【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4年8月12日(2022.8.12)

【国際公開番号】WO2020/182528
【公表番号】特表2022-522702(P2022-522702A)
【公表日】令和4年4月20日(2022.4.20)
【年通号数】公開公報(特許)2022-071
【出願番号】特願2021-550114(P2021-550114)
【国際特許分類】
G06F 12/14(2006.01)
G06F 12/109(2016.01)
G06F 9/455(2006.01)
G06F 12/02(2006.01)
【FI】
G06F 12/14 510E
G06F 12/109100
G06F 12/109110
G06F 9/455150
G06F 12/02 570K

【手続補正書】
【提出日】令和4年8月3日(2022.8.3)
【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】
メモリのセキュア・ページに対するセキュア・アクセス・リクエストを、コンピュータ・システムのセキュア・インタフェース制御において受け取ること、
前記セキュア・インタフェース制御によって、前記セキュア・ページに関連づけられた仮想アドレス比較無効化状態をチェックすること、および
複数の仮想アドレスから同じ絶対アドレスへのマッピングをサポートするために、前記セキュア・インタフェース制御によって、前記仮想アドレス比較無効化状態がセットされていることに基づいて、前記セキュア・ページにアクセスする際の仮想アドレス・チェックを、前記セキュア・ページに対して無効化すること
を含む、方法。
【請求項２】
前記セキュア・インタフェース制御によって、複数のセキュア・ドメインのうちのセキュア・ドメインが共用ページにアクセスすることが許可されていることを、ドメイン識別子に基づいて確認すること
をさらに含む、請求項１に記載の方法。
【請求項３】
前記共用ページにアクセスする許可を確かめるために、前記セキュア・ドメインの前記ドメイン識別子が、共用を許すと識別された前記セキュア・ドメインの複数のドメイン識別子と比較される、請求項２に記載の方法。
【請求項４】
仮想アドレスを絶対アドレスにマップする動的アドレス変換テーブルの複数のグループ

がセキュアでないホストによって変更されていないことを確かめることであって、前記セキュアでないホストは前記セキュア・ページにアクセスすることができる複数のセキュア・ドメインのうちのいずれかについて前記動的アドレス変換テーブルの前記グループのうちの１つまたは複数のグループを管理するように構成されており、仮想アドレスに対してマップするそれぞれのテーブルが前記動的アドレス変換テーブルの前記１つまたは複数のグループの中の複数の関連テーブルを含む、確かめること、および
前記動的アドレス変換テーブルの前記１つまたは複数のグループの中で変化を検出したことに基づいて、前記セキュア・アクセス・リクエストを終了すること
を含む、請求項２または請求項３に記載の方法。

【請求項５】
前記仮想アドレス比較無効化状態が、前記セキュア・ページに関連づけられたセキュア・ドメイン識別子、前記セキュア・ページに関連づけられた仮想アドレス・マッピング・データおよび前記仮想アドレス比較無効化状態を含むゾーン・セキュリティ・テーブルを通して記憶および更新される、請求項１から請求項４のいずれか一項に記載の方法。

【請求項６】
前記セキュア・インタフェース制御がファームウェア、ハードウェアもしくは信頼できるソフトウェア、またはファームウェア、ハードウェアおよび信頼できるソフトウェアの組合せを含み、前記セキュア・ページがハイパーバイザまたはオペレーティング・システムによって管理されたセキュア仮想機械またはセキュア・コンテナに割り当てられる、請求項１から請求項５のいずれか一項に記載の方法。

【請求項７】
システムであって、
処理ユニットと、
セキュア・インタフェース制御と、
を備え、前記セキュア・インタフェース制御が、請求項１から請求項６のいずれか一項に記載の方法を前記処理ユニットに実行させるように構成されている、システム。

【請求項８】
処理ユニットに請求項１から請求項６のいずれか一項に記載の方法を実行させるように構成されている、コンピュータ・プログラム。

【請求項９】
請求項８に記載のコンピュータ・プログラムを記録した、コンピュータ可読ストレージ媒体。

【請求項１０】
メモリのセキュア・ページに対するセキュア・アクセス・リクエストを、コンピュータ・システムのセキュア・インタフェース制御において受け取ること、
前記セキュア・インタフェース制御によって、前記セキュア・ページに関連づけられた仮想アドレス比較無効化状態をチェックすること、および
前記セキュア・アクセス・リクエストを出したエンティティの許可ステータス、および前記仮想アドレス比較無効化状態がセットされていることに基づいて、仮想アドレスが指定されていない前記セキュア・ページへの絶対アドレス・アクセスを有効化すること
を含む、方法。

【請求項１１】
前記セキュア・インタフェース制御によって、複数のセキュア・ドメインのうちのセキュア・ドメインが共用ページにアクセスすることが許可されていることを、ドメイン識別子に基づいて確認すること
をさらに含む、請求項１０に記載の方法。

【請求項１２】
前記共用ページにアクセスする許可を確かめるために、前記セキュア・ドメインの前記ドメイン識別子が、共用を許すと識別された前記セキュア・ドメインの複数のドメイン識別子と比較される、請求項１１に記載の方法。

【請求項１３】
前記セキュア・インタフェース制御がファームウェアもしくはハードウェア、またはファームウェアとハードウェアの組合せを含み、前記セキュア・ページがハイパーバイザまたはオペレーティング・システムによって管理されたセキュア・コンテナまたはセキュア仮想機械に割り当てられる、請求項１０から請求項１２のいずれか一項に記載の方法。
【請求項１４】
システムであって、
処理ユニットと、
セキュア・インタフェース制御と、
を備え、前記セキュア・インタフェース制御が、請求項１０から請求項１３のいずれか一項に記載の方法を前記処理ユニットに実行させるように構成されている、システム。