(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)公表番号
特表2024-538674
(P2024-538674A)
(43)公表日　令和6年10月23日(2024.10.23)

(51)国際特許分類		FI			テーマコード（参考）
G06F 12/14 (2006.01)		G06F	12/14	510D	5B017
G06F 9/34 (2018.01)		G06F	9/34	350A	5B033

審査請求　未請求　予備審査請求　未請求　（全37頁）

(21)出願番号　特願2024-520551(P2024-520551)
(86)(22)出願日　令和4年9月14日(2022.9.14)
(85)翻訳文提出日　令和6年5月20日(2024.5.20)
(86)国際出願番号　PCT/GB2022/052321
(87)国際公開番号　WO2023/067295
(87)国際公開日　令和5年4月27日(2023.4.27)
(31)優先権主張番号　2114862.2
(32)優先日　令和3年10月18日(2021.10.18)
(33)優先権主張国・地域又は機関
英国(GB)
(81)指定国・地域　AP(BW,GH,GM,KE,LR,LS,MW,MZ,NA,RW,SD,SL,ST,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,RU,TJ,TM),EP(AL,AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HR,HU,IE,IS,IT,LT,LU,LV,MC,
最終頁に続く

(71)出願人　500395107
アーム・リミテッド
グレート・ブリテン及び北部アイルランド連合王国、イングランド、 シー・ビー１、９エヌ・ジェイ、ケンブリッジ、フルボーン・ロード １１０
(74)代理人　110000855
弁理士法人浅村特許事務所
(72)発明者　ボトマン、フランソワ クリストファージャック
イギリス国 ケンブリッジシャー シービー１ ９エヌジェイ ケンブリッジ，フルボーン ロード １１０，アーム リミテッド宛
(72)発明者　グロカット、トーマス クリストファー
最終頁に続く

(54)【発明の名称】　封止されたケイパビリティを操作するための技法

(57)【要約】
封止されたケイパビリティを操作するための装置及び方法が記載される。装置は、メモリへのアクセス要求がその間に生成される処理動作を実施する処理回路であって、処理回路が、制約情報を識別するケイパビリティを使用してアクセス要求のためのメモリアドレスを生成するように配設されている、処理回路を有する。チェック回路は、次いで所与のケイパビリティを使用してそのメモリアドレスが生成される所与のアクセス要求が、その所与のケイパビリティによって識別される制約情報に基づいて、及び所与のアクセス要求に関連付けられた信頼レベルに基づいて許可されるかどうかを判定する。各ケイパビリティは、それに関連付けられたケイパビリティ信頼レベルを有し、所与のアクセス要求に関連付けられた信頼レベルは、処理回路の現在の動作モードに関連付けられた現在のモード信頼レベル、及び所与のケイパビリティのケイパビリティ信頼レベルの両方に依存する。ケイパビリティのうちの少なくとも１つは、封止されたケイパビリティとして設定可能であり、装置は、現在のモード信頼レベルが所与の封止されたケイパビリティの

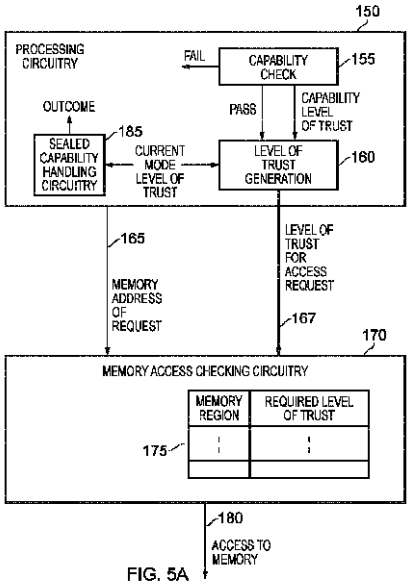


FIG. 5A

【特許請求の範囲】
【請求項１】
装置であって、
メモリへのアクセス要求がその間に生成される処理動作を実施する処理回路であって、前記処理回路が、制約情報を識別するケイパビリティを使用して前記アクセス要求のためのメモリアドレスを生成するように配設されている、処理回路と、
所与のケイパビリティを使用してそのメモリアドレスが生成される所与のアクセス要求が、その所与のケイパビリティによって識別される前記制約情報に基づいて、及び前記所与のアクセス要求に関連付けられた信頼レベルに基づいて許可されるかどうかを判定するチェック回路とを備え、
各ケイパビリティが、それに関連付けられたケイパビリティ信頼レベルを有し、前記所与のアクセス要求に関連付けられた前記信頼レベルが、前記処理回路の現在の動作モードに関連付けられた現在のモード信頼レベル、及び前記所与のケイパビリティの前記ケイパビリティ信頼レベルの両方に依存し、
前記ケイパビリティのうちの少なくとも１つが、封止されたケイパビリティとして設定可能であり、
前記装置が、前記現在のモード信頼レベルが所与の封止されたケイパビリティの前記ケイパビリティ信頼レベルよりも低い信頼レベルであるときに、前記処理回路が前記所与の封止されたケイパビリティを使用して少なくとも１つの処理動作を実施することを防止するために、封止されたケイパビリティ操作回路を更に備える、装置。
【請求項２】
各ケイパビリティが、それに関連付けられた封止フラグを有し、前記封止されたケイパビリティ操作回路が、選択されたケイパビリティに対する封止要求に応答して、前記選択されたケイパビリティの前記封止フラグを設定して前記選択されたケイパビリティを封止されたケイパビリティとして識別するかどうかを、前記選択されたケイパビリティの前記ケイパビリティ信頼レベルと前記現在のモード信頼レベルとの比較に応じて判定する、請求項１に記載の装置。
【請求項３】
前記封止されたケイパビリティ操作回路が、前記封止要求に応答して、前記選択されたケイパビリティの前記ケイパビリティ信頼レベルが前記現在のモード信頼レベルよりも大きいときに、前記封止フラグの設定を禁止するように配設されている、請求項２に記載の装置。
【請求項４】
前記封止されたケイパビリティ操作回路が、前記封止要求に応答して、前記選択されたケイパビリティの前記ケイパビリティ信頼レベルが前記現在のモード信頼レベルと一致するときに、前記封止フラグを設定するように配設されている、請求項３に記載の装置。
【請求項５】
各ケイパビリティが、そのケイパビリティを封止されたケイパビリティとして示すように設定可能である、それに関連付けられた封止フラグを有し、前記封止されたケイパビリティ操作回路が、選択された封止されたケイパビリティに対する開封要求に応答して、前記選択された封止されたケイパビリティの前記ケイパビリティ信頼レベルが前記現在のモード信頼レベルよりも大きいときに、前記選択された封止されたケイパビリティの前記封止フラグのクリアを禁止する、請求項１～４のいずれか一項に記載の装置。
【請求項６】
前記封止されたケイパビリティ操作回路が、前記開封要求に応答して、前記選択された封止されたケイパビリティの前記ケイパビリティ信頼レベルが前記現在のモード信頼レベルと一致するときに、前記封止フラグをクリアするように配設されている、請求項５に記載の装置。
【請求項７】
前記封止されたケイパビリティ操作回路が、前記現在のモード信頼レベルが前記所与の

封止されたケイパビリティの前記ケイパビリティ信頼レベルよりも低い信頼レベルであるときに、前記処理回路が前記所与の封止されたケイパビリティを使用して複数の処理動作のいずれかを実施することを防止するが、前記所与の封止されたケイパビリティを記憶要素間で移動させることを可能にするように配設されている、請求項１～６のいずれか一項に記載の装置。

【請求項８】

前記封止されたケイパビリティ操作回路が、前記現在のモード信頼レベルにかかわらず、前記所与の封止されたケイパビリティが後続の処理動作において前記処理回路によって使用されることが可能になる前に、前記所与の封止されたケイパビリティが開封されることを要求するように配設されている、請求項１～７のいずれか一項に記載の装置。

【請求項９】

前記封止されたケイパビリティ操作回路が、少なくとも前記現在のモード信頼レベルが前記所与の封止されたケイパビリティの前記ケイパビリティ信頼レベルと同じであるときに、前記処理回路が前記所与の封止されたケイパビリティを開封することなく前記所与の封止されたケイパビリティを使用して１つ以上の処理動作を実施可能であるように配設されている、請求項１～７のいずれか一項に記載の装置。

【請求項１０】

前記封止されたケイパビリティ操作回路が、前記現在のモード信頼レベルが前記所与の封止されたケイパビリティの前記ケイパビリティ信頼レベル以上である場合、前記所与の封止されたケイパビリティを使用して前記１つ以上の処理動作を実施可能であるように配設されている、請求項９に記載の装置。

【請求項１１】

実施可能になる前記１つ以上の処理動作が、

前記所与の封止されたケイパビリティを使用してメモリアドレスを生成するための逆参照動作と、

前記所与の封止されたケイパビリティによって識別される前記情報を修正するためのケイパビリティ修正動作とのうちの少なくとも１つを含む、請求項９又は１０に記載の装置。

【請求項１２】

前記処理回路が、少なくとも特権状態と、非特権状態と、を含む複数の状態のうちの１つにおいてプログラムコードを実行するように配設され、前記現在のモード信頼レベルは、前記複数の状態のうちのいずれにおいて前記現在のプログラムコードが実行されるかに依存する、請求項１～１１のいずれか一項に記載の装置。

【請求項１３】

前記処理回路は、少なくともセキュアドメイン及び低セキュアドメインを含む複数のセキュリティドメインのうちの１つにおいてプログラムコードを実行するように配設され、前記現在のモード信頼レベルは、前記複数のセキュリティドメインのうちのいずれにおいて前記現在のプログラムコードが実行されるかに依存する、請求項１～１２のいずれか一項に記載の装置。

【請求項１４】

前記現在のモード信頼レベルが、前記現在のプログラムコードが実行される前記状態と前記セキュリティドメインとの両方に依存する、請求項１３又は１４に記載の装置。

【請求項１５】

前記処理回路による参照のために、ケイパビリティを記憶するためのケイパビリティレジスタのセットと、

１つ以上のケイパビリティを記憶するためのメモリ回路と、を更に備え、

前記処理回路が、前記メモリ回路から選ばれたケイパビリティを、前記ケイパビリティレジスタのセットから選択されたケイパビリティレジスタにロードするためのロード動作を実施するように配設され、

前記処理回路が、前記ロード動作中に、前記選択されたケイパビリティレジスタに記憶

された前記選ばれたケイパビリティが、前記現在のモード信頼レベル又は前記メモリ回路に記憶された前記選ばれたケイパビリティの前記ケイパビリティ信頼レベルを超えないように制約されたケイパビリティ信頼レベルを有するように、前記ケイパビリティ信頼レベルを選択的に修正するように配設され、

前記処理回路が、前記選択されたケイパビリティが封止されたケイパビリティであるときに、前記ロード動作中に前記ケイパビリティ信頼レベルの修正を禁止する、

ように更に配設されている、請求項１～１４のいずれか一項に記載の装置。

【請求項１６】

前記封止されたケイパビリティ操作回路が、前記選択された封止されたケイパビリティに対する開封要求を処理した結果を示す結果情報を生成するように配設されている、請求項５に従属する場合の請求項１～１５のいずれか一項に記載の装置。

【請求項１７】

前記封止されたケイパビリティ操作回路が、前記処理回路にアクセス可能な１つ以上の状態フラグを設定することによって前記結果情報を生成するように配設されている、請求項１６に記載の装置。

【請求項１８】

前記封止されたケイパビリティ操作回路が、前記現在のモード信頼レベルにかかわらず、少なくとも１つの所定のタイプのケイパビリティの開封を禁止するように配設されている、請求項１～１７のいずれか一項に記載の装置。

【請求項１９】

前記所与のアクセス要求に関連付けられた前記信頼レベルは、前記現在のモード信頼レベル、及び前記ケイパビリティ信頼レベルのうちのいずれが、より低い信頼レベルを表すかに制約される、請求項１～１８のいずれか一項に記載の装置。

【請求項２０】

前記ケイパビリティ信頼レベルが、前記所与のケイパビリティ内で符号化される、請求項１～１９のいずれか一項に記載の装置。

【請求項２１】

封止されたケイパビリティを操作する方法であって、

メモリへのアクセス要求がその間に生成される処理動作を実施するために処理回路を採用することであって、前記処理回路が、制約情報を識別するケイパビリティを使用して、前記アクセス要求のためのメモリアドレスを生成する、採用することと、

所与のケイパビリティを使用してそのメモリアドレスが生成される所与のアクセス要求が、その所与のケイパビリティによって識別される前記制約情報に基づいて、及び前記所与のアクセス要求に関連付けられた信頼レベルに基づいて許可されるかどうかを判定することとを含み、

各ケイパビリティが、それに関連付けられたケイパビリティ信頼レベルを有し、前記所与のアクセス要求に関連付けられた前記信頼レベルが、前記処理回路の現在の動作モードに関連付けられた現在のモード信頼レベル、及び前記所与のケイパビリティの前記ケイパビリティ信頼レベルの両方に依存し、

前記ケイパビリティのうちの少なくとも１つが、封止されたケイパビリティとして設定可能であり、

前記方法が、前記現在のモード信頼レベルが所与の封止されたケイパビリティの前記ケイパビリティ信頼レベルよりも低い信頼レベルであるときに、前記処理回路が前記所与の封止されたケイパビリティを使用して少なくとも１つの処理動作を実施することを防止するために、封止されたケイパビリティ操作回路を採用することを更に含む、方法。

【請求項２２】

命令実行環境を提供するようにホストデータ処理装置を制御するコンピュータプログラムであって、

メモリへのアクセス要求がその間に生成される処理動作を実施する処理プログラムロジックであって、前記処理プログラムロジックが、制約情報を識別するケイパビリティを使

用して前記アクセス要求のためのメモリアドレスを生成するように配設されている、処理プログラムロジックと、
所与のケイパビリティを使用してそのメモリアドレスが生成される所与のアクセス要求が、その所与のケイパビリティによって識別される前記制約情報に基づいて、及び前記所与のアクセス要求に関連付けられた信頼レベルに基づいて許可されるかどうかを判定するチェックプログラムロジックとを備え、
各ケイパビリティが、それに関連付けられたケイパビリティ信頼レベルを有し、前記所与のアクセス要求に関連付けられた前記信頼レベルが、前記処理プログラムロジックの現在の動作モードに関連付けられた現在のモード信頼レベル、及び前記所与のケイパビリティの前記ケイパビリティ信頼レベルの両方に依存し、
前記ケイパビリティのうちの少なくとも１つが、封止されたケイパビリティとして設定可能であり、
前記装置が、前記現在のモード信頼レベルが所与の封止されたケイパビリティの前記ケイパビリティ信頼レベルよりも低い信頼レベルであるときに、前記処理プログラムロジックが前記所与の封止されたケイパビリティを使用して少なくとも１つの処理動作を実施することを防止するために、封止されたケイパビリティ操作プログラムロジックを更に備える、装置。
【発明の詳細な説明】
【技術分野】
【０００１】
本技法は、データ処理の分野に関し、より具体的には、封止されたケイパビリティの操作に関する。
【０００２】
所与のプロセスに対して特定のケイパビリティが定義され、定義されたケイパビリティ外の動作を実行しようとする試みがある場合に、エラーがトリガされ得る、ケイパビリティベースのアーキテクチャへの関心が高まっている。ケイパビリティは、様々な形態を採ることができるが、ケイパビリティの１つのタイプは、有界ポインタ（「ファットポインタ」とも称され得る）である。
【０００３】
データ処理装置の処理回路によるアクセスのためのケイパビリティを記憶するために、いくつかのケイパビリティ記憶要素（例えば、レジスタ）が提供され得る。各ケイパビリティは、そのケイパビリティを使用するときに実施することができる動作を制限するために使用される制約情報を含むことができる。例えば、有界ポインタを考慮すると、これは、関連付けられた許可を識別する１つ以上の許可フラグと共に、そのケイパビリティを使用するときに処理回路によってアクセス可能なメモリアドレスの拡張不可能な範囲を識別するために使用される情報を提供し得る。
【０００４】
いくつかのケイパビリティアーキテクチャが、封止されたケイパビリティの概念を導入してきた。ケイパビリティを封止することによって、これは、そのケイパビリティが逆参照不能（メモリアドレスがそのケイパビリティを使用してアクセスされ得ないことを意味する）及び不変としてマークされることを可能にし、そのようなケイパビリティを修正又は逆参照しようとする試みが行われる場合、ハードウェア例外を生じさせる。信頼できるコードなどのソフトウェアユースケースが、あまり信頼されないコードに、その信頼されるコードへのコールバック中に使用されるトークン、例えばファイルハンドルを与えることを可能にするので、封止されたケイパビリティのサポートが望ましい。このトークンは、あまり信頼されないモード内で使用可能であるべきではなく、ソフトウェア又はアーキテクチャ内の任意の他の挙動によって修正されるべきではない。
【０００５】
しかしながら、マルチビットフィールド（「オブジェクトタイプ」フィールドと呼ばれる場合がある）は、典型的には、ケイパビリティの封止された状態についての情報を取り

込むためにケイパビリティ内に提供される必要があり、更に、典型的には、特定の開封キー、典型的には、開封許可及び一致するオブジェクトタイプを有するケイパビリティが、そのような封止されたケイパビリティを開封するために使用される必要がある場合がある。しかしながら、いくつかの現代のシステムでは、ケイパビリティのメタデータを表すために利用可能なビット数は、非常に制約されており、それは、そのような封止されたケイパビリティの使用をサポートすることを困難にし得る。更に、鍵の開封を必要とする要件は煩雑である。

【０００６】

したがって、封止されたケイパビリティの提供をサポートするための代替機構を提供することが望ましい。

【発明の概要】

【０００７】

第１の例示的な配設では、装置であって、メモリへのアクセス要求がその間に生成される処理動作を実施する処理回路であって、この処理回路が、制約情報を識別するケイパビリティを使用してアクセス要求のためのメモリアドレスを生成するように配設されている、処理回路と、所与のケイパビリティを使用してそのメモリアドレスが生成される所与のアクセス要求が、所与のケイパビリティによって識別される所与の制約情報に基づいて、及び所与のアクセス要求に関連付けられた信頼レベルに基づいて許可されるかどうかを判定するチェック回路とを備え、各ケイパビリティが、それに関連付けられたケイパビリティ信頼レベルを有し、所与のアクセス要求に関連付けられた信頼レベルが、処理回路の現在の動作モードに関連付けられた現在のモード信頼レベル、及び所与のケイパビリティのケイパビリティ信頼レベルの両方に依存し、ケイパビリティのうちの少なくとも１つが、封止されたケイパビリティとして設定可能であり、装置が、現在のモード信頼レベルが所与の封止されたケイパビリティのケイパビリティ信頼レベルよりも低い信頼レベルであるときに、処理回路が所与の封止されたケイパビリティを使用して少なくとも１つの処理動作を実施することを防止するために、封止されたケイパビリティ操作回路を更に備える、装置が提供される。

【０００８】

更なる例示的な配設では、封止されたケイパビリティを操作する方法であって、メモリへのアクセス要求が生成される処理動作を実施するために処理回路を採用することであって、処理回路が、制約情報を識別するケイパビリティを使用してアクセス要求のためのメモリアドレスを生成することと、所与のケイパビリティを使用してそのメモリアドレスが生成される所与のアクセス要求が、その所与のケイパビリティによって識別される制約情報に基づいて、及び所与のアクセス要求に関連付けられた信頼レベルに基づいて許可されるかどうかを判定することとを含み、各ケイパビリティが、それに関連付けられたケイパビリティ信頼レベルを有し、所与のアクセス要求に関連付けられた信頼レベルが、処理回路の現在の動作モードに関連付けられた現在のモード信頼レベルと、所与のケイパビリティのケイパビリティ信頼レベルとの両方に依存し、ケイパビリティのうちの少なくとも１つが、封止されたケイパビリティとして設定可能であり、方法が、現在のモード信頼レベルが、所与の封止されたケイパビリティのケイパビリティ信頼レベルよりも低い信頼レベルであるときに、処理回路が所与の封止されたケイパビリティを使用して少なくとも１つの処理動作を実施することを防止するために、封止されたケイパビリティ操作回路を採用することを更に含む、方法が提供される。

【０００９】

また更なる例示的な配設では、命令実行環境を提供するようにホストデータ処理装置を制御するコンピュータプログラムであって、メモリへのアクセス要求がその間に生成される処理動作を実施する処理プログラムロジックであって、処理プログラムロジックが、制約情報を識別するケイパビリティを使用してアクセス要求のためのメモリアドレスを生成するように配設されている、処理プログラムロジックと、所与のケイパビリティを使用してそのメモリアドレスが生成される所与のアクセス要求が、所与のケイパビリティによっ

て識別される制約情報に基づいて、及び所与のアクセス要求に関連付けられた信頼レベルに基づいて許可されるかどうかを判定するために、チェックプログラムロジックとを備え、各ケイパビリティが、それに関連付けられたケイパビリティ信頼レベルを有し、所与のアクセス要求に関連付けられた信頼レベルが、処理プログラムロジックの現在の動作モードに関連付けられた現在のモード信頼レベル、及び所与のケイパビリティのケイパビリティ信頼レベルの両方に依存し、ケイパビリティのうちの少なくとも１つが、封止されたケイパビリティとして設定可能であり、装置が、現在のモード信頼レベルが所与の封止されたケイパビリティのケイパビリティ信頼レベルよりも低い信頼レベルであるときに、処理プログラムロジックが所与の封止されたケイパビリティを使用して少なくとも１つの処理動作を実施することを防止するために、封止されたケイパビリティ操作プログラムロジックを更に備える、コンピュータプログラムが提供される。

【００１０】

また更なる例示的な構成では、装置であって、メモリへのアクセス要求がその間に生成される処理動作を実施する処理手段であって、処理手段が、制約情報を識別するケイパビリティを使用してアクセス要求のためのメモリアドレスを生成するように配設されている、処理手段と、所与のケイパビリティを使用してそのメモリアドレスが生成される所与のアクセス要求が、所与のケイパビリティによって識別される制約情報に基づいて、及び所与のアクセス要求に関連付けられた信頼レベルに基づいて許可されるかどうかを判定するチェック手段とを備え、各ケイパビリティが、それに関連付けられたケイパビリティ信頼レベルを有し、所与のアクセス要求に関連付けられた信頼レベルが、処理手段の現在の動作モードに関連付けられた現在のモード信頼レベル、及び所与のケイパビリティのケイパビリティ信頼レベルの両方に依存し、ケイパビリティのうちの少なくとも１つが、封止されたケイパビリティとして設定可能であり、装置が、現在のモード信頼レベルが所与の封止されたケイパビリティのケイパビリティ信頼レベルよりも低い信頼レベルであるときに、処理手段が所与の封止されたケイパビリティを使用して少なくとも１つの処理動作を実施することを防止するために、封止されたケイパビリティ操作手段を更に備える、装置が提供される。

【図面の簡単な説明】

【００１１】

本技法について、添付の図面に示す本技法の例を参照して、例示としてのみ更に説明する。

【図１】例示的な一実装形態による装置のブロック図である。

【図２】有界ポインタ記憶要素のセット内のポインタ値を設定するか、又はそれにアクセスしようとする場合にエラーがトリガされ得る命令のタイプの例を示し、ポインタ値は、関連付けられた範囲情報によって示された範囲外のアドレスを指定するために使用される。

【図３】例示的な一実装形態による、有界ポインタに関連するタグビットの使用を例示する。

【図４】本明細書に説明される技法に従って使用され得るケイパビリティの形態を概略的に例示し、信頼レベル指標が、ケイパビリティに関連して提供され、封止フラグが、ケイパビリティが封止されるかどうかを示すために提供される。

【図５Ａ】例示的な一実装形態による、個々のアクセス要求に対する信頼レベルがどのように生成され、その後、メモリへのアクセスを制約するためにどのように使用され得るかを概略的に例示する図であり、封止されたケイパビリティの適切な操作もサポートする。

【図５Ｂ】例示的な一実装形態による、図５Ａに概略的に示された装置の動作を例示する流れ図である。

【図６】例示的な一実装形態による、封止要求の操作を例示する流れ図である。

【図７】例示的な一実装形態による、開封要求の操作を例示する流れ図である。

【図８】例示的な一実装形態による、処理回路の異なるドメイン及び処理状態の一例を示し、処理回路がドメイン及び処理状態の特定の組み合わせで動作しているときに、サポー

トされる場合がある封止及び開封能力を概略的に示す。
【図９Ａ】２つの例示的な実装形態による、封止されたケイパビリティを使用する要求が操作され得る異なる方法を例示する流れ図である。
【図９Ｂ】２つの例示的な実装形態による、封止されたケイパビリティを使用する要求が操作され得る異なる方法を例示する流れ図である。
【図１０】例示的な一実装形態による、ケイパビリティを修正する要求がどのように操作され得るかを例示する流れ図である。
【図１１】例示的な一実装形態による、メモリからケイパビリティをロードするために実施されるステップを例示する流れ図である。
【図１２】例示的な一実装形態による、ケイパビリティが所定のタイプであるか否かに応じて開封要求がどのように操作され得るかを例示する流れ図である。
【図１３】使用され得るシミュレータ例を示す。
【発明を実施するための形態】
【００１２】
本明細書で説明する技法によれば、装置であって、動作を実施するための処理回路であって、その動作中に、メモリへのアクセス要求が生成される、処理回路を有する装置が提供される。処理回路は、制約情報を識別するケイパビリティを使用してアクセス要求のためのメモリアドレスを生成するように配設されている。処理回路によって生成されたメモリアドレスは、アドレス変換が実施されるシステムにおける仮想アドレスであり得るか、又は代替的にアドレス変換をサポートしないシステムにおける物理アドレスであり得る。
【００１３】
この装置はまた、所与のケイパビリティを使用してそのメモリアドレスが生成される所与のアクセス要求が、その所与のケイパビリティによって識別された制約情報に基づいて許可されるかどうかを判定するために、チェック回路を有する。上記チェックを実施するチェック回路の機能は、処理回路とは別個の構成要素であり得るか、又は代替的に装置の処理回路内に提供され得る。
【００１４】
制約情報が関連付けられたケイパビリティによって識別され得るいくつかの方法がある。例えば、ケイパビリティは、１つの例示的な実装形態において、制約情報を直接含む場合がある。しかしながら、代替的な実装形態では、ケイパビリティは代わりに、制約情報が位置するメモリにおけるロケーションを（直接的又は間接的に）示し得る。
【００１５】
チェック回路はまた、所与のアクセス要求に関連付けられた信頼レベルに依存して、所与のアクセス要求によるメモリへのアクセスを更に制約するために、配設されている。チェック回路の機能は、様々な形態、例えば、メモリ管理ユニット（memory management unit、ＭＭＵ）、メモリ保護ユニット（memory protection unit、ＭＰＵ）、セキュリティ属性ユニット（security attribute unit、ＳＡＵ）、又はこれらの構成要素の組み合わせで実装することができる。そのようなチェック回路は、従来、メモリへのアクセスを更に制約するときに、任意の特定の信頼レベルを個々のアクセス要求に関連付けるのではなく、処理回路の現在の動作モードに関連付けられた信頼レベルを考慮するように配設されてきた。しかしながら、本明細書で説明する技法によれば、所与のケイパビリティは、それに関連付けられたケイパビリティ信頼レベルを有し、その情報はまた、チェック回路によって実施されるチェックに織り込まれ得る。特に、本明細書で説明する技法によれば、所与のアクセス要求に関連付けられた信頼レベルは、処理回路の現在の動作モードに関連付けられた現在のモード信頼レベル、及び所与のケイパビリティのケイパビリティ信頼レベルの両方に依存する。
【００１６】
個々のケイパビリティに関連してケイパビリティ信頼レベルを提供することによって、これは、ケイパビリティが管理及び使用され得る方法を強化することができる。例えば、上で考察されるように、ケイパビリティ信頼レベルは、所与のアクセス要求によって指定

されたメモリへのアクセスを進めることができるかどうかを判定するときにチェック回路によって考慮されるので、ある特定の事情において処理回路によってケイパビリティが生成されることを可能にする機構を提供することができ、特定のケイパビリティに関連付けられたケイパビリティ信頼レベルは、次いで、そのケイパビリティの出所を追跡し、そのケイパビリティを使用して後に行われるアクセスを制約するために効果的に使用される。

【００１７】

加えて、そのような機構は、例えば、混乱した代理攻撃に対抗するために、特定のユースケース保護がサポートされることを更に可能にする。混乱した代理攻撃は、より特権の低いコードがより特権の高いコードにポインタを渡し、より特権の高いコードを使用して、その代わりに特定の動作を実施しようとするときに発生する可能性がある。ケイパビリティ信頼レベルの使用を通して、これは、非特権コードにアクセス可能であるべきではないメモリのエリアを悪意を持ってアドレス指定する非特権コードによって作成されたポインタを、より特権の高いコードが誤って使用することを防止することができる。特に、そのような状況では、ポインタは、ケイパビリティ信頼レベルが非特権コードのケイパビリティ信頼レベルを超えないケイパビリティを使用して生成されており、したがって、特権コードからアクセスが試みられた場合でも、メモリアクセス回路は、ポインタを生成するために使用されたケイパビリティのケイパビリティ信頼レベルに起因して、特権メモリへのアクセスを防止する。

【００１８】

本明細書で説明する技法によれば、個々のケイパビリティに関連するケイパビリティ信頼レベルの提供も活用し、特に、オブジェクトタイプ及び開封許可を示すために不十分なメタデータビットを利用する必要性を回避し、鍵を開封する必要性も回避する、封止されたケイパビリティを操作するための軽量機構を提供することによって、追加の利益を提供する。

【００１９】

特に、本明細書で説明する技法によれば、装置は、現在のモード信頼レベルが所与の封止されたケイパビリティのケイパビリティ信頼レベルよりも低い信頼レベルであるときに、処理回路が所与の封止されたケイパビリティを使用して少なくとも１つの処理動作を実施することを防止するために、封止されたケイパビリティ操作回路を更に備える。したがって、封止されたケイパビリティを考慮する場合、処理回路が封止されたケイパビリティを操作する方法は、処理回路の現在のモード信頼レベルと、問題の封止されたケイパビリティのケイパビリティ信頼レベルとの両方を考慮して制約され得る。特に、個々のケイパビリティに関連付けられたケイパビリティ信頼レベルの情報を再利用することによって、ケイパビリティが封止されているとマークされている場合、そのケイパビリティ信頼レベルの情報を使用して、封止されたケイパビリティに関連付けられた特定のソフトウェアコンテキスト（ソフトウェア信頼レベル）を識別することができる。

【００２０】

前述の技法は、多種多様な異なるシステムにおいて使用することができる。例えば、処理回路は、様々な形態を採ることができる。例えば、処理回路は、様々な異なる動作モードでプログラムコードを実行するように配設されている中央処理装置（central processing unit、ＣＰＵ）であり得るが、本技法は、他の形態の処理回路、例えば、ダイレクトメモリアクセス（direct memory access、ＤＭＡ）コントローラ、暗号化アクセラレータなどに関連して適用することもできる。

【００２１】

所与のアクセス要求に関連付けられた信頼レベルが、処理回路の現在の動作モード、及び所与のケイパビリティのケイパビリティ信頼レベルの両方に基づいて判定され得るいくつかの方法がある。例えば、システムは、許可の付与又は許可の制限に基づくことができ、所与のアクセス要求に関連付けられた信頼レベルは、それらの技法のうちのどれが使用されるかに依存し得る。しかしながら、例示的な一実装形態によれば、本技法は許可の制限に基づき、所与のアクセス要求に関連付けられた信頼レベルは、現在のモード信頼レベ

ル、及びケイパビリティ信頼レベルのうちのいずれがより低い信頼レベルを表すかに制約される。

【００２２】

ケイパビリティ信頼レベルをケイパビリティについて指定することができるいくつかの方法があるが、例示的な一実装形態では、ケイパビリティ信頼レベルは所与のケイパビリティ内で符号化される。これは、様々な方法で実装することができるが、例示的な一実装形態では、ケイパビリティごとに、制約情報は、そのケイパビリティを使用して生成されたメモリアドレスに許可された様々なタイプのメモリアクセスを識別する許可の少なくとも１つのセットを提供し、ケイパビリティ信頼レベルは、追加の許可として提供される。

【００２３】

しかしながら、上述の例示的な実装形態では、ケイパビリティ信頼レベルは、所与のケイパビリティ内で符号化されるが、これは要件ではなく、ケイパビリティ信頼レベルを所与のケイパビリティに関連付けるための他の機構が提供され得ることに留意されたい。例えば、代替的な実装形態では、所与のケイパビリティは、ケイパビリティ信頼レベルを含むロケーションを示す識別子を提供し得る。したがって、そのような実装形態では、ケイパビリティ信頼レベル情報は、他のロケーション、例えば、メモリに常駐することができ、ケイパビリティ自体は、ケイパビリティ信頼レベルを提供するメタデータのロケーションを示す値を含む。ケイパビリティ信頼レベルを含むロケーションを示すために使用される識別子は、様々な形態を採ることができる。例えば、それは、システムのグローバルレジスタに記憶されたアドレスからのオフセットであり得、したがって、ケイパビリティ信頼レベルがメモリ内のどこに維持されているかを識別するメモリアドレスが判定されることを可能にする。代替的に、識別子は、ケイパビリティ信頼レベル情報が記憶されるメモリにおけるロケーションを直接識別する場合がある。

【００２４】

各ケイパビリティ内で提供された制約情報は、様々な形態を採ることができるが、例示的な一実装形態では、そのケイパビリティを使用して任意のアクセス要求に対して生成されたメモリアドレスに対するメモリアドレスの許容範囲を判定するために使用される境界情報を提供する。例示的な一実装形態では、制約情報は、そのような境界情報及びそのケイパビリティを使用して生成されたメモリアドレスに許可されたメモリアクセスのタイプを識別する許可のセットの両方を含み得る。ケイパビリティはまた、他の情報、例えば、メモリアドレスを生成するためにそのポインタ値を何らかのオフセットに加算することによって、メモリアドレスを生成するときに使用されるポインタ値を含むことができる。次いで、生成されたメモリアドレスを境界情報と比較して、生成されたメモリアドレスが許容範囲内にあるかどうかを判定することができる。

【００２５】

封止されたケイパビリティの説明に戻ると、ケイパビリティが封止されているものとして識別することができ、したがって、封止されたケイパビリティ操作回路に、所与の封止されたケイパビリティのケイパビリティ信頼レベルと、処理回路に関連付けられた現在のモード信頼レベルとの両方を考慮して、そのケイパビリティがどのように操作されるべきかを判定させる、いくつかの方法がある。しかしながら、例示的な一実装形態では、各ケイパビリティは、それに関連付けられた封止フラグを有し、封止されたケイパビリティ操作回路は、選択されたケイパビリティに対する封止要求に応答して、選択されたケイパビリティの封止フラグを設定して選択されたケイパビリティを封止されたケイパビリティとして識別するかどうかを、選択されたケイパビリティのケイパビリティ信頼レベルと現在のモード信頼レベルとの比較に応じて判定する。

【００２６】

封止フラグがセット（すなわち封止された）状態又はクリア（すなわち開封された）状態を示すことができるいくつかの方法がある。例えば、ロジック１値又はロジック０値のいずれかが、セット状態に関連付けられてもよく、実際に、いくつかの実装形態では、マルチビット符号化を提供することが適切であり得る。更に、封止要求は様々な方法で行わ

れてもよいが、例示的な一実装形態では、例えば、処理回路が封止命令を実行した結果として行われてもよい。

【００２７】

例示的な一実装形態では、封止されたケイパビリティ操作回路は、封止要求に応答して、選択されたケイパビリティのケイパビリティ信頼レベルが現在のモード信頼レベルよりも大きいときに、封止フラグを設定することを禁止するように配設されている。封止フラグが設定できるようにするために必要とされる実際の現在のモード信頼レベルは、実装形態に依存して変化し得る。例えば、ケイパビリティの封止は、現在のモード信頼レベルがケイパビリティ信頼レベル以上であるときはいつでも可能であってもよく、あるいは、ケイパビリティの封止は、現在のモード信頼レベルがケイパビリティ信頼レベルと同じである場合のみに制限されてもよい。

【００２８】

例示的な一実装形態では、封止されたケイパビリティは、ある特定の状況で開封されることも可能になる。例えば、例示的な一実装形態では、封止されたケイパビリティ操作回路は、選択された封止されたケイパビリティに対する開封要求に応答して、選択された封止されたケイパビリティのケイパビリティ信頼レベルが現在のモード信頼レベルよりも大きいときに、選択された封止されたケイパビリティの封止フラグのクリアを禁止する。封止と同様に、封止フラグがクリアできるようにするために必要とされる実際の現在のモード信頼レベルは、実装形態に依存して変化し得る。例えば、ケイパビリティの開封は、現在のモード信頼レベルがケイパビリティ信頼レベル以上であるときはいつでも可能であってもよく、あるいは、ケイパビリティの開封は、現在のモード信頼レベルがケイパビリティ信頼レベルと同じである場合のみに制限されてもよい。

【００２９】

更に、開封要求は様々な方法で行われてもよいが、例示的な一実装形態では、例えば、処理回路が開封命令を実行した結果として行われてもよい。

【００３０】

上述の技法によれば、ケイパビリティを封止することを可能にするか、又は封止されたケイパビリティを開封することを可能にするかの判定が、現在のモード信頼レベル及びケイパビリティ信頼レベルの両方を考慮して行われるので、使用される鍵を封止したり開封したりする必要がないことに留意されたい。

【００３１】

先に述べたように、封止されたケイパビリティ操作回路は、現在のモード信頼レベルが所与の封止されたケイパビリティのケイパビリティ信頼レベルよりも低い信頼レベルであるときに、処理回路が所与の封止されたケイパビリティを使用して少なくとも１つの処理動作を実施することを防止する。禁止される処理動作の数は、実装形態に応じて変化することができるが、一実施例では、封止されたケイパビリティ操作回路は、現在のモード信頼レベルが所与の封止されたケイパビリティのケイパビリティ信頼レベルよりも低い信頼レベルであるときに、処理回路が所与の封止されたケイパビリティを使用して複数の処理動作のいずれかを実施することを防止するが、所与の封止されたケイパビリティを記憶要素間で移動させることを可能にするように配設されている。

【００３２】

封止されたケイパビリティを記憶要素間で移動させることを可能にし、そのような封止されたケイパビリティをレジスタとメモリとの間で転送することを可能にし、実際に、必要に応じてレジスタ間移動を可能にすることが有用であり得る。しかしながら、典型的には、処理回路は、現在のモード信頼レベルが、その封止されたケイパビリティのケイパビリティ信頼レベルよりも低い場合、封止されたケイパビリティを使用して、全部ではないにしても大部分の処理動作を実施することを防止される場合がある。それにもかかわらず、ある特定の活動が可能にされる場合もあり得る。例えば、現在のモード信頼レベルが、問題の封止されたケイパビリティのケイパビリティ信頼レベルよりも低い場合であっても、ケイパビリティを、汎用データではなくケイパビリティとして識別するフィールド（本

明細書ではタグビットと呼ばれる）をクリアして、そのケイパビリティを効果的に無効にすることが可能であり得る。

【００３３】

例示的な一実装形態では、封止されたケイパビリティ操作回路は、現在のモード信頼レベルにかかわらず、所与の封止されたケイパビリティが後続の処理動作において処理回路によって使用されることが可能になる前に、所与の封止されたケイパビリティが開封されることを要求するように配設されている。

【００３４】

しかしながら、代替的な実装形態では、封止されたケイパビリティ操作回路は、少なくとも現在のモード信頼レベルが所与の封止されたケイパビリティのケイパビリティ信頼レベルと同じであるときに、処理回路が所与の封止されたケイパビリティを開封することなく所与の封止されたケイパビリティを使用して１つ以上の処理動作を実施可能であるように配設され得る。この機能は、例えば、現在のモード信頼レベルがケイパビリティ信頼レベルと同じである状況に制限されてもよく、あるいは、現在のモード信頼レベルがケイパビリティ信頼レベル以上である状況において可能にされてもよい。

【００３５】

上記で識別された事情において所与の封止されたケイパビリティを使用して実施可能になる１つ以上の処理動作は、実装形態に応じて変化し得る。例えば、所与の封止されたケイパビリティを使用してメモリアドレスを生成するために、逆参照動作が可能にされ得る。その代わりに、又はそれに加えて、所与の封止されたケイパビリティによって識別される情報を修正するために、ケイパビリティ修正動作も可能にされ得る。ケイパビリティの情報及び関連付けられたメタデータのいずれも、そのような修正動作を実施するときに変更され得る（特にメタデータが変わるときに、突然変異されると呼ばれることがある）が、典型的には、そのような動作は、ケイパビリティによって指定された制約を低減しないように制約される。例えば、典型的には、範囲情報又は許可に対する任意の変更は、それらが範囲を低減する、又は許可を低減するように働く場合にのみ可能にされる場合もある。

【００３６】

処理回路は、様々な異なる方法で動作するように配設することができ、現在のモード信頼レベルは、処理回路が現在どのように動作しているかに依存する。例えば、一実装形態では、処理回路は、少なくとも特権状態及び非特権状態を含む複数の状態のうちの１つにおいてプログラムコードを実行するように配設され得、現在のモード信頼レベルは、複数の状態のうちのいずれにおいて現在のプログラムコードが実行されるかに依存し得る。２つの異なる状態、すなわち、特権状態及び非特権状態があり得るか、又は異なるレベルの特権を有するＮ個の異なる状態があり得、ここでＮは２より大きく、これらのシナリオのいずれにおいても、現在のプログラムコードがどの状態で実行されるかに依存して、現在のモード信頼レベルを設定することができることに留意されたい。例えば、特定の実装形態は、異なる状態として、ＥＬ０、ＥＬ１及びＥＬ２などの異なる例外レベル（ＥＬ）を提供し得、ここで、ＥＬ２は、ＥＬ１よりも特権が与えられ、ＥＬ１はＥＬ０よりも特権が与えられる。

【００３７】

代替的に、又は加えて、処理回路は、少なくともセキュアドメイン及び低セキュアドメインを含む複数のセキュリティドメインのうちの１つにおいてプログラムコードを実行するように配設され得、現在のモード信頼レベルは、複数のセキュリティドメインのうちのいずれにおいて現在のプログラムコードが実行されるかに依存し得る。処理状態と同様に、２つのドメイン、すなわち、セキュアドメイン及び非セキュアドメインだけが存在し得るか、又は代替的に、Ｍ個の異なるドメインが存在し得、ここで、Ｍは２より大きく、各ドメインは異なるレベルのセキュリティを有し、現在のモード信頼レベルは、次いで、現在のプログラムコードがどのセキュリティドメインで実行されるかに依存して、設定され得る。

【００３８】
現在のモード信頼レベルは、複数の異なる直交信頼レベルに依存して設定され得、３つ以上の直交信頼レベルがあり得ることにも留意されたい。したがって、例えば、一実装形態では、処理回路は、上で考察される異なる状態及び異なるセキュリティドメインの両方で動作することが可能であり得、現在のモード信頼レベルは、それらの要因の両方に依存して設定され得る。
【００３９】
ケイパビリティは、システム内の様々なロケーションに記憶することができる。例えば、装置は、処理回路による参照のためにケイパビリティを記憶するために使用されるケイパビリティレジスタのセットを有し得るが、１つ以上のケイパビリティを記憶するために使用され得るメモリ回路も有し得る。処理回路は、メモリ回路から選ばれたケイパビリティを、ケイパビリティレジスタのセットから選択されたケイパビリティレジスタにロードするためのロード動作を実施するように配設され得る。このプロセスの間、処理回路は、選択されたケイパビリティレジスタに記憶された選ばれたケイパビリティが、現在のモード信頼レベル又はメモリ回路に記憶された選ばれたケイパビリティのケイパビリティ信頼レベルを超えないように制約されたケイパビリティ信頼レベルを有するように、ケイパビリティ信頼レベルを選択的に修正するように配設され得る。したがって、メモリ回路内に依然として保持され得るケイパビリティの元のバージョンは、変更されたその関連付けられたケイパビリティ信頼レベルを有さないが、ケイパビリティレジスタに記憶されたバージョンは、そのケイパビリティ信頼レベルを制約し、したがって、ケイパビリティレジスタ内に記憶されたそのケイパビリティのケイパビリティ信頼レベルに依存して、そのロードされたケイパビリティを使用して実施される後続のメモリアクセス動作を制約するように、ロード動作中に処理回路によって変更されたそのケイパビリティ信頼レベルを有することができる。
【００４０】
ケイパビリティ信頼レベルのそのような選択的なデモーションは、標準ケイパビリティに適切であり得るが、封止されたケイパビリティが修正されないことが要件であるため、そのような活動は、封止されたケイパビリティに関して抑制される必要がある。したがって、例示的な一実装形態では、処理回路は、選択されたケイパビリティが封止されたケイパビリティであるときに、そのようなロード動作中にケイパビリティ信頼レベルの修正を禁止するように更に配設されている。封止されたケイパビリティの場合、封止されたケイパビリティ操作回路の以前に識別された活動が、あまり信頼されないコードがより信頼されている封止されたケイパビリティを使用することを防止するので、あまり信頼されないコードがより信頼されている封止されたケイパビリティを提供されることを可能にすることから生じるセキュリティ問題はない。
【００４１】
いくつかの実装形態では、ロード動作は、いくつかの事例では、通常のデータ（ケイパビリティではなく）をケイパビリティレジスタにロードするために実施され得、そのような事例では、ケイパビリティ信頼レベルに関連付けられるデータにおけるビットが、実際にはケイパビリティが修正されないデータであったことが重要であり得る。なぜなら、この場合、処理されているのはケイパビリティではなく、それらのビットを修正することはデータを破損するからである。したがって、例示的な一実装形態では、処理回路は、ロード動作中に、選ばれたケイパビリティが有効なケイパビリティである（ケイパビリティが封止されたケイパビリティではない）ことを識別する制御値を選ばれたケイパビリティが有するときに、ケイパビリティ信頼レベルのみを選択的に修正するように配設され得る。そのような手法によって、ロード動作中のケイパビリティ信頼レベルの上述の選択的修正は、実際に封止されていないケイパビリティがケイパビリティレジスタにロードされている場合にのみ実施される。
【００４２】
例示的な一実装形態では、封止されたケイパビリティ操作回路は、選択された封止され

たケイパビリティに対する開封要求を処理した結果を示す結果情報を生成するように配設されている。結果情報は、様々な形態を採ることができるが、一般に、ケイパビリティが首尾よく開封されたか否かに関する判定を行うことを可能にするのに十分である。例えば、開封が成功しなかった場合、障害が発生する可能性がある。あるいは、ソフトウェアに障害を示すために、１つ以上の状態フラグを設定することができる。別の例として、ケイパビリティが首尾よく開封されたことを識別するための指標をソフトウェアに返すことができ、必要に応じて、首尾よく開封されたケイパビリティが、現在のモード信頼レベルと正確に一致するケイパビリティ信頼レベルを有する状況を識別するための指標を提供することもできる。別の例として、失敗した開封動作は静かに失敗する場合があり、開封が成功したことを示す情報が生成されず、後で開封動作が失敗したことを判定するために使用される。

【００４３】

必要に応じて、封止要求を処理した結果を識別するために、例えば、封止動作が成功したか失敗したかを識別するために、結果情報を生成することもできる。例示的な一実装形態では、成功を仮定することができ、封止動作が失敗であった場合にのみ、情報が出力され得る。また更なる例示的な実装形態では、封止要求が成功したか失敗したかにかかわらず、情報は生成されない場合があり、失敗した封止動作は、後の段階で、例えば開封中に検出され得る。

【００４４】

いくつかの例示的な実装形態では、予約タイプであり、例えば、特定のイベント又は機能を示すためにアーキテクチャによって使用される、いくつかのケイパビリティがあり得る。例示的な一実装形態では、封止されたケイパビリティ操作回路は、現在のモード信頼レベルにかかわらず、そのようなケイパビリティの開封を禁止するように配設され得る。必要に応じて、そのようなケイパビリティを開封しようとする試みは、エラーがアサートされること、タグビットがクリアされてケイパビリティを効果的に無効にすること、又は何らかの他の指標がソフトウェアに提供されることをもたらす可能性がある。そのような予約タイプのケイパビリティが識別され得るいくつかの方法が存在する。特定の例として、それらは、例えば、上限が下限を下回ることによって、無効な範囲を定義する範囲境界情報を有し得る。

【００４５】

ここで、特定の例について、図を参照して説明する。

【００４６】

本明細書で説明する技法は、様々なデータ処理システムにおいて、そのようなシステム内の異なるタイプの処理回路に関連して採用することができる。例えば、本技法は、中央処理装置（ＣＰＵ）の形態を採る処理回路に関連して使用することができるが、代替的に、ダイレクトメモリアクセス（ＤＭＡ）コントローラ、暗号化アクセラレータなどの他の処理回路に関連して採用することもできる。純粋に以下の図１の用例として、ＣＰＵの処理パイプラインは、説明される技法が使用され得る処理回路の例として考慮される。

【００４７】

図１は、命令を処理するための処理パイプライン４を備えるデータ処理装置２の例を概略的に示す。この例では、処理パイプライン４は、フェッチステージ６、復号ステージ８、発行ステージ１０、実行ステージ１２、及びライトバックステージ１４を含む、多数のパイプラインステージを含むが、他のタイプのステージ又はステージの組み合わせが提供され得ることが理解されるであろう。例えば、レジスタリネームを実施するためのリネームステージが、いくつかの例示的な実装形態に含まれ得る。処理されることになる命令がステージからステージに移動し、ある命令が、１つのステージで保留中である間に、別の命令が、パイプライン４の異なるステージで保留中であり得る。

【００４８】

フェッチステージ６は、レベル１（Ｌ１）命令キャッシュ２０から命令をフェッチする。フェッチステージ６は通常、連続する命令アドレスから逐次的に命令をフェッチし得る

。しかしながら、フェッチステージは、分岐命令の結果を予測するための分岐予測器２２も有し得、フェッチステージ６は、分岐が行われたと予測される場合に（非逐次的な）分岐先アドレスから、又は分岐が行われなかったと予測される場合に次の逐次アドレスから命令をフェッチすることができる。分岐予測器２２は、ある分岐が行われる可能性が高いかどうかを予測するための情報を記憶するための１つ以上の分岐履歴テーブルを含み得る。例えば、分岐履歴テーブルは、従前に実行された分岐の実際の結果を追跡するための、又は分岐のために行われた予測の信頼度を表すためのカウンタを含み得る。分岐予測器２２は、分岐命令の従前の目標アドレスを、同じ分岐命令に後で遭遇した際に、それらが予測され得るように、キャッシュするための分岐先アドレスキャッシュ（branch target address cache、ＢＴＡＣ）２４も含み得る。

【００４９】

フェッチされた命令は、命令を復号して復号された命令を生成する復号ステージ８に渡される。復号された命令は、実行ステージ１２を制御して適切な処理動作を実行するための制御情報を含み得る。キャッシュ２０からフェッチされたいくつかのより複雑な命令に対して、復号ステージ８は、それらの命令を復号された複数の命令（マイクロオペレーション（μｏｐ又はｕｏｐ）として知られ得る）にマッピングし得る。それゆえに、Ｌ１命令キャッシュ２０からフェッチされた命令と、パイプラインの後のステージで見られる命令との間に１対１の関係が存在しない場合がある。概して、本出願における「命令」に対する参照は、マイクロオペレーションを含むものと解釈されるべきである。

【００５０】

復号された命令は、発行ステージ１０に渡され、これは、命令の実行に必要なオペランドが利用可能であるかどうかを判定し、オペランドが利用可能である場合に実行のための命令を発行する。いくつかの例示的な実装形態は、Ｌ１命令キャッシュ２０から命令がフェッチされたプログラム順序に対応する順序での実行のための命令が発行されるように、インオーダ処理をサポートし得る。他の例示的な実装形態は、プログラム順序とは異なる順序で実行ステージ１２に命令を発行できるようにアウトオブオーダ実行をサポートし得る。アウトオブオーダ処理は、先の命令がオペランド待ちの間停止させられている間に、そのオペランドが利用可能である、プログラム順序では後の命令を先に実行できるため、性能向上に有用であり得る。

【００５１】

発行ステージ１０は、様々なデータ処理動作を実施するために命令が実行される実行ステージ１２に命令を発行する。例えば、実行ステージは、整数値に算術演算又は論理演算を行うための算術／論理ユニット（arithmetic/logic unit、ＡＬＵ）３０、浮動小数点形式で表された値に演算を行うための浮動小数点（floating-point、ＦＰ）ユニット３２、及びレベル１（Ｌ１）データキャッシュ３６からレジスタ４０にデータ値をロードするためのロード動作、又はレジスタ４０からＬ１データキャッシュ３６にデータ値を記憶するための記憶動作を行うためのロード／記憶ユニット３４を含む、いくつかの実行ユニット３０、３２、３４を含み得る。これらは、提供され得る実行ユニットのタイプのほんのいくつかの例であり、多くの他の種類が提供され得ることが理解されるであろう。処理動作を行うために、実行ステージ１２は、レジスタ４０のセットからデータ値を読み取り得る。次いで、実行された命令の結果は、ライトバックステージ１４によってレジスタ４０にライトバックされ得る。

【００５２】

Ｌ１命令キャッシュ２０及びＬ１データキャッシュ３６は、複数のレベルのキャッシュを含むキャッシュ階層の一部であり得る。例えば、レベル２（Ｌ２）キャッシュ４４も提供され得、任意選択的に、キャッシュの更なるレベルが提供され得る。この例では、Ｌ２キャッシュ４４は、Ｌ１命令キャッシュ２０とＬ１データキャッシュ３６との間で共有されるが、他の例は、別個のＬ２命令キャッシュ及びデータキャッシュを有し得る。フェッチされることになる命令がＬ１命令キャッシュ２０にないときには、それをＬ２キャッシュ４４からフェッチすることができ、同様に、命令がＬ２キャッシュ４４にない場合、そ

れをメインメモリ５０からフェッチすることができる。同様に、ロード命令に応答して、データがＬ１データキャッシュ３６にない場合、それをＬ２キャッシュ４４からフェッチすることができ、必要とされる場合、メモリ５０からフェッチすることができる。キャッシュ階層を管理するために、任意の既知のスキームを使用し得る。

【００５３】

プログラム命令及びデータ値を参照するためにパイプライン４によって使用されるアドレスは、仮想アドレスであり得るが、少なくともメインメモリ５０、及び任意選択的に、少なくともいくつかのレベルのキャッシュ階層も、物理的にアドレス指定され得る。したがって、トランスレーションルックアサイドバッファ（translation lookaside buffer、ＴＬＢ）が、パイプライン４によって使用される仮想アドレスをキャッシュ又はメモリにアクセスするために使用される物理アドレスに変換するために（例えば、後でより詳細に説明するメモリアクセスチェック回路５２内に）提供され得る。例えば、ＴＬＢは、仮想アドレス空間の対応するページの仮想ページアドレスと、対応するページ内の仮想アドレスを物理アドレスに変換するために仮想ページアドレスがマッピングされるべき対応する物理ページアドレスとをそれぞれが指定する、多数のエントリを含み得る。例えば、仮想ページアドレス及び物理ページアドレスは、対応する仮想アドレス及び物理アドレスの最上位部分に対応し得、仮想アドレスを物理アドレスにマッピングするときに残りの最下位部分は変化しないままである。アドレス変換情報と同様に、各ＴＬＢエントリは、アドレスのあるページがパイプライン４のあるモードでアクセス可能であるかどうかを示すような、アクセス許可を指定するいくつかの情報も含み得る。いくつかの例示的な実装形態では、ＴＬＢエントリは、読み取り又は書き込み動作に応答して更新されるレベルのキャッシュ階層を定義するキャッシュポリシー情報など、アドレスの対応するページの他の特性（例えば、キャッシュがライトバックモードで動作するべきか、若しくはライトスルーモードで動作するべきか）、又は対応するページ内のアドレスに対するデータアクセスを、パイプライン４によって発行されたデータアクセスの順序と比較して、メモリシステムによって再順序付けできるかどうかを定義する情報を定義することもできる。

【００５４】

単一レベルＴＬＢが使用され得るが、代わりに、レベル１（Ｌ１）ＴＬＢが、いくつかの最近アクセスされたページにおいてアドレスを変換するためのＴＬＢエントリを含み得、レベル２（Ｌ２）ＴＬＢがより多数のページのエントリを記憶するために提供され得るように、ＴＬＢの階層が提供され得ることが理解されよう。必要とされるエントリがＬ１ＴＬＢに存在しないときには、それをＬ２ＴＬＢ、又は階層内の更なるＴＬＢからフェッチすることができる。アクセスされるページのために必要とされるエントリがいずれのＴＬＢにもない場合、メモリ５０内のページテーブルにアクセスするために、ページテーブルウォークを実施することができる。本技法では、任意の既知のＴＬＢ管理スキームを使用することができる。

【００５５】

また、いくつかのシステムは、複数のレベルのアドレス変換をサポートし得、その結果、例えば、第１のＴＬＢ（又はＴＬＢ階層）を使用して仮想アドレスを中間アドレスに変換し得、かつ１つ以上の更なるＴＬＢを使用する第２のレベルのアドレス変換が、中間アドレスを、キャッシュ又はメモリにアクセスするために使用する物理アドレスに変換し得ることが理解されよう。これは、例えば、第１のレベルのアドレス変換がオペレーティングシステムによって管理され得、第２のレベルのアドレス変換がハイパーバイザによって管理され得る、仮想化をサポートするのに有用であり得る。

【００５６】

図１に示すように、装置２は、有界ポインタレジスタ６０のセットを有し得る。有界ポインタレジスタのセットは、汎用データレジスタ４０のセットとは物理的に別個のものとして図１に示しているが、代替的かつ例示的な実装形態では、汎用データレジスタと有界ポインタレジスタの両方を提供するために同じ物理的ストレージを使用し得る。

【００５７】

各有界ポインタレジスタ６０は、アクセスされることになるデータ値のアドレスを判定するために使用し得るポインタ値６２と、対応するポインタ６２を使用するときのアドレスの許容範囲を指定する範囲情報６４とを含む。有界ポインタレジスタ６０は、ポインタの使用に関する１つ以上の制限／許可を定義し得る制限情報６６（本明細書では許可情報とも称される）も含み得る。例えば、制限６６は、ポインタ６２を使用し得る命令のタイプ、又はポインタを使用し得るパイプライン４のモードを制限するために使用することができる。それゆえに、範囲情報６４及び制限情報６６は、その中でポインタ６２の使用が許可されるケイパビリティを定義すると考えられ得る。定義されたケイパビリティ外でポインタ６２を使用する試みが行われると、エラーをトリガすることができる。範囲情報６４は、例えば、ポインタがある既知の境界内に留まり、かつセンシティブな情報又はセキュアな情報を含む可能性があるメモリアドレス空間の他の領域に迷い込まないことを確実にするために、有用であり得る。汎用データレジスタと有界ポインタレジスタの両方に同じ物理的ストレージを使用する例示的な実装形態において、例示的な一実装形態では、ポインタ値６２は、例えば、対応する汎用レジスタのために使用されるのと同じ記憶ロケーション内に記憶され得る。

【００５８】

図２は、データ又は命令に対する不正アクセスから保護するために許容範囲が使用される命令のタイプの例を示す。図２の頂部に示すように、特定の有界ポインタレジスタＰＲ１が、所与のポインタ値６２と、この例では、許容範囲の下側境界を定義する下側境界アドレス６８及び許容範囲の上側境界を定義する上側境界アドレス６９を使用して指定される、範囲情報６４とを含む。例えば、境界６８、６９は、８００００～８１０００のアドレス範囲を定義するように設定される。ある命令が有界ポインタレジスタＰＲ１を参照し、ポインタ６２から判定されたアドレスがこの範囲外である場合に、エラーがトリガされ得る。

【００５９】

例えば、図２の部分Ａに示すように、いくつかのシステムでは、ポインタレジスタ６０内のポインタ６２の値を、範囲情報６４によって指定された範囲外にある値（ここでは、ポインタがアドレスを直接指定すると仮定する）に設定する試みがある場合、エラーがトリガされ得る。これは、ポインタを使用するアクセスが許容範囲内に間違いなくあることを確実にできるように、ポインタ６２が指定範囲外の値を取ることが回避させる。代替的に、図２の部分Ｂに示すように、命令が、ポインタ６２のアドレスによって識別された位置へのアクセスを試み、そのアドレスが指定範囲外にあるときに、エラーをトリガすることができる。それゆえに、ポインタ６２を指定範囲外の値に設定することは許容できるが、ポインタアドレス（又はポインタから導き出されたアドレス）のデータアクセスが試みられ、アドレスが許容範囲外にある場合、エラーがトリガされ得る。他のシステムは、図２の部分Ａ及びＢに示す両方の命令のタイプに応答してエラーをトリガし得る。

【００６０】

範囲情報６４は、異なる方法で設定され得る。例えば、セキュリティコード、又はオペレーティングシステム若しくはハイパーバイザが、所与のポインタに対して許可された範囲を指定し得る。例えば、命令セットアーキテクチャは、所与のポインタ６２に対する範囲情報６４を設定又は修正するためのいくつかの命令を含み得、これらの命令の実行は、プロセッサ４の特定のソフトウェア又は特定のモード又は例外状態に制限することができる。範囲情報６４を設定又は修正するための任意の既知の技法が使用され得る。

【００６１】

ポインタを参照するある命令を実行するときに実行状態１２で使用し得る有界ポインタ記憶要素６０のセットに加えて、命令がレベル１命令キャッシュ２０からフェッチされるときに、フェッチステージ６で同様の機能を提供するためにプログラムカウンタケイパビリティ（program counter capability、ＰＣＣ）レジスタ８０も使用され得る。具体的には、プログラムカウンタポインタは、フィールド８２に記憶され得、ＰＣＣ８０は、有界ポインタ記憶要素６０のセット内のポインタの各々に提供される範囲及び制限情報

と同様の、範囲情報８４及び任意の適切な制限情報８６も提供する。

【００６２】

図３は、個々のデータブロックがケイパビリティ（すなわち、有界ポインタ及び関連付けられた制限情報）を表すか、又は通常データを表すかを識別するために、それらのデータブロックに関連してタグビットがどのように使用されるかを概略的に示している。具体的には、メモリアドレス空間１１０は、指定されたサイズを典型的に有する一連のデータブロック１１５を記憶する。純粋に例示のために、この例では、各データブロックが１２８ビットを含むと仮定されるが、他の例示的な実装形態では、異なるサイズのデータブロック、例えば、ケイパビリティが６４ビットの情報によって定義されるときの６４ビットデータブロックが使用され得る。各データブロック１１５に関連して、一例では、タグビットと称される単一ビットフィールドであるタグフィールド１２０が提供され、これは、関連付けられたデータブロックがケイパビリティを表すことを識別するために設定され、関連付けられたデータブロックが通常データを表し、それゆえにケイパビリティとして取り扱えないことを示すためにクリアされる。設定又はクリア状態に関連付けられた実際の値は、例示的な実装形態に依存して変化し得るが、純粋に例示のために、例示的な一実装形態では、タグビットが１の値を有する場合に、関連付けられたデータブロックがケイパビリティであることを示し、それが０の値を有する場合に、関連付けられたデータブロックが通常データを含むことを示すことが理解されるであろう。

【００６３】

ケイパビリティが、図３に示されるケイパビリティレジスタ１００などの有界ポインタレジスタ６０（本明細書ではケイパビリティレジスタとも称される）のうちの１つにロードされるときに、タグビットはケイパビリティ情報と共に移動する。したがって、ケイパビリティレジスタ１００にケイパビリティがロードされた場合、ポインタ１０２、範囲情報１０４及び制限情報１０６（以下、許可情報と称される）がケイパビリティレジスタにロードされることになる。加えて、そのケイパビリティレジスタに関連して、又はそのうちの特定のビットフィールドとして、タグビット１０８は、コンテンツがケイパビリティを表すことを識別するために設定されることになる。同様に、ケイパビリティがメモリからストアバックされた場合、関連するタグビット１２０は、ケイパビリティが記憶されているデータブロックに関連して設定される。そのようなアプローチにより、ケイパビリティと通常データを区別し、それゆえに、通常データがケイパビリティとして使用できないことを確実にする。

【００６４】

図１に戻ると、装置２には、アクセス要求が、ケイパビリティによって識別された制約情報に基づいて許可されるかどうかを判定するために、所与のケイパビリティを使用してそのメモリアドレスが生成される所与のアクセス要求に関連してケイパビリティチェック動作を実施することができるケイパビリティチェック回路３３が提供され得る。これは、例えば、先に考察される範囲情報及び制限／許可情報を参照して実施することができ、これらは、まとめてケイパビリティの制約情報と称され得る。したがって、純粋に例として、メモリアドレスへの書き込みアクセス要求は、ケイパビリティが読み取りにのみ使用され、書き込みには使用されないことを示すケイパビリティを使用して実施されることを求めている場合、ケイパビリティチェック回路３３は、アクセス要求を進めることができないと判定し得、例えば、そのような状況下で障害信号を発行し得る。

【００６５】

しかしながら、ケイパビリティチェック動作に合格すると仮定すると、メモリアクセス要求は、アクセスに進むことを許可されることを確実にするために、いくつかの更なるチェックを提供することができるメモリアクセスチェック回路５２に伝搬され得る。例えば、処理回路は、複数の異なる動作モードで動作することが可能であり得、各動作モードは、例えば、特定の特権状態、及び／又は装置が動作している特定のセキュリティドメインに関連付けられ得、メモリの特定の領域は、処理回路が可能な動作モードのうちの１つ又はサブセットで動作しているときにのみアクセス可能であり得る。

【００６６】
メモリアクセスチェック回路５２はしたがって、メモリアドレス空間の様々な領域に対して指定された属性データに基づいて、メモリシステムへのアクセスが許可されているかどうかをチェックし得る。メモリアクセスチェック回路は、メモリアドレス空間の対応する領域のそれぞれに関連するセキュリティドメインを定義するセキュリティドメイン定義データを記憶するセキュリティ属性ユニット（ＳＡＵ）５６を含み得る。セキュリティ属性データに基づいて、セキュリティ属性ユニット５６は、メモリアクセスが許可されているかを、処理回路の動作の現在のセキュリティドメインと、目標アドレス及びメモリアクセスを含む領域に関連するセキュリティドメインと、に依存して、チェックすることができる。他の実装形態では、ＳＡＵ５６は、セキュリティドメイン定義データを直接記憶するのではなく、メモリアクセスチェックを実施するために、他のロケーションに記憶されたセキュリティ定義データにアクセスし得る。いくつかのシステムにおいて、セキュリティドメイン定義データは、メモリシステム５０に記憶され得るか、又はシステム２内の他のロケーションで構成レジスタに記憶され得る。

【００６７】
処理回路４は、動作の現在のセキュリティドメインにおいて動作し得、動作の現在のセキュリティドメインは、概して、現在実行されている命令のアドレスに関連付けられたセキュリティドメインに対応し得る（ただし、例えば、ドメイン間の移行を処理するときに、いくつかの例外があり得る）。セキュアドメインで動作している間、処理回路は、セキュアドメイン及び低セキュアドメインの両方に関連するメモリ領域内のデータにアクセスすることができ、低セキュアドメインで動作するときは、処理回路は低セキュアドメインに関連する領域内のデータにアクセスすることはできるが、ＳＡＵ５６がセキュアドメインに関連すると指定するアドレス空間の領域内のデータにアクセスすることは許可されないことがある。これにより、低セキュアドメインで動作しているコードからの不正アクセスに対する機密データの保護が可能になる。本明細書でより詳細に考察されるように、ＳＡＵ５６は、アクセスを進めることができるかどうかを判定するためにそのようなチェックを実施しているときに、処理回路の現在のセキュリティドメインだけでなく、考慮されている個々のアクセス要求に関連付けられた詳細情報も考慮する。この詳細情報は、処理回路のセキュリティドメイン、及びアクセス要求のメモリアドレスを生成するために使用されるケイパビリティに関連付けられた信頼レベル指標の両方に基づく。

【００６８】
また、図１を参照すると、メモリアクセスチェック回路５２は、メモリシステム５０へのメモリアクセスがアクセス許可を満たすかどうかをチェックするメモリ保護ユニット（ＭＰＵ）５４を含み得、アクセス許可は、例えば、処理回路４のどの特権レベルがメモリの所与の領域にアクセスすることが可能にされているかを指定し得るか、又はアドレス空間のメモリ領域が、読み取り動作及び書き込み動作の両方によってアクセスされ得るか、若しくは書き込みが禁止されている読み取り専用領域であるかを指定し得る。ＭＰＵ５４によって使用されるアクセス許可は、特権の低いプロセス（アプリケーションなど）が、メモリのどの領域に、どのように（読み出し専用又は読み出し／書き込み）アクセスすることを許可されるかを制御するために、例えば、特権の高いプロセス（ハイパーバイザ又はオペレーティングシステムなど）によって指定され得る。ＭＰＵ５４によって提供される許可は、ＳＡＵ５６によって提供される許可とは独立していてもよく、よって、所与のメモリアクセス要求が許可されるためには、ＭＰＵ５４及びＳＡＵ５６の両方について定義されたアクセス許可に基づくチェックに合格しなければならない。ＭＰＵ５４は、図１に単一のエンティティとして示されているが、いくつかの例では、それぞれがセキュリティドメインの１つに関連する別個のセキュアＭＰＵ及び低セキュアＭＰＵが提供され得、よって、現在のドメインがセキュアドメインであるか低セキュアドメインであるかに依存して、メモリの所与の領域に異なるメモリアクセス許可を指定することができる（例えば、ある領域は低セキュアドメインでは読み出し専用であるが、セキュアドメインでは読み出し可能及び書き込み可能である）。

【００６９】
ＳＡＵの先の考察と同様に、ＭＰＵがそのアクセス許可チェックを実施しているとき、ＭＰＵは、処理回路の現在の動作モードだけでなく、メモリアドレスを生成するために使用されるケイパビリティに関連付けられたケイパビリティ信頼レベルにも依存する、所与のアクセス要求に関連付けられた信頼レベルを考慮に入れることができる。
【００７０】
１つ以上の制御レジスタ９０が、本明細書で説明する実装形態によって提供される特定の特徴のためのイネーブル／ディセーブルフラグを記憶するために提供され得る。特定の例として、処理回路の現在の動作モードの信頼レベルよりも低い信頼レベルを有する不変ケイパビリティを選択的に修正することが可能であり得るが、この挙動は、制御レジスタ９０内の別個のビットによって制御することができる。同様に、処理回路の特権の低い動作モード内から、関連付けられたより高い信頼レベルを有するケイパビリティを逆参照しようとするときに障害が発生する場合があり、この場合もやはり、そのような機能は、制御レジスタ９０内のイネーブル制御ビットによってゲート制御される可能性がある。また後で考察されるように、ケイパビリティはメモリからケイパビリティレジスタにロードされ得、このプロセス中に、ロードされているケイパビリティの関連付けられた信頼レベルが選択的にデモートされ得るが、この場合も、そのような機能は、制御レジスタ９０における別個の制御ビットによって制御され得る。
【００７１】
本明細書で説明する技法によれば、ケイパビリティは、関連付けられたケイパビリティ信頼レベル情報と共に提供され、その信頼レベル指標は、メモリアクセスチェック回路５２によって実装されたメモリアクセスチェック手順に織り込まれ得る。この信頼レベルの指標がケイパビリティに関連して提供され得る様々な方法があるが、図４は、例示的な一実装形態を例示する。図４に示される例では、ケイパビリティ１００は、ポインタ値１０２及び何らかの範囲情報１０４（本明細書では境界情報とも称される）を含む。データの対応するブロックがケイパビリティとして取り扱われるべきかどうかを識別するために設定又はクリアされ得る前述のタグビット１０８と共に、許可のセットもケイパビリティ内に提供され得る。
【００７２】
ケイパビリティに対して指定された許可は、実装形態に依存して変化し得るが、例示的な一実装形態では、許可は、読み取りアクセスのためのメモリアドレスを生成するためにケイパビリティが使用され得るかどうかを値が示す読み取り許可ビット１３０、書き込みアクセスのためのメモリアドレスを生成するためにケイパビリティが使用され得るかどうかを値が示す書き込み許可ビット１３２、並びにフェッチ及び実行される命令のメモリアドレスを生成するためにケイパビリティが使用され得るかどうかを値が示す実行許可ビット１３４を含む。例えば、ケイパビリティが不変であると考えられるかどうかを示すために、ケイパビリティ内で他の情報を識別することができる。そのような情報は、ケイパビリティ内における追加情報として直接指定することができるが、いくつかの例示的な実装形態では、ケイパビリティ内に既に提供されている他の情報の状態から推論することができる。例えば、１つの特定の実装形態では、実行ビットが設定されているときに、ケイパビリティは不変であるとみなされ、ケイパビリティによって指定された情報は、命令実行から生じ得るポインタ値の通常の増分を介する場合を除いて、タグビットをクリアする（事実上ケイパビリティを無効化する）ことなく修正することができない。
【００７３】
図４に示すように、例示的な一実装形態では、許可フィールドは、信頼レベル指標フィールド１３６を提供するように拡張され、信頼レベル指標は、ケイパビリティ１００に関連付けられた信頼レベルを識別する。信頼レベルは、ケイパビリティ１００のフィールド１３６に直接符号化することができるか、又は代替的に、信頼レベル指標フィールド１３６は、信頼レベル情報を含むメモリアドレスを示すために使用される識別子を提供することができる。このような識別子は、信頼レベル情報のメモリロケーションを直接示すこと

ができるか、又は、例えば、信頼レベル情報を含むロケーションを識別するために、システムにおけるグローバルレジスタに記憶されたアドレスに適用することができるオフセットを指定することができる。

【００７４】

図５Ａは、例示的な一実装形態による、ケイパビリティ信頼レベル情報がメモリへのアクセスを制約するためにどのように使用されるかを概略的に例示するブロック図である。この例では、処理回路１５０は、メモリアドレスが所与のケイパビリティを使用して生成されるアクセス要求が考慮されているときに、所与のケイパビリティによって識別される制約情報に基づいてそのアクセス要求が許可されるかどうかを判定するためのケイパビリティチェック動作を実施するために使用され得るケイパビリティチェックブロック１５５を含む。したがって、ケイパビリティチェックは、アクセスに進むことを許可されるかどうかを判定するために、ケイパビリティの範囲及び許可情報への参照を伴い得る。ケイパビリティチェックに不合格であった場合、不合格指標を処理回路に提供することができ、これは、例えば、障害信号などの様々な形態を採ることができる。しかしながら、ケイパビリティチェックに合格した場合、これは、信頼レベル生成ブロック１６０に示され、信頼レベル生成ブロック１６０は、ケイパビリティ１００のケイパビリティ信頼レベル情報１３６も受信する。

【００７５】

ケイパビリティ信頼レベルに加えて、信頼レベル生成ブロック１６０はまた、現在のモード信頼レベルの指標を受信し、これは、処理回路の現在の動作モードに関連付けられた信頼レベルである。次いで、ケイパビリティ信頼レベル及び現在のモード信頼レベルの両方が、アクセス要求に対する信頼レベルを形成するために組み合わせて使用され、アクセス要求は、パス１６５を介して発行された要求のメモリアドレスに関連してパス１６７を介して伝搬される。信頼レベル生成ブロック１６０が、現在のモード信頼レベル及びケイパビリティ信頼レベルの両方を使用して、アクセス要求に対する信頼レベルを決定することができる様々な方法があるが、例示的な一実装形態では、アクセス要求に関連付けられた信頼レベルは、現在のモード信頼レベル及びケイパビリティ信頼レベルのうちの、より低い信頼レベルを表す方に制約される。

【００７６】

メモリアクセスチェック回路１７０は、要求のメモリアドレス、及びアクセス要求に対する関連付けられた信頼レベルの両方を受信し、異なるメモリ領域に対して指定され得る記憶されたアクセス許可情報１７５を参照して、メモリアクセスチェック動作を実施することができる。特に、いくつかの異なるメモリ領域の各々について、アクセス許可情報は、アクセスに進むことを可能にするためにアクセス要求に提供される必要がある要求される信頼レベルを効果的に示すことができる。パス１６７を介して受信されたアクセス要求に対する信頼レベルが、要求された信頼レベルを満たさない場合、アクセスは不合格にされ得、そうでない場合、メモリへのアクセスは、メモリアクセスチェック回路１７０からパス１８０を介して伝搬させることができる。

【００７７】

先に論じたように、本明細書で説明する技法によれば、個々のケイパビリティに関連するケイパビリティ信頼レベルの提供は、オブジェクトタイプ及び開封許可を示すために不十分なメタデータビットを利用する必要性を回避し、鍵を開封する必要性も回避する、封止されたケイパビリティを操作するための軽量機構を提供するためにも活用される。

【００７８】

特に、本明細書で説明する技法によれば、関連付けられたケイパビリティが封止されているか、又は開封されているかを識別するために、封止フラグフィールド１３８がケイパビリティに追加され、この封止フラグフィールド１３８は図４に例示されている（本明細書ではＩｓＳｅａｌｅｄフラグと呼ばれることもある）。一実装形態では、これは、ケイパビリティが封止されていることを示す一方の状態（例えば、ロジック１値）と、ケイパビリティが開封されていることを示す他方の状態（例えば、ロジック０値）とを有する単

一ビットであり得る。しかしながら、封止フラグが単一のビット値である必要はなく、いくつかの実装形態では、いくつかの追加情報を取り込むためにマルチビット値が使用され得る。

【００７９】

更に、図５Ａに示されるように、封止されたケイパビリティ操作回路１８５は、封止されたケイパビリティをどのように操作するかを判定するために使用される。封止されたケイパビリティ操作回路１８５は、別個の構成要素として提供されてもよく、又は図５Ａに示されるように処理回路１５０内に組み込まれてもよい。封止されたケイパビリティを操作するとき、封止されたケイパビリティ操作回路１８５は、封止キー又は開封キーを使用する必要はないが、代わりに、処理回路１５０に関連付けられた現在のモード信頼レベルと組み合わせて、所与のケイパビリティがどのように操作されるべきかを査定するために、その所与のケイパビリティに関連して取り込まれたケイパビリティ信頼レベルの情報を参照することができる。この情報に基づいて、封止されたケイパビリティ操作回路１８５は、例えば、所与のケイパビリティを封止することができるかどうかを判定することができ、その場合、必要なのは、封止されたケイパビリティ操作回路が封止フラグを設定させることだけであり、所与の封止されたケイパビリティを開封することができるかどうかを判定することができ、その場合、必要なのは、封止されたケイパビリティ操作回路が封止フラグをクリアさせることだけであり、封止されたケイパビリティのケイパビリティ信頼レベルと処理回路の現在のモード信頼レベルとの比較に応じて、処理回路によって封止されたケイパビリティをどのように使用することができるかを判定することができる。

【００８０】

図５Ｂは、例示的な一実施形態における図５Ａの回路の動作を例示する流れ図である。ステップ２００において、アクセス要求が必要であると判定される。その後、ステップ２０５において、アクセス要求に対して指定されたケイパビリティが封止されたケイパビリティであるか否かが判定される。そうである場合、ステップ２１０において、封止されたケイパビリティの使用が可能になるかどうかが判定され得る。いくつかの実装形態では、メモリアドレスを生成するために封止されたケイパビリティを逆参照することができない場合が常にあり得（その代わりに、そのような封止されたケイパビリティが最初に開封される必要がある）、その場合、プロセスは、ステップ２１０のチェックを実施する必要なしに直接ステップ２１５に進むことができ、それによってアクセス要求が防止される。しかしながら、いくつかの実装形態では、処理回路の現在のモードの相対的な信頼レベル及び指定されたケイパビリティのケイパビリティ信頼レベルに応じて、最初に開封される必要なく、封止されたケイパビリティが使用されるように提供されてもよい。例えば、一実装形態では、現在のモード信頼レベルがケイパビリティ信頼レベル以上である場合、封止されたケイパビリティの使用が可能になり得る。

【００８１】

したがって、ステップ２１０において、封止されたケイパビリティの使用が可能であると判定された場合、プロセスはステップ２２０に進み、実際には、先のステップ２０５において、指定されたケイパビリティが封止されたケイパビリティではないと判定された場合もステップ２２０に進む。しかしながら、ステップ２１０において、封止されたケイパビリティの使用が可能でないと判定された場合、プロセスはステップ２１５に進み、アクセス要求の発生が防止される。アクセス要求が防止され得るいくつかの方法がある。例えば、ケイパビリティチェック失敗信号がアサートされ得るか、又は、アクセス要求が封止されたケイパビリティを使用して試みられたことを識別するために、何らかの他の活動を行うことができる。

【００８２】

プロセスがステップ２２０に進むと仮定すると、そのステップにおいて、アクセス要求のためのメモリアドレスが、指定されたケイパビリティのポインタ値を参照して判定される。ステップ２２５において、アクセスを進めることができるかどうかを判定するために、指定されたケイパビリティの境界及び許可情報を参照して、ケイパビリティチェックが

実施される。

【００８３】

したがって、ステップ２３０において、ケイパビリティチェックに合格したかどうかが判定され、合格していない場合、プロセスはステップ２３５に進み、ケイパビリティチェック失敗信号がアサートされる。ステップ２３５は、例示的な一実装形態では、ステップ２１５と同じ方法で実装され得る。

【００８４】

典型的には、ステップ２２５でケイパビリティチェックを実施するとき、信頼レベル情報は使用されないが、代わりに、メモリアクセスチェック回路１７０に渡すために保持される。しかしながら、いくつかの実装形態では、信頼レベル情報は、ケイパビリティチェックプロセス中に使用することもできる。例えば、処理回路は、所与のアクセス要求のためのメモリアドレスを生成するために使用されているケイパビリティに関連付けられたケイパビリティ信頼レベルが、処理回路の現在の動作モードに関連付けられた現在のモード信頼レベルを超える状況において、そのアクセス要求によって識別されたアクセスを実施する試みがなされたときに、ステップ２３５で障害信号を発行するように配設され得る。特に、いくつかの実装形態では、ある特定の信頼レベルで動作する処理回路が、より高いケイパビリティ信頼レベルを有するケイパビリティを利用しようとすることは、正しくない挙動であるとみなされ得る。

【００８５】

ステップ２３０において、ケイパビリティチェックに合格したと判定される場合、次いで、ステップ２４０において、現在のモード信頼レベル及びケイパビリティ信頼レベルの両方に基づいて、信頼レベル生成ブロック１６０によって、アクセス要求に対する信頼レベルが判定される。その後、ステップ２４５において、アクセス要求は、アクセス要求に対する判定された信頼レベルと共にメモリアクセスチェック回路１７０に伝搬され、その結果、メモリアクセスチェック回路１７０は、アクセス要求に対するその示された信頼レベルに基づいて、アクセス許可チェックを実施することができる。

【００８６】

図６は、例示的な一実装形態による、封止要求を処理するときに実施されるステップを例示する流れ図である。封止要求は、様々な方法で生成され得るが、例示的な一実装形態では、処理回路が封止命令を実行した結果として生じ得る。ステップ３００において、封止要求が受信されたかどうかが判定され、そうである場合、任意選択のステップとして、ステップ３０５において、現在のモード信頼レベルにおいて封止が可能であるかどうかが判定され得る。いくつかの実装形態では、実装形態は原則として、以下で説明する更なるチェックを条件として、任意の現在のモード信頼レベルで封止することを可能にし得るので、そのようなチェックは不要であるとみなされ得る。しかしながら、代替的な実装形態では、封止をある特定の動作モードに限定することができ、その場合、ステップ３０５でのチェックを実施することができる。

【００８７】

現在のモード信頼レベルにおいて封止が可能でないと判定された場合、ステップ３１０において、識別されたケイパビリティの封止が防止される。ステップ３１０において、装置は、例えば、失敗信号をアサートすることによって、又はある特定の状態フラグを更新することによって、封止プロセスの失敗を識別するための情報を更に出力し得る。しかしながら、代替的な実装形態では、封止の失敗は、後の段階で、例えば後続の開封プロセス中にピックアップされるように配設することができるので、封止プロセスの成功又は失敗の何らかの指標を出力することは不要であると考えることができる。

【００８８】

ステップ３０５において、現在のモード信頼レベルにおいて封止が可能であると判定された場合、又は任意選択のステップ３０５が実施されない場合にステップ３００において封止要求が受信されたときはいつでも、プロセスはステップ３１５に進み、識別されたケイパビリティのケイパビリティ信頼レベルが判定される。図４を参照して前述したように

、この情報は、例えば、ケイパビリティにおいて、特に信頼レベル指標フィールド１３６において直接利用可能であってもよい。

【００８９】

ステップ３２０では、次いで、封止されたケイパビリティ操作回路１８５は、処理回路の現在のモード信頼レベルが、識別されたケイパビリティのケイパビリティ信頼レベル以上であるかどうかを判定する。そうでない場合、プロセスはステップ３１０に進み、識別されたケイパビリティの封止が防止される。

【００９０】

しかしながら、現在のモード信頼レベルがケイパビリティ信頼レベル以上であると仮定すると、プロセスはステップ３２５に進み、識別されたケイパビリティは、封止フラグ１３８を設定することによって封止される。ステップ３１０を参照して前述したのとほぼ同じ方法で、所望であれば、装置は、ケイパビリティの封止が成功したことを示す情報を出力するように配設されてもよい。しかしながら、例示的な一実装形態では、封止が成功したと仮定され、したがって情報は出力されない。封止が失敗であった場合、これは、ステップ３１０において出力された情報によって示されてもよく、又は、先に述べたように、後の段階で、例えば、ケイパビリティの開封中にピックアップされてもよい。

【００９１】

図７は、開封要求が受信されたことに応答して実施されるステップを例示する流れ図である。ステップ３５０でそのような要求が受信されると、任意選択のステップ３５５として、現在のモード信頼レベルで開封が可能であるかどうかを判定することができる。図６の封止プロセスにおける同等のステップ３０５に関して前述したように、必要に応じて、開封する能力を特定の動作モードに限定することができる。しかしながら、例示的な一実装形態では、そのような一般的な制限は課されず、したがって、ステップ３５５は必要とされない。

【００９２】

ステップ３５５が実装され、現在のモード信頼レベルにおいて開封が可能でないと判定された場合、ステップ３６０において、識別されたケイパビリティの開封が防止される。開封が失敗したことを識別するために、この時点で情報が出力されてもよい。例えば、障害信号を発生させることができ、あるいはソフトウェアに障害を示すために１つ以上の状態フラグを設定することができる。別の例として、失敗した開封動作は静かに失敗する場合があり、開封が成功したことを示す情報が生成されず、後で開封動作が失敗したことを判定するために使用される。

【００９３】

ステップ３５５において、現在のモード信頼レベルにおいて開封が可能であると判定された場合、又はステップ３５５が必要とされない場合にステップ３５０における開封要求に直接応答して、プロセスはステップ３６５に進み、識別されたケイパビリティのケイパビリティ信頼レベルが、信頼レベル指標フィールド１３６を参照して判定される。

【００９４】

次に、ステップ３７０において、現在のモード信頼レベルがケイパビリティ信頼レベル以上であるかどうかが判定され、そうでない場合、ステップ３６０において、識別されたケイパビリティの開封が防止される。

【００９５】

しかしながら、現在のモード信頼レベルがケイパビリティ信頼レベル以上であると仮定すると、ステップ３７５において、封止フラグをクリアすることによって、識別されたケイパビリティが開封される。必要に応じて、この時点で情報を出力して、ケイパビリティの開封が成功したことを示すことができる。特定の一実装形態では、この時点で２つの出力信号が生成される。第１の信号は、ケイパビリティが封止され、首尾よく開封されたことを識別するために使用され、第２の信号は、処理回路の同じモード信頼レベルから、ケイパビリティが封止され、開封されたかどうかを識別することができる。したがって、第２の信号は、ケイパビリティが現在のモード信頼レベルに関連付けられたことを示すため

に使用することができ、これは、いくつかの実装形態では、例えば、ケイパビリティがそれを参照しようとしているコンテキストと同じコンテキストによって生成されたことを保証するために、ソフトウェアにとって有用であり得る。

【００９６】

図８は、システム内に存在し得る様々な異なるモード信頼レベルを概略的に例示する図であり、そのような配設においてサポートされ得る封止／開封能力を示す。図８に示されるように、処理回路は、セキュアドメイン及び低セキュアドメインにおいて動作するように配設され得、現在のモード信頼レベルは、現在のプログラムコードがそれらのセキュリティドメインのうちのいずれにおいて実行されるかに依存し得る。加えて、又は代替的に、処理回路は、複数の異なる状態でプログラムコードを実行するように配設され得、図８の例では、特権状態又は非特権状態でプログラムコードを動作させるように配設され得る。特権のレベル及び異なるセキュリティドメインは、直交信頼レベルであるとみなすことができ、処理回路の異なるモード信頼レベルは、セキュア／低セキュアドメイン及び特権／非特権状態の各組み合わせに関連付けられ得る。したがって、図８に示すように、示される例では、４つの異なる信頼レベルがあり得る。

【００９７】

先に説明した封止及び開封能力に関して、図８の矢印によって示されるように、処理回路がセキュアモード及び特権モードで動作しているとき、処理回路は、ケイパビリティ信頼レベルが他の３つの信頼レベル動作モードのいずれかに関連付けられているケイパビリティを封止及び開封することが可能であり得る。また、円形の矢印によって示されるように、それはまた、ケイパビリティ信頼レベルがセキュア特権の信頼レベルを示すケイパビリティに対して封止及び開封動作を実施することができる。

【００９８】

同様に、処理回路が低セキュア特権モードで動作しているとき、処理回路は、低セキュア非特権の信頼レベルに関連付けられたケイパビリティに関連して封止及び開封動作を実施することができ、再び、図８の円形矢印によって示されるように、それ自体の信頼レベルに関連付けられたケイパビリティを封止及び開封することができる場合がある。更に、必要に応じて、処理回路がセキュア非特権モードで動作しているとき、処理回路は、低セキュア非特権の信頼レベルに関連付けられたケイパビリティを封止及び開封することが可能であってもよく、再び、それ自体の信頼レベルに関連付けられたケイパビリティを封止及び開封することも可能であってもよい。最後に、低セキュア非特権モードでは、処理回路は、低セキュア非特権の信頼レベルに関連付けられたケイパビリティを封止及び開封することしかできない場合がある。

【００９９】

図８は、４つの異なる信頼レベルを示すが、本明細書で説明される技法は、そのような構成に限定されず、図８に示される直交方向のいずれか又は両方で、追加の信頼レベルが提供され得ることが理解されよう。特権及び非特権モード動作は、様々な形態を採ることができるが、純粋に例として、特権モードは、いくつかの実装形態では、ハンドラモードと称され得、非特権モードは、スレッドモードと称され得る。ハンドラモードは、典型的には、例外処理のために使用され、したがって、例えば、信頼された例外処理ルーチンは、ハンドラモードで実行され得る。スレッドモードは、典型的には、複数の異なるスレッド、例えば、複数の異なるアプリケーションスレッドを実行するために使用される。

【０１００】

図９Ａ及び図９Ｂは、封止されたケイパビリティの使用を考慮するときに採ることができる異なる手法を例示する流れ図である。最初に、図９Ａに示されるように、ステップ４００において、要求が、封止されたケイパビリティを使用するように試みられる場合、ステップ４０５において、そのような使用は、例示的な一実装形態によると、現在のモード信頼レベルにかかわらず、防止され得る。特に、図９Ａに例示される実装形態によれば、システムは、最初に開封された場合にのみ、封止されたケイパビリティの使用が可能になる。したがって、そのような実装形態では、封止されたケイパビリティに関して試みられ

るすべての処理動作が失敗する。しかしながら、処理回路は、依然として、記憶構造間、例えば、レジスタとメモリとの間、又は異なるレジスタ間で、封止されたケイパビリティを移動させることが可能であり得ることに留意されたい。更に、例示的な一実装形態では、通常、ケイパビリティに関連付けられた前述のタグビットをクリアすることによって、封止されたケイパビリティを無効にすることが依然として可能であり得る。

【０１０１】

図９Ｂは、封止されたケイパビリティの何らかの使用がある特定の状況において可能になり得る代替的な実装形態を例示する流れ図である。したがって、ステップ４１０において、要求が封止されたケイパビリティを使用しようと試みていると判定された場合、ステップ４１５において、現在のモード信頼レベルがケイパビリティ信頼レベル以上であるかどうかが判定される。そうでない場合には、ステップ４２０において、封止されたケイパビリティの使用が防止されるが、そうでない場合には、プロセスはステップ４２５に進み、問題の特定の使用が、封止されたケイパビリティに対して実施可能であるタイプの使用であるかどうかが判定される。そうでない場合には、再び、ステップ４２０において、封止されたケイパビリティの使用が防止されるが、そうでない場合には、プロセスはステップ４３０に進み、要求された動作は、使用を進めることを可能にする前に実施され得る任意の通常のチェックを条件として、封止されたケイパビリティを使用して実施可能になる。

【０１０２】

先のステップ４２５に関して、封止されたケイパビリティの使用は、特定のタイプの動作に制限され得る。例えば、現在のモード信頼レベルが、封止されたケイパビリティのケイパビリティ信頼レベル以上であるとき、処理回路は、メモリアドレスを生成するために、その封止されたケイパビリティを使用して逆参照動作を実施することが可能になり得る。これは、それが使用される前にケイパビリティを開封する必要性を回避することによって、いくつかの性能利益を生じさせることができる。

【０１０３】

想定され得る別のタイプの処理動作は、封止されたケイパビリティの修正であり、再び、これは、いくつかの事例においてサポートされ得る。特に、図１０は、ケイパビリティを修正する要求を操作するときに実施され得るステップを例示する流れ図である。図１０に示すように、ステップ４５０において、ケイパビリティを修正する要求が受信された場合、ステップ４５５において、ケイパビリティが封止されているかどうかが判定される。そうでない場合、プロセスはステップ４６０に進み、ケイパビリティを修正することができるかどうかを判定するために必要な通常のチェックが実施される。

【０１０４】

しかしながら、ケイパビリティが封止されている場合、随意に、ステップ４６５において、処理回路の現在の動作モードに関連付けられた信頼レベルが、ケイパビリティの修正が行われることを可能にするのに十分であるかどうかが判定されてもよい。これは、例えば、現在のモード信頼レベルがケイパビリティ信頼レベル以上である場合であり得る。そうである場合、プロセスは前述のステップ４６０に進み、通常のチェックを実施することができる。しかしながら、信頼レベルが不十分である場合、プロセスは代わりにステップ４７０に進むことができ、ケイパビリティに対する修正が防止されるか、又は代わりにケイパビリティが無効にされる。任意選択のステップ４６５が省略される代替的な実装形態では、ケイパビリティが封止されている場合、プロセスは、ステップ４５５からステップ４７０に直接進んで、ケイパビリティの修正を防止するか、又はケイパビリティを無効にすることができる。

【０１０５】

図６～図１０を参照して説明した上記の例のすべてにおいて、現在のモード信頼レベルがケイパビリティ信頼レベルと比較されたとき、現在のモード信頼レベルがケイパビリティ信頼レベル以上であるときはいつでも、説明した活動が許可され得ると仮定される。代替的な実装形態では、それらの活動を実施する能力は、現在のモード信頼レベルがケイパ

ビリティ信頼レベルに一致する状況に制限され得る。

【０１０６】

メモリからケイパビリティレジスタ６０、８０のうちの１つにケイパビリティをロードするとき、処理回路は、ある特定の状況において、ケイパビリティ信頼レベルを選択的に修正するように配設され得、この手法の例示的な一実装形態が、図１１に示される。ステップ５００において、メモリからのケイパビリティのロードが要求されているかどうかが判定される。ステップ５０５において、ロード動作のために識別されたケイパビリティが封止されたケイパビリティであるかどうかが判定される。そうである場合、プロセスはステップ５１５に進み、ケイパビリティが、ロード動作のために、識別されたケイパビリティレジスタに修正されない形で記憶される。特に、封止されたケイパビリティの特性のために、ロード動作中になされるべきケイパビリティ信頼レベルのいかなる変更にも不適切である。更に、封止されたケイパビリティの使用を制御するために封止されたケイパビリティ操作回路１８５によって採用される前述の機構により、封止されたケイパビリティをケイパビリティレジスタにロードするときに、ケイパビリティ信頼レベルの低減が行われなくても、封止されたケイパビリティに対してセキュリティを依然として保証することができる。

【０１０７】

ステップ５０５において、ケイパビリティが封止されたケイパビリティではないと判定された場合、プロセスはステップ５１０に進み、現在のモード信頼レベルが、メモリからロードされるケイパビリティのケイパビリティ信頼レベル未満であるかどうかが判定される。そうでない場合、例示的な一実装形態では、プロセスはステップ５１５に進み、ケイパビリティは、ケイパビリティレジスタ内に修正されずに記憶される。

【０１０８】

しかしながら、図１１に示される技法によれば、現在のモード信頼レベルがケイパビリティ信頼レベル未満である場合、プロセスはステップ５２０に進み、現在のモード信頼レベルがもはやケイパビリティ信頼レベル未満にならないように、ケイパビリティレジスタに記憶されているケイパビリティのコピーに関連付けられたケイパビリティ信頼レベルがデモートされる。そのようなアプローチによって、メモリからロードされているケイパビリティが、より高い関連付けられた特権レベルを有する場合であっても、処理回路のケイパビリティレジスタにロードされる結果として生じるケイパビリティは、現在のモード信頼レベルで動作するときに処理回路によってアクセスされるべきではないメモリにアクセスするために使用され得ないように、デモートされたそのケイパビリティ信頼レベルを有することが保証され得る。逆に、メモリにおけるケイパビリティが、現在のモード信頼レベルよりも低い信頼レベルを有する場合、その信頼レベルは、ケイパビリティレジスタに移動されるときに「そのまま」のままである。これは、ケイパビリティの偶発的なプロモーションを回避することができ、例えば、例外ハンドラがスタックされた値を偶発的にプロモーションさせる場合を回避することができる。

【０１０９】

例示的な一実装形態では、ケイパビリティロードプロセスは、特定の状況において、汎用データをケイパビリティではなくケイパビリティレジスタにロードするために使用されることが可能である。これは、ステップ５００で検出することができ、実際にロード動作が汎用データをロードするために使用されている場合、ケイパビリティ内のケイパビリティ信頼レベルを指定するビットの選択的なデモーションを防止することができ、したがって、ロードされているデータの破損を回避することができる。

【０１１０】

図１１のステップ５２０によって示されるように、ケイパビリティ信頼レベルを選択的にデモートする能力は、例えば、制御レジスタ９０内に記憶された制御情報を条件とすることによって、構成可能にすることができる。ケイパビリティの選択的なデモーションは、ある特定のタイプのケイパビリティに対してディセーブルすることもでき（既に上述した封止されたケイパビリティに加えて）、したがって、例えば、ロードされているケイパ

ビリティが不変ケイパビリティであるときにディセーブルすることができる。そのような能力は、例えば、不変ケイパビリティを修正することなく、非特権動作モード内から特権不変ケイパビリティをスピルすることを可能にするために有益であり得る。更に、上述したように、メモリからロードされているケイパビリティの選択的なデモーションを条件付きでイネーブル又はディセーブルするために使用される制御情報は、制御レジスタに記憶することができるが、その制御情報は、他のロケーションに、例えば、ケイパビリティ自体内のフィールドとして、又は、例えば、ＭＰＵ領域属性に基づくデモーションをイネーブルするように、記憶することもできる。この後者のアプローチでは、読み出し専用としてマークされたＭＰＵ領域（例えば、コードメモリ）からケイパビリティがロードされる場合、デモーションが発生するが、関連する領域が読み出し－書き込みとしてマークされる場合（例えば、ヒープ又はスタックメモリ）にはデモーションが発生しないように、機構を配設することができる。いくつかの実装形態では、ＭＰＵにおける専用制御ビットを使用して、挙動を指示することができる。

【０１１１】

図１２は、ある所定のタイプのケイパビリティに対して、ケイパビリティの開封をどのように選択的に禁止することができるかを例示する流れ図である。特に、ステップ５５０で開封要求が受信されると、ステップ５５５で、識別されたケイパビリティが所定のタイプであるかどうかが判定される。そうでない場合、ステップ５６５において、プロセスは、先に論じた図７の残りの部分のように進む。しかしながら、ステップ５５５において、識別されたケイパビリティが所定のタイプである場合、プロセスはステップ５６０に進み、識別されたケイパビリティの開封が防止される。図７のステップ３６０を説明する際に前述したように、識別されたケイパビリティの開封が行われていないことを識別するために、所望であれば様々な情報を出力することができ、この場合、例えば、所定のタイプのケイパビリティを開封する試みが行われたことを示すフラグを立てるか、又はエラーをアサートすることができる。別のオプションとして、又は加えて、タグビットは、ケイパビリティを無効にするためにクリアされ得る。

【０１１２】

上記のプロセスが採用され得る所定のタイプのケイパビリティは、様々な形態を採ることができるが、例えば、特定のイベント又は機能を示すためにアーキテクチャによって使用される１つ以上のタイプのケイパビリティであってもよい。そのような予約タイプのケイパビリティが識別され得るいくつかの方法が存在する。特定の例として、それらは、例えば、上限が下限を下回ることによって、無効な範囲を定義する範囲境界情報を有し得る。

【０１１３】

必要に応じて、先に説明した封止フラグに加えて、ケイパビリティに１つ以上の余分なフィールドを設けて、そのケイパビリティを使用することができる特定の目的を識別するために使用される追加の指標を提供することができる。更に、必要に応じて、ケイパビリティ内で符号化されたアドレス値は、メモリアドレスを直接識別するのではなく、ソフトウェアがそれ自体のレコードに対して検証することを可能にする間接参照を提供することができる。

【０１１４】

図１３は、使用され得るシミュレータ実装形態を例示する。前述の例は、当該技法をサポートする特定の処理ハードウェアを動作させるための装置及び方法の観点で本発明を実施するが、本明細書に記載の例による命令実行環境を提供することも可能であり、命令実行環境は、コンピュータプログラムの使用により実施される。このようなコンピュータプログラムは、コンピュータプログラムがハードウェアアーキテクチャのソフトウェアベースの実装形態を提供する限り、シミュレータと称されることがよくある。様々なシミュレータコンピュータプログラムは、エミュレータ、仮想マシン、モデル、及び動的バイナリトランスレータを含むバイナリトランスレータを含む。典型的には、シミュレータ実装形態は、ホストプロセッサ６１５で実行し得、ホストプロセッサ６１５は、任意選択的に、

ホストオペレーティングシステム６１０を実行し、ホストオペレーティングシステム６１０は、シミュレータプログラム６０５をサポートする。いくつかの配設では、ハードウェアと提供された命令実行環境との間に複数層のシミュレーションがあり得、かつ／又は、複数の異なる命令実行環境が同じホストプロセッサ上に提供され得る。歴史的に、強力なプロセッサが、合理的な速度で実行されるシミュレータ実装形態を提供するのに必要とされてきたが、このようなアプローチは、互換性又は再使用の理由から別のプロセッサにネイティブなコードを実行することが望まれるようなときなど一定の状況では、正当化され得る。例えば、シミュレータ実装形態は、ホストプロセッサハードウェアによってサポートされていない追加の機能性を有する命令実行環境を提供し得るか、又は典型的には異なるハードウェアアーキテクチャに関連付けられた命令実行環境を提供し得る。シミュレーションの概要は、「Ｓｏｍｅ　Ｅｆｆｉｃｉｅｎｔ　Ａｒｃｈｉｔｅｃｔｕｒｅ　Ｓｉｍｕｌａｔｉｏｎ　Ｔｅｃｈｎｉｑｕｅｓ」、Ｒｏｂｅｒｔ　Ｂｅｄｉｃｈｅｋ、１９９０年冬、ＵＳＥＮＩＸ　Ｃｏｎｆｅｒｅｎｃｅ、第５３～６３頁に記載されている。

【０１１５】

例が、特定のハードウェア構築又は特徴を参照して前述されている程度に、シミュレーションされた実装では、同等の機能が、好適なソフトウェア構築又は特徴によって提供され得る。例えば、特定の回路は、シミュレーションされた実装では、コンピュータプログラムロジックとして提供され得る。同様に、レジスタ又はキャッシュなどのメモリハードウェアは、シミュレーションされた実装では、ソフトウェアデータ構造として提供され得る。また、ハードウェア装置２内のメモリ５０にアクセスするために使用される物理アドレス空間は、シミュレートされたアドレス空間としてエミュレートされ得、シミュレートされたアドレス空間は、ホストオペレーティングシステム６１０によって使用される仮想アドレス空間に、シミュレータ６０５によってマッピングされている。前述の例で言及されているハードウェア要素のうち１つ以上がホストハードウェア（例えば、ホストプロセッサ６１５）に存在する配設では、いくつかのシミュレートされた実装形態は、好適である場合、ホストハードウェアを使用し得る。

【０１１６】

シミュレータプログラム６０５は、（非一時的媒体であり得る）コンピュータ読み取り可能な記憶媒体に記憶され得、（アプリケーション、オペレーティングシステム、及びハイパーバイザを含み得る）ターゲットコード６００への仮想ハードウェアインタフェース（命令実行環境）を提供し、仮想ハードウェアインタフェースは、シミュレータプログラム６０５によってモデル化されたハードウェアアーキテクチャのハードウェアインタフェースと同じである。したがって、ターゲットコード６００のプログラム命令は、シミュレータプログラム６０５を使用して命令実行環境内から実行され得、このため、上で考察される装置２のハードウェア特徴を実際には有しないホストコンピュータ６１５は、これらの特徴をエミュレートすることができる。シミュレータプログラムは、処理パイプライン４の挙動をエミュレートするための処理プログラムロジック６２０と、図１のハードウェア装置２のケイパビリティチェック回路３３及びメモリアクセスチェック回路５２の挙動をエミュレートするためのチェックプログラムロジック６２２と、封止されたケイパビリティ操作回路１８５の挙動をエミュレートするための封止されたケイパビリティ操作プログラムロジック６０５とを含み得る。したがって、ケイパビリティ及びそれらの関連付けられたケイパビリティ信頼レベルを管理するための本明細書で説明される技法は、封止されたケイパビリティを操作するための説明された技法と共に、図１３の例では、シミュレータプログラム６０５によってソフトウェアで実施され得る。

【０１１７】

本出願において、「～ように構成された（ｃｏｎｆｉｇｕｒｅｄ　ｔｏ．．．）」という用語は、装置の要素が、定義された動作を実施することが可能である構成を有することを意味するために使用される。この文脈において、「構成」とは、ハードウェア又はソフトウェアの配設又は相互接続の方法を意味する。例えば、装置は、定義された動作を提供する専用ハードウェアを有し得るか、又はプロセッサ若しくは他の処理デバイスが、機能

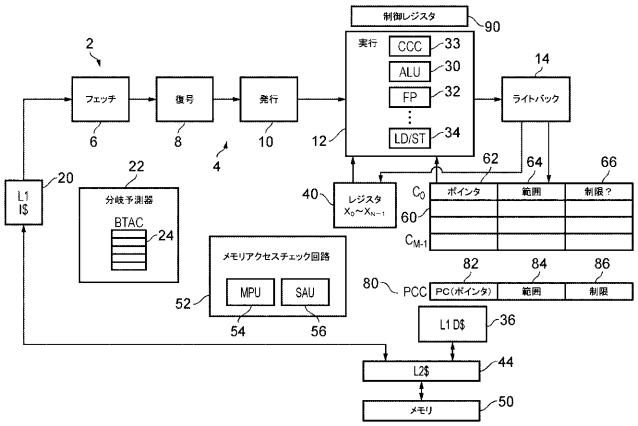
を実行するようにプログラムされ得る。「ように構成された」は、装置要素が、定義された動作を提供するために何らかの変更がなされる必要があることを意味しない。

【０１１８】

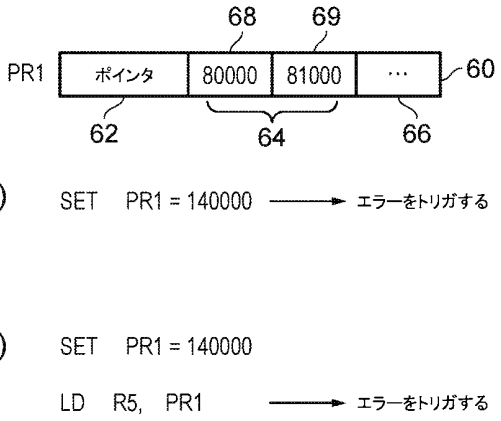
本発明の例示的な実施形態が添付の図面を参照して本明細書で詳細に説明されてきたが、本発明はそれらの正確な実施形態に限定されないこと、及び添付の特許請求の範囲によって規定される本発明の範囲及び趣旨から逸脱することなく、当業者によって様々な変更、追加、及び修正が当業者によって実施され得ることが理解されるであろう。例えば、従属請求項の特徴の様々な組み合わせは、本発明の範囲から逸脱することなく、独立請求項の特徴でなされ得る。

【図面】

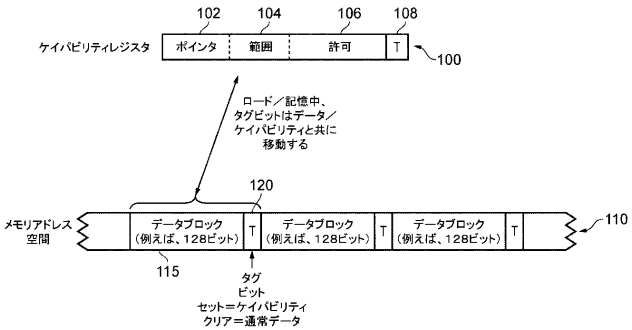
【図１】



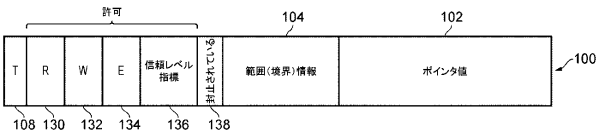
【図２】



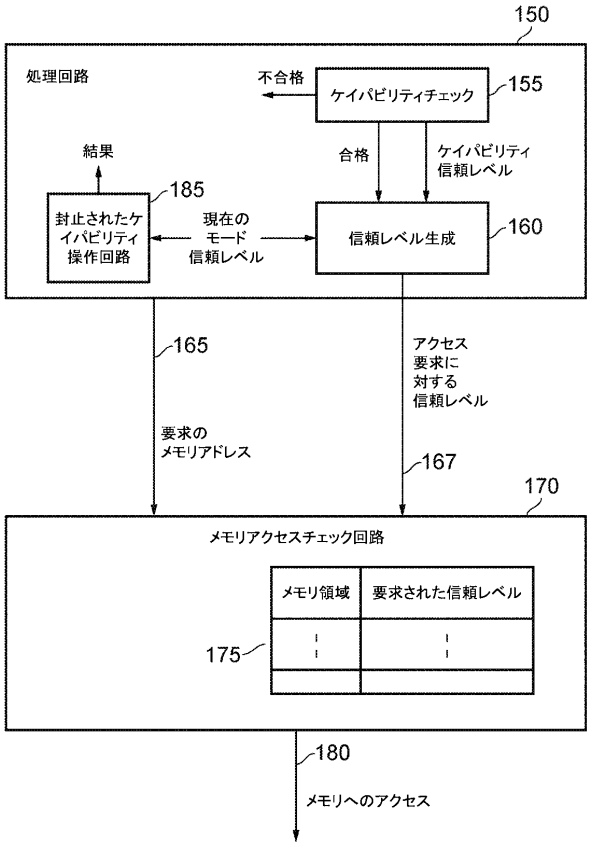
【図３】



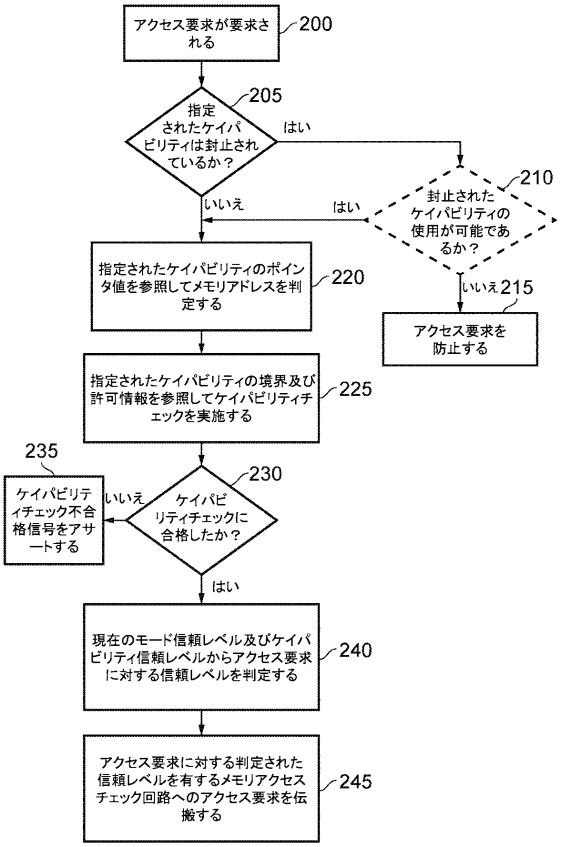
【図４】



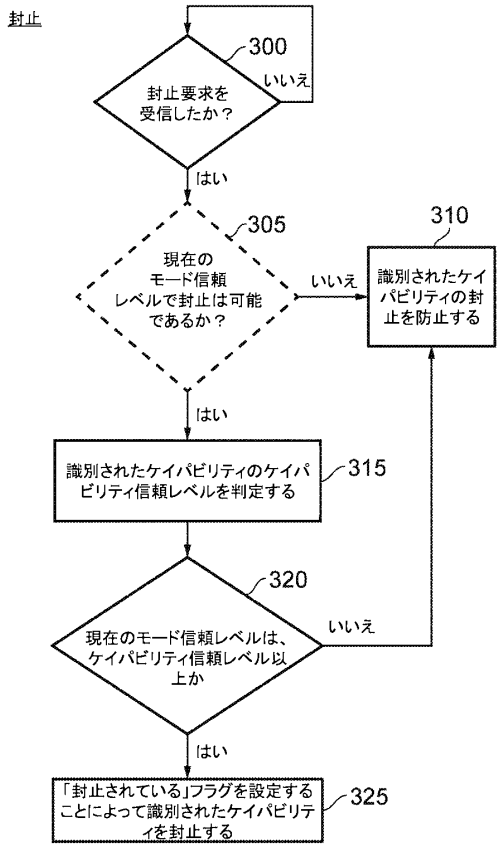
【図５Ａ】


150
処理回路
不合格
ケイパビリティチェック
155
結果
合格
ケイパビリティ信頼レベル
185
封止されたケイパビリティ操作回路
現在のモード信頼レベル
信頼レベル生成
160
165
アクセス要求に対する信頼レベル
要求のメモリアドレス
167
170
メモリアクセスチェック回路
メモリ領域
要求された信頼レベル
175
180
メモリへのアクセス

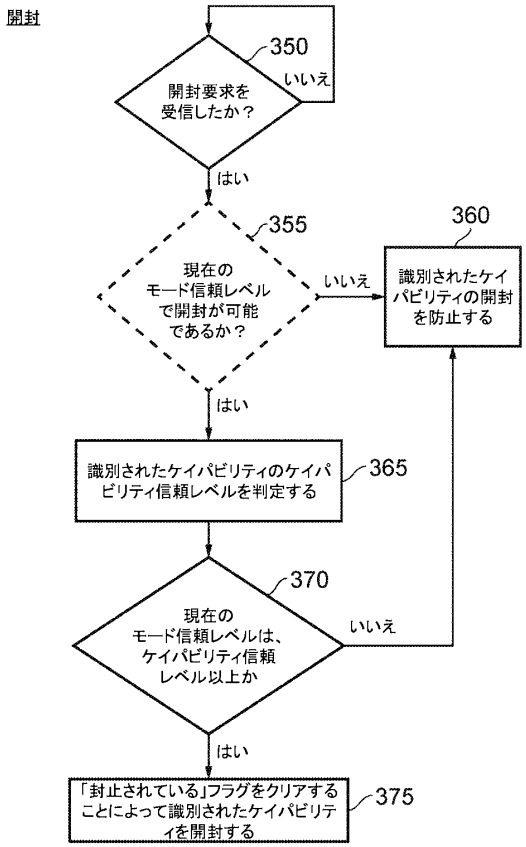
【図５Ｂ】


アクセス要求が要求される
200
指定されたケイパビリティは封止されているか？
205
はい
いいえ
封止されたケイパビリティの使用が可能であるか？
210
はい
いいえ
215
アクセス要求を防止する
指定されたケイパビリティのポインタ値を参照してメモリアドレスを判定する
220
指定されたケイパビリティの境界及び許可情報を参照してケイパビリティチェックを実施する
225
235
ケイパビリティチェック不合格信号をアサートする
いいえ
ケイパビリティチェックに合格したか？
230
はい
現在のモード信頼レベル及びケイパビリティ信頼レベルからアクセス要求に対する信頼レベルを判定する
240
アクセス要求に対する判定された信頼レベルを有するメモリアクセスチェック回路へのアクセス要求を伝搬する
245

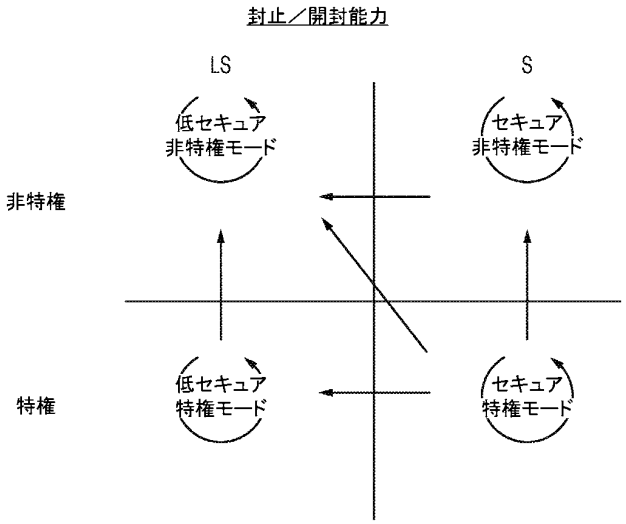
【図６】


封止
300
封止要求を受信したか？
いいえ
はい
305
現在のモード信頼レベルで封止は可能であるか？
310
いいえ
識別されたケイパビリティの封止を防止する
はい
識別されたケイパビリティのケイパビリティ信頼レベルを判定する
315
320
現在のモード信頼レベルは、ケイパビリティ信頼レベル以上か
いいえ
はい
「封止されている」フラグを設定することによって識別されたケイパビリティを封止する
325

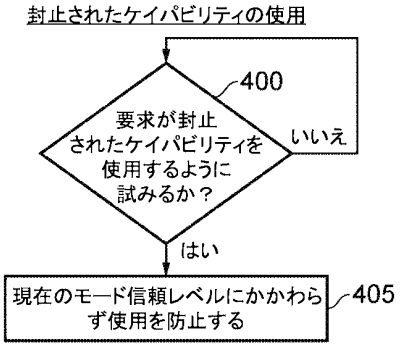
【図７】


開封
350
開封要求を受信したか？
いいえ
はい
355
現在のモード信頼レベルで開封が可能であるか？
360
いいえ
識別されたケイパビリティの開封を防止する
はい
識別されたケイパビリティのケイパビリティ信頼レベルを判定する
365
370
現在のモード信頼レベルは、ケイパビリティ信頼レベル以上か
いいえ
はい
「封止されている」フラグをクリアすることによって識別されたケイパビリティを開封する
375

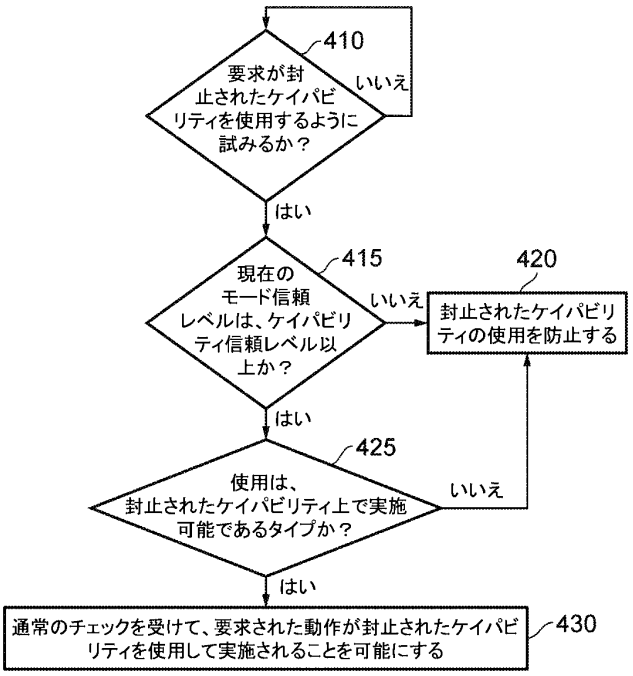
【図８】



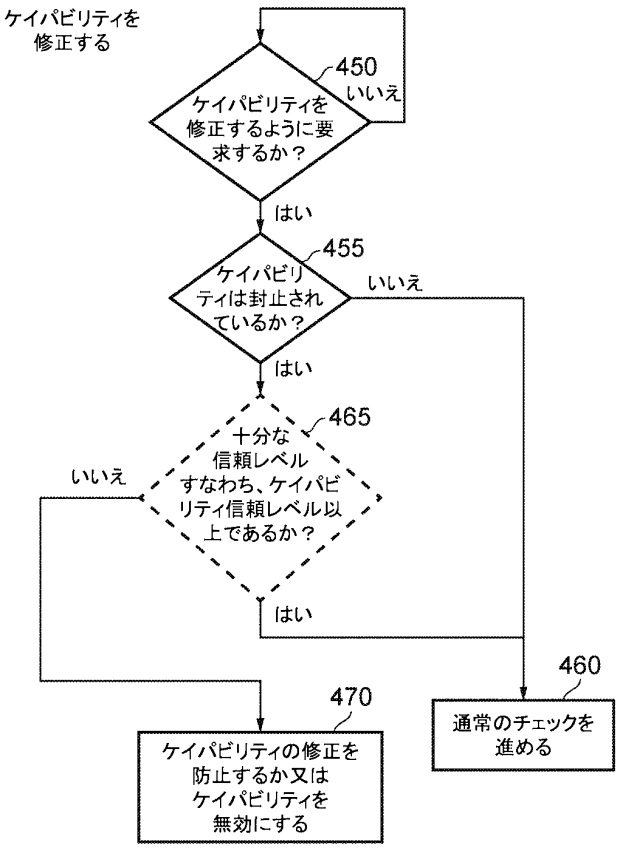
【図９Ａ】



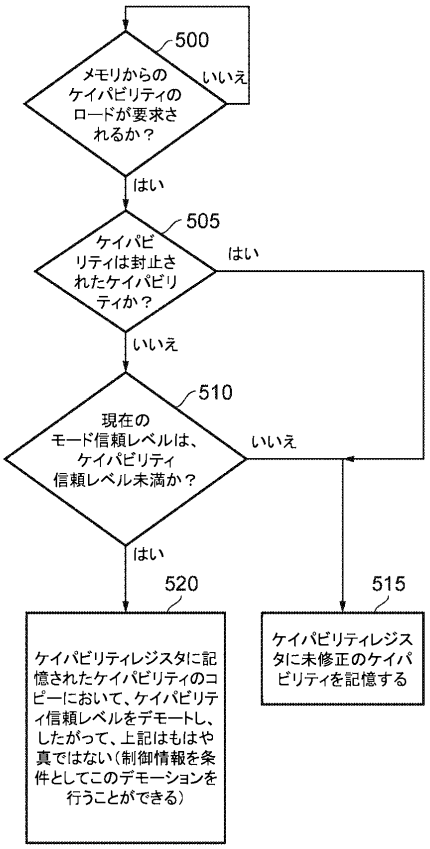
【図９Ｂ】



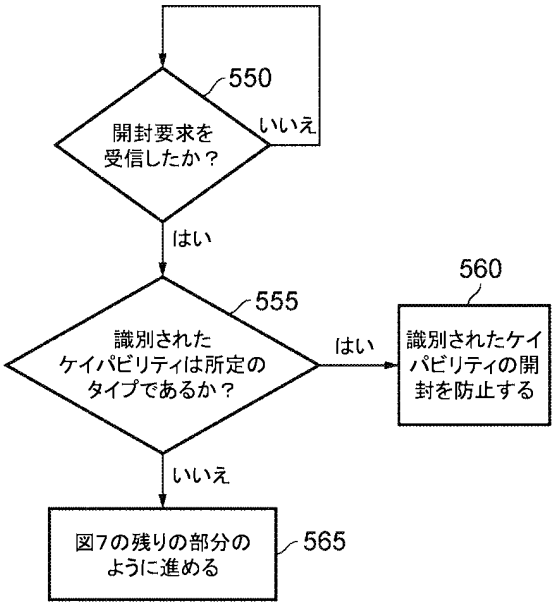
【図１０】



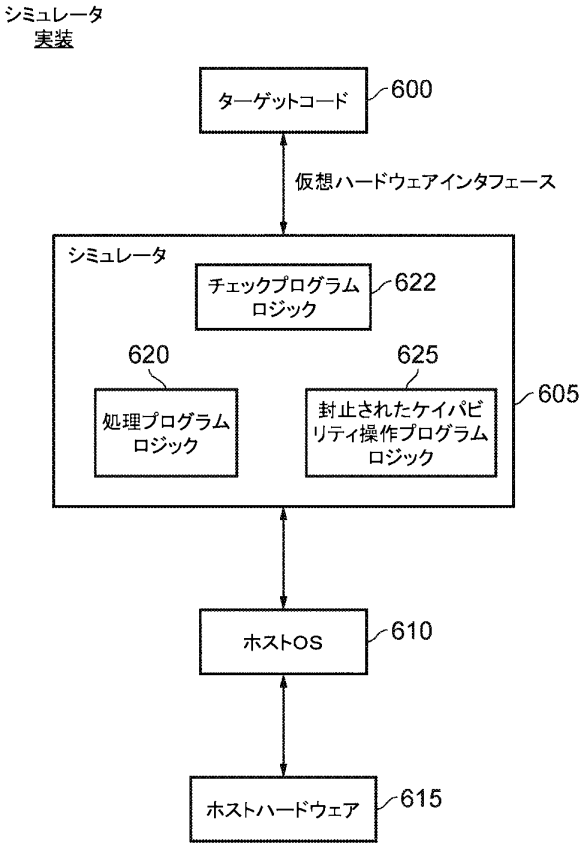
【図１１】


500
メモリからのケイパビリティのロードが要求されるか？
いいえ
はい
505
ケイパビリティは封止されたケイパビリティか？
はい
いいえ
510
現在のモード信頼レベルは、ケイパビリティ信頼レベル未満か？
いいえ
はい
520
ケイパビリティレジスタに記憶されたケイパビリティのコピーにおいて、ケイパビリティ信頼レベルをデモートし、したがって、上記はもはや真ではない（制御情報を条件としてこのデモーションを行うことができる）
515
ケイパビリティレジスタに未修正のケイパビリティを記憶する

【図１２】


550
開封要求を受信したか？
いいえ
はい
555
識別されたケイパビリティは所定のタイプであるか？
はい
560
識別されたケイパビリティの開封を防止する
いいえ
図7の残りの部分のように進める
565

【図１３】


シミュレータ
実装
ターゲットコード
600
仮想ハードウェアインタフェース
シミュレータ
チェックプログラムロジック
622
620
処理プログラムロジック
625
封止されたケイパビリティ操作プログラムロジック
605
ホストOS
610
ホストハードウェア
615

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No
PCT/GB2022/052321

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/52 G06F9/30
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2016/110298 A1 (KOUFATY DAVID A [US] ET AL) 21 April 2016 (2016-04-21) abstract paragraphs [0017] - [0050] paragraphs [0055] - [0057] paragraph [0062] paragraphs [0107] - [0132] claims 1-22 figures 1-12 ----- -/--	1-22

[x] Further documents are listed in the continuation of Box C. [x] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance;; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance;; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
4 November 2022	14/11/2022

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Bichler, Marc

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No
PCT/GB2022/052321

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2021/224380 A1 (GROCUTT THOMAS CHRISTOPHER [GB]) 22 July 2021 (2021-07-22) abstract paragraph [0004] paragraphs [0025] - [0032] paragraphs [0038] - [0041] paragraphs [0052] - [0059] paragraphs [0104] - [0106] paragraphs [0119] - [0124] claims 1-23 figures 1-11	1-22
X A	GB 2 482 700 A (ADVANCED RISC MACH LTD [GB]) 15 February 2012 (2012-02-15) abstract page 2, line 21 - page 5, line 28 page 7, line 4 - page 10, line 16 claims 1-27 figures 1-4	1,5,6, 8-20 2-4,7

Form PCT/ISA/210 (continuation of second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/GB2022/052321

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2016110298 A1	21-04-2016	CN 106716434 A	24-05-2017
		EP 3210123 A1	30-08-2017
		KR 20170043635 A	21-04-2017
		TW 201633153 A	16-09-2016
		US 2016110298 A1	21-04-2016
		WO 2016064469 A1	28-04-2016
US 2021224380 A1	22-07-2021	CN 112805709 A	14-05-2021
		CN 112805710 A	14-05-2021
		EP 3864554 A1	18-08-2021
		EP 3864555 A1	18-08-2021
		GB 2577878 A	15-04-2020
		GB 2577947 A	15-04-2020
		IL 280715 A	25-03-2021
		JP 2022503899 A	12-01-2022
		JP 2022503921 A	12-01-2022
		KR 20210060443 A	26-05-2021
		KR 20210068006 A	08-06-2021
		TW 202029045 A	01-08-2020
		TW 202030634 A	16-08-2020
		US 2021224380 A1	22-07-2021
		US 2021294924 A1	23-09-2021
		WO 2020074853 A1	16-04-2020
		WO 2020074854 A1	16-04-2020
GB 2482700 A	15-02-2012	CN 103069398 A	24-04-2013
		EP 2603872 A1	19-06-2013
		GB 2482700 A	15-02-2012
		IL 223732 A	30-07-2015
		JP 5718463 B2	13-05-2015
		JP 2013533567 A	22-08-2013
		KR 20130136436 A	12-12-2013
		MY 168732 A	29-11-2018
		TW 201207615 A	16-02-2012
		US 2012042144 A1	16-02-2012
		WO 2012020236 A1	16-02-2012

Form PCT/ISA/210 (patent family annex) (April 2005)

フロントページの続き

MK,MT,NL,NO,PL,PT,RO,RS,SE,SI,SK,SM,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,KM,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AO,AT,AU,AZ,BA,BB,BG,BH,BN,BR,BW,BY,BZ,CA,CH,CL,CN,CO,CR,CU,CV,CZ,DE,DJ,DK,DM,DO,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,GT,HN,HR,HU,ID,IL,IN,IQ,IR,IS,IT,JM,JO,JP,KE,KG,KH,KN,KP,KR,KW,KZ,LA,LC,LK,LR,LS,LU,LY,MA,MD,ME,MG,MK,MN,MW,MX,MY,MZ,NA,NG,NI,NO,NZ,OM,PA,PE,PG,PH,PL,PT,QA,RO,RS,RU,RW,SA,SC,SD,SE,SG,SK,SL,ST,SV,SY,TH,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC,VN,WS,ZA,ZM,ZW

イギリス国 ケンブリッジシャー シービー１ ９エヌジェイ ケンブリッジ，フルボーン ロード １１０，アーム リミテッド宛

Ｆターム（参考） 5B017 AA01 BA01 BB05 CA01 CA02
5B033 DB02 FA27

【要約の続き】
ケイパビリティ信頼レベルよりも低い信頼レベルであるとき、処理回路が所与の封止されたケイパビリティを使用して少なくとも１つの処理動作を実施することを防止するために、封止されたケイパビリティ操作回路を更に備える。