(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
2009 年5 月22 日 (22.05.2009)

PCT

(10) 国際公開番号
WO 2009/063552 A1

(51) 国際特許分類:
G06F 21/24 (2006.01) *G06F 12/00* (2006.01)

(21) 国際出願番号: PCT/JP2007/072028

(22) 国際出願日: 2007 年11 月13 日 (13.11.2007)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(71) 出願人 (米国を除く全ての指定国について): 富士通株式会社 (FUJITSU LIMITED) [JP/JP]; 〒2118588 神奈川県川崎市中原区上小田中４丁目１番１号 Kanagawa (JP).

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 梅月 豪 (UMEZUKI, Takeshi) [JP/JP]; 〒2118588 神奈川県川崎市中原区上小田中４丁目１番１号 富士通株式会社内 Kanagawa (JP).

(74) 代理人: 酒井 宏明 (SAKAI, Hiroaki); 〒1006020 東京都千代田区霞が関三丁目２番５号 霞が関ビルディング 酒井国際特許事務所 Tokyo (JP).

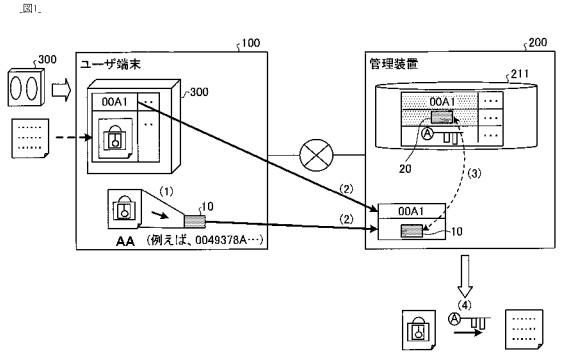
(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN,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

[続葉有]

WO 2009/063552 A1

(54) Title: ARCHIVE SYSTEM CONTROL PROGRAM, ARCHIVE SYSTEM, MANAGEMENT DEVICE, AND CONTROL METHOD

(54) 発明の名称: アーカイブシステム制御プログラム、アーカイブシステム、管理装置および制御方法



100 USER TERMINAL
AA (FOR EXAMPLE, 0049378A…)
200 MANAGEMENT DEVICE

(57) Abstract: A user terminal reads out encrypted contents to be authenticated from an encrypted content storage medium for storing the encrypted contents in association with management information and assigns data for forming the read out encrypted contents to the same hash function as that of the management device to calculate a first hash value. The management device acquires the calculated first hash value and management information from the user terminal, reads out, from a management information storage section for assigning the data for forming the encrypted contents which retain the authenticity to the hash function to store a second hash value which is a previously calculated hash value in association with the management information, the corresponding second hash value by using the acquired management information as a search key, authenticates whether the acquired first hash value and second hash value are matched, and permits a decoding processing if the result of the authentication shows that the first and second hash values are matched.

(57) 要約: ユーザ端末は、暗号化コンテンツを管理情報に対応付けて記憶する暗号化コンテンツ記憶媒体から認証対象となる暗号化コンテンツを読み出し、読み出した暗号化コンテンツを形成するデータを管理装置が有するものと同一のハッシュ関数に代入して第１のハッシュ値を算出し、管理装置は、算出された第１のハッシュ値と管理情報とをユーザ端末から取得し、真正性を保った暗号化コンテンツを形成するデータをハッシュ関数に代入して予め算出されているハッシュ値である第２のハッシュ値を管理情報に対応付けて記憶する管理情報記憶部から、取得した管理情報

[続葉有]

(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, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書

を検索キーとして対応する第２のハッシュ値を読み出し、取得した第１のハッシュ値と第２のハッシュ値とが一致するかを認証し、認証結果が、第１のハッシュ値と第２のハッシュ値とが一致すると判定する認証成功結果である場合に、復号する処理を許可する。

明 細 書

アーカイブシステム制御プログラム、アーカイブシステム、管理装置および制御方法

技術分野

[0001] この発明は、アーカイブシステム制御プログラム、アーカイブシステム、管理装置および制御方法に関する。

背景技術

[0002] 従来より、暗号化されたコンテンツを管理する方法について、様々な研究がなされている。例えば、特許文献1には、管理ID用に設定される乱数と暗号化前のファイル名とをハッシュ関数に代入し、得られるハッシュ値を管理IDとして用いる手法が開示されている。

[0003] さらに詳細に説明すると、特許文献1に記載されているファイル管理システムは、暗号化ファイルと、暗号化前のファイル名と、管理ID用乱数と、ハッシュ関数種別とを保管するファイル格納装置と、暗号化ファイルを復号する復号鍵と管理IDとを対応付けて管理する鍵管理装置とから構成されるファイル管理システムが開示されている。このような構成のもと、ファイル格納装置は、暗号化前のファイル名と管理ID用乱数とハッシュ関数種別とを鍵管理装置に送信する。そして、鍵管理装置は、受信した暗号化前のファイル名と管理ID用乱数とから、受信したハッシュ関数種別を用いてハッシュ値を算出する。鍵管理装置は、算出したハッシュ値と一致する管理IDがある場合に、対応する復号鍵をファイル格納装置に送信する。

[0004] なお、特許文献2には、携帯端末装置内のデータをネットワークを介して接続されたバックアップ装置にバックアップする手法について開示されている。

[0005] 特許文献1:特開2006－285697号公報(第1—5、9頁、第1、11図)
特許文献2:特開2006－211051号公報(第1、2、4頁、第1図)

発明の開示

発明が解決しようとする課題

[0006] ところで、上記した従来の技術は、アーカイブシステムのセキュリティの程度が十分

ではないという課題があった。

[0007] 例えば、上記した特許文献1においては、管理ID用乱数やコンテンツ名を用いてハッシュ値を算出し、管理IDとして用いるので、管理ID用乱数やコンテンツ名が漏洩することによって、復号鍵が漏洩してしまい、アーカイブシステムのセキュリティの程度が十分ではない。また、上記した特許文献1においては、用いられるのはコンテンツ名などから算出されるハッシュ値であり、コンテンツ自体に不正なデータの改ざん等があった場合に検知することはできず、アーカイブシステムのセキュリティの程度が十分ではない。

[0008] そこで、この発明は、上述した従来技術の課題を解決するためになされたものであり、アーカイブシステムのセキュリティを向上することが可能なアーカイブシステム制御プログラム、アーカイブシステム、管理装置および制御方法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

[0009] 上述した課題を解決し、目的を達成するため、本発明は、暗号化された暗号化コンテンツを暗号化コンテンツ記憶媒体から参照するユーザ端末と、管理対象とする当該暗号化コンテンツを復号する復号鍵を記憶する管理装置とから構成され、前記管理装置が、前記暗号化コンテンツを一意に特定する情報である管理情報を前記ユーザ端末から取得し、当該管理情報によって特定される当該暗号化コンテンツを当該復号鍵を用いて復号する処理を許可するか否かを認証するアーカイブシステムであって、前記ユーザ端末は、前記暗号化コンテンツを前記管理情報に対応付けて記憶する前記暗号化コンテンツ記憶媒体から認証対象となる当該暗号化コンテンツを読み出し、読み出した当該暗号化コンテンツを形成するデータを前記管理装置が有するものと同一のハッシュ関数に代入して第1のハッシュ値を算出する算出手段を備え、前記管理装置は、前記算出手段によって算出された第1のハッシュ値と前記管理情報とを前記ユーザ端末から取得する取得手段と、真正性を保った前記暗号化コンテンツを形成するデータを前記ハッシュ関数に代入して予め算出されているハッシュ値である第2のハッシュ値を前記管理情報に対応付けて記憶する管理情報記憶部から、前記取得手段が取得した前記管理情報を検索キーとして対応する前記第2のハ

ッシュ値を読み出し、当該取得手段が取得した前記第1のハッシュ値と当該第2のハッシュ値とが一致するかを認証するハッシュ値認証手段と、前記ハッシュ値認証手段による認証結果が、前記第1のハッシュ値と前記第2のハッシュ値とが一致すると判定する認証成功結果である場合に、前記復号する処理を許可する復号制御手段と、を備えることを特徴とする。

[0010] また、本発明は、上記の発明において、前記復号制御手段が前記復号する処理を許可し、その後、前記ユーザ端末が前記暗号化コンテンツを前記復号鍵を用いて復号した場合に、復号されたコンテンツを当該ユーザ端末が書き込むユーザ端末記憶媒体を一意に識別する格納媒体識別情報を当該ユーザ端末から取得してコンテンツ管理簿記憶部に記憶し、当該ユーザ端末が前記コンテンツを廃棄する際には、廃棄する旨の情報を当該ユーザ端末から取得してコンテンツ管理簿記憶部に記憶する管理簿記憶手段をさらに備えることを特徴とする。

[0011] また、本発明は、上記の発明において、前記ハッシュ値認証手段による認証結果が、前記第1のハッシュ値と前記第2のハッシュ値とが一致しないと認証する認証失敗結果である場合に、当該認証失敗結果を前記管理情報に対応付けて認証結果記憶部に記憶する認証結果記憶手段と、前記認証結果記憶手段によって前記認証失敗結果を記憶する前記認証結果記憶部から、前記取得手段が取得した前記管理情報を検索キーとして対応する前記認証失敗結果があるかを認証する失敗結果認証手段と、をさらに備え、前記復号制御手段は、前記ハッシュ値認証手段による認証結果が、前記認証成功結果であり、かつ、前記失敗結果認証手段による認証結果が、前記認証失敗結果がないと認証する結果である場合に、前記復号する処理を許可することを特徴とする。

[0012] また、本発明は、上記の発明において、前記暗号化コンテンツ記憶媒体は、複数の暗号化コンテンツを記憶し、前記管理装置は、前記管理情報記憶部に、前記管理情報に対応付けて、当該管理情報によって特定される暗号化コンテンツを記憶する前記暗号化コンテンツ記憶媒体を一意に識別する記憶媒体識別情報をさらに記憶するものであって、前記認証結果記憶手段は、前記ハッシュ値認証手段による認証結果が前記認証失敗結果である場合に、前記取得手段が取得した前記管理情報を検

索キーとして対応する1つの前記記憶媒体識別情報を前記管理情報記憶部から取得し、取得した1つの前記記憶媒体識別情報を検索キーとして対応する複数の前記管理情報を取得し、取得した前記管理情報に対応付けて、当該暗号化コンテンツ記憶媒体に何らかの異常があることを示す記憶媒体異常情報を認証結果記憶部にさらに記憶し、前記失敗結果認証手段は、前記認証結果記憶手段によって記憶される前記認証結果記憶部から、前記取得手段が取得した前記管理情報を検索キーとして、対応する前記認証失敗結果または前記記憶媒体異常情報があるかを認証し、前記復号制御手段は、前記ハッシュ値認証手段による認証結果が、前記認証成功結果であり、かつ、前記失敗結果認証手段による認証結果が、前記認証失敗結果および記憶媒体異常情報がないと判定する結果である場合に、前記復号する処理を行うことを許可することを特徴とする。

[0013] また、本発明は、上記の発明において、管理装置記憶部は、暗号化コンテンツ記憶媒体に記憶する前記暗号化コンテンツと同一の暗号化コンテンツを前記管理情報に対応付けて記憶するものであって、

前記認証結果記憶手段によって記憶される前記認証結果記憶部から前記認証失敗結果および／または前記記憶媒体異常情報に対応する管理情報を取得し、取得した当該管理情報を検索キーとして対応する暗号化コンテンツを取得し、取得した当該暗号化コンテンツについてマイグレーションを行うマイグレーション手段をさらに備えることを特徴とする。

発明の効果

[0014] 本発明によれば、アーカイブシステムのセキュリティを向上することが可能である。

[0015] また、本発明によれば、管理装置は、復号されたコンテンツが、どの記憶媒体に書き込まれているかを管理することが可能である。

[0016] また、本発明によれば、認証に失敗している暗号化コンテンツに対する復号処理を制限することが可能である。

[0017] また、本発明によれば、管理装置は、例えば、暗号化コンテンツを記憶している暗号化コンテンツ記憶媒体に劣化が生じて信頼性が低下し、暗号化コンテンツの内容に誤りが発生した結果、認証に失敗した場合に、当該暗号化コンテンツ記憶媒体に

記憶されている他の暗号化コンテンツに対するアクセスを制限することが可能である。

[0018] また、本発明によれば、管理装置は、例えば、暗号化コンテンツ記憶媒体の信頼性が低下している場合に、当該暗号化コンテンツ記憶媒体に記憶されている暗号化コンテンツについてマイグレーションを行うことで、信頼できるバックアップを保持することが可能である。

図面の簡単な説明

[0019] [図1]図1は、アーカイブシステムの概要および特徴を説明するための図である。

[図2]図2は、アーカイブシステムによる全体処理の流れを示すフローチャートである。

[図3]図3は、アーカイブシステムによるユーザ認証処理の流れを示すフローチャートである。

[図4]図4は、アーカイブシステムによる暗号化コンテンツ認証処理の流れを示すフローチャートである。

[図5]図5は、アーカイブシステムによる認証失敗処理の流れを示すフローチャートである。

[図6]図6は、アーカイブシステムによる復号処理の流れを示すフローチャートである。

[図7]図7は、アーカイブシステムの構成を示すためのブロック図である。

[図8]図8は、暗号化コンテンツ記憶媒体に記憶されている情報の一例を示す図である。

[図9]図9は、管理情報記憶部に記憶されている情報の一例を示す図である。

[図10]図10は、コンテンツ記憶簿記憶部に記憶されている情報の一例を示す図である。

[図11]図11は、認証結果記憶部に記憶されている情報の一例を示す図である。

[図12]図12は、実施例1におけるアーカイブシステムのプログラムを示す図である。

符号の説明

[0020] 10 第1のハッシュ値

20 第2のハッシュ値

100 ユーザ端末

110 ユーザ端末記憶部

120 ユーザ端末側参照管理部

121 算出部

122 認証問い合わせ部

123 制限情報通知部

124 格納先情報通知部

125 暗号化コンテンツ送信部

126 ユーザ端末側コンテンツ管理部

127 復号部

200 管理装置

210 管理装置記憶部

211 管理情報記憶部

212 コンテンツ管理簿記憶部

213 認証結果記憶部

214 アーカイブストレージ装置記憶部

220 管理装置側参照管理部

221 取得部

222 認証部

223 復号制御部

224 コンテンツ管理簿格納部

225 認証結果格納部

226 管理装置側コンテンツ管理部

300 暗号化コンテンツ記憶媒体

発明を実施するための最良の形態

[0021] 以下に添付図面を参照して、この発明に係るアーカイブシステム制御プログラム、アーカイブシステム、管理装置および制御方法の実施例を詳細に説明する。なお、以下では、本実施例で用いる主要な用語、本実施例に係るアーカイブシステムの概要および特徴、アーカイブシステムの処理の流れおよび構成を順に説明し、最後に

本実施例に対する種々の変形例を説明する。

実施例 1

[0022] [用語の説明]

まず最初に、実施例1で用いる主要な用語を説明する。ユーザ端末とは、暗号化されたコンテンツである暗号化コンテンツを暗号化コンテンツ記憶媒体から参照する装置である。具体的には、ユーザ端末は、暗号化コンテンツ記憶媒体に記憶されている情報を読み出す。例えば、ユーザ端末は、暗号化コンテンツ記憶媒体を読み取る光ディスクドライブなどを有し、ユーザ端末にセットされた暗号化コンテンツ記憶媒体(光ディスク)から情報を読み出す。なお、暗号化コンテンツ記憶媒体は、バックアップをとることを目的として管理装置外に搬出する暗号化コンテンツを記憶するものであり、例えば、光ディスクの他、テープや、HDD、USBメモリなどの可搬記憶媒体(持ち運び可能な記憶媒体)が該当する。

[0023] また、実施例1で用いる管理装置とは、管理対象とする暗号化コンテンツを復号する復号鍵を記憶する装置であり、暗号化コンテンツ記憶媒体に記憶されている暗号化コンテンツを復号鍵を用いて復号する処理を許可するか否かを認証する装置である。

[0024] ここで、上記したユーザ端末と管理装置と暗号化コンテンツ記憶媒体との関係について整理する。まず、管理装置とユーザ端末とは、ネットワーク(例えば、有線ネットワークや無線ネットワーク)を介して接続されるものであり、情報(認証に必要な情報や復号鍵など)をネットワークを介して送受信するものである。そして、ユーザ端末と暗号化コンテンツ記憶媒体とは、例えば、ドライブ(メディア読取部)とメディアとの関係にある。例えば、アーカイブシステムを使用する使用者が暗号化コンテンツ記憶媒体をユーザ端末に接続し、ユーザ端末が暗号化コンテンツ記憶媒体に記憶されている情報を読み取るものである。

[0025] また、実施例1に係るアーカイブシステムにおいて、管理装置の数とユーザ端末の数と暗号化コンテンツ記憶媒体の数とは、1対1対1に限られず、一つの管理装置に対して、多数のユーザ端末や暗号化コンテンツ記憶媒体があってもよい。

[0026] また、実施例1で用いるアーカイブ管理ID(特許請求の範囲に記載の「管理情報」

に対応する。)とは、暗号化コンテンツを一意に特定するものであり、例えば、コンテンツ(または、暗号化コンテンツ)を示すコンテンツ名(ファイル名)や、アーカイブストレージにおいて暗号化コンテンツを一意に特定することを目的として、コンテンツ名とは別途に付加された識別情報(例えば、ID)などが該当する。

[0027] また、実施例1で用いるハッシュ関数とは、ドキュメントや数字などの文字列の羅列から、一定長のデータであるハッシュ値を算出するための関数や手順のことである。実施例1で用いるハッシュ関数は、不可逆な関数である一方向関数を含むものであり、ハッシュ値から原文を再現することはできず、また、同じハッシュ値を持つ異なるデータを作成することが事実上不可能なものである。

[0028] [アーカイブシステムの概要および特徴]

次に、図1を用いて、実施例1に係るアーカイブシステムの概要および特徴を説明する。図1は、アーカイブシステムの概要および特徴を説明するための図である。

[0029] 同図に示すように、実施例1に係るアーカイブシステムは、ユーザ端末100と管理装置200とがネットワークを介して接続され、ユーザ端末100には、暗号化コンテンツ記憶媒体300が接続されている。そして、実施例1に係るアーカイブシステムでは、管理装置200が、管理情報をユーザ端末100から取得し、管理情報によって特定される暗号化コンテンツを復号鍵を用いて復号する処理を許可するか否かを認証する。このような概要を有するアーカイブシステムは、以下で説明するように、アーカイブシステムのセキュリティを向上することが可能である点に主たる特徴がある。

[0030] この主たる特徴について説明すると、まず、実施例1に係るアーカイブシステムでは、暗号化コンテンツ記憶媒体300が、暗号化コンテンツを管理情報に対応付けて記憶する。例えば、図1の暗号化コンテンツ記憶媒体300に示すように、暗号化コンテンツ記憶媒体300は、管理情報「00A1」と、暗号化コンテンツとを対応付けて記憶する。

[0031] また、実施例1に係るアーカイブシステムでは、管理装置200は、真正性を保った暗号化コンテンツを形成するデータをハッシュ関数に代入して予め算出されているハッシュ値である第2のハッシュ値20を、管理情報に対応付けて管理情報記憶部211に記憶する。例えば、図1の管理情報記憶部211に示すように、管理情報「00A1」と

、第2のハッシュ値20とを対応付けて記憶する。なお、実施例1では、管理情報と対応付けて、さらに、対応する暗号化コンテンツを復号する復号鍵(図1では、Aという記号が記載されている鍵の絵として記載)を記憶する場合について説明する。

[0032] ここで、実施例1で用いられる第2のハッシュ値20は、真正性を保った暗号化コンテンツを形成するデータから算出される点に特徴があり、例えば、当該暗号化コンテンツが暗号化コンテンツ記憶媒体300に格納される際や、当該暗号化コンテンツが実施例1に係るアーカイブシステムによる管理対象とされた際に算出されるものである。これにより、第2のハッシュ値20は、暗号化コンテンツ記憶媒体300の劣化によるデータの変化や不正なデータの改ざんなどの影響を一切受けていない値として算出され、これらの影響を受けない状態で管理情報記憶部211に記憶されているものである。なお、実施例1では、暗号化コンテンツを形成するデータ全体から、第2のハッシュ値20を算出する手法について説明する。

[0033] このような構成のもと、実施例1に係るアーカイブシステムでは、ユーザ端末100が、暗号化コンテンツ記憶媒体300から、認証対象となる暗号化コンテンツを読み出し、読み出した暗号化コンテンツを形成するデータを管理装置200が有するものと同一のハッシュ関数に代入して第1のハッシュ値10を算出する。例えば、図1の(1)に示すように、ユーザ端末100は、認証対象となる暗号化コンテンツを形成するデータから、第1のハッシュ値10を算出する。

[0034] ここで、実施例1で用いられる第1のハッシュ値10は、単に暗号化コンテンツを識別するために付与されている情報であるファイル名などだけではなく、暗号化コンテンツ自身を形成するデータを用いて算出される点に特徴があり、例えば、認証する暗号化コンテンツが指定された際に(または、認証に必要な情報を管理装置200が取得する際に)、その都度算出されるものである。これにより、第1のハッシュ値10は、認証を行う際に、暗号化コンテンツ記憶媒体300の劣化によるデータの変化や不正なデータの改ざんなどの影響を受けている場合に、これらの影響を受けている(反映している)値として算出されるものである。なお、実施例1では、暗号化コンテンツを形成するデータ全体から、第1のハッシュ値10を算出する手法について説明する。

[0035] そして、実施例1に係るアーカイブシステムでは、管理装置200が、ユーザ端末10

0が算出した第1のハッシュ値10と、管理情報とを、ユーザ端末100から取得する。例えば、図1の(2)に示すように、管理装置200は、管理情報「00A1」と、第1のハッシュ値10とを取得する。

[0036] そして、実施例1に係るアーカイブシステムでは、管理装置200が、管理情報記憶部211から、取得した管理情報を検索キーとして対応する第2のハッシュ値20を読み出し、取得した第1のハッシュ値10と第2のハッシュ値20とが一致するかを認証する。例えば、図1の(3)に示すように、管理装置200は、同じ管理情報と対応付けられている第1のハッシュ値10と第2のハッシュ値20とが一致するか否かを認証する。

[0037] そして、実施例1に係るアーカイブシステムでは、管理装置200が、認証結果が第1のハッシュ値10と第2のハッシュ値20とが一致すると判定する認証成功結果である場合に、復号する処理を許可する。例えば、図1の(4)に示すように、管理装置200は、第1のハッシュ値10と第2のハッシュ値20とが一致する場合に、取得した管理情報で一意に識別される暗号化コンテンツを復号する処理を許可し、管理装置200またはユーザ端末100が、復号鍵を用いて、暗号化コンテンツを復号する処理を行う。

[0038] このようなことから、実施例1に係るアーカイブシステムは、上記した主たる特徴の如く、アーカイブシステムのセキュリティを向上することが可能である。

[0039] 例えば、管理IDのみを管理装置200に送信し、ユーザ端末100が復号鍵を取得する(復号鍵を用いた処理の一例)手法や、コンテンツ名からハッシュ値を算出して管理装置200に送信し、ユーザ端末100が復号鍵を取得する手法では、管理IDやコンテンツ名が漏洩することによって、復号鍵が簡単に漏洩してしまうのに対して、本発明を適用することにより、暗号化コンテンツ自体を保持していない限り、認証に必要なハッシュ値を算出して送信することはできず、復号鍵が簡単に漏洩することを防止することが可能であり、アーカイブシステムのセキュリティを向上することが可能である。

[0040] また、暗号化コンテンツ自体を管理装置200に送信するのではなく、暗号化コンテンツから算出されたハッシュ値を送信することによって、認証処理の際に、暗号化コンテンツが漏洩することを防止することが可能であり、アーカイブシステムのセキュリティを向上することが可能である。

[0041] また、本発明を適用することにより、例えば、暗号化コンテンツを記憶している記憶媒体に劣化が生じ、暗号化コンテンツの内容に誤りが発生した場合に、管理装置200が、暗号化コンテンツから算出されるハッシュ値に差異が生じていることを認証する結果、管理装置200は、暗号化コンテンツに問題が生じていることを把握することが可能であり、アーカイブシステムのセキュリティを向上することが可能である。

[0042] また、本発明を適用することにより、例えば、第三者によって暗号化コンテンツに改ざんが行われた場合には、管理装置200が、暗号化コンテンツから算出されるハッシュ値に差異が生じていることを認証する結果、管理装置200は、暗号化コンテンツに問題が生じていることを把握することが可能であり、アーカイブシステムのセキュリティを向上することが可能である。

[0043] [アーカイブシステムによる処理]

次に、図2～図6を用いて、アーカイブシステムによる処理を説明する。図2は、アーカイブシステムによる全体処理の流れを示すフローチャートである。図3は、アーカイブシステムによるユーザ認証処理の流れを示すフローチャートである。図4は、アーカイブシステムによる暗号化コンテンツ認証処理の流れを示すフローチャートである。図5は、アーカイブシステムによる認証失敗処理の流れを示すフローチャートである。図6は、アーカイブシステムによる復号処理の流れを示すフローチャートである。なお、以下の説明に記載する各部の符号は、図7に基づくものである。

[0044] なお、アーカイブシステムは、本発明の特徴である、暗号化コンテンツを形成するデータからハッシュ値を算出して行う『暗号化コンテンツ認証処理』だけでなく、それぞれ特徴を有する処理として、アーカイブシステムにアクセスを許可するユーザか否かを認証する『ユーザ認証処理』と、コンテンツ各々に対するアクセスを許可するユーザか否かを認証する『アクセスユーザ認証処理』と、暗号化コンテンツの復号を制限する情報があるか否かを確認する『制限情報確認処理』と、暗号化コンテンツ認証処理を失敗した際に行う処理である『認証失敗処理』と、暗号化コンテンツ認証処理に成功した際に行う処理である『復号処理』とを併せて実行する。

[0045] 以下では、まず、アーカイブシステムによる全体処理に関する記載においては、暗号化コンテンツその他の処理各々について、全体処理の流れにおける個々の処理

の関係について主に説明する。その後、アーカイブシステムによるユーザ認証に関する記載において、『ユーザ認証処理』について説明する。続いて、アーカイブシステムによる暗号化コンテンツ認証に関する記載において、『暗号化コンテンツ認証処理』と『アクセスユーザ認証処理』とを説明する。その後、アーカイブシステムによる認証失敗処理に関する記載において、『認証失敗処理』について説明する。そして、アーカイブシステムによる復号処理に関する記載において、『復号処理』について説明する。

[0046] なお、本発明に係るアーカイブシステムは、これらすべての処理を併用しなければならないわけではなく、任意の処理のみを実行してもよい。

[0047] [アーカイブシステムによる全体処理]

まず、図2を用いて、アーカイブシステムによる全体処理の流れを説明する。

[0048] 同図に示すように、ユーザ端末100において、アーカイブ管理IDが指定されると(ステップS101肯定)、アーカイブシステムは、ユーザ認証処理を行う(ステップS102)。

[0049] ここで、ユーザ認証処理が失敗である場合には(ステップS103否定)、アーカイブシステムは、処理を終了する。一方、ユーザ認証処理が成功である場合には(ステップS103肯定)、アーカイブシステムは、暗号化コンテンツ認証処理を行う(ステップS104)。

[0050] ここで、認証結果が、失敗である場合には(ステップS105否定)、アーカイブシステムは、認証失敗処理を行い(ステップS106)、処理を終了する。

[0051] 一方、認証結果が、成功である場合には(ステップS105肯定)、アーカイブシステムは、制限情報確認処理を行う(ステップS107)。つまり、例えば、管理装置200では、認証部222が、取得したアーカイブ管理IDを検索キーとして認証結果記憶部213を検索し、当該アーカイブ管理IDに対応付けられて、認証失敗結果または記憶媒体異常情報が認証結果記憶部213に記憶されているかを確認する。ここで、図11の例を用いて説明すると、認証部222は、アーカイブ管理ID「0011」を検索キーとする場合に、認証失敗結果または記憶媒体異常情報が認証結果記憶部213に記憶されていないと認証し、アーカイブ管理ID「0012」を検索キーとする場合に、認証失敗結

果が認証結果記憶部213に記憶されていると認証する。

[0052] そして、管理装置200(認証部222)によって制限情報ありと判定された場合には(ステップS108肯定)、アーカイブシステムでは、復号制御部223が、制限内容をユーザ端末100に通知し(ステップS109)、その後、ユーザ端末100では、制限情報通知部123が、通知された制限内容を出力する(ステップS110)。つまり、例えば、制限情報通知部123は、認証失敗結果ありと通知し、記憶媒体異常情報ありと通知する。

[0053] 一方、管理装置200(認証部222)によって制限情報なしと判定された場合には(ステップS108否定)、アーカイブシステムは、復号処理を行い(ステップS111)、処理を終了する。

[0054] [アーカイブシステムによるユーザ認証処理]

次に、図3を用いて、アーカイブシステムによるユーザ認証処理の流れを説明する。

[0055] 同図に示すように、ユーザ端末100では、認証問い合わせ部122が、暗号化コンテンツ記憶媒体300から、認証先情報と、アーカイブ管理IDとを取得する(ステップS201)。そして、認証問い合わせ部122は、取得した認証先情報を用いて管理装置200にアクセスし(ステップS202)、ユーザ認証処理に必要な情報としてアクセスユーザを送信する(ステップS203)。つまり、例えば、アクセスユーザとして、ユーザによって「山田一郎」が入力された場合には、「山田一郎」と送信する。

[0056] そして、管理装置200では、認証部222が、認証問い合わせ部122からアクセスユーザを受信すると、ユーザ認証処理を行う(ステップS204)。つまり、受信したアクセスユーザが管理装置200にアクセスすることが許可されているユーザか否かを認証する。そして、認証部222は、認証結果をユーザ端末100に送信する(ステップS205)。例えば、認証部222は、受信したアクセスユーザが、管理装置200にアクセスすることが許可されているユーザである場合には、認証成功と送信し、管理装置200にアクセスすることが許可されていないユーザである場合には、認証失敗と送信する。

[0057] そして、ユーザ端末100では、認証問い合わせ部122が、認証部222から、ユーザ認証処理に関する認証結果を受信する(ステップS206)。そして、認証問い合わせ部122は、認証結果が認証成功であるかを判定する(図2のステップS103)。

[0058] [アーカイブシステムによる暗号化コンテンツ認証処理]

次に、図4を用いて、アーカイブシステムによる暗号化コンテンツ認証処理の流れを説明する。なお、アクセスユーザ認証処理についても、併せて説明する。

[0059] 同図に示すように、ユーザ認証処理が成功である場合に(図2のステップS103肯定)、ユーザ端末100では、算出部121が、第1のハッシュ値を算出する(ステップS301)。つまり、例えば、入力部から暗号化コンテンツを参照する指示と参照する暗号化コンテンツを示すアーカイブ管理IDとが、ユーザ端末100を使用しているユーザによって指定されると、暗号化コンテンツを形成するデータから、第1のハッシュ値を算出する。具体的に例を挙げて説明すると、算出部121は、アーカイブ管理IDに紐づく暗号化コンテンツのコンテンツ内容全体から、第1のハッシュ値を算出する。言い換えると、算出部121は、読み出した暗号化コンテンツを形成するデータを管理装置200が有するものと同一のハッシュ関数に代入して、第1のハッシュ値を算出する。

[0060] そして、ユーザ端末100では、認証問い合わせ部122が、アーカイブ管理IDと第1のハッシュ値とを管理装置200に送信する(ステップS302)。

[0061] そして、管理装置200では、認証部222が、ハッシュ値が一致するかを判別する(ステップS303)。例えば、認証部222は、受信したアーカイブ管理IDと対応付けて管理情報記憶部211に記憶している第2のハッシュ値と、受信した第1のハッシュ値とが一致するかを判別する。さらに詳細な一例をあげて説明すると、認証部222は、ハッシュ値が一致するかを判別する(暗号化コンテンツ認証処理)とともに、受信したアーカイブ管理IDと対応付けて管理情報記憶部211に記憶しているアクセスユーザと、受信したアクセスユーザとが一致するかを判別する(アクセスユーザ認証処理)。ここで、上記したハッシュ値やアクセスユーザが一致すると判別される場合に、認証成功と判定する。一方、上記したハッシュ値やアクセスユーザが一致しないと判別される場合に、認証失敗と判定する。そして、認証部222は、暗号化コンテンツ認証処理が成功であるかを判定する(図2のステップS105)。

[0062] [アーカイブシステムによる認証失敗処理]

次に、図5を用いて、アーカイブシステムによる認証失敗処理の流れを説明する。なお、以下の処理では、アーカイブ管理ID「0012」について認証失敗結果が得られた

場合について説明する。

[0063] 同図に示すように、認証部222によって認証失敗であると判定された場合に(図2のステップS105否定)、管理装置200では、認証結果格納部225が、認証結果管理記憶部に、受信したアクセスユーザと受信したアーカイブ管理IDとを書き込む(ステップS401)。

[0064] そして、管理装置200では、復号制御部223が、認証失敗であるとユーザ端末100に送信する(ステップS402)。つまり、例えば、復号制御部223は、アーカイブ管理ID「0012」が参照不可である旨をユーザ端末100に通知する。

[0065] そして、ユーザ端末100では、制限情報通知部123が、出力部から、参照不可である旨を出力する(ステップS403)。つまり、例えば、制限情報通知部123は、アーカイブ管理ID「0012」について認証失敗であり、参照することはできないと出力する。

[0066] そして、管理装置200では、認証結果格納部225が、受信したアーカイブ管理IDに対応付けて認証失敗結果を認証結果記憶部213に格納する(ステップS404)。例えば、図11に示すように、認証結果格納部225は、アーカイブ管理ID「0012」に対応付けて認証失敗結果「あり」を認証結果記憶部213に格納する。

[0067] そして、管理装置200では、認証結果格納部225が、受信したアーカイブ管理IDと対応付けられている暗号化コンテンツが記憶されている暗号化コンテンツ記憶媒体300の識別情報を取得する(ステップS405)。つまり、例えば、図9の例を用いて説明すると、認証結果格納部225は、アーカイブ管理ID「0012」に対応付けられている暗号化コンテンツが記憶されている記憶媒体識別情報「A2222」を取得する。続いて、認証結果格納部225は、取得した記憶媒体識別情報に対応付けられているアーカイブ管理IDを取得する(ステップS406)。例えば、図9の例を用いて説明すると、認証結果格納部225は、記憶媒体識別情報「A2222」に対応付けられたアーカイブ管理IDである「0013」と「0014」とを取得する。

[0068] そして、管理装置200では、認証結果格納部225が、取得したアーカイブ管理IDに対応付けて、記憶媒体異常情報を格納する(ステップS407)。つまり、例えば、図11の例を用いて説明すると、認証結果格納部225は、取得したアーカイブ管理IDである「0013」と「0014」とに対応付けて、記憶媒体異常情報「あり」を認証結果記憶部

213に格納する。そして、管理装置200は、処理を終了する。

[0069] [アーカイブシステムによる復号処理]

次に、図6を用いて、アーカイブシステムによる復号処理の流れを説明する。なお、以下の処理では、アーカイブ管理ID「0011」について認証成功結果が得られ、さらに、制限情報が得られなかった場合について説明する。

[0070] 同図に示すように、認証部222によって制限情報なしと判定された場合には(図2のステップS108肯定)、管理装置200では、復号制御部223が、暗号化コンテンツの参照方法として、管理装置200で管理するかを判定する(ステップS501)。つまり、復号制御部223は、管理装置200において復号して管理するか、または、暗号化コンテンツをユーザ端末100において復号して管理するかを判定する。

[0071] ここで、復号制御部223が、管理装置200で管理すると判定された場合には(ステップS501肯定)、つまり、例えば、管理装置200において復号して管理する旨の指示がユーザからユーザ端末100に入力され、その旨の信号を管理装置200が受信している場合には、ユーザ端末100では、暗号化コンテンツ送信部125が、参照する暗号化コンテンツを管理装置200へと送信(アップロード)する(ステップS502)。

[0072] なお、復号制御部223は、上記したコンテンツを管理装置200で管理するか否かの判定において、ユーザからの指示を受信する場合について説明したが、本発明はこれに限定されるものではなく、予め設定されている内容に基づいて、復号制御部が、ユーザからの指示を受信せずに、判定してもよい。例えば、コンテンツごとに、参照する場所(例えば、管理装置や、特定のユーザ端末(または、記憶部)など。)を対応付けてテーブルとして記憶しておき、かかるテーブルを用いて参照してもよい。

[0073] そして、管理装置200では、管理装置側コンテンツ管理部226が、受信した暗号化コンテンツをアーカイブストレージ装置記憶部214に書き込む(ステップS503)。そして、管理装置側コンテンツ管理部226は、アップロードされた暗号化コンテンツに対応する復号鍵を管理情報記憶部211から取得し、アップロードされた暗号化コンテンツを復号する(ステップS504)。つまり、例えば、図9の例を用いて説明すると、管理装置側コンテンツ管理部226は、アーカイブ管理ID「0011」に対応付けられた復号鍵「鍵A」を取得し、アップロードされた暗号化コンテンツを鍵Aを用いて復号する。そ

して、処理を終了する。

[0074] 一方、管理装置200では、復号制御部223が、管理装置200で管理しないと判定した場合には(ステップS501否定)、つまり、例えば、暗号化コンテンツをユーザ端末100において復号して管理する指示がユーザからユーザ端末100に入力され、その旨の信号を管理装置200が受信している場合には、参照する暗号化コンテンツに対応する復号鍵を管理情報記憶部211から取得し、ユーザ端末100へと送信する(ステップS505)。つまり、例えば、図9の例を用いて説明すると、復号制御部223は、アーカイブ管理ID「0011」に対応付けられた復号鍵「鍵A」を取得し、ユーザ端末100へと送信する。

[0075] そして、ユーザ端末100では、復号部127が、管理装置200から受信した復号鍵を用いて、参照する暗号化コンテンツを復号する(ステップS506)。例えば、アーカイブ管理ID「0011」に対応する暗号化コンテンツを、取得した鍵Aを用いて復号する。

[0076] そして、ユーザ端末100では、格納先情報通知部124が、復号されたコンテンツを当該ユーザ端末100が書き込むユーザ端末100記憶媒体を一意に識別する格納媒体識別情報を送信する(ステップS507)。つまり、例えば、図9の例を用いて説明すると、ユーザ端末100が復号したコンテンツをユーザ端末記憶部110に格納した場合には、格納先情報通知部124は、ユーザ端末記憶部110であると送信する。さらに詳細には、例えば、格納先情報通知部124は、格納媒体識別情報「B111」を送信する。

[0077] 続いて、管理装置200では、コンテンツ管理簿格納部224が、受信した復号済みコンテンツが格納されている場所を、コンテンツ管理簿記憶部212に書き込む(ステップS508)。例えば、図10の例を用いて説明すると、コンテンツ管理簿格納部224は、アーカイブ管理ID「0011」に対応付けて、格納媒体識別情報「B111」をコンテンツ管理簿記憶部212に格納する。

[0078] その後、ユーザ端末100では、ユーザ端末側コンテンツ管理部126が、復号済みコンテンツをその後もユーザ端末100にて管理するかを判定する(ステップS509)。つまり、例えば、ユーザ端末100において、復号済みコンテンツを参照した後削除するのではなく、その後も復号済みコンテンツを管理するかを判定する。ここで、ユーザ

端末側コンテンツ管理部126は、復号済みコンテンツをその後も管理すると判定する場合には(ステップS509肯定)、処理を終了する。一方、ユーザ端末側コンテンツ管理部126は、復号済みコンテンツを管理しないと判定した場合には(ステップS509否定)、復号済みコンテンツを廃棄し(ステップS510)、管理装置200へと、復号済みコンテンツを廃棄した旨を示す廃棄情報を送信する(ステップS511)。

[0079] そして、管理装置200では、コンテンツ管理簿格納部224が、復号されたコンテンツを廃棄した旨を受信すると、対応するアーカイブ管理IDに対応付けて廃棄情報を、コンテンツ管理簿記憶部212に格納する(ステップS512)。つまり、例えば、コンテンツ管理簿格納部224は、アーカイブ管理ID「0011」に対応付けて、廃棄情報「廃棄済み」を格納する。そして、処理を終了する。

[0080] [アーカイブシステムの構成]

次に、図7～図11を用いて、図1に示したアーカイブシステムの構成について説明する。図7に示すように、このアーカイブシステムは、ユーザ端末100と、管理装置200とから構成される。図7は、アーカイブシステムの構成を示すためのブロック図である。図8は、暗号化コンテンツ記憶媒体300に記憶されている情報の一例を示す図である。図9は、管理情報記憶部211に記憶されている情報の一例を示す図である。図10は、コンテンツ管理簿記憶部212に記憶されている情報の一例を示す図である。図11は、認証結果記憶部213に記憶されている情報の一例を示す図である。

[0081] ユーザ端末100は、暗号化コンテンツ記憶媒体300と、ユーザ端末記憶部110と、ユーザ端末側参照管理部120とから構成され、管理装置200は、管理装置記憶部210と、管理装置側参照管理部220とから構成される。ここで、ユーザ端末記憶部110は、特許請求の範囲に記載の「ユーザ端末記憶媒体」に対応する。

[0082] なお、図7には図示していないが、ユーザ端末100は、各種の情報の入力を受付ける入力部と、各種の情報を出力する出力部とを備えて構成されてもよい。ここで、入力部とは、キーボードやマウス、マイクなどが該当し、例えば、ユーザ端末100を使用する使用者から、ユーザ認証処理を行う旨の指示を受付ける。また、復号したコンテンツをユーザ端末100で管理する旨の指示や、復号したコンテンツを管理装置200で管理する旨の指示を受付ける。出力部とは、モニタ(若しくはディスプレイ、タッチパ

ネル）やスピーカなどが該当し、例えば、後述する認証問い合わせ部122によって行われた認証結果などを表示（または、スピーカーから音声で出力）する。

[0083] ［ユーザ端末記憶部等］

暗号化コンテンツ記憶媒体300は、暗号化コンテンツを管理情報に対応付けて記憶する。例えば、暗号化コンテンツ記憶媒体300は、複数の暗号化コンテンツを記憶する。また、暗号化コンテンツ記憶媒体300は、それぞれに、暗号化コンテンツ記憶媒体300を一意に識別する情報である記憶媒体識別情報が付与されている。例えば、図8に示すように、暗号化コンテンツ記憶媒体300は、暗号化コンテンツをアーカイブ管理IDに対応付けて記憶し、また、記憶媒体識別情報と、ネットワークにおいて管理装置200を一意に特定するための情報である認証先情報とを記憶する。

[0084] さらに詳細な一例をあげて説明すると、図8に示す例では、暗号化コンテンツ記憶媒体300は、暗号化コンテンツ記憶媒体300の記憶媒体識別情報「A0112」と、認証先情報「211．9．・・・（IPアドレスなど）」とを記憶し、アーカイブ管理ID「0011」と、暗号化コンテンツ「A（図8においては、「A」が記載されている暗号化コンテンツを示す絵として記載）」とを対応付けて記憶し、アーカイブ管理ID「0012」と、暗号化コンテンツ「B（図8においては、「B」が記載されている暗号化コンテンツを示す絵として記載）」とを対応付けて記憶する。

[0085] ユーザ端末記憶部110は、ユーザ端末側参照管理部120による各種処理に必要なデータおよび認証プログラムを格納する。例えば、各種処理に必要なデータとして、後述する復号部127が復号が復号したコンテンツを記憶する。また、ユーザ端末記憶部110は、他の記憶媒体または記憶部から一意に識別する情報であるユーザ端末記憶媒体識別情報が付与されている。例えば、ユーザ端末記憶部110は、後述するように、ユーザ端末100が暗号化コンテンツを復号すると、復号されたコンテンツを記憶する。

[0086] ［管理装置記憶部等］

管理装置記憶部210は、管理装置側参照管理部220による各種処理に必要なデータおよび認証プログラムを格納する。本発明に密接に関連するものとしては、図7に示すように、管理情報記憶部211と、コンテンツ管理簿記憶部212と、認証結果記

憶部213と、アーカイブストレージ装置記憶部214とを備える。ここで、管理情報記憶部211は、特許請求の範囲に記載の「管理情報記憶部」に対応し、コンテンツ管理簿記憶部212は、特許請求の範囲に記載の「コンテンツ管理簿記憶部」に対応し、認証結果記憶部213は、特許請求の範囲に記載の「認証結果記憶部」に対応し、アーカイブストレージ装置記憶部214は、特許請求の範囲に記載の「管理装置記憶部」に対応する。

[0087] 管理情報記憶部211は、真正性を保った暗号化コンテンツを形成するデータをハッシュ関数に代入して予め算出されているハッシュ値である第2のハッシュ値を、アーカイブ管理IDに対応付けて予め記憶する。また、記憶媒体識別情報(アーカイブ管理IDに対応付けて、アーカイブ管理IDによって特定される暗号化コンテンツを記憶する暗号化コンテンツ記憶媒体300を一意に識別する情報)をさらに記憶する。例えば、図9に示すように、管理情報記憶部211は、アーカイブ管理IDに対応付けて、第2のハッシュ値と、当該アーカイブ管理IDによって特定される暗号化コンテンツを復号する処理に用いる復号鍵を示す「復号鍵」と、当該アーカイブ管理IDによって特定される暗号化コンテンツへのアクセスを許可するアクセスユーザを示す「アクセスユーザ」と、記憶媒体識別情報とを記憶する。

[0088] さらに詳細な一例をあげて説明すると、図9に示すように、管理情報記憶部211は、アーカイブ管理ID「0011」と、第2のハッシュ値と「A246K8・・・」と、復号鍵「鍵A」と、アクセスユーザ「山田一郎」と、記憶媒体識別情報「A0112」とを対応付けて記憶し、アーカイブ管理ID「0012」と、第2のハッシュ値と「B3453・・・」と、復号鍵「鍵B」と、アクセスユーザ「山田一郎、山田次郎」と、記憶媒体識別情報「A2222」とを対応付けて記憶する。

[0089] なお、ここでいう第2のハッシュ値とは、真正性を保った暗号化コンテンツを形成するデータから算出される点に特徴があり、例えば、当該暗号化コンテンツが暗号化コンテンツ記憶媒体300に格納される際や、当該暗号化コンテンツが実施例1に係るアーカイブシステムによる管理対象とされた際に算出されるものである。これにより、第2のハッシュ値は、暗号化コンテンツ記憶媒体300の劣化によるデータの変化や不正なデータの改ざんなどの影響を一切受けていない値として算出され、これらの影響を

受けない状態で管理情報記憶部211に記憶されているものである。

[0090] コンテンツ管理簿記憶部212は、格納媒体識別情報(復号されたコンテンツをユーザ端末100が書き込むユーザ端末記憶媒体を一意に識別する情報)を記憶し、対応するコンテンツを廃棄する旨の情報を記憶する。例えば、図10に示すように、コンテンツ管理簿記憶部212は、アーカイブ管理IDと対応付けて、格納媒体識別情報と廃棄する旨の情報とを記憶する。なお、この格納媒体識別情報は、後述するコンテンツ管理簿格納部224によって格納されるものである。さらに詳細な一例をあげて説明すると、図10に示す例では、コンテンツ管理簿記憶部212は、アーカイブ管理ID「0011」と対応付けて、格納媒体識別情報「B111」と、廃棄する旨の情報として「廃棄済み」とを記憶する。

[0091] 認証結果記憶部213は、後述する認証部222による暗号化コンテンツ認証の認証結果が、認証失敗結果(第1のハッシュ値と第2のハッシュ値とが一致しないと認証する認証結果)である場合に、認証失敗結果をアーカイブ管理IDに対応付けて記憶する。また、認証結果記憶部213は、アーカイブ管理IDに対応付けて、暗号化コンテンツ記憶媒体300に何らかの異常があることを示す記憶媒体異常情報を記憶する。なお、この認証結果は、後述する認証結果格納部225によって格納されるものである。例えば、図11に示すように、認証結果記憶部213は、アーカイブ管理IDに対応付けて、認証失敗結果と、記憶媒体異常情報とを対応付けて記憶する。さらに詳細な一例をあげて説明すると、図11に示す例では、認証結果記憶部213は、アーカイブ管理ID「0012」に対応付けて、認証失敗結果「あり」を記憶し、アーカイブ管理ID「0013」に対応付けて、記憶媒体異常情報「あり」を記憶する。

[0092] なお、実施例1では、上記した認証失敗結果および記憶媒体異常情報として、「あり」とのみ記憶する場合について説明するが、本発明はこれに限定されるものではなく、一定期間のアクセスを禁止する旨の情報を書き込んでもよく、また、特定範囲のユーザによるアクセスを禁止する旨の情報を書き込んでもよい。

[0093] アーカイブストレージ装置記憶部214は、暗号化コンテンツや、復号されたコンテンツを記憶する。例えば、復号するコンテンツを管理装置200にて管理する場合に、ユーザ端末100からアップロードされた暗号化コンテンツを記憶し、また、当該暗号化

コンテンツを復号したコンテンツを記憶する。

[0094] [ユーザ端末側参照管理部等]

ユーザ端末側参照管理部120は、認証制御プログラム、各種の処理手順などを規定したプログラムおよび所要データを格納するためのメモリを有し、これらによって種々の処理を実行する。そして、本発明に密接に関連するものとしては、算出部121と、認証問い合わせ部122と、制限情報通知部123と、格納先情報通知部124と、暗号化コンテンツ送信部125と、ユーザ端末側コンテンツ管理部126と、復号部127とを備える。なお、算出部121は、特許請求の範囲に記載の「算出手順」に対応する。

[0095] 算出部121は、暗号化コンテンツ記憶媒体300から、認証対象となる暗号化コンテンツを読み出し、読み出した暗号化コンテンツを形成するデータを管理装置200が有するものと同一のハッシュ関数に代入して第1のハッシュ値を算出する。具体的には、算出部121は、単に暗号化コンテンツを識別するために付与されている情報であるファイル名などだけではなく、暗号化コンテンツ自身を形成するデータを用いて、第1のハッシュ値を算出する。

[0096] 例えば、算出部121は、第1のハッシュ値を算出する際に、ハッシュ関数に代入するデータとして、暗号化コンテンツを形成するデータ全体を設定し、第1のハッシュ値を算出する。言い換えると、算出部121は、アーカイブ管理IDに紐づく暗号化コンテンツのコンテンツ内容全体から、第1のハッシュ値を算出する。また、例えば、算出部121は認証する暗号化コンテンツが指定された際に(または、認証に必要な情報を管理装置200が取得する際に)、その都度第1のハッシュ値を算出する。

[0097] なお、ここで算出する第1のハッシュ値とは、単に暗号化コンテンツを識別するために付与されている情報であるファイル名などだけではなく、暗号化コンテンツ自身を形成するデータを用いて算出される点に特徴があり、例えば、認証する暗号化コンテンツが指定された際に(または、認証に必要な情報を管理装置200が取得する際に)、その都度算出されるものである。これにより、第1のハッシュ値は、認証を行う際に、暗号化コンテンツ記憶媒体300の劣化によるデータの変化や不正なデータの改ざんなどの影響を受けている場合に、これらの影響を受けている(反映している)値として算出されるものである。

[0098] ここで、算出部121は、対応する真正性を保った暗号化コンテンツから第2のハッシュ値を算出する際に用いたハッシュ関数と同一のハッシュ関数をもちいて、対応する暗号化コンテンツから第1のハッシュ値を算出する。

[0099] なお、本実施例では、算出部121は、第1のハッシュ値を算出する際に、ハッシュ関数に代入するデータとして、暗号化コンテンツを形成するデータ全体を設定する場合について説明するが、本発明はこれに限定されるものではなく、暗号化コンテンツの一部分のみを設定し、第1のハッシュ値を算出してもよい。これにより、認証する毎に行う第1のハッシュ値算出処理に必要な時間を短縮することができ、認証処理を迅速に行うことが可能である。

[0100] 認証問い合わせ部122は、ユーザ認証処理および暗号化コンテンツ認証処理を行う際に必要となる情報を管理装置200へと送信する。例えば、認証問い合わせ部122は、ユーザ認証処理の際には、暗号化コンテンツ記憶媒体300から、認証先情報と、アーカイブ管理IDとを取得する。そして、認証問い合わせ部122は、取得した認証先情報を用いて管理装置200にアクセスし、ユーザ認証処理に必要な情報としてアクセスユーザを送信する。つまり、例えば、アクセスユーザとして、ユーザによって「山田一郎」が入力された場合には、「山田一郎」と送信する。

[0101] そして、認証問い合わせ部122は、後述する認証部222から、ユーザ認証処理に関する認証結果を受信する。そして、認証問い合わせ部122は、認証結果が認証成功であるかを判定する。

[0102] なお、ここで、ユーザ認証処理とは、例えば、システムへのログインを行う処理などが該当する。実施例1では、ユーザ認証処理が、ユーザ端末100を使用するユーザがアーカイブシステムを利用できる(または、管理装置200へのアクセスが許可されている)ユーザであるかを認証する場合について説明する。しかし、本発明はこれに限定されるものではなく、どのユーザ端末100から、管理装置200に対するアクセスがなされたかを判定することにより、アーカイブシステムを構成する適切なユーザ端末100からのアクセスであるかどうかを認証してもよい。

[0103] また、本実施例では、ユーザ認証処理の際に、認証問い合わせ部122が、アクセスユーザのみを送信する場合について説明するが、本発明はこれに限定されるもので

はなく、アクセスユーザとともにパスワード（例えば、各アクセスユーザごとに付与されたパスワードなど）を送信し、アーカイブシステムの不正使用を防止してもよい。

[0104] また、認証問い合わせ部122は、暗号化コンテンツ認証処理の際には、アーカイブ管理IDと第1のハッシュ値とを管理装置200に送信する。例えば、認証問い合わせ部122は、暗号化コンテンツ記憶媒体300から、アーカイブ管理IDを取得し、算出部121が算出する第1のハッシュ値と併せて、管理装置200に送信する。

[0105] 制限情報通知部123は、管理装置200（復号制御部223）から受信した制限情報確認処理の確認結果を、ユーザに通知する。例えば、制限情報通知部123は、通知された制限内容を出力する。つまり、例えば、制限情報通知部123は、認証失敗結果ありと出力し、記憶媒体異常情報ありとユーザに通知する。また、例えば、制限情報通知部123は、参照不可である旨を出力する。つまり、例えば、制限情報通知部123は、認証失敗であり参照することはできないと出力部から出力する。つまり、例えば、制限情報通知部123は、アーカイブ管理ID「0012」について認証失敗であり、参照することはできないと出力部から出力する。

[0106] 格納先情報通知部124は、復号されたコンテンツを当該ユーザ端末100が書き込むユーザ端末記憶媒体を一意に識別する格納媒体識別情報を管理装置200に送信する。例えば、格納先情報通知部124は、ユーザ端末100が復号したコンテンツをユーザ端末記憶部110に格納した場合には、格納先情報通知部124は、ユーザ端末記憶部110であると送信する。さらに詳細には、例えば、格納先情報通知部124は、コンテンツを書き込んだユーザ端末100を示す格納媒体識別情報「B111」を送信する。

[0107] 暗号化コンテンツ送信部125は、復号処理において、管理装置200が復号し、その後参照される暗号化コンテンツを、管理装置200へと送信（アップロード）する。

[0108] ユーザ端末側コンテンツ管理部126は、復号済みコンテンツをその後もユーザ端末100にて管理するかを判定する。例えば、ユーザ端末100において、復号済みコンテンツを参照した後削除するのではなく、その後も復号済みコンテンツを管理するかを判定する。また、ユーザ端末側コンテンツ管理部126は、復号済みコンテンツを管理しないと判定した場合には、復号済みコンテンツを廃棄し、復号済みコンテンツ

を廃棄した旨を示す廃棄情報を管理装置200へと送信する。さらに詳細には、ユーザ端末側コンテンツ管理部126は、ユーザによって、ユーザ端末100にてさらに管理する旨の指示が入力されると、ユーザ端末100にてさらに管理すると判定し、ユーザによって、今後管理しない旨の指示が入力されると、管理しないと判定してコンテンツを廃棄する。

[0109] 復号部127は、管理装置200から受信した復号鍵を用いて、参照する暗号化コンテンツを復号する。例えば、アーカイブ管理ID「0011」に対応する暗号化コンテンツを、管理装置200の復号制御部223から取得した鍵Aを用いて復号する。

[0110] [管理装置側参照管理部等]

管理装置側参照管理部220は、認証制御プログラム、各種の処理手順などを規定したプログラムおよび所要データを格納するためのメモリを有し、これらによって種々の処理を実行する。そして、本発明に密接に関連するものとしては、取得部221と、認証部222と、復号制御部223と、コンテンツ管理簿格納部224と、認証結果格納部225と、管理装置側コンテンツ管理部226とを備える。

[0111] なお、ここで、取得部221は、特許請求の範囲に記載の「取得手順」に対応し、認証部222は、特許請求の範囲に記載の「ハッシュ値認証手順」と「失敗結果認証手順」とに対応し、復号制御部223は、特許請求の範囲に記載の「復号制御手順」に対応し、コンテンツ管理簿格納部224は、特許請求の範囲に記載の「管理簿記憶手順」に対応し、認証結果格納部225は、特許請求の範囲に記載の「認証結果記憶手順」に対応する。

[0112] 取得部221は、ユーザ端末(認証問い合わせ部122)から、第1のハッシュ値とアーカイブ管理IDとをユーザ端末100から取得する。例えば、取得部221は、ユーザ認証処理の際に、アクセスユーザとアーカイブ管理IDとを認証問い合わせ部122から取得し、暗号化コンテンツ認証処理の際に、アーカイブ管理IDと第1のハッシュ値とを認証問い合わせ部122から取得する。なお、取得部221が取得する第1のハッシュ値とアーカイブ管理IDとは、後述する認証部222によるユーザ認証処理や暗号化コンテンツ認証処理やアクセスユーザ認証処理に用いられる。

[0113] 認証部222は、ユーザ認証処理や暗号化コンテンツ認証処理やアクセスユーザ認

証処理や制限情報確認処理を行う。例えば、認証部222は、ユーザ認証処理の際に、認証問い合わせ部122からアクセスユーザを受信すると、受信したアクセスユーザが管理装置200にアクセスすることが許可されているユーザか否かを認証し、認証結果をユーザ端末100に送信する。さらに詳細には、認証部222は、受信したアクセスユーザが、管理装置200にアクセスすることが許可されているユーザである場合には、認証成功と送信し、管理装置200にアクセスすることが許可されていないユーザである場合には、認証失敗と送信する。

[0114] また、認証部222は、暗号化コンテンツ認証処理の際に、取得部221が取得したアーカイブ管理IDを検索キーとして対応する第2のハッシュ値を管理情報記憶部211から読み出し、取得部221が取得した第1のハッシュ値と第2のハッシュ値とが一致するかを認証する。

[0115] 例えば、暗号化コンテンツ認証処理とアクセスユーザ認証処理とを併せて行う場合には、認証部222は、受信したアーカイブ管理IDと対応付けて管理情報記憶部211に記憶している第2のハッシュ値と、受信した第1のハッシュ値とが一致し、また、受信したアーカイブ管理IDと対応付けて管理情報記憶部211に記憶しているアクセスユーザと、受信したアクセスユーザとが一致する場合に、認証成功と判定する。一方、上記したハッシュ値やアクセスユーザが一致しない場合に、認証失敗と判定する。

[0116] また、認証部222は、制限情報確認処理の際に、認証結果記憶部213から、取得部221が取得した管理情報を検索キーとして、対応する認証失敗結果または記憶媒体異常情報があるかを認証する。例えば、認証部222は、認証失敗結果または記憶媒体異常情報が認証結果記憶部213に記憶されているかを確認する。さらに詳細な一例をあげると、認証部222は、取得したアーカイブ管理IDを検索キーとして認証結果記憶部213を検索し、当該アーカイブ管理IDに対応付けられて、認証失敗結果または記憶媒体異常情報が認証結果記憶部213に記憶されているかを確認する。図11の例を用いて説明すると、認証部222は、アーカイブ管理ID「0011」を検索キーとする場合に、認証失敗結果または記憶媒体異常情報が認証結果記憶部213に記憶されていないと認証し、アーカイブ管理ID「0012」を検索キーとする場合に、認証失敗結果が認証結果記憶部213に記憶されていると認証する。

[0117] なお、実施例1では、認証部222は、第1のハッシュ値と第2のハッシュ値とが一致するかのみならず（暗号化コンテンツ認証処理のみならず）、認証失敗結果の有無および記憶媒体異常情報の有無を認証する場合（制限情報確認処理を行う場合）について説明する。しかし、本発明はこれに限定されるものではなく、第1のハッシュ値と第2のハッシュ値とが一致するかに関する認証のみを行ってもよく、第1のハッシュ値と第2のハッシュ値とが一致するかに関する認証と、認証失敗結果の有無に関する認証のみを行ってもよい。

[0118] 言い換えると、暗号化コンテンツ認証処理に、『ユーザ認証処理』や『アクセスユーザ認証処理』や『制限情報確認処理』や『認証失敗処理』や『復号処理』の内、任意の一つまたは複数の処理を組み合わせて実施してよい。

[0119] 復号制御部223は、認証部222による認証結果が、第1のハッシュ値と第2のハッシュ値とが一致すると判定する認証成功結果（暗号化コンテンツ認証が認証成功）である場合に、復号する処理を許可する。例えば、復号制御部223は、認証部222による認証結果が、認証成功結果（例えば、暗号化コンテンツ認証が認証成功、ユーザ認証が成功、アクセスユーザ認証が成功）であり、かつ、認証失敗結果および記憶媒体異常情報がないと判定する結果である場合（制限情報確認処理に制限情報なしと確認）に、復号する処理を行うことを許可する。

[0120] なお、実施例1では、復号制御部223は、認証結果のみならず、認証失敗結果の有無および記憶媒体異常情報の有無を用いて、復号制御を行う場合について説明するが、本発明はこれに限定されるものではなく、認証結果のみを用いて復号制御を行ってもよく、認証結果と認証失敗結果との有無のみを用いて復号制御を行ってよい。

[0121] また、復号制御部223は、制限内容をユーザ端末100に通知する。例えば、復号制御部223は、認証部222によって認証失敗結果であると判定されると、認証失敗であるとユーザ端末100に送信する。例えば、復号制御部223は、アーカイブ管理ID「0012」が参照不可である旨をユーザ端末100に通知する。

[0122] また、復号制御部223は、暗号化コンテンツの参照方法として、管理装置200で管理するかを判定する。具体的には、復号制御部223は、管理装置200において復号

して管理するか、または、暗号化コンテンツをユーザ端末100において復号して管理するかを判定する。さらに詳細には、ユーザによって管理装置200にて参照する旨の指示が入力されると、復号制御部223は、管理装置200で管理すると判定し、一方、ユーザによってユーザ端末100にて参照する旨の指示が入力されると、復号制御部223は、ユーザ端末100で管理すると判定する。

[0123] また、例えば、復号制御部223は、参照する暗号化コンテンツに対応する復号鍵を管理情報記憶部211から取得し、ユーザ端末100へと送信する。例えば、図9に例を用いて説明すると、認証部222が認証成功であると判定し、ユーザがユーザ端末100にてコンテンツを参照する旨の指示が入力されると、復号制御部223は、アーカイブ管理ID「0011」に対応付けられた復号鍵「鍵A」を取得し、ユーザ端末100へと送信する。

[0124] なお、復号制御部223は、上記したコンテンツを管理装置200で管理するか否かの判定において、ユーザからの指示を受信する場合について説明したが、本発明はこれに限定されるものではなく、予め設定されている内容に基づいて、復号制御部が、ユーザからの指示を受信せずに、判定してもよい。例えば、コンテンツごとに、参照する場所(例えば、管理装置や、特定のユーザ端末(または、記憶部)など。)を対応付けてテーブルとして記憶しておき、かかるテーブルを用いて参照してもよい。

[0125] コンテンツ管理簿格納部224は、復号制御部223が復号する処理を許可し、ユーザ端末100が暗号化コンテンツを復号鍵を用いて復号した場合に、復号されたコンテンツをユーザ端末100が書き込むユーザ端末記憶媒体を一意に識別する格納媒体識別情報をユーザ端末100から取得してコンテンツ管理簿記憶部212に記憶し、ユーザ端末100がコンテンツを廃棄する際には、廃棄する旨の情報をユーザ端末100から取得してコンテンツ管理簿記憶部212に記憶する。

[0126] 例えば、図10の例を用いて説明すると、コンテンツ管理簿格納部224は、アーカイブ管理ID「0011」に対応付けて、ユーザ端末100(格納先通知部)から取得する格納媒体識別情報「B111」を、コンテンツ管理簿記憶部212に格納する。また、コンテンツ管理簿格納部224は、復号されたコンテンツが廃棄した旨を受信すると、対応するアーカイブ管理IDに対応付けて、ユーザ端末100(格納先通知部)から取得する

廃棄情報を、コンテンツ管理簿記憶部212に格納する。例えば、コンテンツ管理簿格納部224は、アーカイブ管理ID「0011」に対応付けて、廃棄情報「廃棄済み」を格納する。

[0127] 認証結果格納部225は、認証部222による暗号化コンテンツ認証の認証結果が、第1のハッシュ値と第2のハッシュ値とが一致しないと認証する認証失敗結果である場合に、認証失敗結果をアーカイブ管理IDに対応付けて認証結果記憶部213に記憶する。例えば、図11に示すように、認証結果格納部225は、アーカイブ管理ID「0012」に対応付けて認証失敗結果「あり」を認証結果記憶部213に格納する。

[0128] また、認証結果格納部225は、認証部222による暗号化コンテンツ認証の認証結果が認証失敗結果である場合に、取得部221が取得したアーカイブ管理IDを検索キーとして対応する1つの記憶媒体識別情報を管理情報記憶部211から取得し、取得した1つの記憶媒体識別情報を検索キーとして対応する複数の管理情報を取得し、取得したアーカイブ管理IDに対応付けて、記憶媒体異常情報を認証結果記憶部213にさらに記憶する。

[0129] 例えば、認証結果格納部225は、受信したアーカイブ管理IDと対応付けられている暗号化コンテンツが記憶されている暗号化コンテンツ記憶媒体300の識別情報を取得する。つまり、例えば、図9の例を用いて説明すると、認証結果格納部225は、アーカイブ管理ID「0012」に対応付けられている暗号化コンテンツが記憶されている記憶媒体識別情報「A2222」を取得する。続いて、認証結果格納部225は、取得した記憶媒体識別情報に対応付けられているアーカイブ管理IDを取得する。

[0130] 例えば、図9の例を用いて説明すると、認証結果格納部225は、記憶媒体識別情報「A2222」に対応付けられたアーカイブ管理IDである「0013」と「0014」とを取得する。その後、認証結果格納部225は、取得したアーカイブ管理IDに対応付けて、記憶媒体異常情報を格納する。つまり、例えば、図11の例を用いて説明すると、認証結果格納部225は、取得したアーカイブ管理IDである「0013」と「0014」とに対応付けて、記憶媒体異常情報「あり」を認証結果記憶部213に格納する。

[0131] 管理装置側コンテンツ管理部226は、管理装置200にて参照する暗号化コンテンツを復号する。例えば、管理装置側コンテンツ管理部226は、受信した暗号化コンテ

ンツをアーカイブストレージ装置記憶部214に書き込む。そして、管理装置側コンテンツ管理部226は、アップロードされた暗号化コンテンツに対応する復号鍵を管理情報記憶部211から取得し、アップロードされた暗号化コンテンツを復号する。つまり、例えば、図9に例を用いて説明すると、管理装置側コンテンツ管理部226は、アーカイブ管理ID「0011」に対応付けられた復号鍵「鍵A」を取得し、アップロードされた暗号化コンテンツを鍵Aを用いて復号する。

[0132] [実施例1による効果]

上述してきたように、実施例1によれば、ユーザ端末100は、暗号化コンテンツ記憶媒体300から認証対象となる暗号化コンテンツを読み出し、第1のハッシュ値を算出し、管理装置200は、第1のハッシュ値とアーカイブ管理IDとをユーザ端末100から取得し、管理情報記憶部211から、取得したアーカイブ管理IDを検索キーとして対応する第2のハッシュ値を読み出し、第1のハッシュ値と第2のハッシュ値とが一致するかを認証し、認証成功結果である場合に、復号する処理を許可するので、アーカイブシステムのセキュリティを向上することが可能である。

[0133] 例えば、管理IDのみを管理装置200に送信し、ユーザ端末100が復号鍵を取得する(復号鍵を用いた処理の一例)手法や、コンテンツ名からハッシュ値を算出して管理装置200に送信し、ユーザ端末100が復号鍵を取得する手法では、アーカイブ管理IDやコンテンツ名が漏洩することによって、復号鍵が簡単に漏洩してしまうのに対して、本発明を適用することにより、暗号化コンテンツ自体を保持していない限り、認証に必要なハッシュ値を算出して送信することはできず、復号鍵が簡単に漏洩することを防止することが可能であり、アーカイブシステムのセキュリティを向上することが可能である。

[0134] また、暗号化コンテンツ自体を管理装置200に送信するのではなく、暗号化コンテンツから算出されたハッシュ値を送信することによって、認証処理の際に、暗号化コンテンツが漏洩することを防止することが可能であり、アーカイブシステムのセキュリティを向上することが可能である。

[0135] また、本発明を適用することにより、例えば、暗号化コンテンツを記憶している記憶媒体に劣化が生じ、暗号化コンテンツの内容に誤りが発生した場合に、管理装置20

0が、暗号化コンテンツから算出されるハッシュ値に差異が生じていることを認証する結果、管理装置200は、暗号化コンテンツに問題が生じていることを把握することが可能であり、アーカイブシステムのセキュリティを向上することが可能である。

[0136] また、本発明を適用することにより、例えば、第三者によって暗号化コンテンツに改ざんが行われた場合には、管理装置200が、暗号化コンテンツから算出されるハッシュ値に差異が生じていることを認証する結果、管理装置200は、暗号化コンテンツに問題が生じていることを把握することが可能であり、アーカイブシステムのセキュリティを向上することが可能である。

[0137] また、実施例1によれば、管理装置200は、復号制御部223が復号する処理を許可し、その後、ユーザ端末100が暗号化コンテンツを復号鍵を用いて復号した場合に、復号されたコンテンツをユーザ端末100が書き込むユーザ端末記憶媒体を一意に識別する格納媒体識別情報をユーザ端末100から取得してコンテンツ管理簿記憶部212に記憶し、ユーザ端末100がコンテンツを廃棄する際には、廃棄する旨の情報をユーザ端末100から取得してコンテンツ管理簿記憶部212に記憶するので、管理装置200は、復号されたコンテンツが、どの記憶媒体に書き込まれているかを管理することが可能である。

[0138] また、実施例1によれば、管理装置200は、第1のハッシュ値と第2のハッシュ値とが一致しないと認証する認証失敗結果である場合に、認証失敗結果をアーカイブ管理IDに対応付けて記憶する認証結果記憶部213を備え、認証結果記憶部213から取得した管理情報を検索キーとして対応する認証失敗結果があるかを認証し、認証結果が認証成功結果であり、かつ、認証失敗結果がないと認証する結果である場合に、復号する処理を許可するので、認証に失敗している暗号化コンテンツに対する復号処理を制限することが可能である。

[0139] 例えば、暗号化コンテンツを記憶している記憶媒体に劣化が生じ、暗号化コンテンツの内容に誤りが発生した結果、認証に失敗した場合に、管理装置200は、当該暗号化コンテンツに対するアクセスを制限することが可能である。

[0140] また、例えば、第三者によって暗号化コンテンツに改ざんが行われた結果、認証に失敗した場合に、管理装置200は、当該暗号化コンテンツに対するアクセスを制限

することが可能である。

[0141] また、実施例1によれば、暗号化コンテンツ記憶媒体300は、複数の暗号化コンテンツを記憶し、管理装置200は、管理情報記憶部211に、管理情報に対応付けて、管理情報によって特定される暗号化コンテンツを記憶する暗号化コンテンツ記憶媒体300を一意に識別する記憶媒体識別情報をさらに記憶し、認証結果が認証失敗結果である場合に、取得したアーカイブ管理IDを検索キーとして対応する1つの記憶媒体識別情報を管理情報記憶部211から取得し、取得した1つの記憶媒体識別情報を検索キーとして対応する複数のアーカイブ管理IDを取得し、取得したアーカイブ管理IDに対応付けて、記憶媒体異常情報を認証結果記憶部213にさらに記憶し、その上で、認証結果記憶部213から、取得したアーカイブ管理IDを検索キーとして、対応する認証失敗結果または記憶媒体異常情報があるかを認証し、認証結果が、認証成功結果であり、かつ、認証失敗結果および記憶媒体異常情報がないと判定する結果である場合に、復号する処理を行うことを許可するので、管理装置200は、当該暗号化コンテンツ記憶媒体300に記憶されている他の暗号化コンテンツに対するアクセスを制限することが可能である。

[0142] 例えば、実際に認証失敗結果が得られた場合に、該暗号化コンテンツへのアクセスを制限する手法と比較して、本発明を適用することにより、例えば、暗号化コンテンツを記憶している暗号化コンテンツ記憶媒体に劣化が生じて信頼性が低下し、暗号化コンテンツの内容に誤りが発生した結果、認証に失敗した場合に、管理装置は、未だ認証失敗結果がえられていない暗号化コンテンツである場合にも、該暗号化コンテンツ記憶媒体に記憶されている他の暗号化コンテンツに対するアクセスを制限することが可能である。

実施例 2

[0143] さて、これまで、実施例1として、暗号化コンテンツ認証処理の認証失敗結果が得られると、アーカイブ管理IDと対応付けて、認証失敗結果と記憶媒体異常情報とを格納する手法について説明してきたが、本発明はこれに限定されるものではなく、さらに、記憶媒体異常情報等と対応付けられているアーカイブ管理IDが示す暗号化コンテンツについて、マイグレーションを行ってもよい。具体的には、記憶媒体異常情報

が格納されている場合に、言い換えると、記憶媒体になんらかの異常や劣化があると疑われる場合等に、当該記憶媒体に格納されている暗号化コンテンツについて、他記憶媒体に新たに格納してもよい。

[0144] そこで、以下では、認証失敗結果と記憶媒体異常情報とを格納するだけでなく、マイグレーションを行う手法について説明する。なお、以下では、上記実施例に係るアーカイブシステムと同様の点については、簡単に説明することにする。

[0145] すなわち、実施例2に係るアーカイブシステムは、管理装置200において、アーカイブストレージ装置記憶部214が、暗号化コンテンツ記憶媒体300に記憶する暗号化コンテンツと同一の暗号化コンテンツを管理情報に対応付けて記憶する。図8の例を用いて説明すると、暗号化コンテンツ記憶媒体300は、アーカイブ管理IDに対応付けて、暗号化コンテンツを記憶し、例えば、「0011」に対応付けて暗号化コンテンツ「A」を、「0012」に対応付けて「B」を、「0013」に対応付けて「C」を記憶している。このため、アーカイブストレージ装置記憶部214は、暗号化コンテンツ記憶媒体300と同様に、「0011」に対応付けて暗号化コンテンツ「A」を、「0012」に対応付けて「B」を、「0013」に対応付けて「C」を記憶する。

[0146] このような構成のもと、実施例2に係るアーカイブシステムは、実施例1に係るアーカイブシステムが備える構成要素の他に、管理装置200において、管理装置側参照管理部220が、マイグレーション部をさらに備える。なお、マイグレーション部は、特許請求の範囲に記載の「マイグレーション手順」に対応する。

[0147] ここで、マイグレーション部は、認証結果格納部225によって記憶される認証結果記憶部213から、認証失敗結果や記憶媒体異常情報に対応するアーカイブ管理IDを取得し、取得したアーカイブ管理IDを検索キーとして対応する暗号化コンテンツを、アーカイブストレージ装置記憶部214から取得し、取得した暗号化コンテンツについてマイグレーションを行う。

[0148] 例えば、図9および図10の例を用いて説明すると、マイグレーション部は、検索タイミングとなると、認証結果記憶部213から、認証失敗結果および／または記憶媒体異常情報に対応するアーカイブ管理IDである「0012」と「0013」とを取得する。そして、マイグレーション部は、アーカイブストレージ装置記憶部214から、アーカイブ管理I

D「0012」を検索キーとして暗号化コンテンツ「B」を取得し、アーカイブ管理ID「0013」を検索キーとして暗号化コンテンツ「C」取得する。

[0149] そして、例えば、マイグレーション部は、取得した暗号化コンテンツ「B」と「C」とについて、新たな(異なる)暗号化コンテンツ記憶媒体300に格納する。さらに詳細には、マイグレーション部は、暗号化コンテンツ記憶媒体300の内、認証失敗結果や記憶媒体異常情報が対応付けられている暗号化コンテンツ(認証失敗結果や記憶媒体異常情報が対応付けられているアーカイブ管理IDによって特定される暗号化コンテンツ)を格納していない暗号化コンテンツ記憶媒体300を選択し、取得した暗号化コンテンツ「B」と「C」とを格納する。あるいは、マイグレーション部は、未だ使用されていない暗号化コンテンツ記憶媒体300に、取得した暗号化コンテンツ「B」と「C」とを格納する。

[0150] なお、実施例2では、検索タイミングとなると、マイグレーション部がマイグレーションを行う手法について説明したが、本発明はこれに限定されるものではなく、認証失敗結果や記憶媒体異常情報が格納された際に、マイグレーションを行ってもよい。例えば、図5のステップS407の後に、マイグレーションを行ってもよい。

[0151] [実施例2による効果]

上述してきたように、実施例2によれば、管理装置200は、アーカイブストレージ装置記憶部214に、暗号化コンテンツ記憶媒体300に記憶する暗号化コンテンツと同一の暗号化コンテンツをアーカイブ管理IDに対応付けて記憶するものであって、認証結果記憶部213によって記憶される認証結果記憶部213から、認証失敗結果や記憶媒体異常情報に対応するアーカイブ管理IDを取得し、取得したアーカイブ管理IDを検索キーとして対応する暗号化コンテンツを取得し、取得した暗号化コンテンツについてマイグレーションを行うので、管理装置200は、例えば、暗号化コンテンツ記憶媒体300の信頼性が低下している場合に、当該暗号化コンテンツ記憶媒体300に記憶されている暗号化コンテンツについてマイグレーションを行うことで、信頼できるバックアップを保持することが可能である。

[0152] [実施例3]

さて、これまで本発明の実施例について説明したが、本発明は上述した実施例1や

実施例2以外にも、種々の異なる形態にて実施されてよいものである。

[0153] (1)コンテンツの配置

例えば、実施例1では、管理装置200が、アップロードされた暗号化コンテンツを、アーカイブストレージ側記憶部にどのように格納するかについて特に言及しなかったが、管理装置200は、当該コンテンツを、ユーザ端末100において格納されている際と同様のアクセス・配置で格納してもよい。また、例えば、もともと管理装置200に格納されていた暗号化コンテンツを暗号化コンテンツ記憶媒体300に格納し、管理装置200からは当該暗号化コンテンツを廃棄した場合において、ユーザ端末100から(暗号化コンテンツ記憶媒体300から)、当該暗号化コンテンツがアップロードされると、管理装置200は、もともと管理装置200に格納されていた際と同様のアクセス・配置で格納してもよい。これにより、アーカイブシステムは、当該暗号化コンテンツ(または、復号されたコンテンツ)について、以前と同等の参照方法によるアクセスを実現することができ、また、当該暗号化コンテンツ(または、復号されたコンテンツ)を、真正性(アクセスや配置)を保った状態で、ユーザ端末100から容易に管理装置200へとリストアすることが可能となる。

[0154] (2)システム構成等

また、本実施例において説明した各処理のうち、自動的におこなわれるものとして説明した処理の全部または一部を手動的におこなうこともでき、例えば、マイグレーションを行う記憶媒体を、自ら設定し、また、暗号化コンテンツを算出する際にハッシュ関数に代入する範囲の設定を手動で設定してもよい。この他、上記文書中や図面中で示した処理手順、制御手順、具体的名称、各種のデータやパラメータを含む情報(例えば、図2～図10など)については、特記する場合を除いて任意に変更することができる。

[0155] また、図示した各装置の各構成要素は機能概念的なものであり、必ずしも物理的に図示の如く構成されていることを要しない。すなわち、各装置の分散・統合の具体的形態は図示のものに限られず、その全部または一部を、各種の負荷や使用状況などに応じて、任意の単位で機能的または物理的に分散・統合して構成することができる(例えば、図7において、暗号化コンテンツ記憶媒体300をユーザ端末100から分離

してもよく、ユーザ端末側参照管理部120に設けられたユーザ端末側コンテンツ管理部126を管理装置側参照管理部220と統合してもよい)。

[0156] (3)プログラム

ところで、上記実施例1では、ハードウェアロジックによって各種の処理を実現する場合を説明したが、本発明はこれに限定されるものではなく、予め用意されたプログラムをコンピュータで実行することによって実現するようにしてもよい。そこで、以下では、図11を用いて、上記の実施例1に示したアーカイブシステムと同様の機能を有するアーカイブシステム制御プログラムを実行するコンピュータの一例を説明する。なお、図12は、実施例1におけるアーカイブシステムのプログラムを示す図である。

[0157] 同図に示すように、実施例3における管理装置3000は、操作部3001、マイク3002、スピーカ3003、ディスプレイ3005、通信部3006、CPU3010、ROM3011、HDD3012、RAM3013をバス3009などで接続して構成されている。

[0158] ROM3011には、上記の実施例1で示した取得部と、認証部と、復号制御部と、コンテンツ管理簿格納部と、認証結果格納部と、管理装置側コンテンツ管理部と同様の機能を発揮する制御プログラム、つまり、図12に示すように、取得プログラム3011aと、認証プログラム3011bと、復号制御プログラム3011cと、コンテンツ管理簿格納プログラム3011dと、認証結果格納プログラム3011eと、アーカイブ側コンテンツ管理プログラム3011fとが予め記憶されている。なお、これらのプログラム3011a～3011fについては、図7に示した管理装置の各構成要素と同様、適宜統合または分離してもよい。

[0159] そして、CPU3010が、これらのプログラム3011a～3011fをROM3011から読み出して実行することにより、図12に示すように、各プログラム3011a～3011fについては、取得プロセス3010aと、認証プロセス3010bと、復号制御プロセス3010cと、コンテンツ管理簿格納プロセス3010dと、認証結果格納プロセス3010eと、アーカイブ側コンテンツ管理プロセス3010fとして機能するようになる。なお、各プロセス3010a～3010fは、図7に示した、取得部と、認証部と、復号制御部と、コンテンツ管理簿格納部と、認証結果格納部と、管理装置側コンテンツ管理部とにそれぞれ対応する。

[0160] そして、HDD3012には、管理情報テーブル3012aと、コンテンツ管理簿テーブル

3012bと、認証結果テーブル3012cと、アーカイブストレージ装置テーブル3012dとが設けられている。この管理情報テーブル3012aは、管理情報記憶部に対応する。このコンテンツ管理簿テーブル3012bは、コンテンツ管理簿記憶部に対応する。この認証結果テーブル3012cは、認証結果記憶部に対応する。このアーカイブストレージ装置テーブル3012dは、アーカイブストレージ装置記憶部に対応する。

[0161] そして、CPU3010は、HDD3012から管理情報テーブル3012aとコンテンツ管理簿テーブル3012bと認証結果テーブル3012cとアーカイブストレージ装置テーブル3012dとを読み出してRAM3013に格納し、RAM3013に格納された管理情報データ3013aと、コンテンツ管理簿データ3013bと、認証結果データ3013cと、アーカイブストレージ装置データ3013dとを用いて、アーカイブストレージ制御プログラムを実行する。

また、同図に示すように、実施例3におけるユーザ端末3100は、操作部3101、マイク3102、スピーカ3103、ディスプレイ3105、通信部3106、CPU3110、ROM3111、HDD3112、RAM3113をバス3109などで接続して構成されている。

[0162] ROM3111には、上記の実施例1で示した算出部と、認証問い合わせ部と、制限情報通知部と、格納先情報通知部と、暗号化コンテンツ送信部と、ユーザ端末側コンテンツ管理部と、復号部と同様の機能を発揮する制御プログラム、つまり、図12に示すように、算出プログラム3111aと、認証問い合わせプログラム3111bと、制限情報通知プログラム3111cと、格納先情報通知プログラム3111dと、暗号化コンテンツ送信プログラム3111eと、ユーザ側コンテンツ管理プログラム3111fと、復号プログラム3111gとが予め記憶されている。なお、これらのプログラム3111a～3111gについては、図2に示したユーザ端末の各構成要素と同様、適宜統合または分離してもよい。

[0163] そして、CPU3110が、これらのプログラム3111a～3111gをROM3111から読み出して実行することにより、図12に示すように、各プログラム3111a～3111gについては、算出プロセス3110aと、認証問い合わせプロセス3110bと、制限情報通知プロセス3110cと、格納先情報通知プロセス3110dと、暗号化コンテンツ送信プロセス3110eと、ユーザ側コンテンツ管理プロセス3110fと、復号プロセス3110gとして機能するようになる。なお、各プロセス3110a～3110gは、図7に示した、算出部と、認証

問い合わせ部と、制限情報通知部と、格納先情報通知部と、暗号化コンテンツ送信部と、ユーザ端末側コンテンツ管理部と、復号部とにそれぞれ対応する。

[0164] そして、HDD3112には、暗号化コンテンツ記憶媒体テーブル3112aと、ユーザ端末テーブル3112bとが設けられている。この暗号化コンテンツ記憶媒体テーブル3112aは、暗号化コンテンツ記憶媒体に対応する。このユーザ端末テーブル3112bは、ユーザ端末記憶部に対応する。

[0165] そして、CPU3110は、HDD3112から暗号化コンテンツ記憶媒体テーブル3112aとユーザ端末テーブル3112bとを読み出してRAM3113に格納し、RAM3113に格納された暗号化コンテンツ記憶媒体データ3113aと、ユーザ端末データ3113bとを用いて、アーカイブストレージ制御プログラムを実行する。

[0166] (4)その他

なお、本実施例で説明したアーカイブストレージ制御方法は、あらかじめ用意されたプログラムをパーソナルコンピュータやワークステーションなどのコンピュータで実行することによって実現することができる。このプログラムは、インターネットなどのネットワークを介して配布することができる。また、このプログラムは、ハードディスク、フレキシブルディスク(FD)、CD－ROM、MO、DVDなどのコンピュータで読み取り可能な記録媒体に記録され、コンピュータによって記録媒体から読み出されることによって実行することもできる。

産業上の利用可能性

[0167] 以上のように、本発明に係るアーカイブストレージ、アーカイブストレージ制御方法、アーカイブストレージ制御プログラム、管理装置は、ユーザ端末と、管理装置とから構成され、管理装置が、暗号化コンテンツを一意に特定する情報である管理情報をユーザ端末から取得し、管理情報によって特定される暗号化コンテンツを復号鍵を用いて復号する処理を許可するか否かを認証するアーカイブシステムに有用であり、特に、アーカイブシステムのセキュリティを向上するアーカイブストレージ、アーカイブストレージ制御方法、アーカイブストレージ制御プログラム、管理装置の実現に適する。

請求の範囲

[1] 暗号化された暗号化コンテンツを暗号化コンテンツ記憶媒体から参照するユーザ端末と、管理対象とする当該暗号化コンテンツを復号する復号鍵を記憶する管理装置とから構成され、前記管理装置が、前記暗号化コンテンツを一意に特定する情報である管理情報を前記ユーザ端末から取得し、当該管理情報によって特定される当該暗号化コンテンツを当該復号鍵を用いて復号する処理を許可するか否かを認証するアーカイブシステムであって、

前記ユーザ端末は、

前記暗号化コンテンツを前記管理情報に対応付けて記憶する前記暗号化コンテンツ記憶媒体から認証対象となる当該暗号化コンテンツを読み出し、読み出した当該暗号化コンテンツを形成するデータを前記管理装置が有するものと同一のハッシュ関数に代入して第1のハッシュ値を算出する算出手段を備え、

前記管理装置は、

前記算出手段によって算出された第1のハッシュ値と前記管理情報とを前記ユーザ端末から取得する取得手段と、

真正性を保った前記暗号化コンテンツを形成するデータを前記ハッシュ関数に代入して予め算出されているハッシュ値である第2のハッシュ値を前記管理情報に対応付けて記憶する管理情報記憶部から、前記取得手段が取得した前記管理情報を検索キーとして対応する前記第2のハッシュ値を読み出し、当該取得手段が取得した前記第1のハッシュ値と当該第2のハッシュ値とが一致するかを認証するハッシュ値認証手段と、

前記ハッシュ値認証手段による認証結果が、前記第1のハッシュ値と前記第2のハッシュ値とが一致すると判定する認証成功結果である場合に、前記復号する処理を許可する復号制御手段と、

を備えることを特徴とするアーカイブシステム。

[2] 前記復号制御手段が前記復号する処理を許可し、その後、前記ユーザ端末が前記暗号化コンテンツを前記復号鍵を用いて復号した場合に、復号されたコンテンツを当該ユーザ端末が書き込むユーザ端末記憶媒体を一意に識別する格納媒体識別

情報を当該ユーザ端末から取得してコンテンツ管理簿記憶部に記憶し、当該ユーザ端末が前記コンテンツを廃棄する際には、廃棄する旨の情報を当該ユーザ端末から取得してコンテンツ管理簿記憶部に記憶する管理簿記憶手段をさらに備えることを特徴とする請求項1に記載のアーカイブシステム。

[3] 前記ハッシュ値認証手段による認証結果が、前記第1のハッシュ値と前記第2のハッシュ値とが一致しないと認証する認証失敗結果である場合に、当該認証失敗結果を前記管理情報に対応付けて認証結果記憶部に記憶する認証結果記憶手段と、

前記認証結果記憶手段によって前記認証失敗結果を記憶する前記認証結果記憶部から、前記取得手段が取得した前記管理情報を検索キーとして対応する前記認証失敗結果があるかを認証する失敗結果認証手段と、

をさらに備え、

前記復号制御手段は、前記ハッシュ値認証手段による認証結果が、前記認証成功結果であり、かつ、前記失敗結果認証手段による認証結果が、前記認証失敗結果がないと認証する結果である場合に、前記復号する処理を許可することを特徴とする請求項1または2に記載のアーカイブシステム。

[4] 前記暗号化コンテンツ記憶媒体は、複数の暗号化コンテンツを記憶し、

前記管理装置は、前記管理情報記憶部に、前記管理情報に対応付けて、当該管理情報によって特定される暗号化コンテンツを記憶する前記暗号化コンテンツ記憶媒体を一意に識別する記憶媒体識別情報をさらに記憶するものであって、

前記認証結果記憶手段は、前記ハッシュ値認証手段による認証結果が前記認証失敗結果である場合に、前記取得手段が取得した前記管理情報を検索キーとして対応する1つの前記記憶媒体識別情報を前記管理情報記憶部から取得し、取得した1つの前記記憶媒体識別情報を検索キーとして対応する複数の前記管理情報を取得し、取得した前記管理情報に対応付けて、当該暗号化コンテンツ記憶媒体に何らかの異常があることを示す記憶媒体異常情報を認証結果記憶部にさらに記憶し、

前記失敗結果認証手段は、前記認証結果記憶手段によって記憶される前記認証結果記憶部から、前記取得手段が取得した前記管理情報を検索キーとして、対応する前記認証失敗結果または前記記憶媒体異常情報があるかを認証し、

前記復号制御手段は、前記ハッシュ値認証手段による認証結果が、前記認証成功結果であり、かつ、前記失敗結果認証手段による認証結果が、前記認証失敗結果および記憶媒体異常情報がないと判定する結果である場合に、前記復号する処理を行うことを許可することを特徴とする請求項3に記載のアーカイブシステム。

[5] 管理装置記憶部は、暗号化コンテンツ記憶媒体に記憶する前記暗号化コンテンツと同一の暗号化コンテンツを前記管理情報に対応付けて記憶するものであって、

前記認証結果記憶手段によって記憶される前記認証結果記憶部から前記認証失敗結果および／または前記記憶媒体異常情報に対応する管理情報を取得し、取得した当該管理情報を検索キーとして対応する暗号化コンテンツを取得し、取得した当該暗号化コンテンツについてマイグレーションを行うマイグレーション手段をさらに備えることを特徴とする請求項4に記載のアーカイブシステム。

[6] 暗号化された暗号化コンテンツを暗号化コンテンツ記憶媒体から参照するユーザ端末と、管理対象とする当該暗号化コンテンツを復号する復号鍵を記憶する管理装置とから構成され、前記管理装置が、前記暗号化コンテンツを一意に特定する情報である管理情報を前記ユーザ端末から取得し、当該管理情報によって特定される当該暗号化コンテンツを当該復号鍵を用いて復号する処理を許可するか否かを認証するアーカイブシステムを制御する方法をコンピュータに実行させるアーカイブシステム制御プログラムであって、

前記ユーザ端末としてのコンピュータに、

前記暗号化コンテンツを前記管理情報に対応付けて記憶する前記暗号化コンテンツ記憶媒体から認証対象となる当該暗号化コンテンツを読み出し、読み出した当該暗号化コンテンツを形成するデータを前記管理装置が有するものと同一のハッシュ関数に代入して第1のハッシュ値を算出する算出手順を実行させ、

前記管理装置としてのコンピュータに、

前記算出手順によって算出された第1のハッシュ値と前記管理情報とを前記ユーザ端末から取得する取得手順と、

真正性を保った前記暗号化コンテンツを形成するデータを前記ハッシュ関数に代入して予め算出されているハッシュ値である第2のハッシュ値を前記管理情報に対応

付けて記憶する管理情報記憶部から、前記取得手順が取得した前記管理情報を検索キーとして対応する前記第2のハッシュ値を読み出し、当該取得手順が取得した前記第1のハッシュ値と当該第2のハッシュ値とが一致するかを認証するハッシュ値認証手順と、

前記ハッシュ値認証手順による認証結果が、前記第1のハッシュ値と前記第2のハッシュ値とが一致すると判定する認証成功結果である場合に、前記復号する処理を許可する復号制御手順と、

を実行させることを特徴とするアーカイブシステム制御プログラム。

[7] 前記管理装置としてのコンピュータに、

前記復号制御手順が前記復号する処理を許可し、その後、前記ユーザ端末が前記暗号化コンテンツを前記復号鍵を用いて復号した場合に、復号されたコンテンツを当該ユーザ端末が書き込むユーザ端末記憶媒体を一意に識別する格納媒体識別情報を当該ユーザ端末から取得してコンテンツ管理簿記憶部に記憶し、当該ユーザ端末が前記コンテンツを廃棄する際には、廃棄する旨の情報を当該ユーザ端末から取得してコンテンツ管理簿記憶部に記憶する管理簿記憶手順をさらに実行させることを特徴とする請求項6に記載のアーカイブシステム制御プログラム。

[8] 前記管理装置としてのコンピュータに、

前記ハッシュ値認証手順による認証結果が、前記第1のハッシュ値と前記第2のハッシュ値とが一致しないと認証する認証失敗結果である場合に、当該認証失敗結果を前記管理情報に対応付けて認証結果記憶部に記憶する認証結果記憶手順と、

前記認証結果記憶手順によって前記認証失敗結果を記憶する前記認証結果記憶部から、前記取得手順が取得した前記管理情報を検索キーとして対応する前記認証失敗結果があるかを認証する失敗結果認証手順と、

をさらに実行させ、

前記復号制御手順は、前記ハッシュ値認証手順による認証結果が、前記認証成功結果であり、かつ、前記失敗結果認証手順による認証結果が、前記認証失敗結果がないと認証する結果である場合に、前記復号する処理を許可することを特徴とする請求項6または7に記載のアーカイブシステム制御プログラム。

[9] 前記暗号化コンテンツ記憶媒体は、複数の暗号化コンテンツを記憶し、

前記管理装置としてのコンピュータは、前記管理情報記憶部に、前記管理情報に対応付けて、当該管理情報によって特定される暗号化コンテンツを記憶する前記暗号化コンテンツ記憶媒体を一意に識別する記憶媒体識別情報をさらに記憶するものであって、

前記認証結果記憶手順は、前記ハッシュ値認証手順による認証結果が前記認証失敗結果である場合に、前記取得手順が取得した前記管理情報を検索キーとして対応する1つの前記記憶媒体識別情報を前記管理情報記憶部から取得し、取得した1つの前記記憶媒体識別情報を検索キーとして対応する複数の前記管理情報を取得し、取得した前記管理情報に対応付けて、当該暗号化コンテンツ記憶媒体に何らかの異常があることを示す記憶媒体異常情報を認証結果記憶部にさらに記憶し、

前記失敗結果認証手順は、前記認証結果記憶手順によって記憶される前記認証結果記憶部から、前記取得手順が取得した前記管理情報を検索キーとして、対応する前記認証失敗結果または前記記憶媒体異常情報があるかを認証し、

前記復号制御手順は、前記ハッシュ値認証手順による認証結果が、前記認証成功結果であり、かつ、前記失敗結果認証手順による認証結果が、前記認証失敗結果および記憶媒体異常情報がないと判定する結果である場合に、前記復号する処理を行うことを許可することを特徴とする請求項8に記載のアーカイブシステム制御プログラム。

[10] 前記管理装置としてのコンピュータは、管理装置記憶部に、暗号化コンテンツ記憶媒体に記憶する前記暗号化コンテンツと同一の暗号化コンテンツを前記管理情報に対応付けて記憶するものであって、

前記認証結果記憶手順によって記憶される前記認証結果記憶部から前記認証失敗結果および／または前記記憶媒体異常情報に対応する管理情報を取得し、取得した当該管理情報を検索キーとして対応する暗号化コンテンツを取得し、取得した当該暗号化コンテンツについてマイグレーションを行うマイグレーション手順をさらに前記管理装置としてのコンピュータに実行させることを特徴とする請求項9に記載のアーカイブシステム制御プログラム。

[11] 管理対象とする暗号化コンテンツを復号する復号鍵を記憶し、暗号化された暗号化コンテンツを暗号化コンテンツ記憶媒体から参照するユーザ端末から、前記暗号化コンテンツを一意に特定する情報である管理情報を取得し、当該管理情報によって特定される当該暗号化コンテンツを当該復号鍵を用いて復号する処理を許可するか否かを認証する管理装置であって、

算出手段によって算出された第1のハッシュ値と前記管理情報とを前記ユーザ端末から取得する取得手段と、

真正性を保った前記暗号化コンテンツを形成するデータをハッシュ関数に代入して予め算出されているハッシュ値である第2のハッシュ値を前記管理情報に対応付けて記憶する管理情報記憶部から、前記取得手段が取得した前記管理情報を検索キーとして対応する前記第2のハッシュ値を読み出し、当該取得手段が取得した前記第1のハッシュ値と当該第2のハッシュ値とが一致するかを認証するハッシュ値認証手段と、

前記ハッシュ値認証手段による認証結果が、前記第1のハッシュ値と前記第2のハッシュ値とが一致すると判定する認証成功結果である場合に、前記復号する処理を許可する復号制御手段と、

を備えることを特徴とする管理装置。

[12] 前記復号制御手段が前記復号する処理を許可し、その後、前記ユーザ端末が前記暗号化コンテンツを前記復号鍵を用いて復号した場合に、復号されたコンテンツを当該ユーザ端末が書き込むユーザ端末記憶媒体を一意に識別する格納媒体識別情報を当該ユーザ端末から取得してコンテンツ管理簿記憶部に記憶し、当該ユーザ端末が前記コンテンツを廃棄する際には、廃棄する旨の情報を当該ユーザ端末から取得してコンテンツ管理簿記憶部に記憶する管理簿記憶手段をさらに備えることを特徴とする請求項11に記載の管理装置。

[13] 前記ハッシュ値認証手段による認証結果が、前記第1のハッシュ値と前記第2のハッシュ値とが一致しないと認証する認証失敗結果である場合に、当該認証失敗結果を前記管理情報に対応付けて認証結果記憶部に記憶する認証結果記憶手段と、

前記認証結果記憶手段によって前記認証失敗結果を記憶する前記認証結果記憶

部から、前記取得手段が取得した前記管理情報を検索キーとして対応する前記認証失敗結果があるかを認証する失敗結果認証手段と、

をさらに備え、

前記復号制御手段は、前記ハッシュ値認証手段による認証結果が、前記認証成功結果であり、かつ、前記失敗結果認証手段による認証結果が、前記認証失敗結果がないと認証する結果である場合に、前記復号する処理を許可することを特徴とする請求項11または12に記載の管理装置。

[14] 前記暗号化コンテンツ記憶媒体は、複数の暗号化コンテンツを記憶し、

前記管理装置は、前記管理情報記憶部に、前記管理情報に対応付けて、当該管理情報によって特定される暗号化コンテンツを記憶する前記暗号化コンテンツ記憶媒体を一意に識別する記憶媒体識別情報をさらに記憶するものであって、

前記認証結果記憶手段は、前記ハッシュ値認証手段による認証結果が前記認証失敗結果である場合に、前記取得手段が取得した前記管理情報を検索キーとして対応する1つの前記記憶媒体識別情報を前記管理情報記憶部から取得し、取得した1つの前記記憶媒体識別情報を検索キーとして対応する複数の前記管理情報を取得し、取得した前記管理情報に対応付けて、当該暗号化コンテンツ記憶媒体に何らかの異常があることを示す記憶媒体異常情報を認証結果記憶部にさらに記憶し、

前記失敗結果認証手段は、前記認証結果記憶手段によって記憶される前記認証結果記憶部から、前記取得手段が取得した前記管理情報を検索キーとして、対応する前記認証失敗結果または前記記憶媒体異常情報があるかを認証し、

前記復号制御手段は、前記ハッシュ値認証手段による認証結果が、前記認証成功結果であり、かつ、前記失敗結果認証手段による認証結果が、前記認証失敗結果および記憶媒体異常情報がないと判定する結果である場合に、前記復号する処理を行うことを許可することを特徴とする請求項13に記載の管理装置。

[15] 前記管理装置は、管理装置記憶部に、暗号化コンテンツ記憶媒体に記憶する前記暗号化コンテンツと同一の暗号化コンテンツを前記管理情報に対応付けて記憶するものであって、

前記認証結果記憶手段によって記憶される前記認証結果記憶部から前記認証失

敗結果および／または前記記憶媒体異常情報に対応する管理情報を取得し、取得した当該管理情報を検索キーとして対応する暗号化コンテンツを取得し、取得した当該暗号化コンテンツについてマイグレーションを行うマイグレーション手段をさらに備えることを特徴とする請求項14に記載の管理装置。

[16] 暗号化された暗号化コンテンツを暗号化コンテンツ記憶媒体から参照するユーザ端末と、管理対象とする当該暗号化コンテンツを復号する復号鍵を記憶する管理装置とから構成され、前記管理装置が、前記暗号化コンテンツを一意に特定する情報である管理情報を前記ユーザ端末から取得し、当該管理情報によって特定される当該暗号化コンテンツを当該復号鍵を用いて復号する処理を許可するか否かを認証する制御方法であって、

前記ユーザ端末は、

前記暗号化コンテンツを前記管理情報に対応付けて記憶する前記暗号化コンテンツ記憶媒体から認証対象となる当該暗号化コンテンツを読み出し、読み出した当該暗号化コンテンツを形成するデータを前記管理装置が有するものと同一のハッシュ関数に代入して第1のハッシュ値を算出する算出ステップを含み、

前記管理装置は、

前記算出ステップによって算出された第1のハッシュ値と前記管理情報とを前記ユーザ端末から取得する取得ステップと、

真正性を保った前記暗号化コンテンツを形成するデータを前記ハッシュ関数に代入して予め算出されているハッシュ値である第2のハッシュ値を前記管理情報に対応付けて記憶する管理情報記憶部から、前記取得ステップが取得した前記管理情報を検索キーとして対応する前記第2のハッシュ値を読み出し、当該取得ステップが取得した前記第1のハッシュ値と当該第2のハッシュ値とが一致するかを認証するハッシュ値認証ステップと、

前記ハッシュ値認証ステップによる認証結果が、前記第1のハッシュ値と前記第2のハッシュ値とが一致すると判定する認証成功結果である場合に、前記復号する処理を許可する復号制御ステップと、

を含むことを特徴とする制御方法。

[17] 前記管理装置は、

前記復号制御ステップが前記復号する処理を許可し、その後、前記ユーザ端末が前記暗号化コンテンツを前記復号鍵を用いて復号した場合に、復号されたコンテンツを当該ユーザ端末が書き込むユーザ端末記憶媒体を一意に識別する格納媒体識別情報を当該ユーザ端末から取得してコンテンツ管理簿記憶部に記憶し、当該ユーザ端末が前記コンテンツを廃棄する際には、廃棄する旨の情報を当該ユーザ端末から取得してコンテンツ管理簿記憶部に記憶する管理簿記憶ステップをさらに含むことを特徴とする請求項16に記載の制御方法。

[18] 前記管理装置は、

前記ハッシュ値認証ステップによる認証結果が、前記第1のハッシュ値と前記第2のハッシュ値とが一致しないと認証する認証失敗結果である場合に、当該認証失敗結果を前記管理情報に対応付けて認証結果記憶部に記憶する認証結果記憶ステップと、

前記認証結果記憶ステップによって前記認証失敗結果を記憶する前記認証結果記憶部から、前記取得ステップが取得した前記管理情報を検索キーとして対応する前記認証失敗結果があるかを認証する失敗結果認証ステップと、

をさらに含み、

前記復号制御ステップは、前記ハッシュ値認証ステップによる認証結果が、前記認証成功結果であり、かつ、前記失敗結果認証ステップによる認証結果が、前記認証失敗結果がないと認証する結果である場合に、前記復号する処理を許可することを特徴とする請求項16または17に記載の制御方法。

[19] 前記暗号化コンテンツ記憶媒体は、複数の暗号化コンテンツを記憶し、

前記管理装置は、前記管理情報記憶部に、前記管理情報に対応付けて、当該管理情報によって特定される暗号化コンテンツを記憶する前記暗号化コンテンツ記憶媒体を一意に識別する記憶媒体識別情報をさらに記憶するものであって、

前記認証結果記憶ステップは、前記ハッシュ値認証ステップによる認証結果が前記認証失敗結果である場合に、前記取得ステップが取得した前記管理情報を検索キーとして対応する1つの前記記憶媒体識別情報を前記管理情報記憶部から取得

し、取得した1つの前記記憶媒体識別情報を検索キーとして対応する複数の前記管理情報を取得し、取得した前記管理情報に対応付けて、当該暗号化コンテンツ記憶媒体に何らかの異常があることを示す記憶媒体異常情報を認証結果記憶部にさらに記憶し、

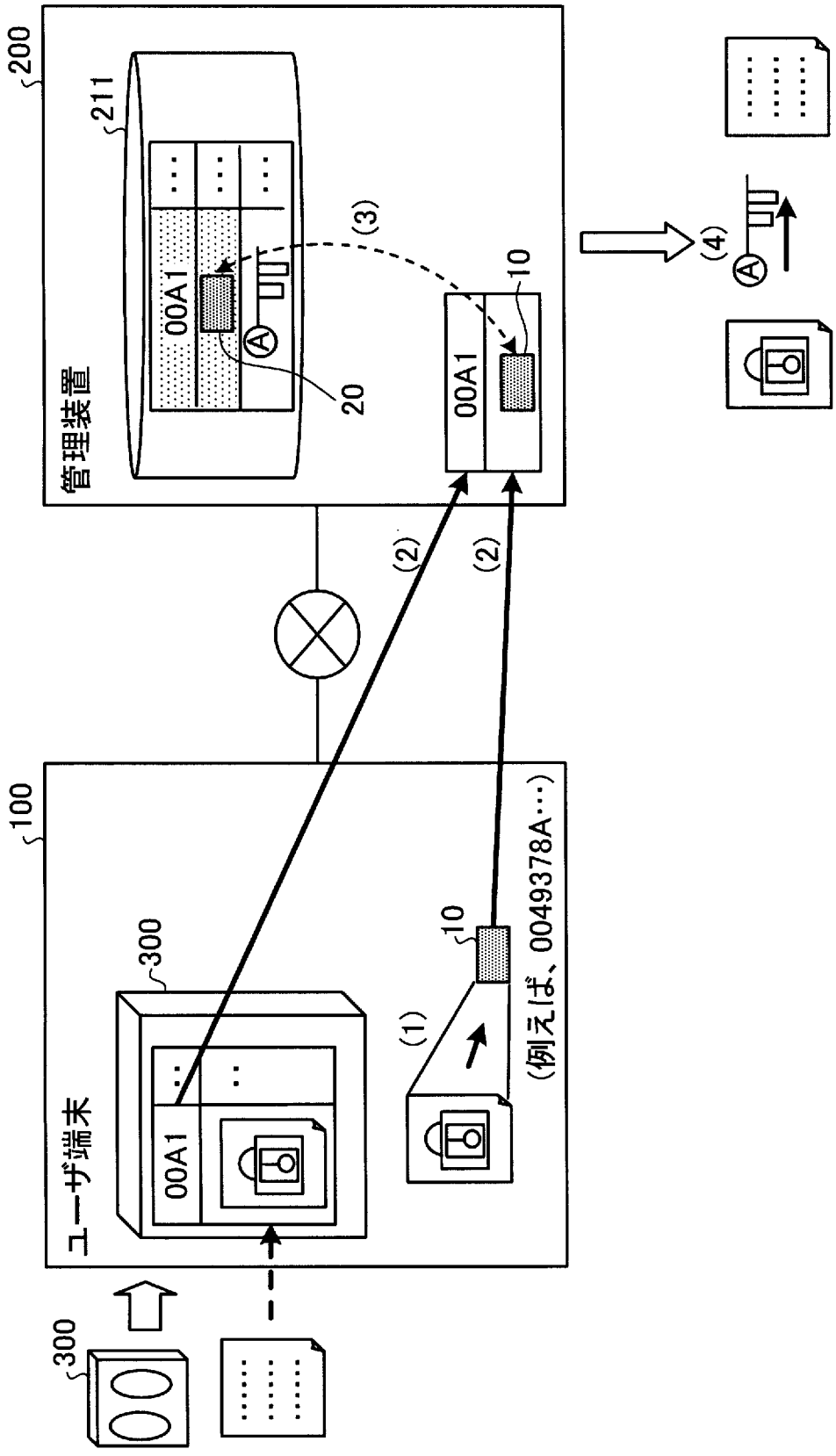
前記失敗結果認証ステップは、前記認証結果記憶ステップによって記憶される前記認証結果記憶部から、前記取得ステップが取得した前記管理情報を検索キーとして、対応する前記認証失敗結果または前記記憶媒体異常情報があるかを認証し、

前記復号制御ステップは、前記ハッシュ値認証ステップによる認証結果が、前記認証成功結果であり、かつ、前記失敗結果認証ステップによる認証結果が、前記認証失敗結果および記憶媒体異常情報がないと判定する結果である場合に、前記復号する処理を行うことを許可することを特徴とする請求項18に記載の制御方法。

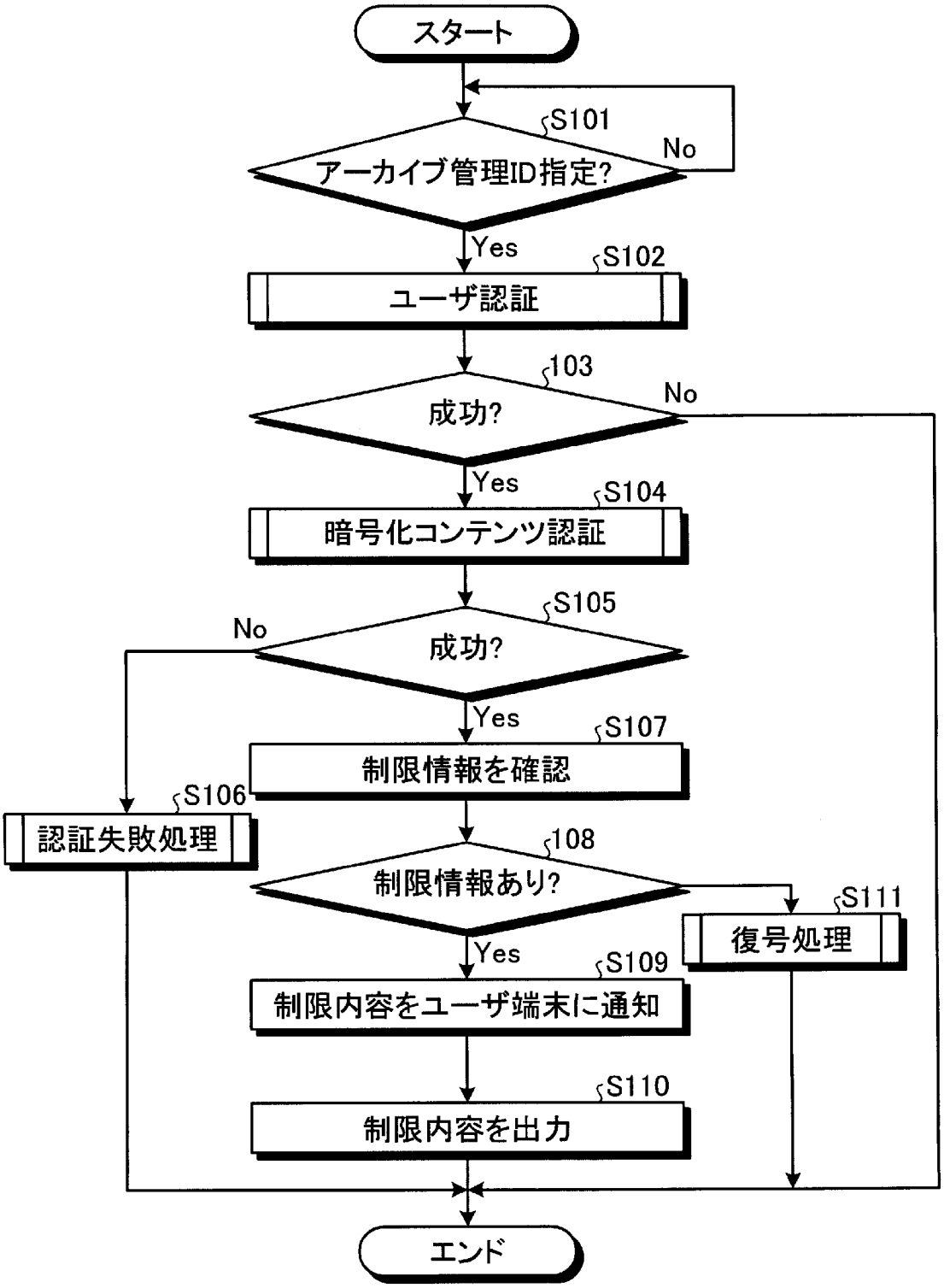
[20] 前記管理装置は、管理装置記憶部に、暗号化コンテンツ記憶媒体に記憶する前記暗号化コンテンツと同一の暗号化コンテンツを前記管理情報に対応付けて記憶するものであって、

前記認証結果記憶ステップによって記憶される前記認証結果記憶部から前記認証失敗結果および／または前記記憶媒体異常情報に対応する管理情報を取得し、取得した当該管理情報を検索キーとして対応する暗号化コンテンツを取得し、取得した当該暗号化コンテンツについてマイグレーションを行うマイグレーションステップをさらに含むことを特徴とする請求項19に記載の制御方法。

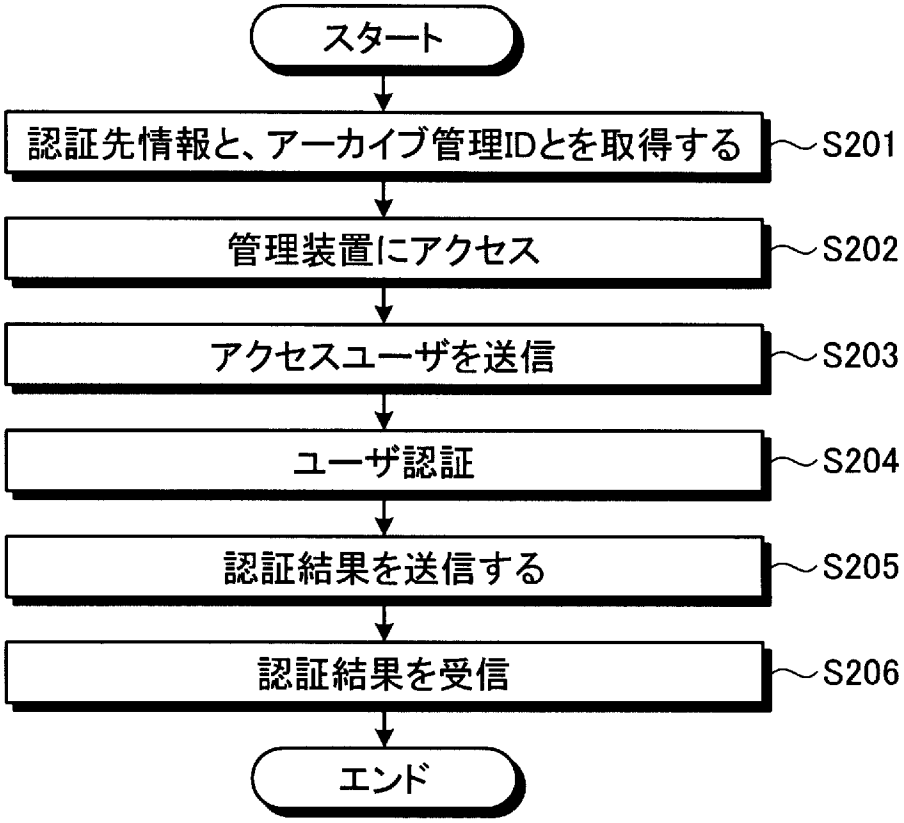
[図1]


200
211
00A1
20
管理装置
(3)
10
00A1
(4)
(2)
(2)
100
300
00A1
10
(1)
(例えば、0049378A…)
ユーザ端末
300

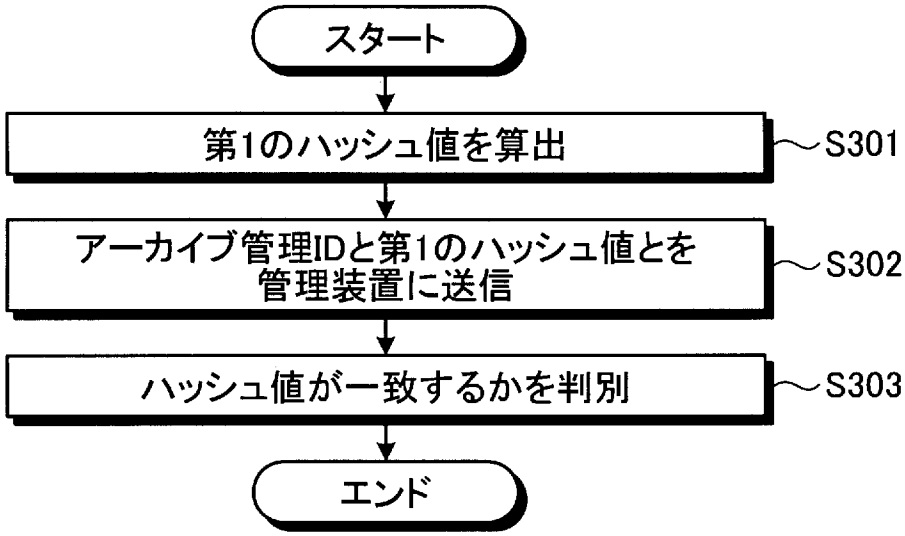
[図2]


スタート
S101
アーカイブ管理ID指定?
No
Yes
S102
ユーザ認証
103
成功?
No
Yes
S104
暗号化コンテンツ認証
S105
No
成功?
Yes
S107
制限情報を確認
S106
認証失敗処理
108
制限情報あり?
S111
復号処理
Yes
S109
制限内容をユーザ端末に通知
S110
制限内容を出力
エンド

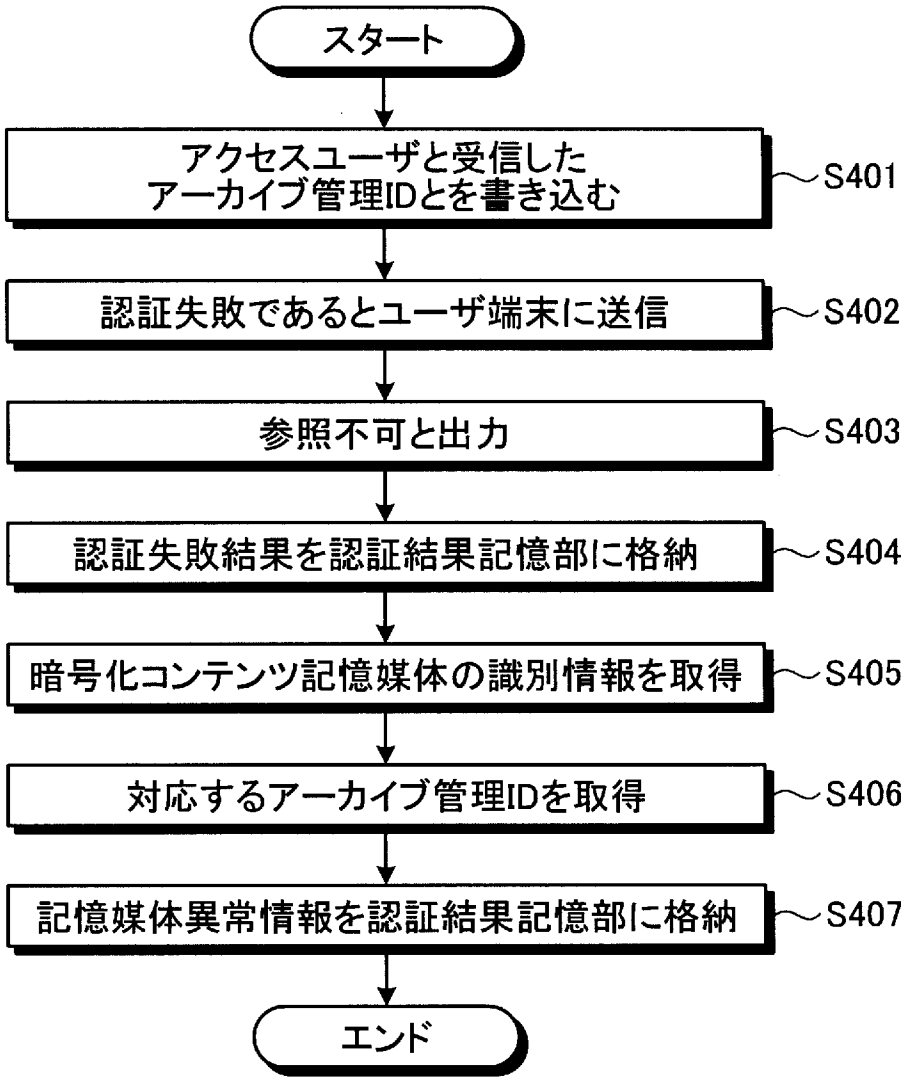
[図3]


スタート
認証先情報と、アーカイブ管理IDとを取得する
S201
管理装置にアクセス
S202
アクセスユーザを送信
S203
ユーザ認証
S204
認証結果を送信する
S205
認証結果を受信
S206
エンド

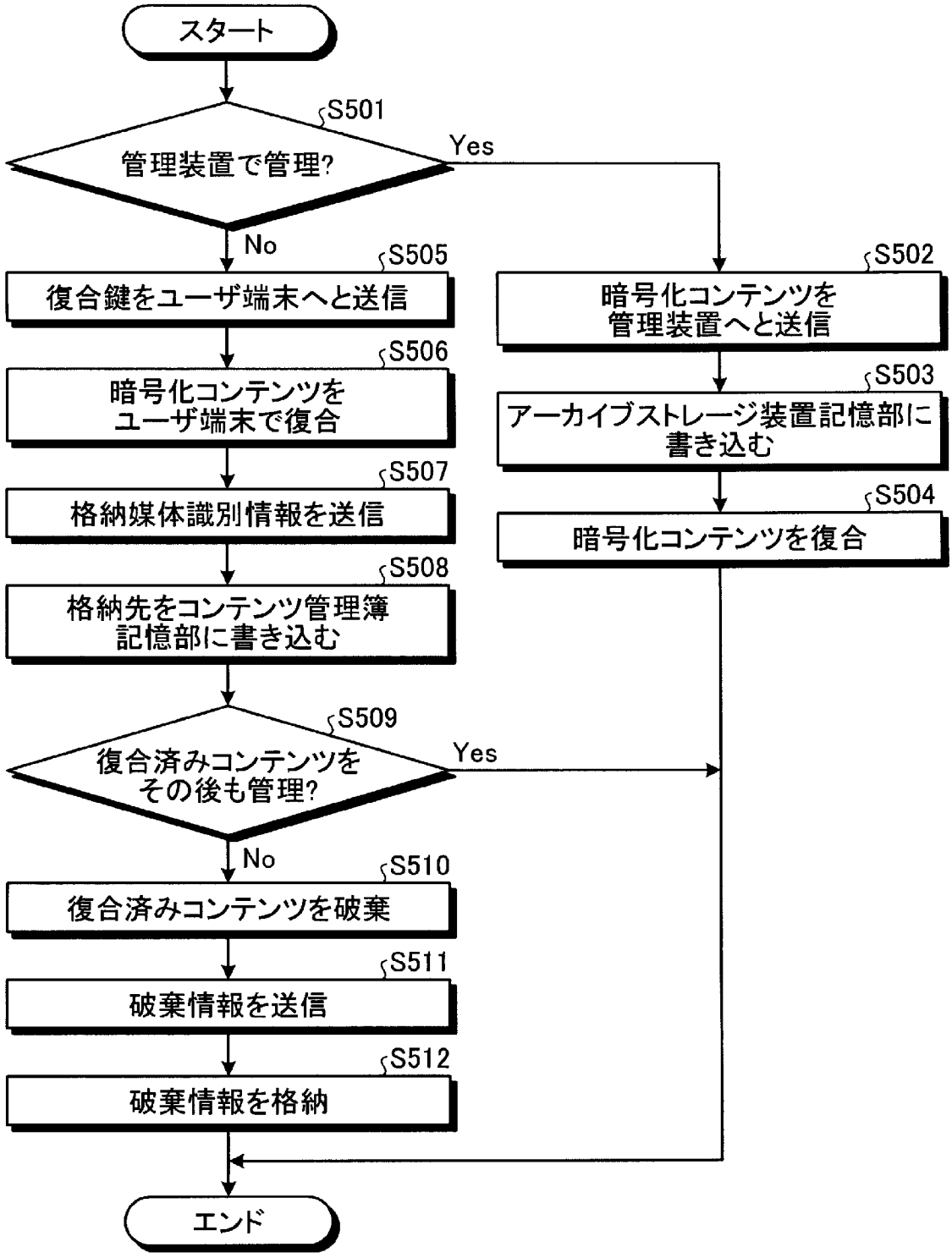
[図4]


スタート
第1のハッシュ値を算出
S301
アーカイブ管理IDと第1のハッシュ値とを
管理装置に送信
S302
ハッシュ値が一致するかを判別
S303
エンド

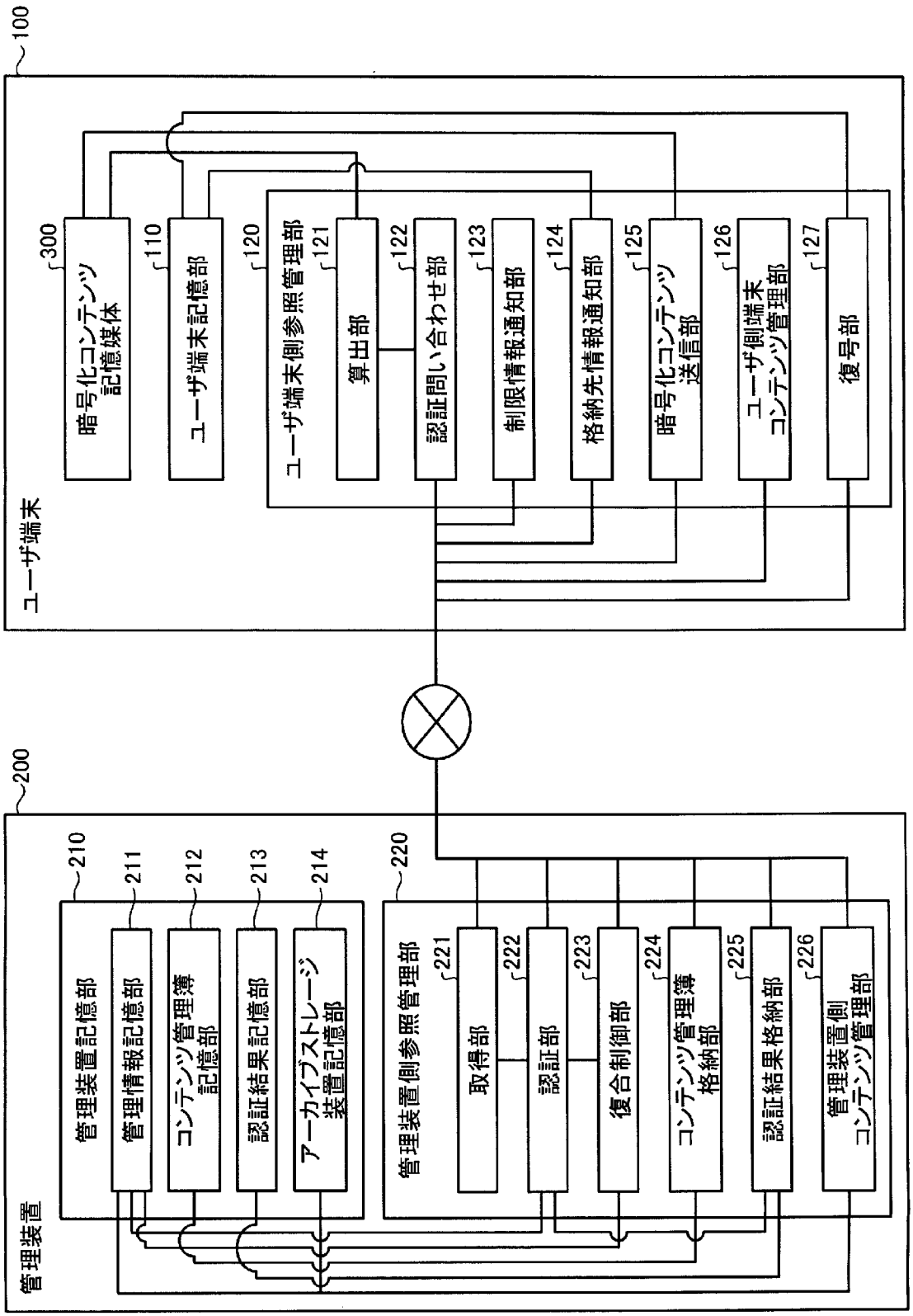
[図5]


スタート
アクセスユーザと受信した
アーカイブ管理IDとを書き込む
S401
認証失敗であるとユーザ端末に送信
S402
参照不可と出力
S403
認証失敗結果を認証結果記憶部に格納
S404
暗号化コンテンツ記憶媒体の識別情報を取得
S405
対応するアーカイブ管理IDを取得
S406
記憶媒体異常情報を認証結果記憶部に格納
S407
エンド

[図6]


スタート
S501
管理装置で管理?
Yes
No
S505
復合鍵をユーザ端末へと送信
S506
暗号化コンテンツを
ユーザ端末で復合
S507
格納媒体識別情報を送信
S508
格納先をコンテンツ管理簿
記憶部に書き込む
S509
復合済みコンテンツを
その後も管理?
Yes
No
S510
復合済みコンテンツを破棄
S511
破棄情報を送信
S512
破棄情報を格納
エンド
S502
暗号化コンテンツを
管理装置へと送信
S503
アーカイブストレージ装置記憶部に
書き込む
S504
暗号化コンテンツを復合

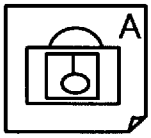
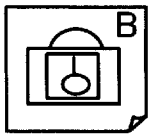
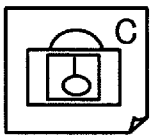
[図7]


100
ユーザ端末
300
暗号化コンテンツ記憶媒体
110
ユーザ端末記憶部
120
ユーザ端末側参照管理部
121
算出部
122
認証問い合わせ部
123
制限情報通知部
124
格納先情報通知部
125
暗号化コンテンツ送信部
126
ユーザ側端末コンテンツ管理部
127
復号部
200
管理装置
210
管理装置記憶部
211
管理情報記憶部
212
コンテンツ管理簿記憶部
213
認証結果記憶部
214
アーカイブストレージ装置記憶部
220
管理装置側参照管理部
221
取得部
222
認証部
223
復合制御部
224
コンテンツ管理簿格納部
225
認証結果格納部
226
管理装置側コンテンツ管理部

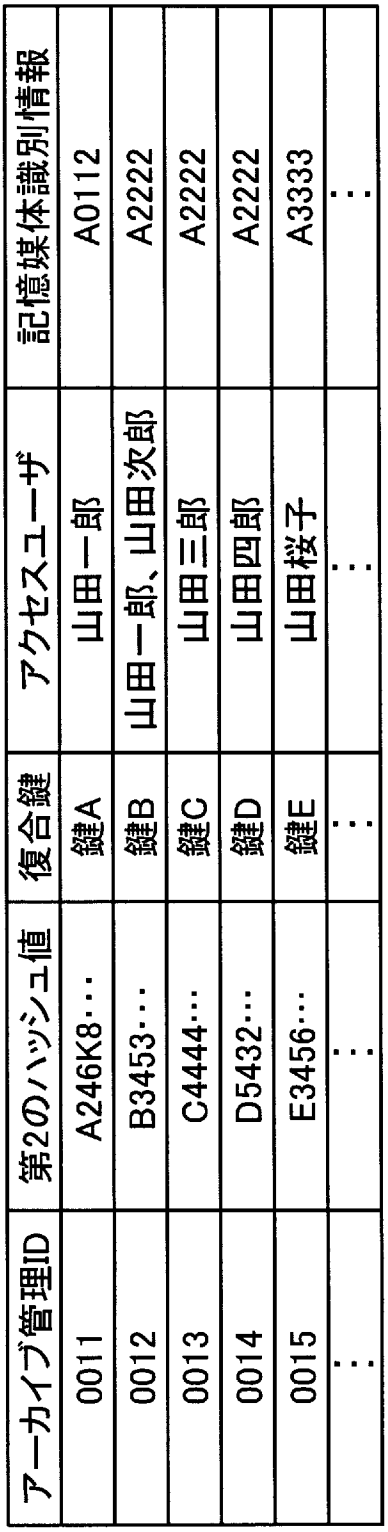
[図8]

記憶媒体識別情報	A0112

認証先情報	211.9.・・・

アーカイブ管理ID	暗号化コンテンツ
0011	
0012	
0013	
⋮	⋮

[図9]



アーカイブ管理ID	第2のハッシュ値	復合鍵	アクセスユーザ	記憶媒体識別情報
0011	A246K8…	鍵A	山田一郎	A0112
0012	B3453…	鍵B	山田一郎、山田次郎	A2222
0013	C4444…	鍵C	山田三郎	A2222
0014	D5432…	鍵D	山田四郎	A2222
0015	E3456…	鍵E	山田桜子	A3333
⋮	⋮	⋮	⋮	⋮

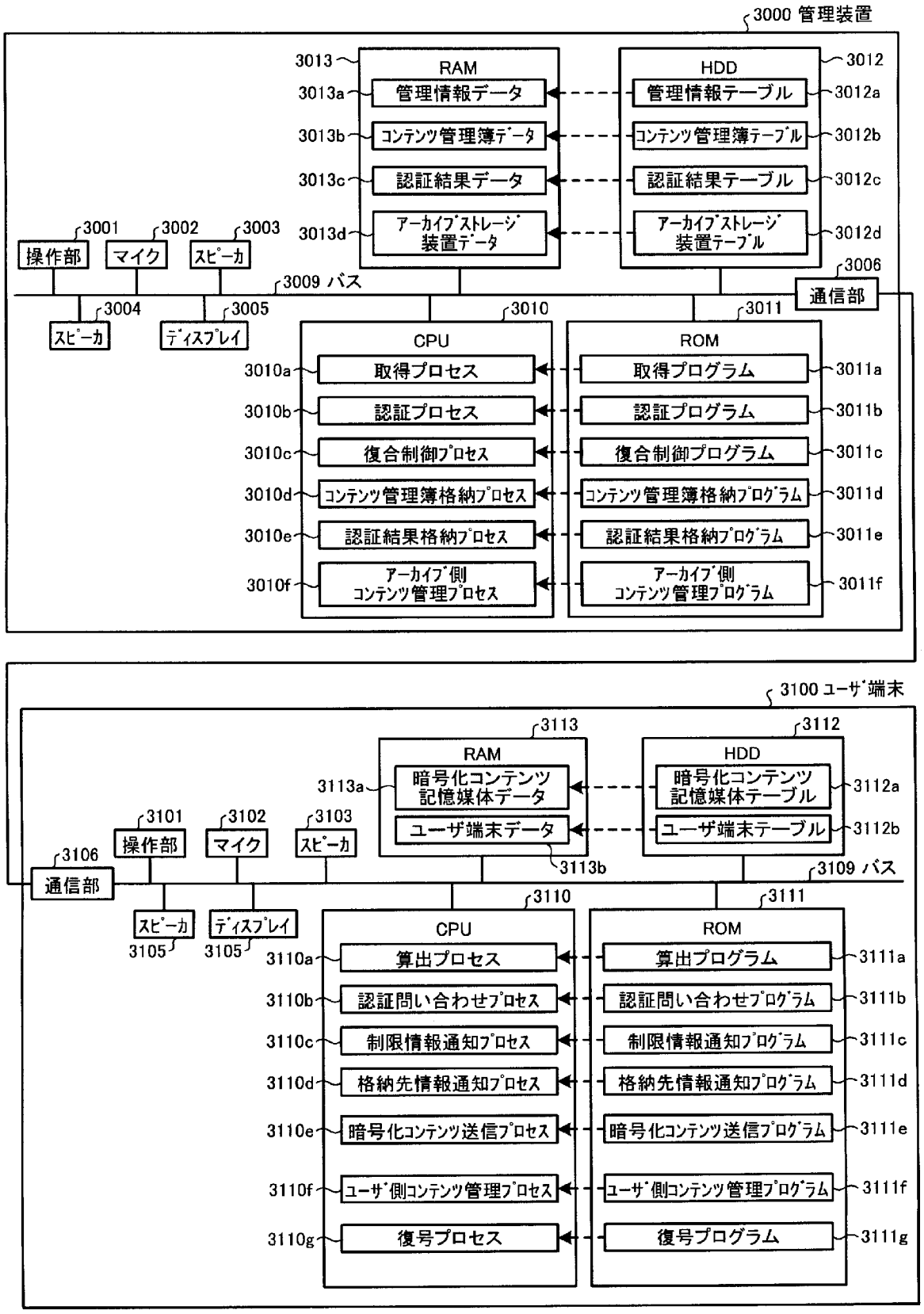
[図10]

アーカイブ管理ID	格納媒体識別情報	破棄情報
0011	B111	破棄済み
⋮	⋮	⋮

[図11]

アーカイブ管理ID	認証失敗結果	記憶媒体異常情報
0012	あり	
0013		あり
0014		あり
⋮	⋮	⋮

[図12]


3000 管理装置
3013
RAM
3013a
管理情報データ
3013b
コンテンツ管理簿データ
3013c
認証結果データ
3013d
アーカイブストレージ装置データ
HDD
3012
管理情報テーブル
3012a
コンテンツ管理簿テーブル
3012b
認証結果テーブル
3012c
アーカイブストレージ装置テーブル
3012d
3001 操作部
3002 マイク
3003 スピーカ
3009 バス
3006 通信部
3004 スピーカ
3005 ディスプレイ
3010
CPU
3010a 取得プロセス
3010b 認証プロセス
3010c 複合制御プロセス
3010d コンテンツ管理簿格納プロセス
3010e 認証結果格納プロセス
3010f アーカイブ側コンテンツ管理プロセス
3011
ROM
3011a 取得プログラム
3011b 認証プログラム
3011c 複合制御プログラム
3011d コンテンツ管理簿格納プログラム
3011e 認証結果格納プログラム
3011f アーカイブ側コンテンツ管理プログラム
3100 ユーザ端末
3113
RAM
3113a 暗号化コンテンツ記憶媒体データ
ユーザ端末データ
3113b
3112
HDD
3112a 暗号化コンテンツ記憶媒体テーブル
3112b ユーザ端末テーブル
3101 操作部
3102 マイク
3103 スピーカ
3106 通信部
3109 バス
スピーカ 3105
ディスプレイ 3105
3110
CPU
3110a 算出プロセス
3110b 認証問い合わせプロセス
3110c 制限情報通知プロセス
3110d 格納先情報通知プロセス
3110e 暗号化コンテンツ送信プロセス
3110f ユーザ側コンテンツ管理プロセス
3110g 復号プロセス
3111
ROM
3111a 算出プログラム
3111b 認証問い合わせプログラム
3111c 制限情報通知プログラム
3111d 格納先情報通知プログラム
3111e 暗号化コンテンツ送信プログラム
3111f ユーザ側コンテンツ管理プログラム
3111g 復号プログラム

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2007/072028

A. CLASSIFICATION OF SUBJECT MATTER
G06F21/24(2006.01)i, *G06F12/00*(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)
G06F21/24, G06F12/00

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 1996-2007
Kokai Jitsuyo Shinan Koho 1971-2007 Toroku Jitsuyo Shinan Koho 1994-2007

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.
Y A	JP 2005-71245 A (Victor Company Of Japan, Ltd.), 17 March, 2005 (17.03.05), Par. Nos. [0041] to [0064]; Fig. 4 (Family: none)	1-2,6-7, 11-12,16-17 3-5,8-10, 13-15,18-20
Y A	US 2006/0075245 A1 (Meier), 06 April, 2006 (06.04.06), Par. No. [0081] & EP 1643402 A2	1-2,6-7, 11-12,16-17 3-5,8-10, 13-15,18-20
Y	JP 2004-46592 A (Fujitsu Ltd.), 12 February, 2004 (12.02.04), Abstract & US 2004/0010509 A1	2,7,12,17

☒ 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
12 December, 2007 (12.12.07)	25 December, 2007 (25.12.07)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2007/072028

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 2004-185500 A (Matsushita Electric Industrial Co., Ltd.), 02 July, 2004 (02.07.04), Full text; all drawings (Family: none)	1-20

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２００７／０７２０２８

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　G06F21/24(2006.01)i, G06F12/00(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.　G06F21/24, G06F12/00

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	１９７１－２００７年
日本国実用新案登録公報	１９９６－２００７年
日本国登録実用新案公報	１９９４－２００７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	関連する請求の範囲の番号
Y	JP 2005-71245 A（日本ビクター株式会社）2005.03.17, [0041]-[0064], 図４（ファミリーなし）	1-2, 6-7, 11-12, 16-17
A		3-5, 8-10, 13-15, 18-20

☑　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 １２．１２．２００７	国際調査報告の発送日 ２５．１２．２００７
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　９０７１ 平井　誠 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	関連する請求の範囲の番号
Y	US 2006/0075245 A1 (Meier) 2006.04.06, [0081] & EP 1643402 A2	1-2, 6-7, 11-12, 16-17
A		3-5, 8-10, 13-15, 18-20
Y	JP 2004-46592 A（富士通株式会社）2004.02.12, ［要約］& US 2004/0010509 A1	2, 7, 12, 17
A	JP 2004-185500 A（松下電器産業株式会社）2004.07.02, 全文, 全図（ファミリーなし）	1-20