(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2008-9717
(P2008-9717A)
(43)公開日　平成20年1月17日(2008.1.17)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/22	(2006.01)	G06F	9/06	660Z	5B017
G09C 1/00	(2006.01)	G09C	1/00	660D	5B276
G06F 21/24	(2006.01)	G06F	12/14	540A	5J104
		G06F	12/14	550B	

審査請求 未請求　請求項の数 13　ＯＬ　（全 14 頁）

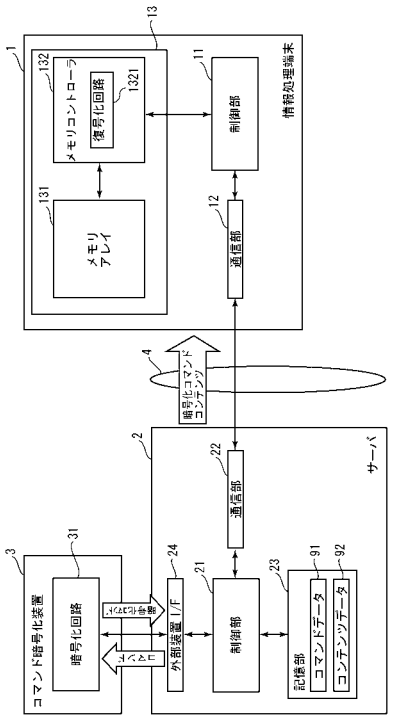
(21)出願番号　特願2006-179565 (P2006-179565)
(22)出願日　平成18年6月29日 (2006.6.29)

(71)出願人　504134265
株式会社メガチップスＬＳＩソリューションズ
大阪府大阪市淀川区宮原４丁目１番６号
(74)代理人　100125704
弁理士　坂根　剛
(72)発明者　塚嵜　史明
大阪市淀川区宮原４丁目１番６号　株式会社メガチップスＬＳＩソリューションズ内

Ｆターム(参考)　5B017 AA06 AA07 BA07 CA16
5B276 FA00 FD07
5J104 AA12 AA32 JA03 NA02 NA27 PA14

(54)【発明の名称】情報処理端末およびコンテンツ書き込みシステム

(57)【要約】
【課題】コンテンツデータの格納処理の観測を困難にし、コンテンツデータの不正コピーを有効に防止しえる技術を提供することを目的とする。
【解決手段】情報処理端末１からサーバ２に対してコンテンツデータ９２のダウンロード要求が送信される。サーバ２は、コマンドデータ９１をコマンド暗号化装置３に転送する。コマンド暗号化装置３は、暗号化回路３１においてコマンドデータ９１を暗号化する。サーバ２は、コンテンツデータ９２と暗号化されたコマンドデータ９１とを情報処理端末１に送信する。情報処理端末１の制御部１１は、メモリコントローラ１３２にコンテンツデータ９２と暗号化コマンドデータ９１を転送する。メモリコントローラ１３２は、復号化回路１３２１によりコマンドデータ９１を復号化し、コンテンツデータ９２をメモリアレイ１３１に格納する。
【選択図】図１



【特許請求の範囲】
【請求項１】
メモリにコンテンツデータを書き込む情報処理端末であって、
端末外部からコンテンツデータを入力するコンテンツ入力手段と、
端末外部から暗号化コマンドデータを入力するコマンド入力手段と、
前記メモリに暗号化コマンドデータとコンテンツデータとを与える制御手段と、
を備え、
前記メモリは、
メモリアレイと、
復号化回路により暗号化コマンドデータを復号化し、復号化されたコマンドデータにより前記メモリアレイに対するコンテンツデータの書き込み制御を行うメモリコントローラと、
を備えることを特徴とする情報処理端末。
【請求項２】
請求項１に記載の情報処理端末において、
前記コマンド入力手段は、
ネットワーク経由でサーバから暗号化コマンドデータをダウンロードする手段、
を含むことを特徴とする情報処理端末。
【請求項３】
請求項２に記載の情報処理端末において、
前記サーバには、暗号化回路を備えたコマンド暗号化装置が外部機器として接続されており、前記サーバから与えられたコマンドデータが前記コマンド暗号化装置において暗号化され、当該暗号化コマンドデータが、前記情報処理端末にダウンロードされることを特徴とする情報処理端末。
【請求項４】
請求項２に記載の情報処理端末において、
前記サーバには、暗号化回路を備えたコマンド暗号化装置が外部機器として接続されており、前記コマンド暗号化装置に格納されているコマンドデータが前記コマンド暗号化装置において暗号化され、当該暗号化コマンドデータが、前記情報処理端末にダウンロードされることを特徴とする情報処理端末。
【請求項５】
請求項２に記載の情報処理端末において、
前記サーバには、暗号化処理を実行可能な暗号化サーバがネットワークを介して接続されており、前記サーバから与えられたコマンドデータが前記暗号化サーバにおいて暗号化され、当該暗号化コマンドデータが、前記情報処理端末にダウンロードされることを特徴とする情報処理端末。
【請求項６】
請求項２に記載の情報処理端末において、
前記サーバには、暗号化処理を実行可能な暗号化サーバがネットワークを介して接続されており、前記暗号化サーバに格納されているコマンドデータが前記暗号化サーバにおいて暗号化され、当該暗号化コマンドデータが、前記情報処理端末にダウンロードされることを特徴とする情報処理端末。
【請求項７】
請求項３ないし請求項６のいずれかに記載の情報処理端末において、さらに、
前記サーバに対して前記メモリの識別情報を送信する手段、
を含み、
前記コンテンツ入力手段は、
ネットワーク経由で前記サーバから暗号化コンテンツデータをダウンロードする手段、
を含み、
前記サーバには、さらに、暗号化回路を備えたコンテンツ暗号化装置が外部機器として

接続されており、前記サーバから与えられたコンテンツデータが前記コンテンツ暗号化装置において前記識別情報を利用して暗号化され、当該暗号化コンテンツデータが、前記情報処理端末にダウンロードされることを特徴とする情報処理端末。

【請求項８】

メモリにコンテンツデータを書き込むシステムであって、

情報処理端末と、

サーバと、

を備え、

前記情報処理端末は、

端末外部からコンテンツデータを入力するコンテンツ入力手段と、

前記サーバから暗号化コマンドデータをダウンロードする手段と、

前記メモリに暗号化コマンドデータとコンテンツデータとを与える制御手段と、

を備え、

前記メモリは、

メモリアレイと、

復号化回路により暗号化コマンドデータを復号化し、復号化されたコマンドデータにより前記メモリアレイに対するコンテンツデータの書き込み制御を行うメモリコントローラと、

を備えることを特徴とするコンテンツ書き込みシステム。

【請求項９】

請求項８に記載のコンテンツ書き込みシステムにおいて、

前記サーバには、暗号化回路を備えたコマンド暗号化装置が外部機器として接続されており、前記サーバから与えられたコマンドデータが前記コマンド暗号化装置において暗号化され、当該暗号化コマンドデータが、前記情報処理端末にダウンロードされることを特徴とするコンテンツ書き込みシステム。

【請求項１０】

請求項８に記載のコンテンツ書き込みシステムにおいて、

前記サーバには、暗号化回路を備えたコマンド暗号化装置が外部機器として接続されており、前記コマンド暗号化装置に格納されているコマンドデータが前記コマンド暗号化装置において暗号化され、当該暗号化コマンドデータが、前記情報処理端末にダウンロードされることを特徴とするコンテンツ書き込みシステム。

【請求項１１】

請求項８に記載のコンテンツ書き込みシステムにおいて、

前記サーバには、暗号化処理を実行可能な暗号化サーバがネットワークを介して接続されており、前記サーバから与えられたコマンドデータが前記暗号化サーバにおいて暗号化され、当該暗号化コマンドデータが、前記情報処理端末にダウンロードされることを特徴とするコンテンツ書き込みシステム。

【請求項１２】

請求項８に記載のコンテンツ書き込みシステムにおいて、

前記サーバには、暗号化処理を実行可能な暗号化サーバがネットワークを介して接続されており、前記暗号化サーバに格納されているコマンドデータが前記暗号化サーバにおいて暗号化され、当該暗号化コマンドデータが、前記情報処理端末にダウンロードされることを特徴とするコンテンツ書き込みシステム。

【請求項１３】

請求項９ないし請求項１２のいずれかに記載のコンテンツ書き込みシステムにおいて、

前記情報処理端末は、さらに、

前記サーバに対して前記メモリの識別情報を送信する手段、

を備え、

前記コンテンツ入力手段は、

ネットワーク経由で前記サーバから暗号化コンテンツデータをダウンロードする手段、

を含み、
前記サーバには、さらに、暗号化回路を備えたコンテンツ暗号化装置が外部機器として接続されており、前記サーバから与えられたコンテンツデータが前記コンテンツ暗号化装置において前記識別情報を利用して暗号化され、当該暗号化コンテンツデータが、前記情報処理端末にダウンロードされることを特徴とするコンテンツ書き込みシステム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、メモリに対するデータの不正な書き込みを排除する技術に関する。
【背景技術】
【０００２】
インターネットを介してサーバからコンテンツをダウンロードするシステムが、様々なサービスで利用されている。たとえば、音楽データをダウンロードするサービスでは、ユーザは、ダウンロードした音楽データを音楽プレーヤに格納し、音楽を再生して楽しむことができる。あるいは、ゲームプログラムをダウンロードするサービスがある。ユーザは、ダウンロードしたゲームプログラムをメモリに格納することで、最新のゲームを楽しむことができる。
【０００３】
このようなネットワークを利用したダウンロードサービスは、手軽に、短時間で、コンテンツを入手できるという点で非常に便利である。しかし、コンテンツの不正なコピーを防止するための対策が必要である。
【０００４】
ダウンロードサービスは、ユーザがダウンロードしたコンテンツを各種の記憶媒体に格納して利用できるサービスである。つまり、記憶媒体に対するコンテンツの書き込み処理を、ユーザ側で実行させるサービスである。このため、コンテンツを書き込む処理が観測される可能性が生じることになり、この処理が悪意ある者によって自由に行われるようになると、不正なコピーが行われることになる。このような行為を放置すれば、コンテンツ作成者の権利や利益が不当に奪われることになる。
【０００５】
たとえば、コンテンツの不正なコピーを防止するために、ＣＰＲＭという技術が用いられている。非特許文献１の１０ページ目に、著作権保護機能「ＣＰＲＭ」の仕組みが紹介されている。ホスト機器はネットワーク暗号のかかったコンテンツをダウンロードする。そして、機器のデバイス鍵やメモリカードの鍵束、メディアＩＤなどを利用して暗号鍵を作成し、その暗号鍵を用いて暗号化したコンテンツをメモリカードに格納するのである。
【０００６】
【非特許文献１】“著作権保護技術”、２００６年５月１７日、（社）電子情報技術産業協会、[平成１８年６月１５日検索]、インターネット＜ＵＲＬ：http://www.mext.go.jp/b_menu/shingi/bunka/gijiroku/020/06051709/004.pdf＞
【発明の開示】
【発明が解決しようとする課題】
【０００７】
非特許文献１で紹介されているＣＰＲＭなどの技術は、コンテンツデータを暗号化して、不正な利用を排除しようとするものである。つまり、記憶媒体に書き込まれるデータ自体を暗号化することで、不正な利用を防止しようとするアプローチである。今後、さらなる不正コピーの巧妙化が進むことを考慮すると、新たな観点から不正コピーを防止するための技術が開発されることが望まれる。
【０００８】
また、非特許文献１の技術は、ネットワーク暗号のかかったコンテンツを一旦、ホスト機器で復号化する。したがって、ホスト機器内には、一時的に復号化されたコンテンツがＲＡＭなどに格納されることになるので、その状態を観測される恐れがある。

【０００９】
本発明は前記問題点に鑑み、コンテンツデータの格納処理の観測を困難にし、コンテンツデータの不正コピーを有効に防止しえる技術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】
【００１０】
上記課題を解決するため、請求項１記載の発明は、メモリにコンテンツデータを書き込む情報処理端末であって、端末外部からコンテンツデータを入力するコンテンツ入力手段と、端末外部から暗号化コマンドデータを入力するコマンド入力手段と、前記メモリに暗号化コマンドデータとコンテンツデータとを与える制御手段と、を備え、前記メモリは、メモリアレイと、復号化回路により暗号化コマンドデータを復号化し、復号化されたコマンドデータにより前記メモリアレイに対するコンテンツデータの書き込み制御を行うメモリコントローラと、を備えることを特徴とする。
【００１１】
請求項２記載の発明は、請求項１に記載の情報処理端末において、前記コマンド入力手段は、ネットワーク経由でサーバから暗号化コマンドデータをダウンロードする手段、を含むことを特徴とする。
【００１２】
請求項３記載の発明は、請求項２に記載の情報処理端末において、前記サーバには、暗号化回路を備えたコマンド暗号化装置が外部機器として接続されており、前記サーバから与えられたコマンドデータが前記コマンド暗号化装置において暗号化され、当該暗号化コマンドデータが、前記情報処理端末にダウンロードされることを特徴とする。
【００１３】
請求項４記載の発明は、請求項２に記載の情報処理端末において、前記サーバには、暗号化回路を備えたコマンド暗号化装置が外部機器として接続されており、前記コマンド暗号化装置に格納されているコマンドデータが前記コマンド暗号化装置において暗号化され、当該暗号化コマンドデータが、前記情報処理端末にダウンロードされることを特徴とする。
【００１４】
請求項５記載の発明は、請求項２に記載の情報処理端末において、前記サーバには、暗号化処理を実行可能な暗号化サーバがネットワークを介して接続されており、前記サーバから与えられたコマンドデータが前記暗号化サーバにおいて暗号化され、当該暗号化コマンドデータが、前記情報処理端末にダウンロードされることを特徴とする。
【００１５】
請求項６記載の発明は、請求項２に記載の情報処理端末において、前記サーバには、暗号化処理を実行可能な暗号化サーバがネットワークを介して接続されており、前記暗号化サーバに格納されているコマンドデータが前記暗号化サーバにおいて暗号化され、当該暗号化コマンドデータが、前記情報処理端末にダウンロードされることを特徴とする。
【００１６】
請求項７記載の発明は、請求項３ないし請求項６のいずれかに記載の情報処理端末において、さらに、前記サーバに対して前記メモリの識別情報を送信する手段、を含み、前記コンテンツ入力手段は、ネットワーク経由で前記サーバから暗号化コンテンツデータをダウンロードする手段、を含み、前記サーバには、さらに、暗号化回路を備えたコンテンツ暗号化装置が外部機器として接続されており、前記サーバから与えられたコンテンツデータが前記コンテンツ暗号化装置において前記識別情報を利用して暗号化され、当該暗号化コンテンツデータが、前記情報処理端末にダウンロードされることを特徴とする。
【００１７】
請求項８記載の発明は、メモリにコンテンツデータを書き込むシステムであって、情報処理端末と、サーバと、を備え、前記情報処理端末は、端末外部からコンテンツデータを入力するコンテンツ入力手段と、前記サーバから暗号化コマンドデータをダウンロードする手段と、前記メモリに暗号化コマンドデータとコンテンツデータとを与える制御手段と

、を備え、前記メモリは、メモリアレイと、復号化回路により暗号化コマンドデータを復号化し、復号化されたコマンドデータにより前記メモリアレイに対するコンテンツデータの書き込み制御を行うメモリコントローラと、を備えることを特徴とする。

【００１８】

請求項９記載の発明は、請求項８に記載のコンテンツ書き込みシステムにおいて、前記サーバには、暗号化回路を備えたコマンド暗号化装置が外部機器として接続されており、前記サーバから与えられたコマンドデータが前記コマンド暗号化装置において暗号化され、当該暗号化コマンドデータが、前記情報処理端末にダウンロードされることを特徴とする。

【００１９】

請求項１０記載の発明は、請求項８に記載のコンテンツ書き込みシステムにおいて、前記サーバには、暗号化回路を備えたコマンド暗号化装置が外部機器として接続されており、前記コマンド暗号化装置に格納されているコマンドデータが前記コマンド暗号化装置において暗号化され、当該暗号化コマンドデータが、前記情報処理端末にダウンロードされることを特徴とする。

【００２０】

請求項１１記載の発明は、請求項８に記載のコンテンツ書き込みシステムにおいて、前記サーバには、暗号化処理を実行可能な暗号化サーバがネットワークを介して接続されており、前記サーバから与えられたコマンドデータが前記暗号化サーバにおいて暗号化され、当該暗号化コマンドデータが、前記情報処理端末にダウンロードされることを特徴とする。

【００２１】

請求項１２記載の発明は、請求項８に記載のコンテンツ書き込みシステムにおいて、前記サーバには、暗号化処理を実行可能な暗号化サーバがネットワークを介して接続されており、前記暗号化サーバに格納されているコマンドデータが前記暗号化サーバにおいて暗号化され、当該暗号化コマンドデータが、前記情報処理端末にダウンロードされることを特徴とする。

【００２２】

請求項１３記載の発明は、請求項９ないし請求項１２のいずれかに記載のコンテンツ書き込みシステムにおいて、前記情報処理端末は、さらに、前記サーバに対して前記メモリの識別情報を送信する手段、を備え、前記コンテンツ入力手段は、ネットワーク経由で前記サーバから暗号化コンテンツデータをダウンロードする手段、を含み、前記サーバには、さらに、暗号化回路を備えたコンテンツ暗号化装置が外部機器として接続されており、前記サーバから与えられたコンテンツデータが前記コンテンツ暗号化装置において前記識別情報を利用して暗号化され、当該暗号化コンテンツデータが、前記情報処理端末にダウンロードされることを特徴とする。

【発明の効果】

【００２３】

本発明の情報処理端末は、コンテンツデータと暗号化されたコマンドデータを外部から取得し、復号化回路により暗号化コマンドデータを復号化してコンテンツデータの書き込みを行う。これにより、情報処理端末において実行される書き込みコマンドの観測を困難とすることができる。書き込みコマンドの観測を困難とすることで、コンテンツデータの不正コピーを有効に防止することができる。

【００２４】

また、情報処理端末は、ネットワーク経由でサーバから暗号化コマンドデータをダウンロードする。したがって、書き込みコマンドの観測を困難としながら、迅速に、コンテンツデータの書き込み処理を実行することができる。

【００２５】

また、サーバに接続されたコマンド暗号化装置によりコマンドデータの暗号化が行われる。これにより、暗号化ロジックの観測も困難とすることができ、コンテンツデータの不

正コピーを、さらに有効に防止できる。
【００２６】
また、暗号化されるコマンドデータは、コマンド暗号化装置に格納されている。したがって、コマンドデータの平文が、コマンド暗号化装置内にのみ存在することになり、よりセキュリティ強度が高められる。
【００２７】
また、サーバに接続された暗号化サーバにおいて、暗号化処理が実行される。暗号化サーバがセキュリティの高い構成である場合には、ソフトウェア処理により、コマンドデータを暗号化する構成とすることができる。
【００２８】
また、サーバにコンテンツ暗号化装置が接続され、コンテンツデータがメモリの識別情報を利用して暗号化された後、情報処理端末にダウンロードされる。コマンドデータの暗号化とあわせて、コンテンツデータも暗号化することで、コンテンツの不正利用をより有効に防止することができる。
【発明を実施するための最良の形態】
【００２９】
｛第１の実施の形態｝
以下、図面を参照しつつ本発明の第１の実施の形態について説明する。図１は、本実施の形態に係るコンテンツ書き込みシステムの全体図である。このシステムは、情報処理端末１と、サーバ２と、コマンド暗号化装置３とを備えて構成される。情報処理端末１とサーバ２とは、インターネットなどのネットワーク４を介して接続されている。
【００３０】
情報処理端末１は、制御部１１、通信部１２、半導体メモリ１３を備えている。制御部１１は、ＣＰＵ、ＲＡＭなどを備え、情報処理端末１の全体制御を行う。通信部１２は、ネットワーク４を介してサーバ２との間で通信処理を実行する。情報処理端末１は、半導体メモリ１３からデータを読み出し、制御部１１において各種のデータ処理を実行する。あるいは、半導体メモリ１３に対してデータの書き込み処理を実行する。
【００３１】
情報処理端末１としては、たとえば、ＰＤＡ（Personal Digital Assistance）、セットトップボックス、ゲーム装置などが考えられる。情報処理端末１が、ＰＤＡやセットトップボックスである場合には、半導体メモリ１３は、アプリケーションプログラムなどが記録されるメモリであり、情報処理端末１がゲーム装置である場合には、半導体メモリ１３は、ゲームプログラムが格納されるゲームカートリッジである。
【００３２】
半導体メモリ１３は、情報を記憶する多数のメモリセルからなる不揮発性メモリであるメモリアレイ１３１と、メモリアレイ１３１に対するアクセスをコントロールするためのメモリコントローラ１３２とを備えている。半導体メモリ１３は、情報処理端末１に対して取り外し可能なメモリである。したがって、情報処理端末１は、半導体メモリ１３を差し替えることで様々なデータにアクセスして処理を実行することができる。ただし、情報処理端末１が半導体メモリ１３を内蔵する構成であってもよい。
【００３３】
メモリコントローラ１３２は、制御部１１から与えられる暗号化されたコマンドデータを復号化する復号化回路１３２１を備えている。メモリコントローラ１３２は、復号化回路１３２１によりコマンドの復号化を行った後、コマンドの内容を判別し、コマンドの内容に応じた処理を実行する回路である。
【００３４】
制御部１１から与えられたコマンドが、データの読み出しコマンドである場合には、コマンドには読み出し命令と読み出しアドレスが含まれている。メモリコントローラ１３２は、制御信号としてread命令をメモリアレイ１３１に与え、メモリバスを介して読み出しアドレスをメモリアレイ１３１に出力することで、データを読み出すことができる。制御

部１１から与えられたコマンドがデータの書き込みコマンドである場合には、コマンドには書き込み命令と書き込みアドレスが含まれる。メモリコントローラ１３２は、制御信号としてwrite命令をメモリアレイ１３１に与え、アドレスバスを介して書き込みアドレスをメモリアレイ１３１に出力し、さらに、データバスを介して書き込みデータをメモリアレイ１３１に出力することで、書き込み処理を実行する。

【００３５】

これら読み出し／書き込みコマンドは、制御部１１において生成される場合と、サーバ２からダウンロードされる場合とがある。本発明は、特に、サーバ２からダウンロードされる書き込みコマンドに対する処理に特徴がある。したがって、以下においては、サーバ２からダウンロードされた書き込みコマンドに対する処理について説明する。

【００３６】

サーバ２は、制御部２１、通信部２２、記憶部２３、外部装置インタフェース２４を備えている。制御部２１は、ＣＰＵ、ＲＡＭなどを含み、サーバ２の全体制御を行う。通信部２２は、情報処理端末１との間で通信処理を実行する。記憶部２３は、ハードディスク、ＲＯＭなどの記憶媒体であり、コマンドデータ９１とコンテンツデータ９２とが格納されている。

【００３７】

コマンドデータ９１は、具体的には、コンテンツデータ９２を半導体メモリ１３に書き込むための書き込みコマンドである。コンテンツデータ９２は、たとえば、アプリケーションプログラム、著作権保護データ、ゲームプログラムなどである。

【００３８】

外部装置インタフェース２４は、コマンド暗号化装置３を接続するインタフェースである。たとえば、外部装置インタフェース２４がＵＳＢインタフェースであり、コマンド暗号化装置３もＵＳＢインタフェースを備えている。そして、外部装置インタフェース２４とコマンド暗号化装置３がＵＳＢケーブルで接続される。あるいは、外部装置インタフェース２４がＰＣＩスロットであり、コマンド暗号化装置３がＰＣＩスロットに装着可能なデバイスであるような形態が想定される。いずれにしても、コマンド暗号化装置３は、ネットワークなどを介在させず、直接信号ケーブルなどを介してサーバ２に接続される形態である。そのインタフェースの規格は特に限定されるものではない。

【００３９】

コマンド暗号化装置３は、暗号化回路３１を備えている。暗号化回路３１は、サーバ２から与えられたコマンドデータ９１を暗号化回路３１により暗号化する。コマンド暗号化装置３は、また、暗号化したコマンドデータ９１を制御部２１に転送する。

【００４０】

以上の如く構成されたシステムにより実行されるコンテンツデータ９２のダウンロードおよび書き込み処理の流れについて説明する。

【００４１】

まず、ユーザは、情報処理端末１の操作を行い、コンテンツデータ９２のダウンロード指示を行う。この指示は、情報処理端末１が備える図示せぬ操作ボタンなどを利用して行われる。ダウンロードの指示が行われると、制御部１１がサーバ２に対してコンテンツデータ９２のダウンロード要求を送信する。

【００４２】

サーバ２の制御部２１は、ダウンロード要求を受信すると、記憶部２３からコマンドデータ９１を取得し、コマンド暗号化装置３に転送する。コマンド暗号化装置３は、取得したコマンドデータ９１を暗号化回路３１により暗号化する。暗号化されたコマンドデータ９１は制御部２１に転送される。

【００４３】

次に、制御部２１は、コンテンツデータ９２と暗号化されたコマンドデータ９１とを情報処理端末１に対して送信する。これにより、情報処理端末１は、コンテンツデータ９２と暗号化されたコマンドデータ９１とをダウンロードする。

【００４４】
続いて、情報処理端末１では、制御部１１が、コンテンツデータ９２と暗号化されたコマンドデータ９１とをメモリコントローラ１３２に転送する。メモリコントローラ１３２では、復号化回路１３２１が、暗号化コマンドデータの復号化を行う。つまり、復号化回路１３２１は、コマンド暗号化装置３において暗号化されたデータを復号可能なアルゴリズムを持った回路として構成されている。
【００４５】
復号化回路１３２１において、コマンドデータ９１が復号化されると、メモリコントローラ１３２は、このコマンドデータ９１に従った処理を実行する。上述したように、コマンドデータ９１は、コンテンツデータ９２の書き込みコマンドである。メモリコントローラ１３２は、コマンドデータ９１に含まれる書き込み命令と書き込みアドレスを取得し、制御信号としてwrite命令をメモリアレイ１３１に与える。また、アドレスバスを介して書き込みアドレスをメモリアレイ１３１に与える。さらに、データバスを介してコンテンツデータ９２をメモリアレイ１３１に与える。これにより、メモリアレイ１３１に対するコンテンツデータ９２の書き込み処理が実行されるのである。
【００４６】
本実施の形態のメモリ書き込みシステムは、以上のような構成としているので、コンテンツデータ９２の不正なコピーを防止することができる。つまり、コンテンツデータ９２を半導体メモリ１３に書き込むためには、書き込みコマンドであるコマンドデータ９１が必要である。そして、ユーザが使用する情報処理端末１にダウンロードされるコマンドデータ９１は、既に暗号化されている。したがって、ユーザが書き込みコマンドを観測することは困難である。さらに、暗号化コマンドは、情報処理端末１の制御部１１においても復号化されることなく、メモリコントローラ１３２に与えられる。メモリコントローラ１３２は、ハードウェアにより暗号化されたコマンドデータ９１を復号化するが、この復号化されたコマンドデータ９１は、メモリアレイ１３１に対して命令やアドレス情報を出力する回路を制御する信号として利用されるが、平文としてＲＡＭなどに格納されることはない。したがって、ユーザが、書き込みコマンドを観測することは非常に困難となっているのである。
【００４７】
さらに、コマンドデータ９１は、サーバ２においてソフトウェア処理により暗号化されるのではなく、外部に接続されたハードウェア装置であるコマンド暗号化装置３により暗号化される。したがって、暗号化ロジックを観測することが困難であり、不正コピーを有効に防止することができる。
【００４８】
なお、第１の実施の形態においては、サーバ２の記憶部２３に、コマンドデータ９１が平文として格納されているため、サーバ２が信頼のおける者によって管理され、セキュリティ強度が高くなっていることが条件となる。
【００４９】
｛第２の実施の形態｝
次に、本発明の第２の実施の形態について説明する。図２は、第２の実施の形態に係るメモリ書き込みシステムの全体図である。第１の実施の形態と異なる点は、サーバ２の記憶部２３には、コマンドデータ９１が格納されていない点である。コマンド暗号化装置３の記憶部３２に、コマンドデータ９１が格納されている。
【００５０】
第１の実施の形態と同様、サーバ２は、情報処理端末１からコンテンツデータ９２のダウンロード要求を受信する。ダウンロード要求を受信すると、制御部２１は、コマンド暗号化装置３に対してコマンド要求信号および暗号化パラメータを与える。つまり、暗号化されたコマンドデータ９１の転送を要求する信号を出力する。
【００５１】
コマンド暗号化装置３は、コマンド要求信号および暗号化パラメータを受けると、記憶

部３２からコマンドデータ９１を取得し、暗号化回路３１においてコマンドデータ９１を暗号化する。このとき、サーバ２から受け取った暗号化パラメータを鍵情報として暗号化処理を実行する。そして、暗号化されたコマンドデータ９１を制御部２１に転送するのである。

【００５２】

この後の処理は、第１の実施の形態と同様である。サーバ２から情報処理端末１に対してコンテンツデータ９２と暗号化されたコマンドデータ９１とが送信される。情報処理端末１では、メモリコントローラ１３２においてコマンドデータ９１が復号化され、コンテンツデータ９２のメモリアレイ１３１に対する書き込み処理が実行されるのである。

【００５３】

この実施の形態のメモリ書き込みシステムを利用することで、第１の実施の形態と同様、ユーザが書き込みコマンドを観測することを困難とすることができる。これにより悪意ある者によるコンテンツデータ９２の不正な書き込み処理を排除することができる。

【００５４】

また、上述したように、第２の実施の形態においては、コマンドデータ９１がサーバ２の記憶部２３にも格納されていない。コマンドデータ９１は、コマンド暗号化装置３の記憶部３２に格納されているが、この記憶部３２は、外部からアクセスするインタフェースを備えていない。記憶部３２は、暗号化回路３１によってのみアクセス可能となっており、コマンドデータ９１が暗号化されずに、コマンド暗号化装置３の外部に出力されることはない。したがって、コマンドデータ９１の平文が、ハードウェアで隠蔽された状態となっており、よりセキュリティを高めることができる。この第２の実施の形態であれば、サーバ２には、コマンドデータ９１が格納されないため、サーバ２として、委託業者により管理されるサーバを利用することも可能となる。

【００５５】

｛第３の実施の形態｝

次に、本発明の第３の実施の形態について説明する。図３は、第３の実施の形態に係るメモリ書き込みシステムの全体図である。第１の実施の形態と異なる点は、サーバ２には、コマンド暗号化装置３が接続されていない。サーバ２には、ネットワーク６を介して暗号化サーバ５が接続されている。

【００５６】

ここで、ネットワーク６および暗号化サーバ５は、セキュリティ強度の高い構成となっている。つまり、ネットワーク６は、ＬＡＮなどの閉じたネットワークであり、ネットワーク６や暗号化サーバ５が設置される部屋の入退出管理も徹底されている。

【００５７】

暗号化サーバ５は、暗号処理部５１と通信部５２を備えている。暗号処理部５１は、暗号化サーバ５に格納されている暗号処理プログラムが、ＣＰＵなどのハードウェア資源を利用して実行することにより実現される機能部である。つまり、ソフトウェア処理によりコマンドデータ９１を暗号化する処理部である。通信部５２は、サーバ２との間で通信処理を実行する。

【００５８】

第１の実施の形態と同様、サーバ２は、情報処理端末１からコンテンツデータ９２のダウンロード要求を受信する。ダウンロード要求を受信すると、制御部２１は、ネットワーク６経由で暗号化サーバ５に対してコマンドデータ９１を送信する。

【００５９】

暗号化サーバ５は、コマンドデータ９１を受信すると、暗号化処理部５１においてコマンドデータ９１を暗号化する。そして、暗号化されたコマンドデータ９１をサーバ２に送信するのである。

【００６０】

この後の処理は、第１の実施の形態と同様である。サーバ２から情報処理端末１に対してコンテンツデータ９２と暗号化されたコマンドデータ９１とが送信される。情報処理端

末１では、メモリコントローラ１３２においてコマンドデータ９１が復号化され、コンテンツデータ９２のメモリアレイ１３１に対する書き込み処理が実行されるのである。

【００６１】

この実施の形態のメモリ書き込みシステムを利用することで、第１の実施の形態と同様、ユーザが書き込みコマンドを観測することを困難とすることができる。これにより悪意ある者によるコンテンツデータ９２の不正な書き込み処理を排除することができる。

【００６２】

また、第３の実施の形態に、第２の実施の形態と同様の考え方を取り入れる構成としてもよい。つまり、コマンドデータ９１をサーバ２に格納するのではなく、信頼のおけるセキュアなエリア内に設置された暗号化サーバ５内に格納するのである。サーバ２は、情報処理端末１からコンテンツのダウンロード要求を受けると、第２の実施の形態と同様、コマンド要求信号および暗号化パラメータを暗号化サーバ５に送信するのである。暗号化サーバ５は、内部に記憶しているコマンドデータ９１を、受信した暗号化パラメータを鍵情報として暗号化するのである。このような構成とすることで、コマンドデータ９１の平文が信頼性のある暗号化サーバ５内にだけ存在することになり、セキュリティ強度の高い構成となる。また、サーバ２には、コマンドデータ９１が格納されないため、サーバ２として、委託業者により管理されるサーバを利用することも可能となる。

【００６３】

｛第４の実施の形態｝

次に、本発明の第４の実施の形態について説明する。図４は、第４の実施の形態に係るメモリ書き込みシステムの全体図である。第１の実施の形態と異なる点は、サーバ２の外部装置インタフェース２４に、さらに、コンテンツ暗号化装置７が接続されている。コンテンツ暗号化装置７は、暗号化回路７１を備えている。コンテンツ暗号化装置７も、ＵＳＢやＰＣＩなどのインタフェースで接続された外部装置であり、ハードウェア処理により、コンテンツデータ９２の暗号化を行う。

【００６４】

第１の実施の形態と、さらに異なる点は、情報処理端末１がコンテンツデータ９２のダウンロード要求を行うとき、この要求データに半導体メモリ１３のメモリＩＤ９３が含められる点である。このメモリＩＤ９３は、コンテンツデータ９２を暗号化するときの鍵情報として利用される。メモリＩＤ９３は、メモリコントローラ１３２内のＲＯＭ等に格納されている。メモリＩＤ９３は、半導体メモリ１３に固有の情報である。

【００６５】

まず、ユーザによって、コンテンツデータ９２のダウンロード操作が行われると、制御部１１は、サーバ２に対してコンテンツデータ９２のダウンロード要求を送信する。このとき、制御部１１は、メモリコントローラ１３２からメモリＩＤ９３を取得し、ダウンロード要求にメモリＩＤ９３を含める。

【００６６】

サーバ２では、ダウンロード要求を受信すると、制御部２１が、記憶部２３からコマンドデータ９１とコンテンツデータ９２とを取得する。そして、制御部２１は、コマンドデータ９１をコマンド暗号化装置３に転送し、コンテンツデータ９２をコンテンツ暗号化装置７に転送する。また、制御部２１は、情報処理端末１から受信したメモリＩＤ９３をコンテンツ暗号化装置７に転送する。

【００６７】

コマンド暗号化装置３は、暗号化回路３１によりコマンドデータ９１を暗号化し、暗号化したコマンドデータ９１を制御部２１に転送する。コンテンツ暗号化装置７は、暗号化回路７１によりコンテンツデータ９２を暗号化する。このとき、メモリＩＤ９３を暗号化の鍵情報として利用する。あるいは、鍵情報の一部として利用してもよい。暗号化されたコンテンツデータ９２は、制御部２１に転送される。

【００６８】

次に、制御部２１は、情報処理端末１に対して、暗号化されたコマンドデータ９１と暗

号化されたコンテンツデータ９２とを送信する。このようにして、情報処理端末１は、暗号化コマンドと暗号化コンテンツを取得する。

【００６９】

続いて、制御部１１が、暗号化されたコマンドデータ９１とコンテンツデータ９２とをメモリコントローラ１３２に出力する。メモリコントローラ１３２は、復号化回路１３２１により、コマンドデータ９１とコンテンツデータ９２とを復号化する。コンテンツデータ９２の復号化には、メモリＩＤ９３が鍵情報として利用される。そして、メモリコントローラ１３２は、復号されたコマンドを利用して復号されたコンテンツデータ９２をメモリアレイ１３１に格納するのである。

【００７０】

この実施の形態のメモリ書き込みシステムを利用することで、第１の実施の形態と同様、ユーザが書き込みコマンドを観測することを困難とすることができる。これにより悪意ある者によるコンテンツデータ９２の不正な書き込み処理を排除することができる。

【００７１】

また、第４の実施の形態においては、コンテンツデータ９２が、半導体メモリ１３に固有の情報を利用して暗号化されている。したがって、書き込みコマンドの観測を困難とすることとあわせて、コンテンツ自体にもセキュリティを施すことで、コンテンツデータ９２の不正利用を有効に防止することが可能である。また、コンテンツデータ９２は、半導体メモリ１３に固有の情報であるメモリＩＤ９３を鍵情報として暗号化されるので、第三者が取得したとしても、復号化が不可能であり、セキュリティ強度の高い処理となっている。

【００７２】

なお、第４の実施の形態においては、コマンドデータ９１がサーバ２の記憶部２３に格納される形態となっているが、第２の実施の形態と同様、コマンド暗号化装置３内の記憶部にコマンドデータ９１を格納するようにしてもよい。この場合、制御部１１は、コマンド暗号化装置３に対しては、コマンド要求信号を与えるようにすればよい。これにより、第２の実施の形態と同様、コマンドの平文が暗号化装置内だけに存在する構成となり、セキュリティの強化を図ることができる。また、コンテンツ暗号化装置７内の記憶部にコンテンツデータ９２を格納するようにしてもよい。

【００７３】

また、第４の実施の形態と第３の実施の形態とを合わせた構成としてもよい。つまり、コマンドデータ９１については、第３の実施の形態と同様、ネットワーク６を介して接続された暗号化サーバ５において暗号化し、コンテンツデータ９２については、この第４の実施の形態で説明したように、コンテンツ暗号化装置７において暗号化するのである。つまり、コマンドデータ９１については、暗号化サーバ５においてソフトウェア処理により暗号化を行い、コンテンツデータ９２については、ハードウェア処理により暗号化を行うのである。ただし、第３の実施の形態でも説明したように、暗号化サーバ５およびネットワーク６がセキュアな状態であることが条件となる。また、コマンドデータ９１の平文は、サーバ２に格納されていてもよいし、暗号化サーバ５に格納されていてもよい。あるいは、その逆で、コマンドデータ９１を外部のハードウェア装置で暗号化し、コンテンツデータ９２をネットワーク経由で接続されたサーバでソフトウェア処理により暗号化させる形態であってもよい。さらには、コマンドデータ９１をネットワークで接続されたサーバにおいて暗号化し、コンテンツデータ９２もネットワークで接続されたサーバにおいて暗号化するようにしてもよい。つまり、コマンドとコンテンツの両方をソフトウェア処理により暗号化する形態でもよい。

【００７４】

｛変形例｝

以上、本発明の各実施の形態について説明したが、情報処理端末１が、コマンドデータ９１やコンテンツデータ９２を取得する方法は、ネットワークを介したダウンロードに限られるものではない。たとえば、暗号化されたコマンドデータ９１が、メモリＫＥＹなど

に格納されて供給されてもよい。ユーザは、そのメモリＫＥＹを情報処理端末１に挿入することで、暗号化コマンドを取得することが可能である。同様に、コンテンツデータ９２に関しても、メモリカードなどの記録媒体を利用して供給される形態であってもよい。

【００７５】

また、上記の実施の形態において、情報処理端末１は、暗号化されたコマンドデータ９１と、コンテンツデータ９２の両方を外部から取得した。これ以外の構成として、暗号化コマンドはダウンロードや各種の媒体を介して外部から取得し、コンテンツデータについては、情報処理端末１内で生成するという形態であってもよい。

【００７６】

また、上記の各実施の形態においては、同じサーバ２からコマンドデータ９１とコンテンツデータ９２をダウンロードする場合を例に説明したが、もちろん、これらのデータが別のサーバからダウンロードされる形態であってもよい。

【図面の簡単な説明】

【００７７】

【図１】第１の実施の形態に係るメモリ書き込みシステムの全体構成図である。

【図２】第２の実施の形態に係るメモリ書き込みシステムの全体構成図である。

【図３】第３の実施の形態に係るメモリ書き込みシステムの全体構成図である。

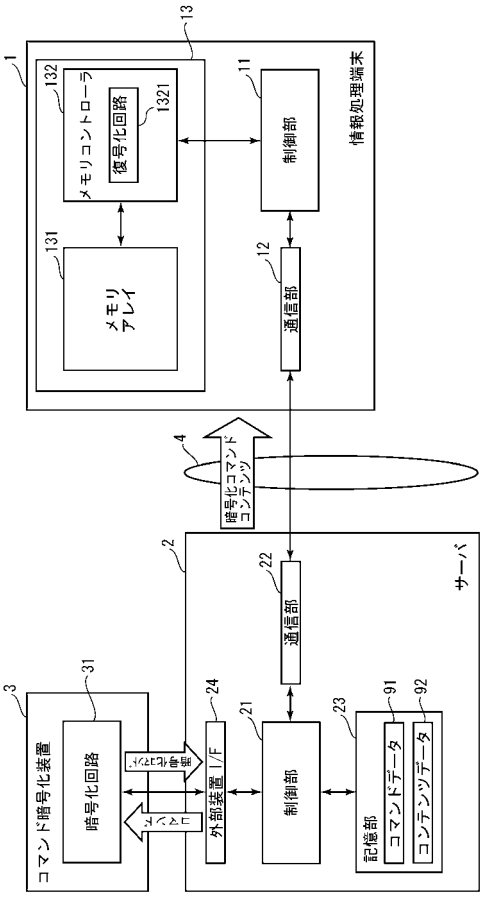
【図４】第４の実施の形態に係るメモリ書き込みシステムの全体構成図である。

【符号の説明】

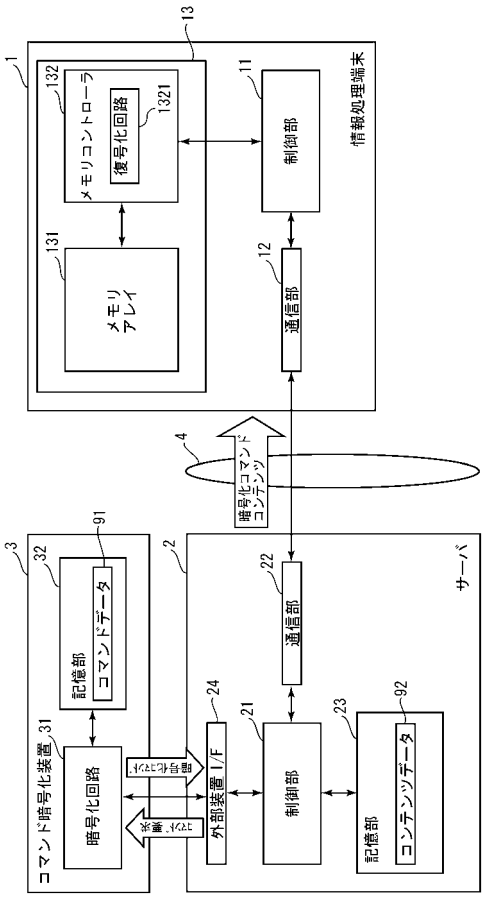
【００７８】

１　　情報処理端末
２　　サーバ
３　　コマンド暗号化装置
４　　ネットワーク
１３　半導体メモリ
３１　暗号化回路
９１　コマンドデータ
９２　コンテンツデータ
１３２　メモリコントローラ

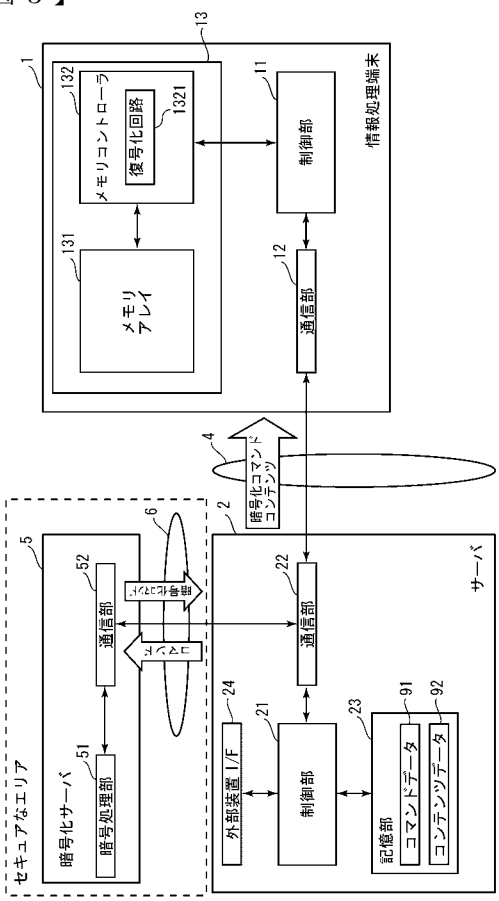
【図１】


情報処理端末
メモリコントローラ
復号化回路
メモリアレイ
制御部
通信部
暗号化コマンド
コンテンツ
サーバ
コマンド暗号化装置
暗号化回路
外部装置I/F
記憶部
コマンドデータ
コンテンツデータ

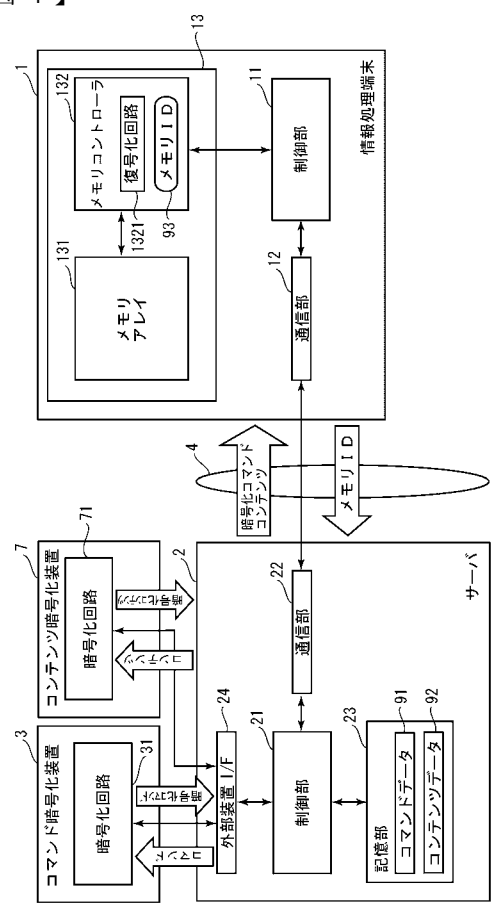
【図２】


情報処理端末
メモリコントローラ
復号化回路
メモリアレイ
制御部
通信部
暗号化コマンド
コンテンツ
サーバ
コマンド暗号化装置
暗号化回路
外部装置I/F
記憶部
コマンドデータ
コンテンツデータ

【図３】


情報処理端末
メモリコントローラ
復号化回路
メモリアレイ
制御部
通信部
暗号化コマンド
コンテンツ
サーバ
セキュアなエリア
暗号化サーバ
暗号処理部
外部装置I/F
記憶部
コマンドデータ
コンテンツデータ

【図４】


情報処理端末
メモリコントローラ
復号化回路
メモリID
メモリアレイ
制御部
通信部
暗号化コマンド
コンテンツ
メモリID
サーバ
コンテンツ暗号化装置
暗号化回路
コマンド暗号化装置
外部装置I/F
記憶部
コマンドデータ
コンテンツデータ