(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4765485号
(P4765485)
(45)発行日　平成23年9月7日(2011.9.7)　(24)登録日　平成23年6月24日(2011.6.24)

(51)Int.Cl.　　F I
G06F 21/24 (2006.01)　　G06F 12/14 560A
H04N 5/91 (2006.01)　　H04N 5/91 P

請求項の数 20　(全 56 頁)

(21)出願番号　特願2005-245943(P2005-245943)
(22)出願日　平成17年8月26日(2005.8.26)
(65)公開番号　特開2007-58749(P2007-58749A)
(43)公開日　平成19年3月8日(2007.3.8)
審査請求日　平成18年6月1日(2006.6.1)

前置審査

(73)特許権者　000002185
ソニー株式会社
東京都港区港南１丁目７番１号
(74)代理人　100093241
弁理士　宮田　正昭
(72)発明者　高島　芳和
東京都品川区北品川６丁目７番３５号　ソニー株式会社内

審査官　田中　慎太郎

最終頁に続く

(54)【発明の名称】情報処理装置、情報記録媒体、および情報処理方法、並びにコンピュータ・プログラム

(57)【特許請求の範囲】
【請求項１】
情報記録媒体からのコンテンツ再生処理を実行する情報処理装置であり、
コンテンツ再生シーケンスにおけるセキュリティチェック情報に基づいて出力メッセージを決定し、出力メッセージの選択情報を伴うメッセージ出力命令をユーザインタフェース処理部に出力するセキュリティ情報処理部と、
前記セキュリティ情報処理部から入力する選択情報に基づくメッセージ情報取得を行ない、表示部に出力するユーザインタフェース処理部と、
前記セキュリティ情報処理部が書き込み、前記ユーザインタフェース処理部が読み出す第１レジスタと、
前記ユーザインタフェース処理部が書き込み、前記セキュリティ情報処理部が読み出す第２レジスタを有し、
前記セキュリティ情報処理部は、前記第１レジスタにメッセージ選択情報を格納し、
前記ユーザインタフェース処理部は、前記第１レジスタから前記メッセージ選択情報を取得し、取得したメッセージ選択情報に対応するメッセージを前記表示部に出力し、表示メッセージに対応したユーザ入力を受信し、該受信ユーザ入力情報を前記第２レジスタに格納し、
前記セキュリティ情報処理部は、前記第２レジスタから前記ユーザ入力情報を取得する処理を実行する構成であることを特徴とする情報処理装置。
【請求項２】

前記セキュリティ情報処理部は、
セキュリティチェック情報に基づく出力メッセージ内容の決定、およびコンテンツ再生プレーヤ情報に基づく出力メッセージ言語の決定処理を実行し、該決定情報に従って選択するメッセージ選択情報を前記ユーザインタフェース処理部に出力する処理を実行する構成であることを特徴とする請求項１に記載の情報処理装置。
【請求項３】
前記ユーザインタフェース処理部は、
オンスクリーン・ディスプレイ（ＯＳＤ）機能実行部として構成され、
前記セキュリティ情報処理部は、
出力メッセージの選択情報を伴うメッセージ出力命令をＯＳＤ呼び出し（ＯＳＤ＿ＣＡＬＬ）に基づいて実行する構成であることを特徴とする請求項１に記載の情報処理装置。
【請求項４】
前記セキュリティ情報処理部は、
情報記録媒体に記録された命令コードを取得して命令コードに従ったデータ処理を実行するバーチャルマシンとして構成されることを特徴とする請求項１に記載の情報処理装置。
【請求項５】
情報記録媒体からのコンテンツ再生処理を実行する情報処理装置であり、
コンテンツ再生シーケンスにおけるセキュリティチェック情報に対応するエラーコードを取得し、該エラーコードを第１レジスタに書き込む処理を実行するセキュリティ情報処理部と、
前記第１レジスタからエラーコードを取得し、取得エラーコードに対応するメッセージ情報取得を行ない、取得メッセージを表示部に出力するアプリケーション実行部と、
前記セキュリティ情報処理部が書き込み、前記アプリケーション実行部が読み出す第１レジスタと、
前記アプリケーション実行部が書き込み、前記セキュリティ情報処理部が読み出す第２レジスタを有し、
前記セキュリティ情報処理部は、前記第１レジスタに前記エラーコードを格納し、
前記アプリケーション実行部は、前記第１レジスタから前記エラーコードを取得し、取得したエラーコードに対応して設定されたメッセージを表示部に出力し、表示メッセージに対応したユーザ入力を受信し、該受信ユーザ入力情報を前記第２レジスタに書き込む処理を実行する構成であり、
前記セキュリティ情報処理部は、
前記第２レジスタに書き込まれたユーザ入力情報の取得処理を実行する構成であることを特徴とする情報処理装置。
【請求項６】
前記セキュリティ情報処理部は、
前記アプリケーション実行部に対する実行アプリケーションの切り替え命令を出力する構成を有し、
前記アプリケーション実行部は、
前記アプリケーションの切り替え命令に基づいて、
前記セキュリティ情報処理部との前記第１レジスタを介したデータ転送処理および前記表示部に対するメッセージ出力を実行するアプリケーションへの切り替えを実行する構成であることを特徴とする請求項５に記載の情報処理装置。
【請求項７】
前記セキュリティ情報処理部、および前記アプリケーション実行部は、処理状況を示す状態値を、前記第１レジスタまたは前記第２レジスタに書き込み、前記セキュリティ情報処理部、および前記アプリケーション実行部は、前記第１レジスタまたは前記第２レジスタに書き込まれた処理状況を示す状態値の読み取りを実行して処理状況の確認を行う構成であることを特徴とする請求項５に記載の情報処理装置。

【請求項８】
前記セキュリティ情報処理部、および前記アプリケーション実行部は、相互の信頼性確認処理を、前記第１レジスタまたは前記第２レジスタを適用したデータ転送処理によって実行する構成であることを特徴とする請求項５に記載の情報処理装置。
【請求項９】
前記セキュリティ情報処理部は、
情報記録媒体に記録された命令コードを取得して命令コードに従ったデータ処理を実行するバーチャルマシンとして構成されることを特徴とする請求項５に記載の情報処理装置。
【請求項１０】
情報処理装置において、情報記録媒体からのコンテンツ再生処理を実行する情報処理方法であり、
セキュリティ情報処理部において、コンテンツ再生シーケンスにおけるセキュリティチェック情報に基づいて出力メッセージを決定し、出力メッセージの選択情報を伴うメッセージ出力命令をユーザインタフェース処理部に出力するセキュリティ情報処理ステップと、
ユーザインタフェース処理部において、前記セキュリティ情報処理部から入力する選択情報に基づくメッセージ情報取得を行ない、表示部に出力するユーザインタフェース処理ステップを有し、
前記情報処理装置は、前記セキュリティ情報処理部が書き込み、前記ユーザインタフェース処理部が読み出す第１レジスタと、前記ユーザインタフェース処理部が書き込み、前記セキュリティ情報処理部が読み出す第２レジスタを有し、
前記セキュリティ情報処理ステップは、前記セキュリティ情報処理部が前記第１レジスタに対して前記選択情報を格納するステップを含み、
前記ユーザインタフェース処理ステップは、前記ユーザインタフェース処理部が前記第１レジスタから前記選択情報を取得し、取得した選択情報に対応して設定されたメッセージを表示部に出力するステップを含み、
さらに、
前記ユーザインタフェース処理部において、前記表示部に対する表示メッセージに対応したユーザ入力を受信し、該受信ユーザ入力情報を、前記ユーザインタフェース処理部が前記第２レジスタに格納するステップと、
前記セキュリティ情報処理部が、前記第２レジスタから前記ユーザ入力情報を取得する処理を実行するステップを有することを特徴とする情報処理方法。
【請求項１１】
前記セキュリティ情報処理ステップは、
セキュリティチェック情報に基づく出力メッセージ内容の決定、およびコンテンツ再生プレーヤ情報に基づく出力メッセージ言語の決定処理を実行し、該決定情報に従って選択するメッセージ選択情報を前記ユーザインタフェース処理部に出力する処理を実行することを特徴とする請求項１０に記載の情報処理方法。
【請求項１２】
前記ユーザインタフェース処理部は、オンスクリーン・ディスプレイ（ＯＳＤ）機能実行部として構成され、
前記セキュリティ情報処理ステップは、
出力メッセージの選択情報を伴うメッセージ出力命令をＯＳＤ呼び出し（ＯＳＤ＿ＣＡＬＬ）に基づいて実行することを特徴とする請求項１０に記載の情報処理方法。
【請求項１３】
情報処理装置において、情報記録媒体からのコンテンツ再生処理を実行する情報処理方法であり、
セキュリティ情報処理部において、コンテンツ再生シーケンスにおけるセキュリティチェック情報に対応するエラーコードを取得し、該エラーコードを、第１レジスタに書き込

む処理を実行するセキュリティ情報処理ステップと、
アプリケーション実行部において、前記第１レジスタからエラーコードを取得し、取得エラーコードに対応するメッセージ情報取得を行ない、取得メッセージを表示部に出力するアプリケーション実行ステップを有し、
前記情報処理装置は、前記セキュリティ情報処理部が書き込み、前記アプリケーション実行部が読み出す第１レジスタと、前記アプリケーション実行部が書き込み、前記セキュリティ情報処理部が読み出す第２レジスタを有し、
前記セキュリティ情報処理ステップは、前記セキュリティ情報処理部が前記第１レジスタに前記エラーコードを格納するステップを含み、
前記アプリケーション実行ステップは、前記アプリケーション実行部が前記第１レジスタから前記エラーコードを取得し、取得したエラーコードに対応して設定されたメッセージを表示部に出力するステップを含み、
さらに、
前記アプリケーション実行部において、
前記表示部に対する表示メッセージに対応したユーザ入力を受信し、該受信ユーザ入力情報を、前記第２レジスタに書き込む処理を実行するステップと、
前記セキュリティ情報処理部において、
前記第２レジスタに書き込まれたユーザ入力情報の取得処理を実行するステップと、
を有することを特徴とする情報処理方法。
【請求項１４】
前記情報処理方法は、さらに、
前記セキュリティ情報処理部において、前記アプリケーション実行部に対する実行アプリケーションの切り替え命令を出力するステップと、
前記アプリケーション実行部において、前記アプリケーションの切り替え命令に基づいて、前記セキュリティ情報処理部との前記第１レジスタを介したデータ転送処理および前記表示部に対するメッセージ出力を実行するアプリケーションへの切り替えを実行するステップと、
を有することを特徴とする請求項１３に記載の情報処理方法。
【請求項１５】
前記情報処理方法は、さらに、
前記セキュリティ情報処理部、または前記アプリケーション実行部において、処理状況を示す状態値を、前記第１レジスタまたは前記第２レジスタに書き込むステップと、
前記セキュリティ情報処理部、または前記アプリケーション実行部において、前記第１レジスタまたは前記第２レジスタに書き込まれた処理状況を示す状態値の読み取りを実行して処理状況の確認を行うステップと、
を有することを特徴とする請求項１３に記載の情報処理方法。
【請求項１６】
前記情報処理方法は、さらに、
前記セキュリティ情報処理部、および前記アプリケーション実行部間において、相互の信頼性確認処理を、前記第１レジスタまたは前記第２レジスタを適用したデータ転送処理によって実行するステップを有することを特徴とする請求項１３に記載の情報処理方法。
【請求項１７】
セキュリティ情報処理部とユーザインタフェース処理部とを有する情報処理装置の前記セキュリティ情報処理部で実行されるコンピュータ・プログラムであり、
前記セキュリティ情報処理部において、コンテンツ再生シーケンスにおけるセキュリティチェック情報に基づいて出力メッセージを決定し、出力メッセージの選択情報をユーザインタフェース処理部に出力させるセキュリティ情報処理コードを有し、
前記情報処理装置は、前記セキュリティ情報処理部が書き込み、前記ユーザインタフェース処理部が読み出す第１レジスタと、前記ユーザインタフェース処理部が書き込み、前記セキュリティ情報処理部が読み出す第２レジスタを有し、

前記出力メッセージの選択情報をユーザインタフェース処理部に出力させるセキュリティ情報処理コードは、前記セキュリティ情報処理部が前記第１レジスタに対して前記選択情報を格納するコードを含み、

ユーザインタフェース処理コードが前記ユーザインタフェース処理部で実行されることで、

前記セキュリティ情報処理部が格納する選択情報を前記第１レジスタから取得し、

前記取得された選択情報に基づくメッセージ情報取得を行ない、

前記ユーザインタフェース処理部が前記選択情報を取得し、取得した選択情報に対応して設定されたメッセージを表示部に出力し、表示メッセージに対応したユーザ入力を受信し、該受信ユーザ入力情報を前記第２レジスタに格納し、

前記セキュリティ情報処理コードは、さらに、前記セキュリティ情報処理部に、前記第２レジスタから前記ユーザ入力情報を取得する処理を実行させるコードを含むことを特徴とするコンピュータ・プログラム。

【請求項１８】

セキュリティ情報処理部とユーザインタフェース処理部とを有する情報処理装置の前記ユーザインタフェース処理部で実行されるコンピュータ・プログラムであり、

前記情報処理装置は、前記セキュリティ情報処理部が書き込み、前記ユーザインタフェース処理部が読み出す第１レジスタと、前記ユーザインタフェース処理部が書き込み、前記セキュリティ情報処理部が読み出す第２レジスタを有し、

前記ユーザインタフェース処理部において、前記セキュリティ情報処理部が前記第１レジスタに格納したメッセージ選択情報を取得し、取得情報に基づく処理を実行させるユーザインタフェース処理コードを有し、

前記ユーザインタフェース処理コードは、

前記セキュリティ情報処理部がコンテンツ再生シーケンスにおけるセキュリティチェック情報に基づいて決定したメッセージ選択情報を前記第１レジスタから取得するコードと、

前記第１レジスタから取得したメッセージ選択情報に対応して設定されたメッセージを表示部に出力するコードと、

表示メッセージに対応したユーザ入力を受信し、該受信ユーザ入力情報を前記第２レジスタに格納するコードを含むことを特徴とするコンピュータ・プログラム。

【請求項１９】

セキュリティ情報処理部とアプリケーション実行部とを有する情報処理装置の前記セキュリティ情報処理部で実行されるコンピュータ・プログラムであり、

前記セキュリティ情報処理部において、コンテンツ再生シーケンスにおけるセキュリティチェック情報に対応するエラーコードを取得し、該エラーコードをアプリケーション実行部に出力させるセキュリティ情報処理コードを有し、

前記情報処理装置は、前記セキュリティ情報処理部が書き込み、前記アプリケーション実行部が読み出す第１レジスタと、前記アプリケーション実行部が書き込み、前記セキュリティ情報処理部が読み出す第２レジスタを有し、

前記エラーコードをアプリケーション実行部に出力させるセキュリティ情報処理コードは、前記セキュリティ情報処理部が前記第１レジスタに対して前記エラーコードを格納するコードであり、

アプリケーション実行部処理コードが前記アプリケーション実行部で実行されることで、

前記セキュリティ情報処理部が前記第１レジスタに格納するエラーコードを前記第１レジスタから取得し、取得エラーコードに対応するメッセージ取得を行ない、取得したエラーコードに対応して設定されたメッセージを表示部に出力し、表示メッセージに対応したユーザ入力を受信し、該受信ユーザ入力情報を前記第２レジスタに格納し、

前記セキュリティ情報処理コードは、さらに、前記セキュリティ情報処理部に、前記第２レジスタから前記ユーザ入力情報を取得する処理を実行させるコードを含むことを特徴

とするコンピュータ・プログラム。
【請求項２０】
セキュリティ情報処理部とアプリケーション実行部とを有する情報処理装置の前記アプリケーション実行部で実行されるコンピュータ・プログラムであり、
前記情報処理装置は、前記セキュリティ情報処理部が書き込み、前記アプリケーション実行部が読み出す第１レジスタと、前記アプリケーション実行部が書き込み、前記セキュリティ情報処理部が読み出す第２レジスタを有し、
前記アプリケーション実行部において、前記セキュリティ情報処理部が前記第１レジスタに格納したエラーコードを取得し、エラーコードに基づく処理を実行させるアプリケーション実行部処理コードを有し、
前記アプリケーション実行部処理コードは、
前記セキュリティ情報処理部がコンテンツ再生シーケンスにおけるセキュリティチェック情報に基づいて決定したエラーコードを前記第１レジスタから取得する処理コードと、
前記第１レジスタから取得したエラーコードに対応して設定されたメッセージを表示部に出力する処理コードと、
表示メッセージに対応したユーザ入力を受信し、該受信ユーザ入力情報を前記第２レジスタに格納するコードを含むことを特徴とするコンピュータ・プログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、情報処理装置、情報記録媒体、および情報処理方法、並びにコンピュータ・プログラムに関する。さらに、詳細には、コンテンツ利用管理の要求される様々なコンテンツに対するデータ変換処理により、不正なコンテンツ利用を排除し、厳格なコンテンツ利用管理を実現し、さらにコンテンツの利用停止状況などのメッセージ提示や、ユーザ確認を可能とした情報処理装置、情報記録媒体、および情報処理方法、並びにコンピュータ・プログラムに関する。
【背景技術】
【０００２】
音楽等のオーディオデータ、映画等の画像データ、ゲームプログラム、各種アプリケーション・プログラム等、様々なソフトウエアデータ（以下、これらをコンテンツ（Content）と呼ぶ）は、記録メディア、例えば、青色レーザを適用したＢｌｕ－ｒａｙディスク、あるいはＤＶＤ(Digital Versatile Disc)、ＭＤ(Mini Disc)、ＣＤ(Compact Disc)にデジタルデータとして格納することができる。特に、青色レーザを利用したＢｌｕ－ｒａｙディスクは、高密度記録可能なディスクであり大容量の映像コンテンツなどを高画質データとして記録することができる。
【０００３】
これら様々な情報記録媒体（記録メディア）にデジタルコンテンツが格納され、ユーザに提供される。ユーザは、所有するＰＣ（Personal Computer）、ディスクプレーヤ等の再生装置においてコンテンツの再生、利用を行う。
【０００４】
音楽データ、画像データ等、多くのコンテンツは、一般的にその作成者あるいは販売者に頒布権等が保有されている。従って、これらのコンテンツの配布に際しては、一定の利用制限、すなわち、正規なユーザに対してのみ、コンテンツの利用を許諾し、許可のない複製等が行われないようにする構成をとるのが一般的となっている。
【０００５】
デジタル記録装置および記録媒体によれば、例えば画像や音声を劣化させることなく記録、再生を繰り返すことが可能であり、不正コピーコンテンツのインターネットを介した配信や、コンテンツをＣＤ－Ｒ等にコピーした、いわゆる海賊版ディスクの流通や、ＰＣ等のハードディスクに格納したコピーコンテンツの利用が蔓延しているといった問題が発生している。

【０００６】
ＤＶＤ、あるいは近年開発が進んでいる青色レーザを利用した記録媒体等の大容量型記録媒体は、１枚の媒体に例えば映画１本～数本分の大量のデータをデジタル情報として記録することが可能である。このように映像情報等をデジタル情報として記録することが可能となってくると不正コピーを防止して著作権者の保護を図ることが益々重要な課題となっている。昨今では、このようなデジタルデータの不正なコピーを防ぐため、デジタル記録装置および記録媒体に違法なコピーを防止するための様々な技術が実用化されている。
【０００７】
例えば、ＤＶＤプレーヤでは、コンテンツ・スクランブルシステム（Ｃｏｎｔｅｎｔ Ｓｃｒａｍｂｌｅ Ｓｙｓｔｅｍ）が採用されている。コンテンツ・スクランブルシステムでは、例えばＤＶＤ－ＲＯＭ(Read Only Memory)にビデオデータやオーディオデータ等が暗号化されて記録されている構成において、スクランブルを解除することでコンテンツ再生を可能とするものである。
【０００８】
スクランブル解除処理には、ライセンスを受けたＤＶＤプレーヤに与えられた鍵などの特定データを適用した処理を実行することが必要となる。ライセンスは、不正コピーを行わない等の所定の動作規定に従うように設計されたＤＶＤプレーヤに対して与えられる。従って、ライセンスを受けたＤＶＤプレーヤでは、与えられた鍵などの特定データを利用して、ＤＶＤ－ＲＯＭに記録されたデータのスクランブル解除を行なうことにより、ＤＶＤ－ＲＯＭから画像や音声を再生することができる。
【０００９】
一方、ライセンスを受けていないＤＶＤプレーヤは、スクランブル処理されたデータのスクランブル解除に適用する鍵などの特定データを有していないため、ＤＶＤ－ＲＯＭに記録されたデータの再生を行うことができない。このように、コンテンツ・スクランブルシステム構成では、ライセンス時に要求される条件を満たしていないＤＶＤプレーヤは、デジタルデータを記録したＤＶＤ－ＲＯＭの再生を行なえないことになり、不正コピーが防止されるようになっている。
【００１０】
しかし、このようなコンテンツ・スクランブルシステムは、再生処理を実行するユーザデバイスとしての情報処理装置側の処理負荷が高くなるという問題がある。また、既存のスクランブルシステムの中には、既にスクランブル解除手法が解読され解読方法がインターネット等の通信手段を介して流通しているものも多く存在する。このように、一旦スクランブル手法が解読されてしまうと、不正なスクランブル解除処理によってコンテンツが不正に再生され、また複製されるなど、コンテンツの著作権、利用権の侵害という問題が発生する。
【００１１】
このスクランブル手法以外にも、様々なコンテンツ保護手法によって、正当なコンテンツ利用権のないユーザや再生装置における再生を禁止する構成が提案されている。例えば、特許文献１（特開平１０－４１９３４号公報）では、仮想マシンを用いて暗号データを解読するプログラムを実行することにより、暗号アルゴリズムを追加する技術について開示されている。しかし、このようなコンテンツ保護機構に基づいてコンテンツ再生が行なわれない場合、ユーザは、なぜコンテンツの再生ができないのかの理由や、コンテンツを利用するためにはどうすべきかなどの解決法を取得することができず、正当な権限を得てコンテンツを利用したいというユーザの要請に応えるための構成が十分ではないというのが現状である。
【００１２】
また、これまでのコンテンツの保護機構は、特定の映画などの大型コンテンツとしてのＡＶストリームを中心として保護を行なう構成としたものが多く、例えばＪａｖａ（登録商標）のようなプログラムによって処理されるコンテンツなど、映画等とは異なる小型のコンテンツについての保護については、あまり、考慮されていなかったという問題がある

。
【特許文献１】特開平１０－４１９３４号公報
【発明の開示】
【発明が解決しようとする課題】
【００１３】
本発明は、このような状況に鑑みてなされたものであり、コンテンツ保護機構に基づいてコンテンツ再生が行なわれない場合に、例えば、ユーザに対する状況提示や、解決手法の提示、ユーザの確認などを可能とした情報処理装置、情報記録媒体、および情報処理方法、並びにコンピュータ・プログラムを提供することを目的とするものである。
【００１４】
さらに、本発明は、映画等のＡＶストリームデータとは異なる小型のコンテンツについても、ＡＶストリームデータと同様、コンテンツ利用制限を設定し、厳格なコンテンツ保護を実現する情報処理装置、情報記録媒体、および情報処理方法、並びにコンピュータ・プログラムを提供することを目的とするものである。
【課題を解決するための手段】
【００１５】
本発明の第１の側面は、
情報記録媒体からのコンテンツ再生処理を実行する情報処理装置であり、
コンテンツ再生シーケンスにおけるセキュリティチェック情報に基づいて出力メッセージを決定し、出力メッセージの選択情報を伴うメッセージ出力命令をユーザインタフェース処理部に出力するセキュリティ情報処理部と、
前記セキュリティ情報処理部から入力する選択情報に基づくメッセージ情報取得を行ない、表示部に出力するユーザインタフェース処理部と、
前記セキュリティ情報処理部が書き込み、前記ユーザインタフェース処理部が読み出す第１レジスタと、
前記ユーザインタフェース処理部が書き込み、前記セキュリティ情報処理部が読み出す第２レジスタを有し、
前記セキュリティ情報処理部は、前記第１レジスタにメッセージ選択情報を格納し、
前記ユーザインタフェース処理部は、前記第１レジスタから前記メッセージ選択情報を取得し、取得したメッセージ選択情報に対応するメッセージを前記表示部に出力することを特徴とする情報処理装置にある。
【００１６】
さらに、本発明の情報処理装置の一実施態様において、前記セキュリティ情報処理部は、セキュリティチェック情報に基づく出力メッセージ内容の決定、およびコンテンツ再生プレーヤ情報に基づく出力メッセージ言語の決定処理を実行し、該決定情報に従って選択するメッセージ選択情報を前記ユーザインタフェース処理部に出力する処理を実行する構成であることを特徴とする。
【００１７】
さらに、本発明の情報処理装置の一実施態様において、前記ユーザインタフェース処理部は、前記表示部に対する表示メッセージに対応したユーザ入力を受信し、該受信ユーザ入力情報を前記第２レジスタに格納し、前記セキュリティ情報処理部は、前記第２レジスタから前記ユーザ入力情報を取得する処理を実行する構成であることを特徴とする。
【００１８】
さらに、本発明の情報処理装置の一実施態様において、前記ユーザインタフェース処理部は、オンスクリーン・ディスプレイ（ＯＳＤ）機能実行部として構成され、前記セキュリティ情報処理部は、出力メッセージの選択情報を伴うメッセージ出力命令をＯＳＤ呼び出し（ＯＳＤ＿ＣＡＬＬ）に基づいて実行する構成であることを特徴とする。
【００１９】
さらに、本発明の情報処理装置の一実施態様において、前記セキュリティ情報処理部は、情報記録媒体に記録された命令コードを取得して命令コードに従ったデータ処理を実行

するバーチャルマシンとして構成されることを特徴とする。

【００２０】

さらに、本発明の第２の側面は、

情報記録媒体からのコンテンツ再生処理を実行する情報処理装置であり、

コンテンツ再生シーケンスにおけるセキュリティチェック情報に対応するエラーコードを取得し、該エラーコードを第１レジスタに書き込む処理を実行するセキュリティ情報処理部と、

前記第１レジスタからエラーコードを取得し、取得エラーコードに対応するメッセージ情報取得を行ない、取得メッセージを表示部に出力するアプリケーション実行部と、

前記セキュリティ情報処理部が書き込み、前記アプリケーション実行部が読み出す第１レジスタと、

前記アプリケーション実行部が書き込み、前記セキュリティ情報処理部が読み出す第２レジスタを有し、

前記セキュリティ情報処理部は、前記第１レジスタに前記エラーコードを格納し、

前記アプリケーション実行部は、前記第１レジスタから前記エラーコードを取得し、取得したエラーコードに対応して設定されたメッセージを表示部に出力することを特徴とする情報処理装置にある。

【００２１】

さらに、本発明の情報処理装置の一実施態様において、前記アプリケーション実行部は、前記表示部に対する表示メッセージに対応したユーザ入力を受信し、該受信ユーザ入力情報を前記第２レジスタに書き込む処理を実行する構成であり、前記セキュリティ情報処理部は、前記第２レジスタに書き込まれたユーザ入力情報の取得処理を実行する構成であることを特徴とする。

【００２２】

さらに、本発明の情報処理装置の一実施態様において、前記セキュリティ情報処理部は、前記アプリケーション実行部に対する実行アプリケーションの切り替え命令を出力する構成を有し、前記アプリケーション実行部は、前記アプリケーションの切り替え命令に基づいて、前記セキュリティ情報処理部との前記第１レジスタを介したデータ転送処理および前記表示部に対するメッセージ出力を実行するアプリケーションへの切り替えを実行する構成であることを特徴とする。

【００２３】

さらに、本発明の情報処理装置の一実施態様において、前記セキュリティ情報処理部、および前記アプリケーション実行部は、処理状況を示す状態値を、前記第１レジスタまたは前記第２レジスタに書き込み、前記セキュリティ情報処理部、および前記アプリケーション実行部は、前記第１レジスタまたは前記第２レジスタに書き込まれた処理状況を示す状態値の読み取りを実行して処理状況の確認を行う構成であることを特徴とする。

【００２４】

さらに、本発明の情報処理装置の一実施態様において、前記セキュリティ情報処理部、および前記アプリケーション実行部は、相互の信頼性確認処理を、前記第１レジスタまたは前記第２レジスタを適用したデータ転送処理によって実行する構成であることを特徴とする。

【００２５】

さらに、本発明の情報処理装置の一実施態様において、前記セキュリティ情報処理部は、情報記録媒体に記録された命令コードを取得して命令コードに従ったデータ処理を実行するバーチャルマシンとして構成されることを特徴とする。

【００３１】

さらに、本発明の第３の側面は、

情報処理装置において、情報記録媒体からのコンテンツ再生処理を実行する情報処理方法であり、

セキュリティ情報処理部において、コンテンツ再生シーケンスにおけるセキュリティチ

ェック情報に基づいて出力メッセージを決定し、出力メッセージの選択情報を伴うメッセージ出力命令をユーザインタフェース処理部に出力するセキュリティ情報処理ステップと、

ユーザインタフェース処理部において、前記セキュリティ情報処理部から入力する選択情報に基づくメッセージ情報取得を行ない、表示部に出力するユーザインタフェース処理ステップを有し、

前記情報処理装置は、前記セキュリティ情報処理部が書き込み、前記ユーザインタフェース処理部が読み出す第１レジスタと、前記ユーザインタフェース処理部が書き込み、前記セキュリティ情報処理部が読み出す第２レジスタを有し、

前記セキュリティ情報処理ステップは、前記セキュリティ情報処理部が前記第１レジスタに対して前記選択情報を格納するステップを含み、

前記ユーザインタフェース処理ステップは、前記ユーザインタフェース処理部が前記第１レジスタから前記選択情報を取得し、取得した選択情報に対応して設定されたメッセージを表示部に出力するステップを含むことを特徴とする情報処理方法にある。

【００３２】

さらに、本発明の情報処理方法の一実施態様において、前記セキュリティ情報処理ステップは、セキュリティチェック情報に基づく出力メッセージ内容の決定、およびコンテンツ再生プレーヤ情報に基づく出力メッセージ言語の決定処理を実行し、該決定情報に従って選択するメッセージ選択情報を前記ユーザインタフェース処理部に出力する処理を実行することを特徴とする。

【００３３】

さらに、本発明の情報処理方法の一実施態様において、前記情報処理方法は、さらに、前記ユーザインタフェース処理部において、前記表示部に対する表示メッセージに対応したユーザ入力を受信し、該受信ユーザ入力情報を、前記ユーザインタフェース処理部が前記第２レジスタに格納するステップと、前記セキュリティ情報処理部が、前記第２レジスタから前記ユーザ入力情報を取得する処理を実行するステップを有することを特徴とする。

【００３４】

さらに、本発明の情報処理方法の一実施態様において、前記ユーザインタフェース処理部は、オンスクリーン・ディスプレイ（ＯＳＤ）機能実行部として構成され、前記セキュリティ情報処理ステップは、出力メッセージの選択情報を伴うメッセージ出力命令をＯＳＤ呼び出し（ＯＳＤ＿ＣＡＬＬ）に基づいて実行することを特徴とする。

【００３５】

さらに、本発明の第４の側面は、

情報処理装置において、情報記録媒体からのコンテンツ再生処理を実行する情報処理方法であり、

セキュリティ情報処理部において、コンテンツ再生シーケンスにおけるセキュリティチェック情報に対応するエラーコードを取得し、該エラーコードを、第１レジスタに書き込む処理を実行するセキュリティ情報処理ステップと、

アプリケーション実行部において、前記第１レジスタからエラーコードを取得し、取得エラーコードに対応するメッセージ情報取得を行ない、取得メッセージを表示部に出力するアプリケーション実行ステップを有し、

前記情報処理装置は、前記セキュリティ情報処理部が書き込み、前記アプリケーション実行部が読み出す第１レジスタと、前記アプリケーション実行部が書き込み、前記セキュリティ情報処理部が読み出す第２レジスタを有し、

前記セキュリティ情報処理ステップは、前記セキュリティ情報処理部が前記第１レジスタに前記エラーコードを格納するステップを含み、

前記アプリケーション実行ステップは、前記アプリケーション実行部が前記第１レジスタから前記エラーコードを取得し、取得したエラーコードに対応して設定されたメッセージを表示部に出力するステップを含むことを特徴とする情報処理方法にある。

【００３６】
さらに、本発明の情報処理方法の一実施態様において、前記情報処理方法は、さらに、前記アプリケーション実行部において、前記表示部に対する表示メッセージに対応したユーザ入力を受信し、該受信ユーザ入力情報を、前記第２レジスタに書き込む処理を実行するステップと、前記セキュリティ情報処理部において、前記第２レジスタに書き込まれたユーザ入力情報の取得処理を実行するステップと、を有することを特徴とする。
【００３７】
さらに、本発明の情報処理方法の一実施態様において、前記情報処理方法は、さらに、前記セキュリティ情報処理部において、前記アプリケーション実行部に対する実行アプリケーションの切り替え命令を出力するステップと、前記アプリケーション実行部において、前記アプリケーションの切り替え命令に基づいて、前記セキュリティ情報処理部との前記第１レジスタを介したデータ転送処理および前記表示部に対するメッセージ出力を実行するアプリケーションへの切り替えを実行するステップと、
を有することを特徴とする。
【００３８】
さらに、本発明の情報処理方法の一実施態様において、前記情報処理方法は、さらに、前記セキュリティ情報処理部、または前記アプリケーション実行部において、処理状況を示す状態値を、前記第１レジスタまたは前記第２レジスタに書き込むステップと、前記セキュリティ情報処理部、または前記アプリケーション実行部において、前記第１レジスタまたは前記第２レジスタに書き込まれた処理状況を示す状態値の読み取りを実行して処理状況の確認を行うステップと、を有することを特徴とする。
【００３９】
さらに、本発明の情報処理方法の一実施態様において、前記情報処理方法は、さらに、前記セキュリティ情報処理部、および前記アプリケーション実行部間において、相互の信頼性確認処理を、前記第１レジスタまたは前記第２レジスタを適用したデータ転送処理によって実行するステップを有することを特徴とする。
【００４４】
さらに、本発明の第５の側面は、
セキュリティ情報処理部とユーザインタフェース処理部とを有する情報処理装置の前記セキュリティ情報処理部で実行されるコンピュータ・プログラムであり、
前記セキュリティ情報処理部において、コンテンツ再生シーケンスにおけるセキュリティチェック情報に基づいて出力メッセージを決定し、出力メッセージの選択情報をユーザインタフェース処理部に出力させるセキュリティ情報処理コードを有し、
前記情報処理装置は、前記セキュリティ情報処理部が書き込み、前記ユーザインタフェース処理部が読み出す第１レジスタと、前記ユーザインタフェース処理部が書き込み、前記セキュリティ情報処理部が読み出す第２レジスタを有し、
前記出力メッセージの選択情報をユーザインタフェース処理部に出力させるセキュリティ情報処理コードは、前記セキュリティ情報処理部が前記第１レジスタに対して前記選択情報を格納するコードであり、
ユーザインタフェース処理コードが前記ユーザインタフェース処理部で実行されることで、
前記セキュリティ情報処理部が格納する選択情報を前記第１レジスタから取得し、
前記取得された選択情報に基づくメッセージ情報取得を行ない、
前記ユーザインタフェース処理部が前記選択情報を取得し、取得した選択情報に対応して設定されたメッセージを表示部に出力することを特徴とするコンピュータ・プログラムにある。
さらに、本発明の第６の側面は、
セキュリティ情報処理部とユーザインタフェース処理部とを有する情報処理装置の前記ユーザインタフェース処理部で実行されるコンピュータ・プログラムであり、
前記情報処理装置は、前記セキュリティ情報処理部が書き込み、前記ユーザインタフェ

ース処理部が読み出す第１レジスタと、前記ユーザインタフェース処理部が書き込み、前記セキュリティ情報処理部が読み出す第２レジスタを有し、
前記ユーザインタフェース処理部において、前記セキュリティ情報処理部が前記第１レジスタに格納したメッセージ選択情報を取得し、取得情報に基づく処理を実行させるユーザインタフェース処理コードを有し、
前記ユーザインタフェース処理コードは、
前記セキュリティ情報処理部がコンテンツ再生シーケンスにおけるセキュリティチェック情報に基づいて決定したメッセージ選択情報を前記第１レジスタから取得するコードと、
前記第１レジスタから取得したメッセージ選択情報に対応して設定されたメッセージを表示部に出力するコードを含むことを特徴とするコンピュータ・プログラムにある。

【００４５】

さらに、本発明の第７の側面は、
セキュリティ情報処理部とアプリケーション実行部とを有する情報処理装置の前記セキュリティ情報処理部で実行されるコンピュータ・プログラムであり、
前記セキュリティ情報処理部において、コンテンツ再生シーケンスにおけるセキュリティチェック情報に対応するエラーコードを取得し、該エラーコードをアプリケーション実行部に出力させるセキュリティ情報処理コードを有し、
前記情報処理装置は、前記セキュリティ情報処理部が書き込み、前記アプリケーション実行部が読み出す第１レジスタと、前記アプリケーション実行部が書き込み、前記セキュリティ情報処理部が読み出す第２レジスタを有し、
前記エラーコードをアプリケーション実行部に出力させるセキュリティ情報処理コードは、前記セキュリティ情報処理部が前記第１レジスタに対して前記エラーコードを格納するコードであり、
アプリケーション実行部処理コードが前記アプリケーション実行部で実行されることで、
前記セキュリティ情報処理部が前記第１レジスタに格納するエラーコードを前記第１レジスタから取得し、取得エラーコードに対応するメッセージ取得を行ない、取得したエラーコードに対応して設定されたメッセージを表示部に出力することを特徴とするコンピュータ・プログラムにある。
さらに、本発明の第８の側面は、
セキュリティ情報処理部とアプリケーション実行部とを有する情報処理装置の前記アプリケーション実行部で実行されるコンピュータ・プログラムであり、
前記情報処理装置は、前記セキュリティ情報処理部が書き込み、前記アプリケーション実行部が読み出す第１レジスタと、前記アプリケーション実行部が書き込み、前記セキュリティ情報処理部が読み出す第２レジスタを有し、
前記アプリケーション実行部において、前記セキュリティ情報処理部が前記第１レジスタに格納したエラーコードを取得し、エラーコードに基づく処理を実行させるアプリケーション実行部処理コードを有し、
前記アプリケーション実行部処理コードは、
前記セキュリティ情報処理部がコンテンツ再生シーケンスにおけるセキュリティチェック情報に基づいて決定したエラーコードを前記第１レジスタから取得する処理コードと、
前記第１レジスタから取得したエラーコードに対応して設定されたメッセージを表示部に出力する処理コードを含むことを特徴とするコンピュータ・プログラムにある。

【００４７】

なお、本発明のコンピュータ・プログラムは、例えば、様々なプログラム・コードを実行可能なコンピュータ・システムに対して、コンピュータ可読な形式で提供する記憶媒体、通信媒体、例えば、ＣＤやＦＤ、ＭＯなどの記録媒体、あるいは、ネットワークなどの通信媒体によって提供可能なコンピュータ・プログラムである。このようなプログラムをコンピュータ可読な形式で提供することにより、コンピュータ・システム上でプログラム

に応じた処理が実現される。

【００４８】

本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。なお、本明細書においてシステムとは、複数の装置の論理的集合構成であり、各構成の装置が同一筐体内にあるものには限らない。

【発明の効果】

【００４９】

本発明の一実施例の構成によれば、情報記録媒体の格納コンテンツ再生において、正当なコンテンツ利用権に基づくコンテンツ利用を許容する構成とし、さらに、セキュリティチェックに基づいて不正なコンテンツ利用であると判定された場合などにおいて、コンテンツ再生の停止された理由などメッセージ表示や、表示メッセージに対するユーザ応答の受領などを可能としたので、ユーザに対して状況を説明する処理や、ユーザからの確認や対処を受け付けることが可能となる。

【００５０】

また、本発明の一実施例構成によれば、Ｊａｖａ（登録商標）やＨＤＭＶコンテンツなどの小型のコンテンツについても、これらのコンテンツを実行するアプリケーション実行部と、セキュリティ情報処理部としてのセキュアＶＭ間でレジスタやメモリを介してデータを転送することで、コンテンツの利用制御を行なうことが可能となる。

【発明を実施するための最良の形態】

【００５１】

以下、図面を参照しながら本発明の情報処理装置、情報記録媒体、および情報処理方法、並びにコンピュータ・プログラムの詳細について説明する。なお、説明は、以下の記載項目に従って行う。

１．情報記録媒体の格納データと、ドライブおよびホストにおける処理の概要
２．コンテンツ管理ユニット（ＣＰＳユニット）について
３．コンテンツ再生処理
（３．１）コンテンツ再生処理例１
（３．２）コンテンツ再生処理例２
４．メッセージ表示およびコンテンツ利用制御処理
（４．１）ＵＩ（ユーザインタフェース）処理部を利用したメッセージ表示
（４．２）レジスタを利用したメッセージ表示およびコンテンツ利用制御
（４．２．１）レジスタを利用したＵＩ機能提供アプリケーションの実行例
（４．２．２）レジスタ利用およびタイトル切り替えによるＵＩ機能提供例
（４．２．３）レジスタ利用によるコンテンツ利用制御処理例
（４．２．４）アプリケーション実行部の使用レジスタの利用による処理例１
（４．２．５）アプリケーション実行部の使用レジスタの利用による処理例２
（４．３）共有メモリ空間を利用したメッセージ表示およびコンテンツ利用制御
（４．４）オーサリングプロセスについて
５．情報処理装置の構成

【００５２】

［１．情報記録媒体の格納データと、ドライブおよびホストにおける処理の概要］

まず、情報記録媒体の格納データと、ドライブおよびホストにおける処理の概要について説明する。図１に、コンテンツの格納された情報記録媒体１００、ドライブ１２０およびホスト１５０の構成を示す。ホスト１５０は、例えばＰＣ等の情報処理装置で実行されるデータ再生（または記録）アプリケーションであり、所定のデータ処理シーケンスに従ってＰＣ等の情報処理装置のハードウェアを利用した処理を行なう。

【００５３】

情報記録媒体１００は、例えば、Ｂｌｕ－ｒａｙディスク、ＤＶＤなどの情報記録媒体であり、正当なコンテンツ著作権、あるいは頒布権を持ついわゆるコンテンツ権利者の許

可の下にディスク製造工場において製造された正当なコンテンツを格納した情報記録媒体（ＲＯＭディスクなど）、あるいはデータ記録可能な情報記録媒体（ＲＥディスクなど）である。なお、以下の実施例では、情報記録媒体の例としてディスク型の媒体を例として説明するが、本発明は様々な態様の情報記録媒体を用いた構成において適用可能である。

【００５４】

図１に示すように、情報記録媒体１００には、暗号化処理および一部データの置き換え処理の施された暗号化コンテンツ１０１と、ブロードキャストエンクリプション方式の一態様として知られる木構造の鍵配信方式に基づいて生成される暗号鍵ブロックとしてのＭＫＢ（Media Key Block）１０２、コンテンツ復号処理に適用するタイトル鍵を暗号化したデータ（Encrypted CPS Unit Key）等から構成されるタイトル鍵ファイル１０３、コンテンツのコピー・再生制御情報としてのＣＣＩ（Copy Control Information）等を含む使用許諾情報１０４、コンテンツ中の所定領域の置き換えデータに対応する変換データを登録した変換テーブル（Ｆｉｘ－ｕｐ　Ｔａｂｌｅ）１０５、変換テーブル（Ｆｉｘ－ｕｐ　Ｔａｂｌｅ）１０５の登録データによるデータ変換処理を実行するための処理命令を含むデータ変換処理プログラム１０６、エラーメッセージなど、たとえばコンテンツ再生が停止された場合に、ディスプレイに提示するメッセージデータなどの表示データを格納したメッセージデータファイル１０７が格納される。なお、図に示すデータ例は一例であり、格納データは、ディスクの種類などによって多少異なる。以下、これらの各種情報の概要について説明する。

【００５５】

（１）暗号化コンテンツ１０１

情報記録媒体１００には、様々なコンテンツが格納される。例えば高精細動画像データであるＨＤ（High Definition）ムービーコンテンツなどの動画コンテンツのＡＶ(Audio Visual)ストリームや特定の規格で規定された形式のゲームプログラム、画像ファイル、音声データ、テキストデータなどからなるコンテンツである。これらのコンテンツは、特定のＡＶフォーマット規格データであり、特定のＡＶデータフォーマットに従って格納される。具体的には、例えばＢｌｕ－ｒａｙディスクＲＯＭ規格データとして、Ｂｌｕ－ｒａｙディスクＲＯＭ規格フォーマットに従って格納される。

【００５６】

さらに、例えばサービスデータとしてのゲームプログラムや、画像ファイル、音声データ、テキストデータなどが格納される場合もある。これらのコンテンツは、特定のＡＶデータフォーマットに従わないデータフォーマットを持つデータとして格納される場合もある。

【００５７】

コンテンツの種類としては、音楽データ、動画、静止画等の画像データ、ゲームプログラム、ＷＥＢコンテンツなど、様々なコンテンツが含まれ、これらのコンテンツには、情報記録媒体１００からのデータのみによって利用可能なコンテンツ情報と、情報記録媒体１００からのデータと、ネットワーク接続されたサーバから提供されるデータとを併せて利用可能となるコンテンツ情報など、様々な態様の情報が含まれる。情報記録媒体に格納されるコンテンツは、区分コンテンツ毎の異なる利用制御を実現するため、区分コンテンツ毎に異なる鍵（ＣＰＳユニット鍵またはユニット鍵（あるいはタイトル鍵と呼ぶ場合もある））が割り当てられ暗号化されて格納される。１つのユニット鍵を割り当てる単位をコンテンツ管理ユニット（ＣＰＳユニット）と呼ぶ。さらに、コンテンツは、構成データの一部が、正しいコンテンツデータと異なるデータによって置き換えられたブロークンデータとして設定され、復号処理のみでは正しいコンテンツ再生が実行されず、再生を行なう場合は、ブロークンデータを変換テーブルに登録されたデータに置き換える処理が必要となる。これらの処理は後段で詳細に説明する。

【００５８】

（２）ＭＫＢ

ＭＫＢ（Media Key Block）１０２は、ブロードキャストエンクリプション方式の一態

様として知られる木構造の鍵配信方式に基づいて生成される暗号鍵ブロックである。ＭＫＢ１０２は有効なライセンスを持つユーザの情報処理装置に格納されたデバイス鍵［Ｋｄ］に基づく処理（復号）によってのみ、コンテンツの復号に必要なキーであるメディア鍵［Ｋｍ］の取得を可能とした鍵情報ブロックである。これはいわゆる階層型木構造に従った情報配信方式を適用したものであり、ユーザデバイス（情報処理装置）が有効なライセンスを持つ場合にのみ、メディア鍵［Ｋｍ］の取得を可能とし、無効化（リボーク処理）されたユーザデバイスにおいては、メディア鍵［Ｋｍ］の取得が不可能となる。

【００５９】

ライセンスエンティテイとしての管理センタはＭＫＢに格納する鍵情報の暗号化に用いるデバイス鍵の変更により、特定のユーザデバイスに格納されたデバイス鍵では復号できない、すなわちコンテンツ復号に必要なメディア鍵を取得できない構成を持つＭＫＢを生成することができる。従って、任意タイミングで不正デバイスを排除（リボーク）して、有効なライセンスを持つデバイスに対してのみ復号可能な暗号化コンテンツを提供することが可能となる。コンテンツの復号処理については後述する。

【００６０】

（３）タイトル鍵ファイル

前述したように各コンテンツまたは複数コンテンツの集合は、コンテンツの利用管理のため、各々、個別の暗号鍵（タイトル鍵（ＣＰＳユニット鍵））を適用した暗号化がなされて情報記録媒体１００に格納される。すなわち、コンテンツを構成するＡＶ(Audio Visual)ストリーム、音楽データ、動画、静止画等の画像データ、ゲームプログラム、ＷＥＢコンテンツなどは、コンテンツ利用の管理単位としてのユニットに区分され、区分されたユニット毎に異なるタイトル鍵を生成して、復号処理を行なうことが必要となる。このタイトル鍵を生成するための情報がタイトル鍵データであり、例えばメディア鍵等によって生成された鍵で暗号化タイトル鍵を復号することによってタイトル鍵を得る。タイトル鍵データを適用した所定の暗号鍵生成シーケンスに従って、各ユニット対応のタイトル鍵が生成され、コンテンツの復号が実行される。

【００６１】

（４）使用許諾情報

使用許諾情報には、例えばコピー・再生制御情報（ＣＣＩ）が含まれる。すなわち、情報記録媒体１００に格納された暗号化コンテンツ１０１に対応する利用制御のためのコピー制限情報や、再生制限情報である。このコピー・再生制御情報（ＣＣＩ）は、コンテンツ管理ユニットとして設定されるＣＰＳユニット個別の情報として設定される場合や、複数のＣＰＳユニットに対応して設定される場合など、様々な設定が可能である。

【００６２】

（５）変換テーブル

前述したように、情報記録媒体１００に格納された暗号化コンテンツ１０１は、所定の暗号化が施されているとともに、コンテンツ構成データの一部が、正しいデータと異なるブロークンデータによって構成されている。コンテンツ再生に際しては、このブロークンデータを正しいコンテンツデータである変換データに置き換えるデータ上書き処理が必要となる。この変換データを登録したテーブルが変換テーブル（Ｆｉｘ－ｕｐ　Ｔａｂｌｅ）１０５である。ブロークンデータはコンテンツ中に散在して多数設定され、コンテンツ再生に際しては、これらの複数のブロークンデータを変換テーブルに登録された変換データに置き換える（上書き）する処理が必要となる。この変換データを適用することにより、例えば、暗号鍵が漏洩しコンテンツの復号が不正に行なわれた場合であっても、コンテンツの復号のみでは、置き換えデータの存在によって正しいコンテンツの再生が不可能となり、不正なコンテンツ利用を防止することができる。

【００６３】

なお、変換テーブル１０５には、通常の変換データに加え、コンテンツ再生装置またはコンテンツ再生アプリケーションを識別可能とした識別情報の構成ビットを解析可能としたデータを含む変換データが含まれる。具体的には、例えば、プレーヤ（ホストアプリケ

ーションを実行する装置）の識別データとしてのプレーヤＩＤあるいはプレーヤＩＤに基づいて生成された識別情報が記録された「識別マークを含む変換データ」が含まれる。識別マークを含む変換データは、コンテンツの再生に影響を与えないレベルで、正しいコンテンツデータのビット値をわずかに変更したデータである。これらの変換データを利用した処理についての詳細は、後段で説明する。

【００６４】

なお、図１には、変換テーブル１０５を独立したデータファイルとして設定した例を示しているが、変換テーブルを独立ファイルとせずに、暗号化コンテンツ１０１の構成パケット中に散在させて含ませる構成としてもよい。これらの構成および処理については後段で説明する。

【００６５】

（６）データ変換処理プログラム

データ変換処理プログラム１０６は、変換テーブル（Ｆｉｘ－ｕｐ　Ｔａｂｌｅ）１０５の登録データによるデータ変換処理を実行するための処理命令を含むプログラムであり、コンテンツ再生を実行するホストによって利用される。図１におけるホスト１００のデータ変換処理部１５４において実行される。

【００６６】

ホストでは、データ変換処理を実行するバーチャルマシン（ＶＭ）を設定し、バーチャルマシン（ＶＭ）において、情報記録媒体１００から読み出したデータ変換処理プログラム１０６を実行して、変換テーブル（Ｆｉｘ－ｕｐ　Ｔａｂｌｅ）１０５の登録データを適用して、復号コンテンツに対して、その一部構成データのデータ変換処理を実行する。これらの処理の詳細については後述する。

【００６７】

（７）メッセージデータファイル

メッセージデータファイルは、エラーメッセージなど、たとえばコンテンツ再生が停止された場合に、ディスプレイに提示するメッセージデータなどの表示データを格納したファイルであり、エラー内容や、言語に応じた複数のデータを有している。たとえばセキュリティ上の問題によって、コンテンツ再生が停止された場合などにおいて、メッセージデータファイルから適切なメッセージデータを選択して、ディスプレイに定時する。ユーザはディスプレイに表示された情報に基づいて、エラー状況や対処情報などを確認することができる。なお、これらの処理の詳細については、後段の［４．メッセージ表示およびコンテンツ利用制御処理］の項目において説明する。

【００６８】

次に、ホスト１５０とドライブ１２０の構成、処理の概要について、図１を参照して説明する。情報記録媒体１００に格納されたコンテンツの再生処理は、ドライブ１２０を介してホスト１５０にデータが転送されて実行される。コンテンツの利用に先立ち、ドライブ１２０と、ホスト１５０間では相互認証処理が実行され、この認証処理の成立によって双方の正当性が確認された後、ドライブからホストに暗号化コンテンツが転送され、ホスト側でコンテンツの復号処理が行なわれ、さらに上述の変換テーブルによるデータ変換処理が実行されてコンテンツ再生が行なわれる。

【００６９】

ホスト１５０と、ドライブ１２０間において実行する相互認証においては、各機器またはアプリケーションが不正な機器またはアプリケーションとして登録されていないかを示す管理センタの発行したリボケーション（無効化）リストを参照して、正当性を判定する処理を実行する。

【００７０】

ドライブ１２０は、ホストの証明書（公開鍵証明書）のリボーク（無効化）情報を格納したホストＣＲＬ（Certificate Revocation List）を格納するためのメモリ１２２を有する。一方、ホスト１５０は、ドライブの証明書（公開鍵証明書）のリボーク（無効化）情報を格納したドライブＣＲＬ（Certificate Revocation List）を格納するためのメモ

リ１５２を有する。メモリは不揮発性メモリ（ＮＶＲＡＭ）であり、例えば、情報記録媒体１００から読み出されるＣＲＬがより新しいバージョンである場合には、それぞれのデータ処理部１２１，１５１は、メモリ１２２．１５２に新しいバージョンのホストＣＲＬまたはドライブＣＲＬを格納する更新処理を行なう。

【００７１】

ホストＣＲＬ、ドライブＣＲＬ等のＣＲＬは管理センタが逐次更新する。すなわち新たな不正機器が発覚した場合、その不正機器に対して発行された証明書のＩＤまたは機器ＩＤなどを新規エントリとし追加した更新ＣＲＬを発行する。各ＣＲＬにはバージョン番号が付与されており、新旧比較が可能な構成となっている。例えばドライブが装着した情報記録媒体から読み出されたＣＲＬが、ドライブ内のメモリ１２２に格納されたＣＲＬより新しい場合、ドライブは、ＣＲＬの更新処理を実行する。ホスト１５０も同様に、ドライブＣＲＬの更新を実行する。

【００７２】

ドライブ１２０のデータ処理部１２１は、このＣＲＬの更新処理の他、コンテンツ利用に際して実行されるホストとの認証処理、さらに、情報記録媒体からのデータ読み出し、ホストへのデータ転送処理などを実行する。

【００７３】

ホスト１５０は、前述したように、例えばＰＣ等の情報処理装置で実行されるデータ再生（または記録）アプリケーションであり、所定のデータ処理シーケンスに従ってＰＣ等の情報処理装置のハードウェアを利用した処理を行なう。

【００７４】

ホスト１５０は、ドライブ１２０との相互認証処理や、データ転送制御などを実行するデータ処理部１５１、暗号化コンテンツの復号処理を実行する復号処理部１５３、前述の変換テーブル１０５の登録データに基づくデータ変換処理を実行するデータ変換処理部１５４、デコード（例えばＭＰＥＧデコード）処理を実行するデコード処理部１５５を有する。

【００７５】

データ処理部１５１は、ホスト－ドライブ間の認証処理を実行し、認証処理においては、不揮発性メモリ（ＮＶＲＡＭ）としてのメモリａ１５２に格納されたドライブＣＲＬを参照して、ドライブがリボークされたドライブでないことを確認する。ホストも、また、メモリａ１５２に新しいバージョンのドライブＣＲＬを格納する更新処理を行なう。

【００７６】

復号処理部１５３では、メモリｂ１５６に格納された各種情報、および、情報記録媒体１００からの読み取りデータを適用して、コンテンツの復号に適用する鍵を生成し、暗号化コンテンツ１０１の復号処理を実行する。データ変換処理部１５４は、情報記録媒体１００から取得されるデータ変換処理プログラムに従って、情報記録媒体１００から取得される変換テーブルに登録された変換データを適用してコンテンツの構成データの置き換え処理（上書き）を実行する。デコード処理部１５５は、デコード（例えばＭＰＥＧデコード）処理を実行する。

【００７７】

情報処理装置１５０のメモリｂ１５６には、デバイス鍵：Ｋｄや、相互認証処理に適用する鍵情報や復号に適用する鍵情報などが格納される。なお、コンテンツの復号処理の詳細については後述する。デバイス鍵：Ｋｄは、先に説明したＭＫＢの処理に適用する鍵である。ＭＫＢは有効なライセンスを持つユーザの情報処理装置に格納されたデバイス鍵［Ｋｄ］に基づく処理（復号）によってのみ、コンテンツの復号に必要なキーであるメディア鍵［Ｋｍ］の取得を可能とした鍵情報ブロックであり、暗号化コンテンツの復号に際して、情報処理装置１５０は、メモリｂ１５６に格納されたデバイス鍵：Ｋｄを適用してＭＫＢの処理を実行することになる。なお、コンテンツの復号処理の詳細については後述する。

【００７８】

［２．コンテンツ管理ユニット（ＣＰＳユニット）について］

前述したように、情報記録媒体に格納されるコンテンツは、ユニット毎の異なる利用制御を実現するため、ユニット毎に異なる鍵が割り当てられ暗号化処理がなされて格納される。すなわち、コンテンツはコンテンツ管理ユニット（ＣＰＳユニット）に区分されて、個別の暗号化処理がなされ、個別の利用管理がなされる。

【００７９】

コンテンツ利用に際しては、まず、各ユニットに割り当てられたＣＰＳユニット鍵（タイトル鍵とも呼ばれる）を取得することが必要であり、さらに、その他の必要な鍵、鍵生成情報等を適用して予め定められた復号処理シーケンスに基づくデータ処理を実行して再生を行う。コンテンツ管理ユニット（ＣＰＳユニット）の設定態様について、図２を参照して説明する。

【００８０】

図２に示すように、コンテンツは、（Ａ）インデックス２１０、（Ｂ）ムービーオブジェクト２２０、（Ｃ）プレイリスト２３０、（Ｄ）クリップ２４０の階層構成を有する。再生アプリケーションによってアクセスされるタイトルなどのインデックスを指定すると、例えばタイトルに関連付けられた再生プログラムが指定され、指定された再生プログラムのプログラム情報に従ってコンテンツの再生順等を規定したプレイリストが選択される。

【００８１】

プレイリストには、再生対象データ情報としてのプレイアイテムが含まれる。プレイリストに含まれるプレイアイテムによって規定される再生区間としてのクリップ情報によって、コンテンツ実データとしてのＡＶストリームあるいはコマンドが選択的に読み出されて、ＡＶストリームの再生、コマンドの実行処理が行われる。なお、プレイリスト、プレイアイテムは多数、存在し、それぞれに識別情報としてのプレイリストＩＤ、プレイアイテムＩＤが対応付けられている。

【００８２】

図２には、２つのＣＰＳユニットを示している。これらは、情報記録媒体に格納されたコンテンツの一部を構成している。ＣＰＳユニット１，２７１、ＣＰＳユニット２，２７２の各々は、インデックスとしてのタイトルと、再生プログラムファイルとしてのムービーオブジェクトと、プレイリストと、コンテンツ実データとしてのＡＶストリームファイルを含むクリップを含むユニットとして設定されたＣＰＳユニットである。

【００８３】

コンテンツ管理ユニット（ＣＰＳユニット）１，２７１には、タイトル１，２１１とタイトル２，２１２、再生プログラム２２１，２２２、プレイリスト２３１，２３２、クリップ２４１、クリップ２４２が含まれ、これらの２つのクリップ２４１，２４２に含まれるコンテンツの実データであるＡＶストリームデータファイル２６１，２６２が、少なくとも暗号化対象データであり、原則的にコンテンツ管理ユニット（ＣＰＳユニット）１，２７１に対応付けて設定される暗号鍵であるタイトル鍵（Ｋｔ１）（ＣＰＳユニット鍵とも呼ばれる）を適用して暗号化されたデータとして設定される。

【００８４】

コンテンツ管理ユニット（ＣＰＳユニット）２，２７２には、インデックスとしてアプリケーション１，２１３、再生プログラム２２４、プレイリスト２３３、クリップ２４３が含まれ、クリップ２４３に含まれるコンテンツの実データであるＡＶストリームデータファイル２６３がコンテンツ管理ユニット（ＣＰＳユニット）２，２７２に対応付けて設定される暗号鍵である暗号鍵であるタイトル鍵（Ｋｔ２）適用して暗号化される。

【００８５】

例えば、ユーザがコンテンツ管理ユニット１，２７１に対応するアプリケーションファイルまたはコンテンツ再生処理を実行するためには、コンテンツ管理ユニット（ＣＰＳユニット）１，２７１に対応付けて設定された暗号鍵としてのタイトル鍵：Ｋｔ１を取得して復号処理を実行することが必要となる。コンテンツ管理ユニット２，２７２に対応する

アプリケーションファイルまたはコンテンツ再生処理を実行するためには、コンテンツ管理ユニット（ＣＰＳユニット）２，２７２に対応付けて設定された暗号鍵としてのタイトル鍵：Ｋｔ２を取得して復号処理を実行することが必要となる。

【００８６】

ＣＰＳユニットの設定構成、およびタイトル鍵の対応例を図３に示す。図３には、情報記録媒体に格納される暗号化コンテンツの利用管理単位としてのＣＰＳユニット設定単位と、各ＣＰＳユニットに適用するタイトル鍵（ＣＰＳユニット鍵）の対応を示している。なお、予め後発データ用のＣＰＳユニットおよびタイトル鍵を格納して設定しておくことも可能である。例えばデータ部２８１が後発データ用のエントリである。

【００８７】

ＣＰＳユニット設定単位は、コンテンツのタイトル、アプリケーション、データグループなど、様々であり、ＣＰＳユニット管理テーブルには、それぞれのＣＰＳユニットに対応する識別子としてのＣＰＳユニットＩＤが設定される。

【００８８】

図３において、例えばタイトル１はＣＰＳユニット１であり、ＣＰＳユニット１に属する暗号化コンテンツの復号に際しては、タイトル鍵Ｋｔ１を生成し、生成したタイトル鍵Ｋｔ１に基づく復号処理を行なうことが必用となる。

【００８９】

このように、情報記録媒体１００に格納されるコンテンツは、ユニット毎の異なる利用制御を実現するため、ユニット毎に異なる鍵が割り当てられ暗号化処理がなされて格納される。各コンテンツ管理ユニット（ＣＰＳユニット）に対する個別の利用管理のために、各コンテンツ管理ユニット（ＣＰＳユニット）に対する使用許諾情報（ＵＲ：Ｕｓａｇｅ Ｒｕｌｅ）が設定されている。使用許諾情報は、前述したように、コンテンツに対する例えばコピー・再生制御情報（ＣＣＩ）を含む情報であり、各コンテンツ管理ユニット（ＣＰＳユニット）に含まれる暗号化コンテンツのコピー制限情報や、再生制限情報である。

【００９０】

なお、タイトル鍵の生成には、情報記録媒体に格納された様々な情報を適用したデータ処理が必要となる。これらの処理の具体例についは、後段で詳細に説明する。

【００９１】

次に、図４を参照して、図２に示す階層構造を持つコンテンツに対応するディレクトリ構成について説明する。

（Ａ）図２におけるインデックス２１０は、図４に示すディレクトリ中のindex.bdmvファイル

（Ｂ）図２におけるムービーオブジェクト２２０は図４に示すディレクトリ中のMovieObject.bdmvファイル

（Ｃ）図２におけるプレイリスト２３０は図４に示すディレクトリ中のPLAYLISTディレクトリ下のファイル、

（Ｄ）図２におけるクリップ２４０は図４に示すディレクトリ中のCLIPINFディレクトリ下のファイルとSTREAMディレクトリ下のファイルで同じファイル番号持つものの対に対応している。

【００９２】

情報記録媒体に格納されるコンテンツは、前述したように、コンテンツの構成データの一部が、正しいコンテンツデータと異なるデータによって置き換えられたブロークンデータとして設定され、復号処理のみでは正しいコンテンツ再生が実行されず、再生を行なう場合は、ブロークンデータを変換テーブルに登録されたデータに置き換える処理が必要となる。この置き換え処理には、情報記録媒体に格納されたデータ変換処理プログラム１０６を適用して、変換テーブル（Ｆｉｘ－ｕｐ Ｔａｂｌｅ）１０５の登録データによるデータ変換処理を実行する。

【００９３】

前述したように、変換テーブル１０５、データ変換処理プログラム１０６を情報記録媒体に記録されている。図４に示すディレクトリ構成を持つコンテンツに対応する変換テーブルと、データ変換処理プログラムのディレクトリ構成を図５に示す。図５は、図４のディレクトリ構造を持つＡＶコンテンツに対して作成されるデータ変換処理プログラム、および変換テーブルのディレクトリ構成である。

図５に示す［ContentCode.svm］がデータ変換処理プログラムであり、

図５に示す［FixUpXXXXX.tbl］はクリップ１つごとに定義される変換テーブルである。（XXXXXはクリップ情報ファイルのファイル番号と一致している）

【００９４】

［３．コンテンツ再生処理］

以下、ドライブとホスト間の相互認証処理を実行し、認証の成立を条件として、ドライブに装着した情報記録媒体に格納されたコンテンツをドライブからホストに転送してコンテンツ再生処理を実行する場合の複数の処理例について説明する。

【００９５】

（３．１）コンテンツ再生処理例１

まずコンテンツ再生処理例１について、図６を参照して説明する。図６には、左から暗号化コンテンツの格納された情報記録媒体３１０、情報記録媒体３１０をセットし、データの読み取りを実行するドライブ３３０、ドライブとデータ通信可能に接続され、情報記録媒体３１０に格納されたコンテンツをドライブ３３０を介して取得して再生処理を実行する再生アプリケーションを実行するホスト３５０を示している。ホスト３５０は、例えばＰＣ等の情報処理装置において実行される。

【００９６】

情報記録媒体３１０には、ＭＫＢ（Media Key Block）３１１、タイトル鍵ファイル３１２、暗号化コンテンツ３１３、変換テーブル３１４、データ変換処理プログラム３１５が格納されている。ホスト３５０は、ＭＫＢの処理に適用するデバイス鍵３５１を保持している。

【００９７】

図６に示すホスト３５０がドライブ３３０を介して情報記録媒体３１０の格納コンテンツを取得して再生する処理シーケンスについて説明する。まず、情報記録媒体３１０の格納コンテンツの読み出しに先立ち、ホスト３５０とドライブ３３０は、ステップＳ１０１において、相互認証を実行する。この相互認証は、ホストおよびドライブがそれぞれ正当な機器またはアプリケーションソフトであるかを確認する処理である。この相互認証処理シーケンスとしては、様々な処理が適用可能である。その一例を図７を参照して説明する。

【００９８】

図７は、公開鍵暗号方式に従った相互認証シーケンスの１例である。まず、ステップＳ１２１において、ドライブ３３０は、自己のメモリ（ＮＶＲＡＭ）に格納されたドライブ公開鍵証明書と、任意に生成した乱数をホストに送信する。ステップＳ１２２において、ホスト３５０も、自己のメモリ（ＮＶＲＡＭ）に格納されたホスト公開鍵証明書と、任意に生成した乱数をドライブに送信する。

【００９９】

ステップＳ１２３において、ドライブ３３０は、ホストから受信したホスト公開鍵証明書の正当性と、ホストのリボーク状況をホスト証明書リボケーションリスト（ホストＣＲＬ:Certificate Revocation list）に基づいて検証する。ステップＳ１２３において、ドライブ３３０は、まず、ホスト公開鍵証明書に設定された署名検証を実行する。図７に示すＥＣＤＳＡ＿Ｖは、楕円曲線暗号に基づく署名検証（Verification）の実行を示している。この署名検証は、鍵管理エンティティの秘密鍵に対応する公開鍵を適用して実行する。ドライブは、署名検証用の鍵管理エンティティの公開鍵をメモリ（ＮＶＲＡＭ）に保持しており、これを適用して署名検証を実行する。署名検証によって、ホスト公開鍵証明書が改ざんされていないものであることを確認する。署名検証によって、ホスト公開鍵証明

書が改ざんされていることが判明した場合は処理を中止する。

【０１００】

さらに、ドライブ３３０は、改ざんのないことが明確になったホスト公開鍵証明書に基づいて、この証明書がリボーク（無効化）されているものでないことを、ホストＣＲＬを参照して確認する。ホストＣＲＬは、ホストに対して発行済みの公開鍵証明書について、無効化された証明書のＩＤをリスト化したものである。ホストＣＲＬはドライブ内のメモリまたは情報記録媒体から取得する。

【０１０１】

ドライブ３３０は、改ざんのないことが明確になったホスト公開鍵証明書からＩＤを取得し、このＩＤがホストＣＲＬに登録されているＩＤと一致するか否かを判定する。一致するＩＤがホストＣＲＬに存在する場合、そのホストは、リボーク（無効化）されたホストであると判定し、以降の処理を中止する。ホスト公開鍵証明書から取得したＩＤが、ホストＣＲＬに記録されていない場合は、正当なリボークのなされていないホストであると判定して、処理を続ける。

【０１０２】

一方、ホスト３５０においても、ステップＳ１２４において、ドライブ３３０から受領したドライブ公開鍵証明書に基づいて、ドライブ公開鍵証明書の正当性の確認（改ざん検証）と、ドライブＣＲＬを適用したドライブのリボークの有無判定を実行する。ドライブの公開鍵証明書が正当なものであり、リボークされていないことが確認された場合にのみ、処理を継続する。ドライブＣＲＬはホスト内のメモリまたは情報記録媒体から取得する。

【０１０３】

次に、ドライブ３３０、ホスト３５０は、それぞれの認証結果をドライブレスポンス（Ｓ１２５）、ホストレスポンス（Ｓ１２６）として通知する。この認証結果の通知に際して、双方では、楕円曲線暗号を適用した値としてのＥＣＤＨ（Elliptic Curve Diffie Hellman）の値を生成して、双方に通知しあう。

【０１０４】

ドライブ３３０は、ホスト３５０からのドライブ認証結果とＥＣＤＨの値を受信すると、ステップＳ１２７において、ホストのレスポンスを検証し、ドライブ認証の成立を確認して、受信したＥＣＤＨの値を適用して共通鍵としてのセッション鍵を生成する。ホスト３５０においても、ドライブ３３０からのホスト認証結果とＥＣＤＨの値を受信すると、ステップＳ１２８において、ドライブレスポンスを検証し、ホスト認証の成立を確認して、ＥＣＤＨの値に基づいて共通鍵としてのセッション鍵を生成する。

【０１０５】

このような相互認証処理によって、ドライブ３３０とホスト３５０は共通鍵としてのセッション鍵を共有する。

【０１０６】

図６に戻り、コンテンツ利用処理のシーケンスについての説明を続ける。ステップＳ１０１において、ホストドライブ間の相互認証が実行され、セッション鍵（Ｋｓ）を共有した後、ホスト３５０は、ステップＳ１０２において、情報記録媒体３１０に記録されたＭＫＢ３１１を、ドライブを介して取得して、メモリに格納されたデバイス鍵３５１を適用したＭＫＢ３１１の処理を実行して、ＭＫＢからメディア鍵（Ｋｍ）を取得する。

【０１０７】

前述したように、ＭＫＢ（Media Key Block）３１１は、ブロードキャストエンクリプション方式の一態様として知られる木構造の鍵配信方式に基づいて生成される暗号鍵ブロックであり、有効なライセンスを持つ装置に格納されたデバイス鍵（Ｋｄ）に基づく処理（復号）によってのみ、コンテンツの復号に必要なキーであるメディア鍵（Ｋｍ）の取得を可能とした鍵情報ブロックである。

【０１０８】

次に、ステップＳ１０３において、ステップＳ１０２におけるＭＫＢ処理で取得したメ

ディア鍵（Ｋｍ）を適用して、情報記録媒体３１０から読み取ったタイトル鍵ファイルの復号を実行して、タイトル鍵（Ｋｔ）を取得する。情報記録媒体３１０に格納されるタイトル鍵ファイルはメディア鍵によって暗号化されたデータを含むファイルであり、メディア鍵を適用した処理によってコンテンツ復号に適用するタイトル鍵（Ｋｔ）を取得することができる。なお、ステップＳ１０３の復号処理は、例えばＡＥＳ暗号アルゴリズムが適用される。

【０１０９】

次に、ホスト３５０は、ドライブ３３０を介して情報記録媒体３１０に格納された暗号化コンテンツ３１３を読み出して、トラックバッファ３５２に読み出しコンテンツを格納し、このバッファ格納コンテンツについて、ステップＳ１０４において、タイトル鍵（Ｋｔ）を適用した復号処理を実行し、復号コンテンツを取得する。

【０１１０】

復号コンテンツは、平文ＴＳバッファ３５３に格納する。（Ｐｌａｉｎ　ＴＳ）は復号された平文トランスポートストリームを意味する。ここで、平文ＴＳバッファ３５３に格納される復号コンテンツは、前述したブロークンデータを含むコンテンツであり、このままでは再生できず、所定のデータ変換（上書きによるデータ置き換え）を行なう必要がある。

【０１１１】

このデータ変換処理を示すのが、図６のブロック３７１である。図６のブロック３７１は図１に示したホスト１５０のデータ変換処理部１５４の処理に相当する。このデータ変換処理の概要について、図８を参照して説明する。

【０１１２】

図６に示す暗号化コンテンツ３１３は、情報記録媒体に格納された暗号化コンテンツであり、この暗号化コンテンツが、一旦、ホスト側のトラックバッファ３５２に格納される。図８（１）に示すトラックバッファ格納データ４０１である。

【０１１３】

ホスト側の復号処理によって、トラックバッファ格納データ４０１としての暗号化コンテンツの復号が実行されて、復号結果データが平文ＴＳバッファ３５３に格納される。図８（２）に示す復号結果データ４０２である。

【０１１４】

復号結果データ４０２には、正常なコンテンツ構成データではない、ブロークンデータ４０３が含まれる。ホストのデータ変換処理部は、このブロークンデータ４０３を、図６に示す情報記録媒体３１０に記録された変換テーブル３１４から取得される正しいコンテンツ構成データとしての変換データ４０４に置き換える処理を実行する。この置き換え処理は、例えば平文ＴＳバッファ３５３に書き込み済みのデータに対する一部データの再書き込み（上書き）処理として実行される。

【０１１５】

さらに、ホストの実行するデータ変換処理は、ブロークンデータを正常なコンテンツデータである変換データに置き換える処理のみならず、図８に示すように、識別マークを含む変換データ４０５によって、復号結果データ４０２の一部構成データを置き換える処理を実行する。

【０１１６】

識別マークとは、コンテンツ再生装置またはコンテンツ再生アプリケーションを識別可能とした識別情報の構成ビットを解析可能としたデータである。具体的には例えば、ホストアプリケーションを実行するプレーヤとしての情報処理装置の識別情報（プレーヤＩＤ）の構成データまたは、プレーヤＩＤに基づいて生成される識別マークである。識別マークを含む変換データは、コンテンツの再生に影響を与えないレベルで、正しいコンテンツデータのビット値をわずかに変更したデータである。

【０１１７】

識別マークを含む変換データ４０５は、コンテンツ中に多数設定され、これら複数の識

別マークを含む変換データ４０５を集積して解析することで、例えばプレーヤＩＤが判別される。識別マークを含む変換データ４０５は、コンテンツとして通常再生可能なレベルで正常コンテンツデータの構成ビットを変更したデータであり、ＭＰＥＧビットストリーム解析によりビット（識別マーク構成ビット）判別が可能なデータである。

【０１１８】

情報記録媒体に格納される変換テーブルには、図８に示す変換データ４０４、識別マークを含む変換データ４０５が多数登録されており、さらに、これらの書き込み位置情報についても登録されている。この変換テーブル格納情報に基づくデータ変換処理を実行することで、平文ＴＳバッファ３５３に格納されたデータは、図８（３）に示す変換処理済みデータ４０６に置き換えられることになる。

【０１１９】

図６に戻り、点線ブロック３７１内の処理、すなわちホスト側のデータ変換処理について説明する。データ変換処理は、例えば、ホスト内にバーチャルマシンとして設定されるセキュアＶＭ３５６によって実行される。バーチャルマシン（ＶＭ）は中間言語を直接解釈して実行する仮想コンピュータであり、プラットホームに依存しない中間言語での命令コード情報を解釈して実行する。

【０１２０】

セキュアＶＭ３５６は、命令コード情報を含むデータ変換処理プログラム３１５を情報記録媒体３１０から読み出して処理を実行する。セキュアＶＭ３５６は、イベントハンドラ３５４による処理制御がなされ、また、ホストアプリケーションを実行しているプレーヤ（情報処理装置）のＩＤ情報などをプレーヤ情報３５５として入力して、情報記録媒体３１０から取得したデータ変換処理プログラム３１５を実行する。イベントハンドラ３５４は、処理監視を実行する。セキュアＶＭ３５６によって実行される処理が正しく行なわれているか否かのエミュレータチェックや、その他のホストアプリケーションや、ホストアプリケーション実行機器としてのプレーヤ（情報処理装置）の処理、状態を監視し、処理エラー、不正処理などが検出された場合には、セキュアＶＭ３５６によるデータ変換処理を中止させる。

【０１２１】

セキュアＶＭ３５６は、情報記録媒体３１０から読み出した変換テーブルを適用して、平文ＴＳバッファ３５３に格納されたデータの変換処理を実行する。すなわち図６に示すステップＳ１０５のデータ変換処理であり、図８に示す復号結果データ４０２に対して、ブロークンデータ４０３を正当なコンテンツ構成データである変換データ４０４に置き換え、さらに、識別マークを含む変換データ４０５をコンテンツの一部データと入れ替えるデータ上書き処理を実行して、平文ＴＳバッファ３５３の格納データを変換処理済みデータ４０６に変更する。

【０１２２】

その後、変換済みのＴＳ（トランスポートストリーム）は、ネットワークなどを介して外部出力され、外部の再生機器において再生される。あるいは、ステップＳ１０６において、デマルチプレクサによる処理によって、トランスポートストリーム（ＴＳ）からエレメンタリストリーム（ＥＳ）への変換が実行され、さらに、デコード処理（ステップＳ１０７）が行なわれた後、ディスプレイおよびスピーカを介して再生される。

【０１２３】

情報記録媒体に記録されるデータ変換テーブルのデータ構成について、図９を参照して説明する。情報記録媒体に記録されるデータ変換テーブルは、例えば図９に示すデータ構成を持つ。すなわち、

Number of Fix-Up Entry：変換データエントリ数（Number of Fix-Up Entry）

Fix-Up Entry Length：１変換データエントリのバイト数（Byte Length of one Fix-Up Entry()=(N+6)）

SPN（ソースパケットナンバー）：変換データ書き込みパケットのＡＶストリームファイルの開始位置からのパケットナンバー（Absolute Transformed Packet Number from th

e beginning of AV Stream File）
Byte Offset：ＳＰＮで指定されたパケット中の変換データ書き込み開始位置を示すバイトオフセット（Start byte position of transformed data in the packet）
player_id_bit_position：識別マーク（プレーヤＩＤなど）のビット位置（Indicate bit position of Player ID for forensic）
Fix-Up Data：変換上書きデータ（Value to be overwritten (N byte is transformed in one TS Packet)）
これらのデータを持つ。

【０１２４】

１つのコンテンツ中には、多数のブロークンデータが散在して配置されており、このブロークンデータの位置に変換テーブルに記録された変換データを上書きする。また、プレーヤＩＤなどの識別マークを持つ変換データについても、１つのコンテンツデータ中に多数の書き込み位置が設定される。変換テーブルは、これらの
（ａ）変換データ
（ｂ）識別マーク入り変換データ
の実体データとしての「変換上書きデータ」と、
これらのデータの書き込み位置の指定情報を記録したテーブルとして設定される。

【０１２５】

なお、どの程度の頻度で、変換データ（識別マーク入り変換データも含む）の置き換え領域を設定するか、また変換データのサイズについては、様々な設定が可能であるが、各設定により変換テーブルサイズは異なるサイズとなる。例えばＭＰＥＧコンテンツを構成する１ＧＯＰ(Group Of Pictures)あたり、２つの変換データまたは識別マーク入り変換データを設定する構成においては、変換データ（識別マーク入り変換データも含む）が８バイトである場合、約４００ＫＢ程度のテーブル、１６バイトである場合、約６００ＫＢ程度のテーブルサイズとなる。

【０１２６】

また、ＭＰＥＧコンテンツを構成する１ＧＯＰ(Group Of Pictures)あたり、５つの変換データまたは識別マーク入り変換データを設定する構成においては、変換データ（識別マーク入り変換データも含む）が８バイトである場合、約１ＭＢ程度のテーブル、１６バイトである場合、約１，５ＭＢ程度のテーブルサイズとなる。

【０１２７】

ホスト３５０のセキュアＶＭは、情報記録媒体３１０に記録された変換テーブル３１４に従って、
（ａ）変換データ
（ｂ）識別マーク入り変換データ
を変換テーブルの指定位置に書き込む処理を実行する。データ書き込みは、平文ＴＳバッファ２５３に格納されたデータに対する変換データ、または識別マーク入り変換データの上書き処理として実行され、この処理の結果、平文ＴＳバッファ２５３に格納されたデータは、先に説明した図８（３）のデータに置き換えられることになる。

【０１２８】

ホストを実装しているプレーヤ（ＰＣなどの情報処理装置）からのコンテンツの外部出力、あるいはコンテンツ再生は、この図８（３）に示す変換処理済みデータに基づく処理として実行される。

【０１２９】

変換データは正しいコンテンツ構成データであり、また識別マーク入り変換データも、正しいコンテンツの再生に適用されるデータであるので、これらのデータに基づくデコード再生によって正しいコンテンツ再生が可能となる。また、このコンテンツが、例えば不正にコピーされ、コピーデータが多数外部流出した場合には、識別マーク入り変換データを解析することで、プレーヤＩＤを取得することが可能であり、不正コンテンツデータの流出源を特定することが可能となる。

【０１３０】
（３．２）コンテンツ再生処理例２
次に、コンテンツ再生処理例２について、図１０を参照して説明する。図１０は、左から暗号化コンテンツの格納された情報記録媒体３１０、情報記録媒体３１０をセットし、データの読み取りを実行するドライブ３３０、ドライブとデータ通信可能に接続され、情報記録媒体３１０に格納されたコンテンツをドライブ３３０を介して取得して再生処理を実行する再生アプリケーションを実行するホスト３５０を示している。ホスト３５０は、例えばＰＣ等の情報処理装置において実行される。
【０１３１】
図１０には、情報記録媒体３１０に記録されているＭＫＢ（Media Key Block）と、タイトル鍵ファイルは省略してある。ホスト３５０は、ＭＫＢの処理に適用するデバイス鍵を保持し、情報記録媒体３１０に記録されているＭＫＢ（Media Key Block）と、タイトル鍵ファイルを適用して、図６を参照して説明したと全く同様の処理を実行してタイトル鍵（Ｋｔ）を算出する。これらの処理についても、図１０においては省略してある。情報記録媒体には、さらに、暗号化コンテンツ３１３、変換テーブル３１４、データ変換処理プログラム３１５が格納されている。
【０１３２】
図１０に示すコンテンツ再生処理例２では、点線枠で示すブロック３８１の処理をリアルタイム処理として実行し、ブロック３８２の処理を、コンテンツ再生あるいは出力前の一括処理として実行する点が特徴である。すなわち、セキュアＶＭ３５６は、コンテンツの再生やコンテンツの外部出力の開始前などに、命令コード情報を含むデータ変換処理プログラム３１５を情報記録媒体３１０から読み出し、イベントハンドラ３５４の制御、プレーヤ情報３５５の入力に基づいて、情報記録媒体３１０から読み出した変換テーブル３１４の復号処理などを実行する。
【０１３３】
情報記録媒体３１０に記録された変換テーブル３１４は、例えばＡＥＳ暗号や、排他論理和演算などの演算によって難読化処理が施されており、セキュアＶＭ３５６は、データ変換処理プログラム３１５に従って、復号処理、あるいは所定の演算処理を実行して、平文データとしての変換テーブルを取得する。ここまでの処理は、コンテンツの再生やコンテンツの外部出力の開始前などに一括して実行する。
【０１３４】
その後の処理は、コンテンツ再生やコンテンツ外部出力処理に並行して実行するリアルタイム処理として実行する。すなわち、ステップＳ２０１におけるコンテンツ復号処理、ステップＳ２０２におけるデータ変換処理、すなわち、情報記録媒体３１０に記録された変換テーブル３１４に登録された変換データ、すなわち、
（ａ）変換データ
（ｂ）識別マーク入り変換データ
を、変換テーブル３１４に記録された指定位置に書き込むデータ変換処理、さらに、変換済みのＴＳ（トランスポートストリーム）の外部出力処理、あるいは、ステップＳ２０３におけるデマルチプレクサ処理、すなわちトランスポートストリーム（ＴＳ）からエレメンタリストリーム（ＥＳ）への変換処理、ステップＳ２０４におけるデコード処理、これらの処理は、コンテンツ再生または外部出力に並行したリアルタイム処理として実行する。
【０１３５】
このような処理シーケンスとすることで、セキュアＶＭ３５６による変換テーブル３１４の処理に時間がかかる場合であっても、コンテンツ再生、外部出力の処理に影響を与えることのないリアルタイム処理が実現される。
【０１３６】
［４．メッセージ表示およびコンテンツ利用制御処理］
上述したように、正当コンテンツ構成データと異なるブロークンデータを含むコンテン

ツを情報記録媒体に記録し、さらに、ブロークンデータの置き換え対象となる正当コンテンツ構成データである変換データと、変換データのコンテンツに対する設定位置情報を記録した変換テーブルを情報記録媒体に格納する構成とし、コンテンツ再生処理に際して、情報記録媒体に記録された変換テーブルに従って、コンテンツ構成データを変換データに置き換える処理を行なう構成によって、情報記録媒体に記録された暗号化コンテンツに対応する暗号鍵の漏洩が発生した場合でも、変換データの取得ができない装置においてはコンテンツの再生が実行されず、コンテンツの不正利用が防止される。

【０１３７】

また、変換データとして、コンテンツ再生装置またはコンテンツ再生アプリケーションを識別可能とした識別情報の構成ビットを解析可能としたデータを含む変換データを適用したので、万が一不正コンテンツが流出した場合でも、変換データの解析によって、不正コンテンツの流出源を特定することが可能となる。

【０１３８】

このように、厳格なコンテンツの利用制限が実現されることになる。しかし、一方、コンテンツを再生、利用しようとするユーザは、上述のコンテンツ保護機能によって、再生が禁止された場合、コンテンツが再生されない理由を知ることができず、また再生するための解決方法についても知ることができない。ユーザは機器の故障、あるいはディスクが不良品であるなどと判断する可能性もある。

【０１３９】

また、上述したデータ変換処理を適用したコンテンツの保護機構は、特定の映画などの大型コンテンツとしてのＡＶストリームを中心とした保護機構として構成したものであり、このような大型コンテンツではない例えばＪａｖａ（登録商標）のようなプログラムによって処理される小型のコンテンツについては変換データを設定するといった処理は負担が大きくなるという問題がある。

【０１４０】

以下では、このような問題を解決する構成として、コンテンツの再生禁止処理が実行された場合の処置として、ユーザに対するメッセージ提示、ユーザからの確認入力を可能とした構成例、および例えばＪａｖａ（登録商標）などによって処理される小型のコンテンツについての簡易なコンテンツ利用制限構成について説明する。

【０１４１】

（４．１）ＵＩ（ユーザインタフェース）処理部を利用したメッセージ表示

まず、ＵＩ（ユーザインタフェース）処理部を利用したメッセージの表示処理例について説明する。図１１は、左から暗号化コンテンツの格納された情報記録媒体３１０、情報記録媒体３１０をセットし、データの読み取りを実行するドライブ３３０、ドライブとデータ通信可能に接続され、情報記録媒体３１０に格納されたコンテンツをドライブ３３０を介して取得して再生処理を実行する再生アプリケーションを実行するホスト３５０を示している。ホスト３５０は、例えばＰＣ等の情報処理装置において実行される。

【０１４２】

図１１は、先に、図６を参照して説明したコンテンツ再生処理構成例に、メッセージ表示処理機能を追加した図である。すなわち、図６との相違点は、情報記録媒体３１０にメッセージデータファイル３１６が格納され、ホスト３５０側のセキュアＶＭ３５６において、ＵＩ（ユーザインタフェース）処理部３９１を利用して表示部３９２にメッセージ表示を行なう構成とした点である。

【０１４３】

正当なコンテンツ利用権を有するホストは、暗号化コンテンツ３１３の復号に成功し、変換テーブル３１４から取得する変換データを適用したデータ変換によって正常なコンテンツ再生が実行されることになる。また、正当なコンテンツ利用権を持たないホストは、コンテンツの復号処理、あるいは変換データに基づくデータ変換処理の少なくいずれかの処理に失敗し、正常なコンテンツ再生が不可能となる。これらの処理は、先に、図６を参照して説明した処理と同様の処理である。

【０１４４】
本実施例では、セキュアＶＭ３５６は、セキュリティ情報処理部として機能し、コンテンツ再生シーケンスにおけるセキュリティチェック情報に基づいて出力メッセージを決定し、出力メッセージの選択情報を伴うメッセージ出力命令をＵＩ（ユーザインタフェース）処理部３９１に出力する。
【０１４５】
ＵＩ（ユーザインタフェース）処理部３９１は、セキュリティ情報処理部としてのセキュアＶＭ３５６から入力する選択情報に基づくメッセージ情報を情報記録媒体３１０のメッセージデータファイル３１６から取得して、ホストを実行するＰＣ等のディスプレイである表示部３９２に出力（表示）する。表示部３９２は、ＵＩ（ユーザインタフェース）処理部３９１の出力するメッセージの表示を行なう。この表示は、例えば再生コンテンツに重畳した表示として実行される。
【０１４６】
ＵＩ（ユーザインタフェース）処理部３９１は、例えば、ＯＳＤ（オンスクリーン・ディスプレイ）機能を適用した構成とすることができる。ＯＳＤは、表示部３９２に表示された表示情報に重畳して、警告メッセージや、ディスプレイ調整画面などを割り込み表示させる機能を有する。ホスト３５０の処理と独立して並列に処理を行い、表示部３９２にメッセージ表示を実行し、また図示しない入力部を介したユーザ入力を受信することができる。本実施例では、このユーザ入力は、ＵＩ（ユーザインタフェース）処理部３９１からセキュアＶＭ３５６に入力される。
【０１４７】
具体的な処理例について説明する。セキュアＶＭ３５６は、コンテンツ再生シーケンスにおけるセキュリティチェック情報に基づいて出力メッセージを決定し、出力メッセージの選択情報を伴うメッセージ出力命令をＵＩ（ユーザインタフェース）処理部３９１に出力する。ＵＩ（ユーザインタフェース）処理部３９１は、選択情報に基づくメッセージ情報を情報記録媒体３１０のメッセージデータファイル３１６から取得して、ホストを実行するＰＣ等のディスプレイである表示部３９２に出力（表示）する。
【０１４８】
図１２は、情報記録媒体に記録されたメッセージデータファイル４０１～４０４を含むディレクトリを示した図である。図１２に示すように、情報記録媒体には、様々な内容、言語のメッセージデータファイル４０１～４０４が格納されている。
【０１４９】
前述したように、セキュアＶＭ３５６は、ホストアプリケーションを実行しているプレーヤ（情報処理装置）のＩＤ情報などをプレーヤ情報３５５として入力し、また、イベントハンドラ３５４からの監視情報を入力する。イベントハンドラ３５４は、セキュアＶＭ３５６によって実行される処理が正しく行なわれているか否かのエミュレータチェックや、その他のホストアプリケーションや、ホストアプリケーション実行機器としてのプレーヤ（情報処理装置）の処理、状態を監視し、処理エラー、不正処理などが検出された場合には、セキュアＶＭ３５６に監視情報を入力し、必要に応じて、例えばデータ変換処理を中止させる。
【０１５０】
セキュアＶＭ３５６は、例えば、プレーヤ情報３５５に基づいて、出力するメッセージの言語を特定し、また、イベントハンドラ３５４からの監視情報に基づいて出力するメッセージの内容を決定する処理を実行する。このようにして決定した言語および内容を持つメッセージデータファイルに対応するメッセージ選択情報を決定してＵＩ（ユーザインタフェース）処理部３９１に出力する。
【０１５１】
ＵＩ（ユーザインタフェース）処理部３９１は、この選択情報に基づいて、情報記録媒体３１０のメッセージデータファイル３１６から選択して取得し、メッセージデータを、ホストを実行するＰＣ等のディスプレイである表示部３９２に出力（表示）する。

【０１５２】
ＵＩ（ユーザインタフェース）処理部３９１として、ＯＳＤ（オンスクリーン・ディスプレイ）機能を適用した場合、セキュリティ情報処理部としてのセキュアＶＭ３５６からＵＩ（ユーザインタフェース）処理部３９１に対するメッセージ選択情報を伴うメッセージ表示命令には、ＯＳＤ呼び出し（ＣＡＬＬ＿ＯＳＤ）機能が利用される。ＯＳＤ呼び出し（ＣＡＬＬ＿ＯＳＤ）機能は、
（ａ）メッセージデータファイルを指定するナンバー指定情報（ｎｕｍ）、
（ｂ）ユーザ入力情報を指定するオペレーションＩＤ（ｏｐＩＤ）、
これら（ａ），（ｂ）の各指定情報を持つコマンドとして定義される。
【０１５３】
具体的なＯＳＤ呼び出し（ＣＡＬＬ＿ＯＳＤ）を利用したメッセージ表示処理例について、図１３を参照して説明する。例えば、ＯＳＤ呼び出し（ＣＡＬＬ＿ＯＳＤ）に対応するコマンド４１１には、
（ａ）メッセージデータファイルを指定するナンバー指定情報（ｎｕｍ）、
（ｂ）ユーザ入力情報を指定するオペレーションＩＤ（ｏｐＩＤ）、
の各指定情報が設定される。
【０１５４】
ナンバー指定情報（ｎｕｍ）は、先に、図１３を参照して説明したジヨウホウ記録媒体に格納されたメッセージデータファイルの指定情報として利用される。また、オペレーションＩＤ（ｏｐＩＤ）は、１４に示すように、各ＩＤに応じて、ユーザの入力部として、
［ＯＫ］のみを表示、
［ＯＫ］，［Ｃａｎｃｅｌ］を表示、
［Ｙｅｓ］，［Ｎｏ］を表示、
［Ｙｅｓ］，［Ｎｏ］、［Ｃａｎｃｅｌ］を表示、
これら、ユーザ入力部を表示する設定や、あるいは単にメッセージのみを表示し続ける設定などの設定情報として利用される。
【０１５５】
ユーザ入力部として［ＯＫ］のみを表示したメッセージ表示例を図１４に示す。ＵＩ（ユーザインタフェース）処理部３９１として、ＯＳＤ（オンスクリーン・ディスプレイ）機能を適用した場合、例えば図１４に示すようなメッセージデータが、表示部３９２の前面に表示されることになる。
【０１５６】
ユーザは、この表示メッセージの［ＯＫ］ボタンを例えばマウスを適用してクリックすることで入力情報はＯＳＤによって検出され、セキュアＶＭ３５６に入力される。なお、表示メッセージに例えばコンテンツ提供サーバあるいはコンテンツ管理サーバなどのＵＲＬを提示し、ＵＲＬのリックによって、各サーバに対するアクセスを可能とした設定としてもよい。
【０１５７】
このように、メッセージの提示を行なうことで、例えばコンテンツ復号や、正常なデータ変換ができず、正常なコンテンツ再生ができない場合であっても、セキュアＶＭは、その状況に応じて、適切なメッセージを表示部に出力することが可能となり、ユーザは状況を把握することができ、また、コンテンツ再生に必要な手続きなどの情報を提供することも可能となる。
【０１５８】
また、ユーザの入力情報としては、図１３、図１４を参照して説明した［ＯＫ］，［Ｃａｎｃｅｌ］、［Ｙｅｓ］，［Ｎｏ］の単純データではなく、例えば特定のパスワードなどの番号や文字列を入力させて、この入力値をセキュアＶＭ３５６が受け取り、パスワード確認処理によって、再生条件が満足されるか否かの判定を行ない、再生条件を満足すると判定した場合には、再生可能とするなどの処理を行なう構成としてもよい。
【０１５９】

（４．２）レジスタを利用したメッセージ表示およびコンテンツ利用制御

次に、レジスタを利用したメッセージ表示処理、さらに、コンテンツの利用制御処理例について説明する。

【０１６０】

図１５にレジスタを利用したメッセージ表示処理、さらに、コンテンツの利用制御処理を実現する基本構成を示す。図１５に示すセキュアＶＭ３５６は、図６、図１０および図１１を参照して説明したセキュアＶＭ３５６と同様のセキュアＶＭ３５６である。すなわち、データ変換処理を実行するホスト内にバーチャルマシンとして設定されるセキュアＶＭ３５６であり、セキュリティ情報処理部として機能する。

【０１６１】

セキュリティ情報処理部として機能するセキュアＶＭ３５６は、図６他を参照して説明したように、命令コード情報を含むデータ変換処理プログラム３１５を情報記録媒体３１０から読み出してデータ変換処理を実行する。さらに、セキュアＶＭ３５６は、ホストアプリケーションを実行しているプレーヤ（情報処理装置）のＩＤ情報などをプレーヤ情報３５５として入力し、また、イベントハンドラ３５４からの監視情報を入力する。イベントハンドラ３５４は、セキュアＶＭ３５６によって実行される処理が正しく行なわれているか否かのエミュレータチェックや、その他のホストアプリケーションや、ホストアプリケーション実行機器としてのプレーヤ（情報処理装置）の処理、状態を監視し、処理エラー、不正処理などが検出された場合には、セキュアＶＭ３５６に監視情報を入力し、必要に応じて、例えばデータ変換処理を中止させる。

【０１６２】

本処理例では、このセキュリティ情報処理部として機能するセキュアＶＭ３５６と、アプリケーション実行部５０１の間でレジスタを利用してメッセージやコマンド、あるいはパラメータ、データ等を転送する。アプリケーション実行部５０１は、アプリケーションレイヤ（またはＡＶレイヤとも呼ばれる）でのデータ処理実行部であり、このアプリケーション実行部５０１で実行されるアプリケーションには、様々なデータ処理を実行するアプリケーション・プログラムが含まれる。

【０１６３】

図６、図１０および図１１を参照して説明したホスト３５０によるコンテンツ再生処理を実行するＰＣ等の情報処理装置においては、様々なアプリケーション・プログラムが実行される。例えば、先に、項目（４．１）において説明したと同様、ＰＣ等の情報処理装置の表示部に、各種のメッセージ表示を実行しユーザ入力を受領するＵＩ機能を提供するＵＩ機能提供プログラムや、あるいは、情報記録媒体に格納された例えばＪａｖａ（登録商標）やＨＤＭＶ対応のコンテンツを実行するアプリケーション・プログラムなどが実行される。なお、このアプリケーション・プログラムは、情報処理装置がハードディスクなどに記憶して予め保持していたプログラム、あるいは情報記録媒体から読み出されたプログラムのいずれでもよい。

【０１６４】

情報記録媒体には、例えば映画等のＡＶストリームが格納されるとともに、例えばサービスコンテンツ、おまけコンテンツなどの設定などでゲームや映像、動画コンテンツなどの小型コンテンツが併せて記録されることがある。これらのコンテンツの多くはＪａｖａ（登録商標）やＨＤＭＶ対応のコンテンツとして記録される。これらの小型のコンテンツは、前述した暗号化処理やデータ変換処理の施されるＡＶコンテンツとは異なり、暗号化処理やデータ変換処理のようなコンテンツ保護が施されることは少ない。

【０１６５】

しかし、このような小型のコンテンツであっても、不正にコピーされ利用されることは好ましくない。本処理例では、このようなコンテンツについて、図１５に示すレジスタを利用した構成を適用してコンテンツの利用制御を実現する。

【０１６６】

図１５に示すように、セキュアＶＭ３５６と、アプリケーション実行部５０１の間では

、レジスタ５１１，５１２を利用してメッセージやコマンド、あるいはパラメータ、データ等が転送される。図１５に示す例では、セキュアＶＭ３５６の書き込みレジスタおよびアプリケーション実行部５０１の読み出しレジスタとしてレジスタ（ＰＳＲ）５１１を使用し、セキュアＶ３５６の読み出しレジスタおよびアプリケーション実行部５０１の書き込みレジスタとしてレジスタ（ＧＰＲ）５１２を使用した例を示している。レジスタ（ＰＳＲ）５１１は、プレイヤ・ステータスレジスタ、レジスタ（ＧＰＲ）５１２は、ジェネラル・パーパスレジスタであり既存のレジスタを利用した構成となっている。なお、レジスタの使用構成は、一例を示しているにすぎず、セキュアＶＭ３５６と、アプリケーション実行部５０１の間でデータのやり取りが可能なレジスタを適用すればよい。

【０１６７】

（４．２．１）レジスタを利用したＵＩ機能提供アプリケーションの実行例

まず、図１５に示すレジスタ利用構成において、アプリケーションレイヤにおいて実行するアプリケーションをＵＩ機能提供アプリケーションとして設定した場合の処理例について図１６を参照して説明する。

【０１６８】

アプリケーションレイヤにおいて通常実行されるアプリケーションは、情報記録媒体に格納された例えばＪａｖａ（登録商標）やＨＤＭＶ対応のコンテンツを実行するアプリケーション・プログラムである。本処理例では、これらのアプリケーションにＵＩ機能を実行させる。すなわち、アプリケーションレイヤにおいて実行されるアプリケーションをＵＩ機能提供アプリケーション実行部５２１として設定する。

【０１６９】

図１６には、セキュリティ情報処理部として機能するセキュアＶＭ３５６と、ＵＩ機能提供アプリケーション実行部５２１と、レジスタ５１１，５１２を示しており、セキュアＶＭ３５６と、ＵＩ機能提供アプリケーション実行部５２１が実行する処理シーケンスを処理ステップＳ２０１～Ｓ２０７として示してある。各処理ステップについて説明する。

【０１７０】

まず、ステップＳ２０１において、セキュアＶＭ３５６が、コンテンツ再生処理において、何らかのセキュリティ問題を検出したとする。先に図６他を参照して説明したように、セキュアＶＭ３５６は、イベントハンドラ３５４からの監視情報を受け取り、処理エラー、不正処理などが検出された場合には、セキュアＶＭ３５６にこれらの情報が入力される。

【０１７１】

コンテンツ再生処理において、何らかのセキュリティ問題などエラーが検出された場合、セキュアＶＭ３５６は、ステップＳ２０２において、予め各エラーに対応して設定されたエラーコードをレジスタ（ＰＳＲ）５１１に書き込む。

【０１７２】

次に、ステップＳ２０３において、ＵＩ機能提供アプリケーション実行部５２１は、レジスタ（ＰＳＲ）５１１に書き込まれたエラーコードを取得する。ＵＩ機能提供アプリケーション実行部５２１は、例えば予め設定される間隔で定期的にレジスタ（ＰＳＲ）５１１を参照する処理を実行する。ＵＩ機能提供アプリケーション実行部５２１は、レジスタ（ＰＳＲ）５１１に書き込まれたエラーコードを取得した後、ステップＳ２０４において、取得エラーコードに対応して設定されたメッセージを表示部に出力する。

【０１７３】

表示部に表示されるメッセージデータは、たとえば、先に図１４を参照して説明したようなメッセージおよびユーザ入力部が設定された表示データなどである。ＵＩ機能提供アプリケーション実行部５２１は、ステップＳ２０５において、ユーザ入力を検出すると、ステップＳ２０６において、ユーザ入力情報をレジスタ（ＧＰＲ）５１２に書き込む。さらに、ステップＳ２０７において、セキュアＶＭ３５６は、レジスタ（ＧＰＲ）５１２に書き込まれたユーザ入力情報を取得する。セキュアＶＭ３５６は、定期的にレジスタ（ＧＰＲ）５１２をチェックし、書き込み情報が得られるまで、あるいは所定のタイムアウト

時間に至るまでレジスタチェックを繰り返し実行する。

【０１７４】

この図１６に示す処理構成は、セキュアＶＭ３５６と、ＵＩ機能提供アプリケーション実行部５２１がレジスタを介した情報入出力を行なうことで、表示部を適用したユーザに対するメッセージ提示とユーザ入力の検出を可能とした構成である。このように、メッセージの提示を行なうことで、例えばコンテンツ復号や、正常なデータ変換ができず、正常なコンテンツ再生ができない場合であっても、セキュアＶＭは、レジスタおよびアプリケーションを介してその状況に応じて、適切なメッセージを表示部に出力することが可能となり、ユーザは状況を把握することができ、また、コンテンツ再生に必要な手続きなどの情報を提供することも可能となる。

【０１７５】

（４．２．２）レジスタ利用およびタイトル切り替えによるＵＩ機能提供例

次に、セキュリティ情報処理部として機能するセキュアＶＭ３５６が、タイトル切り替えコマンドをアプリケーションレイヤに出力して、アプリケーションレイヤで実行中のプログラムのタイトルを切り替えて、メッセージ提示などのＵＩ機能提供アプリケーションに切り替えて、メッセージ提示やユーザ入力を受領する処理例について、図１７を参照して説明する。

【０１７６】

図１７には、セキュリティ情報処理部として機能するセキュアＶＭ３５６と、アプリケーション実行部５２２と、レジスタ５１１，５１２を示している。本処理例では、セキュアＶＭ３５６が、タイトル切り替えコマンドをアプリケーション実行部５２２に出力して、アプリケーション実行部５２２で実行中のプログラムのタイトルを切り替えて、メッセージ提示などのＵＩ機能提供アプリケーションに切り替える処理を実行する。従って、アプリケーション実行部５２２は、ＵＩ機能提供アプリケーション以外のアプリケーションＡやＵＩ機能提供アプリケーションなど様々なアプリケーション・プログラムが実行されるアプリケーションレイヤを示している。

【０１７７】

セキュアＶＭ３５６と、アプリケーション実行部５２２において実行される処理シーケンスを処理ステップＳ２１１～Ｓ２１９として示してある。各処理ステップについて説明する。

【０１７８】

まず、ステップＳ２１１において、セキュアＶＭ３５６が、コンテンツ再生処理において、何らかのセキュリティ問題を検出する。先に図６他を参照して説明したように、セキュアＶＭ３５６は、イベントハンドラ３５４からの監視情報を受け取り、処理エラー、不正処理などが検出された場合には、セキュアＶＭ３５６にこれらの情報が入力される。コンテンツ再生処理において、何らかのセキュリティ問題などエラーが検出された場合、セキュアＶＭ３５６は、ステップＳ２１２において、予め各エラーに対応して設定されたエラーコードをレジスタ（ＰＳＲ）５１１に書き込む。

【０１７９】

次に、ステップＳ２１３において、セキュアＶＭ３５６はアプリケーション実行部５２２に対して、タイトル切り替え指示を出力する。このタイトル切り替え指示は、アプリケーション実行部５２２において実行中のプログラムのタイトルを切り替えて、メッセージ提示などのＵＩ機能提供アプリケーションに切り替える指示コマンドである。ステップＳ２１４において、アプリケーション実行部５２２は、セキュアＶＭ３５６からのタイトル切り替えコマンドに従って、実行中のアプリケーションのタイトル切り替え処理を実行し、ＵＩ機能提供アプリケーションを実行する。

【０１８０】

その後の処理は、先に図１６を参照して説明したと同様の処理であり、ステップＳ２１５において、アプリケーション実行部５２２におけるＵＩ機能提供アプリケーションは、レジスタ（ＰＳＲ）５１１に書き込まれたエラーコードを取得し、ステップＳ２１６にお

いて、取得エラーコードに対応して設定済みのメッセージを表示部に出力する。

【０１８１】

さらに、ステップＳ２１７において、ユーザ入力を検出すると、ステップＳ２１８において、ユーザ入力情報をレジスタ（ＧＰＲ）５１２に書き込む。さらに、ステップＳ２１９において、セキュアＶＭ３５６は、レジスタ（ＧＰＲ）５１２に書き込まれたユーザ入力情報を取得する。

【０１８２】

この図１７に示す処理構成は、セキュリティ情報処理部として機能するセキュアＶＭ３５６が、アプリケーション実行部５２２において実行されるアプリケーションを切り替える権限を有し、このアプリケーション切り替えによって、ＵＩ機能提供アプリケーションをアプリケーションレイヤにおいて実行させ、レジスタを介してユーザに対するメッセージ提示とユーザ入力の検出を可能とした構成である。

【０１８３】

本構成においては、ＵＩ機能提供アプリケーションにおいてのみレジスタチェックなどの処理を実行させ、その他の通常のアプリケーションにおいては、レジスタチェックを行なう設定とする必要がなく、アプリケーションレイヤで実行される一般のアプリケーションについての変更は必要としないという利点がある。

【０１８４】

（４．２．３）レジスタ利用によるコンテンツ利用制御処理例

次に、レジスタ利用によるコンテンツ利用制御処理例について、図１８を参照して説明する。先に説明したデータ変換処理を適用したコンテンツの保護機構は、前述したように、特定の映画などの大型コンテンツとしてのＡＶストリームを中心とした保護機構として構成したものであり、このような大型コンテンツではない例えばＪａｖａ（登録商標）のようなプログラムによって処理される小型のコンテンツについては変換データを設定するといった処理は負担が大きくなるという問題がある。以下では、例えばＪａｖａ（登録商標）やＨＤＭＶなどによって処理される小型のコンテンツについて、レジスタを利用して実行するコンテンツ利用制御構成について説明する。

【０１８５】

図１８には、セキュリティ情報処理部として機能するセキュアＶＭ３５６と、例えばＪａｖａ（登録商標）やＨＤＭＶなどによって処理される小型のコンテンツを実行するアプリケーション実行部５２３と、レジスタ５１１，５１２を示している。アプリケーション実行部５２３は、図に示すようにＡＶコンテンツとともに情報記録媒体５５０に格納されたＪａｖａ（登録商標）やＨＤＭＶなどによって処理される小型のコンテンツ５５１である。

【０１８６】

情報記録媒体５５０から読み出されたＪａｖａ（登録商標）やＨＤＭＶなどによって処理される小型のコンテンツ５５１は、利用制御を実現するため、コンテンツの実行に必要な特定の処理パラメータを有し、セキュアＶＭ３５６は、このパラメータを取得する。アプリケーション実行部５２３は、処理パラメータを含まないＪａｖａ（登録商標）やＨＤＭＶなどによって構成されるコンテンツ実体を取得して再生処理を実行する。ただし、コンテンツの再生処理には、処理パラメータをセキュアＶＭ３５６から取得することが必要となる。

【０１８７】

処理パラメータは、例えば、一定のコンテンツ再生区間毎にセキュアＶＭ３５６が、アプリケーション実行部５２３にレジスタ（ＰＳＲ）５１１を介して提供し、セキュアＶＭ３５６において、何らかのセキュリティ問題が検出された場合は、パラメータの提供を停止する。このパラメータ提供停止によって、アプリケーション実行部５２３はコンテンツ再生が不可能となりコンテンツ再生が停止される。本処理例では、このような構成によって、コンテンツの利用制御を実現する。

【０１８８】

アプリケーション実行部５２３において実行されるアプリケーション（コンテンツ５５１）は、例えばＪａｖａ（登録商標）やＨＤＭＶなどのアプリケーションであり、これらのアプリケーシッョンは、アプリケーションの開始前や実行中に間欠的にアプリケーションの実行または継続に必要なパラメータ（Ｐ１，Ｐ２，Ｐ３・・・）をレジスタ（ＰＳＲ）５１１を介して取得する。

【０１８９】

例えば、アプリケーション実行部５２３は、レジスタ（ＰＳＲ）５１１から取得したパラメータを適用した排他論理和演算処理、または、パラメータを適用した暗号処理、または、パラメータを適用した暗号処理によって生成した暗号鍵による復号処理によって表示コンテンツデータの生成を行う。

【０１９０】

パラメータＰ１，Ｐ２，Ｐ３・・・はアプリケーション実行部５２３において実行されるアプリケーション（コンテンツ５５１）の所定のプログラム実行単位またはコンテンツの提示単位毎に設定される異なるパラメータであり、アプリケーションの開始時や実行中、所定間隔毎にアプリケーション実行部５２３は、レジスタ（ＰＳＲ）５１１から順次、パラメータＰ１，Ｐ２，Ｐ３を取得し、これらの取得パラメータを適用した演算あるいは暗号処理を実行する。

【０１９１】

例えば、パラメータＰ１，Ｐ２，Ｐ３は、アプリケーション実行部５２３において実行されるアプリケーションによって提示されるコンテンツを表示時間単位で区分した部分コンテンツの暗号化パラメータや、演算パラメータとして設定される。たとえば、コンテンツの提示時間毎に、

時間ｔ１～ｔ２の部分コンテンツの提示には、パラメータＰ１を適用した演算処理またはコンテンツ復号処理を必要とする。

時間ｔ２～ｔ３の部分コンテンツの提示には、パラメータＰ２を適用した演算処理またはコンテンツ復号処理を必要とする。

時間ｔ３～ｔ４の部分コンテンツの提示には、パラメータＰ３を適用した演算処理またはコンテンツ復号処理を必要とする。

などのように、コンテンツの提示には、異なるパラメータを順次、レジスタ（ＰＳＲ）５１１から取得して処理を実行することが必要となる設定とされている。

【０１９２】

例えばコンテンツ５５１の構成データとパラメータ（Ｐ１，Ｐ２，Ｐ３・・）の排他論理和（ＸＯＲ）演算によって、正しいコンテンツが取得される。あるいはパラメータ（Ｐ１，Ｐ２，Ｐ３・・）を適用した処理によって、異なる復号鍵が、順次、生成され、これらの復号鍵を適用して、部分コンテンツの復号を順次、実行してコンテンツ提示を継続することが可能な設定とされる。

【０１９３】

セキュアＶＭ３５６は、アプリケーション実行部５２３において実行される所定のコンテンツ再生区間毎に異なるパラメータ（Ｐ１，Ｐ２，Ｐ３・・・）を順次、レジスタ（ＰＳＲ）５１１に格納し、アプリケーション実行部５２３において実行中のアプリケーション、例えばＪａｖａ（登録商標）、ＨＤＭＶプログラムは、定期的にレジスタ（ＰＳＲ）５１１からパラメータ（Ｐ１，Ｐ２，Ｐ３・・・）を取得して、アプリケーションの実行や継続に必要な演算あるいは暗号処理を、取得パラメータを適用して実行する。

【０１９４】

セキュアＶＭ３５６において、何らかのセキュリティ問題が検出された場合は、パラメータの提供を停止する。このパラメータ提供停止によって、アプリケーション実行部５２３はコンテンツ再生が不可能となりコンテンツ再生が停止される。本処理例では、このような構成によって、コンテンツの利用制御を実現する。

【０１９５】

なお、アプリケーション実行部５２３は、定期的に、レジスタ５１２（ＧＰＲ）を介し

てセキュアＶＭ３５６にメッセージを送る構成とし、例えば新たなパラメータの取得が必要となるタイミング毎にレジスタ５１２（ＧＰＲ）にパラメータ要求メッセージかを書き込み、セキュアＶＭ３５６がレジスタ５１２（ＧＰＲ）に書き込まれたパラメータ要求に応じてレジスタ（ＰＳＲ）５１１に対してパラメータ書き込みを行なう設定としてもよい。

【０１９６】

図１８を参照して、コンテンツ利用制御処理シーケンスについて説明する。セキュアＶＭ３５６と、アプリケーション実行部５２３において実行される処理シーケンスを処理ステップＳ２２１～Ｓ２２４として示してある。各処理ステップについて説明する。

【０１９７】

まず、ステップＳ２２１において、セキュリティ情報処理部として機能するセキュアＶＭ３５６が、セキュリティ問題の有無を判定する。先に図６他を参照して説明したように、セキュアＶＭ３５６は、イベントハンドラ３５４からの監視情報を受け取り、処理エラー、不正処理などが検出された場合には、セキュアＶＭ３５６にこれらの情報が入力される。特にセキュリティ問題が検出されない場合、セキュアＶＭ３５６は、レジスタ（ＰＳＲ）５１１に、アプリケーションの実行に必要となるパラメータを書き込む。

【０１９８】

次に、ステップＳ２２３において、アプリケーション実行部５２３は、レジスタ（ＰＳＲ）５１１に書き込まれたパラメータを取得し、ステップＳ２２４において、レジスタ読み取り値を適用してアプリケーションを実行する。

【０１９９】

セキュアＶＭ３５６によるレジスタ（ＰＳＲ）５１１に対するパラメータ書き込みは、定期的に実行され、アプリケーション実行部５２３は、レジスタ（ＰＳＲ）５１１に書き込まれたパラメータを定期的に取得し、取得したパラメータを利用したアプリケーション実行を行なう。

【０２００】

例えば、セキュアＶＭ３５６は、アプリケーション実行部５２３において実行される所定のコンテンツ再生区間毎に異なるパラメータ（Ｐ１，Ｐ２，Ｐ３・・・）を順次、レジスタ（ＰＳＲ）５１１に格納する。アプリケーション実行部５２３において実行中のアプリケーション、例えばＪａｖａ（登録商標）、ＨＤＭＶプログラムは、定期的にレジスタ（ＰＳＲ）５１１からパラメータ（Ｐ１，Ｐ２，Ｐ３・・・）を取得して、アプリケーションの実行や継続に必要な演算あるいは暗号処理などを、レジスタ（ＰＳＲ）５１１から取得したパラメータを適用して実行する。

【０２０１】

セキュアＶＭ３５６において、不正処理などセキュリティ問題が検出された場合には、セキュアＶＭ３５６は、レジスタ（ＰＳＲ）５１１に対するパラメータの書き込み処理を停止する。このパラメータ書き込み停止によって、アプリケーション実行部５２３は、レジスタ（ＰＳＲ）５１１からのパラメータ取得に失敗し、パラメータを利用したアプリケーション実行が不可能となり、コンテンツ再生は停止される。

【０２０２】

このように、本処理例では、上述した暗号化やデータ変換のようなコンテンツ保護機能を持たない例えば、Ｊａｖａ（登録商標）やＨＤＭＶなどによって処理される小型のコンテンツについても、簡易な構成、すなわちセキュアＶＭからアプリケーションに対するパラメータの提供という簡易な構成で、コンテンツの利用制御が実現される。

【０２０３】

なお、本処理例において、セキュリティ問題が発生し、コンテンツの再生が停止された場合には、先に、説明したメッセージ提示処理によって、ユーザにコンテンツ再生の停止理由などの通知を行なうことができる。

【０２０４】

（４．２．４）アプリケーション実行部の使用レジスタの利用による処理例１

次に、アプリケーション実行部が使用するレジスタの一部をセキュリティ情報処理部として機能するセキュアＶＭ３５６が利用して読み書き可能な構成とすることで、メッセージ提示やユーザ入力の受領、さらに、セキュアＶＭ３５６とアプリケーション実行部との間の信頼性確認処理を可能とした構成例について、図１９を参照して説明する。

【０２０５】

図１９には、セキュリティ情報処理部として機能するセキュアＶＭ３５６と、例えば、ＡＶ－Ｌａｙｅｒに設定されるアプリケーション実行部５２４と、３つのレジスタＸ（ＰＳＲ－Ｘ）５７１，レジスタＹ（ＰＳＲ－Ｙ）５７２，レジスタＺ（ＰＳＲ－Ｚ）５７３を示している。

【０２０６】

レジスタＸ（ＰＳＲ－Ｘ）５７１は、セキュアＶＭ３５６が書き込み（Ｗｒｉｔｅ）を実行し、アプリケーション実行部５２４が読み取り（Ｒｅａｄ）を実行するレジスタである。レジスタＸ（ＰＳＲ－Ｘ）５７１に対して、セキュアＶＭ３５６が書き込み（Ｗｒｉｔｅ）を実行すると、レジスタＸ（ＰＳＲ－Ｘ）５７１の変化に基づくイベント通知が、アプリケーション実行部５２４になされ、アプリケーション実行部５２４は、レジスタＸ（ＰＳＲ－Ｘ）５７１に対する書き込み（Ｗｒｉｔｅ）が実行されたことを知ることができる。

【０２０７】

例えばメッセージ提示や、Ｊａｖａ（登録商標）やＨＤＭＶなどのアプリケーションを実行するアプリケーション実行部５２４は、レジスタＸ（ＰＳＲ－Ｘ）５７１に対する書き込み（Ｗｒｉｔｅ）が実行されたことの通知を受け取ったらレジスタＸ（ＰＳＲ－Ｘ）５７１をチェックし、値に応じて警告メッセージを表示するなどの処理を行う。

【０２０８】

また、レジスタＹ（ＰＳＲ－Ｙ）５７２は、アプリケーション実行部５２４が書き込み（Ｗｒｉｔｅ）を実行し、セキュアＶＭ３５６が読み取り（Ｒｅａｄ）を実行するレジスタである。メッセージ提示や、Ｊａｖａ（登録商標）やＨＤＭＶなどのアプリケーションを実行するアプリケーション実行部５２４は、セキュアＶＭ３５６に対して通知する内容に対応する値をレジスタＹ（ＰＳＲ－Ｙ）５７２に書き込む。

【０２０９】

レジスタＹ（ＰＳＲ－Ｙ）５７２にデータが書き込まれると、セキュアＶＭ３５６に対して通知（ＩＮＴＲＰ：ｉｎｔｅｒｒｕｐｔ）がなされる。セキュアＶＭ３５６は、レジスタＹ（ＰＳＲ－Ｙ）５７２に書き込まれた値に応じた処理を行う。レジスタＹ（ＰＳＲ－Ｙ）５７２には、例えば、アプリケーション実行部５２４が実行したメッセージ表示に対するユーザ入力値が書き込まれる。

【０２１０】

レジスタＺ（ＰＳＲ－Ｚ）５７３は、セキュアＶＭ３５６、およびアプリケーション実行部５２４の双方が書き込み（Ｗｒｉｔｅ）および読み取り（Ｒｅａｄ）を実行可能なレジスタである。このレジスタＺ（ＰＳＲ－Ｚ）５７３は、セキュアＶＭ３５６、およびアプリケーション実行部５２４相互間の処理状況通知用レジスタとして利用される。

【０２１１】

本構成を利用したメッセージ提示およびユーザ入力受領処理シーケンスについて、図２０を参照して説明する。図２０には、セキュリティ情報処理部として機能するセキュアＶＭ３５６と、アプリケーション実行部５２４と、３つのレジスタＸ（ＰＳＲ－Ｘ）５７１，レジスタＹ（ＰＳＲ－Ｙ）５７２，レジスタＺ（ＰＳＲ－Ｚ）５７３を示している。

【０２１２】

アプリケーション実行部５２４において通常実行されるアプリケーションは、情報記録媒体に格納された例えばＪａｖａ（登録商標）やＨＤＭＶ対応のコンテンツを実行するアプリケーション・プログラムである。図２０には、セキュアＶＭ３５６と、アプリケーション実行部５２４が実行する処理シーケンスを処理ステップＳ２３１～Ｓ２３７として示してある。各処理ステップについて説明する。

【０２１３】
まず、ステップＳ２３１において、セキュアＶＭ３５６が、コンテンツ再生処理において、何らかのセキュリティ問題を検出したとする。先に図６他を参照して説明したように、セキュアＶＭ３５６は、イベントハンドラ３５４からの監視情報を受け取り、処理エラー、不正処理などが検出された場合には、セキュアＶＭ３５６にこれらの情報が入力される。
【０２１４】
コンテンツ再生処理において、何らかのセキュリティ問題などエラーが検出された場合、セキュアＶＭ３５６は、ステップＳ２３２において、予め各エラーに対応して設定されたエラーコードをレジスタＸ（ＰＳＲ－Ｘ）５７１に書き込む。このレジスタ書き込みによって、レジスタＸ（ＰＳＲ－Ｘ）５７１の変化に基づくイベント通知が、アプリケーション実行部５２４になされ、アプリケーション実行部５２４は、レジスタＸ（ＰＳＲ－Ｘ）５７１に対する書き込み（Ｗｒｉｔｅ）が実行されたことを知ることができる。
【０２１５】
ステップＳ２３３において、アプリケーション実行部５２４は、イベント通知によって、レジスタ書き込み発生を検知し、レジスタＸ（ＰＳＲ－Ｘ）５７１に書き込まれたエラーコードを取得する。アプリケーション実行部５２４は、レジスタＸ（ＰＳＲ－Ｘ）５７１に書き込まれたエラーコードを取得した後、ステップＳ２３４において、取得エラーコードに対応して設定されたメッセージを表示部に出力する。
【０２１６】
表示部に表示されるメッセージデータは、たとえば、先に図１４を参照して説明したようなメッセージおよびユーザ入力部が設定された表示データなどである。アプリケーション実行部５２４は、ステップＳ２３５において、ユーザ入力を検出すると、ステップＳ２３６において、ユーザ入力情報をレジスタＹ（ＰＳＲ－Ｙ）５７２に書き込む。
【０２１７】
レジスタＹ（ＰＳＲ－Ｙ）５７２にデータが書き込まれると、セキュアＶＭ３５６に対して通知（ＩＮＴＲＰ：ｉｎｔｅｒｒｕｐｔ）がなされる。セキュアＶＭ３５６は、レジスタＹ（ＰＳＲ－Ｙ）５７２に書き込まれたことを通知（ＩＮＴＲＰ：ｉｎｔｅｒｒｕｐｔ）によって検出すると、ステップＳ２３７において、レジスタＹ（ＰＳＲ－Ｙ）５７２の書き込みデータ、例えば、アプリケーション実行部５２４が実行したメッセージ表示に対するユーザ入力値を取得し、ユーザ入力値に対応した処理を実行する。
【０２１８】
なお、以上説明した処理シーケンスにおいては、レジスタＺ（ＰＳＲ－Ｚ）５７３の利用が示されていないが、レジスタＺ（ＰＳＲ－Ｚ）５７３は、前述したように、セキュアＶＭ３５６、およびアプリケーション実行部５２４の双方が書き込み（Ｗｒｉｔｅ）および読み取り（Ｒｅａｄ）を実行可能なレジスタであり、セキュアＶＭ３５６、およびアプリケーション実行部５２４相互間の処理状況通知用レジスタとして利用される。
【０２１９】
例えば、初期状態で、ＰＳＲ－Ｚの設定値＝０として設定され、セキュアＶＭ３５６の処理が終了し、アプリケーション実行部５２４の処理手順になった場合にＰＳＲ－Ｚの設定値＝１として設定し、次に、アプリケーション実行部５２４の処理が終了し、セキュアＶＭ３５６の処理手順になった場合にＰＳＲ－Ｚの設定値＝２として設定するなどによって、双方の処理手順に応じてプロセスの進み具合に応じた値を設定し、双方が処理シーケンスの進行度を確認可能とすることができる。なお、処理の終了や、中断の場合には、ＰＳＲ－Ｚの設定値＝０として初期値に戻す設定とする。
【０２２０】
このように、セキュアＶＭ３５６、およびアプリケーション実行部５２４は、レジスタＺ（ＰＳＲ－Ｚ）５７３をセキュアＶＭ３５６、およびアプリケーション実行部５２４相互間の処理状況通知用レジスタとして利用することで、処理シーケンスに従った確実な処理の実行が可能となる。

【０２２１】
さらに、図１９に示すセキュアＶＭ３５６、およびアプリケーション実行部５２４の双方が利用可能な３つのレジスタＸ（ＰＳＲ－Ｘ）５７１，レジスタＹ（ＰＳＲ－Ｙ）５７２，レジスタＺ（ＰＳＲ－Ｚ）５７３を利用することで、セキュアＶＭ３５６と、アプリケーション実行部５２４との間での信頼性確認処理を実行することができる。
【０２２２】
図２１を参照して、セキュアＶＭ３５６と、アプリケーション実行部５２４との間での信頼性確認処理シーケンスについて説明する。図２１は、セキュアＶＭ３５６と、アプリケーション実行部５２４との間でチャレンジ／レスポンス処理を行うことにより、お互いに正常に動作していることを確認する処理のシーケンスを説明する図である。核ステップについて説明する。
【０２２３】
まず、ステップＳ２４１－ａにおいて、アプリケーション実行部５２４は、適当な値（例えば乱数）を生成し、レジスタＹ（ＰＳＲ－Ｙ）５７２に書き込む。さらに、ステップＳ２４１－ｂにおいて、レジスタＺ（ＰＳＲ－Ｚ）５７３に状態値（例えば２）を書き込む。
【０２２４】
セキュアＶＭ３５６は、レジスタＹ（ＰＳＲ－Ｙ）５７２にデータが書き込まれたことを通知（ＩＮＴＲＰ＿ＰｒｅｓｅｎｔａｔｉｏｎＬａｙｅｒ）により検出し、ステップＳ２４２において、レジスタＹ（ＰＳＲ－Ｙ）５７２の書き込みデータを読み取る。
【０２２５】
さらに、セキュアＶＭ３５６は、レジスタＹ（ＰＳＲ－Ｙ）５７２からの読み取り値（乱数）に対して予め定められたデータ処理、例えば演算処理あるいは暗号処理などを実行し、ステップＳ２４３－ａにおいて、この結果値をレジスタＸ（ＰＳＲ－Ｘ）５７１に書き込む。セキュアＶＭ３５６は、この処理に際してステップＳ２４３－ｂにおいて、レジスタＺ（ＰＳＲ－Ｚ）５７３に状態値（例えば１）を書き込む。
【０２２６】
ステップＳ２４４において、アプリケーション実行部５２４は、レジスタＸ（ＰＳＲ－Ｘ）５７１の書き込みデータを読み取り、ステップＳ２４５において、読み取りデータの検証を実行する。例えば、アプリケーション実行部５２４によって生成し、セキュアＶＭ３５６に通知した乱数に基づいて自ら演算あるいは暗号処理を実行した結果と比較照合を実行し、レジスタＸ（ＰＳＲ－Ｘ）５７１からの読み取り値と一致すれば、セキュアＶＭ３５６は、正当な処理を実行しているセキュアＶＭ３５６であると判断する。なお、セキュアＶＭ３５６と、アプリケーション実行部５２４が乱数に対して実行する演算処理あるいは暗号処理は共有する秘密情報に基づく処理を行なう設定とすることが好ましい。
【０２２７】
なお、図２１に示す信頼性確認処理は、複数回繰り返し実行してもよく、また、乱数発行をセキュアＶＭ３５６が実行する構成としてもよい。この信頼性確認機能を有することによって、アプリケーション実行部５２４において実行されるアプリケーションについての信頼性確認が可能となるため、アプリケーションレイヤ（ＡＶレイヤ）のロバストネス（Ｒｏｂｕｓｔｎｅｓｓ）に特に制限を設けることなく、従来通りの実装で良い点が非常に大きな利点となる。
【０２２８】
アプリケーション実行部５２４としてのＡＶレイヤにおいて実行されるアプリケーションは、通常のＣＰＵで処理されることが多く、高度なロバストネス（Ｒｏｂｕｓｔｎｅｓｓ）が要求されると実装コストが非常に高くなってしまうが、本処理例の如く、セキュアＶＭ３５６と、アプリケーション実行部５２４との間での信頼性確認を実行可能としたことで、プリケーション実行部５２４において実行されるアプリケーションに対して高度なロバストネス（Ｒｏｂｕｓｔｎｅｓｓ）が要求することのない設定が可能となる。
【０２２９】

（４．２．５）アプリケーション実行部の使用レジスタの利用による処理例２

次に、アプリケーション実行部が使用するレジスタの一部をセキュリティ情報処理部として機能するセキュアＶＭ３５６が利用して読み書き可能なもう１つの構成例について図２２を参照して説明する。本処理例も、メッセージ提示やユーザ入力の受領、さらに、セキュアＶＭ３５６とアプリケーション実行部との間の信頼性確認処理を可能とした構成を持つ。

【０２３０】

図２２には、セキュリティ情報処理部として機能するセキュアＶＭ３５６と、例えば、ＡＶ－Ｌａｙｅｒに設定されるアプリケーション実行部５２５と、２つのレジスタＸ（ＰＳＲ－Ｘ）５８１，レジスタＹ（ＰＳＲ－Ｙ）５８２を示している。本構成は、先に図１９を参照して説明した構成からレジスタＺ（ＰＳＲ－Ｚ）を省略した構成である。

【０２３１】

レジスタＸ（ＰＳＲ－Ｘ）５８１は、セキュアＶＭ３５６が書き込み（Ｗｒｉｔｅ）を実行し、アプリケーション実行部５２５が読み取り（Ｒｅａｄ）を実行するレジスタである。レジスタＸ（ＰＳＲ－Ｘ）５８１に対して、セキュアＶＭ３５６が書き込み（Ｗｒｉｔｅ）を実行すると、レジスタＸ（ＰＳＲ－Ｘ）５８１の変化に基づくイベント通知が、アプリケーション実行部５２５になされ、アプリケーション実行部５２５は、レジスタＸ（ＰＳＲ－Ｘ）５８１に対する書き込み（Ｗｒｉｔｅ）が実行されたことを知ることができる。

【０２３２】

例えばメッセージ提示や、Ｊａｖａ（登録商標）やＨＤＭＶなどのアプリケーションを実行するアプリケーション実行部５２５は、レジスタＸ（ＰＳＲ－Ｘ）５８１に対する書き込み（Ｗｒｉｔｅ）が実行されたことの通知を受け取ったらレジスタＸ（ＰＳＲ－Ｘ）５８１をチェックし、値に応じて警告メッセージを表示するなどの処理を行う。

【０２３３】

また、レジスタＹ（ＰＳＲ－Ｙ）５８２は、アプリケーション実行部５２５が書き込み（Ｗｒｉｔｅ）を実行し、セキュアＶＭ３５６が読み取り（Ｒｅａｄ）を実行するレジスタである。メッセージ提示や、Ｊａｖａ（登録商標）やＨＤＭＶなどのアプリケーションを実行するアプリケーション実行部５２５は、セキュアＶＭ３５６に対して通知する内容に対応する値をレジスタＹ（ＰＳＲ－Ｙ）５８２に書き込む。

【０２３４】

レジスタＹ（ＰＳＲ－Ｙ）５８２にデータが書き込まれると、セキュアＶＭ３５６に対して通知（ＩＮＴＲＰ：ｉｎｔｅｒｒｕｐｔ）がなされる。セキュアＶＭ３５６は、レジスタＹ（ＰＳＲ－Ｙ）５８２に書き込まれた値に応じた処理を行う。レジスタＹ（ＰＳＲ－Ｙ）５８２には、例えば、アプリケーション実行部５２５が実行したメッセージ表示に対するユーザ入力値が書き込まれる。

【０２３５】

本構成では、先に図１９を参照して説明したレジスタＺ、すなわち、セキュアＶＭ３５６、およびアプリケーション実行部５２５相互間の処理状況通知用レジスタが設定されていない。本処理例では、セキュアＶＭ３５６、およびアプリケーション実行部５２５相互間の処理状況通知に、レジスタＸ（ＰＳＲ－Ｘ）５８１と、レジスタＹ（ＰＳＲ－Ｙ）５８２の書き込み値を利用する。

【０２３６】

図に示すように、セキュアＶＭ３５６が書き込み（Ｗｒｉｔｅ）を実行し、アプリケーション実行部５２５が読み取り（Ｒｅａｄ）を実行するレジスタＸ（ＰＳＲ－Ｘ）５８１に対して、セキュアＶＭ３５６が書き込み（Ｗｒｉｔｅ）を実行する際、レジスタ書き込みデータ５９１のように、セキュアＶＭ３５６は、通知内容対応値の他に処理状況ビットをレジスタＸ（ＰＳＲ－Ｘ）５８１に書き込む処理を実行する。この処理状況ビットをアプリケーション実行部５２５が読み取り、処理状況を知ることができる。

【０２３７】

また、アプリケーション実行部５２５が書き込み（Ｗｒｉｔｅ）を実行し、セキュアＶＭ３５６が読み取り（Ｒｅａｄ）を実行するレジスタＹ（ＰＳＲ－Ｙ）５８２に対して、アプリケーション実行部５２５が書き込み（Ｗｒｉｔｅ）を実行する際、レジスタ書き込みデータ５９２のように、アプリケーション実行部５２５は、通知内容対応値の他に処理状況ビットをレジスタＹ（ＰＳＲ－Ｙ）５８２に書き込む処理を実行する。この処理状況ビットをセキュアＶＭ３５６５２５が読み取り、処理状況を知ることができる。

【０２３８】

このように本構成では、レジスタＸ（ＰＳＲ－Ｘ）５８１とレジスタＹ（ＰＳＲ－Ｙ）５８２に対するデータ書き込みの際に、処理状況ビットを併せて書き込むことで、セキュアＶＭ３５６、およびアプリケーション実行部５２４相互間の処理状況通知を実現している。

【０２３９】

本構成を利用したメッセージ提示およびユーザ入力受領処理シーケンスについて、図２３を参照して説明する。図２３には、セキュリティ情報処理部として機能するセキュアＶＭ３５６と、アプリケーション実行部５２５と、２つのレジスタＸ（ＰＳＲ－Ｘ）５８１，レジスタＹ（ＰＳＲ－Ｙ）５８２を示している。

【０２４０】

アプリケーション実行部５２５において通常実行されるアプリケーションは、情報記録媒体に格納された例えばＪａｖａ（登録商標）やＨＤＭＶ対応のコンテンツを実行するアプリケーション・プログラムである。図２３には、セキュアＶＭ３５６と、アプリケーション実行部５２５が実行する処理シーケンスを処理ステップＳ２４１～Ｓ２４７として示してある。各処理ステップについて説明する。

【０２４１】

まず、ステップＳ２４１において、セキュアＶＭ３５６が、コンテンツ再生処理において、何らかのセキュリティ問題を検出したとする。先に図６他を参照して説明したように、セキュアＶＭ３５６は、イベントハンドラ３５４からの監視情報を受け取り、処理エラー、不正処理などが検出された場合には、セキュアＶＭ３５６にこれらの情報が入力される。

【０２４２】

コンテンツ再生処理において、何らかのセキュリティ問題などエラーが検出された場合、セキュアＶＭ３５６は、ステップＳ２４２において、予め各エラーに対応して設定されたエラーコードをレジスタＸ（ＰＳＲ－Ｘ）５８１に書き込む。このレジスタＸ（ＰＳＲ－Ｘ）５８１に対するデータ書き込みに際しては、所定の状況通知ビットを併せて書き込む。

【０２４３】

このレジスタ書き込みによって、レジスタＸ（ＰＳＲ－Ｘ）５８１の変化に基づくイベント通知が、アプリケーション実行部５２５になされ、アプリケーション実行部５２５は、レジスタＸ（ＰＳＲ－Ｘ）５８１に対する書き込み（Ｗｒｉｔｅ）が実行されたことを知ることができる。

【０２４４】

ステップＳ２４３において、アプリケーション実行部５２５は、イベント通知によって、レジスタ書き込み発生を検知し、レジスタＸ（ＰＳＲ－Ｘ）５８１に書き込まれたエラーコードと状況通知ビットを取得する。アプリケーション実行部５２５は、レジスタＸ（ＰＳＲ－Ｘ）５８１に書き込まれたエラーコードを取得した後、ステップＳ２４４において、取得エラーコードに対応して設定されたメッセージを表示部に出力する。

【０２４５】

表示部に表示されるメッセージデータは、たとえば、先に図１４を参照して説明したようなメッセージおよびユーザ入力部が設定された表示データなどである。アプリケーション実行部５２５は、ステップＳ２４５において、ユーザ入力を検出すると、ステップＳ２４６において、ユーザ入力情報をレジスタＹ（ＰＳＲ－Ｙ）５８２に書き込む。このレジ

スタＹ（ＰＳＲ－Ｙ）５８２に対するデータ書き込みに際しては、所定の状況通知ビットを併せて書き込む。

【０２４６】

レジスタＹ（ＰＳＲ－Ｙ）５８２にデータが書き込まれると、セキュアＶＭ３５６に対して通知（ＩＮＴＲＰ：ｉｎｔｅｒｒｕｐｔ）がなされる。セキュアＶＭ３５６は、レジスタＹ（ＰＳＲ－Ｙ）５８２に書き込まれたことを通知（ＩＮＴＲＰ：ｉｎｔｅｒｒｕｐｔ）によって検出すると、ステップＳ２４７において、レジスタＹ（ＰＳＲ－Ｙ）５８２の書き込みデータ、例えば、アプリケーション実行部５２４が実行したメッセージ表示に対するユーザ入力値を取得し、ユーザ入力値に対応した処理を実行する。なお、この際にセキュアＶＭ３５６レジスタＹ（ＰＳＲ－Ｙ）５８２に書き込まれた状況通知ビットも併せて読み取り、処理状況を確認する。

【０２４７】

なお、各レジスタに書き込む状況ビットは、先に図２０を参照して説明したＰＳＲ－Ｚの設定値の例と同様の設定態様が可能である。例えば初期値としては、状況ビット設定値＝０として設定され、セキュアＶＭ３５６の処理が終了し、アプリケーション実行部５２５の処理手順になった場合に状況ビット設定値＝１として設定し、次に、アプリケーション実行部５２５の処理が終了し、セキュアＶＭ３５６の処理手順になった場合に状況ビット設定値＝２として設定するなどによって、双方の処理手順に応じてプロセスの進み具合に応じた値を設定し、双方が処理シーケンスの進行度を確認可能とすることができる。なお、処理の終了や、中断の場合には、状況ビットの設定値＝０として初期値に戻す設定とする。

【０２４８】

このように、セキュアＶＭ３５６、およびアプリケーション実行部５２５は、レジスタＸ（ＰＳＲ－Ｘ）５８１と、レジスタＹ（ＰＳＲ－Ｙ）５８２を利用して相互間の処理状況通知を行い、処理シーケンスに従った確実な処理の実行を実現する。

【０２４９】

さらに、本構成においても、セキュアＶＭ３５６、およびアプリケーション実行部５２５の双方が利用可能なレジスタＸ（ＰＳＲ－Ｘ）５８１，レジスタＹ（ＰＳＲ－Ｙ）５８２を利用することで、セキュアＶＭ３５６と、アプリケーション実行部５２５との間での信頼性確認処理を実行することができる。

【０２５０】

図２４を参照して、セキュアＶＭ３５６と、アプリケーション実行部５２５との間での信頼性確認処理シーケンスについて説明する。図２４は、セキュアＶＭ３５６と、アプリケーション実行部５２５との間でチャレンジ／レスポンス処理を行うことにより、お互いに正常に動作していることを確認する処理のシーケンスを説明する図である。核ステップについて説明する。

【０２５１】

まず、ステップＳ２５１において、アプリケーション実行部５２５は、適当な値（例えば乱数）を生成し、レジスタＹ（ＰＳＲ－Ｙ）５８２に書き込む。この際、アプリケーション実行部５２５は、レジスタＹ（ＰＳＲ－Ｙ）５８２に対して処理状態を示す状況ビットを併せて書き込む。

【０２５２】

セキュアＶＭ３５６は、レジスタＹ（ＰＳＲ－Ｙ）５８２にデータが書き込まれたことを通知（ＩＮＴＲＰ＿ＰｒｅｓｅｎｔａｔｉｏｎＬａｙｅｒ）により検出し、ステップＳ２５２において、レジスタＹ（ＰＳＲ－Ｙ）５８２の書き込みデータを読み取る。この読み取りに際して、状況ビットの読み取りも実行し、処理状況の確認を行う。

【０２５３】

次に、セキュアＶＭ３５６は、レジスタＹ（ＰＳＲ－Ｙ）５８２からの読み取り値（乱数）に対して予め定められたデータ処理、例えば演算処理あるいは暗号処理などを実行し、ステップＳ２５３において、この結果値をレジスタＸ（ＰＳＲ－Ｘ）５８１に書き込む

。セキュアＶＭ３５６は、この処理に際して、セキュアＶＭ３５６は、レジスタＸ（ＰＳＲ－Ｘ）５８１に対して処理状態を示す状況ビットを併せて書き込む。

【０２５４】

ステップＳ２５４において、アプリケーション実行部５２５は、レジスタＸ（ＰＳＲ－Ｘ）５８１の書き込みデータを読み取る。この読み取りに際して、状況ビットの読み取りも実行し、処理状況の確認を行う。

【０２５５】

次に、ステップＳ２５５において、アプリケーション実行部５２５は、読み取りデータの検証を実行する。例えば、アプリケーション実行部５２５によって生成し、セキュアＶＭ３５６に通知した乱数に基づいて自ら演算あるいは暗号処理を実行した結果と比較照合を実行し、レジスタＸ（ＰＳＲ－Ｘ）５８１からの読み取り値と一致すれば、セキュアＶＭ３５６は、正当な処理を実行しているセキュアＶＭ３５６であると判断する。なお、セキュアＶＭ３５６と、アプリケーション実行部５２５が乱数に対して実行する演算処理あるいは暗号処理は共有する秘密情報に基づく処理を行なう設定とすることが好ましい。

【０２５６】

なお、図２４に示す信頼性確認処理は、複数回繰り返し実行してもよく、また、乱数発行をセキュアＶＭ３５６が実行する構成としてもよい。この信頼性確認機能を有することによって、先に説明した（４．２．４）アプリケーション実行部の使用レジスタの利用による処理例１と同様、アプリケーション実行部５２５において実行されるアプリケーションについての信頼性確認が可能となるため、アプリケーションレイヤ（ＡＶレイヤ）のロバストネス（Ｒｏｂｕｓｔｎｅｓｓ）に特に制限を設けることなく、従来通りの実装で良い点が非常に大きな利点となる。

【０２５７】

（４．３）共有メモリ空間を利用したメッセージ表示およびコンテンツ利用制御

次に、共有メモリ空間を利用したメッセージ表示およびコンテンツ利用制御処理について説明する。

【０２５８】

図２５に共有メモリ空間を利用したメッセージ表示処理、さらに、コンテンツの利用制御処理を実現する基本構成を示す。図２５に示すセキュアＶＭ３５６は、図６、図１０および図１１を参照して説明したセキュアＶＭ３５６と同様のセキュアＶＭ３５６である。すなわち、データ変換処理を実行するホスト内にバーチャルマシンとして設定されるセキュリティ情報処理部として機能するセキュアＶＭ３５６である。

【０２５９】

セキュリティ情報処理部として機能するセキュアＶＭ３５６は、図６他を参照して説明したように、命令コード情報を含むデータ変換処理プログラム３１５を情報記録媒体３１０から読み出してデータ変換処理を実行する。さらに、セキュアＶＭ３５６は、ホストアプリケーションを実行しているプレーヤ（情報処理装置）のＩＤ情報などをプレーヤ情報３５５として入力し、また、イベントハンドラ３５４からの監視情報を入力する。イベントハンドラ３５４は、セキュアＶＭ３５６によって実行される処理が正しく行なわれているか否かのエミュレータチェックや、その他のホストアプリケーションや、ホストアプリケーション実行機器としてのプレーヤ（情報処理装置）の処理、状態を監視し、処理エラー、不正処理などが検出された場合には、セキュアＶＭ３５６に監視情報を入力し、必要に応じて、例えばデータ変換処理を中止させる。

【０２６０】

本処理例では、このセキュリティ情報処理部として機能するセキュアＶＭ３５６と、アプリケーション実行部６０１の間で共有するメモリ空間６１２をメモリ６１１に設定し、共有メモリ空間６１２を利用してメッセージやコマンド、あるいはパラメータ、データ等を転送する。アプリケーション実行部６０１で実行するアプリケーションは、様々なデータ処理を実行するアプリケーション・プログラムであり、例えば図６、図１０および図１１を参照して説明したホスト３５０によるコンテンツ再生処理が実行されるＰＣ等の情報

処理装置において実行される様々なアプリケーション・プログラムである。

【０２６１】

アプリケーション・プログラムは、例えば、先に、説明した各種のメッセージ表示を実行しユーザ入力を受領するＵＩ機能を提供するＵＩ機能提供プログラムや、あるいは、情報記録媒体に格納された例えばＪａｖａ（登録商標）やＨＤＭＶ対応のコンテンツを実行するアプリケーション・プログラムなどである。なお、このアプリケーション・プログラムは、情報処理装置がハードディスクなどに記憶して予め保持していたプログラム、あるいは情報記録媒体から読み出されたプログラムのいずれでもよい。

【０２６２】

図２５に示す共有メモリ空間６１２は、セキュアＶＭ３５６と、アプリケーション実行部６０１の双方が書き込み、読み取り可能なメモリ空間として利用される。従って、図１５～図２４を参照して説明した各種の処理と同様の処理が、レジスタの代わりにメモリ空間を適用することで実現される。すなわち、先にレジスタ適用処理として説明した以下の各種の処理、

（ａ）図１６を参照して説明したレジスタを利用したＵＩ機能提供アプリケーションの実行

（ｂ）図１７を参照して説明したレジスタ利用およびタイトル切り替えによるＵＩ機能提供

（ｃ）図１８を参照して説明したレジスタ利用によるコンテンツ利用制御処理

（ｄ）図１９～図２４を参照して説明したレジスタ利用処理

これらの処理を、共有メモリ空間６１２を介してメッセージやコマンド、あるいはパラメータ、データをセキュアＶＭ３５６と、アプリケーション実行部６０１間で転送することで実現される。

【０２６３】

メモリ空間をデータ書き込み領域として利用することで、レジスタを利用する場合に比較して、書き込みデータサイズを大きく設定でき、利用範囲が広がるというメリットがある。例えばセキュアＶＭ３５６が生成したデータを共有メモリに書き込むことで、アプリケーション実行部６０１に提供することも可能であり、逆にアプリケーション実行部６０１の生成データをセキュアＶＭ３５６に渡す処理も容易に実現され、セキュアＶＭ３５６の処理と、アプリケーション実行部６０１の処理との共同のデータ処理を行なうこともできる。

【０２６４】

（４．４）オーサリングプロセスについて

上述したレジスタまたはメモリ空間を適用して、セキュアＶＭとアプリケーション間においてデータやパラメータの入出力を行なう構成を実現するためには、アプリケーションレイヤにおいて実行するアプリケーションは、定期的なレジスタ参照あるいはメモリ参照処理を実行する処理ルーチンを予め設定したプログラムとして編集（オーサリング）することが好ましい。

【０２６５】

先に、図１７を参照して説明したセキュアＶＭによるタイトル変更を許容した構成とする場合には、セキュアＶＭによって指定されるタイトルを持つアプリケーションのみが、定期的なレジスタ参照あるいはメモリ参照を実行するプログラムとすればよいが、セキュアＶＭによるタイトル変更を許容しない構成では、アプリケーションレイヤで実行するすべてのアプリケーションは、基本的にすべて定期的なレジスタ参照あるいはメモリ参照処理を実行する処理ルーチンを予め設定したプログラムとして編集（オーサリング）することが必要となる。

【０２６６】

前述したように、アプリケーションレイヤにおいて実行されるプログラムは、情報記録媒体に記録された例えばＪａｖａ（登録商標）やＨＤＭＶ対応のコンテンツを実行するアプリケーション・プログラムであり、これらのコンテンツについて、定期的なレジスタ参

照あるいはメモリ参照処理を実行する処理ルーチンを予め設定したプログラムとして編集（オーサリング）することで、上記の処理が可能となる。

【０２６７】

これらのコンテンツのオーサリングプロセスおよび情報記録媒体製造プロセスについて、図２６、図２７を参照して説明する。図２６は、セキュアＶＭによるタイトル切り替えが許容されない場合のコンテンツ編集（オーサリング）プロセスについて説明する図である。

【０２６８】

アプリケーションは、アプリケーションレイヤにおいて実行されるＪａｖａ（登録商標）やＨＤＭＶ対応のコンテンツとしてのアプリケーション・プログラムと、セキュアＶＭが読み取って実行する命令コード情報としてのコンテンツコードを含むコンテンツとして生成される。ステップＳ３０１は、このアプリケーションおよびコンテンツコードの開発・検証プロセスである。

【０２６９】

このステップＳ３０１において生成されるアプリケーションは、定期的なレジスタ参照あるいはメモリ参照処理を実行する処理ルーチンを予め設定したプログラムとして編集（オーサリング）される。またコンテンツコードは、セキュアＶＭによるメッセージ出力や、定期的なパラメータ出力の実行を定義した命令コードを含むものとして設定される。

【０２７０】

このステップＳ３０１において生成されたアプリケーションおよびコンテンツコードは、ステップＳ３０２において、必要に応じて暗号化が施された後、ステップＳ３０３においてディスクに書き込まれディスクが製造される。ステップＳ３０３のディスク製造プロセスは、ディスク原盤の製造およびスタンパプロセスを含んでいる。

【０２７１】

これらの処理によって、情報記録媒体に記録されるコンテンツは、アプリケーション・プログラムおよびバーチャルマシンによって実行されるコード情報を含むコンテンツとなり、アプリケーション・プログラムは、定期的なレジスタまたはメモリ参照処理の実行ルーチンを含むプログラムとして設定され、コード情報は、セキュリティチェック結果として取得するエラーコードをレジスタまたはメモリに書き込む処理の実行命令を含む情報として構成される。

【０２７２】

このような情報記録媒体格納コンテンツは、図１５～図２５を参照して説明した各種の処理を実行可能なコンテンツとされる。

【０２７３】

図２７は、セキュアＶＭによるタイトル切り替えを許容した場合のコンテンツオーサリングプロセスを示している。図１７を参照して説明したセキュアＶＭによるタイトル変更を許容した構成とする場合には、セキュアＶＭによって指定されるタイトルを持つアプリケーションのみが、定期的なレジスタ参照あるいはメモリ参照を実行するプログラムとすればよい。

【０２７４】

従って、通常のアプリケーションについては、定期的なレジスタ参照あるいはメモリ参照を実行するルーチンを含ませたプログラムとして設定する必要がなく、自由にアプリケーションを開発することができる。特定のアプリケーションのみについて、定期的なレジスタ参照あるいはメモリ参照を実行するルーチンを含ませたプログラムとして設定すればよい。

【０２７５】

図２７に示すように、ステップＳ３２１におけるアプリケーションの開発・検証プロセスとステップＳ３２２におけるコンテンツコードの開発・検証プロセスを分離し、基本的に、アプリケーションの開発・検証プロセスは、コンテンツコードにとらわれることなく、自由に開発することができる。セキュアＶＭによるタイトル切り替え先のアプリケーシ

ョンのみを、図２６に示すプロセスに従って編集すればよい。

【０２７６】

図２７のプロセスでは、ステップＳ３２１におけるアプリケーションの開発・検証プロセスの後に、ステップＳ３２２において、コンテンツコードの開発・検証プロセスを実行することができる。その後、ステップＳ３２３において、必要に応じて暗号化が施された後、ステップＳ３２４においてディスクに書き込まれディスクが製造される。ステップＳ３２４のディスク製造プロセスは、ディスク原盤の製造およびスタンパプロセスを含んでいる。

【０２７７】

アプリケーションの開発・検証プロセスと、コンテンツコードの開発・検証プロセスは、運用上、分かれていることが多く、現実的には、図２７に示すプロセスに従う構成とすることが好ましく、セキュアＶＭによるタイトル切り替えを許容した構成として、特定のアプリケーションのみを定期的なレジスタ参照あるいはメモリ参照を実行するルーチンを含ませたプログラムとして設定することで、その他の通常アプリケーションについては、自由な開発を可能とすることができる。

【０２７８】

［５．情報処理装置の構成］

次に、図２８を参照して、ホストとしてのアプリケーションを実行する情報処理装置のハードウェア構成例について説明する。情報処理装置８００は、ＯＳやコンテンツ再生または記録アプリケーション・プログラム、相互認証処理プログラムなどの各種プログラムに従ったデータ処理を実行するＣＰＵ８０９、プログラム、パラメータ等の記憶領域としてのＲＯＭ８０８、メモリ８１０、デジタル信号を入出力する入出力Ｉ／Ｆ８０２、アナログ信号を入出力し、Ａ／Ｄ，Ｄ／Ａコンバータ８０５を持つ入出力Ｉ／Ｆ８０４、ＭＰＥＧデータのエンコード、デコード処理を実行するＭＰＥＧコーデック８０３、ＴＳ（Transport Stream）・ＰＳ(Program Stream)処理を実行するＴＳ・ＰＳ処理手段８０６、相互認証、暗号化コンテンツの復号処理など各種の暗号処理を実行する暗号処理手段８０７、ハードディスクなどの記録媒体８１２、記録媒体８１２の駆動、データ記録再生信号の入出力を行なうドライブ８１１を有し、バス８０１に各ブロックが接続されている。

【０２７９】

情報処理装置（ホスト）８００は、例えばＡＴＡＰＩ－ＢＵＳ等の接続バスによってドライブと接続されている。変換テーブル、コンテンツなどをデジタル信号用入出力Ｉ／Ｆ８０２を介して入出力される。暗号化処理、復号処理は、暗号化処理手段８０７によって、例えば、ＡＥＳアルゴリズムなどを適用して実行される。

【０２８０】

なお、コンテンツ再生あるいは記録処理を実行するプログラムは例えばＲＯＭ８０８内に保管されており、プログラムの実行処理中は必要に応じて、パラメータ、データの保管、ワーク領域としてメモリ８１０を使用する。

【０２８１】

ＲＯＭ８０８または記録媒体８１２には、例えば、管理センタの公開鍵、ホスト対応秘密鍵、ホスト対応の公開鍵証明書、さらに、リボケーションリストとしてのドライブＣＲＬなどが格納される。

【０２８２】

コンテンツ再生処理に際しては、前述したセキュアＶＭ３５６が取得したセキュリティチェック情報に基づいて、様々なメッセージ表示が実行される。

【０２８３】

以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、特許請求の範囲の欄を参酌すべきである。

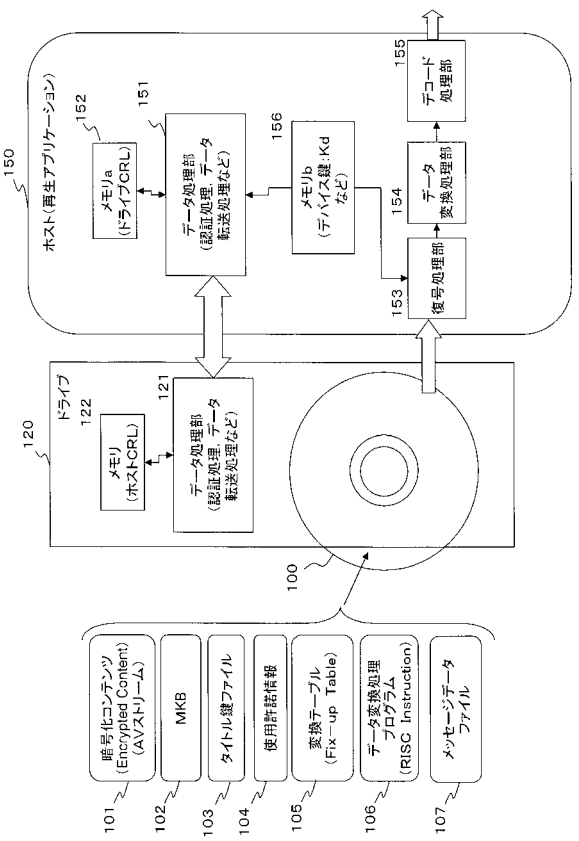
【０２８４】
なお、明細書中において説明した一連の処理はハードウェア、またはソフトウェア、あるいは両者の複合構成によって実行することが可能である。ソフトウェアによる処理を実行する場合は、処理シーケンスを記録したプログラムを、専用のハードウェアに組み込まれたコンピュータ内のメモリにインストールして実行させるか、あるいは、各種処理が実行可能な汎用コンピュータにプログラムをインストールして実行させることが可能である。
【０２８５】
例えば、プログラムは記録媒体としてのハードディスクやＲＯＭ（Read Only Memory）に予め記録しておくことができる。あるいは、プログラムはフレキシブルディスク、ＣＤ－ＲＯＭ(Compact Disc Read Only Memory)，ＭＯ(Magneto optical)ディスク，ＤＶＤ(Digital Versatile Disc)、磁気ディスク、半導体メモリなどのリムーバブル記録媒体に、一時的あるいは永続的に格納（記録）しておくことができる。このようなリムーバブル記録媒体は、いわゆるパッケージソフトウエアとして提供することができる。
【０２８６】
なお、プログラムは、上述したようなリムーバブル記録媒体からコンピュータにインストールする他、ダウンロードサイトから、コンピュータに無線転送したり、ＬＡＮ(Local Area Network)、インターネットといったネットワークを介して、コンピュータに有線で転送し、コンピュータでは、そのようにして転送されてくるプログラムを受信し、内蔵するハードディスク等の記録媒体にインストールすることができる。
【０２８７】
なお、明細書に記載された各種の処理は、記載に従って時系列に実行されるのみならず、処理を実行する装置の処理能力あるいは必要に応じて並列的にあるいは個別に実行されてもよい。また、本明細書においてシステムとは、複数の装置の論理的集合構成であり、各構成の装置が同一筐体内にあるものには限らない。
【産業上の利用可能性】
【０２８８】
以上、説明したように、本発明の一実施例の構成によれば、情報記録媒体の格納コンテンツ再生において、正当なコンテンツ利用権に基づくコンテンツ利用を許容する構成とし、さらに、セキュリティチェックに基づいて不正なコンテンツ利用であると判定された場合などにおいて、コンテンツ再生の停止された理由などメッセージ表示や、表示メッセージに対するユーザ応答の受領などを可能としたので、ユーザに対して状況を説明する処理や、ユーザからの確認や対処を受け付けることが可能となる。
【０２８９】
また、本発明の一実施例構成によれば、Ｊａｖａ（登録商標）やＨＤＭＶコンテンツなどの小型のコンテンツについても、これらのコンテンツを実行するアプリケーション実行部と、セキュリティ情報処理部としてのセキュアＶＭ間でレジスタやメモリを介してデータを転送することで、コンテンツの利用制御を行なうことが可能となる。
【図面の簡単な説明】
【０２９０】
【図１】情報記録媒体の格納データおよびドライブ装置、情報処理装置の構成および処理について説明する図である。
【図２】情報記録媒体の格納コンテンツに対して設定するコンテンツ管理ユニットの設定例について説明する図である。
【図３】情報記録媒体の格納コンテンツに対して設定するコンテンツ管理ユニットとユニット鍵との対応について説明する図である。
【図４】情報記録媒体の格納コンテンツに対して設定されるディレクトリ構成について説明する図である。
【図５】変換テーブルおよびデータ変換処理プログラムのディレクトリ構成について説明する図である。

【図６】コンテンツ再生処理の処理例１を示す図である。
【図７】ドライブとホスト間の相互認証処理シーケンスを説明する図である。
【図８】コンテンツ再生の際に実行する変換データの適用処理について説明する図である。
【図９】情報記録媒体に記録されるデータ変換テーブルのデータ構成について説明する図である。
【図１０】コンテンツ再生処理の処理例２を示す図である。
【図１１】表示部に対するメッセージ提示をセキュアＶＭによって実行する構成を説明する図である。
【図１２】メッセージデータファイルのディレクトリ設定例について説明する図である。
【図１３】ＯＳＤ機能によるメッセージ表示処理において適用するＯＳＤ呼び出し（ＣＡＬＬ＿ＯＳＤ）に対応するコマンドの構成について説明する図である。
【図１４】表示部に対するメッセージ表示例を示す図である。
【図１５】レジスタを利用したメッセージ表示処理、さらに、コンテンツの利用制御処理を実現する基本構成を示す図である。
【図１６】レジスタを利用したメッセージ表示処理の処理シーケンスを説明する図である。
【図１７】タイトル切り替え処理を適用し、レジスタを利用したメッセージ表示処理の処理シーケンスを説明する図である。
【図１８】レジスタを利用したコンテンツの利用制御処理の処理シーケンスを説明する図である。
【図１９】アプリケーション実行部の使用レジスタの利用によるセキュアＶＭとアプリケーション実行部間のデータ転送処理構成例を説明する図である。
【図２０】アプリケーション実行部の使用レジスタの利用によるセキュアＶＭとアプリケーション実行部間のデータ転送処理シーケンスを説明する図である。
【図２１】セキュアＶＭと、アプリケーション実行部との間で実行する信頼性確認処理シーケンスについて説明する図である。
【図２２】アプリケーション実行部の使用レジスタの利用によるセキュアＶＭとアプリケーション実行部間のデータ転送処理構成例を説明する図である。
【図２３】アプリケーション実行部の使用レジスタの利用によるセキュアＶＭとアプリケーション実行部間のデータ転送処理シーケンスを説明する図である。
【図２４】セキュアＶＭと、アプリケーション実行部との間で実行する信頼性確認処理シーケンスについて説明する図である。
【図２５】共有メモリ空間を利用したメッセージ表示処理、さらに、コンテンツの利用制御処理を実現する基本構成を示す図である。
【図２６】コンテンツのオーサリングプロセス、情報記録媒体製造プロセスについて説明する図である。
【図２７】コンテンツのオーサリングプロセス、情報記録媒体製造プロセスについて説明する図である。
【図２８】ホストとしてのアプリケーションを実行する情報処理装置のハードウェア構成例について説明する図である。
【符号の説明】
【０２９１】
１００　情報記録媒体
１０１　暗号化コンテンツ
１０２　ＭＫＢ
１０３　タイトル鍵ファイル
１０４　使用許諾情報
１０５　変換テーブル
１０６　データ変換処理プログラム

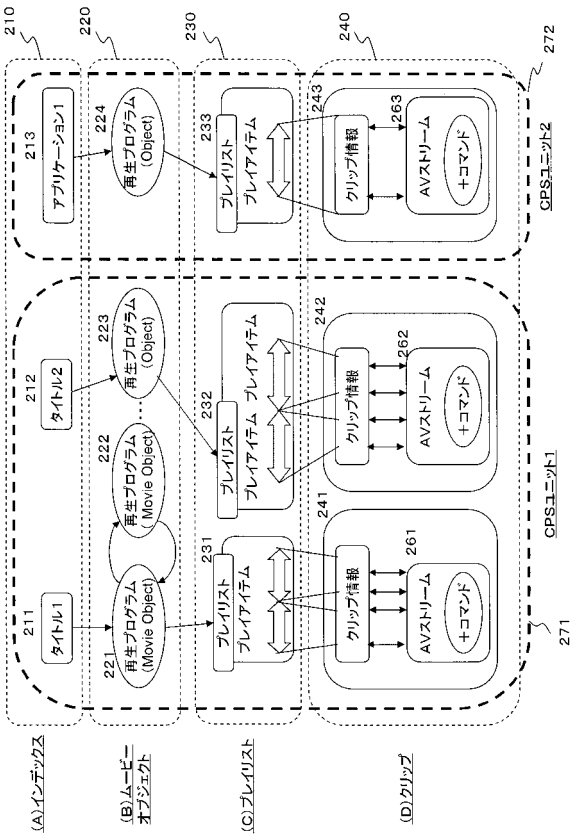
１０７　メッセージデータファイル
１２０　ドライブ
１２１　データ処理部
１２２　メモリ
１５０　ホスト
１５１　データ処理部
１５２　メモリａ
１５３　復号処理部
１５４　データ変換処理部
１５５　デコード処理部
１５６　メモリｂ
２１０　インデックス
２２０　ムービーオブジェクト
２３０　プレイリスト
２４０　クリップ
２６１，２６２，２６３　ＡＶストリーム
２７１，２７２　コンテンツ管理ユニット（ＣＰＳユニット）
２８１　データ部
３１０　情報記録媒体
３１１　ＭＫＢ
３１２　タイトル鍵ファイル
３１３　暗号化コンテンツ
３１４　変換テーブル
３１５　データ変換処理プログラム
３３０　ドライブ
３５０　ホスト
３５１　デバイス鍵
３５２　トラックバッファ
３５３　平文ＴＳバッファ
３５４　イベントハンドラ
３５５　プレーヤ情報
３５６　セキュアＶＭ
３９１　ＵＩ処理部
３９２　表示部
４０１～４０４　メッセージデータファイル
４１１　コマンド
５０１　アプリケーション
５１１，５１２　レジスタ
５２１　ＵＩ機能提供アプリケーション実行部
５２２　アプリケーション実行部
５２３　アプリケーション実行部
５２４　アプリケーション実行部
５２５　アプリケーション実行部
５７１～５７３　レジスタ（ＰＳＲ）
５８１～５８２　レジスタ（ＰＳＲ）
６０１　アプリケーション
８００　情報処理装置
８０１　バス
８０２　入出力Ｉ／Ｆ
８０３　ＭＰＥＧコーデック

８０４　入出力Ｉ／Ｆ
８０５　Ａ／Ｄ，Ｄ／Ａコンバータ
８０６　ＴＳ・ＰＳ処理手段
８０７　暗号処理手段
８０８　ＲＯＭ
８０９　ＣＰＵ
８１０　メモリ
８１１　ドライブ
８１２　記録媒体

【図１】



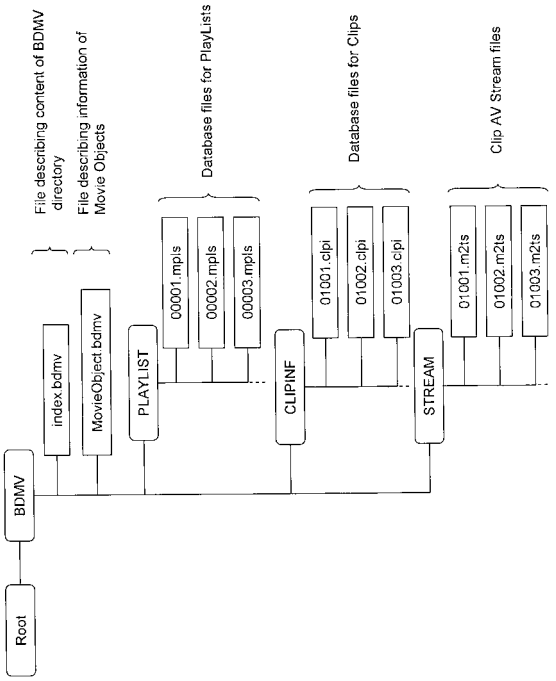
【図２】



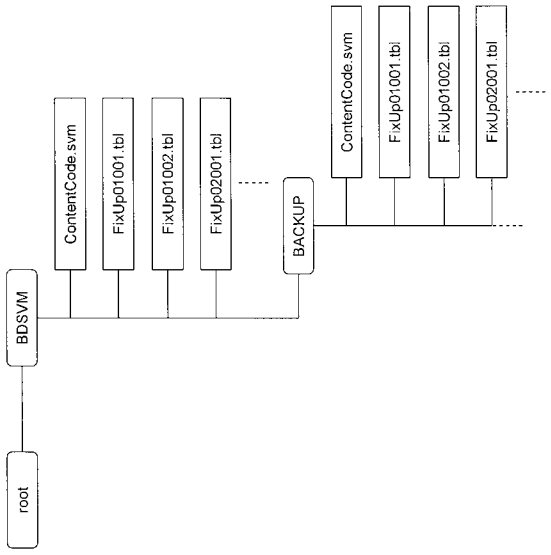
【図３】


生成可能な
タイトル鍵(CPSユニット鍵)
コンテンツ管理ユニット(CPS)設定単位
コンテンツ管理ユニット識別子(CPSユニットID)
タイトル鍵(CPSユニット鍵)
タイトル1
CPS1
Kt1
タイトル2
CPS1
Kt1
アプリケーション1
CPS2
Kt2
アプリケーション2
CPS3
Kt3
データグループ1
CPS4
Kt4
データグループ2
CPS5
Kt5
新規データ1
CPSa
Kta
新規データ2
CPSb
Ktb
281

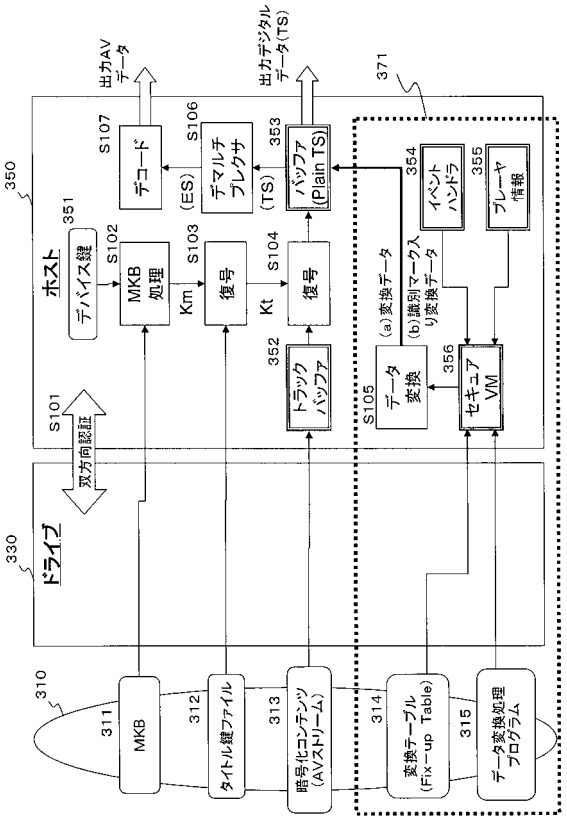
【図４】


Root
BDMV
index.bdmv
MovieObject.bdmv
PLAYLIST
CLIPINF
STREAM
00001.mpls
00002.mpls
00003.mpls
01001.clpi
01002.clpi
01003.clpi
01001.m2ts
01002.m2ts
01003.m2ts
File describing content of BDMV directory
File describing information of Movie Objects
Database files for PlayLists
Database files for Clips
Clip AV Stream files

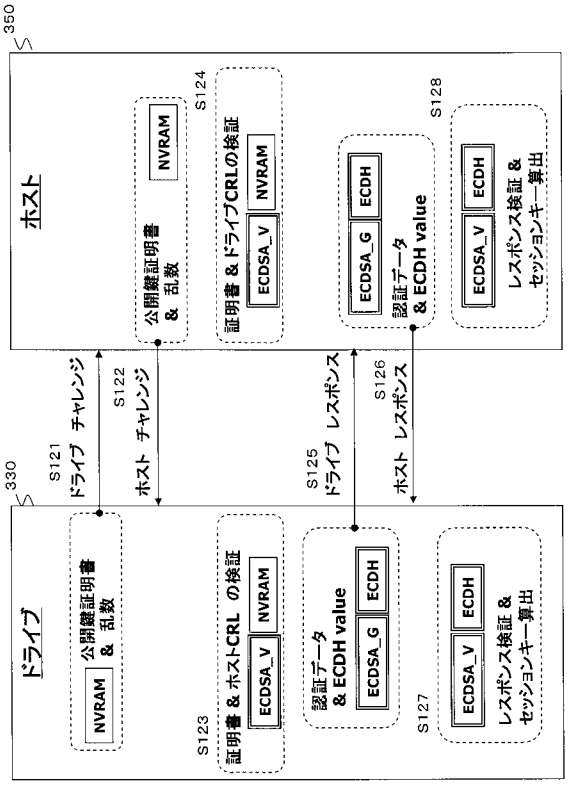
【図５】


root
BDSVM
BACKUP
ContentCode.svm
FixUp01001.tbl
FixUp01002.tbl
FixUp02001.tbl
ContentCode.svm
FixUp01001.tbl
FixUp01002.tbl
FixUp02001.tbl

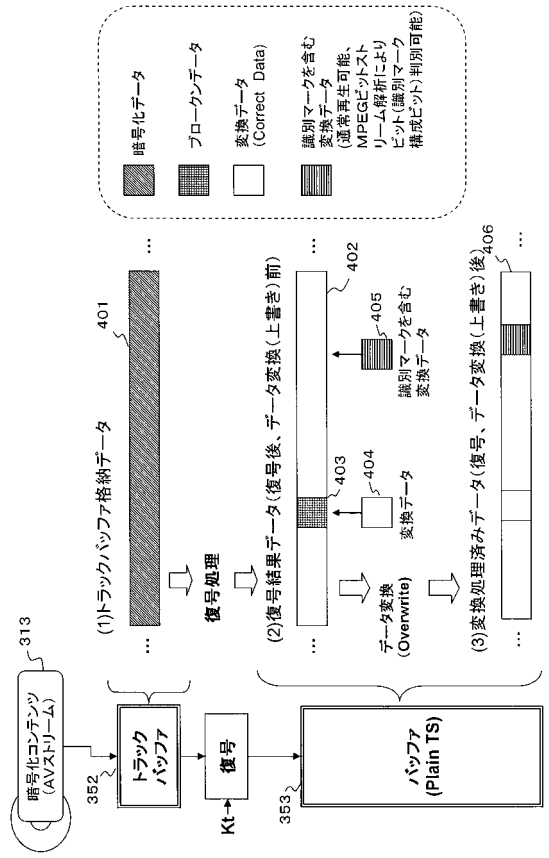
【図６】


310
311 MKB
312 タイトル鍵ファイル
313 暗号化コンテンツ(AVストリーム)
314 変換テーブル(Fix-up Table)
315 データ変換処理プログラム
330 ドライブ
S101 双方向認証
350 ホスト
351 デバイス鍵
S102 MKB処理
S103 復号
Km
S104 復号
Kt
352 トラックバッファ
S105 データ変換
(a)変換データ
(b)識別マークより変換データ
356 セキュアVM
354 イベントハンドラ
355 プレーヤ情報
371
353 バッファ(Plain TS)
(TS)
S106 デマルチプレクサ
(ES)
S107 デコード
出力AVデータ
出力デジタルデータ(TS)

【図７】



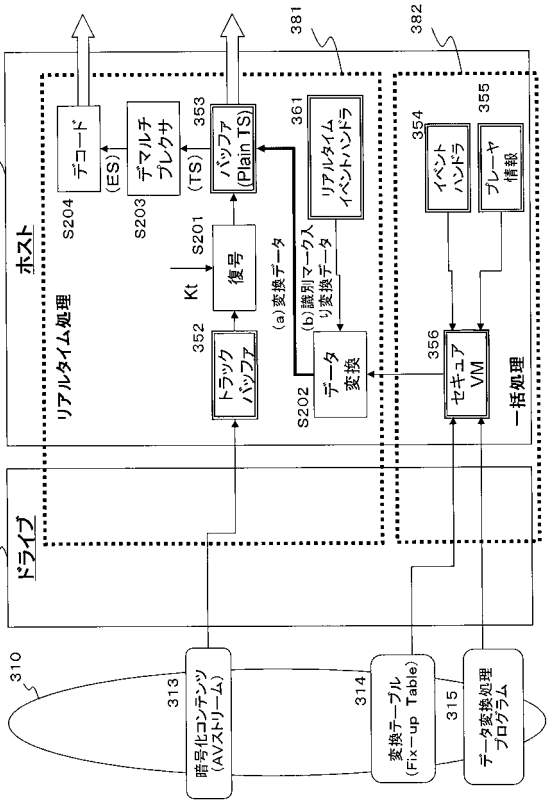
【図８】



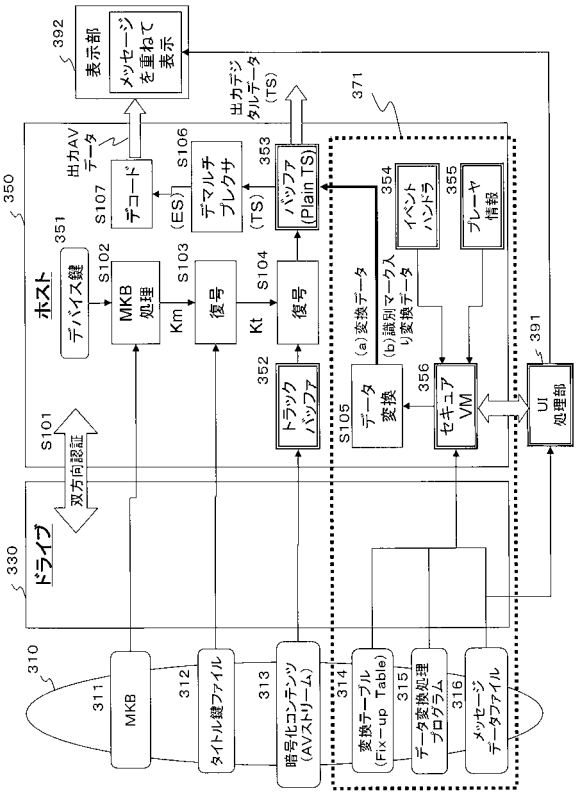
【図９】

FixUpTable() {	Bits	内容 (Description)
Number of FixUpEntry	32	変換データエントリ数 (Number of FixUpEntry)
FixUpEntry Length	8	1変換データエントリのバイト数 (Byte Length of one FixUpEntry() = (N+6))
reserved	8	リザーブ
FixUpEntry(){		
SPN	32	ソースパケットナンバー: 変換データ書き込みパケットのAVストリームファイルの開始位置からのパケットナンバー (Absolute Transformed Packet Number from the beginning of AV Stream File)
Byte Offset	8	パケット中の変換データ書き込み開始位置を示すバイトオフセット (Start byte position of transformed data in the packet)
player_id_bit_position	8	識別マーク(プレイヤーID)のビット位置 (Indicate bit position of Player ID for forensic)
FixUp Data	8xN	変換上書きデータ (Value to be overwritten (N byte is transformed in one TS Packet))
}		

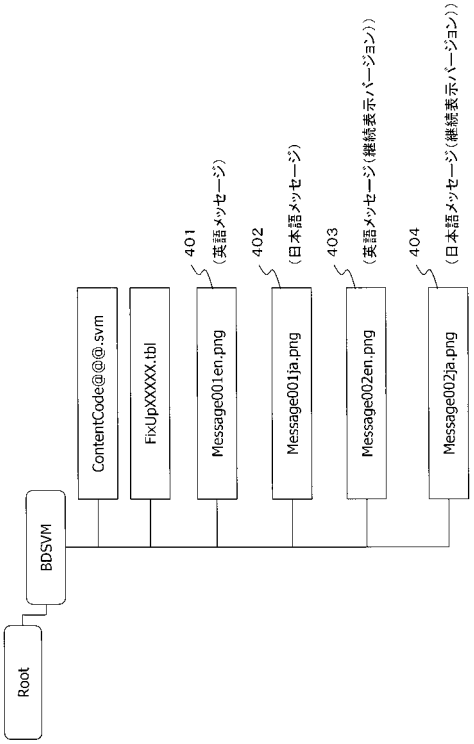
【図１０】



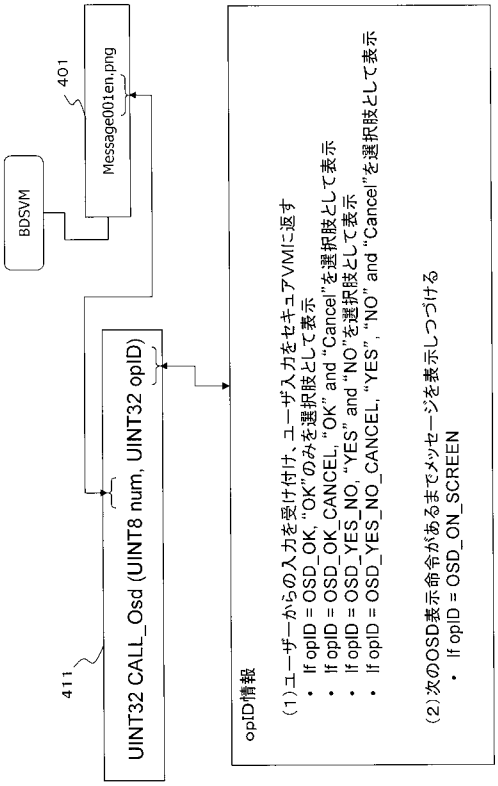
【図１１】



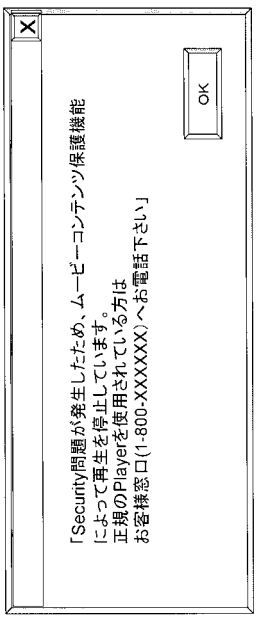
【図１２】



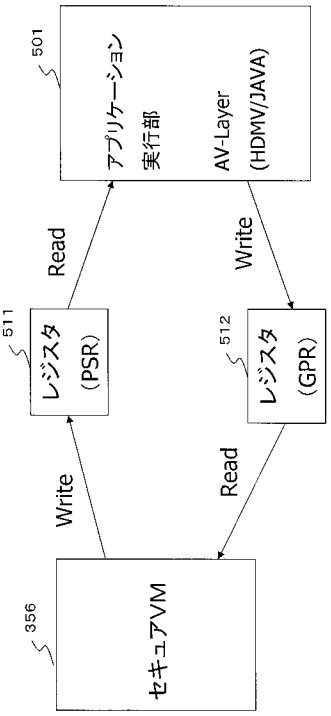
【図１３】



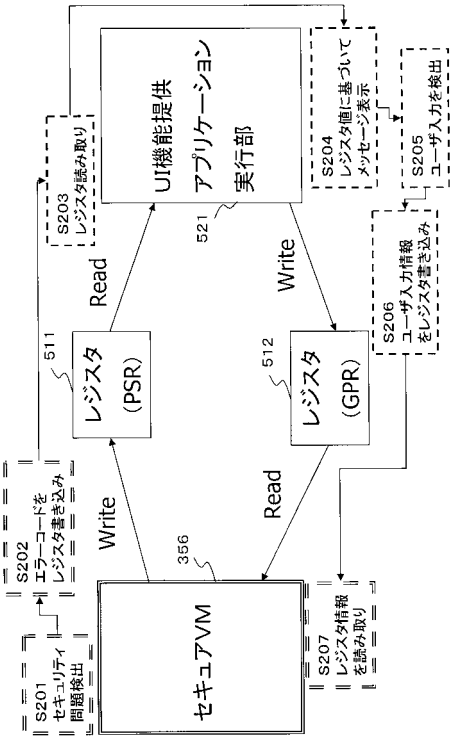
【図１４】



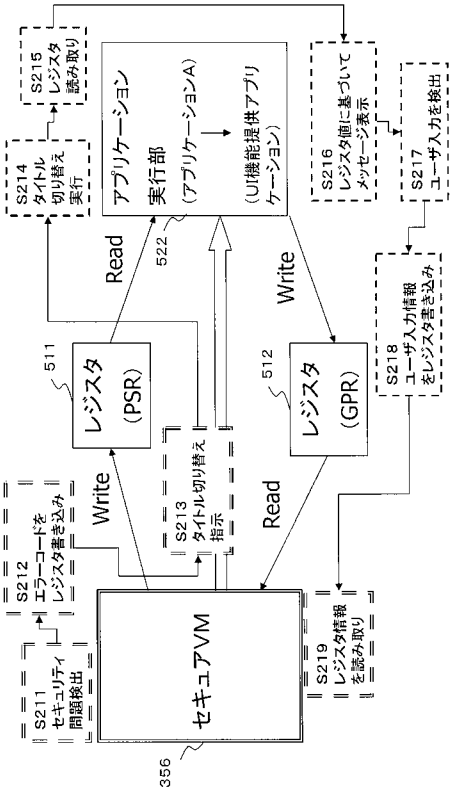
【図１５】



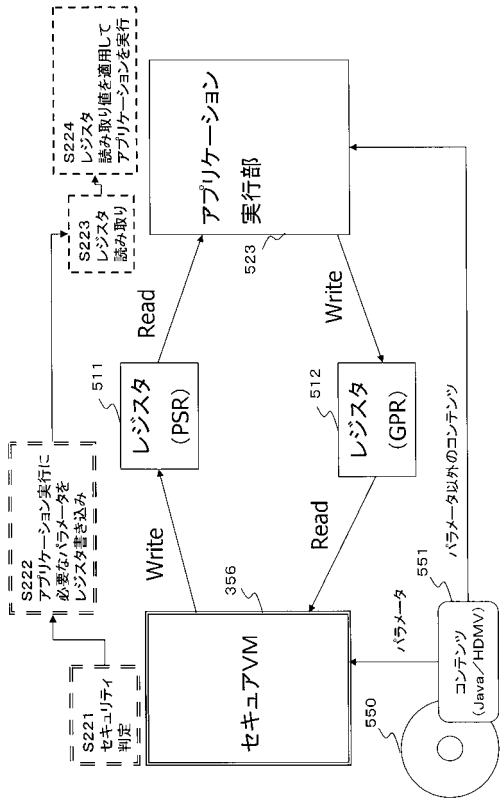
【図１６】



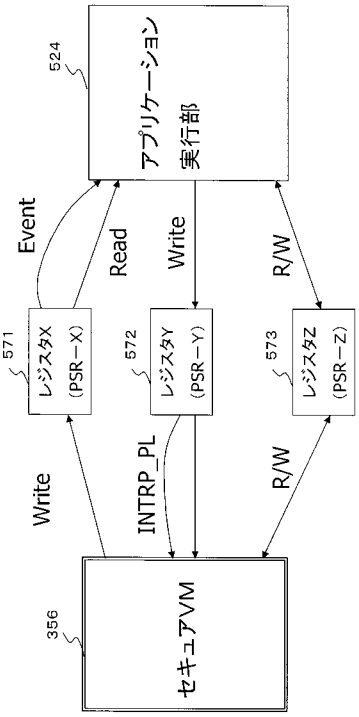
【図１７】



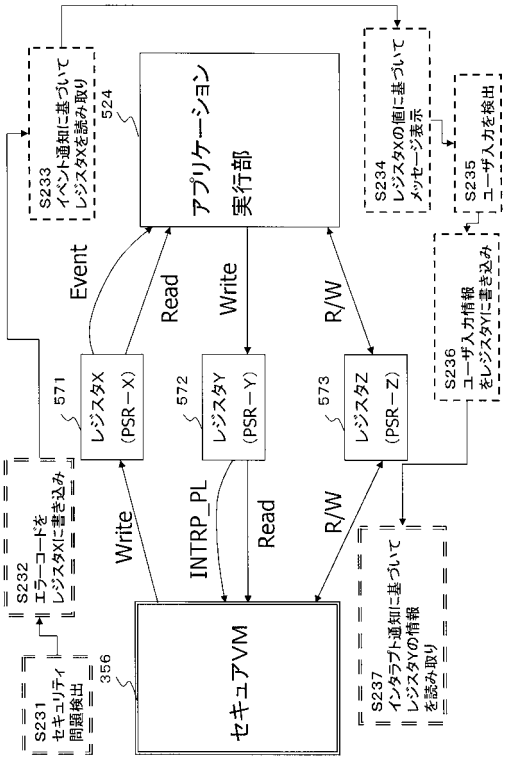
【図１８】



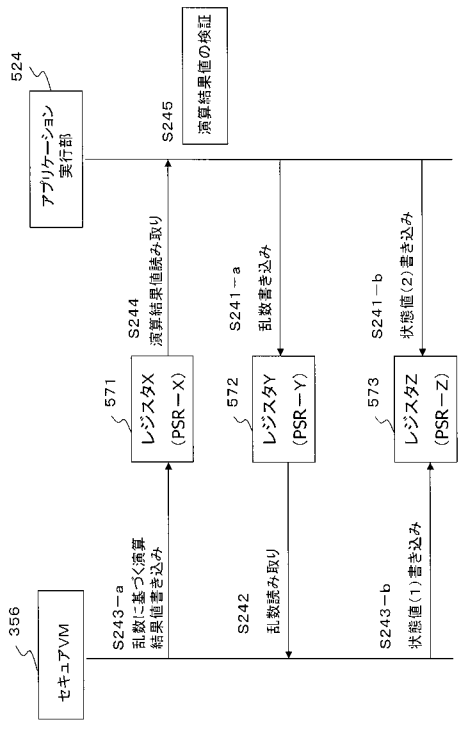
【図１９】



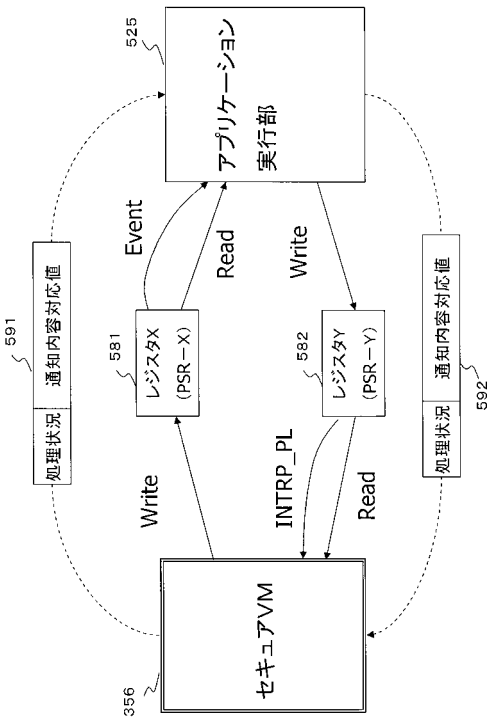
【図２０】



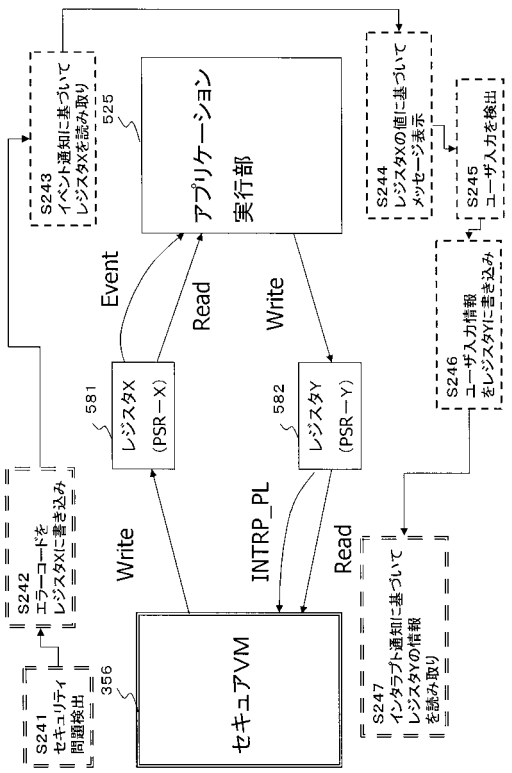
【図２１】



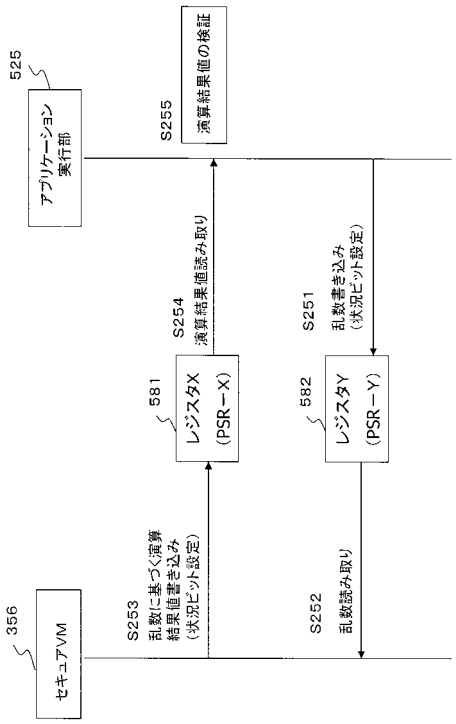
【図２２】



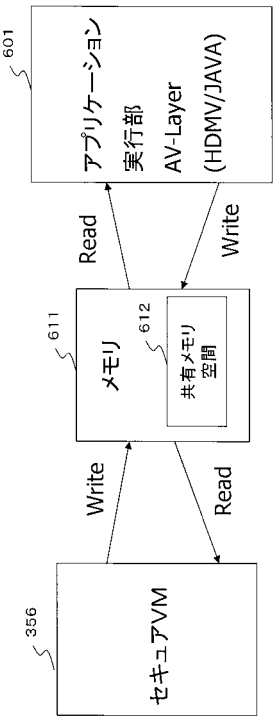
【図２３】



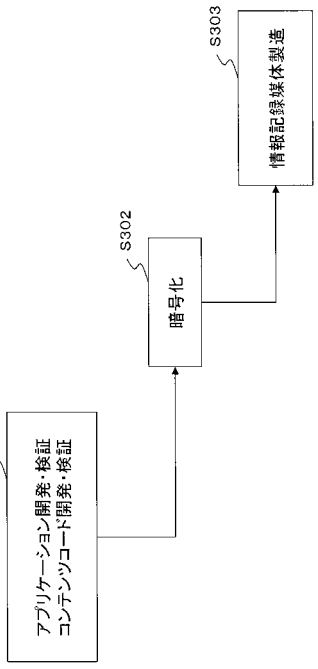
【図２４】



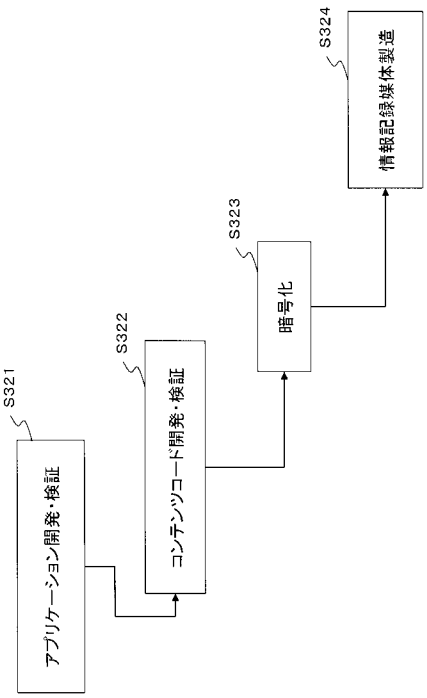
【図２５】



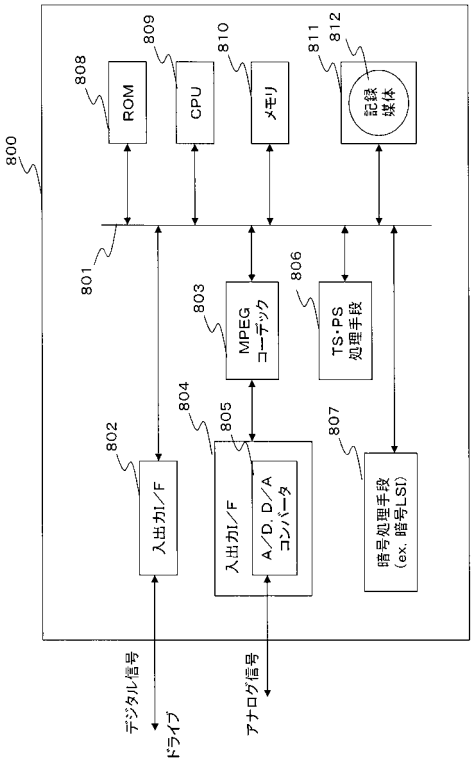
【図２６】



【図２７】


S321
アプリケーション開発・検証
S322
コンテンツコード開発・検証
S323
暗号化
S324
情報記録媒体製造

【図２８】


800
801
808
ROM
809
CPU
810
メモリ
811
812
記録媒体
803
MPEGコーデック
806
TS・PS処理手段
802
入出力I／F
804
805
入出力I／F
A／D、D／Aコンバータ
807
暗号処理手段
(ex. 暗号LSI)
デジタル信号
ドライブ
アナログ信号

フロントページの続き

(56)参考文献 国際公開第２００７／０００９８７（WO，Ａ１）
特開２０００－１６３８０３（ＪＰ，Ａ）
特開２００２－２５１２４０（ＪＰ，Ａ）
特開平１０－０４１９３４（ＪＰ，Ａ）
国際公開第２００５／０１７６５４（WO，Ａ１）
特開平０６－０４４０２６（ＪＰ，Ａ）
特開２００２－３４４６２３（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ ２１／２４
Ｈ０４Ｎ ５／９１