示す検証結果を出力するステップとを含む。

[0216] 本開示の第１３の態様に係るプログラムは、

情報処理装置に実装されたプロセッサによって実行される命令を含むプログラムであって、

前記情報処理装置は、格納されるデータの自己暗号化機能を有する記憶装置をさらに備え、

前記記憶装置は、

記憶領域を有する記憶媒体と、

暗号鍵を格納した不揮発性メモリと、

入力されたデータを前記記憶領域に書き込み、前記記憶領域から読み出されたデータを出力し、前記記憶領域に書き込まれるデータの少なくとも一部を前記暗号鍵を用いて暗号化し、前記記憶領域から読み出されたデータの少なくとも一部を前記暗号鍵を用いて復号する入出力コントローラとを備え、

前記命令は、前記プロセッサに、

前記不揮発性メモリに第１の暗号鍵が格納されている場合、前記記憶領域の指定された位置に格納されるべきデータに基づいて、又は、前記記憶領域の指定された位置に格納されているデータに基づいて計算された第１のハッシュ値を取得することと、

前記不揮発性メモリに格納された前記第１の暗号鍵を第２の暗号鍵に変更するように前記記憶装置を制御することと、

前記不揮発性メモリに前記第２の暗号鍵が格納されている場合、前記記憶領域の前記指定された位置から読み出されたデータに基づいて第２のハッシュ値を計算することと、

前記第２のハッシュ値が前記第１のハッシュ値とは異なる場合、前記記憶装置に格納されたデータの消去に成功したことを示す検証結果を出力することと、

前記第２のハッシュ値が前記第１のハッシュ値に一致する場合、前記記憶装置に格納されたデータの消去に失敗したことを示す検証結果を出力することとを実行させる。

産業上の利用可能性

[0217] 本開示の一態様に係る情報処理装置は、自己暗号化機能を有する記憶装置に格納されたデータの消去に成功したか否かを検証することに有用である。

符号の説明

[0218] １，１Ａ　情報処理装置

１０　バス

１１　中央処理装置（ＣＰＵ）

１２　ランダムアクセスメモリ（ＲＡＭ）

１３　記憶装置

１４　消去コントローラ

１５　不揮発性メモリ

１６　通信装置

１７　入力装置

１８　表示装置

１９　装置インターフェース（Ｉ／Ｆ）

２１　入出力コントローラ

２２　ランダムアクセスメモリ（ＲＡＭ）

２３　不揮発性メモリ

２４　フラッシュメモリ

３１　論理ブロック

４１　外部記憶装置

１００　情報処理システム

１２０　バス

１２１　中央処理装置（ＣＰＵ）

１２２　ランダムアクセスメモリ（ＲＡＭ）

１２３　記憶装置

１２６　通信装置

１２７　入力装置

１２８　表示装置

請求の範囲

[請求項1] 格納されるデータの自己暗号化機能を有する記憶装置と、

前記記憶装置に格納されたデータの消去を制御する消去コントローラとを備え、

前記記憶装置は、

記憶領域を有する記憶媒体と、

暗号鍵を格納した不揮発性メモリと、

入力されたデータを前記記憶領域に書き込み、前記記憶領域から読み出されたデータを出力し、前記記憶領域に書き込まれるデータの少なくとも一部を前記暗号鍵を用いて暗号化し、前記記憶領域から読み出されたデータの少なくとも一部を前記暗号鍵を用いて復号する入出力コントローラとを備え、

前記消去コントローラは、

前記不揮発性メモリに第１の暗号鍵が格納されている場合、前記記憶領域の指定された位置に格納されるべきデータに基づいて、又は、前記記憶領域の指定された位置に格納されているデータに基づいて計算された第１のハッシュ値を取得し、

前記不揮発性メモリに格納された前記第１の暗号鍵を第２の暗号鍵に変更するように前記記憶装置を制御し、

前記不揮発性メモリに前記第２の暗号鍵が格納されている場合、前記記憶領域の前記指定された位置から読み出されたデータに基づいて第２のハッシュ値を計算し、

前記第２のハッシュ値が前記第１のハッシュ値とは異なる場合、前記記憶装置に格納されたデータの消去に成功したことを示す検証結果を出力し、

前記第２のハッシュ値が前記第１のハッシュ値に一致する場合、前記記憶装置に格納されたデータの消去に失敗したことを示す検証結果を出力する、

情報処理装置。

[請求項2] 前記消去コントローラは、予め決められたパターンデータを前記記憶領域の前記指定された位置に格納するように前記記憶装置を制御し、

前記第１のハッシュ値は、前記パターンデータに基づいて計算される、

請求項１記載の情報処理装置。

[請求項3] 前記消去コントローラは、前記記憶領域の前記指定された位置から読み出されたデータに基づいて、前記第１のハッシュ値を計算する、

請求項１記載の情報処理装置。

[請求項4] 前記記憶領域は複数のブロックを含み、

前記第１及び第２のハッシュ値は、予め決められた個数のブロックごとに、当該ブロックに格納されたデータに基づいて計算される、

請求項３記載の情報処理装置。

[請求項5] 前記記憶領域は、前記記憶領域を論理的に分割した複数の部分領域であって、論理的に連続した複数のブロックをそれぞれ含む複数の部分領域を含み、

前記消去コントローラは、前記複数の部分領域のそれぞれに関して、当該部分領域に含まれる複数のブロックのうち、前記部分領域ごとに異なる割合のブロックを指定し、

前記第１及び第２のハッシュ値は、前記指定された複数のブロックに格納されたデータに基づいて計算される、

請求項１～４のうちの１つに記載の情報処理装置。

[請求項6] 前記記憶領域は複数のブロックを含み、

前記第１及び第２のハッシュ値は、論理的に互いに隣接する複数のブロックに格納されたデータに基づいて計算される、

請求項１～４のうちの１つに記載の情報処理装置。

[請求項7] 前記記憶領域は、前記記憶領域を互いに異なる複数のサイズで論理

的に分割した複数の部分領域を含み、

前記第１のハッシュ値は、前記複数のサイズを有する前記複数の部分領域のそれぞれに関して、当該部分領域に格納されたデータに基づいて計算され、

前記消去コントローラは、

前記複数のサイズのうち第１のサイズを有する複数の部分領域のそれぞれに関して、当該部分領域に格納されたデータに基づいて前記第２のハッシュ値を計算し、

前記第１のサイズを有する部分領域に関して前記第２のハッシュ値が前記第１のハッシュ値とは異なる場合、前記記憶装置に格納されたデータの消去に成功したことを示す検証結果を出力し、

前記第１のサイズを有する部分領域に関して前記第２のハッシュ値が前記第１のハッシュ値に一致する場合、前記複数のサイズのうち、前記第１のサイズよりも小さい第２のサイズを有する複数の部分領域のそれぞれに関して、当該部分領域に格納されたデータに基づいて前記第２のハッシュ値を計算し、

前記第２のサイズを有する部分領域に関して前記第２のハッシュ値が前記第１のハッシュ値とは異なる場合、前記記憶装置に格納されたデータの消去に成功したことを示す検証結果を出力する、

請求項１記載の情報処理装置。

[請求項8] 前記検証結果を出力する第１の表示装置を備える、

請求項１記載の情報処理装置。

[請求項9] 前記消去コントローラは、前記記憶装置に格納されたデータの消去の進捗度を前記第１の表示装置に出力する、

請求項８記載の情報処理装置。

[請求項10] 請求項１記載の情報処理装置と、

前記情報処理装置に通信回線を介して接続されたサーバ装置とを備える情報処理システムであって、

前記消去コントローラは、前記サーバ装置から受信された制御信号に従って、前記記憶装置に格納されたデータの消去を制御する、

情報処理システム。

[請求項11] 前記消去コントローラは、前記検証結果を含む第１の通知信号を前記サーバ装置に送信し、

前記サーバ装置は、前記検証結果を出力する第２の表示装置を備える、

請求項１０記載の情報処理システム。

[請求項12] 前記消去コントローラは、前記記憶装置に格納されたデータの消去の進捗度を含む第２の通知信号を前記サーバ装置に送信し、

前記第２の表示装置は前記進捗度を表示する、

請求項１１記載の情報処理システム。

[請求項13] 自己暗号化機能を有する記憶装置に格納されたデータの消去を制御する情報処理方法であって、

前記記憶装置は、

記憶領域を有する記憶媒体と、

暗号鍵を格納した不揮発性メモリと、

入力されたデータを前記記憶領域に書き込み、前記記憶領域から読み出されたデータを出力し、前記記憶領域に書き込まれるデータの少なくとも一部を前記暗号鍵を用いて暗号化し、前記記憶領域から読み出されたデータの少なくとも一部を前記暗号鍵を用いて復号する入出力コントローラとを備え、

前記情報処理方法は、

前記不揮発性メモリに第１の暗号鍵が格納されている場合、前記記憶領域の指定された位置に格納されるべきデータに基づいて、又は、前記記憶領域の指定された位置に格納されているデータに基づいて計算された第１のハッシュ値を取得するステップと、

前記不揮発性メモリに格納された前記第１の暗号鍵を第２の暗号鍵

に変更するように前記記憶装置を制御するステップと、

前記不揮発性メモリに前記第２の暗号鍵が格納されている場合、前記記憶領域の前記指定された位置から読み出されたデータに基づいて第２のハッシュ値を計算するステップと、

前記第２のハッシュ値が前記第１のハッシュ値とは異なる場合、前記記憶装置に格納されたデータの消去に成功したことを示す検証結果を出力するステップと、

前記第２のハッシュ値が前記第１のハッシュ値に一致する場合、前記記憶装置に格納されたデータの消去に失敗したことを示す検証結果を出力するステップとを含む、

情報処理方法。

[請求項14] 情報処理装置に実装されたプロセッサによって実行される命令を含むプログラムであって、

前記情報処理装置は、格納されるデータの自己暗号化機能を有する記憶装置をさらに備え、

前記記憶装置は、

記憶領域を有する記憶媒体と、

暗号鍵を格納した不揮発性メモリと、

入力されたデータを前記記憶領域に書き込み、前記記憶領域から読み出されたデータを出力し、前記記憶領域に書き込まれるデータの少なくとも一部を前記暗号鍵を用いて暗号化し、前記記憶領域から読み出されたデータの少なくとも一部を前記暗号鍵を用いて復号する入出力コントローラとを備え、

前記命令は、前記プロセッサに、

前記不揮発性メモリに第１の暗号鍵が格納されている場合、前記記憶領域の指定された位置に格納されるべきデータに基づいて、又は、前記記憶領域の指定された位置に格納されているデータに基づいて計算された第１のハッシュ値を取得することと、

前記不揮発性メモリに格納された前記第１の暗号鍵を第２の暗号鍵に変更するように前記記憶装置を制御することと、

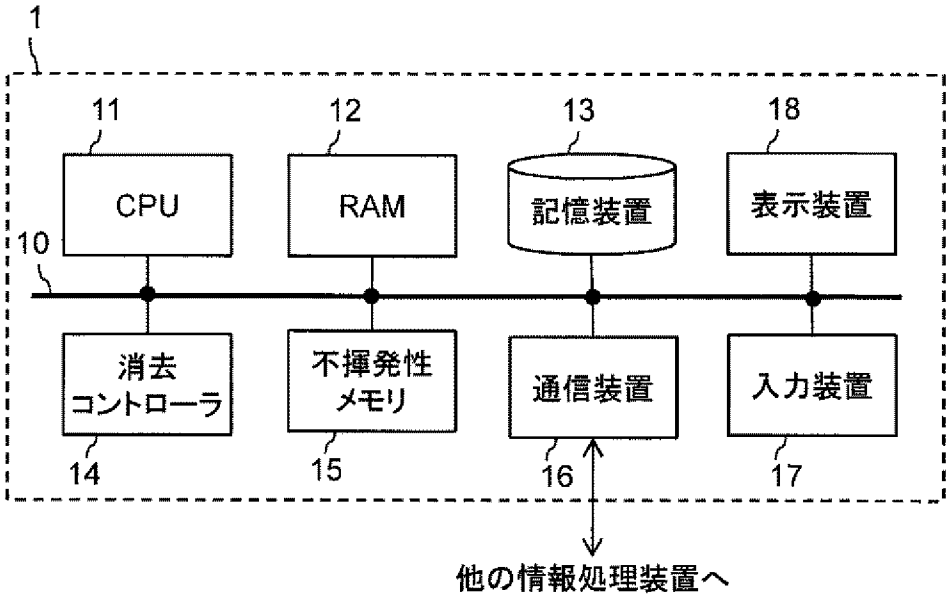
前記不揮発性メモリに前記第２の暗号鍵が格納されている場合、前記記憶領域の前記指定された位置から読み出されたデータに基づいて第２のハッシュ値を計算することと、

前記第２のハッシュ値が前記第１のハッシュ値とは異なる場合、前記記憶装置に格納されたデータの消去に成功したことを示す検証結果を出力することと、

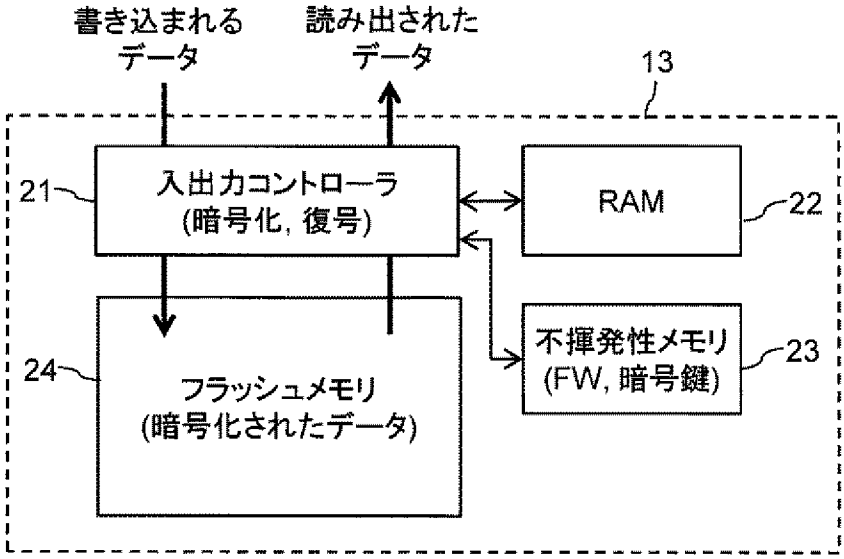
前記第２のハッシュ値が前記第１のハッシュ値に一致する場合、前記記憶装置に格納されたデータの消去に失敗したことを示す検証結果を出力することとを実行させる、

プログラム。

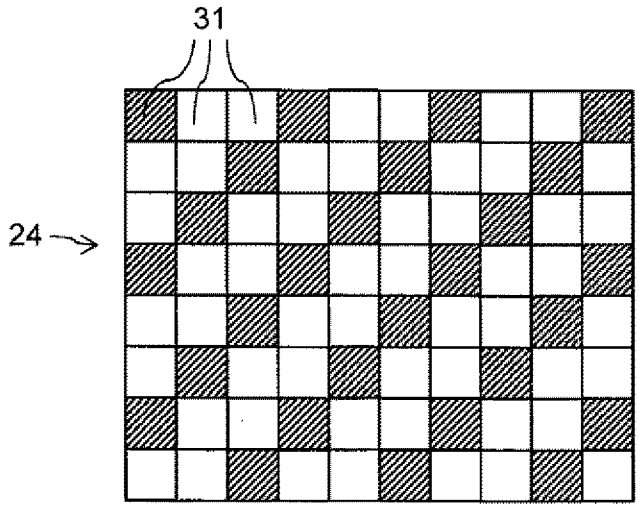
[図1]


1
11
CPU
12
RAM
13
記憶装置
18
表示装置
10
消去
コントローラ
14
不揮発性
メモリ
15
通信装置
16
入力装置
17
他の情報処理装置へ

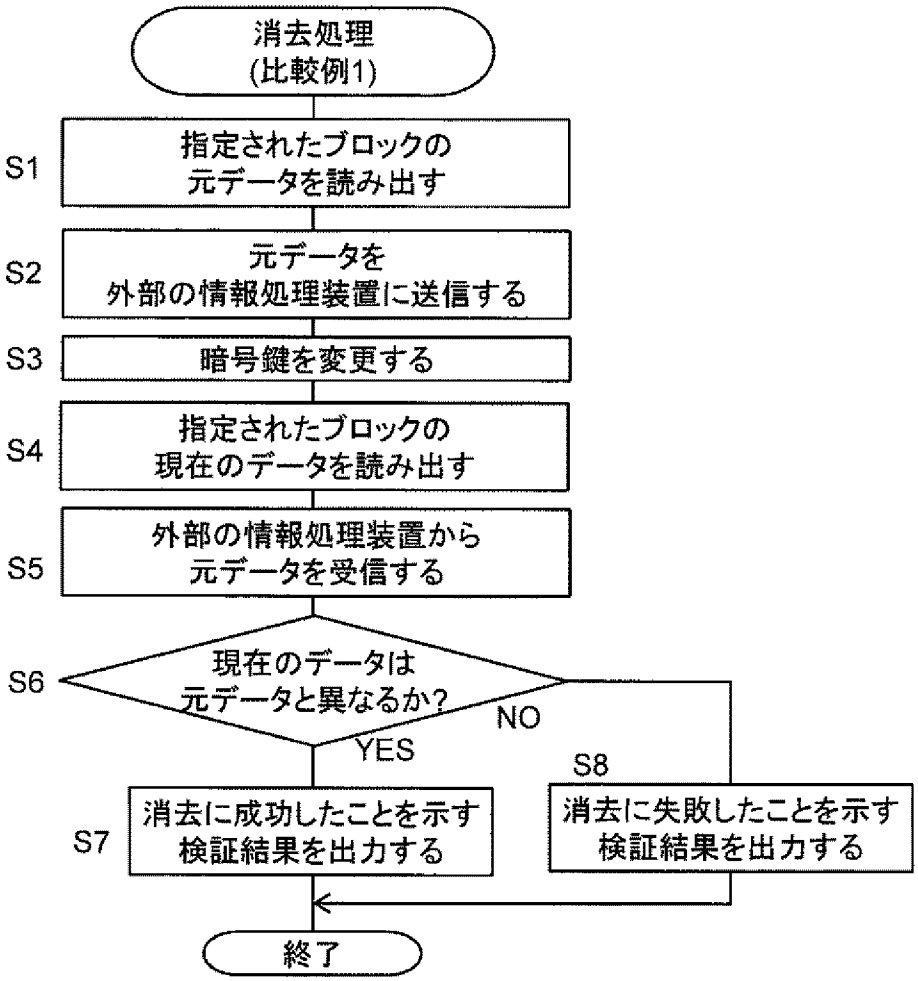
[図2]


書き込まれる
データ
読み出された
データ
13
21
入出力コントローラ
(暗号化, 復号)
RAM
22
24
フラッシュメモリ
(暗号化されたデータ)
不揮発性メモリ
(FW, 暗号鍵)
23

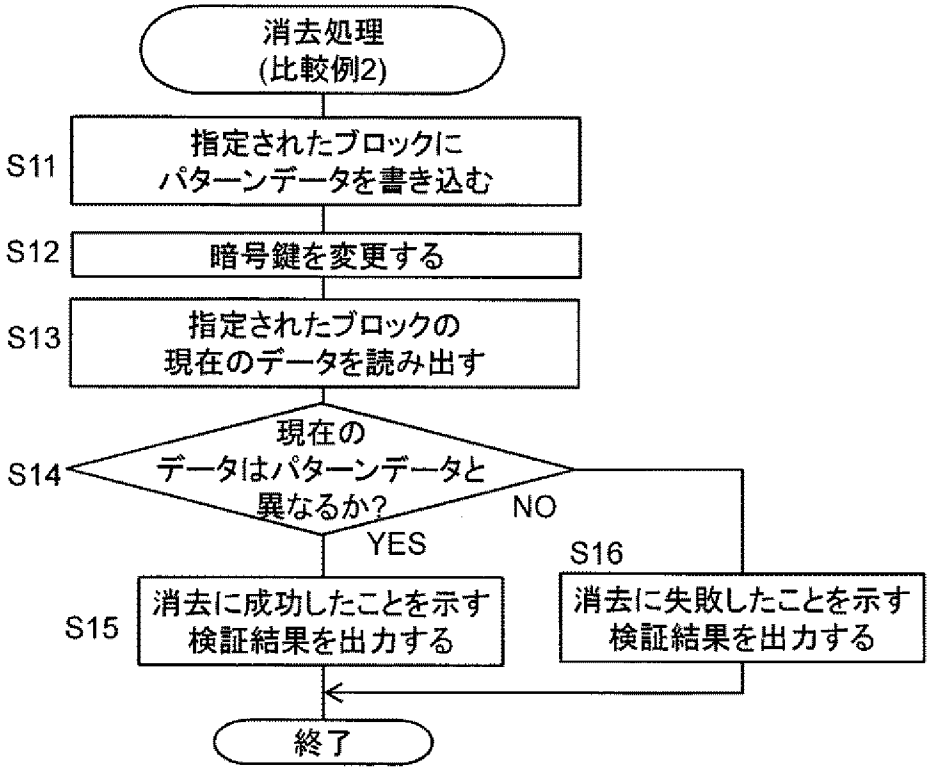
[図3]


31
24

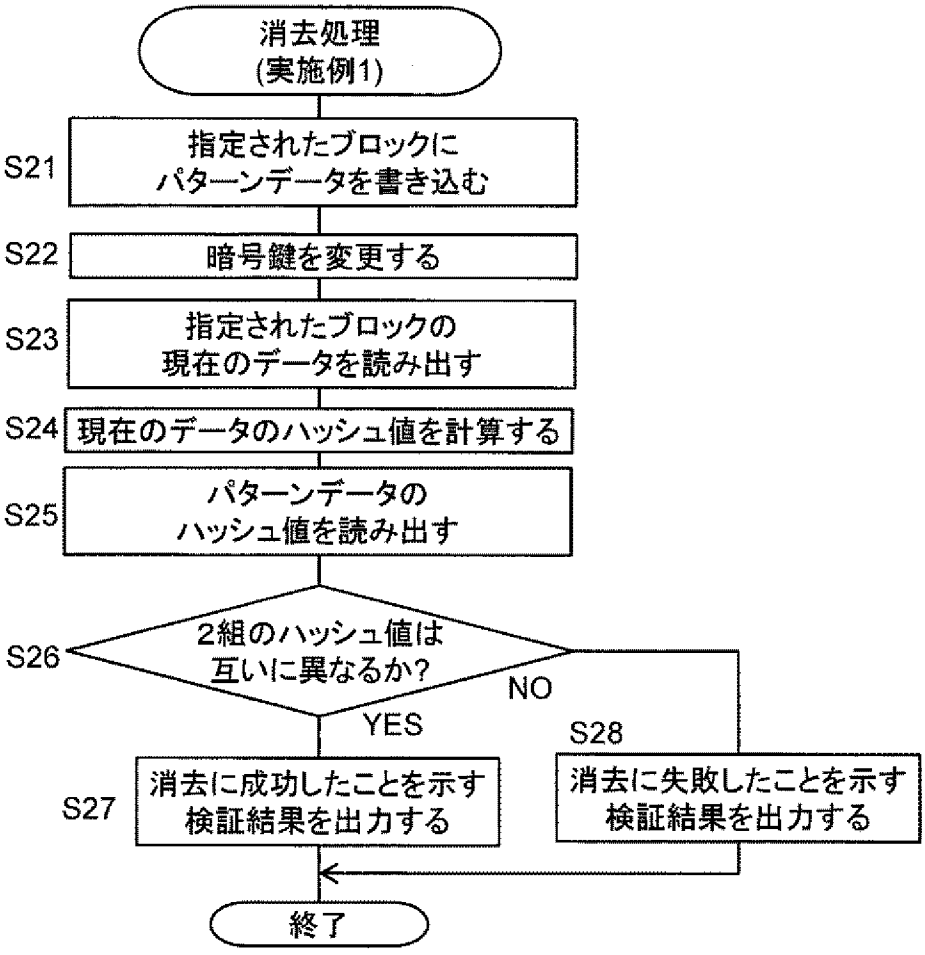
[図4]


消去処理
(比較例1)
S1
指定されたブロックの
元データを読み出す
S2
元データを
外部の情報処理装置に送信する
S3
暗号鍵を変更する
S4
指定されたブロックの
現在のデータを読み出す
S5
外部の情報処理装置から
元データを受信する
S6
現在のデータは
元データと異なるか?
NO
YES
S8
消去に失敗したことを示す
検証結果を出力する
S7
消去に成功したことを示す
検証結果を出力する
終了

[図5]


消去処理
(比較例2)
S11
指定されたブロックに
パターンデータを書き込む
S12
暗号鍵を変更する
S13
指定されたブロックの
現在のデータを読み出す
S14
現在の
データはパターンデータと
異なるか?
NO
YES
S16
S15
消去に成功したことを示す
検証結果を出力する
消去に失敗したことを示す
検証結果を出力する
終了

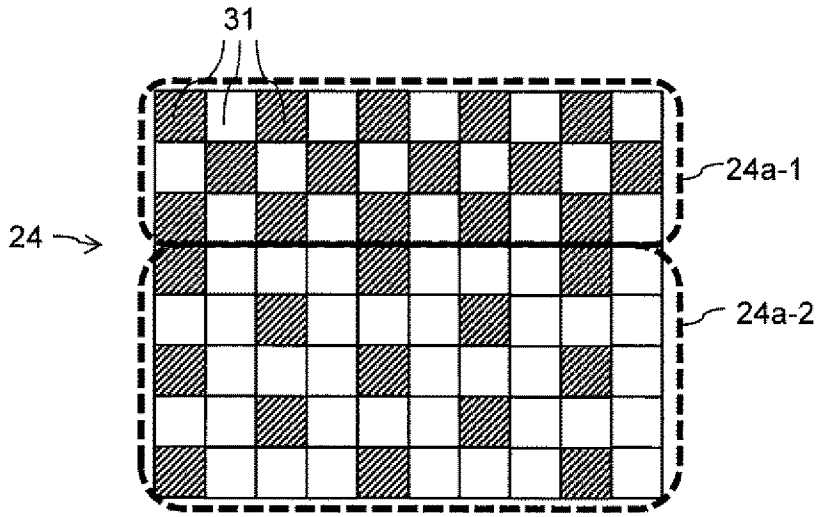
[図6]


消去処理
(実施例1)
S21
指定されたブロックに
パターンデータを書き込む
S22
暗号鍵を変更する
S23
指定されたブロックの
現在のデータを読み出す
S24
現在のデータのハッシュ値を計算する
S25
パターンデータの
ハッシュ値を読み出す
S26
2組のハッシュ値は
互いに異なるか?
NO
YES
S28
S27
消去に成功したことを示す
検証結果を出力する
消去に失敗したことを示す
検証結果を出力する
終了

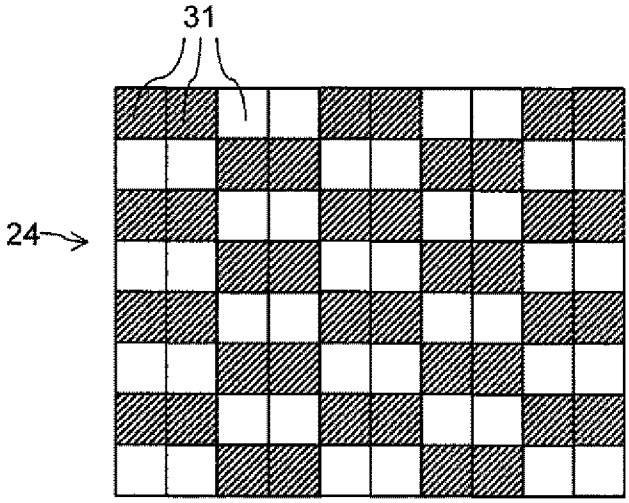
[図7]

検証方法	退避データ量	書き込みデータ量	読み出しデータ量	比較データ量
比較例1	100 GB	0	100 GB	100 GB
比較例2	0	100 GB	100 GB	100 GB
実施例1	0	100 GB	100 GB	32 KB

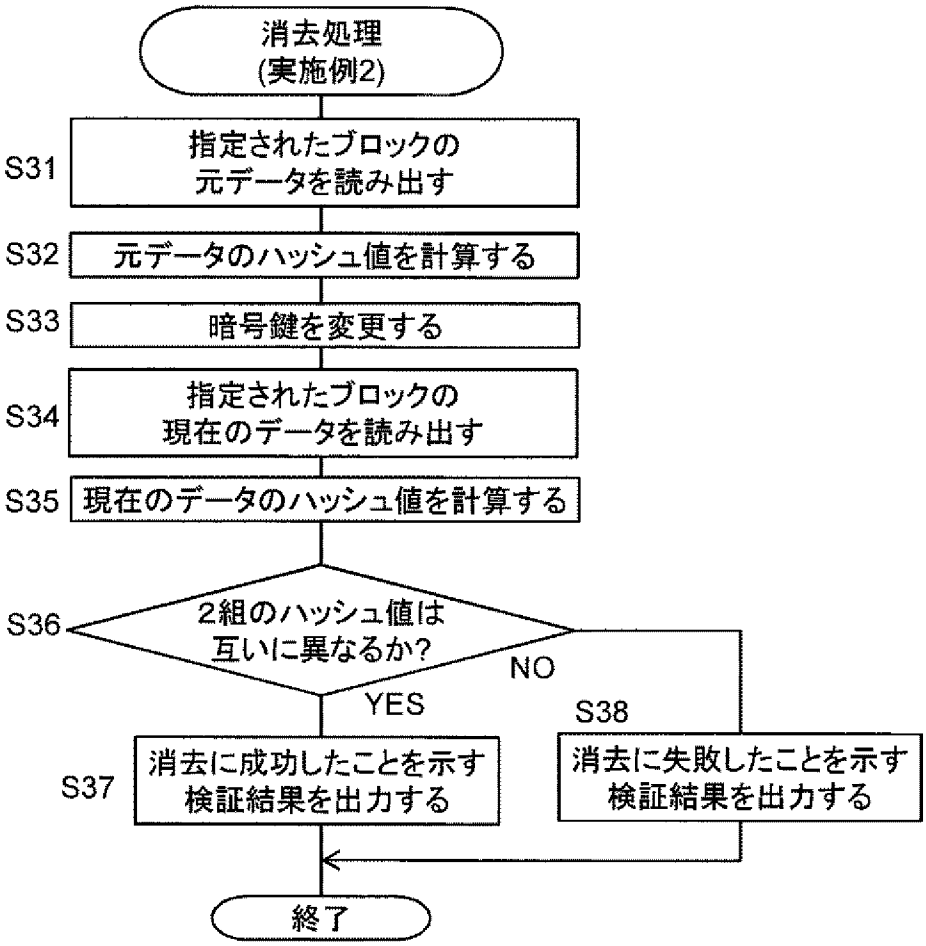
[図8]



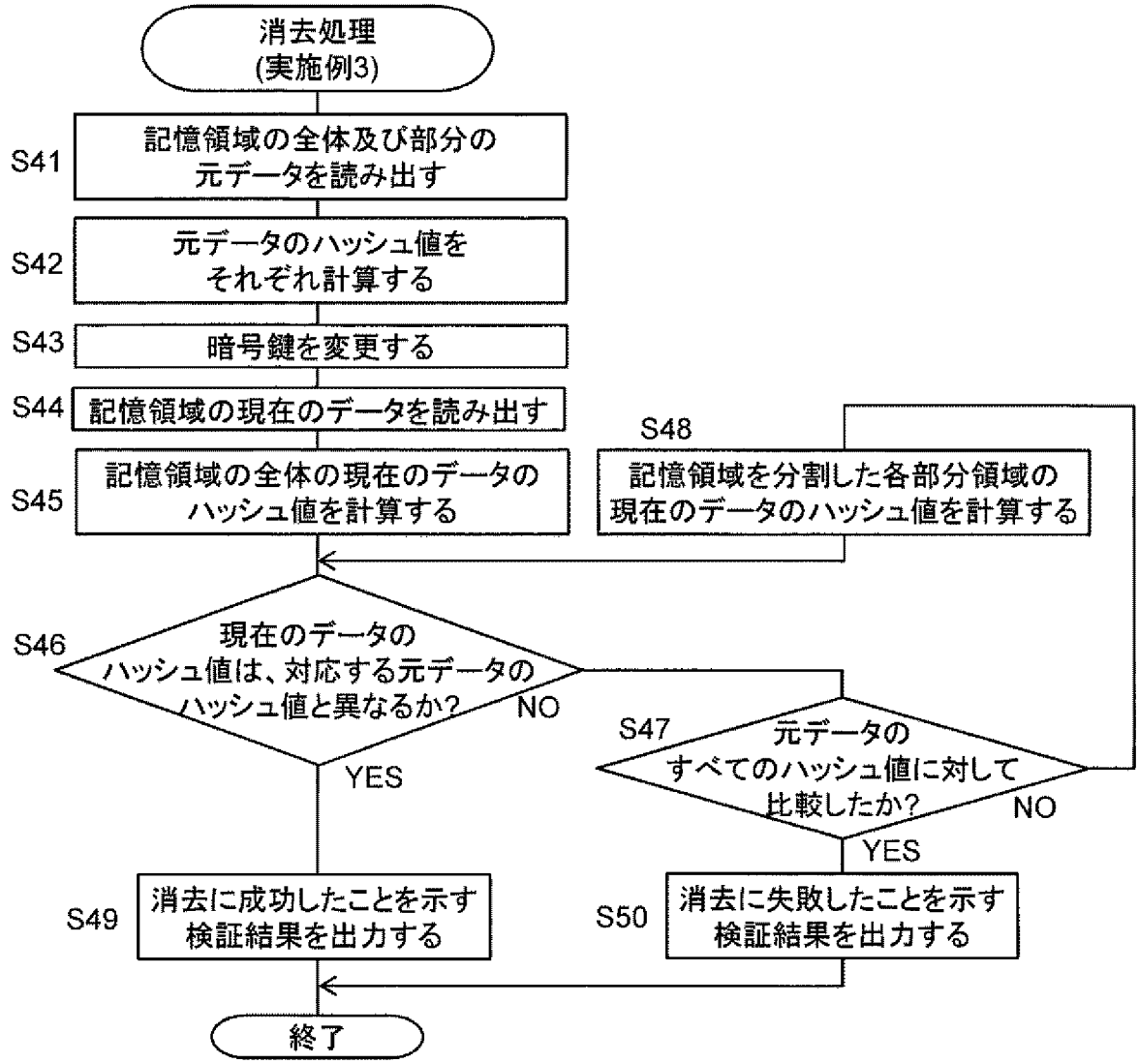
[図9]



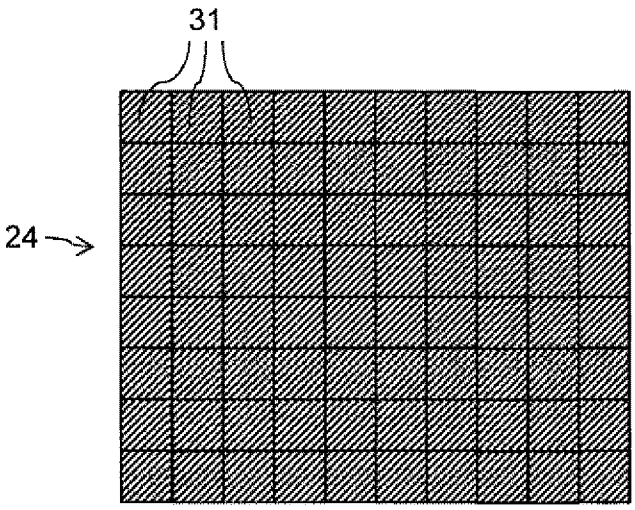
[図10]


消去処理
(実施例2)
S31
指定されたブロックの
元データを読み出す
S32
元データのハッシュ値を計算する
S33
暗号鍵を変更する
S34
指定されたブロックの
現在のデータを読み出す
S35
現在のデータのハッシュ値を計算する
S36
2組のハッシュ値は
互いに異なるか?
NO
YES
S38
消去に失敗したことを示す
検証結果を出力する
S37
消去に成功したことを示す
検証結果を出力する
終了

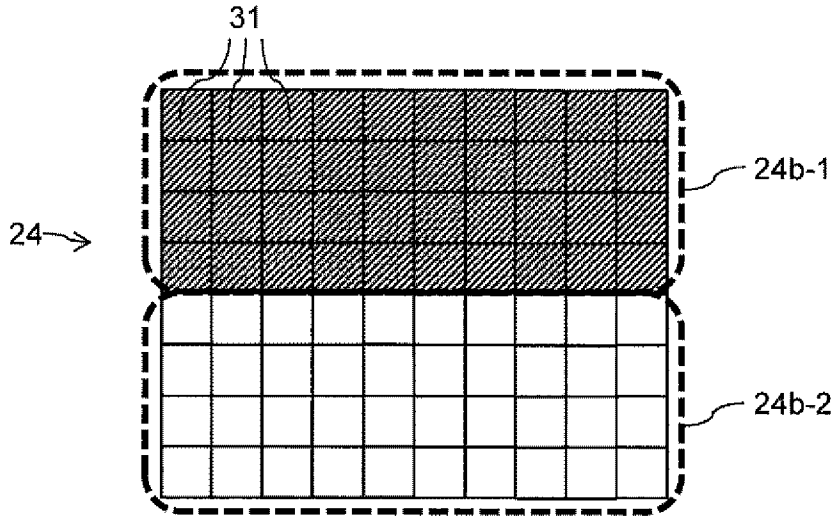
[図11]


消去処理
(実施例3)
S41
記憶領域の全体及び部分の
元データを読み出す
S42
元データのハッシュ値を
それぞれ計算する
S43
暗号鍵を変更する
S44
記憶領域の現在のデータを読み出す
S45
記憶領域の全体の現在のデータの
ハッシュ値を計算する
S48
記憶領域を分割した各部分領域の
現在のデータのハッシュ値を計算する
S46
現在のデータの
ハッシュ値は、対応する元データの
ハッシュ値と異なるか?
NO
YES
S47
元データの
すべてのハッシュ値に対して
比較したか?
NO
YES
S49
消去に成功したことを示す
検証結果を出力する
S50
消去に失敗したことを示す
検証結果を出力する
終了

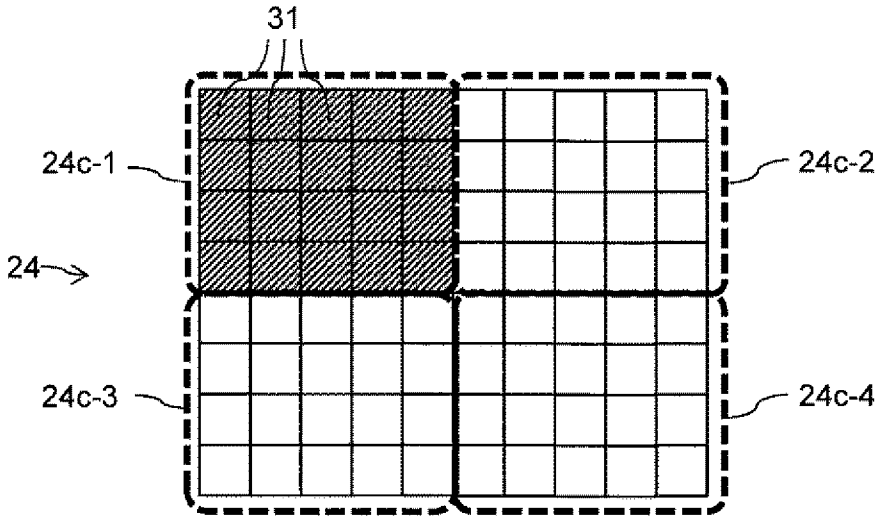
[図12]


31
24

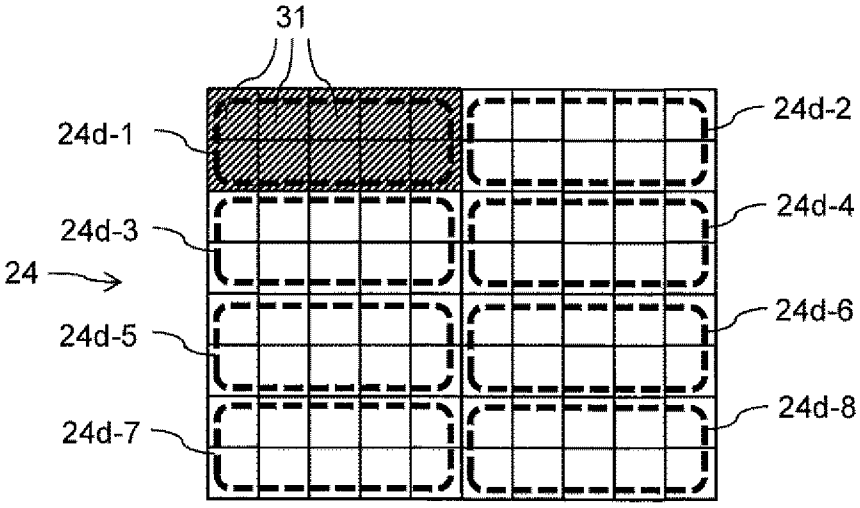
[図13]


31
24
24b-1
24b-2

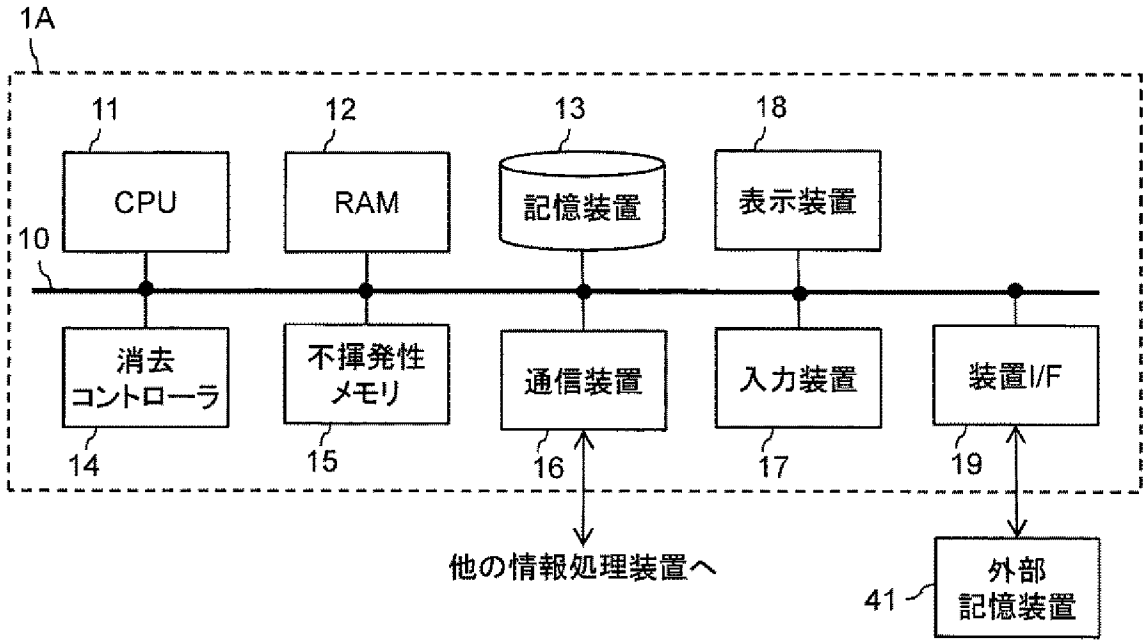
[図14]


31
24c-1
24c-2
24
24c-3
24c-4

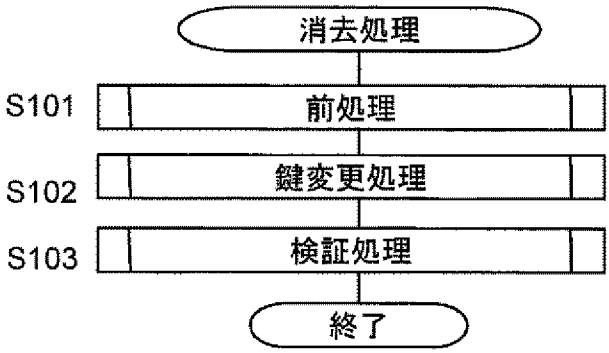
[図15]


31
24d-1
24d-2
24d-3
24d-4
24
24d-5
24d-6
24d-7
24d-8

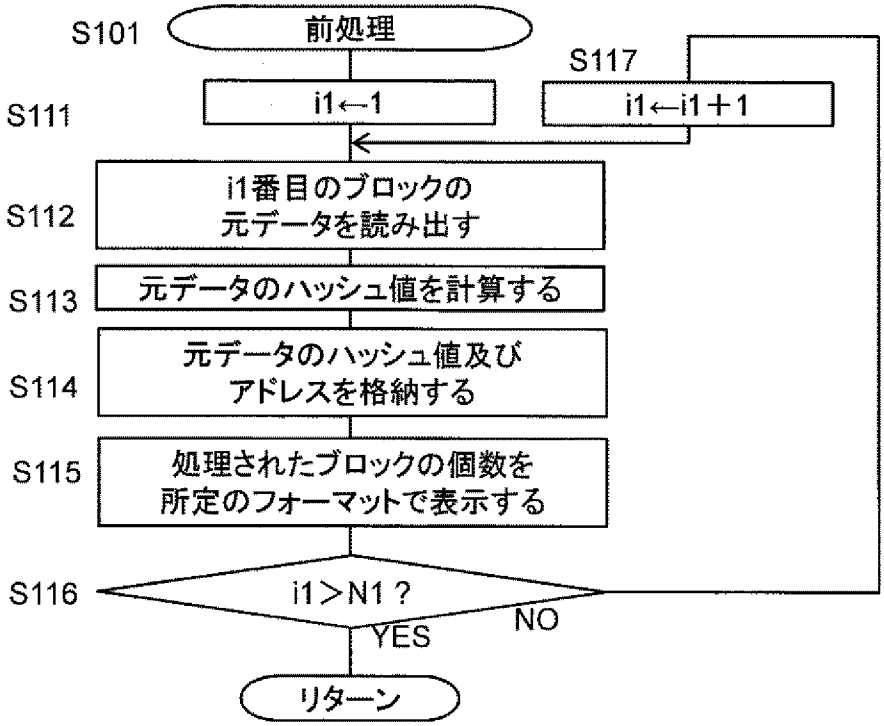
[図16]


1A
11
CPU
12
RAM
13
記憶装置
18
表示装置
10
消去
コントローラ
不揮発性
メモリ
通信装置
入力装置
装置I/F
14
15
16
17
19
他の情報処理装置へ
41
外部
記憶装置

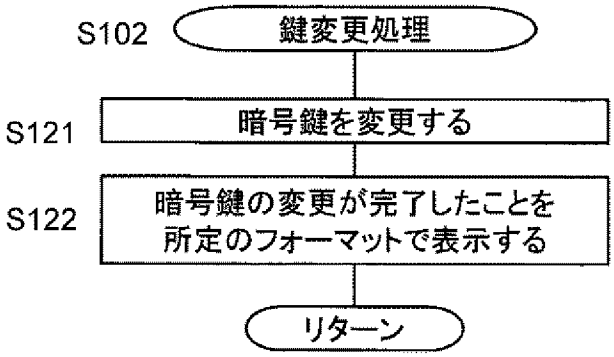
[図17]


消去処理
S101
前処理
S102
鍵変更処理
S103
検証処理
終了

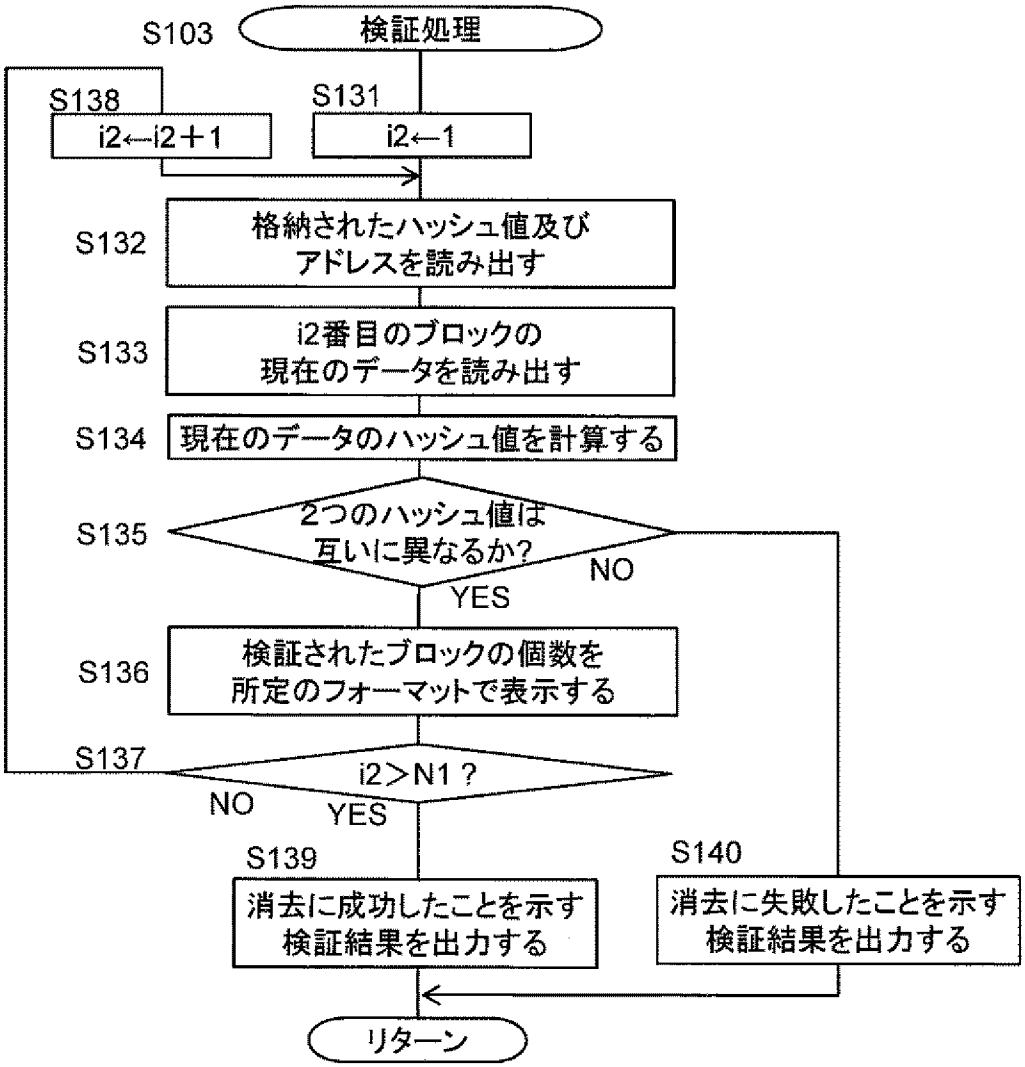
[図18]


S101
前処理
S111
i1←1
S117
i1←i1＋1
S112
i1番目のブロックの
元データを読み出す
S113
元データのハッシュ値を計算する
S114
元データのハッシュ値及び
アドレスを格納する
S115
処理されたブロックの個数を
所定のフォーマットで表示する
S116
i1＞N1？
YES
NO
リターン

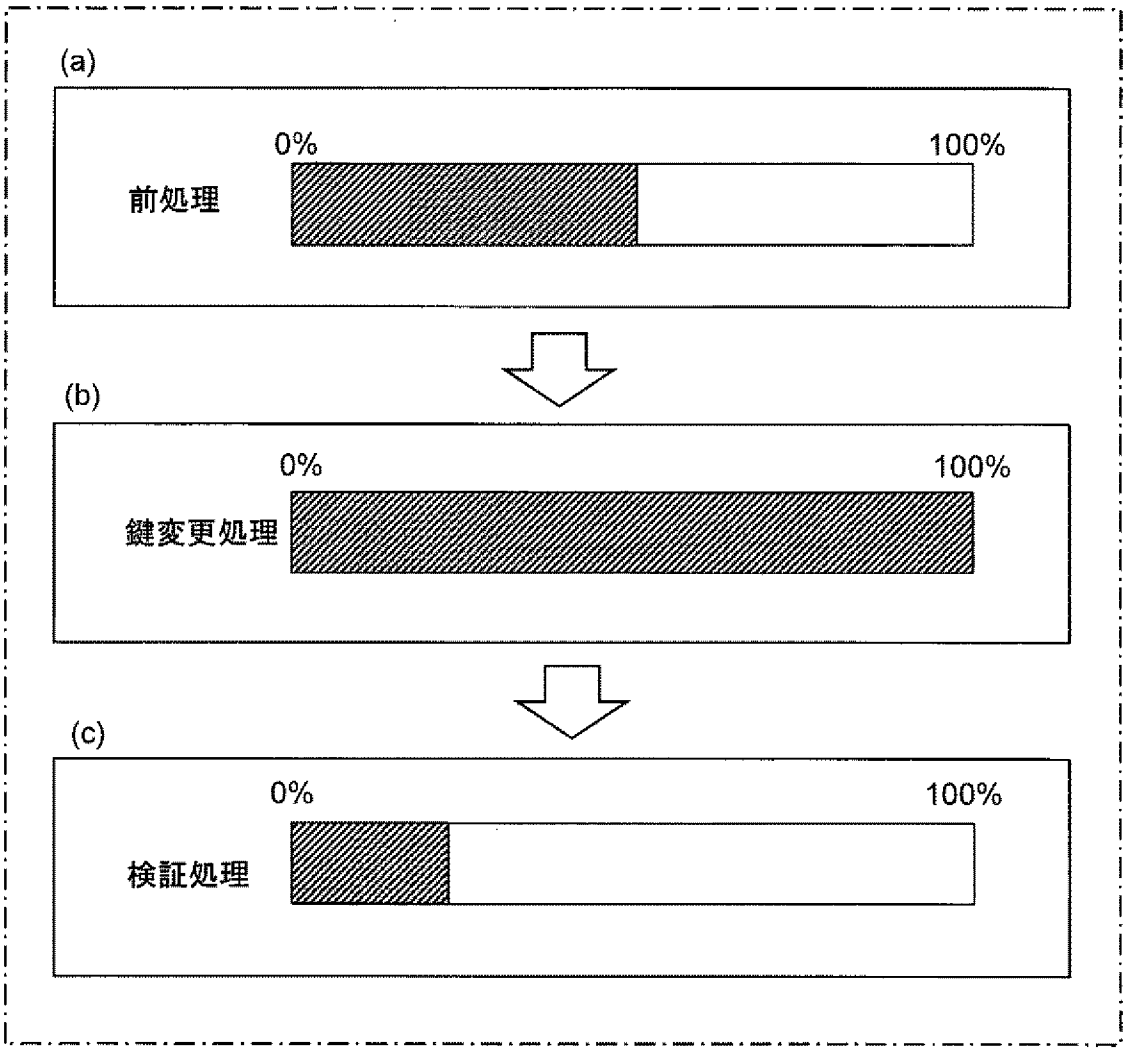
[図19]


S102
鍵変更処理
S121
暗号鍵を変更する
S122
暗号鍵の変更が完了したことを
所定のフォーマットで表示する
リターン

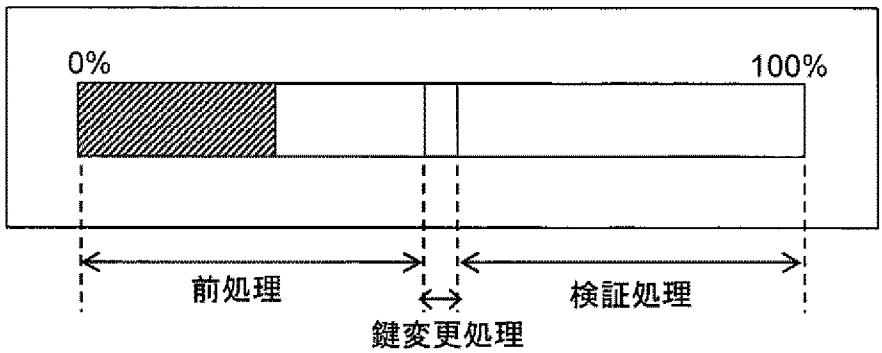
[図20]


S103
検証処理
S138
i2←i2＋1
S131
i2←1
S132
格納されたハッシュ値及び
アドレスを読み出す
S133
i2番目のブロックの
現在のデータを読み出す
S134
現在のデータのハッシュ値を計算する
S135
2つのハッシュ値は
互いに異なるか?
NO
YES
S136
検証されたブロックの個数を
所定のフォーマットで表示する
S137
i2＞N1？
NO
YES
S139
消去に成功したことを示す
検証結果を出力する
S140
消去に失敗したことを示す
検証結果を出力する
リターン

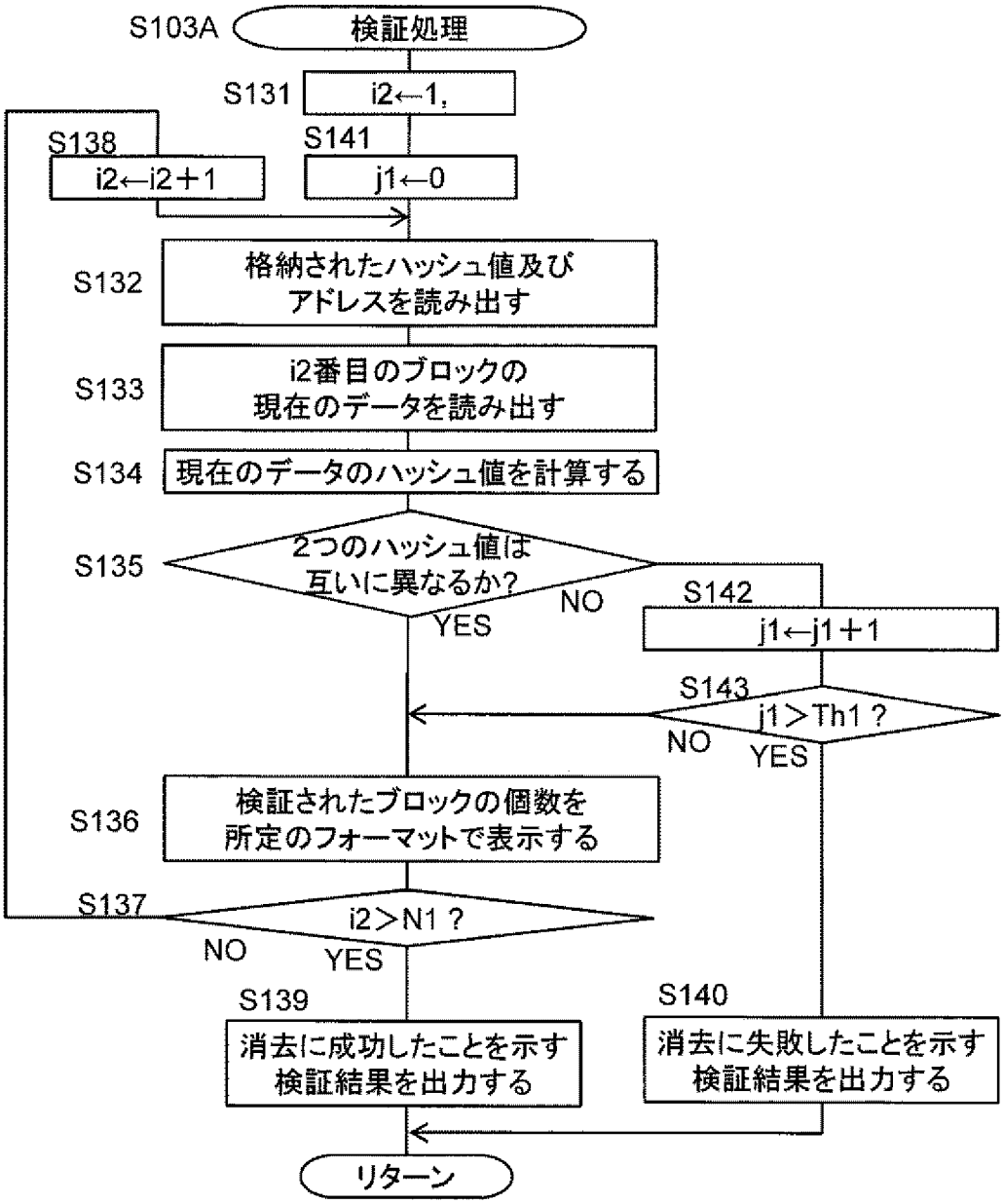
[図21]



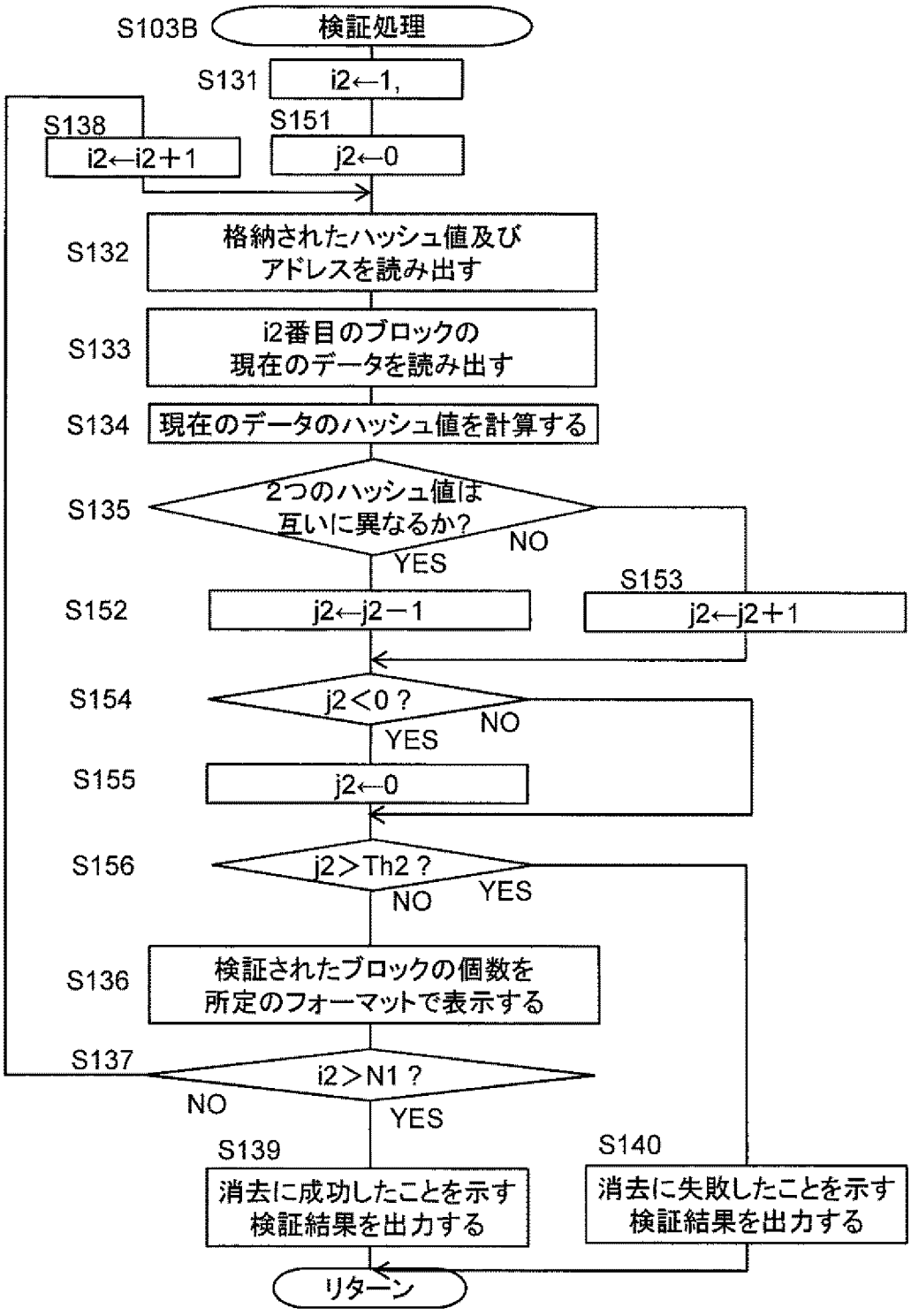
[図22]



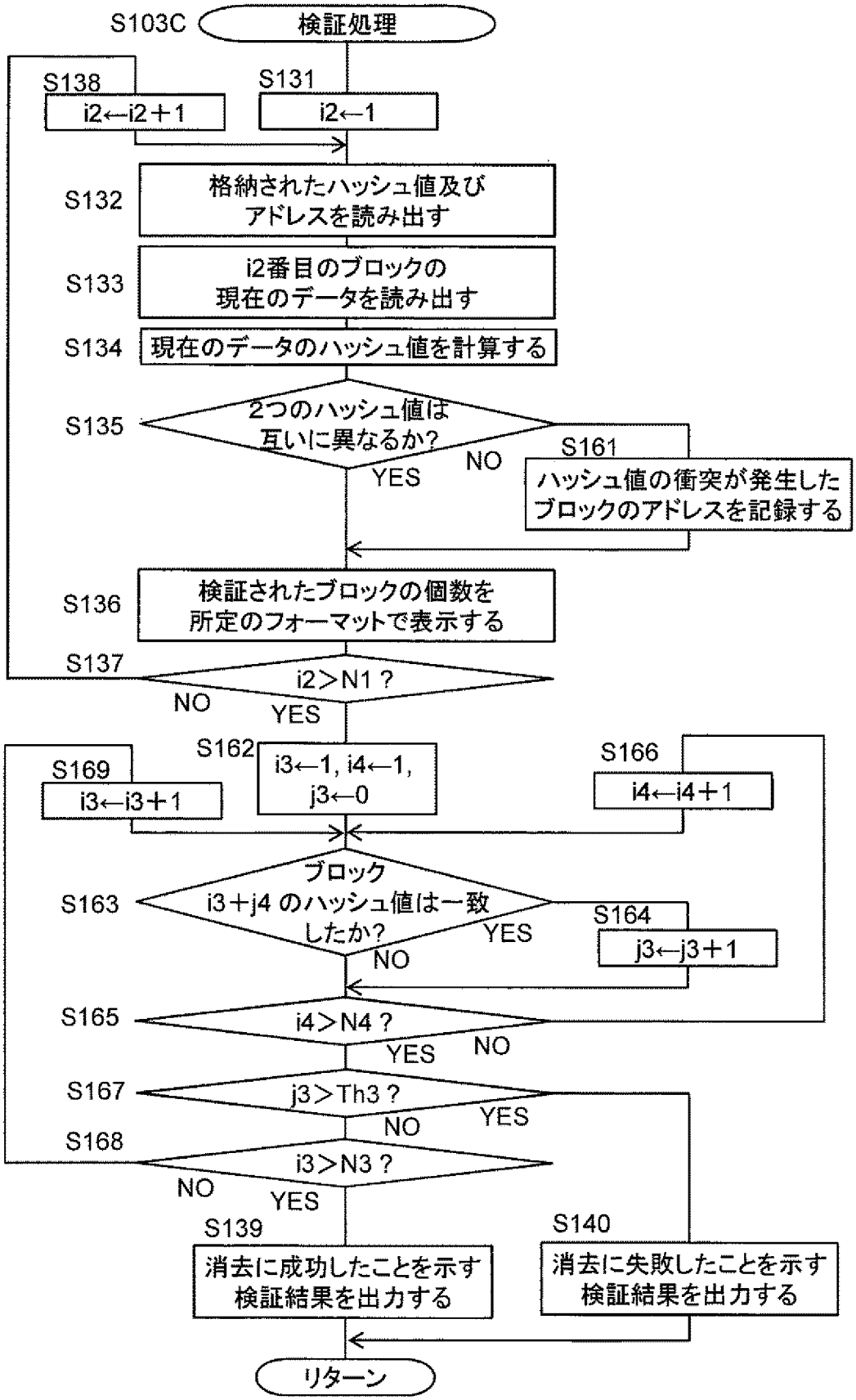
[図23]


S103A
検証処理
S131
i2←1,
S138
i2←i2＋1
S141
j1←0
S132
格納されたハッシュ値及び
アドレスを読み出す
S133
i2番目のブロックの
現在のデータを読み出す
S134
現在のデータのハッシュ値を計算する
S135
2つのハッシュ値は
互いに異なるか?
NO
YES
S142
j1←j1＋1
S143
j1＞Th1？
NO
YES
S136
検証されたブロックの個数を
所定のフォーマットで表示する
S137
i2＞N1？
NO
YES
S139
消去に成功したことを示す
検証結果を出力する
S140
消去に失敗したことを示す
検証結果を出力する
リターン

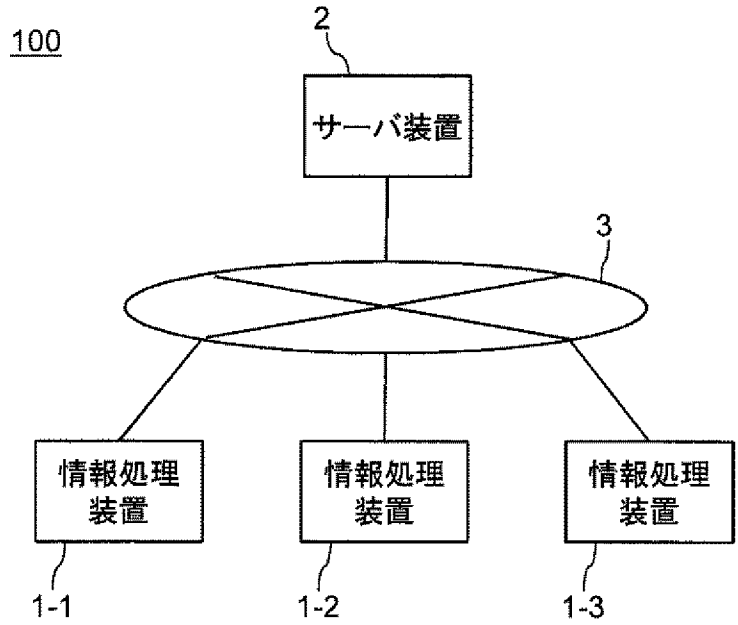
[図24]


S103B
検証処理
S131
i2←1,
S151
j2←0
S138
i2←i2+1
S132
格納されたハッシュ値及び
アドレスを読み出す
S133
i2番目のブロックの
現在のデータを読み出す
S134
現在のデータのハッシュ値を計算する
S135
2つのハッシュ値は
互いに異なるか?
NO
YES
S153
j2←j2+1
S152
j2←j2−1
S154
j2<0 ?
NO
YES
S155
j2←0
S156
j2>Th2 ?
NO
YES
S136
検証されたブロックの個数を
所定のフォーマットで表示する
S137
i2>N1 ?
NO
YES
S139
消去に成功したことを示す
検証結果を出力する
S140
消去に失敗したことを示す
検証結果を出力する
リターン

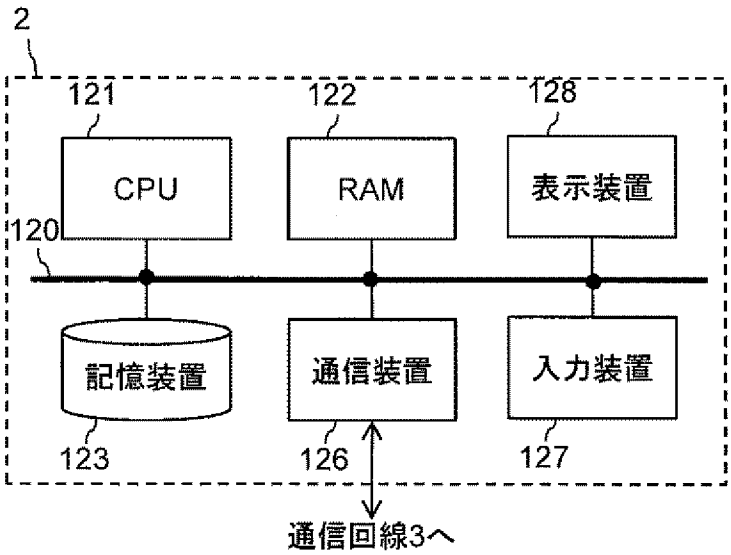
[図25]


S103C
検証処理
S138
i2←i2＋1
S131
i2←1
S132
格納されたハッシュ値及び
アドレスを読み出す
S133
i2番目のブロックの
現在のデータを読み出す
S134
現在のデータのハッシュ値を計算する
S135
2つのハッシュ値は
互いに異なるか?
NO
YES
S161
ハッシュ値の衝突が発生した
ブロックのアドレスを記録する
S136
検証されたブロックの個数を
所定のフォーマットで表示する
S137
i2＞N1？
NO
YES
S162
i3←1, i4←1,
j3←0
S169
i3←i3＋1
S166
i4←i4＋1
S163
ブロック
i3＋j4 のハッシュ値は一致
したか?
YES
NO
S164
j3←j3＋1
S165
i4＞N4？
YES
NO
S167
j3＞Th3？
NO
YES
S168
i3＞N3？
NO
YES
S139
消去に成功したことを示す
検証結果を出力する
S140
消去に失敗したことを示す
検証結果を出力する
リターン

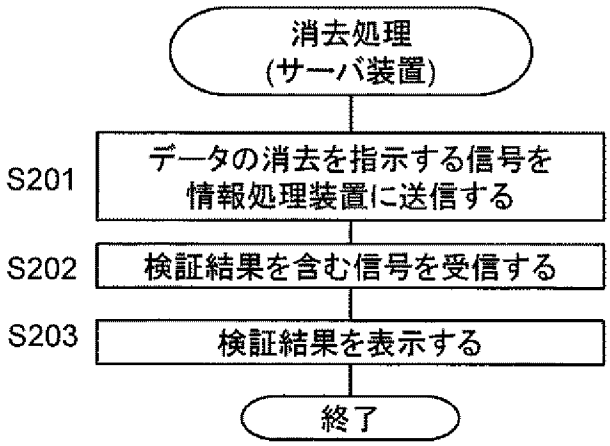
[図26]


100
2
サーバ装置
3
情報処理装置
情報処理装置
情報処理装置
1-1
1-2
1-3

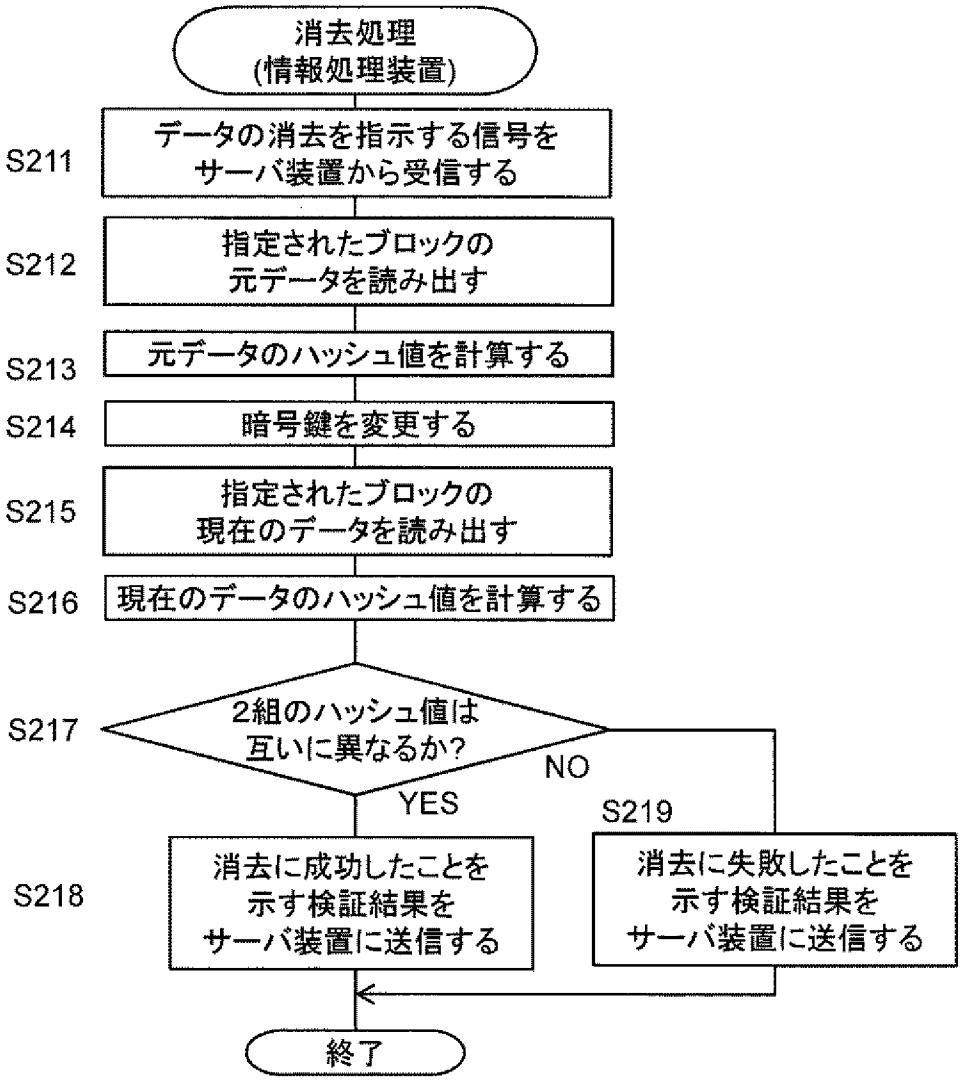
[図27]


2
121
122
128
CPU
RAM
表示装置
120
記憶装置
通信装置
入力装置
123
126
127
通信回線3へ

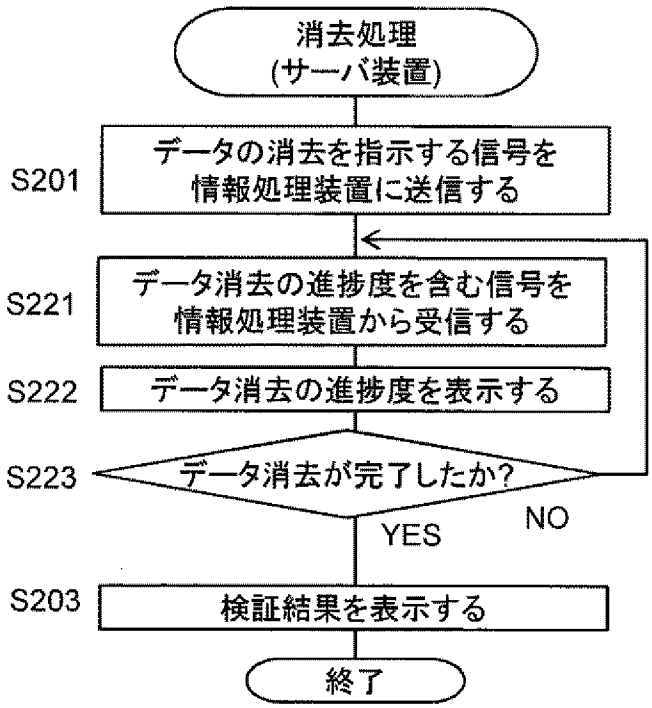
[図28]


消去処理
(サーバ装置)
S201
データの消去を指示する信号を
情報処理装置に送信する
S202
検証結果を含む信号を受信する
S203
検証結果を表示する
終了

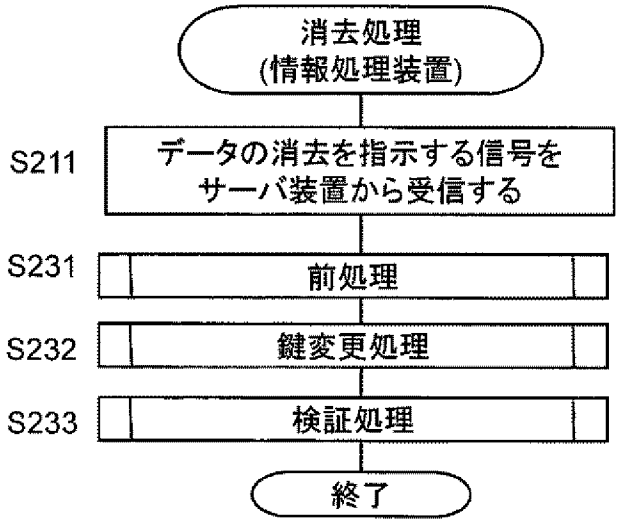
[図29]


消去処理
(情報処理装置)
S211
データの消去を指示する信号を
サーバ装置から受信する
S212
指定されたブロックの
元データを読み出す
S213
元データのハッシュ値を計算する
S214
暗号鍵を変更する
S215
指定されたブロックの
現在のデータを読み出す
S216
現在のデータのハッシュ値を計算する
S217
2組のハッシュ値は
互いに異なるか?
NO
YES
S219
S218
消去に成功したことを
示す検証結果を
サーバ装置に送信する
消去に失敗したことを
示す検証結果を
サーバ装置に送信する
終了

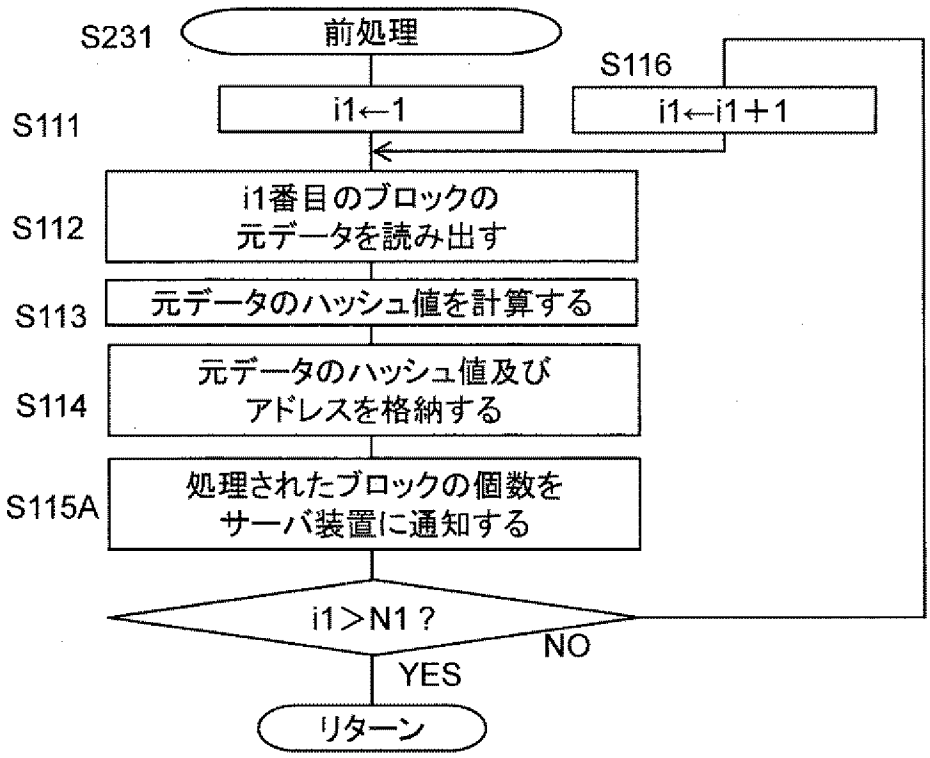
[図30]


消去処理
(サーバ装置)
S201
データの消去を指示する信号を
情報処理装置に送信する
S221
データ消去の進捗度を含む信号を
情報処理装置から受信する
S222
データ消去の進捗度を表示する
S223
データ消去が完了したか?
NO
YES
S203
検証結果を表示する
終了

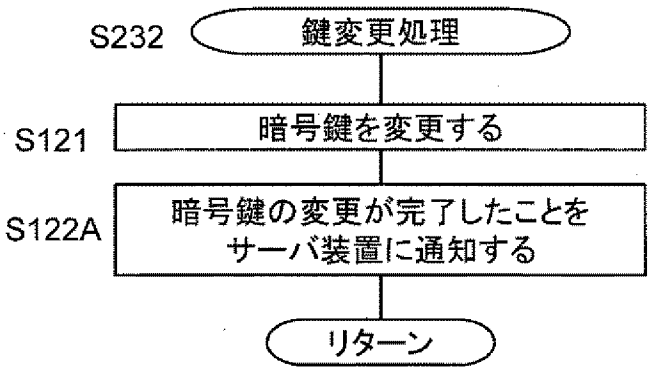
[図31]


消去処理
(情報処理装置)
S211
データの消去を指示する信号を
サーバ装置から受信する
S231
前処理
S232
鍵変更処理
S233
検証処理
終了

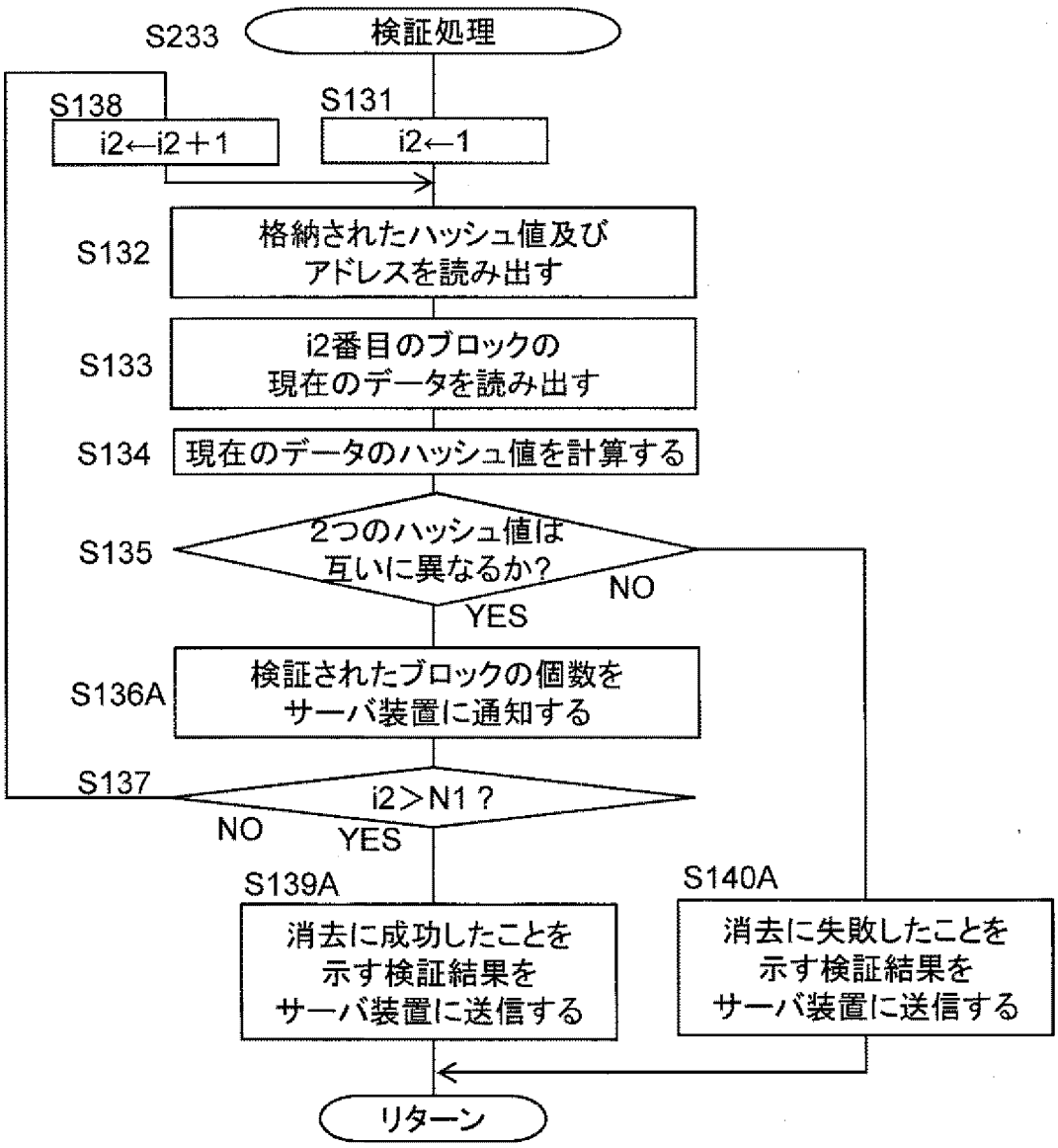
[図32]


S231
前処理
S116
S111
i1←1
i1←i1＋1
S112
i1番目のブロックの
元データを読み出す
S113
元データのハッシュ値を計算する
S114
元データのハッシュ値及び
アドレスを格納する
S115A
処理されたブロックの個数を
サーバ装置に通知する
i1＞N1？
NO
YES
リターン

[図33]


S232
鍵変更処理
S121
暗号鍵を変更する
S122A
暗号鍵の変更が完了したことを
サーバ装置に通知する
リターン

[図34]


S233
検証処理
S138
i2←i2＋1
S131
i2←1
S132
格納されたハッシュ値及び
アドレスを読み出す
S133
i2番目のブロックの
現在のデータを読み出す
S134
現在のデータのハッシュ値を計算する
S135
2つのハッシュ値は
互いに異なるか?
NO
YES
S136A
検証されたブロックの個数を
サーバ装置に通知する
S137
i2＞N1？
NO
YES
S139A
消去に成功したことを
示す検証結果を
サーバ装置に送信する
S140A
消去に失敗したことを
示す検証結果を
サーバ装置に送信する
リターン

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2023/037435

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/60(2013.01)i; ***G06F 21/78***(2013.01)i
FI: G06F21/60; G06F21/60 320; G06F21/78

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)

G06F21/60; G06F21/78

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

Published examined utility model applications of Japan 1922-1996
Published unexamined utility model applications of Japan 1971-2023
Registered utility model specifications of Japan 1996-2023
Published registered utility model applications of Japan 1994-2023

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	US 2008/0082836 A1 (OSAKI, Nobuyuki) 03 April 2008 (2008-04-03) abstract, paragraph [0058]	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
17 November 2023	**28 November 2023**
Name and mailing address of the ISA/JP **Japan Patent Office (ISA/JP)** **3-4-3 Kasumigaseki, Chiyoda-ku, Tokyo 100-8915** **Japan**	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/JP2023/037435

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
US 2008/0082836 A1	03 April 2008	(Family: none)	

国際調査報告

国際出願番号
PCT/JP2023/037435

A. 発明の属する分野の分類（国際特許分類（ＩＰＣ））

G06F 21/60(2013.01)i; G06F 21/78(2013.01)i
FI: G06F21/60; G06F21/60 320; G06F21/78

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））

G06F21/60; G06F21/78

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	１９７１－２０２３年
日本国実用新案登録公報	１９９６－２０２３年
日本国登録実用新案公報	１９９４－２０２３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	US 2008/0082836 A1 (OSAKI, Nobuyuki) 03.04.2008 (2008-04-03) ABSTRACT, par. [0058]	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抵触するものではなく、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
17.11.2023	28.11.2023

名称及びあて先
日本国特許庁(ISA/JP)
〒100-8915
日本国
東京都千代田区霞が関三丁目４番３号

権限のある職員（特許庁審査官）
平井　誠 5S 9071
電話番号 03-3581-1101 内線 3546

国際調査報告
パテントファミリーに関する情報

国際出願番号
PCT/JP2023/037435

引用文献	公表日	パテントファミリー文献	公表日
US 2008/0082836 A1	03.04.2008	（ファミリーなし）	