(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4052978号
(P4052978)
(45)発行日　平成20年2月27日(2008.2.27)　(24)登録日　平成19年12月14日(2007.12.14)

(51)Int.Cl.　　F I
G06F 21/22 (2006.01)　　G06F 9/06 660G
G06F 9/445 (2006.01)　　G06F 9/06 610K

請求項の数 6　(全 13 頁)

(21)出願番号　特願2003-164095(P2003-164095)
(22)出願日　平成15年6月9日(2003.6.9)
(65)公開番号　特開2004-13905(P2004-13905A)
(43)公開日　平成16年1月15日(2004.1.15)
審査請求日　平成18年4月25日(2006.4.25)
(31)優先権主張番号　10/165,519
(32)優先日　平成14年6月7日(2002.6.7)
(33)優先権主張国　米国(US)

早期審査対象出願

前置審査

(73)特許権者　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　100089705
弁理士　社本　一夫
(74)代理人　100140109
弁理士　小野　新次郎
(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】セキュアなブートローダにおけるハッシングの使用

(57)【特許請求の範囲】
【請求項１】
オペレーションのためにブートアップさせなければならない電子装置において、
（ａ）複数の機械命令がストアされた不揮発性メモリであって、主要部分を含み、内容とサイズとロケーションとに関して予め定義されたプリローダ部分を含む不揮発性メモリと、
（ｂ）前記不揮発性メモリに結合されたプロセッサであって前記機械命令を実行するプロセッサと、
（ｃ）ハッシングアルゴリズムを規定し前記電子装置のブートアップ中に前記プロセッサによって最初に実行される機械命令と予想ハッシュ値とを指定する、前記不揮発性メモリと異なる回路要素内にストアされたファームウェアの形で提供されるブートストラップコードであって、前記プロセッサに、
（ｉ）前記不揮発性メモリの前記プリローダ部分をハッシュしてプリローダハッシュ値を決定させ、
（ｉｉ）前記プリローダハッシュ値を前記予想ハッシュ値と比較させ、
（ｉｉｉ）前記プリローダハッシュ値が前記予想ハッシュ値と等しくない場合に、前記電子装置のブートアップを終了させる、
ブートストラップコードファームウエアと、
（ｄ）前記不揮発性メモリの前記プリローダ部分に含まれる複数の２次的機械命令であって、前記プロセッサによって実行された時、該プロセッサをして、

（ｉ）前記不揮発性メモリをハッシュしてメモリハッシュ値を生成させ、
（ｉｉ）前記メモリハッシュ値を、予想メモリハッシュ値と比較させ、
（ｉｉｉ）前記メモリハッシュ値が前記予想メモリハッシュ値と等しくない場合に、前記電子装置のブートアップを終了させ、前記予想メモリハッシュ値は、前記不揮発性メモリ内にデジタル署名として含まれるが、前記不揮発性メモリがハッシュされるとき除外されることを特徴とする２次的機械命令と、
を備えたことを特徴とする電子装置。
【請求項２】
請求項１記載の装置において、前記不揮発性メモリの前記プリローダ部分中の前記機械命令は、さらに、前記プロセッサに、前記予想メモリハッシュ値を決定するために、前記デジタル署名をベリファイさせることを特徴とする電子装置。
【請求項３】
請求項１記載の装置において、前記不揮発性メモリの前記プリローダ部分中の前記機械命令は、さらに、前記プロセッサに、前記プリローダ部分に含まれる公開鍵を適用して前記デジタル署名をベリファイさせることを特徴とする電子装置。
【請求項４】
オペレーションのためにブートアップさせなければならない電子装置において、
（ａ）複数の機械命令がストアされた不揮発性メモリであって、主要部分を含み、内容とサイズとロケーションとに関して予め定義されたプリローダ部分を含む不揮発性メモリと、
（ｂ）前記不揮発性メモリに結合されたプロセッサであって前記機械命令を実行するプロセッサと、
（ｃ）前記不揮発性メモリと異なる回路要素内にストアされ、データ記憶及びブートアップ保護以外の少なくとも１つの機能を実行するように構成されているファームウエアから成り、ハッシングアルゴリズムを規定し前記電子装置のブートアップ中に前記プロセッサによって最初に実行される機械命令と予想ハッシュ値とを指定するブートストラップコードであって、前記プロセッサに、
（ｉ）前記不揮発性メモリの前記プリローダ部分をハッシュしてプリローダハッシュ値を決定させ、
（ｉｉ）前記予想ハッシュ値を前記プリローダハッシュ値と比較させ、
（ｉｉｉ）前記プリローダハッシュ値が前記予想ハッシュ値と等しくない場合に、前記電子装置のブートアップを終了させる、
ブートストラップコードファームウエアと、
を備え、
（ｄ）前記不揮発性メモリの前記プリローダ部分は、前記プロセッサに、
（ｉ）前記不揮発性メモリをハッシュしてメモリハッシュ値を生成させ、
（ｉｉ）前記メモリハッシュ値を、前記不揮発性メモリ内にあるデジタル署名から成り、前記不揮発性メモリがハッシュされるとき除外される予想メモリハッシュ値と比較させ、
（ｉｉｉ）前記メモリハッシュ値が前記予想メモリハッシュ値と等しくない場合に、前記電子装置のブートアップを終了させる、
機械命令を含むことを特徴とする電子装置。
【請求項５】
請求項４記載の装置において、前記不揮発性メモリの前記プリローダ部分中の前記機械命令は、さらに、前記プロセッサに、前記デジタル署名をベリファイさせることを特徴とする電子装置。
【請求項６】
請求項４記載の装置において、前記不揮発性メモリの前記プリローダ部分中の前記機械命令は、さらに、前記プロセッサに、前記プリローダ部分に含まれる公開鍵を適用して前記デジタル署名をベリファイさせることを特徴とする電子装置。

【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は、一般に、プロセッサを含む電子装置をセキュアにブートアップすることに関し、具体的には、このような電子装置をブートアップするときに、所望の機械命令のみがプロセッサによって実行されることを保証し、これによりブートアッププロセス中に置換または代替の機械命令が実行されるのを防止することに関する。
【０００２】
【従来の技術】
電子装置は、多くの場合、起動時またはリセット時に、ブートアッププロセスを経なければならない。ブートアッププロセスにおいては、当該電子装置の基本的なオペレーション特性をコントロールする機械命令であって、ＲＯＭ（read only memory）にストアされている機械命令が、アクセスされ実行されると、当該電子装置が初期化され、この機械命令によりさらに機械命令がＲＡＭ（random access memory）にロードされ、そしてこのロードされた機械命令が実行されると、これにより当該電子装置に機能がさらにインプリメントされる。例えば、パーソナルコンピュータがブートアップされると、ＢＩＯＳ（basic input-output system）を備えた命令が実行され、これにより、ＯＳ（operating system）がハードドライブからＲＡＭにロードされ、このＯＳはコンピュータのＣＰＵ（central processing unit）によって実行される。「ブートアップ」という用語は、初期の「ブートストラップ」という記述的な用語を短縮したものである。
【０００３】
その他、ブートアップしなければならない電子装置としては、ゲームコンソールと、デジタル記録装置と、パーソナルデータシステムとが含まれ、プロセッサを含む電子製品はほとんどのものが含まれる。この種のプロセッサは、次々に機械命令をメモリにロードして実行し機能を追加していくため、初期機械命令のセットを実行しなければならないようになっている。このブートアッププロセスにより電子装置の初期状態が決定されるので、このブートアッププロセスは、当該電子装置の重要なオペレーションパラメータに影響を与え、ブートアッププロセスの完了後に当該電子装置がどのように使用されるかに実質的に影響を与える可能性がある。このブートアッププロセスが修正されないようにすることは、当該電子装置の販売会社にとって、当該電子装置の使用により得られる収益が減じないようにするためにも、重要なことである。
【０００４】
例えば電子ゲーム産業においては、電子ゲームをプレイするために販売されたゲームコンソールの商業的価値は、多くは、ゲームコンソールでラン（run）されるゲームソフトウェアのライセンスからの収益である。そこで、ブートアッププロセスにおいてロードされる機械命令には、ライセンスのないソフトウェアコピーがゲームコンソール上でランされないようにする機能と、電子ゲームをプレイするためのゲームコンソールの使用に関係する製造業者のポリシーを順守させる機能とがインプリメントされている。ユーザの中には、ライセンスのないソフトウェアコピーのランに対する規制や、ゲームコンソールに関するこのようなポリシーを順守させる規制を、ゲームコンソールに対する挑戦的な規制であり歓迎できない規制であるとみる者もいる。このようなユーザは、ゲームコンソール回路やソフトウェアを「ハック（hack）」してこのような規制を打破しようとしている。例えば、これらの規制を回避するための１つの方法としては、ゲームコンソールでランされるブートアッププロセスに、幾つかの変更を加えた改変ソフトウェアカーネルをロードさせる方法がある。変更が加えられたため、ゲームコンソール製造業者による規制が取り除かれるので、結果として、当該製造業者がゲームコンソールの使用をコントロールできなくなるおそれがあり、仮にライセンスのないソフトウェアゲームコピーがゲームコンソール上でランできるようになった場合は収益が減じるおそれがある。そこで、普通は、ゲームコンソール製造業者が、ハッカーがブートアッププロセス中に改変ソフトウェアカーネルを使用できないように、努力している。

【０００５】
ブートアップしなければならない電子装置を利用する他の技術分野においても、同様の問題が存在する。例えば、ユーザから月額料金が支払われたか否かに基づき受信チャネルを制限する衛星ＴＶ（television）レシーバの製造業者においては、当該コンシューマがライセンス条項に従って衛星ＴＶレシーバを使用できるためには、製造業者のセキュリティポリシーと、製造業者の製品の使用に関するポリシーとが順守されることを保証しなければならい。ユーザがビューするためにペイしたＴＶチャネルを衛星ＴＶレシーバ内のプロセッサに決定させるためのコードを、ハッカーが修正すると、これにより、ライセンス料を適正に支払わなくても、全てのチャネルを受信しビューすることができる。
【０００６】
【発明が解決しようとする課題】
そこで、電子装置のブートアップ中においては、オーソライズされたソフトウェアコードのみが実行されるようにすることが望ましい。使用されている技法は、どれも、オーソライズされたソフトウェアであって電子装置のブートアップ中に実行されるようになっているソフトウェアが、修正又は改変された機械命令セットと置換されないようにすべきであり、この技法は、電子装置が、製造側の、および／または当該電子装置をエンドユーザに配布した側の、機能およびポリシーをインプリメントすることを、保証すべきである。電子装置のブートアップ時にロードされるコードに含まれる、電子装置の使用に関する規制およびポリシーを、ハッカーが破るのを防止するための既知の手法は、完全には成功していないようである。アドイン回路カードが代替ソフトウェアコードを含む場合には、ハッカーは、この回路カードを電子装置の回路に結合するだけで、既知のセキュリティアプローチを少なくとも一部は破ることができる。明らかなことであるが、電子装置のブートアッププロセス中に代替コードが挿入されたり実行されたりするのを防止するためには、よりセキュアで厳重な手法が必要である。
【０００７】
【課題を解決するための手段】
本発明は、プロセッサを備えた装置であって、当該電子装置の機能を実行させるために、起動時またはリセット時にブートアップしなければならない装置であればどの装置にも適用可能である。このような装置においては、当該電子装置のオペレーション中に利用されるプロプラエタリ（proprietary）情報を保護すること、及びオーソライズされていないコードがブートアッププロセス中に実行されて、当該電子装置のオペレーションおよびアプリケーション（application）に関係するポリシーが覆されることを防止することが重要であることが多い。
【０００８】
電子装置の所望のポリシーおよび機能を覆すために置換される可能性が最も高いコンポーネントの１つは、電子装置がどのように使用されるかを定義する機械命令がストアされた不揮発性メモリである。したがって、本発明は、このようなメモリ中の機械命令を含むコードがオーソライズされていること（すなわち、電子装置の所望の機能およびポリシーを変更する機械命令で修正または置換されていないこと）を確認することを試みる。本発明においては、オーソライズされているコードは、予め定義された部分（プリローダコードともいう）を含む。この予め定義された部分は、オーソライズされているコードの残りの部分に変更が加えられても、変化しないようにしなければならない。そうでないと、当該電子装置はブートアップしないことになる。
【０００９】
最初に、コードの予め定義された部分がオーソライズされていることを保証するためのプロシージャを実行する。このプロシージャにおいては、予め定義された部分をハッシュして、第１のハッシュ値を生成する。ついで、この第１のハッシュ値を、コードがストアされているメモリとは別の電子装置回路コンポーネントに保持されている保持ハッシュ値と比較し、コードの予め定義された部分がオーソライズされていることをベリファイする。この第１のハッシュ値が保持ハッシュ値と等しい場合は、コードの予め定義された部分

の実行を可能にし、そうでない場合は、電子装置のブートアップを終了する。コードの予め定義された部分が実行可能になった場合、実質的に全てのコードをハッシュして、第２のハッシュ値を決定する。コードの予め定義された部分とは異なるコード部分には、デジタル署名が含まれている。ついで、第２のハッシュ値によりデジタル署名がベリファイされ、署名の妥当性が保証される。デジタル署名が真正であるとベリファイされた場合は、コードの実行を可能にし、そうでない場合は、電子装置のブートアップを終了する。

【００１０】

第１の値を保持ハッシュ値と比較するためには、回路コンポーネントの不揮発性記憶領域で保持される初期コードを実行する。この初期コードは、保持ハッシュ値を含み、グラフィックプロセッサ中で保持されるが、他のタイプの補助プロセッサ、例えば、オーディオプロセッサ、入力プロセッサ、出力プロセッサ、通信プロセッサ、またはデジタル信号プロセッサ中で保持ハッシュ値が保持されるようになっていてもよい。実際、初期コードおよび予想ハッシュ値は、初期コードを実行するプロセッサ中で保持することがより一層好ましい。初期コードを実行して、予め定義された部分をハッシュし、第１のハッシュ値と保持ハッシュ値とを比較する。本発明の好ましい形態においては、初期コードは、ファームウェア中で予め定めたバイト数として永続的に定義される。加えて、コードの予め定義された部分は、コード内の予め定められたロケーションに配置された予め定めたバイト数を含むことが好ましい。これは明らかであるが、保持ハッシュ値が変更されない限り、コードの予め定義された部分のサイズおよび内容を修正することはできない。というのは、修正された場合には、保持ハッシュ値は第１のハッシュ値と等しくなくなるからである。

【００１１】

予め定義された部分は、デジタル署名をベリファイするのに使用される公開鍵も含み、コードの暗号化されたカーネル部分を復号できるようにする機械命令も有する。ついで、復号されたカーネルを実行して、電子装置のブートアップを完了する。予め定義された部分は、ストリーミングサイファ（streaming cipher）を使用して、コードのカーネル部分の復号を実行する。

【００１２】

本発明の別の態様は、コードがオーソライズされているか否かを判定するため、当該電子装置のブートアップ中にアクセスされる機械命令を含むコードがストアされた記憶媒体を対象とする。この記憶媒体は、前に述べた、カーネル部分、ブートローダ部分、プリローダ部分、およびデジタル署名を含む。

【００１３】

本発明の別の態様は、オペレーションするためにブートアップされなければならない電子装置を対象とする。この電子装置は、複数の機械命令がストアされた不揮発性メモリを含む。不揮発性メモリは、主要部分と、予め定義された内容、サイズ、およびロケーションを有するプリローダ部分とを含む。プロセッサが不揮発性メモリに結合されて、ブートアッププロセス中に機械命令を実行する。ブートストラップコードファームウェアが、ハッシングアルゴリズムを規定する機械命令と予想ハッシュ値とを指定する。ブートストラップコードファームウェアの機械命令は、電子装置のブートアップ中にプロセッサによって最初に実行され、プリローダ部分のハッシング、およびその結果と予想ハッシュ値の比較を、プロセッサに実行させる。電子装置およびその機能のその他の詳細は、一般に、前に述べた方法のステップと一致する。

【００１４】

本発明をゲームコンソールのような電子装置に採用すれば、ブートアッププロセス中に実行される機械命令を変更しようとしても、あるいは異なる機械命令をもつ別のメモリと置換しようとしても、装置は首尾よくブートアップされなくなることが明らかである。したがって、本発明は、一般に、電子装置のブートアップ中にオーソライズされているコードのみが実行されるようにすることにより、何者かが基本機能を修正するか、あるいは電子装置によってインプリメントされる所望のポリシーを回避することを防止する。

【００１５】
本発明の前述の態様およびそれに付随する利点の多くは、以下の詳細な説明と添付の図面を参照することによってよりよく理解され、より認識しやすくなるであろう。
【００１６】
【発明の実施の形態】
（システム例）
次のことは強調しておかなければならない。すなわち、本発明の第１の好ましい実施形態は、実際は、ゲームコンソール上で使用されるが、本発明は、ゲームコンソールと共に使用されることに限定されない。本発明は、コードをリバースエンジニアリングしようとするユーザに、プロプラエタリ情報が開示されないようにするため、及び電子ゲームをするためのゲームコンソールの使用に関するライセンス規制およびポリシーを、ユーザが回避するのを防止するために、発明された。
【００１７】
図１に示すように、電子ゲームシステム１００には、ゲームコンソール１０２と、コントローラ１０４ａおよび１０４ｂのような入力装置（最高４人のユーザをサポートする）が含まれている。ゲームコンソール１０２は、（図１に図示しない）内部ハードディスクドライブを備え、種々のフォーマットのポータブル光記憶媒体（図１には光記憶ディスク１０８で表している）をサポートするポータブル媒体ドライブ１０６を備えている。適正なポータブルストア媒体の例には、ＤＶＤディスクおよびＣＤ－ＲＯＭディスクが含まれる。このゲームシステムにおいては、ゲームプログラムは、ゲームコンソールとともに使用するためＤＶＤディスクで配布されるのが好ましいが、しかし、データセキュリティポリシーを順守し、システムに入力されているデジタルデータが真正であることを保証するため、本発明を使用している本システムその他のシステムで、他の記憶媒体を、ＤＶＤの代わりに、使用できるようにしてある。
【００１８】
ゲームコンソール１０２の前面には、コントローラに接続しコントローラをサポートするための４つのスロット１１０がある。ただしスロットの数および構成は変更することができる。電源ボタン１１２とイジェクトボタン１１４もゲームコンソール１０２の前面に配置されている。電源ボタン１１２は、電源のゲームコンソールへの供給をコントロールするものであり、イジェクトボタン１１４は、ゲームコンソール１０２が光記憶ディスク１０８上のデジタルデータをリードして使用できるように、光記憶ディスク１０８を挿入したり取り出すため、ポータブル媒体ドライブ１０６のトレイ（図示せず）をオープン又はクローズするものである。
【００１９】
ゲームコンソール１０２は、ＴＶその他のディスプレイモニタ、または（図示しない）スクリーンに、オーディオ／ビジュアル（Ａ／Ｖ）インタフェースケーブル１２０を介して接続されている。電源ケーブルプラグ１２２は、慣用の（図示しない）交流電源に接続されたとき、ゲームコンソールに電源を供給するものである。ゲームコンソール１０２は、the Internetのようなネットワークを介し、例えば慣用の電話モデムを介して、またはより好ましくはブロードバンド接続により、データを転送するため、データコネクタ１２４を備えることもできる。
【００２０】
コントローラ１０４ａおよび１０４ｂは、リード線を介して（あるいは無線インタフェースを介して）ゲームコンソール１０２に結合されている。本実装形態においては、コントローラ１０４ａおよび１０４ｂは、ＵＳＢ（universal serial bus）コンパチブルであり、ＵＳＢケーブル１３０を介して、ゲームコンソール１０２に接続されている。ゲームコンソール１０２は、ゲームソフトウェアとインタラクト（interact）し、このゲームソフトウェアをコントロールするための種々のユーザ装置を備えることができる。図１には、コントローラ１０４ａの詳細を全て示していないが、コントローラ１０４ａおよび１０４ｂは、２つのサムスティック１３２ａおよび１３２ｂと、Ｄパッド１３４と、ボタン１３

６と、２つのトリガ１３８を備えている。これらのコントローラは代表的なものであるが、他の既知のゲーム入力およびコントロール機構を、ゲームコンソール１０２と共に使用するために、図１に示すものに代えて、又は図１に示すものに追加することもできる。

【００２１】

リムーバブルまたはポータブルＭＵ（memory unit）１４０を、オプションで、コントローラ１０４に挿入することにより、リムーバブルなストレージ（storage）を追加することもできる。ユーザは、ポータブルＭＵにゲームパラメータをストアすることができ、このポータブルＭＵを他のコントローラに挿入すれば、ゲームパラメータをポート（port）することができ、ゲームをプレイすることができる。本実装形態においては、コントローラは、それぞれ、２つのＭＵを挿入できるように構成されているが、この構成に代えて、ＭＵの数を２つよりも多くも少なくもできる。

【００２２】

ゲームシステム１００は、ゲーム、音楽、及びビデオを再生することができる。ハードディスクドライブにストアされたデジタルデータを使用して、あるいはポータブル媒体ドライブ１０６中の光記憶ディスク１０８か、オンラインソースか、又はＭＵ１４０から読み取られたデジタルデータを使用して、その他の機能をインプリメントできるようになっている。このゲームコンソールは、電子ゲームディスクのオーソライズされていないコピーが再生されないように設計されている。あるポリシーも、ゲームコンソールによってインプリメントされている。例えば、ある地域で販売されたソフトウェアが、別の地域で販売されたゲームコンソール上で実行できないようにすることができる。ビデオＤＶＤの複製を防止するためのインダストリ基準方式（MACROVISION（商標））も、ゲームコンソールソフトウェアによってインプリメントされている。

【００２３】

ゲームコンソールによってインプリメントされているこれらの機能制限およびポリシーを破ることを好んでいるユーザもいる。このような制限およびポリシーを回避しようとする１つの方法としては、当該ゲームコンソールをブートアップするのに使用するため、オリジナルのＲＯＭ及びこのＲＯＭにストアされたコードを修正バージョンのものと置換したＩＣ（integrated circuit）またはモジュールを、ゲームコンソールにインストールする方法がある。このような置換モジュール中の機械命令を修正するのは、ブートアッププロセス中にオペレートさせるためであり、次のような規制と、ゲームコンソールの他の態様および／またはポリシーと、を除去または変更しようとするためである。上記規制とは、ゲームコンソールの製造業者または設計者によるものであり、オーソライズされていないコピーの使用を防止し、ビデオＤＶＤの複製を防止するものである。しかし、本発明によれば、オーソライズされていない置換ＲＯＭモジュールを挿入してブートアッププロセスを改変することは、極めて困難であり、仮にゲームコンソールのブートアップ中に代替コードおよびオーソライズされていないコードの利用が検出された場合には、ブートアッププロセスが終了する。

【００２４】

ブートアッププロセスに関するプロプラエタリ情報が発見されるのを防止し、しかも修正コードまたは代替コードがブートアッププロセス中に利用されるのを防止するためには、ブートアップ中に実行される機械命令のうちの少なくとも幾つかは、ゲームコンソールその他の電子装置のＲＯＭに含まれている機械命令の大部分から分離しておかなければならない。一般に、電子装置のプリント回路基板にある、ＩＣ、トレース（trace）、接続点、及びビア（via）は、仮に電子装置の筐体が開けられれば、容易にアクセスでき、当該電子装置をハックするため、新たな接続および修正を物理的に加えることができる。誰かがプリント回路基板にアクセスしないようにすることは困難であるが、本発明によれば、プリント回路基板に実装されたＩＣの１つにファームウェアとしてエンベッド（embed）されている機械命令にアクセスすることは、極めて困難である。好ましくは、使用するＩＣとしては、公衆がサプライヤ（supplier）から容易に入手できないことを目的としたＩＣを用いるべきである。というのは、ＩＣは、当該電子装置の製造業者のためにカスタム

メイドされたものであるからである。この目的のＩＣは、当該電子装置のオペレーションにとって不可欠なものであるから、仮にＩＣにエンベッドされたファームウェアへのアクセスが試みられた場合には、当該ＩＣのオペレーション、したがって当該電子装置のオペレーションに、おそらく不都合が生じることになる。

【００２５】

図２Ａは、ゲームコンソール１００に含まれる幾つかのＩＣコンポーネントを示す。ＣＰＵ２０２はメインプロセッサであり、当該ゲームコンソールの大部分の処理機能を実行するのに使用されている。ＣＰＵ２０２も、大部分のプロセッサと共通して、最初にブートアップされなければならず、これにより、設計上当該ゲームコンソールにインプリメントされている種々の機能を実行することができる。ＣＰＵ２０２は、カスタマイズされたグラフィックプロセッサであって、NVIDIA（登録商標）社製のＮＶ２Ａチップと称されるバス・メモリ・コントローラチップ２０４でもあるグラフィックプロセッサに、双方向接続されている。

このＮＶ２Ａチップは、ＲＡＭ２０６と、別のＮＶＩＤＩＡカスタムメードチップとに接続されている。この別のＮＶＩＤＩＡカスタムメードチップは、ＭＣＰ（media communication processor）２０８に接続されており、このＭＣＰ２０８は、オーディオ信号プロセッサ機能を有し、システムメモリに結合されており、またデータ通信のために、ＵＳＢポートおよびEthernet（登録商標）ポートに結合されている。ＭＣＰ２０８には、ブートストラップコード２１２を備える５１２byteのファームウェアが含まれる。ブートストラップコード２１２は、ＭＣＰ２０８内の他のレイヤー（layer）に実質的に埋め込まれており、このモジュールをディキャップ（decap）するだけではアクセスできない。ブートストラップコード２１２に物理的にアクセスするには、上のレイヤーを除去する必要があるが、そうすると、ＭＣＰモジュールは事実上破壊されて、ＭＣＰモジュールおよびゲームコンソールは使用できなくなる。さらに、ＭＣＰ２０８はゲームコンソールの製造業者向けにカスタムメイドされたものなので、オープンマーケットで他の者が入手できない。ブートストラップコードが何らかの方法でアクセスされ、このファームウェアを備える機械命令が「ビジブル（visible）」になったとしても、本発明により、ブートシーケンスを改変することはできない。ＭＣＰ２０８は、ＲＯＭ２１０に結合されており、このＲＯＭ２１０には、ゲームコンソール１００のブートアップ中に使用される大部分の機械命令が含まれている。

【００２６】

本発明に係る一般的な応用例が、図２Ｂのコンポーネントに関して示されている。カスタムＣＰＵ２２０は、ＣＰＵの他のレイヤーの下に「埋め込まれた」ファームウェアブートストラップコード２２２を内部に含むことができるようになっている。図２Ｂに示すように、ＣＰＵ２２０は、ＲＡＭ２０６およびＲＯＭ２１０に結合される。ファームウェアブートストラップコード２２２がＣＰＵ２２０内のファームウェアを構成するので、ＣＰＵの処理部分とファームウェアブートストラップコード２２２との間の信号には、一般にアクセス不可能である。したがって、図２Ｂに示す実施形態においては、ファームウェアブートストラップコード２２２にアクセスしてその内容を決定するのはより一層困難になり、このため図２Ｂの実施形態においては、図２Ａの実施形態に比較してさらにセキュリティが向上する。

【００２７】

図３は、本発明で使用されているＲＯＭ２１０の別の部分を示す。ゲームコンソール１００で使用される好ましい実施形態においては、ＲＯＭ２１０は、２５６Kbyteのメモリモジュールを備えている。ＲＯＭ２１０には、暗号化されていないプリローダ２３０が含まれている。プリローダ２３０は、好ましい実施形態においては、約１１Kbyteの固定サイズを有し、その内容、サイズ、およびＲＯＭ２１０内でのロケーションは、すべて予め定義済みである。プリローダ２３０が、暗号化された公開鍵２３１を含むことに留意することは、重要なことである。これも重要なことであるが、ブートストラップコード２１２が対応して変更されない限り、プリローダ２３０の内容は変更せずそのままにしておく必

要がある。これについては後程説明するので明らかになる。ＲＯＭ２１０には、暗号化されたブートローダ２３２が含まれている。加えて、ＲＯＭ２１０には、デジタル署名２３４と、対称鍵２３６も含まれている。ＲＯＭ２１０は、その大部分が、カーネル２３８を備える機械命令をストアすることに当てられている。カーネル２３８は圧縮されており、しかも暗号化されている。カーネル２３８内に含まれている機械命令は、ゲームコンソール１００の機能の多くを予め定義するものであり、ゲームコンソール１００のオペレーションに関係するポリシーを確立するものである。最後に、チップセット初期化コード２４０が含まれており、ゲームコンソールに最初に電源が投入されたとき、このチップセット初期化コード２４０が実行される。

【００２８】

図４は、ゲームコンソール１０２の起動時またはリセット時に実行される論理ステップを示す。ステップ２５０にて、ＲＯＭ２１０のチップセット初期化コードをランする。チップセット初期化コード２４０に含まれる機械命令は、暗号化されておらず、これらの機械命令は、具体的な構成情報を定義しており、完全なゲームコンソールのアーキテクチャに適した具体的な構成シーケンスを定義している。チップセット構成を遂行するのに必要な機械コードは、ブートストラップコードに含まれている。具体的な値およびシーケンスは、チップセット初期化コードの一部である。ＣＰＵの初期化シーケンスも、ブートストラップコードに含まれており、チップセット初期化コードの残りの部分の前に実行される。次に、ブロック２５２においては、ＭＣＰ２０８内に埋め込まれているブートストラップコード２１２に含まれる機械命令が、一方向ハッシングアルゴリズムをランして、ＲＯＭ２１０中のプリローダ２３０のハッシュ値を決定する。前述したように、製造時にゲームコンソール１００にインストールされたオリジナルのＲＯＭ２１０においては、プリローダ２３０は、具体的な内容と、サイズと、ＲＯＭ２１０内でのロケーションとを有することになる。したがって、プリローダ２３０内に含まれる機械命令をハッシュすることによって得られたハッシュ値は、プリローダ２３０がオーソライズされていないコードで改変または置換されていない限り、常に同一であるべきである。好ましい実施形態においては、SHA-1 一方向ハッシングアルゴリズムを適用して、プリローダをハッシュする。あるいはまた、これに代えて、ＭＤ５ハッシングアルゴリズムを採用することができ、当業者にとって当然のことであるが、その他のハッシングアルゴリズムも使用することができる。採用されたハッシングアルゴリズムは、ブートストラップコード２１２の機械命令に含まれている。

【００２９】

ブートストラップコード２１２内には、プリローダ２３０の予想ハッシュ値である保持ハッシュ値と、対称鍵とが含まれている。ステップ２５４において、保持ハッシュ値をブートストラップコード２１２からロードする。ブートストラップコード２１２中の機械命令は、ブートストラップコードからの保持ハッシュ値と、ステップ２５２にてプリローダ２３０のために決定したハッシュ値とを比較する。この比較は、判定ステップ２５６で行い、保持ハッシュ値が、決定された実際のハッシュ値と等しいか否かを判定する。等しくないと判定した場合は、ブートストラップコード２１２中の機械命令は、ステップ２５８を実行し、ステップ２５８にて、ゲームコンソール１０２のブートアッププロセスを停止する。したがって、仮に異なるＲＯＭがオリジナルのＲＯＭと置換され、この新しく置換されるか、あるいはオーソライズされていないＲＯＭが、同一のプリローダ部分（一方向ハッシュアルゴリズムで処理されたときに予想ハッシュ値を生成する）を含んでいない場合には、判定ステップ２５６にて、プリローダ２３０への修正が検出され、ブートアッププロセスが終了する、ことは明らかである。

【００３０】

保持予想ハッシュ値が、決定された実際のハッシュ値と等しいと仮定して、ステップ２６０にて、ＲＯＭ２１０のプリローダコード部分を備える機械命令を実行する。このステップ２６０を実行することができるのは、ゲームコンソールの製造業者によってゲームコンソールにインストールされたＲＯＭに元々含まれていたプリローダコードと、このプリ

ローダ機械命令が同一であることが、明らかであるからである。

【００３１】

次に、ステップ２６２において、デジタル署名２３４を除くＲＯＭ２１０全体のハッシュ値を決定することができる。このプリローダは、一方向ハッシュ値を決定するための機械命令を含み、この場合も、ＳＨＡ－１又はＭＤ５のいずれかのハッシングアルゴリズム（あるいは、他の周知の一方向ハッシングアルゴリズムの１つ）を使用して、ＲＯＭ２１０の大部分のハッシュ値を決定する（デジタル署名は、ハッシュされるＲＯＭ２１０の内容に含まれない）、のが好ましい。同一のハッシュアルゴリズムが適用される限り、仮に機械命令が変更されていないか、オーソライズされていない機械命令と置換されていない場合には、その結果は常に同じである。ＲＯＭ２１０中でハッシュされた機械命令が少しでも変更されれば、ハッシュ値は実質的に変更されることになる。

【００３２】

ステップ２６４にて、ＲＯＭ２１０の公開鍵２３１をデジタル署名２３４に適用して、デジタル署名のための対応する値を生成する。（公開鍵を適用できるようになるまでは、この公開鍵は、ＭＣＰのブートストラップコードにストアされた対称鍵で復号されるが、この公開鍵がこの対称鍵で暗号化されない場合は、このステップは不要である。）次に、プリローダ２３０中の機械命令は、図４の判定ステップ２６６において、この公開鍵がこの署名をベリファイできるか否かを判定する。このステップ２６６においては、ステップ２６４からの値が、ステップ２６２で決定したＲＯＭのハッシュ値と等しいか否かを判定する。等しくない場合には、ＲＯＭのオリジナルの内容が作成された後でＲＯＭ中の署名が変更されたことが明らかになるので、ステップ２６８でブートアップオペレーションを停止する。周知のように、署名の値が、元々、ゲームコンソールの製造業者のみが知っている秘密鍵を使用して署名されたものである場合は、公開鍵を使用して署名の妥当性を確認することができる。何者かがゲームコンソール１００をハックしてＲＯＭ２１０のいずれかの部分を修正しようとする場合、判定ステップ２６６にてハッシュ値の変化が検出され、これによりステップ２６８でブートアッププロセスが終了する。これに対して、仮にデジタル署名がＲＯＭのハッシュと一致する場合は、ＲＯＭの内容が、オーソライズされたオリジナルの内容と同一であることは、明らかである。

【００３３】

ステップ２６４でデジタル署名から決定された値が、判定ステップ２６６でＲＯＭのハッシュをベリファイしたと仮定すると、ステップ２７０において、ブートアップを完了させることができ、カーネル２３８をＲＡＭ２０６にコピーし、ついで圧縮解除し復号してＲＡＭにストアすることができる。プリローダ２３０は、ブートローダを復号するための機械命令を含む。ＭＣＰに保持されるファームウェアブートストラップコード中の対称鍵を、ＲＯＭ２１０の対称鍵２３６と組み合わせて、新たに対称コードを生成し、得られた対称コードを使用して、プリローダ中の機械命令に従ってブートローダを復号する。

【００３４】

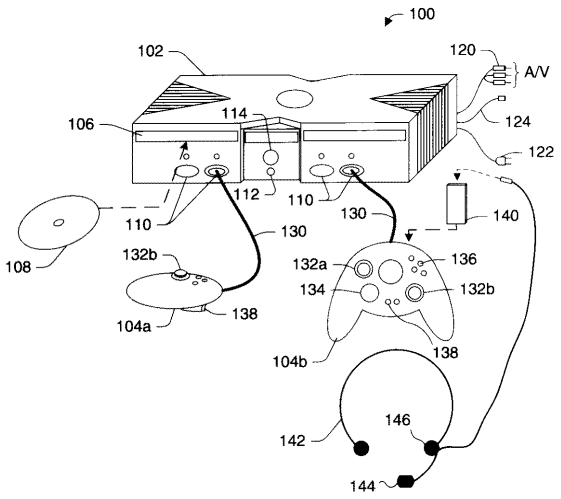
このブートローダは、圧縮され暗号化されたカーネルのストリームサイファ復号を、ＲＣ４ストリームサイファアルゴリズムに従って、実行するための機械命令を含む。このことは、当業者にとって周知のことである。ついで、ＣＰＵ２０２は、ＲＡＭ２０６内に圧縮解除され復号されたカーネルを備える機械命令を実行し、ゲームコンソールの完全な機能を実行することができ、これにより、次のことを保証する。すなわち、例えば、ＣＰＵ２０２が、オーソライズされたゲームソフトウェアのみをロードすること、ビデオＤＶＤの複製を妨げるアルゴリズムを実行すること、及びゲームコンソールの製造業者によって望まれるその他あらゆるポリシーおよび機能であって、オーソライズされたブートアップコードによって定義されるものを実行すること、を保証する。

【００３５】

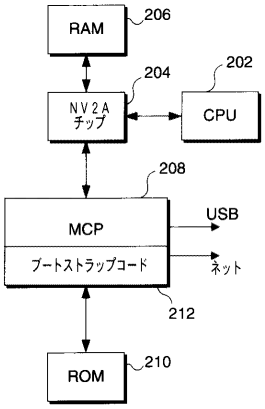
本発明は、本発明に係る実施形態につき述べたが、当業者にとって当然のことであるが、請求の範囲を逸脱することなく、修正をすることができる。したがって、本発明の範囲は、上記記述によって限定されず、請求の範囲により決定される。

【図面の簡単な説明】
【図１】本発明を採用したゲームコンソールを示す等角投影図である。
【図２Ａ】図１のゲームコンソールに含まれる幾つかの機能コンポーネントを示すブロック図である。
【図２Ｂ】ブートアップする電子装置であってプロセッサおよびメモリを含む一般的な電子装置の機能を示すブロック図である。
【図３】本発明において構成されるメモリの各部分を示す図である。
【図４】本発明でインプリメントされるロジックを示すフローチャートである。
【符号の説明】
１００　電子ゲームシステム
１０２　ゲームコンソール
１０４ａ、１０４ｂ　コントローラ
１０６　ポータブル媒体ドライブ
１０８　光記憶ディスク
１１０　スロット
１１２　電源ボタン
１１４　イジェクトボタン
１２０　オーディオ／ビジュアルインタフェースケーブル
１２２　電源ケーブルプラグ
１２４　データコネクタ
１３０　ＵＳＢケーブル
１３２ａ、１３２ｂ　サムスティック
１３４　Ｄパッド
１３６　ボタン
１３８　トリガ
１４０　ポータブルＭＵ
２０２、２２０　ＣＰＵ
２０４　ＮＶ２Ａチップ
２０６　ＲＡＭ
２０８　ＭＣＰ
２１０　ＲＯＭ
２１２、２２２　ブートストラップコード
２３０　プリローダ
２３１　公開鍵
２３２　ブートローダ
２３４　デジタル署名
２３６　対称鍵
２３８　カーネル
２４０　チップセット初期化コード

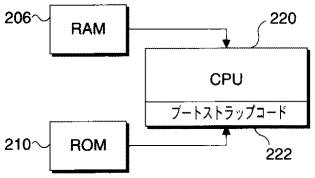
【図１】



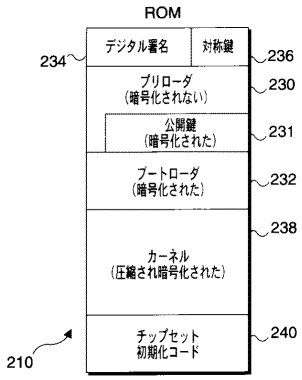
【図２Ａ】



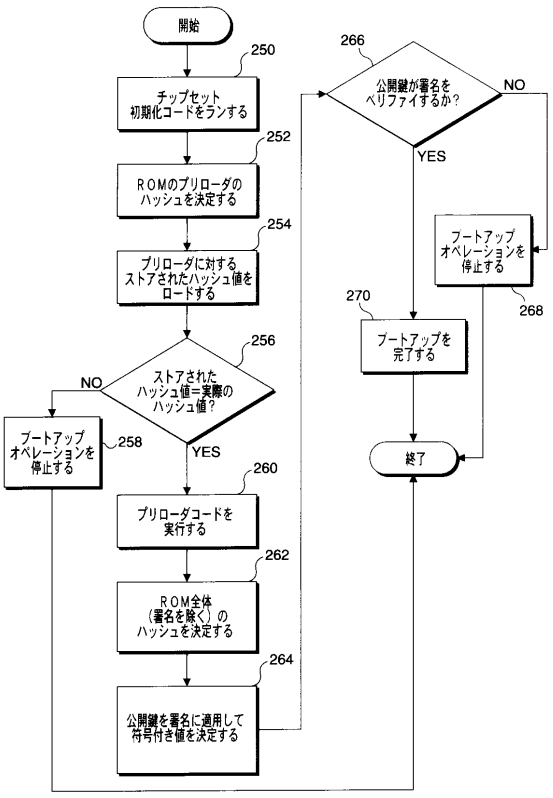
【図２Ｂ】



【図３】



【図４】



フロントページの続き

(72)発明者 ディナルト モレ
アメリカ合衆国 ９８０５２ ワシントン州 レッドモンド １６６ コート ノースイースト ４９５０
(72)発明者 ジョン ランジュ
アメリカ合衆国 ９８００５ ワシントン州 ベルビュー ノースイースト ２６ プレイス １２９２８
(72)発明者 ダン サイモン
アメリカ合衆国 ９８０５２ ワシントン州 レッドモンド ノースイースト ８３ ストリート １６３４０ ナンバーイー２２７
(72)発明者 リン トニー チェン
アメリカ合衆国 ９８００６－５９２２ ワシントン州 ベルビュー １７４ プレイス サウスイースト ５５３３
(72)発明者 ジョシュ ディー. ベナロー
アメリカ合衆国 ９８０５２ ワシントン州 レッドモンド １５９ コート ノースイースト ５０２８

審査官 平井 誠

(56)参考文献 特開２０００－３２２２５４（ＪＰ，Ａ）
国際公開第０１／０２４０１２（WO，Ａ１）
特開平１０－３３３９０２（ＪＰ，Ａ）
米国特許第０６１８５６７８（ＵＳ，Ｂ１）
米国特許第０６２６３４３１（ＵＳ，Ｂ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
G06F 21/22