【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1月19日(2012.1.19)

【公開番号】特開2011-243216(P2011-243216A)
【公開日】平成23年12月1日(2011.12.1)
【年通号数】公開・登録公報2011-048
【出願番号】特願2011-155064(P2011-155064)
【国際特許分類】
Ｇ０６Ｆ　12/14　　(2006.01)
【ＦＩ】
Ｇ０６Ｆ　12/14　　５１０Ｄ

【手続補正書】
【提出日】平成23年10月20日(2011.10.20)
【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】
プロセッサであって、
セキュア環境初期化命令に応じて、
セキュア初期化ソフトウェアをセキュアメモリにコピーし、
前記セキュアメモリにおいて前記セキュア初期化ソフトウェアの実行を開始するロジックを有するプロセッサ。
【請求項２】
前記ロジックは、確認のため、前記セキュア初期化ソフトウェアを前記セキュアメモリにコピーする、請求項１に記載のプロセッサ。
【請求項３】
前記ロジックは、前記セキュア初期化ソフトウェアにコントロールを移すことにより、前記セキュア初期化ソフトウェアの実行を開始する、請求項１に記載のプロセッサ。
【請求項４】
前記ロジックは、さらに、前記セキュア初期化ソフトウェアを前記セキュアメモリにコピーする前に、他のプロセッサが待ち状態に入ったことを確認する、請求項１に記載のプロセッサ。
【請求項５】
前記ロジックは、さらに、前記他のプロセッサが前記セキュア環境における実行を開始する場所を提供する、請求項４に記載のプロセッサ。
【請求項６】
プロセッサであって、
前記プロセッサに、セキュア命令のみに応じて、セキュアシステム環境の初期化をサポートする特殊なバストランザクションを発行させるバストランザクションロジックを有し、
前記初期化は、セキュアバーチャルマシンモニタの確認と、セキュアバーチャルマシンモニタ動作の開始を含む、プロセッサ。
【請求項７】
前記特殊なバストランザクションは、前記セキュアシステム環境の初期化をサポートする情報を転送する、請求項６に記載のプロセッサ。

【請求項８】
前記情報は鍵を含む、請求項７に記載のプロセッサ。
【請求項９】
第１のプロセッサが、セキュア初期化ソフトウェアのセキュアメモリへのコピーを含む、セキュア環境初期化命令を実行する段階と、
前記第１のプロセッサが、前記セキュア環境初期化命令に応じて、前記セキュアメモリにおいて前記セキュア初期化ソフトウェアを実行する段階とを有する方法。
【請求項１０】
さらに、前記セキュア環境初期化命令に応じて、前記セキュアメモリにおいて前記セキュア初期化ソフトウェアを確認する段階を有する、請求項９に記載の方法。
【請求項１１】
前記セキュア環境初期化命令に応じて前記セキュアメモリにおいて前記セキュア初期化ソフトウェアを確認する段階は、前記セキュア初期化ソフトウェアのデジタル署名を用いる段階を含む、請求項１０に記載の方法。
【請求項１２】
前記セキュア初期化ソフトウェアのデジタル署名は、前記セキュア初期化ソフトウェアのハッシュにより生成される、請求項１１に記載の方法。
【請求項１３】
さらに、前記セキュア初期化ソフトウェアの実行後、セキュアバーチャルマシンモニタを実行する段階を有する、請求項９に記載の方法。
【請求項１４】
さらに、前記セキュア初期化ソフトウェアを前記セキュアメモリにコピーする前に、第２のプロセッサが待ち状態に入ったことを確認する段階を有する、請求項９に記載の方法。
【請求項１５】
さらに、前記第２のプロセッサが前記セキュア環境における実行を開始する場所を提供する段階を有する、請求項１４に記載の方法。
【請求項１６】
セキュア環境初期化命令に応じて、
セキュア初期化ソフトウェアをセキュアメモリにコピーし、
前記セキュアメモリにおいて前記セキュア初期化ソフトウェアの実行を開始するする第１のプロセッサと、
前記セキュアメモリにおける前記セキュア初期化ソフトウェアの確認後、前記第１のプロセッサにより提供される場所で、前記セキュア環境における実行を開始する第２のプロセッサとを有する、システム。
【請求項１７】
前記第１のプロセッサは、さらに、前記セキュア初期化ソフトウェアを前記セキュアメモリにコピーする前に、前記第２のプロセッサが待ち状態に入ったことを確認する、請求項１６に記載のシステム。
【請求項１８】
さらに、前記セキュア初期化ソフトウェアの実行後に実行されるセキュアバーチャルマシンモニタを有する、請求項１６に記載のシステム。
【請求項１９】
プロセッサにより実行されると、前記プロセッサに、セキュア初期化ソフトウェアをセキュアメモリにコピーし、前記セキュアメモリにおいて前記セキュア初期化ソフトウェアの実行を開始させるセキュア環境初期化命令を格納した機械読み取り可能媒体。