202418067

(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 202418067 A

(43)公開日： 中華民國 113 (2024) 年 05 月 01 日

(21)申請案號：112136365 (22)申請日： 中華民國 112 (2023) 年 09 月 22 日

(51)Int. Cl.： *G06F9/34 (2006.01)* *G06F9/06 (2006.01)*
G06F9/44 (2018.01)

(30)優先權：2022/10/27 英國 2215944.6

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

(72)發明人：霍利 約翰麥克 HORLEY, JOHN MICHAEL (GB)；克拉斯克 西蒙約翰 CRASKE, SIMON JOHN (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：12 共 69 頁

(54)名稱

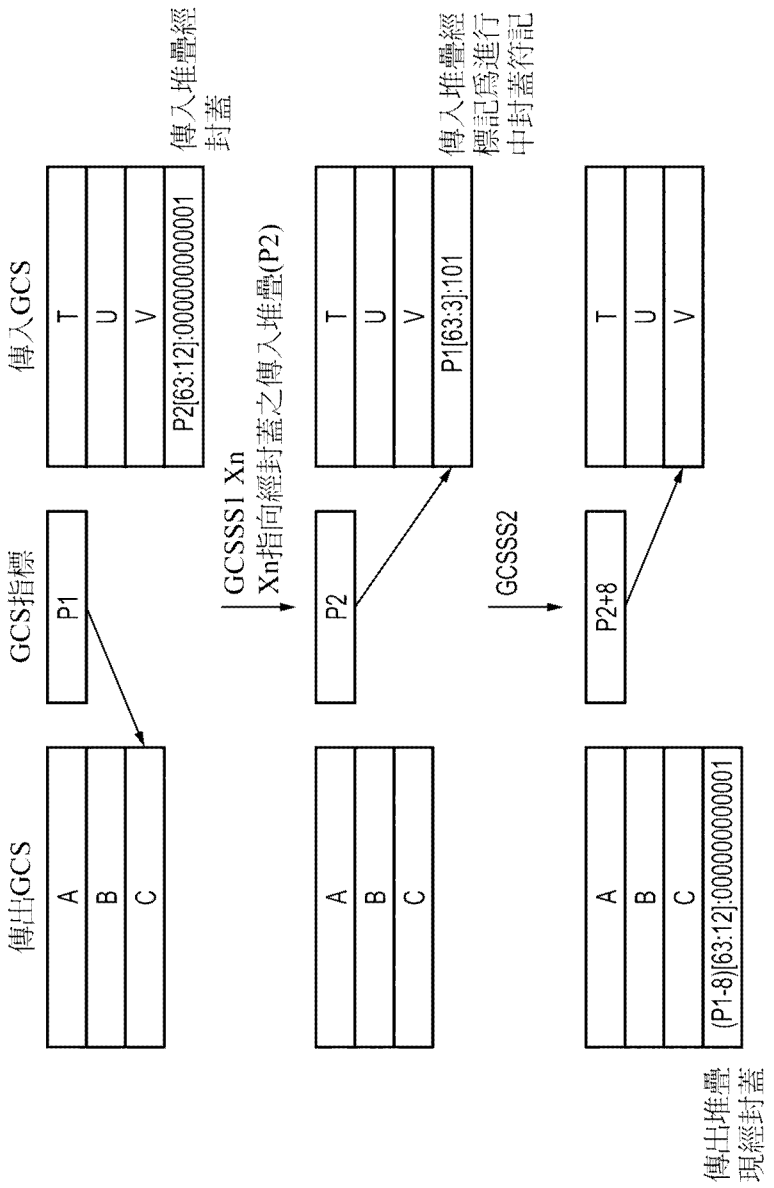
堆疊指標切換有效性檢查

(57)摘要

處理電路系統 16 執行與該堆疊指標從一傳出堆疊指標值至一傳入堆疊指標值之一切換相關聯的一堆疊指標切換有效性檢查操作。該有效性檢查操作包含驗證藉由記憶體存取電路系統 26 回應於指定基於該傳入堆疊指標值判定之一位址的一記憶體存取請求而獲得的一傳入資料值是否符合至少一堆疊封蓋值有效性條件，該至少一堆疊封蓋值有效性條件包括該傳入資料值之一預定部分對應於指示包含基於該傳入堆疊指標值判定之該位址的位址空間之一分頁的一給定分頁位址的一條件。該至少一堆疊封蓋值有效性條件係無關於除了該預定部分以外之該傳入資料值的一進一步部分是否對應於基於該傳入堆疊指標值判定之該位址的子分頁位址位元而判定。錯誤處理回應係回應於判定該傳入資料值不符合該至少一堆疊封蓋值有效性條件而觸發。

Processing circuitry 16 performs a stack pointer switch validity checking operation associated with a switch of the stack pointer from an outgoing stack pointer value to an incoming stack pointer value. The validity checking operation comprises verifying whether an incoming data value obtained by memory access circuitry 26 in response to a memory access request specifying an address determined based on the incoming stack pointer value meets at least one stack cap value validity condition, including a condition that a predetermined portion of the incoming data value corresponds to a given page address indicative of a page of address space comprising the address determined based on the incoming stack pointer value. The at least one stack cap value validity condition is determined independent of whether a further portion of the incoming data value other than the predetermined portion corresponds to sub-page address bits of the address determined based on the incoming stack pointer value. An error handling response is triggered in response to determining that the incoming data value fails to meet the at least one stack cap value validity condition.

指定代表圖：


傳入GCS
傳入堆疊經封蓋
T
U
V
P2[63:12]:000000000001
GCS指標
P1
傳出GCS
A
B
C
GCSSS1 Xn
Xn指向經封蓋之傳入堆疊(P2)
P2
傳入堆疊經標記爲進行中封蓋符記
P1[63:3]:101
GCSSS2
P2+8
(P1-8)[63:12]:000000000001
傳出堆疊現經封蓋

【圖10】

【發明摘要】

【中文發明名稱】　堆疊指標切換有效性檢查

【英文發明名稱】　STACK POINTER SWITCH VALIDITY CHECKING

【中文】

處理電路系統16執行與該堆疊指標從一傳出堆疊指標值至一傳入堆疊指標值之一切換相關聯的一堆疊指標切換有效性檢查操作。該有效性檢查操作包含驗證藉由記憶體存取電路系統26回應於指定基於該傳入堆疊指標值判定之一位址的一記憶體存取請求而獲得的一傳入資料值是否符合至少一堆疊封蓋值有效性條件，該至少一堆疊封蓋值有效性條件包括該傳入資料值之一預定部分對應於指示包含基於該傳入堆疊指標值判定之該位址的位址空間之一分頁的一給定分頁位址的一條件。該至少一堆疊封蓋值有效性條件係無關於除了該預定部分以外之該傳入資料值的一進一步部分是否對應於基於該傳入堆疊指標值判定之該位址的子分頁位址位元而判定。錯誤處理回應係回應於判定該傳入資料值不符合該至少一堆疊封蓋值有效性條件而觸發。

【英文】

Processing circuitry 16 performs a stack pointer switch validity checking operation associated with a switch of the stack pointer from an outgoing stack pointer value to an incoming stack pointer value. The validity checking operation comprises verifying whether an incoming data value obtained by memory access circuitry 26 in response to a memory access request specifying an address determined based on the incoming stack pointer value meets at least one stack cap value validity condition, including a

condition that a predetermined portion of the incoming data value corresponds to a given page address indicative of a page of address space comprising the address determined based on the incoming stack pointer value. The at least one stack cap value validity condition is determined independent of whether a further portion of the incoming data value other than the predetermined portion corresponds to sub-page address bits of the address determined based on the incoming stack pointer value. An error handling response is triggered in response to determining that the incoming data value fails to meet the at least one stack cap value validity condition.

【指定代表圖】圖10

【代表圖之符號簡單說明】

無

【特徵化學式】無

【發明說明書】

【中文發明名稱】　堆疊指標切換有效性檢查

【英文發明名稱】　STACK POINTER SWITCH VALIDITY CHECKING

【技術領域】

【0001】　本技術係關於資料處理領域。

【先前技術】

【0002】　堆疊指標可用以管理對記憶體中之堆疊資料結構的存取。堆疊資料結構係對堆疊上之項目的存取根據後進先出(last in first out, LIFO)策略受到管理的資料結構。堆疊指標提供堆疊上之項的位址可相對於其判定的位址。隨著項被推送至堆疊且從堆疊取出，堆疊指標經更新以追蹤表示堆疊之「頂部」的位置。

【發明內容】

【0003】　至少一些實例提供一種設備，其包含：記憶體存取電路系統，其用以基於一堆疊指標執行對一堆疊資料結構的一堆疊存取；及處理電路系統，其用以執行與該堆疊指標從一傳出堆疊指標值至一傳入堆疊指標值之一切換相關聯的一堆疊指標切換有效性檢查操作，該堆疊指標切換有效性檢查操作包含驗證藉由該記憶體存取電路系統回應於指定基於該傳入堆疊指標值判定之一位址的一記憶體存取請求而獲得的一傳入資料值是否符合至少一堆疊封蓋值(stack cap value)有效性條件，該至少一堆疊封蓋值有效性條件包括該傳入資料值之一預定部分對應於指示包含基於該傳入堆疊指標值判定之該位址的位址空

間之一分頁的一給定分頁位址的一條件，其中：該處理電路系統經組態以判定該傳入資料值是否符合該至少一堆疊封蓋值有效性條件，無關於除了該預定部分以外之該傳入資料值的一進一步部分是否對應於基於該傳入堆疊指標值判定之該位址的子分頁位址位元；且該處理電路系統經組態以回應於判定該傳入資料值不符合該至少一堆疊封蓋值有效性條件而觸發一錯誤處理回應。

【0004】　至少一些實例提供一種方法，其包含：執行與一堆疊指標從一傳出堆疊指標值至一傳入堆疊指標值之一切換相關聯的一堆疊指標切換有效性檢查操作，該堆疊指標切換有效性檢查操作包含驗證藉由記憶體存取電路系統回應於指定基於該傳入堆疊指標值判定之一位址的一記憶體存取請求而獲得的一傳入資料值是否符合至少一堆疊封蓋值有效性條件，該至少一堆疊封蓋值有效性條件包括該傳入資料值之一預定部分對應於指示包含基於該傳入堆疊指標值判定之該位址的位址空間之一分頁的一給定分頁位址的一條件，其中：該傳入資料值是否符合該至少一堆疊封蓋值有效性條件係無關於除了該預定部分以外之該傳入資料值的一進一步部分是否對應於基於該傳入堆疊指標值判定之該位址的子分頁位址位元而判定；且該方法包含回應於判定該傳入資料值不符合該至少一堆疊封蓋值有效性條件而觸發一錯誤處理回應。

【0005】　至少一些實例提供一種包含指令的電腦程式，當該等指令由一主機資料處理設備執行時，控制該主機資料處理設備提供用於執行目標碼的一指令執行環境，該電腦程式包含：記憶體存取程式邏輯，其用以基於一堆疊指標執行對一堆疊資料結構的一堆疊存取；及處理程式邏輯，其用以執行與該堆疊指標從一傳出堆疊指標值至一傳入堆疊指標值之一切換相關聯的一堆疊指標切換有效性檢查操作，該堆疊指標切換有效性檢查操作包含驗證藉由該記憶體

存取程式邏輯回應於指定基於該傳入堆疊指標值判定之一位址的一請求而獲得的一傳入資料值是否符合至少一堆疊封蓋值有效性條件，該至少一堆疊封蓋值有效性條件包括該傳入資料值之一預定部分對應於指示包含基於該傳入堆疊指標值判定之該位址的位址空間之一分頁的一給定分頁位址的一條件，其中：該處理程式邏輯經組態以判定該傳入資料值是否符合該至少一堆疊封蓋值有效性條件，無關於除了該預定部分以外之該傳入資料值的一進一步部分是否對應於基於該傳入堆疊指標值判定之該位址的子分頁位址位元；且該處理程式邏輯經組態以回應於判定該傳入資料值不符合該至少一堆疊封蓋值有效性條件而觸發一錯誤處理回應。

【圖式簡單說明】

【0006】 本技術的進一步態樣、特徵、及優點將由於結合附圖閱讀的以下實例描述而顯而易見，在該等附圖中：

〔圖 1〕繪示資料處理設備的實例；

〔圖 2〕繪示功能呼叫的實例；

〔圖 3〕繪示保護控制堆疊(guarded control stack, GCS)推送及取出操作的實例；

〔圖 4〕繪示 GCS 載入/儲存操作的存取權限檢查；

〔圖 5〕繪示非 GCS 載入/儲存操作的存取權限檢查；

〔圖 6〕繪示指令提取或分支操作的權限檢查；

〔圖 7〕繪示控制堆疊切換以將堆疊指標從傳出堆疊指標值切換至傳入堆疊指標值的方法；

〔圖 8〕繪示第一堆疊指標切換指令的處理；

〔圖 9〕繪示第二堆疊指標切換指令的處理；

〔圖 10〕繪示堆疊指標切換；

〔圖 11〕繪示 GCS 記錄的實例編碼；及

〔圖 12〕繪示模擬實例。

【實施方式】

【0007】 一種設備包含記憶體存取電路系統，其用以基於一堆疊指標執行對一堆疊資料結構的一堆疊存取。軟體之不同部分可與記憶體中之不同堆疊結構相關聯，因此當在軟體之該等部分之間切換時，可所欲的是將一對應堆疊指標從與傳出軟體相關聯的傳出堆疊指標值切換至與傳入軟體相關聯的傳入堆疊指標值。然而，對於一些堆疊而言，可係重要的是堆疊指標無法切換至不意欲為傳入堆疊結構的任意位置。例如，當將項推送至堆疊上及從堆疊取出項時，一些堆疊可與某些安全性措施相關聯。若堆疊指標可切換至任意軟體選擇之位址，則此可繞過該等安全性措施，因為其可導致存取尚未受該等措施保護之資料的未來堆疊存取。

【0008】 因此，可係所欲的是提供用於監管堆疊指標之切換的技術。一種方法可係將對堆疊指標的更新捕捉至更高特權的執行狀態，使得更高特權的軟體可檢查傳入堆疊指標值並判定是否可允許更新。然而，可係所欲的是支援快速軟體執行緒切換，而不需要呼叫核心或其他更高特權的軟體。此類執行緒切換可能頻繁地發生，因此在堆疊指標之每次切換時便呼叫核心的效能負擔可能被視為太高。

【0009】 在下文討論的實例中，處理電路系統支援執行與該堆疊指標從一傳出堆疊指標值至一傳入堆疊指標值之一切換相關聯的一堆疊指標切換有效性檢查操作。該堆疊指標切換有效性檢查操作包含驗證藉由該記憶體存取電路系統回應於指定基於該傳入堆疊指標值判定之一位址的一記憶體存取請求而獲得的一傳入資料值是否符合至少一堆疊封蓋值有效性條件。該至少一堆疊封蓋值有效性條件包括該傳入資料值之一預定部分對應於指示包含基於該傳入堆疊指標值判定之該位址的位址空間之一分頁的一給定分頁位址的一條件。該處理電路系統判定該傳入資料值是否符合該至少一堆疊封蓋值有效性條件，無關於除了該預定部分以外之該傳入資料值的一進一步部分是否對應於基於該傳入堆疊指標值判定之該位址的子分頁位址位元。錯誤處理回應係回應於判定該傳入資料值不符合該至少一堆疊封蓋值有效性條件而觸發。

【0010】 因此，傳入資料值係藉由記憶體存取電路系統從具有基於傳入堆疊指標值判定之記憶體位址的位置獲得。例如，若傳入堆疊指標值確實表示一先前建立的堆疊結構，則傳入資料值可從應代表堆疊之頂部的位置獲得。為了通過有效性檢查，傳入資料值需要在預定部分中指定一給定分頁位址，該給定分頁位址指示包含提供傳入資料值本身的位置之位址的位址空間之分頁。因此，軟體需要確保一非作用中堆疊在相對於稍後將用以參照堆疊之傳入堆疊指標的位置處具有指定在儲存該值之位址空間中的分頁之分頁位址的堆疊封蓋值。此提供一安全性措施以用於濾除提供傳入堆疊指標值之錯誤值（其不對應於待切換至的所意欲堆疊結構）的一些錯誤操作，因為相對不可能的是由錯誤傳入堆疊指標值表示的位置將剛好含有指定該位置本身之分頁位址的資料值。

【0011】 吾人可能認為，可藉由要求以下而進一步提升安全性：為了成為有效值，傳入資料值應指定提供該值之位置的具體位址，包括區分相同分頁中之不同位址的子分頁位址位元。此可進一步提升安全性，因為至儲存該指標本身之位置的相同位址的指標將係極罕見的，使得在將隨機其他位址指定為傳入堆疊指標值時意外地通過堆疊指標切換有效性檢查操作的可能性將係極低的。

【0012】 然而，發明人認知到，在實作上，對於安全性而言，可係足夠的是指示用以識別可有效地切換至之堆疊結構的堆疊封蓋值中之分頁位址。藉由判定至少一堆疊封蓋值有效性條件是否由傳入資料值滿足，無論傳入資料值之任何部分是否對應於從傳入堆疊指標值判定之位址的子分頁位址位元，此釋放提供用於其他目的之堆疊封蓋值的資料字組之位元。此可係特別有用的，因為對於一些使用情況而言，可係所欲的是支援可分配至堆疊上的數個不同堆疊記錄類型。若在檢查堆疊封蓋值的有效性時要求子分頁位址位元有意義，則除了該位址之若干較低位元（其等可能不需要給定任何資料/指令位址對準限制來明確地指定）以外，將需要該資料字組之大部分位元以指定堆疊封蓋值中之位址，進而剩下非常少的位元可用於編碼堆疊記錄類型。相較之下，藉由要求有效堆疊封蓋值指定儲存堆疊封蓋值之位置的分頁位址，但不要求指定子分頁位址位元，此釋放更大量位元以用於編碼堆疊記錄類型，其可極有用於支援處理器架構的未來擴增。

【0013】 該給定分頁位址可係指示包含基於該傳入堆疊指標值判定之一虛擬位址的虛擬位址空間之一分頁的一虛擬分頁位址。為了在堆疊指標之切換時為有效，藉由要求傳入資料值（藉由基於傳入堆疊指標值的記憶體存取電路

系統而獲得）提供儲存該傳入資料值的位置之虛擬分頁位址，此亦提供傳入堆疊係以在先前存取堆疊時使用之相同虛擬至實體位址轉譯映射來存取的一健全性檢查(sanity check)，其可幫助偵測基於攻擊者定義將不同虛擬位址映射至儲存堆疊之位置的實體位址上之混淆虛擬至實體位址轉譯映射的攻擊。

【0014】 該處理電路系統可支援執行與該堆疊指標從該傳出堆疊指標值至該傳入堆疊指標值之該切換相關聯的一傳出堆疊封蓋操作，以將一有效堆疊封蓋值推送至具有基於該傳出堆疊指標值選擇之一位址的一位置，該有效堆疊封蓋值在該有效堆疊封蓋值之該預定部分中指定指示包含基於該傳出堆疊指標值選擇之該位址的位址空間之一分頁的一分頁位址。傳出堆疊封蓋操作與堆疊指標切換有效性檢查操作互補，其中其在傳出堆疊上設定有效堆疊封蓋值，該有效堆疊封蓋值在該堆疊稍後在一稍後堆疊切換操作中切換回作為傳入堆疊時預期將通過該堆疊指標切換有效性檢查操作。

【0015】 傳出堆疊封蓋操作不一定取決於傳入堆疊指標在堆疊指標切換有效性檢查操作中符合至少一堆疊封蓋值有效性條件。即使傳入堆疊指標係錯誤的，導致基於傳入堆疊指標值載入之傳入資料值在堆疊指標切換有效性檢查操作的檢查中失敗，但使用有效堆疊封蓋值來封蓋傳出堆疊仍可係安全的。在如下文描述之任一情況下，在一些實施方案中，傳出堆疊封蓋操作可藉由至堆疊指標切換有效性檢查操作的不同指令觸發，因此實施用於觸發傳出堆疊封蓋操作之指令的功能的電路邏輯可獨立於任何有效性檢查而定義，且可簡單地實行傳出堆疊封蓋操作。即使回應於觸發該堆疊指標切換有效性檢查操作的指令而偵測到一錯誤，此可不必然停止執行用於觸發傳出堆疊封蓋操作之指令（回

應在堆疊指標切換有效性檢查操作中所識別之錯誤的時序可變化，且可不需要立即傳訊一錯誤，如下文進一步解釋）。

【0016】 針對該傳出堆疊封蓋操作之在該有效堆疊封蓋值中指定的該分頁位址可係指示包含基於該傳出堆疊指標值選擇之一虛擬位址的虛擬位址空間之一分頁的一虛擬分頁位址。

【0017】 上文描述之技術可用於以下任何使用情況：其中堆疊資料結構係由處理電路系統使用以維持執行緒特定資料，其中不同的軟體執行緒可分配不同堆疊資料結構，使得可係所欲的是在執行緒切換上將堆疊指標從傳出堆疊指標切換至傳入堆疊指標，以改變哪些堆疊係主動的。該技術可特別有用於堆疊上之資料係敏感的、或否則需要管控堆疊上之資料使用的某些安全性措施的使用情況，使得在堆疊指標切換時存在一風險，即，切換至不表示已經歷該等安全性措施之堆疊的記憶體中之任意位址可能產生可危害所執行之軟體碼之錯誤結果的風險。

【0018】 然而，該技術可係有用的一個具體情境係其中該堆疊指標係一保護控制堆疊(GCS)指標，該保護控制堆疊指標用於控制對一保護控制堆疊(GCS)資料結構的存取，以用於保護從一例外或功能呼叫返回的返回位址。此一GCS資料結構可用作抵抗返回導向程式化(return oriented programming, ROP)攻擊的防禦措施，該等返回導向程式化攻擊係旨在藉由改變在功能返回或例外返回時使用的返回位址（一般藉由在功能呼叫或例外的嵌套序列期間將其儲存在記憶體中時改變返回位址）導致不正確控制流程的常見攻擊形式。可在記憶體之區域中建立經保護GCS資料結構，其具有限制在GCS資料結構中寫入資料之能力的至少一防禦措施，相對於正常記憶體區域提供一些額外保護，從而使

得攻擊者可使未預期寫入至GCS資料結構的指令改變保存於GCS資料結構上的返回狀態較不可能。來自GCS資料結構的經保護返回狀態資訊可用以直接地控制例外/功能返回，或與由來自其他來源之軟體（例如，記憶體中分開的軟體管理堆疊結構）獲得的例外/功能返回資訊比較，以檢查例外/功能返回資訊在觸發對應的例外/功能返回之前是否能安全使用。然而，雖然在某些安全性措施可用以防止對GCS資料結構的錯誤更新，但若攻擊者可藉由將用以存取GCS資料結構的堆疊指標切換至指向由攻擊者控制之記憶體區域的傳入堆疊指標值而輕易地繞過該等安全性措施，使得錯誤返回狀態接著在受害者軟體後續嘗試存取GCS資料結構時返回，則該等措施可係無效的。此外，一些攻擊可基於將傳入堆疊指標切換至正確GCS資料結構，但切換至該GCS資料結構上的錯誤位置（諸如不表示堆疊之目前「頂部」的位置）可產生稍後例外/功能返回表現不正確的風險，因為其等使用意欲用於不同例外/功能返回的返回狀態。

【0019】　因此，堆疊指標切換有效性檢查操作可特別有用於在支援使用GCS資料結構的架構中使用，因為其實現傳入GCS資料結構是否能安全使用的健全性檢查，而不需要各堆疊指標切換被捕捉至較高特權層級。此外，使用分頁位址而非完整位址之堆疊封蓋值的更有效編碼係有用的，因為其釋放大量堆疊記錄編碼以用於其他目的。由於GCS資料結構可用以保護資料免於受惡意攻擊者竄改，因此提供用於額外類型之堆疊記錄的編碼空間可係有用的，以允許使用GCS資料結構保護其他類型的資訊（不僅是功能/例外返回狀態資訊）。

【0020】　可在由處理電路系統使用的指令集架構中支援數個安全性措施，以保護GCS資料結構免於竄改。該設備可具有記憶體管理電路系統，其用以基於與該目標位址相關聯的記憶體屬性資料而判定是否允許對一目標位址的

存取，該記憶體屬性資料指定包括該目標位址的一目標記憶體位址空間區域是否係用於儲存該GCS資料結構的一GCS區域，其中至該GCS區域的寫入存取受限於一專用類別的GCS存取指令。因此，GCS資料結構可分配在專用類型的記憶體區域（由記憶體管理電路系統視為不同於用於一般資料或程式碼之正常記憶體的不同類型的記憶體）。藉由限制可寫入至記憶體之此一GCS區域的指令類別，此減少攻擊者在嘗試修改保存於GCS資料結構上之返回狀態時可利用之攻擊面。

【0021】 該記憶體管理電路系統可回應於判定該目標記憶體位址空間區域係該GCS區域，而拒絕藉由除了該專用類別的GCS存取指令以外的一儲存指令所觸發之至該目標位址的一非GCS儲存操作。藉由對某些GCS存取類型的儲存指令限制寫入至GCS區域的能力，其他更通用儲存指令無法竄改GCS資料結構之內容，從而為GCS資料結構中儲存的經保護返回狀態資訊提供更大安全性保證。此減少攻擊者嘗試安裝ROP攻擊時可利用之攻擊面。

【0022】 類似地，該記憶體管理電路系統可回應於判定該目標記憶體位址空間區域不是該GCS區域，而拒絕藉由該專用類別的GCS存取指令之一者所觸發之至該目標位址的一GCS載入/儲存操作。因此，若存取係由GCS存取類型之指令觸發，則可拒絕對於未指定為GCS資料結構的記憶體區域的存取。此避免GCS存取類型的指令被錯誤使用於存取不意欲用於儲存GCS資料結構之記憶體的區域，且給出GCS讀取將係至不可能已被非GCS存取指令修改之記憶體區域的信心，以防禦抵抗ROP攻擊。堆疊指標切換有效性檢查操作之傳入資料值的載入可被視為GCS載入操作，使得若該位址由記憶體屬性資料識別為對應於除了GCS區域類型以外的記憶體區域類型，則其失敗。

【0023】 在一些實例中，當該記憶體屬性資料指定該目標記憶體位址空間區域係該GCS區域時，該記憶體管理電路系統亦可拒絕一指令提取或至該目標位址的分支。因此，儲存在GCS區域中的資料無法被視為可執行指令（儘管其可被視為指示儲存可執行指令之記憶體中的另一位置的位址指標）。鑒於GCS區域之此性質，可極有用的是設定有效堆疊封蓋值（其在執行堆疊切換操作時預期在經分配作為GCS區域類型之區域中的傳入堆疊上）以指定含有儲存堆疊封蓋值本身的位置之位址的相同分頁之分頁位址。此減少藉由在存取GCS記憶體區域中的GCS資料結構時意外地將堆疊封蓋值解釋為例外返回位址或功能返回位址所導致之不正確控制流程的風險，若攻擊者危害受害者碼中的控制流程使得在堆疊封蓋值處於堆疊之頂部時觸發功能返回或例外返回，則其可能係一風險。即使攻擊者確實導致對堆疊的此一錯誤存取，從而導致堆疊封蓋值被返回作為用於例外返回或功能返回之經保護返回位址，對應返回操作將導致識別一錯誤（直接在堆疊存取或返回操作時識別，或稍後在嘗試從由被錯誤地解譯為返回位址之堆疊封蓋值所表示的位址提取指令時識別），因為當堆疊封蓋值指向其本身的分頁且此預期係分配作為GCS區域類型的分頁時，不允許該分支或指令提取。

【0024】 指定分頁位址之傳入資料值的條件可不是傳入資料值被要求通過以滿足堆疊指標切換有效性檢查操作中之檢查的唯一條件。亦可施加其他條件。

【0025】 例如，在一些實施方案中，該至少一堆疊封蓋值有效性條件亦包含該傳入資料值之一最低有效部分具有不能夠由任何有效指令位址之最低有效部分指定的一位元模式的一條件。更具體而言，至少一堆疊封蓋值有效性條

件可包括最低有效部分具有用以表明有效堆疊封蓋值之特定位元模式的一條件，其中該位元模式不能夠由任何有效指令位址之最低有效部分指定。

【0026】 例如，此特定位元模式可具有位元值為1的至少一位元。對於一些處理器架構，指令編碼可具有一特定數目的位元，且可存在任何指令儲存在對準至在指令大小之倍數下之位址邊界的位址處的要求。例如，指令可具有32位元編碼，且因此可能需要儲存在對準至4位元組位址邊界的位址處（對於具有不同指令大小的架構而言，位址邊界可處於不同的粒度）。若嘗試執行指令提取或至未對準位址的分支，則可傳訊一錯誤。因此，藉由編碼堆疊封蓋值，使得其最低有效位元具有不能夠由任何有效指令位址之最低有效部分指定的非零位元模式（因為若其被視為一指令位址，則該模式將使該值成為一未對準指令位址），此可提供用於偵測使用堆疊封蓋值作為返回位址來執行例外返回或功能返回之錯誤嘗試的另一措施，因此改善安全性。

【0027】 因此，分配至一非作用中堆疊上的「堆疊封蓋值(stack cap value)」（預期在切換回至該堆疊時被驗證）可視為「封蓋(capping)」（或「密封(sealing)」）該堆疊，其在意義上是於該堆疊之頂部處設有堆疊封蓋值以防止將堆疊用於控制返回操作，直到封蓋已移除為止。

【0028】 傳入堆疊指標值可獨立於傳出堆疊指標值而定義，使得從傳出堆疊指標值至傳入堆疊指標值的切換可表示至完全不同堆疊結構的切換，而非僅是在將項目推送至堆疊上或從堆疊取出項目時執行之至目前堆疊指標的增量或減量。

【0029】 該處理電路系統可回應於一第一堆疊指標切換指令指定指示該傳入堆疊指標值的一運算元，而執行該堆疊指標切換有效性檢查操作。因此，

傳入堆疊指標值可定義為第一堆疊指標切換指令之任意指定的運算元（例如，藉由在藉由第一堆疊指標切換指令指定的通用暫存器中指定傳入堆疊指標值）。

【0030】 該設備可具有一堆疊指標暫存器，其用以儲存該堆疊指標。堆疊指標切換之傳出堆疊指標值可係在執行第一堆疊指標切換指令時針對堆疊指標暫存器指定的目前值。

【0031】 回應於第一堆疊指標切換指令，當堆疊指標切換有效性檢查操作成功時（亦即，基於傳入堆疊指標值獲得的傳入資料值符合至少一堆疊封蓋值有效性條件，且滿足任何其他檢查（取決於特定實施方案）），該處理電路系統可將堆疊指標暫存器從傳出堆疊指標值更新至傳入堆疊指標值。

【0032】 在一些實例中，第一堆疊指標切換指令可係在處理電路系統之最低特權執行狀態下執行之軟體（一般係使用者層級軟體）可用之使堆疊指標切換的唯一機制。在最低特權執行狀態下執行的軟體可能不具有至堆疊指標暫存器的直接寫入存取（可能的是軟體可仍能夠在更高特權的執行狀態下執行時直接寫入至堆疊指標暫存器）。藉由限制使用者層級軟體造成堆疊指標切換的能力，此改善安全性。由於該軟體必須使用第一堆疊指標切換指令以使該堆疊指標切換，因此此強制堆疊指標切換有效性檢查操作執行。例如，當目前特權層級具有比某一臨限特權層級低的特權時，由該軟體嘗試執行請求至堆疊指標暫存器之更新的系統暫存器指令可被拒絕。

【0033】 在一些實施方案中，第一堆疊指標切換指令亦可觸發上文提及之傳出堆疊封蓋操作。因此，回應於第一堆疊指標切換指令，在執行第一堆疊指標切換指令時針對堆疊指標暫存器指定的目前值被使用為傳出堆疊指標值，

且形成指定對應於傳出堆疊指標值之（虛擬）分頁位址的有效堆疊封蓋值，並將該有效堆疊封蓋值寫入至對應於傳出堆疊指標值之位址處的位置。

【0034】 然而，在實作上，在相同指令中執行堆疊指標切換有效性檢查操作及傳出堆疊封蓋操作兩者可能需要轉譯兩個不同目標位址：待基於傳入堆疊指標值載入之傳入資料值的載入位址、及待基於傳出堆疊指標值儲存之有效堆疊封蓋值的儲存位址。一些電路實施方案可能不能夠回應於相同指令而處理兩個不同位址轉譯，因此需要在一個指令中執行堆疊指標切換有效性檢查操作及傳出堆疊封蓋操作兩者（雖然是可能的）的指令集架構可對微架構電路設計者產生顯著的設計挑戰。

【0035】 因此，為了簡化電路設計實施方案，可係有用的是定義用於執行堆疊切換的兩個分開架構指令：一第一堆疊指標切換指令，其觸發該堆疊指標切換有效性檢查操作，且若該有效性檢查操作成功，則更新該堆疊指標暫存器以將該堆疊指標切換至該傳入堆疊指標值；及一第二堆疊指標切換指令，其用以執行該傳出堆疊封蓋操作。

【0036】 然而，使用二個指令方法，傳出堆疊指標值（回應於第一堆疊指標切換指令而在堆疊指標暫存器中取代）應在第一堆疊指標切換指令與第二堆疊指標切換指令之間被「記住」。從架構觀點，可非所欲的是消耗架構暫存器以保留傳出堆疊指標值，因為此可增加暫存器壓力，且若架構暫存器經分配以儲存傳出堆疊指標值以用作為第二堆疊指標切換指令的運算元，則亦可非所欲的是將傳出堆疊指標值暴露至在切換堆疊指標之後執行的軟體，這可能是一風險。

【0037】 因此，指令集架構可定義第一堆疊指標切換指令在架構上將傳出堆疊指標值寫入至傳入堆疊（暫時地），使得傳出堆疊指標值藉由將其寫入至記憶體位址空間而保留。此不排除一些微架構實施方案，其能夠使用微架構機制（諸如暫存器重新命名或儲存緩衝），以為第二堆疊指標切換指令提供對藉由第一堆疊指標切換指令在名義上寫入至記憶體之傳出堆疊指標值的更快存取，這快於第二堆疊指標切換指令存取記憶體實際上將有的情況（例如，可使用處理電路系統硬體內的緩衝，因為預期在被第一指令儲存相對不久之後第二指令會頻繁地需要傳出堆疊指標）。儘管如此，此類微架構電路機制係可選的且從架構（軟體可見）觀點，該等指令可經處理，就像第一堆疊指標切換指令將傳出堆疊指標值寫入至記憶體，且第二堆疊指標切換指令將其從記憶體讀取。

【0038】 因此，回應於第一堆疊指標切換指令，該處理電路系統可將指定傳出堆疊指標值的一進行中符記值推送至具有基於傳入堆疊指標值選擇之一位址的一位置。此暫時地使傳出堆疊指標值在架構上可見之記憶體位址空間中可存取，使得可接受覆寫堆疊指標暫存器中的傳出堆疊指標值，以將堆疊指標切換至傳入堆疊指標值，即使傳出堆疊尚未被封蓋。

【0039】 對於用以載入待在該堆疊指標切換有效性檢查操作中驗證之該傳入資料值的一載入操作、及用以將該進行中符記值推送至具有基於該傳入堆疊指標值選擇之該位址的該位置的一儲存操作，該處理電路系統可原子地執行該載入操作及該儲存操作。因此，提供一機構以防止介入至基於正執行之載入及儲存之間的傳入堆疊指標值選擇之位址的存取，或者若此類介入存取係可能的，則偵測其等並校正此原子性(atomicity)的缺乏（例如，藉由觸發管線清除

且重新執行第一堆疊指標切換指令）。可使用用以強制載入與儲存之間的原子性的任何已知原子存取機制。

【0040】 回應於一第二堆疊指標切換指令，該處理電路系統可驗證藉由該記憶體存取電路系統回應於指定基於該堆疊指標暫存器中之一目前堆疊指標判定之一位址的一記憶體存取請求而獲得的一給定資料值是否係一有效地形成的進行中符記值；及回應於驗證該給定資料值係一有效地形成的進行中符記值：觸發一有效堆疊封蓋值至具有基於由該給定資料值之一部分指定的一給定堆疊指標值判定之一位址的一位置的一寫入，一有效堆疊封蓋值在該有效堆疊封蓋值之該預定部分中指定指示包含基於該給定堆疊指標值判定之一位址的分頁空間之一分頁的一分頁位址。在一些實例中，基於給定堆疊指標值判定之位址可係從給定堆疊指標值以對應於一個堆疊項目之大小的量的一位址偏移。若第二堆疊指標切換指令在第一堆疊指標切換指令之後執行，則預期基於目前堆疊指標獲得的給定資料值（在第二堆疊指標切換指令時）應係先前藉由第一堆疊指標切換指令寫入至傳入堆疊資料結構的進行中符記值。然而，應理解，處理電路系統之硬體電路邏輯不可能知道第二堆疊指標切換指令實際上是否跟著第一堆疊指標切換指令，亦即，硬體電路邏輯只是實施「黑箱(black box)」電路邏輯，其基於其定義的運算元而實施第二堆疊指標切換指令的功能，無關於在該指令之前軟體選擇哪些其他指令執行。因此，在硬體中不存在將強制第二堆疊指標切換指令之運算元確實與先前用於第一堆疊指標切換指令之運算元對應的電路系統。

【0041】 因此，第二堆疊指標切換指令檢查基於堆疊指標暫存器中之目前堆疊指標獲得的給定資料值對應於有效地形成的進行中符記值，且若有效，

則使用由該進行中符記值提供的給定堆疊指標值（預期但不保證是先前藉由先前第一堆疊指標切換指令切換遠離之傳出堆疊結構的位址）以存取對應的堆疊結構，並將有效堆疊封蓋值推送至該結構。同樣地，形成有效堆疊封蓋值，使得其在預定部分中指定指示包含由給定堆疊指標值指示之位址的分頁空間之分頁的分頁位址。此確保當軟體稍後希望將對應堆疊切換回作為堆疊指標切換操作之傳入堆疊時，針對堆疊指標切換有效性檢查操作執行的稍後檢查將通過。

【0042】 回應於第二堆疊指標切換指令，當給定資料值經驗證為係有效地形成的進行中符記值時，該處理電路系統經組態以更新堆疊指標暫存器中之目前堆疊指標，以指示將提供給定資料值之項目從對應堆疊資料結構移除。例如，用以指示將項目移除的更新可係與將在從堆疊取出項目時執行之對目前堆疊指標的相同類型更新（例如，增量或減量，取決於堆疊在推送/取出時增長/縮減的方向為何）。此更新意謂進行中符記值將不再在對堆疊之後續取出存取時存取。不必實際地從記憶體刪除進行中符記值，因為至堆疊指標的更新意謂其將不在基於堆疊指標之後續存取時存取。若存在後續推送操作以將新項目推送至堆疊，則進行中符記值稍後可在任何情況下被覆寫。

【0043】 回應於第二堆疊指標切換指令，當給定資料值之最低有效部分具有不能夠由任何有效指令位址之最低有效部分指定且不能夠由符合至少一堆疊封蓋值有效性條件的任何值指定的位元模式時，該處理電路系統可驗證給定資料值係有效地形成的進行中符記值。同樣地，可有用的是進行中符記值具有對應於未對準指令位址的最低有效部分，使得使用進行中符記值作為返回位址的任何嘗試將導致如上文討論之未對準錯誤。此外，可係所欲的是針對有效堆疊封蓋值之最低有效部分及有效進行中符記值具有不同編碼，以避免攻擊者使

用錯誤控制流程繞過保護（例如，此允許僅執行第一/第二堆疊指標切換指令之一者而非兩者一起執行的錯誤被偵測）。

【0044】 回應於第二堆疊指標切換指令，該處理電路系統可回應於判定給定資料值不是一有效地形成的進行中符記值而觸發錯誤處理回應。

【0045】 對於當傳入資料值在堆疊指標切換有效性檢查操作之至少一堆疊封蓋值有效性條件失敗時的錯誤處理回應、及當給定資料值不係有效地形成的進行中符記時回應於第二堆疊指標切換指令的錯誤處理回應兩者而言，該錯誤處理回應可以數個方式實施。例如，錯誤處理回應可包含下列中之至少一者：傳訊一錯誤；設定一錯誤報告指示；及將該堆疊指標設定成一無效值。在一些實施方案中，錯誤處理回應可直接使處理被暫停（例如，在偵測到錯誤時，傳訊一錯誤或例外）。其他實例可使用使錯誤被通知的更間接手段，使得錯誤本身可不發生直至稍後發生。例如，藉由將堆疊指標設定成無法為有效記憶體位址的一無效值，基於無效堆疊指標而存取記憶體的一後續嘗試可能觸發一錯誤。此有時可比直接基於第一/第二堆疊指標切換指令的檢查觸發錯誤而更輕易地在硬體中實施。例如，其中較高位址位元具有除了所有為0或所有為1以外之值的位址空間的保留部分可經保留，使得其無法指定為有效位址，因此若需要錯誤處理回應，則藉由將堆疊指標設定成此保留部分中的位址，此可導致稍後的記憶體存取錯誤，使得仍可避免錯誤處理。應理解，所採取之具體錯誤處理回應可在上文描述之通用技術的不同實施方案之間變化。此外，在一些情況下，針對失敗的堆疊封蓋值有效性檢查所採取的錯誤處理回應可不同於當給定資料值不係有效地形成的進行中符記時針對第二堆疊指標切換指令所採取的錯誤處理回應。

【0046】 上文討論的技術可實施在資料處理設備內，該資料處理設備具有針對實施上文討論之記憶體存取電路系統及處理電路系統而提供的硬體電路系統。

【0047】 然而，相同技術亦可實施在電腦程式內，該電腦程式係在主機資料處理設備上執行以提供用於目標碼之執行的指令執行環境。即使主機資料處理設備本身不支援該架構，此一電腦程式可控制主機資料處理設備以模擬其將提供在實際支援根據某個指令集架構之目標碼的硬體設備上的架構環境。電腦程式可具有記憶體存取程式邏輯及處理程式邏輯，其控制主機資料處理設備以仿真上文所討論之特徵，包括針對堆疊指標切換有效性檢查操作的支援。記憶體存取程式邏輯執行基於堆疊指標執行堆疊存取。處理程式邏輯執行堆疊指標切換有效性檢查操作，其包括基於傳入堆疊指標值載入之傳入資料值之預定部分是否指定包含從傳入堆疊指標值衍生之位址的分頁之給定分頁位址（在經模擬位址空間中，而非主機資料處理設備之主機位址空間）的檢查。因此，當需要堆疊指標從傳出堆疊指標值切換至傳入堆疊指標值的目標碼在由主機資料處理設備上執行的模擬電腦程式所提供的指令執行環境中執行時，即使主機資料處理設備本身在硬體中不支援堆疊指標切換有效性檢查操作，也可達成如上文所論述之相同功能。

【0048】 例如，當針對一個指令集架構所編寫之程式碼係在支援一不同指令集架構的一主機處理器上執行時，此一模擬程式可係有用的。再者，由於軟體在模擬執行環境上的執行可使軟體測試得以與支援新架構之硬體裝置的進行中開發平行，模擬可允許針對一較新版本的指令集架構的軟體開發在支援該

新架構版本的處理硬體就緒之前開始。模擬程式可儲存在儲存媒體上，該儲存媒體可係非暫時性儲存媒體。

【0049】 圖1示意地繪示資料處理設備2的一實例。資料處理設備具有包括若干個管線級的處理管線4。在此實例中，管線級包括用於從指令快取記憶體8提取指令的提取級6；用於解碼提取程式指令之解碼級10，以產生待由管線的其餘級處理的微操作(micro-operation)（經解碼指令）；用於檢查微操作所需的運算元在暫存器檔案14中是否可用，並發布用於將給定微操作的所需運算元執行一次的微操作係可用的發布級12；用於執行對應於藉由處理讀自暫存器檔案14之運算元以產生結果值之微操作的資料處理操作的執行級16；及用於將處理的結果寫回至暫存器檔案14的寫回級18。應瞭解此僅係可能的管線架構的一個實例，且其他系統可具有額外級或不同的級組態。例如，在亂序處理器中，可包括用於將由程式指令或微操作指定的架構暫存器映射至識別暫存器檔案14中之實體暫存器之實體暫存器說明符的暫存器重命名級。在一些實例中，在由解碼級10解碼的程式指令與由執行級所處理之對應微操作之間可有一對一關係。在程式指令與微操作之間亦係可能有一對多或多對一關係，使得，例如，單一程式指令可分成二或更多個微操作，或者二或更多個程式指令可融合以作為單一微操作來處理。

【0050】 執行級16（處理電路系統之實例）包括若干個處理單元，以用於執行不同類別的處理操作。例如，執行單元可包括用於對讀自暫存器14的純量運算元進行算術或邏輯運算的純量算術/邏輯單元(arithmetic/logic unit, ALU) 20；用於對浮點值進行運算的浮點單元22；用於評估分支操作之結果及調整該程式計數器的分支單元24，該程式化計數器據此表示目前的執行點；及用於執

行載入/儲存操作以存取記憶體系統8、30、32、34中之資料的載入/儲存單元26。載入/儲存單元係記憶體存取電路系統的實例。提供一記憶體管理單元(memory management unit, MMU) 28，其係記憶體管理電路系統之實例，以用於執行由載入/儲存單元26基於資料存取指令之運算元所指定的虛擬位址與識別記憶體系統中資料之儲存位置的實體位址之間的位址轉譯。MMU具有一轉譯後備緩衝區(translation lookaside buffer, TLB) 29，其用於從儲存在記憶體系統中的分頁表快取位址轉譯資料，其中分頁表的分頁表項目定義位址轉譯映射及存取權限，其（例如）管控是否允許管線上執行的給定程序從給定記憶體區域讀取或寫入資料或執行指令。當分頁表結構被遍歷以定位對應於所需位址的分頁表項目時，MMU 28可具有在分頁表走訪期間請求記憶體存取的電路系統。記憶體管理單元係記憶體管理電路系統的實例。

【0051】　在此實例中，記憶體系統包括一級資料快取記憶體30、一級指令快取記憶體8、共用二級快取記憶體32、及主系統記憶體34。將理解此僅係可能的記憶體階層的一個實例，並可提供快取記憶體的其他配置。顯示在執行級16中的處理單元20至26的具體類型僅係一個實例，且其他實施方案可具有不同組的處理單元或可包括相同類型的處理單元的多個實例，使得可平行地處理多個相同類型的微操作。應理解圖1僅係一可能的處理器管線實施方案的一些組件的簡化表示，且處理器可包括為了簡潔起見而未繪示的許多其他元件。雖然圖1顯示具有對記憶體34存取的單一處理器核心，該設備2亦可具有一或多個另外的處理器核心，其共享對記憶體34的存取，其中各核心具有各別快取記憶體8、30、32。

【0052】 圖2繪示呼叫功能（為了易於參見，標示為fn1）及自功能返回的實例。功能（亦稱為程序）係可自程式之另一部分呼叫的指令序列，且當完成時其將處理返回至該功能被呼叫之程式流程之部分。相同功能可自程式中之多個不同位置被呼叫，且因此在呼叫功能時儲存功能返回位址，使得功能返回可區分程式流程應返回至哪個位址。

【0053】 例如，如圖2所示，具有連結指令BLR的分支可在功能將被呼叫的該點（由位址#add1表示）處執行，以使程式流程分支至使用具有連結指令的分支的運算元所指定之分支目標位址#add2處的指令。具有連結指令之分支亦導致處理電路系統設定連結暫存器（用於追蹤功能返回位址之指定暫存器）至在具有連結指令之分支之後的下一指令的位址（在此實例中，功能返回位址係#add1+4）。在已採取分支之後，在功能碼中執行數個指令（例如，LD、MUL、ADD等），且當功能完成時，執行返回分支指令RET，其使分支至儲存在連結暫存器中的返回位址指示的指令。

【0054】 若無其他功能自fn1內被呼叫，且在到達fn1之結束處的返回分支之前無例外發生，則在連結暫存器中的位址仍應相同如fn1被呼叫時所設定的一般。

【0055】 然而，通常，由背景程式碼所呼叫的第一功能fn1本身可以嵌套方式呼叫另一功能（就是說fn2），且在此情況中，對fn2之功能呼叫將覆寫儲存在連結暫存器中的返回位址，且因此在呼叫另一功能之前，第一功能fn1的功能程式碼應包括一指令，以將來自連結暫存器之返回位址儲存至記憶體中的資料結構（例如，堆疊結構，以後進先出(last-in-first-out, LIFO)方式操作），且在自fn2返回之後，fn1之功能程式碼應將返回位址恢復至執行返回分

支之前的連結暫存器。用於儲存及恢復功能返回狀態（諸如返回位址）之職責將通常在於軟體（可不存在用於儲存返回位址之架構上強制硬體機構）。

【0056】 然而，當功能返回位址儲存在記憶體中時，可能易於受到攻擊者修改該資料之攻擊，例如使用在另一處理器核心上執行的另一執行緒，或藉由中斷該呼叫功能且同時執行其他程式碼，其覆寫儲存在記憶體中的該返回位址。替代地，該攻擊者可執行一些指令，其目標在於修改將該返回位址自記憶體恢復至暫存器之該指令之位址運算元，使得從記憶體載入的該資料不同於在呼叫嵌套功能之前原本儲存至記憶體的返回位址。若攻擊者可導致返回分支以分支至程式流程中並非功能呼叫分支之後的指令之點，則攻擊者可能夠導致軟體不正確動作，且可能夠繞過某些安全保護或導致執行非所欲操作。

【0057】 功能呼叫係操作的一實例，其產生返回狀態資訊，返回狀態資訊提供關於處理電路系統稍後將被恢復至的狀態的資訊。返回狀態資訊可被擷取之另一情境可係採取例外時，其中提供在硬體中的例外處理電路系統，或軟體例外處理器可擷取例外返回狀態資訊，諸如指示在從處理一例外返回之後將執行之指令的位址的例外返回位址，及/或指示在從例外返回之後處理器將執行的模式或執行狀態之儲存的處理器狀態資訊。例如，儲存的處理器狀態資訊可指示採取例外的例外層級，以及關於採取例外時處理器的操作狀態的其他資訊。如同功能呼叫，例外可被嵌套，且因此當採取另一例外時，針對一例外擷取的例外返回狀態可儲存至記憶體（以硬體自動地，或藉由軟體例外處理器），且因此當其儲存在儲存記憶體中時可能容易受攻擊者竄改。這些類型的攻擊可稱為返回導向程式化(ROP)攻擊。可能期望提供針對此類攻擊的架構反制措施。

【0058】 圖3繪示用於使用在記憶體中稱為「保護控制堆疊(guarded control stack, GCS)」之經保護資料結構40來保護免於ROP攻擊的方法。在記憶體位址空間內之GCS資料結構的位置可藉由軟體選擇，但硬體提供經設計以保護GCS資料結構免於受惡意攻擊者竄改之架構特徵。

【0059】 如圖1所示，暫存器14可包括控制暫存器，其包括用於儲存一堆疊指標的一或多個經保護控制堆疊指標(GCSPR)暫存器36，該堆疊指標指示GCS資料結構上的位址。在一些實例中，GCS指標暫存器可係堆積的暫存器組，分別提供用於至少兩個執行狀態（例如，例外層級），以實現在不同執行狀態下操作的軟體參照記憶體內之不同GCS結構，而不需要在執行狀態之各轉變之後重新程式化共用的堆疊指標暫存器。其他實例可使用單一GCS指標暫存器，且軟體可在執行狀態之間的轉變時更新儲存在GCS指標暫存器中的堆疊指標。

【0060】 如圖3所示，GCS資料結構40儲存在由用於控制位址轉譯及存取權限檢查的記憶體管理單元(MMU) 28所使用之分頁表的相關聯分頁表項目直接或間接指定的記憶體屬性所指定為記憶體之GCS區域的記憶體區域中。GCS區域屬性可直接在包含GCS資料結構之至少部分的記憶體區域之對應分頁表項目之編碼內指定，或可間接參照在由該分頁表項目所參照之暫存器內。

【0061】 當記憶體區域被識別為GCS區域時，則當執行GCS存取指令的一特定子集時，至該區域的寫入存取係限於在由處理電路系統16觸發的寫入請求。由軟體使用用於一般儲存操作而不意欲存取GCS結構的通用儲存指令並不視為GCS存取指令之限制子集中之一者。MMU 28仍可允許使用通用載入指令讀取GCS結構，該通用載入指令導致發布並非GCS記憶體存取請求的讀取請求。當記憶體存取請求請求對GCS區域之存取時，該請求係寫入請求，且該請

求不是由GCS存取指令之限制子集的一者觸發的GCS記憶體存取請求，則該記憶體存取請求被拒絕且傳訊錯誤。GCS存取指令的子集可包括至少一GCS推送指令，其導致返回狀態資訊（諸如來自連結暫存器的功能返回位址，或例外返回位址或採取例外時被擷取之經儲存的處理器狀態）被推送至使用GCS指標暫存器58中指示的堆疊指標所判定的GCS結構上的位置。GCS推送指令亦導致堆疊指標以取決於推送至GCS之堆疊訊框的大小的量前行（例如，若GCS經管理為升序堆疊，則以堆疊訊框之大小來增量堆疊指標；或若GCS經管理為遞減堆疊，則以堆疊訊框之大小來減量堆疊指標）。GCS存取指令亦可包括至少一種形式之GCS取出指令，其自GCS結構取出經保護返回資訊。以及返回從堆疊取出的返回指令，GCS取出指令亦導致堆疊指標在堆疊指標針對GCS推送指令調整之方向的相對方向上調整（例如，若GCS經管理為升序堆疊，則以堆疊訊框之大小來減量堆疊指標；或若GCS經管理為遞減堆疊，則以堆疊訊框之大小來增量堆疊指標）。如下文所述，GCS存取指令亦可包括GCS堆疊指標切換指令GCSSS1、GCSSS2，其等可允許將特殊用途值寫入至GCS記憶體區域中之堆疊上，以用於保護該堆疊免於GCSPR 36中之堆疊指標不適當切換之目的。

【0062】 GCS存取指令可不被允許存取未由分頁表屬性指定為GCS區域類型之記憶體區域。因此，當由該存取之目標記憶體區域未標記為GCS區域類型時，若嘗試執行GCS存取（包括針對GCS堆疊指標切換指令GCSSS1、GCSSS2的記憶體存取），則可傳訊錯誤。藉由禁止使用GCS存取指令存取非GCS區域，此不鼓勵程式設計者使用GCS存取指令，除非真的意欲是GCS存取，以減少可用於攻擊者的攻擊面。此外，此給出由GCS取出指令存取或由

GCS堆疊指標切換指令GCSSS1、GCSSS2中之一者驗證的資料不能夠由非GCS指令修改的信心。

【0063】 GCS結構與由軟體使用的任何資料結構分開，以將儲存的返回狀態資訊維持在記憶體中，以處理功能呼叫或例外的嵌套。因此，當功能呼叫或例外嵌套時，GCS結構不意欲消除軟體本身追蹤返回狀態資訊的儲存及恢復之需求（返回狀態的軟體觸發儲存可以如在不支援上文所討論的GCS保護之架構措施的處理器上相同的方式繼續）。替代地，GCS結構提供經保護記憶體的區域，其被保護免於危害的程式碼的竄改，其可用以提供用於驗證意欲由軟體使用以從功能呼叫或例外的處理返回之返回狀態資訊的資訊。

【0064】 在一些實施方案中，使經保護返回狀態資訊從GCS結構取出的GCS取出指令亦可導致處理電路系統16比較取出的返回狀態與儲存在暫存器中的目前返回狀態資訊（例如，用於功能返回的連結暫存器，或例外返回位址暫存器及/或用於例外返回之經儲存的處理器狀態暫存器），且若從GCS結構40取出的返回狀態資訊與軟體意欲用於功能/異常返回的預期返回狀態資訊之間存在失配，則傳訊錯誤。因此，軟體可藉由包括功能呼叫/返回或例外進入/返回時執行的程式碼內之GCS推送及GCS取出指令之實例而受保護免於竄改。

【0065】 其他實施方案可界定用於驗證意欲的返回狀態資訊是否有效的單獨指令，不同於從GCS結構40取出返回狀態資訊的指令。

【0066】 替代地，GCS取出指令可直接將來自GCS的經保護返回狀態取出至用以指定例外返回或功能返回的返回狀態之一或多個暫存器（或可與例外/功能返回指令組合，以取出經保護返回狀態並且使用該狀態用於控制例外/功能返回），在此情況中，不必實行驗證是否軟體提供的意欲的返回狀態資訊係

有效，因為在此一實施方案中，GCS保護的返回狀態係直接用以控制例外/功能返回。例如，對於功能返回位址的GCS保護，可將功能返回位址直接取出至連結暫存器，取代軟體可基於其自己的經管理堆疊結構而置放在其中的任何軟體管理之功能返回位址。

【0067】　此外，亦可支援存取指令之其他類型之GCS。當啟用GCS模式時（控制暫存器中的控制狀態可控制是否GCS模式啟用），一些指令（其在停用GCS的使用之模式中具有其他功能）在執行時，可導致處理電路系統16執行額外功能（諸如額外的GCS模式特定安全性檢查）。

【0068】　一般而言，藉由提供用於定義用於GCS結構40之GCS記憶體區域類型的架構支援，且將至GCS區域類型的寫入存取限制至GCS存取指令之有限子集（其可能不被允許存取除了GCS區域類型以外的記憶體區域），此減少攻擊者可用於嘗試竄改儲存在GCS結構40上的經保護返回狀態資訊之攻擊面。

【0069】　圖4係繪示GCS載入/儲存操作之存取權限檢查的流程圖。GCS載入/儲存操作係由GCS存取指令之類別之一者觸發的載入/儲存操作（例如，GCS存取指令包括GCS推送及取出指令，及GCS堆疊指標切換指令GCSSS1、GCSSS2）。在步驟110，處理電路系統16基於暫存器36中之GCS指標而判定GCS載入/儲存操作之目標位址。在步驟112，記憶體管理單元28在其TLB 29中查找目標位址，以獲得GCS載入/儲存操作之目標位址的記憶體屬性。在步驟114，MMU 28判定目標位址是否對應於GCS記憶體區域，其係用於儲存GCS資料結構之專用類型的記憶體區域。若目標位址不對應於GCS記憶體區域類型，則在步驟116，拒絕GCS載入/儲存操作。傳訊錯誤，其可中斷正執行的處理且使例外處理器處理錯誤的原因。藉由抑制至未標記為GCS記憶體區域類型

之區域的GCS存取，此防止GCS載入/儲存指令被錯誤使用於存取非GCS記憶體，且亦意謂由GCS載入操作返回的經保護返回狀態可係受信任的，因為其不可能已被非GCS指令竄改。

【0070】 若在步驟114，判定目標位址對應於GCS記憶體區域，則在步驟118，MMU 28判定任何其他存取權限檢查是否通過。此等檢查可檢查其他屬性，諸如指示讀取請求及寫入請求是否允許分別為記憶體區域之讀取/寫入權限資訊的其他屬性，或者定義處理器2之執行狀態子集的屬性，其中該區域被允許存取。若任何其他存取權限檢查失敗，則在步驟116，拒絕GCS載入/儲存操作，且傳訊一錯誤。由處理器在發生錯誤時所設定的錯誤類型資訊可取決於錯誤的原因是否為對非GCS記憶體區域的GCS存取、或另一類型之存取權限違反而不同。若所有任何其他存取權限檢查皆通過，則在步驟120，允許GCS載入/儲存操作。

【0071】 圖5顯示針對非GCS載入/儲存操作（由除了GCS存取指令類別以外之指令所觸發的載入/儲存）執行的類似存取權限檢查。步驟130、132、及134類似於圖4之步驟110、112、114。相較於圖4，在圖5之步驟134，相較於GCS載入/儲存操作，非GCS載入/儲存操作對於目標位址是否對應於GCS記憶體區域之檢查的回應係相反方向，其中當目標位址對應於GCS記憶體區域時，則拒絕非GCS儲存操作，而若目標位址不對應於GCS記憶體區域，則拒絕GCS儲存操作。

【0072】 因此，若在步驟134，判定目標位址對應於GCS記憶體區域，且在步驟135，判定目前載入/儲存操作係非GCS儲存操作，則在步驟136，拒絕非GCS載入/儲存操作，且傳訊一錯誤。取決於在步驟138執行的任何其他存

取權限檢查的結果，即使非GCS載入操作的目標係GCS記憶體區域，該等非GCS載入操作仍可能被允許。若任何其他存取權限檢查失敗，則在步驟136，再次拒絕非GCS載入/儲存操作。否則，若目標位址不對應於GCS記憶體區域（在步驟134的N）、或非GCS操作係載入操作（在步驟135的N），且在步驟138，任何其他存取權限檢查（與GCS存取檢查無關）通過，則在步驟140，允許非GCS載入/儲存操作。

【0073】 圖6係繪示指令提取或分支操作之權限檢查的流程圖。在步驟150，提取級6請求提取與目標位址相關聯的指令、或偵測到至目標位址處之指令的分支（可基於藉由執行級16之分支單元24執行分支指令、或基於藉由與提取級6相關聯之分支預測器所作出的未來分支預測而偵測到該分支）。回應於指令提取或分支，在步驟152，MMU 28在其TLB 29中查找目標位址以識別對應於目標位址的記憶體屬性資料（其中若存在TLB未命中(miss)，則執行至記憶體的分頁表走訪），並判定目標位址是否位於由記憶體屬性資料識別為GCS區域的區域中。若目標位址位於GCS區域中，則在步驟154，拒絕指令提取或分支，且傳訊一錯誤。此防止儲存GCS結構上的資料被視為可能產生不可預測結果之風險的可執行指令。

【0074】 若目標位址不位於GCS區域中，則在原則上可執行從該位址載入的指令，取決於在步驟156執行的任何其他權限檢查。例如，此等檢查可包括基於分頁表的檢查，其檢查內容係在目標位址之記憶體屬性資料中指示的執行權限資料。若該等其他權限檢查通過，則在步驟158，可允許指令提取或分支。若其他權限檢查失敗，則在步驟154，再次拒絕指令提取或分支，且傳訊一錯誤。

【0075】 因此，GCS記憶體區域受限於提供資料值（諸如位址指標及其他資訊）且無法提供可執行指令碼，因為嘗試從其提取指令、或將指令分支至其中，GCS區域將觸發錯誤。

【0076】 上文描述之措施可有用於保護GCS資料結構上的內容在特定程序內處理功能返回及例外返回時免於受惡意攻擊者竄改。

【0077】 然而，對控制流程另一可能的風險可係當暫存器36中的GCS指標從與傳出堆疊資料結構相關聯的一傳出堆疊指標值切換至與傳入堆疊資料結構相關聯的一傳入堆疊指標值時。當在使用不同GCS資料結構的執行緒之間切換時，此類切換可係常見的（且被允許），但可能係攻擊者嘗試使用的途徑，以在嘗試暴露對攻擊者不應可存取之對受害者程序可存取的敏感資訊時導致不正確處理。例如，若堆疊指標切換之傳入堆疊指標值被導致成為不對應於該傳入執行緒之正確GCS資料結構的一位址，則可能存在不適當控制流程被觸發的風險，特別是若針對傳入堆疊指標值指定的位址剛好是在記憶體之GCS區域內的位址（例如，指向與不同執行緒相關聯之GCS結構上的返回狀態的位址）。即使傳入堆疊指標值係在該傳入執行緒之正確GCS資料結構內的位址，若傳入堆疊指標值設定成除了表示堆疊之目前「頂部」之位置以外的位置，則可能仍存在錯誤的風險，因為此可能對正被用作不同例外/功能返回之返回位址的一個例外/功能返回導致有效返回狀態，這仍導致不正確資訊。

【0078】 傳入堆疊指標值中之此類錯誤可能由於程式化錯誤而意外出現，或藉由攻擊者而惡意地出現，該攻擊者危害執行碼以導致將暫存器36中之GCS指標的值切換以指向不正確位置（例如，在受攻擊者控制的GCS資料結構中的位置）（在GCS區域中，因此不被圖4的檢查抓到）的指令被執行，該不

正確位置已預先填入經設計以矇騙受害者軟體程序進行分支至不正確碼序列中的返回位址。

【0079】 用於減輕免於受傳入堆疊指標值之此類錯誤設定的一種方法可係需要使至GCSPR 36之各寫入被捕捉至更高特權的執行狀態，使得更高特權的程序（諸如作業系統或超管理器）可在更新GCSPR 36之前驗證堆疊指標的新值是否安全性。然而，此將不利地影響效能。GCS指標的切換在應用程式層級執行緒之間切換時係非常常見的並確保快速切換且因此確保高效能，可係所欲的是允許此類GCS指標切換在無需呼叫更高特權的程序的情況下進行。

【0080】 亦可係非所欲的是，允許對GCS指標暫存器36的直接存取，以降低上文描述之形式的攻擊風險。

【0081】 因此，可提供一些指令以用於控制GCS指標暫存器36中之堆疊指標值的切換，其可實施用於偵測傳入堆疊指標值之不適當設定的一些健全性檢查。此等GCS指標切換指令被視為是GCS存取指令類別的成員，使得至由此等指令觸發之GCS區域的寫入可通過圖4及圖5所示之檢查。

【0082】 當在不同執行緒之間切換時，軟體堆疊（使用與GCS指標分開的堆疊指標追蹤）藉由軟體切換，且亦可切換目前保護控制堆疊。為了確保軟體無法切換至傳入GCS上的任何任意位置，當從該GCS切換而出時一堆疊封蓋值經添加至傳出GCS，且當堆疊指標上的傳入堆疊切換時，該封蓋值在切換至該GCS時驗證。

【0083】 該封蓋值經設計以可與任何程序返回值區分，這意謂在切換堆疊時，我們可自信我們僅切換至傳入GCS之頂部。例如，封蓋值之較低位址位元可設定成無法由任何有效指令位址指定的非零位元模式，因為指令對準需求

可能需要將所有有效指令位址在指令長度之粒度下對準至位址邊界（例如，對於32位元指令編碼而言，對準位址邊界可係4位元組間隔）。此意謂任何有效程序返回值對於較低位元應具有0，且因此封蓋值可藉由在較低位元中具有至少一個1而區分。

【0084】 封蓋值亦含有我們在切換至GCS時檢查的封蓋位置的位址。此位址提供：

1) 我們正使用 GCS 之 PA 映射的正確 VA 返回至預期 GCS 的一健全性檢查，藉由將封蓋之位址與從封蓋載入的值比較。

2) 一安全性檢查，以防止封蓋（不正確地）用作程序返回之部分的情況。若我們嘗試分支至保持在封蓋中的值，則此隱含地係一*資料*位址，因為其位於 GCS 區域中（因此若存在該位址處執行指令的嘗試，則圖 6 所示之檢查將觸發錯誤），且當處理器嘗試從此位置執行時，其將不具有執行權限且將採用一例外。

【0085】 我們觀察到若保持在封蓋中的位址位於與封蓋之位置相同的記憶體分頁中，則上文第2點中的安全性檢查繼續維持，因為位址仍將係*資料*分頁（GCS記憶體區域，其係使用由記憶體位址空間之分頁的粒度定義之分頁表項目直接或間接指定的記憶體屬性所設定）。若我們僅儲存封蓋之位置的位元[63:12]，則此允許我們儲存較少的位址位元，因為此確保我們位於與封蓋位置相同的4KB分頁。因此，嘗試使用該封蓋作為返回位址仍將導致權限錯誤。

【0086】 健全性檢查#1亦部分保留，其中我們確信我們按預期正切換至相同GCS，儘管僅切換至相同GCS內的位置（但在任何情況下，仍不可能在該GCS先前切換而出時有效地切換至並非堆疊之頂部的該GCS中的位置，因為切

換至不在該堆疊之頂部處的位置將導致除了有效封蓋值以外的資訊被返回，從而導致一無效堆疊封蓋值有效性檢查，且因此執行錯誤處理回應）。

【0087】 因此，封蓋值僅需要指定分頁位址，且不需要指定子分頁位址位元。在切換至傳入堆疊時檢查封蓋值的有效性時，傳入堆疊指標之子分頁位址位元不需要檢查以偵測封蓋值是否有效。

【0088】 此係有用的，因為其允許GCS中之記錄的格式具有更多保留位元，從而允許該架構的未來擴增。此係非常有用的，因為預期GCS可用以保護除了功能/例外返回狀態資訊以外的廣泛範圍的其他資訊，且因此具有編碼其他記錄類型的編碼空間可係有用的。

【0089】 圖7繪示在將在GCSPR 36中之堆疊指標從傳出堆疊指標值切換至傳入堆疊指標值時執行的步驟（其中傳入堆疊指標值係無關於傳出堆疊指標值，亦即，此不僅僅是在推送至堆疊或從堆疊取出時所執行之目前堆疊指標的增量或減量，而是堆疊指標之任意切換以指定提供作為觸發該切換的指令之運算元的一位址）。

【0090】 在步驟200，處理電路系統16執行一堆疊指標切換有效性檢查操作。此包括發布一記憶體存取請求，以從基於傳入堆疊指標值判定之位址X載入一傳入資料值。在許多情況下，位址X可係由傳入堆疊指標值本身所指示的位址。然而，亦將可行的是，傳入資料值之位址X藉由將一偏移施加至由傳入堆疊指標值指示的位址而判定，取決於標記為堆疊之「頂部」的位置相對於暫存器36中之堆疊指標值表示的方式。用於從位址X載入傳入資料值的記憶體存取請求係GCS載入存取，因此若位址X不對應於GCS記憶體，則可能失敗。

【0091】 若軟體正確地運作，預期基於傳入堆疊指標值而從位址X獲得的傳入資料值應是先前在從GCS指標之先前切換上之該GCS結構切換而出時將已置放在傳入GCS結構上的堆疊封蓋值。然而，處理電路系統16並不知道（尚未）傳入堆疊指標值是否實際上對應於先前存取的GCS結構，因此亦可能是傳入資料值可能不對應於有效堆疊封蓋值。

【0092】 因此，在步驟200，處理電路系統16執行堆疊指標切換有效性檢查操作，以檢查傳入資料值是否符合至少一堆疊封蓋值有效性條件。至少一堆疊封蓋值有效性條件至少包括傳入資料值之一預定部分對應於指示包含位址X的位址空間之分頁的一給定分頁位址，無關於傳入資料值之進一步部分是否對應於位址X之子分頁位址位元。更具體而言，傳入資料值之該預定部分必須對應於對應於虛擬位址X的一虛擬分頁位址，使得此檢查可檢查用以基於傳入堆疊指標值存取堆疊的虛擬至實體位址映射是否仍與先前在該堆疊被存取時相同。藉由不考慮用於驗證至少一堆疊封蓋值有效性條件之位址X的子分頁位址位元，此釋放GCS堆疊記錄中顯著量的編碼空間以用於其他目的，如將在下文關於圖11更詳細地討論。如下文討論之圖8的步驟224所示，至少一堆疊封蓋值有效性條件亦可對傳入資料值的編碼施加其他要求。

【0093】 在步驟202，判定傳入資料值是否符合由處理電路系統16施加之至少一堆疊封蓋值有效性條件之各者。需要滿足的至少一堆疊封蓋值有效性條件至少包括傳入資料值指定儲存傳入資料值之位置的虛擬分頁位址。亦可施加一或多個額外堆疊值有效性條件（例如，傳入資料值之較低部分係表示堆疊封蓋值的符記位元模式）。若不符合任何堆疊封蓋值有效性條件，則在步驟204，觸發錯誤處理回應。例如，此回應可傳訊一錯誤、在一錯誤報告暫存器中設定

一錯誤旗標、或將GCSPR 36中之堆疊指標設定成在無法針對任何有效記憶體位址而指定之一保留位址範圍中的一無效位址（若存在任何嘗試對該保留範圍中之一位址執行一載入/儲存操作或一指令提取，則MMU可觸發一錯誤）。

【0094】 若判定傳入資料值不符合所施加之至少一堆疊封蓋值有效性條件之各者時，則在步驟206，處理電路系統16允許堆疊指標從傳出堆疊指標值切換至傳入堆疊指標值（因此傳入堆疊指標值被寫入至GCSPR 36）。

【0095】 此外，在步驟208，處理電路系統16執行一傳出堆疊封蓋操作以將有效堆疊封蓋值推送至具有基於傳出堆疊指標值選擇之位址Y的位置。有效堆疊封蓋值在將於步驟200檢查之預定部分中指定指示包含（虛擬）位址Y的位址空間之分頁的（虛擬）分頁位址）。因此，此確保傳出堆疊經密封（以防止基於對堆疊之頂部的存取觸發返回，因為堆疊封蓋值具有將對該位址之指令提取或分支導致錯誤的值），且具有在對應堆疊指標值經指定為用於堆疊切換的傳入堆疊指標時將稍後允許有效切換回至該堆疊的適當封蓋值。

【0096】 在一些實施方案中，圖7所示之傳出堆疊封蓋操作可回應於亦觸發堆疊指標切換有效性檢查操作的相同指令而執行。

【0097】 然而，圖8及圖9顯示特定實例，其中傳出堆疊封蓋操作係回應於與觸發堆疊指標切換有效性檢查操作之指令不同的指令而執行。將此等操作分成分開的指令可大幅簡化電路實施方案，因為其避免兩個不同記憶體位址在相同指令中由MMU 28轉譯的需求。圖8顯示用以執行堆疊指標切換有效性檢查操作且實施GCSPR 36中之堆疊指標的切換之第一堆疊指標切換指令(GCSSS1)的功能。圖9顯示用以執行傳出堆疊封蓋操作之第二堆疊指標切換指令(GCSSS2)的功能。

【0098】 如圖8之步驟220所示，第一堆疊指標切換指令之運算元係在GCSPR 36中指定的傳出堆疊指標值、及在通用暫存器Xn中指定的傳入堆疊指標值，該通用暫存器Xn之暫存器指定器係在第一堆疊指標切換指令之指令編碼內編碼。因此，軟體可選擇任意通用暫存器以用於定義傳入堆疊指標，且先前的指令可以任何任意軟體特定的方式設定該傳入堆疊指標。GCSPR 36不需在GCSSS1指令之編碼中明確地編碼，因為其係該操作的隱含運算元。

【0099】 回應於GCSSS1指令由解碼級10解碼且經發布以供管線4之發布級12執行，在步驟222，處理電路系統16控制記憶體存取電路系統（載入/儲存單元26）以發布請求從對應於基於傳入堆疊指標值（衍生自暫存器Xn）判定之位址的位置將傳入資料值載入的載入記憶體存取請求。在一個具體實施方案中，由載入記憶體存取請求所指定的位址等於傳入堆疊指標值，但其他實例可藉由施加一偏移至傳入堆疊指標值而衍生載入位址。此載入記憶體存取請求取決於圖4所示之檢查，因為其係GCS載入操作，因為其由GCSSS1指令觸發。假設載入操作通過此等檢查，傳入資料值返回，且在步驟224，處理電路系統16檢查(i)傳入資料值之預定部分是否對應於用於步驟222之載入的虛擬位址之分頁位址部分，及(ii)傳入資料值之最低有效部分是否係識別有效堆疊封蓋值的特定位元模式，該特定位元模式不能夠由任何有效指令位址之最低有效部分指定。若此等檢查之任一者失敗，則傳入資料值不是有效堆疊封蓋值，且在步驟226，觸發一錯誤處理回應（其可係上文針對圖7之步驟204所提及之錯誤處理回應之類型的任一者）。

【0100】 若在步驟224之檢查通過（傳入資料值之預定部分對應於用於在步驟222之載入的虛擬位址之分頁位址部分，且傳入資料值之最低有效部分

具有識別有效堆疊封蓋值的特定位元模式），亦即，傳入資料值符合至少一堆疊封蓋值有效性條件，則在步驟228，處理電路系統16控制記憶體存取電路系統26以發布儲存記憶體存取請求，以將進行中符記值儲存至具有基於傳入堆疊指標選擇之位址的記憶體位置。進行中符記值指定傳出堆疊指標值，且使其最低有效部分設定成不能夠由任何有效指令位址之最低有效部分指定的另一位元模式，其不同於有效堆疊封蓋值之最低有效部分的編碼。吾人可能不會預期對於切換堆疊指標的指令使用傳出堆疊指標作為運算元係必要的，因為吾人將預期可行的是只要使用GCSPR 36中之傳入堆疊指標值覆寫傳出堆疊指標。然而，藉由將傳出堆疊指標寫入至傳入堆疊（在傳入堆疊已藉由執行步驟224之堆疊封蓋值有效性檢查驗證之後），此幫助支援堆疊指標切換操作被分在兩個指令GCSSS1與GCSSS2之間的實施方案，因為其使傳出堆疊指標值能夠被保存，使得其可用於第二堆疊指標切換指令GCSSS2，而不需要其在GCSPR 36中被覆寫之後消耗一架構暫存器以用於保留傳出堆疊指標值。

【0101】 在步驟230，在步驟224之檢查通過的情況下，更新GCSPR 36以指定傳入堆疊指標值（因此傳出堆疊指標值被覆寫）。

【0102】 如圖8所示，在步驟222的載入及在步驟228的儲存係原子地執行，使得藉由軟體執行GCSSS1指令、及另一執行緒存取基於傳入堆疊指標判定之相同位址所見的結果係與若在步驟222的載入及在步驟228的儲存在不具有任何介入寫入至該位址發生在步驟222的載入與在步驟228的儲存之間的情況下連續地執行而將發生的結果一致。可能存在可用以確保此原子性的數個不同技術。例如，可使用基於鎖定的方法以鎖定對相關記憶體位置的存取，使得在載入與儲存之間的週期中沒有至該記憶體位置的其他寫入可被允許。替代地，由

其他執行緒（例如，在不同處理器核心執行）觸發的衝突寫入操作仍可能在介入週期中被允許，但若偵測到此一寫入，則可提供一機制以偵測此類衝突寫入操作並中止由堆疊指標切換指令執行的處理（例如，清除(flush)管線並回繞(rewind)至包括GCSSS1指令之執行緒中的先前執行點，以導致GCSSS1指令稍後被重新執行）。載入及儲存的原子處理藉由減少由GCSSS1指令檢查的狀態在該檢查完成之前改變（其可能有錯誤的風險）的機會，來幫助改善安全性。

【0103】 圖9繪示第二堆疊指標切換指令(GCSSS2)的處理。如步驟250所示，指令之運算元係在GCSPR 36中指定的目前值。預期在GCSSS2指令跟著GCSSS1指令的常見使用情況中，GCSPR 36中的值應係基於GCSSS1指令之Xn運算元指定的傳入堆疊指標值。然而，在實作上，處理器之硬體不可能檢查GCSSS2指令係實際上跟著GCSSS1指令，因此雖然下文GCSSS2的虛擬碼係指如「傳入」堆疊指標值之GCSSS2指令的運算元，但更大致而言，其在儲存於堆疊指標暫存器36中的目前堆疊指標上操作，而不考慮此是否實際上係與先前GCSSS1指令之傳入堆疊指標值相同的值。

【0104】 回應於GCSSS2指令由解碼級10解碼且經發布以供管線4之發布級12執行，在步驟252，處理電路系統16控制記憶體存取電路系統26以發布請求從對應於基於從GCSPR 36獲得之目前堆疊指標判定之位址的位置將一給定資料值載入的載入記憶體存取請求。在一個具體實施方案中，由載入記憶體存取請求所指定的位址等於來自GCSPR 36的目前堆疊指標值，但其他實例可藉由施加一偏移至目前堆疊指標值而衍生載入位址。此載入記憶體存取請求取決於圖4所示之檢查，因為其係GCS載入操作，因為其由GCSSS2指令觸發。假設載入操作通過此等檢查，給定資料值返回，且在步驟254，處理電路系統16檢

查給定資料值是否係一有效地形成的進行中符記。例如，當給定資料值之最低有效位元部分匹配用以編碼進行中符記的特定位元模式時，處理電路系統16判定給定資料值係有效地形成的進行中符記。此位元模式不同於有效堆疊封蓋值之最低有效部分處的位元模式，因此不能夠由符合至少一堆疊封蓋值有效性條件的任何值指定。此外，此位元模式不能夠藉由任何有效指令位址所指定（例如，因為其在較低位元位置中係非零，其等比表示指令對準邊界之有效度(significance)的位元更低有效）。若給定資料值不是一有效地形成的進行中符記，則在步驟256，觸發一錯誤處理回應（同樣地，此可係先前提及的錯誤處理回應類型之任一者）。

【0105】 若給定資料值係一有效地形成的進行中符記，則在步驟258，處理電路系統16控制記憶體存取電路系統26以發布儲存記憶體存取請求，以將有效堆疊封蓋值寫入至具有基於在步驟252載入之給定資料值之部分中指定的給定堆疊指標值判定之位址Y的位置。在一些實例中，位址Y可係相對於給定堆疊指標值以對應於一個堆疊項目之大小的量的偏移，以反映有效堆疊封蓋值至堆疊之頂部上的添加意謂對應堆疊之堆疊指標將從其先前值（由給定堆疊指標值表示）增量或減量，類似於將一新的堆疊項目推送至該堆疊的任何其他堆疊推送操作。因此，在步驟258的儲存操作係至與在步驟252從其載入給定資料值之位址不同的位址Y。若GCSSS2指令並未跟著先前GCSSS1指令，則在步驟258的儲存係至基於GCSSS1指令之傳出堆疊指標的傳出堆疊結構，而在步驟252的儲存係來自傳入堆疊結構。有效堆疊封蓋值在圖8之步驟224針對分頁位址檢查的預定部分內指定包含虛擬位址Y的位址空間之分頁的（虛擬）分頁位址，該虛擬位址Y係由從在步驟252載入之給定資料值獲得之給定堆疊指標值

所指定。此在傳出堆疊上設定堆疊封蓋值，使得在稍後將堆疊指標切換回傳出堆疊（現用作為傳入堆疊）時，該稍後堆疊指標切換可通過在圖8之步驟224針對GCSSS1指令執行的檢查。

【0106】 此外，在圖9之步驟260，處理電路系統回應於GCSSS2指令而更新在GCSPR 36中之堆疊指標，以指示將提供給定資料值之項目從堆疊移除。此更新可係以對應於一個堆疊記錄之大小的量增量或減量目前堆疊指標。是否施加增量或減量取決於堆疊是否經管理為遞減堆疊或升序堆疊（兩個選項皆可能，亦即，對於遞減堆疊而言堆疊指標在推送上減量且在取出上增量，且對於升序堆疊而言反之亦然）。

【0107】 用於表示GCSSS1及GCSSS2指令之功能性的實例虛擬碼顯示如下。應理解，雖然此顯示為在硬體處理器中之虛擬碼，但其將使用實施對應功能之硬體電路邏輯閘而實施。

```
gcsss1(bits(64) Xn)

bits(64) outgoing_pointer, incoming_pointer, incoming_value,
        in_progress_entry;
outgoing_pointer = GCSPR;
incoming_pointer = Xn;

incoming_value = mem[incoming_pointer];

if incoming_value == incoming_pointer[63:12]:'000000000001' then
                // valid entry, as incoming value is a validly formed stack cap //value
        in_progress_entry = outgoing_pointer[63:3]:'101';  // in_progress_token
        mem[incoming_pointer] = in_progress_entry;  // atomic with earlier load
        GCSPR = incoming_pointer[63:3]:'000'; //switch GCS pointer
else
    assert(FALSE);  // take error handling response

gcsss2()
```

```
bits(64) outgoing_pointer, incoming_pointer, outgoing_value;
incoming_pointer = GCSPR;

outgoing_value = mem[incoming_pointer];

if outgoing_value[2:0] == '101' then        // valid in_progress token

        outgoing_pointer[63:0] = (UInt(outgoing_value[63:3]:'000') - 8)<63:0>;
        outgoing_value = outgoing_pointer[63:12]:'000000000001';
         // set up valid entry on outgoing stack, including the stack cap value

        mem[outgoing_pointer] = outgoing_value;
        GCSPR = incoming_pointer + 8;
        // nudge the incoming GCS up one data word, to represent removal of
        //in-progress token
        return outgoing_pointer;
else
        assert(FALSE); // take error handling response.
```

【0108】 當然，用於有效堆疊封蓋值及進行中符記的具體編碼可與虛擬碼顯示者不同。

【0109】 圖10示意地繪示基於上文所討論之操作的堆疊切換的實例。圖10之頂部部分顯示當在GCSPR 36中之傳出GCS指標P1目前指向傳出GCS之頂部時的初始狀態，且傳入GCS（與指標P2相關聯）先前已藉由在堆疊之頂部儲存有效堆疊封蓋值而封蓋。

【0110】 如圖10之中間部分所示，當執行GCSSS1指令將指示指標P2的運算元指定至傳入GCS時，堆疊指標切換有效性檢查操作通過，因為傳入堆疊指標值之分頁位址部分P2匹配從對應於傳入堆疊指標值之傳入GCS上的位置所獲得之值的預定部分P2[63:12]。因此，傳入堆疊標記為指定傳出堆疊指標P1[63:3]的進行中符記值，且GCSPR 36經更新以指示傳入堆疊指標P2。

【0111】 如圖10之下部分所示，當執行GCSSS2指令時，傳入GCS上的進行中符記（基於在GCSPR 36中之目前堆疊指標值P2而存取）經驗證並且其通過檢查，且因此傳出堆疊藉由將有效堆疊封蓋值寫入至基於從進行中封蓋值符記獲得之傳出堆疊指標P1[63:3]所定址的傳出堆疊上的位置而封蓋，該有效堆疊封蓋值指定包含使用有效堆疊封蓋值寫入之位置的分頁的分頁位址部分。此外，在GCSPR 36中之目前堆疊指標經更新，以表示進行中符記從傳入GCS的移除（在此實例中藉由加8，但其他實例可使用減量或可具有不同大小的堆疊記錄，且因此具有不同增量/減量大小）。

【0112】 圖11繪示可置放在GCS堆疊上之GCS記錄的不同格式的實例：

- 一程序（功能）返回位址記錄 300，其提供 62 個位元的程序返回位址。0b00 之較低 2 個位元表明此係程序返回記錄（因為此等位元係 0，位址係 4 位元組對準，且因此可係對準至位址邊界之 32 位元指令編碼的有效指令位址）。
- 一堆疊封蓋值記錄 302，其提供 52 個位元的分頁位址，且對於較低 12 個位元具有 0b000000000001 之值。因為較低位元係 0b01，若解譯為指令位址，則此將係未對準位址，因此將觸發未對準錯誤。
- 一進行中符記記錄 304，其提供 61 個位元的堆疊指標值（用以表示如上文提及之在堆疊指標切換期間的傳出堆疊指標），使用此編碼存在對於此傳出堆疊指標為雙字對準的需求，使得堆疊指標位址之第 62 個位元隱含地為 0。記錄 304 之較低 3 個位元具有編碼 0b101 以表明此係進行中符記。

- 一例外記錄 306，其使較低 5 個位元設定為 0b01001 且所有更有效位元係 0。當在堆疊上偵測到例外記錄 306 時，一經定義數目之隨後記錄（其中完整 64 位元用於記錄例外狀態資訊）提供例外返回狀態的項，例如，例外返回位址、與正傳回之處理相關聯的經儲存處理器狀態等。

【0113】 此編碼意謂存在數個經保留編碼保持空閒，可用於未來擴增：

- 編碼 308，其使較低 3 個位元設定為 0b001（與堆疊封蓋記錄 302 及例外記錄 306 相同），但其使下 9 個位元設定為除了 0b000000000 或 0b000000001 以外的任何者。此等編碼允許編碼至少 $2^9 - 2 = 510$ 種額外記錄類型（藉由在位元[11:3]中設定不同「記錄類型」指示符），各自支援在記錄之位元[63:12]處之剩餘 52 個位元中的其他類型資訊的記錄。此額外的編碼空間因堆疊封蓋值記錄 302 指定分頁位址而非完整位址而釋放。
- 編碼 310，其使較低 2 個位元[1:0]設定為 0b10 或 0b11，其等支援在剩餘位元[63:2]中指定的完整 62 位元值。

【0114】 圖12繪示可使用的模擬器實施方案。雖然稍早所述之實施例以用於操作支援所關注技術的特定處理硬體之設備及方法來實施本發明，但亦可能根據本文所述之實施例提供一指令執行環境，其係透過使用電腦程式實施。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1320、支援模擬器程式1310的主機處理器1330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此需要執行另一處理器原生的程式碼時。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。模擬的綜述係於「Some Efficient Architecture Simulation Techniques」中給出，Robert Bedichek, Winter 1990 USENIX Conference，頁數53至63。

【0115】 在先前已參照特定硬體架構或特徵來描述實施例之情況下，在一模擬實施例中，可藉由合適的軟體架構或特徵提供等效功能。例如，可在模擬實施例中將特定電路系統實施為電腦程式邏輯。類似地，記憶體硬體（諸如暫存器或快取）可在模擬實施例中實施為軟體資料結構。於先前描述實施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1330）上的配置中，一些模擬實施例可在適當時利用主機硬體。

【0116】 模擬器程式1310可儲存在電腦可讀儲存媒體（其可係非暫時性媒體）上，並提供程式介面（指令執行環境）給目標碼1300（其可包括應用程式、作業系統、及超管理器），該程式介面與藉由模擬器程式1310模型化之硬體架構的介面相同。因此，目標碼1300之包括如上文描述之堆疊指標切換指令GCSSS1、GCSSS2的程式指令可在指令執行環境內使用模擬器程式1310執行，使得實際上不具有上文討論之設備2的硬體特徵的主機電腦1330可仿真此等特徵。類似地，如上文針對MMU 28及載入/儲存單元26所討論之各種記憶體管理檢查功能及至記憶體之存取的觸發（包括支援GCS記憶體區域類型），可使用模擬器程式1310之記憶體存取程式邏輯1318來仿真。

【0117】 因此，模擬器程式1310可具有處理程式邏輯1312，其模擬上文描述之處理電路系統4的狀態。例如，處理程式邏輯1312可回應於目標碼1300之模擬執行期間發生的事件而模擬執行狀態的轉變，並執行處理操作。指令解碼程式邏輯1314（其可視為處理程式邏輯之部分）解碼目標碼1300之指令，且將此等指令映射至主機設備1330之原生指令集中的對應指令集。暫存器仿真程式邏輯1316諸如藉由存取主機設備1330之暫存器或記憶體1332中的資料，而將由目標碼所請求之暫存器存取映射至對主機設備1330之主機硬體上維持之對應資料結構的存取（例如，當指令（諸如GCS推送/取出指令或GCSSS1、GCSSS2指令）需要對GCS指標暫存器的存取而執行時，對表示經模擬GCS指標暫存器之主機位置的存取可藉由暫存器仿真程式邏輯1316管理）。記憶體存取程式邏輯1318實施位址轉譯、分頁表走訪及以對應於在上文的硬體實施例中描述的MMU 28之方式存取控制檢查，但亦具有映射模擬實體位址（基於針對目標碼1300所界定的頁表而藉由位址轉譯獲得）的額外功能至用以存取主機記憶體1332的主機虛擬位址。此等主機虛擬位址可本身使用由主機所支援之標準位址轉譯機構來轉譯成主機實體位址（將主機虛擬位址轉譯成主機實體位址係在受到模擬器程式1310控制的範圍之外）。

【0118】 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作業的一組態。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，其提供經定義的作業，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作業。

【0119】 在本申請案中，以片語「之至少一者(at least one of)」前綴的特徵列表意謂著此等特徵的任何一或多者可個別地或組合地提供。例如，「[A]、[B]、及[C]之至少一者」涵蓋下列選項的任一者：單獨A（不具有B或C）、單獨B（不具有A或C）、單獨C（不具有A或B）、A及B的組合（不具有C）、A及C的組合（不具有B）、B及C的組合（不具有A）、或A、B、及C的組合。

【0120】 雖然本文已參照附圖詳細地描述本發明的說明性實施例，應瞭解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於其中實行各種變化與修改，而不脫離如隨附申請專利範圍所定義的本發明的範圍。

【符號說明】

【0121】

2:資料處理設備；設備；處理器

4:處理管線

6:提取級

8:快取記憶體；一級指令快取記憶體；記憶體系統

10:解碼級

12:發布級

14:暫存器檔案；暫存器

16:執行級；處理電路系統

18:寫回級

20:純量算術/邏輯單元(ALU)；處理單元

22:浮點單元；處理單元

24:分支單元；處理單元

26:載入/儲存單元；處理單元；記憶體存取電路系統

28:記憶體管理單元(MMU)

29:轉譯後備緩衝區(TLB)

30:記憶體系統；一級資料快取記憶體；快取記憶體

32:記憶體系統；共用二級快取記憶體；快取記憶

34:記憶體系統；主系統記憶體；記憶體

36:經保護控制堆疊指標(GCSPR)暫存器；GCSPR；暫存器

40:經保護資料結構；GCS 資料結構；GCS 結構

58:GCS 指標暫存器

110:步驟

112:步驟

114:步驟

116:步驟

118:步驟

120:步驟

130:步驟

132:步驟

134:步驟

135:步驟

136:步驟

138:步驟

140:步驟

150:步驟

152:步驟

154:步驟

156:步驟

158:步驟

200:步驟

202:步驟

204:步驟

206:步驟

208:步驟

220:步驟

222:步驟

224:步驟

226:步驟

228:步驟

230:步驟

250:步驟

252:步驟

254:步驟

256:步驟

258:步驟

260:步驟

300:程序（功能）返回位址記錄

302:堆疊封蓋值記錄；堆疊封蓋記錄

304:進行中符記記錄；記錄

306:例外記錄

308:編碼

1300:目標碼

1310:支援模擬器程式

1312:處理程式邏輯

1314:指令解碼程式邏輯

1316:暫存器仿真程式邏輯

1318:記憶體存取程式邏輯

1320:主機作業系統

1330:主機處理器；主機電腦

1332:主機記憶體；暫存器或記憶體

【發明申請專利範圍】

【請求項1】一種設備，其包含：

記憶體存取電路系統，其用以基於一堆疊指標執行對一堆疊資料結構的一堆疊存取；及

處理電路系統，其用以執行與該堆疊指標從一傳出堆疊指標值至一傳入堆疊指標值之一切換相關聯的一堆疊指標切換有效性檢查操作，該堆疊指標切換有效性檢查操作包含驗證藉由該記憶體存取電路系統回應於指定基於該傳入堆疊指標值判定之一位址的一記憶體存取請求而獲得的一傳入資料值是否符合至少一堆疊封蓋值(stack cap value)有效性條件，該至少一堆疊封蓋值有效性條件包括該傳入資料值之一預定部分對應於指示包含基於該傳入堆疊指標值判定之該位址的位址空間之一分頁的一給定分頁位址的一條件，其中：

該處理電路系統經組態以判定該傳入資料值是否符合該至少一堆疊封蓋值有效性條件，無關於除了該預定部分以外之該傳入資料值的一進一步部分是否對應於基於該傳入堆疊指標值判定之該位址的子分頁位址位元；及

該處理電路系統經組態以回應於判定該傳入資料值不符合該至少一堆疊封蓋值有效性條件而觸發一錯誤處理回應。

【請求項2】如請求項1之設備，其中該給定分頁位址係指示包含基於該傳入堆疊指標值判定之一虛擬位址的虛擬位址空間之一分頁的一虛擬分頁位址。

【請求項3】如請求項1及2中任一項之設備，其中該處理電路系統經組態以執行與該堆疊指標從該傳出堆疊指標值至該傳入堆疊指標值之該切換相關聯的一傳出堆疊封蓋操作，以將一有效堆疊封蓋值推送至具有基於該傳出堆疊指標值選擇之一位址的一位置，該有效堆疊封蓋值在該有效堆疊封蓋值之該預定

部分中指定指示包含基於該傳出堆疊指標值選擇之該位址的位址空間之一分頁的一分頁位址。

【請求項4】如請求項3之設備，其中在該有效堆疊封蓋值中指定的該分頁位址係指示包含基於該傳出堆疊指標值選擇之一虛擬位址的虛擬位址空間之一分頁的一虛擬分頁位址。

【請求項5】如前述請求項中任一項之設備，其中該堆疊指標係一保護控制堆疊(guarded control stack, GCS)指標，該保護控制堆疊指標用於控制對一保護控制堆疊(GCS)資料結構的存取，以用於保護從一例外或功能呼叫返回的返回位址。

【請求項6】如請求項5之設備，其包含記憶體管理電路系統，其用以基於與該目標位址相關聯的記憶體屬性資料而判定是否允許對一目標位址的存取，該記憶體屬性資料指定包括該目標位址的一目標記憶體位址空間區域是否係用於儲存該GCS資料結構的一GCS區域，其中至該GCS區域的寫入存取受限於一專用類別的GCS存取指令。

【請求項7】如請求項6之設備，其中當該記憶體屬性資料指定該目標記憶體位址空間區域係該GCS區域時，該記憶體管理電路系統經組態以拒絕一指令提取或至該目標位址的分支。

【請求項8】如請求項6及7中任一項之設備，其中該記憶體管理電路系統經組態以回應於判定該目標記憶體位址空間區域係該GCS區域，而拒絕藉由除了該專用類別的GCS存取指令以外的一儲存指令所觸發之至該目標位址的一非GCS儲存操作。

【請求項9】如請求項6至8中任一項之設備，其中該記憶體管理電路系統經組態以回應於判定該目標記憶體位址空間區域不是該GCS區域，而拒絕藉由該專用類別的GCS存取指令之一者所觸發之至該目標位址的一GCS載入/儲存操作。

【請求項10】如前述請求項中任一項之設備，其中該至少一堆疊封蓋值有效性條件亦包含該傳入資料值之一最低有效部分具有不能夠由任何有效指令位址之最低有效部分指定的一位元模式的一條件。

【請求項11】如前述請求項中之設備，其中該處理電路系統經組態以回應於一第一堆疊指標切換指令指定指示該傳入堆疊指標值的一運算元，而執行該堆疊指標切換有效性檢查操作。

【請求項12】如請求項11之設備，其包含一堆疊指標暫存器，其用以儲存該堆疊指標；其中：

回應於該第一堆疊指標切換指令，當該堆疊指標切換有效性檢查操作成功時，該處理電路系統經組態以將該堆疊指標暫存器從該傳出堆疊指標值更新至該傳入堆疊指標值。

【請求項13】如請求項12之設備，其中回應於該第一堆疊指標切換指令，該處理電路系統經組態以將指定該傳出堆疊指標值的一進行中符記值推送至具有基於該傳入堆疊指標值選擇之一位址的一位置。

【請求項14】如請求項13之設備，其中對於用以載入待在該堆疊指標切換有效性檢查操作中驗證之該傳入資料值的一載入操作、及用以將該進行中符記值推送至具有基於該傳入堆疊指標值選擇之該位址的該位置的一儲存操作，該處理電路系統經組態以原子地執行該載入操作及該儲存操作。

【請求項15】如請求項13及14中任一項之設備，其中回應於一第二堆疊指標切換指令，該處理電路系統經組態以：

驗證藉由該記憶體存取電路系統回應於指定基於該堆疊指標暫存器中之一目前堆疊指標判定之一位址的一記憶體存取請求而獲得的一給定資料值是否係一有效地形成的進行中符記值；及

回應於驗證該給定資料值係一有效地形成的進行中符記值：

觸發一有效堆疊封蓋值至具有基於由該給定資料值之一部分指定的一給定堆疊指標值判定之一位址的一位置的一寫入，該有效堆疊封蓋值在該有效堆疊封蓋值之該預定部分中指定指示包含基於該給定堆疊指標值判定之一位址的分頁空間之一分頁的一分頁位址。

【請求項16】如請求項15之設備，其中回應於該第二堆疊指標切換指令，當該給定資料值經驗證為係該有效地形成的進行中符記值時，該處理電路系統經組態以更新該堆疊指標暫存器中之該目前堆疊指標，以指示將提供該給定資料值之一項目從一對應堆疊資料結構移除。

【請求項17】如請求項15及16中任一項之設備，其中當該給定資料值之一最低有效部分具有不能夠由任何有效指令位址之最低有效部分指定且不能夠由符合該至少一堆疊封蓋值有效性條件的任何值指定的一位元模式時，該處理電路系統經組態以驗證該給定資料值係該有效地形成的進行中符記值。

【請求項18】如請求項15至17中任一項之設備，其中該處理電路系統經組態以回應於判定該給定資料值不是一有效地形成的進行中符記值而觸發一錯誤處理回應。

【請求項19】如前述請求項中任一項之設備，其中該錯誤處理回應包含下列中之至少一者：

傳訊一錯誤；

設定一錯誤報告指示；及

將該堆疊指標設定成一無效值。

【請求項20】一種方法，其包含：

執行與一堆疊指標從一傳出堆疊指標值至一傳入堆疊指標值之一切換相關聯的一堆疊指標切換有效性檢查操作，該堆疊指標切換有效性檢查操作包含驗證藉由記憶體存取電路系統回應於指定基於該傳入堆疊指標值判定之一位址的一記憶體存取請求而獲得的一傳入資料值是否符合至少一堆疊封蓋值有效性條件，該至少一堆疊封蓋值有效性條件包括該傳入資料值之一預定部分對應於指示包含基於該傳入堆疊指標值判定之該位址的位址空間之一分頁的一給定分頁位址的一條件，其中：

該傳入資料值是否符合該至少一堆疊封蓋值有效性條件係無關於除了該預定部分以外之該傳入資料值的一進一步部分是否對應於基於該傳入堆疊指標值判定之該位址的子分頁位址位元而判定；及

該方法包含回應於判定該傳入資料值不符合該至少一堆疊封蓋值有效性條件而觸發一錯誤處理回應。

【請求項21】一種包含指令的電腦程式，當該等指令由一主機資料處理設備執行時，控制該主機資料處理設備提供用於執行目標碼的一指令執行環境，該電腦程式包含：

記憶體存取程式邏輯，其用以基於一堆疊指標執行對一堆疊資料結構的一堆疊存取；及

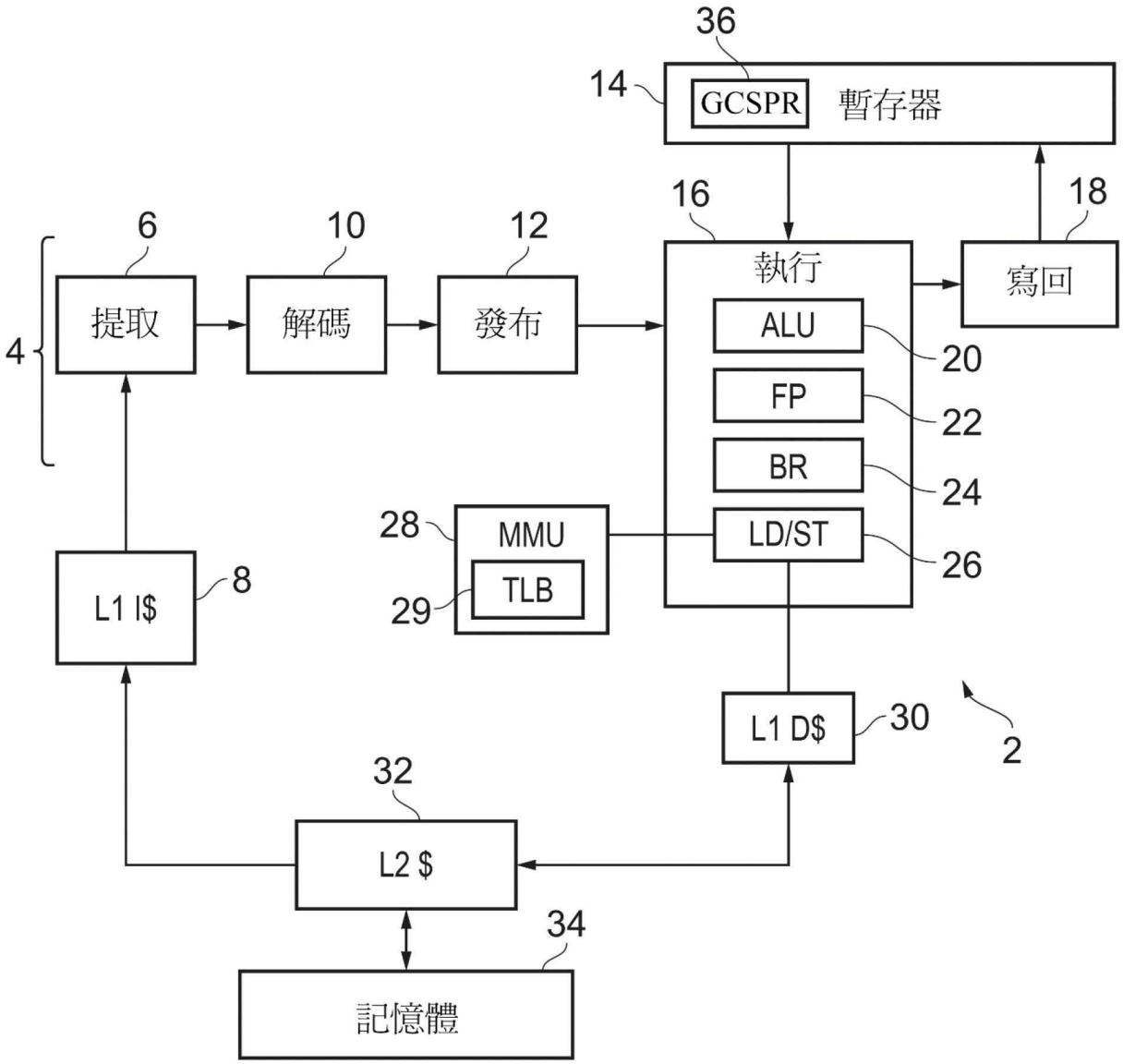
處理程式邏輯，其用以執行與該堆疊指標從一傳出堆疊指標值至一傳入堆疊指標值之一切換相關聯的一堆疊指標切換有效性檢查操作，該堆疊指標切換有效性檢查操作包含驗證藉由該記憶體存取程式邏輯回應於指定基於該傳入堆疊指標值判定之一位址的一請求而獲得的一傳入資料值是否符合至少一堆疊封蓋值有效性條件，該至少一堆疊封蓋值有效性條件包括該傳入資料值之一預定部分對應於指示包含基於該傳入堆疊指標值判定之該位址的位址空間之一分頁的一給定分頁位址的一條件，其中：

該處理程式邏輯經組態以判定該傳入資料值是否符合該至少一堆疊封蓋值有效性條件，無關於除了該預定部分以外之該傳入資料值的一進一步部分是否對應於基於該傳入堆疊指標值判定之該位址的子分頁位址位元；及

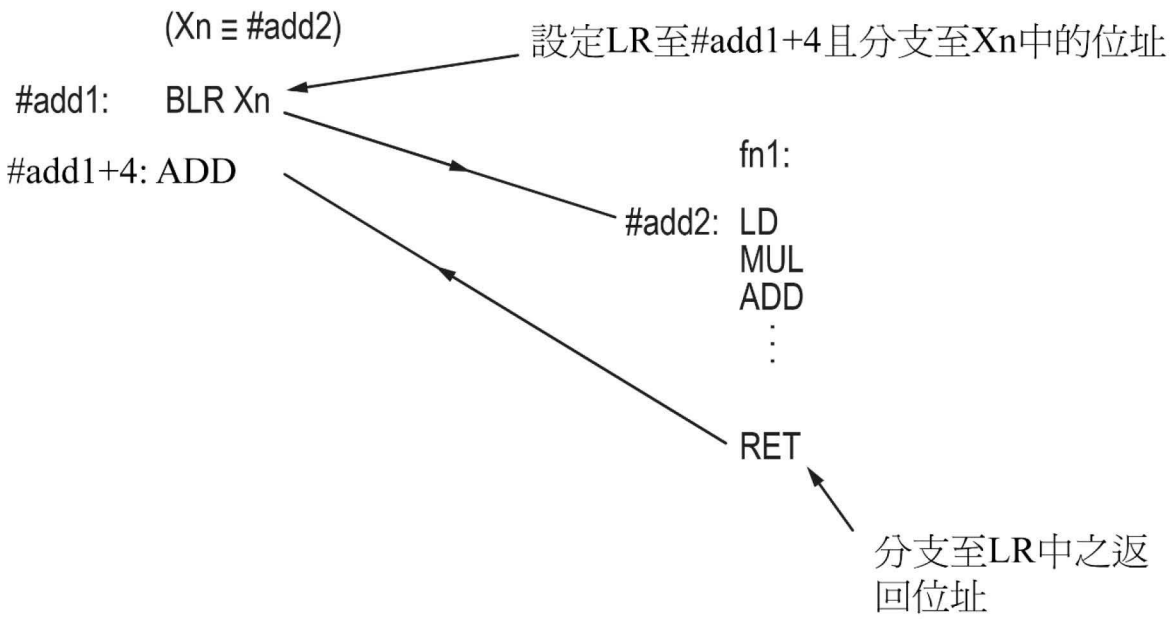
該處理程式邏輯經組態以回應於判定該傳入資料值不符合該至少一堆疊封蓋值有效性條件而觸發一錯誤處理回應。

【請求項22】一種儲存媒體，其儲存如請求項21的電腦程式。

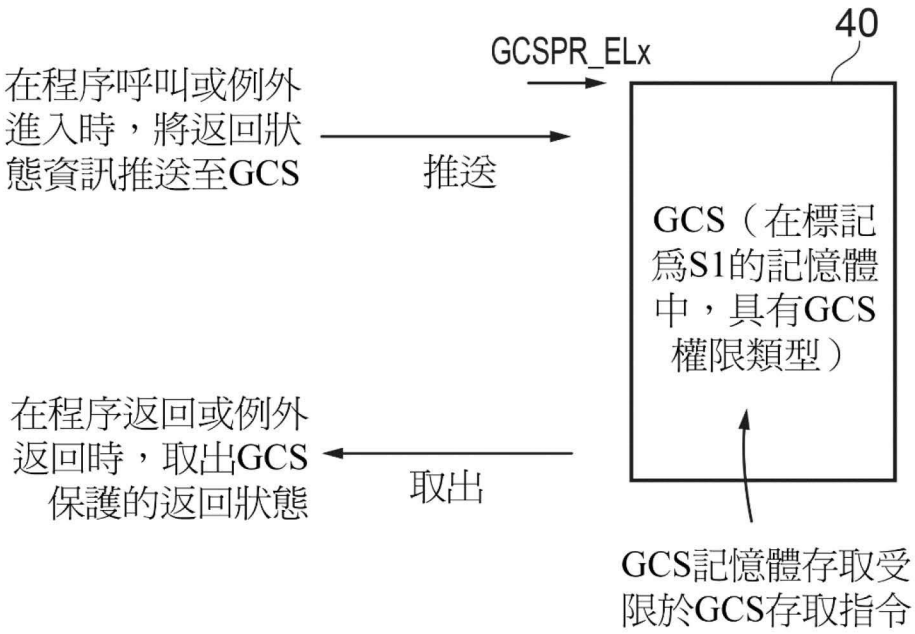
【發明圖式】


36
14
GCSPR
暫存器
16
18
6
10
12
執行
寫回
提取
解碼
發布
4
ALU
20
FP
22
BR
24
28
MMU
LD/ST
26
29
TLB
L1 I$
8
L1 D$
30
2
32
L2 $
34
記憶體

【圖1】

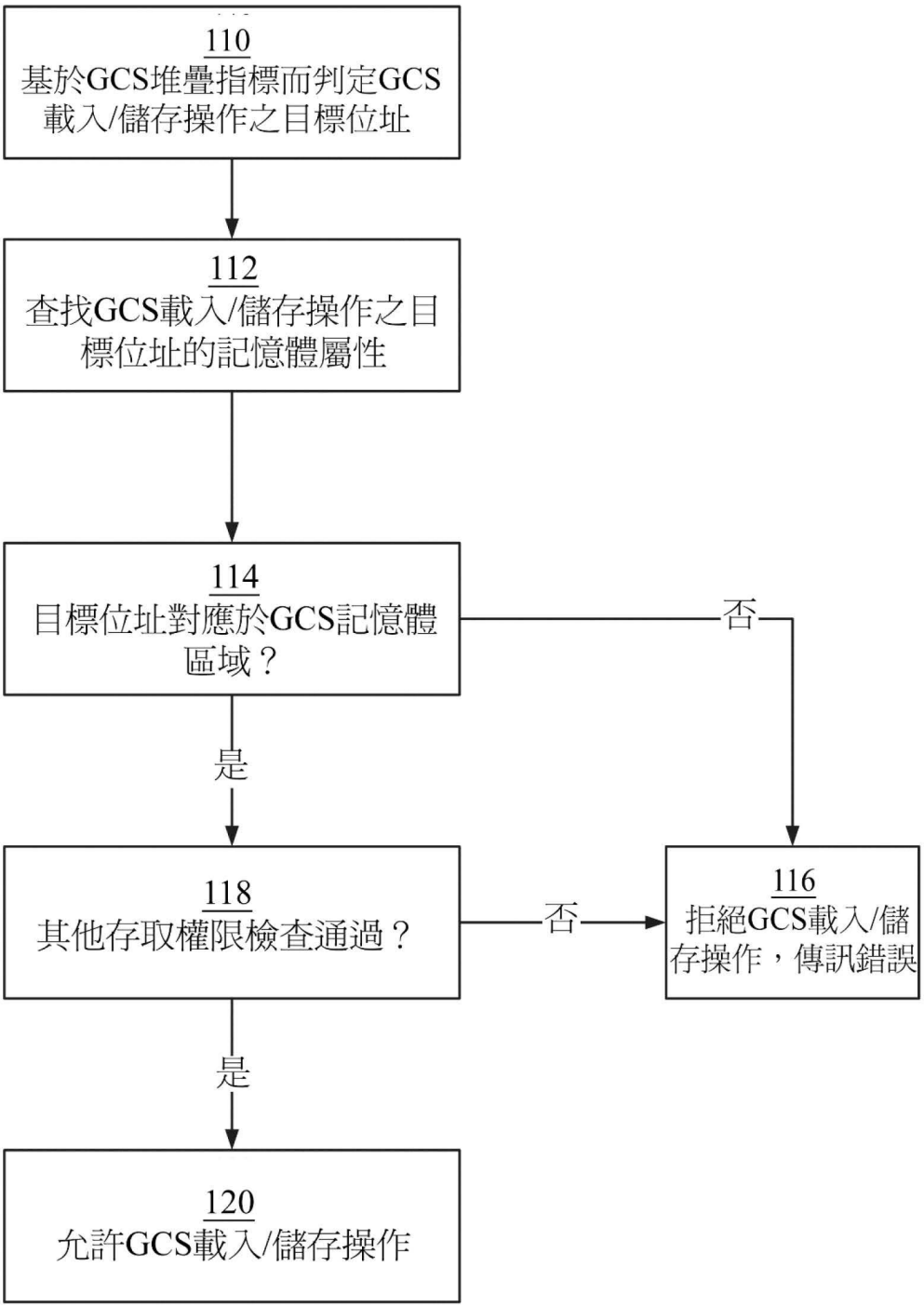

(Xn ≡ #add2)
設定LR至#add1+4且分支至Xn中的位址
#add1: BLR Xn
#add1+4: ADD
fn1:
#add2: LD
MUL
ADD
RET
分支至LR中之返回位址

【圖2】


40
GCSPR_ELx
在程序呼叫或例外進入時，將返回狀態資訊推送至GCS
推送
GCS（在標記爲S1的記憶體中，具有GCS權限類型）
在程序返回或例外返回時，取出GCS保護的返回狀態
取出
GCS記憶體存取受限於GCS存取指令

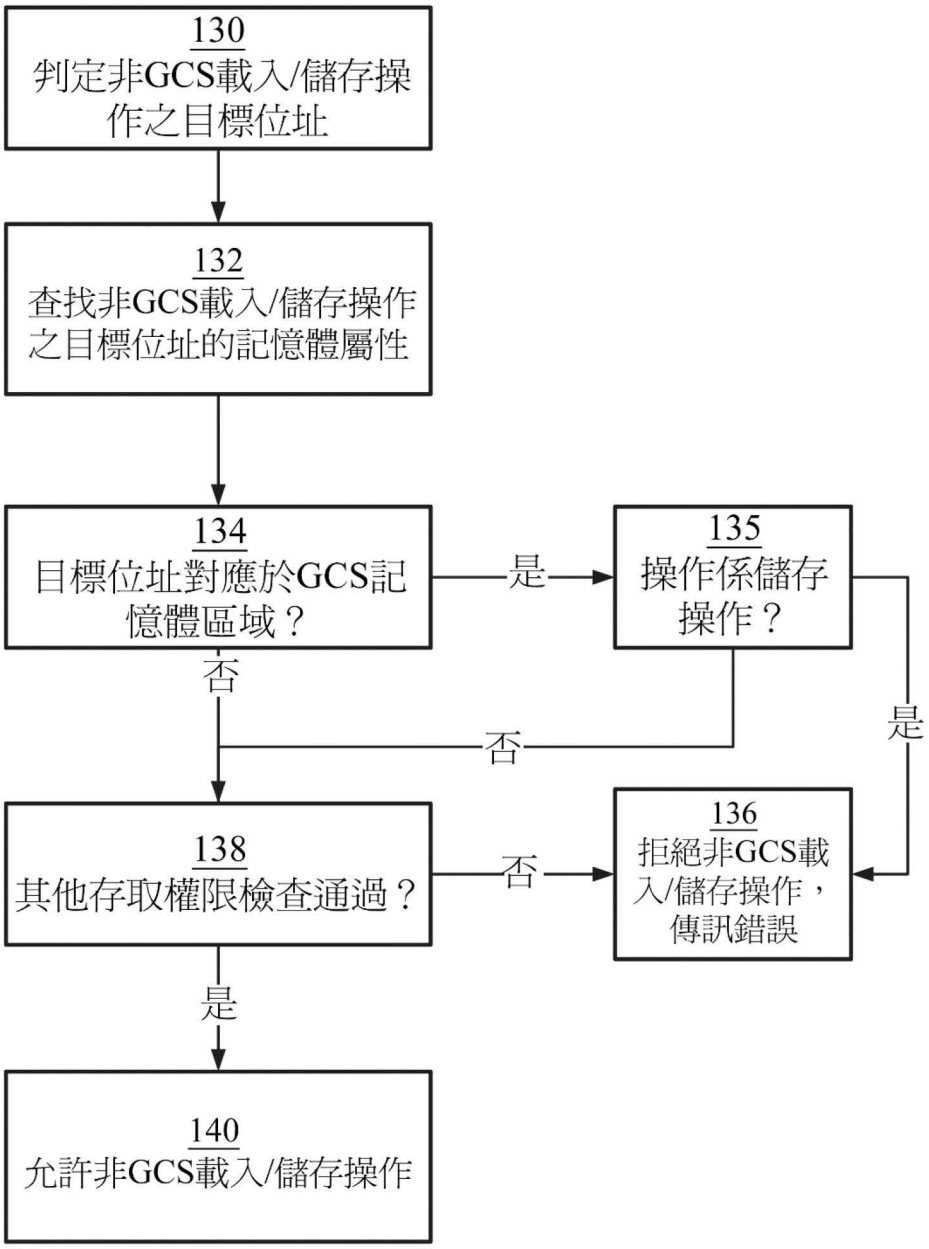
【圖3】

GCS載入/儲存操作的存取權限檢查

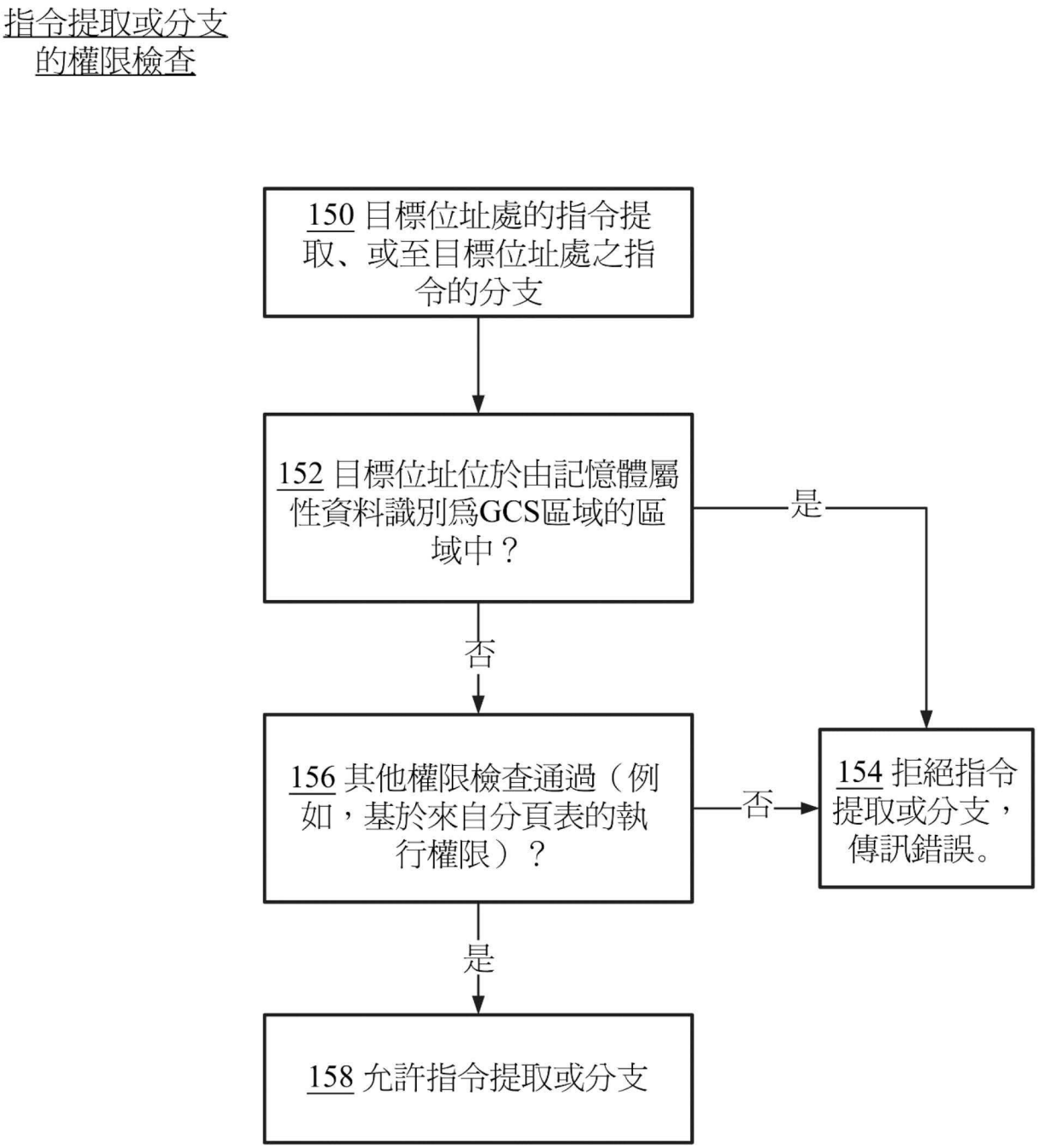


【圖4】

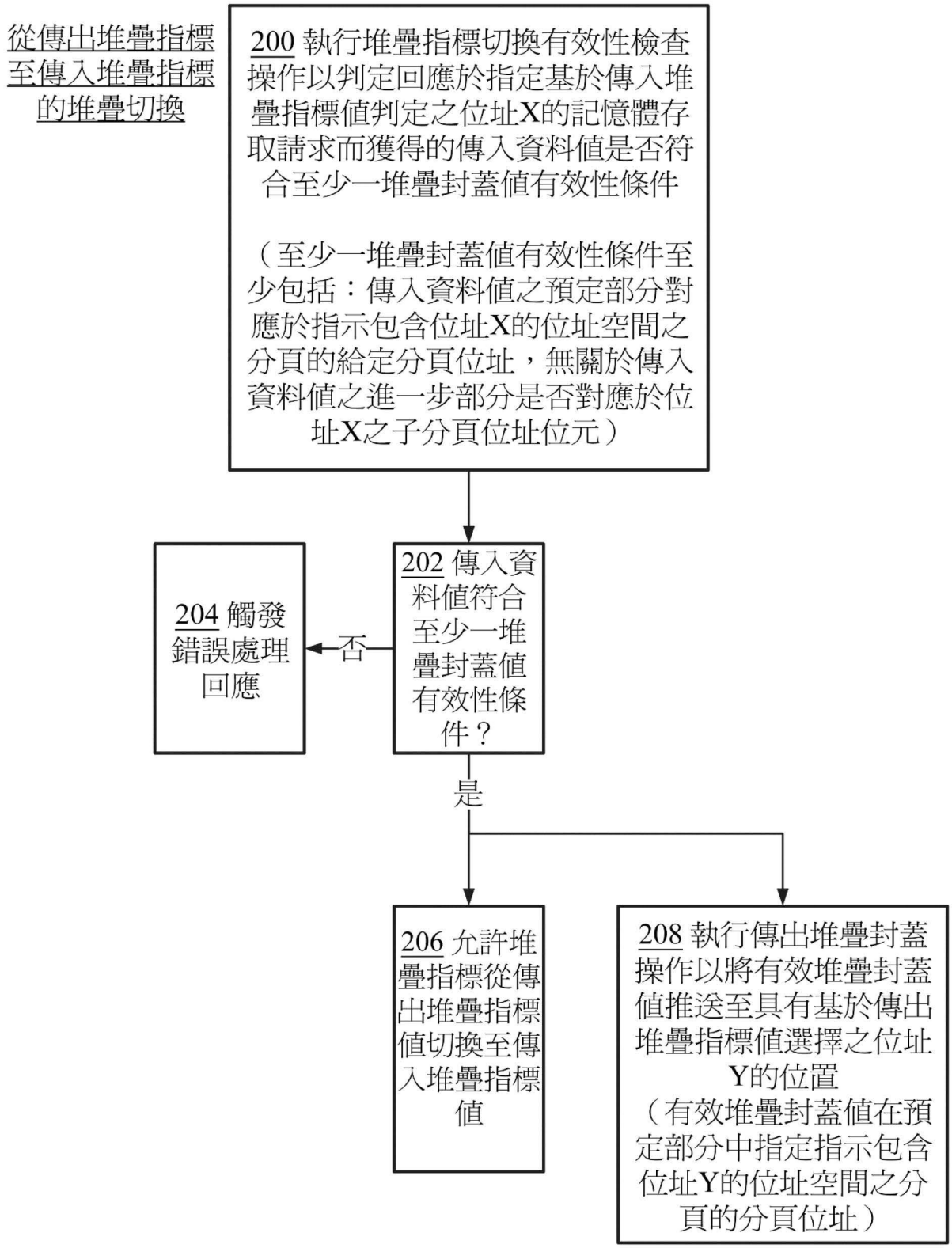
非GCS載入/儲存操作
的存取權限檢查



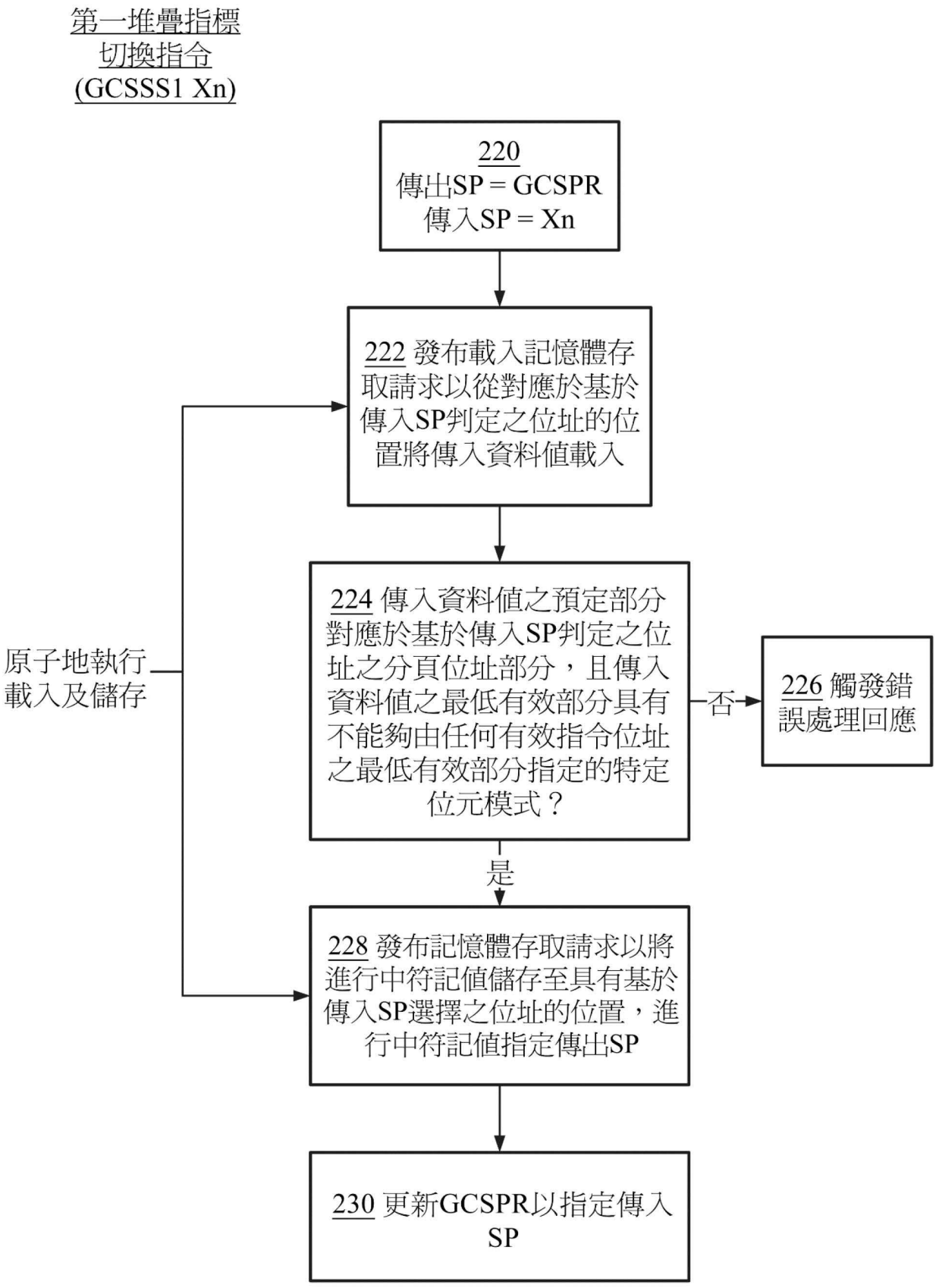
【圖5】


指令提取或分支的權限檢查
150 目標位址處的指令提取、或至目標位址處之指令的分支
152 目標位址位於由記憶體屬性資料識別爲GCS區域的區域中？
是
否
156 其他權限檢查通過（例如，基於來自分頁表的執行權限）？
否
154 拒絕指令提取或分支，傳訊錯誤。
是
158 允許指令提取或分支

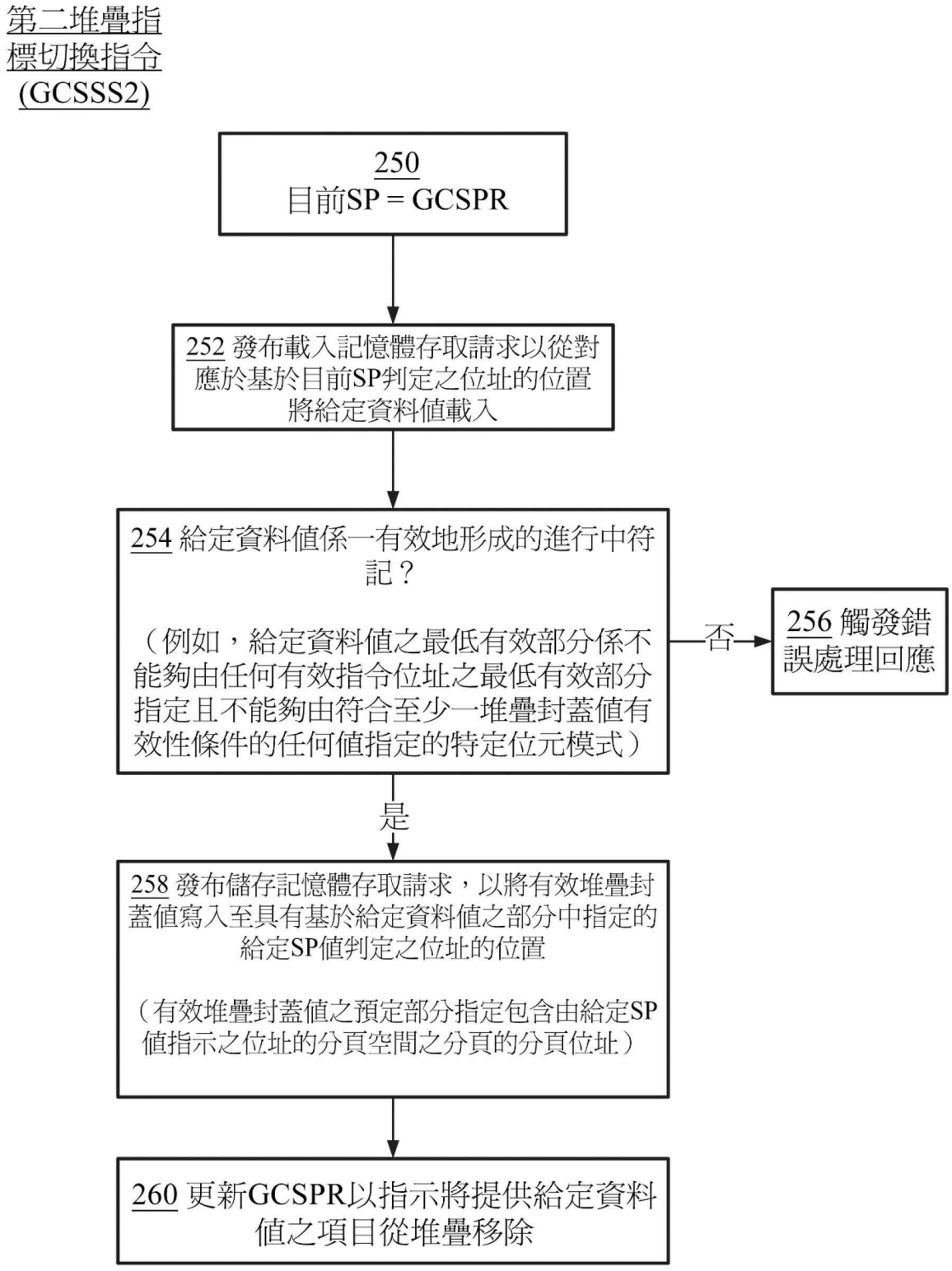
【圖6】


從傳出堆疊指標至傳入堆疊指標的堆疊切換
200 執行堆疊指標切換有效性檢查操作以判定回應於指定基於傳入堆疊指標值判定之位址X的記憶體存取請求而獲得的傳入資料值是否符合至少一堆疊封蓋值有效性條件
（至少一堆疊封蓋值有效性條件至少包括：傳入資料值之預定部分對應於指示包含位址X的位址空間之分頁的給定分頁位址，無關於傳入資料值之進一步部分是否對應於位址X之子分頁位址位元）
202 傳入資料值符合至少一堆疊封蓋值有效性條件？
否
204 觸發錯誤處理回應
是
206 允許堆疊指標從傳出堆疊指標值切換至傳入堆疊指標值
208 執行傳出堆疊封蓋操作以將有效堆疊封蓋值推送至具有基於傳出堆疊指標值選擇之位址Y的位置
（有效堆疊封蓋值在預定部分中指定指示包含位址Y的位址空間之分頁的分頁位址）

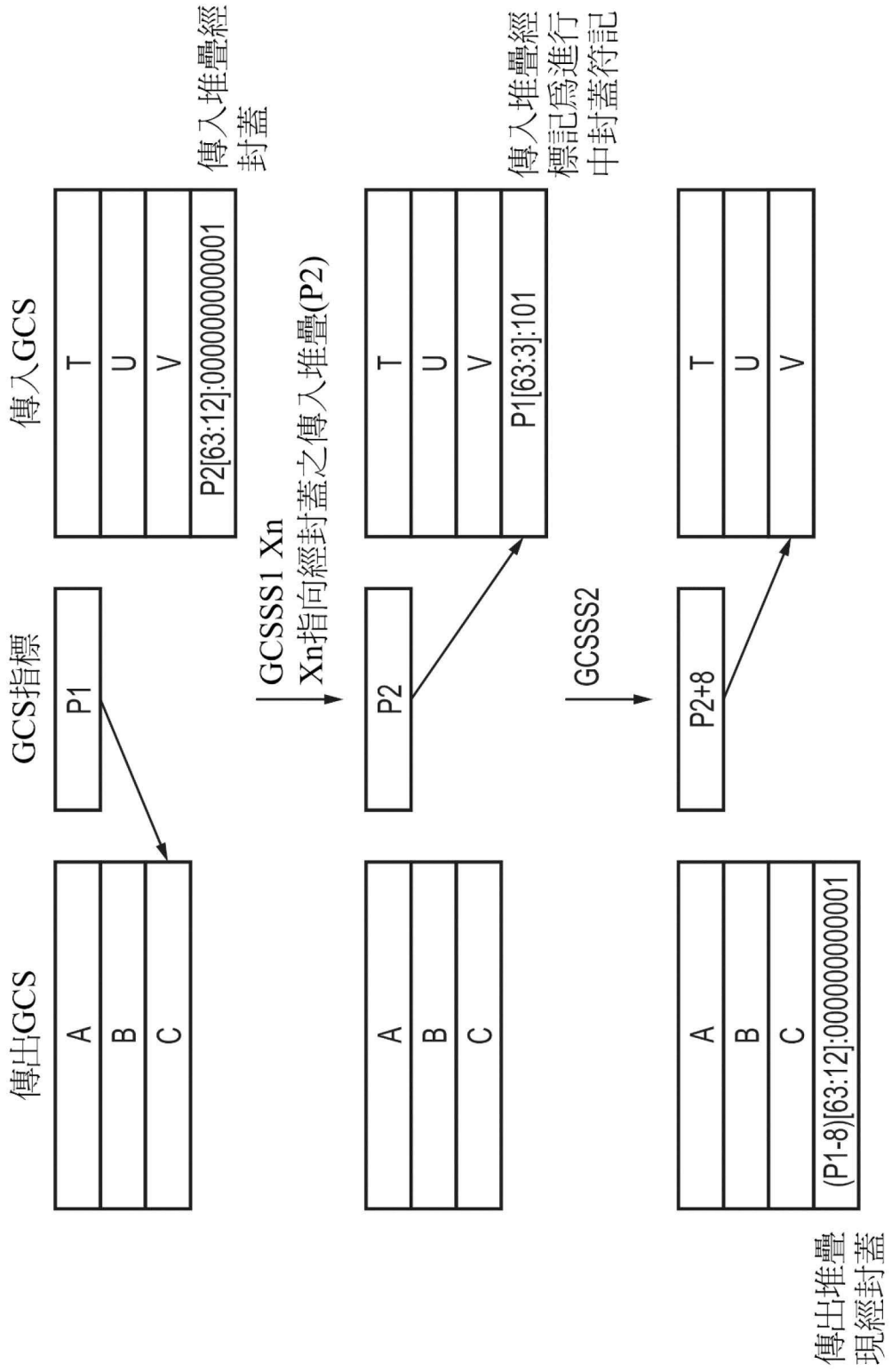
【圖7】


第一堆疊指標
切換指令
(GCSSS1 Xn)
220
傳出SP = GCSPR
傳入SP = Xn
222 發布載入記憶體存取請求以從對應於基於傳入SP判定之位址的位置將傳入資料值載入
224 傳入資料值之預定部分對應於基於傳入SP判定之位址之分頁位址部分，且傳入資料值之最低有效部分具有不能夠由任何有效指令位址之最低有效部分指定的特定位元模式？
否
226 觸發錯誤處理回應
是
228 發布記憶體存取請求以將進行中符記值儲存至具有基於傳入SP選擇之位址的位置，進行中符記值指定傳出SP
230 更新GCSPR以指定傳入SP
原子地執行載入及儲存

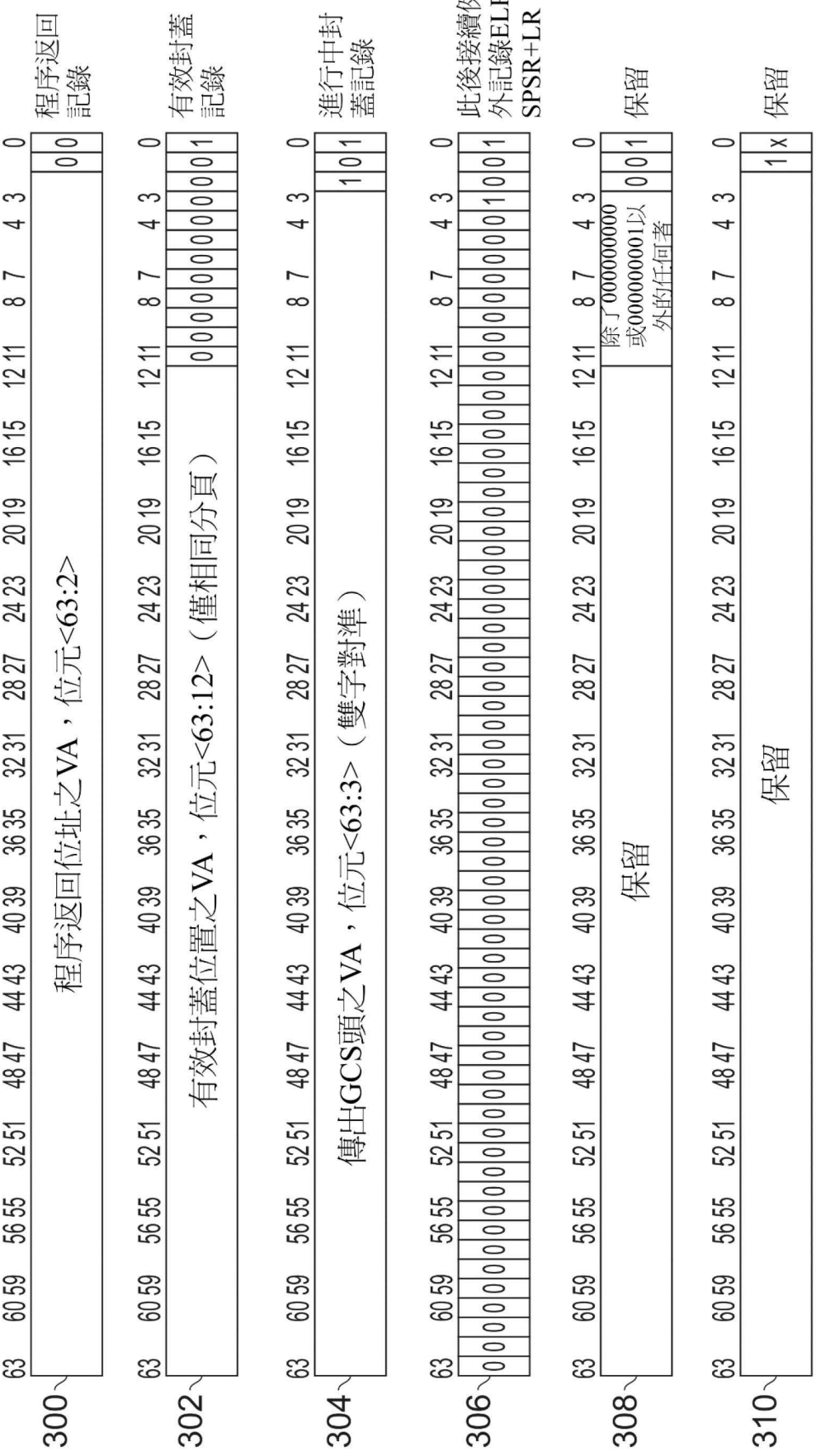
【圖8】


第二堆疊指標切換指令(GCSSS2)
250
目前SP = GCSPR
252 發布載入記憶體存取請求以從對應於基於目前SP判定之位址的位置將給定資料值載入
254 給定資料值係一有效地形成的進行中符記？
（例如，給定資料值之最低有效部分係不能夠由任何有效指令位址之最低有效部分指定且不能夠由符合至少一堆疊封蓋值有效性條件的任何值指定的特定位元模式）
否
256 觸發錯誤處理回應
是
258 發布儲存記憶體存取請求，以將有效堆疊封蓋值寫入至具有基於給定資料值之部分中指定的給定SP值判定之位址的位置
（有效堆疊封蓋值之預定部分指定包含由給定SP值指示之位址的分頁空間之分頁的分頁位址）
260 更新GCSPR以指示將提供給定資料值之項目從堆疊移除

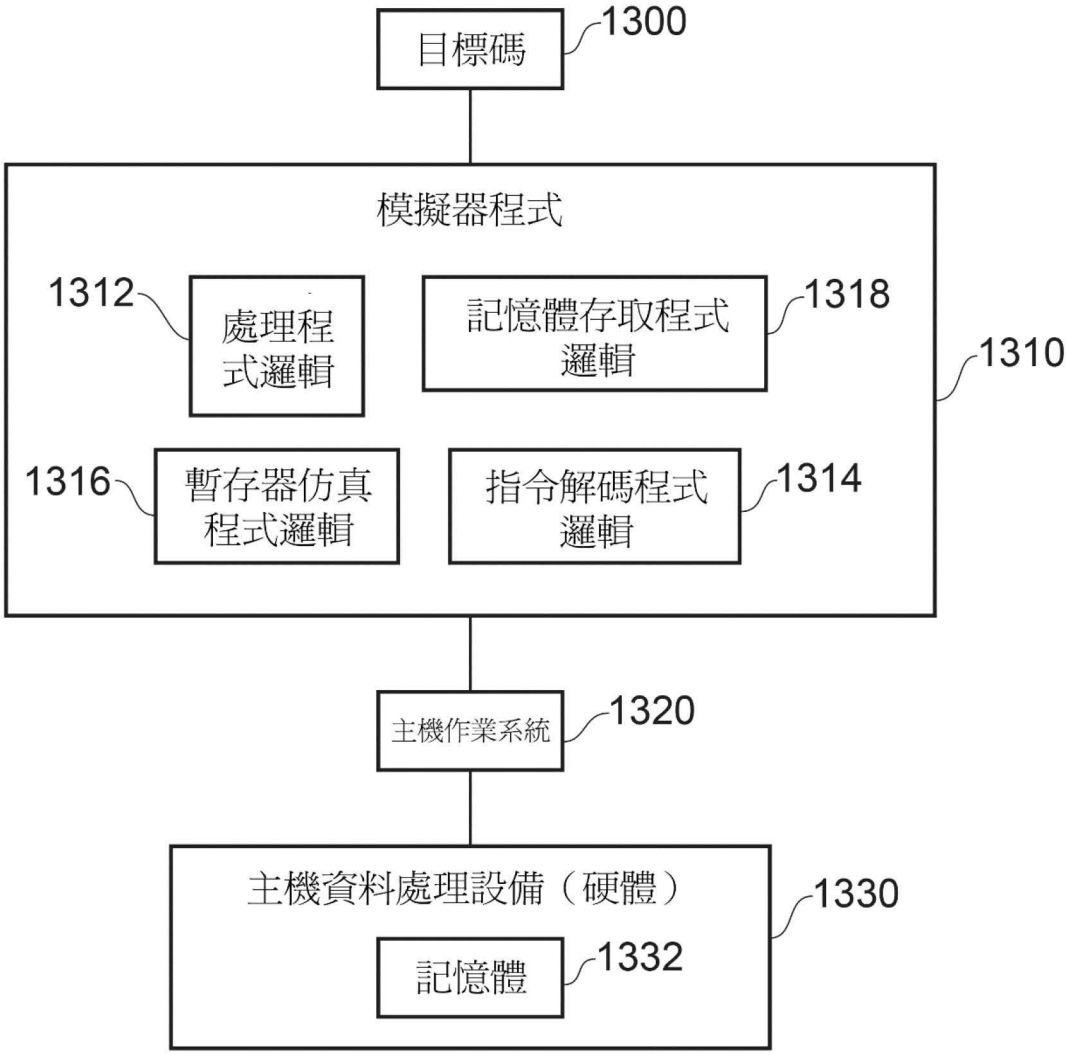
【圖9】


傳出GCS
GCS指標
傳入GCS
A
B
C
P1
T
U
V
P2[63:12]:000000000001
傳入堆疊經封蓋
GCSSS1 Xn
Xn指向經封蓋之傳入堆疊(P2)
P2
P1[63:3]:101
傳入堆疊經標記爲進行中封蓋符記
GCSSS2
P2+8
(P1-8)[63:12]:000000000001
傳出堆疊現經封蓋

【圖10】


63 60 59 56 55 52 51 48 47 44 43 40 39 36 35 32 31 28 27 24 23 20 19 16 15 12 11 8 7 4 3 0
300
程序返回位址之VA，位元<63:2>
0 0
程序返回記錄
302
有效封蓋位置之VA，位元<63:12>（僅相同分頁）
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1
有效封蓋記錄
304
傳出GCS頭之VA，位元<63:3>（雙字對準）
1 0 1
進行中封蓋記錄
306
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1
此後接續例外記錄ELR+SPSR+LR
308
保留
除了0000000000或0000000001以外的任何者
0 0 1
保留
310
保留
1 x
保留

【圖11】


目標碼
1300
模擬器程式
1312
處理程式邏輯
記憶體存取程式邏輯
1318
1310
1316
暫存器仿真程式邏輯
指令解碼程式邏輯
1314
主機作業系統
1320
主機資料處理設備（硬體）
1330
記憶體
1332

【圖12】