(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2006-209690
(P2006-209690A)
(43)公開日　平成18年8月10日(2006.8.10)

| (51)Int.Cl. | | F I | | | テーマコード（参考） |
|---|---|---|---|---|---|
| G06F 21/22 | (2006.01) | G06F | 9/06 | 660G | 5B017 |
| G06F 21/24 | (2006.01) | G06F | 12/14 | 560A | 5B076 |
| G09C 1/00 | (2006.01) | G09C | 1/00 | 660D | 5B176 |
| G06F 9/445 | (2006.01) | G06F | 9/06 | 610K | 5B276 |
| H04L 9/10 | (2006.01) | H04L | 9/00 | 621Z | 5J104 |

審査請求 未請求　請求項の数 14　ＯＬ　（全 19 頁）

(21)出願番号　特願2005-24358(P2005-24358)
(22)出願日　平成17年1月31日(2005.1.31)

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番３５号
(74)代理人　100082740
弁理士　田辺　恵基
(72)発明者　武田　大輔
東京都品川区北品川６丁目７番３５号ソニー株式会社内

Ｆターム(参考)　5B017 AA07 AA08 BA07 BA09 BB04 BB09 CA04 CA15
5B076 AA01 AA06 CA07 EB01 FB06
5B176 AA01 AA06 CA07 EB01
5B276 FB06
5J104 AA08 AA12 AA46 JA03 NA02 NA27

(54)【発明の名称】データ処理回路

(57)【要約】　（修正有）
【課題】コストを抑えつつ、セキュリティを向上し得るデータ処理回路を実現する。
【解決手段】ＰＣＩ－Ｌｏｃａｌブリッジ８Ｂが、モジュール外から供給されるプロセッサ起動コマンドに応じて、自身に記憶してある初期設定ファームを汎用プロセッサ８Ａの実行開始アドレスに書き込んでから汎用プロセッサ８Ａを起動させるようにしたことにより、例えば、不正なファームウェアがこの実行開始アドレスに書き込まれていたとしても、汎用プロセッサ８Ａが起動する際には、この不正なファームウェアを初期設定ファームで上書き消去するので、汎用プロセッサ８Ａを不正に起動させる不正起動攻撃を確実に防ぐことができ、またこのような初期設定ファームの書き込み及び汎用プロセッサ８Ａの起動を、ＰＣＩ－Ｌｏｃａｌブリッジ８Ｂが担うようにしたことにより、汎用のプロセッサを用いることができる。
【選択図】図４

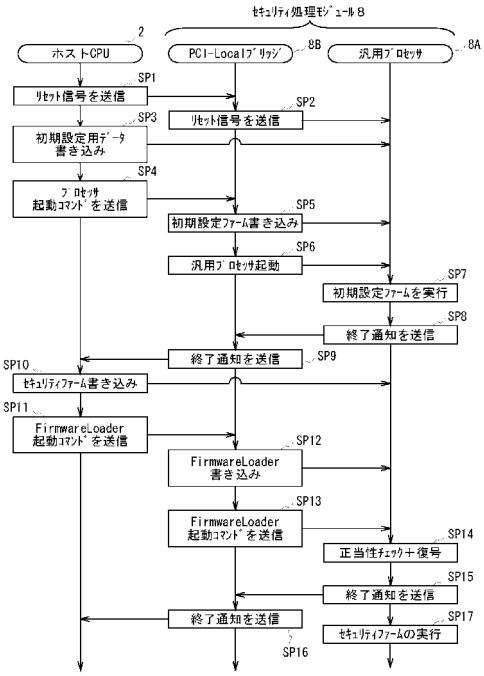


図４　セキュリティ処理の実行手順

【特許請求の範囲】
【請求項１】
アクセス可能なメモリに書き込まれるファームウェアを実行する汎用プロセッサと、
第１のファームウェアを記憶すると共に、上記汎用プロセッサと外部とを中継して、外部からの命令に応じて上記汎用プロセッサを制御する中継回路と
を具え、
上記中継回路は、
外部から供給される第１の起動命令に応じて、上記第１のファームウェアを上記メモリの実行開始アドレスから書き込み、続いて上記汎用プロセッサに対して上記第１の起動命令に応じた第２の起動命令を出力し、
上記汎用プロセッサは、
上記第２の起動命令に応じて起動すると共に、上記実行開始アドレスに書き込まれた上記第１のファームウェアを実行する
ことを特徴とするデータ処理回路。
【請求項２】
上記メモリには、上記汎用プロセッサを初期設定するための初期設定用データが書き込まれ、
上記汎用プロセッサは、
上記第２の起動命令に応じて起動すると共に、上記実行開始アドレスに書き込まれた上記第１のファームウェアを実行することにより、上記初期設定用データに基づいて初期設定を行う
ことを特徴とする請求項１に記載のデータ処理回路。
【請求項３】
上記メモリには、第２のファームウェアが書き込まれ、
上記中継回路は、
上記第２のファームウェアの正当性を検出して実行するための実行用プログラムを記憶し、外部から供給される第３の起動命令に応じて、上記実行用プログラムを上記メモリの上記第２のファームウェアが書き込まれた位置とは異なる位置に書き込み、続いて上記汎用プロセッサに対して上記第３の起動命令に応じた第４の起動命令を出力し、
上記汎用プロセッサは、
上記第４の起動命令に応じて、上記メモリに書き込まれた上記実行用プログラムを実行することにより、上記メモリに書き込まれた上記第２のファームウェアの正当性を検出し、当該検出結果に応じて、当該第２のファームウェアを実行する
ことを特徴とする請求項２に記載のデータ処理回路。
【請求項４】
上記中継回路は、
外部のバスと上記汎用プロセッサのバスとをブリッジするブリッジ回路である
ことを特徴とする請求項３に記載のデータ処理回路。
【請求項５】
上記実行用プログラムは、
暗号化された上記第２のファームウェアを復号する機能を有し、
上記汎用プロセッサは、
上記第４の起動命令に応じて、上記メモリに書き込まれた上記実行用プログラムを実行することにより、上記メモリに書き込まれた暗号化された上記第２のファームウェアの正当性を検出し、当該検出結果に応じて、当該暗号化された第２のファームウェアを復号して実行する
ことを特徴とする請求項３に記載のデータ処理回路。
【請求項６】
制御部と、
アクセス可能なメモリに書き込まれるファームウェアを実行する汎用プロセッサと、

第１のファームウェアを記憶すると共に、上記汎用プロセッサと外部とを中継して、制御部からの命令に応じて上記汎用プロセッサを制御する中継回路と
を具え、
上記中継回路は、
上記制御部から供給される第１の起動命令に応じて、上記第１のファームウェアを上記メモリの実行開始アドレスから書き込み、続いて上記汎用プロセッサに対して上記第１の起動命令に応じた第２の起動命令を出力し、
上記汎用プロセッサは、
上記第２の起動命令に応じて起動すると共に、上記実行開始アドレスに書き込まれた上記第１のファームウェアを実行する
ことを特徴とするデータ処理装置。
【請求項７】
外部から供給される第１の起動命令に応じて、汎用プロセッサと外部とを中継する中継回路に記憶された第１のファームウェアを、汎用プロセッサがアクセスするメモリの実行開始アドレスに書き込む第１ファームウェア書込ステップと、
上記第１ファームウェア書込ステップで上記第１のファームウェアが書き込まれた後、上記第１の起動命令に応じた第２の起動命令を上記汎用プロセッサに出力して当該汎用プロセッサを起動させると共に、当該汎用プロセッサに、上記実行開始アドレスに書き込まれた上記第１のファームウェアを実行させる第１ファームウェア実行ステップと
を具えることを特徴とするデータ処理方法。
【請求項８】
上記メモリに上記汎用プロセッサを初期設定するための初期設定用データを書き込む初期設定用データ書込ステップを具え、
上記第１ファームウェア実行ステップでは、
上記実行開始アドレスに書き込まれた上記第１のファームウェアを、上記汎用プロセッサに実行させることにより、上記初期設定用データに基づいて上記汎用プロセッサの初期設定を行う
ことを特徴とする請求項７に記載のデータ処理方法。
【請求項９】
上記メモリに第２のファームウェアを書き込む第２ファームウェア書込ステップと、
外部から供給される第３の起動命令に応じて、上記中継回路に記憶された、上記第２のファームウェアの正当性を検出して実行するための実行用プログラムを、上記メモリの上記第２のファームウェアが書き込まれた位置とは異なる位置に書き込む実行用プログラム書込ステップと、
上記実行用プログラム書込ステップで上記実行用プログラムが書き込まれた後、上記第３の起動命令に応じた第４の起動命令を上記汎用プロセッサに出力して、上記メモリに書き込まれた上記実行用プログラムを上記汎用プロセッサに実行させることにより、上記メモリに書き込まれた上記第２のファームウェアの正当性を検出し、当該検出結果に応じて、当該第２のファームウェアを上記汎用プロセッサに実行させる実行用プログラム実行ステップと
を具えることを特徴とする請求項８に記載のデータ処理方法。
【請求項１０】
上記中継回路は、外部のバスと上記汎用プロセッサのバスとをブリッジするブリッジ回路である
ことを特徴とする請求項９に記載のデータ処理方法。
【請求項１１】
上記実行用プログラムは、暗号化された上記第２のファームウェアを復号する機能を有し、
上記実行用プログラム実行ステップでは、
上記メモリに書き込まれた上記実行用プログラムを上記汎用プロセッサに実行させるこ

とにより、上記メモリに書き込まれた暗号化された上記第２のファームウェアの正当性を検出し、当該検出結果に応じて、当該暗号化された第２のファームウェアを上記汎用プロセッサに復号させて実行させる
　ことを特徴とする請求項９に記載のデータ処理方法。
【請求項１２】
　アクセス可能なメモリに書き込まれるファームウェアを実行する汎用プロセッサと、第１のファームウェアを記憶すると共に上記汎用プロセッサと外部とを中継して外部からの命令に応じて上記汎用プロセッサを制御する中継回路とを有するデータ処理回路に対し、上記第１のファームウェアを上記中継回路から上記メモリの実行開始アドレスに書き込ませ、続いて上記実行開始アドレスに書き込ませた上記第１のファームウェアを上記汎用プロセッサに実行させるための起動命令を供給する供給ステップ
　を具えることを特徴とするデータ処理制御方法。
【請求項１３】
　データ処理回路に対して、
　外部から供給される第１の起動命令に応じて、汎用プロセッサと外部とを中継する中継回路に記憶された第１のファームウェアを、汎用プロセッサがアクセスするメモリの実行開始アドレスに書き込む第１ファームウェア書込ステップと、
　上記第１ファームウェア書込ステップで上記第１のファームウェアが書き込まれた後、上記第１の起動命令に応じた第２の起動命令を上記汎用プロセッサに出力して当該汎用プロセッサを起動させると共に、当該汎用プロセッサに、上記実行開始アドレスに書き込まれた上記第１のファームウェアを実行させる第１ファームウェア実行ステップと
　を実行させることを特徴とするデータ処理プログラム。
【請求項１４】
　データ処理装置に対して、
　アクセス可能なメモリに書き込まれるファームウェアを実行する汎用プロセッサと、第１のファームウェアを記憶すると共に上記汎用プロセッサと外部とを中継して外部からの命令に応じて上記汎用プロセッサを制御する中継回路とを有するデータ処理回路に対し、上記第１のファームウェアを上記中継回路から上記メモリの実行開始アドレスに書き込ませ、続いて上記実行開始アドレスに書き込ませた上記第１のファームウェアを上記汎用プロセッサに実行させるための起動命令を供給する供給ステップ
　を実行させることを特徴とするデータ処理制御プログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
　本発明はデータ処理回路に関し、特にセキュリティ処理を行うデータ処理回路に適用して好適なものである。
【背景技術】
【０００２】
　近年、インターネット等のネットワークを介した種々のコンテンツ配信サービスが広く普及している。このようなコンテンツ配信サービスでは、ＣＤやＤＶＤといった媒体を介してではなく、コンテンツのデータ（以下、これをコンテンツデータとも呼ぶ）そのものをネットワークを介してユーザの端末に提供するようになされているため、コンテンツの不正利用を防止することがいっそう強く求められており、このため様々なセキュリティ対策が講じられている。
【０００３】
　かかるセキュリティ対策の一つとして、例えばサービスを利用するための端末に、外部からの解析や改竄を困難にしたタンパレジスタントモジュールと呼ばれる特殊なハードウェアモジュールを組み込み、このモジュール内で、外部から隠蔽することが望ましいコンテンツ保護のためのセキュリティ処理を行うことにより、このセキュリティ処理をブラックボックス化してコンテンツの不正利用を防止するようになされたものがある（例えば特

許文献１参照）。
【特許文献１】特開２００１－２２２７１公報（第９図）
【発明の開示】
【発明が解決しようとする課題】
【０００４】
しかしながら、上述のような特定のセキュリティ処理に特化した専用のハードウェアモジュール（以下、これを専用モジュールと呼ぶことにする）は、その特殊性から、汎用のハードウェアモジュール（以下、これを汎用モジュールと呼ぶことにする）と比べて多大なコストがかかるという問題がある。
【０００５】
このような問題を解決するため、例えばファームウェアを書き替えることで種々の処理を行い得る汎用の演算プロセッサ（以下、これを単に汎用プロセッサと呼ぶ）を有する汎用モジュールを、専用モジュールの代わりとして用いることが考えられるが、このような汎用モジュールを用いた場合、コンテンツの不正利用を防止し得るのに十分なセキュリティを得ることが難しかった。
【０００６】
例えば図５に示すような汎用モジュール１００を実装した従来の端末Ｔ１００で、セキュリティ処理を実行する場合、以下のようなセキュリティ上の問題が生じる。
【０００７】
端末Ｔ１００は、全体を統括制御するＣＰＵ１０１、及び各種ファームウェアを記録するハードディスクドライブ１０２が、ＰＣＩバスＰＢ等を介して汎用モジュール１００と接続されており、ＣＰＵ１０１の制御のもと、ハードディスクドライブ１０２から読み出したファームウェアを汎用モジュール１００で実行させることにより、上述のようなセキュリティ処理を行うようになされている。
【０００８】
汎用モジュール１００は、汎用プロセッサ１００Ａと、汎用プロセッサ１００Ａのメモリ（以下、これをプロセッサメモリとも呼ぶ）ＰＭと、汎用プロセッサ１００ＡのＬｏｃａｌバスＬＢとモジュール外のＰＣＩバスＰＢとを中継するＰＣＩ－Ｌｏｃａｌブリッジ１００Ｂとを有し、ＣＰＵ１０１の制御のもと、ハードディスクドライブ１０２から読み出されたファームウェアが、このＰＣＩ－ローカルブリッジ１００Ｂを介して汎用プロセッサ１００Ａのプロセッサメモリ ＰＭに書き込まれる。
【０００９】
ちなみに、このプロセッサメモリＰＭには、図５（Ｂ）に示すように、汎用プロセッサ１００Ａが起動時最初にアクセスするアドレス（以下、これを実行開始アドレスとも呼ぶ）が予め設定されており、ファームウェアはこの実行開始アドレスから順に書き込まれるようになされている。
【００１０】
このようにしてＣＰＵ１０１は、ファームウェアを汎用プロセッサ１００Ａのプロセッサメモリ ＰＭに実行開始アドレスから書き込んだ後、汎用プロセッサ１００Ａを起動させるためのプロセッサ起動コマンドを、ＰＣＩバスＰＢを介して汎用モジュール１００に供給する。
【００１１】
汎用モジュール１００のＰＣＩ－ローカルブリッジ１００Ｂは、ＣＰＵ１０１からプロセッサ起動コマンドを受け取ると、このプロセッサ起動コマンドを汎用プロセッサ１００Ａ用のプロセッサ起動コマンドに変換して、これを汎用プロセッサ１００Ａに送信する。
【００１２】
汎用プロセッサ１００Ａは、このプロセッサ起動コマンドに応じて起動すると共に、プロセッサメモリＰＭの実行開始アドレスにアクセスして、ここに書き込まれたファームウェアを実行することにより、当該ファームウェアに基づくセキュリティ処理を開始する。
【００１３】

このように、かかる汎用モジュール１００は、外部からファームウェアがプロセッサメモリＰＭの実行開始アドレスから書き込まれた後、プロセッサ起動コマンドが供給されさえすれば、この書き込まれたファームウェアを汎用プロセッサ１００Ａに実行させるようになされているため、例えば外部から不正なファームウェアがプロセッサメモリＰＭの実行開始アドレスから書き込まれた状態で、プロセッサ起動コマンドが供給されてしまえば、この不正なファームウェアを正当なファームウェアと同様に汎用プロセッサ１００Ａに実行させることになる。ちなみに、この場合の不正なファームウェアとは、コンテンツの不正利用を目的として、例えばセキュリティ処理の内容を解析・改竄するようなファームウェアのことである。

【００１４】

すなわち、このような汎用モジュール１００でセキュリティ処理を実行する場合、汎用モジュールを不正に起動させて不正なファームウェアを実行させるといった不正起動攻撃を防ぐことが難しく、このためセキュリティ処理の内容を容易に解析・改竄される恐れがあり、結果として、コンテンツの不正利用を防止し得るのに十分なセキュリティを得ることが困難であった。

【００１５】

このように、汎用モジュール１００を用いた場合、専用モジュールを用いる場合と比べて、コストは抑えられるものの、セキュリティが著しく低くなるという問題があった。

【００１６】

本発明は以上の点を考慮してなされたもので、コストを抑えつつ、セキュリティを向上し得るデータ処理回路を提案しようするものである。

【課題を解決するための手段】

【００１７】

かかる課題を解決するため本発明のデータ処理回路においては、アクセス可能なメモリに書き込まれるファームウェアを実行する汎用プロセッサと、第１のファームウェアを記憶すると共に、汎用プロセッサと外部とを中継して、外部からの命令に応じて汎用プロセッサを制御する中継回路とを設け、中継回路が、外部から供給される第１の起動命令に応じて、第１のファームウェアをメモリの実行開始アドレスから書き込み、続いて汎用プロセッサに対して第１の起動命令に応じた第２の起動命令を出力し、汎用プロセッサが、第２の起動命令に応じて起動すると共に、実行開始アドレスに書き込まれた第１のファームウェアを実行するようにした。

【００１８】

このようにこのデータ処理回路では、中継回路が、外部から供給される汎用プロセッサを起動させるための第１の起動命令に応じて、中継回路に記憶してあるファームウェアを汎用プロセッサの実行開始アドレスに書き込んでから汎用プロセッサを起動させてこのファームウェアを実行させるようにしたことにより、例えば、不正なファームウェアが汎用プロセッサの実行開始アドレスに書き込まれた状態で、外部から第１の起動命令が供給されたとしても、汎用プロセッサが起動する際、この不正なファームウェアを中継回路に記憶してあるファームウェアで上書き消去するので、汎用プロセッサを不正に起動させて不正なファームウェアを実行させるといった不正起動攻撃を確実に防ぐことができる。

【００１９】

またこのようにこのデータ処理回路では、第１の起動命令に応じたファームウェアの書き込み及び汎用プロセッサの起動を、中継回路が担うようにしたことにより、中継回路以外の部分であるプロセッサ及びメモリには、汎用のものを用いることができる。

【発明の効果】

【００２０】

本発明によれば、中継回路が、外部から供給される汎用プロセッサを起動させるための第１の起動命令に応じて、中継回路に記憶してあるファームウェアを汎用プロセッサの実行開始アドレスに書き込んでから汎用プロセッサを起動させてこのファームウェアを実行させるようにしたことにより、例えば、不正なファームウェアが汎用プロセッサの実行開

始アドレスに書き込まれた状態で、外部から第１の起動命令が供給されたとしても、汎用プロセッサが起動する際、この不正なファームウェアを中継回路に記憶してあるファームウェアで上書き消去するので、汎用プロセッサを不正に起動させて不正なファームウェアを実行させるといった不正起動攻撃を確実に防ぐことができ、またこのように第１の起動命令に応じたファームウェアの書き込み及び汎用プロセッサの起動を、中継回路が担うようにしたことにより、中継回路以外の部分であるプロセッサ及びメモリには、汎用のものを用いることができ、かくしてコストを抑えつつ、セキュリティを向上し得るデータ処理回路を実現できる。

【発明を実施するための最良の形態】

【００２１】

以下図面について、本発明の一実施の形態を詳述する。

【００２２】

（１）コンテンツ再生装置の構成

図１において、１は全体としてネットワークＮＴを介して配信される楽曲コンテンツを再生可能なコンテンツ再生装置を示し、ホストＣＰＵ（Central Processing Unit）２、ＲＯＭ（Read Only Memory）３、ＲＡＭ（Random Access Memory）４、ハードディスクドライブ５、及び操作部６（以下、これらをホスト側とも呼ぶ）が、ホストバスＨＢに接続されると共に、ネットワークインタフェース部７、及びセキュリティ処理モジュール８（後述する）がＰＣＩバスＰＢに接続され、さらにホストバスＨＢとＰＣＩバスＰＢとがホスト－ＰＣＩブリッジ９を介して接続されている。また、セキュリティ処理モジュール８には、音声処理部１０を介してスピーカＳＰが接続されている。

【００２３】

このコンテンツ再生装置１は、ホストＣＰＵ２が全体を統括制御するようになされており、操作部６を介して、ネットワークＮＴ上のコンテンツ配信サーバ（図示せず）から配信される楽曲コンテンツの取得操作が行われると、これに応じて、楽曲コンテンツの配信を要求する要求信号を、ネットワークインタフェース部７を介して、ネットワークＮＴ上のコンテンツ配信サーバに送信する。

【００２４】

コンテンツ配信サーバは、コンテンツ再生装置１から、かかる要求信号を受信すると、これに応じて、要求された楽曲コンテンツの配信にともなう対価をコンテンツ再生装置１のユーザに対して課金するための課金処理を実行すると共に、要求された楽曲コンテンツに対応するコンテンツデータと、当該コンテンツデータを利用する権利がある旨を示す権利情報とを、ネットワークＮＴを介して、コンテンツ再生装置１に送信する。

【００２５】

コンテンツ再生装置１は、コンテンツ配信サーバから、コンテンツデータとその権利情報とを、ネットワークインタフェース部７を介して受信すると、これらをハードディスクドライブ５に記録する。その後、コンテンツ再生装置１は、操作部６を介してコンテンツデータの再生操作が行われると、これに応じて、コンテンツデータとその権利情報とをハードディスクドライブ５から読み出し、これらをセキュリティ処理モジュール８に供給する。

【００２６】

セキュリティ処理モジュール８は、ホストＣＰＵ２からの命令に応じて、ハードディスクドライブ５から読み出されたセキュリティ処理用のファームウェア（以下、これをセキュリティファームとも呼ぶ）を実行することにより、権利情報が正しいものであるか否か（すなわちコンテンツ再生装置１で正規に取得した権利情報であるか否か）を確認して、正しいものであると確認できた場合にのみ、この権利情報に対応するコンテンツデータの利用を許可するといったコンテンツ保護のためのセキュリティ処理を実行するようになされている。

【００２７】

ここで、ハードディスクドライブ５に記録されているコンテンツデータ、権利情報、及

びセキュリティファームは、それぞれが異なる暗号鍵で暗号化されているものとする。

【００２８】

実際上、セキュリティ処理モジュール８は、その内部に、暗号化されたセキュリティファームウェアを復号するための復号鍵（以下、これをセキュリティファームキーとも呼ぶ）と、このセキュリティファームキーを用いてセキュリティファームを復号すると共に、復号したセキュリティファームを実行するためのプログラム（以下、これをＦｉｒｍｗａｒｅＬｏａｄｅｒとも呼ぶ）とを格納しており、ホストＣＰＵ２からの命令に応じて、このＦｉｒｍｗａｒｅＬｏａｄｅｒを起動することにより、セキュリティファームを実行してセキュリティ処理を開始するようになされている。

【００２９】

セキュリティ処理を開始したセキュリティ処理モジュール８は、まずハードディスクドライブ５から読み出された権利情報を、例えば自身が持つ、暗号化された権利情報を復号するための復号鍵（以下、これを権利情報キー）を用いて復号する。

【００３０】

次いで、このセキュリティ処理モジュール８は、復号した権利情報が正しいものであるか否かを確認し、正しいものであると確認できた場合にのみ、この権利情報と、例えば自身が持つコンテンツデータ用の鍵情報とを用いて、暗号化されたコンテンツデータを復号するための復号鍵（以下、これをコンテンツキーとも呼ぶ）を生成し、このコンテンツキーを用いて、権利情報と共に読み出されたコンテンツデータを復号することで、このコンテンツデータの利用を許可し、この復号したコンテンツデータ（以下、これを復号済コンテンツデータとも呼ぶ）を音声処理部１０に供給する。

【００３１】

音声処理部１０は、セキュリティ処理モジュール８から供給された復号済コンテンツデータに対して所定のデジタルアナログ変換処理を施すことにより音声信号を得、この音声信号に基づく音声（すなわち楽曲コンテンツ）を、スピーカＳＰを介して出力する。

【００３２】

このようにコンテンツ再生装置１では、楽曲コンテンツの再生時、権利情報の確認や暗号化されたコンテンツデータの復号といったコンテンツ保護のためのセキュリティ処理をセキュリティ処理モジュール８内で実行するようになされており、以下、このセキュリティ処理の実行手順について、セキュリティ処理モジュール８の内部構成と合わせて説明する。

【００３３】

（２）セキュリティ処理モジュールの内部構成及びセキュリティ処理の実行手順

まず、セキュリティ処理モジュール８の内部構成について、図２を用いて説明する。セキュリティ処理モジュール８は、汎用プロセッサ８Ａと、汎用プロセッサ８Ａの外部メモリ（以下、これをプロセッサ外メモリとも呼ぶ）ＰＭｅと、汎用プロセッサ８ＡのＬｏｃａｌバスＬＢとモジュール外のＰＣＩバスＰＢとを中継するＰＣＩ－Ｌｏｃａｌブリッジ８Ｂとを有しており、このうち汎用プロセッサ８Ａ及びプロセッサ外メモリＰＭｅには、既存の汎用ＤＳＰ（Digital Signal Processor）及び汎用ＲＡＭが用いられているのに対し、ＰＣＩ－Ｌｏｃａｌブリッジ８Ｂには、コンテンツ再生装置１専用のデバイスが用いられている。

【００３４】

汎用プロセッサ８Ａは、複数のレジスタ（図示せず）と、これとは異なる内蔵メモリ（以下、これをプロセッサ内メモリとも呼ぶ）ＰＭｉとを有し、これら複数のレジスタ及びプロセッサ内メモリＰＭｉのアドレスと、プロセッサ外メモリＰＭｅのアドレスとをまとめて、１つのアドレス空間として利用するようになされている。

【００３５】

つまり、汎用プロセッサ８Ａのアドレス空間は、図３に示すように、プロセッサ内メモリ領域２０と、レジスタ領域２１と、プロセッサ外メモリ領域２２とでなり、さらにこのうちのレジスタ領域２１は、後述する外部メモリインタフェース設定レジスタ２１ａとそ

の他の設定レジスタ２１ｂとに分けられ、プロセッサ外メモリ領域２２は、使用部２２ａと未使用部２２ｂとに分けられている。

【００３６】

さらに、プロセッサ外メモリ領域２２の使用部２２ａは、その先頭アドレスから順に、上述のＦｉｒｍｗａｒｅＬｏａｄｅｒなどを格納するＦｉｒｍｗａｒｅＬｏａｄｅｒエリアａ１と、セキュリティ処理モジュール８の状態を示すステータス情報を格納するＳｔａｔｕｓエリアａ２と、セキュリティ処理モジュール８がＣＰＵ２に通知する（ホストＣＰＵ２が読み出す）応答コマンドやイベントコマンドを格納するＭｏｄｕｌｅＣｏｍｍａｎｄエリアａ３と、セキュリティ処理モジュール８がホストＣＰＵ２に転送する（ホストＣＰＵ２が読み出す）データを格納するＲｅａｄＢｕｆｆｅｒエリアａ４と、ホストＣＰＵ２がセキュリティ処理モジュール８に発行する（ホストＣＰＵ２が書き込む）コマンドを格納するＨｏｓｔＣｏｍｍａｎｄエリアａ５と、ホストＣＰＵ２がセキュリティ処理モジュール８に転送する（ホストＣＰＵ２が書き込む）データを格納するＷｒｉｔｅＢｕｆｆｅｒエリアａ６と、復号後のセキュリティファームを格納するファームウェア実行エリアａ７とに分けられている。

【００３７】

また、このうちのＭｏｄｕｌｅＣｏｍｍａｎｄエリアａ３、ＲｅａｄＢｕｆｆｅｒエリアａ４、ＨｏｓｔＣｏｍｍａｎｄエリアａ５、及びＷｒｉｔｅＢｕｆｆｅｒエリアａ６は、ホストＣＰＵ２から転送される復号前の暗号化されたセキュリティファームなどを一時的に格納する暗号化ファームウェア転送エリアａ８を兼用するようにもなされている。

【００３８】

さらにこの汎用プロセッサ８Ａでは、プロセッサ内メモリ領域２０の先頭アドレスが、起動時最初にアクセスするアドレス（すなわち実行開始アドレス）に規定されている。

【００３９】

一方、ＰＣＩ－Ｌｏｃａｌブリッジ８Ｂ（図２）は、外部からのアクセスが禁止された内蔵メモリ（以下、これをブリッジ内メモリとも呼ぶ）ＢＭを有し、このブリッジ内メモリＢＭに、上述した権利情報キー、コンテンツデータ用の鍵情報、セキュリティファームキー、及びＦｉｒｍｗａｒｅＬｏａｄｅｒと、後述する汎用プロセッサ８Ａを初期設定する初期設定処理用のファームウェア（以下、これを初期設定ファームとも呼ぶ）とを格納しており、必要に応じて、これらを汎用プロセッサ８Ａが利用するアドレス空間の所定エリアに書き込むようになされている。

【００４０】

セキュリティ処理モジュール８は、ホストＣＰＵ２からの命令を、ＰＣＩ－Ｌｏｃａｌブリッジ８Ｂで受け取り、当該ＰＣＩ－Ｌｏｃａｌブリッジ８Ｂが、この命令に応じて、汎用プロセッサ８Ａを制御することにより、上述のセキュリティ処理を実行するようになされている。

【００４１】

ここで、汎用プロセッサ８Ａの起動からセキュリティ処理を実行するまでの手順（すなわちセキュリティ処理の実行手順）について、図４のシーケンスチャートを用いて説明する。このシーケンスチャートは、ホストＣＰＵ２、ＰＣＩ－Ｌｏｃａｌブリッジ８Ｂ、及び汎用プロセッサ８Ａによるセキュリティ処理の実行手順を示すものであり、このときホストＣＰＵ２はＲＯＭ３に記録してあるプログラムに従って、またＰＣＩ－Ｌｏｃａｌブリッジ８Ｂはブリッジ内メモリＢＭに記録してあるプログラムに従って動作するようになされている。

【００４２】

コンテンツ再生装置１のホストＣＰＵ２は、例えば電源投入時、あるいは操作部６を介した手動操作に応じて、開始ステップＳＰ１において、セキュリティ処理モジュール８をリセットするためのリセット信号を、ＰＣＩ－Ｌｏｃａｌブリッジ８Ｂに送信する。

【００４３】

ＰＣＩ－Ｌｏｃａｌブリッジ８Ｂは、ホストＣＰＵ２から送られてくるリセット信号を

受け取ると、ステップＳＰ２において、受け取ったリセット信号を汎用プロセッサ８Ａ用のリセット信号に変換して、これを汎用プロセッサ８Ａに送信する。ここで、このリセット信号により汎用プロセッサ８Ａが一旦リセットされる。

【００４４】

つづいてホストＣＰＵ２は、ステップＳＰ１からステップＳＰ３に移り、このステップＳＰ３において、汎用プロセッサ８Ａ内のレジスタを初期設定するための初期設定用データを、汎用プロセッサ８Ａが利用するアドレス空間の暗号化ファームウェア転送エリアａ８に書き込み、次のステップＳＰ４に移る。ここで、この初期設定用データとは、汎用プロセッサ８Ａのクロックを設定するクロック設定用データや、汎用プロセッサ８Ａのキャッシュメモリのサイズを設定するキャッシュメモリ設定用データや、プロセッサ外メモリＰＭｅのインタフェースを設定する外部メモリＩ／Ｆ設定データ等である。

【００４５】

ステップＳＰ４においてホストＣＰＵ２は、一旦リセットされた汎用プロセッサ８Ａを起動させるためのプロセッサ起動コマンドを、ＰＣＩ－Ｌｏｃａｌブリッジ８Ｂに送信する。

【００４６】

ＰＣＩ－Ｌｏｃａｌブリッジ８Ｂは、ホストＣＰＵ２から送られてくるプロセッサ起動コマンドを受け取ると、ステップＳＰ５において、自身のブリッジ内メモリＢＭに記憶されている初期設定ファームを読み出し、これを汎用プロセッサ８Ａの実行開始アドレス（プロセッサ内メモリ領域２０の先頭アドレス）から書き込み、次のステップＳＰ６に移る。

【００４７】

ステップＳＰ６においてＰＣＩ－Ｌｏｃａｌブリッジ８Ｂは、ホストＣＰＵ２から受け取ったプロセッサ起動コマンドを汎用プロセッサ８Ａ用のプロセッサ起動コマンドに変換して、これを汎用プロセッサ８Ａに送信する。

【００４８】

このようにこのＰＣＩ－Ｌｏｃａｌブリッジ８Ｂは、ホストＣＰＵ２から受け取ったプロセッサ起動コマンドに応じて、ＰＣＩ－Ｌｏｃａｌブリッジ８Ｂ内に格納された初期設定ファームを、汎用プロセッサ８Ａの実行開始アドレスに書き込んでから、この汎用プロセッサ８Ａにプロセッサ起動コマンドを送るようにしたことにより、何らかのモジュール上の不具合（例えばセキュリティホール）などを利用して、外部から不正なファームウェアが、汎用プロセッサ８Ａの実行開始アドレスに書き込まれたとしても、この不正なファームウェアを初期設定ファームで上書き消去して、この不正なファームウェアが復号及び実行されることを防止することができる。

【００４９】

汎用プロセッサ８Ａは、ＰＣＩ－Ｌｏｃａｌブリッジ８Ｂから送られてくるプロセッサ起動コマンドに応じて起動すると共に、ステップＳＰ７において、規定されている実行開始アドレス（プロセッサ内メモリ領域２０の先頭アドレス）にアクセスして、ここに書き込まれている初期設定ファームを実行する。この初期設定ファームは、暗号化ファームウェア転送エリアａ８に書き込まれた初期設定データに基づいて、汎用プロセッサ８Ａの初期設定処理を行うファームウェアであり、汎用プロセッサ８Ａは、この初期設定ファームを実行することにより自身の初期設定を行う。

【００５０】

そして汎用プロセッサ８Ａは、この初期設定処理が終了すると、ステップＳＰ８に移り、このステップＳＰ８において、初期設定処理が終了したことを示す終了通知情報をＰＣＩ－Ｌｏｃａｌブリッジ８Ｂに送信する。

【００５１】

ＰＣＩ－Ｌｏｃａｌブリッジ８Ｂは、汎用プロセッサ８Ａから初期設定処理が終了したことを示す終了通知情報を受け取ると、ステップＳＰ９において、受け取った終了通知情報をホストＣＰＵ２用の終了通知情報に変換して、これをホストＣＰＵ２に送信する。

【００５２】
ホストＣＰＵ２は、ＰＣＩ－Ｌｏｃａｌブリッジ８Ｂから初期設定処理が終了したことを示す終了通知情報を受け取ると、汎用プロセッサ８Ａが起動して初期設定処理が終了したことを認識し、ステップＳＰ１０において、ハードディスクドライブ５から読み出した暗号化された状態のセキュリティファームを、汎用プロセッサ８Ａの暗号化ファームウェア転送エリアａ８に書き込み、次のステップＳＰ１１に移る。
【００５３】
ステップＳＰ１１においてホストＣＰＵ２は、汎用プロセッサ８Ａに、ＦｉｒｍｗａｒｅＬｏａｄｅｒを起動させるためのコマンド（以下、これをＦｉｒｍｗａｒｅＬｏａｄｅｒ起動コマンドとも呼ぶ）を、ＰＣＩ－Ｌｏｃａｌブリッジ８Ｂに送信する。
【００５４】
ＰＣＩ－Ｌｏｃａｌブリッジ８Ｂは、ホストＣＰＵ２から送られてくるＦｉｒｍｗａｒｅＬｏａｄｅｒ起動コマンドを受け取ると、ステップＳＰ１２において、自身のブリッジ内メモリＢＭに記憶されているＦｉｒｍｗａｒｅＬｏａｄｅｒとセキュリティファームキーとを読み出し、読み出したＦｉｒｍｗａｒｅＬｏａｄｅｒを汎用プロセッサ８ＡのＦｉｒｍｗａｒｅＬｏａｄｅｒエリアａ１の先頭アドレスから書き込み、またセキュリティファームキーをプロセッサ内メモリ領域２０に書き込み、次のステップＳＰ１３に移る。
【００５５】
ステップＳＰ１３においてＰＣＩ－Ｌｏｃａｌブリッジ８Ｂは、ステップＳＰ１１でホストＣＰＵ２から受け取ったＦｉｒｍｗａｒｅＬｏａｄｅｒ起動コマンドを、汎用プロセッサ８Ａ用のＦｉｒｍｗａｒｅＬｏａｄｅｒ起動コマンドに変換し、この変換したＦｉｒｍｗａｒｅＬｏａｄｅｒ起動コマンドを汎用プロセッサ８Ａに送信する。
【００５６】
汎用プロセッサ８Ａは、ＰＣＩ－Ｌｏｃａｌブリッジ８Ｂから送られてくるＦｉｒｍｗａｒｅＬｏａｄｅｒ起動コマンドを受け取ると、ステップＳＰ１４において、ＦｉｒｍｗａｒｅＬｏａｄｅｒエリアａ１の先頭アドレスにアクセスして、ここに書き込まれているＦｉｒｍｗａｒｅＬｏａｄｅｒを実行する。
【００５７】
このＦｉｒｍｗａｒｅＬｏａｄｅｒは、上述したように、暗号化された状態のセキュリティファームを、セキュリティファームキーを用いて復号してから実行するファームウェアであり、くわえて本実施の形態のＦｉｒｍｗａｒｅＬｏａｄｅｒは、復号する前にセキュリティファームの正当性をチェックするようにもなされている。
【００５８】
すなわち汎用プロセッサ８Ａは、このステップＳＰ１４において、ＦｉｒｍｗａｒｅＬｏａｄｅｒを実行することにより、まず自身の暗号化ファームウェア転送エリアａ８に書き込まれている暗号化された状態のセキュリティファームの正当性をチェックする。
【００５９】
ここで、このセキュリティファームの正当性をチェックする手法については、例えば、このセキュリティファームのハッシュ値や、ＭＡＣ値を取るなどの手法を用いればよく、また、セキュリティファームの正当性をチェックし得る手法であれば、この他種々の手法を用いてもよい。
【００６０】
そして汎用プロセッサ８Ａは、セキュリティファームが正当なものであると確認できた場合には、このセキュリティファームをプロセッサ内メモリ領域２０に書き込まれているセキュリティファームキーを用いて復号し、この復号したセキュリティファームをファームウェア実行エリアａ７に書き込み、次のステップＳＰ１５に移る。
【００６１】
また一方で、セキュリティファームが正当であると確認できなかった場合、汎用プロセッサ８Ａは、このセキュリティファームを復号せずに、次のステップＳＰ１５に移る。
【００６２】

ステップＳＰ１５において汎用プロセッサ８Ａは、ＦｉｒｍｗａｒｅＬｏａｄｅｒによる、正当性のチェック及びセキュリティファームの復号（ただし復号は、セキュリティファームが正当なものであると確認できた場合にのみ）が終了したことを示す終了通知情報をＰＣＩ－Ｌｏｃａｌブリッジ８Ｂに送信する。ここで、この終了通知情報には、正当性のチェック結果も含まれているものとする。

【００６３】

ＰＣＩ－Ｌｏｃａｌブリッジ８Ｂは、汎用プロセッサ８Ａから、正当性のチェック及びセキュリティファームの復号が終了したこと及び正当性のチェック結果を示す終了通知情報を受け取ると、ステップＳＰ１６において、受け取った終了通知情報をホストＣＰＵ２用の終了通知情報に変換して、これをホストＣＰＵ２に送信する。

【００６４】

これによりホストＣＰＵ２は、暗号化ファームウェア転送エリアａ８に書き込まれたセキュリティファームが正当なものであるか否かを判断し得、このセキュリティファームが正当なものではない、すなわち不正なものであると判断した場合には、例えば、再度リセット信号をＰＣＩ－Ｌｏｃａｌブリッジ８Ｂに送信して汎用プロセッサ８Ａを再起動させるようにしてもよいし、あるいは不正なファームウェアが書き込まれたことを音声等でユーザに通知して、以降の処理を中断するようにしてもよい。

【００６５】

上述のステップＳＰ１４で、セキュリティファームが正当なものであると確認でき、このセキュリティファームを復号した汎用プロセッサ８Ａは、上述のようにステップＳＰ１５で終了通知情報を送信した後、次のステップＳＰ１７に移る。

【００６６】

ステップＳＰ１７において汎用プロセッサ８Ａは、ＦｉｒｍｗａｒｅＬｏａｄｅｒによるセキュリティファームの実行に移行し、ファームウェア実行エリアａ７に書き込まれている復号されたセキュリティファームを実行する。これにより汎用プロセッサ８Ａは、このセキュリティファームに基づいて、上述のセキュリティ処理を行う。

【００６７】

以上で、汎用プロセッサ８Ａの起動からセキュリティ処理を実行するまでの手順（すなわちセキュリティ処理の実行手順）の説明を終了する。なお、ステップＳＰ８からステップＳＰ９、及びステップＳＰ１５からステップＳＰ１６においては、説明の便宜上、汎用プロセッサ８ＡがＰＣＩ－Ｌｏｃａｌブリッジ８Ｂを介してホストＣＰＵ２に終了通知情報を送信すると述べたが、実際には、この終了通知情報が、汎用プロセッサ８Ａにより、ＲｅａｄＢｕｆｆｅｒエリアａ４などに書き込まれ、これをホストＣＰＵ２が、読み出すようになされている。

【００６８】

このようにこのセキュリティ処理モジュール８では、モジュール外（すなわちホストＣＰＵ２）からプロセッサ起動コマンドが供給されると、これに応じて、モジュール内のＰＣＩ－Ｌｏｃａｌブリッジ８Ｂが、自身のブリッジ内メモリＢＭに格納されている初期設定ファームを、汎用プロセッサ８Ａが利用するアドレス空間の実行開始アドレスに書き込み、つづいてこのＰＣＩ－Ｌｏｃａｌブリッジ８Ｂが、汎用プロセッサ８Ａにプロセッサ起動コマンドを送信して、汎用プロセッサ８Ａを起動させ、初期設定ファームを実行させるようにした。

【００６９】

すなわちこのセキュリティ処理モジュール８では、モジュール外から供給されるプロセッサ起動コマンドに応じて、ＰＣＩ－Ｌｏｃａｌブリッジ８Ｂ内に格納された初期設定ファームを、汎用プロセッサ８Ａの実行開始アドレスに書き込んでから、この汎用プロセッサ８Ａを起動させるようにしたことにより、例えば、不正なファームウェアが汎用プロセッサ８Ａの実行開始アドレスに書き込まれた状態で、プロセッサ起動コマンドが供給されたとしても、このときこの不正なファームウェアが初期設定ファームで上書き消去されるので、汎用プロセッサ８Ａを不正に起動させて不正なファームウェアを実行させるような

不正起動攻撃を確実に防ぐことができる。

【００７０】

また、このセキュリティ処理モジュール８では、上述したように、暗号化されたセキュリティファームを復号するためのセキュリティファームキーと、このセキュリティファームキーを用いて暗号化されたセキュリティファームを復号して実行するＦｉｒｍｗａｒｅＬｏａｄｅｒとを、ＰＣＩ－Ｌｏｃａｌブリッジ８Ｂのブリッジ内メモリＢＭに格納しておき、モジュール外から供給されるＦｉｒｍｗａｒｅＬｏａｄｅｒ起動コマンドに応じて、ＰＣＩ－Ｌｏｃａｌブリッジ８ＢがＦｉｒｍｗａｒｅＬｏａｄｅｒを実行させるようにした。

【００７１】

すなわちこのセキュリティ処理モジュール８では、モジュール内に格納されているセキュリティファームキーとＦｉｒｍｗａｒｅＬｏａｄｅｒとを用いて、モジュール外から供給される暗号化されたセキュリティファームをモジュール内で復号して実行するようにしたことにより、モジュール外に格納されたセキュリティファームが不正に読み出されて容易に解析・改竄されることを防止することができる。また、このセキュリティファームキーとＦｉｒｍｗａｒｅＬｏａｄｅｒとを、モジュール内のＰＣＩ－Ｌｏｃａｌブリッジ８Ｂに格納しておくようにしたことにより、このセキュリティファームキーとＦｉｒｍｗａｒｅＬｏａｄｅｒとをモジュール外から隠蔽することができると共に、ＰＣＩ－Ｌｏｃａｌブリッジ８Ｂ以外の部分（すなわち汎用プロセッサ８Ａ及びプロセッサ外メモリＰＭｅなど）については、汎用のものを用いることができる。

【００７２】

さらに、このセキュリティ処理モジュール８では、暗号化されたセキュリティファームの復号前に、このセキュリティファームに対する正当性のチェックを行い、正当なものであると確認できた場合にのみ、セキュリティファームを復号して実行するようにした。これにより、外部から不正なファームウェアや改竄された暗号化ファームウェアが、セキュリティ処理モジュール８内の暗号化ファームウェア転送エリアａ８に書き込まれたとしても、この不正なファームウェアや改竄された暗号化ファームウェアの復号及び実行を防止することができる。

【００７３】

（３）アドレス空間のアクセス制限

さらにこのセキュリティ処理モジュール８では、ＰＣＩ－Ｌｏｃａｌブリッジ８Ｂにより、汎用プロセッサ８Ａのアドレス空間の各領域に対して、その領域に格納される情報の用途に応じたアクセス制限がかけられている。

【００７４】

実際上、このアクセス制限としては、図３に示すように、モジュール外からの書き込みのみを許可するＷｒｉｔｅＯｎｌｙと、モジュール外からの読み出し及び書き込みの両方を許可するＲｅａｄ／Ｗｒｉｔｅと、モジュール外からのアクセスを禁止するアクセス禁止との３種類があり、アドレス空間の各領域は、これら３種類のアクセス制限によりＷｒｉｔｅＯｎｌｙエリア、Ｒｅａｄ／Ｗｒｉｔｅエリア、及びアクセス禁止エリアのいずれかに設定されている。

【００７５】

ここで、ＷｒｉｔｅＯｎｌｙエリアに設定される領域は、ホストＣＰＵ２がセキュリティ処理モジュール８に発行する（ホストＣＰＵ２が書き込む）コマンドを格納するＨｏｓｔＣｏｍｍａｎｄエリアａ５と、ホストＣＰＵ２がセキュリティ処理モジュール８に転送する（ホストＣＰＵ２が書き込む）データを格納するＷｒｉｔｅＢｕｆｆｅｒエリアａ６とする。このように、ホストＣＰＵ２から送られてくる情報を格納する領域は、ＷｒｉｔｅＯｎｌｙエリアに設定する。

【００７６】

次に、Ｒｅａｄ／Ｗｒｉｔｅエリアに設定される領域は、外部メモリインタフェース設定レジスタ２１ａと、セキュリティ処理モジュール８の状態を示すステータス情報を格納

するＳｔａｔｕｓエリアａ２と、セキュリティ処理モジュール８がホストＣＰＵ２に通知する（ホストＣＰＵ２が読み出す）応答コマンドやイベントコマンドを格納するＭｏｄｕｌｅＣｏｍｍａｎｄエリアａ３と、セキュリティ処理モジュール８がホストＣＰＵ２に転送する（ホストＣＰＵ２が読み出す）データを格納するＲｅａｄＢｕｆｆｅｒエリアａ４とする。

【００７７】

実際上、外部メモリインタフェース設定レジスタ２１ａは、プロセッサ外メモリＰＭｅを使用するためにホストＣＰＵ２が設定するレジスタであり、正しく設定できたかどうかをホストＣＰＵ２が確認できるように、この外部メモリインタフェース設定レジスタ２１ａに対してはモジュール外からの書き込みだけでなく読み出しも許可する。

【００７８】

また同様に、Ｓｔａｔｕｓエリアａ２、ＭｏｄｕｌｅＣｏｍｍａｎｄエリアａ３及びＲｅａｄＢｕｆｆｅｒエリアａ４についても、ホストＣＰＵ２が情報を読み出した後にこの情報を書換／消去する場合などもあるので、モジュール外からの読み出しだけでなく書き込みも許可する。

【００７９】

このように、ホストＣＰＵ２から送られてくる情報、及びホストＣＰＵ２に送る情報を格納する領域はＲｅａｄ／Ｗｒｉｔｅエリアに設定する。

【００８０】

そして、これ以外の領域である、プロセッサ内メモリ領域２０、その他の設定レジスタ２１ｂ、プロセッサ外メモリ領域２２の未使用部２２ｂ、ＦｉｒｍｗａｒｅＬｏａｄｅｒエリアａ１、及びファームウェア実行エリアａ７は、アクセス禁止エリアに設定される。

【００８１】

実際上、プロセッサ内メモリ領域２０は、汎用プロセッサ８Ａの実行開始アドレスを含み、ＰＣＩ－Ｌｏｃａｌブリッジ８Ｂから送られてくる初期設定ファームやセキュリティキーを格納する領域であると共に、セキュリティ処理の最重要部分を実行するために使用される領域であり、セキュリティ処理の改竄・解析を防ぐためにモジュール外からのアクセスが禁止される。

【００８２】

また、その他の設定レジスタ２１ｂは、汎用プロセッサ８Ａの各種設定を行うレジスタであり、この設定がモジュール外から不正に変更されてセキュリティホールを作られることを防ぐために、モジュール外からのアクセスが禁止される。

【００８３】

さらに、プロセッサ外メモリ領域２２の未使用部２２ｂには、使用部２２ａに書き込まれたデータの写像が現れる恐れがあるので、モジュール外からのアクセスが禁止される。

【００８４】

さらに、ＦｉｒｍｗａｒｅＬｏａｄｅｒエリアａ１は、ＰＣＩ－Ｌｏｃａｌブリッジ８ＢからくるＦｉｒｍｗａｒｅＬｏａｄｅｒを格納する領域であり、ＦｉｒｍｗａｒｅＬｏａｄｅｒの改竄・解析を防ぐためにモジュール外からのアクセスが禁止される。

【００８５】

さらに、ファームウェア実行エリアａ７は、ＦｉｒｍｗａｒｅＬｏａｄｅｒによって復号されたファームウェアを格納して実行する領域であり、復号したファームウェアの改竄・解析を防ぐためにモジュール外からのアクセスが禁止される。

【００８６】

このように、ホストＣＰＵ２がアクセスする必要がなく、セキュリティ処理に係わるセキュリティキー、ＦｉｒｍｗａｒｅＬｏａｄｅｒ、及び復号したセキュリティファームなどの秘密情報を格納する領域はアクセス禁止エリアに設定する。

【００８７】

また、暗号化ファームウェア転送エリアａ８は、ＭｏｄｕｌｅＣｏｍｍａｎｄエリアａ３、ＲｅａｄＢｕｆｆｅｒエリアａ４、ＨｏｓｔＣｏｍｍａｎｄエリアａ５、及びＷｒｉ

ｔｅＢｕｆｆｅｒエリアａ６と兼用されているので、ＷｒｉｔｅＯｎｌｙエリア又はＲｅａｄ／Ｗｒｉｔｅエリアとなる。

【００８８】

このようにしてセキュリティ処理モジュール８では、ＰＣＩ－Ｌｏｃａｌブリッジ８Ｂにより、汎用プロセッサ８Ａのアドレス空間の各領域に対して、その領域に格納される情報の用途に応じたアクセス制限をかけるようにし、特に、ホストＣＰＵ２がアクセスする必要がなく、セキュリティ処理に係わる秘密情報を格納する領域については、モジュール外からのアクセスを禁止するようにした。これにより、秘密情報が漏洩してセキュリティ処理が解析・改竄されることを防止することができる。

【００８９】

（４）動作及び効果

以上の構成においてセキュリティ処理モジュール８では、ホストＣＰＵ２からプロセッサ起動コマンドが供給されると、これに応じて、モジュール内のＰＣＩ－Ｌｏｃａｌブリッジ８Ｂが、自身のブリッジ内メモリＢＭに格納されている初期設定ファームを、汎用プロセッサ８Ａが利用するアドレス空間の実行開始アドレスに書き込み、つづいてこのＰＣＩ－Ｌｏｃａｌブリッジ８Ｂが、汎用プロセッサ８Ａにプロセッサ起動コマンドを送信して、汎用プロセッサ８Ａを起動させ、初期設定ファームを実行させるようにした。

【００９０】

すなわちこのセキュリティ処理モジュール８では、モジュール外から供給されるプロセッサ起動コマンドに応じて、ＰＣＩ－Ｌｏｃａｌブリッジ８Ｂ内に格納された初期設定ファームを、汎用プロセッサ８Ａの実行開始アドレスに書き込んでから、この汎用プロセッサ８Ａを起動させるようにしたことにより、例えば、不正なファームウェアが汎用プロセッサ８Ａの実行開始アドレスに書き込まれた状態で、プロセッサ起動コマンドが供給されたとしても、この不正なファームウェアが初期設定ファームにより上書き消去されるので、汎用プロセッサ８Ａを不正に起動させて不正なファームウェアを実行させるような不正起動攻撃を確実に防ぐことができる。

【００９１】

また、このセキュリティ処理モジュール８では、モジュール内のＰＣＩ－Ｌｏｃａｌブリッジ８Ｂ内に格納された、暗号化されたセキュリティファームを復号して実行するプログラムであるＦｉｒｍｗａｒｅＬｏａｄｅｒに、暗号化されたセキュリティファームに対する正当性のチェック機能を設けるようにした。

【００９２】

すなわち、セキュリティ処理モジュール８では、セキュリティ処理を実行する前に、このＦｉｒｍｗａｒｅＬｏａｄｅｒを汎用プロセッサ８Ａに実行させることで、暗号化されたセキュリティファームの復号前に、このセキュリティファームに対する正当性のチェックを行い、正当なものであると確認できた場合にのみ、セキュリティファームを復号して実行するようにした。

【００９３】

これにより、セキュリティ処理モジュール８では、外部から不正なファームウェアや改竄された暗号化ファームウェアが、モジュール内に書き込まれたとしても、この不正なファームウェアや改竄された暗号化ファームウェアの復号及び実行を防止することができる。

【００９４】

また、このようなセキュリティを向上させるための初期設定ファーム及びＦｉｒｍｗａｒｅＬｏａｄｅｒなどをＰＣＩ－Ｌｏｃａｌブリッジ８Ｂに記憶し、またこれら初期設定ファーム及びＦｉｒｍｗａｒｅＬｏａｄｅｒなどの所定エリアへの書き込みをこのＰＣＩ－Ｌｏｃａｌブリッジ８Ｂが担うようにしたことにより、セキュリティ処理モジュール８のＰＣＩ－Ｌｏｃａｌブリッジ８Ｂ以外の部分（すなわち汎用プロセッサ８Ａが及びプロセッサ外メモリＰＭｅなど）には、汎用のものを採用することができる。またこのことを言い換えれば、新規に開発する部分がＰＣＩ－Ｌｏｃａｌブリッジ８Ｂだけでよく、この

ためセキュリティ処理モジュール８の全てを新規に開発する場合と比して、その開発費、開発時間、コストを大幅に削減できる。

【００９５】

以上の構成によれば、ＰＣＩ－Ｌｏｃａｌブリッジ８Ｂが、モジュール外から供給されるプロセッサ起動コマンドに応じて、ブリッジ内メモリＢＭに記憶してある初期設定ファームを汎用プロセッサ８Ａが利用するアドレス空間の実行開始アドレスに書き込んでから汎用プロセッサ８Ａを起動させてこの初期設定ファームを実行させるようにしたことにより、例えば、不正なファームウェアがこの実行開始アドレスに書き込まれた状態で、モジュール外からプロセッサ起動コマンドが供給されたとしても、汎用プロセッサ８Ａが起動する際には、この不正なファームウェアを初期設定ファームで上書き消去するので、汎用プロセッサ８Ａを不正に起動させて不正なファームウェアを実行させるといった不正起動攻撃を確実に防ぐことができ、またこのようにプロセッサ起動コマンドに応じた初期設定ファームの書き込み及び汎用プロセッサ８Ａの起動を、ＰＣＩ－Ｌｏｃａｌブリッジ８Ｂが担うようにしたことにより、ＰＣＩ－Ｌｏｃａｌブリッジ８Ｂ以外の部分には、汎用のものを用いることができ、かくして汎用プロセッサを用いてコストを抑えつつ、セキュリティを向上させることができる。

【００９６】

（５）他の実施の形態

なお上述の実施の形態においては、コンテンツの不正利用を防止するためのセキュリティ処理を実行するセキュリティ処理モジュール８に本発明を適用する場合について述べたが、本発明はこれに限らず、例えば、個人情報、暗号データ、ネットワーク認証データ、及び接続機器認証データなどのような外部から隠蔽したい秘密情報を処理するモジュールに適用することができ、この場合も、コストを抑えてセキュリティを向上させたモジュールを実現することができる。また、このようなモジュールに本発明を適用することができるので、セキュリティ処理モジュール８を有するコンテンツ再生装置１に限らず、例えば、ＩＣカード、携帯電話機、及び防犯装置などのような、種々のセキュリティ処理を行う装置に適用することができる。

【００９７】

また上述の実施の形態においては、ホストＣＰＵ２から供給されるプロセッサ起動コマンドに応じて、ＰＣＩ－Ｌｏｃａｌブリッジ８Ｂが、初期設定ファームを汎用プロセッサ８Ａが利用するアドレス空間の実行開始アドレスに書き込んでから汎用プロセッサ８Ａを起動させるようにした場合について述べたが、本発明はこれに限らず、このとき例えば初期設定用ファーム以外の役割を担うファームウェアをこの実行開始アドレスに書き込むようにしてもよい。実際上、本発明では、プロセッサ起動コマンドに応じて、汎用プロセッサ８Ａを起動させる直前に、何らかのファームウェアを実行開始アドレスに書き込めばよく、こうすることで、不正なファームウェアを上書き消去することができる。

【００９８】

さらに上述の実施の形態においては、ＦｉｒｍｗａｒｅＬｏａｄｅｒを、プロセッサ外メモリ領域２２のＦｉｒｍｗａｒｅＬｏａｄｅｒエリアａ１の先頭アドレスから書き込むようにしたが、本発明はこれに限らず、セキュリティファームが書き込まれる暗号化ファームウェア転送エリアａ８及びファームウェア実行エリアａ７と違う領域であり、かつモジュール外からのアクセスが禁止されたエリアであれば、どのエリアに書き込んでもよい。

【００９９】

さらに上述の実施の形態においては、ホストＣＰＵ２が初期設定用データを汎用プロセッサ８Ａの暗号化ファームウェア転送エリアａ８に書き込むようにした場合について述べたが、本発明はこれに限らず、この初期設定用データを、ＰＣＩ－Ｌｏｃａｌブリッジ８Ｂのブリッジ内メモリＢＭに記憶しておき、ホストＣＰＵ２からのプロセッサ起動コマンドに応じて、ＰＣＩ－Ｌｏｃａｌブリッジ８Ｂが、汎用プロセッサ８Ａの例えばアクセス禁止エリアに書き込むようにしてもよい。このようにすれば、さらにセキュリティを向上

させることができる。

【０１００】

さらに上述の実施の形態においては、汎用プロセッサ８Ａが利用するアドレス空間の各領域を図３に示すように割り当て、それぞれの領域にアクセス制限をかけるようにした場合について述べたが、本発明はこれに限らず、汎用プロセッサ８Ａ及び各領域の用途に応じて、領域の割り当て及びアクセス制限を設定すればよく、必ずしも、図３に示すような領域の割り当て及びアクセス制限に限定するものではない。

【０１０１】

さらに上述の実施の形態においては、汎用プロセッサ８Ａの実行開始アドレスを、プロセッサ内メモリ領域２０の先頭アドレスとした場合について述べたが、本発明はこれに限らず、汎用プロセッサ８Ａの仕様などに合わせて、他の領域のアドレスを実行開始アドレスとして規定するようにしてもよい。

【０１０２】

さらに上述の実施の形態においては、セキュリティファームを暗号化した状態で、モジュール外のハードディスクドライブ５に記録しておくようにした場合について述べたが、本発明はこれに限らず、このセキュリティファームが仮に暗号化されていなくとも、ＦｉｒｍｗａｒｅＬｏａｄｅｒによりこのセキュリティファームの正当性をチェックするので、不正なセキュリティファームの実行を防止することができる。ただし、セキュリティファームを暗号化しておくほうが、セキュリティが強固になることは言うまでもない。

【０１０３】

さらに上述の実施の形態においては、ＰＣＩ－Ｌｏｃａｌブリッジ８Ｂに記憶されているセキュリティファームキーを、汎用プロセッサ８Ａのプロセッサ内メモリ領域２０に書き込み、このセキュリティファームキーを用いて、暗号化されたセキュリティファームを復号するようにした場合について述べたが、本発明はこれに限らず、例えば、ＰＣＩ－Ｌｏｃａｌブリッジ８Ｂには、セキュリティファームキーを生成するための鍵情報を書き込んでおき、この鍵情報を用いてＦｉｒｍｗａｒｅＬｏａｄｅｒ上でセキュリティファームキーを生成して、セキュリティファームを復号するようにしてもよい。この場合、セキュリティファームキーは、実際にセキュリティファームを復号するときになって初めてＦｉｒｍｗａｒｅＬｏａｄｅｒ上で生成されるので、ＰＣＩ－Ｌｏｃａｌブリッジ８Ｂから不正に読み出される恐れをなくすことができる。このことは、セキュリティファームキーに限らず、秘密情報である権利情報キーや、コンテンツデータ用の鍵情報に対しても同様であり、こうすることで、さらにセキュリティを向上させることができる。

【０１０４】

さらに上述の実施の形態においては、第１のファームウェアとしての初期設定ファームや、実行用プログラムとしてのＦｉｒｍｗａｒｅＬｏａｄｅｒや、第２のファームウェアとしてのセキュリティファームを実行する汎用プロセッサと、初期設定ファーム及びＦｉｒｍｗａｒｅＬｏａｄｅｒを記憶すると共に、ＣＰＵ２から供給されるプロセッサ起動コマンド（第１の起動命令）を汎用プロセッサ用のプロセッサ起動コマンド（第２の起動命令）に変換し、またホストＣＰＵ２から供給されるＦｉｒｍｗａｒｅＬｏａｄｅｒ起動コマンド（第３の起動命令）を汎用プロセッサ用のＦｉｒｍｗａｒｅＬｏａｄｅｒ起動コマンド（第４の起動命令）に変換して出力する中継回路としてのＰＣＩ－Ｌｏｃａｌブリッジ８Ｂと、汎用プロセッサ８Ａがアクセス可能なメモリであるプロセッサ外メモリＰＭｅなどによって、データ処理回路としてのセキュリティ処理モジュール８を構成するようにした場合について述べたが、本発明はこれに限らず、この他種々の構成を用いるようにしてもよい。

【０１０５】

さらに上述の実施の形態においては、制御部としてのホストＣＰＵ２や、データ処理回路としてのセキュリティ処理モジュール８などによって、データ処理装置としてのコンテンツ再生装置１を構成するようにした場合について述べたが、本発明はこれに限らず、この他種々の構成を用いるようにしてもよい。

【産業上の利用可能性】
【０１０６】
本発明は、セキュリティ処理を実行する様々な回路及び装置で広く利用できる。
【図面の簡単な説明】
【０１０７】
【図１】コンテンツ再生装置の全体構成を示す略線図である。
【図２】セキュリティ処理モジュールの内部構成を示す略線図である。
【図３】汎用プロセッサのアドレス空間を示す略線図である。
【図４】セキュリティ処理の実行手順を示すシーケンスチャートである。
【図５】汎用モジュールを実装した従来端末の構成を示す略線図である。
【符号の説明】
【０１０８】
１……コンテンツ再生装置、２……ホストＣＰＵ、３……ＲＯＭ、４……ＲＡＭ、５……ハードディスクドライブ、６……操作部、７……ネットワークインタフェース部、８……セキュリティ処理モジュール、８Ａ……汎用プロセッサ、８Ｂ……ＰＣＩ－Ｌｏｃａｌブリッジ、９……ホスト－ＰＣＩブリッジ、１０……音声処理部、２０……プロセッサ内メモリ領域、２１……レジスタ領域、２１ａ……外部メモリ設定インタフェース設定レジスタ、２１ｂ……その他の設定レジスタ、２２……プロセッサ外メモリ領域、２２ａ……使用部、２２ｂ……未使用部、ａ１……ＦｉｒｍｗａｒｅＬｏａｄｅｒエリア、ａ２……ＳｔａｔｕｓエリアＭｏｄｕｌｅＣｏｍｍａｎｄエリア、ａ４……ＲｅａｄＢｕｆｆｅｒエリア、ａ５……ＨｏｓｔＣｏｍｍａｎｄエリア、ａ６……ＷｒｉｔｅＢｕｆｆｅｒエリア、ａ７……ファームウェア実行エリア、ａ８……暗号化ファームウェア転送エリア、ＢＭ……ブリッジ内メモリ、ＨＢ……ホストバス、ＬＢ……Ｌｏｃａｌバス、ＮＴ……ネットワーク、ＰＢ……ＰＣＩバス、ＰＭｅ……プロセッサ外メモリ、ＰＭｉ……プロセッサ内メモリ。

【図１】

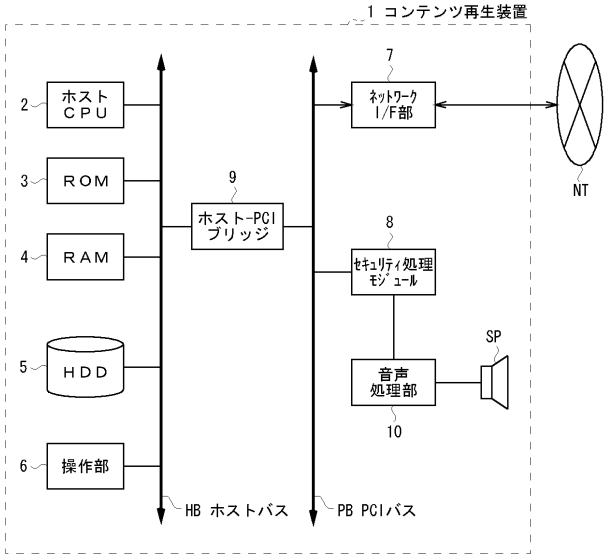


図１　コンテンツ再生装置の全体構成

【図２】

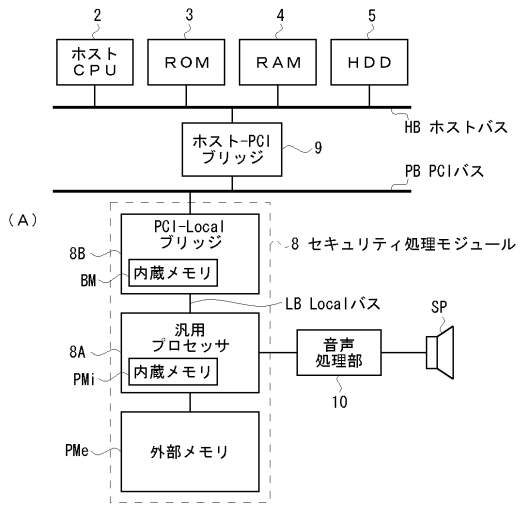


図２　セキュリティ処理モジュールの内部構成

【図３】

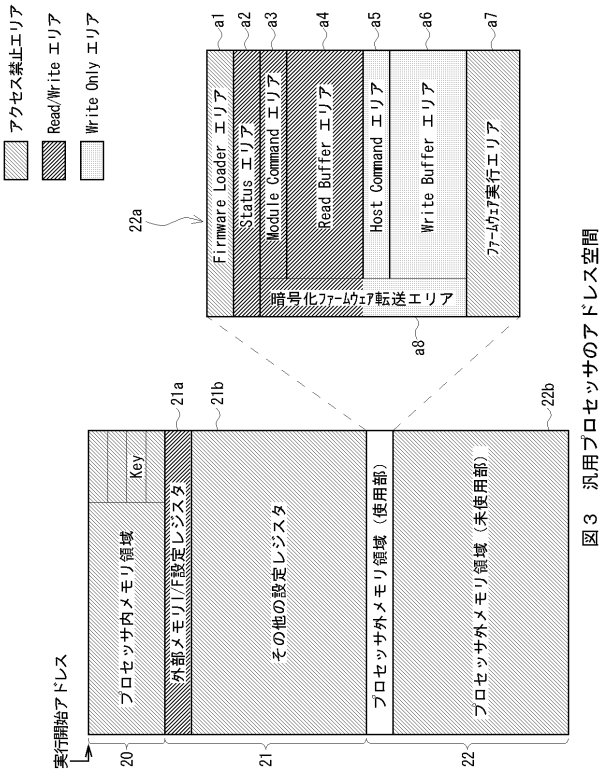


図３　汎用プロセッサのアドレス空間

【図４】

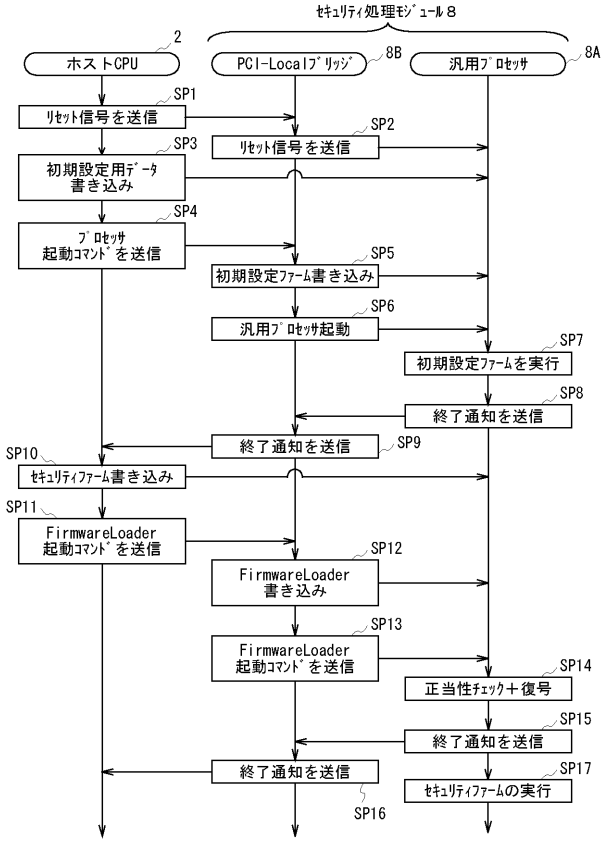


図４　セキュリティ処理の実行手順

【図５】

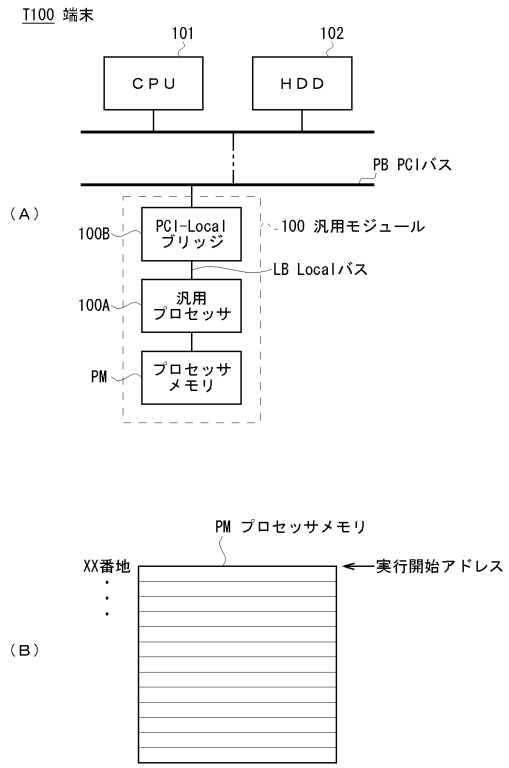


図５　汎用モジュールを実装した従来端末の構成