(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4945454号
(P4945454)
(45)発行日　平成24年6月6日(2012.6.6)　(24)登録日　平成24年3月9日(2012.3.9)

(51)Int.Cl.　　F I
G06F 21/00 (2006.01)　　G06F 21/00　157A
G06F 11/30 (2006.01)　　G06F 11/30　310A

請求項の数 7　(全 15 頁)

(21)出願番号　特願2007-548385 (P2007-548385)
(86)(22)出願日　平成17年12月20日 (2005.12.20)
(65)公表番号　特表2008-525892 (P2008-525892A)
(43)公表日　平成20年7月17日 (2008.7.17)
(86)国際出願番号　PCT/US2005/046091
(87)国際公開番号　WO2006/071630
(87)国際公開日　平成18年7月6日 (2006.7.6)
審査請求日　平成20年12月18日 (2008.12.18)
(31)優先権主張番号　11/021,021
(32)優先日　平成16年12月23日 (2004.12.23)
(33)優先権主張国　米国 (US)

(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　100077481
弁理士　谷　義一
(74)代理人　100088915
弁理士　阿部　和夫
(72)発明者　アレクサンダー　フランク
アメリカ合衆国　９８０５２－６３９９　ワシントン州　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　コーポレーション内

最終頁に続く

(54)【発明の名称】モニタを用いてＴＰＭを常に“オン”にロックする方法及びシステム

(57)【特許請求の範囲】
【請求項１】
モニタのオペレーションを行使し、信頼されたコンピューティングベースを実装するコンピュータであって、
前記モニタを実行するプロセッサと、
前記プロセッサに接続され、汎用入出力ポートを備えた信頼された環境であって、所与のモニタ計測値を格納し、当該コンピュータに対する妨害を防ぐためのメッセージを前記モニタから受信すると、前記計測値に基づいて前記モニタを検証して前記汎用入出力ポートへのアクセスが許可されるか判断する、信頼された環境と、
期間を判断するためのタイマを有し、前記信頼された環境に接続されたウォッチドッグ回路であって、前記期間内に、前記信頼された環境または前記モニタから前記タイマをリスタートするためのリスタート信号を受信しない限り、前記期間後に前記コンピュータを妨害するウォッチドッグ回路と
を備え、前記信頼された環境は、前記モニタが前記汎用入出力ポートへのアクセスを許可されると判断したとき、前記リスタート信号を前記汎用入出力ポートから前記ウォッチドッグ回路に送信するか、前記メッセージに署名をして前記モニタに送信するように構成され、前記署名されたメッセージは、前記リスタート信号として前記モニタから前記ウォッチドッグ回路に送信されることを特徴とするコンピュータ。
【請求項２】
前記信頼された環境は、前記モニタが前記汎用入出力ポートへのアクセスを許可される

と判断したとき、前記モニタに前記汎用入出力ポートへのアクセス権を与えることを特徴とする、請求項１に記載のコンピュータ。
【請求項３】
前記信頼された環境は、前記ウォッチドッグ回路に専用通信線を介して接続されていることを特徴とする、請求項１に記載のコンピュータ。
【請求項４】
前記ウォッチドッグ回路は、前記コンピュータを妨害するとき、前記コンピュータをリブートさせることを特徴とする、請求項１に記載のコンピュータ。
【請求項５】
前記ウォッチドッグ回路は、前記コンピュータをリブートさせるための信号を、改ざんから保護された接続を介して送信することを特徴とする、請求項４に記載のコンピュータ。
【請求項６】
前記モニタは、前記メッセージを送信したあと、少なくとも一回、前記コンピュータが所定のポリシーを満たしているかどうかを判断し、前記所定のポリシーは、前記コンピュータが指定のアプリケーションプログラムを有していること、指定の周辺機器に接続されるべきこと、または指定の周辺機器に接続されていないことのうちの少なくとも１つを規定することを特徴とする、請求項１に記載のコンピュータ。
【請求項７】
コンピュータのオペレーションを制御するための方法であって、前記コンピュータは、プロセッサと、信頼された環境と、ウォッチドッグ回路とを備え、前記信頼された環境は、汎用入出力ポートを備え、および所与のモニタ計測値を格納し、前記ウォッチドッグ回路は、期間を判断するためのタイマを備え、前記方法は、
前記プロセッサがモニタを実行するステップと、
前記コンピュータのオペレーションを妨害するのを防ぐためのメッセージを前記モニタから前記信頼された環境に送るステップと、
前記信頼された環境において、前記メッセージを受信すると、前記計測値に基づいて前記モニタを検証して前記汎用入出力ポートへのアクセスが許可されるか判断するステップと、
前記信頼された環境において前記モニタは前記汎用入出力ポートへのアクセスが許可されると判断したとき、前記タイマをリスタートさせるためのリスタート信号を前記汎用入出力ポートから前記ウォッチドッグ回路に送信するか、前記メッセージに署名をして前記モニタに送信するステップと、
前記モニタが前記信頼された環境から前記署名されたメッセージを受信したとき、該受信した署名されたメッセージを前記リスタート信号として前記ウォッチドッグ回路に送信するステップと、
前記ウォッチドッグ回路が前記期間内に前記信頼された環境または前記モニタから前記リスタート信号を受信したとき、前記タイマをリスタートさせることで前記コンピュータのオペレーションを妨害するのを防ぐステップと
を含むことを特徴とする方法。
【発明の詳細な説明】
【背景技術】
【０００１】
パーソナルコンピュータなどのコンピューティング・デバイスに用いられるＴＰＭ(Trusted Platform Module)が知られている。ＴＰＭの目的は、コンピュータにアイデンティティを提供し、トランザクションや、アプリケーションやメディアのライセンシングや、ユーザデータの保護や、特殊な機能に関するサービスのセキュリティを確保することにある。
【発明の開示】
【発明が解決しようとする課題】

【０００２】
ＴＰＭは市販されており、例えば、ＳＴＭマイクロエレクトロニクスのＳＴ１９ＷＰ１８などから取得可能である。ＴＰＭは鍵を格納し、これらの鍵を用いてアプリケーションプログラムや、ＢＩＯＳ情報や、アイデンティティの認証をする。しかし、ＴＰＭの利用は任意のものであり、現行の及び今後予測される基準及び実施においては、コンピューティング・デバイスにある状態(condition)を要求するために利用することはできない。ビジネスモデルには、コンピュータがコンピュータの所有者、供給者の直接のコントロール外であると仮定するものもあり、例えば使用毎支払い（pay-per-use）ビジネスモデルである。このような場合においては、ＴＰＭサービスを回避することが可能であり、もし回避が起きると、ビジネスに望ましくない悪影響が及ぼされることがある。

【課題を解決するための手段】
【０００３】
ＴＰＭは、コンピューティング・デバイスに状態を強いる監視プログラムを認証するために用いることができる。ＴＰＭに注入されたまたは書き込まれたオーナー鍵は、オーナーによって許可されたモニタが作動可能であることを要求するために用いられる。その代わり、許可されたモニタは、その認証されてステータスにより、ＴＰＭのリソースにアクセスすることができる。このようなＴＰＭのセキュアなリソースとは、例えば汎用入出力（ＧＰＩＯ）ポートである。ＧＰＩＯで受信された信号によってウォッチドッグタイマが一定計時時間以内にリスタートされない限り、該一定計時時間後にコンピュータをリセットするように、簡単なウォッチドッグタイマを設定してもよい。
【０００４】
コンピュータをこのように設定することにより、知っているモニタが機能していることを確実にするためにＴＰＭを用い、モニタとＴＰＭとが不能化しておらず、かついたずらをされないことを確実にするためにウォッチドッグタイマを用いることができる。

【発明を実施するための最良の形態】
【０００５】
下記の文章は、数々の異なる実施例を詳述するものであるが、該記載の法的範囲はこの開示の最後に記す特許請求の範囲の文言によって定義されるべきであることが理解されよう。可能な実施形態の全てにつき記載することは不可能ではなくても非現実的であるので、本詳述は、例示としてのみ解釈されるべきであり可能な実施形態の全てを記載するものではない。現在の技術または本特許の出願日の後に開発される技術を用いて、本特許請求の範囲に該当する数多くの代替実施例が実施され得る。
【０００６】
また、本特許において「ここで用いられる『＿＿』という用語は、…を意味するとここにおいて定義される」という文章またはこれに類似した文章によって明示的に定義されない限り、用語の明らかなまたは通常の意味以上にその用語の意味を、明示的にも暗示的にも限定することを意図するものではなく、如何なる用語も、本特許のどの部分（特許請求の範囲を除く）に書かれた如何なる記載によってでも限定的に解釈されるべきではない。本特許の終わりの特許請求の範囲に記載された用語が、如何なる用語であっても一つの意味に一貫して本特許内で言及される限りにおいては、読者を混乱させないように明確さのためになされたものであって、その特許請求の範囲の用語を暗示または他の方法によってその一つの意味に限定することを意図するものではない。最後に、特許請求の範囲の要素が、構造を記載することなく「手段」という言葉及び機能によって定義されているのでなければ、如何なる特許請求の範囲の要素も、米国法３５ＵＳＣ１１２条の第６パラグラフを元に解釈されることを意図するものではない。
【０００７】
発明の機能の大部分及び発明の理論の多くは、ソフトウェアプログラムやインストラクションやＡＳＩＣ（Application Specific Integration Circuit）などの集積回路（ＩＣ）と共に、またはこれらによって最良に実施される。通常の能力を有する者は、ここに開示する概念や理論を手引きとすることにより、利用可能な時間や現在の技術や経済的状況

などによって動機付けられる多大であるかもしれない努力と多くの設計選択肢にも拘らず、そのようなソフトウェアインストラクションやプログラムやＩＣを最小の実験により作成することが十分に可能であることが期待される。従って、本発明に基づく理論、概念をあいまいにするリスクを最小化し、簡潔化するため、このようなソフトウェア、ＩＣに関する更なる議論は、仮にあるとすれば、望ましい実施形態の理論及び概念に比して必要なものに限定されている。

【０００８】

図１は、ダイナミックソフトウェア提供システムを実施するのに使われるネットワーク１０を図示している。ネットワーク１０は、インターネット、バーチャルプライベートネットワーク（ＶＰＮ）、または一つまたはそれ以上のコンピュータ、通信デバイス、データベースなどを互いに通信可能に接続する如何なる他のネットワークであってもよい。ネットワーク１０は、パーソナルコンピュータ１２とコンピュータ端末１４とに、イーサネット（登録商標）接続子(Ethernet（登録商標） connection)１６と、ルータ１８と、地上線２０とを介して接続されている。一方、ネットワーク１０は、ラップトップコンピュータ２２とパーソナルデジタルアシスタント２４とに、ワイヤレス通信局２６とワイヤレスリンク２８とを介して接続されている。同様に、サーバ３０は通信リンク３２を用いてネットワーク１０に接続され、メインフレーム３４は別の通信リンク３６を用いてネットワーク１０に接続されている。

【０００９】

図２はコンピューティング・デバイスをコンピュータ１１０として図示する。コンピュータ１１０の構成要素には、処理部１２０と、システムメモリ１３０と、システムバス１２１とが含まれるが、これらに限定されるものではない。システムバス１２１は、システムメモリを含む様々なシステム構成要素を処理部１２０に結合する。システムバス１２１は、メモリバスまたはメモリコントローラ、周辺バス、多数のバスアーキテクチャのいずれかを用いたローカルバスを含む、いくつかの種類のバス構造のいずれであってもよい。限定でなく例として、そのようなアーキテクチャにはＩＳＡ(Industry Standard Architecture)バスと、マイクロチャネルアーキテクチャ（ＭＣＡ）バスと、ＥＩＳＡ（Enhanced ISA）バスと、ビデオエレクトロニクス標準協会（ＶＥＳＡ）ローカルバスと、メザニンバスとしても知られているＰＣＩ(Peripheral Component Interconnect)バスとを含む。

【００１０】

コンピュータ１１０は、多様なコンピュータ読み込み可能なメディアを典型的に含む。コンピュータ読み込み可能なメディアは、コンピュータ１１０がアクセス可能な如何なる利用可能なメディアでもよく、揮発性及び不揮発性メディア、取り外し可能及び取り外し不能メディアの両方を含む。限定でなく例として、コンピュータ読み取り可能メディアは、コンピュータ格納メディアと通信メディアとを含む。コンピュータ格納メディアは、コンピュータ読み込み可能インストラクションやデータ構造やプログラムモジュールまたは他のデータなどの情報の格納のための如何なる方法または技術によって実施され得る、揮発性及び不揮発性メディア、取り外し可能及び取り外し不能メディアをも含む。コンピュータ格納メディアは、ＲＡＭ、ＲＯＭ、ＥＥＰＲＯＭ、フラッシュメモリまたはその他のメモリ技術、ＣＤ－ＲＯＭ、ＤＶＤまたはその他光ディスクストレージ、磁気カセット、磁気テープ、磁気ディスクストレージまたはその他の磁気格納デバイス、または望みの情報を格納しコンピュータ１１０でアクセスし得るその他の如何なる媒体をも含むが、これらに限定されるものではない。通信メディアは、典型的には、コンピュータ読み取り可能インストラクション、データ構造、プログラムモジュールまたは他のデータを、搬送波または他のトランスポート機構などの変調されたデータ信号により実現し、如何なる情報伝達メディアをも含む。「変調されたデータ信号」とは、信号中に情報を符号化するようにその特徴の一つまたは複数を設定または変更した信号を意味する。限定でなく例として、通信メディアは有線ネットワークまたは直接有線接続などの有線メディアや、音響、ラジオ周波数、赤外線及び他の無線メディアなどの無線メディアを含む。コンピュータ読み取り可能なメディアの範囲には、上記の如何なる組み合わせも含まれるべきである。

【００１１】
システムメモリ１３０は、リードオンリーメモリ（ＲＯＭ）１３１やランダムアクセスメモリ（ＲＡＭ）１３２などの揮発性及び／または不揮発性メモリの形をとるコンピュータ格納メディアを含む。スタートアップの間などに、コンピュータ１１０内の要素間の情報伝達を助ける基本ルーチンを含むベーシックインプット／アウトプットシステム（ＢＩＯＳ）１３３は、典型的にはＲＯＭ１３１に格納されている。ＲＡＭ１３２は、処理ユニット１２０によってすぐにアクセス可能または処理ユニット１２０に現在用いられているデータ及び／またはプログラムモジュールを典型的には含む。限定でなく例として、図１はオペレーティングシステム１３４、アプリケーションプログラム１３５、その他プログラムモジュール１３６、プログラムデータ１３７を図示している。

【００１２】
コンピュータ１１０は、その他の取り外し可能及び取り外し不能、揮発性及び不揮発性コンピュータ格納メディアも含んでいてよい。例としてのみ、図１は、取り外し不能不揮発性磁気メディアに読み書きするハードディスクドライブ１４１と、取り外し可能揮発性磁気ディスク１５２に読み書きする磁気ディスクドライブ１５１と、ＣＤＲＯＭや他の光メディアなどの取り外し可能不揮発性光ディスクに読み書きする光ディスクドライブ１５５とを図示している。例示のオペレーティング環境において用いることのできる他の取り外し可能及び取り外し不能、揮発性及び不揮発性コンピュータ格納メディアには、磁気テープカセット、フラッシュメモリカード、ＤＶＤ，デジタルビデオテープ、ソリッドステートＲＡＭ、ソリッドステートＲＯＭなどを含まれるが、これらに限定されるものではない。ハードディスクドライブ１４１は、典型的にはインタフェース１４０などの取り外し不能メモリインタフェースを通してシステムバス１２１に接続されており、磁気ディスクドライブ１５１と光ディスクドライブ１５５は、典型的にはインタフェース１５０などの取り外し可能メモリインタフェースによりシステムバス１２１に接続されている。

【００１３】
上述され図２に図示されたドライブとそれらに関連するコンピュータ格納メディアは、コンピュータ読み取り可能なインストラクション、データ構造、プログラムモジュール、及びコンピュータ１１０のためのその他データの格納部を提供する。図１では、例えば、ハードディスクドライブ１４１が、オペレーティングシステム１４４、アプリケーションプログラム１４５、その他プログラムモジュール１４６、プログラムデータ１４７を格納するものとして図示されている。これら構成要素は、オペレーティングシステム１３４、アプリケーションプログラム１３５、その他プログラムモジュール１３６、プログラムデータ１３７と同じでも異なっていてもよいことに注意されたい。ここでは、オペレーティングシステム１４４、アプリケーションプログラム１４５、その他プログラムモジュール１４６、プログラムデータ１４７は、異なるコピーであることを少なくとも示すために異なる番号を与えられている。ユーザは、キーボード１６２と、一般にマウス、トラックボール、またはタッチパッドと呼ばれるポインティングデバイス１６１となどの入力デバイスによって、コンピュータ２０にコマンドや情報を入力する。その他の入力デバイス（図示せず）には、マイクロフォン、ジョイスティック、ゲームパッド、サテライトディッシュ、スキャナなどが含まれる。これらの、またその他の入力デバイスは、システムバスに結合されたユーザインタフェース１６０を介して処理ユニット１２０に接続されていることが多いが、パラレルポート、ゲームポート、ユニバーサルシリアルバス（ＵＳＢ）などの他のインタフェースやバス構造によって接続されていてもよい。陰極線管１９１または他の種類のディスプレイデバイスも、ビデオインタフェース１９０などのインタフェースを介してシステムバス１２１に接続されている。モニタに加えてコンピュータはさらに、外部周辺インタフェース１９０を介して接続されたスピーカ１９７やプリンタ１９６などの、他の周辺出力デバイスを含んでもよい。

【００１４】
コンピュータ１１０は、ネットワーク化された環境の中で、リモートコンピュータ１８０などの一つまたは複数のリモートコンピュータへの論理接続を用いて作動する。リモー

トコンピュータ１８０は、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、または他の一般的なネットワークノードでよく、図１にはメモリ格納デバイス１８１しか図示されていないものの、典型的には、コンピュータ１１０に関連して上述された要素の多くまたは全てを含んでいる。図１に図示された論理接続は、構内通信網（ＬＡＮ）１７１と、広域通信網（ＷＡＮ）１７３とを含むが、他のネットワークをさらに含んでも良い。このようなネットワーキング環境は、オフィスや企業ワイドコンピュータネットワーク、イントラネット、インターネットにはよく見られる。

【００１５】

LANネットワーキング環境で用いられるとき、コンピュータ１１０はネットワークインタフェースまたはアダプタ１７０を介してLAN１７１に接続されている。WANネットワーキング環境で用いられるとき、コンピュータ１１０は典型的には、モデム１７２、またはインターネットなどのWAN１７３上で通信を設立するための他の手段を備えている。モデム１７２は、内蔵でも外付けでもよく、ユーザインプットインタフェース１６０または他の適当な機構を介してシステムバス１２１に接続されている。ネットワークされた環境においては、コンピュータ１１０に関連して図示されたプログラムモジュール、またはその一部は、リモートメモリ格納デバイスに格納されていてよい。限定としてではなく例として、図１にはメモリデバイス１８１に存するリモートアプリケーションプログラム１８５が開示されている。

【００１６】

通信接続１７０、１７２は、デバイスが他のデバイスと通信できるようにする。通信接続１７０、１７２は、通信メディアの一例である。通信メディアは典型的には、搬送波または他の伝送機構のような変調されたデータ信号中のコンピュータ読み取り可能なインストラクションや、データ構造や、プログラムモジュールや、他のデータを具現し、如何なる情報配達メディアをも含む。「変調されたデータ信号」とは、信号中に情報を符号化するようにその特徴の一つまたはそれ以上を設定または変更した信号である。限定としてではなく例として、通信メディアには、有線ネットワークまたは直接有線接続などの有線メディアや、音響、RF,赤外線及びその他の無線メディアなどの無線メディアが含まれる。コンピュータ読み取り可能なメディアには、格納メディアと通信メディアとが共に含まれる。

【００１７】

下記に詳述する、TPM１２５または他の信頼された環境は、データと鍵を格納し、実行可能なコードとデータを検証する。TPMの仕様書は、セクション４，５，２，１に「システム初期化の一部として、プラットフォームの構成要素の計測及び設定が行われる。計測によって安全でない設定を検知することはできず、さらに初期化プロセスの継続を防止するための作用を行うこともしない。この責任は、オペレーティングシステムなどの適当なレファレンスモニタが負う。」と記している。TPMは、行使ツールとして定義されていないため、以下に記す追加事項は一般的なTPMを補足する。

【００１８】

ウォッチドッグ回路１２６は、時間を計測し、期限が切れるとコンピュータ１１０のオペレーションを妨害するシグナル１２７をトリガするよう設定されている。この妨害は、コンピュータ１１０を再起動させる、システムリセットであってよい。この妨害により、システムバス１２１または周辺バスにあるデータが遮断される。ウォッチドッグ１２６が、コンピュータ１１０のオペレーションを妨害しないよう、期限をリセットし計時処理をやり直す信号が通信接続１２８上に要求される。図２に示すように、ウォッチドッグタイマリセット信号が通信接続１２８上に伝播される。以下に詳述するように、TPM１２５は、モニタプログラムからの信号に応答してウォッチドッグタイマリセットを開始してもよい。以下に記すステップは、TPM１２５とウォッチドッグ回路１２６との組み合わせを用いることによって、特定の希望のモニタが存在し作動していることを確実にする手助けとして用いられる。

【００１９】

図３には、図２のような代表的なコンピュータの中の機能層の階層的な表現を示す簡単化されたブロック図が説明及び記載されている。TPM２０２は、基礎入出力構造（BIOS）２０４の下に存するハードウェアである。TPM２０２は、コンピュータおよびBIOS２０４などの高層のオペレーションにとってのリソースとして機能する。BIOSはモニタ２０４を作動させる。モニタ２０６は、オペレーティングシステム２０８の下のモニタレベル２１０に存する。モニタ２０６は、ＴＰＭ２０２にアクセスしそのリソースを用いて高レベルのエンティティのオペレーションに関するポリシーを実行する。オペレーティングシステム２０８は、コンピュータ１１０の主要な機能をサポートし、（最初のブートストラップ処理ハンドオーバー制御の後は）通信、ユーザ入出力、ディスク及び他のメモリアクセス、アプリケーション開始などの責任を持つ。オペレーティングシステムは、TPM２０２に直接アクセスしTPM２０２を使用することもできる。図示されているように、第１および第２アプリケーション２１２、２１４はオペレーティングシステム２０８上で実行される。場合によっては、モニタはオペレーティングシステム２０８及びアプリケーション２１２、２１４の両方に関連するポリシーを行使する。例えば、アプリケーション２１４がディスク２１６から実行される前に、オペレーティングシステムは、線２１８で示されるようにライセンスの状態をチェックし、アプリケーション２１４が与えられた実行開始基準を満たしているかを判断する。モニタ機能を用いた、実行開始及び以後のアプリケーションのメータリングの基準は、代理人事務所番号30835/40476の2004年12月8日出願の米国特許出願「進行型支払い(Pay-As-You-Go)コンピュータ及び動的相対的価格付け(Dynamic Differential Pricing)の方法」に詳細に述べられている。簡単に言うとモニタ２０６は、例えばアプリケーションプログラムやユーティリティやコンピュータリソースを、進行型支払いまたは前払いのシナリオにおいて計測しメータするために用いられる。

【００２０】

図６を簡単に参照して、TPM２０２についてより詳細に述べる。TPM２０２は、揮発性及び不揮発性のメモリを共に有する内蔵メモリ５０２を有し、そのうちの少なくとも一部は改ざんや権限の無い者による書き込み操作などから保護されている。メモリはオーナー鍵５０４を格納し、オーナー鍵５０４は、TPM２０２を設定し外部の存在と信頼関係を確立する目的で、オーナーとの関係を主張するエンティティを確認するのに用いられる。メモリには、他のものに加えてさらに、プラットフォーム設定レジスタ(PCR: Platform Configuration Register)５０６が含まれている。PCR５０６は、ハッシュまたはモニタ２０６と関連付けられた他の強い識別子を格納するのに用いられる。TPM２０２は、時計５０８及び暗号サービス５１０をさらに備えている。これらは共に、以下により詳細に述べるように、認証および権限付与プロセスに用いられる。TPM２０２はさらに、シングルピンバス(Single-pin bus)または汎用入出力（GPIO）としてときに言及されるバス５１２をさらに備える。一つの実施例では、他箇所に記載の通り、GPIO５１２はウォッチドッグ回路に接続される。

【００２１】

TPM２０２は、モニタ５２６を実行する処理などのコンピュータ内のデータ通信のために、汎用バス５１４に接続されている。バス５１４または場合によっては他の機構５１６を用いて、TPM２０２はモニタを計測することができる。モニタの計測には、モニタの暗号ハッシュのチェック、つまりモニタによって占用されているメモリ領域のハッシュのチェックが含まれる。計測データ５０６を格納するのにPCRが用いられてもよい。オーナー鍵５０４は、例ばモニタのデジタル署名されたハッシュで確認にオーナー鍵５０４を要求するものによって、モニタ５０６のハッシュと関係付けられている。オーナー鍵５０４は、製造時またはその後、例えば顧客への配送時などに、TPM２０２に書き込まれる、または注入される。そしてオーナー鍵５０４は、モニタ２０６を認証するのに用いられる。

【００２２】

例示の実施形態では、モニタ２０６は、ブートシークエンスでそれに先行する信用されたモジュール、例えばBIOS２０４によって計測される。モニタの計測、例えばBIOS２０４によって計算されるハッシュなどは、バス５１４を介してTPM PCR５０６に格納される。T

PM２０２が計測（ハッシュ）を確証するとき、TPM２０２は、モニタ２０６に割り当てられTPM２０２に格納された一意の鍵及び／または他の秘密のモニタ２０６へのアクセスを許可する。TPM２０２は、如何なるモニタにも対応する鍵と秘密とを、そのモニタの計測値に応じた計測値によって割り当てる。

【００２３】

TPMは、対応するモニタメトリック５０９、例えば知られたモニタ２０６のハッシュなどと、オーナー鍵５０４とでプログラムされている。オーナー鍵は、モニタメトリック５０９をプログラムまたは更新するのに用いられ、オーナー鍵５０４を有するエンティティだけが知られたモニタ２０６のPCRレジスタ５０６を設定し得るようにする。標準的なTPM２０２には、与えられた計測値５０６に対して検証されたモニタ２０６のみがGPIO５１２を制御できるという特徴がある。GPIO５１２が、改ざんから保護されつつウォッチドッグ回路１２６に接続されているとき、信頼の鎖が完成される。つまり、検証されたモニタ２０６のみがGPIO５１２を制御してよく、GPIO５１２のみがウォッチドッグ回路１２６をリスタートすることができる。従って、モニタ２０６が交換されたり変更されたりしても、オーナー鍵５０６が設定したPCR５０６によって検証されたモニタ２０６のみがウォッチドッグ回路１２６をリスタートするのに用いられ得る。従って、権限を付与されたモニタのみが、ウォッチドッグがコンピュータ１１０をリセットするなどによりコンピュータ１１０を妨害するのをやめさせるのに用いられ得る。ウォッチドッグ回路１２６のタイマは、コンピュータ１１０の変造、改ざんの回復は可能であるがコンピュータ１１０で有意義な実用的作業をするのを妨げるに十分な短さとなるよう選択された期間に設定される。例えばウォッチドッグは、確証されたモニタ２０６がリスタートしない限り、コンピュータ１１０を１０から２０分おきに妨害するよう設定される。

【００２４】

オーナー秘密とモニタ計測値５０６とは、安全な製造環境においてプログラムされてもよいし、オーナー鍵５０４をプログラムするエンティティに知られているトランスポート鍵を用いてフィールドプログラムされてもよい。オーナー鍵５０４が知られると、サービスプロバイダなどのプログラミングを行うエンティティは、どのモニタがGPIOバスへのアクセス権を与えられるかを決定するモニタ計測値を設定する。オーナー鍵を再プログラムするには、オーナー鍵５０４が要求される。生成された鍵を使うことによって、鍵の分配や、ローカルのオーナー鍵５０４が侵害された場合の広範な喪失からの保護やスケーリングを容易にする。鍵管理技術は、データセキュリティの分野では公知である。

【００２５】

図４は、コンピュータ１１０と同じまたは類似のコンピュータ３００の代表的アーキテクチャのブロック図である。コンピュータは第1および第2インタフェースブリッジ３０２、３０４を有している。インタフェースブリッジ３０２，３０４は高速３０６バスによって接続されている。第1インタフェースブリッジはプロセッサ３０８と、グラフィックコントローラ３１０と、メモリ３１２とを接続されている。メモリ３１２はモニタプログラム３１４や他の一般的なメモリ使用をホストする。

【００２６】

第2インタフェースブリッジ３０４は、例えばユニバーサルシリアルバス（USB）３１６、IDE（Integrated Drive Electronics）３１８、または周辺装置相互接続（PCI: Peripheral Component Interconnect）３２０などの、ディスクドライブやプリンタやスキャナなどに接続するために用いられる、周辺バス及び構成要素に接続される。第2インタフェースブリッジはTPM３２２にも接続されている。上述のように、TPM３２２は、鍵及びハッシュデータのための安全なメモリ３２４と、汎用入出力（GPIO）３２６とを備えている。TPM３２２は、接続３２８によって物理的にまたは論理的にモニタに連結されている。既述の通り、BIOS２０４はモニタ２０６を計測し、計測値をTPM３２２に格納し、TPM３２２は、提供された計測値に応じてモニタ314に鍵及び秘密を割り当てる。こうしてモニタ３１４はこれらの鍵及び秘密でロックされたリソース及びデータへのアクセス権を与えられる。接続３２８は、ウォッチドッグ回路３３０に信号を送る目的で、モニタによってGPIO

３２６を制御するために用いられてよい。信号は、ウォッチドッグをリセットさせる。信号が、ウォッチドッグ回路３３０の設定で禁止(proscribe)されている期間に、ウォッチドッグ回路３３０によって受信されなかったとき、リセットまたは他の妨害的信号が接続３３２を介して送信される。改ざんを抑えるために、GPIO３２６とウォッチドッグ回路３３０との間の接続は、ウォッチドッグ回路３３０の手動再起動を抑止するため、例えば回路基盤層間のポッティング(potting)やルーティングによって保護されている。コンピュータリセット信号接続３３２は同様に改ざんから保護されており、またはコンピュータリセット信号接続３３２のウォッチドッグ回路３３０とメインプロセッサコンピュータリセット点（図示なし）の間の少なくとも一部が同様に保護されている。

【００２７】

図５は、図２のコンピュータの代替アーキテクチャのブロック図である。図４の記載に比較して同様の番号を付された構成要素は同じである。ウォッチドッグ回路３３０は第2インタフェースブリッジ３０４内に移動されており、ウォッチドッグ回路３３０が改ざん耐久性向上のために如何に他の回路に組み合わされ得るかを示している。ウォッチドッグ回路３３０の第2インタフェースブリッジ３０４への組み合わせは、それ自体適当なものであるが、事例にすぎない。第2インタフェースブリッジ３０４はコンピュータアーキテクチャの主要な構成要素であるので、望みのレベルの妨害を第2インタフェースブリッジ３０４の内部から実行することができる。従って、接続３３２のような、第2インタフェースブリッジ３０４の外側のウォッチドッグ回路３３０からの接続を必要としない。

【００２８】

この代替実施形態では、GPIO３２６がリセットの信号をウォッチドッグ回路３３０に送るために用いられることはない。代わりに、メッセージが論理接続３３４上モニタ３１４からウォッチドッグ回路３３０に直接送信される。

【００２９】

２つのエンティティ（３１４、３３０）の間に十分な信頼が存在しないので、メッセージはTPM３２２で保持された鍵を用いて書名される。例えばこれらの鍵は、第1ブートの間（例えば、製造ライン上で－信頼性のため）モニタ３１４と関連付けられている。鍵は、任意に割り当てられてよく、または、上述のように、ルート認証、シリアル番号または製造シークエンス番号などの知られたデータとマスター鍵とから階層的に生成されてもよい。ウォッチドッグタイマ３３０は、例えばアセンブリラインにおけるコンピュータ１１０の最初のブートの間、これらの鍵を用いて書名されたメッセージのみを尊重するように設定される。さらに、モニタはこれらの鍵をTPM３２２にロックし、同一の計測値を持つモニタ３１４のみがこれらの鍵にアクセスできるようにしてもよい。このアーキテクチャの変形例では、これらの鍵が計測値に応じてそれぞれ一意になるようにモニタに分配されるよう、モニタがTPM３２２に依存している。

【００３０】

通常のオペレーションの間、モニタ３１４は、ウォッチドッグ回路３３０に送信するメッセージに自分のために署名するよう、TPM３２２に要求する。TPM３２２は、モニタ３１４に対応する鍵（ブートの度にBIOSによってTPM３２２に格納される、その計測値に基づいて）でメッセージに署名する。モニタ３１４は、署名されたメッセージをTPM３２２から、例えば接続３２８などの論理接続を介して署名されたメッセージを受け取り、論理接続３３４を介してウォッチドッグ回路３３０にそれを提供する。

【００３１】

ウォッチドッグ回路３３０がメッセージを受け取ると、ウォッチドッグ回路３３０は鍵（製造過程で設定されたもの）を用いてメッセージを認証する。若しくは、TPM３２２内の鍵または秘密を用いての検証を、論理接続３３６を用いて要求してもよい。別のモニタが実行している場合、その計測値は異なるため、TPMは異なる鍵及び秘密を割り当てる結果となる。従って別のモニタは、ウォッチドッグ回路３３０に認証されるようにメッセージに適格に署名することができない。結果としてウォッチドッグ回路３３０は、コンピュータ１１０のタイミングインターバル期間終了の後にリセットを発するなどの制裁措置を

開始する。署名されたまたは暗号化されたメッセージを使うことによって、論理接続３２８、３３４への攻撃の機会を減らすことができる。

【００３２】

モニタを使ってTPMを常に「オン」にロックする方法を図示する図７のフローチャートについて、記載及び既述する。典型的なTPM,例えばTPM１２５が、ユーザによって任意に有効にされていてもよい。後述のようにこの方法は、コンピュータ１１０の無能化などの制裁により、TPM１２５が有効な状態を保ち、かつビジネスのオーナーに選択されたモニタ２０６が実行されることを確実にする助けとなる。

【００３３】

スタート４０２における電源入力に始まって、コンピュータ１１０は通常のブート機構によって様々なハードウェア構成要素を起動する。これはTPM３２２にも適用される。ブートシークエンスはTCPA(Trusted Computing Platform Alliance)の方法に従ってもよい。CRTM (Core Root of Trusted Measurements)（図示なし）はBIOS１３３を計測し、その計測値をTPM３２２に格納（４０３）する。そして、CRTMはBIOS１３３をロードし実行する。（CRTMは、理想的には、攻撃が困難なコンピュータ内の信頼のおける位置に格納される。）

【００３４】

BIOS１３３は、従来のように実行されてよく、種々のコンピュータ構成要素を起動し列挙するが、一つ例外がある－BIOS１３３は、各ソフトウェアモジュールをロードし実行する前に計測する。さらにBIOS１３３は、これらの計測値をTPM３２２に格納する。特にBIOS１３３は、モニタ３１４を計測し、モニタの計測値をTPM３２２に格納する（４０５）。

【００３５】

TPM３２２は、鍵と秘密とをモニタ計測値それぞれに一意的に割り当てる（４０８）。大事なのは、TPM３２２が鍵及び秘密を与えられた計測値に対して一貫して一意的に割り当てる（４０８）ことである。結果的に、モニタ３１４が利用できる秘密はそれぞれ一貫して一意的である。その結果、如何なるモニタでも、そのモニタだけが独占的に利用できるよう、リソースをロックすることができる。例えばこれにより、ウォッチドッグ回路３３０に接続されたGPIO３２６が正真正銘のモニタ３１４と関連付けられた計測値のみを尊重するようにGPIO３２６をプログラムすることによって、正真正銘のモニタ３１４をウォッチドッグ回路３３０に連結することができるようになる。GPIO３２６はこれにより、正真正銘のモニタ３１４と同一の計測値を持つモニタにのみ利用可能となる。

【００３６】

ロードされたモニタが正真正銘であるか否かに関わらず、ブートシークエンスはモニタをロードし実行する（４１０）。通常のブートプロセスを継続し（４１１）、ブートが成功したと仮定して、コンピュータ１１０の通常のオペレーション（４１２）が続く。

【００３７】

モニタ３１４が４１０においてロードされ実行されるとすぐに、モニタ３１４はそのループを開始する（４１３－４１９）。初めに、モニタ３１４はTPM GPIO３２６を介してウォッチドッグ回路３３０にメッセージを送信する（４１３）。メッセージは、TPM３２２に対し、タイマ（図示なし）をリスタートするようにウォッチドッグ回路３３０に信号を送るのにGPIO３２６を使用するよう、信号を送る。

【００３８】

メッセージをTPM３２２に送った後、モニタはテスト状態４１４に戻る。モニタは、コンピュータ１１０の状態が現行のポリシーを遵守していることをテスト（４１４）する。現行のポリシーとは、知られたプログラムやユーティリティや周辺機器の具体的な存在または非存在に関係していてよい。テストはまた、メータリングやまたは他の使用毎支払いメトリクスに関連していてもよい。例えばテストは、特定のアプリケーションプログラムオペレーションでなく消費のために利用可能な消費用提供パケットをチェックしてもよい。別の実施形態においては、テストはカレンダー月など、特定の期間におけるオペレーションに関するものでもよい。

【００３９】
テストが失敗すると、No肢に続いて４１６があり、モニタはポリシーに従って行動する。この行動は、オペレーティングシステムに対して送る警告コードのみか、ユーザに示す警告メッセージでもよい。オペレーティングシステム及びユーザに対する何らかの制裁、例えばコンピュータの特定の機能を限定するまたは消去するといったものでもよい。これは、ハードウェア及び／またはソフトウェアの機能に適用される。例えば、コンピュータが遅くなったり、特定のソフトウェアを使用不能にしたり、ウェブカムなど特定のデバイスを使用不能にしたりする。より厳しい制裁としては、OSが利用できるRAMの量を制限する、オペレーティングシステムが利用できるInstruction-Set-Architectureを減少させることである。例示の実施形態では、遵守しない状態が発見されたときにモニタ３１４が取りえる行動としては、ウォッチドッグ回路３３０のタイマをリスタートする行動を取らずにウォッチドッグ回路３３０に制裁を加えさせることである。

【００４０】
テストが成功すると、４１４からYes肢をたどる。いずれの場合にしても、実行はステップ４１３に戻る前にある期間待つ（４１９）。待ち期間により、モニタ３１４を繰り返し実行することによるコンピュータリソースの使い果たしを避ける。明らかに、この待ち期間４１９はウォッチドッグタイマの計測期間に比してごく短い期間である。使用できるごく短い期間の決定は、コンピュータの通常のオペレーションがループの実行完成を遅らせる見込みによる。そしてループは上述のステップ４１３に戻る。ループを繰り返す期間は、ウォッチドッグ回路のタイムアウト期間より短ければどのような時間でもよく、さもなければ不当な妨害が起きてしまう。

【００４１】
TPM３２２がメッセージを受信する（４２０）と、TPM３２２はモニタ計測値に従って行動する。もし計測値が正真正銘ではないと判断されると、４２０が失敗し、ボックス４２２へのNo肢が取られる。ボックス４２２は何の行動も取らず、つまり、ウォッチドッグ回路３３０への信号は送られない。ウォッチドッグ回路３３０がコンピュータ１１０を妨害するのを阻止する手段が取られない限りウォッチドッグ回路３３０はコンピュータ１１０を妨害するので、TPM３２２それ以上行動を取る必要がない。オプションとして、TPM３２２は４２２で、ログ用のエラーを生成し、警告／エラーコードを生成し、オペレーティングシステムに通知し、及びメッセージをユーザに表示してもよい。

【００４２】
TPM３２２が、モニタ計測値が正真正銘であることを検証すると、GPIO３２６は起動されウォッチドッグ回路３３０に対してタイマをリスタートするよう信号４２４を送る。上述のように、ウォッチドッグ回路タイマをリスタートすることにより、コンピュータ１１０をリセットするなどの妨害的行動をウォッチドッグ回路３３０が開始することが妨げられる。ウォッチドッグ回路３３０はそして、初期値においてタイマをリスタート４２６する。タイマはそして、予め決められた期間が切れるまでタイマのカウント（４２８）及びテスト（４３０）を行う。タイマの期間は設定可能である。タイマの実施は公知であり、タイマが所定の数値まで下から数えるか、上から数えてゼロにするか、設定された時計の時間に応じて数えるか、またはその他の機構によるかは、設定選択事項である。

【００４３】
タイマの時間が切れていなければ、４３０からNo肢をたどって４２８に戻り、タイマから再びカウントを始める。時間が切れれば、４３０からYes肢をたどり、ウォッチドッグはコンピュータを妨害する（４３２）ことにより制裁を実行する。妨害とは、システムリセットや、リブートさせることや、周辺機器を不能化することなどである。ウォッチドッグ回路タイマがカウントダウンして妨害４３２するまでの期間は、ユーザがコンピュータ１１０の非遵守状態を矯正するに十分な時間であっても、コンピュータ１１０の信頼できるまたは有効な行動を制限するに十分なほど頻繁でなければならない。

【００４４】
４３２から４２６へのリンクは概念的なものである。妨害がコンピュータ全体のリセッ

トによって実施されれば、このリンクは無為である。コンピュータを遅くするなど、より微妙な妨害の場合は、カウントダウンをリスタートするのにこのリンクが用いられ、リセットさせるなどのより支障をきたすような妨害をする。

【００４５】

上記の方法により、利用毎支払いベースでコンピュータを供給に関連する事業のオーナーまたは他のスポンサーの目的を２つ達成することができる。第1に、ユーザがTPM３２２を使わないことを選択した、またはTPM３２２を不能化するようコンピュータをハックしたことによりTPM３２２が不能化されると、ウォッチドッグ回路３３０へのメッセージは生成されず、コンピュータ１１０が妨害される。

【００４６】

同様に、もしTPMが可動化され作動しているときでも、モニタが変更または取り替えられて有効であるポリシー（使用ポリシーなど）を変更または無視するようになると、TPMはモニタからの要求を尊重しなくなる。実際、変更されたモニタ計測値は正真正銘のモニタの計測値とは異なる。結果的に、モニタ計測値がTPM３２２に格納されている場合、TPM３２２は、それぞれ一意な鍵及び秘密のセットを変更されたモニタに割り当て、これらはGPIO２６のオペレーションに必要となるものとは異なる。この結果、GPIO３２６に信号を送ろうとする変更されたモニタからTPMへの如何なるメッセージも尊重されない。従って、ウォッチドッグ回路３３０はリスタート信号を受信せず、コンピュータ１１０が妨害される。

【００４７】

いずれの場合でも、コンピュータ１１０の正しいオペレーションのためには、TPM３２２は可動化されていなければならず、正真正銘のモニタがあって作動していなければならない。

【００４８】

上記方法及び装置の他の使用方法が考え得る。例えば、ブートプロセスの一部が権限を受けたユーザからの信用証明を要求してもよい。もし正しい信用証明が提示されなければ、ブートプロセスは正真正銘のモニタをロードせず、最終的にはコンピュータ１１０の不能化につながる。

【図面の簡単な説明】

【００４９】

【図１】複数のコンピュータリソースを互いに接続するネットワークのブロック図である。

【図２】開示の実施形態に係るコンピュータを示す、簡易化された代表的ブロック図である。

【図３】図２のコンピュータ内の機能層の階層的表示を示す、簡易化された代表的ブロック図である。

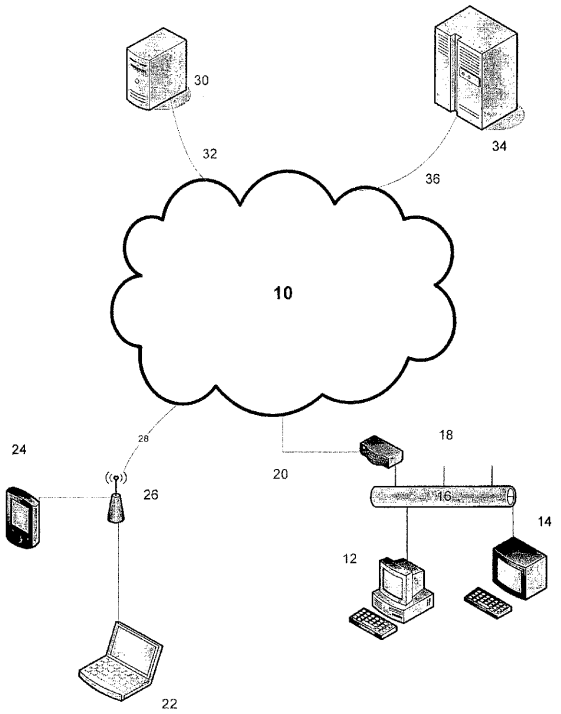
【図４】図２のコンピュータのコンピュータアーキテクチャの、簡易化された代表的ブロック図である。

【図５】図２のコンピュータの代替コンピュータアーキテクチャの、簡易化された代表的ブロック図である。

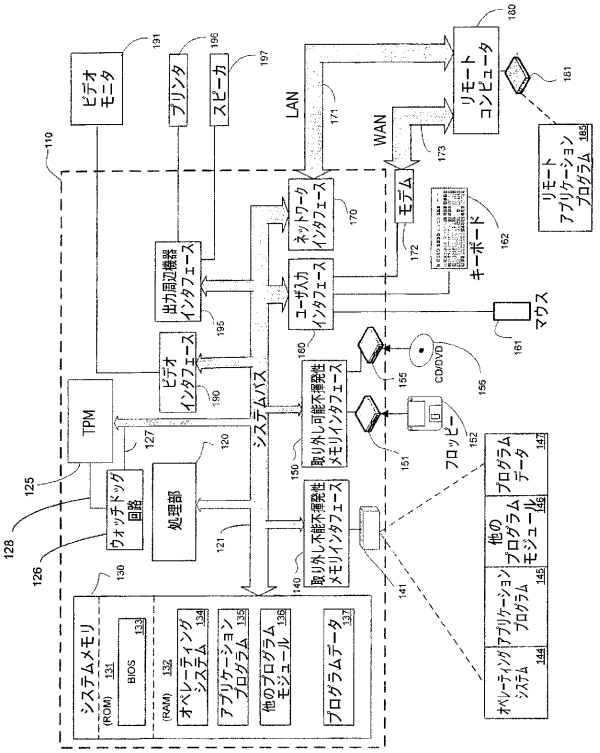
【図６】TPMの簡易化された代表的ブロック図である。

【図７】モニタを用いてTPMをロックオンする方法を示すフローチャートである。

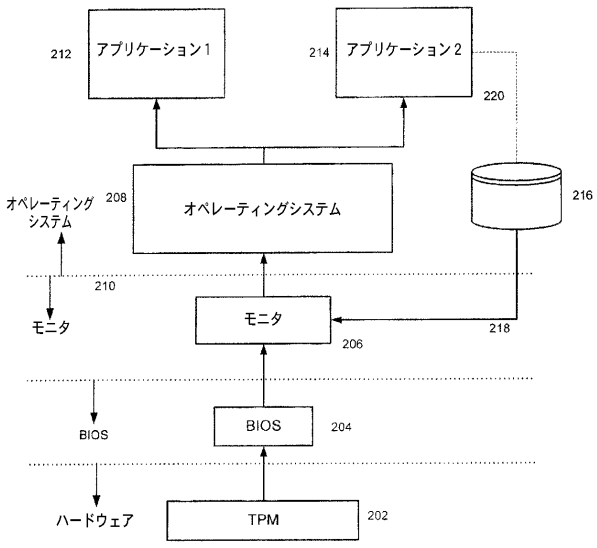
【図１】


30
32
34
36
10
24
26
28
20
18
16
14
12
22

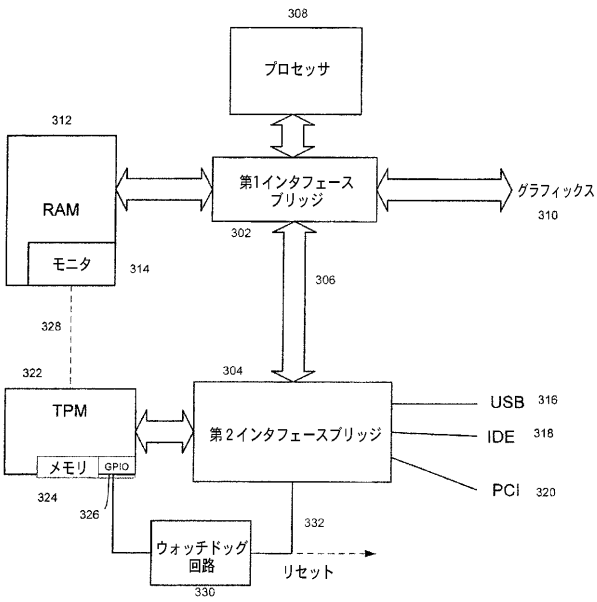
【図２】


ビデオモニタ
プリンタ
スピーカ
LAN
WAN
リモートコンピュータ
リモートアプリケーションプログラム
ネットワークインタフェース
モデム
キーボード
出力周辺機器インタフェース
ユーザ入力インタフェース
マウス
ビデオインタフェース
CD/DVD
TPM
システムバス
取り外し可能不揮発性メモリインタフェース
フロッピー
プログラムデータ
他のプログラムモジュール
アプリケーションプログラム
オペレーティングシステム
ウォッチドッグ回路
処理部
取り外し不能不揮発性メモリインタフェース
システムメモリ
(ROM)
BIOS
(RAM)
オペレーティングシステム
アプリケーションプログラム
他のプログラムモジュール
プログラムデータ

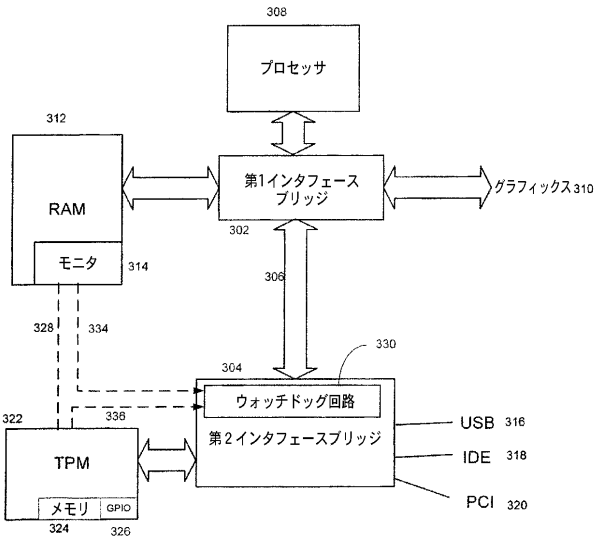
【図３】


アプリケーション1
212
アプリケーション2
214
220
216
オペレーティングシステム
208
オペレーティングシステム
210
モニタ
モニタ
206
218
BIOS
BIOS
204
ハードウェア
TPM
202

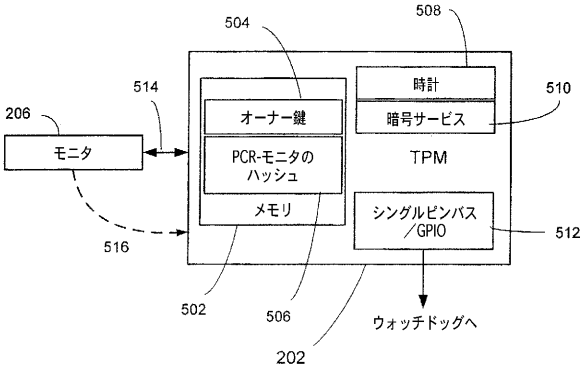
【図４】


308
プロセッサ
312
RAM
モニタ
314
第1インタフェースブリッジ
302
グラフィックス
310
306
328
322
TPM
メモリ
GPIO
324
326
304
第2インタフェースブリッジ
USB
316
IDE
318
PCI
320
332
ウォッチドッグ回路
330
リセット

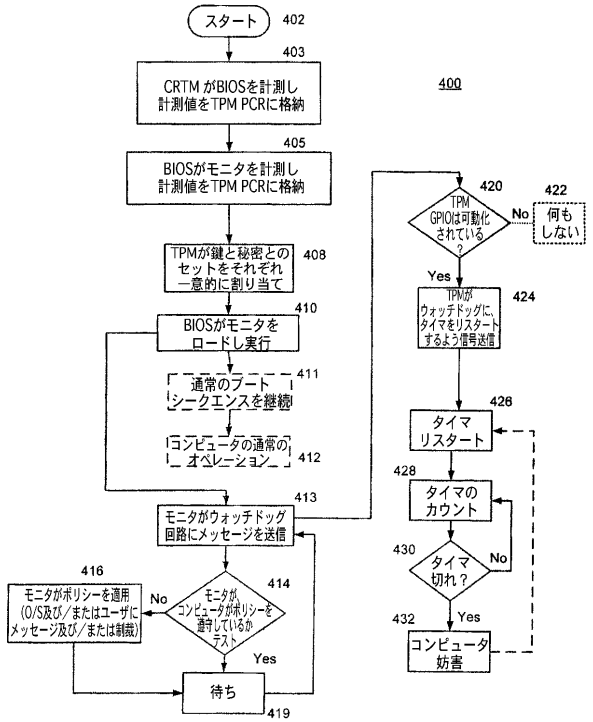
【図５】


308
プロセッサ
312
RAM
モニタ
314
第1インタフェース
ブリッジ
302
グラフィックス310
306
328
334
304
330
ウォッチドッグ回路
336
322
TPM
メモリ
GPIO
324
326
第２インタフェースブリッジ
USB 316
IDE 318
PCI 320

【図６】


504
508
514
206
モニタ
オーナー鍵
PCR-モニタの
ハッシュ
メモリ
時計
暗号サービス
510
TPM
シングルピンバス
／GPIO
512
516
502
506
202
ウォッチドッグへ

【図７】


スタート
402
403
CRTM がBIOSを計測し
計測値をTPM PCRに格納
400
405
BIOSがモニタを計測し
計測値をTPM PCRに格納
408
TPMが鍵と秘密とのセットをそれぞれ一意的に割り当て
410
BIOSがモニタをロードし実行
411
通常のブートシーケンスを継続
412
コンピュータの通常のオペレーション
413
モニタがウォッチドッグ回路にメッセージを送信
414
モニタが、コンピュータがポリシーを遵守しているかテスト
No
416
モニタがポリシーを適用(O/S及び／またはユーザにメッセージ及び／または制裁)
Yes
待ち
419
420
TPM GPIOは可動化されている？
No
422
何もしない
Yes
424
TPMがウォッチドッグに、タイマをリスタートするよう信号送信
426
タイマリスタート
428
タイマのカウント
430
タイマ切れ？
No
Yes
432
コンピュータ妨害

フロントページの続き

(72)発明者　ポール　イングランド
アメリカ合衆国　９８０５２－６３９９　ワシントン州　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　コーポレーション内

審査官　宮司　卓佳

(56)参考文献　特開２００１－１０１０３３（ＪＰ，Ａ）
特開平０６－０３５７１８（ＪＰ，Ａ）
特開２００１－０５１７４２（ＪＰ，Ａ）
特開２００３－２０８３１４（ＪＰ，Ａ）
特表２００３－５０７７８５（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
G06F　21/00
G06F　11/30