(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第4335707号
(P4335707)

(45)発行日　平成21年9月30日(2009.9.30)　(24)登録日　平成21年7月3日(2009.7.3)

(51)Int.Cl.		F I		
G06F 21/22	(2006.01)	G06F	9/06	660J
G06F 12/14	(2006.01)	G06F	12/14	510D
G06F 21/24	(2006.01)	G06F	12/14	540A
G09C 1/00	(2006.01)	G09C	1/00	660D
H04L 9/14	(2006.01)	H04L	9/00	641

請求項の数 22　(全 21 頁)　最終頁に続く

(21)出願番号　特願2004-31272(P2004-31272)
(22)出願日　平成16年2月6日(2004.2.6)
(65)公開番号　特開2005-222418(P2005-222418A)
(43)公開日　平成17年8月18日(2005.8.18)
審査請求日　平成18年12月7日(2006.12.7)

(73)特許権者　302062931
ＮＥＣエレクトロニクス株式会社
神奈川県川崎市中原区下沼部１７５３番地
(74)代理人　100102864
弁理士　工藤　実
(72)発明者　中澤　武
神奈川県川崎市中原区下沼部１７５３番地
ＮＥＣエレクトロニクス株式会社内

審査官　岸野　徹

最終頁に続く

(54)【発明の名称】プログラム改竄検出装置、及びプログラム改竄検出プログラムおよびプログラム改竄検出方法

(57)【特許請求の範囲】

【請求項１】

改竄検出用コードと暗号化されたプログラムとを格納する外部メモリと、

前記暗号化されたプログラムを復号化するための復号化プログラムを格納する起動ＲＯＭと、

ＣＰＵと、

プログラム改竄検出装置を識別するための識別子を格納する第２記憶部と

を具備し、

前記暗号化されたプログラムは、前記識別子との照合に用いられる識別子確認情報を、暗号化した状態で保持し、

前記ＣＰＵは、

前記復号化プログラムを実行することにより、前記暗号化されたプログラムを復号化して、復号化された識別子確認情報を含む復号済プログラムを生成し、前記復号済プログラムのコードに対して所定の演算を実行して得られた演算結果と前記改竄検出用コードとの比較、及び、前記復号済プログラムを実行することによって前記復号済プログラムのコードから得られる前記復号化された識別子確認情報と前記識別子との照合結果に基づいて、前記暗号化されたプログラムの改竄を検出する

プログラム改竄検出装置。

【請求項２】

請求項１に記載のプログラム改竄検出装置において、

さらにＲＡＭを具備し、
前記ＣＰＵは、前記復号化プログラムを実行することにより生成する前記復号済プログラムを前記ＲＡＭに格納し、前記ＲＡＭから前記コードを読み出し、読み出した前記コードに対して前記演算を実行し、前記演算結果と前記改竄検出用コードとの比較に基づいて前記プログラムの改竄を検出する
プログラム改竄検出装置。
【請求項３】
請求項２に記載のプログラム改竄検出装置において、
前記外部メモリは、前記ＲＡＭのアドレスを指定するアドレス情報を有し、
前記ＣＰＵは、前記アドレス情報に基づいて、前記復号済プログラムを前記ＲＡＭに格納し、
前記ＣＰＵは、前記アドレス情報に基づいて、前記ＲＡＭから前記コードを読み出す
プログラム改竄検出装置。
【請求項４】
請求項１乃至３の何れか１項に記載のプログラム改竄検出装置において、
前記起動ＲＯＭは起動プログラムを格納し、
前記ＣＰＵは、前記起動プログラムを実行することにより前記復号化プログラムを実行し、前記復号済プログラムを生成する
プログラム改竄検出装置。
【請求項５】
請求項１乃至４の何れか１項に記載のプログラム改竄検出装置において、
前記起動ＲＯＭは複数の領域を備え、
前記複数の領域の各々は、暗号化方式が異なる複数の復号化プログラムを一対一に格納し、
前記ＣＰＵは、前記複数の領域から一つの領域を選択し、前記選択された領域に格納された復号化プログラムを実行する
プログラム改竄検出装置。
【請求項６】
請求項５に記載のプログラム改竄検出装置において、
第1記憶部を備え、前記第1記憶部は前記複数の領域から一つの領域を選択するために用いられる領域情報を格納し、
前記ＣＰＵは、前記領域情報に基づいて前記複数の領域から一つの領域を選択し、前記選択された領域に格納された復号化プログラムを実行することにより前記プログラムを復号化して復号済プログラムを生成する
プログラム改竄検出装置。
【請求項７】
請求項1乃至６の何れかに記載のプログラム改竄検出装置において、
さらに、ネットワークに接続され、
前記起動ＲＯＭは、改竄通知プログラムを格納し、
前記ＣＰＵは、前記プログラムの改竄の検出に応答して前記改竄通知プログラムを実行することによって、前記プログラムの改竄を通知する改竄検出メッセージを生成し、前記改竄通知メッセージを前記ネットワークを介して所定のアドレスに送信する
プログラム改竄検出装置。
【請求項８】
請求項１乃至７の何れか１項に記載のプログラム改竄検出装置において、
前記ＣＰＵと前記起動ＲＯＭとが一の半導体デバイス内部に備えられ、
前記半導体デバイスは、前記外部メモリと前記ＲＡＭの各々と接続する
プログラム改竄検出装置。
【請求項９】
請求項１乃至８の何れか１項に記載のプログラム改竄検出装置で使用され、前記ＣＰＵ

と前記起動ＲＯＭとを具備する
半導体デバイス。
【請求項１０】
改竄検出用コードと暗号化されたプログラムとを格納する外部メモリと、前記暗号化されたプログラムを復号化する復号化プログラムを格納する起動ＲＯＭと、前記起動ＲＯＭと一の半導体デバイスに備えられえたＣＰＵとを具備するプログラム改竄検出装置を動作させる改竄検出プログラムにおいて、
前記暗号化されたプログラムは、前記半導体デバイスを識別するための識別子との照合に用いられる識別子確認情報を暗号化した状態で保持し、
前記起動ＲＯＭから復号化プログラムを読み出すステップと、
前記復号化プログラムを実行することにより前記暗号化されたプログラムを復号化して、復号化された識別子確認情報を含む復号済プログラムを生成するステップと、
前記復号済プログラムのコードに対して、所定の演算を実行し、前記演算結果と前記改竄検出用コードとの比較に基づいて前記暗号化されたプログラムの改竄を検出するステップと、
前記識別子を読み出すステップと、
前記復号済プログラムを実行することによって、前記復号済プログラムのコードから前記識別子に対応する前記復号化された識別子確認情報を抽出するステップと、
前記復号済プログラムを実行することによって前記識別子確認情報と前記識別子とを照合するステップと、
その照合結果に基づいて前記プログラムの改竄を検出するステップ
を具備する方法をコンピュータで実行可能な
改竄検出プログラム。
【請求項１１】
請求項１０に記載の改竄検出プログラムであって、
前記プログラム改竄検出装置はさらにＲＡＭを具備し、
前記復号化プログラムを実行することにより生成する前記復号済プログラムを前記ＲＡＭに格納するステップと、
前記ＲＡＭから前記復号済プログラムのコードを読み出すステップと、
読み出した前記コード対して、所定の演算を実行し、前記演算結果と前記改竄検出用コードとの比較に基づいて前記プログラムの改竄を検出するステップ
を具備する方法をコンピュータで実行可能な
改竄検出プログラム。
【請求項１２】
請求項１０または１１に記載の改竄検出プログラムにおいて、
前記外部メモリから前記ＲＡＭのアドレスを指定するアドレス情報を読み出すステップと、
前記アドレス情報に基づいて、前記復号済プログラムを前記ＲＡＭに格納するステップと、
前記アドレス情報に基づいて、前記ＲＡＭから前記コードを読み出すステップ
を具備する方法をコンピュータで実行可能な
改竄検出プログラム。
【請求項１３】
請求項１０乃至１２の何れか１項に記載の改竄検出プログラムにおいて、
前記起動ＲＯＭから起動プログラムを読み出すステップと、
前記起動プログラムを実行することにより前記復号化プログラムを実行し、前記復号済プログラムを生成するステップと
を具備する方法をコンピュータで実行可能な
改竄検出プログラム。
【請求項１４】

請求項１０乃至１３の何れか１項に記載の改竄検出プログラムにおいて、
前記起動ＲＯＭは、暗号化方式が異なる複数の復号化プログラムを一対一に格納する複数の領域を備え、
前記複数の領域から一つの領域を選択するステップと、
前記選択された領域に格納された復号化プログラムを読み出すステップと、
読み出した前記復号化プログラムを実行するステップ
を具備する方法をコンピュータで実行可能な
改竄検出プログラム。
【請求項１５】
請求項１４に記載の改竄検出プログラムにおいて、
領域情報を読み出すステップと、
前記領域情報に基づいて前記複数の領域から一つの領域を選択するステップと、
その選択された領域に格納された復号化プログラムを実行することにより前記プログラムを復号化して復号済プログラムを生成するステップ
を具備する方法をコンピュータで実行可能な
改竄検出プログラム。
【請求項１６】
請求項１０乃至１５の何れか1項に記載の改竄検出プログラムにおいて、
前記プログラム改竄検出装置はネットワークに接続され、
前記起動ＲＯＭから改竄通知プログラムを読み出すステップと、
前記プログラムの改竄の検出に応答して前記改竄通知プログラムを実行することによって、改竄検出メッセージを生成するステップと、
前記改竄通知メッセージを前記ネットワークを介して所定のアドレスに送信するステップ
を具備する方法をコンピュータで実行可能な
改竄検出プログラム。
【請求項１７】
復号化プログラムを読み出すステップと、
前記復号化プログラムを実行することにより、半導体デバイスを識別するための識別子との照合に用いられる識別子確認情報を暗号化した状態で保持する暗号化プログラムを復号化して、復号化された識別子確認情報を含む復号済プログラムを生成するステップと、
前記復号済プログラムのコードに対して、所定の演算を実行し、前記演算結果と予め格納された改竄検出用コードとの比較に基づいて前記プログラムの改竄を検出するステップと、
前記識別子を読み出すステップと、
前記復号済プログラムを実行することによって、前記復号済プログラムのコードから前記識別子に対応する前記復号化された識別子確認情報を抽出するステップと、
前記復号済プログラムを実行することによって前記復号化された識別子確認情報と前記識別子とを照合するステップと、
その照合結果に基づいて前記プログラムの改竄を検出するステップ
を具備する
プログラム改竄検出方法。
【請求項１８】
請求項１７に記載のプログラム改竄検出方法において、
ＲＡＭのアドレスを指定するアドレス情報を読み出すステップと、
前記アドレス情報に基づいて、前記復号済プログラムを前記ＲＡＭに格納するステップと、
前記アドレス情報に基づいて、前記ＲＡＭから前記コードを読み出すステップ
を具備する
プログラム改竄検出方法。

【請求項１９】
請求項１７または１８に記載のプログラム改竄検出方法において、
起動プログラムを読み出すステップと、
前記起動プログラムを実行することにより前記復号化プログラムを実行し、前記復号済プログラムを生成するステップ
を具備する
プログラム改竄検出方法。
【請求項２０】
請求項１７乃至１９の何れか１項に記載のプログラム改竄検出方法において、
予め格納された、暗号化方式が異なる複数の復号化プログラムの中から一つの復号化プログラムを選択するステップと、
前記選択された復号化プログラムを読み出すステップと、
読み出した前記復号化プログラムを実行するステップ
を具備する
プログラム改竄検出方法。
【請求項２１】
請求項２０に記載のプログラム改竄検出方法において、
領域情報を読み出すステップと、
前記領域情報に基づいて複数の復号化プログラム格納領域から一つの復号化プログラム格納領域を選択するステップと、
その選択された復号化プログラム格納領域に格納された復号化プログラムを実行することにより前記プログラムを復号化して復号済プログラムを生成するステップと
を具備する
プログラム改竄検出方法。
【請求項２２】
請求項１７乃至２１の何れか１項に記載のプログラム改竄検出方法において、
改竄通知プログラムを読み出すステップと、
前記プログラムの改竄の検出に応答して前記改竄通知プログラムを実行することによって、改竄検出メッセージを生成するステップと、
前記改竄通知メッセージをネットワークを介して所定のアドレスに送信するステップ
を具備する
プログラム改竄検出方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、コンピュータプログラムの改竄を防止するためのプログラム改竄検出装置、及びプログラム改竄防止プログラムに関する。
【背景技術】
【０００２】
近年、コンピュータ技術の急速な進歩に伴って、様々な製品にコンピュータが搭載されるようになった。そのようなコンピュータはＣＰＵ（Central Processing Unit）とＣＰＵを動作させるためのコンピュータプログラムが必要である。家電製品や通信機器などの製品に搭載されたコンピュータプログラムは、その製品独自の仕様に基づいて設計されている。例えば、有料放送システムなどに用いられる受信装置は、受信契約を交わした個人だけがその装置を利用できるようなものであることが望ましい。したがって搭載されるプログラムもその受信装置が適切に利用される場合のみ動作するように設計されていることが望ましい。そのような受信用装置を起動するためのプログラムは、装置に備えられたＲＯＭ（Read Only Memory）に格納され、受信装置の起動時に読み込まれる。コンピュータは読み込んだプログラムを実行することによって、その受信装置の制御を行っている。

【０００３】
近年、コンピュータを用いて電子的な制御を行っている装置においては、その装置に備えられたＲＯＭに格納されたプログラムは、その装置本体と同様に、開発に大きなコストが費やされており、企業にとって重要な財産になっている。上記の有料放送システムを例に述べるならば、有料放送の受信用装置を起動するためのプログラムを受信契約を結んでいない第三者に容易に知られてしまうということは、その有料放送システムが提供するサービスを不正な第三者に利用されてしまう可能性を含んでいる。さらに、上記のプログラムはシステム上の知的財産であり、その知的財産であるプログラムを適切に保護するために、そのプログラムが第三者に容易に知られてしまうということを防止する技術が望まれている。

【０００４】
従来、汎用のＣＰＵやＲＯＭの動作仕様は広く公開されているため、そのようなＣＰＵやＲＯＭを使用するコンピュータを搭載した装置を入手した第三者は、容易にプログラムの解析を行うことができる。上記のような装置において、そのＲＯＭに格納されたプログラムの解析を防止する技術が知られている（例えば、特許文献１から特許文献４参照）。

【０００５】
また、近年の半導体技術の進歩により、不揮発性で、且つ、書き換え可能なＲＯＭ（例えば、FlashＲＯＭなど）が登場し、このようなＲＯＭが上記の製品等に用いられることが多い。このようなＲＯＭを使用することよって、装置を動作させるプログラムのバージョンアップ等が容易になる。書き換え可能なＲＯＭを使用する装置においても、ＲＯＭに格納されたプログラムの不正な書き換えを防止する技術が望まれている。

【０００６】
図１は、従来の装置に搭載されたＣＰＵとＲＯＭ（FlashＲＯＭ）との構成を示すブロック図である。図１を参照すると、従来の装置はFlashＲＯＭ１０１とＣＰＵ１０２を備え、それらはバス１０３を介して接続されている。FlashＲＯＭ１０１は更にNormal Area１０１ａとOne Time Program Area１０１ｂとを備えている。

【０００７】
Normal Area１０１ａは、書込まれた情報の書き換えが可能な領域であり、暗号化されたコンピュータプログラムを格納する。One Time Program Area１０１ｂは、書き換えが不可能な（一度の書込みしかできない）領域である。One Time Program Area１０１ｂはその暗号化されたプログラムを復号化するための復号化プログラムを格納している。装置を起動するための起動プログラムはOne Time Program Area１０１ｂに格納されている。

【０００８】
このＣＰＵ１０２は起動時に最初にOne Time Program Area１０１ｂの起動用プログラムを読み出し、装置の起動を開始する。更にOne Time Program Area１０１ｂの復号化プログラムにより、FlashＲＯＭ１０１のNormal Area１０１ａに格納された暗号化されているプログラムを解読しながら外部のＲＡＭ（図示されず）上に展開する。その後、展開されたプログラムにより、装置を動作させる。

【０００９】
従来の技術は、第三者の不正使用を防止できる。そのコンピュータプログラムの不正な解析を防止している点において優れておるが、より強固なプログラムの解析防止の技術が望まれている。さらに、プログラムの改竄も防止する技術が望まれている。また、仮にコンピュータプログラムが改竄された場合には、その改竄を検出し警告などを出力する技術が望まれている。

【００１０】
【特許文献１】特開昭５９－１８８８９７号公報
【特許文献２】特開平５－１９７６３３号公報
【特許文献３】特開平８－３０５５５８号公報
【特許文献４】特開平１１－１２６１７４号公報
【発明の開示】

【発明が解決しようとする課題】
【００１１】
本発明が解決しようとする課題は、暗号化されたコンピュータプログラムを備える装置において、その暗号化方式が容易に外部に漏洩しない構成を有する装置、およびそのプログラムを提供することにある。
【００１２】
本発明が解決しようとする他の課題は、その暗号化方式が漏洩した場合でも、暗号化されたコンピュータプログラムの改竄を防止する構成を有する装置、およびそのプログラムを提供することにある。
【００１３】
本発明が解決しようとするさらなる課題は、仮にコンピュータプログラムが改竄された場合には、その改竄を検出する構成を有する装置、およびそのプログラムを提供することにある。
【課題を解決するための手段】
【００１４】
以下に、［発明を実施するための最良の形態］で使用される番号を用いて、課題を解決するための手段を説明する。これらの番号は、［特許請求の範囲］の記載と［発明を実施するための最良の形態］との対応関係を明らかにするために付加されたものである。ただし、それらの番号を、［特許請求の範囲］に記載されている発明の技術的範囲の解釈に用いてはならない。
【００１５】
改竄検出用コード（３４）と、暗号化されたプログラム（３５）とを格納する外部メモリ（４）と、復号化プログラムを格納する起動ＲＯＭ（２）と、ＣＰＵ（３）とを具備し、
前記ＣＰＵ（３）は、前記復号化プログラムを実行することにより前記プログラム（３５）を復号化して復号済プログラムを生成し、前記復号済プログラムのコードに対して所定の演算を実行して得られた演算結果と、前記改竄検出用コード（３４）との比較に基づいて前記プログラム（３５）の改竄を検出するプログラム改竄検出装置（２１）によって内蔵されたコンピュータプログラムの改竄を検出する。
【００１６】
これにより、復号化プログラム（暗号解読プログラム）が漏洩してしまい、内蔵されたコンピュータプログラムが改竄されてしまった場合に、その改竄を速やかに検出することが可能になる。
【００１７】
そのプログラム改竄検出装置（２１）において、さらにデータを格納するためのＲＡＭ（５）を具備し、
前記ＣＰＵ（３）は、前記復号化プログラムを実行することにより生成する前記復号済プログラムを前記ＲＡＭ（５）に格納し、前記ＲＡＭ（５）から前記コードを読み出し、読み出した前記コードに対して前記演算を実行し、前記演算結果と前記改竄検出用コード（３４）との比較に基づいて前記プログラム（３５）の改竄を検出することによってプログラムの改竄を検出する。
【００１８】
そのプログラム改竄検出装置（２１）において、前記外部メモリ（４）は、前記ＲＡＭ（５）のアドレスを指定するアドレス情報（３３）を有し、前記ＣＰＵ（３）は、前記アドレス情報（３３）に基づいて、前記復号済プログラムを前記ＲＡＭ（５）に格納し、前記ＣＰＵ（３）は、前記アドレス情報（３３）に基づいて、前記ＲＡＭ（５）から前記コードを読み出すことによってプログラムの改竄を検出する。
【００１９】
これにより、暗号化されたプログラムを復号化した際に、ＲＡＭの所定のアドレスに格納することが可能になる。復号済プログラム（暗号解読が完了したプログラム）を予め決

められたアドレスに格納することで、演算を実行した場合の実行結果を一定に保つことが可能になる。

【００２０】

そのプログラム改竄検出装置（２１）において、前記起動ＲＯＭ（２）は起動プログラムを格納し、前記ＣＰＵ（３）は、前記起動プログラムを実行することにより前記復号化プログラムを実行し、前記復号済プログラムを生成するプログラム改竄検出装置（２１）によってプログラムの改竄を検出する。

【００２１】

これにより、プログラム改竄検出装置（２１）を備える製品の起動に応答して、復号化を行うことが可能になり、起動（またはリセット）時に常にプログラムの改竄を監視することが可能になる。

【００２２】

そのプログラム改竄検出装置（２１）において、前記起動ＲＯＭ（２）は複数の領域（２ａ～２ｃ）を備え、前記複数の領域（２ａ～２ｃ）の各々は、暗号化方式が異なる複数の復号化プログラムを一対一に格納し、前記ＣＰＵ（３）は、前記複数の領域（２ａ～２ｃ）から一つの領域を選択し、前記選択された領域に格納された復号化プログラムを実行することによってプログラムの改竄を検出する。

【００２３】

そのプログラム改竄検出装置（２１）において、さらに第１記憶部（１５）を備え、前記第１記憶部（１５）は前記複数の領域（２ａ～２ｃ）から一つの領域を選択するために用いられる領域情報を格納し、

前記ＣＰＵ（３）は、前記領域情報に基づいて前記複数の領域（２ａ～２ｃ）から一つの領域を選択し、前記選択された領域に格納された復号化プログラムを実行することにより前記プログラム（３５）を復号化して復号済プログラムを生成するプログラム改竄検出装置（２１）を用いてプログラムの改竄を検出する。

【００２４】

これにより、そのプログラム改竄検出装置（２１）を製品（２０）に適用する場合、その製品（２０）を製造するメーカーが複数存在する場合、その複数の異なる製品メーカーに対して、各々異なる暗号化方式に対応したプログラム改竄検出装置（２１）を提供することが可能になる。

【００２５】

そのプログラム改竄検出装置（２１）において、さらに上記の第１記憶部（１５）とは異なる第２記憶部（１２）を備え、前記第２記憶部（１２）はプログラム改竄検出装置（２１）を識別するための識別子を格納し、

前記復号済プログラムは前記識別子に対応する識別子確認情報を含み、前記ＣＰＵ（３）は、前記復号済プログラムを実行することによって前記識別子確認情報と前記識別子とを照合し、その照合結果に基づいて前記プログラム（３５）の改竄を検出するプログラム改竄検出装置（２１）を用いてプログラムの改竄を検出する。

【００２６】

これにより、演算結果による改竄が検出されなかった場合でも、復号済プログラムに含まれる識別子確認情報と、その製品に固有の識別子とを比較することでより強固なプログラムの保護が可能になる。また、その製品の識別子として使用される半導体デバイス（１、１１、１４）に付与されたデバイスＩＤを使用するようにしても良い。

【００２７】

そのプログラム改竄検出装置（２１）を備える製品（２０）がネットワーク（２３）に接続されている場合において、前記起動ＲＯＭ（２）は、改竄通知プログラムを格納し、前記ＣＰＵ（３）は、前記プログラム（３５）の改竄の検出に応答して前記改竄通知プログラムを実行することによって、前記プログラム（３５）の改竄を通知する改竄検出メッセージを生成し、前記改竄通知メッセージを前記ネットワーク（２３）を介して所定のアドレスに送信するプログラム改竄検出装置（２１）を使用する。

【００２８】
これにより、プログラムの改竄を検出した場合に、速やかに所定の端末装置に通知することが可能になる。ネットワークを介してその通知を受信することで、改竄を迅速に把握するので、プログラム改竄検出装置（２１）を備える製品（２０）の設置場所まで赴いて改竄の事実を確認する必要なくなる。また。設定により、改竄検出に応答して復号済プログラムの実行を停止することも可能である。さらに、ネットワークを介して改竄通知メッセージを受信した端末装置は、そのメッセージに含まれる情報から送信元の製品（２０）を特定することも可能である。
【００２９】
そのプログラム改竄検出装置（２１）において、前記ＣＰＵ（３）と前記起動ＲＯＭ（２）とが一の半導体デバイス（１、１１、１４）内部に備えられ、前記半導体デバイス（１、１１、１４）は、前記外部メモリ（４）と前記ＲＡＭ（５）との各々と接続するプログラム改竄検出装置（２１）を用いてプログラムの改竄を検出する。
【００３０】
これにより、起動ＲＯＭ（２）とＣＰＵ（３）とを半導体デバイスの内部に格納することが可能になる。ＣＰＵ（３）と起動ＲＯＭ（２）を１つのチップ内に備えるような構成にすることで、起動ＲＯＭ（３）の復号化プログラム（暗号化方式）を比較的情報が漏洩しにくい半導体デバイス内部に格納することになり、暗号化方式の漏洩防止（改竄防止）の効果がある。
【００３１】
改竄検出用コード（３４）と、暗号化されたプログラムとを格納する外部メモリ（４）と、復号化プログラムを格納する起動ＲＯＭ（２）と、ＣＰＵ（３）とを具備するプログラム改竄検出装置（２１）を動作させる改竄検出プログラムにおいて、
前記起動ＲＯＭ（２）から復号化プログラムを読み出すステップと、前記復号化プログラムを実行することにより前記プログラム（３５）を復号化して復号済プログラムを生成するステップと、前記復号済プログラムのコードに対して、所定の演算を実行し、前記演算結果と前記改竄検出用コード（３４）との比較に基づいて前記プログラム（３５）の改竄を検出するステップを具備する方法をコンピュータで実行可能な改竄検出プログラムを実行することによって外部メモリ（４）に格納されたプログラムの改竄を検出する。
【００３２】
そのプログラム改竄検出装置（２１）はさらにＲＡＭ（５）を具備し、
その改竄検出プログラムにおいて、前記起動ＲＯＭ（２）から復号化プログラムを読み出すステップと、前記復号化プログラムを実行することにより前記プログラム（３５）を復号化して前記復号済プログラムを生成するステップと、前記復号済プログラムを前記ＲＡＭ（５）に格納するステップと、前記ＲＡＭ（５）から前記復号済プログラムのコードを読み出すステップと、読み出した前記コード対して、所定の演算を実行し、前記演算結果と前記改竄検出用コード（３４）との比較に基づいて前記プログラム（３５）の改竄を検出するステップを具備する方法をコンピュータで実行可能な改竄検出プログラムを実行することによってプログラムの改竄を検出する。
【００３３】
その改竄検出プログラムにおいて、前記外部メモリ（４）から前記ＲＡＭ（５）のアドレスを指定するアドレス情報（３３）を読み出すステップと、前記アドレス情報（３３）に基づいて、前記復号済プログラムを前記ＲＡＭ（５）に格納するステップと、前記アドレス情報（３３）に基づいて、前記ＲＡＭ（５）から前記コードを読み出すステップを具備する方法をコンピュータで実行可能な改竄検出プログラムを実行することによってプログラムの改竄を検出する。
【００３４】
その改竄検出プログラムにおいて、前記起動ＲＯＭ（２）から起動プログラムを読み出すステップと、前記起動プログラムを実行することにより前記復号化プログラムを実行し、前記復号済プログラムを生成するステップとを具備する方法をコンピュータで実行可能

な改竄検出プログラムを実行することによってプログラムの改竄を検出する。

【００３５】

その改竄検出プログラムにおいて、前記起動ＲＯＭ（２）は、暗号化方式が異なる複数の復号化プログラムを一対一に格納する複数の領域（２ａ～２ｃ）を備え、

前記複数の領域（２ａ～２ｃ）から一つの領域を選択するステップと、前記選択された領域に格納された復号化プログラムを読み出すステップと、読み出した前記復号化プログラムを実行するステップを具備する方法をコンピュータで実行可能な改竄検出プログラムを実行することによってプログラムの改竄を検出する。

【００３６】

その改竄検出プログラムにおいて、前記領域情報を読み出すステップと、前記領域情報に基づいて前記複数の領域（２ａ～２ｃ）から一つの領域を選択するステップと、その選択された領域に格納された復号化プログラムを実行することにより前記プログラム（３５）を復号化して復号済プログラムを生成するステップを具備する方法をコンピュータで実行可能な改竄検出プログラムを実行することによってプログラムの改竄を検出する。

【００３７】

その改竄検出プログラムにおいて、前記起動ＲＯＭ（２）と前記ＣＰＵ（３）は一の半導体デバイス（１、１１、１４）に備えられ、

前記半導体デバイス（１、１１、１４）を識別するための識別子を読み出すステップと、前記復号済プログラムから前記識別子に対応する識別子確認情報を抽出するステップと、前記復号済プログラムを実行することによって前記識別子確認情報と前記識別子とを照合するステップと、その照合結果に基づいて前記プログラム（３５）の改竄を検出するステップを具備する方法をコンピュータで実行可能な改竄検出プログラムを実行することによってプログラムの改竄を検出する。

【００３８】

その改竄検出プログラムにおいて、前記プログラム改竄検出装置はネットワーク（２３）に接続され、

前記起動ＲＯＭ（２）から改竄通知プログラムを読み出すステップと、前記プログラム（３５）の改竄の検出に応答して前記改竄通知プログラムを実行することによって、改竄検出メッセージを生成するステップと、前記改竄通知メッセージを前記ネットワーク（２３）を介して所定のアドレスに送信するステップを具備する方法をコンピュータで実行可能な改竄検出プログラムを実行することによってプログラムの改竄を検出し、その改竄検出を通知する。

【００３９】

復号化プログラムを読み出すステップと、前記復号化プログラムを実行することにより暗号化プログラムを復号化して復号済プログラムを生成するステップと、前記復号済プログラムのコードに対して、所定の演算を実行し、前記演算結果と予め格納された改竄検出用コード（３４）との比較に基づいて前記プログラム（３５）の改竄を検出するステップを具備するプログラム改竄検出方法によって所定の製品（２０）を動作させるためのコンピュータプログラムの改竄を検出する。

【００４０】

そのプログラム改竄検出方法において、ＲＡＭ（５）のアドレスを指定するアドレス情報（３３）を読み出すステップと、前記アドレス情報（３３）に基づいて、前記復号済プログラムを前記ＲＡＭ（５）に格納するステップと、前記アドレス情報（３３）に基づいて、前記ＲＡＭ（５）から前記コードを読み出すステップを具備するプログラム改竄検出方法によってプログラムの改竄を検出する。

【００４１】

そのプログラム改竄検出方法において、起動プログラムを読み出すステップと、前記起動プログラムを実行することにより前記復号化プログラムを実行し、前記復号済プログラムを生成するステップを具備するプログラム改竄検出方法によってプログラムの改竄を検出する。

【００４２】
そのプログラム改竄検出方法において、予め格納された、暗号化方式が異なる複数の復号化プログラムの中から一つの復号化プログラムを選択するステップと、前記選択された復号化プログラムを読み出すステップと、読み出した前記復号化プログラムを実行するステップを具備するプログラム改竄検出方法によってプログラムの改竄を検出する。
【００４３】
そのプログラム改竄検出方法において、領域情報を読み出すステップと、前記領域情報に基づいて複数の復号化プログラム格納領域から一つの復号化プログラム格納領域を選択するステップと、その選択された復号化プログラム格納領域に格納された復号化プログラムを実行することにより前記プログラム（３５）を復号化して復号済プログラムを生成するステップとを具備するプログラム改竄検出方法によってプログラムの改竄を検出する。
【００４４】
そのプログラム改竄検出方法において、半導体デバイス（１、１１、１４）を識別するための識別子を読み出すステップと、前記復号済プログラムから前記識別子に対応する識別子確認情報を抽出するステップと、前記復号済プログラムを実行することによって前記識別子確認情報と前記識別子とを照合するステップと、その照合結果に基づいて前記プログラム（３５）の改竄を検出するステップを具備するプログラム改竄検出方法によってプログラムの改竄を検出する。
【００４５】
そのプログラム改竄検出方法において、改竄通知プログラムを読み出すステップと、前記プログラム（３５）の改竄の検出に応答して前記改竄通知プログラムを実行することによって、改竄検出メッセージを生成するステップと、前記改竄通知メッセージをネットワーク（２３）を介して所定のアドレスに送信するステップを具備するプログラム改竄検出方法によってプログラムの改竄を検出する。
【発明の効果】
【００４６】
本発明は、暗号化されたコンピュータプログラムを備える装置において、その暗号化方式を容易に外部に漏洩させないための構成を備え、装置に格納された情報の漏洩に関する安全性を向上させる効果がある。
また、本発明はさらに、暗号化方式が漏洩した場合でも、暗号化されたコンピュータプログラムの改竄を防止し、より強固なセキュリティ対策の実現が可能になり、それにより装置に格納された情報の漏洩に関する安全性を向上させる効果がある。
また、本発明はさらに、仮にコンピュータプログラムが改竄された場合には、その改竄を検出するための動作を実行し、その動作によって改竄されたことを認識しないまま、そのコンピュータプログラムを実行しつづけてしまうことを防止する効果がある。
【発明を実施するための最良の形態】
【００４７】
以下に、図面を使用して本発明のプログラム改竄検出装置について述べる。
本発明の実施の形態に述べるプログラム改竄検出機能を備えたコンピュータ（以下、プログラム改竄検出機能付コンピュータ２１と称する）は、コンピュータを用いて電子的な制御を行っている製品全般に適用可能である。以下では、そのプログラム改竄検出機能付コンピュータ２１を搭載した製品本体が、情報通信ネットワークに接続された状態で使用される製品、特に、製品本体に搭載されたプログラムの改竄が問題になりやすい有料放送システムの放送受信装置に適用された場合を例にして述べる。
【００４８】
［第１の実施の形態］
図２は、本発明によるプログラム改竄検出機能付コンピュータ２１を、有料放送システムの放送受信装置に適用した場合のシステム構成の一例を示すブロック図である。図２を参照すると、その有料放送システムは、放送配信側に備えられた配信装置２４、管理装置２５および有料放送を受信する受信側に備えられた有料放送受信装置２０とで構成される

。配信装置２４は、その有料放送システムが提供するサービスである有料放送をネットワーク２３を介して送信する装置である。管理装置２５は、上記の有料放送の配信状況や有料放送受信装置２０の放送受信状態などを管理する装置である。有料放送受信装置２０は、配信装置２４から送信された情報（有料放送）をネットワーク２３を介して受信し、表示装置（図示されず）に出力する。

【００４９】

有料放送受信装置２０は更にプログラム改竄検出機能付コンピュータ２１と通信用インターフェース２２を備える。プログラム改竄検出機能付コンピュータ２１は、ＬＳＩ１（またはＬＳＩ１１、ＬＳＩ１４）と書き換え可能外部ＲＯＭ４とＲＡＭ５を備え、通信用インターフェース２２を介してネットワーク２３に接続する。ネットワーク２３に接続された通信用インターフェース２２は、プログラム改竄検出機能付コンピュータ２１から出力された情報をネットワーク２３を介して配信装置２４に送信する。

【００５０】

図３は、本発明の第１の実施の形態によるプログラム改竄検出機能付コンピュータ２１に備えられたプログラム改竄検出装置の構成を示すブロック図である。図３を参照すると、第１の実施の形態によるプログラム改竄検出装置は、起動用ＲＯＭ２とＣＰＵ３と内部バス６とを内部に備えるＬＳＩ１と、外部ＲＯＭ４とＲＡＭ５とで構成される。ＬＳＩ１はシングルチップで構成された集積回路である。ＬＳＩ１はデータ線９を介して外部ＲＯＭ４に接続され、データ線１０を介してＲＡＭ５に接続されている。

【００５１】

起動用ＲＯＭ２は、格納された情報の書き換えが不可能なＲＯＭである。起動用ＲＯＭ２はデータ線７を介して内部バス６に接続され、その内部バス６を介してＣＰＵ３と外部ＲＯＭ４とＲＡＭ５との各々に接続されている。起動用ＲＯＭ２はプログラム改竄検出機能付コンピュータ２１の起動直後のみ使用され、ＣＰＵ起動専用プログラムと外部ＲＯＭ４上の暗号化されたプログラムの解読・展開を行うための復号化プログラムを格納する。ＣＰＵ３は、そのＣＰＵ起動専用プログラムによって起動され、そのＣＰＵ起動専用プログラムに基づいて起動用ＲＯＭ２から復号化プログラムを読み出す。ＣＰＵ３はさらに、その復号化プログラムに基づいて外部ＲＯＭ４上の暗号化されたプログラムを読出し、プログラムの復号化を実行する。ＣＰＵ３は、復号化されてＲＡＭ５に展開されたプログラムを実行し、そのプログラムを実行することによりプログラム改竄検出機能付コンピュータ２１の制御を行う。ＣＰＵ３はデータ線８を介して内部バス６に接続され、その内部バス６を介して起動用ＲＯＭ２と外部ＲＯＭ４とＲＡＭ５とに接続されている。

【００５２】

書き換え可能外部ＲＯＭ４は、格納された情報の書き換えが可能で、且つ、不揮発性の記憶領域を有する記憶装置である。書き換え可能外部ＲＯＭ４はデータ線９を介してＬＳＩ１に接続され、暗号化プログラムを格納している。書き換え可能外部ＲＯＭ４はＬＳＩ１からの要求に応答して、その暗号化プログラムを出力する。ＲＡＭ５は、復号済プログラムを格納する記憶装置である。ＲＡＭ５はデータ線１０を介してＬＳＩ１に接続され、起動用ＲＯＭ２に格納された復号化プログラムによって復号化された暗号化プログラムを、復号済プログラムとして格納する。

【００５３】

図４は書き換え可能外部ＲＯＭ４の内部フォーマット３０を示す図である。図４を参照すると、書き換え可能外部ＲＯＭ４の情報格納領域はヘッダー部と、ヘッダー部以外の領域とで構成される。ヘッダー部はさらに複数の領域で構成され、各々の領域にはヘッダー検出用ユニークコード３１と、ユーザプログラムコード量情報３２と、ＲＡＭ展開先アドレス情報３３と、参照用セキュリティチェックコード３４とが格納される。

【００５４】

ヘッダー検出用ユニークコード３１は、書き換え可能外部ＲＯＭ４に格納された情報に対するアクセスを確立するために使用されるコードである。ユーザプログラムコード量情報３２から参照用セキュリティチェックコード３４は、ヘッダー検出用ユニークコード３

１に続けて書き換え可能外部ＲＯＭ４に格納される情報である。ユーザプログラムコード量情報３２は、ＲＡＭ５に展開される復号化されたプログラムのコード量が、所定のコード量に達したかどうかの判断に用いられる情報である。ＲＡＭ展開先アドレス情報３３は、ＲＡＭ５のアドレスを示す情報である。ＣＰＵ３は、復号化されたプログラムをＲＡＭ５に展開する場合にアドレス情報３３に基づいて、復号化されたプログラムをＲＡＭ５に展開し、また、ＲＡＭ５に格納された復号済プログラムを読み出す場合にもそのアドレス情報に基づいてデータの読み止しを行う。参照用セキュリティチェックコード３４は、復号化が完了したプログラムの改竄を検出するための用いられるコードである。ユーザコード３５は、書き換え可能外部ＲＯＭ４に格納された暗号化されたプログラムである。

【００５５】

図５は、第１の実施の形態における動作を示すフローチャートである。以下の説明では、暗号化されたプログラムと復号化によってＲＡＭ５に展開されたプログラムとの区別を明確にするために、書き換え可能外部ＲＯＭ４に格納されたプログラム（暗号化されたプログラム）をユーザコード３５と呼び、そのユーザコード３５を復号化してＲＡＭ５に展開されたプログラムをユーザプログラムと呼ぶ。図５を参照すると、第１の実施の形態の動作は、有料放送受信装置２０を起動（またはリセット）することによって電源が投入されると開始する。ステップＳ１０１において、有料放送受信装置２０の起動に応答して、起動用ＲＯＭ２に格納されたＣＰＵ起動専用プログラムが実行され、ＣＰＵ３が起動する。起動したＣＰＵ３は内部バス６を介して起動用ＲＯＭ２にアクセスし、起動用ＲＯＭ２に格納された復号化プログラムの読み出しを実行する。

【００５６】

ステップＳ１０２において、ＣＰＵ３は書き換え可能外部ＲＯＭ４にアクセスし、書き換え可能外部ＲＯＭ４のヘッダー部に格納された情報の読み出しを行う。ステップＳ１０３において、ＣＰＵ３はヘッダー検出用ユニークコード３１を検出したかどうかの判断を行う。ＣＰＵ３がヘッダー検出用ユニークコード３１を検出した場合には、処理はステップＳ１０４に進む。ＣＰＵ３がヘッダー検出用ユニークコード３１を検出しなかった場合には、処理は戻りステップＳ１０２の読み出し動作を再び実行する。ヘッダー検出用ユニークコード３１が検出されない場合には、処理はステップＳ１０２からステップＳ１０３の動作を繰り返す（有料放送受信装置２０は起動されない）。

【００５７】

ステップＳ１０４において、ヘッダー検出用ユニークコード３１を検出したＣＰＵ３は、ヘッダー検出用ユニークコード３１に続くユーザプログラムコード量情報３２、ＲＡＭ展開先アドレス情報３３、参照用セキュリティチェックコード３４の読み出しを行う。ステップＳ１０５において、ユーザプログラムコード量情報３２とＲＡＭ展開先アドレス情報３３と参照用セキュリティチェックコード３４との読み出しが完了したＣＰＵ３は書き換え可能外部ＲＯＭ４に格納されたユーザコード３５を読み出し、読み出したユーザコード３５を復号化プログラムを実行することによって解読し、ＲＡＭ５に展開する。

ここで実行される復号化プログラムの暗号方式としては、任意の暗号方式を使用することが可能である。例えば、ユーザコード３５を複数ビット単位で読み出し、その複数ビットに対応して解読が可能な所定の解読用キーを用いてＥＸＯＲ演算を実行することによりユーザコード３５の復号化を行う方法を用いても良い。さらに複雑な暗号・復号化方式を使用することでより安全性の高いシステムを構成することも可能である。

【００５８】

ステップＳ１０６において、ＲＡＭ５に展開された復号化後のプログラムであるユーザプログラム（バイナリコード）を使用し、所定の演算規則に基づいてセキュリティチェックコードを算出する。実行される演算規則は任意の演算規則を使用することが可能である。

ステップＳ１０７において、ＲＡＭ５に展開されたユーザプログラムのコード量と、ステップＳ１０４で読み出したユーザプログラムコード量情報３２との比較を実行する。その比較の結果、ＲＡＭ５に展開されたユーザプログラムのコード量がユーザプログラムコ

ード量情報３２に達していない場合処理は戻り、読み出したユーザコード３５の復号化とＲＡＭ５への展開および次のセキュリティチェックコードの算出を行う。

【００５９】

上記のステップＳ１０５～ステップＳ１０７の動作を更に具体的に説明すると、例えば、その演算規則としてＥＸＯＲ演算を利用する場合、最初に所定の３２ビットの第１固定値と、３２ビットの第２固定値を設定し、所定の領域に格納する。ＣＰＵ３はその第１固定値とユーザコード３５の最初の３２ビットとのＥＸＯＲ演算を実行し、３２ビットのユーザプログラムを生成する（ステップＳ１０５）。ＣＰＵ３は、その３２ビットのユーザプログラムと第２固定値とのＥＸＯＲ演算に基づいて第１セキュリティチェックコードを算出する。（ステップＳ１０６）

【００６０】

上述の第１セキュリティチェックコード算出後、ＣＰＵ３は、ＲＡＭ５に展開されたユーザプログラムのコード量がユーザプログラムコード量情報３２に達したかどうかの判断を実行する（ステップＳ１０７）。その判断の結果、ＲＡＭ５に展開されたユーザプログラムのコード量がユーザプログラムコード量情報３２に達していない場合には、処理はステップＳ１０５に戻り、ＣＰＵ３は第１固定値とユーザコード３５の次の３２ビットとのＥＸＯＲ演算を実行して新たな３２ビットのユーザプログラムを生成する（ステップＳ１０５）。ＣＰＵ３は、生成された新たな３２ビットのユーザプログラムと第１セキュリティチェックコードとのＥＸＯＲ演算を実行し、第２セキュリティチェックコードを算出する（ステップＳ１０６）。

【００６１】

ＣＰＵ３は、ＲＡＭ５に展開されたユーザプログラムのコード量がユーザプログラムコード量情報３２に一致するまでステップＳ１０５～ステップＳ１０７の処理を繰り返し、その両方が一致したときのセキュリティチェックコードをユーザプログラム全体に対する最終的なセキュリティチェックコードとして決定する。また、ＣＰＵ３は、ＲＡＭ５に展開されたユーザプログラムのコード量とユーザプログラムコード量情報３２とが一致したことに基づいて、ユーザコード３５が全て復号化されたことを認識する。

【００６２】

ステップＳ１０８において、算出された最終的なセキュリティチェックコードと参照用セキュリティチェックコード３４との比較を実行する。その比較の結果、算出されたセキュリティチェックコードと参照用セキュリティチェックコード３４とが一致しなかった場合、ユーザコード３５が改竄されたと判断する（ステップＳ１１０）。ステップＳ１１０において、ユーザコード３５が改竄されたと判断された場合、プログラム改竄検出機能付コンピュータ２１は改竄検出メッセージを生成し、通信用インターフェース２２に出力する。出力されたメッセージはネットワークを介して有料放送システムの管理装置２５に送信される。算出されたセキュリティコードと参照用セキュリティチェックコード３４とが一致した場合、ステップＳ１０９に進み、プログラム改竄検出機能付コンピュータ２１は、ＲＡＭ５に展開されているユーザプログラムを実行することにより有料放送受信装置２０を動作させる。ステップＳ１０９において、ＲＡＭ５に展開されたユーザプログラムによる有料放送受信装置２０の動作開始に応答して、プログラム改竄検出機能付コンピュータ２１のＬＳＩ１は起動用ＲＯＭ２へのアクセスを禁止する。この禁止はプログラム改竄検出機能付コンピュータ２１の動作終了（例えば、電源断など）まで継続する。

【００６３】

このフローチャートの動作によって、起動用ＲＯＭ２に格納された復号化プログラムによるセキュリティ対策だけでなく、復号化されたユーザプログラムのコードを使用したセキュリティチェックを実行することで、より強固なプログラム改竄検出機能付コンピュータ２１に備えられたプログラムの保護が可能になる。

【００６４】

［第２の実施の形態］

図６は、本発明の第２の実施の形態によるプログラム改竄検出機能付コンピュータ２１

に備えられたプログラム改竄検出装置の構成を示すブロック図である。第２の実施の形態に述べるプログラム改竄検出装置は第1の実施の形態同様にコンピュータを用いて電子的な制御を行っている製品全般にコンピュータを用いて電子的な制御を行っている製品全般に適用可能である。したがって以下の説明では第1の実施の形態同様に、そのプログラム改竄検出機能付コンピュータ２１を搭載した製品本体が、情報通信ネットワークに接続された状態で使用される製品、特に、製品本体に搭載されたプログラムの改竄が問題になりやすい、有料放送システムの有料放送受信装置２０である場合を例に述べる。

【００６５】

図６を参照すると、第２の実施の形態で述べるプログラム改竄検出装置は、起動用ＲＯＭ２とＣＰＵ３と内部バス６とデバイスＩＤ情報記憶部１２とを内部に備えるＬＳＩ１１と、書き換え可能外部ＲＯＭ４と、ＲＡＭ５とで構成される。ＬＳＩ１１はＬＳＩ１と同様のシングルチップを備えた集積回路である。ＬＳＩ１１に備えられた起動用ＲＯＭ２とＣＰＵ３とは第1の実施の形態に示す起動用ＲＯＭ２とＣＰＵ３と同様の構成であるので、以下では起動用ＲＯＭ２とＣＰＵ３の構成に関する説明は省力する。また。書き換え可能外部ＲＯＭ４とＲＡＭ５も第1の実施の形態で説明した書き換え可能外部ＲＯＭ４とＲＡＭ５と同様の構成であるので、以下では書き換え可能外部ＲＯＭ４とＲＡＭ５の構成に関する説明は省力する。

【００６６】

デバイスＩＤ情報記憶部１２は、半導体デバイスに割当てられたデバイスＩＤをデバイスＩＤ情報として格納する記憶領域である。レジスタ、または、それに類する情報記憶機能を有し、データ線１３を介して内部バス６に接続されている。デバイスＩＤはその半導体デバイスの設計時に決定された値であり、同じ設計の半導体デバイスには同じデバイスＩＤが付与される。また、同様の設計で品種の異なる半導体デバイスには、異なる品種毎にデバイスＩＤが付与される。

【００６７】

図７は第２の実施の形態の動作を示すフローチャートである。図７を参照すると、第２の実施の形態における動作は、ステップＳ１０１からステップＳ１０９までの動作は第１の実施の形態における動作と同様である。したがって、以下では図７に示されているフローチャートのステップＳ２０１からステップＳ２０４を中心に説明を行う。

【００６８】

ＬＳＩ１１のＣＰＵ３は、ステップＳ２０１の前ステップであるステップＳ１０９でＲＡＭ５に展開されたユーザプログラムを実行することによって有料放送受信装置２０を動作させる。ステップＳ２０１において、そのユーザプログラムの実行開始に応答してＬＳＩ１１に備えられたデバイスＩＤ情報記憶部１２からデバイスＩＤ情報の読み出しを行う。

【００６９】

ステップＳ２０２において、ＣＰＵ３はデバイスＩＤ情報記憶部１２からのデバイスＩＤ情報の読み出し完了に応答して、ＲＡＭ５に展開された復号化後のユーザプログラムに含まれるデバイスチェックＩＤを抽出する。ユーザコード３５には、暗号化されたデバイスチェックＩＤが予め含まれており、ＣＰＵ３は書き換え可能外部ＲＯＭ４に格納されるユーザコード３５を復号化することでユーザプログラムからデバイスチェックＩＤの抽出が可能である。

【００７０】

ステップＳ２０３において、ユーザプログラムから抽出したデバイスチェックＩＤとデバイスＩＤ情報記憶部１２から読み出したデバイスＩＤ情報とが一致するかどうかの判断を行う。その判断の結果、デバイスチェックＩＤとデバイスＩＤ情報とが一致しなかった場合ステップＳ２０５に進み、ユーザプログラムの実行を停止する。また、プログラム改竄検出機能付コンピュータ２１はプログラムの実行の停止に応答してプログラム停止メッセージを生成し、通信用インターフェース２２に出力する。出力されたメッセージはネットワーク２３を介して有料放送システムの管理装置２５のアドレスに送信される。ステッ

プＳ２０３の判断の結果、デバイスチェックＩＤとデバイスＩＤ情報とが一致した場合、ステップＳ２０４に進み、プログラム改竄検出機能付コンピュータ２１は、ＲＡＭ５に展開されているユーザプログラムを実行することによって有料放送受信装置２０を動作を継続する。

【００７１】

このフローチャートの動作によって、復号化プログラムを起動用ＲＯＭ２に格納するというセキュリティ対策だけでなく、復号化されたユーザプログラムから算出されたセキュリティチェックコードを使用した改竄検出を実行し、さらに、ユーザプログラムに含まれるデバイスチェックＩＤと、ＬＳＩ１１内部に格納されたデバイスＩＤ情報とを使用したセキュリティチェックを行うことで、プログラム改竄検出機能付コンピュータ２１に格納されたプログラムをより強固に保護することが可能なる。

【００７２】

［第３の実施の形態］

図８は、本発明の第３の実施の形態によるプログラム改竄検出機能付コンピュータ２１に備えられたプログラム改竄検出装置の構成を示すブロック図である。第３の実施の形態に述べるプログラム改竄検出装置は第1の実施の形態同様にコンピュータを用いて電子的な制御を行っている製品全般に適用可能である。したがって、以下では第1の実施の形態と同様に、そのプログラム改竄検出機能付コンピュータ２１を搭載した製品本体が、情報通信ネットワークに接続された状態で使用される製品、特に、製品本体に搭載されたプログラムの改竄が問題になりやすい、有料放送システムの有料放送受信装置２０である場合を例に述べる。

【００７３】

図８を参照すると、第３の実施の形態で述べるプログラム改竄検出装置は、起動用ＲＯＭ２とＣＰＵ３と内部バス６とレジスタ１５とを内部に備えるＬＳＩ１４と、書き換え可能外部ＲＯＭ４と、ＲＡＭ５とで構成される。ＬＳＩ１４はＬＳＩ１と同様のシングルチップで構成された集積回路である。ＬＳＩ１４に備えられたＣＰＵ３は第1の実施の形態に示したＣＰＵ３と同様の構成であるので、以下では第３の実施の形態におけるＣＰＵ３の構成に関する説明は省力する。また。図８に示される書き換え可能外部ＲＯＭ４とＲＡＭ５も第1の実施の形態で説明した書き換え可能外部ＲＯＭ４とＲＡＭ５と同様の構成であるので、以下では第３の実施の形態における書き換え可能外部ＲＯＭ４とＲＡＭ５の構成に関する説明は省力する。

【００７４】

起動用ＲＯＭ２は、複数の領域（第１エリア２ａ～第３エリア２ｃ）を備え、その各々にＬＳＩ１に備えられた起動用ＲＯＭ２と同様の情報を格納する。また、複数の領域（第１エリア２ａ～第３エリア２ｃ）は、設計変更によって任意に増減させることが可能である。レジスタ１５はＬＳＩ１４内部に備えられた記憶回路である。複数の領域を備える起動用ＲＯＭ２の中から特定の領域を選択するための情報を格納する。レジスタ１５はデータ線１６を介して内部バス６に接続されている。起動用ＲＯＭ２の複数の領域（第１エリア２ａ～第３エリア２ｃ）の各々には、対応する暗号方式が異なる復号化プログラムが一対一に格納される。暗号化されたユーザプログラム（ユーザコード３５）は、上記の複数の暗号方式の中の一つで暗号化され、書き換え可能外部ＲＯＭ４に格納される。

さらに、複数の領域から特定の領域を選択し暗号方式を決定するために、デバイス（ＬＳＩ１４）には特定外部端子を備えることが好ましい。デバイスは起動（またはリセット）時にその特定外部端子でレジスタ１５を決定し、そのレジスタ１５から格納された値を読み出す。

【００７５】

図９は第３の実施の形態の動作を示すフローチャートである。図９を参照すると、第２の実施の形態における動作は、ステップＳ１０２からステップＳ１０９までの動作は第１の実施の形態における動作と概ね同様であることが示されている。したがって、以下では図８に示されているフローチャートのステップＳ３０１からステップＳ３０３までを中心

に説明を行う。

【００７６】

ステップＳ３０１において、有料放送受信装置２０の起動に応答してＬＳＩ１４に内蔵された起動用ＲＯＭ２に格納されたＣＰＵ起動専用プログラムによってＣＰＵ３が起動される。起動したＣＰＵ３は起動直後に内部バス６を介してレジスタ１５にアクセスする。

【００７７】

ステップＳ３０２において、ＣＰＵ３は、起動時に使用された特定外部端子で決定したレジスタ１５に格納された値の読み出しを実行する。ＣＰＵ３は読み出したレジスタ１５の値に基づいて起動用ＲＯＭ２の複数の領域（第１エリア２ａ～第３エリア２ｃ）の中から、復号化プログラムを読み出す領域を決定する（ステップＳ３０３）。その後、処理はステップＳ１０２に進み、以下、第１の実施の形態におけるステップＳ１０２からステップＳ１０９（またはステップＳ１１０）と同様の処理を実行する。

【００７８】

このフローチャートの動作によって、書き換え可能外部ＲＯＭ４に格納する暗号化されたユーザプログラムの暗号化方式を複数設定することが可能になる。さらに、書き換え可能外部ＲＯＭ４に格納された暗号化されたユーザプログラムが解析されてしまった場合でも、起動時に選択される暗号化方式と一致させることが困難になるため、プログラム改竄検出機能付コンピュータ２１に搭載されたプログラムに関する安全性が向上する。さらに、起動用ＲＯＭ２に格納された復号化プログラムによるセキュリティ対策だけでなく、復号化されたユーザプログラムのコードを使用したセキュリティチェックを実行することで、より強固にプログラム改竄検出機能付コンピュータ２１のプログラムの保護が可能になる。

【００７９】

また、複数の領域を備えることで、同一種類のデバイス（ＬＳＩ）において、複数の暗号方式を選択することができる。これにより、複数の異なる有料放送受信装置２０製造メーカーにプログラム改竄検出機能付コンピュータ２１を提供する場合でも、各々のメーカーに異なる暗号方式を提供することができる。デバイスが同じでも、あるメーカーで使用している暗号方式と、他のメーカーで使用している暗号方式とを異なるものに設定することで、書き換え可能外部ＲＯＭ４格納されたユーザコード３５に対する強固なセキュリティ対策が可能になる。

【００８０】

なお、上述した第１の実施の形態から第３の実施の形態は、矛盾が発生しない場合において組合せて実行することが可能である。

【図面の簡単な説明】

【００８１】

【図１】図１は、従来のＣＰＵと書き換え可能なＲＯＭとの構成を示すブロック図である。

【図２】図２は、、本発明によるプログラム改竄検出機能を備えたコンピュータを、有料放送システムの放送受信装置に適用した場合のシステム構成の一例を示すブロック図である。

【図３】図３は、第１の実施の形態の構成を示すブロック図である。

【図４】図４は、書き換え可能外部ＲＯＭのフォーマットを示す図である。

【図５】図５は、第１の実施の形態における動作を示すフローチャートである。

【図６】図６は、第２の実施の形態の構成を示すブロック図である。

【図７】図７は、第２の実施の形態における動作を示すフローチャートである。

【図８】図８は、第３の実施の形態の構成を示すブロック図である。

【図９】図９は、第３の実施の形態における動作を示すフローチャートである。

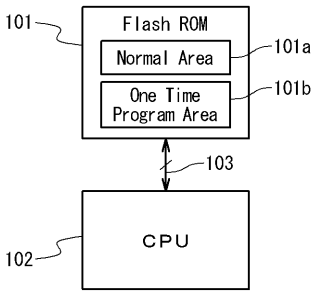
【符号の説明】

【００８２】

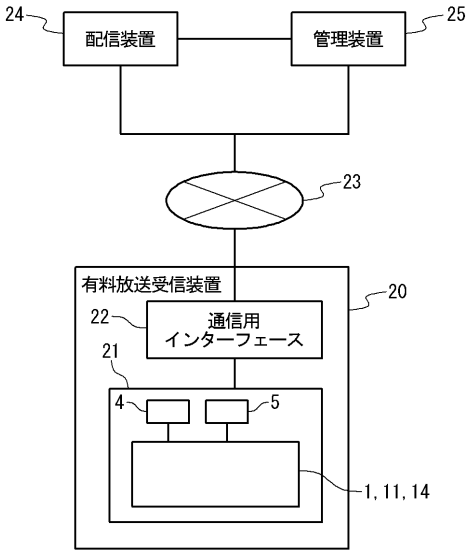
１、１１、１４　…　ＬＳＩ

２　…　起動用ＲＯＭ
３　…　ＣＰＵ
４　…　書き換え可能外部ＲＯＭ
５　…　ＲＡＭ
６　…　内部バス
７、８、９、１０　…　データ線
２０　…　有料放送受信装置
２１　…　プログラム改竄検出機能付コンピュータ
２２　…　通信用インターフェース
２３　…　ネットワーク
２４　…　配信装置
２５　…　管理装置
３０　…　内部フォーマット
３１　…　ヘッダー検出用ユニークコード
３２　…　ユーザコード量情報
３３　…　ＲＡＭ展開先アドレス情報
３４　…　参照用セキュリティチェックコード
３５　…　ユーザコード
１２　…　デバイスＩＤ情報記憶部
１３　…　データ線
１５　…　レジスタ
１６　…　データ線
２ａ～２ｃ　…　起動用ＲＯＭの記憶領域
１０１　…　FlashＲＯＭ
１０１ａ　…　Normal　Area
１０１ｂ　…　One　Time　Program　Area
１０２　…　ＣＰＵ
１０３　…　バス

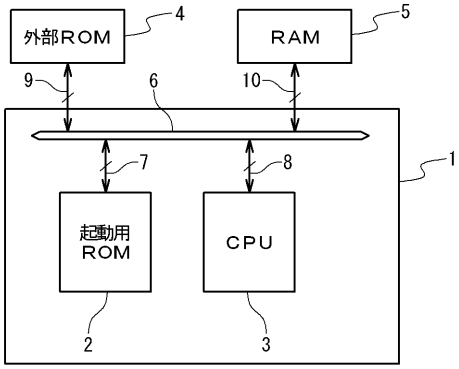
【図１】


101
Flash ROM
Normal Area
101a
One Time
Program Area
101b
103
CPU
102

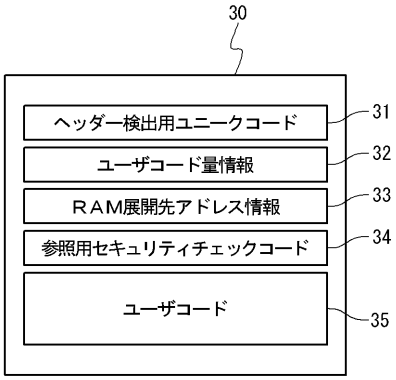
【図２】


24
配信装置
管理装置
25
23
有料放送受信装置
20
22
通信用
インターフェース
21
4
5
1, 11, 14

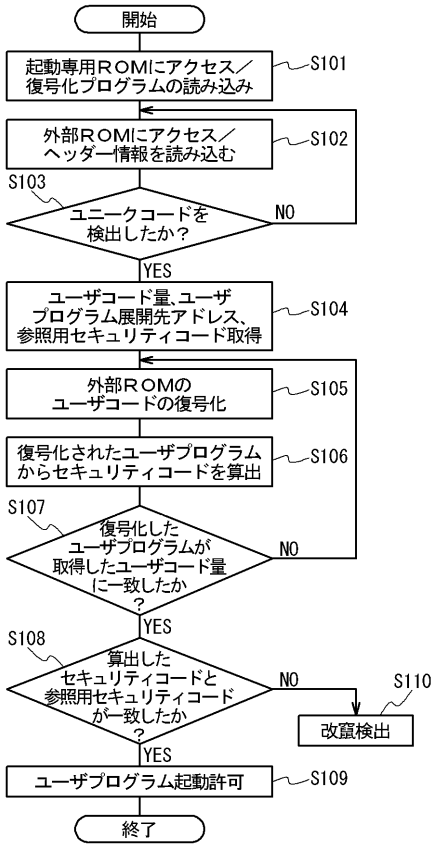
【図３】


外部ROM
4
RAM
5
9
6
10
7
8
1
起動用
ROM
CPU
2
3

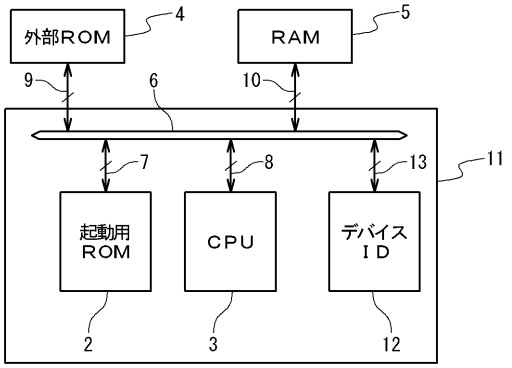
【図４】


30
ヘッダー検出用ユニークコード
31
ユーザコード量情報
32
RAM展開先アドレス情報
33
参照用セキュリティチェックコード
34
ユーザコード
35

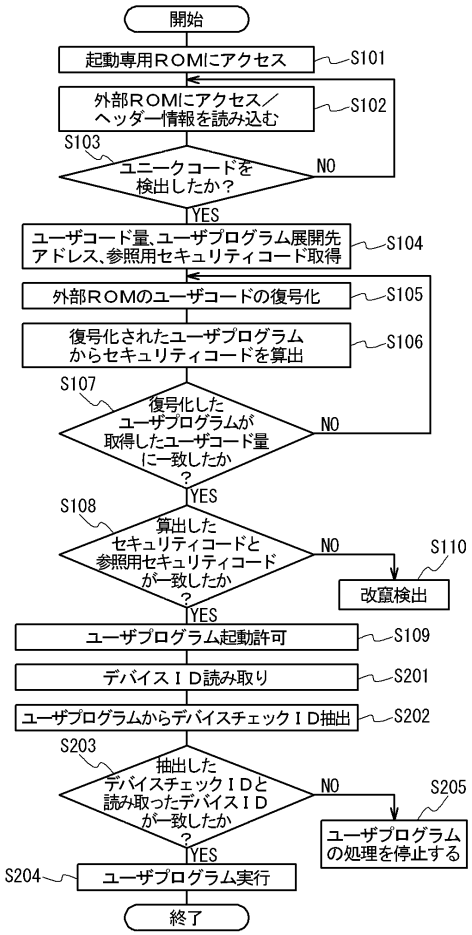
【図５】


開始
起動専用ROMにアクセス／
復号化プログラムの読み込み
S101
外部ROMにアクセス／
ヘッダー情報を読み込む
S102
S103
ユニークコードを
検出したか？
NO
YES
ユーザコード量、ユーザ
プログラム展開先アドレス、
参照用セキュリティコード取得
S104
外部ROMの
ユーザコードの復号化
S105
復号化されたユーザプログラム
からセキュリティコードを算出
S106
S107
復号化した
ユーザプログラムが
取得したユーザコード量
に一致したか
？
NO
YES
S108
算出した
セキュリティコードと
参照用セキュリティコード
が一致したか
？
NO
S110
改竄検出
YES
ユーザプログラム起動許可
S109
終了

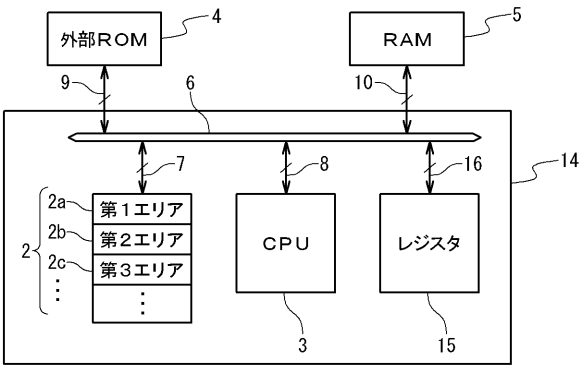
【図６】


外部ROM
4
RAM
5
9
6
10
7
8
13
11
起動用
ROM
CPU
デバイス
ＩＤ
2
3
12

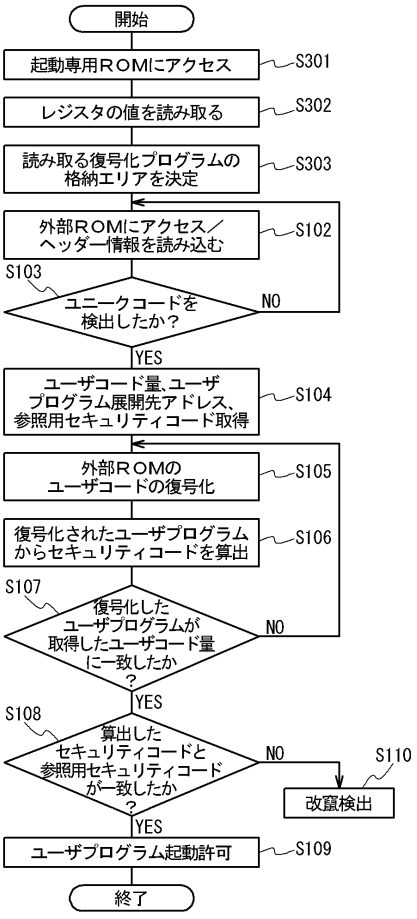
【図７】


開始
起動専用ＲＯＭにアクセス
S101
外部ＲＯＭにアクセス／
ヘッダー情報を読み込む
S102
S103
ユニークコードを
検出したか？
NO
YES
ユーザコード量、ユーザプログラム展開先
アドレス、参照用セキュリティコード取得
S104
外部ＲＯＭのユーザコードの復号化
S105
復号化されたユーザプログラム
からセキュリティコードを算出
S106
S107
復号化した
ユーザプログラムが
取得したユーザコード量
に一致したか
？
NO
YES
S108
算出した
セキュリティコードと
参照用セキュリティコード
が一致したか
？
NO
S110
改竄検出
YES
ユーザプログラム起動許可
S109
デバイスＩＤ読み取り
S201
ユーザプログラムからデバイスチェックＩＤ抽出
S202
S203
抽出した
デバイスチェックＩＤと
読み取ったデバイスＩＤ
が一致したか
？
NO
S205
ユーザプログラム
の処理を停止する
YES
S204
ユーザプログラム実行
終了

【図８】


外部ROM
4
RAM
5
9
6
10
7
8
16
14
2a
第１エリア
2b
第２エリア
2c
第３エリア
2
CPU
レジスタ
3
15

【図９】


開始
起動専用ＲＯＭにアクセス
S301
レジスタの値を読み取る
S302
読み取る復号化プログラムの
格納エリアを決定
S303
外部ＲＯＭにアクセス／
ヘッダー情報を読み込む
S102
S103
ユニークコードを
検出したか？
NO
YES
ユーザコード量、ユーザ
プログラム展開先アドレス、
参照用セキュリティコード取得
S104
外部ＲＯＭの
ユーザコードの復号化
S105
復号化されたユーザプログラム
からセキュリティコードを算出
S106
S107
復号化した
ユーザプログラムが
取得したユーザコード量
に一致したか
？
NO
YES
S108
算出した
セキュリティコードと
参照用セキュリティコード
が一致したか
？
NO
S110
改竄検出
YES
ユーザプログラム起動許可
S109
終了

フロントページの続き

(51)Int.Cl. F I
H04N 7/167 (2006.01) H04N 7/167 Z

(56)参考文献 特開平09－282155（JP，A）
特開2003－186560（JP，A）
特開平05－200153（JP，A）
特開平09－024151（JP，A）
特開平10－040095（JP，A）

(58)調査した分野(Int.Cl.，DB名)
G06F 21／22
G06F 12／14
G06F 21／24
G09C 1／00