【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1年10月17日(2019.10.17)

【公表番号】特表2018-535483(P2018-535483A)
【公表日】平成30年11月29日(2018.11.29)
【年通号数】公開・登録公報2018-046
【出願番号】特願2018-519050(P2018-519050)
【国際特許分類】
Ｇ０６Ｆ　9/34　(2006.01)
Ｇ０６Ｆ　12/14　(2006.01)
Ｇ０６Ｆ　9/312　(2006.01)
【ＦＩ】
Ｇ０６Ｆ　9/34　３５０Ａ
Ｇ０６Ｆ　12/14　５１０Ａ
Ｇ０６Ｆ　9/312　Ｌ
Ｇ０６Ｆ　9/312　Ｗ
Ｇ０６Ｆ　9/34　３８０

【手続補正書】
【提出日】令和1年8月30日(2019.8.30)
【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】
データを処理するための装置であって、
プログラム命令によって指定された処理動作を実行する処理回路と、そして
メモリアクセス命令をデコードしてメモリアクセス動作を実行するように前記処理回路を制御する制御信号を生成するデコーダと、を含み、
前記メモリアクセス命令は、
保護されたメモリアクセス動作に対応する保護されたメモリアクセス命令と、そして
より保護されていないメモリアクセス動作に対応するより保護されていないメモリアクセス命令と、
を指定するそれぞれのエンコードを有し、そして
前記より保護されていないメモリアクセス動作は、前記保護されたメモリアクセス動作よりもより制限の少ないメモリアクセス条件に関連付けられている、装置。
【請求項２】
前記より保護されていないメモリアクセス命令は、前記保護されたメモリアクセス命令とは異なる数の変形を許可するエンコードを有する、請求項１に記載の装置。
【請求項３】
前記より保護されていないメモリアクセス命令は、前記保護されたメモリアクセス命令よりも少ない変形を許可するエンコードを有する、請求項２に記載の装置
【請求項４】
メモリ保護データに依存してメモリアドレス空間の領域へのアクセスを制御するメモリアクセス制御回路を含み、前記メモリ保護データは、前記保護されたメモリアクセス命令よりも前記より保護されていないメモリアクセス命令により制限の少ないメモリアクセス条件を強制するように前記メモリアクセス制御回路によって適用される少なくとも１つの

属性を含む、請求項１乃至３のいずれか一項に記載の装置。
【請求項５】
前記少なくとも１つの属性は、メモリアドレスが共有メモリアドレスであることを示し、
前記メモリアクセス制御回路は、前記保護されたメモリアクセス命令による前記共有メモリアドレスへのメモリアクセスをブロックし、そして
前記メモリアクセス制御回路は、前記より保護されていないメモリアクセス命令による前記共有メモリアドレスへのメモリアクセスを許可する、請求項４に記載の装置。
【請求項６】
前記少なくとも１つの属性は、メモリアドレスがプライベートメモリアドレスであることを示し、
前記メモリアクセス制御回路は、前記保護されたメモリアクセス命令による前記プライベートメモリアドレスへのメモリアクセスを許可し、そして
前記メモリアクセス制御回路は、前記より保護されていないメモリアクセス命令による前記プライベートメモリアドレスへのメモリアクセスをブロックする、請求項５に記載の装置。
【請求項７】
前記メモリアクセス制御回路は、データアボート応答をトリガするために、保護されたメモリアクセス命令による前記共有メモリアドレスへの試みられたメモリアクセスに応答する、請求項５及び６のいずれか一項に記載の装置。
【請求項８】
前記メモリアクセス制御回路は、データアボート応答をトリガするために、より保護されていないメモリアクセス命令による共有メモリアドレス以外への試みられたメモリアクセスに応答する、請求項５，６及び７のいずれか一項に記載の装置。
【請求項９】
前記メモリアクセス制御回路はメモリ管理ユニットであり、前記メモリ保護データはメモリページテーブルデータである、請求項４及び８のいずれか一項に記載の装置。
【請求項１０】
前記メモリアクセス制御回路はメモリ保護ユニットであり、前記メモリ保護データは前記メモリ保護ユニットのためのメモリ領域構成データである、請求項４及び８のいずれか一項に記載の装置。
【請求項１１】
前記保護されたメモリアクセス動作によってメモリに記憶されたデータを暗号化し、前記保護されたメモリアクセス動作によって前記メモリから読み出されたデータを復号化する暗号化回路を含む、請求項１乃至１０のいずれか一項に記載の装置。
【請求項１２】
メモリに記憶されたデータを暗号化し、前記メモリから読み出されたデータを復号するための暗号化回路を含み、前記暗号化回路は前記保護されたメモリアクセス動作に対してアクティブであり、そして前記暗号化回路は前記より保護されていないメモリアクセス動作に対しては非アクティブである、請求項１から１０のいずれか一項に記載の装置。
【請求項１３】
前記処理回路は、複数の例外レベル状態を有し、前記複数の例外レベル状態の内の所定の例外レベル状態で実行するプログラム内のより保護されていないメモリアクセス命令でアクセスされるメモリアドレスは、前記複数の例外レベル状態の内の選択可能な数のさらなる例外レベル状態で実行するプログラムと共有される、請求項１乃至１２のいずれか一項に記載の装置。
【請求項１４】
前記処理動作は、
複数のプログラムを実行するステップと、
前記複数のプログラムの所定のプログラム内の保護されたメモリアクセス命令を実行

して、前記所定のプログラムに専用のメモリアドレスをアクセスするステップと、そして
前記複数のプログラムの間で共有されるメモリアドレスにアクセスするために、前記複数のプログラムのうちの前記所定のプログラム内のより保護されていないメモリアクセス命令を実行するステップと、を含む、
請求項１乃至１３のいずれかに一項に記載の装置。
【請求項１５】
前記複数のプログラムは、特権プログラムと、前記特権プログラムによって提供される実行環境を使用して実行する少なくとも１つのさらなるプログラムとを含み、前記少なくとも１つのさらなるプログラムは、前記特権プログラムからプライベートなメモリアドレスにアクセスするために保護されたメモリアクセス命令を使用する、請求項１４に記載の装置。
【請求項１６】
前記特権プログラムはハイパーバイザプログラムであり、前記少なくとも１つのさらなるプログラムはオペレーティングシステムプログラムである、請求項１５に記載の装置。
【請求項１７】
前記特権プログラムはオペレーティングシステムプログラムであり、前記少なくとも１つのさらなるプログラムはアプリケーションプログラムである、請求項１５に記載の装置。
【請求項１８】
データを処理するための装置であって、
プログラム命令によって指定された処理動作を実行する処理手段と、そして
メモリアクセス動作を実行するように前記処理手段を制御する制御信号を生成するためにメモリアクセス命令をデコードするデコーダ手段と、を含み、
前記メモリアクセス命令は、
保護されたメモリアクセス動作に対応する保護されたメモリアクセス命令と、そして
より保護されていないメモリアクセス動作に対応するより保護されていないメモリアクセス命令と、を指定するそれぞれのエンコードを有し、そして
前記より保護されていないメモリアクセス動作は、前記保護されたメモリアクセス動作よりもより制限の少ないメモリアクセス条件に関連付けられている、装置。
【請求項１９】
データを処理する方法であって、
メモリアクセス動作を実行するように処理回路を制御するための制御信号を生成するためにメモリアクセス命令をデコードすることを含み、
前記メモリアクセス命令は、
保護されたメモリアクセス動作に対応する保護されたメモリアクセス命令と、そして
より保護されていないメモリアクセス動作に対応するより保護されていないメモリアクセス命令と、を指定するそれぞれのエンコードを有し、そして
前記より保護されていないメモリアクセス動作は、前記保護されたメモリアクセス動作よりもより制限の少ないメモリアクセス条件に関連付けられている、方法。
【請求項２０】
請求項１乃至１８のいずれか一項に記載の装置に対応する仮想マシン実行環境を提供するようにコンピュータを制御するための、非一時的な記憶媒体に格納されたコンピュータプログラム。