【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】令和2年10月1日(2020.10.1)

【公表番号】特表2020-515969(P2020-515969A)
【公表日】令和2年5月28日(2020.5.28)
【年通号数】公開・登録公報2020-021
【出願番号】特願2019-553102(P2019-553102)
【国際特許分類】
*Ｇ０６Ｆ　21/52　(2013.01)*
*Ｇ０６Ｆ　 9/455　(2006.01)*
*Ｇ０６Ｆ　 9/50　(2006.01)*
*Ｇ０６Ｆ　12/14　(2006.01)*
【ＦＩ】
Ｇ０６Ｆ　21/52
Ｇ０６Ｆ　 9/455　１５０
Ｇ０６Ｆ　 9/50　１２０Ｚ
Ｇ０６Ｆ　12/14

【手続補正書】
【提出日】令和2年8月21日(2020.8.21)
【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】
少なくとも１つのメモリページを、プロセッサにおいて実行する第１仮想マシンから前記プロセッサにおいて実行する第１ハイパーバイザに遷移させることと、
前記プロセッサのセキュリティモジュールにおいて、前記少なくとも１つのメモリページを前記第１仮想マシンに戻すための要求を前記第１ハイパーバイザから受信することと、
前記プロセッサのセキュリティモジュールにおいて、前記少なくとも１つのメモリページを前記第１ハイパーバイザから前記第１仮想マシンに戻すための要求に応じて、前記少なくとも１つのメモリページの内容を選択的に検証することと、
前記第１仮想マシンによって書き込まれることが予想されないメモリページを保持するために、前記少なくとも１つのメモリページが、前記第１仮想マシンに関連するバルーンプールに割り当てられていることに応じて、前記第１ハイパーバイザが前記少なくとも１つのメモリページを戻すことを要求したことに応じて前記少なくとも１つのメモリページの内容を検証することをバイパスすることと、
前記少なくとも１つのメモリページの内容を検証したことに応じて、又は、前記少なくとも１つのメモリページが、前記第１仮想マシンに関連する前記バルーンプールに割り当てられていることに応じて、前記少なくとも１つのメモリページを前記第１仮想マシンに提供することと、を含む、
方法。
【請求項２】
前記少なくとも１つのメモリページの内容を選択的に検証することは、
前記少なくとも１つのメモリページが前記第１仮想マシンから前記第１ハイパーバイザに遷移したことに応じて、前記少なくとも１つのメモリページの少なくとも１つの特性を

測定して、少なくとも１つの特性測定値を生成することと、
前記少なくとも１つの特性測定値を前記セキュリティモジュールに記憶することと、
前記第１ハイパーバイザが前記少なくとも１つのメモリページを戻したことに応じて、前記少なくとも１つの特性測定値を前記少なくとも１つのメモリページと比較することと、を含む、
請求項１の方法。
【請求項３】
前記少なくとも１つの特性測定値が前記少なくとも１つのメモリページと一致しないことに応じて、前記第１ハイパーバイザが前記少なくとも１つのメモリページを前記第１仮想マシンに提供するのを抑制することをさらに含む、
請求項２の方法。
【請求項４】
複数のメモリページを前記第１仮想マシンに割り当てることと、
前記複数のメモリページの第１サブセットを、前記第１仮想マシンに関連する前記バルーンプールに記憶することであって、前記第１サブセットは、第１期間において前記第１仮想マシンによって書き込まれることが予想されないメモリページを含む、ことと、
前記第１ハイパーバイザが少なくとも１つのメモリページを要求したことに応じて、前記複数のメモリページの前記第１サブセットの少なくとも１つのページを前記第１ハイパーバイザに提供することと、をさらに含む、
請求項１の方法。
【請求項５】
前記第１ハイパーバイザが、メモリページの第１サブセットの少なくとも１つのページを前記第１仮想マシンに関連する前記バルーンプールに戻すことを要求したことに応じて、メモリページの第１サブセットの少なくとも１つのページの内容を検証するのをバイパスすることをさらに含む、
請求項４の方法。
【請求項６】
複数のメモリページを前記第１仮想マシンに割り当てることと、
少なくとも１つのメモリページに対する前記第１ハイパーバイザによる要求に応じて、前記複数のメモリページのサブセットを無効として指定することと、
前記複数のメモリページのサブセットを前記第１ハイパーバイザに提供することと、をさらに含む、
請求項１の方法。
【請求項７】
前記複数のメモリページのサブセットの少なくとも１つの特性を測定して、少なくとも１つの特性測定値を生成することと、
前記少なくとも１つの特性測定値を前記セキュリティモジュールに記憶することと、
前記第１ハイパーバイザが前記複数のメモリページのサブセットを戻したことに応じて、前記少なくとも１つの特性測定値を前記複数のメモリページのサブセットと比較することと、
前記少なくとも１つの特性測定値が前記複数のメモリページのサブセットと一致したことに応じて、前記複数のメモリページのサブセットを前記第１仮想マシンに提供することと、をさらに含む、
請求項６の方法。
【請求項８】
前記複数のメモリページを第１キーで暗号化することと、
前記複数のメモリページのサブセットを第２キーで暗号化することと、をさらに含む、
請求項６の方法。
【請求項９】
前記第２キーは、前記複数のメモリページが前記第１仮想マシンに割り当てられたこと

に応じて生成される、
請求項８の方法。
【請求項１０】
第１メモリページを、プロセッサにおいて実行する第１仮想マシンから前記プロセッサにおいて実行する第１ハイパーバイザに遷移させることと、
前記プロセッサのセキュリティモジュールにおいて、前記第１ハイパーバイザが前記第１メモリページを前記第１仮想マシンに戻すことを要求したことに応じて、前記第１ハイパーバイザが戻すことを要求している前記第１メモリページの内容が、前記第１仮想マシンから前記第１ハイパーバイザに遷移した前記第１メモリページの内容と一致することを選択的に検証することと、
前記第１仮想マシンによって書き込まれることが予想されないメモリページを保持するために、前記少なくとも１つのメモリページが、前記第１仮想マシンに関連するバルーンプールに割り当てられていることに応じて、前記第１ハイパーバイザが戻すことを要求している前記第１メモリページの内容が、前記第１仮想マシンから前記第１ハイパーバイザに遷移した前記第１メモリページの内容と一致するのを検証することをバイパスすることと、
前記第１ハイパーバイザが戻すことを要求している前記第１メモリページの内容が、前記第１仮想マシンから前記第１ハイパーバイザに遷移した前記第１メモリページの内容と一致することを検証したことに応じて、又は、前記第１メモリページが、前記第１仮想マシンに関連する前記バルーンプールに割り当てられていることに応じて、前記第１メモリページを前記第１仮想マシンに提供することと、を含む、
方法。
【請求項１１】
前記第１メモリページの内容を選択的に検証することは、
前記第１メモリページが前記第１仮想マシンから前記第１ハイパーバイザに遷移したことに応じて、前記第１メモリページの少なくとも１つの特性を測定して、少なくとも１つの特性測定値を生成することと、
前記少なくとも１つの特性測定値を前記セキュリティモジュールに記憶することと、
前記第１ハイパーバイザが前記第１メモリページを戻したことに応じて、前記少なくとも１つの特性測定値を前記第１メモリページと比較することと、を含む、
請求項１０の方法。
【請求項１２】
前記少なくとも１つの特性測定値が前記第１メモリページと一致しないことに応じて、前記第１メモリページを前記第１仮想マシンに戻すための前記第１ハイパーバイザからの要求を拒否することをさらに含む、
請求項１１の方法。
【請求項１３】
複数のメモリページを前記第１仮想マシンに割り当てることと、
前記複数のメモリページの第１サブセットを、前記第１仮想マシンに関連する前記バルーンプールに記憶することであって、前記第１サブセットは、前記第１仮想マシンによって書き込まれていないメモリページを含む、ことと、
前記第１ハイパーバイザが少なくとも１つのメモリページを要求したことに応じて、前記複数のメモリページの前記第１サブセットの少なくとも１つのページを前記第１ハイパーバイザに提供することと、をさらに含む、
請求項１０の方法。
【請求項１４】
メモリページの第１サブセットの少なくとも１つのページが前記第１ハイパーバイザから前記第１仮想マシンに遷移したことに応じて、さらに、前記第１ハイパーバイザが、メモリページの第１サブセットの少なくとも１つのページを、前記第１仮想マシンに関連するバルーンプールに提供したことに応じて、メモリページの第１サブセットの少なくとも

１つのページの内容を検証するのをバイパスすることをさらに含む、
請求項１３の方法。
【請求項１５】
複数のメモリページを前記第１仮想マシンに割り当てることと、
少なくとも１つのメモリページに対する前記第１ハイパーバイザによる要求に応じて、前記複数のメモリページのサブセットを無効として指定することと、
前記複数のメモリページのサブセットを前記第１ハイパーバイザに提供することと、をさらに含む、
請求項１０の方法。
【請求項１６】
前記複数のメモリページのサブセットの少なくとも１つの特性を測定して、少なくとも１つの特性測定値を生成することと、
前記少なくとも１つの特性測定値を前記セキュリティモジュールに記憶することと、
前記第１ハイパーバイザが前記複数のメモリページのサブセットを戻したことに応じて、前記少なくとも１つの特性測定値を前記複数のメモリページのサブセットと比較することと、
前記少なくとも１つの特性測定値が前記複数のメモリページのサブセットと一致したことに応じて、前記複数のメモリページのサブセットを前記第１仮想マシンに提供することと、をさらに含む、
請求項１５の方法。
【請求項１７】
前記複数のメモリページを第１キーで暗号化することと、
前記複数のメモリページのサブセットを第２キーで暗号化することと、をさらに含む、
請求項１５の方法。
【請求項１８】
第１仮想マシンと、
第１ハイパーバイザと、
セキュリティモジュールと、を備え、
前記セキュリティモジュールは、
第１メモリページを前記第１仮想マシンに戻すための要求を前記第１ハイパーバイザから受信したことに応じて、前記第１ハイパーバイザが前記第１仮想マシンに戻すことを要求している前記第１メモリページの内容が、前記第１仮想マシンから前記第１ハイパーバイザに遷移した前記第１メモリページの内容と一致することを選択的に検証し、
前記第１仮想マシンによって書き込まれることが予想されないメモリページを保持するために、前記少なくとも１つのメモリページが、前記第１仮想マシンに関連するバルーンプールに割り当てられていることに応じて、前記第１ハイパーバイザが戻すことを要求している前記第１メモリページの内容が、前記第１仮想マシンから前記第１ハイパーバイザに遷移した前記第１メモリページの内容と一致するのを検証することをバイパスすることと、
前記第１ハイパーバイザが戻すことを要求している前記第１メモリページの内容が、前記第１仮想マシンから前記第１ハイパーバイザに遷移した前記第１メモリページの内容と一致することを検証したことに応じて、又は、前記第１メモリページが、前記第１仮想マシンに関連する前記バルーンプールに割り当てられていることに応じて、前記第１メモリページを前記第１仮想マシンに提供する、
プロセッサ。
【請求項１９】
前記セキュリティモジュールは、
前記第１メモリページが前記第１仮想マシンから前記第１ハイパーバイザに遷移したことに応じて、前記第１メモリページの少なくとも１つの特性を測定して、少なくとも１つの特性測定値を生成することと、

前記少なくとも１つの特性測定値を前記セキュリティモジュールに記憶することと、
前記第１ハイパーバイザが前記第１メモリページを戻すように要求したことに応じて、前記少なくとも１つの特性測定値を前記第１メモリページと比較することと、
によって、前記第１メモリページの内容を選択的に検証する、
請求項１８のプロセッサ。
【請求項２０】
前記セキュリティモジュールは、
前記少なくとも１つの特性測定値が前記第１メモリページと一致しないことに応じて、前記第１メモリページを前記第１仮想マシンに戻すための前記第１ハイパーバイザからの要求を拒否する、
請求項１９のプロセッサ。
【請求項２１】
前記セキュリティモジュールは、
複数のメモリページを前記第１仮想マシンに割り当てることと、
前記複数のメモリページの第１サブセットを、前記第１仮想マシンに関連する前記バルーンプールに記憶することであって、前記第１サブセットは、前記第１仮想マシンによって書き込まれていないメモリページを含む、ことと、
前記第１ハイパーバイザが少なくとも１つのメモリページを要求したことに応じて、前記複数のメモリページの前記第１サブセットの少なくとも１つのページを前記第１ハイパーバイザに提供することと、を行う、
請求項１８のプロセッサ。
【請求項２２】
前記セキュリティモジュールは、
前記第１ハイパーバイザが、メモリページの第１サブセットの少なくとも１つのページを前記第１仮想マシンに関連する前記バルーンプールに提供したことに応じて、メモリページの第１サブセットの少なくとも１つのページの内容を検証するのをバイパスする、
請求項２１のプロセッサ。
【請求項２３】
前記セキュリティモジュールは、
複数のメモリページを前記第１仮想マシンに割り当てることと、
少なくとも１つのメモリページに対する第１ハイパーバイザによる要求に応じて、前記複数のメモリページのサブセットを無効として指定することと、
前記複数のメモリページのサブセットを前記第１ハイパーバイザに提供することと、を行う、
請求項１８のプロセッサ。
【請求項２４】
前記セキュリティモジュールは、
前記第１メモリページの少なくとも１つの特性を測定して、少なくとも１つの特性測定値を生成することと、
前記少なくとも１つの特性測定値を前記セキュリティモジュールに記憶することと、
前記第１ハイパーバイザが前記第１メモリページを戻すことを要求したことに応じて、前記少なくとも１つの特性測定値を前記第１メモリページと比較することと、
前記少なくとも１つの特性測定値が前記第１メモリページと一致したことに応じて、前記第１メモリページを前記第１仮想マシンに提供することと、を行う、
請求項２３のプロセッサ。
【請求項２５】
前記セキュリティモジュールは、
前記複数のメモリページを第１キーで暗号化することと、
前記複数のメモリページのサブセットを第２キーで暗号化することと、を行う、
請求項２３のプロセッサ。