【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第６部門第３区分
【発行日】平成21年9月24日(2009.9.24)

【公表番号】特表2009-508259(P2009-508259A)
【公表日】平成21年2月26日(2009.2.26)
【年通号数】公開・登録公報2009-008
【出願番号】特願2008-531184(P2008-531184)
【国際特許分類】
Ｇ０６Ｆ　21/24　　(2006.01)
Ｇ０６Ｆ　21/06　　(2006.01)
Ｇ０６Ｆ　21/22　　(2006.01)
【ＦＩ】
Ｇ０６Ｆ　12/14　　５６０Ｂ
Ｇ０６Ｆ　12/14　　５６０Ｅ
Ｇ０６Ｆ　12/14　　５２０Ｆ
Ｇ０６Ｆ　12/14　　５３０Ｄ
Ｇ０６Ｆ　12/14　　５４０Ａ
Ｇ０６Ｆ　 9/06　　６６０Ｄ

【手続補正書】
【提出日】平成21年8月4日(2009.8.4)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
メモリ構成、処理能力、計量要求及び周辺機器に対する認証のうち少なくとも１つに対応するポリシーに従う利用に適合する計算機であって、
揮発性メモリと、
不揮発性メモリと、
入力インタフェースと、
通信インタフェースと、
及び、前記揮発性メモリ、前記不揮発性メモリ、前記入力インタフェース及び出力インタフェースと接続された単一の処理ユニットを含み、前記処理ユニットが、
命令処理ユニットと、
データバスインタフェースと、
汎用マイクロコード命令セットと、
ポリシー管理機能をサポートするマイクロコードから成り、前記汎用マイクロコード命令セットから分離されたセキュアマイクロコード命令セットと、
強制機能と、
耐タンパー性クロックと、を含み、
前記計算機がセキュアメモリにストアされた前記ポリシーに従って稼働するものと、を含む計算機。
【請求項２】
前記ポリシーに対応するデータが、前記入力インタフェース及び前記通信インタフェースのうち１つを介し受信されることを特徴とする請求項１記載の計算機。
【請求項３】

前記処理ユニットが更に、暗号機能を含むことを特徴とする請求項１の計算機。
【請求項４】
耐タンパー性メモリと共に処理ユニットを有する計算機を稼働する方法であって、
前記計算機を起動するための計算機命令を実行するステップと、
前記耐タンパー性メモリからポリシーを読み込むための計算機命令を実行するステップであって、前記ポリシーが、メモリ構成、処理能力、計量要求及び周辺機器に対する認証のうち少なくとも１つに対応するものと、
前記ポリシーに従って前記計算機を稼働するための計算機命令を実行して、前記耐タンパー性メモリにシステムメモリを再割り当てし、前記計算機による一般的利用に対して前記システムメモリを無効にするための計算機命令を実行するステップと、を含む方法。
【請求項５】
更に、
限定利用モードに前記計算機を設定するステップと、
時間指標を含む回復コードを受信するステップと、
前記時間指標と内部クロック機能とを比較するステップと、を含む請求項４記載の方法。
【請求項６】
更に、
前記ポリシーが前記計算機の利用を計量要求する時刻を決定するステップと、
前記ポリシーに従って前記利用を計量するステップと、を含む請求項４記載の方法。
【請求項７】
双方向データ通信をサポートするシステムバスと、
前記システムバスに接続された主メモリと、
前記システムバスに接続され、グラフィカル出力をサポートするビデオインターフェースと、
前記システムバスに接続された不揮発性メモリと、
前記システムバスに接続された処理装置と、
から成る計算機であって、
前記処理装置が、
　前記システムバスに接続された通信インターフェースと、
　前記通信インターフェースに接続された汎用処理ユニット（GPU）と、
　オペレーティングシステム機能をサポートする実行可能命令を有する汎用マイクロコードメモリと、
　セキュア機能を実装するオペレーティングシステムにアクセス不可能なGPU実行可能コードを有する、前記処理装置内のセキュアメモリと、
　前記セキュア機能への監視下のアクセスを許す、GPUに接続されたセキュアなハードウエアインターフェースと、
を含むことを特徴とする計算機。
【請求項８】
前記セキュア機能が、セキュアクロック機能と、計量機能と、ストアドバリュー機能と、強制機能とを含むことを特徴とする、請求項７に記載の計算機。
【請求項９】
前記強制機能が、主メモリの一部を前記セキュアメモリに再割り当てし、当該主メモリの再割り当てされた部分がオペレーティングシステム機能によって使用不可能になるように動作する事を特徴とする、請求項８記載の計算機。
【請求項１０】
前記通信インターフェースが、第1の動作モードの第1のメモリ構成と第2の動作モードの第2のメモリ構成とに対応する通信ポリシ更新に対して、アプリケーションプログラムインターフェースへデータを供給することを特徴とする、請求項７記載の計算機。
【請求項１１】

前記セキュアなハードウエアインターフェースが、基本入出力システム（BIOS）への制限されたアクセスを許す事を特徴とする、請求項７記載の計算機。

【請求項１２】

前記処理装置が、割込みベクトルに応答して、前記処理装置内のセキュアメモリからの命令を実行する事を特徴とする、請求項７記載の計算機。