(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第3804670号
(P3804670)
(45)発行日　平成18年8月2日(2006.8.2)　(24)登録日　平成18年5月19日(2006.5.19)

(51)Int.Cl.　F I
G06F 21/24 (2006.01)　G06F 12/14 520A
G06F 12/14 530D
G06F 12/14 530P
G06F 12/14 540A

請求項の数 9　(全 26 頁)

(21)出願番号　特願2004-125735(P2004-125735)
(22)出願日　平成16年4月21日(2004.4.21)
(65)公開番号　特開2005-309758(P2005-309758A)
(43)公開日　平成17年11月4日(2005.11.4)
審査請求日　平成17年8月5日(2005.8.5)

早期審査対象出願

(73)特許権者　000002369
セイコーエプソン株式会社
東京都新宿区西新宿２丁目４番１号
(74)代理人　100104710
弁理士　竹腰　昇
(74)代理人　100124626
弁理士　榎並　智和
(74)代理人　100124682
弁理士　黒田　泰
(74)代理人　100090479
弁理士　井上　一
(74)代理人　100090387
弁理士　布施　行夫
(74)代理人　100090398
弁理士　大渕　美千栄

最終頁に続く

(54)【発明の名称】半導体装置、電子機器及び半導体装置のアクセス制御方法

(57)【特許請求の範囲】
【請求項１】
中央演算処理装置と、
前記中央演算処理装置がアクセスするメインメモリと、
前記中央演算処理装置のエミュレーション機能を有し前記中央演算処理装置に代行して前記メインメモリへのアクセスを行うデバッガの前記メインメモリへのアクセス又は前記中央演算処理装置の前記メインメモリへのアクセスを制限するセキュリティ回路と、
前記デバッガのデバッグ機能をイネーブルにするためのデバッグイネーブル信号が入力されるデバッグイネーブル信号入力端子と、
予め秘密固有データが設定される秘密固有データ保持部と、
前記秘密固有データと前記半導体装置へのアクセス信号の少なくとも一部により表される入力データとに基づいてパスワードデータを生成し、該パスワードデータを暗号化した暗号化パスワードデータを出力する暗号化パスワードデータ生成部とを含み、
前記デバッグイネーブル信号がインアクティブのとき、
前記デバッガから前記半導体装置へのアクセス信号を無効にすると共に、前記セキュリティ回路が前記中央演算処理装置の前記メインメモリへのアクセスを許可し、
前記デバッグイネーブル信号がアクティブのとき、
前記デバッガから前記半導体装置へのアクセス信号を有効にし、前記セキュリティ回路が前記メインメモリへのアクセスを不許可にした後に、前記暗号化パスワードデータと照合用パスワードデータとが一致したとき、前記セキュリティ回路が前記デバッガの前記メ

インメモリへのアクセスを許可することを特徴とする半導体装置。
【請求項２】
請求項１において、
前記暗号化パスワードデータ生成部が、
前記秘密固有データと前記入力データとに基づく一方向暗号化処理によって前記暗号化パスワードデータを生成することを特徴とする半導体装置。
【請求項３】
請求項１又は２において、
前記デバッガの前記メインメモリへのアクセスが不許可となったとき、
前記半導体装置をハードウェアリセットすることを条件に、前記デバッガからの次のアクセス信号を受け付けることを特徴とする半導体装置。
【請求項４】
請求項１乃至３のいずれかにおいて、
復号化鍵データを記憶する復号化鍵データ保持部と、
不揮発性メモリから読み出されて前記メインメモリに書き込まれるソースコードの復号化処理を、前記復号化鍵データを用いて行う復号化処理部とを含み、
前記セキュリティ回路が前記メインメモリへのアクセスを許可したときに、前記中央演算処理装置又は前記デバッガが、前記復号化処理部の復号化処理後のソースコードを読み込むことを特徴とする半導体装置。
【請求項５】
請求項４において、
予め復号化鍵固有データが設定される復号化鍵固有データ保持部を含み、
予め設定される復号化用データと前記復号化鍵固有データとに基づいて前記復号化鍵データを生成し、該復号化鍵データを前記復号化鍵データ保持部に保持させることを特徴とする半導体装置。
【請求項６】
請求項１乃至５のいずれかにおいて、
前記セキュリティ回路が、
前記デバッガ又は前記中央演算処理装置の前記メインメモリへのアクセスを許可するとき、前記デバッガ又は前記中央演算処理装置が出力するアクセス信号のマスクを解除し、
前記デバッガ又は前記中央演算処理装置の前記メインメモリへのアクセスを不許可にするとき、前記デバッガ又は前記中央演算処理装置が出力するアクセス信号をマスクすることを特徴とする半導体装置。
【請求項７】
請求項４又は５記載の半導体装置と、
汎用シリアルバスインタフェースとを含み、
前記半導体装置が、
前記不揮発性メモリに記憶されたソースコードが前記メインメモリに転送され記憶された後に、前記中央演算処理装置が、前記メインメモリが記憶した前記ソースコードに基づいて、前記汎用シリアルバスインタフェースを介して転送されるデータの加工処理を行うことを特徴とする電子機器。
【請求項８】
中央演算処理装置と、
前記中央演算処理装置がアクセスするメインメモリと、
前記中央演算処理装置のエミュレーション機能を有し前記中央演算処理装置に代行して前記メインメモリへのアクセスを行うデバッガの前記メインメモリへのアクセス又は前記中央演算処理装置の前記メインメモリへのアクセスを制限するセキュリティ回路と、
前記デバッガのデバッグ機能をイネーブルにするためのデバッグイネーブル信号が入力されるデバッグイネーブル信号入力端子と、
予め秘密固有データが設定される秘密固有データ保持部と、

前記秘密固有データと前記半導体装置へのアクセス信号の少なくとも一部により表される入力データとに基づいてパスワードデータを生成し、該パスワードデータを暗号化した暗号化パスワードデータを出力する暗号化パスワードデータ生成部とを含む半導体装置のアクセス制御方法であって、

前記デバッグイネーブル信号がインアクティブのとき、前記セキュリティ回路が、前記デバッガから前記半導体装置へのアクセス信号を無効にすると共に、前記中央演算処理装置の前記メインメモリへのアクセスを許可するステップと、

前記デバッグイネーブル信号がアクティブのとき、前記セキュリティ回路が、前記デバッガからの前記半導体装置へのアクセス信号を有効にし、前記セキュリティ回路が前記メインメモリへのアクセスを不許可にした後に、前記暗号化パスワードデータと照合用パスワードデータとが一致したとき、前記セキュリティ回路が前記デバッガの前記メインメモリへのアクセスを許可するステップとを含むことを特徴とする半導体装置のアクセス制御方法。

【請求項９】

請求項８において、

前記デバッガの前記メインメモリへのアクセスが不許可となったとき、

前記半導体装置をハードウェアリセットすることを条件に、前記デバッガからの次のアクセス信号を受け付けることを特徴とする半導体装置のアクセス制御方法。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、半導体装置、電子機器及び半導体装置のアクセス制御方法に関する。

【背景技術】

【０００２】

半導体装置に内蔵されるメモリには、極秘にしたいデータが記憶される場合がある。特に、半導体装置にＣＰＵ（Central Processing Unit）とメモリが内蔵され、該メモリにＣＰＵのアクセスデータであるソースコードが記憶される場合、このソースコードに極秘にしたいデータが含まれることがある。このような場合に、当該半導体装置を用いたシステム開発時に使用されるデバッガ等によりメモリに不正にアクセスされることを防止する必要がある。そのため、半導体装置のデバッグ環境を考慮して何らかのセキュリティ対策を採用する必要がある。

【特許文献１】特開２００３－１７７９３８号公報

【発明の開示】

【発明が解決しようとする課題】

【０００３】

上述のように半導体装置のデバッグ環境を考慮してセキュリティ対策を採用する一方で、半導体装置のコスト高、或いは該半導体装置を用いたシステム開発のコスト高を回避する必要もある。

【０００４】

しかしながら、特許文献１に開示された技術では、新たな外部装置を必要とするため、開発環境のコスト高を招いてしまう。またセキュリティ機能を実現するためのソフトウェアが半導体装置内に搭載されるため、外部装置との間の通信制御が複雑化してしまう。更に、半導体装置内においてセキュリティ機能を実現するためのデータと極秘にしたいデータとを分けて記憶する等の新たなセキュリティ対策が必要となり、半導体装置の構成及び制御が複雑化してしまう。

【０００５】

本発明は、以上のような技術的課題に鑑みてなされたものであり、その目的とするところは、低コストでセキュリティ機能を実現し、汎用のデバッガを用いてデバッグ可能なメモリ内蔵の半導体装置、電子機器及び半導体装置のアクセス制御方法を提供することにある。

【課題を解決するための手段】
【０００６】
上記課題を解決するために本発明は、中央演算処理装置と、前記中央演算処理装置がアクセスするメインメモリと、前記中央演算処理装置のエミュレーション機能を有し前記中央演算処理装置に代行して前記メインメモリへのアクセスを行うデバッガの前記メインメモリへのアクセス又は前記中央演算処理装置の前記メインメモリへのアクセスを制限するセキュリティ回路と、前記デバッガのデバッグ機能をイネーブルにするためのデバッグイネーブル信号が入力されるデバッグイネーブル信号入力端子とを含み、前記デバッグイネーブル信号がインアクティブのとき、前記デバッガから前記半導体装置へのアクセス信号を無効にすると共に、前記セキュリティ回路が前記中央演算処理装置の前記メインメモリへのアクセスを許可し、前記デバッグイネーブル信号がアクティブのとき、前記デバッガから前記半導体装置へのアクセス信号を有効にし、前記セキュリティ回路が前記デバッガの前記メインメモリへのアクセスを許可する半導体装置に関係する。
【０００７】
本発明によれば、デバッグイネーブル信号入力端子を設けたので、デバッガ等に付加回路を設けることなく、汎用的なデバッガが接続されたことを検出できるようになる。そして、このデバッグイネーブル信号によりデバッグ機能をイネーブルにし、このイネーブル状態では、デバッガからの半導体装置へのアクセス信号を有効にし、且つセキュリティ回路がデバッガの接続を検出して一旦メインメモリへのアクセスを不許可にするようにした。その後、アクセス信号の少なくとも一部により表される入力データが所定のデータであることを条件に、セキュリティ回路がデバッガのメインメモリへのアクセスを許可することができる。これにより、汎用的なデバッガを使用することが可能となり、かつ、簡素な構成で、汎用的なデバッガの不正なメモリへのアクセスを制限できるようになるため、システムの開発の低コスト化を図ることができる。
【０００８】
また本発明に係る半導体装置では、前記デバッグイネーブル信号がアクティブのとき、前記デバッガから前記半導体装置へのアクセス信号を有効にし、前記セキュリティ回路が前記メインメモリへのアクセスを不許可にした後に、前記アクセス信号の少なくとも一部により表される入力データが所定のデータであることを条件に、前記セキュリティ回路が前記デバッガの前記メインメモリへのアクセスを許可することができる。
【０００９】
また本発明に係る半導体装置では、予め秘密固有データが設定される秘密固有データ保持部と、前記秘密固有データと前記入力データとに基づいて暗号化パスワードデータを生成する暗号化パスワードデータ生成部とを含み、予め設定された照合用パスワードデータと前記暗号化パスワードデータとが一致したとき、前記セキュリティ回路が前記デバッガの前記メインメモリへのアクセスを許可することができる。
【００１０】
また本発明に係る半導体装置では、前記暗号化パスワードデータ生成部が、前記秘密固有データと前記入力データとに基づく一方向暗号化処理によって前記暗号化パスワードデータを生成することができる。
【００１１】
本発明によれば、上記の暗号化処理を一方向暗号化処理にしたので、暗号鍵を不要とし、簡素な構成でセキュリティを確保できる。
【００１２】
また本発明によれば、前記秘密固有データと前記入力データとを用い一方向暗号処理によって暗号化パスワードを生成するので、該入力データと前記照合用パスワードの関係を推測されることなく、該入力データをユーザごとに変更することができる。
【００１３】
また本発明に係る半導体装置では、前記デバッガの前記メインメモリへのアクセスが不許可となったとき、前記半導体装置をハードウェアリセットすることを条件に、前記デバ

ッガからの次のアクセス信号を受け付けることができる。

【００１４】

本発明においては、デバッガからのアクセスが不正であると判別されたとき、半導体装置のハードウェアリセットを行わない限り、次のアクセス信号、即ち、次の入力データを受け付けないようにしている。これにより、専用ソフトウェアなどによる不正な総当り攻撃を防ぐことができるため、その分だけ入力データのビット数を節約できる。

【００１５】

また本発明に係る半導体装置では、復号化鍵データを記憶する復号化鍵データ保持部と、不揮発性メモリから読み出されて前記メインメモリに書き込まれるソースコードの復号化処理を、前記復号化鍵データを用いて行う復号化処理部とを含み、前記セキュリティ回路が前記メインメモリへのアクセスを許可したときに、前記中央演算処理装置又は前記デバッガが、前記復号化処理部の復号化処理後のソースコードを読み込むことができる。

【００１６】

また本発明に係る半導体装置では、予め復号化鍵固有データが設定される復号化鍵固有データ保持部を含み、予め設定される復号化用データと前記復号化鍵固有データとに基づいて前記復号化鍵データを生成し、該復号化鍵データを前記復号化鍵データ保持部に保持させることができる。

【００１７】

本発明においては、デバッガからのアクセスが正当であると判別された後に、メモリに対して復号化したデータを展開するようにしたので、デバッガからの不正アクセスに対するセキュリティをより高めることができるようになる。

【００１８】

また本発明に係る半導体装置では、前記セキュリティ回路が、前記デバッガ又は前記中央演算処理装置の前記メインメモリへのアクセスを許可するとき、前記デバッガ又は前記中央演算処理装置が出力するアクセス信号のマスクを解除し、前記デバッガ又は前記中央演算処理装置の前記メインメモリへのアクセスを不許可にするとき、前記デバッガ又は前記中央演算処理装置が出力するアクセス信号をマスクすることができる。

【００１９】

本発明のよれば、簡素な構成で、セキュリティ回路を実現できる。

【００２０】

以上のような本発明に係る半導体装置によれば、汎用的なデバッグによる開発を可能にすると共に、該デバッガからの不正なアクセスによってメインメモリ内のデータが解析されるリバースエンジニアリングを防止したり、ライセンス化された極秘情報を保護したりできるようになる。

【００２１】

また本発明は、上記記載の半導体装置と、汎用シリアルバスインタフェースとを含み、前記半導体装置が、前記不揮発性メモリに記憶されたソースコードが前記メインメモリに転送され記憶された後に、前記中央演算処理装置が、前記メインメモリが記憶した前記ソースコードに基づいて、前記汎用シリアルバスインタフェースを介して転送されるデータの加工処理を行う電子機器に関係する。

【００２２】

本発明によれば、汎用的なデバッガで開発できる上に、該デバッガからの不正なアクセスによってメインメモリ内のデータが解析されるリバースエンジニアリングを防止したり、ライセンス化された極秘情報を保護したりできる半導体装置を含む電子機器を提供できるようになる。

【００２３】

また本発明は、中央演算処理装置がアクセスするソースコードがメインメモリに記憶される半導体装置のアクセス制御方法であって、前記中央演算処理装置のエミュレーション機能を有し前記中央演算処理装置に代行して前記メインメモリへのアクセスを行うデバッガのデバッグ機能をイネーブルにするためのデバッグイネーブル信号がインアクティブの

とき、前記デバッガから前記半導体装置へのアクセス信号を無効にすると共に、前記中央演算処理装置の前記メインメモリへのアクセスを許可するステップと、前記デバッグイネーブル信号がアクティブのとき、前記デバッガからの前記半導体装置へのアクセス信号を有効にし、前記デバッガの前記メインメモリへのアクセスを許可するステップとを含む半導体装置のアクセス制御方法に関係する。

【００２４】

また本発明に係る半導体装置のアクセス制御方法において、前記デバッガの前記メインメモリへのアクセスを許可するステップでは、前記デバッガの前記メインメモリへのアクセスを不許可にした後に、前記アクセス信号の少なくとも一部により表される入力データが所定のデータであることを条件に、前記デバッガの前記メインメモリへのアクセスを許可することができる。

【００２５】

また本発明に係る半導体装置のアクセス制御方法では、予め設定された秘密固有データと前記入力データとに基づいて暗号化パスワードデータを生成するステップを含み、予め設定された照合用パスワードデータと前記暗号化パスワードデータとが一致したとき、前記デバッガの前記メインメモリへのアクセスを許可することができる。

【００２６】

また本発明に係る半導体装置のアクセス制御方法では、前記デバッガの前記メインメモリへのアクセスが不許可となったとき、前記半導体装置をハードウェアリセットすることを条件に、前記デバッガからの次のアクセス信号を受け付けることができる。

【発明を実施するための最良の形態】

【００２７】

以下、本発明の実施の形態について図面を用いて詳細に説明する。なお、以下に説明する実施の形態は、特許請求の範囲に記載された本発明の内容を不当に限定するものではない。また以下で説明される構成のすべてが本発明の必須構成要件であるとは限らない。

【００２８】

図１に、本実施形態の半導体装置の原理的構成の構成図を示す。

【００２９】

半導体装置（ＩＣ、半導体回路、半導体集積回路）１０は、メモリ２０と、セキュリティ回路３０とを含む。メモリ２０は、ＣＰＵ（中央演算処理装置）のアクセスデータを記憶する。このメモリ２０を、メインメモリと呼ぶことができる。セキュリティ回路３０は、ＣＰＵ又はデバッガ１００のメモリ２０へのアクセスを制限する。デバッガ１００は、該ＣＰＵのエミュレーション機能を有し、デバッグモード時にＣＰＵに代行してメモリ２０にアクセスする。このデバッガ１００のＣＰＵのエミュレーション機能は、ソフトウェア及び該ソフトウェアを読み込んでソフトウェアに対応した処理を行うハードウェアによって実現される。

【００３０】

半導体装置１０は、ＣＰＵマクロ４０を含むことができる。ＣＰＵマクロ４０は、ＣＰＵコア４２を含む。ＣＰＵコア４２が、プログラムを読み込んで該プログラムに対応した処理を実行するＣＰＵということができる。ＣＰＵマクロ４０のＣＰＵコア４２以外の部分は、ＣＰＵ以外の周辺回路ということができる。本実施形態では、該周辺回路が、デバッグモード時にデバッガ１００からのデバッグ信号（アドレス信号、データ信号、アクセス制御信号等）をＣＰＵコア４２の信号として出力するセレクタ４４等を含む。

【００３１】

なお図１では、セレクタ４４のみを示しているが、デバッグモード時にＣＰＵコア４２に入力される信号をデバッガ１００に対して出力するためのセレクタを含むことができる。

【００３２】

このような構成により、通常動作モード時には、ＣＰＵコア４２が、セキュリティ回路３０を介してメモリ２０へのアクセスを行う。メモリ２０に記憶されたデータを読み出す

場合、ＣＰＵコア４２が、該データが記憶されたメモリ２０のアドレス信号、読み出し制御信号及びチップセレクト信号（アクセス制御信号）を出力し、メモリ２０に記憶されたデータをＣＰＵコア４２が読み込む。この場合、メモリ２０へのアドレス信号、読み出し制御信号及びチップセレクト信号（アクセス制御信号）をアクセス信号ということができる。より具体的には、このアクセス信号は、メモリ２０の記憶データを読み出すための信号である。

【００３３】

同様に、メモリ２０にデータを書き込む場合、ＣＰＵコア４２が、メモリ２０のデータを書き込む領域のアドレス信号、データ信号、書き込み制御信号及びチップセレクト信号を出力し、データ信号に対応したデータをメモリ２０に書き込む。この場合、メモリ２０にデータを書き込む領域のアドレス信号、データ信号、書き込み制御信号及びチップセレクト信号をアクセス信号ということができる。より具体的には、このアクセス信号は、メモリ２０にデータを書き込むための信号である。

【００３４】

デバッグモード時には、ＣＰＵコア４２の機能をディセーブルにして、デバッガ１００がＣＰＵコア４２の機能を代行し、デバッガ１００がＣＰＵマクロ４０及びセキュリティ回路３０を介して、上述と同様にメモリ２０へのアクセスを行う。この場合、デバッガ１００が、メモリ２０のアドレス信号、読み出し制御信号及びチップセレクト信号（アクセス制御信号）（広義にはアクセス信号）を出力し、メモリ２０に記憶されたデータをデバッガ１００が読み込むということができる。同様に、デバッガ１００が、メモリ２０のデータを書き込む領域のアドレス信号、データ信号、書き込み制御信号及びチップセレクト信号（アクセス制御信号）（広義にはアクセス信号）を出力し、データ信号に対応したデータをメモリ２０に書き込むということができる。

【００３５】

このデバッグ機能は、デバッグイネーブル信号によりイネーブル（enable）状態又はディセーブル（disable）状態に設定される。デバッグ機能がイネーブル状態の場合、デバッグモード時ということができる。デバッグ機能がディセーブル状態の場合、通常動作モード時ということができる。半導体装置１０は、デバッグイネーブル信号入力端子１２を含み、デバッグイネーブル信号は、半導体装置１０の外部から該デバッグイネーブル信号入力端子１２を介して入力される。

【００３６】

デバッグイネーブル信号がインアクティブとなって、デバッガ１００のデバッグ機能がディセーブルに設定されたとき、半導体装置１０は、デバッガ１００から半導体装置１０へのアクセス信号を無効にする。またセキュリティ回路３０が、メモリ２０へのアクセスを有効にして、ＣＰＵコア４２のメモリ２０へのアクセスを許可する。

【００３７】

一方、デバッグイネーブル信号がアクティブとなって、デバッグ機能がイネーブルに設定されたとき、半導体装置１０は、デバッガ１００から半導体装置１０へのアクセス信号を有効にする。そしてセキュリティ回路３０が、メモリ２０へのアクセスを有効にしてデバッガ１００のメモリ２０へのアクセスを許可する。

【００３８】

このようなデバッガ１００からのアクセス信号の有効化制御及び無効化制御を行うため半導体装置１０は、マスク回路５０を含むことができる。マスク回路５０は、デバッグイネーブル信号に基づいて、デバッガ１００からのアクセス信号を無効にしたり、有効にしたりできる。

【００３９】

図２に、マスク回路５０の構成例の回路図を示す。図２では、デバッガ１００からＣＰＵマクロ４０への入力信号（アクセス信号）をマスクするマスク回路５０の構成例を示している。図２において、デバッグイネーブル信号がＨレベルのとき（アクティブのとき）にデバッグ機能がイネーブル状態に設定されるものとする。

【００４０】
デバッガ１００からの入力信号は、入力端子５２－１を介して半導体装置１０に入力される。入力端子５２－１を介して入力された入力信号は、入力バッファ５４－１によりバッファリングされて、マスク回路５６－１の入力に供給される。マスク回路５６－１は、デバッグイネーブル信号と、入力バッファ５４－１との論理積演算を行い、その結果をＣＰＵマクロ４０への入力信号として出力する。こうすることで、デバッグイネーブル信号がインアクティブのとき、デバッガ１００からの入力を無効にし、デバッグイネーブル信号がアクティブのとき、デバッガ１００からの入力を有効にできる。
【００４１】
図３に、マスク回路５０の他の構成例の回路図を示す。図３では、ＣＰＵマクロ４０からデバッガ１００への出力信号（アクセス信号）をマスクするマスク回路５０の構成例を示している。
【００４２】
ＣＰＵマクロ４０からの出力信号は、マスク回路５６－２の入力に供給される。マスク回路５６－２は、デバッグイネーブル信号と、ＣＰＵマクロ４０からの出力信号との論理積演算を行い、その結果を出力バッファ５４－２に出力する。
【００４３】
出力バッファ５４－２は、出力制御信号により出力制御が行われ、該出力制御信号がアクティブのときマスク回路５６－２の出力をバッファリングして出力し、該出力制御信号がインアクティブのとき出力バッファ５４－２の出力をハイインピーダンス状態に設定する。出力バッファ５４－２の出力は、出力端子５２－２に接続されている。
【００４４】
こうすることで、デバッグイネーブル信号がインアクティブのとき、デバッガ１００への出力を無効にし、デバッグイネーブル信号がアクティブのとき、デバッガ１００への出力を有効にできる。
【００４５】
図４に、マスク回路５０の更に他の構成例の回路図を示す。図４では、ＣＰＵマクロ４０とデバッガ１００との間の入出力信号（アクセス信号）をマスクするマスク回路５０の構成例を示している。ここでは、半導体装置１０では、該半導体装置１０への入力信号はマスク回路５０の入力バッファから入力専用バスに出力され、該半導体装置１０の出力信号は出力専用バスから出力バッファに入力されるものとする。
【００４６】
入力バッファ５４－３及び出力バッファ５４－４は、出力制御信号により入出力制御が行われ、該出力制御信号がアクティブのときマスク回路５６－４の出力をバッファリングして入出力端子５２－３に出力し、該出力制御信号がインアクティブのとき入出力端子５２－３の入力信号をバッファリングしてマスク回路５６－３に出力する。
【００４７】
従って、デバッガ１００からの入力信号は、入出力端子５２－３を介して半導体装置１０に入力されると、入力バッファ５４－３によりバッファリングされて、マスク回路５６－３の入力に供給される。マスク回路５６－３は、デバッグイネーブル信号と、入力バッファ５４－３の出力との論理積演算を行い、その結果をＣＰＵマクロ４０への入力信号として出力する。
【００４８】
ＣＰＵマクロ４０からの出力信号は、マスク回路５６－４の入力に供給される。マスク回路５６－４は、デバッグイネーブル信号と、ＣＰＵマクロ４０からの出力信号との論理積演算を行い、その結果を出力バッファ５４－４に出力する。この出力バッファ５４－４の出力は、入出力端子５２－３に接続されている。
【００４９】
以上のように、デバッガ１００と半導体装置１０との間のアクセス信号の有効化及び無効化を制御できる。そして本実施形態においては、デバッグイネーブル信号をデバッガ１

００で生成する必要がなく、例えばデバッグシステムにおいてデバッグイネーブル信号入力端子１２を固定的にHレベルに設定するようにできる。これによりデバッガ１００を、専用に設計する必要がなくなり、汎用的なデバッガを用いることができる。言い換えれば、デバッグイネーブル信号をアクティブにしない限り、デバッガ１００からメモリ２０へのアクセスを不能にできることを意味し、簡素な構成でメモリ２０の機密性を維持できる。

【００５０】

なお本実施形態では、デバッグイネーブル信号がアクティブとなるデバッグモード時において、デバッガ１００からの不正なアクセスを制限できることが望ましい。以下では、汎用的なデバッガ１００を用いながら、デバッガ１００からの不正なアクセスを制限できる半導体装置及びこれを用いたシステムの詳細な構成例について説明する。

【００５１】

図５に、本実施形態における半導体装置の詳細な構成例及び該半導体装置を用いたシステムの構成例のブロック図を示す。但し、図１に示す半導体装置１０と同一部分には同一符号を付し、適宜説明を省略する。なお本実施形態の半導体装置では、図５に示すすべての回路、ユニット（部）を含む必要はなく、その一部を省略する構成にしてもよい。

【００５２】

図５において半導体装置２００は、図１に示す半導体装置１０の機能を有する。半導体装置２００は、デバッグイネーブル信号入力端子１２、図１のメモリ２０の機能を有するＲＡＭ（Random Access Memory）２１０、セキュリティ回路３０、ＣＰＵマクロ４０及びマスク回路５０を含む。ＣＰＵマクロ４０は、ＣＰＵコア４２を含む。

【００５３】

半導体装置２００では、デバッグモード時において、デバッガ１００から半導体装置２００へのアクセス信号を有効にし、セキュリティ回路３０がＲＡＭ２１０へのアクセスを一旦不許可にする。そして、その後、デバッガ１００からのアクセス信号の少なくとも一部により表される入力データが所定のデータであることを条件に、セキュリティ回路３０がＲＡＭ２１０へのアクセスを有効にしてデバッガ１００のＲＡＭ２１０へのアクセスを許可する。

【００５４】

このためセキュリティ回路３０は、アクセス制御部２２０を含むことができる。

【００５５】

図６に、アクセス制御部２２０の構成例のブロック図を示す。ここでは、ＣＰＵマクロ４０からのアドレス信号の制御を行う構成のみを示しているが、ＣＰＵマクロ４０からのアクセス制御信号（読み出し制御信号、書き込み制御信号、チップセレクト信号）の制御も同様に実現できる。

【００５６】

アクセス制御部２２０は、セレクタ２２２、２２４を含む。アクセス制御部２２０には、通常動作モード時にＣＰＵコア４２が出力するアドレス信号、又はデバッグモード時にデバッガ１００が出力するアドレス信号が入力される。このアドレス信号は、セレクタ２２２、２２４に入力される。

【００５７】

セレクタ２２２は、アドレス信号の各ビットが例えば０に固定された固定値とＣＰＵマクロ４０からのアドレス信号とのいずれかを、認証信号に基づいて出力する。デバッガ１００からのアクセスが不正であると判断されるとき認証信号がインアクティブとなり、デバッガ１００からのアクセスが正当である（不正ではない）と判断されるとき認証信号がアクティブとなる。そしてセレクタ２２２は、認証信号がインアクティブのとき固定値を出力し、該認証信号がアクティブのときＣＰＵマクロ４０からのアドレス信号を出力する。なお固定値が０であることに本発明が限定されるものではなく、デバッグモード時において認証信号がインアクティブとなったとき、ＲＡＭ２１０へのアクセスが無効となるような値のアドレス信号であればよい。

【００５８】
セレクタ２２４は、デバッグイネーブル信号に基づいて、ＣＰＵマクロ４０からアドレス信号又はセレクタ２２２の出力のいずれかを選択して出力する。デバッグイネーブル信号がインアクティブのとき、即ち通常動作モード時においてはＣＰＵマクロ４０からのアドレス信号を選択出力する。従って、通常動作モード時では、ＣＰＵマクロ４０からアドレス信号はＣＰＵコア４２が出力するアドレス信号であるため、ＣＰＵコア４２が出力するアドレス信号がＲＡＭ２１０に出力される。
【００５９】
一方、セレクタ２２４において、デバッグイネーブル信号がアクティブのとき、即ちデバッグモード時においてはセレクタ２２２の出力を選択する。デバッグモード時においては、ＣＰＵマクロ４０からアドレス信号はデバッガ１００が出力するアドレス信号である。そのため、デバッグモード時において認証信号がアクティブのとき、デバッガ１００が出力するアドレス信号がＲＡＭ２１０に出力され、デバッグモード時において認証信号がインアクティブのとき、ＲＡＭ２１０へのアクセスを無効とする値のアドレス信号がＲＡＭ２１０に出力されることになる。
【００６０】
以上のようにして、デバッガ１００又はＣＰＵコア４２のＲＡＭ２１０へのアクセスを許可するとき、アクセス制御部２２０は、デバッガ１００又はＣＰＵコア４２が出力するアドレス信号及びアクセス制御信号のマスクを解除できる。またデバッガ１００又はＣＰＵコア４２のＲＡＭ２１０へのアクセスを不許可にするとき、アクセス制御部２２０は、デバッガ１００又はＣＰＵコア４２が出力するアドレス信号及びアクセス制御信号をマスクすることができる。
【００６１】
このような認証信号を生成するため、セキュリティ回路３０は更に比較部２３０を含むことができる。
【００６２】
図５において、比較部２３０は、デバッグモード時において、デバッガ１００からの入力データが所定のデータか否かを比較し、両データが一致したときデバッガ１００からのアクセスが正当であると判断して、アクティブとなる認証信号を出力する。また比較部２３０は、両データが一致しないとき、デバッガ１００からのアクセスが不正であると判断して、インアクティブとなる認証信号を出力する。
【００６３】
また半導体装置２００が、上述のようにデバッガ１００からの入力データをパスワードデータとして受け付ける場合、デバッガ１００から不正に該パスワードデータを総当たりで入力されることがある。このような事態においても、ある程度のセキュリティを確保する必要がある。そこで半導体装置２００では、デバッガ１００からのパスワードデータに対して暗号化処理を行って、この暗号化処理後のパスワードデータと予め設定された照合用パスワードデータとを照合することで、デバッガ１００からのアクセスが不正であるか否かを判別するようになっている。
【００６４】
更にデバッガ１００の各ユーザが同じパスワードデータで、ＲＡＭ２１０にアクセスできることはセキュリティを確保する点で望ましくない。そのため、本実施形態では、ユーザごとに秘密固有データを設け、デバッガ１００からのパスワードデータと該秘密固有データとに基づいて暗号化処理を行って、この暗号化処理後のパスワードデータと照合用パスワードデータとを照合することで、デバッガ１００からのアクセスが不正であるか否かを判別する。
【００６５】
以上の機能を実現するため、半導体装置２００は、パスワードデータ保持部２４０、秘密固有データ保持部２５０、パスワードデータ結合部２６０、一方向暗号化処理部（広義には暗号化パスワードデータ生成部）２７０とを含むことができる。

【００６６】
パスワードデータ保持部２４０には、デバッグモード時においてデバッガ１００からの入力データがパスワードデータ（ベンダユニークなパスワードデータ）として保持される。秘密固有データ保持部２５０には、予め秘密固有データが設定される。この秘密固有データは、１又は複数の半導体装置ごとに異なるデータであり、例えば半導体装置の製造ロットごとに、或いはデバッガ１００のユーザごとに異ならせることが望ましい。
【００６７】
パスワードデータ結合部２６０は、パスワードデータ保持部２４０に保持されたデバッガ１００からの入力データと秘密固有データ保持部２５０に保持された秘密固有データとに基づいて結合パスワードデータを生成する。このようなパスワードデータ結合部２６０は、例えば該入力データと該秘密固有データとの排他的論理和演算結果を結合パスワードデータとして出力できる。或いはパスワードデータ結合部２６０は、例えば該入力データと該秘密固有データとをデータのビットの並び方向に連結して結合パスワードデータとして出力できる。更には、パスワードデータ結合部２６０は、例えば該入力データ及び該秘密固有データの少なくとも一方の所定のビットの入れ替え、除去等の予め定められたルールに従ったビット操作を行って、結合パスワードデータとして出力できる。
【００６８】
一方向暗号化処理部２７０は、パスワードデータ結合部２６０によって生成された結合パスワードデータに対して、一方向暗号化処理を行って生成された暗号化パスワードデータを出力する。ここで一方向暗号化処理は、処理中に情報を欠落させることで、処理後の結果から処理前の値を推測することを不可能にできる。一方向暗号化処理部２７０は、単に暗号鍵を用いて暗号化処理を行う暗号化処理部に置き換えることも可能であるが、一方向暗号化処理は、暗号鍵を必要とせず、且つ比較的簡素な構成で実現できるため、一方向暗号化処理の方が望ましい。一方向暗号化処理としては、ハッシュ関数を用いるもの、例えばＳＨＡ－１（Secure Hash Algorithm 1）やＭＤ５アルゴリズム（The MD5 Message-Digest Algorithm）等がある。ＳＨＡ－１、ＭＤ５アルゴリズムの内容については公知であるため、詳細な説明を省略する。
【００６９】
そして比較部２３０は、一方向暗号化処理部２７０によって出力される暗号化パスワードデータと予め設定される照合用パスワードデータとを比較する。そして両パスワードデータが一致したときに、デバッガ１００からのアクセスが正当であると判断して、アクティブとなる認証信号を出力する。この結果、アクセス制御部２２０が、デバッガ１００からのアドレス信号やアクセス制御信号をＲＡＭ２１０に対して出力し、セキュリティ回路３０がＲＡＭ２１０へのアクセスを有効にしてデバッガ１００のＲＡＭ２１０へのアクセスを許可することができる。
【００７０】
一方、両パスワードデータが不一致のときに、デバッガ１００からのアクセスが不正であると判断して、インアクティブとなる認証信号を出力する。この結果、アクセス制御部２２０が、デバッガ１００からのアドレス信号やアクセス制御信号がマスクされてしまい、セキュリティ回路３０がＲＡＭ２１０へのアクセスを無効にする。
【００７１】
なお照合用パスワードデータは、半導体装置２００の外部に設けられた不揮発性メモリ（外部メモリ）としてのフラッシュＲＯＭ（Read Only Memory）３００に記憶される。図５に示すシステムを構成するシステム基板上には、半導体装置２００とフラッシュＲＯＭ３００とが実装され、半導体装置２００のデバッグを行う時点では、フラッシュＲＯＭ３００には、照合用パスワードデータ３１０が書き込まれている。
【００７２】
なおフラッシュＲＯＭ３００を、半導体装置２００の内部に設けることも可能である。また、ＣＰＵ（中央演算処理装置）のアクセスがあるため、メモリ２０（メインメモリ）の書き込み／読み出し動作が半導体装置２００の処理速度に関与するため、メモリ２０の

書き込み／読み出し動作は、フラッシュＲＯＭ３００の読み出し動作よりも高速であることが望ましい。

【００７３】

更に半導体装置２００では、デバッガ１００からのパスワードデータの総当たり攻撃を有効に防止できることが望ましい。半導体装置２００では、デバッガ１００のＲＡＭ２１０へのアクセスが不許可（無効）となったとき、半導体装置２００をハードウェアリセットすることを条件に、デバッガ１００からの次のアクセス信号（入力データ）を受け付けるようにしている。これは、例えばマスク回路５０で、半導体装置２００のハードウェアリセットしない限り次のアクセス信号（入力データ）を有効にしないようにしてもよいし、比較部２３０において、認証信号が一旦インアクティブに設定された場合、半導体装置２００のハードウェアリセットを行わない限り認証信号を変化できないようにしてもよい。以下では、後者の方法により実現した場合について説明する。

【００７４】

図７に、比較部２３０の動作を説明するためのハードウェア記述言語の記載例を示す。ここでは、半導体装置２００のハードウェアリセットを行うハードウェアリセット信号をhreset、暗号化パスワードデータをPSWD、照合用パスワードデータをCWD、認証信号をPassとしている。そして認証信号Passがアクティブのとき１、認証信号Passがインアクティブのとき０とする。

【００７５】

図７に示すように比較部２３０を動作させることにより、認証信号Passが、一旦０になった後は、ハードウェアリセット信号hresetが１にならない限り、認証信号Passの状態を更新できなくなる。これにより、照合用パスワードデータCWDと暗号化パスワードデータPSWDとが一致しないとき、半導体装置２００をハードウェアリセットすることを条件に、デバッガ１００からの次の入力データ（アクセス信号）を受け付けることができる。

【００７６】

ここで、例えば半導体装置２００に対してデバッガ１００のユーザが、不正な専用ソフトウェアなどで総当り攻撃を行った場合、パスワードが誤っていた場合でも次のパスワードをすぐに受け付ける仕組みでは、短時間で正しいパスワードを見つけることが可能となり、これを防ぐためにパスワードのビット長は十分長くする必要がある。

【００７７】

ところが本実施形態のように、パスワードが誤っていた場合、半導体装置２００のハードウェアリセットをすることを条件に、デバッガ１００から次のパスワードをうけつけるような仕組みとすることで、より短いパスワードビット長でセキュリティを確保できる。例えば、ハードウェアリセットによるリセット時間を１秒、パスワードデータ長をｓ（ｓは正の整数）ビットとすると、2^s×１秒経過時に認証信号Passをアクティブにできる。

【００７８】

更にまた、以上のようにデバッガ１００からの不正なアクセスを防止した上で、フラッシュＲＯＭ３００上のソースコード（ソースコードデータ）もまた暗号化されていることが望ましい。

【００７９】

この場合、図５に示すように、半導体装置２００は、復号化処理部２８０、復号化鍵データ保持部２８２を含むことができる。復号化処理部２８０は、復号化鍵データ保持部２８２に保持された復号化鍵データを用いて、復号化処理を行う。この復号化処理部２８０は、例えばＤＥＳ（Data Encryption Standard）のアルゴリズムで復号化処理を行うことができる。ここで、復号処理部のアルゴリズムはＤＥＳ以外の方式でもかまわない。なおＤＥＳのアルゴリズムについては公知であるため、説明を省略する。

【００８０】

この結果、セキュリティ回路３０が、デバッガ１００のＲＡＭ２１０へのアクセスを許可したときに、デバッガ１００が、復号化処理部２８０の復号化処理後のデータを読み込むことができる。この際、デバッガ１００のアクセスが正当であると確認されたことを条

件に、復号化処理部２８０が、復号化したソースコードデータ（ソースコード）をＲＡＭ２１０に展開し、該ＲＡＭ２１０に展開されたデータに対してデバッガ１００がアクセスすることが望ましい。

【００８１】

なお復号化処理部２８０が復号化処理を行うソースコードデータは、フラッシュＲＯＭ３００に記憶される。このデータは、ＣＰＵコア４２又はデバッガ１００が実行するプログラムのソースコード（コンパイル後のコード）３２０であり、パラメータやその他の情報も含むものとする。また、このソースコードデータ３２０はフラッシュＲＯＭ３００に書き込まれる時点で既に暗号化処理が行われている。この暗号化処理は、ＤＥＳのアルゴリズムを用いて行われる。即ち、復号化処理部２８０の復号化処理に対応した暗号化処理を用いて暗号化されたソースコードがフラッシュＲＯＭ３００に保持される。

【００８２】

復号化鍵データ結合部２８６は、復号化鍵固有データ保持部２８４に保持された復号化鍵固有データと予め設定される復号化用データ３３０とに基づいて、復号化鍵データを生成する。このような復号化鍵データ結合部２８６は、例えば該復号化鍵固有データと該復号化用データとの排他的論理和演算結果を復号化鍵データとして出力できる。或いは復号化鍵データ結合部２８６は、例えば該復号化鍵固有データと該復号化用データとをデータのビットの並び方向に連結して復号化鍵データ保持部２８２に出力できる。更には、復号化鍵データ結合部２８６は、例えば該復号化鍵固有データ及び該復号化用データの少なくとも一方の所定のビットの入れ替え、除去等の予め定められたルールに従ったビット操作を行って、復号化鍵データとして出力できる。なお復号化用データ３３０は、フラッシュＲＯＭ３００に記憶される。

【００８３】

この復号化用データ３３０は半導体装置ごとに変更することが可能である。その結果、半導体装置ごとに異なる鍵データで暗号化、復号化することとなり、高い安全性が確保可能となる。

【００８４】

ここで、フラッシュＲＯＭ３００に記憶されるデータの設定例について説明する。フラッシュＲＯＭ３００には、システム開発（設計）時に照合用パスワードデータ３１０、ソースコード３２０及び復号化用データ３３０が書き込まれる。本実施形態では、外部システムによって、フラッシュＲＯＭ３００のデータの設定が行われる。ここで外部システムは、パーソナルコンピュータ等のハードウェアと、該パーソナルコンピュータに搭載されるオペレーティングシステム上で動作するアプリケーションプログラム（ソフトウェア）とによってその機能が実現される。そして、外部システムにより設計されたソースコード（ソースプログラム及びパラメータ）、各種鍵データ及び各種固有データがフラッシュＲＯＭ３００に書き込まれる。

【００８５】

図８に、本実施形態における外部システムの機能ブロック図の構成例を示す。

【００８６】

外部システム４００は、処理部４１０、記憶部４２０、フラッシュＲＯＭ書き込み部４３０を含む。外部システム４００では、バス４４０を介して、処理部４１０、記憶部４２０、フラッシュＲＯＭ書き込み部４３０が接続される。

【００８７】

処理部４１０は、記憶部４２０に記憶されたデータ又はプログラムを読み込んで処理を行う。この処理部４１０は、暗号化処理部４１２、ユニークパスワード受付処理部４１４、一方向暗号化処理部４１６を含む。処理部４１０の機能は、ＣＰＵや、ＡＳＩＣ（Application Specific Integrated Circuit）等のハードウェアにより実現される。

【００８８】

記憶部４２０は、暗号化鍵固有データ４２２、暗号化用データ４２４、ソースコード（平文）４２６、秘密固有データ４２８を含む。また記憶部４２０は、処理部４１０の暗号

化処理部４１２、ユニークパスワード受付処理部４１４及び一方向暗号化処理部４１６の各処理を実現するためのプログラムデータを記憶する。記憶部４２０の機能は、ＲＡＭやＲＯＭ等のハードウェアにより実現される。

【００８９】

フラッシュＲＯＭ書き込み部４３０は、処理部４１０によって生成されたデータを、フラッシュＲＯＭ３００の所定の領域に書き込む処理を行う。

【００９０】

図９に、図８の外部システム４００によって行われる照合用パスワードデータの書き込み処理のフローの一例を示す。図９に示すフローを実現するためのプログラムが記憶部４２０に記憶され、処理部４１０がこのプログラムを読み込むことで以下の処理を実現できる。

【００９１】

まず処理部４１０が、ユーザからのベンダユニークなパスワードデータを受け付ける処理を行う（ステップＳ１０）。

【００９２】

次に、処理部４１０は、記憶部４２０から秘密固有データ４２８を読み出す（ステップＳ１１）。ここで、秘密固有データ４２８は、半導体装置２００の秘密固有データ保持部２５０に保持される秘密固有データと同じデータである。

【００９３】

そして、処理部４１０は、ステップＳ１０において受け付けられたベンダユニークなパスワードデータと秘密固有データ４２８とを用いて、半導体装置２００のパスワードデータ結合部２６０と同様の処理によって、一方向暗号化用データを生成する（ステップＳ１２）。

【００９４】

続いて、処理部４１０は、ステップＳ１２で生成された一方向暗号化用データに対して一方向暗号化処理を行う（ステップＳ１３）。ここで、ステップＳ１３における一方向暗号化処理は、半導体装置２００の一方向暗号化処理部２７０と同じ処理である。

【００９５】

そして処理部４１０はフラッシュＲＯＭ書き込み部４３０に対して指示を出して、ステップＳ１３で求められた一方向暗号化処理の処理結果を、照合用パスワードデータとしてフラッシュＲＯＭ３００に書き込む処理を行わせ（ステップＳ１４）、一連の処理を終了する（エンド）。

【００９６】

このように、ユーザごとに異なるパスワードデータが割り当てられており、デバッグ時においてデバッガ１００からのパスワードデータが、ステップＳ１０で受け付けたベンダユニークなパスワードデータと異なる場合、デバッガ１００からのアクセスが不正と判断される。また、ステップＳ１１において読み出される秘密固有データとデバッグ対象の半導体装置の秘密固有データとが異なる場合、デバッガ１００からのアクセスが不正と判断される。

【００９７】

図１０に、図８の外部システム４００によって行われるソースコードの書き込み処理のフローの一例を示す。図１０に示すフローを実現するためのプログラムが記憶部４２０に記憶され、処理部４１０がこのプログラムを読み込むことで以下の処理を実現できる。

【００９８】

まず処理部４１０が、記憶部４２０に記憶された暗号化鍵固有データ４２２と暗号化用データ４２４とを読み出す（ステップＳ２０）。

【００９９】

続いて処理部４１０は、暗号化鍵固有データ４２２と暗号化用データ４２４とに基づいて、暗号化鍵データを生成する（ステップＳ２１）。ここで、暗号化鍵データと、復号化鍵データ保持部２８２に保持される復号化鍵データとは対をなす。

【０１００】
そして処理部４１０は、ステップＳ２１で生成された暗号化鍵データを用いたＤＥＳのアルゴリズムに従って、記憶部４２０に記憶されたソースコード４２６の暗号化処理を行う（ステップＳ２２）。この暗号化処理は、半導体装置２００の復号化処理部２８０の復号化処理と対をなす処理であり、暗号化処理部４１２の処理前のデータが、復号化処理部２８０の処理後のデータと同じになるようになっている。
【０１０１】
その後、処理部４１０はフラッシュＲＯＭ書き込み部４３０に対して指示を出して、ステップＳ２２で暗号化されたソースコードを、フラッシュＲＯＭ３００に書き込む処理を行わせ（ステップＳ２３）、一連の処理を終了する（エンド）。
【０１０２】
次に、上記のようにしてフラッシュＲＯＭ３００の設定が行われた後の図５に示すシステムの動作例について説明する。
【０１０３】
図１１に、図５のシステムの動作シーケンスの一例を示す。図１１では、デバッガ１００、半導体装置２００及びフラッシュＲＯＭ３００の各ユニットの動作例のシーケンスとユニット間の動作例のシーケンスとを示している。図１１では、デバッガ１００からのパスワードデータにより、デバッガ１００からのアクセスが正当であると判断された場合のシーケンスを示している。
【０１０４】
まず半導体装置２００では、デバッガ１００が接続され、アクティブのデバッグイネーブル信号がデバッグイネーブル信号入力端子１２に供給される（Ｂ１）。これにより半導体装置２００では、セキュリティ回路３０によりＣＰＵマクロ４０のＲＡＭ２１０に対するアクセスが一旦不許可にされる（Ｂ２）。またマスク回路５０は、デバッガ１００からの入力データを有効にする。
【０１０５】
一方、デバッガ１００においては、ソフトウェアによりユニークパスワード受付処理が行われる（Ａ１）。ここでユーザが、ベンダユニークなパスワードデータを入力すると、デバッガ１００が、半導体装置２００のパスワードデータ保持部２４０に対して該パスワードデータを書き込む。
【０１０６】
半導体装置２００では、デバッガ１００からのパスワードデータがパスワードデータ保持部２４０に書き込まれると、秘密固有データ保持部２５０から秘密固有データが読み出される（Ｂ３）。続いて半導体装置２００は、パスワードデータ保持部２４０に書き込まれたパスワードデータと秘密固有データとから、結合パスワードデータを生成し（Ｂ４）、該結合パスワードデータに対して一方向暗号化処理を行う（Ｂ５）。
【０１０７】
その後、半導体装置２００は、フラッシュＲＯＭ３００の照合用パスワードデータ３１０を読み出す（Ｂ６）。そして一方向暗号化処理の処理結果と、フラッシュＲＯＭ３００からの照合用パスワードデータ３１０とを比較する認証処理を行う（Ｂ７）。
【０１０８】
デバッガ１００からのパスワードデータと、図９のステップＳ１０で受け付けられたパスワードデータとが同じで、かつ秘密固有データ保持部２５０に保持される秘密固有データ保持部と、秘密固有データ４２８とが同じ場合には、両者が一致する。
【０１０９】
そして、一方向暗号化処理の処理結果と照合用パスワードデータ３１０とが一致したとき、デバッガ１００からのアクセスが正当であると判断され、デバッガ１００のＲＡＭ２１０へのアクセスが有効化される（Ｂ８）。
【０１１０】
その後、半導体装置２００では、復号化鍵固有データ保持部２８４に保持された復号化

鍵固有データと、フラッシュＲＯＭ３００に記憶された復号化用データ３３０とが読み出される（Ｂ９）。

【０１１１】

半導体装置２００は、復号化鍵固有データと復号化用データとに基づいて、復号化鍵データを生成する（Ｂ１０）。この復号化鍵データは、復号化鍵データ保持部２８２に保持される。これにより半導体装置２００は、フラッシュＲＯＭ３００に記憶されたソースコード３２０を読み出しながら、復号化鍵データ保持部２８２に保持された復号化鍵データを用いて、復号化処理を行う（Ｂ１１）。そしてこの復号化処理後のデータをＲＡＭ２１０に書き込んで、復号化したソースコードをＲＡＭ２１０に展開する（Ｂ１２）。

【０１１２】

これにより、ＣＰＵコア４２のエミュレーション機能を有するデバッガ１００が、ＲＡＭ２１０に展開された復号化後のソースコードを読み込んで、該ソースコードに対応した処理の実行や、該ソースコードに含まれるデータを参照できるようになる（Ｃ１）。

【０１１３】

図１２に、図５のシステムの動作シーケンスの他の例を示す。図１２では、図１１と同様にデバッガ１００、半導体装置２００及びフラッシュＲＯＭ３００の各ユニットの動作例のシーケンス等を示している。また図１２では、デバッガ１００からのパスワードデータにより、デバッガ１００からのアクセスが不正であると判断された場合のシーケンスを示す。但し、図１２において、図１１と同一処理部分には同一符号を付し、適宜説明を省略する。

【０１１４】

半導体装置２００の照合用パスワードデータの読み込み（Ｂ６）までのシーケンスは図１１と同様であるため、説明を省略する。

【０１１５】

照合用パスワードデータの読み込み後、一方向暗号化処理の処理結果と照合用パスワードデータ３１０とが一致しないとき、デバッガ１００からのアクセスが不正であると判断され、デバッガ１００のＲＡＭ２１０へのアクセスが無効化される（Ｂ１３）。

【０１１６】

その後、デバッガ１００においてユニークパスワードの受付処理が行われて新たにユニークパスワードデータが半導体装置２００に入力されたとしても、デバッガ１００からのアクセスが正当であると判断されることはない。そのため、半導体装置２００をハードウェアリセットするより他はないようになっている。

【０１１７】

次に、本実施形態における半導体装置２００が適用されたデータ転送制御装置の構成例について説明する。

【０１１８】

図１３に、本実施形態における半導体装置２００が適用されたデータ転送制御装置の構成例のブロック図を示す。なお図１３に示すデータ転送制御装置では、図１３に示すすべての回路、ユニット（部）を含む必要はなく、その一部を省略する構成にしてもよい。

【０１１９】

データ転送制御装置６００は、ストリームデータ受信装置と、記憶媒体と、汎用（高速）シリアルインタフェースとの間のデータ転送を制御する。ストリームデータ受信装置としては、例えばデジタル放送復調回路がある。記憶媒体としては、例えばハードディスクドライブ（Hard Disk Drive：ＨＤＤ）がある。汎用（高速）シリアルインタフェースとしては、ＩＥＥＥ（Institute of Electrical and Electronics Engineers）１３９４インタフェースやＵＳＢ（Universal Serial Bus）２．０インタフェースがあり、以下ではＩＥＥＥ１３９４インタフェースであるものとして説明する。

【０１２０】

図１３では、データ転送制御装置６００は、リンクコントローラ６１０、物理層インタフェース６２０を含む。リンクコントローラ６１０は、ＩＥＥＥ１３９４規格に準拠した

リンク層のデータ転送制御を実現する。物理層インタフェース６２０は、データ転送制御装置６００の外部に設けられた物理層コントローラ（図示せず）との物理層のインタフェースを実現する。この物理層コントローラがＩＥＥＥ１３９４規格に準拠したバスに接続され、ＩＥＥＥ１３９４規格に準拠した物理層のデータ転送制御を実現する。このバスは、ＩＥＥＥ１３９４インタフェースを有する他の電子機器に接続される。なおこの物理層コントローラもまた、データ転送制御装置６００に内蔵するようにしてもよい。

【０１２１】

データ転送制御装置６００は、ＩＤＥ（Integrated Drive Electronics）インタフェース６３０、ストリームインタフェース６４０、６４２を含む。ＩＤＥインタフェース６３０は、データ転送制御装置６００と記憶媒体との間のインタフェースを実現する回路である。

【０１２２】

ＡＶ（Audio Visual）用の記憶媒体においては、パーソナルコンピュータ用として広く使用されているＩＤＥ（ＡＴＡ）のインタフェースを持つ安価なＨＤＤが用いられる。一方、デジタルチューナ（ＢＳチューナ、ＣＳチューナ）等の電子機器においては、デジタルデータ（デジタルビデオデータ、デジタルオーディオデータ）のインタフェースとしてＩＥＥＥ１３９４インタフェースが広く用いられている。

【０１２３】

図１３のように１３９４インタフェースとＩＤＥインタフェースとを設けることで、ＩＥＥＥ１３９４とＩＤＥの変換ブリッジ機能をデータ転送制御装置に実現させることが可能になる。

【０１２４】

ストリームインタフェース６４０、６４２は、データ転送制御装置６００とストリームデータ受信装置や映像出力装置との間のインタフェースを実現する回路である。例えばデジタル放送の受信波から抽出した動画のストリームデータの受信処理や、映像出力装置に対するストリームデータの送信処理が行われる。

【０１２５】

またデータ転送制御装置６００は、ＤＥＳに準拠した暗号化処理及び復号化処理を行うＤＥＳ回路６５０、６６０、６６２を含む。ＤＥＳ回路６５０は、暗号化処理したデータをＩＤＥインタフェース６３０に出力したり、ＩＤＥインタフェース６３０からのデータを復号化処理したりする。ＤＥＳ回路６６０は、暗号化処理したデータをストリームインタフェース６４０に出力したり、ストリームインタフェース６４０からのデータを復号化処理したりする。ＤＥＳ回路６６２は、暗号化処理したデータをストリームインタフェース６４２に出力したり、ストリームインタフェース６４２からのデータを復号化処理したりする。

【０１２６】

データ転送制御装置は、ＳＤＲＡＭ（Synchronous Dynamic Random Access Memory）とのインタフェースを実現するＳＤＲＡＭインタフェース６７０を含む。ここでＳＤＲＡＭは、ランダムアクセスに比べてシーケンシャルアクセス（連続したアドレスへのアクセス）を高速に行うことができるメモリである。また、連続したアドレスのデータ（バーストデータ）をクロックに同期して入出力できるメモリである。このＳＤＲＡＭはアイソクロナスデータのキャッシュメモリとして機能する。

【０１２７】

なお、ＳＤＲＡＭは、データ転送制御装置６００の外部に設けることが望ましいが、データ転送制御装置の内部に設けることも可能である。また、通常のＳＤＲＡＭの代わりに、例えばＤＤＲ型ＳＤＲＡＭ、ラムバス（Rambus）社のＲＤＲＡＭなどの高速な同期型メモリを採用してもよい。

【０１２８】

また、ＳＤＲＡＭの記憶領域を、送信領域と受信領域に分離したり、アシンクロナス領域とアイソクロナス領域に分離したりしてもよい。

【０１２９】
データ転送制御装置６００は、パケットメモリ６８０を含む。パケットメモリ６８０は、パケット転送用のＲＡＭであり、ＳＤＲＡＭに比べて小容量なメモリである。またパケットメモリ６８０は、ランダムアクセスを高速に行うことができるメモリである。
【０１３０】
パケットメモリ６８０は、ＩＥＥＥ１３９４規格に準拠したバスを介して受信したパケットを一時的に記憶する機能を有する。また記憶媒体から読み出されたパケットを、ＩＥＥＥ１３９４に準拠したバスを介して転送するために、一時的に記憶する機能も有する。更にストリームインタフェース６４０、６４２を介して受信されたストリームデータのパケットを、ＩＤＥに準拠したバスやＩＥＥＥ１３９４規格に準拠したバスを介して転送するために、一時的に記憶する機能も有する。或いは、ＩＥＥＥ１３９４規格に準拠したバスを介して受信したパケットや、記憶媒体から読み出されたパケットを、ストリームインタフェース６４０、６４２を介して送信するために、一時的に記憶する機能も有する。
【０１３１】
データ転送制御装置６００は、コンテンツ保護回路６９０を含む。コンテンツ保護回路６９０は、パケットメモリ６８０から読み出されたデータ（アイソクロナスデータ）を暗号化処理により暗号化し、リンクコントローラ６１０側に転送するための処理を行う。また、リンクコントローラ６１０側から転送される暗号化データ（暗号化アイソクロナスデータ）を復号化処理により復号化し、パケットメモリ６８０に書き込むための処理を行う。
【０１３２】
このコンテンツ保護回路６９０の処理は、ＩＥＥＥ１３９４規格に準拠したバスにより接続された電子機器（デバイス）間で、暗号化データを送受信するために行われる。この場合、保護されるべき暗号化データを電子機器間で送受信する前に、データ保護機構を受信側の電子機器が備えているか否かを確認する認証処理を行う。そして、保護機構を備えている事が認証処理により確認されると、暗号を解くための鍵を電子機器間で交換する。そして、送信側の電子機器は暗号化データを送信し、受信側の電子機器は受信した暗号化データを復号化する。
【０１３３】
このようにすることで、電子機器間でのみ保護データの送受信を行えるようになる。これにより、保護機構を有しない電子機器や、データを改変してしまうような電子機器から、データのコンテンツを保護できる。
【０１３４】
また、コンテンツ提供者が設定したコピー制御情報が電子機器間でやり取りされる。これにより、「コピー禁止」、「１回だけコピー可能」、「コピー・フリー」などのコピー制御が可能になる。また、コンテンツと共に改訂情報（System Renewability Messages）が配布される。これにより、不正な電子機器へのデータ転送を禁止したり制限したりすることが可能になり、不正コピーを将来に渡り禁止できる。
【０１３５】
データ転送制御装置６００は、ＣＰＵマクロ７００、セキュリティ回路７１０、ＣＰＵＲＡＭ７２０、ＤＥＳ回路７３０を含む。ＣＰＵマクロ７００は、図１及び図５に示すＣＰＵマクロ４０の機能を有する。セキュリティ回路７１０は、図１及び図５に示すセキュリティ回路３０の機能を有する。ＣＰＵＲＡＭ７２０は、図１に示すメモリ２０又は図５に示すＲＡＭ２１０の機能を有する。ＤＥＳ回路７３０は、図５に示す復号化処理部２８０等（復号化処理部２８０、復号化鍵データ保持部２８２、復号化鍵固有データ保持部２８４、復号化鍵データ結合部２８６）の機能を有する。
【０１３６】
ＣＰＵマクロ７００は、ＣＰＵＲＡＭ７２０に記憶されたソースコード（ソースプログラム及びコンテンツ保護回路６９０の処理をするためのパラメータ（鍵データ））に対応した処理を実行し、データ転送制御装置６００の各部を制御する。このＣＰＵマクロ７０

０は、例えばコンテンツ保護回路６９０の処理を実行する。ソースコードは、データ転送制御装置６００の内部又は外部に設けられたフラッシュＲＯＭから、暗号化されたソースコードの状態で読み出され、一旦ＣＰＵＲＡＭ７２０に書き込まれる。その後、ＤＥＳ回路７３０で復号化して再びＣＰＵＲＡＭ７２０に展開する。セキュリティ回路７１０は、デバッガによる機密漏洩を防止するために、上記の実施形態で説明したようにＣＰＵＲＡＭ７２０へのセキュリティプロテクトを行う。

【０１３７】

図１４に、図１３のデータ転送制御装置を含む電子機器のブロック図の例を示す。図１４では、電子機器としてデジタルテレビ放送を受信するためのデジタルチューナとしての機能を有するセットトップボックス（set-top box）のブロック図の例を示している。また図１５に、図１４の電子機器の外観図の例を示す。

【０１３８】

電子機器８００は、データ転送制御装置６００、デジタル放送復調回路８２０、物理層コントローラ８３０、フラッシュＲＯＭ８４０、操作部８５０、表示部８６０、ＭＰＥＧデコーダ８７０を含む。この電子機器８００は、ＩＥＥＥ１３９４又はＵＳＢ２．０に準拠したバスを介してＨＤＤレコーダ９００に接続される。

【０１３９】

即ち本実施形態における電子機器は、データ転送制御装置６００と、フラッシュＲＯＭ３００（外部メモリ、不揮発性メモリ）とを含むということができる。データ転送制御装置６００は、本実施形態における半導体装置１０、２００の機能と、汎用シリアルバスインタフェース（リンクコントローラ等）の機能とを含むということができる。この場合、データ転送制御装置６００では、フラッシュＲＯＭ３００に記憶されたデータが、ＣＰＵＲＡＭ７２０に転送され、ＣＰＵマクロ７００が、ＣＰＵＲＡＭ７２０の記憶データに基づいて、汎用シリアルバスインタフェースを介して転送されるデータの加工処理（コンテンツ保護のための処理）を行うということができる。

【０１４０】

なお図１４では、ＩＤＥインタフェースにＨＤＤを設けずに、外部に設けられたＨＤＤレコーダ９００に、ストリームデータが保存される。

【０１４１】

デジタル放送復調回路８２０は、チャネルデコーダ８２２、デスクランブラ８２４を含む。チャネルデコーダ８２２は、アンテナ９１０で受信されたデジタル放送の受信波から１チャネル分のストリームデータを抽出する。デスクランブラ８２４は、スクランブル処理されたストリームデータに対して該スクランブル処理を解除する処理を行う。デスクランブラ８２４は、図１３のストリームインタフェース６４０に接続される。

【０１４２】

物理層コントローラ８３０は、図１３の物理層インタフェース６２０に接続され、ＨＤＤレコーダ９００との間で、ＩＥＥＥ１３９４規格に準拠した物理層のデータ転送制御を行う。

【０１４３】

フラッシュＲＯＭ８４０は、図１３のＣＰＵマクロ７００に接続される。このフラッシュＲＯＭ８４０には、ＣＰＵマクロ７００が実行するプログラム及びパラメータ（コンテンツ保護のためのパラメータ）が暗号化された状態で記憶される。

【０１４４】

ＭＰＥＧデコーダ８７０は、図１３のストリームインタフェース６４２に接続され、データ転送制御装置６００からのストリームデータをデコードし、デジタルテレビ９２０に出力する。

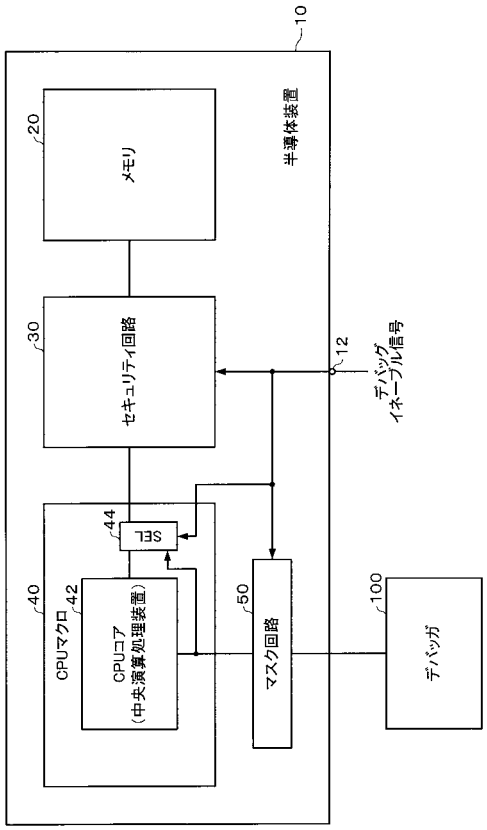
【０１４５】

ユーザは、操作部８５０を操作することで、デジタル放送の受信チャネルの指定などを行うことができる。また、表示部８６０に表示される情報を見ることで、現在の受信チャネルなどを確認できる。

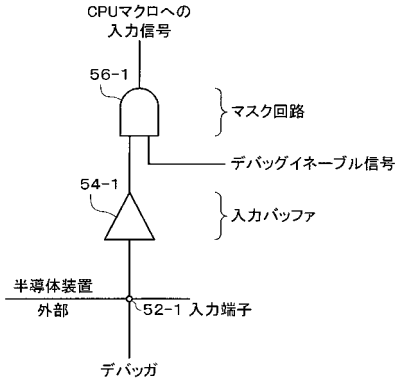
【０１４６】
この電子機器８００は、ＩＥＥＥ１３９４バス又はＵＳＢ２．０などの汎用（高速）シリアルバスを介してＨＤＤレコーダ９００に接続されている。そしてデジタル放送復調回路８２０からのＭＰＥＧ（Moving Picture Experts Group）規格に準拠したストリームデータを、ＨＤＤレコーダ９００に保存したり、ＭＰＥＧデコーダ８７０でデコードしてデジタルテレビ９２０に映像を出力させたりできる。
【０１４７】
ＨＤＤレコーダ９００へのストリームデータの記録時においては、アンテナ９１０で受信されたＭＰＥＧ規格に準拠したストリームデータ（ＴＳパケット）が、データ転送制御装置６００、ＩＥＥＥ１３９４（ＵＳＢ２．０）を介してＨＤＤレコーダ９００に書き込まれる。
【０１４８】
一方、ＨＤＤレコーダ９００のストリームデータの再生時においては、ＩＥＥＥ１３９４のバスを介してＨＤＤレコーダ９００からＭＰＥＧ規格に準拠したストリームデータ（ＴＳパケット、アイソクロナスデータ）が読み出される。そして、読み出されたＭＰＥＧ規格に準拠したストリームデータを、ＭＰＥＧデコーダ８７０がデコードする。これにより、デジタルテレビ９２０に映像が映し出される。
【０１４９】
なお、本実施形態が適用される電子機器は図１４及び図１５に示す電子機器に限定されない。例えば、ＨＤＤレコーダ、ＤＶＤレコーダ、ビデオテープレコーダ（ＨＤＤ内蔵）、光ディスク（ＤＶＤ）レコーダ、デジタルビデオカメラ、パーソナルコンピュータ或いは携帯型情報端末などの種々の電子機器に適用できる。また図１４では、ＨＤＤを内蔵しないものとして説明したが、ＨＤＤを内蔵させることも可能である。またＨＤＤレコーダ９００に代えてＤＶＤレコーダ等の記録装置であってもよい。
【０１５０】
図１４の構成によれば、汎用的なデバッガを用いて低コストなシステム開発ができるようになる。しかも、デバッガからの不正なアクセスによるリバースエンジニアリングを防止でき、ライセンス化された極秘情報を確実に保護できるようになる。
【０１５１】
なお、本発明は上述した実施の形態に限定されるものではなく、本発明の要旨の範囲内で種々の変形実施が可能である。例えば、明細書又は図面中の記載において広義や同義な用語は、明細書又は図面中の他の記載においても広義や同義な用語に置き換えることができる。
【０１５２】
更に、上記の実施形態では、主として半導体装置に内蔵するメモリからの読み出しについて説明したが、当業者であれば該メモリへの書き込みについても同様に実現できる。
【０１５３】
更に本実施形態の半導体装置の構成も図１、図５等で説明した構成に限定されず、種々の変形実施が可能である。
【０１５４】
また、本発明のうち従属請求項に係る発明においては、従属先の請求項の構成要件の一部を省略する構成とすることもできる。また、本発明の１の独立請求項に係る発明の要部を、他の独立請求項に従属させることもできる。
【図面の簡単な説明】
【０１５５】
【図１】本実施形態の半導体装置の原理的構成の構成図。
【図２】マスク回路の構成例の回路図。
【図３】マスク回路の他の構成例の回路図。
【図４】マスク回路の更に他の構成例の回路図。
【図５】本実施形態の半導体装置の詳細な構成例及び該半導体装置を用いたシステムの構

成例のブロック図。
【図６】アクセス制御部の構成例のブロック図。
【図７】比較部の動作を説明するためのハードウェア記述言語の記載例を示す図。
【図８】外部システムの機能ブロック図の構成例を示す図。
【図９】図８の外部システムによって行われる照合用パスワードデータの書き込み処理のフローの一例を示す図。
【図１０】図８の外部システムによって行われるソースコードの書き込み処理のフローの一例を示す図。
【図１１】図５のシステムの動作シーケンスの一例を示す図。
【図１２】図５のシステムの動作シーケンスの他の例を示す図。
【図１３】本実施形態における半導体装置が適用されたデータ転送制御装置の構成例のブロック図。
【図１４】図１３のデータ転送制御装置を含む電子機器のブロック図の例。
【図１５】図１４の電子機器の外観図の例を示す図。
【符号の説明】
【０１５６】
１０、２００　半導体装置、１２　デバッグイネーブル信号入力端子、２０　メモリ、
３０　セキュリティ回路、４０　ＣＰＵマクロ、
４２　ＣＰＵコア（中央演算処理装置）、４４　セレクタ、５０　マスク回路、
１００　デバッガ、２１０　ＲＡＭ、２２０　アクセス制御部、２３０　比較部、
２４０　パスワードデータ保持部、２５０　秘密固有データ保持部、
２６０　パスワードデータ生成部、２７０　一方向暗号化処理部、
２８０　復号化処理部、２８２　復号化鍵データ保持部、
２８４　復号化鍵固有データ保持部、２８６　復号化鍵データ生成部、
３００　フラッシュＲＯＭ、３１０　照合用パスワードデータ、
３２０　ソースコード（暗号化）、３３０　復号化用データ

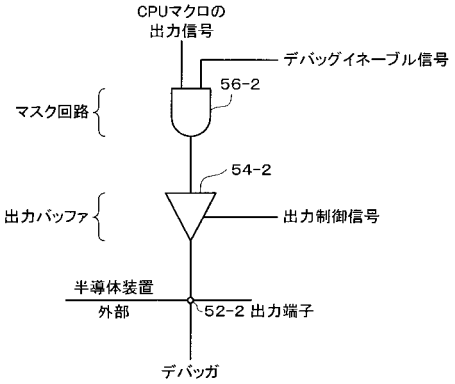
【図１】


10
半導体装置
20
メモリ
30
セキュリティ回路
12
デバッグイネーブル信号
40
CPUマクロ
42
CPUコア
（中央演算処理装置）
44
SEL
50
マスク回路
100
デバッガ

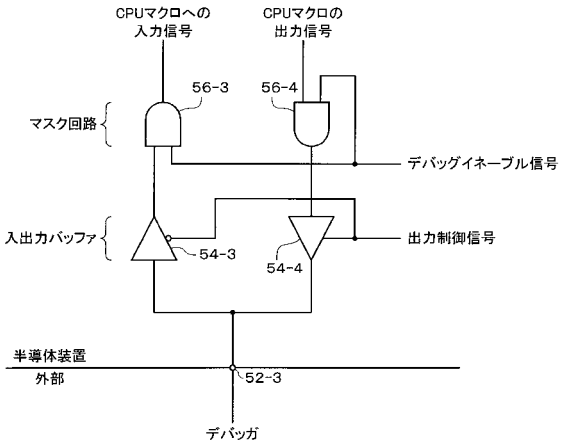
【図２】


CPUマクロへの
入力信号
56-1
マスク回路
デバッグイネーブル信号
54-1
入力バッファ
半導体装置
外部
52-1 入力端子
デバッガ

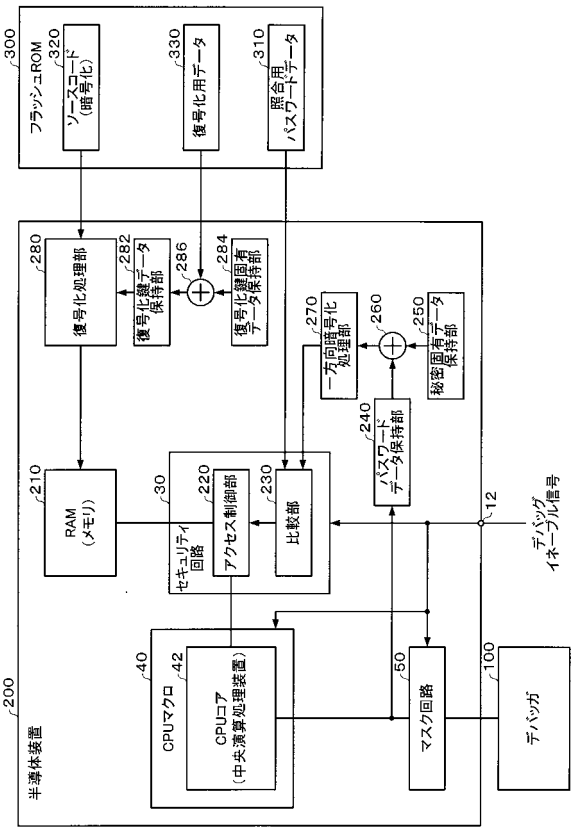
【図３】


CPUマクロの
出力信号
デバッグイネーブル信号
56-2
マスク回路
54-2
出力バッファ
出力制御信号
半導体装置
外部
52-2 出力端子
デバッガ

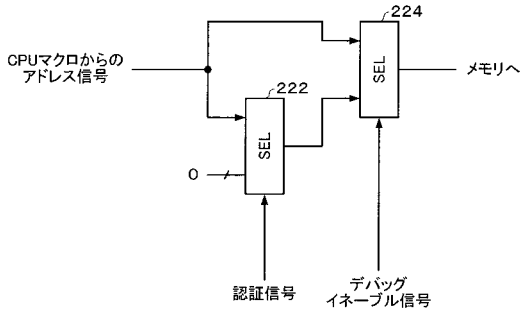
【図４】


CPUマクロへの
入力信号
CPUマクロの
出力信号
56-3
56-4
マスク回路
デバッグイネーブル信号
入出力バッファ
54-3
54-4
出力制御信号
半導体装置
外部
52-3
デバッガ

【図５】


300
フラッシュROM
320
ソースコード
（暗号化）
330
復号化用データ
310
照合用
パスワードデータ
280
復号化処理部
282
復号化鍵データ
保持部
286
284
復号化鍵固有
データ保持部
270
一方向暗号化
処理部
260
250
秘密固有データ
保持部
240
パスワード
データ保持部
210
RAM
（メモリ）
30
セキュリティ
回路
220
アクセス制御部
230
比較部
12
デバッグ
イネーブル信号
200
半導体装置
40
CPUマクロ
42
CPUコア
（中央演算処理装置）
50
マスク回路
100
デバッガ

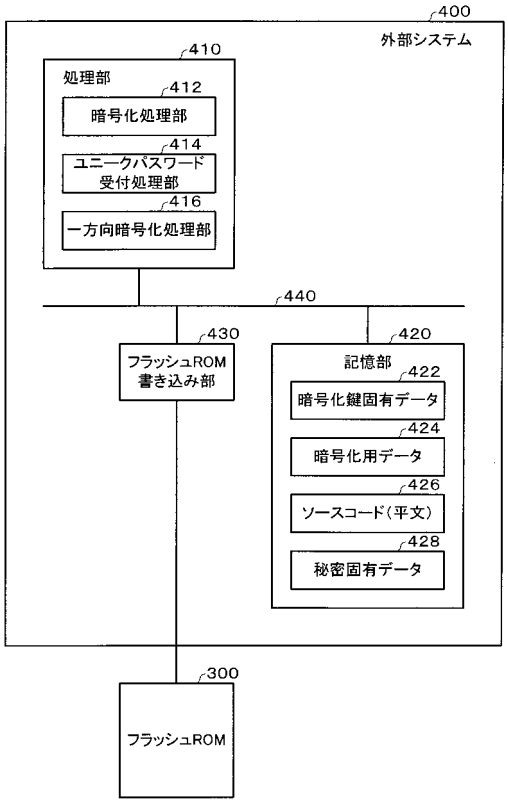
【図６】



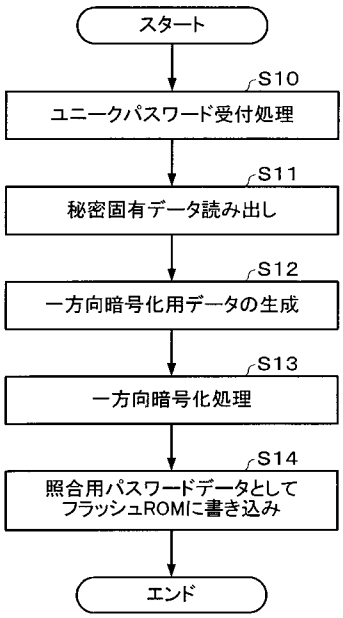
【図７】

```
if (hreset) {
   Flag = 0; Pass = 0;
}
else if ((PSWD == CWD)&&(Flag == 0)) {
        Flag = 1; Pass = 1;
}
else if ((PSWD != CWD)
        Flag = 1; Pass = 0;
}
```

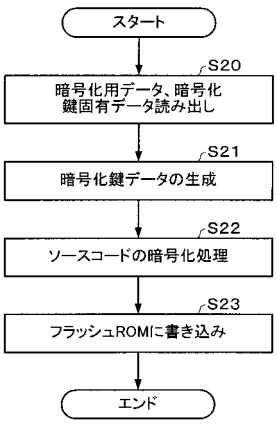
【図８】



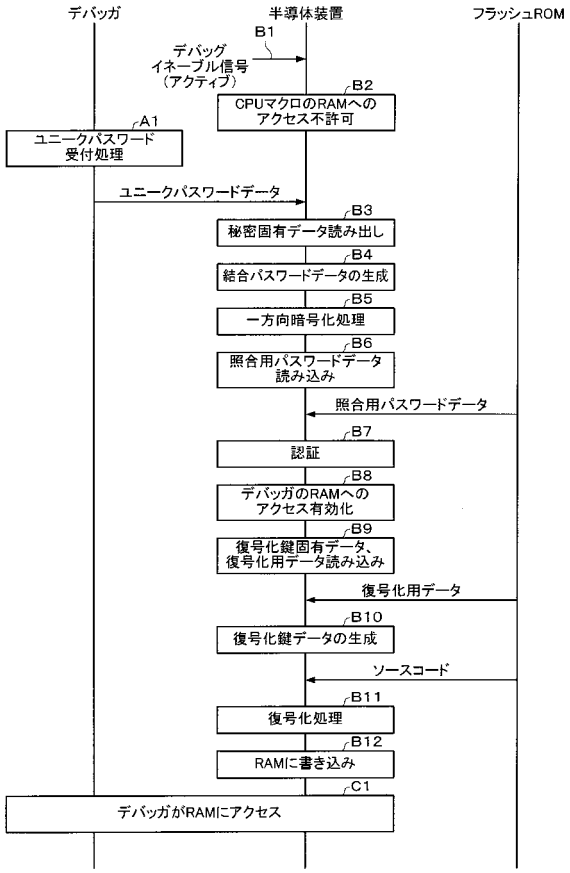
【図９】



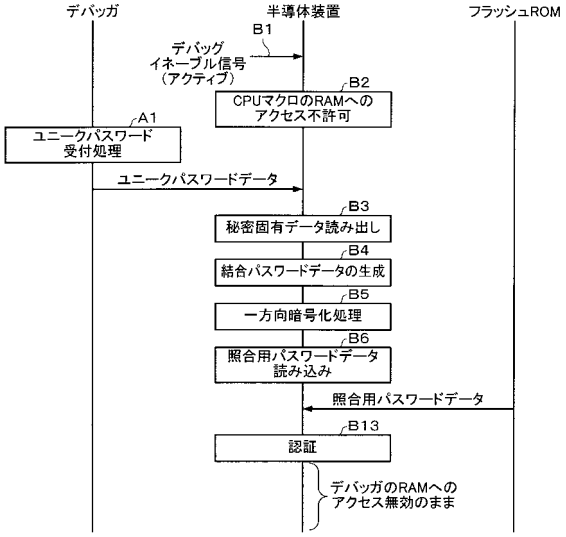
【図１０】



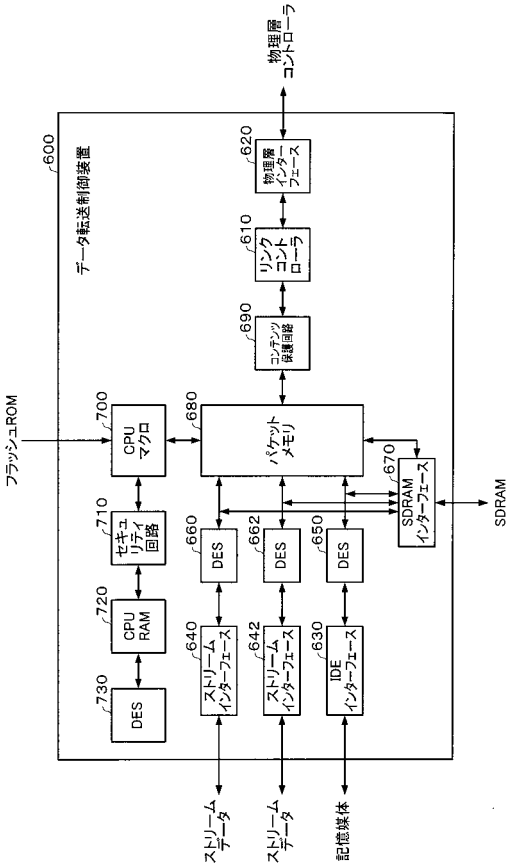
【図１１】



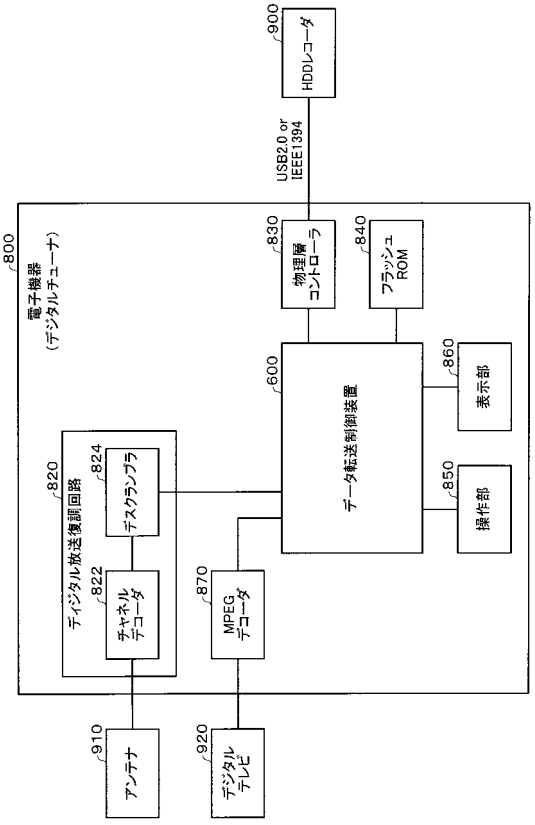
【図１２】



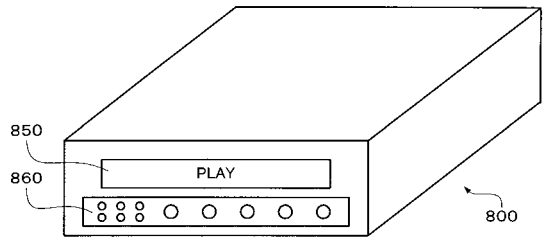
【図１３】



【図１４】



【図１５】



フロントページの続き

(72)発明者　熊谷　友則
長野県諏訪市大和３丁目３番５号　セイコーエプソン株式会社内

審査官　石川　正二

(56)参考文献　特開平０５－２６５８６７（ＪＰ，Ａ）
特開２００３－１７７９３８（ＪＰ，Ａ）
特開平０６－１２４２４１（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／２４