I746523

(19)中華民國智慧財產局

(12)發明說明書公告本 **(11)證書號數：TW I746523 B**

(45)公告日： 中華民國 110 (2021) 年 11 月 21 日

(21)申請案號：106106608 (22)申請日： 中華民國 106 (2017) 年 03 月 01 日

(51)Int. Cl.： ***G06F13/18 (2006.01)*** ***G06F12/02 (2006.01)***

G06F12/14 (2006.01)

(30)優先權：2016/03/02 英國 1603622.0

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

英國

(72)發明人：派克 傑森 PARKER, JASON (GB)

(74)代理人：李世章；彭國洋

(56)參考文獻：

TW	200844749A	TW	201207615A
TW	201320100A	TW	201502993A
US	2011/0052053A1	US	2011/0225402A1

審查人員：李惟任

申請專利範圍項數：項 圖式數： 共頁

(54)名稱

暫存器存取控制

(57)摘要

資料處理系統 2 在複數個異常位準 ELx 下操作並支援受保護執行環境的使用。暫存器組 16 含有具有指示擁有異常位準之關聯所有權變數的暫存器。暫存器存取控制電路 30 回應於各別暫存器之所有權值，以根據所有權值藉由處理電路 14 來控制存取該等暫存器。可提供目標受約束的資料傳輸操作及關聯程式指令，此些目標受約束的資料傳輸操作及關聯程式指令能夠存取不由與彼等程式指令之執行關聯之異常位準所擁有的暫存器中之資料值，但限於向或從記憶體 6 內之記憶體位址執行資料傳輸，該記憶體 6 內之記憶體位址藉由擁有異常位準之已架構儲存指標來指示。在給定異常位準下之目標無約束的傳輸指令不能存取暫存器資料值，該暫存器資料值經標記為藉由不同異常位準所有。

A data processing system 2 operates at a plurality of exception levels ELx and supports the use of protected execution environments. A register bank 16 contains registers having associated ownership variables indicating an owning exception level. Register access control circuitry 30 is responsive to the ownership values for respective registers to control access to those registers by processing circuitry 14 in dependence upon the ownership values. Target-constrained data transfer operations and associated program instructions may be provided which are able to access data values in registers not owned by the exception level associated with the execution of those program instructions, but are limited to perform data transfers to or from memory locations within a memory 6 indicated by an architected storage pointer for the owning exception level. Target-unconstrained transfer instructions at a given exception level are not able to access register data value marked as owned by a different exception level.

指定代表圖：

目標約束的加載/儲存指令

```
STR Blind [BRI]
        //由於BRI所有參數隱含
        data = GPR [BRI].Data
        bi = GPR [BRI].Owner              //哪個BDEC
        bp = BDEC [bi]                    // BDEC指標
        brp = bp [BRI]                    // BDEC 暫存器進入點
        STORE. bi data, brp               // 儲存至受保護區域
        (BRI++)                           // 可選的索引增量及旗標
                                            設定

LDR Blind [BRI, BTEL]
        // 將BTEL設定為更低異常位準
        bp = BDEC [BTEL]
        brp = bp [BRI]
        LOAD, BTEL data, brp              //自受保護區域加載
        GPR [BRI].Data = data
        GPR [BRI].Owner = BTEL
        (BRI–)                            // 可選的索引減量及旗標
                                            設定
```

第6圖

專利案號：106106608

公告本

申請日：

I746523

IPC分類：

【發明摘要】

【中文發明名稱】暫存器存取控制

【英文發明名稱】REGISTER ACCESS CONTROL

【中文】

資料處理系統2在複數個異常位準ELx下操作並支援受保護執行環境的使用。暫存器組16含有具有指示擁有異常位準之關聯所有權變數的暫存器。暫存器存取控制電路30回應於各別暫存器之所有權值，以根據所有權值藉由處理電路14來控制存取該等暫存器。可提供目標受約束的資料傳輸操作及關聯程式指令，此些目標受約束的資料傳輸操作及關聯程式指令能夠存取不由與彼等程式指令之執行關聯之異常位準所擁有的暫存器中之資料值，但限於向或從記憶體6內之記憶體位址執行資料傳輸，該記憶體6內之記憶體位址藉由擁有異常位準之已架構儲存指標來指示。在給定異常位準下之目標無約束的傳輸指令不能存取暫存器資料值，該暫存器資料值經標記為藉由不同異常位準所有。

【英文】

A data processing system 2 operates at a plurality of exception levels ELx and supports the use of protected execution environments. A register bank 16 contains registers having associated ownership variables indicating an owning exception level. Register access control circuitry 30 is responsive to the ownership values for respective registers to control access to those registers by processing circuitry 14 in dependence upon the ownership values. Target-constrained data transfer operations and associated program instructions may be provided which are able to access data values in registers

not owned by the exception level associated with the execution of those program instructions, but are limited to perform data transfers to or from memory locations within a memory 6 indicated by an architected storage pointer for the owning exception level. Target-unconstrained transfer instructions at a given exception level are not able to access register data value marked as owned by a different exception level.

【指定代表圖】第（ 6 ）圖。

【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】暫存器存取控制

【英文發明名稱】REGISTER ACCESS CONTROL

【技術領域】

【0001】 本揭示案係關於資料處理系統之領域。更特定而言，本揭示案係關於對在資料處理系統內儲存資料值之暫存器之存取控制。

【先前技術】

【0002】 眾所周知，提供具有儲存各別資料值之暫存器之資料處理系統，以用於藉由程式指令指定之資料處理操作。當回應於異常時，作為異常處理程式代碼之責任的部分，一些已知系統依賴異常處理代碼來保存暫存器之當前內容，並且在異常處理程式代碼執行結束時將該內容恢復至暫存器。

【發明內容】

【0003】 本揭示案之至少一些實施例提供用於處理資料之裝置，其包含：

複數個暫存器，用以保存各別資料值，該複數個暫存器之每一者具有關聯所有權變數；

處理電路，用以對在該複數個暫存器內保存之資料值執行藉由程式指令指定之資料處理操作；

暫存器存取控制電路，回應於藉由該複數個暫存器之一暫存器的該關聯所有權變數指定之所有權值，以根據該所有權值藉由該處理電路來控制存取該暫存器；以及

異常位準控制電路，用以控制該處理電路以在複數個異常位準中之當前異常位準中操作，其中

該所有權值指定該複數個異常位準狀態之一個，以及

該暫存器存取控制電路約束藉由該處理電路存取該暫存器，以當該當前異常位準以預定方式不同於藉由該所有權值指定之異常位準時，執行藉由至少一些程式指令指定之資料處理操作，以及

該複數個異常位準對應於自最低特權位準至最高特權位準延伸之特權位準之層次，異常情況在該處理電路之操作中出現，當在對應於低於該最高特權位準之特權位準的異常位準下操作時，觸發切換至具有更高特權位準之異常位準，以及

該預定方式為該當前異常位準在該層次中高於由該所有權值指定之異常位準，

其中該最低特權位準之特權低於最高特權位準。

【0004】 本揭示案之至少一些實施例提供了處理資料之方法，其包含以下步驟：

在複數個暫存器內保存各別資料值，該複數個暫存器之每一者具有關聯所有權變數；

對保存在該複數個暫存器內之資料值執行藉由程式指令指定之資料處理操作；

回應於藉由該複數個暫存器之一暫存器的該關聯所有權變數指定之所有權值，根據該所有權值藉由該處理電路來控制存取該暫存器，

控制該處理電路以在複數個異常位準中之當前異常位準中操作，其中該所有權值指定該複數個異常位準狀態之一個，以及

該方法進一步包含約束藉由該處理電路存取該暫存器，以當該當前異常位準以預定方式不同於藉由該所有權值指定之異常位準時，執行藉由至少一些程式指令指定之資料處理操作，以及

其中該複數個異常位準對應於自最低特權位準至最高特權位準延伸之特權位準之層次，異常情況在該處理電路之操作中出現，當在對應於低於該最高特權位準之特權位準的異常位準下操作時，觸發切換至具有更高特權位準之異常位準，以及

該預定方式為該當前異常位準在該層次中高於由該所有權值指定之異常位準，

其中該最低特權位準之特權低於最高特權位準。

【圖式簡單說明】

【0005】 現將參看附圖僅以實例之方式描述示例性實施例，其中：

【0006】 第1圖示意地圖示了包括複數個暫存器及暫存器存取控制電路之資料處理系統；

【0007】 第2圖示意地圖示了異常（特權）位準之層次及在彼等不同異常位準下運行之關聯程式；

【0008】 第3圖示意地圖示了暫存器及其關聯所有權值；

【0009】 第4圖示意地圖示了受保護執行環境上下文資料；

【0010】 第5圖示意地圖示了目標無約束的加載/儲存指令；

【0011】 第6圖示意地圖示了目標受約束的加載/儲存指令；

【0012】 第7A圖示意地圖示了與目標受約束的加載/儲存指令關聯使用之另外指令；

【0013】 第7B圖示意地圖示了暫存器保存及暫存器恢復代碼序列之實例；

【0014】 第8圖示意地圖示了巢套異常處理；

【0015】 第9圖為示意圖示異常進入之流程圖；以及

【0016】 第10圖為示意地圖示了異常返回之流程圖。

【實施方式】

【0017】 第1圖示意地圖示了包括耦接至記憶體6之處理器核心4的資料處理系統2。處理器核心4包括指令擷取單元8，指令擷取單元8自記憶體6擷取程式指令並供應該等程式指令至指令管線10。耦接至指令管線10之解碼器電路12解碼該等程式指令以產生控制訊號，該等控制訊號控制處理電路14以執行藉由解碼程式指令指定之資料處理操作。資料處理操作包括儲存在暫存器之暫存器組16內之資料值之操縱。在暫存器組16內之該等暫存器包括純量通用暫存器、浮點暫存器及配置暫存器。另外類型

之暫存器可能提供在其他實施例中，但並非所有實施例需要具有所有該等類型暫存器。

【0018】 加載儲存單元18在暫存器組16內之暫存器與記憶體6內之儲存位置之間執行資料值之資料傳輸操作。該等傳輸操作可產生自如下文進一步描述之受約束儲存指令、受約束加載指令、無約束儲存指令或無約束加載指令。

【0019】 資料處理系統2在給定時間內在複數個可能異常位準（特權位準）之一個中操作。對何者為當前異常位準及在異常位準之間之切換的控制藉由異常位準控制電路20來處理。一般而言，當在較高異常位準下操作時，對儲存在記憶體6內之資料值提供更大之存取權限。然而，本揭示案提供了受保護之執行上下文，其中當在該受保護之執行環境外部操作時，甚至當在更高異常位準（更高特權位準）下操作時，與該受保護之執行上下文關聯之資料的至少一些是不可存取的。

【0020】 在第1圖中圖示之記憶體6示出了複數個記憶體區域，該等記憶體區域具有與其關聯之不同存取約束。超管理器記憶體區域22為超管理器程式可存取的，但在更低異常位準（更低特權位準）下為程式不可存取的。當系統在第一受保護之執行上下文或第二受保護之執行上下文中操作時，分別可存取第一受保護區域24及第二受保護區域26，但在該等各別上下文外部不可存取。例如，第一受保護區域24當資料處理系統2在第一受保護之執

行上下文中操作時可存取，但當資料處理系統執行超管理器程式（儘管此可具有更高異常位準）時及當在第二受保護之執行上下文中執行時不可存取。共享區域28對超管理器程式及當在第一執行上下文及第二執行上下文中執行時都可存取，以便促進不同程式之間之資料值的共享。受保護執行環上下文之每一個可對應於各別受保護虛擬機執行環境之提供。受保護虛擬機執行環境藉由對其分配各別保護區域24、26可便於確保其資料為私密的，受保護虛擬機執行環境可將其私密資料儲存在受保護區域24、26中，使得其他私密虛擬機乃至超管理器程式不可存取該私密資料。

【0021】 處理器核心4包括耦接至暫存器組16之存取控制電路30。暫存器組16內之暫存器之每一個具有關聯所有權值。多個暫存器可共享所有權值，或在其他實施例中每個暫存器可具有個別可設定的所有權值。亦可能在一些實施例中，並非暫存器組16內之所有暫存器具有所有權值，或將參與在異常處理操作時保護其內容之機制，如下文將描述。

【0022】 暫存器存取控制電路用於根據所有權值控制存取暫存器組16內之暫存器，該所有權值根據藉由處理電路14或藉由加載儲存單元18存取之暫存器指定。若處理器核心4嘗試執行違反藉由所有權值指定之所有權約束的資料處理操作，則暫存器存取控制電路30產生暫存

器所有權異常，其可觸發諸如關閉受保護執行環境之動作，以作為避免進一步試圖破壞其安全性之保障。

【0023】 在本示例性實施例之上下文中，暫存器組內之暫存器指定之所有權值將複數個可能異常位準中之異常位準關聯為「擁有」相關暫存器之異常位準。自異常位準控制電路20供應異常位準訊號EL至暫存器存取控制電路30以指示資料處理系統2正在操作之當前異常位準。若暫存器存取控制電路30偵測到當前異常位準不同於記錄為待存取暫存器之當前所有者之異常位準，則觸發上述提及之暫存器所有權異常並不允許嘗試存取。儘管在當前示例性實施例中所有權值對應於擁有異常位準，但其他實施例可使用不同形式之所有權屬性，諸如基於執行緒所有權等是可能的。

【0024】 在一些實施例中，暫存器存取控制電路30可用以約束存取給定暫存器，以便僅當處理系統2當前處於與指示為擁有相關暫存器之異常位準相同的異常位準時允許存取。在其他實施例中，暫存器存取控制電路可用以當處理系統2處在與指示為當前所有者之異常位準相同之異常位準下時，或在更低（較少特權）異常位準下提供存取給定暫存器，儘管若資料處理系統2處在更高異常位準（更高特權位準）下不允許存取。這與正常模型相反，藉以更高特權位準提供更大之存取，但是當期望不允許超管理器程式具有存取權限時，其用於保護暫存器的內容遠離超管理器程式。該超管理器程式可稱為「盲」超管理器

程式，儘管允許在更低異常位準下在受保護執行環境中排程處理操作，但不能存取與彼等受保護執行環境關聯之私密資料，因為該資料儲存在藉由各別受保護執行環境設立及「擁有」之受保護區域24、受保護區域26內。

【0025】 第2圖示意地圖示了在各別異常位準下執行之複數個程式。在第2圖之實例中，超管理器程式32在異常位準EL2下執行。此異常位準具有高於亦在第2圖中圖示之異常位準EL1、異常位準EL0之更高特權位準。超管理器程式32管理在兩個受保護執行環境34、36中執行之排程。該等受保護執行環境34、36之每一個包括在異常位準EL1下執行之各別作業系統38、40及在異常位準EL0下執行之一或多個應用程式42、44、46。受保護執行環境34、36之每一個提供虛擬機執行環境，其能夠在記憶體6中設立其自身受保護區域24、26，在受保護區域24、26中其可儲存受保護免於被超管理器程式32存取之私密資料。若在受保護執行環境32、36內執行之程式希望與超管理器程式22或與其他程式諸如在其他受保護執行環境34、36中執行之程式共享資料，則亦可將該資料儲存在共享區域28內。

【0026】 第3圖示意地圖示了例如可在暫存器組16內找到之儲存64位元資料值之64位元通用暫存器48。與此暫存器48關聯的為指示擁有暫存器48內之資料值之異常位準ELx的2位元所有權值。所有權有效位元指示所有權值ELx在給定時間內是否為有效的。當對暫存器48內之

資料值進行存取時，則暫存器存取控制電路30讀取當前所有權值ELx並將其與資料處理系統2之當前異常位準比較，資料處理系統2藉由異常位準控制電路20供應，以決定是否應當允許相關存取(例如資料處理系統之當前異常位準等於或低於藉由所有權值ELx指示之異常位準)。

【0027】 第4圖示意地圖示了受保護執行環境上下文資料，該受保護執行環境上下文資料至少當該受保護執行環境當前不在執行時儲存在受保護執行環境自身的受保護區域24、26內，例如當異常發生並正由在受保護執行環境外執行之異常處理程式處理時，例如異常處理程式正在更高異常位準下執行時如此。如上述所提及，在此示例性實施例中，基於每個異常位準來處理暫存器值之所有權並因此將儲存指標(用於加載及儲存兩者)提供為與每一個異常位準關聯之已架構狀態暫存器。儲存指標為僅藉由下文描述之目標約束指令正常地存取且並不為通用暫存器組之部分的額外暫存器。此儲存指標指示受保護執行環境之受保護區域24、26內之起始位址，在受保護執行環境中儲存其64位元上下文資料陣列。此上下文資料包括當停止執行此上下文時，諸如當出現異常時從由關聯上下文所有之暫存器組16讀取之儲存資料值塊50。索引值與每個異常位準之儲存指標關聯並指示64位元陣列內之具體位置，該64位元陣列儲存給定暫存器Rx之對應資料值。其他配置暫存器狀態資料亦可能儲存在64位元陣列內。

【0028】 當異常發生導致離開受保護執行環境時，異常處理代碼之職責為經調用以儲存暫存器組16之當前內容，以便該等當前內容能夠在控制返回至原始受保護執行環境之前於其處理結束時藉由異常處理程式恢復。藉由與異常位準關聯之儲存指標指示之64位元陣列（該異常位準擁有暫存器組16內之特定暫存器資料值），用以直接將資料值保存至儲存在記憶體6內之各別受保護區域24、26內之適宜64位元陣列中。

【0029】 第5圖示意地圖示了目標無約束的加載及儲存指令。該等指令能夠自由地定義記憶體6內之位址，以常規方式使用記憶體6進行傳輸。若該目標無約束的加載及儲存指令用於自與受保護執行環境關聯之暫存器儲存及恢復資料值，則它們可允許該等資料值儲存在適宜受保護區域24、26之外部，並因此在關聯受保護執行環境之外部變得不適當地可用。

【0030】 本揭示案提供如第6圖圖示之目標受約束的加載及儲存指令，該等指令藉由解碼器電路12解碼並控制加載/儲存單元18，以對藉由關於第4圖論述之暫存器之擁有異常位準的儲存指標指定之位置使用記憶體6執行目標受約束的資料傳輸操作。該等目標受約束的加載及儲存指令具有STRBlind指令及LDRBlind指令之形式。該等指令當藉由解碼器電路12解碼時用於控制加載/儲存單元18及處理核心4之其他部分，以執行在第6圖中圖示之偽代碼中指定之處理操作。

【0031】 在目標受約束的儲存指令STRBlind之情況下，此用以將來自藉由暫存器索引變數BRI之當前值指示之通用暫存器的資料儲存至記憶體位置中，該記憶體位置藉由與64位元陣列50之開始關聯之擁有異常位準之儲存指標及當前暫存器值BRI之組合指示。索引值可在執行具有設定之旗標之目標受約束的儲存指令結束時選擇性地增加（若該索引值上溢或下溢出其最大值或最小值，該最大值或最小值指示已完成之暫存器儲存操作之序列）。

【0032】 應理解，在給定時間點下，暫存器組16內之暫存器可藉由其所有權值標記為具有不同各別擁有異常位準是可能的。此情況可發生，例如係因為巢套中斷之發生，其中部分地保存暫存器組之當前內容，並藉由新異常位準主張所有權，當另一異常發生時，其本身獲得暫存器組之暫存器之所有權，並因此應當將暫存器組16之內容保存至其當前所有權值所指示之適宜的受保護區域24、26中。自目標受約束的儲存指令之操作之偽代碼表示可見，此指令遵循之參數為暫存器索引值BRI及識別給定暫存器之特定所有者之所執行操作（bi值），關聯受保護上下文資料陣列之儲存指標（bp值）及用於自暫存器保存之資料值之個別儲存位置（brp值）根據待保存之暫存器之當前所有權值全部動態地導出。

【0033】 第6圖中圖示之目標受約束的加載指令LDRBlind採取暫存器索引BRI及目標異常位準BTEL兩者作為輸入運算元。處理所返回之目標異常位準

BTEL，及因此自適宜受保護區域24、26恢復之暫存器組16之關聯資料值藉由異常處理代碼設定，因為其對在異常處理之後處理返回至哪個異常位準處理之控制負責。圖示目標受約束的加載指令之功能之偽代碼亦指示在執行給定暫存器索引值BRI之該加載之結束時，若其如上文論述上溢，則暫存器索引值可視情況減小，並設定旗標。

【0034】 當進入異常時，異常處理代碼用以執行遵循暫存器索引值BRI之序列之目標受約束的儲存指令STRBlind之序列，以便將暫存器組16之當前內容保存至適宜的受保護區域24、26。在保存具有STRBlind指令之暫存器內容之後，可將暫存器設定為預定值，例如零。當完成異常處理時及在處理返回至目標異常位準之前，異常處理程式對執行目標受約束的加載指令LDRBlind之序列負責，該目標受約束的加載指令LDRBlind用以將儲存在目標執行位準之各別受保護區域24、26之受保護上下文資料陣列內的資料值加載回至暫存器組16，使得所返回之受保護執行環境可重新開始其處理。

【0035】 允許目標受約束的加載及儲存指令STRBlind及LRDBlind存取與不由執行彼等目標受約束的加載及儲存指令的異常位準所擁有之暫存器關聯之資料值，但服從約束，即傳輸進出記憶體6發生在一位置處，該位置藉由與擁有相關暫存器值（以及如上文論述之當前索引值）的異常位準關聯之儲存指標指定。相反，第

5圖之目標無約束的加載及儲存指令不能夠存取暫存器內之資料值，該暫存器不由執行彼等目標無約束的加載及儲存指令的異常位準所擁有。

【0036】 第7A圖示意地圖示了藉由解碼器電路12解碼並與目標受約束的加載及儲存指令關聯使用之三個另外程式指令之操作，以及執行盲暫存器保存之異常處理及執行盲暫存器恢復之異常返回之實例。

【0037】 索引重設程式指令ResetBRI藉由解碼器電路12解碼並控制處理電路14以重設索引值BRI至零值（其他實施例可使用不同重設值）。改變程式指令IncrementBRI之索引用以改變當前暫存器索引值BRI，以便遵循索引值之預定序列。在此實例中，此序列以單調遞增序列自零開始至高達對應於暫存器組16內之暫存器之數目之最大數，該暫存器組16之暫存器之數目需要使用目標受約束的加載及儲存指令來保存。應理解，可使用暫存器索引值之其他序列，諸如單調遞減暫存器索引值。另外實施例可使用非典型之索引值之序列，但在資料處理系統2之正常操作期間遵循暫存器組16內之對應暫存器之使用的遞減統計頻率之順序。以此種方式，藉由遵循此序列保存或恢復暫存器組16內之第一暫存器為具有最高使用可能性之彼等暫存器。可能異常處理常式將僅用以正常地保存暫存器組內容之部分以便釋放暫存器供其自身異常處理使用，並在需要額外暫存器空間時使得可保存其他暫存器。以此種方式，先保存或恢復最經常使用

之暫存器之序列用於為異常處理程式代碼提供其最可能需要使用之暫存器，而不必保存暫存器組之全部內容。

【0038】 如上文所提及，當異常處理程式將處理返回至遵循異常處理之程式時，其將目標異常位準設定為與使用第6圖之目標受約束的加載指令恢復暫存器組內容關聯。解碼器電路12回應於目標所有者設定程式指令SetBTEL以設定待恢復之目標異常位準。目標異常位準限於低於執行目標所有者設定程式指令(SetBTEL)之當前異常位準。

【0039】 第7B圖圖示了異常處理盲暫存器保存常式。代碼部分意圖在異常處理程式常式之開始時或接近開始時執行。在一些實施例中圖示之代碼當自受保護執行環境進入時儲存在待處理之異常之目標向量位置處。保存常式之盲暫存器開始於重設暫存器索引值及隨後以增量暫存器索引值執行之目標受約束的儲存指令直到上溢指示完成此序列。在圖示之實例中，藉由目標受約束的儲存指令本身執行索引值之改變，而不是使用改變程式指令之獨立索引。

【0040】 在一些示例性實施例中，可將儲存序列完成標記值儲存在64位元陣列50內以形成受保護執行環境上下文資料。儲存序列完成標記值可用以指示來自暫存器組16之完整資料值集，該待儲存之全部資料值集事實上已經儲存在64位元陣列內。在第7B圖中圖示之異常處理盲暫存器保存程式可在其結束時包括為獨立指令，或在來自

目標受約束的儲存指令之溢出動作內隱含將儲存序列完成標記值儲存在64位元陣列50之動作。可以在異常返回時讀取此儲存序列完成標記值，該異常返回執行盲暫存器恢復以驗證全部資料值集正被恢復到目標異常位準，即，當剩餘異常位準時正確地保存全部集，且因此在此點處恢復全部資料值集是正確的。若全部集不可恢復，則可產生異常來指示未遵循正常行為。目標受約束的加載操作可在其被允許繼續之前檢查該儲存序列完成標記值是否存在。第7B圖圖示之異常返回盲暫存器恢復程式序列開始於目標所有者設定程式指令之執行以識別該異常位準之資料值將恢復至暫存器組16的目標異常位準。此暫存器索引值隨後藉由索引重設程式指令來重設。此後，對暫存器索引值序列執行循環，以自藉由用於目標異常位準之儲存指標和暫存器索引值之當前值指示之記憶體位址執行約束加載操作，直到暫存器索引值達到由溢出指示之序列末端。

【0041】 應理解，一些已知系統可當進入異常時自動保存暫存器。本文描述之機制提供更有效之方法，例如其不一定當進入異常時保存及恢復所有暫存器，因為異常處理可能僅需要使得暫存器之適當子集可供自己使用。

【0042】 第8圖示意地圖示了當巢套異常發生時執行暫存器保存之操作。資料處理系統2開始時在異常位準EL0處操作。在步驟1異常發生，使得資料處理系統進入異常位準EL1。在異常位準EL1執行之異常處理程式隨

後開始保存來自異常位準EL0所有之暫存器組16之資料值至與異常位準EL0關聯之受保護區域24、26中。此藉由第8圖中之步驟2圖示。在步驟2保存藉由異常位準EL0所有之資料值的半程中，出現由步驟3指示之另一異常，其將資料處理系統2從在異常位準EL1處執行變化至在異常位準EL2處執行。在異常位準EL2之異常處理程式代碼隨後開始保存來自暫存器組16之資料值並再次從暫存器索引值之序列之開始處開始。此藉由步驟4指示。待保存之資料值之第一部分對應於已經保存且在異常位準EL1執行之異常處理程式所主張之暫存器。藉由步驟5指示的待保存之資料值之第二部分為與異常位準EL0關聯之資料值之剩餘部分，且並未藉由異常位準EL1之異常處理程式保存。在結束保存來自暫存器之資料值時，所有暫存器標記有所有權值，該所有權值指示暫存器由異常位準EL2所擁有。

【0043】 當每個資料值藉由約束儲存指令保存為異常處理之部分時，使用對應於執行約束儲存指令執行之異常位準之所有權值設定暫存器之新所有者。從而，當所有資料值自暫存器組16保存至適宜的受保護區域24、26時，所有暫存器將標記為由異常位準EL2所擁有。

【0044】 可見，與暫存器組16內之暫存器關聯之所有權值藉由約束儲存指令來設定，該約束儲存指令保存之前資料值並主張它們當前異常位準之暫存器之所有權。所有權值藉由受約束加載指令返回至其原始值，該受約束加載

指令將所有權值設定為該等受約束加載指令之關聯目標異常位準。

【0045】 一旦來自暫存器組16之資料值之保存已藉由異常位準EL2之異常處理器完成，則可執行異常位準EL2之異常處理之剩餘部分。當此完成時，異常處理程式可將處理返回至異常位準EL1之異常處理器，以及將此資料值恢復至與退出時異常位準EL1所關聯之暫存器。

【0046】 第9圖為示意地圖示了當進入異常時處理之流程圖。在步驟52處理等到偵測到異常。在步驟54，資料處理系統2正在操作之異常位準藉由異常位準控制電路20來增加。在步驟56，判定之前使用的處理是否為受保護執行環境之一部分。若中斷之執行為受保護執行環境之部分，則處理按照與受保護執行環境之中斷關聯之異常向量指導進行至步驟58，以便可執行在第7圖中圖示之盲暫存器保存序列。若此中斷處理不來自受保護執行環境，則處理進行至步驟60，在步驟60來自暫存器之資料值可藉由異常處理代碼以常規方式儲存至堆疊記憶體。在步驟58或步驟60之後，處理進行至步驟62，在步驟62執行另外的異常處理。

【0047】 第10圖為示意地圖示了異常返回之流程圖。在步驟64，處理等到期望異常返回。步驟66隨後決定進入彼異常是否來自在受保護執行環境中執行之處理。若進入來自於受保護執行環境，則處理進行至步驟68，在步驟68，執行第7圖之盲暫存器恢復操作。若進入不來自受

保護執行環境，則處理進行至步驟70，在步驟70，暫存器內容以常規方式自堆疊記憶體恢復。在步驟68或步驟70之後，處理進行至步驟72，在步驟72，資料處理系統2之異常位準切換至正返回到之目標異常位準。步驟74隨後在目標異常位準處重新開始處理。

【0048】 儘管本揭示案已參考所附圖式詳細地描述本發明之說明性實施例，但應理解，本揭示案並不限於彼等精確實施例且熟習此項技術者可在不背離如隨附申請專利範圍所定義之本揭示案之範疇及精神之情況下在其中實施各種改變及修改。例如，可以進行附屬項之特徵與獨立項的特徵之各種組合。

【符號說明】

【0049】

2 資料處理系統

4 處理器核心

6 記憶體

8 指令擷取單元

10 指令管線

12 解碼器電路

14 處理電路

16 暫存器組

18 加載儲存單元

20 異常位準控制電路

22 超管理器記憶體區域

24 第一受保護區域

26 第二受保護區域

28 共享區域

30 存取控制電路

32 超管理器程式

34 受保護執行環境

36 受保護執行環境

38 作業系統

40 作業系統

42 應用程式

44 應用程式

46 應用程式

48 64位元通用暫存器

50 儲存資料值塊/64位元陣列

52 步驟

54 步驟

56 步驟

58 步驟

60 步驟

62 步驟

64 步驟

66 步驟

68 步驟

70 步驟

72 步驟

74 步驟

【生物材料寄存】

無

【序列表】(請換頁單獨記載)

無

【發明申請專利範圍】

【第1項】 一種用於處理資料之裝置，其包含：

複數個暫存器，用以保存各別資料值，該複數個暫存器之每一者具有一關聯所有權變數；

處理電路，用以對保存在該複數個暫存器內之資料值執行藉由程式指令指定之資料處理操作；

暫存器存取控制電路，用以回應於藉由該複數個暫存器之一暫存器之該關聯所有權變數指定的一所有權值，根據該所有權值藉由該處理電路來控制存取該暫存器；以及

異常位準控制電路，用以控制該處理電路以在複數個異常位準中間之一當前異常位準中操作，其中

該所有權值指定該複數個異常位準狀態之一個，以及

該暫存器存取控制電路約束藉由該處理電路存取該暫存器，以當該當前異常位準以一預定方式不同於藉由該所有權值指定之異常位準時，執行藉由至少一些程式指令指定之資料處理操作，以及

該複數個異常位準對應於自一最低特權位準至一最高特權位準延伸之特權位準之一層次，一異常情況在該處理電路之操作中出現，當在對應於低於該最高特權位準之一特權位準的一異常位準下操作時，觸發一

切換至具有一更高特權位準之一異常位準，以及

該預定方式為該當前異常位準在該層次中高於藉由該所有權值指定之一異常位準，

其中該最低特權位準之特權低於該最高特權位準。

【第2項】 如請求項 1 所述之裝置，其中該所有權值具有一儲存指標且該暫存器存取控制電路允許該處理電路回應於目標受約束的資料傳輸程式指令而在該暫存器與一記憶體內藉由該儲存指標指定之一目標記憶體位址之間執行目標受約束的資料傳輸操作。

【第3項】 如請求項 2 所述之裝置，其中該暫存器存取控制電路阻止該處理電路回應於目標無約束的資料傳輸程式指令而在該暫存器與該記憶體內並非藉由該儲存指標指定之一目標記憶體位址之間執行目標無約束的資料傳輸操作。

【第4項】 如請求項 2 所述之裝置，其中

該所有權值及該儲存指標與該處理電路之一受保護執行上下文關聯，

該受保護執行上下文具有該記憶體內之一受保護儲存區域，以及

該受保護儲存區域除了當在該受保護執行上下文中操作時藉由該處理電路及藉由回應於該目標受約束的資料傳輸程式指令執行之該目標受約束的資料傳輸操

作之外是不可存取的。

【第5項】 如請求項 4 所述之裝置，其中藉由該儲存指標指定之該目標記憶體位址在該受保護儲存區域內。

【第6項】 如請求項 2 所述之裝置，其中該儲存指標具有一關聯暫存器索引值，其與該儲存指標組合使用以指定該目標受約束的資料傳輸操作之該目標記憶體位址。

【第7項】 如請求項 6 所述之裝置，其中該暫存器索引值為索引值之一序列之部分，該等索引值包括用於指定該目標記憶體位址之一索引值，該目標記憶體位址用於該複數個暫存器之每一個。

【第8項】 如請求項 7 所述之裝置，其中該處理電路回應於一索引重設程式指令以將該索引值設定為該序列內之一起始值。

【第9項】 如請求項 7 所述之裝置，其中該處理電路回應於一索引變化程式指令以將該索引值設定為該序列內之一下一個索引值。

【第10項】 如請求項 7 所述之裝置，其中該複數個暫存器之每一個具有一各別暫存器號，並對應於以下各者之一個以一單調順序遍歷索引值之該序列：

以一單調順序遍歷該等暫存器號；以及

在該裝置之操作期間以對應於減少該複數個暫存器

內之對應暫存器之使用的統計頻率之順序遍歷該等暫存器號。

【第11項】 如請求項2所述之裝置，其中當該目標受約束的資料傳輸操作為儲存該暫存器內之一資料值至該目標記憶體位址之一目標受約束的儲存操作時，該處理電路使用該暫存器之該所有權值以識別用於指定該目標記憶體位址之該儲存指標。

【第12項】 如請求項11所述之裝置，其中該目標受約束的儲存操作儲存一預定值至該暫存器並設定該暫存器之該所有權值以匹配該處理電路之一當前狀態。

【第13項】 如請求項11所述之裝置，其中當該目標受約束的儲存操作執行該序列內之一最後暫存器索引值之一儲存時，儲存一儲存序列完成標記值。

【第14項】 如請求項2所述之裝置，其中當該目標受約束的資料傳輸操作為自該目標記憶體位址加載一資料值至該暫存器之一目標受約束的加載操作時，該處理電路使用一目標所有者變數以識別用於指定該目標記憶體位址之該儲存指標。

【第15項】 如請求項14所述之裝置，其中該目標受約束的加載操作在將該資料值加載至該暫存器之前檢驗該儲存序列完成標記值之存在。

【第16項】 如請求項14所述之裝置，其中該目標受約

束的資料傳輸操作亦將該暫存器索引值設定為該序列內之一下一個暫存器索引值。

【第17項】 如請求項16所述之裝置，其中該處理電路回應於一目標所有者設定程式指令，以將該目標所有者變數設定為對應於低於該當前異常位準之特權位準之一指定異常位準。

【第18項】 如請求項1所述之裝置，其中具有低於該最高特權位準之一特權位準之該異常位準的每一個為一受保護執行上下文提供支援，該受保護執行上下文對應於該複數個暫存器內之暫存器之一所有者。

【第19項】 如請求項1所述之裝置，其中當該暫存器存取控制電路偵測藉由該處理電路之一嘗試執行對具有該處理電路之一狀態之該暫存器的一存取，該處理電路之該狀態與該所有權值不匹配，該暫存器存取控制電路觸發一暫存器所有權異常。

【第20項】 如請求項1所述之裝置，其中該複數個暫存器包含以下各者之一或多個：

純量通用暫存器；

浮點暫存器；以及

配置暫存器。

【第21項】 一種處理資料之方法，其包含以下步驟：

在複數個暫存器內保存各別資料值，該複數個暫存

器之每一者具有一關聯所有權變數；

對保存在該複數個暫存器內之資料值執行藉由程式指令指定之資料處理操作；

回應於藉由該複數個暫存器之一暫存器之該關聯所有權變數指定的一所有權值，根據該所有權值藉由該處理電路來控制存取該暫存器，

控制該處理電路以在複數個異常位準中間之一當前異常位準中操作，其中該所有權值指定該複數個異常位準狀態之一個，以及

該方法進一步包含限制藉由該處理電路存取該暫存器，以當該當前異常位準以一預定方式不同於藉由該所有權值指定之異常位準時，執行藉由至少一些程式指令指定之資料處理操作，以及

其中該複數個異常位準對應於自一最低特權位準至一最高特權位準延伸之特權位準之一層次，一異常情況在該處理電路之操作中出現，當在對應於低於該最高特權位準之一特權位準的一異常位準下操作時，觸發一切換至具有一更高特權位準之一異常，以及

該預定方式為該當前異常位準在該層次中高於藉由該所有權值指定之一異常位準，

其中該最低特權位準之特權低於該最高特權位準。

【第22項】 如請求項21所述之方法，其中

該所有權值具有一關聯儲存指標，

該控制允許回應於目標受約束的資料傳輸程式指令而在該暫存器與一記憶體內藉由該儲存指標指定之一目標記憶體位址之間執行目標受約束的資料傳輸操作；

該所有權值及該儲存指標與一受保護執行上下文關聯，

該受保護執行上下文具有一記憶體內之一受保護儲存區域，以及

該受保護儲存區域除了當在該受保護執行上下文中操作時藉由該處理電路及藉由回應於該目標受約束的資料傳輸程式指令執行之該目標受約束的資料傳輸操作之外是不可存取的。

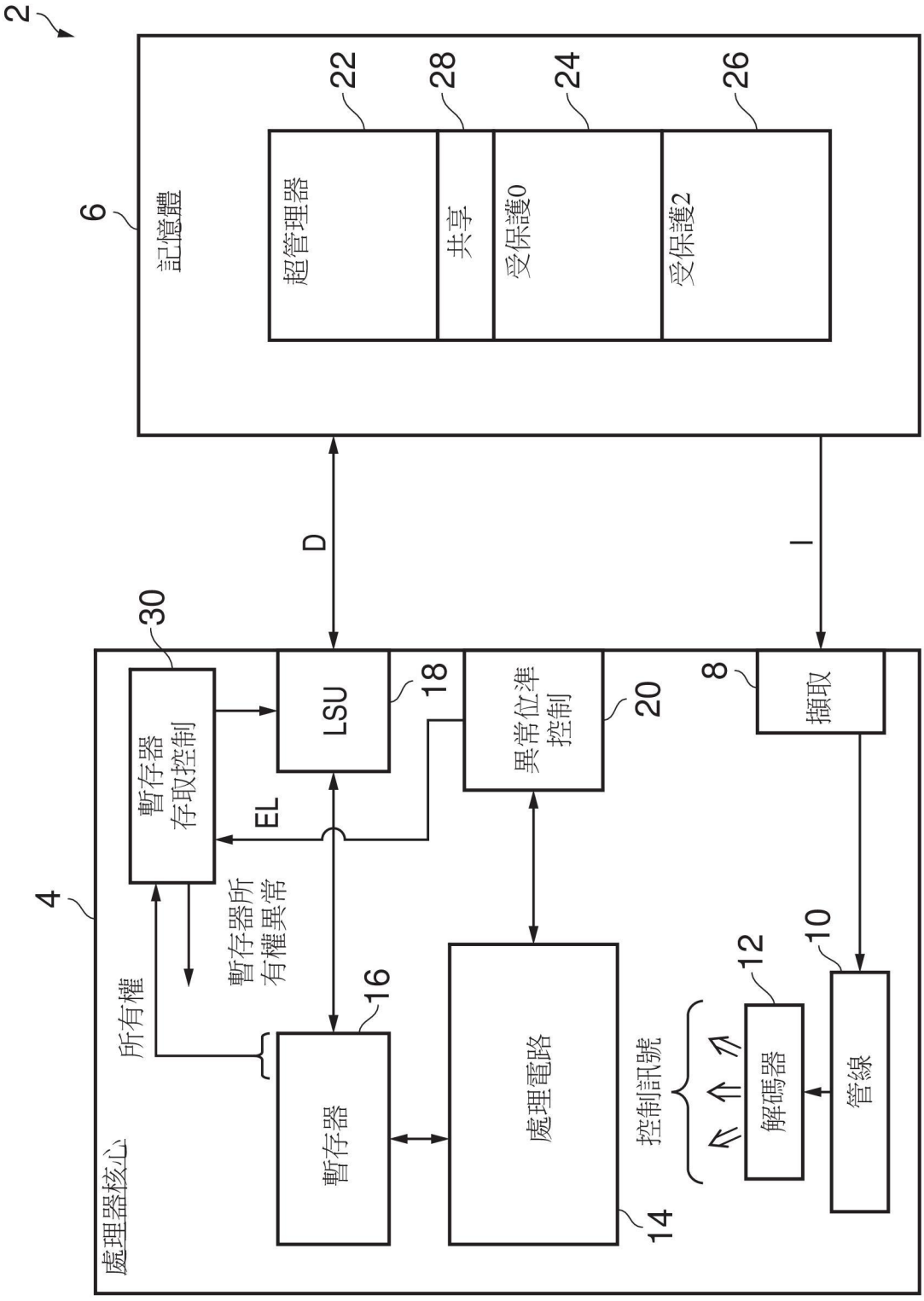
【第23項】 如請求項22所述之方法，其包含以下步驟：

當產生一異常並切換至特權位準之一層次內之一更高特權位準時，執行一或多個目標受約束的程式指令以將儲存在該複數個暫存器內之值儲存至該受保護儲存器區域；以及

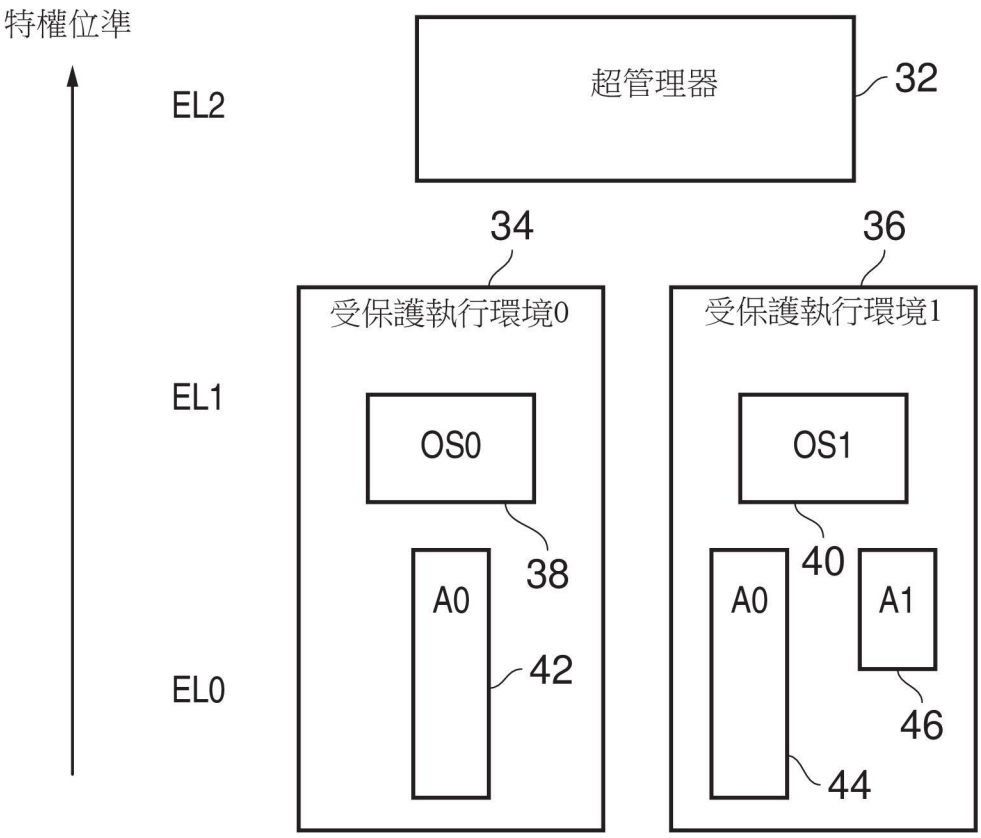
當對應於該受保護執行上下文自該異常返回並切換至特權位準之一層次內之一更低特權位準時，執行一或多個目標受約束的程式指令以將儲存在保護儲存器

區域內之值加載至該複數個暫存器。

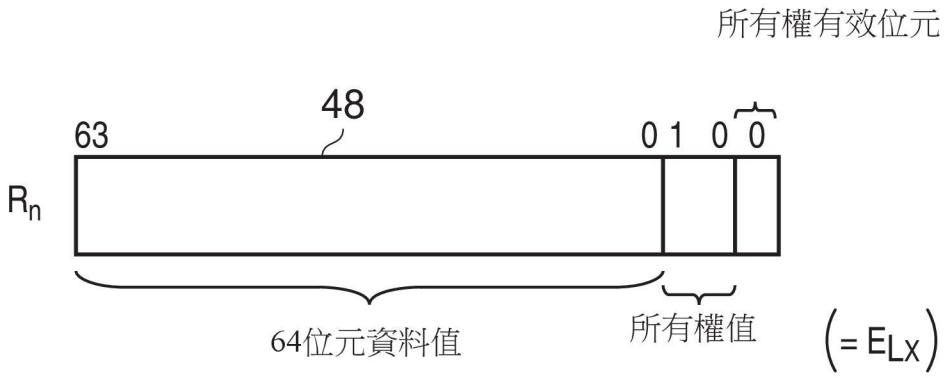
【發明圖式】


2
6
記憶體
超管理器
22
共享
28
受保護0
24
受保護2
26
D
I
4
處理器核心
30
暫存器存取控制
LSU
18
異常位準控制
20
8
擷取
EL
暫存器所有權異常
所有權
16
暫存器
處理電路
14
控制訊號
12
解碼器
10
管線

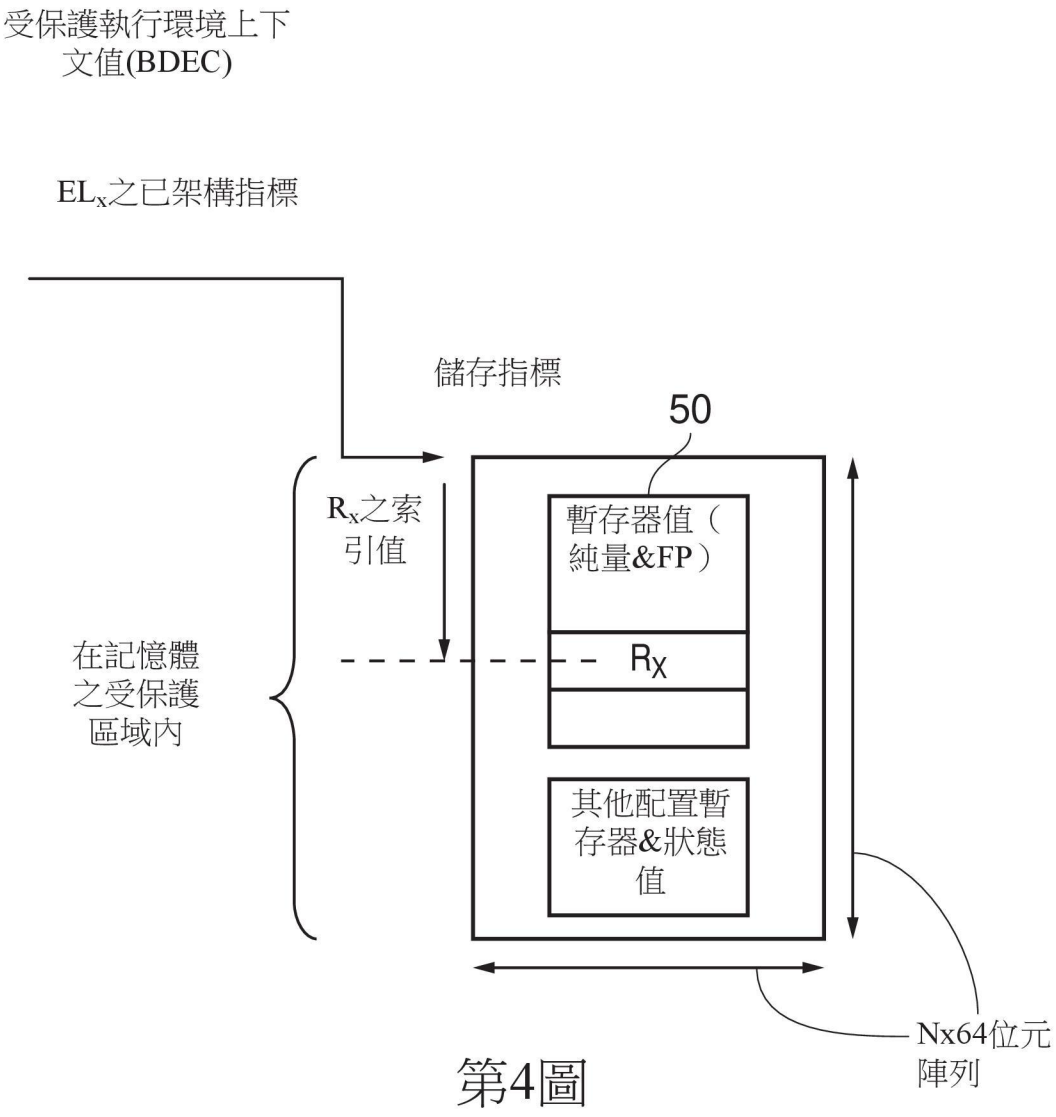
第1圖


特權位準
EL2
EL1
EL0
超管理器
32
34
36
受保護執行環境0
受保護執行環境1
OS0
OS1
38
40
A0
A0
A1
42
44
46

第2圖


所有權有效位元
48
63
0 1 0 0
R_n
64位元資料值
所有權值
(= E_{LX})

第3圖


受保護執行環境上下文值(BDEC)
ELx之已架構指標
儲存指標
50
Rx之索引值
暫存器值（純量&FP）
RX
在記憶體之受保護區域內
其他配置暫存器&狀態值
Nx64位元陣列

第4圖

目標無約束的加載/儲存指令

STR（自由定義之位址）

LDR（自由定義之位址）

第5圖

目標約束的加載/儲存指令

```
STR Blind [BRI]
        //由於BRI所有參數隱含
        data = GPR [BRI].Data
        bi = GPR [BRI].Owner          // 哪個BDEC
        bp = BDEC [bi]                // BDEC指標
        brp = bp [BRI]                // BDEC 暫存器進入點
        STORE. bi data, brp           // 儲存至受保護區域
        (BRI++)                       // 可選的索引增量及旗標
                                         設定

LDR Blind [BRI, BTEL]
        // 將BTEL設定為更低異常位準
        bp = BDEC [BTEL]
        brp = bp [BRI]
        LOAD, BTEL data, brp          // 自受保護區域加載
        GPR [BRI].Data = data
        GPR [BRI].Owner = BTEL
        (BRI--)                       // 可選的索引減量及旗標
                                         設定
```

第6圖

索引重設程式指令

```
Reset BRI
        BRI=0
```

索引改變程式指令

```
Increment BRI.S    //旗標設定
        BRI++
        if BRI>MaxReg, set overflow flag
```

目標所有者設定程式指令

```
Set BTEL Rn
        If Rn.Owner < current ELX, BTEL=Rn.Owner
```

第7A圖

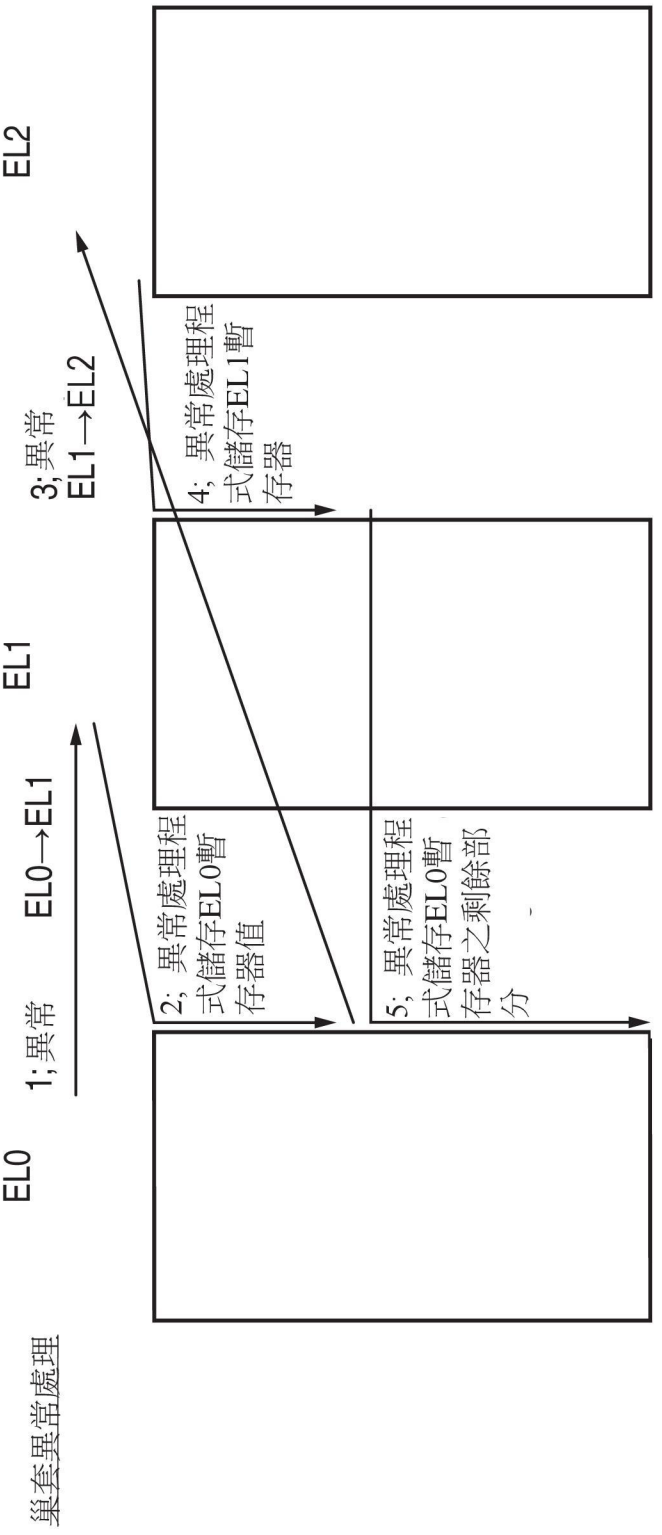
異常處理-盲暫存器保存

```
    Reset BRI
loop:
    STRBlind [BRI]
    B.VS  loop      //不上溢，循環至下一個暫存器
```

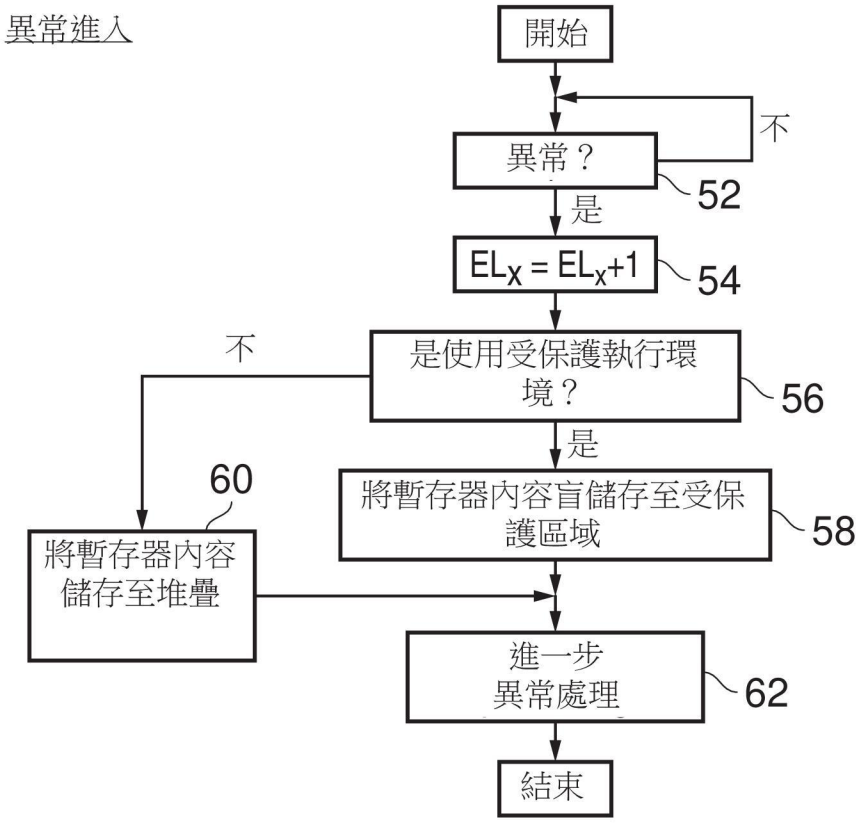
異常返回-盲暫存器恢復

```
    Set BTEL Rn
    Reset BRI
loop:
    LDR Blind[BRI.BTEL]
    B.LZ            //不小於零，循環至下一個暫存器
```

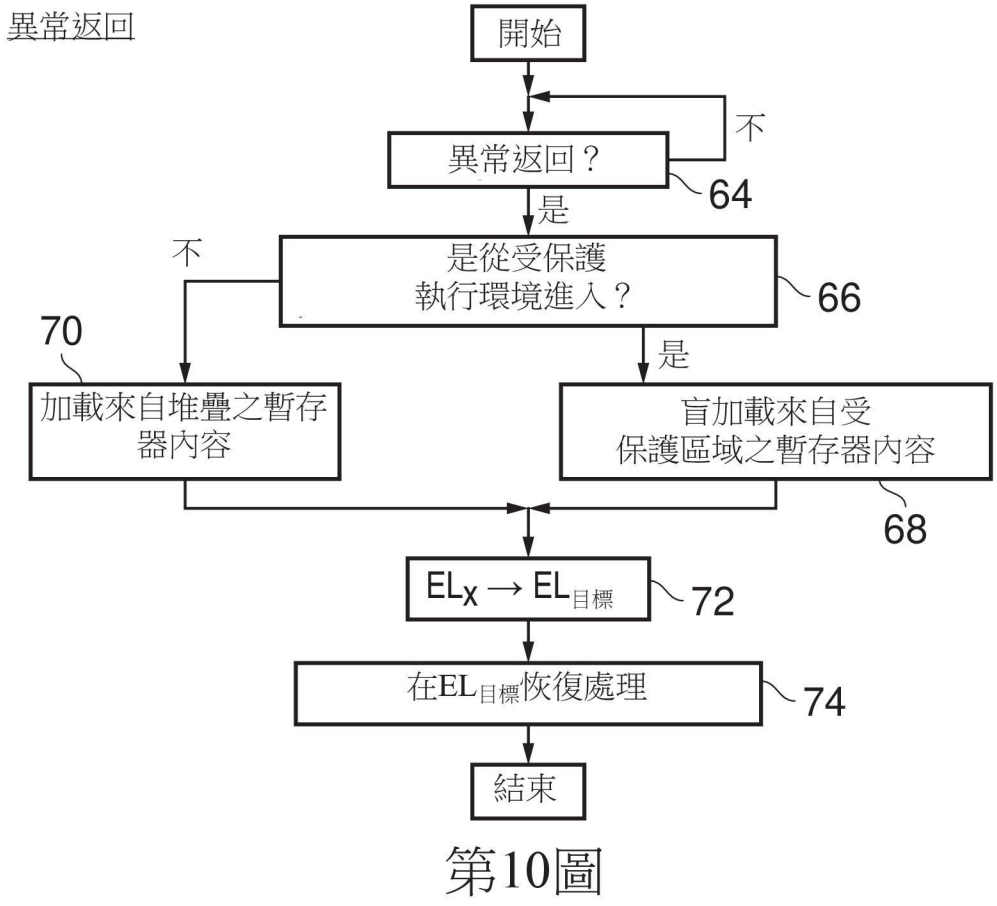
第7B圖


巢套異常處理
EL0
1; 異常
EL0→EL1
EL1
2; 異常處理程式儲存EL0暫存器值
5; 異常處理程式儲存EL0暫存器之剩餘部分
3; 異常
EL1→EL2
EL2
4; 異常處理程式儲存EL1暫存器
所有標記為
所有者 = EL2
a)單調順序
b)非典型順序；使用頻率
EL2之剩餘部分及隨後執行
之EL1異常處理

第8圖


異常進入
開始
異常？
不
52
是
ELx = ELx+1
54
不
是使用受保護執行環境？
56
是
60
將暫存器內容儲存至堆疊
將暫存器內容盲儲存至受保護區域
58
進一步異常處理
62
結束

第9圖


異常返回
開始
異常返回？
不
64
是
不
是從受保護執行環境進入？
66
70
是
加載來自堆疊之暫存器內容
盲加載來自受保護區域之暫存器內容
68
ELx → EL目標
72
在EL目標恢復處理
74
結束

第10圖