【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15日(2022.8.15)

【国際公開番号】WO2020/182664
【公表番号】特表2022-523785(P2022-523785A)
【公表日】令和4年4月26日(2022.4.26)
【年通号数】公開公報(特許)2022-075
【出願番号】特願2021-551611(P2021-551611)
【国際特許分類】
Ｇ０６Ｆ 12/14(2006.01)
Ｇ０６Ｆ 12/1036(2016.01)
Ｇ０６Ｆ 9/455(2006.01)
Ｇ０６Ｆ 21/78(2013.01)
【ＦＩ】
Ｇ０６Ｆ 12/14 ５１０Ｅ
Ｇ０６Ｆ 12/1036１００
Ｇ０６Ｆ 9/455１５０
Ｇ０６Ｆ 21/78

【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】
コンピュータ・システムのセキュア・インターフェース制御において、前記コンピュータ・システムのセキュア・ドメイン内のセキュア・エンティティに関連するデータ構造へのアクセス要求を受信することと、
前記セキュア・インターフェース制御によって、前記データ構造の位置に関連付けられた仮想ストレージ・アドレスをチェックすることと、
前記セキュア・インターフェース制御によって、前記データ構造の前記位置が前記仮想ストレージ・アドレスに関連付けられているとの判定に基づいて、前記コンピュータ・システムの非セキュア・エンティティの仮想アドレス空間を使用するアドレス変換を要求することと、
前記セキュア・インターフェース制御によって、前記アドレス変換の結果に基づいて前記データ構造にアクセスすることと
を含む、方法。
【請求項２】
前記セキュア・インターフェース制御によって、前記データ構造の前記位置が前記仮想ストレージ・アドレスに関連付けられていないとの判定に基づいて、絶対アドレスを使用して前記データ構造にアクセスすることをさらに含む、請求項１に記載の方法。
【請求項３】
前記非セキュア・エンティティによって提供された前記仮想ストレージ・アドレスのマッピングを検証することをさらに含む、請求項１または２に記載の方法。
【請求項４】
前記仮想ストレージ・アドレスの前記マッピングを検証することが、以前のマッピング

と比較して前記マッピングの変化をチェックすることを含む、請求項３に記載の方法。
【請求項５】
前記セキュア・ドメイン内の前記セキュア・エンティティに関連する前記データ構造が、メモリの複数のページ間に分散される、請求項１ないし４のいずれか一項に記載の方法。
【請求項６】
前記非セキュア・エンティティによって提供されたメモリの前記ページが、連続した範囲の仮想アドレスに常駐する、請求項５に記載の方法。
【請求項７】
前記仮想ストレージ・アドレスをチェックすることが、ホスト仮想アドレスに関連付けられた仮想アドレス比較が有効であるか無効であるかを判定するために、ゾーン・セキュリティ・テーブルを検査することをさらに含む、請求項１ないし６のいずれか一項に記載の方法。
【請求項８】
前記セキュア・インターフェース制御が、ファームウェア、ハードウェア、信頼できるソフトウェア、またはファームウェアと、ハードウェアと、信頼できるソフトウェアとの組合せを含む、請求項１ないし７のいずれか一項に記載の方法。
【請求項９】
前記非セキュア・エンティティが、１つまたは複数のセキュア・ゲストを前記セキュア・エンティティとしてホストするように構成されたハイパーバイザを含む、請求項１ないし８のいずれか一項に記載の方法。
【請求項１０】
システムであって、
メモリと、
処理ユニットと、
セキュア・インターフェース制御と
を備え、前記セキュア・インターフェース制御が、
セキュア・ドメイン内のセキュア・エンティティに関連するデータ構造へのアクセス要求を受信することと、
前記メモリ内の前記データ構造の位置に関連付けられた仮想ストレージ・アドレスをチェックすることと、
前記データ構造の前記位置が前記仮想ストレージ・アドレスに関連付けられているとの判定に基づいて、前記処理ユニットの非セキュア・エンティティの仮想アドレス空間を使用するアドレス変換を要求することと、
前記アドレス変換の結果に基づいて前記データ構造にアクセスすることと
を含む複数の動作を実行するように構成される、システム。
【請求項１１】
前記セキュア・インターフェース制御が、
前記データ構造の前記位置が前記仮想ストレージ・アドレスに関連付けられていないとの判定に基づいて、絶対アドレスを使用して前記データ構造にアクセスすることを含む動作を実行するように構成される、請求項１０に記載のシステム。
【請求項１２】
前記セキュア・インターフェース制御が、
前記非セキュア・エンティティによって提供された前記仮想ストレージ・アドレスのマッピングを検証することを含む動作を実行するように構成される、請求項１０または１１に記載のシステム。
【請求項１３】
前記仮想ストレージ・アドレスの前記マッピングを検証することが、以前のマッピングと比較して前記マッピングの変化をチェックすることを含む、請求項１２に記載のシステム。

【請求項１４】
前記セキュア・ドメイン内の前記セキュア・エンティティに関連する前記データ構造が、前記メモリの複数のページ間に分散される、請求項１０ないし１３のいずれか一項に記載のシステム。
【請求項１５】
前記非セキュア・エンティティによって提供された前記メモリの前記ページが、連続した範囲の仮想アドレスに常駐する、請求項１４に記載のシステム。
【請求項１６】
前記仮想ストレージ・アドレスをチェックすることが、ホスト仮想アドレスに関連付けられた仮想アドレス比較が有効であるか無効であるかを判定するために、ゾーン・セキュリティ・テーブルを検査することをさらに含む、請求項１０ないし１５のいずれか一項に記載のシステム。
【請求項１７】
前記セキュア・インターフェース制御が、ファームウェア、ハードウェア、信頼できるソフトウェア、またはファームウェアと、ハードウェアと、信頼できるソフトウェアとの組合せを含む、請求項１０ないし１６のいずれか一項に記載のシステム。
【請求項１８】
前記非セキュア・エンティティが、１つまたは複数のセキュア・ゲストを前記セキュア・エンティティとしてホストするように構成されたハイパーバイザを含む、請求項１０ないし１７のいずれか一項に記載のシステム。
【請求項１９】
請求項１～８の何れか1項に記載の方法をコンピュータに実行させる、コンピュータ・プログラム。
【請求項２０】
請求項１９に記載の前記コンピュータ・プログラムをコンピュータ可読記憶媒体に記録した、記憶媒体。