202318210

(19)中華民國智慧財產局

(12)發明說明書公開本 (11)公開編號：TW 202318210 A

(43)公開日： 中華民國 112 (2023) 年 05 月 01 日

(21)申請案號：111138999 (22)申請日： 中華民國 111 (2022) 年 10 月 14 日

(51)Int. Cl.： *G06F12/14 (2006.01)*

(30)優先權：2021/10/18 英國 2114862.2

(71)申請人：英商ＡＲＭ股份有限公司 (英國) ARM LIMITED (GB)
英國

(72)發明人：博特曼 法蘭克斯克里斯多夫雅克 BOTMAN, FRANCOIS CHRISTOPHER JACQUES (GB)；格羅卡特 湯瑪士克里斯多夫 GROCUTT, THOMAS CHRISTOPHER (GB)

(74)代理人：李世章；彭國洋

申請實體審查：無 申請專利範圍項數：22 項 圖式數：13 共 70 頁

(54)名稱

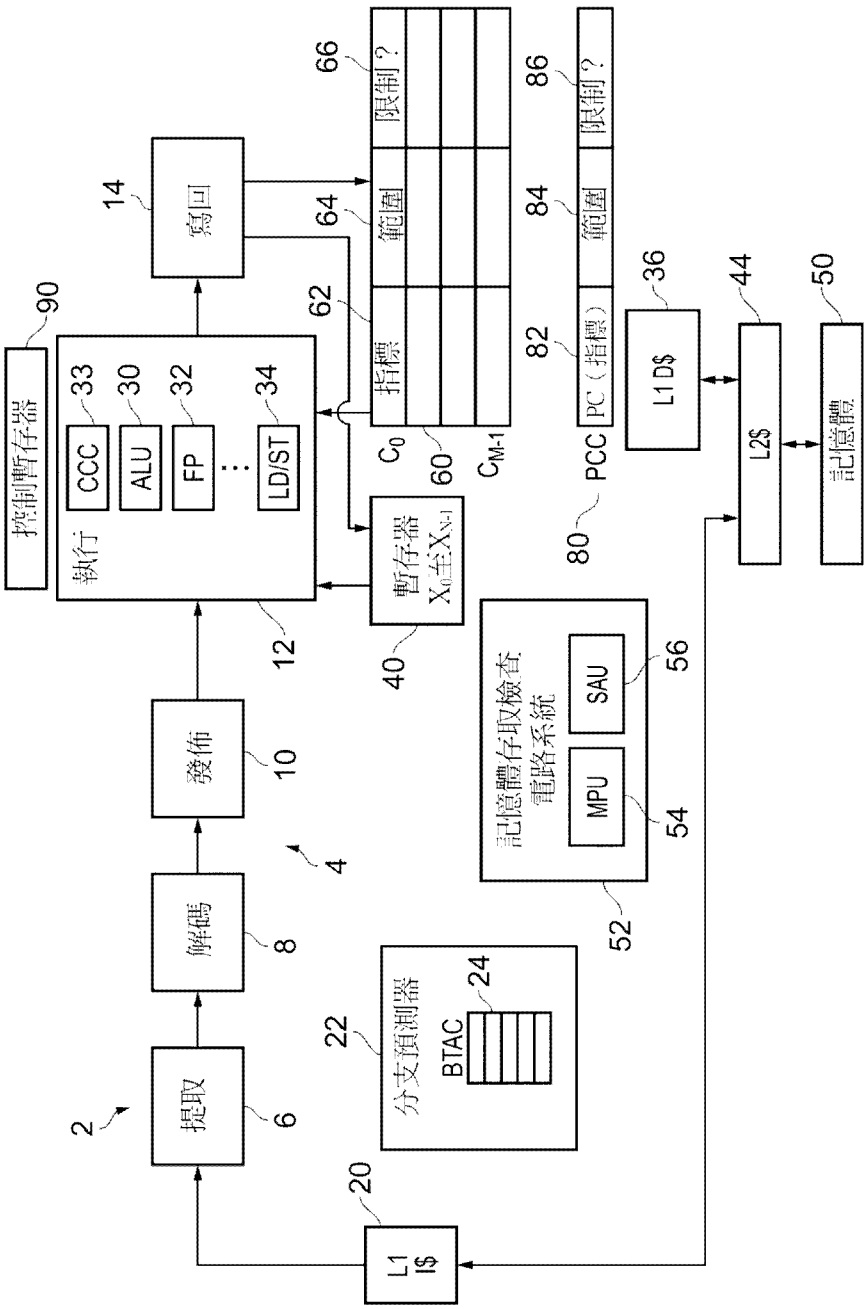
用於處理密封能力之技術

(57)摘要

描述用於處理密封能力的一種設備及方法。該設備具有處理電路系統以執行在其期間產生對記憶體之存取請求的處理操作，其中該處理電路系統經配置以使用識別約束資訊的能力產生用於該等存取請求的記憶體位址。檢查電路系統接著基於由一給定能力識別的該約束資訊，且基於與一給定存取請求關聯的一信任等級，判定是否允許其記憶體位址係使用該給定能力產生的該給定存取請求。各能力具有與其關聯的一能力信任等級，且與該給定存取請求關聯的該信任等級取決於與該處理電路系統的一目前操作模式關聯的一目前模式信任等級及該給定能力的該能力信任等級二者。該等能力中之至少一者可設定為一密封能力，且該設備進一步包含密封能力處理電路系統以在該目前模式信任等級係比一給定密封能力的該能力信任等級更低的一信任等級時防止該處理電路系統使用該給定密封能力執行至少一個處理操作。

An apparatus and method are described for handling sealed capabilities. The apparatus has processing circuitry to perform processing operations during which access requests to memory are generated, wherein the processing circuitry is arranged to generate memory addresses for the access requests using capabilities that identify constraining information. Checking circuitry then determines whether a given access request whose memory address is generated using a given capability is permitted based on the constraining information identified by that given capability, and based on a level of trust associated with the given access request. Each capability has a capability level of trust associated therewith, and the level of trust associated with the given access request is dependent on both a current mode level of trust associated with a current mode of operation of the processing circuitry, and the capability level of trust of the given capability. At least one of the capabilities is settable as a sealed capability, and the apparatus further comprises sealed capability handling circuitry to prevent the processing circuitry performing at least one processing operation using a given sealed capability when the current mode level of trust is a lower level of trust than the capability level of trust of the given sealed capability.

指定代表圖：



【圖1】

符號簡單說明：

2:資料處理設備；設備；硬體設備；系統

4:處理管線；管線；處理器；處理電路系統

6:提取級

8:解碼級

10:發布級

12:執行級

14:寫回級

20:1 級(L1)指令快取記憶體；快取記憶體

22:分支預測器

24:分支目標位址快取記憶體(BTAC)

30:執行單元；算術/邏輯單元(ALU)

32:執行單元；浮點(FP)單元

33:能力檢查電路系統

34:執行單元；載入/儲存單元

36:1 級(L1)資料快取記憶體

40:暫存器；通用資料暫存器

44:二級(L2)快取記憶體

50:主記憶體；記憶體；記憶體系統

52:記憶體存取檢查電路系統

54:記憶體保護單元(MPU)

56:安全屬性單元(SAU)

60:有界指標暫存器；有界指標儲存元件；

指標暫存器；能力暫存器

62:指標值；指標

64:範圍資訊

66:限制資訊；限制

80:程式計數器能力(PCC)暫存器；能力暫存器

82:欄位

84:範圍資訊

86:限制資訊

90:控制暫存器

202318210

【發明摘要】

【中文發明名稱】 用於處理密封能力之技術

【英文發明名稱】 TECHNIQUE FOR HANDLING SEALED CAPABILITIES

【中文】

描述用於處理密封能力的一種設備及方法。該設備具有處理電路系統以執行在其期間產生對記憶體之存取請求的處理操作，其中該處理電路系統經配置以使用識別約束資訊的能力產生用於該等存取請求的記憶體位址。檢查電路系統接著基於由一給定能力識別的該約束資訊，且基於與一給定存取請求關聯的一信任等級，判定是否允許其記憶體位址係使用該給定能力產生的該給定存取請求。各能力具有與其關聯的一能力信任等級，且與該給定存取請求關聯的該信任等級取決於與該處理電路系統的一目前操作模式關聯的一目前模式信任等級及該給定能力的該能力信任等級二者。該等能力中之至少一者可設定為一密封能力，且該設備進一步包含密封能力處理電路系統以在該目前模式信任等級係比一給定密封能力的該能力信任等級更低的一信任等級時防止該處理電路系統使用該給定密封能力執行至少一個處理操作。

【英文】

An apparatus and method are described for handling sealed capabilities. The apparatus has processing circuitry to perform processing operations during which access requests to memory are generated, wherein the processing circuitry is arranged to generate memory addresses for the access requests using capabilities that identify constraining

information. Checking circuitry then determines whether a given access request whose memory address is generated using a given capability is permitted based on the constraining information identified by that given capability, and based on a level of trust associated with the given access request. Each capability has a capability level of trust associated therewith, and the level of trust associated with the given access request is dependent on both a current mode level of trust associated with a current mode of operation of the processing circuitry, and the capability level of trust of the given capability. At least one of the capabilities is settable as a sealed capability, and the apparatus further comprises sealed capability handling circuitry to prevent the processing circuitry performing at least one processing operation using a given sealed capability when the current mode level of trust is a lower level of trust than the capability level of trust of the given sealed capability.

【指定代表圖】　　圖1

【代表圖之符號簡單說明】

2:資料處理設備；設備；硬體設備；系統

4:處理管線；管線；處理器；處理電路系統

6:提取級　　8:解碼級

10:發布級　　12:執行級

14:寫回級

20:1級(L1)指令快取記憶體；快取記憶體

22:分支預測器　　24:分支目標位址快取記憶體(BTAC)

30:執行單元；算術/邏輯單元(ALU)　　32:執行單元；浮點(FP)單元

33:能力檢查電路系統　　34:執行單元；載入/儲存單元

36:1級(L1)資料快取記憶體　　40:暫存器；通用資料暫存器

44:二級(L2)快取記憶體　　50:主記憶體；記憶體；記憶體系統

52:記憶體存取檢查電路系統　　54:記憶體保護單元(MPU)

56:安全屬性單元(SAU)

60:有界指標暫存器；有界指標儲存元件；指標暫存器；能力暫存器

62:指標值；指標　　64:範圍資訊

66:限制資訊；限制

80:程式計數器能力(PCC)暫存器；能力暫存器

82:欄位　　84:範圍資訊

86:限制資訊　　90:控制暫存器

【特徵化學式】

無

【發明說明書】

【中文發明名稱】　用於處理密封能力之技術

【英文發明名稱】　TECHNIQUE FOR HANDLING SEALED CAPABILITIES

【技術領域】

【0001】　本技術係關於資料處理領域，且更明確地關於密封能力的處理。

【先前技術】

【0002】　對在其中某些能力係針對給定程序定義，且若嘗試在經定義能力外側實行操作，可觸發錯誤之基於能力之架構的關注日益增加。能力可採取各種形式，但一種類型的能力係有界指標（其亦可稱為「胖指標」）。

【0003】　可提供若干個能力儲存元件（例如，暫存器）以用於儲存用於由資料處理設備的處理電路系統存取的能力。各能力可包括在使用該能力時用以限制可執行之操作的約束資訊。例如，考慮有界指標，此可提供用以識別在使用該能力時可由處理電路系統存取之記憶體位址的非可延伸範圍，以及識別關聯權限的一或多個權限旗標的資訊。

【0004】　若干個能力架構已引入密封能力的概念。藉由將能力密封，此允許將能力標記為非可解參考的（意謂著記憶體位址不可使用該能力存取）及不可變的，導致若嘗試修改或解參考此一能力，導致硬體例外。由於密封能力允許諸如受信任碼將在呼叫回該受信任碼期間使用的符記提供給較不受信任碼

的軟體使用情形（例如，檔案處理），支援密封能力係所欲的。此符記在較不受信任模式內不應係可用的，且不應由軟體或架構中的任何其他行為修改。

【0005】　然而，多位元欄位（其可稱為「物件類型(object type)」欄位）一般需要提供在能力內以擷取與能力之密封狀態有關的資訊，且進一步地，一般的情形係需要使用特定解密封金鑰以將此一密封能力解密封，一般係具有解密封權限及匹配物件類型的能力。然而，在一些現代系統中，可用以表示能力之後設資料之位元的數目受高度約束，可使其難以支援此類密封能力的使用。進一步地，需要解密封金鑰的要求係麻煩的。

【0006】　提供支援密封能力之提供的替代機制因此將係所欲的。

【發明內容】

【0007】　在一第一實例配置中，提供一種設備，其包含：處理電路系統，以執行在其期間產生對記憶體之存取請求的處理操作，其中該處理電路系統經配置以使用識別約束資訊的能力產生用於該等存取請求的記憶體位址；及檢查電路系統，以基於由一給定能力識別的該約束資訊，且基於與一給定存取請求關聯的一信任等級，判定是否允許其記憶體位址係使用該給定能力產生的該給定存取請求；其中：各能力具有與其關聯的一能力信任等級，且與該給定存取請求關聯的該信任等級取決於與該處理電路系統的一目前操作模式關聯的一目前模式信任等級及該給定能力的該能力信任等級二者；該等能力中之至少一者可設定為一密封能力；及該設備進一步包含密封能力處理電路系統，以在該目前模式信任等級係比一給定密封能力的該能力信任等級更低的一信任等級時防止該處理電路系統使用該給定密封能力執行至少一個處理操作。

【0008】 在一進一步實例配置中，提供一種處理密封能力之方法，其包含：利用處理電路系統以執行在其期間產生對記憶體之存取請求的處理操作，其中該處理電路系統使用識別約束資訊的能力產生用於該等存取請求的記憶體位址；及基於由一給定能力識別的該約束資訊，且基於與一給定存取請求關聯的一信任等級，判定是否允許其記憶體位址係使用該給定能力產生的該給定存取請求；其中：各能力具有與其關聯的一能力信任等級，且與該給定存取請求關聯的該信任等級取決於與該處理電路系統的一目前操作模式關聯的一目前模式信任等級及該給定能力的該能力信任等級二者；及該等能力中之至少一者可設定為一密封能力；且該方法進一步包含利用密封能力處理電路系統，以在該目前模式信任等級係比一給定密封能力的該能力信任等級更低的一信任等級時防止該處理電路系統使用該給定密封能力執行至少一個處理操作。

【0009】 在一又進一步實例配置中，提供一種用於控制一主機資料處理設備以提供一指令執行環境的電腦程式，其包含：處理程式邏輯，以執行在其期間產生對記憶體之存取請求的處理操作，其中該處理程式邏輯經配置以使用識別約束資訊之能力產生用於該等存取請求的記憶體位址；及檢查程式邏輯，以基於由一給定能力識別的該約束資訊，且基於與一給定存取請求關聯的一信任等級，判定是否允許其記憶體位址係使用該給定能力產生的該給定存取請求；其中：各能力具有與其關聯的一能力信任等級，且與該給定存取請求關聯的該信任等級取決於與該處理程式邏輯的一目前操作模式關聯的一目前模式信任等級及該給定能力的該能力信任等級二者；該等能力中之至少一者可設定為一密封能力；及該設備進一步包含密封能力處理程式邏輯，以在該目前模式信

任等級係比一給定密封能力的該能力信任等級更低的一信任等級時防止該處理程式邏輯使用該給定密封能力執行至少一個處理操作。

【0010】 在一又進一步實例配置中，提供一種設備，其包含：處理機構，用於執行在其期間產生對記憶體之存取請求的處理操作，其中該處理機構經配置以使用識別約束資訊的能力產生用於該等存取請求的記憶體位址；及檢查機構，用於基於由一給定能力識別的該約束資訊，且基於與一給定存取請求關聯的一信任等級，判定是否允許其記憶體位址係使用該給定能力產生的該給定存取請求；其中：各能力具有與其關聯的一能力信任等級，且與該給定存取請求關聯的該信任等級取決於與該處理機構的一目前操作模式關聯的一目前模式信任等級及該給定能力的該能力信任等級二者；該等能力中之至少一者可設定為一密封能力；及該設備進一步包含密封能力處理機構，用於在該目前模式信任等級係比一給定密封能力的該能力信任等級更低的一信任等級時防止該處理機構使用該給定密封能力執行至少一個處理操作。

【圖式簡單說明】

【0011】 本技術將僅藉由說明、參照如附圖中所繪示之其實例進一步描述，其中：

〔圖1〕係根據一個實例實施方案之設備的方塊圖；

〔圖2〕顯示若嘗試設定或存取該組有界指標儲存元件內的指標值，可觸發錯誤之指令之類型的實例，其中指標值係用以指定在由關聯範圍資訊所指示之範圍外側的位址；

〔圖3〕繪示根據一個實例實施方案之與有界指標有關聯之標籤位元的使用；

〔圖4〕示意地繪示可根據本文描述之技術使用的能力的形式，其中提供與能力有關聯的信任等級指示，並提供用於指示能力是否係密封的密封旗標；

〔圖5A〕係根據一個實例實施方案之示意地繪示用於個別存取請求的信任等級可如何產生且於之後用以約束對記憶體之存取，同時亦支援密封能力之適當處理的圖；

〔圖5B〕係根據一個實例實施方案之繪示示意地顯示於圖5A中之設備的操作的流程圖；

〔圖6〕係根據一個實例實施方案繪示密封請求之處理的流程圖；

〔圖7〕係根據一個實例實施方案繪示解密封請求之處理的流程圖；

〔圖8〕顯示根據一個實例實施方案之處理電路系統的不同域及處理狀態的實例，且示意地指示在處理電路系統在域及處理狀態的特定組合中操作時可支援的密封及解密封能力；

〔圖9A〕及〔圖9B〕係根據二個實例實施方案之繪示可以其處理使用密封能力之請求的不同方式的流程圖；

〔圖10〕係根據一個實例實施方案繪示可如何處理修改能力之請求的流程圖；

〔圖11〕係根據一實例實施方案之繪示經執行以從記憶體載入能力之步驟的流程圖；

〔圖12〕係根據一個實例實施方案繪示解密封請求可如何取決於能力是否係預定類型而處理的流程圖；及

〔圖13〕顯示可使用的模擬器實例。

【實施方式】

【0012】 根據本文描述的技術，提供具有處理電路系統之設備，該處理電路系統用於執行在其期間產生對記憶體之存取請求的操作。處理電路系統經配置以使用識別約束資訊的能力產生用於存取請求的記憶體位址。由處理電路系統產生的記憶體位址可係執行位址轉譯之系統中的虛擬位址，或替代地可係不支援位址轉譯之系統中的實體位址。

【0013】 該設備亦具有檢查電路系統，以基於由該給定能力提供的約束資訊判定是否允許其記憶體位址係使用給定能力產生的給定存取請求。檢查電路系統之執行上述檢查的功能性可係與處理電路系統分開的組件，或替代地可提供在設備的處理電路系統內。

【0014】 有約束資訊可以其由關聯能力識別的若干種方法。例如，在一個實例實施方案中，能力可直接含有約束資訊。然而，在一替代實施方案中，能力可取而代之地指示（直接或間接地）約束資訊位於記憶體中的位置。

【0015】 檢查電路系統亦經配置以取決於與給定存取請求關聯的信任等級而進一步約束藉由給定存取請求對記憶體的存取。檢查電路系統的此功能性可以各種方式實施，例如，使用記憶體管理單元(MMU)、記憶體保護單元(MPU)、安全屬性單元(SAU)、或該等組件的組合。此類檢查電路系統傳統上已配置成在進一步約束對記憶體的存取時考慮與處理電路系統的目前操作模式關聯的信任等級，而非將任何特定信任等級與個別存取請求關聯。然而，根據本文描述的技術，給定能力具有與其關聯的能力信任等級，且該資訊亦可作為因素計入在由檢查電路系統執行的檢查中。具體而言，根據本文描述的技術，

與給定存取請求關聯的信任等級取決於與處理電路系統的目前操作模式關聯的目前模式信任等級及給定能力的能力信任等級二者。

【0016】 藉由提供與個別能力有關聯的能力信任等級，此可增強可以其管理及使用能力的方式。例如，由於如上文所討論的，在判定是否允許由給定存取請求所指定之對記憶體的存取繼續進行時，能力信任等級將由檢查電路系統列入考量，可提供在某些情形中允許能力由處理電路系統產生的機制，其中與特定能力關聯的能力信任等級有效地用以接著追蹤能力的起源及約束隨後使用該能力產生的存取。

【0017】 額外地，此一機制進一步促成支援特定使用情形保護，例如，以對抗混淆副攻擊。混淆副攻擊可在較低特權碼將指標傳至較高特權碼，尋求使用較高特權碼代表其執行某些操作時發生。通過能力信任等級的使用，此可防止較高特權碼意外地使用由非特權碼建立之惡意地定址記憶體之不應可由無特權碼存取之區域的指標。具體而言，在此類情況中，指標將已使用其能力信任等級不超過非特權碼之能力信任等級的能力產生，且因此即使嘗試從特權碼存取，導因於用以產生指標之能力的能力信任等級，記憶體存取電路系統將防止對特權記憶體的存取。

【0018】 根據本文描述的技術，與個別能力有關聯之能力信任等級的提供亦用以提供額外利益，尤其係藉由提供避免需要使用稀有的後設資料位元指示物件類型及解密封權限且亦避免需要解密封金鑰之用於處理密封能力的輕量機制。

【0019】　具體而言，根據本文描述的技術，設備進一步包含密封能力處理電路系統，以在目前模式信任等級係比給定密封能力的能力信任等級更低的信任等級時防止處理電路系統使用給定密封能力執行至少一個處理操作。因此，當考慮密封能力時，可將處理電路系統處理該密封能力的方式約束成將處理電路系統的目前模式信任等級及所關注之密封能力的能力信任等級二者列入考量。具體而言，藉由重使用與個別能力關聯的能力信任等級資訊，當將能力標記成密封時，該能力信任等級資訊可用以識別與密封能力關聯的特定軟體本文（軟體信任等級）。

【0020】　上述技術可使用在各式各樣的不同系統中。例如，處理電路系統可採取各種形式。例如，處理電路系統可係中央處理單元(CPU)，其經配置以在各種不同的操作模式中執行程式碼，但技術亦可有關於其他形式的處理電路系統施加，例如，直接記憶體存取(DMA)控制器、加密加速器等。

【0021】　有與給定存取請求關聯的信任程度可基於處理電路系統的目前操作模式及給定能力的能力信任程度二者以其判定的若干種方法。例如，系統可基於權限的授予或權限的限制，且與給定存取請求關聯的信任等級可取決於使用該等技術的何者。然而，根據一個實例實施方案，技術係基於權限的限制，且將與給定存取請求關聯的信任等級約束成目前模式信任等級及能力信任等級中表示較低信任等級的任一者。

【0022】　有可為能力指定能力信任等級的若干種方法，但在一個實例實施方案中，能力信任等級係編碼在給定能力內。此可以各種方式實施，但在一個實例實施方案中，用於各能力的約束資訊提供識別各種類型之允許對使用該

能力產生之記憶體位址的記憶體存取的至少一組權限，且將能力信任等級提供為額外權限。

【0023】 然而，雖然在上文描述的實例實施方案中將能力信任等級編碼在給定能力內，應注意到此係非要求，且可提供用於使能力信任等級與給定能力關聯的其他機制。例如，在一替代實施方案中，給定能力可提供指示含有能力信任等級之位置的識別符。因此，在此一實施方案中，能力信任等級資訊可駐存在他處，例如，在記憶體中，其中能力本身含有指示提供能力信任等級之後設資料之位置的值。用以指示含有能力信任等級之位置的識別符可採取各種形式。例如，其可係儲存在系統之全域暫存器中之位址的偏移，因此促成識別能力信任等級維持在記憶體中之何處的記憶體位址的判定。替代地，識別符可直接識別能力信任等級資訊在記憶體中儲存的位置。

【0024】 提供在各能力內的約束資訊可採取各種形式，但在一個實例實施方案中，提供用以判定用於使用該能力產生之用於任何存取請求的記憶體位址之記憶體位址的可允許範圍的邊界資訊。在一個實例實施方案中，約束資訊可包含此類邊界資訊且亦可包含識別允許用於使用該能力產生之記憶體位址之記憶體存取的類型的一組權限二者。該能力亦可含有其他資訊，例如，在產生記憶體位址時使用的指標值，例如，藉由將該指標值加至某個偏移以產生記憶體位址。所產生的記憶體位址接著可與邊界資訊比較，以判定所產生的記憶體位址是否在可允許範圍內。

【0025】 返回密封能力的討論，有可將能力識別為係密封的若干種方式，因此導致密封能力處理電路系統將給定密封能力的能力信任等級及與處理

電路系統關聯的目前模式信任等級二者列入考量而判定該能力應如何處理。然而，在一個實例實施方案中，各能力具有與其關聯的密封旗標，且密封能力處理電路系統回應於用於經選取能力的密封請求而取決於經選取能力的能力信任等級與目前模式信任等級的比較判定是否設定經選取能力的密封旗標以將經選取能力識別為密封能力。

【0026】　有密封旗標可以其指示設定（亦即，密封）或清除（亦即，解密封）狀態的若干種方式。例如，邏輯一值或邏輯零值其中一者可與設定狀態關聯，且實際上在一些實施方案中，提供多位元編碼可係適當的。進一步地，密封請求可以各種方式發生，但在一個實例實施方案中可，例如，由於處理電路系統執行密封指令而發生。

【0027】　在一個實例實施方案中，密封能力處理電路系統經配置以回應於密封請求而在經選取能力的能力信任等級大於目前模式信任等級時禁止設定密封旗標。允許密封旗標設定所需要的實際目前模式信任等級可取決於實施方案改變。例如，每當目前模式信任等級大於或等於能力信任等級時，可允許將能力密封，或替代地，能力的密封可僅限制於目前模式信任等級與能力信任等級相同的情形。

【0028】　在一個實例實施方案中，亦允許密封能力在某些情況中解密封。例如，在一個實例實施方案中，密封能力處理電路系統回應於用於經選取密封能力的解密封請求而在經選取密封能力的能力信任等級大於目前模式信任等級時禁止清除經選取密封能力的密封旗標。與密封一樣，允許密封旗標清除所需要的實際目前模式信任等級可取決於實施方案改變。例如，每當目前模式

信任等級大於或等於能力信任等級時，可允許將能力解密封，或替代地，能力的解密封可僅限制於目前模式信任等級與能力信任等級相同的情形。

【0029】 進一步地，解密封請求可以各種方式發生，但在一個實例實施方案中可，例如，由於處理電路系統執行解密封指令而發生。

【0030】 應注意根據上述技術，由於是否允許將能力密封或將密封能力解密封的決定係將目前模式信任等級及能力信任等級二者列入考量而作出，不需要使用密封或解密封金鑰。

【0031】 如先前提及的，密封能力處理電路系統將在目前模式信任等級係比給定密封能力的能力信任等級更低的信任等級時防止處理電路系統使用給定密封能力執行至少一個處理操作。所禁止的處理操作的數目可取決於實施方案而變化，但在一個實例中，密封能力處理電路系統經配置以在目前模式信任等級係比給定密封能力的能力信任等級更低的信任等級時防止處理電路系統使用給定密封能力執行複數個處理操作的任何者，但允許給定密封能力在儲存元件之間移動。

【0032】 其可用以允許密封能力在儲存元件之間移動，用以允許此類密封能力在暫存器與記憶體之間移轉，且實際上若有需要，允許暫存器間移動。然而，一般會係若目前模式信任等級低於密封能力的能力信任等級，將防止處理電路系統使用密封能力執行大部分（若係非全部）處理操作的情形。然而，仍可能係允許某些動作的情形。例如，即使目前模式信任等級小於所關注密封能力的能力信任等級，允許清除將能力識別成能力而非通用資料的欄位（在本文中稱為標籤位元）可係可行的，有效地使能力無效化。

【0033】 在一個實例實施方案中，密封能力處理電路系統經配置以與目前模式信任等級無關地要求給定密封能力在允許能力在後續處理操作中由處理電路系統使用之前解密封。

【0034】 然而，在一替代實施方案中，密封能力處理電路系統可經配置以至少在目前模式信任等級與給定密封能力的能力信任等級相同時允許處理電路系統使用給定密封能力執行一或多個處理操作而無需將給定密封能力解密封。此功能性可，例如，限制於目前模式信任等級與能力信任等級相同的情況，或可替代地可在目前模式信任等級大於或等於能力信任等級的情況中允許。

【0035】 允許在上文識別的情形中使用給定密封能力執行的一或多個處理操作可取決於實施方案而改變。例如，可允許解參考操作以使用給定密封能力產生記憶體位址。取而代之地或額外地，亦可允許能力修改操作以修改由給定密封能力識別的資訊。當執行此類修改操作時，可改變能力的資訊及關聯後設資料的任何者（有時稱為突變，特別係後設資料正被改變時），但一般而言，此類操作將受約束以不降低由能力指定的約束。例如，一般會係若變化係用以降低範圍或降低權限，將僅允許對範圍資訊或對權限的任何變化的情形。

【0036】 處理電路系統可經配置以各種不同方式操作，其中目前模式信任等級取決於處理電路系統目前如何操作。例如，在一個實施方案中，處理電路系統可經配置以在複數個狀態的一者中執行程式碼，該複數個狀態包含至少特權狀態及非特權狀態，且目前模式信任等級可取決於目前程式碼在複數個狀態的何者中執行。應注意到可有二種不同狀態，亦即，特權狀態非特權狀態，

或可有具有不同特權等級的N個不同狀態，其中N大於2，且在此等情境的其中一者中，目前模式信任等級可取決於目前程式碼正在哪個狀態中執行而設定。例如，一特定實施方案可將不同的例外等級(exception level, EL)（諸如EL0、EL1、及EL2）提供為不同狀態，其中EL2比EL1有更多特權，且EL1比EL0有更多特權。

【0037】　替代地，或額外地，處理電路系統可經配置以在複數個安全領域的一者中執行程式碼，該複數個安全領域包含至少安全域及較不安全域，且目前模式信任等級可取決於目前程式碼在複數個安全領域的何者中執行。與處理狀態一樣，可能僅有二個域，亦即安全域或不安全域，或替代地可有M個不同域，其中M大於2，該等域的各者具有不同的安全等級，且目前模式信任等級接著可取決於目前程式碼在安全領域的何者中執行而設定。

【0038】　亦應注意到目前模式信任等級可取決於多個不同的正交信任等級設定，且可有二個以上的正交信任等級。因此，例如，在一個實施方案中，處理電路系統可能能夠在上文討論的不同狀態及不同安全領域二者中操作，且目前模式信任等級可取決於該等因素二者設定。

【0039】　能力可儲存在系統內的各種位置中。例如，設備可具有用以儲存能力以用於由處理電路系統參考的一組能力暫存器，但亦可具有可用以儲存一或多個能力的記憶體電路系統。處理電路系統可經配置以執行載入操作，以將經選取能力從記憶體電路系統載入至來自該組能力暫存器的經選擇能力暫存器中。在此程序期間，處理電路系統可經配置以選擇性地修改能力信任等級，使得經選取能力在儲存至經選擇能力暫存器中時具有受約束不超過目前模式信

任等級或經選取能力在儲存在記憶體電路系統中時的能力信任等級的能力信任等級。因此，雖然能力之仍可保持在記憶體電路系統內的原始版本將不使其之關聯能力信任等級改變，該版本在儲存至能力暫存器中時可使其之能力信任等級在載入操作期間由處理電路系統改變，以約束該能力信任等級，且因此約束使用該經載入能力執行的後續記憶體存取操作取決於能力在儲存在能力暫存器中時的能力信任等級。

【0040】　雖然能力信任等級的此類選擇性降級對標準能力可係適當的，與密封能力有關的此一動作需要受抑制，因為要求密封能力不被修改。因此，在一個實例實施方案中，處理電路系統進一步經配置以在經選取能力係密封能力時禁止在此一載入操作期間修改能力信任等級。在密封能力的情形中，沒有由允許較不受信任碼具備更受信任密封能力所導致的安全問題，因為密封能力處理電路系統的較早經識別動作將防止較不受信任碼使用更受信任密封能力。

【0041】　在一些實施方案中，載入操作可在一些情況中執行以將一般資料（而非能力）載入至能力暫存器中，且在此類情況中，資料中之會與能力信任等級關聯的位元實際上係該資料，能力不被修改可係重要的，因為在此情形中，其係非正受處理的能力且修改該等位元會損壞資料。因此，在一個實例實施方案中，處理電路系統可經配置以僅在經選取能力具有識別經選取能力係有效能力的控制值（且能力係非密封能力）時在載入操作期間選擇性地修改能力信任等級。藉由此一方法，上文描述之能力信任等級在載入操作期間的選擇性修改將僅在非密封能力實際上正在載入至能力暫存器中時執行。

【0042】 在一個實例實施方案中，密封能力處理電路系統經配置以產生指示處理用於經選取密封能力的解密封請求的結果的結果資訊。結果資訊可採取各種形式，但通常將足以促成作出能力是否已成功地解密封的判定。例如，在解密封不成功的事件中，可引起故障。替代地，可設定一或多個狀態旗標以對軟體指示失敗。作為另一實例，可將指示傳回至軟體以識別能力已成功地解密封，且若有需要，亦可提供指示以識別已成功解密封的能力具有恰匹配目前模式信任等級之能力信任等級的情況。作為另一實例，可允許未成功的解密封操作悄悄地失敗，其中經產生以指示成功解密封之資訊的缺少稍後用以判定解密封操作失敗。

【0043】 若有需要，亦可產生結果資訊以識別處理密封請求的結果，例如，以識別密封操作已成功或未成功。在一個實例實施方案中，可假設成功，且資訊可僅在密封操作未成功時輸出。在又一進一步實例實施方案中，資訊可與密封請求成功或未成功無關地不產生，且未成功密封操作可在稍後階段偵測到，例如，在解密封期間。

【0044】 在一些實例實施方案中，可有係保留類型的一些能力，且其等，例如，由架構使用以指示特定事件或功能。在一個實例實施方案中，密封能力處理電路系統可經配置而與目前模式信任等級無關地禁止此類能力的解密封。若有需要，嘗試將此一能力解密封可導致錯誤確立，清除標籤位元以有效地使能力無效化，或將某些其他指示提供給軟體。有可識別此類保留類型能力的若干種方式。作為一特定實例，其等可具有定義無效範圍（例如，藉由使上邊界低於下邊界）的範圍邊界資訊。

【0045】 現在將參照圖式描述特定實例。

【0046】 本文描述的技術可使用在各種資料處理系統中，且與此類系統內的不同類型的處理電路系統有關聯。例如，技術可與採用中央處理單元(CPU)之形式的處理電路系統有關聯地使用，但可替代地與其他處理電路系統有關聯地使用，諸如直接記憶體存取(DMA)控制器、加密加速器等。純粹作為以下圖1中的說明性實例，將CPU的處理管線視為係可將所描述之技術使用於其內之處理電路系統的實例。

【0047】 圖1示意地繪示包含用於處理指令之處理管線4之資料處理設備2的實例。在此實例中，處理管線4包括若干個管線級，該等管線級包括提取級6、解碼級8、發布級10、執行級12、及寫回級14，但將理解可提供其他類型的級或級的組合。例如，在一些實例實施方案中，可包括用於執行暫存器重命名的重命名級。待處理的指令在級間移動，且在指令在管線4的一個級待決的同時，另一指令可在不同級待決。

【0048】 提取級6從1級(L1)指令快取記憶體20提取指令。提取級6通常可循序地從連續指令位址提取指令。然而，提取級亦可具有用於預測分支指令之結果的分支預測器22，且提取級6可在採用經預測分支時提取來自（非循序）分支目標位址的指令，或在未採用經預測分支時從次一循序位址提取指令。分支預測器22可包括用於儲存用於預測某些分支是否可能採用之資訊的一或多個分支歷史表。例如，分支歷史表可包括用於追蹤先前經執行分支的實際結果或表示對分支作出之預測的信心的計數器。分支預測器22亦可包括分支目標位址

快取記憶體(BTAC) 24以用於快取分支指令的先前目標位址，使得此等可在後續遭遇到相同分支指令時預測。

【0049】 將經提取指令傳至解碼指令以產生經解碼指令的解碼級8。經解碼指令可包含用於控制執行級12執行適當的處理操作的控制資訊。對於提取自快取記憶體20的一些更複雜指令，解碼級8可將該等指令映射成可稱為微操作(micro-operation)（μops或uop）的多個經解碼指令。因此，提取自L1指令快取記憶體20的指令與由管線的稍後級所見的指令之間可能沒有一對一關係。一般而言，本申請案中對「指令(instruction)」的引用應解釋為包括微操作。

【0050】 將經解碼指令傳至判定執行指令所需的運算元是否可用且當運算元可用時發布指令以用於執行的發布級10。一些實例實施方案可支援依序處理，使得指令以對應於指令係從L1指令快取記憶體20提取的程式順序的順序發布以用於執行。其他實例實施方案可支援亂序執行，使得指令可在不同於程式順序的順序發布至執行級12。亂序處理對改善效能可係有用的，由於在較早指令在等待運算元時而推遲的同時，可先執行程式順序中之其運算元可用的稍後指令。

【0051】 發布級10將指令發布至執行指令以實行各種資料處理操作的執行級12。例如，執行級可包括若干個執行單元30、32、34，該等執行單元包括用於在整數值上實行算術或邏輯操作的算術/邏輯單元(ALU) 30、用於在以浮點形式表示的值上實行操作的浮點(FP)單元32、及用於實行將資料值從1級(L1)資料快取記憶體36載入至暫存器40的載入操作或用於將資料值從暫存器40儲存至L1資料快取記憶體36之儲存操作的載入/儲存單元34。應理解此等僅係可提供之

執行單元的類型的一些實例，且亦可提供許多其他種類。為實行處理操作，執行級12可從一組暫存器40讀取資料值。經執行指令的結果可接著藉由寫回級14寫回至暫存器40。

【0052】 L1指令快取記憶體20及L1資料快取記憶體36可係包括多級快取記憶體的快取記憶體階層的部分。例如，亦可提供二級(L2)快取記憶體44且可可選地提供更多級的快取記憶體。在此實例中，L2快取記憶體44係在L1指令快取記憶體20與L1資料快取記憶體36之間共用，但其他實例可具有分開的L2指令及資料快取記憶體。當待提取指令不在L1指令快取記憶體20中時，則其可從L2快取記憶體44提取，且類似地，若指令不在L2快取記憶體44中，則其可從主記憶體50提取。類似地，回應於載入指令，若資料不在L1資料快取記憶體36中，其可自L2快取記憶體44提取，且若有需要，從記憶體50提取。任何已知方案皆可用於管理快取記憶體階層。

【0053】 由管線4使用以參考程式指令及資料值的位址可係虛擬位址，但至少主記憶體50且亦可選地快取記憶體階層的至少一些級可實體地定址。因此，可提供轉譯後備緩衝區(TLB)（例如，在待於稍後更詳細地描述的記憶體存取檢查電路系統52內）以用於將由管線4使用的虛擬位址轉譯成用於存取快取記憶體或記憶體的實體位址。例如，TLB可包括各指定虛擬位址空間之對應頁的虛擬頁位址及虛擬頁位址應映射至其的對應實體頁位址，以將對應頁內的虛擬位址轉譯成實體位址的若干個項。例如，虛擬及實體頁位址可對應於對應虛擬及實體位址的最高有效部分，其中當將虛擬位址映射至實體位址時，剩餘的最低有效部分保持不變。以及位址轉譯資訊，各TLB項亦可包括指定存取權

限的一些資訊，諸如指示位址的某些頁是否在管線4的某些模式中可存取。在一些實例實施方案中，TLB項亦可定義位址之對應頁的其他性質，諸如定義回應於讀取或寫入操作而更新快取記憶體階層的哪些級的快取記憶體策略資訊（例如，快取記憶體是否應以寫回或完全寫入模式操作），或與管線4發布資料存取的順序相比，定義對對應頁中之位址的資料存取是否可由記憶體系統重排序的資訊。

【0054】 雖然可使用單一級TLB，將理解可替代地提供TLB的階層，使得一級(L1) TLB可包括用於轉譯若干個最近存取頁中之位址的TLB項，且可提供二級(L2) TLB以用於儲存用於更大數目之頁的項。當所需項不存在於L1 TLB中時，則其可從L2 TLB或從階層中的進一步TLB提取。若用於待存取頁之所需項不在TLB的任何者中，則可執行頁表遍歷以存取記憶體50中的頁表。任何已知的TLB管理方案皆可使用在本技術中。

【0055】 再者，將理解一些系統可支援多級位址轉譯使得，例如，第一TLB（或TLB的階層）可用以將虛擬位址轉譯成中間位址，且使用一或多個進一步（多個）TLB的第二級位址轉譯可接著將中間位址轉譯成用以存取快取記憶體或記憶體的實體位址。例如，此可用於支援第一級位址轉譯可由作業系統管理且第二級位址轉譯可由超管理器管理的虛擬化。

【0056】 如圖1所示，設備2可具有一組有界指標暫存器60。雖然在圖1中將一組有界指標暫存器顯示成與該組通用資料暫存器40實體地分開，在一替代實例實施方案中，相同實體儲存器可用以提供通用資料暫存器及有界指標暫存器二者。

【0057】　各有界指標暫存器60包括可用以判定待存取之資料值的位址的指標值62，及在使用對應指標62時指定可允許位址範圍的範圍資訊64。有界指標暫存器60亦可包括可定義指標之使用上的一或多個限制/權限的限制資訊66（在本文中亦稱為權限資訊）。例如，限制66可用於限制可使用指標62之指令的類型，或可使用指標之管線4的模式。因此，可認為範圍資訊64及限制資訊66定義允許指標62在其內使用的能力。當嘗試在經定義能力外側使用指標62時，可觸發錯誤。範圍資訊64可用於，例如，確保指標保持在某些已知邊界內且不分散至記憶體位址空間之可能含有敏感或安全資訊的其他區域。在相同實體儲存器用於通用資料暫存器及有界指標暫存器二者的一實例實施方案中，則在一個實例實施方案中，指標值62可，例如，儲存在與用於對應通用暫存器相同的儲存位置內。

【0058】　圖2顯示其之可允許範圍係用以防止對資料或指令的未授權存取之指令類型的實例。如圖2之頂部部分所示，特定有界指標暫存器PR1包括給定指標值62及範圍資訊64，該範圍資訊在此實例中係使用定義可允許範圍之下邊界的下邊界位址68及定義可允許範圍之上邊界的上邊界位址69指定。例如，邊界68、69經設定以定義位址範圍80000至81000。當某些指令參考有界指標暫存器PR1且從指標62判定的位址在此範圍外側，可觸發錯誤。

【0059】　例如，如圖2之部分A所示，在一些系統中，若嘗試將指標暫存器60中之指標62的值設定成位於範圍資訊64所指定之範圍外側的值（此處，假設指標直接指定位址），可觸發錯誤。此避免指標62採用指定範圍外側的任何值，使得可確保使用指標的任何存取安全地位於允許範圍內。替代地，如圖2

之部分B所示，當指標62的位址位於指定範圍外側時，當指令嘗試存取由該位址識別的位置時，可觸發錯誤。因此，可能仍可允許將指標62設定成指定範圍外側的值，但若該位址位於允許範圍外側，一旦在該指標位址（或衍生自該指標的位址）嘗試資料存取，則可觸發錯誤。其他系統可回應於顯示於圖2之部分A及B中的指令的類型而觸發錯誤。

【0060】 範圍資訊64可以不同方式設定。例如，安全碼或操作系統或超管理器可為給定指標指定所允許的範圍。例如，指令集架構可包括用於設定或修改給定指標62之範圍資訊64的若干個指令，且此等指令的執行可限制於某些軟體或處理器4的某些模式或例外狀態。可使用用於設定或修改範圍資訊64的任何已知技術。

【0061】 除了在執行參考指標的某些指令時可在執行級12使用的該組有界指標儲存元件60外，程式計數器能力(program counter capability, PCC)暫存器80亦可用以在指令正從一級指令快取記憶體20提取時在提取級6提供類似功能性。具體而言，程式計數器指標可儲存在欄位82中，其中PCC 80亦提供範圍資訊84及任何適當的限制資訊86，與以該組有界指標儲存元件60中之指標的各者提供範圍及限制資訊類似。

【0062】 圖3示意地繪示標籤位元如何與個別資料區塊有關聯地使用以識別該等資料區塊表示能力（亦即，有界指標及關聯限制資訊）或表示正常資料。具體而言，記憶體位址空間110將儲存一般將具有指定尺寸的一系列資料區塊115。純粹為了說明起見，在此實例中假設各資料區塊包含128個位元，但在其他實例實施方案中，可使用不同尺寸的資料區塊，例如，在能力由64位元

的資訊定義時，64位元的資料區塊。提供與各資料區塊115有關聯的標籤欄位120，該標籤欄位在一個實例中係稱為標籤位元的單一位元欄位，其經設定以識別關聯資料區塊表示能力，且經清除以指示關聯資料區塊表示正常資料，且因此無法作為能力處理。將理解與設定或清除狀態關聯的實際值可取決於實例實施方式而變化，但純粹作為說明，在一個實例實施方案中，若標籤位元具有1的值，其指示關聯資料區塊係能力，且若其具有0的值，其指示關聯資料區塊含有正常資料。

【0063】 當將能力載入至有界指標暫存器60的一者（在本文中亦稱為能力暫存器）中時，諸如圖3所示的能力暫存器100，則標籤位元隨能力資訊移動。因此，當將能力載入至能力暫存器100中時，指標102、範圍資訊104、及限制資訊106（以下稱為權限資訊）將載入至能力暫存器中。額外地，與能力暫存器有關聯或作為其內的特定位元欄位的標籤位元108將設定以識別內容表示能力。類似地，當能力儲存回記憶體時，有關標籤位元120將與能力儲存於其中之資料區塊有關聯地設定。藉由此一方法，可能在能力與正常資料之間區分，且因此確保不可將正常資料使用為能力。

【0064】 返回圖1，設備2可具備能力檢查電路系統33，該能力檢查電路系統可與其記憶體位址係使用給定能力產生的給定存取請求有關聯地執行能力檢查操作，以基於由能力識別的約束資訊判定是否允許存取請求。此可，例如，參考先前討論之可統稱為能力之約束資訊的範圍資訊及限制/權限資訊執行。因此，純粹作為實例，若對記憶體位址的寫入存取請求尋求使用指示該能

力僅可用於讀取而非寫入的能力執行，則能力檢查電路系統33可判定存取請求不可繼續進行，且可，例如，在此類情形下發布故障信號。

【0065】 然而，假設能力檢查操作通過，則可將記憶體存取請求傳播至可提供一些進一步檢查以確保允許存取繼續進行的記憶體存取檢查電路系統52。例如，處理電路系統可能能夠在多個不同的操作模式中操作，且各操作模式可，例如，與某些特權狀態、及/或與設備在其中操作的特定安全領域關聯，且記憶體的某些區域僅可在處理電路系統正在操作的一個可能模式中或操作之可能模式的子集中操作時存取。

【0066】 記憶體存取檢查電路系統52因此可基於針對記憶體位址空間的各種區域指定的屬性資料檢查是否允許對記憶體系統的存取。記憶體存取檢查電路系統可包括用於儲存安全領域定義資料的安全屬性單元(SAU) 56，該安全領域定義資料定義與記憶體位址空間的各別區域關聯的安全領域。基於安全屬性資料，安全屬性單元56可取決於處理迂迴之操作的目前安全領域且取決於與包括目標位址之區域及記憶體存取關聯的安全領域而檢查是否允許記憶體存取。在其他實施方案中，SAU 56可不直接儲存安全領域定義資料，而取而代之地可存取儲存於他處的安全定義資料以執行記憶體存取檢查。在一些系統中，安全領域定義資料可儲存在記憶體系統50中，或可儲存在系統2中之他處的組態暫存器中。

【0067】 處理電路系統4可在操作的目前安全領域中操作，操作的目前安全領域通常對應於與目前正執行之指令的位址關聯的安全領域（雖然可有一些例外，例如，當處理域之間的轉變時）。雖然在安全域中操作，處理電路系統

可具有對與安全域及較不安全域二者關聯之記憶體區域中之資料的存取，雖然在較不安全域中操作時，處理電路系統可具有對與較不安全域關聯之區域中之資料的存取，但可能不允許存取位址空間之SAU 56指定為與安全域關聯之區域中的資料。此促成保護敏感資料免於來自在較不安全域中操作之碼的未授權存取。如將在本文中更詳細地討論的，當SAU 56正在執行此類檢查以判定存取是否可繼續進行時，其不僅考慮處理電路系統的目前安全領域，也考慮與個別存取請求關聯的更精細粒化資訊。此更精細粒化資訊係基於處理電路系統的安全領域，及與用以產生存取請求之記憶體位址的能力關聯的信任等級指示。

【0068】 如圖1所示，記憶體存取檢查電路系統52可包括檢查對記憶體系統50的記憶體存取是否滿足存取權限的記憶體保護單元(MPU) 54，該等存取權限可指定，例如，允許處理電路系統4的哪些存取權限存取記憶體的給定區域，或可指定位址空間的記憶體區域是否可由讀取及寫入操作二者存取或係禁止對其寫入的唯讀區域。由MPU 54使用的存取權限可，例如，由更多特權程序（諸如超管理器或作業系統）指定以控制允許較少特權程序（諸如應用程式）存取及如何存取（唯讀或讀取/寫入）記憶體的哪些區域。由MPU 54提供的權限可正交於由SAU 56提供的該等權限，使得對待允許之給定記憶體存取請求的檢查應基於對MPU 54及SAU 56二者定義的存取權限通過。雖然MPU 54在圖1中顯示成單一實體，在一些實例中，可提供各與安全領域的一者關聯之分開的安全MPU及較不安全MPU，使得不同記憶體存取權限可取決於目前域係安全域或較不安全域而對記憶體的給定區域指定（例如，區域在較不安全域中可係唯讀的，但在安全域中係可讀及可寫的）。

【0069】 與SAU的先前討論一樣，當MPU正在執行其存取權限檢查時，其將與給定存取請求關聯的信任等級列入考量，該給定存取請求不僅取決於處理電路系統的目前操作模式，且亦取決於與用以產生記憶體位址之能力關聯的能力信任等級。

【0070】 可提供一或多個控制暫存器90以儲存啓用/停用旗標以用於由本文描述之實施方案提供的某些特徵。作為特定實例，選擇性地修改具有比處理電路系統的目前操作模式的信任等級更低的信任等級的不可變能力可係可行的，但此行為可由控制暫存器90內的單獨位元控制。類似地，當尋求將具有與其關聯之較高信任等級的能力從處理電路系統之較低特權操作模式內解參考時，可引起故障，且此類功能性可可能性再度由在控制暫存器90內的啟用控制位元所閘控。如亦將於稍後討論的，能力可從記憶體載入至能力暫存器中，且在此程序期間，所載入之能力的關聯信任等級可選擇性地降級，但此類功能可再度由控制暫存器90中的單獨控制位元所控制。

【0071】 根據本文描述的技術，能力具備關聯的能力信任等級資訊，且該信任等級指示可作為因素計入在由記憶體存取檢查電路系統52實施的記憶體存取檢查程序中。有此信任等級指示可以其與能力有關聯地提供的各種方式，但圖4繪示一個實例實施方案。在圖4所示的實例中，能力100含有指標值102及一些範圍資訊104（在本文中亦稱為邊界資訊）。亦可將一組權限連同先前描述的標籤位元108提供在能力內，該標籤位元可經設定或清除以識別對應的資料區塊是否將作為能力處理。

【0072】 對能力指定的權限可取決於實施方案而改變，但在一個實例實施方案中，權限包括其值指示能力是否可用以產生用於讀取存取之記憶體位址的讀取權限位元130、其值指示能力是否可用以產生用於寫入存取之記憶體位址的寫入權限位元132、及其值指示能力是否可用以產生待提取及執行之指令的記憶體位址的執行權限位元134。其他資訊可在能力內識別，例如，以指示是否將能力視為係不變的。儘管此類資訊可直接指定為能力中的額外資訊，在一些實例實施方案中，其可從已提供在能力內的其他資訊的狀態推斷。例如，在一個特定實施方案中，當執行位元經設定時，除非通過指標值之可導因於指令執行的正常遞增，能力視為係不可變的，其中由能力指定的資訊不可在標籤位元未清除的狀態下修改（有效地使能力無效化）。

【0073】 如圖4所示，在一個實例實施方案中，使權限欄位延伸以提供信任等級指示欄位136，該信任等級指示識別與能力100關聯的信任等級。信任等級可直接編碼至能力100的欄位136中，或替代地，信任等級指示欄位136可提供用以指示含有信任等級資訊之記憶體位址的識別符。此一識別符可直接指示信任等級資訊的記憶體位置，或其可，例如，指定可施加至儲存在系統中的全域暫存器中的位址的偏移以識別含有信任等級資訊的位置。

【0074】 圖5A係根據一個實例實施方案之示意地繪示能力信任等級資訊如何用以約束對記憶體之存取的方塊圖。在此實例中，處理電路系統150包括在正在考慮其記憶體位址係使用給定能力產生之存取請求時可使用的能力檢查區塊155，以執行能力檢查操作以基於由給定能力指定的約束資訊判定是否允許存取請求。因此，能力檢查可涉及對能力之範圍及權限資訊的參考以判定是

否允許存取繼續進行。在能力檢查失敗的事件中，可提供失敗指示給處理電路系統，且此失敗指示可採取多種形式，例如，故障信號。然而，若能力檢查通過，則將此指示給信任等級產生區塊160，該信任等級產生區塊亦接收能力100的能力信任等級資訊136。

【0075】 除了能力信任等級外，信任等級產生區塊160亦接收目前模式信任等級的指示，此係與處理電路系統的目前操作模式關聯的信任等級。接著將能力信任等級及目前模式信任等級二者組合地用以形成存取請求的信任等級，該存取請求的信任等級與透過路徑165發布之請求的記憶體位址有關聯地透過路徑167傳播。有信任等級產生區塊160可使用目前模式信任等級及能力信任等級二者以決定存取請求的信任等級的各種方式，但在一個實例實施方案中，將與存取請求關聯的信任等級約束成目前模式信任等級及能力信任等級中表示較低信任等級的任一者。

【0076】 記憶體存取檢查電路系統170接收請求的記憶體位址及存取請求的關聯信任等級二者，且可參考可對不同記憶體區域指定的經儲存存取權限資訊175執行記憶體存取檢查操作。具體而言，對於若干個不同記憶體區域的各者，存取權限資訊可有效地指示需要為存取請求提供的所需信任等級以使存取能繼續進行。若透過路徑167接收的存取請求的信任等級不符合所需信任等級，則可導致存取失敗，然而對記憶體的存取可另外從記憶體存取檢查電路系統170透過路徑180傳播。

【0077】 如先前討論的，根據本文描述的技術，與個別能力有關聯之能力信任等級的提供亦用以提供避免需要使用稀有的後設資料位元指示物件類型及解密封權限且亦避免需要解密封金鑰之用於處理密封能力的輕量機制。

【0078】 具體而言，根據本文描述的技術，將密封旗標欄位138加至能力以識別關聯能力係密封或解密封的，此密封旗標欄位138繪示於圖4中（其亦可稱為IsSealed旗標）。在一個實施方案中，此可係具有一個狀態（例如，邏輯一值）指示能力係密封的，且另一狀態（例如，邏輯零值）指示能力係解密封的單一位元。然而，密封旗標不需要係單一位元值，且在一些實施方案中，可使用多位元值以擷取一些額外資訊。

【0079】 進一步地，如圖5A所示，使用密封能力處理電路系統185判定如何處理密封能力。可將密封能力處理電路系統185提供為單獨組件，或可併入處理電路系統150內，如圖5A所示。當處理密封能力時，密封能力處理電路系統185不需要使用密封金鑰或解密封金鑰，而取而代之地能夠參考與給定能力有關聯地擷取的能力信任等級資訊，以與處理電路系統150關聯的目前模式信任等級結合以存取該給定能力應如何處理。基於此資訊，密封能力處理電路系統185可，例如，判定給定能力是否可密封，在該事件中，所需要的係密封能力處理電路系統導致密封旗標設定、判定給定密封能力是否可解密封、在該事件中，所需要的係密封能力處理電路系統導致密封旗標清除、及取決於密封能力的能力信任等級與處理電路系統的目前模式信任等級的比較，判定密封能力可如何由處理電路系統使用。

【0080】 圖5B係繪示圖5A的電路系統在一個實例實施方案中的操作的流程圖。在步驟200，判定需要存取請求。之後，在步驟205，判定為存取請求指定的能力是否係密封能力。若係如此，則可在步驟210判定是否允許使用密封能力。在一些實施方案中，可始終有不可將密封能力解參考以產生記憶體位址的情形（取而代之地，任何此類密封能力需要先解密封），且在該事件中，程序可直接進行至步驟215而不需要執行步驟210的檢查，從而將防止存取請求。然而，在一些實施方案中，取決於處理電路系統的目前模式的相對信任等級及指定能力的能力信任等級，可為待使用的密封能力提供準備而不需要先解密封。例如，在一個實施方案中，若目前模式信任等級大於或等於能力信任等級，則可允許使用密封能力。

【0081】 因此，若在步驟210，判定允許使用密封能力，程序繼續進行至步驟220，且若在先前步驟205，判定指定能力係非密封能力，實際上亦繼續進行至步驟220。然而，若在步驟210，判定不允許使用密封能力，則程序繼續進行至步驟215，防止存取請求發生。有可防止存取請求的若干種方式。例如，可確立能力檢查失敗信號，或可採取某個其他動作以識別存取請求已嘗試使用密封能力。

【0082】 假設程序確實繼續進行至步驟220，則在該步驟，參考指定能力的指標值判定用於存取請求的記憶體位址。在步驟225，接著參考指定能力的邊界及權限資訊執行能力檢查，以判定存取是否可繼續進行。

【0083】 因此，在步驟230，判定能力檢查是否已通過，且若係否，程序繼續進行至步驟235，確立能力檢查失敗信號。在一個實例實施方案中，步驟235可用與步驟215相同的方式實施。

【0084】 一般而言，當在步驟225執行能力檢查時，信任等級資訊並未使用而取而代之地保留以用於傳遞至記憶體存取檢查電路系統170。然而，在某些實施方案中，信任等級資訊亦可在能力檢查程序期間使用。例如，處理電路系統可經配置以在與用以產生用於存取請求之記憶體位址的能力關聯的能力信任等級超過與處理電路系統的目前操作模式關聯的目前模式信任等級的情況中在嘗試執行藉由給定存取請求識別的存取時在步驟235發布故障信號。具體而言，在一些實施方案中，可將在某個信任等級操作的處理電路系統尋求使用具有更高能力信任等級的能力視為係不正確行為。

【0085】 若能力檢查經判定已在步驟230通過，則在步驟240，存取請求的信任等級係基於目前模式信任等級及能力信任等級二者由信任等級產生區塊160判定。之後，在步驟245，將存取請求與存取請求的經判定信任等級一起傳播至記憶體存取檢查電路系統170，使得記憶體存取檢查電路系統170接著可基於存取請求的該經指示信任等級執行存取權限檢查。

【0086】 圖6係根據一個實例實施方案繪示當處理密封請求時所執行之步驟的流程圖。密封請求可以各種方式產生，但在一個實例實施方案中可由於處理電路系統執行密封指令而發生。在步驟300，判定密封請求是否已接收，且若係如此，則可在作為可選步驟的步驟305判定在目前模式信任等級中是否允許密封。在一些實施方案中，此一檢查可視為係不必要的，因為實施方案原則

上可在任何目前模式信任等級中允許密封，受於下文描述的進一步檢查。然而，在一替代實施方案中，可將密封限制在某些操作模式，且在該事件中，可在步驟305執行檢查。

【0087】 若判定在目前模式信任等級中不允許密封，則在步驟310，防止密封經識別能力。在步驟310，設備可進一步輸出識別密封程序失敗的資訊，例如，藉由確立失敗信號，或藉由更新某些狀態旗標。然而，在一替代實施方案中，可將輸出密封程序的任何成功或失敗指示視為係不必要的，因為密封失敗可經配置以在稍後階段拾取，例如，在後續解密封程序期間。

【0088】 若在步驟305，判定在目前模式信任等級中允許密封，或在不執行可選步驟305的事件中，每當在步驟300接收到密封請求時，則程序繼續進行至步驟315，判定經識別能力的能力信任等級。如參照圖4於先前討論的，此資訊可，例如，在能力中係直接可用的，具體而言，在信任等級指示欄位136中。

【0089】 在步驟320，密封能力處理電路系統185接著判定處理電路系統的目前模式信任等級是否大於或等於經識別能力的能力信任等級。若係否，則程序繼續進行至步驟310，防止經識別能力密封。

【0090】 然而，假設目前模式信任等級大於或等於能力信任等級，則程序繼續進行至步驟325，藉由設定密封旗標138而將經識別能力密封。以參考步驟310於先前討論的相同方式，若有需要，設備可經配置以輸出指示能力成功密封的資訊。然而，在假定密封成功的一個實例實施方案中，且因此不輸出資

訊。在密封不成功的事件中，此可藉由在步驟310輸出的資訊指示，或如先前提及的，可在稍後階段中拾取，例如，在能力的解密封期間。

【0091】 圖7係繪示回應於接收到解密封請求而執行之步驟的流程圖。當在步驟350接收到此一請求時，則作為可選步驟355，可判定在目前模式信任等級中是允許解密封。如相關於圖6之密封程序中的等效步驟305於先前討論的，若有需要，可將解密封的能力限制在特定操作模式。然而，在一個實例實施方案中，不施加此類通用限制，且因此不需要步驟355。

【0092】 若實施步驟355，且判定在目前模式信任等級中不允許解密封，則在步驟360，防止經識別能力解密封。資訊可在此點輸出以識別解密封尚未成功。例如，可引起故障信號，或替代地可設定一或多個狀態旗標以對軟體指示失敗。作為另一實例，可允許未成功的解密封操作悄悄地失敗，其中經產生以指示成功解密封之資訊的缺少稍後用以判定解密封操作失敗。

【0093】 若在步驟355，判定在目前模式信任等級中允許解密封，或若不需要步驟355，在步驟350，直接回應於解密封請求，程序繼續進行至步驟365，參考信任等級指示欄位136判定經識別能力的能力信任等級。

【0094】 接著在步驟370，判定目前模式信任等級是否大於或等於能力信任等級，且若係否，在步驟360，防止經識別能力解密封。

【0095】 然而，假設目前模式信任等級大於或等於能力信任等級，則在步驟375，藉由清除密封旗標而將經識別能力解密封。若有需要，資訊可在此點輸出以指示能力成功解密封。在一個特定實施方案中，在此點產生二個輸出信號。第一信號用以識別能力經密封且成功地解密封，同時第二信號可識別能

力是否從處理電路系統的相同模式信任等級密封及解密封。因此，第二信號可用以指示能力與目前模式信任等級關聯，其在一些實施方案中可對軟體有用，例如，以確保能力係由與嘗試參考其的相同本文產生。

【0096】 圖8係示意地繪示可存在於系統內的各種不同模式信任等級的圖，且指示可在此一配置中受支援的密封/解密封能力。如圖8所示，處理電路系統可經配置以在安全域及較不安全域中操作，且目前模式信任等級可取決於處理電路系統在該等安全領域的何者中執行。額外地，或替代地，處理電路系統可經配置在複數個不同狀態中執行程式碼，且在圖8的實例中，可經配置以在特權狀態或非特權狀態中操作程式碼。可將特權等級及不同安全領域視為係正交的信任等級，且處理電路系統的不同模式信任等級可與安全/較不安全域及特權/非特權狀態的各組合關聯。因此，如圖8所示，在所示實例中可有四個不同的信任等級。

【0097】 相關於先前描述的密封及解密封能力，接著，如圖8中之箭號所示，當處理電路系統在安全及特權模式中操作時，其可能能夠將其能力信任等級與操作的其他三個信任等級模式的任何者關聯的能力密封及解密封。再者，如圓形箭號所示，其亦可對其能力信任等級指示安全特權信任等級的能力執行密封及解密封操作。

【0098】 類似地，當處理電路系統在較不安全特權模式中操作時，其可能能夠相關於與較不安全非特權信任等級關聯的能力執行密封及解密封操作，且再次可能能夠將與其自身的信任等級關聯的能力密封及解密封，如由圖8中的圓形箭號所指示的。進一步地，若有需要，當處理電路系統在安全非特權模

式中操作時，可能允許其將與較不安全非特權信任等級關聯的能力密封及解密封，且再次可能能夠亦將與其自身的信任等級關聯的能力密封及解密封。最後，在較不安全非特權模式中，處理電路系統可僅能夠將與較不安全非特權信任等級關聯的能力密封及解密封。

【0099】 雖然圖8顯示四種不同的信任等級，將理解本文描述的技術不限於此一組態，且可在圖8中所示之正交方向的其中一者或二者上提供額外的信任等級。操作的特權及非特權模式可採取各種形式，但純粹作為實例，特權模式在一些實施方案中可稱為處置器模式，且非特權模式可稱為執行緒模式。處置器模式一般用於異常處理，且因此，例如，受信任例外處理常式可在處置器模式中執行。執行緒模式一般用於運行不同的執行緒，例如，不同的應用程式執行緒。

【0100】 圖9A及圖9B係繪示可在考慮使用密封能力時所採取的不同方法的流程圖。首先，根據一個實例實施方案，如圖9A所示，若在步驟400，請求嘗試使用密封能力，則在步驟405，可與目前模式信任等級無關地防止此類使用。具體而言，根據繪示於圖9A中的實施方案，若密封能力最初已解密封，系統將僅允許使用該等密封能力。因此，在此一實施方案中，相關於密封能力嘗試的所有處理操作皆將失敗。然而，應注意到仍可允許處理電路系統在儲存結構之間移動密封能力，例如，在暫存器與記憶體之間，或在不同暫存器之間。進一步地，在一個實例實施方案中，使密封能力無效化可仍係可行的，一般藉由清除先前提及之與能力關聯的標籤位元。

【0101】 圖9B係繪示可在某些情況下允許密封能力的某種使用的一替代實施方案的流程圖。因此，當在步驟410判定請求嘗試使用密封能力時，接著在步驟415判定目前模式信任等級是否大於或等於能力信任等級。若係否，在步驟420防止使用密封能力，否則程序繼續進行至步驟425，判定所關注的特定使用是否係允許在密封能力上執行的使用類型。若係否，則在步驟420，再度防止使用密封能力，否則程序繼續進行至步驟430，允許經請求操作使用密封能力執行，受可在允許使用繼續進行之前執行的任何正常檢查。

【0102】 關於先前步驟425，可將密封能力的使用限制在特定類型的操作。例如，可能係在目前模式信任等級超過密封能力的能力信任等級或與其相同時，允許處理電路系統使用密封能力執行解參考操作以產生記憶體位址。藉由避免需要在使用能力之前將其解密封，此可引起一些效能利益。

【0103】 可設想的另一種類型的處理操作係密封能力的修改，且此再度可在某些情況下受支援。具體而言，圖10係繪示可在處理修改能力之請求時執行之步驟的流程圖。如圖10所指示的，若在步驟450，接收到修改能力的請求，在步驟455，判定能力是否經密封。若係否，則程序繼續進行至步驟460，執行所需正常檢查以判定能力是否可修改。

【0104】 然而，若能力經密封，則可選地在步驟465，可判定與處理電路系統的目前操作模式關聯的信任等級是否足以允許能力的修改發生。此可係，例如，目前模式信任等級大於或等於能力信任等級時的情形。若係如此，則程序可繼續進行至先前提及的步驟460以執行正常檢查。然而，若信任等級不足，則程序可取而代之地繼續進行至步驟470，防止對能力的修改，或取而代

之地使能力無效。在省略可選步驟465的一替代實施方案中，若能力經密封，則程序可直接從步驟455繼續進行至步驟470以防止對能力的修改或使能力無效。

【0105】 在參照圖6至圖10討論的所有以上實例中，假設在目前模式信任等級已與能力信任等級比較時，可在每當目前模式信任等級大於或等於能力信任等級時允許所描述的動作。在一替代實施方案中，可將執行該等動作的能力限制在目前模式信任等級匹配能力信任等級的情況。

【0106】 當能力從記憶體載入至能力暫存器60、80的一者中時，處理電路系統可經配置以在某些情況下選擇性地修改能力信任等級，此方法的一個實例實施方案顯示在圖11中。在步驟500，判定是否請求從記憶體載入能力。在步驟505，接著判定針對載入操作識別的能力是否係密封能力。若係如此，則程序繼續進行至步驟515，能力以非修改形式儲存在經識別能力暫存器中以用於載入操作。具體而言，導因於密封能力的性質，在載入操作期間在能力信任等級上作出任何改變會係不適當的。進一步地，導因於由密封能力處理電路系統185所採用以控制密封能力的使用的先前描述機制，仍可為密封能力確保安全性，甚至在將密封能力載入至能力暫存器中時不在能力信任等級上降低。

【0107】 若在步驟505，判定能力係非密封能力，則程序繼續進行至步驟510，判定目前模式信任等級是否小於待從記憶體載入之能力的能力信任等級。若係否，則在一個實例實施方案中，程序繼續進行至步驟515，能力未修改地儲存在能力暫存器內。

【0108】 然而，根據顯示在圖11中的技術，若目前模式信任等級小於能力信任等級，則程序繼續進行至步驟520，將與能力之將儲存至能力暫存器中的複本關聯的能力信任等級降級，使得目前模式信任等級不再小於能力信任等級。藉由此一方法，可確保即使從記憶體載入的能力具有較高的關聯特權等級，載入至處理電路系統的能力暫存器中的所得能力將使其能力信任等級降級，使得當以目前模式信任等級操作時，其不可用以存取不應由處理電路系統存取的記憶體。相反地，若記憶體中的能力具有比目前模式信任等級更低的信任等級，其信任等級停留在其移動至能力暫存器中時的「現狀」。此可避免意外地提昇能力，例如，避免例外處置器意外地提昇堆疊值的情形。

【0109】 在一個實例實施方案中，在某些情形中使用能力載入程序將通用資料而非能力載入至能力暫存器中係可行的。此可在步驟500偵測到，且若實際上載入操作正用以載入通用資料，則可防止會在能力內指定能力信任等級的位元的選擇性降級，因此避免所載入的資料損壞。

【0110】 如圖11中之步驟520所指示的，可使選擇性降級能力信任等級的能力可組態，例如，藉由使其取決於儲存在控制暫存器90內的控制資訊。能力的選擇性降級亦可對某些類型的能力停用（除了已於上文提及的密封能力外），且因此，例如，在所載入的能力係不可變能力時可停用。此一能力可係有益的，例如，允許特權不可變能力從非特權操作模式內下跌而無需修改不可變能力。進一步地，雖然如上文提及之用以有條件地啟用或停用從記憶體載入之能力的選擇性降級的控制資訊可儲存在控制暫存器中，該控制資訊亦可儲存於他處，例如，作為能力本身內的欄位，或以使降級能基於，例如，MPU區域

屬性。使用此後一方法，機制可經配置使得若能力從標記為唯讀的MPU區域（例如，碼記憶體）載入，降級會發生，但若有關區域經標記為讀寫（例如，堆積或堆疊記憶體），則不會發生。在一些實施方案中，MPU中的專用控制位元可用以指示行為。

【0111】 圖12係說明能力的解密封可如何選擇性地對某些預定類型的能力禁止的流程圖。具體而言，當在步驟550接收到解密封請求時，在步驟555，判定經識別能力是否係預定類型的。若係否，則在步驟565，程序按照先前討論之圖7的其餘部分繼續進行。然而，若在步驟555，經識別能力係預定類型的，則程序繼續進行至步驟560，防止經識別能力解密封。如在討論圖7之步驟360時於先前提及的，若有需要，可輸出各種資訊以識別經識別能力的解密封尚未發生，且在此實例中，例如，可標記已嘗試將預定類型的能力解密封或確立錯誤。作為另一選項，或額外地，可清除標籤位元以使能力無效化。

【0112】 上述程序可用於其之預定類型的能力可採取各種形式，但，例如，可係由架構使用以指示特定事件或功能的一或多種類型的能力。有可識別此類保留類型能力的若干種方式。作為一特定實例，其等可具有定義無效範圍（例如，藉由使上邊界低於下邊界）的範圍邊界資訊。

【0113】 若有需要，除了先前討論的密封旗標外，能力可具備一或多個額外欄位以提供用以識別能力可用於其之特定目的的額外指示。額外地，若有需要，編碼在能力中的位址值可不直接識別記憶體位址，而係可提供允許軟體驗證其自身記錄的間接法。

【0114】 圖13繪示可使用的模擬器實施方案。雖然先前描述的實例以用於操作支援所關注技術的特定處理硬體的設備及方法實施本發明，但亦可能根據本文描述之實例提供指令執行環境，其係通過電腦程式的使用而實施。此類電腦程式常稱為模擬器，因為其等提供硬體架構之基於軟體的實施方案。模擬器電腦程式的種類包括仿真器、虛擬機、模型、及二進制轉譯器（包括動態二進制轉譯器）。一般而言，模擬器實施方案可在可選地運行主機作業系統610、支援模擬器程式605的主機處理器615上運行。在一些配置中，在硬體與所提供的指令執行環境及/或相同的主機處理器上提供的多個相異指令執行環境之間可有多層模擬。歷史上，已需要強大的處理器來提供模擬器實施方案，其以合理速度執行，但此種方法在某些情況下可係有正當理由的，諸如當因為相容性或再使用原因而需要運行另一處理器本體的碼時。例如，模擬器實施方案可提供具有不為主機處理器硬體所支援之額外功能性的指令執行環境，或提供一般與不同的硬體架構相關聯的指令執行環境。模擬的綜述提供在「Some Efficient Architecture Simulation Techniques」，Robert Bedichek, Winter 1990 USENIX Conference，頁數53至63中。

【0115】 在先前已參照特定硬體架構或特徵描述實施例的情況下，在模擬實施例中，等效功能性可藉由合適的軟體架構或特徵提供。例如，可在模擬實施方案中將特定電路系統提供為電腦程式邏輯。類似地，可在模擬實施方案中將記憶體硬體（諸如暫存器或快取記憶體）提供為軟體資料結構。再者，可將用於存取硬體設備2中之記憶體50的實體位址空間仿真為由模擬器605映射至由主機作業系統610使用的虛擬位址空間的模擬位址空間。在之前描述的實例

中提及的硬體元件的一或多者存在於主機硬體（例如，主機處理器615）上的配置中，一些模擬實施方案可（在適當處）利用主機硬體。

【0116】 模擬器程式605可儲存在電腦可讀儲存媒體（其可係非暫時性媒體）上，並提供虛擬硬體介面（指令執行環境）給目標碼600（其可包括應用程式、作業系統、及超管理器），該虛擬硬體介面與藉由模擬器程式605模型化的硬體架構的硬體介面相同。因此，目標碼600的程式指令可在指令執行環境內使用模擬器程式605執行，使得實際上不具有上文討論之設備2之硬體特徵的主機電腦615可仿真該等特徵。模擬器程式可包括處理程式邏輯620以仿真處理管線4的行為、檢查程式邏輯622以仿真圖1之硬體設備2之能力檢查電路系統33及記憶體存取檢查電路系統52的行為、及密封能力處理程式邏輯605以仿真密封能力處理電路系統185的行為。因此，本文描述之用於管理能力及其等之關聯信任等級的技術連同所描述之用於處理密封能力的技術在圖13的實例中可藉由模擬器程式605以軟體執行。

【0117】 在本申請案中，用語「經組態以...(configured to...)」係用以意指一設備的一元件具有能夠實行該經定義操作的一組態。在此上下文中，「組態(configuration)」意指硬體或軟體之互連的配置或方式。例如，該設備可具有專用硬體，其提供經定義的操作，或者一處理器或其他處理裝置可經程式化以執行該功能。「經組態以(configured to)」並不意味著設備元件需要以任何方式改變以提供所定義的操作。

【0118】 雖然本文中已參照附圖詳細描述本發明的說明性實施例，應明白本發明不限於該等精確實施例，且所屬技術領域中具有通常知識者可實行各

種變化、增加、及修改於其中，而不脫離如隨附申請專利範圍所定義的本發明的範圍與精神。例如，可用獨立項的特徵在不脫離本發明之範疇的情況下作出與附屬項之特徵的各種組合。

【符號說明】

【0119】

2:資料處理設備；設備；硬體設備；系統

4:處理管線；管線；處理器；處理電路系統

6:提取級

8:解碼級

10:發布級

12:執行級

14:寫回級

20:1級(L1)指令快取記憶體；快取記憶體

22:分支預測器

24:分支目標位址快取記憶體(BTAC)

30:執行單元；算術/邏輯單元(ALU)

32:執行單元；浮點(FP)單元

33:能力檢查電路系統

34:執行單元；載入/儲存單元

36:1級(L1)資料快取記憶體

40:暫存器；通用資料暫存器

44:二級(L2)快取記憶體

50:主記憶體；記憶體；記憶體系統

52:記憶體存取檢查電路系統

54:記憶體保護單元(MPU)

56:安全屬性單元(SAU)

60:有界指標暫存器；有界指標儲存元件；指標暫存器；能力暫存器

62:指標值；指標

64:範圍資訊

66:限制資訊；限制

68:下邊界位址；邊界

69:上邊界位址；邊界

80:程式計數器能力(PCC)暫存器；能力暫存器

82:欄位

84:範圍資訊

86:限制資訊

90:控制暫存器

100:能力暫存器；能力

102:指標；指標值

104:範圍資訊

106:限制資訊

108:標籤位元

110:記憶體位址空間

115:資料區塊

120:標籤欄位

130:讀取權限位元

132:寫入權限位元

134:執行權限位元

136:信任等級指示欄位；欄位；能力信任等級資訊

138:密封旗標欄位；密封旗標

150:處理電路系統

155:能力檢查區塊

160:信任等級產生區塊

165:路徑

167:路徑

170:記憶體存取檢查電路系統

175:存取權限資訊

180:路徑

185:密封能力處理電路系統

200:步驟

205:步驟

210:步驟

215:步驟

220:步驟

225:步驟

230:步驟

235:步驟

240:步驟

245:步驟

300:步驟

305:步驟

310:步驟

315:步驟

320:步驟

325:步驟

350:步驟

355:步驟

360:步驟

365:步驟

370:步驟

375:步驟

400:步驟

405:步驟

410:步驟

415:步驟

420:步驟

425:步驟

430:步驟

450:步驟

455:步驟

460:步驟

465:步驟

470:步驟

500:步驟

505:步驟

510:步驟

515:步驟

520:步驟

550:步驟

555:步驟

560:步驟

565:步驟

600:目標碼

605:模擬器程式；模擬器

610:主機作業系統

615:主機處理器；主機電腦

620:處理程式邏輯

622:檢查程式邏輯

625:密封能力處理程式邏輯

PR1:有界指標暫存器

【發明申請專利範圍】

【請求項1】一種設備，其包含：

處理電路系統，其用以執行在其期間產生對記憶體之存取請求的處理操作，其中該處理電路系統經配置以使用識別約束資訊的能力產生用於該等存取請求的記憶體位址；及

檢查電路系統，其用以基於由一給定能力識別的該約束資訊，且基於與一給定存取請求關聯的一信任等級，判定是否允許其記憶體位址係使用該給定能力產生的該給定存取請求；

其中：

各能力具有與其關聯的一能力信任等級，且與該給定存取請求關聯的該信任等級取決於與該處理電路系統的一目前操作模式關聯的一目前模式信任等級及該給定能力的該能力信任等級二者；

該等能力中之至少一者可設定為一密封能力；且

該設備進一步包含密封能力處理電路系統，用以在該目前模式信任等級係比一給定密封能力的該能力信任等級更低的一信任等級時防止該處理電路系統使用該給定密封能力執行至少一個處理操作。

【請求項2】如請求項1之設備，其中：

各能力具有與其關聯的一密封旗標，且該密封能力處理電路系統回應於用於一經選取能力的一密封請求而取決於該經選取能力的該能力信任等級與該目前模式信任等級的一比較判定是否設定該經選取能力的該密封旗標以將該經選取能力識別成一密封能力。

【請求項3】如請求項2之設備，其中該密封能力處理電路系統經配置以回應於該密封請求而在該經選取能力的該能力信任等級大於該目前模式信任等級時禁止設定該密封旗標。

【請求項4】如請求項3之設備，其中該密封能力處理電路系統經配置以回應於該密封請求而在該經選取能力的該能力信任等級匹配該目前模式信任等級時設定該密封旗標。

【請求項5】如前述請求項中任一項之設備，其中各能力具有與其關聯之可設定以將該能力指示為一密封能力的一密封旗標，且該密封能力處理電路系統回應於一經選取密封能力的一解密封請求而在該經選取密封能力的該能力信任等級大於該目前模式信任等級時禁止清除該經選取密封能力的該密封旗標。

【請求項6】如請求項5之設備，其中該密封能力處理電路系統經配置以回應於該解密封請求而在該經選取密封能力的該能力信任等級匹配該目前模式信任等級時清除該密封旗標。

【請求項7】如前述請求項中任一項之設備，其中該密封能力處理電路系統經配置以在該目前模式信任等級係比該給定密封能力的該能力信任等級更低的一信任等級時防止該處理電路系統使用該給定密封能力執行複數個處理操作的任一者，但允許該給定密封能力在儲存元件之間移動。

【請求項8】如前述請求項中任一項之設備，其中該密封能力處理電路系統經配置以與該目前模式信任等級無關地要求該給定密封能力在允許該能力在後續處理操作中由該處理電路系統使用之前解密封。

【請求項9】如請求項1至7中任一項之設備，其中該密封能力處理電路系統經配置以至少在該目前模式信任等級與該給定密封能力的該能力信任等級相同時允許該處理電路系統使用該給定密封能力執行一或多個處理操作而無需將該給定密封能力解密封。

【請求項10】如請求項9之設備，其中假如該目前模式信任等級與該給定密封能力的該能力信任等級相同或大於該能力信任等級，該密封能力處理電路系統經配置以允許該一或多個處理操作使用該給定密封能力執行。

【請求項11】如請求項9或請求項10之設備，其中經允許執行的該一或多個處理操作包含下列中之至少一者：

一解參考操作，其用以使用該給定密封能力產生一記憶體位址；

一能力修改操作，其用以修改由該給定密封能力識別的該資訊。

【請求項12】如前述請求項中任一項之設備，其中：

該處理電路系統經配置以在複數個狀態的一者中執行程式碼，該複數個狀態包含至少一特權狀態及一非特權狀態，且該目前模式信任等級取決於該目前程式碼在該複數個狀態的何者中執行。

【請求項13】如前述請求項中任一項之設備，其中該處理電路系統經配置以在複數個安全領域的一者中執行程式碼，該複數個安全領域包含至少一安全域及一較不安全域，且該目前模式信任等級取決於該目前程式碼在該複數個安全領域的何者中執行。

【請求項14】如請求項13及請求項14之設備，其中該目前模式信任等級取決於該目前程式碼在其中執行的該狀態及該安全領域二者。

【請求項15】如前述請求項中任一項之設備，其進一步包含：

一組能力暫存器，其用以儲存用於由該處理電路系統參考的能力；及

記憶體電路系統，其用以儲存一或多個能力；

其中：

該處理電路系統經配置以執行一載入操作以將一經選取能力從該記憶體電路系統載入至來自該組能力暫存器的一經選擇能力暫存器中；且

該處理電路系統經配置以在該載入操作期間選擇性地修改該能力信任等級，使得該經選取能力在儲存至該經選擇能力暫存器中時具有受約束不超過該目前模式信任等級或該經選取能力在儲存在該記憶體電路系統中時的該能力信任等級的一能力信任等級；

該處理電路系統進一步經配置以在該經選取能力係一密封能力時禁止在該載入操作期間修改該能力信任等級。

【請求項16】如前述請求項中任一項之設備，當依附於請求項5時，其中該密封能力處理電路系統經配置以產生指示處理該經選取密封能力的一解密封請求的一結果的結果資訊。

【請求項17】如請求項16之設備，其中該密封能力處理電路系統經配置以藉由設定可由該處理電路系統存取的一或多個狀態旗標而產生該結果資訊。

【請求項18】如前述請求項中任一項之設備，其中該密封能力處理電路系統經配置以與該目前模式信任等級無關地禁止將至少一預定類型的能力解密封。

【請求項19】如前述請求項中任一項之設備，其中將與該給定存取請求關聯的該信任等級約束成該目前模式信任等級及該能力信任等級中表示一較低信任等級的任一者。

【請求項20】如前述請求項中任一項之設備，其中該能力信任等級經編碼在該給定能力內。

【請求項21】一種處理密封能力之方法，其包含：

利用處理電路系統執行在其期間產生對記憶體之存取請求的處理操作，其中該處理電路系統使用識別約束資訊的能力產生用於該等存取請求的記憶體位址；及

基於由一給定能力識別的該約束資訊，且基於與一給定存取請求關聯的一信任等級，判定是否允許其記憶體位址係使用該給定能力產生的該給定存取請求；

其中：

各能力具有與其關聯的一能力信任等級，且與該給定存取請求關聯的該信任等級取決於與該處理電路系統的一目前操作模式關聯的一目前模式信任等級及該給定能力的該能力信任等級二者；且

該等能力中之至少一者可設定為一密封能力；

且該方法進一步包含利用密封能力處理電路系統，以在該目前模式信任等級係比一給定密封能力的該能力信任等級更低的一信任等級時防止該處理電路系統使用該給定密封能力執行至少一個處理操作。

【請求項22】一種電腦程式，其用於控制一主機資料處理設備以提供一指令執行環境，該電腦程式包含：

處理程式邏輯，其用以執行在其期間產生對記憶體之存取請求的處理操作，其中該處理程式邏輯經配置以使用識別約束資訊之能力產生用於該等存取請求的記憶體位址；及

檢查程式邏輯，其用以基於由一給定能力識別的該約束資訊，且基於與一給定存取請求關聯的一信任等級，判定是否允許其記憶體位址係使用該給定能力產生的該給定存取請求；

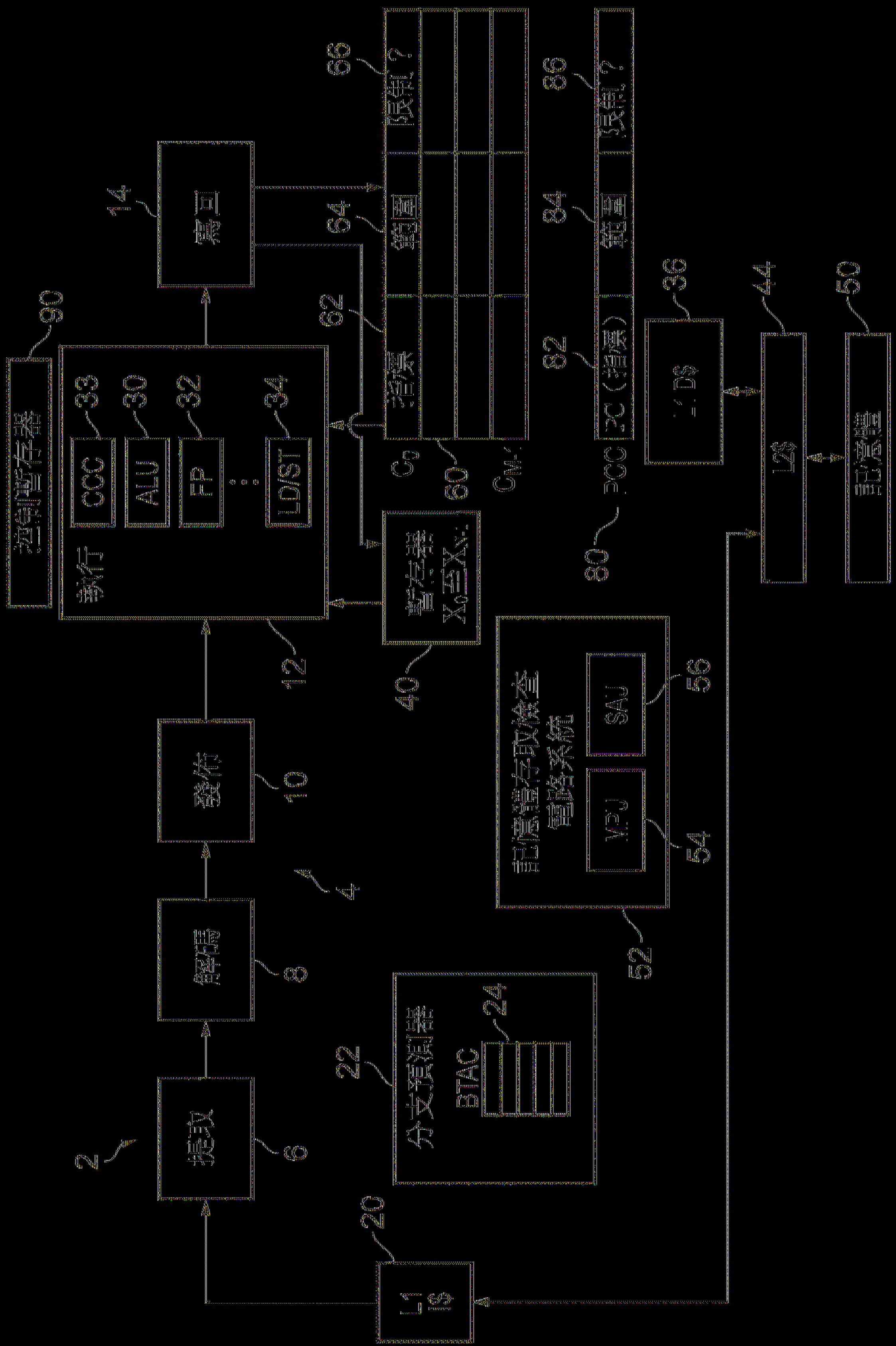
其中：

各能力具有與其關聯的一能力信任等級，且與該給定存取請求關聯的該信任等級取決於與該處理程式邏輯的一目前操作模式關聯的一目前模式信任等級及該給定能力的該能力信任等級二者；

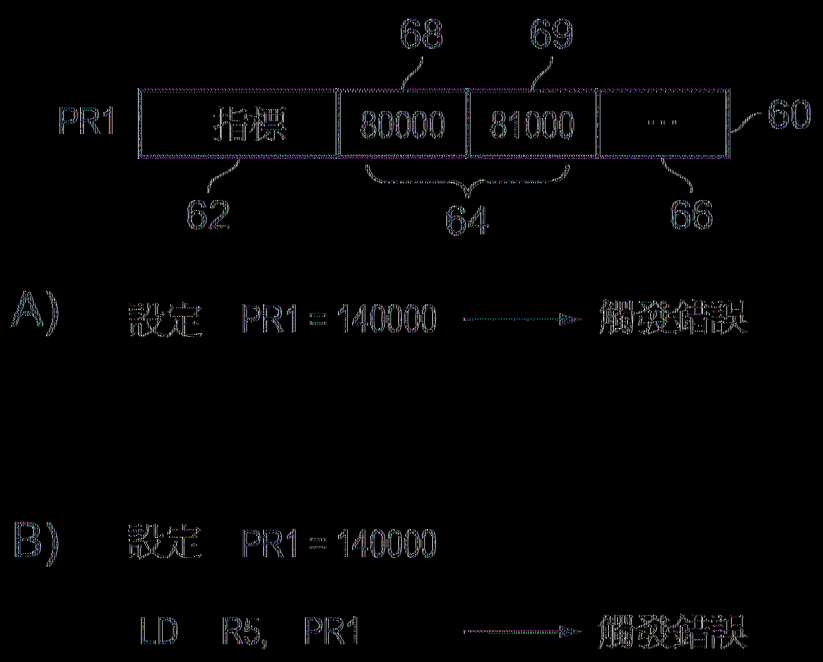
該等能力中之至少一者可設定為一密封能力；且

該設備進一步包含密封能力處理程式邏輯，以在該目前模式信任等級係比一給定密封能力的該能力信任等級更低的一信任等級時防止該處理程式邏輯使用該給定密封能力執行至少一個處理操作。

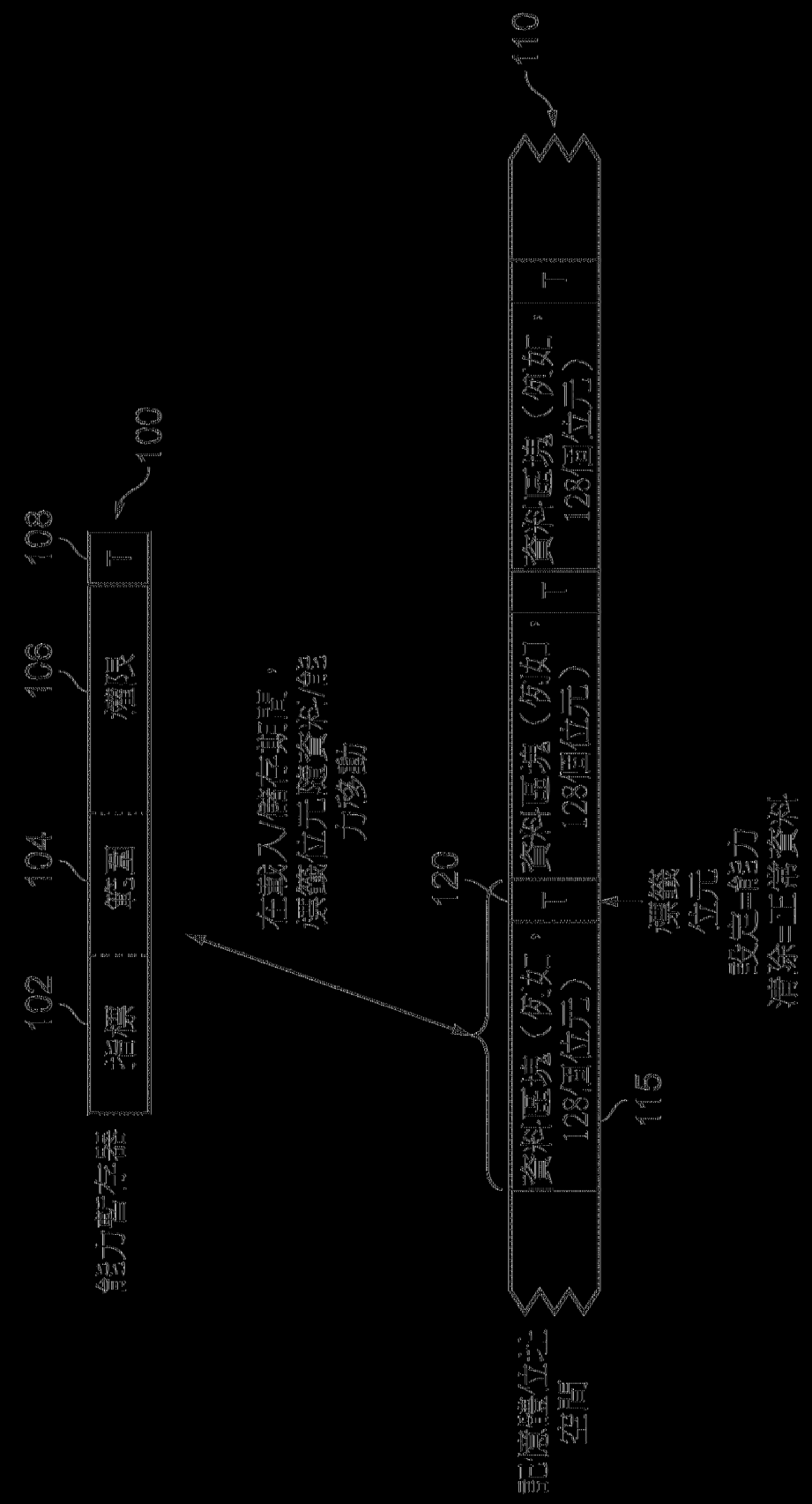
【發明圖式】


提取
解碼
發佈
執行
回寫
CCC
ALU
FP
LD/ST
控制暫存器
暫存器
X_0至X_{N-1}
指標
範圍
限制?
C_0
C_{M-1}
PCC
PC(指標)
範圍
限制?
分支預測器
BTAC
記憶體存取檢查電路系統
MPU
SAU
L1 I$
L1 D$
L2$
記憶體
2
4
6
8
10
12
14
20
22
24
30
32
33
34
36
40
44
50
52
54
56
60
62
64
66
80
82
84
86
90

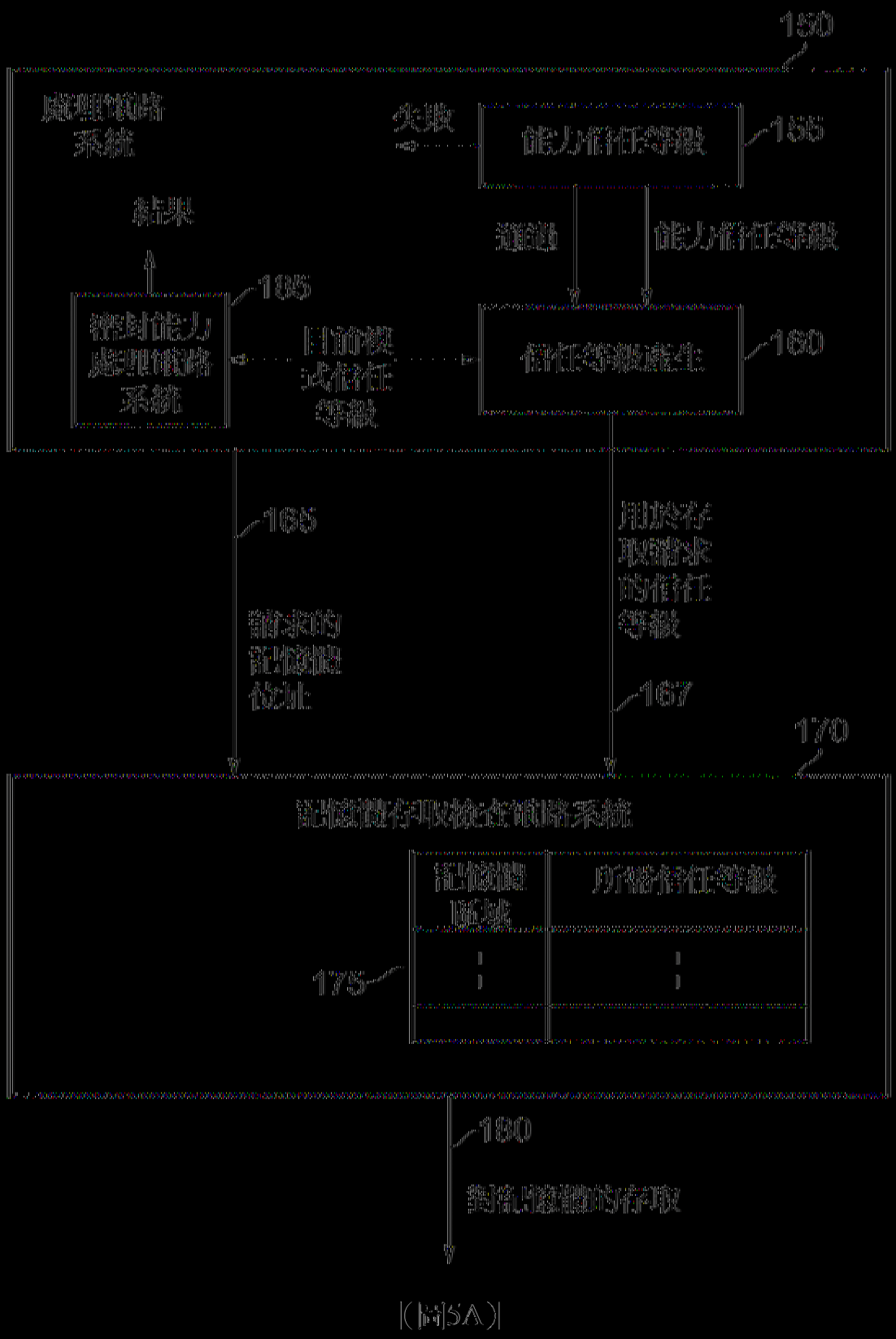
【圖1】


68
69
PR1
指標
80000
81000
…
60
62
64
66
A)
設定 PR1 = 140000
觸發錯誤
B)
設定 PR1 = 140000
LD R5, PR1
觸發錯誤

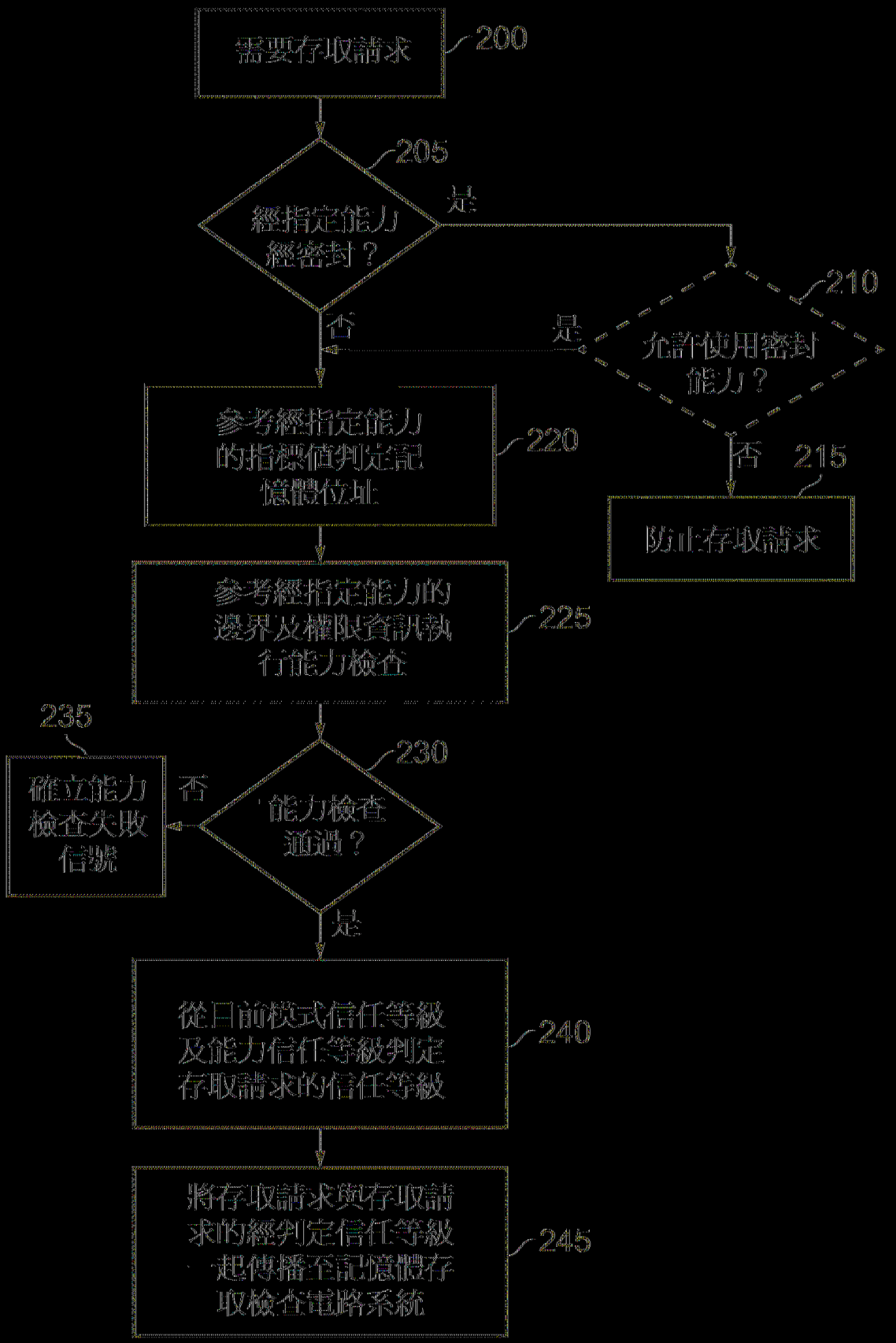
|(圖2)|


110
監視画面
128画素×128画素
監視画面
128画素×128画素
監視画面
128画素×128画素

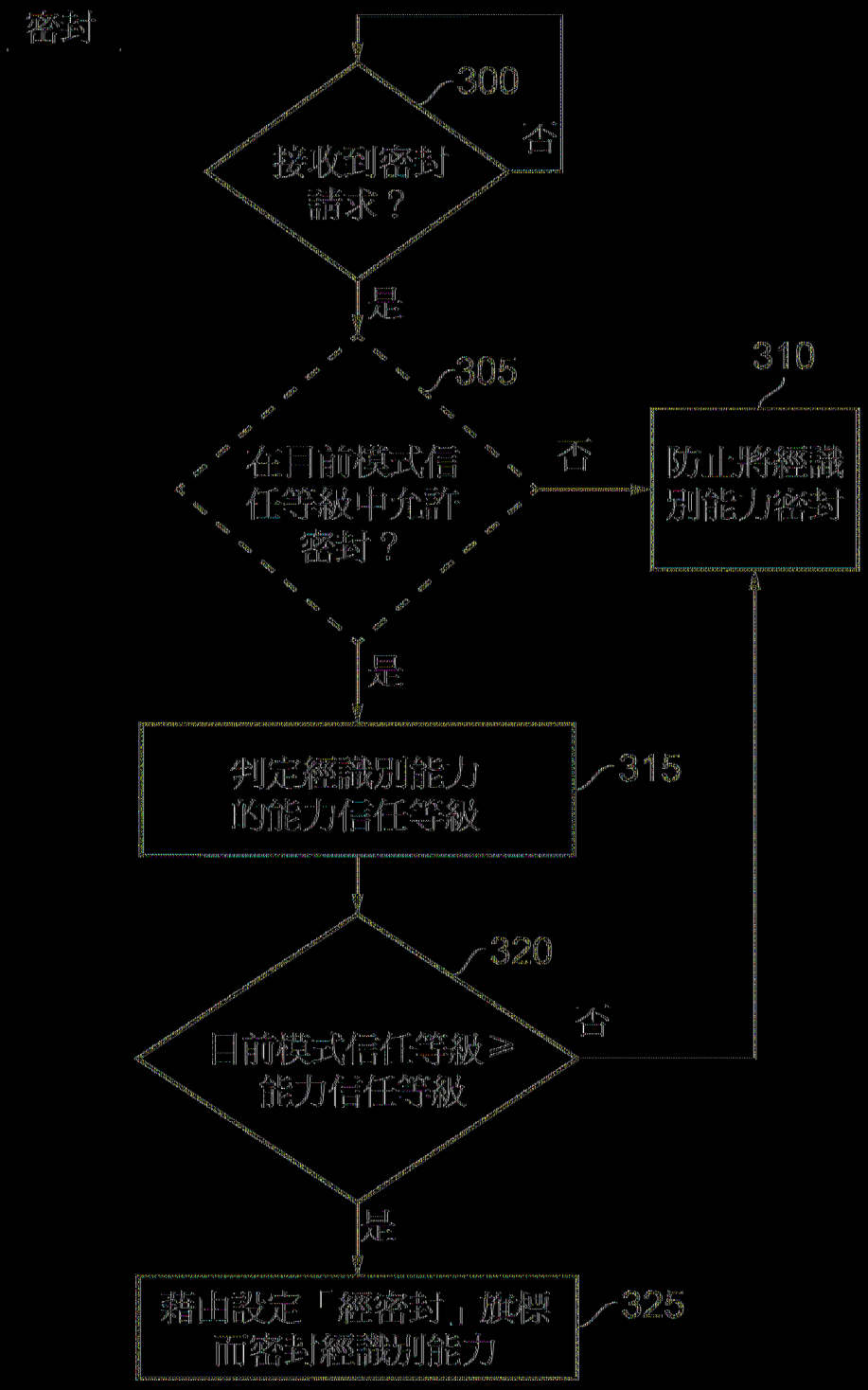
圖(圖4)


150
處理電路系統
失敗
能力信任等級
155
結果
通過
能力信任等級
185
密封能力處理電路系統
目前模式信任等級
信任等級產生
160
165
請求的記憶體位址
用於存取請求的信任等級
167
170
記憶體存取後查電路系統
記憶體區域
所需信任等級
175
180
對記憶體的存取

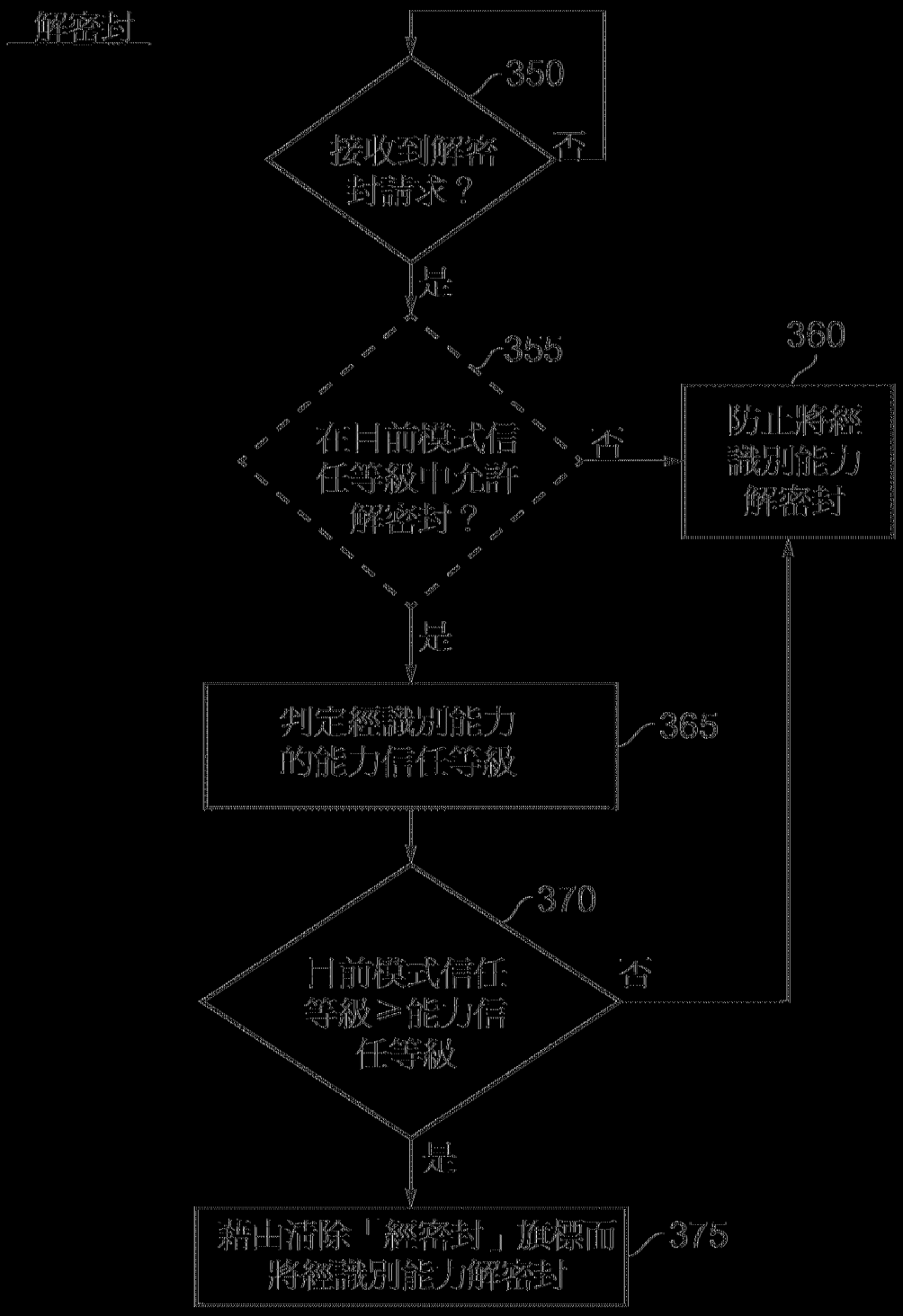
（圖5A）


需要存取請求
200
經指定能力經密封？
205
是
否
允許使用密封能力？
210
是
否
215
防止存取請求
參考經指定能力的指標值判定記憶體位址
220
參考經指定能力的邊界及權限資訊執行能力檢查
225
能力檢查通過？
230
否
確立能力檢查失敗信號
235
是
從目前模式信任等級及能力信任等級判定存取請求的信任等級
240
將存取請求與存取請求的經判定信任等級一起傳播至記憶體存取檢查電路系統
245

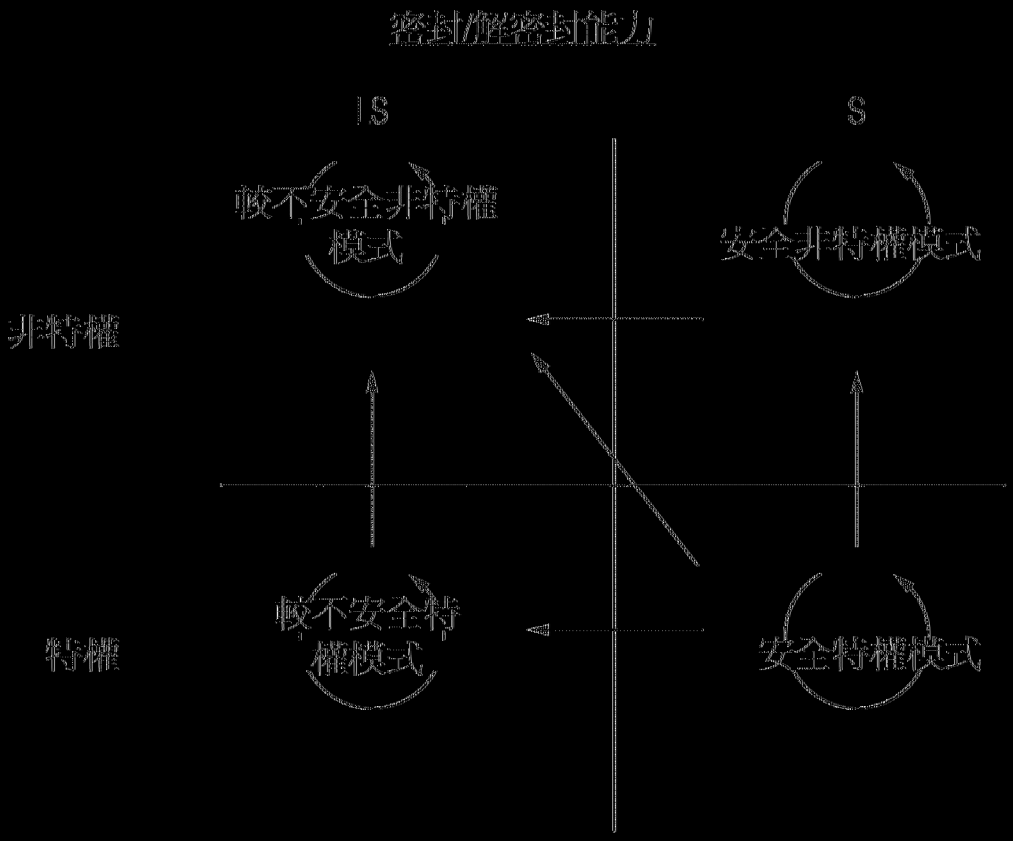
（圖5B）


密封
300
接收到密封請求？
否
是
305
在目前模式信任等級中允許密封？
否
310
防止將經識別能力密封
是
判定經識別能力的能力信任等級
315
320
目前模式信任等級≥能力信任等級
否
是
藉由設定「經密封」旗標而密封經識別能力
325

|(圖6)|


解密封
350
接收到解密封請求？
否
是
355
在目前模式信任等級中允許解密封？
否
360
防止將經識別能力解密封
是
判定經識別能力的能力信任等級
365
370
目前模式信任等級≥能力信任等級
否
是
藉由清除「經密封」旗標而將經識別能力解密封
375

[圖7]



[圖8]

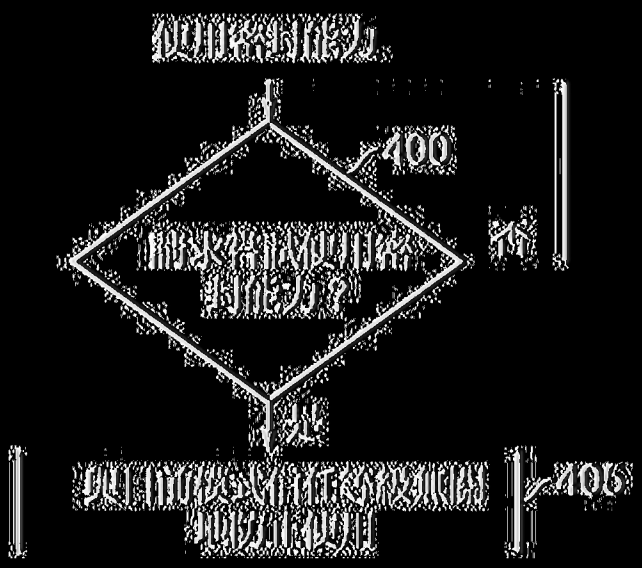
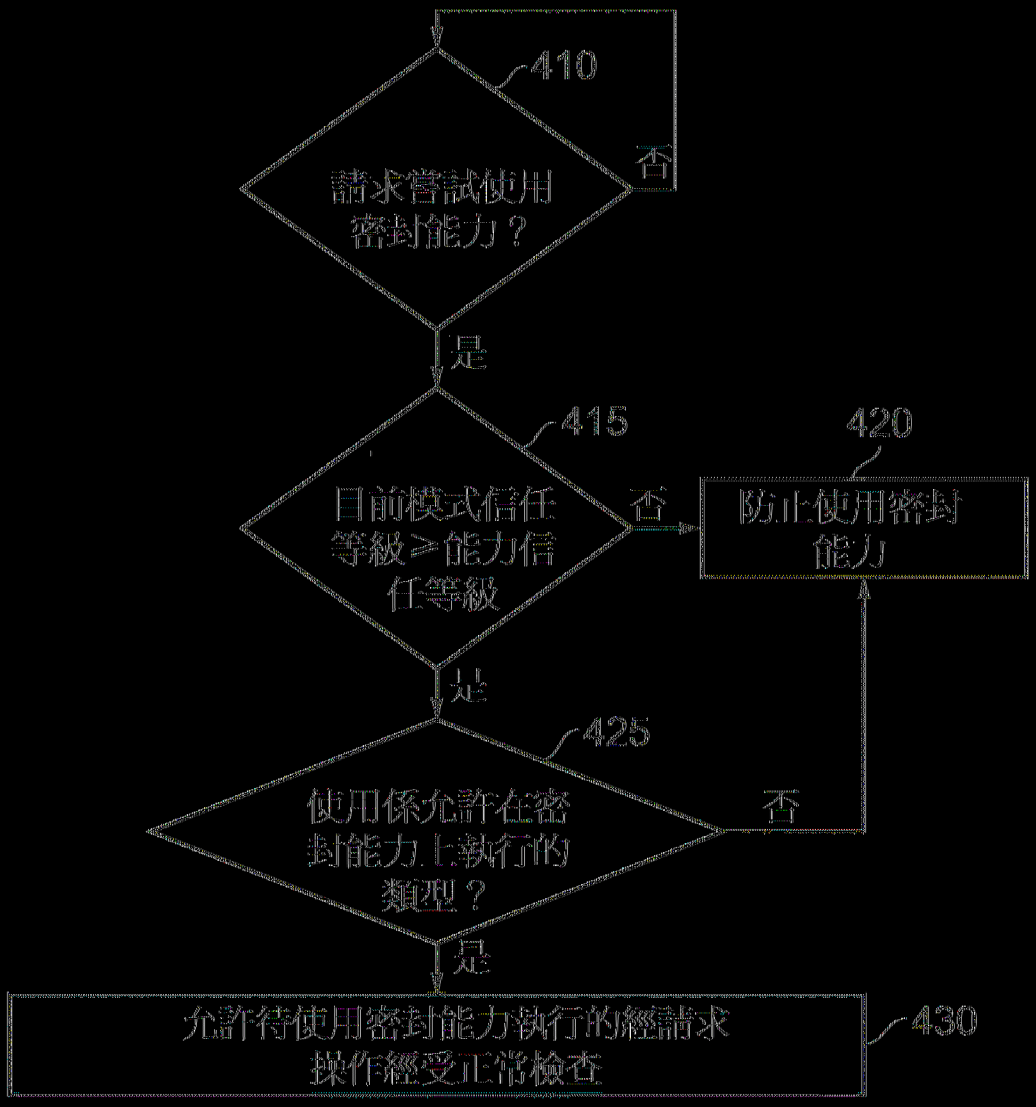
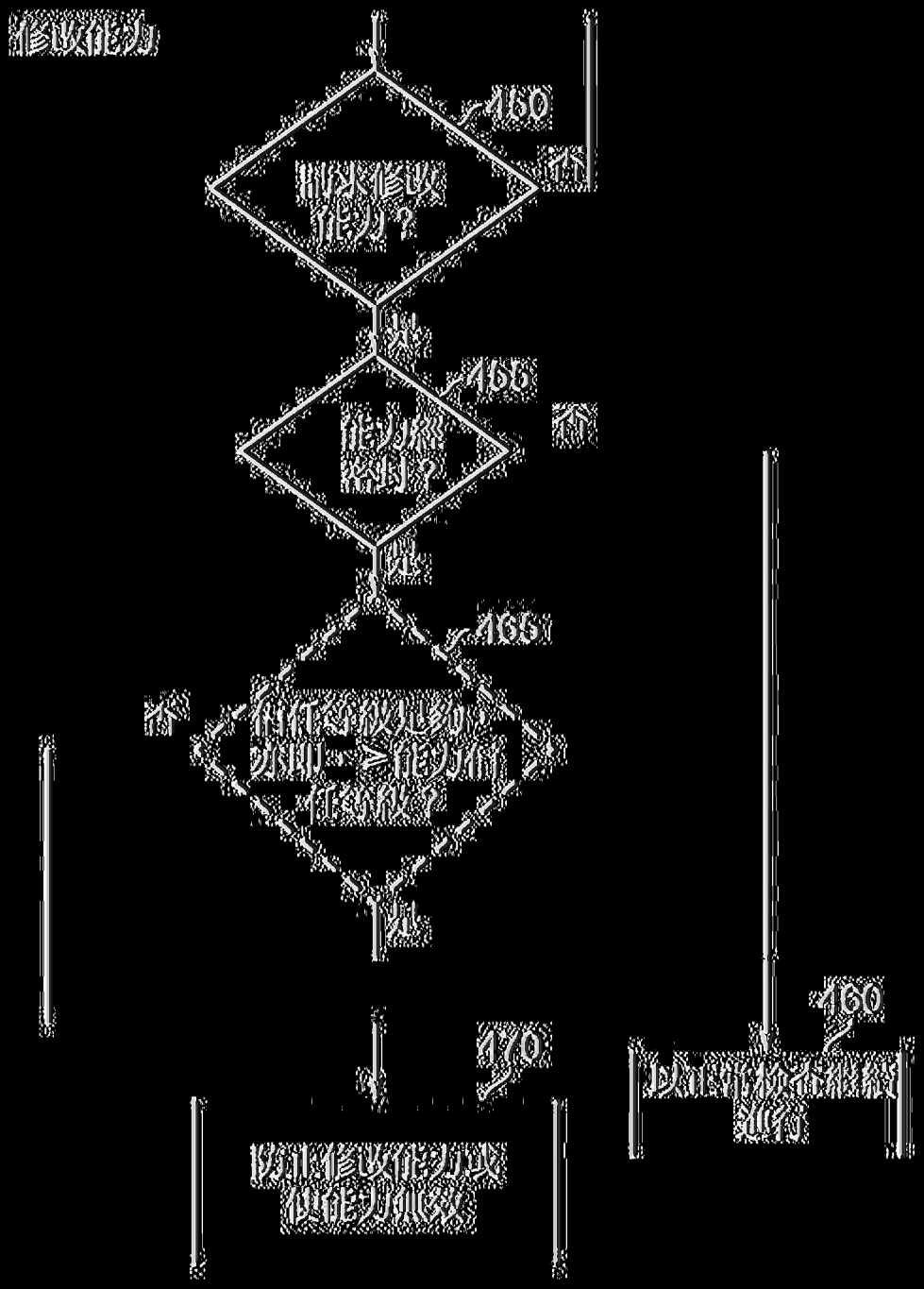


圖9A


410
請求嘗試使用密封能力？
否
是
415
目前模式信任等級≥能力信任等級
否
420
防止使用密封能力
是
425
使用係允許在密封能力上執行的類型？
否
是
允許待使用密封能力執行的經請求操作經受正常檢查
430

（圖9B）


修改能力
460
否
開始修改能力？
是
465
否
能力經濟對？
是
465
否
相任等級是夠，亦即 ⇒ 能力相任等級？
是
470
防止修改能力或使能力無效
460
以正常檢查繼續進行

【圖10】

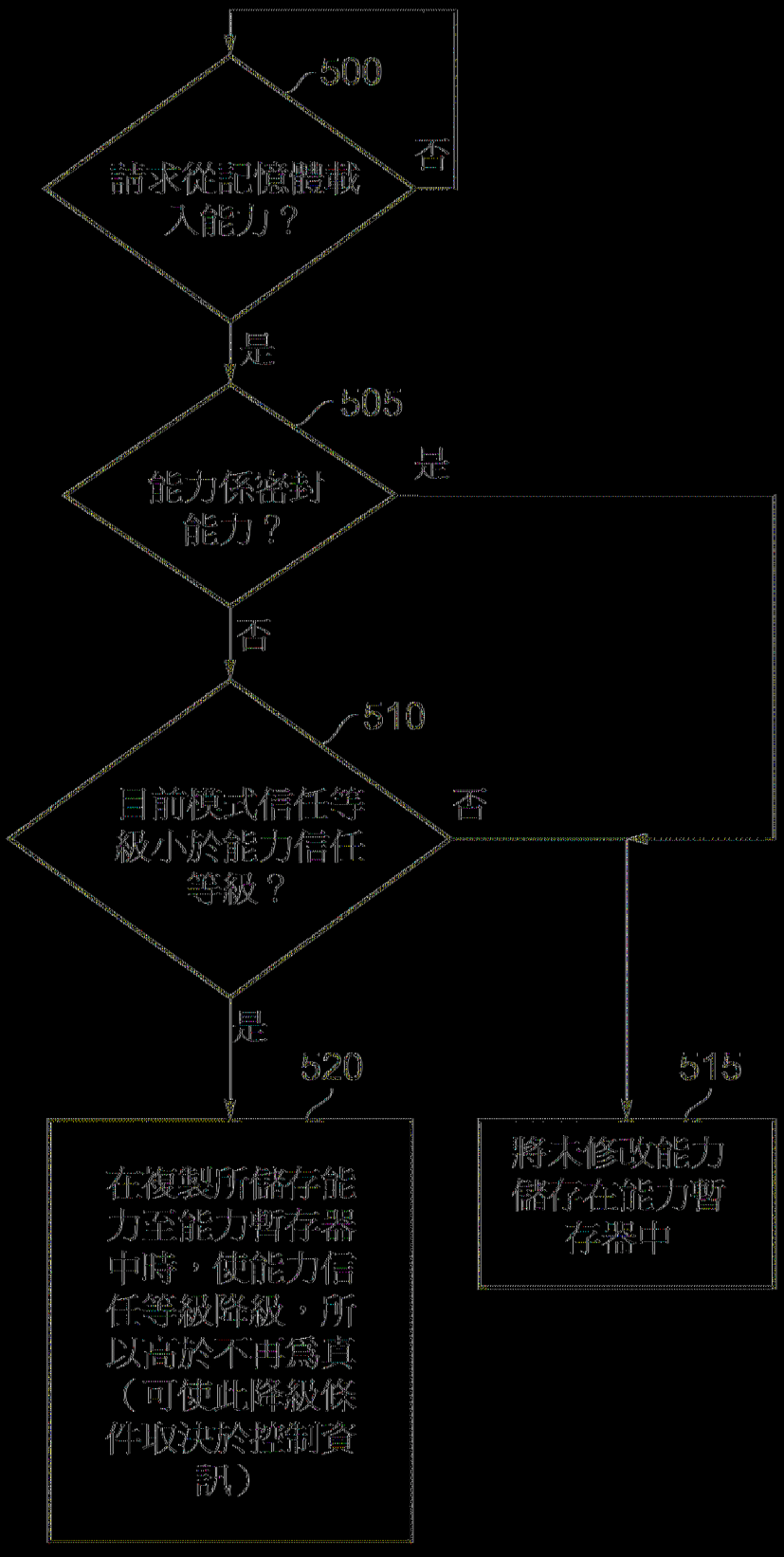
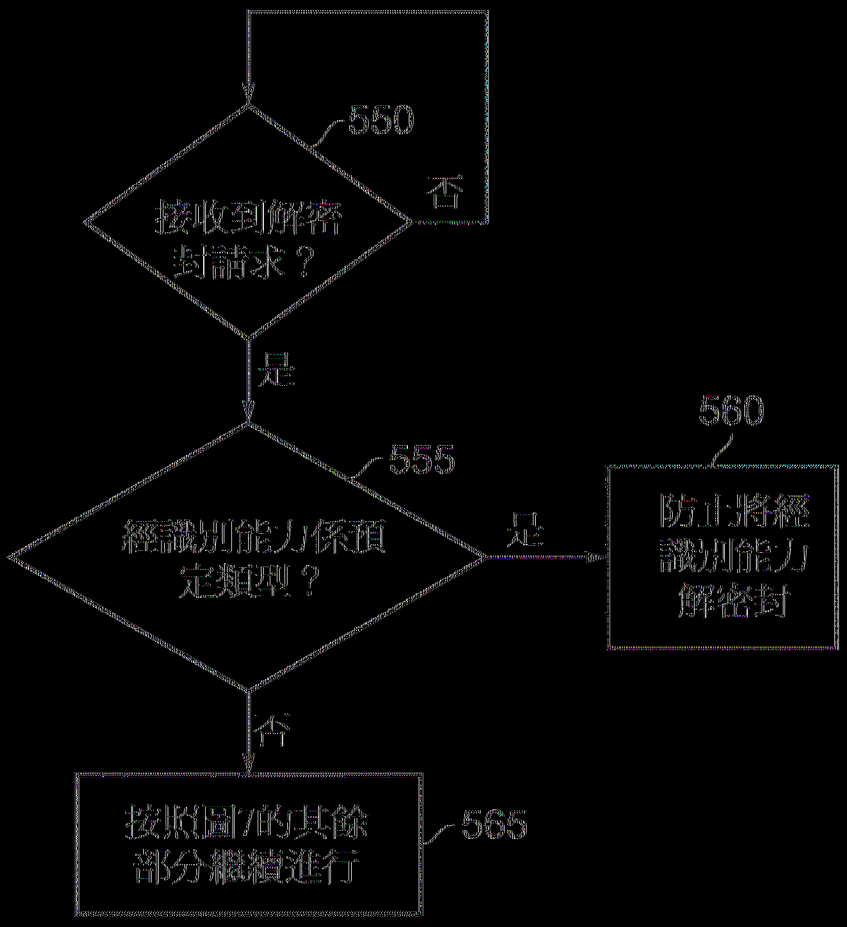
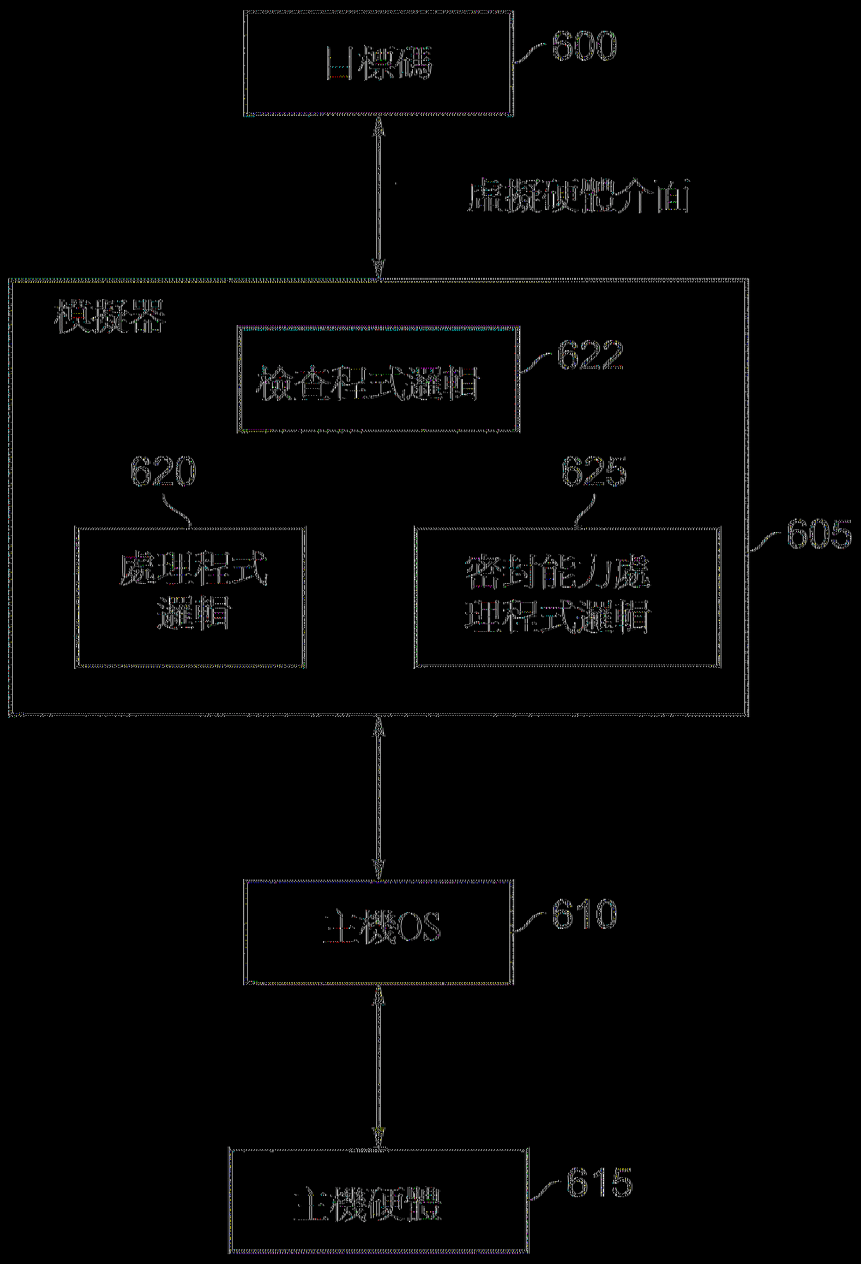

500
請求從記憶體載入能力？
否
是
505
能力係密封能力？
是
否
510
目前模式信任等級小於能力信任等級？
否
是
520
在複製所儲存能力至能力暫存器中時，使能力信任等級降級，所以高於不再爲真（可使此降級條件取決於控制資訊）
515
將未修改能力儲存在能力暫存器中

圖11


550
接收到解密封請求？
否
是
555
經識別能力係預定類型？
是
560
防止將經識別能力解密封
否
按照圖7的其餘部分繼續進行
565

[圖12]

模擬器實施方案


目標碼
600
虛擬硬體介面
模擬器
檢查程式邏輯
622
620
625
處理程式
邏輯
密封能力處
理程式邏輯
605
主機OS
610
主機硬體
615

(圖13)