(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2010-508578
(P2010-508578A)
(43)公表日　平成22年3月18日(2010.3.18)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/20	(2006.01)	G06F	15/00	330B	5B017
G06F 21/24	(2006.01)	G06F	12/14	530D	5B285
		G06F	15/00	330F	
		G06F	15/00	330G	

審査請求 未請求　予備審査請求 未請求　（全 20 頁）

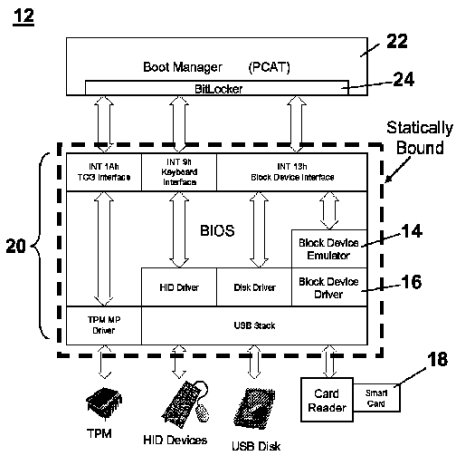
(21)出願番号　特願2009-534741 (P2009-534741)
(86)(22)出願日　平成19年9月27日 (2007.9.27)
(85)翻訳文提出日　平成20年12月16日 (2008.12.16)
(86)国際出願番号　PCT/US2007/079737
(87)国際公開番号　WO2008/051679
(87)国際公開日　平成20年5月2日 (2008.5.2)
(31)優先権主張番号　11/586,283
(32)優先日　平成18年10月25日 (2006.10.25)
(33)優先権主張国　米国 (US)

(71)出願人　500046438
マイクロソフト　コーポレーション
アメリカ合衆国　ワシントン州　９８０５２－６３９９　レッドモンド　ワン　マイクロソフト　ウェイ
(74)代理人　100140109
弁理士　小野　新次郎
(74)代理人　100089705
弁理士　社本　一夫
(74)代理人　100075270
弁理士　小林　泰
(74)代理人　100080137
弁理士　千葉　昭男
(74)代理人　100096013
弁理士　富田　博行

最終頁に続く

(54)【発明の名称】透明な二次因子を介したプラットフォーム認証

(57)【要約】
システムのファームウェアは、スマート・カードのような二次デバイスが認証に使用されることを可能にするように構成される。一例の実施例では、二次デバイスはＩＳＯ７８１６仕様に準拠するＣＣＩＤスマート・カードである。スマート・カードは、システムをブートする前に、システムに結合されたカード・リーダに挿入される。ファームウェアは、スマート・カードからの認証情報がブート処理の実行を許可するために利用されることを可能にするように構成されたエミュレータ及びドライバを含む。一例の実施例では、スマート・カードは、ＢＩＴＬＯＣＫＥＲ（商標）とともに使用する外部鍵を含む。二次デバイスはＢＩＯＳをインプリメントするシステム及びＥＦＩをインプリメントするシステムと互換である。認証はまた、バイオメトリック・デバイス等のデータ保存を提供しないデバイスによって遂行することができる。



【特許請求の範囲】
【請求項１】
ＢＩＯＳ部及びＥＦＩ部のうち少なくとも１つを含む、プラットフォーム認証システムであって、前記ＢＩＯＳ部及びＥＦＩ部のうち少なくとも１つが、
前記システムに結合されたブロック・デバイスを検出し、前記ブロック・デバイス上のファイルを開くように構成された、ブロック・デバイス・エミュレータと、
前記ブロック・デバイス上の情報にアクセスするように構成されたブロック・デバイス・ドライバとを含む、プラットフォーム認証システム。
【請求項２】
前記ブロック・デバイスはスマート・カードを含む請求項１記載のシステム。
【請求項３】
前記ブロック・デバイスはＣＣＩＤスマート・カードを含む請求項２記載のシステム。

【請求項４】
前記ブロック・デバイスはＵＳＢ互換のブロック・デバイスを含む請求項１記載のシステム。
【請求項５】
前記ブロック・デバイスはＰＣＭＣＩＡ互換のブロック・デバイスを含む請求項１記載のシステム。
【請求項６】
前記ブロック・デバイス上の前記情報へのアクセスが保護される請求項１記載のシステム。
【請求項７】
前記ブロック・デバイスはバイオメトリック・デバイスを含む請求項１記載のシステム。
【請求項８】
前記バイオメトリック・デバイス上でアクセスされる情報は、前記システムのブート処理の実行を可能にするトークンを含む請求項７記載のシステム。
【請求項９】
前記ブロック・デバイスは指紋読み取り装置を含む請求項７記載のシステム。
【請求項１０】
前記ブロック・デバイス上でアクセスされる情報は、前記システムのブート処理の実行を可能にする鍵情報を含む請求項１記載のシステム。
【請求項１１】
ブロック・デバイスを介してプラットフォームを認証する方法であって、
前記プラットフォームのＢＩＯＳ部及び前記プラットフォームのＥＦＩ部のうち少なくとも１つを介してブロック・デバイスを検出するステップと、
前記検出されたブロック・デバイスを認証するステップと、
前記システムのブート処理の実行を可能にするために前記ブロック・デバイスから情報を検索するステップとを含む方法。
【請求項１２】
前記ブロック・デバイスはスマート・カード及びＣＣＩＤスマート・カードの少なくとも１つを含む請求項１１記載の方法。
【請求項１３】
前記ブロック・デバイスはＵＳＢ互換のブロック・デバイス及びＰＣＭＣＩＡ互換のブロック・デバイスの少なくとも１つを含む請求項１１記載の方法。
【請求項１４】
前記ブロック・デバイスから前記情報を検索するための認証の指示を提供するステップをさらに含む請求項１１記載の方法。
【請求項１５】

前記ブロック・デバイスはバイオメトリック・デバイス及び指紋読み取り装置の少なくとも１つを含む請求項１１記載の方法。
【請求項１６】
コンピュータ可読媒体であって、
プラットフォーム・システムのＢＩＯＳ部及びプラットフォームのＥＦＩ部のうち少なくとも１つのブロック・デバイス・エミュレータを介してブロック・デバイスを検出するステップと、
前記ブロック・デバイス・エミュレータを介して前記ブロック・デバイス上のファイルを開くステップと、
前記ＢＩＯＳ部及び前記ＥＦＩ部のうち少なくとも１つのブロック・ドライバを介して、前記ブロック・デバイス上の情報にアクセスするステップと
を実行することにより、ブロック・デバイスを介してプラットフォームを認証するための格納されたコンピュータ実行可能命令を有するコンピュータ可読媒体。
【請求項１７】
前記ブロック・デバイスはスマート・カード及びＣＣＩＤスマート・カードのうち少なくとも１つを含む請求項１６記載のコンピュータ可読媒体。
【請求項１８】
前記ブロック・デバイスはＵＳＢ互換のブロック・デバイス及びＰＣＭＣＩＡ互換のブロック・デバイスの少なくとも１つを含む請求項１６記載のコンピュータ可読媒体。
【請求項１９】
前記ブロック・デバイスはバイオメトリック・デバイス及び指紋読み取り装置の少なくとも１つを含む請求項１６記載のコンピュータ可読媒体。
【請求項２０】
前記ブロック・デバイス上でアクセスされる情報は、前記システムのブート処理の実行を可能にするための鍵情報を含む請求項１６記載のコンピュータ可読媒体。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、一般にコンピュータ処理に関し、より具体的には、保護されたファイルへのアクセスに関する。
【背景技術】
【０００２】
現在の処理システムはデータ保護を提供する。例えば、ＢＩＴＬＯＣＫＥＲ（商標）ドライブ暗号化（ＢＩＴＬＯＣＫＥＲ（商標）とも呼ばれる）というマイクロソフト（登録商標）・コーポレーションの製品は、様々なＷＩＮＤＯＷＳ（登録商標）オペレーティング・システムとともに利用可能なデータ保護機能である。ＢＩＴＬＯＣＫＥＲ（商標）は、別のオペレーティング・システムをブートしたりソフトウェア・ハッカー用ツールを実行したりするユーザが、ファイルもしくはシステムの保護を破ったり保護されたドライブ上に格納されたファイルのオフラインでの閲覧を実行したりすることを防止する。ＢＩＴＬＯＣＫＥＲ（商標）は、ユーザデータを保護し、ＷＩＮＤＯＷＳ（登録商標）オペレーティング・システム（例えば、ＷＩＮＤＯＷＳ（登録商標）ＶＩＳＴＡ）を実行するプロセッサが、システムがオフラインである間に手を加えられなかったことを保証する。
【発明の開示】
【発明が解決しようとする課題】
【０００３】
ＢＩＴＬＯＣＫＥＲ（商標）は、ユーザがＰＩＮを供給するまで、あるいは鍵材料（キーマテリアル、keying material）を含んでいるＵＳＢフラッシュドライブを挿入するまで、正常なブート処理をロックすることができる。例えば、ＵＳＢフラッシュデバイスは、ブート処理に先立って処理システムに挿入することができる。ブート処理中に、ＵＳＢフラッシュデバイスが認識され、鍵材料はそこからアクセスすることができる。しかし、

現在の処理システムは、ブート処理中に、この目的のためにスマート・カード及びＣＣＩＤ（集積回路カード・インターフェース・デバイス）スマート・カードのようなデバイスを認識しない。

【課題を解決するための手段】

【０００４】

この概要は説明に役立つ実施例についての詳細な説明においてさらに以下に述べられている単純化された形式における概念の選択を導入するために提供される。 この概要は、特許請求の範囲に記載の主題の重要な特徴あるいは本質的な特徴を特定するようには意図されず、特許請求の範囲に記載の主題の範囲を制限するために使用されるようにも意図されない。

【０００５】

プラットフォームは、プラットフォームのファームウェアによりサポートされる任意の認証機構によってゲート制御された、保護されたファイルへの透明なアクセスを提供する。プラットフォームは、ＰＩＮを受け取り、ＵＳＢフラッシュドライブやスマート・カード等の各種デバイスからのキーを消費することができ、バイオメトリック・デバイス等のデータ保存を提供しない他のデバイスと互換性がある。一例としての実施例では、プラットフォーム・ファームウェアは、ＢＩＴＬＯＣＫＥＲ（商標）がデバイス（例えばＣＣＩＤスマート・カード）上の特別に設定されたファイルにアクセスし及び／又は当該デバイスの保護されたＢＩＯＳ（基本入出力システム）部分にアクセスすることを可能にする。

【０００６】

添付の図面と共に読むことで、以下の詳細な説明と同様に上述の概要もさらによく理解される。透明な二次因子（transparent second factor）を介したプラットフォーム認証を説明する目的で、図面中にその例示的な構成が示される。しかしながら、透明な二次因子を介したプラットフォーム認証は、開示された特定の方法と手段に制限されない。

【発明を実施するための最良の形態】

【０００７】

プラットフォームの認証をサポートするための透明な二次因子、又はデバイスは、例示的な実施例では、例えば、スマート・カード、ＣＣＩＤスマート・カード（集積回路カード・インターフェース・デバイス・スマート・カード）、バイオメトリック・デバイス（例えば指紋読み取り装置、網膜スキャナなど）あるいはその組み合わせを含む。プラットフォームの認証をサポートする透明な二次因子は、本明細書において、ＢＩＴＬＯＣＫＥＲ（商標）ドライブ暗号化（ＢＩＴＬＯＣＫＥＲ（商標）とも呼ばれる）というマイクロソフト（登録商標）・コーポレーションの製品に適用されるものとして記述されるが、それに制限されるものではない。二次因子は、ユーザーが様々な因子間の差異の詳細について把握している必要がないという点で、プラットフォームのユーザの観点から透明である。

【０００８】

ＢＩＴＬＯＣＫＥＲ（商標）は、ブロック・デバイス上に格納される外部鍵（external key）を消費することができる。ブロック・デバイスは、例えばハードディスクドライブ等の、ブロックの形式の情報を送信し及び／又は受信するデバイスである。ブロック・デバイスへのアクセスはプラットフォームのファームウェアによって提供される。プラットフォームは任意の適切なプロセッサ等を含むことができる。例えば、適切なプラットフォームは、パーソナルコンピュータ、サーバコンピュータ、携帯型のデバイスあるいはラップトップデバイス、マルチプロセッサ・システム、マイクロプロセッサベースのシステム、セットトップ・ボックス、プログラム可能な家電、ネットワークＰＣ、ミニコンピュータ、メインフレーム・コンピュータ、携帯機器、例えばＭＰ３プレイヤー、ウォークマン（商標）などの携帯音楽プレーヤーのようなポータブル・メディア・プレイヤー、携帯情報端末（「ＰＤＡ」）、携帯電話、ポータブルの電子メールデバイス、シン・クライアント及びポータブルの賭け事装置等のポータブル計算デバイス、テレビ、ＤＶＤプレーヤー、セットトップ・ボックス、モニタ、ディスプレイなどのような消費者電子デバイス、キ

オスク、店内の音楽サンプリングデバイス、自動預金受払機（ＡＴＭ）、キャッシュレジスターなどの共同で使用する計算デバイス、携帯型又は車両内にインストールされたナビゲーションデバイス、及び／又は、キッチン用品、自動車制御｛（例えばステアリングホイール）等の従来型でない計算デバイス、あるいはその組み合わせを含んでもよいが、それに制限されない。一例としての実施例では、プラットフォームのファームウェアは、認証目的で、スマート・カード、ＣＣＩＤスマート・カード及び／又はバイオメトリック・デバイス等の二次因子をＢＩＴＬＯＣＫＥＲ（商標）が利用することを可能にするための能力を提供するように構成される。従って、ＢＩＴＬＯＣＫＥＲ（商標）は、例えばハードディスク等の記憶デバイスからファイルを読み出すことと同様に、ブロック・デバイス上の特別に設定されたファイルあるいはブロック・デバイスの保護されたＢＩＯＳエリア内のファイルを読み取る。

【０００９】

このようにして適用可能な一例のスマート・カードは、ＩＳＯ７８１６仕様に従うスマート・カードである。この仕様は、スマート・カードの特性及び機能性について記述する。一例の実施例では、スマート・カードにアクセスするために利用されるコマンドは、単純なファイルシステム及びファイルシステム自体にアクセスするための基本のコマンドを定義する、ＩＳＯ７８１６仕様、例えばセクションＩＳＯ７８１６－４に従う。

【００１０】

一例の実施例において、ＢＩＴＬＯＣＫＥＲ（商標）鍵（例えば、ＢＩＴＬＯＣＫＥＲ（商標）によって利用される外部鍵）は、ブロック・デバイスのファイルシステムに格納される。ブロック・デバイスが認証されると、当該鍵はブロック・デバイスから取り出され、続いて、プラットフォームのブート処理の間にＢＩＴＬＯＣＫＥＲ（商標）によって利用される。一例の実施例では、ブロック・デバイスへのアクセスは読み出し専用のアクセスである。別の一例の実施例では、ブロック・デバイス上のファイルは保護される。例えば、ＰＩＮ等が提供されるまで、ブロック・デバイス上のファイルへのアクセスは与えられなくてもよい。あるいは、別の例として、ブロック・デバイス上の所定のファイルのみがプラットフォームによってアクセス可能なように選択される。したがって、ブロック・デバイスが失われるか盗まれると、ブロック・デバイス上の情報は保護され、無許可のエンティティ（entity）によってアクセスすることができない。

【００１１】

図１は、例示的なシステム１２のＢＩＯＳ（基本入出力システム）部２０を介してブロック・デバイス１８にアクセスするためのシステム１２の機能ブロック図である。図１に示されるように、システム１２は、ＰＣＡＴ（PC advanced technology）互換のブート・マネージャ２２、ＢＩＴＬＯＣＫＥＲ（商標）ソフトウェア２４及びＢＩＯＳ部２０を含む。ＢＩＯＳ部２０はブロック・デバイス・エミュレータ部１４及びブロック・デバイス・ドライバ部１６を含む。ブロック・デバイス・エミュレータ１４は、ブロック・デバイス１８を検出し、ブロック・デバイス１８上のファイルを開くように構成される。ＢＩＯＳ部２０は、ブロック・デバイス１８上に格納された情報にアクセスするよう構成されたブロック・デバイス・ドライバ１６を含む。

【００１２】

ＢＩＯＳ部２０は、システム１２を含むプラットフォームのブート処理を制御するためのファームウェアを含む。一例の実施例では、ＢＩＯＳ部２０は、例えば信頼されたプラットフォーム・モジュール（trusted platform module、ＴＰＭ）等の信頼されたコンピューティング・グループ（ＴＣＧ）・デバイスへのインターフェースを扱うための割り込みハンドラ（例えば、割り込みＩＡ１６進法（interrupt 1A hexadecimal）、ＩＮＴ １Ａｈ））、例えばキーボード等のヒューマン・インターフェース・デバイス（ＨＩＤ）へのインターフェースを扱う割り込みハンドラ（例えば、ＩＮＴ ９ｈ）、及び例えばユニバーサル・シリアル・バス（ＵＳＢ）互換デバイス（例えば、ＵＳＢディスク、ＵＳＢカード読取り装置）等のブロック・デバイス・インターフェースへのインターフェースを扱うための割り込みハンドラ（例えば、ＩＮＴ １３ｈ）を含む。特定の割り込みハンドラ

についての図１中の描写は例示的なものであり、任意のインターフェースを使用することができることが強調される。

【００１３】

ＢＩＯＳ部２０は、ＨＩＤ及び記憶ブロック・デバイスのような、ＵＳＢコントローラ及び基本デバイスをサポートする。一例の実施例では、ＢＩＯＳ部２０は、例えばスマート・カード１８又はバイオメトリック・デバイス（図１に示されない）等のデバイスと互換性を有するように、ブロック・デバイス・エミュレータ１４及びブロック・デバイス・ドライバ１６を含むように構成される。一例の実施例では、ブロック・デバイス・ドライバ１６は、少なくとも部分的に、例えば集積回路カード・インターフェース・デバイス改訂１．１の仕様等の集積回路カード・インターフェース・デバイス用の仕様に従って構成され、機能する。集積回路カード・インターフェース・デバイス用の仕様に記述されているような完全なデバイスクラスをインプリメントすることは必要ではなく、当該デバイスクラスのサブセットが適切である。カード・リーダとの基本的な相互作用、及び、例えば、スマート・カード１８へ電力を提供したり、スマート・カード１８から電力を取り除いたり、スマート・カード１８に対して及びスマート・カード１８からコマンド及び応答ＡＰＤＵ（Application Protocol Data Unit、アプリケーション・プロトコル・データ・ユニット）を中継したりする等のスマート・カード１８との通信を可能にするために利用される要素が適切である。

【００１４】

一例の実施例では、カード・リーダは、ＰＣＭＣＩＡ（ＰＣメモリーカード国際協会、又は周辺コンポーネントマイクロチャネル相互接続アーキテクチャ）インターフェースを介してスマート・カード１８に適合する。この実施例は、モバイル・コンピュータなどのための有利な使用を提供する。スマート・カード１８は、カード、キーホブ（key fob）あるいは任意の適切な構成の形式をとることができる。

【００１５】

一例の実施例において、図２に示されるように、ブロック・デバイス１８は、指紋読み取り装置、網膜スキャナなどのようなバイオメトリック・デバイスを含む。バイオメトリック・デバイスは、通常、データ保存を提供しない。ブロック・デバイス１８がデータ保存を提供しないバイオメトリック・デバイスあるいは他の二次因子を含む実施例において、ＢＩＯＳ部２０のファームウェアは、ブロック・デバイス１８の認証を実行する。ブロック・デバイス１８の認証が成功する場合、トークンはブロック・デバイス１８によって提供することができ、それは、例えばＢＩＴＬＯＣＫＥＲ（商標）を開始することによって、ブート処理を続けるのに必要な鍵を含むプラットフォームの保護区域にアクセスするために使用することができる。この実施例では、プラットフォームの保護区域に格納される情報は、ブロック・デバイス１８について先立って成功した認証なしでは読み取ることができない。

【００１６】

図１及び図２に示されるように、プラットフォームのＢＩＯＳ部２０は静的に結合される。すなわち、プラットフォームのブート処理あるいはオペレーティング・システムが開始される前に、識別子に値を関連付ける処理が遂行される。したがって、ブロック・デバイス・エミュレータ１４及びブロック・デバイス・ドライバ１６は、すべてのタイプのブロック・デバイス１８用に固定される。

【００１７】

図３は、例示的なシステム２８の拡張可能なファームウェア・インターフェース（ＥＦＩ）２６を介してブロック・デバイス１８にアクセスするためのシステム２８の機能ブロック図である。システム２８は、システム１２のＢＩＯＳ実装であるかシステム２８のＥＦＩ実装であるかという差異はあるが、上述のシステム１２と同様に機能する。ＥＦＩはＢＩＯＳに代わって利用されるものとして知られている。ＢＩＯＳと同様、ＥＦＩは、オペレーティング・システムのブート処理をコントロールし、オペレーティング・システムとハードウェアとの間のインターフェースを提供する責務を負う。ＥＦＩ２６は動的に結

合される。すなわち、結合はブート処理の間に遂行される。したがって、ブロック・デバイス・エミュレータ１４及びブロック・デバイス・ドライバ１６は、別個に実施することができ、１つの静的なユニットに結合される必要はない。ブロック・デバイス・ドライバ１６はＥＦＩブート時間においてロードすることができる。

【００１８】

図３に示されるように、システム２８は、ＥＦＩ互換のブート・マネージャ３０、ＢＩＴＬＯＣＫＥＲ（商標）ソフトウェア２４及びＥＦＩ部２６を含む。ＥＦＩ部２６はブロック・デバイス・エミュレータ部１４及びブロック・デバイス・ドライバ部１６を含む。ブロック・デバイス・エミュレータ１４は、ブロック・デバイス１８を検出し、ブロック・デバイス１８上のファイルを開くように構成される。ＥＦＩ部２６は、ブロック・デバイス１８上に格納された情報にアクセスするように構成されたブロック・デバイス・ドライバ１６を含む。

【００１９】

ＥＦＩ部２６は、システム１２を含むプラットフォームのブート処理を制御するためのファームウェアを含む。一例の実施例では、ＥＦＩ部２６は、例えば信頼されたプラットフォーム・モジュール（ＴＰＭ）等の信頼されたコンピューティング・グループ（ＴＣＧ）・デバイスへのインターフェースを扱うための割り込みハンドラ、例えばキーボード等のヒューマン・インターフェース・デバイス（ＨＩＤ）へのインターフェースを扱う割り込みハンドラ、及び例えばユニバーサル・シリアル・バス（ＵＳＢ）互換デバイス（例えば、ＵＳＢディスク、ＵＳＢカード読取り装置）等のブロック・デバイス・インターフェースへのインターフェースを扱うための割り込みハンドラを含む。特定の割り込みハンドラについての図１中の描写は例示的なものであり、任意のインターフェースを使用することができることが強調される。

【００２０】

ＥＦＩ部２６は、ＨＩＤ及び記憶ブロック・デバイスのような、ＵＳＢコントローラ及び基本デバイスをサポートする。一例の実施例では、ＥＦＩ部２６は、例えばスマート・カード１８又はバイオメトリック・デバイス（図３に示されない）等のデバイスと互換性を有するように、ブロック・デバイス・エミュレータ１４及びブロック・デバイス・ドライバ１６を含むように構成される。一例の実施例では、ブロック・デバイス・ドライバ１６は、少なくとも部分的に、例えば集積回路カード・インターフェース・デバイス改訂１．１の仕様等の集積回路カード・インターフェース・デバイス用の仕様に従って構成され、機能する。集積回路カード・インターフェース・デバイス用の仕様に記述されているような完全なデバイスクラスをインプリメントすることは必要ではなく、当該デバイスクラスのサブセットが適切である。例えば、カード・リーダとの基本的な相互作用、及び、スマート・カード１８へ電力を提供したり、スマート・カード１８から電力を取り除いたり、スマート・カード１８に対して及びスマート・カード１８からコマンド及び応答ＡＰＤＵ（Application Protocol Data Unit、アプリケーション・プロトコル・データ・ユニット）を中継したりする等のスマート・カード１８との通信を可能にするために利用される要素が適切である。

【００２１】

一例の実施例では、カード・リーダは、ＰＣＭＣＩＡ（ＰＣメモリーカード国際協会、又は周辺コンポーネントマイクロチャネル相互接続アーキテクチャ）インターフェースを介してスマート・カード１８に適合する。この実施例は、モバイル・コンピュータなどのための有利な使用を提供する。スマート・カード１８は、カード、キーホブ（key fob）あるいは任意の適切な構成の形式をとることができる。

【００２２】

一例の実施例において、図４に示されるように、ブロック・デバイス１８は、指紋読み取り装置、網膜スキャナなどのようなバイオメトリック・デバイスを含む。バイオメトリック・デバイスは、通常、データ保存を提供しない。ブロック・デバイス１８がデータ保存を提供しないバイオメトリック・デバイスあるいは他の二次因子を含む実施例において

、ＥＦＩ部２６のファームウェアは、ブロック・デバイス１８の認証を実行する。ブロック・デバイス１８の認証が成功する場合、トークンはブロック・デバイス１８によって提供することができ、それは、例えばＢＩＴＬＯＣＫＥＲ（商標）を開始することによって、ブート処理を続けるのに必要な鍵を含むプラットフォームの保護区域にアクセスするために使用することができる。この実施例では、プラットフォームの保護区域に格納される情報は、ブロック・デバイス１８について先立って成功した認証なしでは読み取ることができない。

【００２３】

別の一例の実施例では、ＥＦＩはハードディスクなどからＢＩＯＳ上でブートされる。

【００２４】

オペレーティング・システムがプラットフォームにロードされるのに先立って、ブロック・デバイスが認証される。一例の実施例では、ＢＩＯＳが実装される場合、ＢＩＯＳ上の割り込み１９ｈが呼び出される前に、ブロック・デバイスが認証される。すなわち、ブート処理中に、ＢＩＯＳがオペレーティング・システムをロードし始める前に、ブロック・デバイスが認証される。一例の実施例において、ＥＦＩが実装される場合、ブート・マネージャがＥＦＩ上で呼び出される前に、ブロック・デバイスが認証される。ブロック・デバイスは、例えばＰＩＮ等の使用によってなど、任意の適切な手段によって認証することができる。ブロックが首尾よく認証された後、仮想ブロック・デバイスがプラットフォームのメモリに生成される。

【００２５】

プラットフォーム・メモリにおいて仮想ブロック・デバイスを生成するために、ブロック・デバイスの記憶装置は、ブート処理が実行を開始／継続することを可能にする情報を含んでいる位置を求めて探索される。ブロック・デバイス上の記憶装置の構造はいかなる適切な構造も含むことができ、ブート処理の実行を可能にする情報を含むブロック・デバイス上の記憶の位置は、任意の適切な方法で識別することができる。

【００２６】

図５は、ＩＳＯ　７８１６仕様に準拠するブロック・デバイスの一例のファイルシステム４０の図である。このファイルシステム４０が例示的なものであり、如何なる適切なファイルシステムもブロック・デバイス上に実装できることが強調される。一例の実施例では、ブロック・デバイスのファイルシステム４０は、少なくとも１つのマスタファイル３２（図５のＭＦとして描かれている）、少なくとも１つの専用ファイル３４（図５のＤＦとして描かれている）及び少なくとも１つの基本ファイル３６（図５のＥＦとして描かれている）を含む。簡単にするために、各タイプのファイルのうちの１つだけ（３２、３２及び３６）にラベルが付けられている。ファイルシステム４０の階層は、専用ファイル及び基本ファイルがマスタファイル３２の下位となるような状態である。マスタファイル３２はルート・ファイルである。専用ファイルはファイル制御情報を含んでいる。専用ファイルは、オプションとして、割り当てに利用可能なメモリの指示を含むことができる。専用ファイルは基本ファイルの親となることができ、及び／又は、専用ファイルは基本ファイルであってもよい。

【００２７】

一例の実施例では、基本ファイルは、基本ファイルがブート処理の実行を可能にするための情報を含んでいるという指示を含む。例えば、基本ファイルは、それがＢＩＴＬＯＣＫＥＲ（商標）によって利用されるための鍵を含んでいるという指示を含むことができる。一例の実施例において、図５に描かれるように、基本ファイルは、それがブート処理の実行を可能にするための情報を含むことを示すために、ＶＦＡＴ（仮想ファイル属性テーブル）として指定される。ＶＦＡＴのＩＤを有する基本ファイルに含まれる情報のタイプの一例がブロック３８に描かれる。他の情報の中で、ＢＩＴＬＯＣＫＥＲ（商標）によって利用可能な鍵は次のように示される：ＬＦＮ（論理ファイル名）：　Ｅ５Ｅ１Ａ４２０－０１３４－４６７７－８８Ｂ１－８５５Ｅ９ＤＣ２００Ｆ７．ＢＥＫ、及びＬＦＮ：ＡＥ３２４Ｂ１４－５２６４－Ｅ３２Ａ－９Ａ２３－２２５ＡＢ６８２３Ａ３２．ＢＥＫ。

【００２８】
図６は、プラットフォーム・メモリ中の仮想ブロック・デバイスを生成する一例の処理のフロー図である。ステップ４０において、プラットフォーム中のメモリが割り当てられ、すべての必要なシステム構造が初期化される。一例の実施例において、ブロック・デバイスは、ブート処理の実行の前にプラットフォームに結合される。ブロック・デバイス上のファイルシステムは、一例の実施例において、プラットフォームがブロック・デバイスからブートするのを防止するためにゼロに等しいブートセクタを有する、読み出し専用のＦＡＴとして実装される。プラットフォームにオペレーティング・システムをロードする前に、ブロック・デバイスのマスタファイルはステップ４２でプラットフォーム・メモリにロードされる。ＢＩＯＳ又はＥＦＩ等のファームウェアは、ステップ４４において、ＩＤ　ＶＦＡＴ（ＩＤ番号を表す）を有する基本ファイルを求めて、ブロック・デバイス上のマスタファイル及び下位の専用ファイルを再帰的に探索する。ステップ４６において、ＩＤ　ＶＦＡＴを有する基本ファイルが見つからない場合、未使用のリソースはステップ５８において解放され、処理が終了する。ステップ４６において、ＩＤ　ＶＦＡＴを有する基本ファイルが見つかる場合、そのような基本ファイルはすべてステップ４８においてプラットフォーム・メモリにロードされる。ＩＤ　ＶＦＡＴを有する基本ファイルが見つかることは、ブロック・デバイスがブートアクセスのために設定されており、仮想ブロック・デバイスの生成が開始できるという指示である。

【００２９】
基本ファイルはステップ５０で開かれて解析される。ＩＳＯ　７８１６仕様に従う一例の実施例では、基本ファイルは５バイトの識別子に制限されている。したがって、プラットフォームは、５ビットより長い名前を持っている外部鍵をＢＩＴＬＯＣＫＥＲ（商標）が使用することを許可するための仮想ブロック・デバイスに含まれるべき、ブロック・デバイス上のすべてのファイルのカタログを維持する。例えばＢＩＴＬＯＣＫＥＲ（商標）鍵等の情報は、ステップ５２において、解析された基本ファイルから抽出される。ステップ５４で、例えばＢＩＴＬＯＣＫＥＲ（商標）鍵等の抽出された情報は、プラットフォーム・メモリ中の仮想ブロック・デバイスの個々の適切なファイルに加えられる。ＩＤ　ＶＦＡＴを有する、より多くの基本ファイルが存在する場合（ステップ５６）、上述のように、処理はステップ５０に移り継続する。ＩＤ　ＶＦＡＴを有する基本ファイルがそれ以上存在しない場合（ステップ５６）、未使用のリソースは解放され、処理はステップ５８で終了する。ＥＦにおいてＶＦＡＴであると識別されない、ブロック・デバイス上で見つかったファイルは、アクセスされないか又は読み取られず、したがって、露出されない。

【００３０】
仮想ブロック・デバイスは、プラットフォーム・メモリにおいて動的に生成される。仮想ブロック・デバイスは、ブート処理（例えばプラットフォームに電源が入れられる）の間に一度生成される。ブロック・デバイスがプラットフォームから分離されても、仮想ブロック・デバイスのファイルはプラットフォーム・メモリに残る。しかし、仮想ブロック・デバイスはプリブート時間中に存在し、プラットフォーム・オペレーティング・システムがロードされる時破壊される。

【００３１】
仮想ブロック・デバイスのフォルダ階層は、ブロック・デバイスのフォルダの階層に従う。ＩＤ　ＶＦＡＴを有する基本ファイルだけがロードされるので、ブロック・デバイス上の望まれないファイルは仮想ブロック・デバイス中で表現されない。したがって、データで実際に占められるブロック用のプラットフォーム・メモリのみが割り当てられる。仮想ブロック・デバイスのためのプラットフォーム・メモリの例示的な割り当ての描写は、図７に示される。図７に示されるように、プラットフォーム・メモリは、ブート記録セクタ６０、ファイル割り当てテーブル・セクタ６２、バックアップ・ファイル割り当てテーブル・セクタ６４、ルート・ディレクトリ６６及び少なくとも１つのデータ記憶領域セクタ６８に割り当てられる。データ記憶領域６８は、例えばＢＩＴＬＯＣＫＥＲ（商標）鍵のようなブート処理が実行することを可能にするための情報使用を含むことができる。一

例の実施例では、各セクタは５１２バイトを含む。プラットフォーム・メモリは、例えば隣接するようにするなどして、任意の適切な方法で割り当てることができる。一例の実施例では、ブート・アプリケーションから要求されると、ステップ６６が行なわれ、他のすべてのブロックはオンザフライで計算される。

【００３２】

上述のように、ブロック・デバイスはＣＣＩＤスマート・カードを含むことができる。図８は、ＣＣＩＤスマート・カードにアクセスする例示的な処理のフロー図である。図８に描かれた処理が任意の適切なブロック・デバイスに適用可能であることが強調される。ステップ７０では、ＣＣＩＤカード・リーダが検出されるか否かが決定される。上述のように、カード・リーダが検出されない場合（ステップ７０）、ステップ９０として、ＢＩＯＳが実装される場合には割り込み１９ｈが呼び出され、ＥＦＩが実装される場合にはブート・マネージャがロードされる。カード・リーダが検出される場合（ステップ７０）、ステップ７２で、カード・リーダに結合されたスマート・カードが検出されるか否かが決定される。スマート・カードが検出されない場合（ステップ７２）、処理はステップ９０に移る。スマート・カードが検出される場合（ステップ７２）、ステップ７４で、スマート・カードがＩＳＯ　７８１６－４、あるいは他の適切なプロトコルに準拠するか否かが決定される。スマート・カードが準拠しない場合（ステップ７４）、処理はステップ９０に移る。スマート・カードが準拠する場合（ステップ７４）、スマート・カードからの専用のブート・ファイルはステップ７６でプラットフォーム・メモリにロードされる。

【００３３】

ステップ７８において、ＤＦブート・ファイルが例えばＰＩＮによって保護されるか否かが決定される。ＤＦブート・ファイルが保護されない場合（ステップ７８）、プラットフォーム・メモリ中の仮想ブロック・デバイスの生成はステップ８８で初期化される。ＤＦブート・ファイルが保護される場合（ステップ７８）、ステップ８０において、ＰＩＮなどのためにプロンプトが表示される。ＰＩＮなどが入力されることを可能にするために利用されるユーザ・インターフェース（ＵＩ）は、イニシャル・プログラム・ロード（ＩＰＬ）、又はブートのコードが開始される前に遂行される。キーボード、ディスプレイ及び／又は他のＵＩデバイスの制御が一旦ＩＰＬコードに渡されれば、認証プロンプトは表示可能でなくてもよい。一例の実施例では、スマート・カードがプラットフォームへの電源供給の前にカード・リーダへ結合されること（例えば、挿入されること）が期待される。

【００３４】

ＰＩＮ等はステップ８２で受け取られる。ステップ８４では、ＰＩＮ等はスマート・カードのロックを解除するために利用される。ステップ８６では、スマート・カードがロックを解除されるか否かが決定される。スマート・カードがロックを解除される場合（ステップ８６）、処理はステップ８８に移る。スマート・カードがロックを解除されない場合（ステップ８６）、処理はステップ８０に移る。

【００３５】

仮想ブロック・デバイスが首尾よく生成された後、ＩＰＬコードは仮想ブロック・デバイスを列挙し、ＢＩＴＬＯＣＫＥＲ（商標）外部鍵などの捜索にそれを含める。一旦鍵がブート・マネージャによってロードされ、当該鍵が暗号化されたボリュームのロックを首尾よく解除したならば、制御はオペレーティング・システム・ローダに渡される。一例の実施例では、仮想ブロック・デバイスのプラットフォームメモリにおける記憶位置は、オペレーティング・システム・ローダーによって保護されず、維持されず、知られていない。したがって、オペレーティング・システム・ファイルはロードされ、仮想ブロック・デバイスの記憶スペースに結局上書きすることができる。

【００３６】

プラットフォームの認証をサポートする透明な二次因子の様々な実施例は、計算デバイス上で実行可能である。図９及び以下の説明は、そのような計算デバイスを実施することができる適切なコンピュータ環境の簡潔な概説を提供する。必要ではないが、プラットフ

ォームの認証をサポートする透明な二次因子の様々な態様は、クライアントワークステーション又はサーバのようなコンピュータによって実行されるプログラムモジュール等のコンピュータ実行可能命令の一般的な文脈で記述することができる。一般に、プログラムモジュールは、特定のタスクを実行したり、特定の抽象データ型を実装したりするルーチン、プログラム、オブジェクト、コンポーネント、データ構造などを含んでいる。さらに、透明な二次因子によるプラットフォームの認証は、ハンドヘルド・デバイス、マルチプロセッサ・システム、マイクロプロセッサ・ベースあるいはプログラム可能な家電、ネットワークＰＣ、ミニコンピュータ、メインフレーム・コンピュータ等を含む、他のコンピュータ・システム構成で実施することができる。さらに、透明な二次因子によるプラットフォームの認証は、タスクが通信ネットワークを介して結合された遠隔処理装置で実行される分散コンピューティング環境中で実行することができる。分散コンピューティング環境では、プログラムモジュールはローカル及び遠隔のメモリ記憶装置の両方に位置することができる。

【００３７】

コンピュータ・システムは、大きく３つのコンポーネント群に分割することができる：ハードウェア・コンポーネント、ハードウェア／ソフトウェアインターフェース・システム・コンポーネント及びアプリケーション・プログラム・コンポーネント（「ユーザ・コンポーネント」あるいは「ソフトウエア・コンポーネント」とも呼ばれる）。コンピュータ・システムの様々な実施例では、ハードウェア・コンポーネントは中央処理部（ＣＰＵ）６２１、メモリ（ＲＯＭ６６４及びＲＡＭ６２５の両方）、基本入出力システム（ＢＩＯＳ）６６６、及びキーボード６４０、マウス６４２、モニタ６４７及び／又はプリンタ（図示せず）のような各種入力／出力（Ｉ／Ｏ）デバイスを含んでもよい。ハードウェア・コンポーネントは、コンピュータ・システム用の基本的な物理的インフラストラクチャを含む。

【００３８】

アプリケーション・プログラム・コンポーネントは、コンパイラ、データベース・システム、ワード・プロセッサ、ビジネス・プログラム、ビデオゲームなどを含み、これらに限定されない様々なソフトウエアプログラムを含む。アプリケーション・プログラムは、様々なユーザ（機械、他のコンピュータ・システム及び／又はエンドユーザ）のために問題を解決し、ソリューションを提供し、データを処理するのにコンピュータリソースを利用する手段を提供する。一例の実施例において、アプリケーション・プログラムは、ブロック・デバイスを検出し、ブロック・デバイス上でファイルを開き、ブロック・デバイス上でファイルを検索し、プラットフォーム・メモリ内に仮想ブロック・デバイスを生成し、ブロック・デバイスのロックを解除してブート処理を開始するためにＰＩＮ等を利用するなど、上述のように、透明な二次因子を介したプラットフォームの認証に関連付けられた機能を実行する。

【００３９】

ハードウェア／ソフトウェア・インターフェース・システム・コンポーネントは、それ自体がほとんどの場合にシェル及びカーネルを含むオペレーティング・システムを含む（そして、いくつかの実施例において、オペレーティング・システムのみからなってもよい）。「オペレーティング・システム」（ＯＳ）は、アプリケーション・プログラムとコンピュータ・ハードウェアとの間の媒介として働く特別なプログラムである。ハードウェア／ソフトウェア・インターフェース・システム・コンポーネントは、コンピュータ・システム中のオペレーティング・システムの代わりに、あるいはそのオペレーティング・システムに加えて、仮想マシンマネージャ（ＶＭＭ）、共通言語ランタイム（ＣＬＲ）あるいはそれと機能的に等価なもの、Ｊａｖａ（登録商標）仮想マシン（ＪＶＭ）あるいはそれと機能的に等価なもの、あるいはそのようなソフトウエアコンポーネントを含んでもよい。ハードウェア／ソフトウェア・インターフェース・システムの目的は、ユーザがアプリケーション・プログラムを実行することができる環境を提供することである。

【００４０】

ハードウェア／ソフトウェア・インターフェース・システムは、一般に起動時にコンピュータ・システムにロードされ、コンピュータ・システム中のアプリケーション・プログラムをすべてその後に管理する。アプリケーション・プログラムは、アプリケーション・プログラム・インターフェース（ＡＰＩ）を介してサービスを要求することによって、ハードウェア／ソフトウェア・インターフェース・システムとやりとりする。いくつかのアプリケーション・プログラムによって、エンドユーザは、コマンド言語あるいはグラフィカル・ユーザ・インターフェース（ＧＵＩ）のようなユーザ・インターフェースによってハードウェア／ソフトウェア・インターフェース・システムとやりとりすることができる。

【００４１】

ハードウェア／ソフトウェア・インターフェース・システムは、従来、アプリケーションのための様々なサービスを行っている。複数のプログラムが同時に動作し得るマルチタスク・ハードウェア／ソフトウェア・インターフェース・システムでは、ハードウェア／ソフトウェア・インターフェース・システムは、どのアプリケーションがどの順序で動作すべきか、その後別のアプリケーションにスイッチする前に各アプリケーションのためにどれだけの時間を許可しなければならないかを決定する。ハードウェア／ソフトウェア・インターフェース・システムは、複数のアプリケーション中で内部メモリの共有を管理し、ハードディスク、プリンタ及び電話回線ポートのような付属のハードウェアデバイス間の入出力を扱う。ハードウェア／ソフトウェア・インターフェース・システムはまた、動作及び生じたかもしれないあらゆるエラーの状態に関して各アプリケーション（そして、ある場合にはエンドユーザ）にメッセージを送信する。開始するアプリケーションがこの作業から解放され、他の処理及び／又は動作を再開することができるように、ハードウェア／ソフトウェア・インターフェース・システムはまた、バッチジョブ（例えば印刷）の管理から解放されることができる。並列処理を提供することができるコンピュータにおいては、ハードウェア／ソフトウェア・インターフェース・システムはまた、一度に１つを超えるプロセッサ上で走るようにプログラムを分割することを管理する。

【００４２】

ハードウェア／ソフトウェア・インターフェース・システム・シェル（「シェル」と呼ばれる）は、ハードウェア／ソフトウェア・インターフェース・システムへの対話型のエンドユーザ・インターフェースである。（シェルも、「コマンド・インタープリタ」あるいはオペレーティング・システムで「オペレーティング・システム・シェル」と呼ばれてもよい）。シェルは、アプリケーション・プログラム及び／又はエンドユーザによって直接アクセス可能なハードウェア／ソフトウェア・インターフェース・システムの外層である。シェルとは対照的に、カーネルは、ハードウェア・コンポーネントと直接やりとりするハードウェア／ソフトウェア・インターフェース・システムの最も内側の層である。

【００４３】

図９に示されるように、例示的な汎用コンピュータ・システムは、処理装置６２１、システムメモリ６６２、及び処理装置６２１に対してシステムメモリを含む様々なシステムコンポーネントを結合するシステム・バス６２３を含む、従来のコンピュータ装置６６０を含んでいる。システム・バス６２３は、様々なバス方式のうちの任意のものを使用する、メモリバス又はメモリ・コントローラ、周辺バス及びローカルバスを含むいくつかのタイプのバス構造のいずれであってもよい。システムメモリは読み取り専用メモリ（ＲＯＭ）６６４及びランダム・アクセス・メモリ（ＲＡＭ）６２５を含んでいる。起動中などにコンピュータ装置６６０内の要素間で情報を転送するのを支援する基本ルーチンを含んでいる基本入出力システム（ＢＩＯＳ）６６６は、ＲＯＭ６６４に格納される。コンピュータ装置６６０はさらに、ハードディスク（図示されないハードディスク）から読み書きするためのハードディスクドライブ６２７、取外し可能な磁気ディスク６２９（例えばフロッピー（登録商標）ディスク、取り外し可能な記憶装置）から読み書きするための磁気ディスクドライブ６２８（例えばフロッピー（登録商標）ドライブ）、及びＣＤＲＯＭや他の光媒体のような取外し可能な光ディスク６３１から読み書きするための光ディスクドラ

イブ６３０を含んでいる。ハードディスクドライブ６２７、磁気ディスクドライブ６２８及び光ディスクドライブ６３０は、ハードディスクドライブ・インターフェース６３２、磁気ディスクドライブ・インターフェース６３３及び光ドライブインターフェース６３４によってシステム・バス６２３にそれぞれ接続される。ドライブ及びそれらに関連するコンピュータ読取り可能な媒体は、コンピュータ装置６６０にコンピュータ読取り可能な命令、データ構造、プログラムモジュール及び他のデータの不揮発性記憶装置を提供する。ここに説明される例示的な環境は、ハードディスク、取外し可能な磁気ディスク６２９及び取外し可能な光ディスク６３１を使用するが、当業者であれば、磁気カセット、フラッシュ・メモリカード、ディジタル・ビデオ・ティスク、ベルヌーイ・カートリッジ、ランダム・アクセス・メモリ（ＲＡＭ）、読み取り専用メモリ（ＲＯＭ）等のようなコンピュータによってアクセス可能なデータを格納することができる、他のタイプのコンピュータ読取り可能なメディアも当該例示的な動作環境において使用できることを理解すべきである。同様に、例示的な環境はまた、熱センサ、セキュリティ警報システムあるいは火災警報システム及び他の情報源などの多くのタイプの監視装置を含んでもよい。

【００４４】

オペレーティング・システム６３５、１つ又は複数のアプリケーション・プログラム６３６、他のプログラムモジュール６３７及びプログラムデータ６３８を含む多くのプログラムモジュールは、ハードディスク、磁気ディスク６２９、光ディスク６３１、ＲＯＭ６４又はＲＡＭ６２５上に格納することができる。 ユーザは、キーボード６４０及びポインティングデバイス６４２（例えばマウス）のような入力デバイスを介してコンピュータ装置６６０へコマンド及び情報を入力できる。他の入力デバイス（図示せず）は、マイクロホン、ジョイスティック、ゲーム・パッド、衛星ディスク、スキャナなどを含んでもよい。これら及び他の入力デバイスは、システム・バスに結合されたシリアルポート・インターフェース６４６を介して処理装置６２１にしばしば接続されるが、パラレルポート、ゲームポートあるいはユニバーサル・シリアル・バス（ＵＳＢ）のような他のインターフェースによって接続されてもよい。モニタ６４７あるいは他のタイプの表示装置もビデオアダプター６４８のようなインターフェース経由でシステム・バス６２３に接続される。モニタ６４７に加えて、コンピュータ装置は、通常、スピーカやプリンタのような他の周辺の出力装置（図示せず）を含んでいる。図９の例示的な環境はまた、ホストアダプタ６５５、小型コンピューター用周辺機器インターフェース（ＳＣＳＩ）バス６５６、及びＳＣＳＩバス６５６に接続された外部記憶装置６６２を含んでいる。

【００４５】

コンピュータ装置６６０は、リモートコンピュータ６４９のような１つ又は複数のリモートコンピュータへの論理接続を使用して、ネットワーク化された環境で動作してもよい。リモートコンピュータ６４９は、別のコンピュータ装置（例えばパーソナルコンピュータ）、サーバ、ルータ、ネットワークＰＣ、ピアデバイスあるいは他の共通ネットワークノードであってもよく、通常、コンピュータ装置６６０に関連のある上述の要素の多く又は全てを含んでいるが、図９においてはメモリ記憶装置６５０（フロッピー（登録商標）ドライブ）のみ説明された。図９に描かれた論理接続はローカル・エリア・ネットワーク（ＬＡＮ）６５１及び広域ネットワーク（ＷＡＮ）６５２を含んでいる。そのようなネットワーキング環境は、オフィス、企業規模のコンピュータネットワーク、イントラネット及びインターネットにおいて一般的である。

【００４６】

ＬＡＮネットワーキング環境で使用される場合、コンピュータ装置６６０は、ネットワークインターフェース又はアダプタ６５３によってＬＡＮ６５１に接続される。ＷＡＮネットワーキング環境で使用される場合、コンピュータ装置６６０は、インターネットのような広域ネットワーク６５２を介して通信を確立するためのモデム６５４あるいは他の手段を含んでもよい。モデム６５４は、内蔵型又は外付型であり得るが、シリアルポート・インターフェース６４６経由でシステム・バス６２３に接続される。ネットワーク化された環境では、コンピュータ装置６６０又はその一部に関連して描かれたプログラムモジュ

ールは、遠隔メモリ記憶装置に格納されてもよい。示されたネットワーク接続が例示的なものであって、コンピュータ間の通信リンクを確立する他の手段を使用してもよいことが理解されよう。

【００４７】

透明な二次因子を介するプラットフォームの認証についての多数の実施例がコンピュータ化されたシステムには特に良く適するものと思われるが、本明細書に記載のいずれの事項も、本発明をそのような実施例に制限するようには意図されない。 反対に、使用される「コンピュータ・システム」なる用語は、そのような装置がその特性において電子的か否か、機械的か否か、論理的か否か、仮想的か否かにかかわらず、情報を格納して処理することができ、及び／又はデバイス自体の振る舞い又は実行をコントロールするために格納した情報を使用することができる任意の及び全ての装置を包含するように意図される。

【００４８】

本明細書に記述された様々な技術は、ハードウェア又はソフトウェアで実施することができ、あるいは、適切な場合、両者の組み合わせで実施できる。したがって、透明な二次因子を介するプラットフォームの認証のための方法及び装置、あるいはその特定の態様又は一部は、フロッピー（登録商標）ディスク、ＣＤ－ＲＯＭ、ハードドライブあるいは任意の機械可読記憶媒体のような有形の媒体に組み込まれるプログラムコード（つまり命令）の形をとることができ、プログラムコードがコンピュータのようなマシンへロードされ、マシンによって実行される場合、当該マシンは透明な二次因子を介したプラットフォームの認証のための装置となる。

【００４９】

必要であれば、プログラムはアセンブリ又は機械語でインプリメントすることができる。どんな場合も、言語はコンパイルされ又は解釈された言語とすることができ、ハードウェア実装と組み合わせることができる。透明な二次因子を介したプラットフォームの認証のための方法及び装置はまた、電気配線あるいはケーブル、光ファイバ、あるいは他の形式の伝送を介するなどして、ある伝送媒体を介して送信されるプログラムコードの形で具体化された通信によって実行することができ、プログラムコードがＥＰＲＯＭ、ゲート・アレイ、プログラム可能ロジックデバイス（ＰＬＤ）、クライアントコンピュータなどのマシンへ受け取られてロードされ、マシンによって実行される場合、当該マシンは、特性によって仮想マシンを管理するための装置になる。汎用プロセッサ上にインプリメントされる場合、プログラム・コードは、プロセッサと組み合わさって、透明な二次因子を介してプラットフォームの機能認証を呼び出すように動作する独自のデバイスを提供する。さらに、透明な二次因子を介したプラットフォームの認証に関して使用されるいかなる記憶技術も、常にハードウェアとソフトウェアの組み合わせになりえる。

【００５０】

透明な二次因子を介したプラットフォームの認証は様々な図の例示的な実施例に関して記述されてきたが、他の同様の実施例を使用することができ、発明の範囲から逸脱することなく、透明な二次因子を介したプラットフォームの認証のための同じ機能を実行するために、説明された実施例に対して変更及び追加をなすことができることが理解されよう。したがって、本明細書に記述されるような透明な二次因子を介したプラットフォームの認証は、いかなる単一の実施例にも制限されたべきでなく、添付の特許請求の範囲に従う範囲において解釈されるべきである。

【図面の簡単な説明】

【００５１】

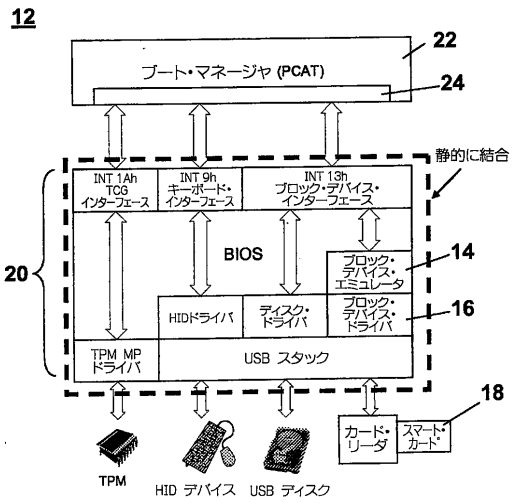
【図１】システムのＢＩＯＳ部を介してブロック・デバイスにアクセスするための一例のシステムの機能ブロック図である。

【図２】システムのＢＩＯＳ部を介してバイオメトリック・デバイスにアクセスするための一例のシステムの機能ブロック図である。

【図３】システムのＥＦＩを介してブロック・デバイスにアクセスするための一例のシステムの機能ブロック図である。

【図４】システムのＥＦＩを介してバイオメトリック・デバイスにアクセスするための一例のシステムの機能ブロック図である。
【図５】ＩＳＯ　７８１６仕様に準拠するブロック・デバイスの一例のファイルシステムの図である。
【図６】プラットフォーム・メモリ中の仮想ブロック・デバイスを生成する一例の処理のフロー図である。
【図７】仮想ブロック・デバイス用のプラットフォーム・メモリの一例の割り当ての図である。
【図８】ＣＣＩＤスマート・カードにアクセスする一例の処理のフロー図である。
【図９】透明な二次因子を介したプラットフォーム認証を実施することができる一例のコンピュータ環境の図である。

【図１】



【図２】

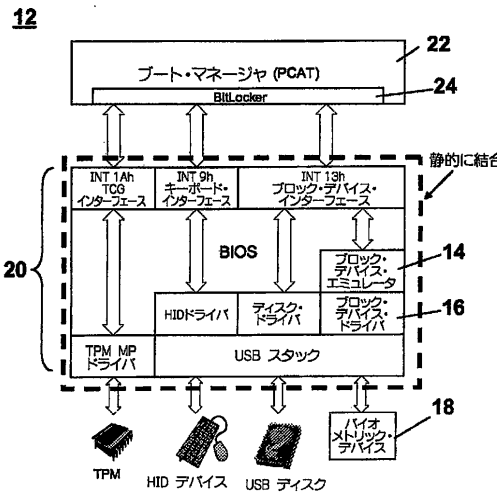
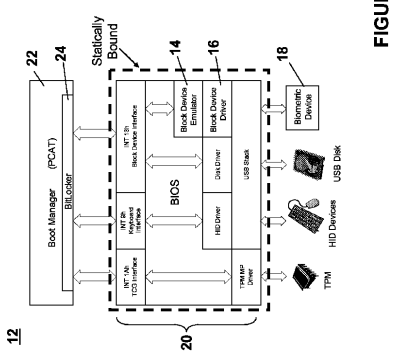
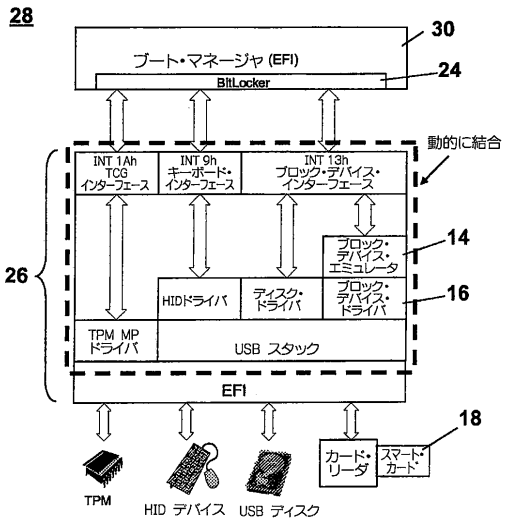


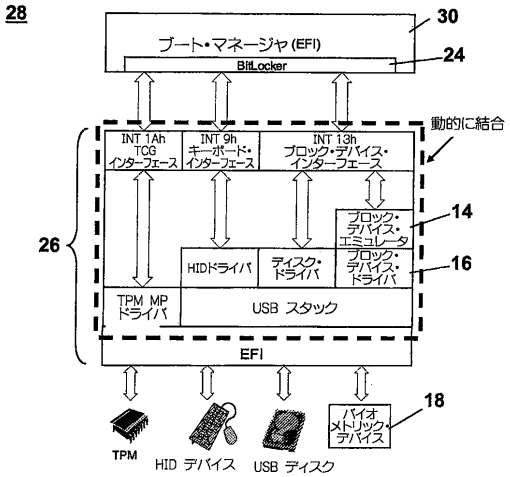
FIGURE 2



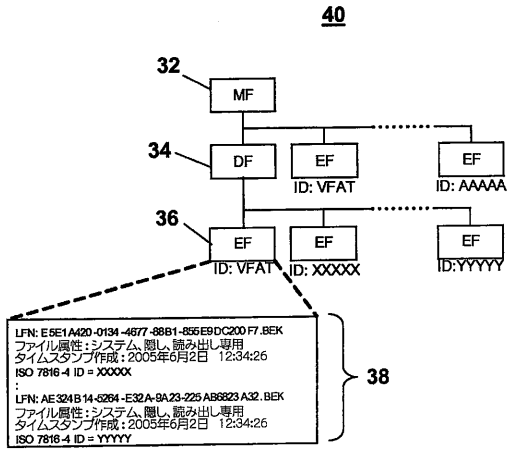
【図３】



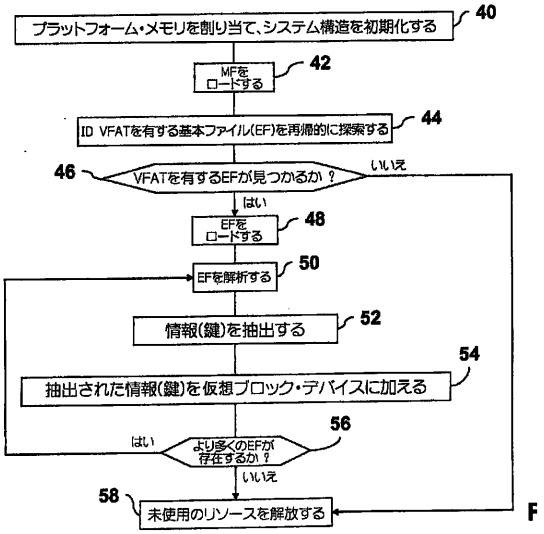
【図４】



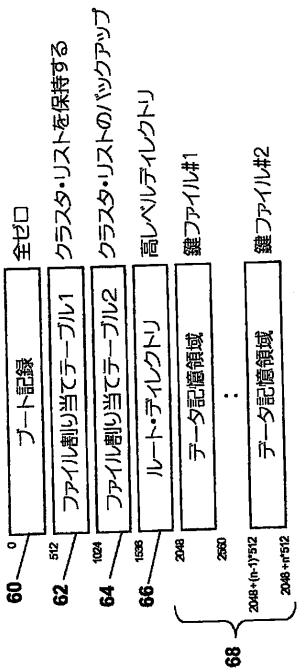
【図５】



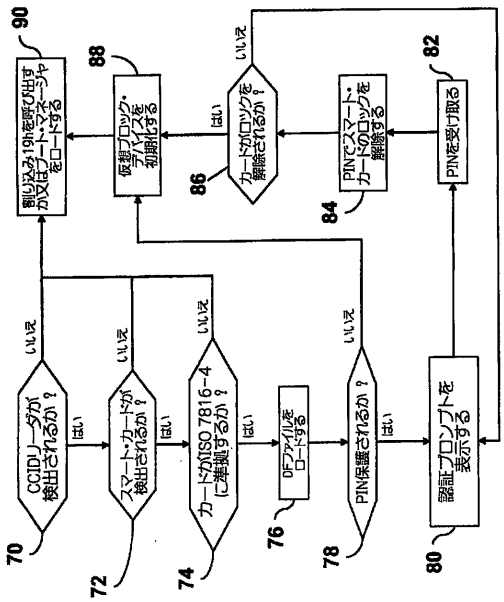
【図６】


プラットフォーム・メモリを割り当て、システム構造を初期化する
40
MFをロードする
42
ID VFATを有する基本ファイル(EF)を再帰的に探索する
44
VFATを有するEFが見つかるか？
46
いいえ
はい
EFをロードする
48
EFを解析する
50
情報(鍵)を抽出する
52
抽出された情報(鍵)を仮想ブロック・デバイスに加える
54
より多くのEFが存在するか？
56
はい
いいえ
未使用のリソースを解放する
58
F

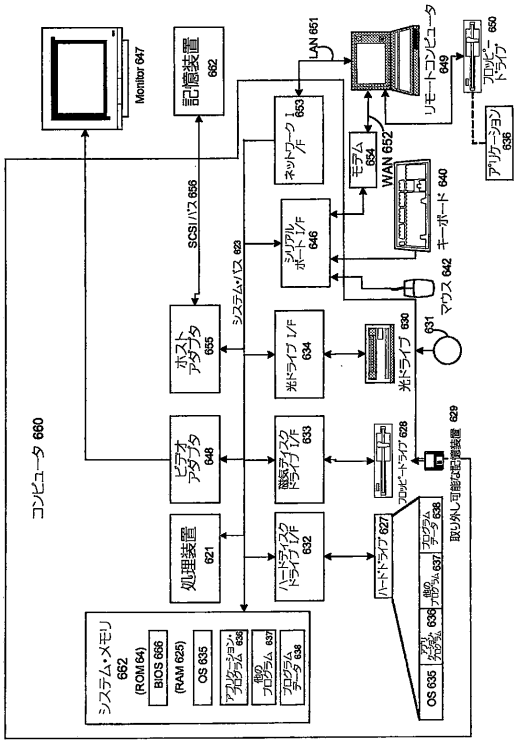
【図７】


全ゼロ
ブート記録
クラスタ・リストを保持する
ファイル割り当てテーブル1
クラスタ・リストのバックアップ
ファイル割り当てテーブル2
高レベルディレクトリ
ルート・ディレクトリ
鍵ファイル#1
データ記憶領域
鍵ファイル#2
データ記憶領域
0
512
1024
1536
2048
2560
2048+(n-1)*512
2048+n*512
60
62
64
66
68

【図８】


割り込み13hを呼び出すBIOSルーチンをロードする
90
仮想ブロック・デバイスを初期化する
88
カードがロックを解除されるか？
86
PINでスマート・カードのロックを解除する
84
PINを受け取る
82
CCIDリーダが検出されるか？
70
スマート・カードが検出されるか？
72
カードがISO 7816-4に準拠するか？
74
DFファイルをロードする
76
PIN保護されるか？
78
認証プロンプトを表示する
80
いいえ
はい

【図９】


コンピュータ 660
Monitor 647
記憶装置 682
LAN 651
リモート・コンピュータ 649
プリンター 650
アプリケーション 636
フロッピー・ドライブ
ネットワーク I/F 653
モデム 654
WAN 652
キーボード 640
マウス 642
シリアル・ポート I/F 646
システム・バス 622
SCSIバス 656
ホスト・アダプタ 655
光ドライブ I/F 634
光ドライブ 631
ビデオ・アダプタ 648
磁気ディスク I/F 633
フロッピー・ドライブ 628
処理装置 621
ハード・ドライブ I/F 632
ハード・ドライブ 627
取り外し可能な記憶装置 629
システム・メモリ 622
(ROM 64)
BIOS 666
(RAM 625)
OS 635
アプリケーション・プログラム 638
他のプログラム 637
プログラム・データ 638

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2007/079737

A. CLASSIFICATION OF SUBJECT MATTER

G06F 9/06(2006.01)i, G06F 15/00(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 8 G06F, H04Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Korean Utility models and applications for Utility models since 1975
Japanese Utility models and applications for Utility models since 1975

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
eKIPASS(KIPO internal) "Keywords: pre-booting, BIOS, device driver, smartcard and similar terms"

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	KR 10-1999-0058372 A (SAMSUNG ELECTRONICS CO., LTD.) 15 July 1999 See the abstract, figures 1-2, and pages 2-3.	1-6, 10-14, 16-18, 20 7-9, 15, 19
Y	KR 10-2000-0018098 A (SOLID SYSTEM CO., LTD.) 06 April 2000 See the abstract, figures 1-2 and 7, and pages 2-3.	7-9, 15, 19
A	US 6,463,537 B1 (TELLO, J. A.) 08 October 2002 See the abstract, figures 1 and 13A-13V, and col.2 line 57 - col.3 line 48 and col.14 lines 1-44.	1-20
A	KR 10-2002-0004368 A (KOO, SEUNG YUB) 16 January 2002 See the abstract, figures 1-3, and pages 2-4.	1-20
A	KR 10-2001-0087034 A (KIM, H. H. et al.) 15 September 2001 See the abstract, figures 2-3, and pages 3-4.	1-20
A	KR 10-2006-0004584 A (SAMSUNG ELECTRONICS CO., LTD.) 12 January 2006 See the abstract, figures 2-3, and pages 2-3.	1-20

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents,such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
05 MARCH 2008 (05.03.2008)	**05 MARCH 2008 (05.03.2008)**
Name and mailing address of the ISA/KR Korean Intellectual Property Office Government Complex-Daejeon, 139 Seonsa-ro, Seo-gu, Daejeon 302-701, Republic of Korea Facsimile No. 82-42-472-7140	Authorized officer NHO, Ji Myong Telephone No. 82-42-481-8528

Form PCT/ISA/210 (second sheet) (April 2007)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/US2007/079737

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
KR 1019990058372 A	15.07.1999	None	
KR 1020000018098 A	06.04.2000	None	
US 06463537 B1	08.10.2002	None	
KR 1020020004368 A	16.01.2002	KR 1020020004366 A KR 1020020004367 A	16.01.2002 16.01.2002
KR 1020010087034 A	15.09.2001	None	
KR 1020060004584 A	12.01.2006	None	

フロントページの続き

(81)指定国 AP(BW,GH,GM,KE,LS,MW,MZ,NA,SD,SL,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,MD,RU,TJ,TM),EP(AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HU,IE,IS,IT,LT,LU,LV,MC,MT,NL,PL,PT,RO,SE,SI,SK,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AT,AU,AZ,BA,BB,BG,BH,BR,BW,BY,BZ,CA,CH,CN,CO,CR,CU,CZ,DE,DK,DM,DO,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,GT,HN,HR,HU,ID,IL,IN,IS,JP,KE,KG,KM,KN,KP,KR,KZ,LA,LC,LK,LR,LS,LT,LU,LY,MA,MD,ME,MG,MK,MN,MW,MX,MY,MZ,NA,NG,NI,NO,NZ,OM,PG,PH,PL,PT,RO,RS,RU,SC,SD,SE,SG,SK,SL,SM,SV,SY,TJ,TM,TN,TR,TT,TZ,UA,UG,UZ,VC,VN,ZA,ZM,ZW

(74)代理人 100147991
弁理士 鳥居 健一
(72)発明者 ウーテン, ディヴィッド・アール
アメリカ合衆国ワシントン州９８０５２, レッドモンド, ワン・マイクロソフト・ウェイ, マイクロソフト コーポレーション, インターナショナル・パテンツ
(72)発明者 ホルト, エリック
アメリカ合衆国ワシントン州９８０５２, レッドモンド, ワン・マイクロソフト・ウェイ, マイクロソフト コーポレーション, インターナショナル・パテンツ
(72)発明者 トム, ステファン
アメリカ合衆国ワシントン州９８０５２, レッドモンド, ワン・マイクロソフト・ウェイ, マイクロソフト コーポレーション, インターナショナル・パテンツ
(72)発明者 ウレチェ, トニー
アメリカ合衆国ワシントン州９８０５２, レッドモンド, ワン・マイクロソフト・ウェイ, マイクロソフト コーポレーション, インターナショナル・パテンツ
(72)発明者 スレッズ, ダン
アメリカ合衆国ワシントン州９８０５２, レッドモンド, ワン・マイクロソフト・ウェイ, マイクロソフト コーポレーション, インターナショナル・パテンツ
(72)発明者 マックルヴァー, ダグラス・エム
アメリカ合衆国ワシントン州９８０５２, レッドモンド, ワン・マイクロソフト・ウェイ, マイクロソフト コーポレーション, インターナショナル・パテンツ

Ｆターム(参考) 5B017 AA03 BA05 CA07 CA15 CA16
5B285 AA01 AA04 BA01 CB02 CB06 CB12 CB83