(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4833294号
(P4833294)
(45)発行日　平成23年12月7日(2011.12.7)　(24)登録日　平成23年9月30日(2011.9.30)

(51)Int.Cl.　　F I
G06F 21/20 (2006.01)　　G06F 15/00 330F
G06F 21/22 (2006.01)　　G06F 9/06 660E
G06F 1/00 (2006.01)　　G06F 1/00 370E

請求項の数 4　(全 12 頁)

(21)出願番号　特願2008-535231 (P2008-535231)
(86)(22)出願日　平成18年9月20日 (2006.9.20)
(86)国際出願番号　PCT/JP2006/318636
(87)国際公開番号　WO2008/035412
(87)国際公開日　平成20年3月27日 (2008.3.27)
審査請求日　平成20年11月21日 (2008.11.21)

(73)特許権者　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
(74)代理人　100089118
弁理士　酒井　宏明
(72)発明者　鈴木　雅人
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
(72)発明者　小谷　誠剛
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

審査官　平井　誠

最終頁に続く

(54)【発明の名称】情報処理装置および起動方法

(57)【特許請求の範囲】
【請求項１】
情報処理装置内に実装され、所定の処理を独立して実行するチップおよび情報処理装置を制御する制御装置を備えた情報処理装置であって、
前記チップは、
前記情報処理装置の操作を許可された利用者の生体情報を示す生体認証情報および前記情報処理装置にインストールされたソフトウェアに関する情報を記憶する記憶手段と、
前記情報処理装置に対する起動要求を取得した場合に、利用者の生体情報を取得し、当該生体情報および前記生体認証情報を基にして前記情報処理装置の起動を許可するか否かを判定する生体判定手段と、
前記情報処理装置に対する起動要求を取得した場合に、前記記憶手段に記憶されたソフトウェアに関する情報に基づいて不正なソフトウェアがインストールされているか否かを判定するソフトウェア判定手段と、
前記生体判定手段および前記ソフトウェア判定手段の判定結果に基づいて、前記制御装置の起動を制御する起動制御手段と
を備えたことを特徴とする情報処理装置。
【請求項２】
前記チップは、前記情報処理装置にインストールされたソフトウェアに関する情報を取得し、前記記憶手段に記憶されたソフトウェアに関する情報を更新する情報更新手段を更に備えたことを特徴とする請求項１に記載の情報処理装置。

【請求項３】
情報処理装置内に実装され、所定の処理を独立して実行するチップおよび情報処理装置を制御する制御装置を備えた情報処理装置の起動方法であって、
前記チップは、
前記情報処理装置の操作を許可された利用者の生体情報を示す生体認証情報および前記情報処理装置にインストールされたソフトウェアに関する情報を記憶装置に記憶する記憶工程と、
前記情報処理装置に対する起動要求を取得した場合に、利用者の生体情報を取得し、当該生体情報および前記生体認証情報を基にして前記情報処理装置の起動を許可するか否かを判定する生体判定工程と、
前記情報処理装置に対する起動要求を取得した場合に、前記記憶装置に記憶されたソフトウェアに関する情報に基づいて不正なソフトウェアがインストールされているか否かを判定するソフトウェア判定工程と、
前記生体判定工程および前記ソフトウェア判定工程の判定結果に基づいて、前記制御装置の起動を制御する起動制御工程と
を含んだことを特徴とする起動方法。
【請求項４】
前記チップ内で、前記情報処理装置にインストールされたソフトウェアに関する情報を取得し、前記記憶装置に記憶されたソフトウェアに関する情報を更新する情報更新工程を更に含んだことを特徴とする請求項３に記載の起動方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、情報処理装置内に実装され、所定の処理を独立して実行するチップを備えた情報処理装置等に関し、特に情報漏洩の問題を解消することができる情報処理装置および起動方法に関するものである。
【背景技術】
【０００２】
近年、情報処理装置に記憶された情報（機密情報や利用者のプライバシーに関わる情報等）の漏洩などの問題を解消するために、指紋、虹彩、顔貌、静脈といった利用者本人の生体情報を利用して情報処理装置に記憶された情報を保護するバイオメトリック認証機能を情報処理装置に搭載する試みがなされている。かかる従来のバイオメトリック認証機能では、情報処理装置に電源が投入された後、情報処理装置に組み込まれたＯＳ（Operating System）やバイオメトリック認証機能を実現させる認証プログラム等のシステムが起動した後に、利用者からの生体情報を取得して、情報処理装置の操作を許可するか否かを判定している。
【０００３】
なお、特許文献１では、利用者に対する認証処理を実行するためのプログラムおよびデータの更新を柔軟かつ厳粛に実行可能とする情報管理装置が提案されている。
【０００４】
【特許文献１】国際公開第２００５／１０６６２０号パンフレット
【発明の開示】
【発明が解決しようとする課題】
【０００５】
しかしながら、上述した従来の技術では、情報処理装置に組み込まれたシステムが起動した後にはじめて本人の生体情報による認証機能（セキュリティ機能）が有効となるため、情報処理装置が起動してから認証機能が有効となる間に、情報処理装置に記憶された情報を保護することができないという問題があった。
【０００６】
つまり、電源投入直後のＯＳ等のシステム起動前の状態では、何ら内部の情報は保護さ

れることはなく、外部のＯＳ起動方法（ＦＤＤ、ＣＤ－ＲＯＭ等）からのゲストＯＳ等の起動により、簡単に情報処理装置内部の情報が盗難にあう問題があった。

【０００７】

この発明は、上述した従来技術による問題点を解消するためになされたものであり、情報処理装置に記憶された情報を保護することができる情報処理装置および起動方法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】

【０００８】

上述した課題を解決し、目的を達成するため、本発明は、情報処理装置内に実装され、所定の処理を独立して実行するチップを備えた情報処理装置であって、前記チップは、前記情報処理装置の操作を許可された利用者の生体情報を生体認証情報として記憶する記憶手段と、前記情報処理装置に対する起動要求を取得した場合に、利用者の生体情報を取得し、当該生体情報および前記生体認証情報を基にして前記情報処理装置の起動を許可するか否かを判定する生体判定手段と、を備えたことを特徴とする。

【０００９】

また、本発明は、上記発明において、前記記憶手段は、前記情報処理装置に係る環境の情報を更に記憶し、前記チップは、前記情報処理装置に対する起動要求を取得した場合に、前記記憶手段に記憶された環境の情報に基づいて前記情報処理装置の起動を許可するか否かを判定する環境判定手段を更に備えたことを特徴とする。

【００１０】

また、本発明は、上記発明において、前記情報処理装置は、前記チップを除いた情報処理装置全体を制御する制御装置を備え、前記チップは、前記生体判定手段および前記環境判定手段の判定結果に基づいて、前記制御装置の起動を制御する起動制御手段を更に備えたことを特徴とする。

【００１１】

また、本発明は、上記発明において、前記チップは、前記情報処理装置に係る環境の情報を取得し、前記記憶手段に記憶された環境の情報を更新する環境情報更新手段を更に備えたことを特徴とする。

【００１２】

また、本発明は、情報処理装置内に実装され、所定の処理を独立して実行するチップを備えた情報処理装置の起動方法であって、前記チップは、前記情報処理装置の操作を許可された利用者の生体情報を生体認証情報として記憶装置に記憶する記憶工程と、前記情報処理装置に対する起動要求を取得した場合に、利用者の生体情報を取得し、当該生体情報および前記生体認証情報を基にして前記情報処理装置の起動を許可するか否かを判定する生体判定工程と、を含んだことを特徴とする。

【００１３】

また、本発明は、上記発明において、前記記憶工程は、前記情報処理装置に係る環境の情報を更に記憶装置に記憶し、前記チップ内で、前記情報処理装置に対する起動要求を取得した場合に、前記記憶装置に記憶された環境の情報に基づいて前記情報処理装置の起動を許可するか否かを判定する環境判定工程を更に含んだことを特徴とする。

【００１４】

また、本発明は、上記発明において、前記情報処理装置は、前記チップを除いた情報処理装置全体を制御する制御装置を備え、前記チップ内で、前記生体判定工程および前記環境判定工程の判定結果に基づいて、前記制御装置の起動を制御する起動制御工程を更に含んだことを特徴とする。

【００１５】

また、本発明は、上記発明において、前記チップ内で、前記情報処理装置に係る環境の情報を取得し、前記記憶装置に記憶された環境の情報を更新する環境情報更新工程を更に含んだことを特徴とする。

【発明の効果】

【００１６】
本発明によれば、所定の処理を独立して実行するチップにおいて、情報処理装置の操作を許可された利用者の生体情報を生体認証情報として記憶し、情報処理装置に対する起動要求を取得した場合に、利用者の生体情報を取得し、生体情報および生体認証情報を基にして情報処理装置の起動を許可するか否かを判定するので、情報処理装置の電源投入時にかかる情報漏洩を防ぐことができる。
【００１７】
また、本発明によれば、チップに情報処理装置に係る環境の情報を更に記憶し、情報処理装置に対する起動要求を取得した場合に、記憶手段に記憶された環境の情報に基づいて情報処理装置の起動を許可するか否かを判定するので情報処理装置の安全性を向上させることができる。
【００１８】
また、本発明によれば、情報処理装置は、チップを除いた情報処理装置全体を制御する制御装置を備え、チップは、生体情報に対する判定結果および環境の情報に対する判定結果に基づいて、制御装置の起動を制御するので、情報処理装置に電源が投入されてから制御装置が起動するまでの間に情報が盗まれることを防止することができる。
【００１９】
また、本発明によれば、チップは、情報処理装置に係る環境の情報を取得し、環境の情報を更新するので、不正な周辺機器およびプログラム等を情報処理装置から排除し、情報処理装置の安全性を向上させることができる。
【発明を実施するための最良の形態】
【００２０】
以下に添付図面を参照して、この発明に係る情報処理装置および起動方法の好適な実施の形態を詳細に説明する。
【実施例】
【００２１】
まず、本実施例にかかる情報処理装置の概要および特徴について説明する。本実施例にかかる情報処理装置は、所定の処理を独立して実行するセキュリティチップ（例えば、国際公開第２００５／１０６６２０号パンフレットに開示されているような生体認証機能を有するＬＳＩ）を実装し、このセキュリティチップが、情報処理装置への電源投入時に、情報処理装置のＣＰＵ等の主要なＬＳＩまたはシステム全体の起動に先立って単独で起動する。
【００２２】
そして、セキュリティチップは、外部に接続された生体認証用のセンサから利用者の生体情報（指紋、虹彩、顔貌、静脈などの生体情報）を取得し、取得した生体情報と、予め記憶していた利用者の生体情報とを基にして情報処理装置の起動を許可するか否かを判定し、情報処理装置の起動を許可すると判定した場合に、情報処理装置のＣＰＵ等の主要なＬＳＩまたはシステム全体を起動させる。
【００２３】
このように、セキュリティチップが情報処理装置のＣＰＵ等に先立って起動し、情報処理装置の起動を許可するか否かを判定するので、情報処理装置に記録された情報の漏洩あるいはセキュリティホールを悪用した情報の盗難が防止できる。
【００２４】
つぎに、本実施例にかかる情報処理装置の構成について説明する。図１は、本実施例にかかる情報処理装置の構成を示す機能ブロック図である。同図に示すように、この情報処理装置１００は、通信Ｉ／Ｆ（インターフェース）１１０と、生体センサ１２０と、ＣＰＵ１３０と、メモリ／ストレージ１４０と、セキュリティチップ１５０とを備えて構成される。なお、メモリ／ストレージ１４０には、各種ソフトウェア１６０が記憶されている。
【００２５】

通信Ｉ／Ｆ１１０は、ネットワークと内部とのインターフェースを司り、外部装置からのデータの入出力を制御する。通信Ｉ／Ｆ１１０には、例えば、モデムやＬＡＮ（Local Area Network）アダプタなどを採用することができる。なお、図示しないが、情報処理装置１００は、通信Ｉ／Ｆ１１０を介して、認証局の端末や、様々なサービスにかかる実行プログラムや各種データを開発するベンダーやメーカー、情報処理装置１００を製造または販売する業者などが管理するサービス提供事業者端末などとデータ通信を行う。なお、通信Ｉ／Ｆ１１０は、セキュリティチップ１５０によって起動を制御される。

【００２６】

生体センサ１２０は、例えば、指紋センサ、カメラおよびマイクなどが挙げられる。指紋センサは、およそ５０μｍ間隔で指の指紋の凹凸を検出して電気信号に変換する装置であり、指紋の読取方式としては、たとえば、半導体式、光学式、感圧式、感熱式などが挙げられる。カメラは、眼球の虹彩や網膜を撮影する生体センサである。また、マイクは声の特徴をあらわす声紋を検出する生体センサである。

【００２７】

ＣＰＵ１３０は、情報処理装置全体の処理をつかさどる装置である。なお、本実施例にかかるＣＰＵ１３０は、情報処理装置１００に対する電源投入時には起動せず、セキュリティチップ１５０に起動を許可された後に起動し、各種処理を実行する。

【００２８】

メモリ／ストレージ１４０は、ＣＰＵ１３０において利用される種々の情報を記憶する記憶装置である。このメモリ／ストレージ１４０は、情報処理装置１００内であれば、セキュリティチップ１５０内またはセキュリティチップ１５０外のいずれの領域に設けられてもよい。セキュリティチップ１５０内に設けられる場合は、メモリ／ストレージ１４０の取り外しや改竄を防止することができる。

【００２９】

セキュリティチップ１５０は、情報処理装置１００のメインボードに実装される。セキュリティチップ１５０は、セキュリティやプライバシーを実現するための基本機能のみを提供するチップである。また、このセキュリティチップ１５０は、ＴＣＧ（Trusted Computing Group）の仕様書によって定義されている。一の情報処理装置１００に実装されたセキュリティチップ１５０は、他の情報処理装置に実装できないようになっており、情報処理装置１００からセキュリティチップ１５０を取り外すと、当該情報処理装置１００は起動することができなくなる。また、セキュリティチップ１５０は、情報処理装置に電源が投入された場合に、情報処理装置の通信Ｉ／Ｆ１１０、ＣＰＵ１３０、メモリ／ストレージ１４０などに先立って起動する。

【００３０】

セキュリティチップ１５０は、その内部に、ＬＳＩ固有鍵記憶部１５１と、セキュアメモリ１５２と、通信認証処理部１５３と、監視処理部１５４と、検証処理部１５５と、生体認証処理部１５６と、装置内情報認証処理部１５７と、起動制御処理部１５８とを備える。

【００３１】

ＬＳＩ固有鍵記憶部１５１は、セキュリティチップ１５０固有の暗号鍵を記憶する記憶部である。セキュアメモリ１５２は、セキュリティチップ１５０において用いられる種々の情報を記憶する記憶部である。

【００３２】

ここで、セキュアメモリ１５２の説明を行う。図２は、セキュアメモリ１５２に記憶された電子証明書を示す説明図であり、図３は、セキュアメモリ１５２に記憶された生体認証情報を示す説明図であり、図４は、セキュアメモリ１５２に記憶された装置内情報を示す説明図である。

【００３３】

図２において、電子証明書Ｃａ～Ｃｚは、被証明者ごとに記憶されている。「被証明者」とは、電子証明書Ｃａ～Ｃｚによって証明された者、例えば、利用者、メーカー、ベン

ダー、認証局などが挙げられる。また、電子証明書Ｃａ～Ｃｚには、バージョン情報、署名アルゴリズム、発行者名、有効期限、公開鍵、その他の関連情報が含まれている。この電子証明書Ｃａ～Ｃｚは、セキュリティチップ１５０に含まれる装置内情報認証処理部１５７によって暗号処理等のセキュアな方法によって管理されている。

【００３４】

図３において、生体認証情報５０は、利用者名５１、センサ種情報５２、生体情報５３によって構成される。図３では、その一例として、情報処理装置１００の操作を許可された利用者「Ｘ」が、「指紋センサ」によって検出された利用者「Ｘ」の指紋の画像データ「Ｘａ」を、生体情報５３として登録している。生体認証情報５０は、セキュリティチップ１５０に含まれる装置内情報認証処理部１５７によって暗号化され記憶されている。

【００３５】

図４において、装置内情報（情報処理装置１００に係る環境情報）として、周辺機器、ソフトウェア１６０、および各ハードウェアにインストールされた各種実行プログラムの名称およびバージョン情報が記憶されている。

【００３６】

通信認証処理部１５３は、情報処理装置１００外、たとえば、ネットワークを介して接続されたサービス提供事業者端末や、認証局の端末等との間で実行される通信の安全性を保証する処理部である。通信認証処理部１５３は、具体的には、認証局を利用した電子証明書による本人認証（ＰＫＩ（Public Key Infrastructure）認証）を行うことにより、外部と通信を行う者が、認証局によって正規に登録された者であるか否かを判定することができる。

【００３７】

監視処理部１５４は、情報処理装置１００内の情報の受け渡しを監視する処理部であり、検証処理部１５５は、通信認証処理部１５３によって外部との通信の安全性が認証された場合に、当該外部からセキュリティチップ１５０に入力されてくる情報の正当性の検証や一致検証を行う処理部である。

【００３８】

生体認証処理部１５６は、生体センサ１２０によって検出された生体情報とセキュアメモリ１５２に登録された利用者の生体認証情報（図３参照）とが一致するか否かを認証する処理部である。生体認証処理部１５６では、情報処理装置１００を操作するものが正規の利用者であるか否かを判定することができる。

【００３９】

また、生体認証処理部１５６は、情報処理装置１００に対する起動要求を受け付けた場合（電源が情報処理装置１００に投入された場合）、利用者の生体情報を生体センサ１２０から取得し、セキュアメモリ１５２に記憶された生体認証情報と比較して、一致するか否かを判定し、判定結果を起動制御処理部１５８に出力する。

【００４０】

装置内情報認証処理部１５７は、セキュアメモリ１５２内の情報（装置内情報）を認証する処理部である。この装置内情報は、環境情報と呼ばれ、情報処理装置１００に接続された周辺機器から取得した周辺機器に関する情報（たとえば、機器名、バージョン情報）や、情報処理装置１００内にインストールされているソフトウェア６０に関する情報（たとえば、ソフトウェア名、バージョン情報）、メモリ／ストレージ１４０に記憶されている各種情報（たとえば、電子証明書）などを含む。

【００４１】

また、装置内情報認証処理部１５７は、セキュアメモリ１５２に記憶されている情報を機密管理する。具体的には、装置内情報認証処理部１５７が取得した情報を、ＬＳＩ固有鍵記憶部１５１に記憶された固有の暗号鍵で暗号化して、セキュアメモリ１５２に記憶する。一方、他のハードウェアからの呼び出しがあった場合、暗号鍵と対になる復号鍵（ＬＳＩ固有鍵記憶部１５１に記憶されている）で、暗号化されていた情報を復号する。この暗号化および復号化処理により、情報処理装置１００内において改竄されていないことを

認証することができる。

【００４２】

また、装置内情報認証処理部１５７は、情報処理装置１００に対する起動要求を受け付けた場合（電源が情報処理装置１００に投入された場合）、セキュアメモリ１５２に記憶された装置内情報（情報処理装置１００に係る環境の情報）を取得し、装置内情報を認証する。すなわち、装置内情報認証処理部１５７は、情報処理装置１００に使用を許可していない不正なソフトウェアがインストールされているか否か、あるいは不正な周辺機器が情報処理装置１００に接続されているか否かを判定し、判定結果を起動制御処理部１５８に出力する。なお、装置内情報認証処理部１５７は、使用を許可するソフトウェアの情報および周辺機器の情報を予め保持しているものとする。

【００４３】

また、装置内情報認証処理部１５７は、情報処理装置内に接続された周辺機器から周辺機器に関する情報、情報処理装置１００内にインストールされているソフトウェア１６０に関する情報を定期的（あるいは、情報処理装置１００の処理を終了して電源供給を中止する直前など）に取得し、セキュアメモリ１５２に記憶された装置内情報（情報処理装置１００の環境に係る情報）を更新する。

【００４４】

起動制御処理部１５８は、生体認証処理部１５６および装置内情報認証処理部１５７から判定結果を取得し、取得した判定結果に基づいてＣＰＵ１３０の起動を制御する処理部である。具体的に、この起動制御処理部１５８は、利用者の生体情報が生体認証情報と合致し、かつ、装置内情報が適切である場合に、ＣＰＵ１３０および通信Ｉ／Ｆ１１０を起動させる。

【００４５】

つぎに、本実施例にかかる情報処理装置の起動処理について説明する。図５は、本実施例にかかる起動処理を示すフローチャートである。同図に示すように、情報処理装置１００に電源が入力された場合に（ステップＳ１０１）、セキュリティチップ１５０および生体センサ１２０が起動する（ステップＳ１０２）。

【００４６】

そして、装置内情報認証処理部１５７は、セキュアメモリ１５２から装置内情報（環境情報）を取得し（ステップＳ１０３）、装置内情報を認証し（ステップＳ１０４）、認証結果（装置内情報が適切か否かの判定結果）を起動制御処理部１５８に出力する（ステップＳ１０５）。

【００４７】

続いて、生体認証処理部１５６が生体センサ１２０から利用者の生体情報を取得し（ステップＳ１０６）、生体情報と生体認証情報と比較して合致するか否かを判定し（ステップＳ１０７）、判定結果を起動制御処理部１５８に出力する（ステップＳ１０８）。

【００４８】

そして、起動制御処理部１５８は、取得した判定結果に基づいてＣＰＵ１３０および通信Ｉ／Ｆ１１０を起動させるか否かを判定し（ステップＳ１０９）、起動させない場合には（ステップＳ１１０，Ｎｏ）、そのまま処理を終了し、起動させる場合には（ステップＳ１１０，Ｙｅｓ）、通信Ｉ／Ｆ１１０およびＣＰＵ１３０を起動させる（ステップＳ１１１）。ＣＰＵ１３０は、起動後に情報処理装置１００の各種装置およびシステムを起動させる（ステップＳ１１２）。

【００４９】

このように、起動制御処理部１５８が、生体認証処理部１５６および装置内情報認証処理部１５７の判定結果に基づいて、ＣＰＵ１３０の起動を制御するので、情報処理装置１００に記憶された情報が悪意のある第三者によって盗まれることを防止することができる。

【００５０】

上述してきたように、本実施例にかかる情報処理装置１００は、所定の処理を独立して

実行するセキュリティチップ１５０を備え、セキュリティチップ１５０は、情報処理装置１００への電源投入時に、情報処理装置１００のＣＰＵ１３０などの主要なＬＳＩ又はシステム全体に先立って単独で起動する。そして、セキュリティチップ１５０は、生体センサ１２０から利用者の生体情報を取得し、取得した生体情報と、予め記憶していた利用者の生体情報とを基にして情報処理装置の起動を許可するか否かを判定し、情報処理装置１００の起動を許可すると判定した場合に、情報処理装置１００のＣＰＵ１３０等の主要なＬＳＩまたはシステム全体を起動させるので、情報処理装置に記録された情報の漏洩あるいはセキュリティホールを悪用した情報の盗難が防止できる。

【００５１】

例えば、盗難にあった情報処理装置に対し、ＦＤＤ、ＣＤ－ＲＯＭ等ゲストＯＳ等の起動を行い、情報処理装置の記憶媒体からの情報の盗用が行えなくなる。また、利用者にとっては、煩わしいログインＩＤ／パスワードの組み合わせを記憶する必要はなく、またＯＳ等のソフトウェアに依存するしくみではないため、ＯＳのセキュリティホール等の危殆化を心配する必要がなくなる。

【００５２】

つぎに、本実施例において示した情報処理装置１００のハードウェア構成について説明する。図６は、情報処理装置のハードウェア構成を示す図である。図６において、情報処理装置は、ＣＰＵ１１と、ＲＯＭ１２と、ＲＡＭ１３と、ＨＤＤ（ハードディスクドライブ）１４と、ＨＤ（ハードディスク）１５と、ＦＤＤ（フレキシブルディスクドライブ）１６と、ＦＤ（フレキシブルディスク）１７と、ディスプレイ１８と、通信Ｉ／Ｆ１９と、入力キー（キーボード、マウスを含む）２０と、生体センサ２１と、セキュリティチップ２２とから構成される。また、各構成部はバス１０にそれぞれ接続されている。

【００５３】

ここで、ＣＰＵ１１は、情報処理装置全体の制御を司る。ＲＯＭ１２は、ブートプログラムなどのプログラムを記憶している。ＲＡＭ１３は、ＣＰＵ１１のワークエリアとして使用される。ＨＤＤ１４は、ＣＰＵ１１の制御にしたがってＨＤ１５に対するデータのリード／ライトを制御する。ＨＤ１５は、ＨＤＤ１４の制御で書き込まれたデータを記憶する。

【００５４】

ＦＤＤ１６は、ＣＰＵ１１の制御にしたがってＦＤ１７に対するデータのリード／ライトを制御する。ＦＤ１７は、ＦＤＤ１６の制御で書き込まれたデータを記憶したり、ＦＤ１７に記憶されたデータを情報処理装置に読み取らせたりする。

【００５５】

また、着脱可能な記録媒体として、ＦＤ１７のほか、ＣＤ－ＲＯＭ（ＣＤ－Ｒ、ＣＤ－ＲＷ）、ＭＯ、ＤＶＤ（Digital Versatile Disk）、メモリーカードなどであってもよい。ディスプレイ１８は、カーソル、アイコンあるいはツールボックスをはじめ、文書、画像、機能情報等のデータを表示する。このディスプレイ１８は、たとえば、ＣＲＴ、ＴＦＴ液晶ディスプレイ、プラズマディスプレイなどを採用することができる。

【００５６】

通信Ｉ／Ｆ１９は、図１に示した通信Ｉ／Ｆ１１０に対応し、インターネットなどのネットワーク３０に接続されている。入力キー２０は、文字、数字、各種指示などの入力のためのキーを備え、データの入力を行う。また、タッチパネル式の入力パッドやテンキーなどであってもよい。

【００５７】

生体センサ２１およびセキュリティチップ２２は、図１に示した生体センサ１１０およびセキュリティチップ１５０にそれぞれ対応する。また、セキュリティチップ２２には図１に示した各種処理部を実現するための各種プログラム２２ａが記憶されており、かかるプログラムから各種プロセスが実行される。各種プロセスは、図１に示した、通信認証処理部１５３、監視処理部１５４、検証処理部１５５、生体認証処理部１５６、装置内情報認証処理部１５７、起動制御処理部１５８に対応する。また、セキュリティチップ１５０

は、各種プロセスを実行する上で利用される各種データ２２ｂ（実施例において説明した生体認証情報、装置内情報、ＬＳＩ固有鍵の情報などに対応する）が記憶されている。

【００５８】

さて、これまで本発明の実施例について説明したが、本発明は上述した実施例以外にも、特許請求の範囲に記載した技術的思想の範囲内において種々の異なる実施例にて実施されてもよいものである。

【００５９】

また、本実施例において説明した各処理のうち、自動的におこなわれるものとして説明した処理の全部または一部を手動的におこなうこともでき、あるいは、手動的におこなわれるものとして説明した処理の全部または一部を公知の方法で自動的におこなうこともできる。

【００６０】

この他、上記文書中や図面中で示した処理手順、制御手順、具体的名称、各種のデータやパラメータを含む情報については、特記する場合を除いて任意に変更することができる。

【００６１】

また、図示した各装置の各構成要素は機能概念的なものであり、必ずしも物理的に図示のように構成されていることを要しない。すなわち、各装置の分散・統合の具体的形態は図示のものに限られず、その全部または一部を、各種の負荷や使用状況などに応じて、任意の単位で機能的または物理的に分散・統合して構成することができる。

【産業上の利用可能性】

【００６２】

以上のように、本発明にかかる情報処理装置および起動方法は、重要な情報を記憶する情報処理装置などに有用であり、特に、情報処理装置の起動時にかかるセキュリティホールを無くし情報漏洩の問題を解消する場合に適している。

【図面の簡単な説明】

【００６３】

【図１】図１は、本実施例にかかる情報処理装置の構成を示す機能ブロック図である。

【図２】図２は、セキュアメモリに記憶された電子証明書を示す説明図である。

【図３】図３は、セキュアメモリに記憶された生体認証情報を示す説明図である。

【図４】図４は、セキュアメモリに記憶された装置内情報を示す説明図である。

【図５】図５は、本実施例にかかる起動処理を示すフローチャートである。

【図６】図６は、情報処理装置のハードウェア構成を示す図である。

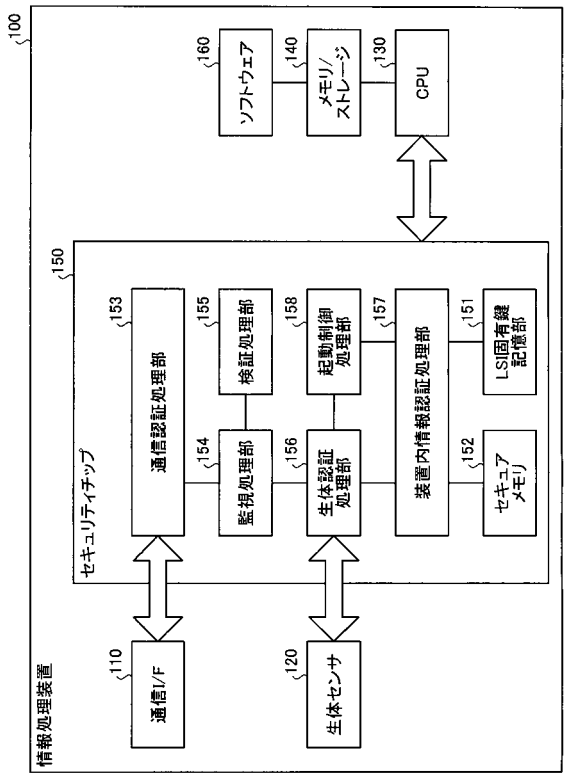
【符号の説明】

【００６４】

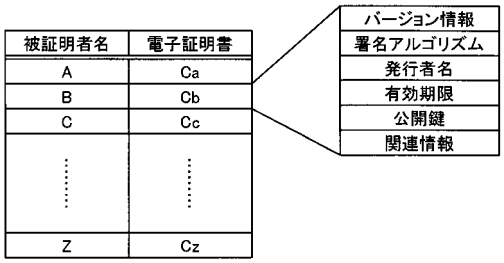
１０　バス
１１，１３０　ＣＰＵ
１２　ＲＯＭ
１３　ＲＡＭ
１４　ＨＤＤ
１５　ＨＤ
１６　ＦＤＤ
１７　ＦＤ
１８　ディスプレイ
１９，１１０　通信Ｉ／Ｆ
２０　入力キー
２１，１２０　生体センサ
２２，１５０　セキュリティチップ
３０　ネットワーク
１００　情報処理装置

１４０　メモリ／ストレージ
１５１　ＬＳＩ固有鍵記憶部
１５２　セキュアメモリ
１５３　通信認証処理部
１５４　監視処理部
１５５　検証処理部
１５６　生体認証処理部
１５７　装置内情報認証処理部
１５８　起動制御処理部
１６０　ソフトウェア

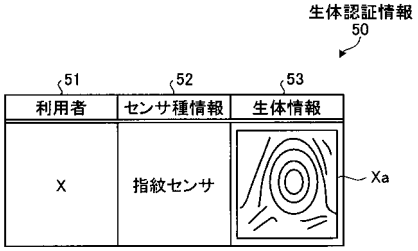
【図１】



【図２】



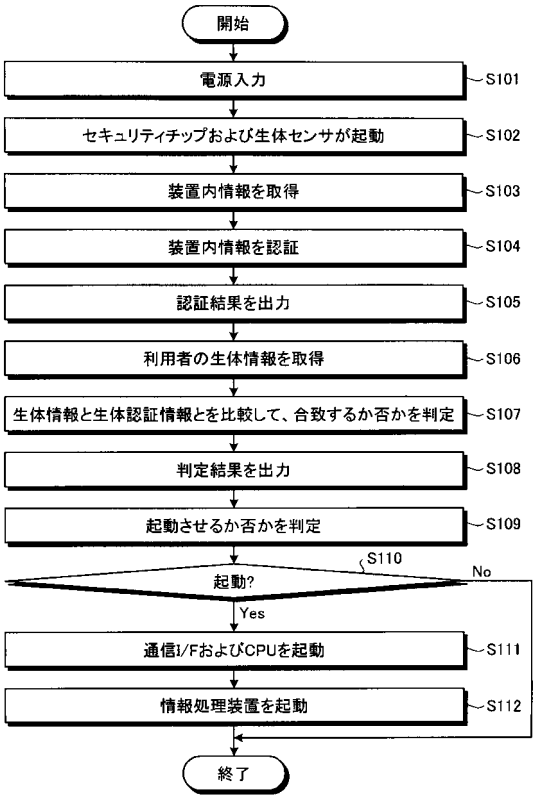
【図３】



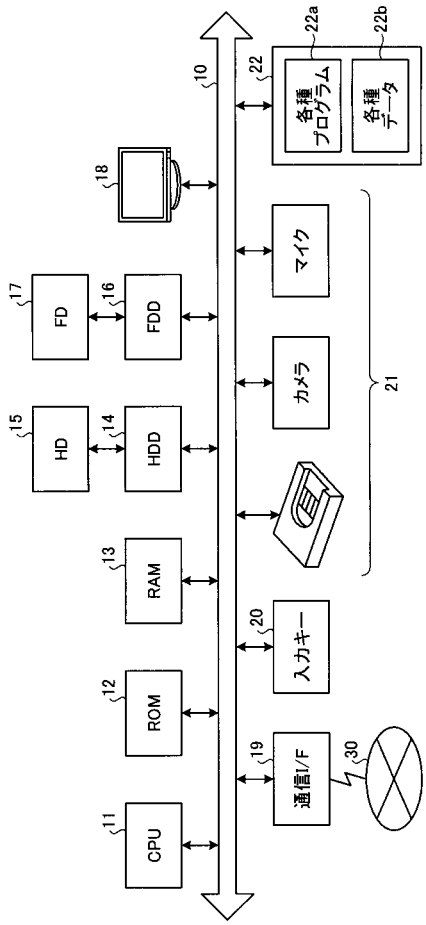
【図４】

周辺機器		ソフトウェア		実行プログラム	
周辺機器名	バージョン	ソフトウェア名	バージョン	プログラム名	バージョン
D1	1.1	Sa	5.0	生体認証	2.5
D2	3.2	Sb	4.1	通信認証	1.0
D3	1.0	Sc	1.0	装置内情報認証	6.1
.....	.....	.....	.....	.....	.....

【図５】



【図６】



フロントページの続き

(56)参考文献 特開平０４－３４８４０８（ＪＰ，Ａ）
特開２０００－２４２７７１（ＪＰ，Ａ）
特開２００２－３１２３２３（ＪＰ，Ａ）
米国特許出願公開第２００４／００７８４９７（ＵＳ，Ａ１）
特開２０００－２０７０４８（ＪＰ，Ａ）
国際公開第０２／０１３２８（WO，Ａ２）
特開２００１－１２５６６０（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
G06F 21/