【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24年4月12日(2012.4.12)

【公表番号】特表2011-527777(P2011-527777A)
【公表日】平成23年11月4日(2011.11.4)
【年通号数】公開・登録公報2011-044
【出願番号】特願2010-548742(P2010-548742)
【国際特許分類】
Ｇ０６Ｆ　21/22　　(2006.01)
【ＦＩ】
Ｇ０６Ｆ　9/06　　６６０Ｊ

【手続補正書】
【提出日】平成24年2月22日(2012.2.22)
【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】
コンピュータシステムを起動するための方法であって、
中央処理ユニットの不揮発性メモリに記憶され、前記中央処理ユニットのコア回路に前記中央処理ユニットのランダムアクセスメモリを初期化させる第１の命令を含む第１の一連のデータにアクセスするステップと、
前記第１の命令の少なくとも第１の部分の完全性を照合するために、前記第１の命令の第２の部分を実行するステップと、
第２の一連のデータの完全性を照合するための署名と前記中央処理ユニットに前記コンピュータシステムのシステムメモリを初期化させる第２の命令とを備える前記第２の一連のデータのイメージを、前記第１の命令の前記第１の部分の完全性を照合することに応じて不揮発性メモリから前記初期化されたランダムアクセスメモリに読み込むステップと、
前記署名と前記第１の一連のデータに含まれる復号化鍵とを用いて前記第２の一連のデータの前記完全性を照合するステップと、
前記第２の一連のデータの照合が成功したときに前記第２の命令を用いて前記システムメモリを初期化するステップとを備えた方法。
【請求項２】
前記第１の命令の前記第１の部分の前記完全性を照合するために前記第１の命令の前記第２の部分を実行するステップを更に備えている、請求項１の方法。
【請求項３】
前記ランダムアクセスメモリを初期化するために前記第１の命令のある部分を実行するステップと、
前記第１の一連のデータの一部を初期化された前記ランダムアクセスメモリに複写するステップと、
前記ランダムアクセスメモリに複写された前記第１の一連のデータの一部を用いて前記第１の命令の前記第１の部分の前記完全性を照合するために前記第１の命令の前記第２の部分を実行するステップとを更に備えている、請求項１の方法。
【請求項４】
前記不揮発性メモリから前記システムメモリに第３の一連のデータを読み込むと共に前記第３の一連のデータの完全性を照合することと、

前記第３の一連のデータに含まれ、前記コンピュータシステムに接続された起動可能デバイスから前記システムメモリにオペレーティングシステムを読み込ませる第３の命令を実行することとを更に備えている、請求項１の方法。
【請求項５】
前記第３の一連のデータの完全性を照合することは、前記第３の一連のデータに対するハッシュ値を決定することと、前記決定されたハッシュ値を前記第２の一連のデータに含まれる前記第３の一連のデータの当初のハッシュ値と比較することとを備えている、請求項４の方法。
【請求項６】
前記ランダムアクセスメモリを初期化することは、前記中央処理ユニットのデータキャッシュ及び命令キャッシュを初期化することを備えており、前記第２の一連のデータは前記データキャッシュに読み込まれ、
前記方法は、前記第２の一連のデータの完全性の照合が成功したときに前記第２の一連のデータを前記命令キャッシュに複写して前記第２の命令を実行することを更に備えている、請求項１の方法。
【請求項７】
前記第２の一連のデータを前記ランダムアクセスメモリに読み込むことは、ハッシュアルゴリズムを実行して前記第２の一連のデータのハッシュ値を決定することを備えており、
前記第２の一連のデータの完全性を照合することは、前記第２の一連のデータの前記ハッシュ値を、前記復号化鍵を前記署名に適用することによって得られる当初のハッシュ値と比較することを備えている、請求項１の方法。
【請求項８】
前記中央処理ユニットがリセットされ又は電源投入されるときはいつでも前記第１の一連のデータがアクセスされる、請求項１の方法。
【請求項９】
前記第２の一連のデータの照合成功の後に少なくとも前記復号化鍵への外部アクセスが可能になるように前記第１の一連のデータのアドレスを前記中央処理ユニットの仮想アドレス空間内で再配置することを更に備えた、請求項１の方法。
【請求項１０】
少なくとも前記第２の一連のデータの照合状態に関する状態情報を提供することを更に備えた、請求項１の方法。
【請求項１１】
前記第１の一連のデータを前記システムメモリ内に複写することを更に備えた、請求項４の方法。
【請求項１２】
前記第１の一連のデータは前記中央処理ユニットの前記ランダムアクセスメモリを初期化するための起動前命令及びデータ値を備えており、前記第２の一連のデータは起動命令及び起動データ値を備えている、請求項１の方法。
【請求項１３】
ＣＰＵコア、揮発性ランダムアクセスメモリ、不揮発性メモリ並びに前記ＣＰＵコア、前記揮発性ランダムアクセスメモリ及び前記不揮発性メモリを接続するためのバスシステムを画定する回路素子が形成された基板と、
前記不揮発性メモリに記憶され、前記ＣＰＵコアによって実行可能な命令と前記揮発性ランダムアクセスメモリを初期化すると共に起動ルーチンの少なくとも一部を照合するためのデータ値とを含む起動前情報と、を備えた中央処理ユニット。
【請求項１４】
前記起動前情報は前記起動ルーチンの前記少なくとも一部の署名を復号化することを可能にするように構成された一つ以上の復号化鍵を含む、請求項１３の中央処理ユニット。