(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2020-194464
(P2020-194464A)
(43)公開日　令和2年12月3日(2020.12.3)

(51)Int.Cl.		F I		テーマコード（参考）
G06F 21/57	(2013.01)	G06F 21/57	350	
G06F 21/62	(2013.01)	G06F 21/62		

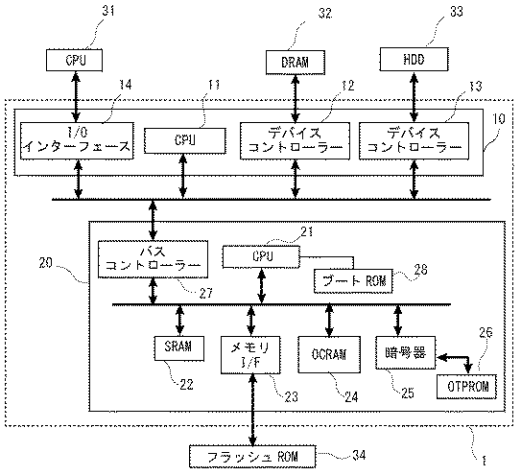
審査請求 未請求　請求項の数 10　ＯＬ　（全 12 頁）

(21)出願番号　特願2019-100841 (P2019-100841)
(22)出願日　令和1年5月30日 (2019.5.30)

(71)出願人　000006150
京セラドキュメントソリューションズ株式会社
大阪府大阪市中央区玉造１丁目２番２８号
(74)代理人　100111202
弁理士　北村　周彦
(72)発明者　立山　善貴
大阪府大阪市中央区玉造１丁目２番２８号　京セラドキュメントソリューションズ株式会社内
(72)発明者　塩瀬　昌人
大阪府大阪市中央区玉造１丁目２番２８号　京セラドキュメントソリューションズ株式会社内

(54)【発明の名称】集積回路及び集積回路の制御方法

(57)【要約】
【課題】集積回路及び集積回路内のデータをセキュリティ脅威から保護する。
【解決手段】データを処理するデータ処理部１０と、データ処理部のセキュリティを管理するセキュリティ管理部２０と、を備える集積回路１であって、セキュリティ管理部２０は、セキュリティ強度の設定値を保持する設定値保持部２６と、設定値によって示されるセキュリティ強度が所定レベル以上である場合に、ブートプログラムに対して署名検証を行うセキュアブートにより集積回路１を起動させる起動制御部と、セキュアブートにおける署名検証によりブートプログラムの改竄が検知されたときに、データ処理部１０をリセット状態にする状態制御部と、を有する。
【選択図】図１



【特許請求の範囲】
【請求項１】
データを処理するデータ処理部と、前記データ処理部のセキュリティを管理するセキュリティ管理部と、を備える集積回路であって、
前記セキュリティ管理部は、
セキュリティ強度の設定値を保持する設定値保持部と、
前記設定値によって示される前記セキュリティ強度が所定レベル以上である場合に、ブートプログラムに対して署名検証を行うセキュアブートにより前記集積回路を起動させる起動制御部と、
前記セキュアブートにおける前記署名検証により前記ブートプログラムの改竄が検知されたときに、前記データ処理部をリセット状態にする状態制御部と、を有することを特徴とする集積回路。
【請求項２】
前記セキュリティ管理部は、
前記設定値によって示される前記セキュリティ強度が所定レベル以上である場合に、前記データ処理部との接続を遮断する接続制御部をさらに備えることを特徴とする請求項１に記載の集積回路。
【請求項３】
前記接続制御部は、前記設定値によって示される前記セキュリティ強度が前記所定レベル以上である場合において前記データ処理部に対するセキュリティ脅威が検知されたときに、前記データ処理部との接続を遮断することを特徴とする請求項２に記載の集積回路。
【請求項４】
前記接続制御部は、前記設定値保持部が前記設定値を保持していない場合に、前記データ処理部との接続を遮断することを特徴とする請求項２又は請求項３に記載の集積回路。
【請求項５】
前記状態制御部は、前記設定値保持部が前記設定値を保持していない場合に、前記データ処理部をリセット状態にすることを特徴とする請求項１から請求項４のうちのいずれか１項に記載の集積回路。
【請求項６】
前記データ処理部は、外部デバイスとの間で入出力されるデータを監視する入出力データ監視部を有し、
前記セキュリティ管理部は、前記データ処理部に対するセキュリティ脅威を検知するセキュリティ脅威検知部をさらに有し、
前記セキュリティ脅威検知部は、前記設定値によって示される前記セキュリティ強度が前記所定レベル以上である場合において前記入出力データ監視部によって検知された平文が不当であるときに、セキュリティ脅威を検知することを特徴とする請求項１から請求項５のうちのいずれか１項に記載の集積回路。
【請求項７】
前記セキュリティ脅威検知部は、前記外部デバイスとの間で入出力されるデータが暗号化格納領域から読み出されたデータである場合において該データから平文が検知されたときに、該平文が不当であると判断することを特徴とする請求項６に記載の集積回路。
【請求項８】
前記セキュリティ管理部は内蔵メモリをさらに有し、
前記内蔵メモリには、前記集積回路の外部から前記ブートプログラムを書き込むことが可能であり、
前記起動制御部は、前記内蔵メモリに前記ブートプログラムが書き込まれている場合には、前記セキュアブートにおいて、前記内蔵メモリに書き込まれている前記ブートプログラムに対して前記署名検証を行い、該ブートプログラムを用いて前記集積回路を起動させることを特徴とする請求項１から請求項７のうちのいずれか１項に記載の集積回路。
【請求項９】

前記起動制御部は、前記設定値によって示される前記セキュリティ強度が前記所定レベル未満である場合には、前記署名検証を行わない通常ブートにより前記集積回路を起動させることを特徴とする請求項１から請求項８のうちのいずれか１項に記載の集積回路。
【請求項１０】
データを処理するデータ処理部と、前記データ処理部のセキュリティを管理するセキュリティ管理部と、を有する集積回路の制御方法であって、
前記セキュリティ管理部が、セキュリティ強度の設定値を予め保持し、該設定値によって示される前記セキュリティ強度が所定レベル以上である場合に、ブートプログラムに対して署名検証を行うセキュアブートにより前記集積回路を起動させる起動制御工程と、
前記セキュリティ管理部が、前記セキュアブートにおける前記署名検証により前記ブートプログラムの改竄が検知されたときに、前記データ処理部をリセット状態にする接続制御工程と、を有することを特徴とする制御方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、集積回路及び集積回路の制御方法に関する。
【背景技術】
【０００２】
画像形成装置等の情報処理装置には、各種処理を実行させるための集積回路が搭載されている。例えば、ＭＦＰ（Ｍｕｌｔｉ　Ｆｕｎｃｔｉｏｎ　Ｐｅｒｉｐｈｅｒａｌ）等の画像形成装置には、画像処理を実行させるためのＬＳＩ（大規模集積回路）が搭載されている。
【０００３】
上記のようなＬＳＩでは、セキュリティの保護を必要とするデータが扱われる場合があり、近年、それらのデータをセキュリティ脅威から保護するための技術が提案されている。特許文献１には、フラッシュメモリを含むメモリシステムにおいて、暗号化エンジンが、ＣＰＵによって予め設定されたセキュリティコンフィグレーション情報に基づいて、外部デバイスとの間で入出力されるデータの暗号化及び復号を行う方法が記載されている。特許文献１に記載の方法によれば、外部デバイスへの意図しないデータの流出を防止することができる。
【先行技術文献】
【特許文献】
【０００４】
【特許文献１】特表２００８－５２４９６９号公報
【発明の概要】
【発明が解決しようとする課題】
【０００５】
ところで、集積回路がセキュリティ脅威に侵された場合、集積回路のファームウェア（ＦＷ）が改竄され、集積回路が異常動作する可能性がある。
【０００６】
一方、特許文献１に記載の方法は、ＣＰＵにより設定されるセキュリティコンフィグレーション情報によって、暗号化エンジンを制御している。そのため、セキュリティ脅威によりＦＷが改竄されＣＰＵが異常動作した場合、暗号化エンジンが正常に機能しなくなる可能性がある。またその場合、外部デバイスへの意図しないデータの流出が発生するなどして、システムのセキュリティが保護されなくなるおそれがある。
【０００７】
本発明は例えば上述したような問題に鑑みなされたものであり、本発明の課題は、集積回路及び集積回路内のデータをセキュリティ脅威から保護することにある。
【課題を解決するための手段】
【０００８】

上記課題を解決するために、本発明の集積回路は、データを処理するデータ処理部と、データ処理部のセキュリティを管理するセキュリティ管理部と、を備える集積回路であって、セキュリティ管理部は、セキュリティ強度の設定値を保持する設定値保持部と、設定値によって示されるセキュリティ強度が所定レベル以上である場合に、ブートプログラムに対して署名検証を行うセキュアブートにより集積回路を起動させる起動制御部と、セキュアブートにおける署名検証によりブートプログラムの改竄が検知されたときに、データ処理部をリセット状態にする状態制御部と、を有することを特徴とする。

【０００９】

また、上記本発明の集積回路において、セキュリティ管理部は、設定値によって示されるセキュリティ強度が所定レベル以上である場合に、データ処理部との接続を遮断する接続制御部をさらに備える構成としてもよい。

【００１０】

また、上記本発明の集積回路において、接続制御部は、設定値によって示されるセキュリティ強度が所定レベル以上である場合においてデータ処理部に対するセキュリティ脅威が検知されたときに、データ処理部との接続を遮断することとしてもよい。

【００１１】

また、上記本発明の集積回路において、接続制御部は、設定値保持部が設定値を保持していない場合に、データ処理部との接続を遮断することとしてもよい。

【００１２】

また、上記本発明の集積回路において、状態制御部は、設定値保持部が設定値を保持していない場合に、データ処理部をリセット状態にすることとしてもよい。

【００１３】

また、上記本発明の集積回路において、データ処理部は、外部デバイスとの間で入出力されるデータを監視する入出力データ監視部を有し、セキュリティ管理部は、データ処理部に対するセキュリティ脅威を検知するセキュリティ脅威検知部をさらに有し、セキュリティ脅威検知部は、設定値によって示されるセキュリティ強度が所定レベル以上である場合において入出力データ監視部によって検知された平文が不当であるときに、セキュリティ脅威を検知する構成としてもよい。

【００１４】

また、上記本発明の集積回路において、セキュリティ脅威検知部は、外部デバイスとの間で入出力されるデータが暗号化格納領域から読み出されたデータである場合において該データから平文が検知されたときに、該平文が不当であると判断することとしてもよい。

【００１５】

また、上記本発明の集積回路において、セキュリティ管理部は内蔵メモリをさらに有し、内蔵メモリには、集積回路の外部からブートプログラムを書き込むことが可能であり、起動制御部は、内蔵メモリにブートプログラムが書き込まれている場合には、セキュアブートにおいて、内蔵メモリに書き込まれているブートプログラムに対して署名検証を行い、該ブートプログラムを用いて集積回路を起動させる構成としてもよい。

【００１６】

さらに、上記本発明の集積回路において、起動制御部は、設定値によって示されるセキュリティ強度が所定レベル未満である場合には、署名検証を行わない通常ブートにより集積回路を起動させることとしてもよい。

【００１７】

上記課題を解決するために、本発明の集積回路の制御方法は、データを処理するデータ処理部と、制御方法ことを特徴とするデータ処理部のセキュリティを管理するセキュリティ管理部と、を有する集積回路の制御方法であって、セキュリティ管理部が、セキュリティ強度の設定値を予め保持し、該設定値によって示されるセキュリティ強度が所定レベル以上である場合に、ブートプログラムに対して署名検証を行うセキュアブートにより集積回路を起動させる起動制御工程と、セキュリティ管理部が、セキュアブートにおける署名検証によりブートプログラムの改竄が検知されたときに、データ処理部をリセット状態に

する接続制御工程と、を有することを特徴とする。
【発明の効果】
【００１８】
本発明によれば、集積回路及び集積回路内のデータをセキュリティ脅威から保護する。
【図面の簡単な説明】
【００１９】
【図１】本発明の一実施形態に係る集積回路の構成の一例を示すブロック図である。
【図２】セキュリティ管理部の機能ブロックを示す図である。
【図３】セキュアブートの流れの一例を示すフローチャートである。
【図４】セキュアブートの流れの他の例を示すフローチャートである。
【発明を実施するための形態】
【００２０】
以下、図面を参照しつつ、本発明の一実施形態に係る集積回路について説明する。
【００２１】
（集積回路の構成）
図１は、本発明の一実施形態に係る集積回路の構成の一例を示すブロック図である。図１に示すように、集積回路１は、データ処理部１０と、ＳＣＵ（セキュリティ管理部）２０とを備える。集積回路１は、ＬＳＩであり、画像処理装置などの情報処理装置に搭載されるＳｏＣ（Ｓｙｓｔｅｍ ｏｎ ａ ｃｈｉｐ）やＡＳＩＣ（Ａｐｐｌｉｃａｔｉｏｎ Ｓｐｅｃｉｆｉｃ Ｉｎｔｅｇｒａｔｅｄ Ｃｉｒｃｕｉｔ）である。集積回路１は、ＣＰＵ３１（以下、外部ＣＰＵ３１と記す）、ＤＲＡＭ３２、ＨＤＤ３３、及びフラッシュＲＯＭ３４と接続され、これらの外部デバイス３１～３４との間でデータの入出力を行う。なお、集積回路１には、その他の外部デバイスが接続されていてもよい。
【００２２】
データ処理部１０は、ＣＰＵ１１（以下、メインＣＰＵ１１と記す）と、デバイスコントローラー１２，１３と、Ｉ／Ｏインターフェース１４とを有する。
【００２３】
デバイスコントローラー１２は、ＤＤＲメモリコントローラ（ＤＤＲＭＣ）であり、ＤＲＡＭ３２を制御する。なお、ＤＲＡＭ以外のメモリがデバイスコントローラー１２に接続されていてもよい。つまり、デバイスコントローラー１２は、ＤＲＡＭ以外のメモリを制御するメモリコントローラであってもよい。
【００２４】
デバイスコントローラー１３は、ＨＤＤ３３を制御する。本実施形態では、デバイスコントローラー１３とＨＤＤ３３とは、シリアルＡＴＡ（ＳＡＴＡ）で接続されているものとする。また、デバイスコントローラー１３は、フルディスクエンクリプション（Ｆｕｌｌ Ｄｉｓｋ Ｅｎｃｒｙｐｔｉｏｎ）機能を有し、ＨＤＤ３３内のデータを一括して暗号化することが可能である。なお、デバイスコントローラー１３は、ＨＤＤ３３内のデータをセクター単位で暗号化することも可能である。また、デバイスコントローラー１３に接続される記憶装置はＨＤＤに限らず、例えばＳＡＴＡのＳＳＤ（Ｓｏｌｉｄ Ｓｔａｔｅ Ｄｒｉｖｅ）が接続されていてもよい。また、ＳＡＴＡ以外のインターフェースの記憶装置が接続されてもよい。
【００２５】
また、デバイスコントローラー１２，１３は、ＤＲＡＭ３２やＨＤＤ３３との間で入出力されるデータを監視し、平文を検知した場合に、ハードウェア割り込みを発する、入出力データ監視部として機能を有する。
【００２６】
Ｉ／Ｏインターフェース１４は、シリアルインターフェースである。本実施形態では、Ｉ／Ｏインターフェース１４は、ＰＣＩｅＥＰ（ＰＣＩＥｘｐｒｅｓｓエンドポイント）である。
【００２７】

セキュリティ管理部２０は、集積回路１のセキュリティを管理する。セキュリティ管理部２０は、ＣＰＵ２１（以下、サブＣＰＵ２１と記す）と、ＳＲＡＭ２２と、メモリＩ／Ｆ２３と、ＯＣＲＡＭ（内蔵メモリ）２４と、暗号器２５と、ＯＴＰ（Ｏｎｅ Ｔｉｍｅ Ｐｒｏｇｒａｍｍａｂｌｅ）ＲＯＭ２６とを有する。また、セキュリティ管理部２０は、ブートＲＯＭ２８と、バスコントローラ２７とを有する。

【００２８】

メモリＩ／Ｆ２３は、フラッシュＲＯＭ３４を接続するインターフェースである。本実施形態では、フラッシュＲＯＭ３４に、集積回路１を起動させるためのプログラム（起動プログラム又はブートプログラムと呼ぶ）が格納されているものとする。ＯＴＰＲＯＭ２６は、後述するセキュリティ強度の設定値を記憶する、設定値保持部として機能する。またＯＴＰＲＯＭ２６は、暗号器２５で使用される情報（例えば秘密鍵）を記憶する。

【００２９】

バスコントローラ２７は、データ処理部１０とセキュリティ管理部２０とを接続するバスを制御する。

【００３０】

（集積回路のセキュリティ保護）

【００３１】

セキュリティ管理部２０は、ＯＴＰＲＯＭ２６が保持するセキュリティ強度の設定値に応じて、集積回路１のセキュリティ強度を切り替える。本実施形態では、セキュリティ強度の設定値が０である場合には、セキュリティ管理部２０は、セキュリティ強度を「保護なし（Ｎｏｎ－Ｓｅｃｕｒｅ）」に設定する。一方、セキュリティ強度の設定値が１である場合には、セキュリティ管理部２０は、セキュリティ強度を「保護あり（Ｓｅｃｕｒｅ）」に設定する。なお、セキュリティ強度は０と１の２つのレベルに限らず、３つ以上のレベルを有してもよい。例えば、「保護あり（Ｓｅｃｕｒｅ）」のレベルを複数段階に分けて設定するようにしてもよい。

【００３２】

セキュリティ強度が「保護あり」に設定されている場合には、バスコントローラ２７がデータ処理部１０とセキュリティ管理部２０とのインターフェース（バス）を遮断する。これにより、セキュリティ管理部２０を外部のセキュリティ脅威から保護することができる。

【００３３】

また、セキュリティ強度が「保護あり」に設定されている場合には、集積回路１に電源が投入されたときにセキュアブートが行われる。セキュアブートの詳細については、図３を用いて後述する。セキュアブート中にセキュリティ脅威が検知された場合には、セキュリティ管理部２０は、データ処理部１０をリセット状態にする。これにより、データ処理部１０がセキュリティ脅威によって異常動作することを抑止することができる。

【００３４】

さらに、セキュリティ強度が「保護あり」に設定されている場合において、デバイスコントローラー１２，１３から平文が検知されたことを示すハードウェア割り込みを受信した場合には、セキュリティ管理部２０は、平文の妥当性を検証する。そして、平文が不当であった場合には、セキュリティ管理部２０は、データ処理部１０をリセット状態にする。ここで、「平文の妥当性」の検証とは、平文の内容を検証する意味ではなく、平文の出力があり得るか否かを検証する意味である。例えば、ＨＤＤ３３において暗号化されたデータが記憶されているはずのセクター（暗号化データ格納領域と呼ぶ）から読み取られたデータが平文であった場合、セキュリティ管理部２０は、その平文を不当な平文であると判断する。

【００３５】

セキュリティ強度が「保護なし」に設定されている場合には、電源投入時にセキュアブートは行われず、集積回路１は通常ブートする。また、バスコントローラ２７はデータ処理部１０とセキュリティ管理部２０とのインターフェースを開放する。

【００３６】
なお、集積回路１の製造時などＯＴＰＲＯＭ２６が初期状態にある場合には、上記設定情報がＯＴＰＲＯＭ２６内に存在しない。その場合、セキュリティ管理部２０によるデータ処理部１０のセキュリティ保護が機能しなくなったり、外部デバイス３１～３４への意図しないデータの流出が発生したりする可能性がある。そこで、本実施形態では、ＯＴＰＲＯＭ２６が初期状態にある場合には、セキュリティ管理部２０は、バスコントローラ２７を制御してデータ処理部１０とセキュリティ管理部２０とのインターフェース（バス）を遮断する。これにより、セキュリティ管理部２０を外部のセキュリティ脅威から保護することができる。また、セキュリティ管理部２０は、データ処理部１０をリセット状態にする。これにより、データ処理部１０がセキュリティ脅威によって異常動作することを抑止することができる。
【００３７】
（セキュリティ管理部）
図２は、セキュリティ管理部２０の機能ブロックを示す図である。セキュリティ管理部２０のサブＣＰＵ２１は、例えばフラッシュＲＯＭ３４に記憶されたコンピュータープログラムを読み取って実行することにより、起動制御部２０１、接続制御部２０２、状態制御部２０３、及びセキュリティ脅威検知部２０４として機能する。
【００３８】
起動制御部２０１は、ＯＴＰＲＯＭ２６が保持するセキュリティ強度の設定値に基づいて、集積回路１のブートシーケンスを切り替える。本実施形態では、起動制御部２０１は、セキュリティ強度の設定値が所定値（ここでは１）以上である場合、すなわち、セキュリティ強度が所定レベル以上である場合に、ブートプログラムに対して署名検証を行う、セキュアブートを実行する。セキュアブートについては、図３を用いて詳述する。一方、セキュリティ強度が所定レベル未満である場合には、ブートプログラムに対して署名検証を行わない、通常ブートを実行する。
【００３９】
接続制御部２０２は、バスコントローラ２７を用いて、ＯＴＰＲＯＭ２６が保持するセキュリティ強度の設定値に基づきデータ処理部１０との接続を遮断したり開放したりする。本実施形態では、接続制御部２０２は、セキュリティ強度の設定値が所定値以上である場合、すなわち、セキュリティ強度が所定レベル以上である場合に、データ処理部１０との接続を遮断する。なお、データ処理部１０との接続の遮断は、セキュリティ強度が所定レベル以上である場合において、必要に応じて（例えば、セキュアブートの実行中やセキュリティ脅威が検出されたとき）行われるようにしてもよい。
【００４０】
状態制御部２０３は、セキュアブートの署名検証においてブートプログラムの改竄が検知された場合に、データ処理部１０をリセット状態にする。また、セキュリティ強度の設定値が所定値以上である場合においてセキュリティ脅威が検知された際に、データ処理部１０をリセット状態にする。なお、本実施形態では、サブＣＰＵ２１と、データ処理部１０のメインＣＰＵ１１及びデバイスコントローラー１２，１３のそれぞれとの間に、リセット制御用の信号線（不図示）が設けられているものとする。そして、サブＣＰＵ２１が上記信号線を介して、メインＣＰＵ１１及びデバイスコントローラー１２，１３のそれぞれに、リセット状態とリセット解除状態とを切り替える制御信号を出力するものとする。
【００４１】
セキュリティ脅威検知部２０４は、デバイスコントローラー１２，１３から平文を検知したことを示すハードウェア割り込みを受信した場合に、平文の妥当性を判断する。そして、平文が不当である場合には、セキュリティ脅威検知部２０４は、データ処理部１０がセキュリティ脅威に侵されていると判断する。
【００４２】
（セキュアブート）
【００４３】

セキュアブートでは、セキュリティ管理部２０が、外部デバイス２からロードしたＦＷを復号し、復号したＦＷに対して署名検証を行う。そして、署名検証においてＦＷの改竄が検知された場合、セキュリティ管理部２０はデータ処理部１０をリセット状態にする。図３は、本発明の一実施形態に係るセキュアブートの流れを示すフローチャートである。図３には、集積回路１の内蔵ＣＰＵ（データ処理部１０のメインＣＰＵ１１）がセキュアブートで起動される場合のフローが示されている。ここでは、フラッシュＲＯＭ３４が図１に示されるように、セキュリティ管理部２０に接続されているものとする。

【００４４】

集積回路１に電源が投入されると、図３に示すように、集積回路１内部の初期設定が行われ（ステップＳ３０１）、セキュリティ管理部２０が起動する（ステップＳ３０２）。すると、セキュリティ管理部２０のサブＣＰＵ２１が、ブートＲＯＭ２８に記憶された第１ブートプログラムを読み出して、該第１ブートプログラムに従って第１起動処理（第１ブートシーケンス）を開始する（ステップＳ３０３）。第１起動処理において、サブＣＰＵ２１が、フラッシュＲＯＭ３４との通信を確立する（ステップＳ３０４）。そして、サブＣＰＵ２１が、フラッシュＲＯＭ３４から第２ブートプログラムを読み出して、該第２ブートプログラムをＳＲＡＭ２２に展開する（Ｓ３０５）。ここでは、第２ブートプログラムが暗号化されているものとする。なお、第２ブートプログラムが暗号化されていない場合には、ステップＳ３０５の後、処理はステップＳ３０８に移行する。

【００４５】

次いで、サブＣＰＵ２１が、ＳＲＡＭ２２に展開された第２ブートプログラムを暗号器２５により復号し、署名検証を行う（ステップＳ３０６）。署名検証の結果、改竄が検知された場合は（ステップＳ３０７：ＹＥＳ）、サブＣＰＵ２１が、データ処理部１０をリセット状態にして（ステップＳ３１８）、処理を終了する。改竄が検知されない場合は（ステップＳ３０７：ＮＯ）、サブＣＰＵ２１が、第２ブートプログラムに従って第２起動処理（第２ブート）を開始する（ステップＳ３０８）。

【００４６】

第２起動処理において、サブＣＰＵ２１が、フラッシュＲＯＭ３４から第３ブートプログラムを読み出して、該第３ブートプログラムをＳＲＡＭ２２に展開する（Ｓ３０９）。ここでは、第３ブートプログラムが暗号化されているものとする。なお、第３ブートプログラムが暗号化されていない場合には、処理はステップＳ３１２に移行する。

【００４７】

次いで、サブＣＰＵ２１が、ＳＲＡＭ２２に展開された第３ブートプログラムを暗号器２５により復号し、署名検証を行う（ステップＳ３１０）。署名検証の結果、改竄が検知された場合は（ステップＳ３１１：ＹＥＳ）、サブＣＰＵ２１が、データ処理部１０をリセット状態にして（ステップＳ３１８）、処理を終了する。改竄が検知されない場合は（ステップＳ３１１：ＮＯ）、サブＣＰＵ２１が、第３ブートプログラムに従って第３起動処理（第３ブート）を開始する（ステップＳ３１２）。

【００４８】

第３起動処理において、サブＣＰＵ２１が、システムバスの設定を行い、ＤＲＡＭ３２を初期化し、さらにＤＲＡＭ３２のメモリチェックを行う（ステップＳ３１３）。これにより、ＤＲＡＭ３２が利用可能となる。そしてサブＣＰＵ２１が、フラッシュＲＯＭ３４からメインＣＰＵ１１のブートプログラム（以下、メインＣＰＵ用ブートプログラムと呼ぶ。）を読み出して、該ブートプログラムをＤＲＡＭ３２に展開する（Ｓ３１４）。ここでは、メインＣＰＵ用ブートプログラムが暗号化されているものとする。なお、メインＣＰＵ用ブートプログラムが暗号化されていない場合には、ステップＳ３１４の後、処理はステップＳ３１７に移行する。

【００４９】

次いで、サブＣＰＵ２１が、ＤＲＡＭ３２に展開されたメインＣＰＵ用ブートプログラムを暗号器２５により復号し、署名検証を行う（ステップＳ３１５）。署名検証の結果、改竄が検知された場合は（ステップＳ３１６：ＹＥＳ）、サブＣＰＵ２１が、データ処理

部１０をリセット状態にして（ステップＳ３１８）、処理を終了する。改竄が検知されない場合は（ステップＳ３１６：ＮＯ）、サブＣＰＵ２１は、メインＣＰＵ１１をリセット解除する。リセット解除されたメインＣＰＵ１１は、メインＣＰＵ用ブートプログラムに従って起動処理（メインＣＰＵブート）を開始する（ステップＳ３１７）。メインＣＰＵブートが完了すると、処理は終了する。

【００５０】

以上のようにして、集積回路１の内蔵ＣＰＵ（メインＣＰＵ１１）がセキュアブートで起動される。

【００５１】

なお、データ処理部１０のメインＣＰＵ１１が使用されない場合、例えば、外部ＣＰＵ３１がメインＣＰＵとして使用される場合も想定される。そのような場合には、ステップＳ３０１，Ｓ３０２の後、外部ＣＰＵ３１がステップＳ３０３～Ｓ３１２の処理を行うようにすればよい。この場合、ステップＳ３１３以降の処理は行われない。

【００５２】

また、外部ＣＰＵ３１が集積回路１を起動する場合も想定される。図４は、そのような場合に行われる集積回路１のセキュアブートの流れを示すフローチャートである。なお、ここでは、フラッシュＲＯＭ３４が、セキュリティ管理部２０ではなく外部ＣＰＵ３１に接続されているものとする。

【００５３】

集積回路１と外部ＣＰＵ３１とに電源が投入されると、まず、集積回路１内部の初期設定が行われる（ステップＳ４０１）。次いで、外部ＣＰＵ３１がリセット解除され、初期化処理とＩ／Ｏインターフェース１４のリンクアップとが行われる。そして、外部ＣＰＵ３１が、フラッシュＲＯＭ３４に格納されているサブＣＰＵ２１のブートプログラムを、セキュリティ管理部２０の外部からアクセス可能であるＯＣＲＡＭ２４に書き込む（ステップＳ４０２）。なお、このとき、バスコントローラ２７は、データ処理部１０とセキュリティ管理部２０とのインターフェースを一時的に開放するものとする。

【００５４】

次いで、外部ＣＰＵ３１が、ＯＣＲＡＭ２４に書き込まれたサブＣＰＵ２１のブートプログラムを、セキュリティ管理部２０のＳＲＡＭ２２にコピーする（ステップＳ４０３）。そして、外部ＣＰＵ３１が、サブＣＰＵ２１をリセット解除する（ステップＳ４０４）。リセット解除されたサブＣＰＵ２１は、ブートＲＯＭ２８に記憶された第１ブートプログラムを読み出して、該第１ブートプログラムに従って第１起動処理（第１ブート）を開始する（ステップＳ４０５）。なお、ステップＳ４０６～Ｓ４２０の処理は、ステップＳ３０４～Ｓ３１８の処理と同様であるため、説明を省略する。

【００５５】

このように、サブＣＰＵ２１のブートプログラムをセキュリティ管理部２０のＯＣＲＡＭ２４に書き込むことで、フラッシュＲＯＭ３４が外部ＣＰＵ３１に接続されている場合でも、セキュアブートを行うことが可能となる。

【００５６】

以上に説明したように、本実施形態の集積回路１は、データを処理するデータ処理部１０と、データ処理部１０のセキュリティを管理するセキュリティ管理部２０とを備える。そして、セキュリティ管理部２０は、設定値保持部（ＯＴＰＲＯＭ２６）が保持する設定値によって示されるセキュリティ強度が所定レベル以上である場合に、ブートプログラムに対して署名検証を行うセキュアブートにより集積回路１を起動させる起動制御部２０１を有する。また、セキュリティ管理部２０は、セキュアブートにおける署名検証によりブートプログラムの改竄が検知されたときに、データ処理部１０をリセット状態にする状態制御部２０３を有する。

【００５７】

このように、本実施形態のセキュリティ管理部２０は、自身が保持するセキュリティ強度の設定値に基づいて、ブートシーケンスを切り替えるようにしている。よって、データ

処理部１０に対するセキュリティ脅威が存在する環境下においても、集積回路１を安全に起動させることができる。また、ＦＷの改竄が検知された場合にデータ処理部１０をリセット状態にしているので、集積回路１内のデータの意図しない流出を確実に防ぐことができる。したがって、本実施形態によれば、集積回路１及び集積回路１内のデータをセキュリティ脅威から保護することが可能となる。

【００５８】

また、セキュリティ管理部２０は、設定値保持部が保持する上記設定値によって示されるセキュリティ強度が所定レベル以上である場合に、データ処理部１０との接続を遮断する接続制御部２０２をさらに備える。特に、接続制御部２０２は、設定値保持部が保持する上記設定値によって示されるセキュリティ強度が所定レベル以上である場合においてデータ処理部１０に対するセキュリティ脅威が検知されたときに、データ処理部１０との接続を遮断する。これにより、セキュリティ強度を所定レベル以上に設定しておくことで、データ処理部１０との接続を遮断させることができるので、データ処理部１０がセキュリティ脅威に侵された場合でもセキュリティ管理部２０の内部を確実に保護することが可能となる。

【００５９】

また、接続制御部２０２は、設定値保持部がセキュリティ強度の設定値を保持していない場合に、データ処理部１０との接続を遮断する。これにより、集積回路１の製造時など、ＯＴＰＲＯＭ２６が初期状態にあって上記設定値や秘密鍵を保持していないときに、データ処理部１０がセキュリティ脅威に侵されたとしても、そのセキュリティ脅威からセキュリティ管理部２０を保護することができる。

【００６０】

また、状態制御部２０３は、設定値保持部がセキュリティ強度の設定値を保持していない場合に、データ処理部１０をリセット状態にする。これにより、集積回路１の製造時など、ＯＴＰＲＯＭ２６が初期状態にあって上記設定値や秘密鍵を保持していないときに、データ処理部１０がセキュリティ脅威に侵された場合でも、データ処理部１０が異常動作しないようにすることが可能となる。また、データ処理部１０を異常動作させないことで、データ処理部１０だけでなく、データ処理部１０に接続されている外部デバイスや外部デバイスが保持するデータのセキュリティを保護することができる。

【００６１】

また、データ処理部１０は、外部デバイス（ＤＲＡＭ３２、ＨＤＤ３３）との間で入出力されるデータを監視する入出力データ監視部（デバイスコントローラー１２，１３）を有する。また、セキュリティ管理部２０は、データ処理部１０に対するセキュリティ脅威を検知するセキュリティ脅威検知部２０４をさらに有する。そして、セキュリティ脅威検知部２０４は、設定値保持部が保持する上記設定値によって示されるセキュリティ強度が所定レベル以上である場合において入出力データ監視部によって不当な平文が検知されたときに、セキュリティ脅威を検知する。これにより、不当な平文が検知された場合に、その要因となるセキュリティ脅威からセキュリティ管理部２０を保護することができる。

【００６２】

また、セキュリティ脅威検知部２０４は、外部デバイスとの間で入出力されるデータが暗号化格納領域から読み出されたデータである場合において該データから平文が検知されたときに、該平文が不当であると判断する。これにより、外部デバイス内や集積回路内の暗号化データ格納領域のデータが改竄されていることを検知することができ、集積回路１に不正なＦＷが書き込まれたり、集積回路１に不正なデータが入力されたりすることを防止することができる。

【００６３】

また、セキュリティ管理部２０は内蔵メモリ（ＯＣＲＡＭ）２４をさらに有し、内蔵メモリ２４には、集積回路１の外部からブートプログラムを書き込むことが可能であり、起動制御部２０１は、内蔵メモリ２４にブートプログラムが書き込まれている場合には、セキュアブートにおいて、内蔵メモリ２４に書き込まれているブートプログラムに対して

署名検証を行い、該ブートプログラムを用いて集積回路１を起動させる。これにより、ブートプログラムを格納するフラッシュＲＯＭ３４がセキュリティ管理部２０ではなく外部ＣＰＵ３１に接続されている場合でも、署名検証を伴うセキュアブートを実行することができる。よって、集積回路の構成に柔軟性を持たせることが可能となり、図１に示される構成と異なる集積回路についてもセキュリティ脅威から保護することが可能となる。

【００６４】

さらに、起動制御部２０１は、セキュリティの設定強度が所定レベル未満である場合には、署名検証を行わない通常ブートにより集積回路１を起動させる。これにより、セキュリティ保護を必要としない環境下や暗号化が認められない環境下でも、セキュリティ強度を所定レベル未満に設定することで集積回路１を利用することが可能となる。

【００６５】

また、セキュリティ管理部２０の起動制御部２０１が、ＯＴＰＲＯＭ２６が保持する設定値によって示されるセキュリティ強度が所定レベル以上である場合に、セキュアブートにより集積回路１を起動させる工程が、集積回路１の制御方法における起動制御工程の具体例である。また、セキュリティ管理部２０の状態制御部２０３が、セキュアブートにおける署名検証によりブートプログラムの改竄が検知されたときに、データ処理部１０をリセット状態にする工程が、集積回路１の制御方法における接続制御工程の具体例である。

【００６６】

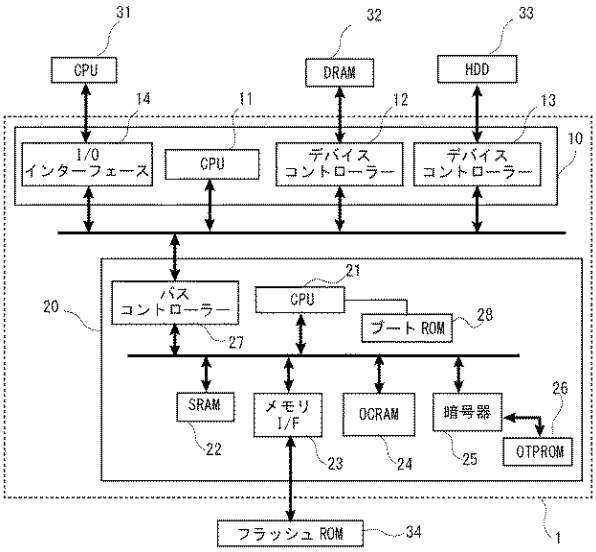
なお、本発明は、請求の範囲及び明細書全体から読み取ることのできる発明の要旨又は思想に反しない範囲で適宜変更可能であり、そのような変更を伴う集積回路及び集積回路の制御方法もまた本発明の技術思想に含まれる。

【符号の説明】

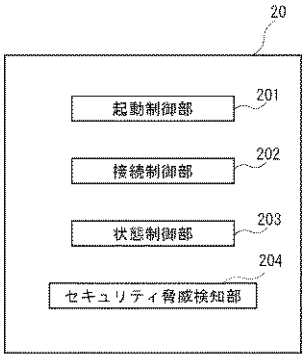
【００６７】

１　集積回路
１０　データ処理部
１２、１３　デバイスコントローラー
２０　セキュリティ管理部
２６　ＯＴＰＲＯＭ（設定値保持部）
２０１　起動制御部
２０２　接続制御部
２０３　状態制御部
２０４　セキュリティ脅威検知部

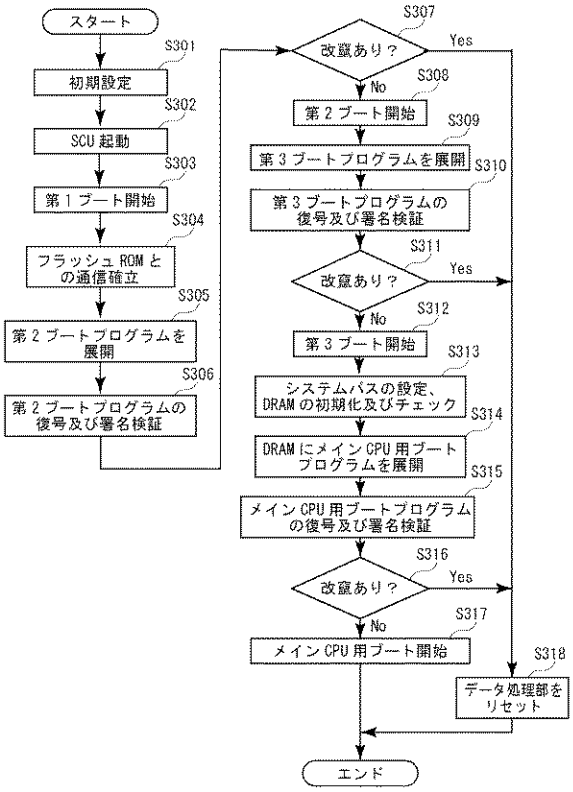
【図１】


31
CPU
32
DRAM
33
HDD
14
11
12
13
I/O
インターフェース
CPU
デバイス
コントローラー
デバイス
コントローラー
10
21
20
バス
コントローラー
CPU
ブート ROM
28
27
SRAM
メモリ
I/F
OCRAM
暗号器
26
OTPROM
22
23
24
25
フラッシュ ROM
34
1

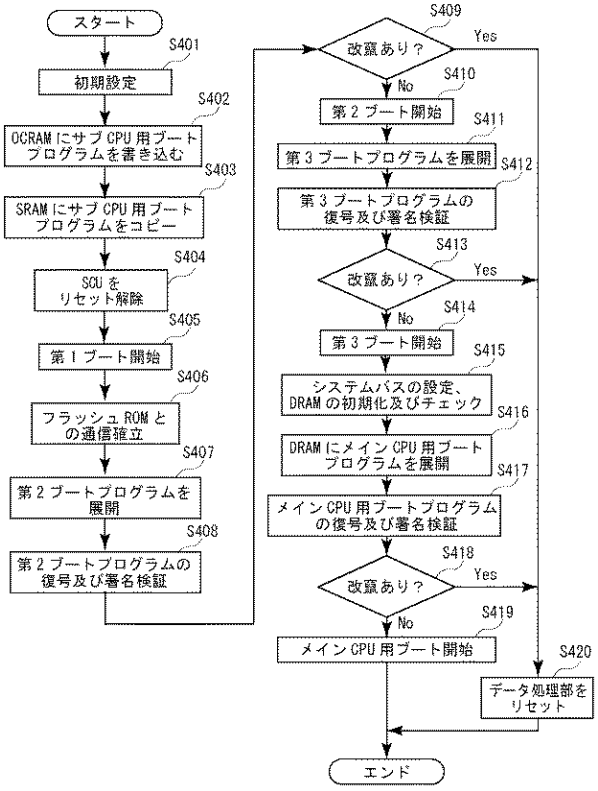
【図２】


20
起動制御部
201
接続制御部
202
状態制御部
203
204
セキュリティ脅威検知部

【図３】


スタート
S301
初期設定
S302
SCU 起動
S303
第 1 ブート開始
S304
フラッシュ ROM と
の通信確立
S305
第 2 ブートプログラムを
展開
S306
第 2 ブートプログラムの
復号及び署名検証
S307
改竄あり？
Yes
No
S308
第 2 ブート開始
S309
第 3 ブートプログラムを展開
S310
第 3 ブートプログラムの
復号及び署名検証
S311
改竄あり？
Yes
No
S312
第 3 ブート開始
S313
システムバスの設定、
DRAM の初期化及びチェック
S314
DRAM にメイン CPU 用ブート
プログラムを展開
S315
メイン CPU 用ブートプログラム
の復号及び署名検証
S316
改竄あり？
Yes
No
S317
メイン CPU 用ブート開始
S318
データ処理部を
リセット
エンド

【図４】


スタート
S401
初期設定
S402
OCRAM にサブ CPU 用ブート
プログラムを書き込む
S403
SRAM にサブ CPU 用ブート
プログラムをコピー
S404
SCU を
リセット解除
S405
第 1 ブート開始
S406
フラッシュ ROM と
の通信確立
S407
第 2 ブートプログラムを
展開
S408
第 2 ブートプログラムの
復号及び署名検証
S409
改竄あり？
Yes
No
S410
第 2 ブート開始
S411
第 3 ブートプログラムを展開
S412
第 3 ブートプログラムの
復号及び署名検証
S413
改竄あり？
Yes
No
S414
第 3 ブート開始
S415
システムバスの設定、
DRAM の初期化及びチェック
S416
DRAM にメイン CPU 用ブート
プログラムを展開
S417
メイン CPU 用ブートプログラム
の復号及び署名検証
S418
改竄あり？
Yes
No
S419
メイン CPU 用ブート開始
S420
データ処理部を
リセット
エンド