【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】WO2020/183317
【公表番号】特表2022-523787(P2022-523787A)
【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2021-551892(P2021-551892)
【国際特許分類】
Ｇ０６Ｆ 21/57(2013.01)
Ｇ０６Ｆ 9/455(2006.01)
【ＦＩ】
Ｇ０６Ｆ 21/57
Ｇ０６Ｆ 9/455１５０

【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】
ホスト・サーバ上で実行されている信頼されていないエンティティによって、セキュア・エンティティをディスパッチするよう求める要求を受信することと、
前記ホスト・サーバのセキュア・インターフェース制御によって、前記ホスト・サーバが補助セキュア（ＡＳ）エンティティをテストするためのＡＳデバッグ・モードであるかどうかを判定することと、
前記ホスト・サーバが前記ＡＳデバッグ・モードであるとの判定に基づいて、セキュア・ゲスト・エンティティ状態を前記セキュア・エンティティの状態記述子からハードウェア内のＡＳエンティティ状態にロードして、前記セキュア・エンティティのディスパッチ時に、セキュアであり、前記ＡＳエンティティに属するものとして登録されているメモリ内のページへのアクセスをテストすることと
を含む、方法。
【請求項２】
前記セキュア・エンティティをディスパッチ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ＡＳエンティティ状態がドメインおよびモード・ビットを含む、請求項１または２に記載の方法。
【請求項４】
前記判定することが、１つまたは複数のハードウェア・ビットに基づく、請求項１～３の何れか１項に記載の方法。
【請求項５】
前記ホスト・サーバが前記ＡＳデバッグ・モードでないとの判定に基づいて、前記セキュア・ゲスト・エンティティ状態を前記セキュア・エンティティの前記状態記述子からハードウェア内のセキュア・ゲスト・エンティティ状態にロードして、前記セキュア・エンティティのディスパッチ時に、セキュアとして登録されているメモリ内のページへのアク

セスをテストすること
をさらに含む、請求項１～４の何れか１項に記載の方法。
【請求項６】
前記信頼されていないエンティティがハイパーバイザであり、前記セキュア・エンティティがセキュア仮想マシン（ＶＭ）である、請求項１～５の何れか１項に記載の方法。
【請求項７】
前記セキュア・エンティティがテスト・ケースである、請求項１～６の何れか１項に記載の方法。
【請求項８】
システムであって、
メモリと、
セキュア・インターフェース制御と、
前記メモリおよび前記セキュア・インターフェース制御に結合されたホスト・サーバとを備え、前記システムが、
前記ホスト・サーバ上で実行されている信頼されていないエンティティによって、セキュア・エンティティをディスパッチするよう求める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、前記ホスト・サーバが補助セキュア（ＡＳ）エンティティをテストするためのＡＳデバッグ・モードであるかどうかを判定することと、
前記ホスト・サーバが前記ＡＳデバッグ・モードであるとの判定に基づいて、セキュア・ゲスト・エンティティ状態を前記セキュア・エンティティの状態記述子からハードウェア内のＡＳエンティティ状態にロードして、前記セキュア・エンティティのディスパッチ時に、セキュアであり、前記ＡＳエンティティに属するものとして登録されているメモリ内のページへのアクセスをテストすることと
を含む動作を実行するように構成される、システム。
【請求項９】
前記動作が、前記セキュア・エンティティをディスパッチすることをさらに含む、請求項８に記載のシステム。
【請求項１０】
前記ＡＳエンティティ状態が、ドメインおよびモード・ビットを含む、請求項８または９に記載のシステム。
【請求項１１】
前記判定することが、１つまたは複数のハードウェア・ビットに基づく、請求項８～１０の何れか１項に記載のシステム。
【請求項１２】
前記動作が、
前記ホスト・サーバが前記ＡＳデバッグ・モードでないとの判定に基づいて、前記セキュア・ゲスト・エンティティ状態を前記セキュア・エンティティの前記状態記述子からハードウェア内のセキュア・ゲスト・エンティティ状態にロードして、前記セキュア・エンティティのディスパッチ時に、セキュアとして登録されているメモリ内のページへのアクセスをテストすること
をさらに含む、請求項８～１１の何れか１項に記載のシステム。
【請求項１３】
前記信頼されていないエンティティがハイパーバイザであり、前記セキュア・エンティティがセキュア仮想マシン（ＶＭ）である、請求項８～１２の何れか１項に記載のシステム。
【請求項１４】
前記セキュア・エンティティがテスト・ケースである、請求項８～１３の何れか１項に記載のシステム。
【請求項１５】

請求項１～７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１６】
ホスト・サーバ上で実行されている信頼されていないエンティティによって、セキュア・エンティティをディスパッチするよう求める要求を受信することと、
前記ホスト・サーバのセキュア・インターフェース制御によって、前記セキュア・エンティティが補助セキュア（ＡＳ）エンティティをテストするためのＡＳモードであるかどうかを判定することと、
前記セキュア・エンティティがＡＳデバッグ・モードであるとの判定に基づいて、ＡＳエンティティ状態を前記セキュア・エンティティの状態記述子からハードウェア内のＡＳエンティティ状態にロードして、前記セキュア・エンティティのディスパッチ時に、セキュアであり、ＡＳエンティティに属するものとして登録されているメモリ内のページへのアクセスをテストすることと
を含む、方法。
【請求項１７】
前記セキュア・エンティティがＡＳモードであるとの判定に基づいて、
前記ホスト・サーバの前記セキュア・インターフェース制御によって、前記セキュア・エンティティがセキュア・ゲスト・モードでもあるかどうかを判定することと、
前記セキュア・エンティティが前記セキュア・ゲスト・モードでもあるとの判定に基づいて、セキュア・ゲスト・エンティティ状態を前記セキュア・エンティティの前記状態記述子からハードウェア内のセキュア・ゲスト・エンティティ状態にロードして、前記セキュア・エンティティのディスパッチ時に、セキュアとして登録されているメモリ内のページへのアクセスをテストすることと
をさらに含む、請求項１６に記載の方法。
【請求項１８】
前記方法が、前記セキュア・エンティティをディスパッチすることをさらに含む、請求項１６または１７に記載の方法。
【請求項１９】
前記セキュア・ゲスト・エンティティ状態が、ドメインおよびモード・ビットを含む、請求項１６～１８の何れか１項に記載の方法。
【請求項２０】
前記ＡＳエンティティ状態が、ドメインおよびモード・ビットを含む、請求項１６～１９の何れか１項に記載の方法。
【請求項２１】
前記判定することが、前記セキュア・エンティティの前記状態記述子内のビットに基づく、請求項１６～２０の何れか１項に記載の方法。
【請求項２２】
前記信頼されていないエンティティがハイパーバイザであり、前記セキュア・エンティティがセキュア仮想マシン（ＶＭ）である、請求項１６～２１の何れか１項に記載の方法。
【請求項２３】
前記セキュア・エンティティがテスト・ケースである、請求項１６～２２の何れか１項に記載の方法。
【請求項２４】
システムであって、
メモリと、
セキュア・インターフェース制御と、
前記メモリおよび前記セキュア・インターフェース制御に結合されたホスト・サーバとを備え、前記システムが、
ホスト・サーバ上で実行されている信頼されていないエンティティによって、セキュ

ア・エンティティをディスパッチするよう求める要求を受信することと、
　前記ホスト・サーバのセキュア・インターフェース制御によって、前記セキュア・エンティティが補助セキュア（ＡＳ）エンティティをテストするためのＡＳモードであるかどうかを判定することと、
　前記セキュア・エンティティがＡＳデバッグ・モードであるとの判定に基づいて、ＡＳエンティティ状態を前記セキュア・エンティティの状態記述子からハードウェア内のＡＳエンティティ状態にロードして、前記セキュア・エンティティのディスパッチ時に、セキュアであり、ＡＳエンティティに属するものとして登録されているメモリ内のページへのアクセスをテストすることと
を含む動作を実行するように構成される、システム。
【請求項２５】
　前記動作が、前記セキュア・エンティティがＡＳデバッグ・モードであるとの判定に基づいて、
　前記ホスト・サーバの前記セキュア・インターフェース制御によって、前記セキュア・エンティティがセキュア・ゲスト・モードでもあるかどうかを判定することと、
　前記セキュア・エンティティが前記セキュア・ゲスト・モードでもあるとの判定に基づいて、セキュア・ゲスト・エンティティ状態を前記セキュア・エンティティの前記状態記述子からハードウェア内のセキュア・ゲスト・エンティティ状態にロードして、前記セキュア・エンティティのディスパッチ時に、セキュアとして登録されているメモリ内のページへのアクセスをテストすることと
をさらに含む、請求項２４に記載のシステム。