(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2005-346182
(P2005-346182A)
(43)公開日　平成17年12月15日(2005.12.15)

(51)Int.Cl.[7]	F I		テーマコード（参考）
G06F 12/14	G06F 12/14	560D	5B017
G06F 1/00	G06F 12/14	520A	5B076
H04L 9/10	G06F 12/14	560C	5J104
	H04L 9/00	621A	
	G06F 9/06	660L	

審査請求 未請求　請求項の数 5　OL　（全 14 頁）

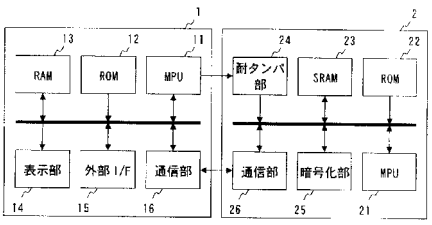
(21)出願番号　特願2004-162050 (P2004-162050)
(22)出願日　平成16年5月31日 (2004.5.31)

(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号
(71)出願人　000237639
富士通フロンテック株式会社
東京都稲城市矢野口１７７６番地
(74)代理人　100101856
弁理士　赤澤　日出夫
(74)代理人　100097250
弁理士　石戸　久子
(72)発明者　伊藤　善規
東京都稲城市矢野口１７７６番地　富士通フロンテック株式会社内

最終頁に続く

(54)【発明の名称】情報処理装置、耐タンパ方法、耐タンパプログラム

(57)【要約】
【課題】　認証に加えて不正な処理の検出を行い、不正な処理をタンパとして認識してセキュリティモジュール内のセキュリティデータを消去する情報処理装置を提供する。
【解決手段】　セキュリティデータを格納するとともに、共通鍵を用いてアプリケーションの署名を復号化し、得られる第１ハッシュを出力するセキュリティモジュール２と、アプリケーションの本体のハッシュである第２ハッシュを算出し、第１ハッシュと第２ハッシュが一致しない場合に信号をセキュリティモジュール２へ出力するメインユニット１とを備え、セキュリティモジュール２は、メインユニット１から信号を受け取るとセキュリティデータを消去する。
【選択図】　図１



【特許請求の範囲】
【請求項１】
セキュリティデータにアクセスするアプリケーションを実行する情報処理装置において、
前記アプリケーションは、アプリケーションの本体のハッシュに共通鍵を用いて暗号化した結果を署名とし、本体と署名を結合したものであって、
前記セキュリティデータを格納するとともに、前記共通鍵を用いて前記署名を復号化し、得られる第１ハッシュを出力するセキュリティモジュールと、
前記本体のハッシュである第２ハッシュを算出し、前記第１ハッシュと前記第２ハッシュが一致しない場合に信号を前記セキュリティモジュールへ出力し、前記第１ハッシュと前記第２ハッシュが一致した場合に前記アプリケーションを実行するメインユニットと、
を備え、
前記セキュリティモジュールは、前記メインユニットから前記信号を受け取ると前記セキュリティデータを消去することを特徴とする情報処理装置。
【請求項２】
セキュリティデータにアクセスするアプリケーションを実行する情報処理装置において、
前記アプリケーションは、共通鍵を用いて生成した署名を、前記アプリケーションのアクセス権限に応じて本体に付加したものであって、
前記セキュリティデータを格納するとともに、前記共通鍵を用いて前記署名を復号化するセキュリティモジュールと、
前記アプリケーションを実行し、前記署名に対応するアクセス権限で許可されていないアクセスが発生した場合に信号を前記セキュリティモジュールへ出力するメインユニットと、
を備え、
前記セキュリティモジュールは、前記メインユニットから前記信号を受け取ると前記セキュリティデータを消去することを特徴とする情報処理装置。
【請求項３】
Flash ROMに格納されたプログラムによって、セキュリティデータにアクセスする情報処理装置において、
前記セキュリティデータを格納するセキュリティモジュールと、
前記プログラムを実行するとともに、前記Flash ROMの書き換えを示す信号が発生した場合に信号を前記セキュリティモジュールへ出力するメインユニットと、
を備え、
前記セキュリティモジュールは、前記メインユニットから前記信号を受け取ると前記セキュリティデータを消去することを特徴とする情報処理装置。
【請求項４】
セキュリティデータにアクセスするアプリケーションを実行する耐タンパ方法において、
前記アプリケーションは、アプリケーションの本体のハッシュに共通鍵を用いて暗号化した結果を署名とし、本体と署名を結合したものであって、
前記セキュリティデータを格納するステップと、
前記共通鍵を用いて前記署名を復号化し、得られる第１ハッシュを出力するステップと、
前記本体のハッシュである第２ハッシュを算出し、前記第１ハッシュと前記第２ハッシュが一致しない場合に信号を出力し、前記第１ハッシュと前記第２ハッシュが一致した場合に前記アプリケーションを実行するステップと、
前記信号を受け取ると前記セキュリティデータを消去するステップと、
を備えてなる耐タンパ方法。
【請求項５】

セキュリティデータにアクセスするアプリケーションを実行する耐タンパ方法をコンピュータに実行させる耐タンパプログラムにおいて、
前記アプリケーションは、アプリケーションの本体のハッシュに共通鍵を用いて暗号化した結果を署名とし、本体と署名を結合したものであって、
前記セキュリティデータを格納するステップと、
前記共通鍵を用いて前記署名を復号化し、得られる第１ハッシュを出力するステップと、
前記本体のハッシュである第２ハッシュを算出し、前記第１ハッシュと前記第２ハッシュが一致しない場合に信号を出力し、前記第１ハッシュと前記第２ハッシュが一致した場合に前記アプリケーションを実行するステップと、
前記信号を受け取ると前記セキュリティデータを消去するステップと、
をコンピュータに実行させる耐タンパプログラム。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、ソフトウェアの改造を検出し、検出した場合にはセキュリティデータの消去等を行う情報処理装置、耐タンパ方法、耐タンパプログラムに関するものである。

【背景技術】

【０００２】

セキュリティ機能を持つ従来の情報処理装置には、端末改造による悪用を防止するための耐タンパ機能が搭載されている。耐タンパ機能とは、タンパ（tamper：開封・改竄）を検出した場合に、情報処理装置におけるセキュリティモジュール内のセキュリティデータを消去する仕組みのことである。ここで、セキュリティデータとは、セキュリティのための鍵、データ、ロジック等のことである。従来の耐タンパ機能では、ハードウェアの開封検出を行うためのタンパスイッチが用いられており、ハードウェアを開封した際にタンパ検出し、セキュリティデータを消去することによって不正使用を防止している。これは、セキュリティ機能を持つ従来の情報処理装置が専用端末としてSI（System Integration）されており、ソフトウェアは非公開情報とされており安全性が高く、ハードウェア改造の可能性の方が高いためである。

【０００３】

なお、本発明の関連ある従来技術として、例えば、下記に示す特許文献１が知られている。特許文献１は、公開鍵により暗号化されたプログラムを認証し、不正なプログラムである場合に動作を停止させるセキュリティ・システムを示している。

【特許文献１】特開２０００－３２２２５３号公報　（第４－７頁、第１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、上述した従来の耐タンパ機能は、開封が必要なハードウェア改造には対抗できるが、Flash ROM（Read Only Memory）の書き換え等によるソフトウェア攻撃を検出することができない。特に、情報処理装置において、仕様が公開された汎用OSを使用する場合はソフトウェア攻撃の可能性が高まり、従来の耐タンパ機能ではソフトウェア攻撃に対して無力となる。

【０００５】

ソフトウェア攻撃を防止するための仕組みとして、認証されていないアプリケーションの実行を禁止する方法は既に広く行なわれているが、この方法も認証されたアプリケーションの脆弱性を利用されると、その脆弱性レベルに応じた権限によって、不正な処理が行なわれる可能性がある。また、カーネルやドライバが書き換えられた場合は、より深刻な情報漏洩等の不正な処理が行われる可能性がある。

【０００６】

本発明は上述した問題点を解決するためになされたものであり、認証に加えて不正な処

理の検出を行い、不正な処理をタンパとして認識してセキュリティモジュール内のセキュリティデータを消去する情報処理装置、耐タンパ方法、耐タンパプログラムを提供することを目的とする。

【課題を解決するための手段】

【０００７】

上述した課題を解決するため、本発明は、セキュリティデータにアクセスするアプリケーションを実行する情報処理装置において、前記アプリケーションは、アプリケーションの本体のハッシュに共通鍵を用いて暗号化した結果を署名とし、本体と署名を結合したものであって、前記セキュリティデータを格納するとともに、前記共通鍵を用いて前記署名を復号化し、得られる第１ハッシュを出力するセキュリティモジュールと、前記本体のハッシュである第２ハッシュを算出し、前記第１ハッシュと前記第２ハッシュが一致しない場合に信号を前記セキュリティモジュールへ出力し、前記第１ハッシュと前記第２ハッシュが一致した場合に前記アプリケーションを実行するメインユニットと、を備え、前記セキュリティモジュールは、前記メインユニットから前記信号を受け取ると前記セキュリティデータを消去することを特徴とするものである。

【０００８】

また、本発明は、セキュリティデータにアクセスするアプリケーションを実行する情報処理装置において、前記アプリケーションは、共通鍵を用いて生成した署名を、前記アプリケーションのアクセス権限に応じて本体に付加したものであって、前記セキュリティデータを格納するとともに、前記共通鍵を用いて前記署名を復号化するセキュリティモジュールと、前記アプリケーションを実行し、前記署名に対応するアクセス権限で許可されていないアクセスが発生した場合に信号を前記セキュリティモジュールへ出力するメインユニットと、を備え、前記セキュリティモジュールは、前記メインユニットから前記信号を受け取ると前記セキュリティデータを消去することを特徴とするものである。

【０００９】

また、本発明は、Flash ROMに格納されたプログラムによって、セキュリティデータにアクセスする情報処理装置において、前記セキュリティデータを格納するセキュリティモジュールと、前記プログラムを実行するとともに、前記Flash ROMの書き換えを示す信号が発生した場合に信号を前記セキュリティモジュールへ出力するメインユニットと、を備え、前記セキュリティモジュールは、前記メインユニットから前記信号を受け取ると前記セキュリティデータを消去することを特徴とするものである。

【００１０】

また、本発明に係る情報処理装置において、前記Flash ROMの書き換えを示す信号は、Write Enable信号とChip Select信号であることを特徴とするものである。

【００１１】

また、本発明に係る情報処理装置において、前記Flash ROMの書き換えを示す信号は、Erase信号またはWrite Protect解除信号であることを特徴とするものである。

【００１２】

また、本発明は、セキュリティデータにアクセスするアプリケーションを実行する耐タンパ方法において、前記アプリケーションは、アプリケーションの本体のハッシュに共通鍵を用いて暗号化した結果を署名とし、本体と署名を結合したものであって、前記セキュリティデータを格納するステップと、前記共通鍵を用いて前記署名を復号化し、得られる第１ハッシュを出力するステップと、前記本体のハッシュである第２ハッシュを算出し、前記第１ハッシュと前記第２ハッシュが一致しない場合に信号を出力し、前記第１ハッシュと前記第２ハッシュが一致した場合に前記アプリケーションを実行するステップと、前記信号を受け取ると前記セキュリティデータを消去するステップとを備えてなるものである。

【００１３】

また、本発明は、セキュリティデータにアクセスするアプリケーションを実行する耐タンパ方法において、前記アプリケーションは、共通鍵を用いて生成した署名を、前記アプ

リケーションのアクセス権限に応じて本体に付加したものであって、前記セキュリティデータを格納するステップと、前記共通鍵を用いて前記署名を復号化するステップと、前記アプリケーションを実行し、前記署名に対応するアクセス権限で許可されていないアクセスが発生した場合に信号を出力するステップと、前記信号を受け取ると前記セキュリティデータを消去するステップとを備えてなるものである。

【００１４】

また、本発明は、Flash ROMに格納されたプログラムによって、セキュリティデータにアクセスする耐タンパ方法において、前記セキュリティデータを格納するステップと、前記プログラムを実行するとともに、前記Flash ROMの書き換えを示す信号が発生した場合に信号を出力するステップと、前記信号を受け取ると前記セキュリティデータを消去するステップとを備えてなるものである。

【００１５】

また、本発明は、セキュリティデータにアクセスするアプリケーションを実行する耐タンパ方法をコンピュータに実行させる耐タンパプログラムにおいて、前記アプリケーションは、アプリケーションの本体のハッシュに共通鍵を用いて暗号化した結果を署名とし、本体と署名を結合したものであって、前記セキュリティデータを格納するステップと、共通鍵を用いて前記署名を前記復号化し、得られる第１ハッシュを出力するステップと、前記本体のハッシュである第２ハッシュを算出し、前記第１ハッシュと前記第２ハッシュが一致しない場合に信号を出力し、前記第１ハッシュと前記第２ハッシュが一致した場合に前記アプリケーションを実行するステップと、前記信号を受け取ると前記セキュリティデータを消去するステップとをコンピュータに実行させるものである。

【００１６】

また、本発明は、セキュリティデータにアクセスするアプリケーションを実行する耐タンパ方法をコンピュータに実行させる耐タンパプログラムにおいて、前記アプリケーションは、共通鍵を用いて生成した署名を、前記アプリケーションのアクセス権限に応じて本体に付加したものであって、前記セキュリティデータを格納するステップと、前記共通鍵を用いて前記署名を復号化するステップと、前記アプリケーションを実行し、前記署名に対応するアクセス権限で許可されていないアクセスが発生した場合に信号を出力するステップと、前記信号を受け取ると前記セキュリティデータを消去するステップとをコンピュータに実行させるものである。

【００１７】

また、本発明は、Flash ROMに格納されたプログラムによって、セキュリティデータにアクセスする耐タンパ方法をコンピュータに実行させる耐タンパプログラムにおいて、前記セキュリティデータを格納するステップと、前記プログラムを実行するとともに、前記Flash ROMの書き換えを示す信号が発生した場合に信号を出力するステップと、前記信号を受け取ると前記セキュリティデータを消去するステップとをコンピュータに実行させるものである。

【００１８】

なお、上述した耐タンパプログラムはコンピュータにより読取り可能な媒体に記録することができる。ここで上記コンピュータにより読取り可能な記録媒体は、ＣＤ－ＲＯＭやフレキシブルディスク、ＤＶＤディスク、光磁気ディスク、ＩＣカード等の可搬型記憶媒体や、コンピュータプログラムを保持するデータベース、或いは、他のコンピュータ並びにそのデータベースや、更に回線上の伝送媒体をも含むものである。

【発明の効果】

【００１９】

本発明によれば、ソフトウェアの脆弱性を利用した攻撃に対して耐タンパ機能を持たせることができる。また、アプリケーションの署名において共通鍵を使用することができるため、暗号化、復号化における演算速度が高く、装置のコストが低い。共通鍵は、漏洩すると使用できなくなるが、セキュリティモジュール内だけで共通鍵を使用することから、共通鍵の漏洩を防ぐことができる。

【００２０】
　また、本発明によれば、セキュリティに関連しないデータやＩ／Ｏへのアクセスを行うアプリケーションについては、セキュリティルームにおける署名の付与を行う必要がなく、常に署名を付与しなければならない方式に比べて生産コストを大幅に削減することができる。さらに、予めアプリケーション毎に適切なアクセス権限を与えることができる。
【００２１】
　また、本発明によれば、Flash ROMの不正な書き換えを防止することができる。さらに、Flash ROMの安全性を高めたことにより、カーネルやドライバ等の基本ソフトウェアをFlash ROMに格納することができ、マスクROMに格納する場合と比較して、アップデート等のコストを大幅に削減することができる。
【発明を実施するための最良の形態】
【００２２】
　以下、本発明の実施の形態について図面を参照しつつ説明する。
実施の形態１．
　本実施の形態１では、メインユニットがアプリケーションの署名チェックを行い、不正なアプリケーションである場合に、セキュリティモジュールにタンパ信号（本発明の信号に対応する）を送り、セキュリティモジュールがセキュリティデータを消去する情報処理装置について説明する。
【００２３】
　まず、実施の形態１に係る情報処理装置の構成について説明する。図１は、実施の形態１に係る情報処理装置（耐タンパ情報処理装置又は耐タンパ情報端末）の構成の一例を示すブロック図である。実施の形態１に係る情報処理装置は、メインユニット１とセキュリティモジュール２で構成される。メインユニット１は、MPU（Microprocessing Unit）１１、ROM１２、RAM（Random Access Memory）１３、表示部１４、外部I/F（インターフェイス）１５、通信部１６で構成される。ROM１２はマスクROM、またはFlash ROMである。セキュリティモジュール２は、MPU２１、ROM２２、SRAM（Static Random Access Memory）２３、耐タンパ部２４、暗号化部２５、通信部２６で構成され、メインユニット１とは別の電源で、常時動作している。
【００２４】
　メインユニット１において、MPU１１は、メインユニット１の制御を行う。ROM１２は、メインユニット１の動作に必要なカーネル、ドライバ等のプログラムを記憶する。RAM１３は、インストールしたアプリケーションを保存する。表示部１４は、アプリケーション等の実行結果を表示する。外部I/F１５は、外部機器に接続され、データの入出力を行う。
【００２５】
　また、セキュリティモジュール２において、MPU２１は、セキュリティモジュール２の制御を行う。ROM２２は、セキュリティモジュール２の動作に必要なプログラムを記憶する。SRAM２３は、共通鍵、データ、ロジック等のセキュリティデータを記憶する。SRAM２３へのセキュリティデータの書き込みはセキュリティルームにおいてのみ行うことができる。暗号化部２５は、メインユニット１からの情報の暗号化、復号化を行い、結果をメインユニット１へ返す。耐タンパ部２４は、タンパ信号を受け取るとSRAM２３のセキュリティデータの消去を行うことにより、セキュリティモジュール２、メインユニット１の動作を不可能にする。
【００２６】
　メインユニット１の通信部１６とセキュリティモジュール２の通信部２６は、ハッシュや署名等の通信を行う。
【００２７】
　次に、実施の形態１に係る情報処理装置のアプリケーション作成の動作について説明する。図２は、実施の形態１に係る情報処理装置におけるアプリケーション作成の動作を示すフローチャートである。まず、MPU１１は、外部I/F１５から入力されたアプリケーショ

ンをRAM１３へ格納する（Ｓ１）。次に、MPU１１は、アプリケーションを本体として、本体のハッシュ化を行い、ハッシュをセキュリティモジュール２へ渡す（Ｓ２）。

【００２８】

次に、MPU２１は、SRAM２３に記憶された共通鍵を用いて暗号化部２５によりハッシュを暗号化し、署名としてメインユニット１へ渡す（Ｓ３）。次に、MPU１１は、本体と署名を結合したものを新たにアプリケーションとして、RAM１３に格納し（Ｓ４）、このフローを終了する。

【００２９】

次に、実施の形態１に係る情報処理装置のアプリケーション認証の動作について説明する。図３は、実施の形態１に係る情報処理装置におけるアプリケーション認証の動作を示すフローチャートである。アプリケーションを起動すると、まず、MPU１１は、RAM１３に格納されたアプリケーションにおいて本体と署名を分離し、署名をセキュリティモジュール２へ渡す（Ｓ１１）。次に、MPU１１は、本体のハッシュ化を行う（Ｓ１２）。次に、MPU２１は、SRAM２３に記憶された共通鍵を用いて暗号化部２５により署名の複合化を行い、得られるハッシュをメインユニット１へ渡す（Ｓ１３）。次に、MPU１１は、本体から得られたハッシュと署名から得られたハッシュの比較を行い、一致するか否かの判断を行う（Ｓ１４）。

【００３０】

ハッシュが一致すれば（Ｓ１４，Ｙｅｓ）、このフローを終了する。一方、ハッシュが一致しなければ（Ｓ１４，Ｎｏ）、MPU１１は、タンパ信号を発生させ、セキュリティモジュール２に渡す（Ｓ１５）。タンパ信号を受け取った耐タンパ部２４は、SRAM２３のセキュリティデータの消去を行い（Ｓ１６）、このフローを終了する。

【００３１】

上述した情報処理装置によれば、ソフトウェアの脆弱性を利用した攻撃に対して耐タンパ機能を持たせることができる。また、アプリケーションの署名において共通鍵を使用することができるため、暗号化、復号化における演算速度が高く、装置のコストが低い。共通鍵は、漏洩すると使用できなくなるが、セキュリティモジュール内だけで共通鍵を使用することから、共通鍵の漏洩を防ぐことができる。

【００３２】

実施の形態２．

実施の形態２では、メインユニットがアプリケーションの署名に応じたアクセス権限を付与し、アプリケーションが許可されていないアクセスを行った場合に、セキュリティモジュールにタンパ信号を送り、セキュリティモジュールがセキュリティデータを消去する情報処理装置について説明する。

【００３３】

まず、実施の形態２に係る情報処理装置の構成について説明する。実施の形態２に係る情報処理装置は、図１と同様の構成である。

【００３４】

次に、実施の形態２に係る情報処理装置のアプリケーション作成の動作について説明する。図４は、実施の形態２に係る情報処理装置におけるアプリケーション作成の動作を示すフローチャートである。まず、MPU１１は、外部I/F１５から入力されたアプリケーションをRAM１３へ格納する（Ｓ２１）。次に、MPU１１は、アプリケーションに対して、より上位の権限を付与するか否かの判断を行う（Ｓ２２）。

【００３５】

上位の権限を付与する場合（Ｓ２２，Ｙｅｓ）、アプリケーションを本体として、本体のハッシュ化を行い、ハッシュをセキュリティモジュール２へ渡す（Ｓ２３）。次に、MPU２１は、SRAM２３に記憶された共通鍵を用いて暗号化部によりハッシュを暗号化し、署名としてメインユニット１へ渡す（Ｓ２４）。次に、MPUは１１、本体と署名を結合したものを新たにアプリケーションとして、RAM１３に格納し（Ｓ２５）、Ｓ２２へ戻る。一方、上位の権限を付与しない場合（Ｓ２２，Ｎｏ）、このフローを終了する。

【００３６】
次に、実施の形態２に係る情報処理装置のアプリケーション実行の動作について説明する。図５は、実施の形態２に係る情報処理装置におけるアプリケーション実行の動作を示すフローチャートである。アプリケーションを起動すると、まず、MPU１１は、RAM１３に格納されたアプリケーションに復号していない署名があるか否かの判断を行う（Ｓ３１）。
【００３７】
復号していない署名があれば（Ｓ３１，Ｙｅｓ）、本体と署名を分離し、署名をセキュリティモジュール２へ渡す（Ｓ３２）。次に、MPU１１は、本体のハッシュ化を行う（Ｓ３３）。次に、MPU２１は、SRAM２３に記憶された共通鍵を用いて暗号化部２５により署名の復号化を行い、復号化の結果をメインユニット１へ渡す（Ｓ３４）。次に、MPU１１は、本体から得られたハッシュと署名から得られたハッシュの比較を行い、一致するか否かの判断を行う（Ｓ３５）。
【００３８】
ハッシュが一致すれば（Ｓ３５，Ｙｅｓ）、他の署名について処理Ｓ３１を行う。一方、ハッシュが一致しなければ（Ｓ３５，Ｎｏ）、MPU１１は、タンパ信号を発生させ、セキュリティモジュール２に渡す（Ｓ４２）。タンパ信号を受け取った耐タンパ回路２４は、SRAM２３のセキュリティデータの消去を行い（Ｓ４３）、このフローを終了する。
【００３９】
処理Ｓ３１において、復号していない署名がなければ（Ｓ３１，Ｎｏ）、MPU１１は、アプリケーションに対して、復号した署名の内容に応じたアクセス権限の付与を行う（Ｓ３６）。例えば、アプリケーションに署名がない場合、セキュリティに関連しないデータやＩ／Ｏへのアクセス権限を付与し、アプリケーションに署名１がある場合、さらにセキュリティレベル１のデータやＩ／Ｏへのアクセス権限を付与し、アプリケーションに署名２がある場合、さらにセキュリティレベル２のデータやＩ／Ｏへのアクセス権限を付与する。
【００４０】
次に、MPU１１は、アプリケーションを実行し（Ｓ３７）、アプリケーションのアクセスを監視し、アクセス権限で許可されていない不正なアクセスが発生したか否かの判断を行う（Ｓ４１）。
【００４１】
不正なアクセスがなかった場合（Ｓ４１，Ｎｏ）、このフローを終了する。一方、不正なアクセスがあった場合（Ｓ４１，Ｙｅｓ）、処理Ｓ４２へ移行する。
【００４２】
上述した情報処理装置によれば、セキュリティに関連しないデータやＩ／Ｏへのアクセスを行うアプリケーションについては、セキュリティルームにおける署名の付与を行う必要がなく、常に署名を付与しなければならない方式に比べて生産コストを大幅に削減することができる。さらに、予めアプリケーション毎に適切なアクセス権限を与えることができる。
【００４３】
実施の形態３．
実施の形態３では、メインユニットにおいて、カーネルやドライバが格納されたFlash ROMの書き換えが行われた場合、セキュリティモジュールにタンパ信号を送り、セキュリティモジュールがセキュリティデータを消去する情報処理装置について説明する。
【００４４】
まず、実施の形態３に係る情報処理装置の構成について説明する。図６は、実施の形態３に係る情報処理装置の構成の一例を示すブロック図である。図６において、図１と同一符号は図１に示された対象と同一又は相当物を示しており、ここでの説明を省略する。図６において、情報処理装置は、メインユニット１の代わりにメインユニット１０を備える。メインユニット１０はROM１２の代わりにFlash ROM４１を備え、新たにタンパ検出部４

２を備える。タンパ検出部４２は、Flash ROM４１の書き換えを監視し、書き換えが行われた場合に、タンパ検出信号を耐タンパ部２４へ出力する。

【００４５】

次に、実施の形態３に係る情報処理装置におけるFlash ROMの書き換え検出の動作について説明する。図７は、実施の形態３に係る情報処理装置におけるFlash ROMの書き換え検出の動作を示すフローチャートである。タンパ検出部４２は、Flash ROM４１のWrite Enable信号とChip Select信号を監視することにより、Flash ROM４１の書き換えがあったか否かの判断を行う（Ｓ５１）。ここで、タンパ検出部４２は、Flash ROM４１のWrite Enable信号とChip Select信号の両方がアクティブになった場合に、Flash ROM４１の書き換えがあったと判断する。書き換えがない場合（Ｓ５１，Ｎｏ）、処理Ｓ４１に戻り、タンパ検出部４２は引き続きFlash ROM４１の監視を行う。一方、書き換えがあった場合（Ｓ５１，Ｙｅｓ）、タンパ検出部４２は、タンパ信号を発生させ、セキュリティモジュール２に渡す（Ｓ５２）。タンパ信号を受け取った耐タンパ回路２４は、SRAM２３のセキュリティデータの消去を行い（Ｓ５３）、このフローを終了する。

【００４６】

なお、実施の形態３では、タンパ検出部４２が監視する信号をWrite Enable信号とChip Select信号としたが、Flash ROM４１に対するErase信号またはWrite Protect解除信号を監視し、Erase信号またはWrite Protect解除信号を検出した場合に、Flash ROM４１の書き換えがあったと判断し、タンパ信号を発生させるようにしても良い。

【００４７】

上述した情報処理装置によれば、Flash ROMの不正な書き換えを防止することができる。さらに、Flash ROMの安全性を高めたことにより、カーネルやドライバ等の基本ソフトウェアをFlash ROMに格納することができ、マスクROMに格納する場合と比較して、アップデート等のコストを大幅に削減することができる。

【００４８】

（付記１）　セキュリティデータにアクセスするアプリケーションを実行する情報処理装置において、

前記アプリケーションは、アプリケーションの本体のハッシュに共通鍵を用いて暗号化した結果を署名とし、本体と署名を結合したものであって、

前記セキュリティデータを格納するとともに、前記共通鍵を用いて前記署名を復号化し、得られる第１ハッシュを出力するセキュリティモジュールと、

前記本体のハッシュである第２ハッシュを算出し、前記第１ハッシュと前記第２ハッシュが一致しない場合に信号を前記セキュリティモジュールへ出力し、前記第１ハッシュと前記第２ハッシュが一致した場合に前記アプリケーションを実行するメインユニットと、

を備え、

前記セキュリティモジュールは、前記メインユニットから前記信号を受け取ると前記セキュリティデータを消去することを特徴とする情報処理装置。

（付記２）　セキュリティデータにアクセスするアプリケーションを実行する情報処理装置において、

前記アプリケーションは、共通鍵を用いて生成した署名を、前記アプリケーションのアクセス権限に応じて本体に付加したものであって、

前記セキュリティデータを格納するとともに、前記共通鍵を用いて前記署名を復号化するセキュリティモジュールと、

前記アプリケーションを実行し、前記署名に対応するアクセス権限で許可されていないアクセスが発生した場合に信号を前記セキュリティモジュールへ出力するメインユニットと、

を備え、

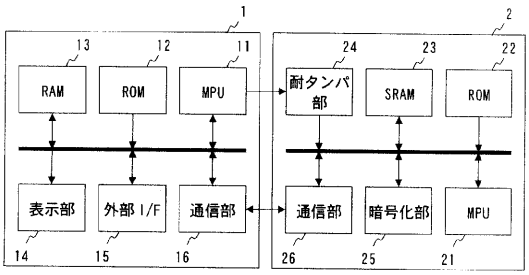
前記セキュリティモジュールは、前記メインユニットから前記信号を受け取ると前記セキュリティデータを消去することを特徴とする情報処理装置。

（付記３）　Flash ROMに格納されたプログラムによって、セキュリティデータにアクセ

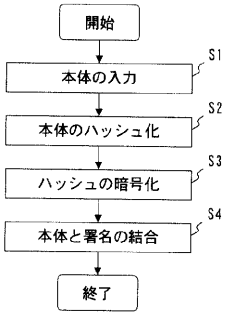
スする情報処理装置において、
前記セキュリティデータを格納するセキュリティモジュールと、
前記プログラムを実行するとともに、前記Flash ROMの書き換えを示す信号が発生した場合に信号を前記セキュリティモジュールへ出力するメインユニットと、
を備え、
前記セキュリティモジュールは、前記メインユニットから前記信号を受け取ると前記セキュリティデータを消去することを特徴とする情報処理装置。
（付記４） 付記３に記載の情報処理装置において、
前記Flash ROMの書き換えを示す信号は、Write Enable信号とChip Select信号であることを特徴とする情報処理装置。
（付記５） 付記３に記載の情報処理装置において、
前記Flash ROMの書き換えを示す信号は、Erase信号またはWrite Protect解除信号であることを特徴とする情報処理装置。
（付記６）セキュリティデータにアクセスするアプリケーションを実行する耐タンパ方法において、
前記アプリケーションは、アプリケーションの本体のハッシュに共通鍵を用いて暗号化した結果を署名とし、本体と署名を結合したものであって、
前記セキュリティデータを格納するステップと、
前記共通鍵を用いて前記署名を復号化し、得られる第１ハッシュを出力するステップと、
前記本体のハッシュである第２ハッシュを算出し、前記第１ハッシュと前記第２ハッシュが一致しない場合に信号を出力し、前記第１ハッシュと前記第２ハッシュが一致した場合に前記アプリケーションを実行するステップと、
前記信号を受け取ると前記セキュリティデータを消去するステップと、
を備えてなる耐タンパ方法。
（付記７）セキュリティデータにアクセスするアプリケーションを実行する耐タンパ方法において、
前記アプリケーションは、共通鍵を用いて生成した署名を、前記アプリケーションのアクセス権限に応じて本体に付加したものであって、
前記セキュリティデータを格納するステップと、
前記共通鍵を用いて前記署名を復号化するステップと、
前記アプリケーションを実行し、前記署名に対応するアクセス権限で許可されていないアクセスが発生した場合に信号を出力するステップと、
前記信号を受け取ると前記セキュリティデータを消去するステップと、
を備えてなる耐タンパ方法。
（付記８） Flash ROMに格納されたプログラムによって、セキュリティデータにアクセスする耐タンパ方法において、
前記セキュリティデータを格納するステップと、
前記プログラムを実行するとともに、前記Flash ROMの書き換えを示す信号が発生した場合に信号を出力するステップと、
前記信号を受け取ると前記セキュリティデータを消去するステップと、
を備えてなる耐タンパ方法。
（付記９） セキュリティデータにアクセスするアプリケーションを実行する耐タンパ方法をコンピュータに実行させる耐タンパプログラムにおいて、
前記アプリケーションは、アプリケーションの本体のハッシュに共通鍵を用いて暗号化した結果を署名とし、本体と署名を結合したものであって、
前記セキュリティデータを格納するステップと、
共通鍵を用いて前記署名を前記復号化し、得られる第１ハッシュを出力するステップと、
前記本体のハッシュである第２ハッシュを算出し、前記第１ハッシュと前記第２ハッシ

ュが一致しない場合に信号を出力し、前記第１ハッシュと前記第２ハッシュが一致した場合に前記アプリケーションを実行するステップと、
前記信号を受け取ると前記セキュリティデータを消去するステップと、
をコンピュータに実行させる耐タンパプログラム。
（付記１０）　セキュリティデータにアクセスするアプリケーションを実行する耐タンパ方法をコンピュータに実行させる耐タンパプログラムにおいて、
前記アプリケーションは、共通鍵を用いて生成した署名を、前記アプリケーションのアクセス権限に応じて本体に付加したものであって、
前記セキュリティデータを格納するステップと、
前記共通鍵を用いて前記署名を復号化するステップと、
前記アプリケーションを実行し、前記署名に対応するアクセス権限で許可されていないアクセスが発生した場合に信号を出力するステップと、
前記信号を受け取ると前記セキュリティデータを消去するステップと、
をコンピュータに実行させる耐タンパプログラム。
（付記１１）　Flash ROMに格納されたプログラムによって、セキュリティデータにアクセスする耐タンパ方法をコンピュータに実行させる耐タンパプログラムにおいて、
前記セキュリティデータを格納するステップと、
前記プログラムを実行するとともに、前記Flash ROMの書き換えを示す信号が発生した場合に信号を出力するステップと、
前記信号を受け取ると前記セキュリティデータを消去するステップと、
をコンピュータに実行させる耐タンパプログラム。
【図面の簡単な説明】
【００４９】
【図１】実施の形態１に係る情報処理装置の構成の一例を示すブロック図である。
【図２】実施の形態１に係る情報処理装置におけるアプリケーション作成の動作を示すフローチャートである。
【図３】実施の形態１に係る情報処理装置におけるアプリケーション認証の動作を示すフローチャートである。
【図４】実施の形態２に係る情報処理装置におけるアプリケーション作成の動作を示すフローチャートである。
【図５】実施の形態２に係る情報処理装置におけるアプリケーション実行の動作を示すフローチャートである。
【図６】実施の形態３に係る情報処理装置の構成の一例を示すブロック図である。
【図７】実施の形態３に係る情報処理装置におけるFlash ROMの書き換え検出の動作を示すフローチャートである。
【符号の説明】
【００５０】
１，１０　メインユニット、１１　MPU、１２　ROM、１３　RAM、１４　表示部、１５　外部I/F、１６　通信部、４１　Flash ROM、４２　タンパ検出部、２　セキュリティモジュール、２１　MPU、２２　ROM、２３　SRAM、２４　耐タンパ部、２５　暗号化部、２６　通信部。

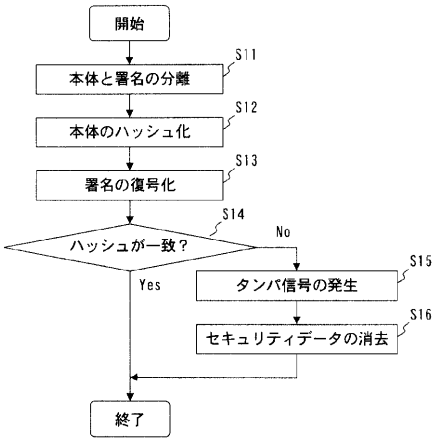
【図１】


1
2
13
12
11
24
23
22
RAM
ROM
MPU
耐タンパ部
SRAM
ROM
表示部
外部 I/F
通信部
通信部
暗号化部
MPU
14
15
16
26
25
21

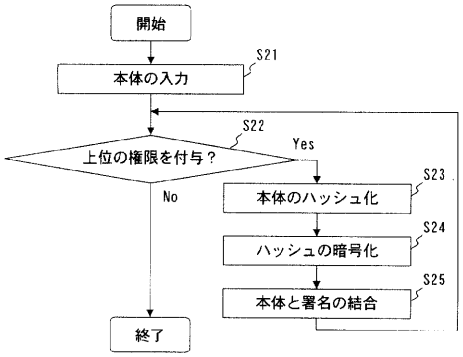
【図２】


開始
本体の入力
S1
本体のハッシュ化
S2
ハッシュの暗号化
S3
本体と署名の結合
S4
終了

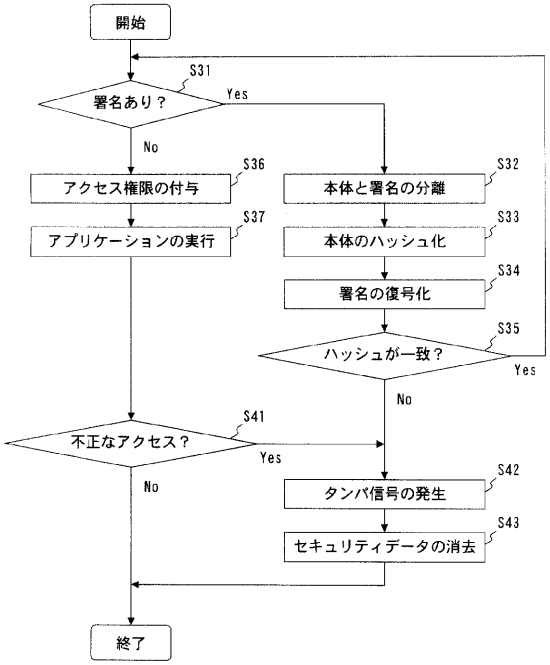
【図３】


開始
本体と署名の分離
S11
本体のハッシュ化
S12
署名の復号化
S13
ハッシュが一致？
S14
No
Yes
タンパ信号の発生
S15
セキュリティデータの消去
S16
終了

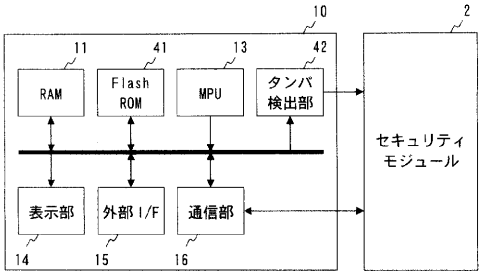
【図４】


開始
本体の入力
S21
上位の権限を付与？
S22
Yes
No
本体のハッシュ化
S23
ハッシュの暗号化
S24
本体と署名の結合
S25
終了

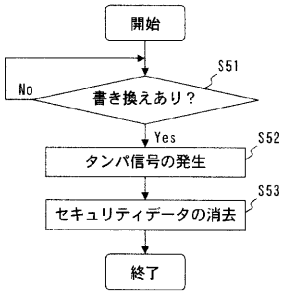
【図５】


開始
署名あり？
S31
Yes
No
アクセス権限の付与
S36
アプリケーションの実行
S37
本体と署名の分離
S32
本体のハッシュ化
S33
署名の復号化
S34
ハッシュが一致？
S35
Yes
No
不正なアクセス？
S41
Yes
No
タンパ信号の発生
S42
セキュリティデータの消去
S43
終了

【図６】


10
2
11
41
13
42
RAM
Flash ROM
MPU
タンパ検出部
セキュリティモジュール
表示部
外部I/F
通信部
14
15
16

【図７】


開始
S51
No
書き換えあり？
Yes
S52
タンパ信号の発生
S53
セキュリティデータの消去
終了

フロントページの続き

Ｆターム(参考) 5B017 AA07 AA08 BA06 BA08 BB03 BB11 CA12 CA15 CA16
5B076 FA01 FA07 FD07
5J104 AA09 AA16 AA46 EA03 EA04 EA09 EA22 LA01 LA02 LA06
NA02 NA05 NA12 NA27 NA38 NA40 NA42 PA14