

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2006-172351

(P2006-172351A)

(43) 公開日 平成18年6月29日(2006.6.29)

(51) Int. Cl.	F I	テーマコード (参考)
G06F 21/24 (2006.01)	G06F 12/14 510F	5B017
G09C 1/00 (2006.01)	G06F 12/14 520F	5J104
	G06F 12/14 530B	
	G06F 12/14 540A	
	G06F 12/14 560D	
審査請求 未請求 請求項の数 20 O L (全 12 頁) 最終頁に続く		

(21) 出願番号	特願2004-367195 (P2004-367195)	(71) 出願人	000005108
(22) 出願日	平成16年12月20日 (2004.12.20)		株式会社日立製作所
			東京都千代田区丸の内一丁目6番6号
		(74) 代理人	100068504
			弁理士 小川 勝男
		(74) 代理人	100086656
			弁理士 田中 恭助
		(74) 代理人	100094352
			弁理士 佐々木 孝
		(72) 発明者	萱島 信
			神奈川県川崎市麻生区王禅寺1099番地
			株式会社日立製作所システム開発研究所
			内
		Fターム(参考)	5B017 AA03 BA07 BA08 BA10 BB10
			CA16
			5J104 PA07 PA10 PA14

(54) 【発明の名称】 リムーバブルメディア利用によるコンテンツの使用期限管理方法及びシステム

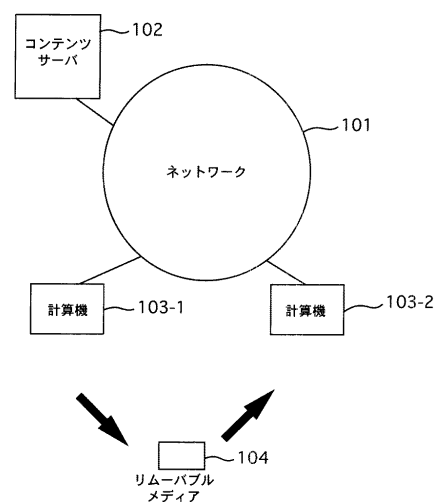
(57) 【要約】

【課題】 機密情報をリムーバブルメディアに入れて持ち出した際に、紛失したり、盗難にあつて第三者に繰り返し攻撃されることによって情報が漏えいする事故を防ぐ。

【解決手段】 計算機103で実行される専用書き込みプログラムは、コンテンツを暗号化して分割し、一部の分割コンテンツを使用期限情報とともにコンテンツサーバ102に送信して保存させ、残りの分割コンテンツをリムーバブルメディア104に格納する。計算機103で実行される専用ビューアプログラムは、コンテンツサーバ102から上記一部の分割コンテンツを受信し、リムーバブルメディア104から読み込んだ残りの分割コンテンツと合成して復号化した後、表示する。コンテンツサーバ102は、計算機103から要求された上記一部の分割コンテンツが使用期限内であれば計算機103へ送信する。

【選択図】 図1

図 1



【特許請求の範囲】

【請求項 1】

専用書き込みプログラムと専用ビューアプログラムとを格納するメモリと、前記メモリに格納されるプログラムを実行するCPUとを有する計算機と、前記計算機に着脱して使用されコンテンツを格納するリムーバブルメディアと、ネットワークを介して前記計算機と通信するコンテンツサーバとを有するシステムにおけるコンテンツの使用期限管理方法であって、

前記計算機により前記専用書き込みプログラムを実行することにより、コンテンツを暗号化して分割し、一部の分割コンテンツを使用期限情報とともに前記コンテンツサーバに送信して保存させ、残りの分割コンテンツを前記リムーバブルメディアに格納し、

10

前記計算機により前記専用ビューアプログラムを実行することにより、前記コンテンツサーバから前記一部の分割コンテンツを受信し、前記リムーバブルメディアから読み込んだ前記残りの分割コンテンツと合成して復号化した後、表示し、

前記コンテンツサーバにより、前記計算機から要求された前記一部の分割コンテンツが使用期限内であれば前記計算機へ送信することを特徴とするコンテンツの使用期限管理方法。

【請求項 2】

前記専用書き込みプログラムおよび前記専用ビューアプログラムは、前記リムーバブルメディアに格納され、前記リムーバブルメディアから前記メモリにロードされることを特徴とする請求項 1 記載のコンテンツの使用期限管理方法。

20

【請求項 3】

前記リムーバブルメディアが前記計算機から取り外されたとき、前記計算機により前記メモリ上の前記コンテンツを消去することを特徴とする請求項 1 記載のコンテンツの使用期限管理方法。

【請求項 4】

前記リムーバブルメディアは、個人識別情報(PIN)を保持し、入力されたPINが保持される前記PINと一致したとき、前記リムーバブルメディアに記憶される情報へのアクセスを許可することを特徴とする請求項 1 記載のコンテンツの使用期限管理方法。

【請求項 5】

前記コンテンツサーバは、前記計算機とは別の計算機であることを特徴とする請求項 1 記載のコンテンツの使用期限管理方法。

30

【請求項 6】

前記専用書き込みプログラムを実行することにより、前記コンテンツを暗号化して3つ以上に分割し、複数の分割コンテンツの各々を使用期限情報とともに複数の前記コンテンツサーバの各々へ送信して保存させることを特徴とする請求項 1 記載のコンテンツの使用期限管理方法。

【請求項 7】

前記コンテンツサーバにより、前記使用期限の切れた前記一部の分割コンテンツを消去することを特徴とする請求項 1 記載のコンテンツの使用期限管理方法。

【請求項 8】

40

専用書き込みプログラムと専用ビューアプログラムとを格納するメモリと、前記メモリに格納されるプログラムを実行するCPUとを有する計算機と、前記計算機に着脱して使用されコンテンツを格納するリムーバブルメディアと、ネットワークを介して前記計算機と通信するコンテンツサーバとを有するシステムにおいて、

前記計算機は、コンテンツを暗号化して分割し、一部の分割コンテンツを使用期限情報とともに前記コンテンツサーバに送信して保存させ、残りの分割コンテンツを前記リムーバブルメディアに格納する前記専用書き込みプログラムの実行により実現される処理手段と、

前記コンテンツサーバから前記一部の分割コンテンツを受信し、前記リムーバブルメディアから読み込んだ前記残りの分割コンテンツと合成して復号化した後、表示より前記専

50

用ビューアプログラムの実行により実現される処理手段とを有し、

前記コンテンツサーバは、前記計算機から要求された前記一部の分割コンテンツが使用期限内であれば前記計算機へ送信する処理手段を有することを特徴とするコンテンツの使用期限管理システム。

【請求項 9】

前記専用書き込みプログラムおよび前記専用ビューアプログラムは、前記リムーバブルメディアに格納され、前記リムーバブルメディアから前記メモリにロードされることを特徴とする請求項 8 記載のコンテンツの使用期限管理システム。

【請求項 10】

前記計算機は、さらに前記リムーバブルメディアが前記計算機から取り外されたとき、前記メモリ上の前記コンテンツを消去する手段を有することを特徴とする請求項 8 記載のコンテンツの使用期限管理システム。 10

【請求項 11】

前記リムーバブルメディアは、個人識別情報（PIN）を保持し、入力された PIN が保持される前記 PIN と一致したとき、前記リムーバブルメディアに記憶される情報へのアクセスを許可する手段を有することを特徴とする請求項 8 記載のコンテンツの使用期限管理システム。

【請求項 12】

前記コンテンツサーバは、前記計算機とは別の計算機であることを特徴とする請求項 8 記載のコンテンツの使用期限管理システム。 20

【請求項 13】

前記専用書き込みプログラムの実行により実現される処理手段は、前記コンテンツを暗号化して 3 つ以上に分割し、複数の分割コンテンツの各々を使用期限情報とともに複数の前記コンテンツサーバの各々へ送信して保存させることを特徴とする請求項 8 記載のコンテンツの使用期限管理システム。

【請求項 14】

前記コンテンツサーバは、前記使用期限の切れた前記一部の分割コンテンツを消去する手段を有することを特徴とする請求項 8 記載のコンテンツの使用期限管理システム。

【請求項 15】

計算機と、前記計算機に着脱して使用されコンテンツを格納するリムーバブルメディアと、ネットワークを介して前記計算機と通信するコンテンツサーバとを有するシステムにおいて前記計算機によって実行されるプログラムであって、 30

前記計算機に、コンテンツを暗号化して分割し、一部の分割コンテンツを使用期限情報とともに前記コンテンツサーバに送信して保存させ、残りの分割コンテンツを前記リムーバブルメディアに格納する機能を実現させるための専用書き込みプログラムと、

前記計算機に、前記コンテンツが使用期限内であれば前記コンテンツサーバから前記一部の分割コンテンツを受信し、前記リムーバブルメディアから読み込んだ前記残りの分割コンテンツと合成して復号化した後、表示する機能を実現させるための専用ビューアプログラムとを有することを特徴とするプログラム。

【請求項 16】

前記専用書き込みプログラムおよび前記専用ビューアプログラムは、前記リムーバブルメディアに格納され、前記リムーバブルメディアから前記計算機のメモリにロードされることを特徴とする請求項 15 記載のプログラム。 40

【請求項 17】

前記専用ビューアプログラムは、前記リムーバブルメディアが前記計算機から取り外されたとき、前記計算機のメモリ上の前記コンテンツを消去する機能を有することを特徴とする請求項 15 記載のプログラム。

【請求項 18】

前記リムーバブルメディアは、個人識別情報（PIN）を保持し、入力された PIN が保持される前記 PIN と一致したとき、前記リムーバブルメディアに記憶される情報への 50

アクセスを許可することを特徴とする請求項 15 記載のプログラム。

【請求項 19】

前記コンテンツサーバは、前記計算機とは別の計算機であることを特徴とする請求項 15 記載のプログラム。

【請求項 20】

前記専用書き込みプログラムは、前記コンテンツを暗号化して 3 つ以上に分割し、複数の分割コンテンツの各々を使用期限情報とともに複数の前記コンテンツサーバの各々へ送信して保存させる機能を有することを特徴とする請求項 15 記載のプログラム。

【発明の詳細な説明】

【技術分野】

10

【0001】

本発明は、リムーバブルメディアに格納されたコンテンツについて使用期限の管理をする方法に関する。

【背景技術】

【0002】

近年、機密情報をリムーバブルメディアに入れて持ち出した際に、紛失したり、盗難にあったりして情報が漏えいする事故が多発している。このような事故を防ぐ手段として、認証機能付きファームウェアを持つリムーバブルメディアと、認証コードを格納する耐タンパ機能を有するメモリデバイスがそろい、認証に成功しないとファイルアクセス不可にする方法がある。

20

また、バックアップデータが第三者の手に渡ったとしても機密性を保つための手段として、ファイルを暗号化して保存し、暗号鍵を持つユーザのみ復号可能にするような対応策がある。

【0003】

また、リムーバブルメディアに格納されたコンテンツに対する使用期限を制御する手段として、リムーバブルデバイス内に搭載したアプリケーションを、使用期限に対応して機能を制限・追加できるようにする技術がある。

【0004】

特開 2003-208406 号公報（特許文献 1）に開示される方式は、各コンテンツの有効期限を有効期限開始時刻と有効期限終了時刻とで管理し、利用するコンテンツの有効期限開始時刻を用いて認証時に参照する時刻を更新することにより、時刻をバックデ

30

【0005】

【特許文献 1】特開 2003-208406 号公報

【発明の開示】

【発明が解決しようとする課題】

【0006】

しかし、メディアに認証機能を持たせアクセス制御を実施する方式は、認証情報の漏えいや解読、偽造といった問題があること、暗号化による機密保護は、(1) 暗号鍵が漏えいした場合には容易に復号することが可能であること (2) 暗号化された機密情報であっても、すべての鍵を総当りで試せばいつかは復号することができること から、第三者が繰り返し攻撃することができ、特に持ち出しが容易なリムーバブルメディア等では、機密情報の漏えいを防ぐことが困難であった。

40

【0007】

また、使用期限に応じた機能の制限・追加を可能にするためには、いかに正確な時刻情報を入手するかということも課題となる。ただひとつのコンテンツのみ使用し続けるような場合には、認証時に参照する時刻が更新されないため、時刻のバックデートによるコンテンツの不正使用を防ぐことはできない。

【0008】

そこで本発明では、メディアに格納する情報を (1) 分散させた秘密情報としてその一

50

部を時間管理することにより、指定した期間だけ参照可能にする (2) 参照可能な期間に情報を複製してとっておくことができないようにすることによって、機密情報をリムーバブルメディアに入れて持ち出した際に、紛失したり、盗難にあって第三者に繰り返し攻撃されることによって情報が漏えいしたりする事故を防ぐことを課題とする。

【課題を解決するための手段】

【0009】

本発明は、計算機によりコンテンツを作成するための専用書き込みプログラム、およびコンテンツを閲覧するための専用ビューアプログラムを実行することにより実現される。またコンテンツサーバは、コンテンツの一部分を保存する。

【0010】

専用書き込みプログラムを用いたコンテンツの編集では、コンテンツをリムーバブルメディアに格納する時点で、秘密分散技術を用いてコンテンツを暗号化した上で分割し、コンテンツサーバとリムーバブルメディアに各々分割コンテンツを保存する。ここでコンテンツサーバは、コンテンツの閲覧可能期限を示す情報もあわせて保存する。

【0011】

専用ビューアプログラムを用いたコンテンツの閲覧では、コンテンツをリムーバブルメディアから読み出す時点で、コンテンツサーバより分割されたコンテンツを取得し、両者をあわせて復号化して表示する。ここでコンテンツサーバは、コンテンツを預託された時点で通知されたコンテンツの閲覧可能期限情報を基に、期限を過ぎていた場合には専用ビューアプログラムに分割コンテンツを返送しないようにする。

【発明の効果】

【0012】

本発明により、コンテンツをリムーバブルメディアとコンテンツサーバに分散して保管し、コンテンツサーバの情報を期限管理することにより、機密情報をリムーバブルメディアに入れて持ち出した際に、紛失したり、盗難にあって第三者に繰り返し攻撃されることによって情報が漏えいしたりする事故を防ぐことが可能になる。特にコンテンツサーバに保存するファイルサイズを大きくすることにより、リムーバブルメディア上の情報のみで復号化される危険性を減少させることができる。

【0013】

さらに本発明の副次的な効果として、コンテンツがリムーバブルメディアとコンテンツサーバに分散して保管されており、サーバ上の情報だけではコンテンツを復元することができないため、悪意を持つコンテンツサーバの管理者や管理ミスによる情報漏えいを防ぐことも可能になる。

【発明を実施するための最良の形態】

【0014】

以下、本発明の実施例について図面に基づいて説明する。

【0015】

図1は、本発明を実施するシステム全体の構成を示す図である。101はネットワーク、102はコンテンツの一部分を格納する機能を提供するコンテンツサーバ、103-1、103-2は、コンテンツの書き込みを実施する組織内に設置された計算機、あるいは組織内もしくはモバイルで利用される計算機、104は計算機103に挿入して使用する耐タンパ機能により保護された記憶領域を持つリムーバブルメディアである。

【0016】

本発明においては、組織内の計算機103-1にリムーバブルメディア104を挿入して作成したコンテンツをリムーバブルメディア内に格納して組織外に持ち出し、モバイルで利用される計算機103-2にリムーバブルメディア104を挿入してリムーバブルメディア内のコンテンツを閲覧する運用を行う。ここで、計算機103-2の利用として、組織が所有するノートPCを持ち出して使用するケースや、他組織が所有するPCを使用するケースがある。

本実施例と別の利用形態として、マルチメディア等のコンテンツ配信において、本システムを利用する場合であってもよい。

10

20

30

40

50

【0017】

また別の利用形態として、インターネット上でメール等のアプリケーションを用いてコンテンツを送信する際に本システムを利用し、コンテンツの一部分をコンテンツサーバ102上において残りのコンテンツをリムーバブルメディア104の代わりにメールに添付するようにすることもできる。

【0018】

図2は、実施形態の計算機103と、リムーバブルメディア104の構成を説明する図である。計算機103は、CPU201と、CPUに接続されたバス202を持ち、バス202にはメモリ203と、外部記憶装置207と、リムーバブルメディアI/Oモジュール209と、クロックデバイス210とネットワークI/Oモジュール211が接続されている。なお図示しないが、計算機103には入力装置と表示装置が接続される。メモリ203には、オペレーティングシステム(OS)204がロードされ、その制御下で専用ビューアプログラム205と専用書き込みプログラム206が実行される。また、外部記憶装置207には、オペレーティングシステムのロードモジュール208が格納される。リムーバブルメディア104は、耐タンパモジュールとして実現されたコントローラ231とフラッシュメモリ234により構成されている。コントローラ231は、公開鍵暗号方式で使用する個人鍵(他人には非公開にする鍵)233を格納する。フラッシュメモリ234は、オペレーティングシステム204の制御下で動作する専用ビューアプログラム205に対応するロードモジュール235と、専用書き込みプログラム206に対応するロードモジュール236と、暗号化した1つ又は複数のコンテンツファイル237と、ユーザが利用可能なコンテンツサーバ102のホスト名等の一覧を保管したコンテンツサーバリスト239を格納する。さらにフラッシュメモリ234内には保護領域238がある。保護領域238は、専用ビューアプログラム205および専用書き込みプログラム206を起動できるユーザの認証を行うためのパスワードファイル240を格納する。コンテンツファイル237には、それぞれ閲覧可能な期限に関する情報が記憶される。保護領域238のアクセスは、リムーバブルメディア104を利用するユーザでも内容を参照および変更できないようにコントローラ231により制御されており、設定された個人識別情報(PIN)を提示できない場合にはアクセスを禁止するようにする。これは、例えばSMCC(Secure Multimedia Card)等の仕組みを用いることにより実現することができる。

【0019】

本実施例においては専用ビューアプログラムのロードモジュール235と、専用書き込みプログラムのロードモジュール236をリムーバブルメディア104上に配置しているが、計算機103の外部記憶装置207上に配置するようにしてもよい。ただしこの場合にコンテンツファイル237はリムーバブルメディア104に格納されなければならない。

【0020】

図3は、実施形態のコンテンツサーバ102の構成を説明する図である。コンテンツサーバ102は、CPU301と、CPUに接続されたバス302を持ち、バス302にはメモリ303と、ネットワークI/Oモジュール306と、外部記憶装置307が接続されている。メモリ303には、オペレーティングシステム304がロードされ、その制御下でコンテンツ管理プログラム305が実行される。コンテンツ管理プログラム305は、クライアントから保管期限を指定して預託されたコンテンツを外部記憶装置307上に保管する機能と、外部記憶装置307上の保管コンテンツ309を、保管期限内であればクライアントに返送する機能を実行する。ここで、実行されるコンテンツ管理プログラム305は、正しい現在時刻情報を入手する必要がある。これには、コンテンツサーバ102のクロックデバイスを管理者がこまめに調整する方法もあるが、より正確に時計あわせを実施するためには、コンテンツサーバ102のシリアルI/Oモジュール310に接続したGPS(Global Positioning System)の受信機を利用することもできる。また、外部記憶装置307には、オペレーティングシステムのロードモジュール308が格納される。

図4は、計算機103上で稼動する専用書き込みプログラム206のコンテンツ作成処理の詳細を示すフローチャートである。

ステップ401は、外部記憶装置207等に保管されている既存コンテンツの読み込み、もし

くは新規コンテンツの作成準備を行うステップである。ステップ402は、図示しない入力装置を介してユーザ入力コマンドを受け付けるステップである。ステップ403は、ステップ402で入力されたユーザ入力コマンドが、コンテンツ保存コマンドか判断するステップである。

【0021】

ステップ404からステップ409は、コンテンツ保存コマンドを受理した際に実施するステップである。ステップ404は、秘密分散技術を用いて保存するデータを暗号化し、複数のコンテンツに分割するステップである。ステップ405は、保存するコンテンツの名称および、閲覧期限を指定するステップである。ステップ406は、コンテンツサーバリスト239で示されたコンテンツサーバ102と接続し、相互認証を実施するステップであり、認証が失敗した場合には処理を終了する。ステップ407は、ステップ404で分割したコンテンツと閲覧期限情報をコンテンツサーバ102に送信するステップである。ステップ408は、コンテンツサーバ102が作成したコンテンツ保管場所情報を受信するステップである。ステップ409は、ステップ404で分割した残りのコンテンツと、ステップ408で受信したコンテンツ保管場所情報をコンテンツファイル237として格納するステップである。ステップ410は、その他コンテンツの編集を行うための各種コマンド処理を実施するステップである。

【0022】

ここで、ステップ404の秘密分散技術として、例えば「岡本龍明、山本博資著、「現代暗号」、産業図書 p p. 209-210」等に記載されている (k, n) 閾値秘密分散法がある。 (k, n) 閾値秘密分散法は、コンテンツを n 個に分割し、そのうちの k 個の分散情報がそろわない限り復号することはできなくなる技術であるが、本発明は特定の秘密分散法に依存しない。たとえば暗号文全体のハッシュ値が復号鍵になるようにドキュメントを暗号化した上で、暗号文を2つのコンテンツに分割し、片側をリムーバブルメディアに、もうひとつをコンテンツサーバ102に保存するようにして、暗号文全体がそろわないと復号鍵を入手することができないようにしてもよい。コンテンツの分割は2つに固定されているわけではなく、3つ以上に分割してもよい。分割されたコンテンツは、1つを除いてそれぞれ別々のコンテンツサーバ102に保存される。また、コンテンツサーバ102に保存するデータのサイズは、長くなればそれだけ暗号強度を上げることができるため、要求される暗号強度に応じてサイズを決めてもよい。また、リムーバブルメディア104の空き容量に応じてコンテンツサーバ102に格納するサイズを決めてもよい。

【0023】

また、専用書き込みプログラム206とコンテンツサーバ102との間でステップ406の相互認証を行うためには、リムーバブルメディア104上の個人鍵233を用いて、たとえばT L S (Transport Layer Security)によるサーバ認証およびクライアント認証を利用してもよい。この個人鍵を使用する際にはP I Nの入力が必要なように制御してもよい。

【0024】

また、専用書き込みプログラム206を用いると、コンテンツの閲覧期限を変更することが可能であるため、起動ユーザを制限できるようにする必要がある。これには、リムーバブルメディア104内のパスワードファイル240を利用して、ステップ401以前にユーザ認証を実施するようにしてもよい。また、コンテンツ全体を保護領域238に格納するようにしてもよい。保護領域238に格納されたコンテンツは、正しいP I Nの入力がなければアクセスできない。

【0025】

図5は、コンテンツサーバ102上で動作するコンテンツ管理プログラム305のコンテンツ作成時における処理の詳細を示すフローチャートである。

ステップ501は接続待ちのステップであり、ステップ502は計算機103上で稼動する専用書き込みプログラム206の接続要求を受け入れ、ステップ406と同様な相互認証を実施するステップであり、相互認証に失敗した場合には処理を終了する。ステップ503は、専用書き込みプログラム206より分割されたコンテンツと閲覧期限情報を受信するステップである。コンテンツ管理プログラム305は、閲覧期限をチェックし、所定の期限を越えている

場合にコンテンツの保存要求を拒絶してもよい。ステップ504は、コンテンツ保管場所を確定し、コンテンツを保管するステップである。ステップ505は、コンテンツ保管場所情報を送信するステップである。

ステップ504において確定するコンテンツ保管場所は、ステップ502の相互認証で特定したユーザ識別子と、コンテンツを表すユニークな識別子を用いて決定してもよい。たとえば、コンテンツサーバ102のホスト名がserver.aaa.jpとすると、ユーザ識別子のkayashi@sdl.hitachi.co.jpと、コンテンツ名称file2004083000001.datとを組み合わせ、さらにコンテンツサーバ102にアクセスする際に使用するプロトコル種別を付加してhttps://server.aaa.jp/kayashi@sdl.hitachi.co.jp/file2004083000001.dat のようにしてもよい。

【0026】

10

図6は、本方式のコンテンツファイル237と、保管コンテンツ309のデータ形式の例を示す図である。コンテンツファイル237は、コンテンツサーバ102上のコンテンツ保管場所を示す保管場所フィールド601と、暗号化された分割コンテンツフィールド602により構成される。保管コンテンツ309は、コンテンツの閲覧期限を示す閲覧期限フィールド603と、暗号化された分割コンテンツフィールド602により構成される。

【0027】

図7は、計算機103上で稼動する専用ビューアプログラム205のコンテンツ閲覧処理の詳細を示すフローチャートである。

ステップ701は、ユーザの指定したコンテンツファイル237を読み込むステップである。ステップ702は、コンテンツファイル237により指定されたコンテンツサーバ102と接続し、相互認証を実施するステップであり、認証に失敗した場合には処理を終了する。ステップ703は、ステップ701でコンテンツファイル237から読み込んだ保管場所フィールド601を基に、コンテンツサーバ102にコンテンツ保管場所情報を送信するステップである。ステップ704は、コンテンツサーバ102からデータを受信するステップである。ステップ705は、受信したデータが分割コンテンツであるかどうかを判断するステップである。ステップ706とステップ707は、受信したデータが分割コンテンツであった場合に実行するステップであり、ステップ706はステップ701で読み込んだコンテンツの一部と、ステップ704で受信したデータからコンテンツを合成し、復号化するステップである。ステップ707はステップ706で合成したコンテンツを表示装置に表示するステップである。ステップ708は、コンテンツの保存期限が切れているなど有効なコンテンツが存在しないことを通知するステップである。

20

30

たとえば暗号文全体のハッシュ値が復号鍵になるようにドキュメントを暗号化した上で、暗号文を2つのコンテンツに分割するようにしている場合、ステップ706ではまず暗号文全体がそろえ、そのハッシュ値を計算することにより復号鍵を入手し、暗号文の復号化処理を実施することになる。

【0028】

また、専用ビューアプログラム205を利用可能なユーザを限定するためには、専用ビューアプログラム205の起動時にユーザ名とパスワードをユーザに提示させ、保護領域234中のパスワードファイル240と比較することにより、不正なユーザが専用ビューアプログラム205を使用することを防止するようにしてもよい。

40

【0029】

また、専用ビューアプログラム205の起動中にリムーバブルメディア104が取り外された際には、メモリ205上に展開されたコンテンツを消去するようにしてもよい。

【0030】

図8は、コンテンツサーバ102上で動作するコンテンツ管理プログラム305のコンテンツ閲覧時における処理の詳細を示すフローチャートである。

ステップ801は接続待ちステップ、ステップ802は計算機103上で稼動する専用ビューアプログラム205の接続要求を受け入れ、相互認証を実施するステップであり、相互認証に失敗した場合には処理を終了する。ステップ803は、専用ビューアプログラム205よりコンテンツ保管場所情報を受信するステップである。ステップ804はコンテンツが存在するか

50

否かを判定するステップである。ステップ805は、コンテンツが存在しかつ有効であるかどうか、すなわち現時点で閲覧が許可されているかどうかを判断するステップである。ステップ806は、コンテンツが有効である場合に実施する処理であり、保管している分割コンテンツを送信するステップである。ステップ807は、コンテンツが無効である場合に実施する処理であり、コンテンツは期限切れなど有効なコンテンツが存在しないことを通知するメッセージを送信するステップである。

また、前述した実施例では、コンテンツファイル237をリムーバブルメディア104内に格納しているが、計算機103の外部記憶装置207に格納したコンテンツを対象として、ロードモジュール235,236を格納する特定のリムーバブルメディア104を計算機103に挿入したときのみコンテンツの書き込みもしくは有効なコンテンツの閲覧を可能とするように制御してもよい。 10

【0031】

また、コンテンツサーバ102の代わりに組織内に設置された計算機103がコンテンツ管理プログラム305を実行するようにしてもよい。

【0032】

また、前述した実施例では、ひとつのコンテンツサーバ102に分割したコンテンツを保存しているが、コンテンツファイル237中の保管場所フィールド601を拡張し、複数のコンテンツサーバに分割コンテンツを保管するようにしてもよい。また、コンテンツサーバ102側に保管するコンテンツのサイズが大きいほど復号は困難になるため、コンテンツの重要度に応じてコンテンツサーバ102での保管サイズを大きくするように制御してもよい。 20

【0033】

また、保管コンテンツ309の閲覧期限フィールド603を拡張し、有効期限の始まりと終わりを記載するようにし、まだ有効期限になっていない場合にはファイルを送信しないよう制御してもよい。

【0034】

また、前述した実施例は、ステップ805においてコンテンツが有効か否か判断しているが、もし有効期限が過ぎていた場合には、保管コンテンツ309を消去したり、他のバックアップ用外部記憶装置に移動したりしてもよい。その他、別のプログラムによりコンテンツが有効か否か判断するステップを定期的の実施し、有効期限が過ぎている保管コンテンツ309を消去したり、他のバックアップ用外部記憶装置に移動したりしてもよい。 30

【図面の簡単な説明】

【0035】

【図1】実施形態のシステムの全体構成を示す図である。

【図2】実施形態の計算機とリムーバブルメディアの構成を示す図である。

【図3】実施形態のコンテンツサーバの構成を示す図である。

【図4】実施形態の書き込みプログラムのコンテンツ作成時処理の手順を示すフローチャートである。

【図5】実施形態のコンテンツ管理プログラムのコンテンツ作成時処理の手順を示すフローチャートである。

【図6】コンテンツのデータ形式の例を示す図である。 40

【図7】実施形態のビューアプログラムのコンテンツ閲覧処理の手順を示すフローチャートである。

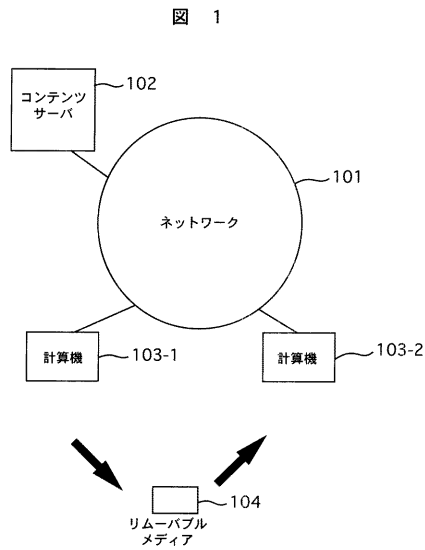
【図8】実施形態のコンテンツ管理プログラムのコンテンツ閲覧処理の手順を示すフローチャートである。

【符号の説明】

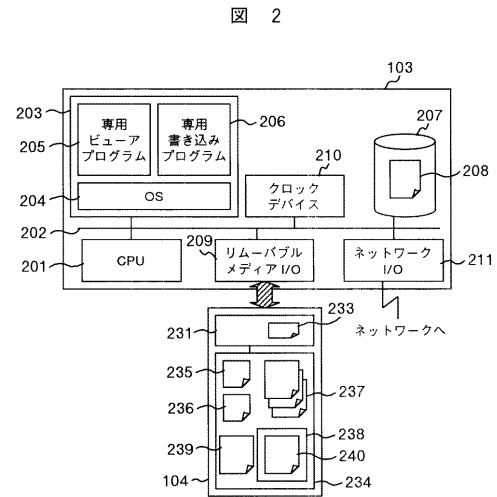
【0036】

102…コンテンツサーバ、103…計算機、104…リムーバブルメディア、205…専用ビューアプログラム、206…専用書き込みプログラム、237…コンテンツファイル、305…コンテンツ管理プログラム

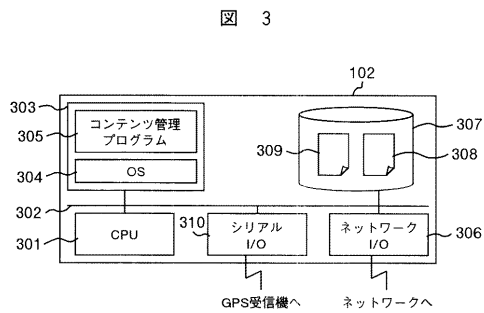
【図 1】



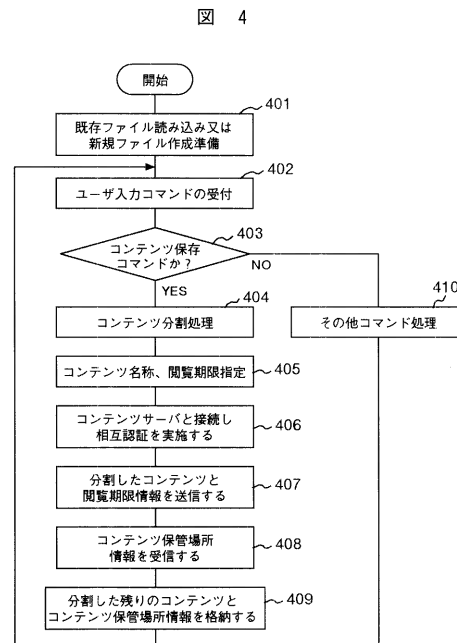
【図 2】



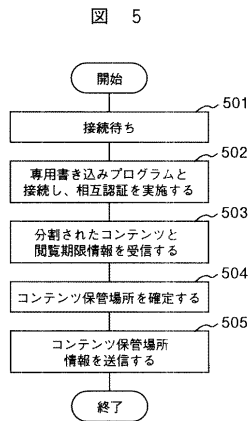
【図 3】



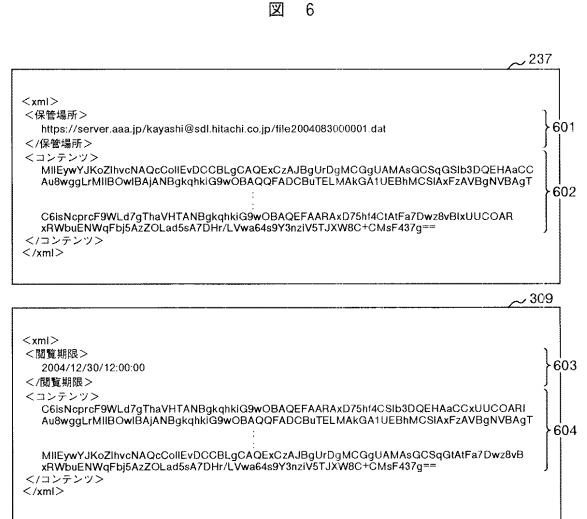
【図 4】



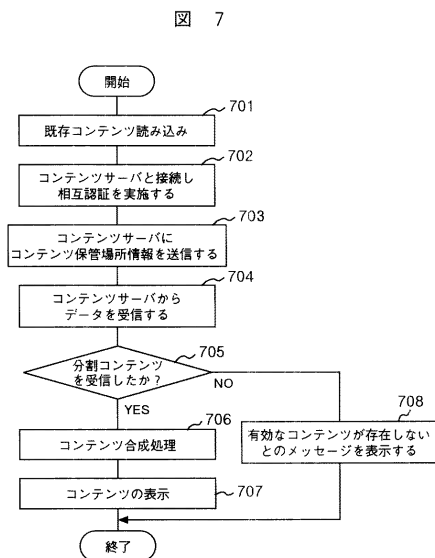
【図 5】



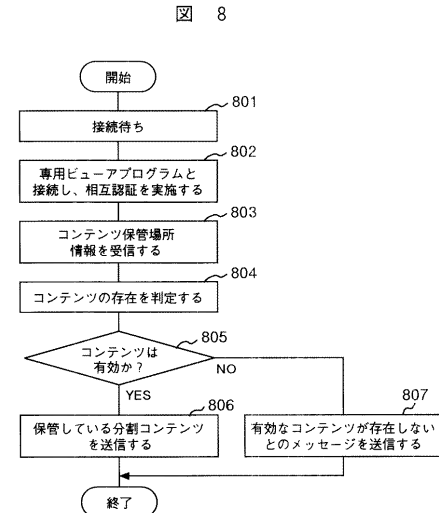
【図 6】



【図 7】



【図 8】



フロントページの続き

(51)Int.Cl.

F I

テーマコード (参考)

G 0 9 C 1/00 6 6 0 D