



(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 202343257 A

(43)公開日：中華民國 112 (2023) 年 11 月 01 日

(21)申請案號：112112991

(22)申請日：中華民國 112 (2023) 年 04 月 07 日

(51)Int. Cl.：

G06F12/0866(2016.01)**G06F12/02 (2006.01)****G06F13/14 (2006.01)**

(30)優先權：2022/04/28

英國

2206166.7

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

英國

(72)發明人：范吉雷迪 馬杜蘇達那雷迪 VANGIREDDY, MADHUSUDANA REDDY (IN)；霍

利 約翰麥克 HORLEY, JOHN MICHAEL (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：19 項 圖式數：25 共 123 頁

(54)名稱

記憶體管理

(57)摘要

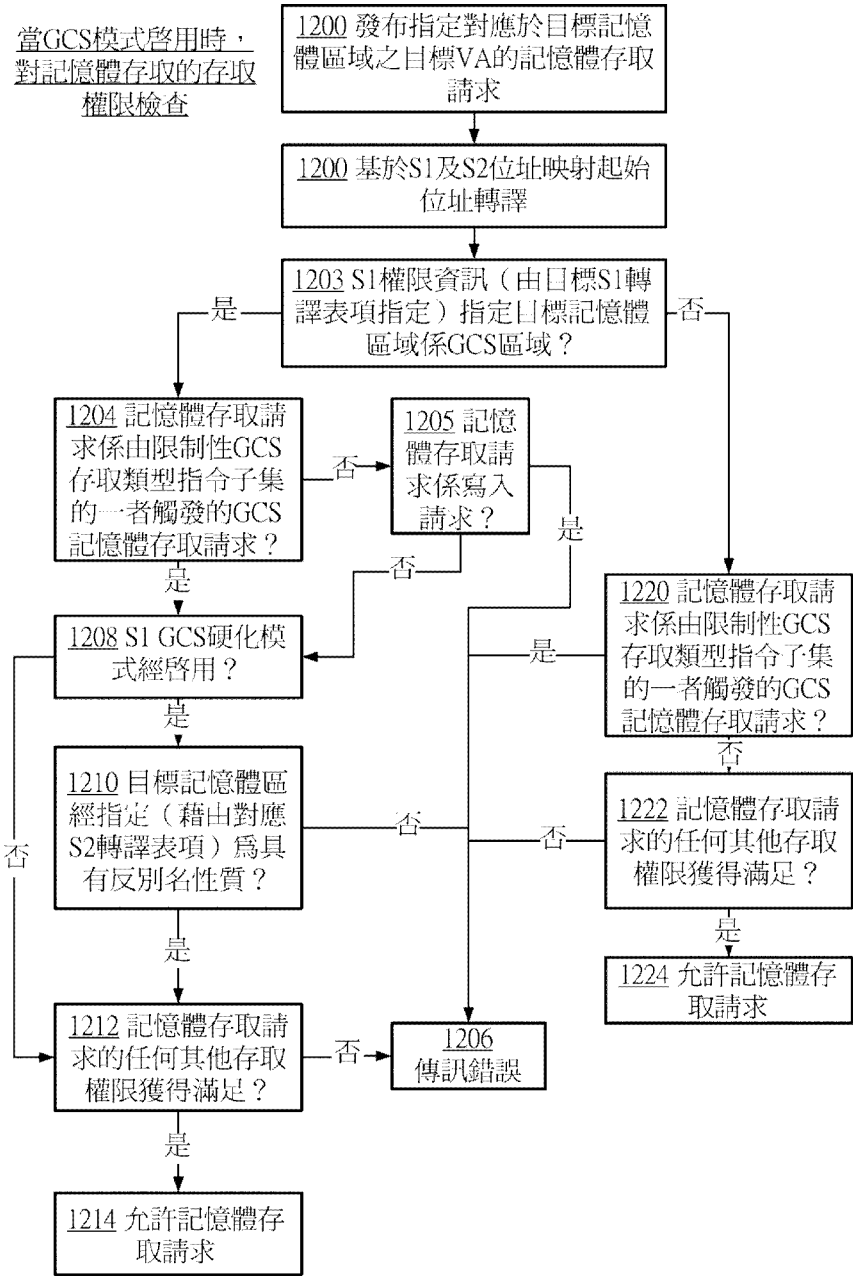
對於一記憶體存取請求，將一目標虛擬位址轉譯成一目標實體位址。至少對於寫入請求，當一目標 1 階轉譯表項指定對應於該目標虛擬位址的一目標記憶體區域係用於存取用於保護返回狀態資訊的一受防護控制堆疊(GCS)資料結構的一 GCS 區域，且該記憶體存取請求不係由一限制性 GCS 存取指令類型子集的一者觸發的一 GCS 記憶體存取請求時，拒絕該記憶體存取請求。當一反別名性質對該目標記憶體區域指定，且該目標 1 階轉譯表項或用以定位該目標 1 階轉譯表項的另一 1 階轉譯表項係未受一轉譯硬化機制保護的一未硬化項時，拒絕該記憶體存取請求。在至少一個操作狀態中，當該反別名性質未對該目標記憶體區域指定時，拒絕一 GCS 記憶體存取請求。

A target virtual address is translated to a target physical address for a memory access request. At least for write requests, the memory access request is rejected when a target stage-1 translation table entry specifies that a target memory region corresponding to the target virtual address is a guarded control stack (GCS) region for storing a GCS data structure for protecting return state information, and the memory access request is not a GCS memory access request triggered by one of a restricted subset of GCS-accessing instruction types. When an anti-aliasing property is specified for the target memory region and the target stage-1 translation table entry or another stage-1 translation table entry used to locate the target stage-1 translation table entry is an unhardened entry unprotected by a translation hardening mechanism, the memory access request is rejected. In at least one operating state, a GCS memory access request is rejected when the anti-aliasing property is not specified for the target memory region.

指定代表圖：

符號簡單說明：

- 1200:步驟
- 1202:步驟
- 1203:步驟
- 1204:步驟
- 1205:步驟
- 1206:步驟
- 1208:步驟
- 1210:步驟
- 1212:步驟
- 1214:步驟
- 1220:步驟
- 1222:步驟
- 1224:步驟



【圖24】

【發明摘要】

【中文發明名稱】 記憶體管理

【英文發明名稱】 MEMORY MANAGEMENT

【中文】

對於一記憶體存取請求，將一目標虛擬位址轉譯成一目標實體位址。至少對於寫入請求，當一目標1階轉譯表項指定對應於該目標虛擬位址的一目標記憶體區域係用於存取用於保護返回狀態資訊的一受防護控制堆疊(GCS)資料結構的一GCS區域，且該記憶體存取請求不係由一限制性GCS存取指令類型子集的一者觸發的一GCS記憶體存取請求時，拒絕該記憶體存取請求。當一反別名性質對該目標記憶體區域指定，且該目標1階轉譯表項或以定位該目標1階轉譯表項的另一1階轉譯表項係未受一轉譯硬化機制保護的一未硬化項時，拒絕該記憶體存取請求。在至少一個操作狀態中，當該反別名性質未對該目標記憶體區域指定時，拒絕一GCS記憶體存取請求。

【英文】

A target virtual address is translated to a target physical address for a memory access request. At least for write requests, the memory access request is rejected when a target stage-1 translation table entry specifies that a target memory region corresponding to the target virtual address is a guarded control stack (GCS) region for storing a GCS data structure for protecting return state information, and the memory access request is not a GCS memory access request triggered by one of a restricted subset of GCS-accessing instruction types. When an anti-aliasing property is specified for the target memory

region and the target stage-1 translation table entry or another stage-1 translation table entry used to locate the target stage-1 translation table entry is an unhardened entry unprotected by a translation hardening mechanism, the memory access request is rejected. In at least one operating state, a GCS memory access request is rejected when the anti-aliasing property is not specified for the target memory region.

【指定代表圖】 圖24

【代表圖之符號簡單說明】

1200:步驟

1202:步驟

1203:步驟

1204:步驟

1205:步驟

1206:步驟

1208:步驟

1210:步驟

1212:步驟

1214:步驟

1220:步驟

1222:步驟

1224:步驟

【特徵化學式】 無

【發明說明書】

【中文發明名稱】 記憶體管理

【英文發明名稱】 MEMORY MANAGEMENT

【技術領域】

【0001】 本技術係關於資料處理領域。

【先前技術】

【0002】 在資料處理設備中，提供記憶體管理電路系統以控制對記憶體系統的存取。記憶體管理電路系統負責執行位址轉譯以將基於由處理電路系統執行之指令的運算元指定的目標虛擬位址轉譯成識別待存取之記憶體系統位置的目標實體位址。記憶體管理電路系統亦可執行，例如，基於指定在轉譯表結構中之資訊的存取權限，該轉譯表結構用以指定從目標虛擬位址至目標實體位址的映射。

【發明內容】

【0003】 至少一些實例提供一種設備，其包含：處理電路系統，以在複數個執行狀態的一者中執行指令；及記憶體管理電路系統，以回應於指定對應於待存取的一目標記憶體區域的一目標虛擬位址的一記憶體存取請求而將該目標虛擬位址轉譯成一目標實體位址，其中從該目標虛擬位址至該目標實體位址的一映射至少取決於由一1階轉譯表結構中的一目標1階轉譯表項對該目標虛擬位址指定的一1階位址映射，該1階轉譯表結構可使用可由在一第一執行狀態中

的該處理電路系統執行的一指令設定的一1階基底位址存取；其中：至少當該記憶體存取請求係一寫入請求時，該記憶體管理電路系統經組態以回應於判定該等下列條件二者皆獲得滿足而拒絕該記憶體存取請求：由該目標1階轉譯表項指定的1階權限資訊指定該目標記憶體區域係用於儲存用於保護用於從一函數呼叫或例外返回的返回狀態資訊的一受防護控制堆疊(guarded control stack, GCS)資料結構的一GCS區域；及該記憶體存取請求係由一限制性GCS存取類型指令子集的一者所觸發的一GCS記憶體存取請求以外的一請求；該記憶體管理電路系統經組態以支援一轉譯硬化機制，該轉譯硬化機制用於至少基於可由在具有比該第一執行狀態更大特權的一第二執行狀態中的該處理電路系統執行的一指令設定的轉譯硬化資訊定義由該轉譯硬化機制保護以免於由在該第一執行狀態中執行的一指令篡改的至少一個經硬化1階轉譯表項；當一反別名性質對該目標記憶體區域指定時，該記憶體管理電路系統經組態以回應於偵測到該目標1階轉譯表項或用以定位該目標1階轉譯表項的另一1階轉譯表項係未受該轉譯硬化機制保護的一未硬化轉譯表項而拒絕該記憶體存取請求；及在該處理電路系統的至少一個操作狀態中，該記憶體管理電路系統經組態以回應於判定該記憶體存取請求係該GCS記憶體存取請求而該反別名性質未對該目標記憶體區域指定而拒絕該記憶體存取請求。

【0004】 至少一些實例提供一種方法，其包含：在複數個執行狀態的一者中執行指令；及回應於指定對應於待存取的一目標記憶體區域的一目標虛擬位址的一記憶體存取請求而將該目標虛擬位址轉譯成一目標實體位址，其中從該目標虛擬位址至該目標實體位址的一映射至少取決於由一1階轉譯表結構中

的一目標1階轉譯表項對該目標虛擬位址指定的一1階位址映射，該1階轉譯表結構可使用可由在一第一執行狀態中的該處理電路系統執行的一指令設定的一1階基底位址存取；其中：至少當該記憶體存取請求係一寫入請求時，回應於判定該等下列條件二者皆獲得滿足而拒絕該記憶體存取請求：由該目標1階轉譯表項指定的1階權限資訊指定該目標記憶體區域係用於儲存用於保護用於從一函數呼叫或例外返回的返回狀態資訊的一受防護控制堆疊(GCS)資料結構的一GCS區域；及該記憶體存取請求係由一限制性GCS存取類型指令子集的一者所觸發的一GCS記憶體存取請求以外的一請求；一轉譯硬化機制，其支援至少基於可由在具有比該第一執行狀態更大特權的一第二執行狀態中執行的一指令設定的轉譯硬化資訊定義由該轉譯硬化機制保護以免於由在該第一執行狀態中執行的一指令篡改的至少一個經硬化1階轉譯表項；且該方法包含：當一反別名性質對該目標記憶體區域指定時，回應於偵測到該目標1階轉譯表項或用以定位該目標1階轉譯表項的另一1階轉譯表項係未受該轉譯硬化機制保護的一未硬化轉譯表項而拒絕該記憶體存取請求；及在該處理電路系統的至少一個操作狀態中，回應於判定該記憶體存取請求係該GCS記憶體存取請求而該反別名性質未對該目標記憶體區域指定而拒絕該記憶體存取請求。

【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：處理程式邏輯，以模擬該目標碼之指令在複數個執行狀態的一者中的執行；及記憶體管理程式邏輯，以回應於指定對應於待存取的一目標記憶體區域的一目標虛擬位址的一記憶體存取請求而將該目標

虛擬位址轉譯成一經模擬目標實體位址，其中從該目標虛擬位址至該經模擬目標實體位址的一映射至少取決於由一1階轉譯表結構中的一目標1階轉譯表項對該目標虛擬位址指定的一1階位址映射，該1階轉譯表結構可使用可由經模擬成在一第一執行狀態中執行的一指令設定的一1階基底位址存取；其中：至少當該記憶體存取請求係一寫入請求時，該記憶體管理程式邏輯經組態以回應於判定該等下列條件二者皆獲得滿足而拒絕該記憶體存取請求：由該目標1階轉譯表項指定的1階權限資訊指定該目標記憶體區域係用於儲存用於保護用於從一函數呼叫或例外返回的返回狀態資訊的一受防護控制堆疊(GCS)資料結構的一GCS區域；及該記憶體存取請求係由一限制性GCS存取類型指令子集的一者所觸發的一GCS記憶體存取請求以外的一請求；該記憶體管理程式邏輯經組態以支援一轉譯硬化機制，該轉譯硬化機制用於至少基於可由經模擬成在具有比該第一執行狀態更大特權的一第二執行狀態中執行的一指令設定的轉譯硬化資訊定義由該轉譯硬化機制保護以免於由經模擬成在該第一執行狀態中執行的一指令篡改的至少一個經硬化1階轉譯表項；當一反別名性質對該目標記憶體區域指定時，該記憶體管理程式邏輯經組態以回應於偵測到該目標1階轉譯表項或以定位該目標1階轉譯表項的另一1階轉譯表項係未受該轉譯硬化機制保護的一未硬化轉譯表項而拒絕該記憶體存取請求；及在該處理電路系統的至少一個操作狀態中，該記憶體管理電路系統經組態以回應於判定該記憶體存取請求係該GCS記憶體存取請求而該反別名性質未對該目標記憶體區域指定而拒絕該記憶體存取請求。

【0006】 該電腦程式可儲存在一電腦可讀儲存媒體上。該儲存媒體可係一非暫時性儲存媒體。

【圖式簡單說明】

【0007】 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〕繪示具有處理電路系統及記憶體管理電路系統之資料處理設備的實例；
- 〔圖 2〕繪示處理電路系統之執行狀態的實例；
- 〔圖 3〕繪示二階段位址轉譯；
- 〔圖 4〕及〔圖 5〕分別繪示 1 階及 2 階位址轉譯之轉譯表查核的實例；
- 〔圖 6〕繪示當考慮到各表基底位址及在 1 階判定的最終中間位址將可使用各別 2 階轉譯轉譯成實體位址時，對 1 階及 2 階轉譯二者的完整轉譯表查核執行的表查找；
- 〔圖 7〕繪示用於控制記憶體管理之記憶體管理電路系統及控制暫存器的實例；
- 〔圖 8〕繪示用於 1 階及 2 階位址轉譯之轉譯表項的實例；
- 〔圖 9〕繪示經容許及經禁止寫入至由 2 階轉譯表項定義之部分唯讀記憶體區域之寫入請求的類型；
- 〔圖 10〕繪示執行位址轉譯及權限檢查的方法；
- 〔圖 11〕係繪示基於部分唯讀權限之檢查的流程圖；
- 〔圖 12〕、〔圖 13〕、及〔圖 14〕繪示受保護項檢查類型之讀取-檢查-寫入指令的不同變體的處理；
- 〔圖 15〕繪示將虛擬位址別名至相同的中間位址上；

〔圖 16〕繪示反別名化檢查；

〔圖 17〕繪示 1 階頂層表存在檢查及 1 階頂層部分唯讀檢查；

〔圖 18〕繪示藉由轉譯表項間接指定的權限資訊；

〔圖 19〕繪示函數呼叫及返回的實例；

〔圖 20〕繪示用於控制對受防護控制堆疊(GCS)資料結構之存取的暫存器；

〔圖 21〕繪示用於保護用於從函數呼叫或例外返回之返回狀態資訊的 GCS 資料結構的使用；

〔圖 22〕係繪示返回狀態推入指令之處理的流程圖；

〔圖 23〕係顯示返回狀態移出指令之處理的流程圖；

〔圖 24〕繪示由記憶體管理電路系統對 GCS 模式啟用時所發布的記憶體存取請求執行的存取權限檢查；及

〔圖 25〕繪示可使用的模擬器實施方案。

【實施方式】

【0008】 一種設備具有處理電路系統以在若干個執行狀態的一者中執行指令，及記憶體管理電路系統以回應於指定對應於待存取的一目標記憶體區域的一目標虛擬位址的一記憶體存取請求而將該目標虛擬位址轉譯成一目標實體位址。從該目標虛擬位址至該目標實體位址的一映射至少取決於由一 1 階轉譯表結構中的一目標 1 階轉譯表項對該目標虛擬位址指定的一 1 階位址映射。該 1 階轉譯表結構可使用可由在一第一執行狀態中的該處理電路系統執行的一指令設定的一 1 階基底位址存取。

【0009】 返回導向程式設計(ROP)為基的攻擊係資料處理系統上的常見攻擊類別。ROP攻擊係藉由損壞用以從函數呼叫或例外返回之返回狀態資訊而企圖導致程式以非預期方式行為的攻擊。軟體常將返回狀態資訊保存至記憶體，例如，以促進函數呼叫或例外的巢套，其中將用於（一組巢套函數呼叫或例外的）外函數呼叫或例外的返回狀態資訊保存至記憶體以在用於內函數呼叫或例外的返回狀態資訊可在暫存器中覆寫其之前保留其。ROP攻擊可企圖在返回狀態資訊儲存在記憶體中時，在將其恢復至暫存器之前篡改其，且用以控制函數返回或例外返回。成功的ROP攻擊可導致函數返回或例外返回使程式流返回至呼叫該函數或取得該例外之該點之後的次一指令以外的指令，其可允許攻擊者控制處理電路系統執行程式設計師所預期之操作序列以外的任意操作。

【0010】 為防護ROP為基的攻擊，提供用以保護用於從函數呼叫或例外返回之返回狀態資訊的受防護控制堆疊(GCS)資料結構可係有用的。1階轉譯表項指定對應於給定虛擬位址的記憶體區域是否係用於儲存GCS資料結構的GCS區域。回應於指定一目標虛擬位址的一記憶體存取請求，至少在該記憶體存取請求係一寫入請求時，該記憶體管理電路系統回應於判定下列條件二者皆獲得滿足而拒絕該記憶體存取請求：

- 由該目標 1 階轉譯表項指定的 1 階權限資訊指定該目標記憶體區域係用於儲存用於保護用於從一函數呼叫或例外返回的返回狀態資訊的一受防護控制堆疊(GCS)資料結構的一 GCS 區域；及
- 該記憶體存取請求係由一限制性 GCS 存取類型指令子集的一者所觸發的一 GCS 記憶體存取請求以外的一請求。

【0011】 因此，記憶體區域可由對應1階轉譯表項指定為用以使用於函數呼叫或例外之返回狀態資訊安全的GCS區域。儲存在該區域中的資訊可用以在繼續進行函數返回或例外返回之前驗證返回狀態資訊是否適當。若對指定為GCS區域之區域的寫入係回應於限制性GCS存取類型指令子集以外的指令而產生，該等寫入受拒絕。藉由將對GCS區域的寫入存取限制為僅某些指令類型，此降低企圖損壞返回狀態資訊之攻擊者可用的攻擊表面，因為由包括在正受執行程式碼內的其他類型的記憶體存取指令觸發的寫入請求（若在修改指令的運算元之後遭騙存取GCS區域）將不能夠用以成功地更新儲存在GCS區域中的資訊。由於讀取請求無法更新儲存在GCS區域中的受保護返回狀態，對於讀取請求施加此限制不係必要的，但可選地，一些實施方案亦可選擇在讀取請求的目標記憶體區域由1階權限資訊指定為GCS區域且讀取請求不係由限制性GCS存取類型指令子集的一者觸發時，發訊錯誤。

【0012】 然而，由於使用1階轉譯表項指定GCS區域，且1階轉譯表結構可經由可由在第一執行狀態（例如，此可係作業系統在其中執行的狀態）中執行的指令控制的基底暫存器存取，接著若攻擊者能夠損壞在第一執行狀態中執行的作業系統或其他軟體，其等可能能夠修改對應於GCS區域的1階轉譯表項，使得記憶體區域不再被指定為GCS區域，及/或建立將不同虛擬位址映射至GCS區域的經轉譯位址而無需將該對應記憶體區域指定為GCS區域的別名1階轉譯表項，企圖規避由指定GCS區域的1階轉譯表項提供的保護。

【0013】 在下文討論的實例中，該記憶體管理電路系統支援一轉譯硬化機制，該轉譯硬化機制用於至少基於可由在具有比該第一執行狀態更大特權的

一第二執行狀態中的該處理電路系統執行的一指令設定的轉譯硬化資訊定義由該轉譯硬化機制保護以免於由在該第一執行狀態中執行的一指令篡改的至少一個經硬化1階轉譯表項。當一反別名性質對該目標記憶體區域指定時，該記憶體管理電路系統回應於偵測到該目標1階轉譯表項或用以定位該目標1階轉譯表項的另一1階轉譯表項係未受該轉譯硬化機制保護的一未硬化轉譯表項而拒絕該記憶體存取請求。在該處理電路系統的至少一個操作狀態中，該記憶體管理電路系統回應於判定該記憶體存取請求係該GCS記憶體存取請求而該反別名性質未對該目標記憶體區域指定而拒絕該記憶體存取請求。

【0014】 因此，實施措施的下列組合：

- 將對（使用 1 階權限資訊指示的）GCS 區域的寫入限制成使用某些指定 GCS 存取類型指令執行；
- 1 階轉譯表項可基於可由在比能夠控制 1 階轉譯表結構之基底位址的第一執行狀態更多特權的執行狀態執行的指令設定的資訊而指定為經硬化；
- 指定為具有反別名性質的記憶體區域不可基於未硬化 1 階轉譯表項存取；及
- 若反別名性質尚未對目標記憶體區域設定，拒絕 GCS 記憶體存取請求。

【0015】 措施的此組合允許更加安全地保護GCS資料結構免於篡改，由於此強制要求將反別名性質施加至任何GCS記憶體區域（否則GCS記憶體存取請求不成功），而當反別名性質對GCS區域定義時，反別名性質迫使未硬化轉

譯表項（其可能易為攻擊者所修改或可係攻擊者已定義以規避經硬化轉譯表項的別名轉譯表項）不可用以促成對GCS區域的存取。因此，此方法提供更大保護以免於基於返回導向程式設計的攻擊。

【0016】 GCS記憶體存取請求可包括讀取請求及寫入請求。GCS讀取請求可由一或多種類型的GCS存取載入指令觸發且GCS寫入請求可由觸發寫入請求的一或多種類型的GCS存取儲存指令觸發。如上文提及的，在至少一個操作狀態中，GCS記憶體存取請求受制於若反別名性質未對目標記憶體區域指定時傳訊錯誤的要求。無論GCS記憶體存取請求係讀取請求或寫入請求皆可傳訊錯誤。因此，GCS存取載入指令及GCS存取儲存指令二者可觸發反別名性質的檢查，且若反別名性質未對目標記憶體區域指定，觸發錯誤（即使在對記憶體之GCS區域的讀取請求在由GCS存取類型指令以外的指令導致時不會觸發錯誤時）。

【0017】 該記憶體管理電路系統可支援二階段位址轉譯，其中該1階段位址映射包含從該目標虛擬位址至一目標中間位址的一映射，且從該目標虛擬位址至該目標實體位址的該位址映射亦取決於從該目標中間位址至該目標實體位址的一2階段位址映射，該目標實體位址係藉由一2階轉譯表結構中的一目標2階轉譯表項對該目標中間位址指定。該2階轉譯表結構可使用可由在該第二執行狀態中的該處理電路系統執行的一指令設定的一2階基底位址存取。二階段位址轉譯對支援若干個客作業系統可共存在相同硬體平台上的虛擬化可係有用的。第二執行狀態可係用於執行用以控制客作業系統之虛擬化的超管理器的執行狀態。

【0018】 反別名性質可由在第二執行狀態中執行的指令設定。反別名性質可對目標記憶體區域指定在由第二執行狀態中執行之軟體維護之與2階轉譯表結構分開的資料結構中。

【0019】 然而，由於2階轉譯表結構可在任何情形中由在第二執行狀態中執行的軟體管理，目標2階轉譯表項指定反別名性質是否對目標記憶體區域指定可係最有效率的。

【0020】 類似地，雖然轉譯硬化資訊可包括由在第二執行狀態中執行的軟體使用與2階轉譯表結構分開的資料結構定義的資訊，重使用2階轉譯表結構以定義包括轉譯硬化資訊的權限資訊可係更有效率的。對於儲存在對應於一給定中間位址的一給定記憶體區域的一給定1階轉譯表項，用於指定該給定1階轉譯表項是否係一經硬化1階轉譯表項的該轉譯硬化資訊包括由對應於該給定中間位址的一對應2階轉譯表項指定的2階權限資訊。

【0021】 提供用於迫使軟體已設定適當的存取權限或位址映射以確保2階轉譯表項受保護以免於由在第一執行狀態或較低特權狀態中執行的軟體更新的任何架構機制不係必要的。在第二執行狀態中執行之負責2階轉譯表結構的超管理器軟體一般採取保護該等結構免於由在第一執行狀態（或比第一執行狀態更低特權的執行狀態）中執行的作業系統軟體或其他軟體修改的措施。例如，超管理器可藉由將2階轉譯表結構的項分配至對應於不映射至在由在第一執行狀態（或較低特權狀態）中執行的軟體使用的2階轉譯表結構中的任何中間實體位址的記憶體區域而作到此，使得在第一執行狀態中的軟體無法取決該等區域（替代地，唯讀權限可用以保護2階轉譯表結構）。用於定義適當轉譯

表映射及/或權限以確保儲存2階轉譯表結構的記憶體區域受保護免於由在第一執行狀態中執行的軟體存取可係在第二執行狀態中執行之控制2階轉譯表結構之軟體的責任。因此，雖然當設備在使用時，超管理器（或在第二執行狀態中執行的其他軟體）使用適於軟體自身需要的位址映射及存取權限組態2階轉譯表結構，使得可將使用2階轉譯表項指定的反別名性質及轉譯硬化資訊限制成由在第二執行狀態（或更高特權執行狀態）中執行的指令設定且無法由在第一執行狀態（或更低特權執行狀態）中執行的指令設定可係較佳的，設備的硬體架構不需要提供用於迫使此等映射/存取權限已實際設定以保護2階轉譯表結構免於由在第一執行狀態或較低特權執行狀態中執行之軟體的修改的任何特殊架構措施。例如，架構定義檢查不需要驗證用以定義反別名性質（或轉譯硬化資訊）的2階轉譯表項是否本身已受保護免於篡改。可假設超管理器軟體將設定適當的2階位址映射/權限以保護其自身的操作。

【0022】 轉譯硬化機制可以不同方式實施。一般而言，轉譯硬化機制可係允許某些經硬化1階轉譯表項具有比未受保護1階轉譯表項更大的保護以免於篡改的任何架構機制。例如，1階轉譯表項可具有將該項標記為經硬化的特定編碼，且處理電路系統或記憶體管理電路系統可在對記憶體的寫入上檢查待寫入的資料是否具有1階轉譯表項的經硬化編碼，在該情形中，可抑制該寫入。然而，實際上在對記憶體的每個寫入上（包括對不儲存轉譯表項之記憶體區域的寫入）執行此類檢查可係極度效能密集的且消耗許多電力。

【0023】 轉譯硬化機構的更有效機制可係使用用以提供儲存經硬化1階轉譯表項之區域的2階位址映射的2階轉譯表項指定2階權限資訊，其中2階權限

資訊具有指示限制用於待修改對應區域中之資料的能力的權限類型的至少一個編碼。例如，該權限類型可係禁止寫入請求的唯讀權限及/或指示僅容許限制性寫入請求類型子集的寫入請求的部分唯讀權限類型。

【0024】 例如，各經硬化1階轉譯表項可包含一1階轉譯表項，對於該1階轉譯表項，儲存其的該給定記憶體區域由該對應2階轉譯表項的該2階權限資訊指示為下列一者：

一唯讀記憶體區域，禁止對於其的寫入請求；及

一部分唯讀記憶體區域，對於其，容許一限制性寫入請求類型子集之對該部分唯讀記憶體區域的寫入請求且禁止該限制性子集以外的寫入請求類型之對該部分唯讀記憶體區域的該等寫入請求，該限制性寫入請求類型子集包含由該記憶體管理電路系統產生的至少一後設資料更新寫入請求以更新一轉譯表項中的存取追蹤後設資料。

【0025】 一些實施方案可僅支援經硬化1階轉譯表項的唯讀選項。由於唯讀權限可已在2階支援且執行唯讀權限可能需要較不複雜的控制邏輯，此可簡化實施方案。

【0026】 其他實施方案可選擇支援部分唯讀權限，其可由於完整唯讀權限可防止轉譯表項中的存取追蹤後設資料由記憶體管理電路系統更新而係有用的。此類後設資料更新寫入請求對啟用對各別記憶體區域之存取頻率的追蹤可係有用的，例如，其對軟體（諸如作業系統）可係有用的，以作出哪些記憶體區域應移出至外部儲存且哪些記憶體區域應保留在更快存取的晶片上記憶體內的決定。由於存取追蹤後設資料可能不影響定義允許什麼記憶體存取存取對應

位址區域的權限，即使對1階轉譯表項的其他部分的寫入存取不被容許，其等可安全地更新。因此，藉由支援部分唯讀權限，此可在安全性與軟體開發者的程式化方便性之間提供更佳平衡。

【0027】 在一些實施方案中，唯一在2階允許用於經硬化1階轉譯表項的權限類型可係部分唯讀權限。

【0028】 然而，在其他實施方案中，若唯讀權限或部分唯讀權限其中一者定義在定義儲存給定1階轉譯表項之記憶體區域的2階位址映射的對應2階轉譯表項的2階權限資訊中，可將給定1階轉譯表項視為經硬化1階轉譯表項。因此，2階權限資訊具有用於指示唯讀記憶體區域及部分唯讀記憶體區域二者的編碼，且對於此等編碼二者，允許將對應1階轉譯表項（儲存在該2階權限資訊施用至其的記憶體區域中）視為經硬化可係有用的。此提供在第二執行狀態中執行的超管理器或其他軟體的程式設計師選擇對於防止對應1階轉譯表項的篡改係唯讀權限或部分唯讀權限較佳的機會。

【0029】 將2階權限設定成唯讀或部分唯讀對儲存在對應記憶體區域中的經硬化1階轉譯表項可係有用的，但實際上2階權限係以頁的粒度設定且單一頁可儲存許多1階轉譯表項。保護儲存在給定頁內的所有1階轉譯表項免於由在第一執行狀態中執行的受損作業系統或其他軟體篡改可能係不需要的。然而，一旦儲存在給定頁中的任何1階轉譯表項需要硬化，則對該頁設定的唯讀或部分唯讀2階權限可導致寫入請求（或至少在部分唯讀權限的情形中，限制性寫入請求子集以外的寫入請求）失敗，導致例外處置器執行。儘管對應記憶體區域在2階存取權限中設定成具有唯讀或部分唯讀權限以保護該區域中的其他項

免於篡改，由於甚至仍期望允許作業系統更新與非敏感資訊關聯的1階轉譯表項，則一個方法可將各更新捕捉給可決定是否容許該更新的超管理器，此可能不係問題。然而，此類更新請求可係相對頻繁的，且因此將各合法轉譯表項更新捕捉給超管理器可導致效能損失。

【0030】 給超管理器的此類捕捉可在實施方案中避免，該實施方案：

- 支援如上文討論之定義在 2 階權限資訊中的部分唯讀權限；
- 與未指定為受保護項的未受保護 1 階轉譯表項相比，提供具有指定該 1 階轉譯表項是否係對其的更新受到限制之受保護項的編碼的各 1 階轉譯表項，及
- 支援包括為允許寫入至記憶體之部分唯讀區域之限制性寫入請求類型子集的一者的寫入請求類型，允許該寫入請求類型更新未受保護 1 階轉譯表項，但禁止更新受保護 1 階轉譯表項的至少一位元子集。

【0031】 使用此方法，使用2階權限資訊標記有部分唯讀權限的記憶體區域可含有受保護項及未受保護項的混合，使得記憶體管理電路系統的硬體可防止在受保護1階轉譯表項內受保護的至少一位元子集免於更新，而未受保護項仍可由軟體更新，即使該等項儲存在部分唯讀區域中。此避免需要將未受保護項的各更新捕捉給超管理器，改善效能。

【0032】 例如，限制性寫入請求類型子集（允許更新儲存在記憶體之部分唯讀區域中的未受保護1階轉譯表項）可包括回應於受保護項檢查類型的讀取-檢查-寫入指令而發布的寫入請求。設備可具有受保護項檢查電路系統，該受保護項檢查電路系統回應於處理電路系統執行用於請求更新給定記憶體系統

位置的受保護項檢查類型的讀取-檢查-寫入指令而：從給定記憶體系統位置讀取資料、檢查從給定記憶體系統位置讀取的資料是否具有與指定為受保護項的1階轉譯表項一致的值、且回應於判定從給定記憶體系統位置讀取的資料具有與指定為受保護項的1階轉譯表項一致的值，防止回應於讀取-檢查-寫入指令而更新1階轉譯表項的更新受限制位元子集。更新受限制位元子集可係1階轉譯表項的所有位元，或可係1階轉譯表項之位元的適當子集（小於所有位元）。可將更新受限制位元子集定義為1階轉譯表項的固定位元子集，或定義為受保護1階轉譯表項的可程式化定義位元子集（例如，使用儲存在控制暫存器中之指示哪些位元係可程式化定義位元子集的控制資訊）。藉由定義由特定類型的讀取-檢查-寫入指令觸發之允許更新記憶體之部分唯讀區域內之未受保護項（及可選地受保護項的未受保護位元）的特殊類型的寫入請求（而可能不將由其他載入/儲存操作觸發的其他類型的寫入請求視為係允許更新儲存在部分唯讀區域中之資料的限制性寫入請求類型子集的一者），此可避免在對記憶體之部分唯讀區域的每一個寫入上觸發捕捉給超管理器之例外（用於檢查待由給定寫入請求更新的資料是否係受保護項）的需要。

【0033】 在支援將1階轉譯表項定義為受保護的實施方案中，亦可將指示是否將給定1階轉譯表項指定為受保護項的資訊視為係轉譯硬化資訊的部分。當由對應2階轉譯表項指定的2階權限資訊指定給定記憶體區域係部分唯讀記憶體區域（儲存在部分唯讀記憶體區域中的未受保護項仍可視為係經硬化的）時，記憶體管理電路系統可將未受保護1階轉譯表項視為係未硬化1階轉譯表項。因此，各經硬化1階轉譯表項可包含以下一者：一1階轉譯表項，用於其

的該給定記憶體區域由該2階權限資訊指示為禁止對於其之寫入請求的一唯讀記憶體區域；及一1階轉譯表項，其經指定為一受保護項，用於其的該給定記憶體區域由該2階權限資訊指示為該部分唯讀記憶體區域。未受保護1階轉譯表項可由在第一執行狀態操作之執行受保護項檢查類型之讀取-檢查-寫入指令的軟體以任意方式修改，且因此即使此等項儲存在由2階權限資訊定義的部分唯讀記憶體區域中，視為未硬化係最安全的。未受保護項若儲存在唯讀記憶體區域中會係不可修改的，因此不需要對儲存在唯讀記憶體區域中的項強加成為受保護項的要求。

【0034】 將理解將轉譯表項指定為受保護或未受保護不係必要特徵且一些實施方案可能不支援此。例如，受限於使用2階唯讀權限（不係部分唯讀權限）硬化1階轉譯表項的實施方案可能不需要支援受保護項編碼，且即使支援部分唯讀權限，則不支援受保護/未受保護1階轉譯表項編碼的實施方案可僅將意圖硬化的轉譯表項分配給以在2階的部分唯讀權限標記的特定頁，或可將對對應區域的所有寫入捕捉給超管理器，該超管理器接著可取決於所更新的資料是否係意圖硬化以免於篡改的1階轉譯表項而判定是否將允許由在第一執行狀態中的作業系統請求的更新。

【0035】 上文描述的轉譯硬化機制及反別名性質可不係特定用於保護用以存取GCS資料結構之轉譯項的通用架構機制，且亦可用以保護用於提供期望受保護免於由受損作業系統所篡改之敏感資訊的其他資料結構的其他1階轉譯表項免於篡改及別名。替代方法會係在2階權限資訊中定義將對應記憶體區域識別為經保留用於提供受防護控制堆疊結構之GCS記憶體區域的專用編碼。在

此替代方法中，與上文描述之會在2階對儲存用以提供對GCS資料結構之存取的1階轉譯表項的記憶體區域施加（當設備在使用中時，藉由軟體）的轉譯硬化資訊（例如，唯讀或部分讀取唯讀權限）相比，GCS 2階權限會施加至實際儲存GCS資料結構的記憶體區域。然而，在2階定義專用GCS權限的缺點係可有有限編碼空間量可用於定義給定2階轉譯表項的權限資訊，且因此定義專用GCS權限可能浪費對其他目的可能更有用的有價值的編碼空間。出於保護GCS結構的目的，藉由重使用通常適用於硬化1階位址轉譯以免於篡改，但若反別名性質未對標定記憶體區域指定時拒絕GCS記憶體存取請求（以若尚未施用轉譯硬化機制的風險存在，防止GCS存取）的通常結構機制，此可避免需要在2階轉譯表項中擴展關於用以保護返回狀態資訊之受防護控制堆疊資料結構之專用保護的編碼空間，且因此可導致轉譯表結構的更有效率的編碼。

【0036】 不需要對在處理電路系統的所有操作狀態中發布的GCS記憶體存取請求檢查反別名性質。可提供可設定成啟用狀態及停用狀態的GCS轉譯硬化檢查啟用控制參數（例如，在控制暫存器中）。該處理電路系統的該至少一個操作狀態（其中若該反別名性質未對該目標記憶體區域設定，拒絕該GCS記憶體存取請求）可包含在其中將該GCS轉譯硬化檢查啟用控制參數設定成一啟用狀態的一操作狀態，該啟用狀態指示GCS記憶體存取請求將受該反別名性質是否對該目標記憶體區域指定的一檢查。若GCS轉譯硬化檢查啟用控制參數係在停用狀態中，是否允許GCS記憶體存取請求可與反別名性質是否對目標記憶體區域設定無關地判定（因此當GCS轉譯硬化檢查停用時，即使反別名性質未對目標記憶體區域設定，允許GCS記憶體存取請求會係可能的）。提供GCS轉

譯硬化檢查的啟用/停用控制可在執行可能已對不支援反別名性質的架構編寫的傳統軟體時對促成回溯相容性（在該情形中，可停用GCS反別名檢查）係有用的。

【0037】 如上文提及的，若對GCS區域的寫入請求不係由限制性GCS存取類型指令子集的一者觸發，拒絕該請求（可選地，若讀取請求不係由GCS存取類型指令觸發，亦可拒絕該等請求，雖然此非必要的）。該記憶體管理電路系統亦可回應於一記憶體存取請求係該GCS記憶體存取請求及該1階權限資訊未指定對應於該目標虛擬位址的該記憶體區域係該GCS區域而拒絕該記憶體存取請求（包括寫入請求及讀取請求二者）。由於其意謂著GCS記憶體存取請求僅可用於存取GCS區域且無法用於存取用以儲存其他資料的標準記憶體區域，此降低攻擊者可用的攻擊表面。此意謂著若GCS存取類型指令的位址運算元由攻擊者所修改（或由強迫不正確程式流序列的攻擊者導致不正確），以導致GCS記憶體存取請求存取非GCS區域，將此偵測為錯誤且將拒絕存取記憶體的請求。

【0038】 可將若干種不同類型的指令支援為限制性GCS存取類型指令子集的部分。

【0039】 例如，該限制性GCS存取類型指令子集可包含一返回狀態推入指令以控制該處理電路系統將基於指示在該處理電路系統的一或多個暫存器中的資訊而獲得的返回狀態資訊推入至該GCS資料結構。在一些實例中，返回狀態推入指令可係專用GCS特定指令，其特定用於控制返回狀態資訊至GCS資料結構的推入。然而，返回狀態推入指令的至少一個變體係除了將返回狀態資訊

推入至GCS資料結構外，亦控制處理電路系統執行另一操作（例如，當呼叫函數或處置例外時常由軟體執行的操作）的指令亦係可能的。例如，其他操作可係觸發至目標位址的分支且亦控制將函數返回位址保存至暫存器（例如，稱為「鏈接暫存器」的暫存器）的函數呼叫分支操作。例如，當在處理電路系統之用於支援GCS資料結構之使用的GCS模式中執行時，「具有鏈接分支(branch-with-link)」指令（用於控制處理電路系統執行此一函數呼叫分支操作）亦可充當返回狀態推入指令。當停用GCS模式時，具有鏈接分支指令可導致處理電路系統執行函數呼叫分支操作，而不係將返回狀態資訊推入至堆疊資料結構的操作。當GCS模式啟用時，具有鏈接分支指令可導致處理電路系統執行函數呼叫分支操作及將返回狀態資訊推入至堆疊資料結構二者（針對此特定實例，返回狀態資訊可包括回應於具有鏈接分支指令而保存至鏈接暫存器的函數返回位址）。

【0040】 該限制性GCS存取類型指令子集亦可包含一返回狀態移出指令以控制該處理電路系統將返回狀態資訊從該GCS資料結構移出。在一些實例中，返回狀態移出指令亦可控制處理電路系統以回應於判定從GCS資料結構移出的返回狀態資訊與基於指示在處理電路系統的一或多個暫存器中的資訊判定的目前返回狀態資訊之間的失配而傳訊錯誤狀況。其他實例可定義其自身不從GCS資料結構移出返回狀態資訊而驗證藉由較早的返回狀態移出指令從GCS資料結構移出的受保護返回狀態是否與基於暫存器中的資訊判定的目前返回狀態資訊匹配的單獨返回狀態驗證指令。返回狀態推入及移出指令的若干個變體可

在由處理電路系統支援的指令集架構中受支援，例如，包括分別專用於推入/移出例外返回狀態資訊及函數（程序）返回狀態資訊的變體。

【0041】 再次，返回狀態移出指令可係專用GCS特定指令，或可係亦執行另一操作之另一類型指令的重利用變體。例如，返回狀態移出指令亦可控制處理電路系統執行例外返回。例如，當在GCS模式停用時執行時，例外返回指令可控制處理電路系統以基於定義在暫存器中的預期例外返回狀態資訊執行例外返回（而不係從GCS資料結構移出受保護返回狀態資訊及比對受保護返回狀態資訊驗證預期例外返回狀態資訊）。當例外返回指令在GCS模式中執行時，例外返回指令可控制處理電路系統執行例外返回及從GCS資料結構移出受保護返回狀態資訊及比對受保護返回狀態資訊驗證預期例外返回狀態資訊二者。

【0042】 該設備可具有至少一個GCS指標暫存器以儲存指示該受防護控制堆疊資料結構的一位址的一堆疊指標。GCS存取類型指令可參考儲存在GCS指標暫存器中的堆疊指標而判定其等的目標虛擬位址。在一些實例中，可有一個以上的GCS指標暫存器，各GCS指標暫存器指示在處理電路系統的各別執行狀態中使用的堆疊指標。

【0043】 當資訊由特定轉譯表項（1階或2階轉譯表項）指定時，該資訊可在轉譯表項的編碼中直接指定，或參考儲存於由轉譯表項參考之暫存器內的資訊間接指定。例如，對於間接參考，可提供包含可由軟體設定以指示特定權限類型的若干個欄位的權限間接暫存器，且轉譯表項可指定指示權限間接暫存器的哪些欄位指定將權限施加至對應記憶體區域的欄位選擇資訊。此間接權限方法可用於若干種不同的權限類型，包括如上文討論之在2階提供的唯讀權限

或部分唯讀權限，及/或將特定記憶體區域定義為1階的GCS區域、及/或定義目標記憶體區域的反別名性質。例如，可將指定該目標記憶體區域是否係該GCS區域的該1階權限資訊指定在由該目標1階轉譯表項所參考的一權限間接暫存器的一欄位中。類似地，亦可將（指定目標記憶體區域係唯讀或部分唯讀）的2階權限資訊指定在由目標2階轉譯表項所參考的權限間接暫存器的欄位中。使用權限間接暫存器的間接權限可由於若干個原因而係有用的。例如，間接權限指定允許軟體使用對暫存器的單一寫入更新施加至二或更多個不同記憶體區域的權限類型（其全部參考權限間接暫存器的相同欄位），而非需要更新對應於該等記憶體區域的各單獨轉譯表項。再者，在一些轉譯表項格式中，可能有不足以將期望編碼的每一種可能權限類型編碼的編碼空間，且因此權限間接性的使用可允許項內之編碼本身的有限數目的位元參考權限間接暫存器之能夠從比該項本身內可能的權限範圍更寬的權限範圍選擇的更大欄位。儘管如此，其他方法可將有關權限直接指定在轉譯表項的編碼內。因此，將理解當此申請案指示資訊係「由」轉譯表項「指定」時，此資訊可直接指定在轉譯表項的編碼中或經由權限間接暫存器間接指定（或資訊的直接及間接指定二者的混合）。

【0044】 再者，在一些實施方案中，轉譯表項或由轉譯表項直接地或間接地指定之權限資訊的某些位元可取決於指定在設備之控制暫存器中的控制狀態以不同方式解譯。例如，儲存在控制暫存器中的控制參數可控制權限資訊的特定位元（或位元欄位）係以第一方式或第二方式解譯。此可有助於使傳統軟體能根據傳統編碼方案操作且較新軟體能根據不同編碼方案解譯相同位元。因此，在陳述權限資訊指定一些資訊（或具有識別該資訊的編碼）時，由於在一

些情形中，是否將該權限資訊視為指定該資訊可取決於儲存在至少一個控制暫存器中的至少一個控制參數的目前設定，權限資訊在設備的所有操作模式中指定該資訊不係必要的。

【0045】 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的處理電路系統及記憶體管理電路系統而提供的硬體電路系統。

【0046】 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。電腦程式可具有仿真上文討論之處理電路系統及記憶體管理電路系統之功能的處理程式邏輯及記憶體管理程式邏輯，包括如上文討論之對GCS區域的支援、轉譯硬化機制、反別名性質、及（針對GCS記憶體存取請求）監督反別名性質是否已對目標記憶體區域指定。例如，當針對一個指令集架構所編寫之傳統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。

資料處理設備的具體實例

【0047】 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。

【0048】 執行級16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；用於在浮點值上執行操作的浮點單元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。提供係記憶體管

理電路系統之實例的記憶體管理單元(memory management unit, MMU) 28，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而指定的虛擬位址與識別資料在記憶體系統中的儲存位置的實體位址之間的位址轉譯。MMU具有轉譯後備緩衝區(translation lookaside buffer, TLB) 29，其用於從儲存在記憶體系統中的頁表快取位址轉譯資料，其中頁表的頁表項定義位址轉譯映射，及管控，例如，是否允許在管線上執行的給定程序從給定記憶體區域讀取、寫入、或執行指令的存取權限。

【0049】 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之存取的單一處理器核心，設備2亦可具有共用對記憶體34之存取的一或多個另外的處理器核心，其中各核心具有各別快取記憶體8、30、32。

【0050】 圖2係繪示處理電路系統4在執行指令時可在其中操作的不同執行狀態（亦稱為例外等級）的圖。在此實例中，有四個例外等級EL0、EL1、EL2、EL3，其中例外等級EL0係最低特權例外等級且例外等級EL3係最高特權

例外等級。一般而言，當在更高特權例外等級中執行時，處理電路系統可具有對不可為較低較少特權例外等級存取的一些記憶體位置或暫存器14的存取。

【0051】 在此實例中，例外等級EL0係用於執行應用程式，該等應用程式係由在例外等級EL1執行的對應作業系統或虛擬機器管理。在多個虛擬機器共存在相同實體平台上的情況下，可接著提供在EL2操作的超管理器，以管理各別虛擬機器。雖然圖2顯示超管理器管理虛擬機器且虛擬機器管理應用程式的實例，超管理器直接管理在EL0的應用程式亦係可能的。

【0052】 雖然不係必要的，一些實施方案可對處理電路系統實施操作的硬體分割的分開的安全域及非安全域。資料處理系統2可具有實施在處理器中的硬體特徵及記憶體系統，以確保將與在安全域中操作之軟體程序關聯的資料及碼與由在非安全域中操作之程序的存取隔離。例如，可使用諸如由Arm® Limited of Cambridge, UK提供之TrustZone®架構的硬體架構。替代地，可使用其他硬體執行的安全分割架構。安全應用程式（受信任服務）可在安全域中的例外等級EL0操作，且安全（受信任）作業系統或虛擬機器可在安全域中的例外等級EL1操作。在一些實施方案中，不存在對安全狀態中的EL2的支援且超管理器可單獨在非安全EL2中執行。在其他實施方案中，如圖2中之星號所指示的，可存在對在安全EL2中執行之安全超管理器的支援。在一些實例中，可提供在例外等級EL3中執行之用於管理非安全域與安全域之間的轉變的安全監測程式。其他實施方案可以硬體監督安全域之間的轉變，使得可能不需要安全監測程式。

位址轉譯

【0053】 由MMU 28執行的一個任務係虛擬位址(virtual address, VA)與實體位址(physical address, PA)之間的位址轉譯。在處理電路系統4上執行的軟體使用虛擬位址指定記憶體位置，但此等虛擬位址可由MMU 28轉譯成識別記憶體系統位置以存取的實體位址。使用虛擬位址的益處係允許管理軟體（諸如作業系統(OS)）控制對軟體呈現之記憶體的視域。OS可控制什麼記憶體可見、位於其的該記憶體可見的虛擬位址、及容許什麼存取存取該記憶體。此允許OS將應用程式沙盒化（將一個應用程式的資源對另一應用程式隱藏）及提供底層硬體的抽象化。使用虛擬位址的另一益處係OS可將記憶體的多個片段實體區域對應用程式呈現為單一連續虛擬位址空間。虛擬位址亦對在編寫其等的應用程式時不會知道系統的確切記憶體位址的軟體開發人員有益。使用虛擬位址，軟體開發人員不需要關心實體記憶體。應用程式知道其取決於一起運作以執行位址轉譯的OS及硬體。

【0054】 實際上，各應用程式可使用其自有之將映射至實體系統中的不同位置的虛擬位址組。由於作業系統在不同應用程式之間切換，其重規畫該映射。此意謂著用於目前應用程式的虛擬位址將映射至記憶體中的正確實體位置。

【0055】 虛擬位址通過映射轉譯成實體位址。虛擬位址與實體位址之間的映射儲存在轉譯表（有時稱為頁表）中。轉譯表儲存在記憶體中且由軟體（一般而言，OS或超管理器）管理。轉譯表不係靜態的，且表可隨著軟體變化的需要更新。此改變虛擬位址與實體位址之間的映射。

【0056】 對於在處理電路系統4在特定執行狀態子集中時（具體而言，在處理電路系統4在非安全EL0或非安全EL1中時）執行的記憶體存取，使用如圖3所示的二階段位址轉譯（對於其他執行狀態，使用1階頁表的一階段位址轉譯即足夠）。因此，來自非安全EL0及非安全EL1的虛擬位址係使用二組表轉譯。此等表支援虛擬化，且允許超管理器將由給定虛擬機器(VM)（該虛擬機器對應於客作業系統及由該客作業系統控制的應用程式）所見的實體記憶體的視域虛擬化。將由OS控制的該組轉譯稱為1階。1階表將虛擬位址轉譯成中間實體位址（IPA –稍早提及的中間位址的實例）。在1階中，OS認為IPA係實體位址空間。然而，超管理器控制稱為2階的第二組轉譯。此第二組轉譯將IPA轉譯成實體位址。

【0057】 將1階及2階轉譯表實施為階層式表結構，包含如圖4及圖5所示之分別用於1階及2階的若干個層的轉譯表。在此實例中，1階表及2階表二者可具有至多4層的頁表，亦即0層(L0)、1層(L1)、2層(L2)、及3層(L3)。

【0058】 為定位給定位址的實體位址映射，執行包含一或多個轉譯表查找的轉譯表查核。轉譯表查核係將虛擬位址轉譯成實體位址所需的該組查找。對於非安全EL1及EL0轉譯方案，此組包括用於1階轉譯及2階轉譯二者的查找（見以下顯示的圖6）。由使用1階及2階查找的成功轉譯表查核傳回的資訊係：

- 所需的實體位址（基於至中間位址的 1 階映射及至實體位址的 2 階映射轉譯）。

- 目標記憶體區域的存取權限及/或記憶體屬性，其提供與如何控制對該記憶體區域之存取有關的資訊。此等可包括定義在 1 階表結構中的 1 階存取權限及/或屬性及定義在 2 階表結構中的 2 階存取權限及/或屬性。

【0059】 為遍歷1階及2階結構的給定一者，查核基於指定在轉譯表基底位址暫存器（TTBR用於1階、VTTBR_EL2用於2階）中的位址針對最初查找以頂層(L0)轉譯表的讀取開始。各轉譯表查找傳回指示下列一者的描述符：

- 該項係 1 階或 2 階結構之遍歷之提供正尋找之位址映射的最終項。若項在最終 L3 中，則將此項稱為頁描述符(Page descriptor, D_Page)，而若提供查核之最終項的該項在較高層的一者，將其稱為區塊描述符(Block descriptor, D_Block)。遍歷的最終項含有存取的輸出位址（OA –亦即，1 階係 IPA 或 2 階係 PA），及權限及屬性。若區塊描述符係在轉譯表結構的較高層找到時，此意謂著區塊描述符表示尺寸比由在 L3 的單一項表示的 4kB 記憶體頁更大的記憶體區域（在 L1 及 L2 由區塊描述符表示的特定尺寸取決於用以索引至 L1 或 L2 表中之索引位元的數目–在此實例中，L1 及 L2 區塊描述符分別表示 1GB 及 2MB 區域）。
- 需要額外的查找層。在此情形中，將該項稱為表描述符(Table descriptor, D_Table)，因為其提供用於在表之另外層中的該查找的轉譯表基底位址。表描述符亦可可選地提供可施用至最終轉譯的其他階層屬性。轉譯表項在層 1 及層 2 的編碼將區塊描述符與表描述符區分開。
- 描述符係無效的。在此情形中，記憶體存取產生轉譯錯誤。

【0060】 圖4繪示使用提供為表查找之輸入位址的虛擬位址的各別位元索引1階轉譯表。頂層表L0的基底位址係從TTBR讀取，且L1、L2、L3表的基底位址係藉由分別儲存在L0、L1、L2表中之索引表描述符中的位址指示（若區塊描述符未於L1或L2表中識別到—若區塊描述符在L1或L2的索引項中找到，則遍歷在已找到輸出位址映射的該層停止）。在1階轉譯表之給定層內選擇的特定項係基於對應於提供為查找之輸入位址的虛擬位址的特定位元子集的索引值a、b、c、d判定。圖4繪示在一個特定實例中將輸入位址的哪些位元用於各索引值a、b、c、d。相關項在給定表中的位址係藉由將索引位元a、b、c、或d的倍數加至該給定表之基於TTBR判定的基底位址或指定在先前層的表描述符中的位址而獲得（施加至索引值的乘數對應於一個轉譯表項的尺寸）。

【0061】 類似地，圖5繪示使用提供為2階表查找之輸入位址的中間位址的各別位元索引2階轉譯表。索引類似於圖4中針對1階所示者，但使用不同的基底位址暫存器VTTBR_EL2以提供L0表的基底位址。如圖5之實例所示，對於2階查找，基於儲存在控制暫存器VTCR_EL2.SL0中之可指定查找應在L0或L1其中一者開始的值改變2階轉譯表的查核在其開始的開始層係可行的。若2階查找在L0開始，則層0、1、2、3的索引分別使用類似於圖4之用於1階的索引值a、b1、c、d。若2階查找在L1開始，則索引以類似方式執行，但現在在查找的頂層(L1)使用更大數目的索引位元b2，如圖5所示。提供可變開始層不為必要特徵，且若有需要，可省略之。雖然未顯示於圖4中，對1階的查找提供之可變開始層亦會係可能的。

【0062】 如圖6所示，實際上，當執行包括1階及2階轉譯二者的完整轉譯表查核時，則從TTRB及在1階L0、L1、L2轉譯表中存取的表描述符獲得的各1階表基底位址將係本身需要使用2階轉譯表轉譯的中間位址。因此，在轉譯表查核未遇到任何區塊描述符而一路繼續進行至找到頁描述符之L3時的情形中，則全部頁表查核程序可包括以下列序列存取多層頁表：

- 1 階 L0 頁的基底位址至實體位址的 2 階轉譯（由於 1 階轉譯係由作業系統組態，1 階 L0 基底位址一般係中間實體位址）。2 階轉譯包括 4 個查找（2 階 L0；2 階 L1；2 階 L2；2 階 L3）。
- 在基於目標虛擬位址之 L0 索引部分「a」及經轉譯 1 階 L0 基底位址而獲得之該位址的項的 1 階 L0 查找，以獲得 1 階 L1 基底位址（中間實體位址）
- 1 階 L1 基底位址至實體位址的 2 階轉譯（再次包含 4 個查找）。
- 在基於目標虛擬位址之 L1 索引部分「b」及經轉譯 1 階 L1 基底位址而獲得之該位址的項的 1 階 L1 查找，以獲得 1 階 L2 基底位址（中間實體位址）
- 1 階 L2 基底位址至實體位址的 2 階轉譯（再次包含 4 個查找）
- 在基於目標虛擬位址之 L2 索引部分「c」及經轉譯 1 階 L2 基底位址而獲得之該位址的項的 1 階 L2 查找，以獲得 1 階 L3 基底位址（中間實體位址）
- 1 階 L3 基底位址至實體位址的 2 階轉譯（再次包含 4 個查找）。

- 在基於目標虛擬位址之 L3 索引部分「d」及經轉譯 1 階 L3 基底位址而獲得之該位址的項的 1 階 L3 查找，以識別對應於目標虛擬位址的目標中間實體位址。
- 目標中間實體位址至目標實體位址的 2 階轉譯（再次包含 4 個查找），該目標實體位址表示記憶體中對應於原始目標虛擬位址存取的位址。

【0063】 因此，不使用任何快取，且假設2階的開始層係L0，轉譯總共將包含24個查找。若2階的開始層係L1，此可將查找的數目降低至19（所執行的5個2階轉譯各者少一個查找）。然而，如可自上述序列見到的，由於執行整個頁表查核程序可能需要大數目的對記憶體的存取以對位址轉譯的各階通過頁表的各層，其可係非常緩慢的。此係為何快取從MMU 28之TLB 29中的轉譯表查核導出的資訊常係所欲的。經快取資訊可不僅包括從VA至IPA的最終1階位址映射、從IPA至PA的最終2階映射、或從VA直接至PA的經組合1階及2階映射（從1階及2階結構的先前查找導出），且亦可將來自1階表及2階表之較高層頁表的項快取在MMU 28的TLB 29內。即使給定目標位址的最終層位址映射目前不在位址轉譯快取記憶體中，此可允許略過全部頁表查核的至少一些步驟。

【0064】 圖6使用指定可對二階段位址轉譯中所涉及之轉譯表項的一些定義的特定權限或性質的資訊註解。一旦此等權限及性質已於下文解釋，此將於稍後更詳細地描述。

記憶體管理單元實例

【0065】 圖7更詳細地繪示記憶體管理單元28。雖然圖1及圖7為了簡潔起見而顯示單一MMU 28，提供分開的指令側及資料側MMU以分別處置用於由

提取級6起始之指令提存取的記憶體管理操作及由載入/儲存單元26起始之資料存取亦係可能的—在此情形中，指令側及資料側MMU二者可具有圖7所示的組件。除了TLB 29外，MMU 28包括存取控制電路系統50以用於檢查指定在經查找轉譯表項中的存取權限，及根據該等存取權限控制記憶體存取請求的處置。例如，存取控制電路系統50可實施用於判定特定類型的記憶體存取請求是否滿足指定在記憶體之經存取之給定區域的對應轉譯表項中的權限的檢查（例如，基於請求係讀取、寫入、或指令提取請求，或基於所執行之導致請求發布之指令的類型）。MMU亦包括轉譯表查核控制電路系統52，該轉譯表查核控制電路系統在來自轉譯表的所需資訊在TLB 29中已不可用的事件中發布對記憶體的記憶體存取請求以在轉譯表查核程序期間請求讀取轉譯表項，如以上圖4至圖6中所示。轉譯表查核控制電路系統52可負責產生待讀取之記憶體系統位置的位址以獲得1階或2階轉譯表結構中的有關轉譯表項。額外地，在執行轉譯表查核的同時，轉譯表查核控制電路系統52可產生請求更新在轉譯表查核中經遍歷的某些轉譯表項內的存取追蹤後設資料的後設資料更新寫入請求。此等後設資料更新寫入請求可更新存取追蹤後設資料以反映特定記憶體區域已存取，其對管理諸如分頁的操作可係有用的。由於後設資料更新寫入請求的位址係在轉譯表查核中存取之轉譯表項的位址，而非經存取之資料或指令的位址，後設資料更新寫入請求係以硬體產生，以指定不直接指定為指令提取位址的位址，或載入/儲存從由處理電路系統4執行之載入/儲存指令的運算元導出的目標位址。

【0066】 MMU 28具有對用於控制轉譯表查核及記憶體管理操作的其他態樣的各種控制暫存器的存取。例如，控制暫存器可包括1階及2階基底位址暫

存器TTBR_EL1、VTTBR_EL2，如相關於圖4及圖5於稍早提及的。回應於在例外等級EL1、EL2、或EL3執行的指令（亦即，在第一執行狀態或具有比第一執行狀態更大特權的執行狀態中），暫存器TTBR_EL1中的1階基底位址係可寫入的。回應於在例外等級EL2或EL3執行的指令（亦即，在第二執行狀態或具有比第二執行狀態更大特權的執行狀態中），暫存器TTBR_EL2中的2階基底位址係可寫入的。在一些情形中，設定控制值以指示應將由在EL1執行之指令觸發的對TTBR_EL1的寫入捕捉至EL2，使得在EL2操作的超管理器可檢查該更新係由作業系統請求，且若有需要，防止該更新係可行的。控制暫存器亦包括暫存器TCR_EL1、VTCR_EL2，該等暫存器用以指定影響以其執行1階及2階轉譯及存取權限檢查之方式的各種控制狀態值。例如，可將指定2階查核之開始層的控制值指定在VTCR_EL2中。再者，TCR_EL1或VTCR_EL2控制暫存器可指定其指定啓用/停用什麼類型之安全檢查的控制值。如下文更詳細地討論的，控制暫存器亦可包括分別用於有效項及無效項之用於指定更新受限制位元子集的遮罩暫存器（標記為RCWMask_Valid_EL2及RCWMask_Invalid_EL2），對該等位元的更新限制在受保護1階轉譯表項中。將理解亦可提供另外的控制暫存器，且用於控制暫存器的標籤可變化。例如，可提供一或多個權限間接暫存器以指定可由給定轉譯表項參考以指定用於給定轉譯表項的存取權限資訊的間接存取權限資訊。相同資訊以不同格式配置在控制暫存器內亦係可能的，使得資訊至一個或另一個控制暫存器的特定分配不係必要特徵。

【0067】 如圖7所示，當請求對經編碼為受保護項的1階轉譯表項更新時（此將於下文更詳細地描述），設備可具有用於執行受保護項檢查的受保護項

檢查電路系統54。如圖7中的虛線所示，將受保護項檢查電路系統54實施在處理系統內的不同位置係可能的。例如，受保護項檢查電路系統54可係MMU 28之存取控制電路系統50的部件。替代地，受保護項檢查電路系統可實施在更接近由待使用受保護項檢查電路系統54檢查之給定記憶體存取請求存取的實體記憶體系統位置的記憶體系統組件56內。例如，記憶體系統組件56可係快取記憶體30、32、用以管理多個處理器核心對共用記憶體之存取的互連、或與特定記憶體儲存單元關聯的記憶體控制器。再者，受保護項檢查電路系統54可包括在系統中的多個位置的分散式邏輯（例如，MMU 28、載入/儲存單元26、及/或記憶體系統組件56）。

轉譯表存取權限及屬性

【0068】 圖8繪示用於1階及2階轉譯表結構中的轉譯表項的實例格式。將理解相同資訊可以不同配置表示，且因此描述符內的欄位的特定排序及布局可與圖8所示者不同。

【0069】 在此實例中，有效轉譯表描述符具有設定成1的最低有效位元且無效轉譯表描述符具有設定成0的最高有效位元。對於在轉譯表結構之0層、1層、2層的一者讀取的有效描述符，第二最低有效位元區分描述符係表描述符（第二最低有效位元設定成1）或區塊描述符（第二最低有效位元設定成0）。在1階或2階結構的L3的頁描述符可具有設定成1的第二最低有效位元，以允許頁描述符與區塊描述符區別開。當然，有效/無效項，及表/區塊/頁描述符亦可藉由其他編碼方法區別開。

【0070】 對於1階及2階項二者，有效表描述符提供指示轉譯表在1階或2階轉譯表結構的次一層的基底位址的次一層表位址60。有效1階區塊或頁描述符提供對應於用以索引1階轉譯表結構的虛擬位址的中間位址映射62。有效2階區塊或頁描述符提供對應於用以索引2階轉譯表結構的中間位址的實體位址映射64。

【0071】 1階區塊及頁描述符亦提供用以控制對對應記憶體區域之存取的1階存取權限66。例如，1階存取權限66（一般由在EL1的OS設定）可指定區域是否允許讀取、寫入、及/或用於可執行指令的指令提取。

【0072】 類似地。2階區塊及頁描述符提供用以控制對對應記憶體區域之存取的2階存取權限68。再次，2階存取權限68（一般由在EL2的超管理器設定）可指定區域是否允許讀取、寫入、及/或用於可執行指令的指令提取。若1階存取權限66與2階存取權限68之間存在衝突，則受更限制性的屬性組可取得優先權。

【0073】 1階或2階區塊/頁描述符亦可指定與記憶體區域關聯其他屬性，未顯示於圖8中。例如，此等屬性可指定性質，諸如是否允許從對應記憶體區域快取資料，該區域是否定義為裝置記憶體，使得裝置記憶體的不同記憶體存取的重排序或合併不被允許等。

【0074】 1階區塊/頁描述符亦可指定可由作業系統使用以追蹤給定記憶體區域之存取頻率的存取追蹤後設資料。例如，後設資料可包括存取旗標 (access flag, AF) 70及髒位元修改符(dirty bit modifier, DBM) 72。

【0075】 作業系統可週期性地清除對應於一組受監測記憶體區域之項中的存取旗標。當對此等記憶體區域的一者進行讀取存取時，可設定對應1階區塊或頁描述符中的存取旗標70（若尚未在稍早存取之後設定）（導致存取旗標70設定的記憶體存取請求可係由稍早提及之轉譯表查核控制電路系統52所產生的後設資料更新寫入請求的一者）。在監測週期之後，作業系統可接著檢查存取旗標70以輔助可從與多頻繁地存取某些頁有關的資訊獲益的操作。例如，作業系統可使用每一記憶體區域之追蹤記憶體區域已存取多少次的項在記憶體中維持另外的追蹤資料結構，且因此在各監測週期的結束，可遞增該另外追蹤結構之對應於具有存取旗標70經設定之記憶體區域的項。在若干個監測週期之後，該另外追蹤結構將因此提供對對應記憶體區域的存取的相對頻率的指示。此可提供用於控制諸如分頁之操作的有用資訊，其中知道記憶體的最不頻繁存取頁可係有用的，可相較於其他更頻繁存取頁優先將其之對應資料移出至外部儲存。

【0076】 類似地，DBM 72有助於追蹤哪些頁已遭受寫入。若作業系統希望追蹤給定頁是否已寫入，當該頁經映射或在監測週期的開始時，作業系統可將該頁的存取權限設定成「唯讀」（即使意圖允許寫入該頁）並設定DBM位元72。關於在DBM位元72經設定時由對唯讀頁的寫入所導致的存取權限錯誤，作業系統可從DBM位元72經設定而判定此不係唯讀權限的「真正」違規，且取而代之地導致作業系統更新儲存在記憶體中之追蹤遭受寫入請求之頁的資料結構，且亦更新該頁的寫入存取權限以指示該頁現在可寫入而不觸發錯誤。在監測週期之後，記憶體中的追蹤資料結構可由軟體使用以在移出特定區域時判定

是否需要將形成該區域的經修改資料寫回至外部儲存，或（若未發生寫入）由於若資料係乾淨的，可假設在外部記憶體中的對應資訊仍係相同的，判定儲存在晶片上記憶體中的資料是否可在移出該區域時簡單地拋棄。

【0077】 存取旗標70及隣位元修改符72僅係可儲存在轉譯表項內之可能的存取追蹤資料的一些實例，且其他實例可提供其他類型的存取追蹤後設資料。例如，在另一實例中，可將多位元存取計數器提供為存取追蹤後設資料。再者，在取代將DBM位元72用以修改寫入請求上的唯讀存取權限違規的處置且觸發寫入權限的更新的另一實例中，DBM旗標72可取而代之地以與如稍早描述之在對頁的首次存取時以其更新存取旗標70之方式類似的方式回應於在清除DBM旗標72之後對頁的首次寫入而直接更新。

【0078】 如圖8所示，各種轉譯表描述符亦可包括對保護1階轉譯表項免於在攻擊者的攻擊下由作業系統碼所損壞係有用的若干個其他資訊片段。一般作業系統碼可包括許多行的碼，其可能難以完全驗證為對攻擊安全，且因此提供用於保護免於企圖修改該等項中的位址映射或權限而以未授權方式提供攻擊者存取記憶體之區域的權力的攻擊者可能能夠修改作業系統碼的行為以導致對用以儲存轉譯表項之記憶體之區域的寫入的可能性的架構機制係所欲的。

【0079】 如圖8所示，為提供轉譯硬化機制，下文描述之用於硬化1階轉譯表以免於攻擊的額外屬性及權限包括下列者：

- 2階區塊/頁描述符指定具有指示對應記憶體區域是否具有部分唯讀 (partially-read-only, PRO)權限之編碼的 2階存取權限 68（部分唯讀權限亦可稱為「通常唯讀(mostly-read-only)」權限）；

- 在 1 階轉譯表結構的所有層的有效 1 階描述符（包括表描述符及區塊/頁描述符）具有指定該轉譯表項是否係「受保護」項的編碼，相較於未受保護項，對該受保護項提供免於未授權更新的額外保護。例如，有效 1 階描述符內的位元欄位 76 可表示該項是否係受保護項。
- 在 1 階轉譯表結構的所有層的無效 1 階描述符亦可具有指定該轉譯表項是否係「受保護」項的編碼。此可使用位元欄位 78 指示，與用以表示有效 1 階轉譯表項的受保護項的位元欄位 76 相比，該位元欄位可在轉譯表項編碼內的不同位置。
- 2 階區塊/頁描述符可具有指定對應記憶體區域是否具有反別名性質的指示符 79。在一些實例中，可將反別名性質的存在與否編碼在亦可傳訊其他類型之性質的經組合位元欄位中，或替代地反別名位元欄位可係不傳訊任何其他資訊的獨立位元欄位。若經指定，反別名性質指示對於待允許之對對應實體位址的存取，在轉譯表查核中存取以獲得用於存取 2 階描述符之中間位址的所有 1 階轉譯表項將需要使用位元欄位 76 指定為受保護項且將需要儲存在記憶體的區域中，用於該等區域的對應 2 階區塊/頁描述符指示部分唯讀權限 74。
- 2 階區塊/頁描述符亦可在 2 階存取權限 68 中指定指示是否允許對應記憶體區域保持用於 1 階轉譯之頂層轉譯表（亦即，圖 4 及圖 6 之實例中的 1 階 L0 表）的 1 階頂層項存在權限 80。在一個實例中，2 階存取權限 68 的編碼可使得將 1 階頂層項存在權限編碼為 PRO 權限的另外

屬性，使得允許經編碼以用於 2 階存取權限 68 的值可包括指示下列者的值：

- o 不具有 1 階頂層項存在權限的 PRO 權限；
- o 具有 1 階頂層項存在權限的 PRO 權限；或
- o 一或多種其他類型之不具有 PRO 權限或 1 階頂層項存在權限的權限（例如唯讀權限、讀/寫權限、及/或執行權限）。

【0080】 在此情形中，與PRO權限無關地指定1階頂層項存在權限可係不可能的。然而，其他實施方案可與PRO權限無關地編碼1階頂層項存在權限，使得即使PRO權限未提供，仍可指定1階頂層項存在權限。

【0081】 此等屬性及權限的使用將於下文更詳細地討論。應理解並非所有此等屬性及權限皆需要在每一個可能實施方案中受支援。雖然圖8繪示將S1及S2存取權限直接指定在轉譯表項之編碼中的實例，使用指定在權限暫存器中的權限間接地指定相同資訊亦係可能的。例如，S1權限欄位66或S2權限欄位68可指定選擇權限暫存器的若干個權限欄位的何者指定對應轉譯表項之存取權限的索引值。轉譯表項的一些欄位取決於儲存在控制暫存器中的控制狀態而以不同方式解譯亦係可能的。例如，1階轉譯表項的受保護項欄位76在儲存在控制暫存器中的控制值具有第一值時可解譯為指示1階轉譯表項是否受保護，及在控制值具有第二值時可以不同方式解譯。類似地，2階轉譯表項的反別名性質欄位79在儲存在控制暫存器中的控制值具有第一值時可解譯為指示2階轉譯表項是否具有反別名性質，及在控制值具有第二值時可以不同方式解譯。

【0082】 雖然將S1權限66及S2權限68顯示為由對應S1或S2描述符直接指定，此等權限（或由轉譯表項指定的其他資訊）使用間接暫存器間接地指定亦係可能的，如相關於圖18於下文所示的。

部分唯讀權限

【0083】 圖9總結對於由2階存取權限68標記成具有部分唯讀(PRO)權限之記憶體區域的寫入存取控制行為。具有PRO權限的記憶體區域至少對於當目前執行狀態係EL1（預期作業系統碼在其中執行的狀態）時發布的寫入請求對限制性寫入請求類型子集係可寫入的，但對寫入請求類型視為係唯讀的。由於僅一些寫入請求類型將記憶體區域視為係唯讀的，因此將此權限描述為部分唯讀權限。

【0084】 圖9總結經容許及經禁止寫入記憶體區域之寫入請求的類型，用於該記憶體區域的對應2階轉譯表項將該區域定義成具有PRO權限。當寫入在EL1發布時容許寫入至PRO區域的限制性寫入請求類型子集包括由MMU 28產生之更新轉譯表項中的存取追蹤後設資料（諸如存取旗標70）的後設資料更新寫入請求、或在隣位元修改符72經設定時的情形中的寫入權限，如上文所討論的。再者，限制性子集可包括在例外狀態EL1執行的至少一個預定類型的轉譯表項更新指令，該指令可係意圖在更新轉譯表項時使用的專用類型的指令，以表達程式碼之將用於更新轉譯表項的此類寫入與用於更新轉譯表項以外之資料的寫入區分開的意圖。例如，預定類型的轉譯表項更新指令可包括相關於以下的圖12至圖14討論的受保護項檢查讀取-檢查-寫入(RCW)指令的變體。如圖9所示，禁止回應於在例外狀態EL0及EL1的一者中執行的至少一個其他類型的

第41頁，共 88 頁(發明說明書)

儲存指令而發布的寫入請求寫入至記憶體**PRO**區域。例如，經禁止寫入請求類型可包括由處理電路系統4支援之指令集架構中的大部分儲存指令。藉由在區域以**PRO**權限標記時將更新轉譯表項的能力限制在一組有限指令類型中，此降低攻擊者可用之在嘗試損壞1階轉譯表項時利用的攻擊表面，例如，使用用於不係限制性寫入請求子集的一者的通用儲存的位址運算元篡改將不允許存取記憶體的**PRO**區域。

【0085】 可選地，可容許回應於在執行狀態**EL2**或**EL3**的一者中執行的儲存指令而發布的寫入請求寫入至部分唯讀區域，即使其等係若在執行狀態**EL0**或**EL1**執行將已被禁止寫入該區域之類型的儲存指令。然而，如稍早提及的，此不係必要的。

【0086】 圖10係繪示處理指令及控制記憶體管理操作之方法的流程圖。在步驟500，處理電路系統4在與不同特權等級關聯的若干個執行狀態**EL0**至**EL3**的一者中執行指令。在步驟502，回應於記憶體存取請求，**MMU 28**執行由記憶體存取請求指定之目標虛擬位址(**VA**)至目標實體位址(**PA**)的二階段位址轉譯，其中從目標**VA**至目標**PA**的映射取決於從目標**VA**至目標中間位址(**IPA**)的1階段位址映射及從目標**IPA**至目標**PA**的2階段位址映射。在步驟504，**MMU 28**的存取控制電路系統50至少基於指定在對應2的轉譯表項中的2階存取權限資訊68對記憶體存取請求執行權限檢查。權限檢查亦可基於1階存取權限資訊66。2階存取權限資訊66具有指定對應於目標**IPA**的記憶體區域是否具有**PRO**權限的編碼。在步驟506，當記憶體存取請求係在預定執行狀態（例如，**EL1**）中發布的寫入請求、2階存取權限資訊確實指定**PRO**權限、且寫入請求係允許寫入至記

記憶體之**PRO**區域的限制性寫入請求類型子集以外的寫入請求類型時，**MMU 28**拒絕該記憶體存取請求。可選地，當記憶體存取請求係在當**PRO**權限由2階存取權限資訊指定時在預定執行狀態以外的執行狀態（例如，**EL0**）中發布的寫入請求且該寫入請求類型不係限制性寫入請求類型子集的一者時，**MMU 28**亦可拒絕該記憶體存取請求。

【0087】 圖11更詳細地繪示藉由**MMU 28**的存取控制電路系統50執行的部分唯讀檢查。在步驟600，當處理電路系統4在預定執行狀態(**EL1**)中時，發布寫入記憶體存取請求。寫入請求指定目標**VA**。寫入請求可回應於由處理電路系統執行的載入/儲存指令而已由處理電路系統4的載入/儲存單元26發布，或在請求指令提取時已由提取級6發布。寫入請求亦可係由**MMU 28**發布的後設資料更新寫入請求，以在轉譯表查核程序期間更新轉譯表項中的存取追蹤後設資料。

【0088】 在步驟602，將目標**VA**轉譯成識別待存取之記憶體系統位置的目標**PA**。為執行轉譯，**MMU 28**可在**TLB 29**內查找目標**VA**，且若從目標**VA**至目標**PA**的映射在**TLB 29**中已可用，則轉譯表查核不係必要的。否則，可能需要圖6所示之轉譯表查核程序的至少部分，雖然若從用於轉譯表查核的該部分的對應轉譯表項導出的資訊已快取在**TLB 29**中，一些部分可能能夠跳過。對於從非安全**EL1**發布的寫入記憶體存取請求，轉譯基於定義在1階及2階轉譯表二者中的映射而執行為二階段位址轉譯，雖然由於提供快取直接從目標**VA**至目標**PA**之映射（取決於1階及2階映射二者）的經組合1階/2階**TLB**，以及對應的1階及2階權限資訊，以避免目標**IPA**需要明確地判定係可能的，此並不必然意謂著需要執行二個單獨轉譯。

【0089】 在步驟604，存取控制電路系統檢查對應2階(S2)轉譯表項（指定從目標IPA至目標PA之映射的2階項）是否指定PRO權限。若如此，則在步驟606，存取控制電路系統檢查受處理的寫入請求是否係限制性寫入請求類型子集的一者。若目前寫入請求不係限制性寫入請求類型子集的一者（包括至少後設資料更新寫入請求），則在步驟608，拒絕記憶體存取請求且傳訊錯誤。若寫入請求係限制性寫入請求類型子集的一者，則部分唯讀檢查通過且因此方法繼續進行至步驟610。再者，若在步驟604，對應2階轉譯表項之前未指定PRO權限，則可省略步驟606的部分唯讀檢查，且因此方法直接從步驟604繼續進行至步驟610。

【0090】 在步驟610，存取控制電路系統判定允許寫入記憶體存取請求繼續進行所需的任何其他檢查是否獲得滿足。例如，此等檢查可包括使用1階存取權限66的檢查、在PRO權限未指定時的情形中，使用其他2階存取權限68的檢查、基於請求之前係從安全或非安全狀態發布的安全檢查（在支援安全狀態的實施方案中）、以及特定用於特定指令類型的其他檢查，諸如相關於圖12至圖14於下文討論之關於在目標記憶體位置的資料是否係受保護轉譯表項的檢查。若此等其他檢查的任一者未獲滿足，則再次在步驟608，拒絕記憶體存取請求且傳訊錯誤。可設定錯誤症候群資訊以區別錯誤的原因。若在步驟610執行的檢查獲得滿足，則在步驟612，可容許記憶體存取請求繼續進行，且因此與目標PA關聯的記憶體系統位置可使用由寫入請求指定的寫入資料更新。

【0091】 因此，如稍早討論之圖6所示，PRO權限可指定在2階轉譯表項的2階存取權限68中，該等項用以提供保持在1階表結構的遍歷中使用的1階轉

譯表的各種層的記憶體系統位置的實體位址，以獲得含有敏感資訊之記憶體區域的中間位址。此保護該等1階轉譯項免於在惡意方的攻擊下由錯誤地運作的碼或作業系統碼所損壞，因為PRO權限將寫入至對應記憶體區域的能力限制在有限指令類型子集，大幅降低可易為1階轉譯表損壞之碼的行數目。然而，用於更新轉譯表項中的存取追蹤後設資料的硬體產生寫入請求仍可容許用於此類區域，以避危及作業系統之分頁操作的效率。

【0092】 雖然圖11顯示對在預定執行狀態EL1中時發布的寫入記憶體存取請求執行的部分唯讀檢查，其亦可對其他執行狀態執行。然而，因為對於在最低特權執行狀態EL0中發布的寫入請求，保持1階轉譯表的記憶體區域在任何情形中將藉由1階存取權限66標記為不可為在EL0操作的應用程式級碼存取，所以1階權限檢查可能已防止此類寫入請求損壞1階轉譯表，此可不係必要的。再者，因為超管理器或監測碼可係正在控制允許什麼更新對1階轉譯表更新上的限制的碼，對於在EL2或EL3執行的碼，轉譯表不會使用二階段位址轉譯，且不可能將寫入限制在儲存1階轉譯表項的區域。因此，一些實施方案可將部分唯讀檢查限制成僅在目前執行狀態係EL1時執行。其他實施方案可不論哪個執行狀態係目前執行狀態，施加部分唯讀檢查。

用於1階轉譯表項的受保護項編碼

【0093】 將特定記憶體區域標記為對限制性寫入類型子集以外的寫入請求係唯讀的PRO權限的使用對保護1階表免於損壞係有幫助的。然而，如圖6所示，一般而言，在轉譯表結構之給定層的給定轉譯表佔據記憶體中的整個頁，且因此PRO權限將施加至在1階轉譯表結構之給定層的整個轉譯表，其可包括用

第45頁，共 88 頁(發明說明書)

於可包括用於需要受保護免於未授權存取之敏感資訊的一些記憶體區域及僅含有不需要此保護之非敏感資訊的其他記憶體區域的各種記憶體區域的轉譯表項。

【0094】 可能提供如下文進一步討論之不支援1階轉譯表項之受保護項編碼的使用的實施方案。在此情形中，為允許作業系統更新與含有非敏感資訊之未受保護區域關聯的某些1階轉譯表項，在不係允許寫入至PRO區域之寫入請求類型的一者的對PRO區域的寫入存取上產生的錯誤可對在EL2操作的超管理器導致陷阱，且超管理器接著可以軟體判定作業系統希望對其更新1階轉譯表項的該區域是否應受保護以免於由作業系統更新，且若該區域不需要受保護，可允許由作業系統請求的更新繼續進行。然而，實際上，作業系統可能需要相對頻繁地改變用於記憶體之未受保護區域的轉譯表項，且因此每次需要更新時捕捉給超管理器就效能而言可係緩慢的。

【0095】 用於1階轉譯表項的受保護項編碼（例如，使用位元76、78）幫助允許作業系統對未受保護項進行更新而無需超管理器干預（且可選地，對於一些實施方案，對受保護項的無更新限制位元進行更新而無需超管理器干預）。即使在給定1階轉譯表儲存在記憶體的PRO區域中時，由於其含有受保護項及未受保護項的混合，此由於可更常避免超管理器介入而幫助改善效能。處理電路系統4的指令解碼器10及執行級16支援至少一種類型的指令，稱為受保護項檢查類型的讀取-檢查-寫入(read-check-write, RCW)指令，其可用以請求對給定記憶體系統位置的更新，其中該更新取決於檢查儲存在經存取記憶體系統位置的資料以檢查其是否具有與受保護1階轉譯表項的編碼一致的值的受保

護項檢查而進行。若發現在經存取記憶體系統位置的資料具有與係受保護1階轉譯表項的資料一致的值，則抑制對給定記憶體系統位置的至少一更新受限制位元子集的更新。允許RCW指令由在EL1執行的作業系統執行。RCW指令係允許更新由對應2階轉譯表項以PRO權限標記之記憶體區域中的資料的限制性指令子集的一者。

【0096】 受保護項檢查藉由受保護項檢查電路系統54以硬體執行，其如圖7所示，可實施在MMU 28內，或實施成更接近儲存資料的記憶體系統位置，例如，在記憶體系統組件56（諸如快取記憶體、互連、或記憶體控制器）內。使用一組分散式邏輯亦係可能的，其中受保護項檢查電路系統54的一些部分實施在MMU 28（或管線的執行級16）中且其他部分實施成更接近記憶體儲存。將在受保護項檢查中執行的讀取、檢查、及寫入操作執行為原子（不可分）操作，使得當藉由在與執行RCW指令之緒相同的處理器電路系統上執行的另一緒或藉由另一處理器核心請求存取給定記憶體系統位置時，其他存取見到給定記憶體系統位置在處理RCW指令之前的值或給定記憶體系統位置在處理RCW指令之後的值不係RCW指令的任何部分效果，且回應於RCW指令，對給定記憶體系統位置的寫入在讀取在給定記憶體系統位置的資料的受保護項檢查與在給定記憶體系統位置的資料的後續更新之間的週期中更新給定系統位置亦係不可能的。用於對記憶體系統位置執行原子讀取/寫入操作的任何已知技術可用以強制該原子性（例如，在讀取與寫入之間的週期中鎖定記憶體位置以免於由其他操作存取，或若在讀取與寫入之間的週期中偵測到衝突存取，在該週期中允許衝突存取，但重開始RCW操作）。藉由迫使讀取、檢查、及寫入的原子性，此

避免可導致不正確處理結果的競賽條件。由於讀取、檢查、及寫入操作原子地執行，受保護項檢查電路系統54實施在更接近經更新的儲存位置的記憶體系統組件56內可係有用的，以相較於若經讀取資料已一路傳回直到處理器管線4之用於在寫入可繼續進行及將寫入資料傳回至儲存該資料之記憶體系統位置之前執行檢查的MMU 28或另一元件的持續時間，降低讀取與寫入之間的週期的持續時間。

【0097】 在圖8所示的實例中，有效及無效的1階轉譯表項二者具有允許將該項指定為受保護項的編碼。然而，能夠指定為受保護對無效項不係必要的，且其他實例可將受保護項編碼位元欄位78從無效項格式省略。再者，不同實施方案可選擇受保護項有多少個位元回應於RCW指令而使其等的更新受抑制的不同選項。一些實施方案可回應RCW指令而防止對受保護項的任何更新，其中僅回應於若在給定記憶體系統位置的資料未編碼為受保護項時的該RCW指令而容許更新。其他實施方案可指定更新受限制位元子集及無更新限制位元子集，且因此甚至對於受保護項，對無更新限制位元子集的更新可係可允許的。例如，可有對安全性並非關鍵的一些欄位，諸如存取旗標70及髒位元修改符72，可甚至允許在受保護項中更新其。哪些位元係更新受限制或無更新限制的可以非可程式化方式對給定架構固定，或可藉由軟體使用儲存在控制暫存器中的選擇值而係可程式化的。例如，選擇值可選自數個不同模式的一者，各模式與哪個位元係更新受限制的不同設定關聯。然而，在圖7的實例中，選擇值經編碼為位元遮罩，該位元遮罩使用儲存在遮罩暫存器（例如，顯示於圖7中之分別用於選擇有效項及無效項之更新受限制位元的RCWMask_Valid_EL2及

RCWMask_Invalid_EL2暫存器–RCW_Mask_Invalid_EL2暫存器可在無效項不能夠編碼為受保護項的實施方案中省略）中的選擇值識別更新受限制位元的位置。可將對選擇值的更新限制在臨限特權等級或更高等級執行的程式指令，例如，可僅允許在EL2或EL3執行的指令更新選擇值。可能有無論選擇值的狀態而強迫其係更新受限制的一些位元。例如，無論哪些其他位元能夠更新，可能不允許更新用以編碼項是否係受保護項的位元欄位76、78。一般而言，可禁止RCW指令改變特定項係受保護或未受保護的狀態。位元欄位76、78的設定將取而代之地由在更高特權等級（諸如EL2或EL3）執行的程式碼控制，其可正使用不同組之不將儲存受保護項的記憶體區域標記為部分唯讀的2階轉譯表存取記憶體，且因此可使用標準通用儲存指令設定受保護1階項的位元欄位76、78。

【0098】 有受保護項檢查可以其實施的各種方式。在一個實例中，若儲存在經存取記憶體系統位置的項係有效的且受保護，則無法改變其，且若其係無效的，則可改變其，包括使其有效（只要亦未使該項受保護）。替代地，有效項中可有受保護位元欄位76且無效項中可有受保護位元欄位78，且不允許改變受保護項，否則允許對以外的未受保護（有效或無效）項的更新（改變項是否受保護的狀態）。另一實例可在有效項中提供受保護位元欄位76，且在無效項中提供受保護位元欄位78，且可允許RCW指令對若其不受保護的項作出任何改變（除非使其受保護），而若其受保護，則RCW指令可如描述地對有效項的一些位元且對無效項中的一些位元作出改變。在一些實例中，除了保護或有效欄位以外，用於描述哪些位元受保護的機制係任何欄位的硬接線架構選擇。替代地，用於描述哪些位元在有效項中受保護的機制可使用由EL2擁有的遮罩暫

存器，及/或用於描述哪些位元在無效項中受保護的機制係由EL2擁有的遮罩暫存器。分別用於有效項及無效項之用於定義更新受限制位元之不同選擇係可行的—例如，一種方法可定義用於定義有效項之更新受限制位元之遮罩暫存器，但將用於無效項之更新受限制位元硬接線。

【0099】 當允許更新受保護項中的一些欄位時，在如何施加檢查上亦可存在變化，二個實例選項係：

- A) 受保護項檢查電路系統 54 讀取目前項以檢查該項是否係有效及/或受保護的，且接著僅儲存允許寫入的位元（不檢查 RCW 指令是否企圖改變不允許寫入之更新受限制位元）。
- B) 受保護項檢查電路系統 54 讀取目前項以檢查該項是否係有效及/或受保護的。若受保護，且 RCW 指令未企圖改變不允許寫入之任何位元，寫入可發生，但若 RCW 指令企圖更新任何更新受限制位元，寫入失敗且沒有寫入。

A及B二者皆係可行替代方案。

【0100】 回應於RCW指令，可將寫入成功或失敗之指示寫入至儲存在處理電路系統4之控制暫存器中之條件狀態旗標。例如，條件狀態暫存器可包括可取決於處理操作之結果設定且可由條件指令測試之若干個條件旗標（例如，負號旗標N、零旗標Z、進位旗標C、及溢位旗標V），該條件指令可有條件地取決於條件狀態旗標之狀態而觸發操作（諸如分支操作或算術/邏輯操作）。因此，基於由RCW指令請求之寫入之任何部分是否不成功而更新條件

狀態旗標，以允許後續指令取決於寫入的結果採取行動而不需要重讀取記憶體系統位置以檢查寫入是否成功可係有用的。

【0101】 圖12、圖13、及圖14繪示受保護項檢查RCW指令的若干個變體的處理。圖12繪示指令之儲存變體或交換變體之處理的實例（大部分處理步驟對二個指令相同，除了取決於變體的最終步驟726或728外）。儲存及交換變體二者皆指定提供用以產生待更新之給定記憶體系統位置之位址的位址運算元的暫存器Xd，及提供待寫入至給定記憶體系統位置的新資料的來源暫存器Xs。交換變體至少亦指定待將從給定記憶體系統位置讀取的舊資料寫至其的目的地暫存器Xt。由於儲存變體與交換變體的不同處在於不將舊資料寫入至任何目的地暫存器，儲存變體不需要指定任何目的地暫存器。然而，在一個實例中，除了在用指定目的地暫存器Xt的欄位具有預定值時可將指令視為儲存變體外，儲存變體及交換變體可使用相同編碼編碼。例如，一些指令集架構可將特定暫存器說明符（例如，暫存器31）定義為對應於「零」暫存器，當將該暫存器指定為指令的運算元時導致將該運算元視為彷彿其具有值零，而不需要實際地從以硬體提供的暫存器讀取該運算元。因此，在一些實例中，當將目的地暫存器Xt指定為「零」暫存器X31時，可將指令視為儲存變體。在其他實例中，可將儲存指令編碼為與交換指令完全不同的指令類型。

【0102】 在圖12的步驟700，位址運算元及待寫入的新資料（「NewData」）分別從由暫存器說明符Xd及Xs識別的暫存器讀取。在步驟702，基於位址運算元判定記憶體存取的目標位址。例如，可將位址運算元視為直接指定目標位址的絕對位址，或可定義相對於參考位址（諸如在另外基底

暫存器中的值或識別RCW指令本身之位址的程式計數器值)的偏移。基於位址運算元計算的目標位址係虛擬位址，且可藉由MMU 28轉譯成實體位址。在步驟704，假設通過目標位址是否可為目前指令存取的(受保護項檢查以外的)任何MMU檢查，可對記憶體系統發布讀取請求以獲得從對應於(經轉譯)目標位址的記憶體系統位置讀取的資料(「ReadData」)。此對應於RCW指令的「讀取」。

【0103】 如步驟706，受保護項檢查電路系統54判定ReadData是否具有與受保護1階(S1)轉譯表項的編碼一致的值。此對應於RCW指令的「檢查」部分。若ReadData不具有與受保護1階轉譯表項一致的值，則在步驟708，受保護項檢查電路系統檢查NewData是否經編碼為受保護1階轉譯表項。若如此，則在步驟710，拒絕由RCW指令請求的寫入，或替代地，可將由RCW指令指定為NewData的1階轉譯表項的無更新限制位元寫入至記憶體系統位置的對應位元，其中至少將用以編碼該項是否受保護的位元視為係不被寫入的更新受限制位元。總之，在步驟712，設定條件狀態旗標以報告失敗，以完全地實行由RCW指令請求的寫入。

【0104】 若在步驟706，將ReadData判定為經編碼為受保護1階轉譯表項，則在步驟716，受保護項檢查電路系統54判定讀取資料是否具有與有效或無效的1階轉譯表項一致的值。若讀取資料具有與無效受保護1階轉譯表項一致的值，則在步驟718，受保護項檢查電路系統54判定NewData是否企圖改變1階轉譯表項的任何無效項更新受限制位元(至少包括用以編碼該項是否受保護的任何位元)，且若如此，方法接著再次繼續進行至步驟710及712以抑制至少無

效項更新受限制位元的更新及設定條件狀態旗標（再次，此可藉由徹底拒絕寫入或藉由僅寫入至無更新限制位元而完成）。

【0105】 另一方面，若在步驟716，判定ReadData具有與經編碼為受保護項之有效1階轉譯表項一致的值，則在步驟720，受保護項檢查電路系統54判定NewData是否企圖改變從對應於目標位址的記憶體系統位置讀取的1階轉譯表項的任何有效項更新受限制位元（至少包括用以編碼該項是否受保護的任何位元）。若如此，則再次在步驟710，拒絕寫入或僅容許寫入無更新限制位元，且在步驟712，設定條件狀態旗標以報告寫入失敗。

【0106】 在不支援將無效轉譯表項編碼為受保護項的實施方案中，可省略步驟716及718，且方法可在將ReadData編碼為受保護項時的情形中直接從步驟706繼續進行至步驟720。

【0107】 若在步驟708，NewData待在ReadData不係未保護項時的情形中寫入，或在步驟718或720，NewData（在ReadData係受保護項時的情形中待寫入）未企圖改變任何更新受限制位元，則在步驟714，容許RCW指令的寫入，且因此將NewData寫入至對應於目標位址的記憶體系統位置。

【0108】 無論寫入成功或受拒絕（至少部分地），在步驟724，操作取決於所執行的目前RCW指令係儲存變體或交換變體而變化。若指令係儲存變體，則在步驟726，不需要進一步動作，且不將ReadData寫入至任何目的地暫存器。若指令係交換變體，則在步驟728，將ReadData寫入至目的地暫存器Xt。一些實施方案可不支援儲存及停止變體二者，在該情形中，步驟724可省略且方法可直接從步驟714繼續前進至步驟726及728的相關一者。

【0109】 在步驟704的讀取、在步驟714的寫入、及在步驟704與714之間執行的各種檢查操作作為一組不可分操作而原子地執行，對記憶體系統位置的中間寫入發生在步驟704的讀取與步驟710或714的寫入之間或另一執行緒見到執行該組操作的部分結果對於該組不可分操作係不可能的。

【0110】 圖13係繪示受保護項檢查RCW指令之比較及交換(compare-and-swap, CAS)變體之處理的流程圖。圖13之使用與圖12中相同的參考數字說明的步驟與上文討論的步驟相同。應注意與圖12相比，用於用以儲存ReadData及提供NewData之暫存器的符號已在圖13中交換– Xt現在係提供NewData的暫存器，且Xs係在寫入之前以ReadData的舊值寫入的目的地暫存器。圖13與圖12的不同處在於由於CAS變體指定額外的稱為比較資料（「CompareData」）的來源運算元，步驟700為步驟750所置換。在此實例中，為降低指令編碼時所需的暫存器欄位的數目，將CompareData指定在與在步驟728使用為用於寫入ReadData的目的地暫存器相同的暫存器Xs中，但此不是必要的，且其他實例可將比較資料指定在與Xs分開的另外暫存器中。

【0111】 步驟702及704與圖12中相同。在步驟704之後，執行額外步驟752以比較從對應於目標位址的給定記憶體系統位置讀取的ReadData及由RCW指令指定在暫存器Xs中的CompareData。受保護項檢查電路系統54基於比較判定比較條件是否獲得滿足。例如，比較條件可係CompareData及ReadData是否相等，或可基於另一比較條件，諸如小於、大於、不相等等。一些實施方案可將比較條件固定為等於條件，而其他實施方案可允許指令的參數選擇執行何種類型的比較。若比較條件未獲得滿足，則在步驟754，拒絕由RCW指令請求的

寫入，且設定條件狀態旗標以報告寫入失敗係由比較條件失敗所導致（例如，設定比較條件失敗上的負旗標N）。若比較條件獲得滿足，則步驟706、708、710、714、716、718、720係以與圖12相同的方式執行以檢查從對應於目標位址的記憶體系統位置讀取的資料的受保護項狀態，並基於檢查的結果控制是否容許寫入。若容許寫入，則步驟714與稍早討論者相同，以允許寫入繼續進行以將NewData寫入至記憶體系統位置。若在步驟710拒絕寫入或僅部分地執行寫入，則圖12的後續步驟712為圖13的步驟762所置換，其在設定條件狀態旗標以報告寫入失敗上相同，但在比較及交換變體的情形中，將條件狀態旗標設定成與在比較條件失敗的情形中在步驟754使用的值不同的值，此可區分失敗係由受保護項檢查失敗所導致。

【0112】 無論比較條件是否獲得滿足或受保護項檢查是否成功，步驟724、726、及728與圖12中相同，以可選地將ReadData寫入目的地暫存器Xs（當目的地暫存器說明符指定預定值，例如，31時，可能再次抑制目的地暫存器Xs的更新）。

【0113】 圖13顯示比較條件評估優先於受保護項檢查的情形，所以若比較條件失敗，但該項亦受保護且在步驟708、718、720的檢查失敗，則條件狀態碼將指示CAS失敗。受保護項檢查優先亦會係可能的，使得若項受保護且在步驟708、718、或720的檢查失敗，則即使比較條件將已失敗，則條件狀態碼將指示寫入失敗導因於受保護項檢查。例如，圖13可經修改以在步驟714之後而非在步驟706之前實施步驟752及754。

【0114】 圖14係繪示受保護項檢查RCW指令之位元設定/清除變體之處理的流程圖。在圖14中，步驟700至728與圖12中相同，除了在圖14中，NewData係基於提供在來源暫存器Xs中之將待設定或清除之位元的位置編碼在經定址記憶體系統位置內的位元遮罩（「BitMask」）計算而非在來源暫存器直接指定。因此，相對於圖12的唯一差異係在步驟700，暫存器Xs定義BitMask而非直接指定NewData，且在步驟704與706之間執行額外步驟770、772、774。在步驟770，方法取決於正在執行位元設定或位元清除指令而不同（其不需要支援二種類型的指令，所以若僅支援此等指令的一者，則步驟770可省略且步驟772、774的有關一者在步驟704之後執行）。若正在執行位元設定指令，則在步驟774，將NewData設定成在讀取自經定址記憶體系統位置的ReadData及由RCW指令指定的BitMask上執行逐位元或操作的結果（因此，對於位元設定指令，要求在經定址記憶體系統位置內將BitMask中以「1」標記的位元位置設定成1）。相比之下，在步驟772，若正在執行位元清除指令，則將NewData設定成在ReadData及BitMask的反轉上執行逐位元及操作的結果（因此，對於位元清除指令，要求在經定址記憶體系統位置內將BitMask中以「1」標記的位元位置清除成0）。對於位元設定及位元清除變體二者，ReadData之對應於BitMask之「0」位元的位元在NewData中保持其等的原始值，所以不為RCW指令所改變。在NewData已於步驟772或774計算後，圖14的後續步驟皆與圖12中相同。

【0115】 對於本申請案中的所有流程圖，將理解相同功能性亦可以不同序列實施，使得雖然流程圖顯示循序的步驟序列，對於不彼此相依的任何步驟，重排序該等步驟或至少部分地平行地執行其等係可行的。

【0116】 因此，如圖6所示，可將用以遍歷轉譯表樹結構以到達對應於敏感記憶體頁（例如，預期用於敏感資料或指令的頁）的中間位址映射的各種1階轉譯表項設定成具有受保護項編碼。此可係甚至將此等項的一者暫時設定成無效以禁止存取該頁的情形（例如，由於分頁操作）。同時，相同頁表中之作為受保護項的其他項可係對於其的更新受較少限制的未受保護項。藉由支援受保護項編碼，此使儲存在記憶體之PRO區域中的給定頁表含有受保護及未受保護項的混合係可能的，其中未受保護項能夠藉由在EL1執行的作業系統碼由執行根據上文討論之變體的任何者的RCW指令更新而無需超管理干預，而受保護項可具有置於其等上的更緊密限制。因為提供用於觸發受保護項檢查的專用類型指令（例如，上文提及之RCW指令之變體的一或多者），且PRO權限防止其他類型指令（諸如大部分的儲存指令）能夠更新記憶體的PRO區域，此避免就效能而言會係非常昂貴之在記憶體的每一個寫入上實行受保護項檢查的需要。

反別名檢查

【0117】 上文討論的機制對保護特定1階轉譯項免於（藉由惡意方駭侵之碼蓄意地或由編寫欠佳碼意外地）損壞係有用的。然而，如圖15所示，藉由定義指定相同的中間位址映射62的1階轉譯表項而將數個不同的虛擬位址別名至相同的中間位址係可能的。為防止攻擊者藉由定義將不同虛擬位址VA2映射至相同中間位址IPA的別名1階項而能夠規避由上文討論之PRO權限及受保護項編碼對將VA1映射至IPA的第一組1階轉譯項提供的保護，如圖8所示，2階轉譯表項可具有指定記憶體的對應區域是否具有反別名性質的位元欄位79（替代地，反別名性質79可由2階轉譯表項參考間接暫存器而間接地指定）。若該

區域經指示為具有反別名性質，則在對該區域的存取上執行額外的反別名檢查以檢查所有的經查核1階轉譯表項（將在轉譯表查核中存取，以定位指定該區域之從虛擬位址至實體位址的1階位址映射的對應1階轉譯表項）：(a)儲存在記憶體之PRO或唯讀區域中且經編碼為受保護項，或(b)儲存在記憶體的唯讀區域中。應注意此不必然需要通過該等經查核1階轉譯表項的頁表查核實際在與具有反別名性質之2階轉譯表項關聯的記憶體區域的每一個存取上執行。資訊可快取在TLB 29中以指示是否通過反別名檢查（或對某些經查核1階轉譯表項指示已將其等判定為儲存在PRO區域中及/或係受保護項），以避免每一次皆需要執行完整轉譯表查核係可行的。

【0118】 圖16係顯示執行反別名檢查之方法的流程圖。在步驟800，發布指定特定目標虛擬位址V_{Ax}的記憶體存取請求。在步驟802，MMU 28取決於從V_{Ax}至中間位址IP_{Ay}的1階映射及從中間位址IP_{Ay}至目標實體位址PA_z的2階映射而起始從目標虛擬位址V_{Ax}至目標實體位址PA_z的位址轉譯（對1階及2階轉譯執行二個分開的動作不係必要的—雖然其係一個選項，其他實例可具有可直接從V_{Ax}映射至PA_z的經組合1階及2階TLB以用於已經快取的轉譯，但在TLB中未命中時，新的VA至PA映射係藉由執行如圖6所示的1階及2階查核而識別）。

【0119】 在步驟804，MMU 28檢查對應於IP_{Ay}的2階轉譯表項（區塊或頁描述符）是否指示反別名性質。若如此，則在步驟806，MMU檢查所有經查核1階轉譯表項是否滿足反別名條件。經查核1階轉譯表項係若對應於虛擬位址V_{Ax}的完整轉譯表項查核已執行時將在轉譯表查核中存取以定位指定從V_{Ax}至IP_{Ay}之S1位址映射的對應S1轉譯表項的項（取決在TLB 29中已快取了什麼，

查核對於目前記憶體存取實際上可能係不需要的）。例如，在圖6中，經查核1階轉譯表項將係在L0、L1、及L2 1階頁表中標記為D_Table的項，及在L3 1階頁表中標記為D_Page的項。當滿足下列條件的任一者時，給定經查核1階轉譯表項的反別名條件獲得滿足：

- a) 將給定經查核 1 階轉譯表項指定為受保護項，且該給定經查核 1 階轉譯表項儲存在實體位址 PA_j，其之 PRO 權限或唯讀權限係由提供用以導出 PA_j 之 2 階位址映射的有關 2 階轉譯表項指定；或
- b) 唯讀權限係由提供用以導出給定經查核 1 階轉譯表項之實體位址 PA_j 的 2 階位址映射的有關 2 階轉譯表項指定。

【0120】 對於圖6的具體實例，用以導出經存取頁之PA的L1 1階項的有關2階轉譯表項會係在圖6中指示為「D_Page」的2階L3項。對於圖6所示的其他經查核1階項，為使反別名條件獲得滿足，將類似地存在應以PRO或唯讀權限標記的有關2階L3項（或若發現2階區塊描述符對應於IPa_y，2階L1或L2項）（此等係在所示之用於獲得各經查核1階轉譯表之實體位址的各種2階轉譯查核結束時的項）。

【0121】 若在圖16的步驟806，MMU 28判定經查核1階轉譯表項的任何一或多者未滿足反別名條件，接著在步驟808，拒絕記憶體存取。可傳訊錯誤，其可觸發例外處置器（例如，在EL2執行）以執行錯誤處置動作。

【0122】 若所有經查核1階轉譯表項皆滿足反別名條件，省略步驟808。在此情形中，在步驟810，MMU 28亦檢查任何其他檢查是否獲得滿足（諸如基於經設定的PRO權限對記憶體區域的存取的任何檢查、若記憶體存取請求回

應於RCW指令發布時的受保護項檢查、或用於保護免於其他不適當存取的任何其他特定檢查，諸如在支援安全/非安全狀態之實施方案中基於該狀態的檢查）。若其他檢查的任何者未獲得滿足，則再度在步驟808，拒絕記憶體存取（所產生的錯誤類型可取決於存取檢查失敗的原因）。否則在步驟812，容許記憶體存取請求繼續進行。

【0123】 因此，如圖6所示，反別名性質可設定在提供經存取之記憶體區域的實體位址映射的2階轉譯表項中（此可係頁描述符或區塊描述符）。若反別名性質經設定，則對於對對應記憶體位置的有效存取，此將需要將在至提供用於該記憶體區域之中間位址映射之該項的路徑上的所有經查核1階轉譯表項(a)標記為受保護且對提供儲存該等經查核1階轉譯表項之區域的實體位址映射的2階項指定PRO權限，或(b)儲存在PA，該PA的唯讀權限係由提供該PA之PA映射的2階項指定。此意謂著攻擊者無法輕易地設定新的別名1階位址映射，以規避對預期用以存取記憶體之對應區域的受信任位址映射施加的保護。由於此將基於VTTBR_EL2暫存器中之無法由在EL1執行的碼更新的基底位址（因此無法導致PRO或唯讀權限變成對儲存攻擊者的新建立別名1階位址映射的區域設定），能夠影響在EL1之作業系統碼的行為的攻擊者將不能控制用以控制記憶體存取的2階項。再者，因為在EL1執行之碼更新1階轉譯表項的機制可係執行上文討論之受保護項檢查類型的RCW指令（禁止其他指令寫入至記憶體的PRO區域），且該指令不能夠改變任何轉譯表項的受保護狀態，攻擊者不能夠導致1階項變成受保護。再者，唯讀區無法由任何寫入指令寫入。因此，攻擊

者能夠建立的任何新項應在用以獲得VA-IPA映射的1階項是否受保護及/或該等項是否儲存在記憶體中的PRO或唯讀區域中的反別名檢查的至少一者失敗。

免於1階頂層基底位址的不適當更新的保護

【0124】 可能為能夠影響在EL1執行之作業系統碼之行為的攻擊者所嘗試的另一攻擊可係修改由基底位址暫存器TTBR_EL1指示的1階頂層基底位址（識別L0 1階頁表在記憶體中的位置）。例如，攻擊者可取代由攻擊者定義的一組新的1階表的位址，以置換正確地形成且如超管理器所驗證的正確地行為的經授權頁表結構的位址。再者，攻擊者可嘗試迫使MMU 28以非預期方式使用現有的經授權1階頁表，例如，藉由取代L1、L2、或L3頁表的一者的基底位址以置換正確的L0基底位址，使得次一層表指標或用於不同記憶體區域的位址映射可不正確地用於所存取的記憶體區域，導因從預期層存取的表在樹的錯誤階層使用，使得使用虛擬位址的不同位元以從該表選擇有關項。

【0125】 圖17繪示可執行以保護免於此等類型之攻擊的1階頂層基底位址檢查。在步驟1000，指定特定目標虛擬位址的記憶體存取請求的需要頁表查核（對於不需要頁表查核的記憶體存取請求，由於所需位址映射已從TLB可用，則任何需要的1階頂層基底位址檢查會在稍早頁表查核之後將該等位址映射分配至快取記憶體時已完成，且因此不需要實行另一檢查）。在步驟1002，基於1階轉譯表基底位址暫存器TTBR_EL1中的值判定1階頂層基底位址。將該基底位址指定為中間位址，IPA_base。在步驟1004，MMU 28獲得由提供從IPA_base至PA_base之映射的關聯2階轉譯表項指定的資訊。例如，若此資訊已

快取在TLB 29中，可從該TLB獲得，或可藉由使用指定在2階轉譯表位址暫存器VTTBR_EL2中的2階基底位址執行2階轉譯表查核而獲得。

【0126】 在步驟1006，MMU 28判定1階頂層表部分唯讀檢查是否啟用。例如，此可基於儲存在控制暫存器中的1階頂層表部分唯讀檢查啟用控制值判定（例如，將2階轉譯控制暫存器VTCR_EL2的更新限制在例外等級EL2或更高等級執行的碼）。替代地，其他實施方案可考慮永久啟用1階頂層表部分唯讀檢查。若啟用1階頂層表部分唯讀檢查，則在步驟1008，MMU 28檢查關聯2階轉譯表項是否指定PRO權限，且若係否，則在步驟1010，拒絕記憶體存取且傳訊錯誤。此意謂著若攻擊者嘗試修改1階轉譯表基底位址暫存器TTBR_EL1以指向由攻擊者建立的新L0頁表，由於攻擊者將已不能夠修改記憶體的PRO區域且因此必須已寫入至非PRO區域，所以1階頂層表PRO檢查將失敗，基於經修改基底位址的存取將失敗。

【0127】 若1階頂層表PRO檢查在步驟1006停用或在步驟1008啟用且通過，則在步驟1012，MMU 28判定1階頂層表存在檢查是否啟用。再次，此可基於儲存在控制暫存器（例如，2階轉譯控制暫存器VTCR_EL2）中的1階頂層表存在檢查啟用控制值判定。用以判定檢查是否在步驟1012啟用的啟用控制值可與上文提及之用於步驟1006的啟用控制值相同（例如，在一些實施方案中，可將步驟1008及1014的檢查視為作為整體啟用或作為整體停用之單一檢查的二個步驟）。若1階頂層表存在檢查啟用，則在步驟1014，MMU 28判定關聯2階轉譯表項是否指定1階頂層項存在權限80。如相關於圖8於上文提及的，1階頂層項存在權限可編碼為PRO權限的替代變體（使得亦將具有1階頂層項存在權

限的記憶體區域假設成具有**PRO**權限），或可替代地編碼為與是否提供**PRO**權限之指示分開的獨立屬性。若關聯2階轉譯表項未指定1階頂層項存在權限，則再度在步驟1010，拒絕記憶體存取且傳訊錯誤。因為可將對應於用以保持L1、L2、或L3表之記憶體區域的2階項定義成不具有1階頂層項存在權限，此可用以保護以免於藉由修改1階頂層基底位址以指向L1、L2、或L3表的位址而使有效且真實的L1、L2、或L3表為L0所取代。僅用以保持任何有效且真實的1階L0表的記憶體區域可在對應的2階項中標記為具有1階頂層項存在權限，以限制可將哪些位址使用為用於有效記憶體存取的1階L0基底位址。

【0128】 若1階頂層表存在檢查在步驟1012停用或在步驟1014啟用且通過，則在步驟1016，MMU實行存取由PA_base識別之記憶體區域所需的任何其他檢查，且若此等檢查失敗，再度在步驟1010拒絕記憶體存取。若通過任何其他檢查，則在步驟1018，1階頂層基底位址IPA_base可有效地用以執行頁表查核。因此，1階頂層轉譯表項的位址係藉由將索引偏移施加至經判定PA_base而獲得，其中該索引偏移基於待轉譯之目標VA的位元子集判定。頁表查核接著如稍早討論地繼續。

【0129】 因此，如圖6所示，在由軟體定義的預期用途中（因此不係由硬體強制的需求），在頁表查核中存取以獲得期望加入對其之保護之記憶體區域的PA映射64的1階項中，提供識別1階L0頁表之儲存位置的PA映射64的2階頁/區塊描述符指定**PRO**及1階頂層存在權限二者、且提供識別1階L1、L2、或L3頁表之儲存位置的PA映射64的2階頁/區塊描述符指定**PRO**權限，但不指定1階頂層存在權限。此提供免於上文描述的基底位址取代攻擊的保護。避免實施

基底位址檢查之需求的替代方案可將對1階基底位址暫存器TTBR_EL1的任何存取捕捉給在EL2執行的超管理器，該超管理器接著可檢查由在EL1執行的作業系統碼請求的更新是否有效，且若有必要，拒絕更新。然而，實際上，作業系統可能在上下文交換時需要頻繁地交換基底位址暫存器TTBR_EL1中的位址，且因此捕捉每一個更新就效能而言可係高成本的。藉由實施圖17所示的1階頂層基底位址檢查，此可避免對於TTBR_EL1之基底位址暫存器更新上的此類捕捉的需求，以改善效能。

【0130】 在一些實例中，可支援1階頂層存在權限的單一變體，在該情形中，在圖17之步驟1014的檢查可簡單地係1階頂層存在權限是否已指定的檢查。

【0131】 其他實例可支援一個以上的1階頂層存在權限的變體，以允許更精細控制哪些特定1階轉譯表基底位址暫存器可指定對應記憶體區域中的位址。例如，一些實施方案可支援二個1階基底位址暫存器：

- TTBR0_EL1，當將待轉譯之虛擬位址的可組態數目(N)個最高有效位元全部設定成0時（N可定義在指定在控制暫存器中的控制值中），對在EL0或EL1中的1階轉譯選擇；及
- TTBR1_EL1，當待轉譯之虛擬位址的N個最高有效位元的任何者係非零時，對在EL0或EL1中的1階轉譯選擇。

【0132】 可接著定義1階頂層存在權限的數個變體，包括：

- Toplevel0：指示允許用於經由TTBR0_EL1存取的頂層轉譯表而不係經由TTBR1_EL1存取的頂層轉譯表的記憶體區域；

- Toplevel1：指示允許用於經由 TTBR1_EL1 存取的頂層轉譯表而不係經由 TTBR0_EL1 存取的頂層轉譯表的記憶體區域；
- Toplevel01：指示允許用於經由 TTBR0_EL1 或 TTBR1_EL1 其中一者存取的頂層轉譯表的記憶體區域。

【0133】 在此情形中，若以下條件的其中一者獲得滿足，在步驟1014之檢查的一個實施方案可導致在圖17的步驟1010傳訊錯誤：

- 使用 TTBR0_EL1 提供其之對應記憶體區域不具有 Toplevel0 或 Toplevel01 權限其中一者的基底位址；或
- 使用 TTBR1_EL1 提供其之對應記憶體區域不具有 Toplevel1 或 Toplevel01 權限其中一者的基底位址。

【0134】 在一些實施方案中，設定在由在EL2的軟體控制的控制暫存器中的進一步控制可控制是否禁止TTBR0_EL1提供對Toplevel1頁的存取，及是否禁止TTBR1_EL1提供對Toplevel0頁的存取。在此情形中，若以下條件的其中一者獲得滿足，在步驟1014的檢查可導致在步驟1010傳訊錯誤：

- 使用 TTBR0_EL1 提供其之對應記憶體區域不具有 Toplevel01 權限或在 TTBR0/Toplevel1 錯誤啟用控制經設定以啟用在使用 TTBR0_EL1 存取 Toplevel1 頁時觸發錯誤時具有 Toplevel1 權限的基底位址；或
- 使用 TTBR1_EL1 提供其之對應記憶體區域不具有 Toplevel01 權限或在 TTBR1/Toplevel0 錯誤啟用控制經設定以啟用在使用 TTBR1_EL1 存取 Toplevel0 頁時觸發錯誤時具有 Toplevel0 權限的基底位址。

【0135】 此等特徵允許更細粒地控制哪些記憶體位址區域可用以提供頂層1階轉譯表，但若使用任何頂層頁提供TTBR0及TTBR1二者的基底位址被認為係可接受的，啟用控制允許停用此等更細粒檢查。

【0136】 在一些實施方案中，各種頂層存在權限Toplevel0、Toplevel1、Toplevel01的編碼可與PRO權限的編碼組合，使得將此等視為Toplevel0 PRO權限、Toplevel1 PRO權限、及Toplevel01 PRO權限。在此一實施方案中，將Toplevel0、Toplevel1、或Toplevel01記憶體區域定義成不具有PRO權限會係不可能的。儘管如此，由於存在不將其視為具有1階頂層表存在權限之任何者的單獨PRO權限編碼，將PRO區域定義成不具有Toplevel0、Toplevel1、或Toplevel01權限的任何者係可能的。

【0137】 在圖8的實例中，將PRO權限及S1頂層項存在權限顯示成指定在直接指定為2階轉譯表項本身之編碼的部分的S2權限欄位68中。類似地，將1階轉譯表項顯示成將1階權限直接編碼在項本身的欄位66中。

【0138】 然而，如圖18所示，權限資訊由2階轉譯表項間接地指定在權限間接暫存器中亦係可能的。在此情形中，2階轉譯表項可指定識別權限間接暫存器的哪個欄位指定該項的2階權限的欄位識別符，並編碼權限間接暫存器的經參考欄位以指示權限類型。此方法可用於，例如，上文描述的PRO權限74、S1頂層項存在權限80、反別名性質79、或下文描述的GCS屬性。使用暫存器的間接權限指定對藉由對暫存器欄位的單一更新而允許軟體快速地更新所有參考相同權限欄位的許多轉譯表項的權限，而非需要更新記憶體中的許多不同的轉譯表項可係有用的。再者，在權限間接暫存器的各欄位具有比轉譯表項的

對應權限欄位更多位元的實施方案中，間接性可幫助支援比使用項內之用於權限的有限編碼空間所可能會支援的類型更多類型的權限。

用於保護以免於返回導向程式設計攻擊的受防護控制堆疊

【0139】 圖19繪示呼叫函數（為易於參考，標記為fn1）及從該函數返回的實例。函數（亦稱為程序）係可從程式的另一部分呼叫且當完成時其將處理傳回至程式流之自其呼叫該函數的該部分的指令序列。相同函數可從程式中的若干個不同位置呼叫，且因此函數返回位址在呼叫函數時儲存，使得函數返回可區分程式流應返回至哪個位址。

【0140】 例如，如圖19所示，具有鏈接分支指令BLR可在將呼叫函數的點執行，以導致程式流分支至在使用具有鏈接分支指令之運算元指定的分支目標位址的指令。具有鏈接分支指令亦導致處理電路系統將鏈接暫存器（用於追蹤函數返回位址的指定暫存器）設定成具有鏈接分支指令之後的次一指令的位址。在已取得分支之後，若干個指令（例如，LD、MUL、ADD等）在函數碼內執行，且當函數完成時，執行導致分支至由儲存在鏈接暫存器中的返回位址指示的指令的返回分支指令RET。

【0141】 若在fn1內未呼叫其他函數，且在到達fn1之結束的返回分支之前沒有例外發生，則鏈接暫存器中的位址仍應與在呼叫fn1時所設定的相同。

【0142】 然而，由背景碼呼叫的第一函數fn1自身常以巢套方式呼叫另外的函數（fn2，比如說），且在此情形中，對fn2的函數呼叫將覆寫儲存在鏈接暫存器中的返回位址，且因此在呼叫該另外函數之前，第一函數fn1的函數碼應包括將返回位址從鏈接暫存器保存至記憶體中的資料結構（例如，堆疊結

第67頁，共 88 頁(發明說明書)

構，以後進先出(LIFO)方式操作)的指令，且在從fn2返回後，fn1的函數碼應在執行返回分支之後將返回位址恢復至鏈接暫存器。用於保存及恢復函數返回狀態(諸如返回位址)的責任一般將係軟體的義務(可能沒有在架構上強制用於保存返回位址的硬體機制)。

【0143】 然而，雖然將函數返回位址儲存在記憶體中，其可能易受修改該資料的攻擊者影響，例如，使用在另一處理器核心上執行的另一緒，或藉由中斷被呼叫函數且在此期間執行覆寫儲存在記憶體中的返回位址的其他碼。替代地，攻擊者可執行旨在修改將返回位址從記憶體恢復至暫存器之指令的位址運算元的一些指令，使得從記憶體載入的資料與在呼叫巢套函數之前最初保存至記憶體的返回位址不同。若攻擊者可導致返回分支分支至程式流中在函數呼叫分支之後的該指令以外的點(圖19之實例中的#add1+4)，攻擊者可能能夠導致軟體不正確的行為，且可能能夠規避某些安全保護或導致非期望操作執行。

【0144】 函數呼叫係產生提供與處理電路系統將於稍後時間恢復至其之狀態有關之資訊的返回狀態資訊的操作的一個實例。在返回狀態資訊可擷取時的另一情境可係當取得例外時，以硬體提供的例外處置電路系統或軟體例外處置器可在該點擷取例外返回狀態資訊，諸如指示在從例外的處置返回後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在其中執行之模式或執行狀態的經保存處理器狀態資訊。例如，經保存處理器狀態資訊可指示例外係從例外等級EL0至EL3的何者取得，以及與處理器在取得例外時的操作狀態有關的其他資訊。由於函數呼叫，例外可係巢套的且因此對一個例外擷取的例外返回狀態可在取得另一例外時(以硬體自動地，或藉由軟體例外

處置器)保存至記憶體，且因此在其儲存在記憶體中的同時可能易為攻擊者的篡改所影響。此等類型的攻擊可稱為返回導向程式化(ROP)攻擊。提供免於此類攻擊的架構對策可係所欲的。

【0145】 圖20及圖21繪示使用記憶體中之稱為「受防護控制堆疊(GCS)」的受保護資料結構保護以免於ROP攻擊的方法。GCS資料結構在記憶體位址空間內的位置可由軟體選擇，但硬體提供經設計以保護GCS資料結構免於由惡意攻擊者篡改(包括由已為攻擊者所損壞之作業系統(在例外等級EL1操作)的篡改)的若干個架構特徵。

【0146】 如圖20所示，暫存器14包括控制暫存器1050，該控制暫存器可包括一或多個暫存器，該一或多個暫存器指定(在其他參數中)用於指定GCS模式啟用或停用的GCS啟用參數1052及(當GCS模式啟用時)控制GCS記憶體存取請求是否受上文討論的反別名性質79是否對由GCS記憶體存取請求存取之記憶體區域設定的檢查的1階GCS硬化檢查啟用控制參數1054。暫存器14亦包括用於儲存指示GCS資料結構上的位址的堆疊指標的一或多個受防護控制堆疊指標(GCS指標)暫存器1056。在一些實例中，GCS指標暫存器1056可係對執行狀態(例外等例EL0至EL3)的至少二者分開提供的一組並聯暫存器，以使在不同執行狀態操作的軟體能參考記憶體內的不同GCS結構而不需要在執行狀態的各轉變後將共用堆疊指標暫存器重程式化。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1054中的堆疊指標。雖然未顯示於圖20中，GCS啟用參數1052及1階GCS硬化檢查啟用控制參數1054亦可對二或更多個不同的執行狀態分開執行。

【0147】 如圖21所示，將GCS資料結構1058儲存在指定（藉由對應1階位址轉譯表項所指定的1階權限66）為記憶體之GCS區域的記憶體區域中。GCS區域權限可直接指定在對應1階位址轉譯表項的編碼內，或可在權限間接暫存器內間接參考，如圖18所示。當記憶體區域經識別為GCS區域時，則將對該區域的寫入存取限制在由處理電路系統4在執行特定GCS存取指令子集時所觸發的寫入請求。不將由軟體使用之用於未意圖存取GCS結構的一般儲存操作的通用儲存指令認為係限制性GCS存取指令子集的一者。MMU 28仍可容許使用導致不係GCS記憶體存取請求之讀取請求發布的通用載入指令讀取GCS結構。當記憶體存取請求正在請求對GCS區域的存取時，請求係寫入請求，且該請求不係由限制性GCS存取指令子集的一者觸發的GCS記憶體存取請求，則拒絕該記憶體存取請求且傳訊錯誤。

【0148】 如圖21所示，GCS存取指令子集可包括至少GCS推入指令，該指令導致返回狀態資訊（諸如來自鏈接暫存器的函數返回位址，或在取得例外時擷取的例外返回位址或經保存處理器狀態）推入至GCS結構上之使用指示在對應於目前執行狀態ELx的GCS指標暫存器1056中的堆疊指標判定的位置。GCS存取指令亦包括將受保護返回資訊從GCS結構移出的至少一種形式的GCS移出指令。

【0149】 GCS結構與由軟體使用的任何資料結構分開，以將經保存返回狀態資訊維持在記憶體內以處置函數呼叫或例外的巢套。因此，GCS結構未意圖消除軟體本身在函數呼叫或例外巢套時追蹤返回狀態資訊的保存或恢復的需求（軟體觸發的返回狀態保存可以與在不支援上文討論之GCS受保護架構措施

的處理器上相同的方式繼續)。取而代之地，GCS結構提供受保護以免於在例外等級EL0或EL1操作的受損碼篡改的受保護記憶體的区域，其可用以提供用於驗證意圖由軟體使用以從函數呼叫或例外的處理返回之返回狀態資訊的資訊。

【0150】 因此，在一些實施方案中，導致受保護返回狀態資訊從GCS結構移出的GCS移出指令亦可導致處理電路系統4比較經移出返回狀態與儲存在暫存器（例如，用於函數返回的鏈接暫存器，或用於例外返回的例外返回位址暫存器及/或經保存處理器狀態暫存器）中的目前返回狀態資訊，且若在從GCS結構1058中移出的返回狀態資訊與軟體意圖用於函數/例外返回的預期返回狀態資訊之間存在失配，傳訊錯誤。因此，軟體可藉由將GCS推入及GCS移出指令的實例包括在待於函數呼叫/返回或例外進入/返回周圍執行的程式碼內而受保護免於篡改。

【0151】 其他實施方案可定義用於驗證預期返回狀態資訊是否有效之與將返回狀態資訊從GCS結構1058移出的指令分開的單獨指令。

【0152】 替代地，GCS移出指令可將受保護返回狀態直接從GCS移出至用以指定例外返回或函數返回之返回狀態的一或多個暫存器（或可與例外/函數返回指令組合以移出受保護返回狀態並使用該狀態控制例外/函數返回），在該情形中，由於在此一實施方案中，GCS受保護返回狀態直接用以控制例外/函數返回，實行驗證軟體提供的預期返回狀態資訊是否有效的步驟不係必要的。

【0153】 再者，亦可支援其他類型的GCS存取指令。在GCS模式使用GCS啟用控制參數1052停用時具有其他功能的一些指令可在GCS模式啟用時導致處理電路系統4在執行時執行額外功能（諸如額外的GCS模式特定安全檢查）。

【0154】 一般而言，藉由提供用於定義用於供GCS結構1058使用的GCS記憶體區域類型，及將對GCS區域類型的寫入存取限制在有限的GCS存取指令子集（其可能不允許存取GCS區域類型以外的記憶體區域）的架構支援，此降低攻擊者可用之嘗試篡改儲存在GCS結構1058上的受保護返回狀態資訊的攻擊表面。

【0155】 然而，由於使用與對應於儲存GCS結構1058之區域的1階轉譯表項關聯的1階權限以指定將該區域指示為係GCS區域的性質，受損作業系統可能企圖修改該1階轉譯表項以移除GCS權限類型，或定義如圖15所示的別名1階轉譯表項以允許使用不指定GCS權限類型的不同1階轉譯表項存取實體記憶體的相同區域。

【0156】 為保護免於此類攻擊，可使用稍早描述的轉譯硬化機制以保護用以指定用於儲存GCS資料結構1058之GCS區域的1階轉譯表項。因此，指定GCS區域類型的1階轉譯表項可藉由將其儲存在由用於儲存1階轉譯表項之記憶體區域的對應2階轉譯表項（直接或間接）指定的2階權限資訊指定的唯讀區域或部分唯讀區域其中一者中而受保護以免於篡改。應注意由於將返回狀態資訊推入至GCS區域會需要將資料寫入至GCS區域，唯讀或部分唯讀區域類型不應指定在對應於GCS區域本身之2階項的2階權限中。再者，若如上文討論地支援受保護項編碼，則亦可將對應於GCS區域的1階轉譯表項指示為受保護項，以如稍早討論地保護其免於由在EL1執行的受保護項檢查類型的RCW指令修改。再者，反別名性質79可對對應於GCS區域的2階轉譯表項指定，以強制將用以定位GCS區域之位址映射的所有經查核1階轉譯表項必須係儲存在記憶體的唯

讀或部分唯讀區域中的經硬化1階轉譯表項（且若支援1階轉譯表項的受保護項編碼且將轉譯表項儲存在部分唯讀區域中，亦需要編碼為受保護項）。此等機制意謂著修改1階轉譯表項以移除GCS區域指定的企圖或使用別名1階轉譯表項規避該項的企圖將失敗。

【0157】 為確保上文描述的轉譯硬化機制用以保護對應於GCS區域的1階轉譯且因此相信GCS存取將不對由提供別名1階轉譯項之攻擊者取代預期GCS結構的替代GCS結構進行，若尋求由GCS記憶體存取存取之對應於目標記憶體區域的2階轉譯表項未指定反別名性質79，當將1階GCS轉譯硬化啟用參數1054設定成啟用狀態且GCS模式由GCS啟用參數1052啟用時，拒絕GCS記憶體存取（包括讀取及寫入存取二者）（且因此導致錯誤）。此確保保護在合適位置，若對GCS區域的任何存取企圖使用皆不係下列一者的未硬化1階轉譯表項，其將導致錯誤產生：(a)儲存在由2階轉譯表項指定為唯讀的區域中，或(b)儲存在由2階轉譯表項指定為部分唯讀的區域中且（在支援受保護項編碼的實施方案中）經編碼為未受保護項。回應於GCS記憶體存取而檢查反別名性質79的需求可藉由將1階GCS轉譯硬化啟用參數1054設定成停用狀態而停用（此可對為不支援反別名性質79或轉譯硬化機制之系統編寫的傳統碼有用）。

【0158】 可將用於控制GCS模式之操作的啟用控制值1052、1054限制成由在執行等級EL2或EL3中執行的指令更新，以防止由在EL1的作業系統或在EL0的應用程式更新。

【0159】 圖22係顯示GCS返回狀態推入指令之處理的流程圖，該指令可係專用於將返回狀態推入至GCS的GCS特定指令、或可係當在GCS模式中執行

時亦可充當GCS返回狀態推入指令的重利用函數呼叫分支指令（具有鏈接分支指令）。在步驟1100，在GCS模式由GCS啟用參數1052指示為啟用的同時，指令解碼電路系統10解碼返回狀態推入指令。若GCS模式經指示為停用，則可將此類型的指令視為未定義指令，且因此可導致錯誤，或可視為不具有架構效果但不導致錯誤的無操作(no-operation, NOP)指令。假設GCS模式啟用，則回應於GCS返回狀態推入指令，指令解碼電路系統10控制處理電路系統4的執行級16以基於暫存器中的資訊（例如，用以儲存函數返回位址的鏈接暫存器，或用以儲存例外返回資訊（諸如例外返回位址及經保存處理器狀態（例如，指示值的模式/執行狀態））的例外返回狀態暫存器）獲得返回狀態資訊。在步驟1104，處理電路系統4的載入/儲存單元26發布一或多個GCS記憶體存取請求以將在步驟1102獲得的返回狀態資訊推入至受防護控制堆疊上之基於儲存在用於目前執行狀態(ELx)之GCS指標暫存器1056中的GCS指標判定的位置，且處理電路系統4更新GCS指標暫存器1056以更新堆疊指標以使堆疊指標向前移動至堆疊上的次一位置。可使用任何已知的堆疊指標更新機制（例如，堆疊可係昇序或降序堆疊，且堆疊指標可指向資訊將推入至其的次一位置，或指向先前將資訊推入至其的最後位置）。

【0160】 圖23係顯示GCS返回狀態移出指令之處理的流程圖，該指令在此實例中亦運作為返回狀態驗證指令，該指令在GCS模式啟用時在步驟1120解碼。GCS返回狀態移出指令可係專用於將返回狀態移出至GCS的GCS特定指令、或可係當在GCS模式中執行時亦可充當GCS返回狀態移出指令的重利用例外返回指令。再次，若GCS模式停用，則可將此指令視為未定義或NOP指令。

回應於GCS返回狀態移出指令的解碼，在步驟1122，指令解碼器10控制處理電路系統4的執行級16（載入/儲存單元26）發布一或多個GCS記憶體存取請求以從受防護控制堆疊上之基於儲存在用於目前執行狀態ELx之GCS指標暫存器1056中的堆疊指標判定的位置移出返回狀態資訊，且處理電路系統4更新堆疊指標以計入該移出操作。

【0161】 在步驟1124，處理電路系統4基於返回狀態暫存器（例如，如上文提及的鏈接暫存器或例外返回狀態暫存器）中的資訊獲得目前返回狀態資訊。在步驟1126，處理電路系統4比較目前返回狀態資訊與在步驟1122從GCS資料結構1058獲得的經移出返回狀態資訊，且判定所比較的狀態是否匹配。由於失配返回狀態可係已嘗試ROP攻擊的徵兆，若在目前返回狀態資訊與經移出（GCS受保護）返回狀態資訊之間偵測到失配，則在步驟1128，傳訊錯誤。若目前返回狀態與從GCS結構1058獲得的經移出返回狀態匹配，則在步驟1130，允許軟體從函數/例外的返回繼續進行。應注意函數返回或例外返回可由單獨指令（諸如圖19所示的返回分支或例外返回指令）的執行而觸發，所以此需要不直接由GCS移出/返回狀態驗證指令觸發。

【0162】 雖然圖23顯示用於從GCS移出返回狀態資訊及比對經移出返回狀態驗證目前返回狀態二者的組合指令，將此等操作分成單獨的指令亦係可行的（一個指令用於從GCS移出返回狀態，且第二指令用於比對目前返回狀態驗證經移出返回狀態）。再者，可提供單獨的GCS移出指令以在不再需要對應的函數/例外返回的情景中允許返回狀態資訊從GCS結構1058移除。再者，若GCS返回狀態移出指令直接控制用於函數/例外返回的函數/例外返回狀態（由

於如上文提及地將GCS返回狀態移出指令與例外返回指令組合，或由於GCS返回狀態移出指令直接將GCS受保護返回狀態移出至用以提供用於控制函數/例外返回之返回狀態的暫存器），可能不需要執行驗證步驟1126、1128。

【0163】 圖24係顯示由MMU 28對在GCS模式由GCS啟用參數1052啟用時發布的記憶體存取執行的存取權限檢查的流程圖。在步驟1200，發布指定對應於目標記憶體區域之目標虛擬位址的記憶體存取請求。該記憶體存取請求可係由顯示在圖22及圖23中的GCS推入/移出指令的一者（或藉由另一類型的GCS存取指令）觸發的GCS記憶體存取請求，或可係不由GCS存取類型指令觸發的另一類型的記憶體存取請求。在步驟1202，MMU 28基於定義在1階及2階位址轉譯結構中的有關1階及2階位址映射而起始位址轉譯。在步驟1203，MMU 28判定由提供目標虛擬位址之位址映射的目標1階轉譯表項直接或間接地指定的1階權限資訊是否指定目標記憶體區域係GCS區域。

【0164】 若目標記憶體區域係GCS區域，則在步驟1204，MMU 28判定記憶體存取請求是否係由限制性GCS存取類型指令子集的一者觸發的GCS記憶體存取請求。若係否，則在步驟1205，MMU 28判定記憶體存取請求是否係寫入請求。若記憶體存取請求係寫入請求，則在步驟1206，傳訊錯誤，以防止其他一般儲存指令類型能夠寫入儲存在GCS區域中的GCS結構1058。

【0165】 若記憶體存取請求係GCS記憶體存取請求或係讀取請求，則在步驟1208，MMU 28判定1階GCS硬化檢查啟用參數1054是否指示1階GCS硬化模式經啟用。當1階GCS硬化模式啟用時，則在步驟1210，在GCS記憶體存取請求上執行額外檢查，以檢查反別名性質79是否藉由對應於目標記憶體區域的

2階轉譯表項對目標記憶體區域指定。若反別名性質79未對目標記憶體區域指定，則在步驟1206，再度傳訊錯誤。

【0166】 若在步驟1208，1階GCS硬化模式經判定為停用，或在步驟1210，目標記憶體區域不具有定義在對應2階轉譯表項中的反別名性質79，則在步驟1212，MMU 28判定記憶體存取請求的任何其他存取權限是否獲得滿足。例如，此可基於指定在對應於目標區域的1階或2階轉譯表項中的其他參數，或基於其他安全條件，諸如基於處理電路系統4的安全狀態、例外等級、或其他操作模式。若任何其他存取權限未獲得滿足，則在步驟1206，再度傳訊錯誤。若所有其他存取權限皆獲得滿足，則在步驟1214，可允許記憶體存取請求。

【0167】 若在步驟1203，MMU 28判定目標記憶體區域不係GCS區域，則在步驟1220，MMU 28判定記憶體存取請求是否係由限制性GCS存取類型指令子集的一者觸發的GCS記憶體存取請求。此與步驟1204的檢查相同，但與步驟1204相比，具有不同結果。在步驟1220，若記憶體存取請求係GCS記憶體存取請求，則在步驟1206，傳訊錯誤（此錯誤可對讀取及寫入請求二者觸發）。此確保GCS記憶體存取請求無法用以存取記憶體的**非GCS**區域，其將避免引誘軟體開發者將GCS存取類型指令用於**非GCS**存取，其將增加攻擊者可用的攻擊表面，且允許偵測基於GCS存取類型指令的位址運算元由攻擊者修改以指向GCS以外的區域的攻擊。藉由將GCS存取類型指令限制為存取GCS區域且將**非GCS**存取類型指令限制為存取**非GCS**區域，可改善安全性。

【0168】 若在步驟1220，記憶體存取請求經判定不係GCS記憶體存取請求，則在步驟1222，MMU 28判定記憶體存取請求的任何其他存取權限是否獲

得滿足。例如，此可包括基於如上文討論之基於安全狀態、例外等級、或操作模式的檢查，且亦可包括基於稍早提及的部分唯讀區域類型或反別名性質79的檢查。再者，若記憶體存取請求係由稍早提及的受保護項檢查檢型的RCW指令觸發，是否允許存取亦可取決於從對應於目標VA的目標位置讀取的舊資料的檢查。若所有必要的存取條件皆獲得滿足，在步驟1224，允許記憶體存取請求。若違反任何存取權限，則在步驟1206，傳訊錯誤。

【0169】 雖然圖24顯示回應於若干個不同的檢查失敗而傳訊錯誤的單一步驟1206，將理解一些實施方案可取決於錯誤的原因而傳訊不同的錯誤類型。

【0170】 再者，雖然圖24顯示當非GCS讀取請求標定GCS區域時錯誤並非必要的實例，其他實例可省略步驟1205且可從步驟1204繼續進行至步驟1206，以若標定記憶體之GCS區域的記憶體存取請求不係GCS記憶體存取請求，無論記憶體存取請求係讀取請求或寫入請求，傳訊錯誤。

【0171】 在目前使用GCS啟用參數1052停用GCS模式時的情形中，則GCS存取指令可觸發錯誤（例如，未定義指令錯誤）或可視為係無操作(NOP)指令。再者，GCS存取請求以外的記憶體存取請求可導致執行顯示在圖24之步驟1212或1222的檢查，但在GCS模式停用時，可省略在步驟1203、1204、1208、1210、及1220的檢查。

【0172】 圖25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。

【0173】 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。在先前描述的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（在適當處）利用主機硬體。

【0174】 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程式介面相同。因此，目標碼1300之包括上文描述之受保護項檢查

RCW指令及GCS存取指令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，如上文討論之包括對PRO區域類型的支援、反別名性質、及GCS記憶體區域類型的各種記憶體管理檢查功能可使用模擬器程式1310的記憶體管理程式邏輯1318仿真。

【0175】 因此，模擬器程式1310可具有模擬上述處理電路系統4之狀態的處理程式邏輯1312。例如，處理程式邏輯1312可回應於在目標碼1300的模擬執行期間發生的事件而控制執行狀態EL0至EL3的轉變。指令解碼程式邏輯1314解碼目標碼1300的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將由目標碼請求的暫存器存取映射成對維護在主機設備1330之主機硬體上的對應資料結構的存取，諸如藉由存取主機設備1330之暫存器或記憶體1332中的資料。記憶體管理程式邏輯1318以對應於在以上硬體實施的實施例中描述的MMU 28的方式實施位址轉譯、頁表查核、及存取控制檢查，但亦具有將藉由基於對目標碼1300定義之頁表的位址轉譯時的2階映射而獲得的經模擬實體位址映射至用於存取主機記憶體1332的主機虛擬位址的額外功能。此等主機虛擬位址可本身使用由主機支援的標準位址轉譯機制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）。

【0176】 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。

【0177】 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】

【0178】

2:資料處理設備；設備

4:處理管線；處理器管線；處理電路系統

6:提取級

8:指令快取記憶體；記憶體系統；一級指令快取記憶體；快取記憶體

10:解碼級；指令解碼器；指令解碼電路系統

12:發布級

14:暫存器檔案；暫存器

16:執行級

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

- 28:記憶體管理單元(MMU)；MMU；記憶體管理單元
- 29:轉譯後備緩衝區(TLB)；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；快取記憶體
- 34:記憶體系統；主系統記憶體；記憶體
- 50:存取控制電路系統
- 52:轉譯表查核控制電路系統
- 54:受保護項檢查電路系統
- 56:記憶體系統組件
- 60:次一層表位址
- 62:中間位址映射
- 64:實體位址映射；PA 映射
- 66:1 階存取權限；S1 權限欄位；1 階權限；S1 權限；1 階存取權限資訊；欄位
- 68:2 階存取權限；S2 權限欄位；S2 權限；2 階存取權限資訊
- 70:存取旗標(AF)；存取旗標
- 72:髒位元修改符(DBM)；DBM；DBM 位元；髒位元修改符；DBM 旗標
- 74:部分唯讀權限；PRO 權限
- 76:位元欄位；受保護項欄位；位元
- 78:位元欄位；位元
- 79:指示符；位元欄位；反別名性質；反別名性質欄位
- 80:1 階頂層項存在權限；S1 頂層項存在權限

- 500:步驟
- 502:步驟
- 504:步驟
- 506:步驟
- 600:步驟
- 602:步驟
- 604:步驟
- 606:步驟
- 608:步驟
- 610:步驟
- 612:步驟
- 700:步驟
- 702:步驟
- 704:步驟
- 706:步驟
- 708:步驟
- 710:步驟
- 712:步驟
- 714:步驟
- 716:步驟
- 718:步驟

- 720:步驟
- 724:步驟
- 726:步驟
- 728:步驟
- 750:步驟
- 752:步驟
- 754:步驟
- 762:步驟
- 770:步驟
- 772:步驟
- 774:步驟
- 800:步驟
- 802:步驟
- 804:步驟
- 806:步驟
- 808:步驟
- 810:步驟
- 812:步驟
- 1000:步驟
- 1002:步驟
- 1004:步驟

1006:步驟

1008:步驟

1010:步驟

1012:步驟

1014:步驟

1016:步驟

1018:步驟

1050:控制暫存器

1052:GCS 啟用參數；啟用控制值；GCS 啟用控制參數

1054:1 階 GCS 硬化檢查啟用控制參數；啟用控制值；1 階 GCS 硬化檢查啟用參數；1 階 GCS 轉譯硬化啟用參數

1056:受防護控制堆疊指標（GCS 指標）暫存器；GCS 指標暫存器

1058:GCS 資料結構；GCS 結構

1100:步驟

1102:步驟

1104:步驟

1120:步驟

1122:步驟

1124:步驟

1126:步驟

1128:步驟

1130:步驟

1200:步驟

1202:步驟

1203:步驟

1204:步驟

1205:步驟

1206:步驟

1208:步驟

1210:步驟

1212:步驟

1214:步驟

1220:步驟

1222:步驟

1224:步驟

1300:目標碼

1310: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:記憶體管理程式邏輯

1320:主機作業系統

1330:主機處理器；主機設備

1332:主機記憶體

a:索引值；索引位元；L0 索引部分

b:索引值；索引位元；L1 索引部分

b1:索引值

b2:索引位元

BitMask:位元遮罩

c:索引值；索引位元；L2 索引部分

CompareData:比較資料

d:索引值；索引位元；L3 索引部分

D_Block:區塊描述符

D_Page:頁描述符

D_Table:表描述符

EL0:例外等級

EL1:例外等級

EL2:例外等級

EL3:例外等級

ELx:目前執行狀態

IPA:中間實體位址

IPA_base:中間位址

IPAy:中間位址

NewData:新資料

PAz:目標實體位址

RCWMask_Valid_EL2:遮罩暫存器；暫存器

RCWMask_Invalid_EL2:遮罩暫存器；暫存器

ReadData:資料

TCR_EL1:暫存器；控制暫存器

TTBR:轉譯表基底位址暫存器

TTBR_EL1:1 階基底位址暫存器；暫存器

TTBR0_EL1:1 階基底位址暫存器

TTBR1_EL1:1 階基底位址暫存器

VA2:虛擬位址

VAx:目標虛擬位址

VTCR_EL2:暫存器；控制暫存器

VTCR_EL2.SL0:控制暫存器

VTTBR_EL2:轉譯表基底位址暫存器；基底位址暫存器；2 階基底位址暫存器；暫存器

X31:「零」暫存器

Xd:暫存器；暫存器說明符

Xs:來源暫存器；暫存器說明符

Xt:目的地暫存器

【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，以在複數個執行狀態的一者中執行指令；及

記憶體管理電路系統，以回應於指定對應於待存取的一目標記憶體區域的一目標虛擬位址的一記憶體存取請求而將該目標虛擬位址轉譯成一目標實體位址，其中從該目標虛擬位址至該目標實體位址的一映射至少取決於由一1階轉譯表結構中的一目標1階轉譯表項對該目標虛擬位址指定的一1階位址映射，該1階轉譯表結構可使用可由在一第一執行狀態中的該處理電路系統執行的一指令設定的一1階基底位址存取；其中：

至少當該記憶體存取請求係一寫入請求時，該記憶體管理電路系統經組態以回應於判定該等下列條件二者皆獲得滿足而拒絕該記憶體存取請求：

由該目標1階轉譯表項指定的1階權限資訊指定該目標記憶體區域係用於儲存用於保護用於從一函數呼叫或例外返回的返回狀態資訊的一受防護控制堆疊(GCS)資料結構的一GCS區域；及

該記憶體存取請求係由一限制性GCS存取類型指令子集的一者所觸發的一GCS記憶體存取請求以外的一請求；

該記憶體管理電路系統經組態以支援一轉譯硬化機制，該轉譯硬化機制用於至少基於可由在具有比該第一執行狀態更大特權的一第二執行狀態中的該處理電路系統執行的一指令設定的轉譯硬化資訊定義由該轉譯硬化機制保護以免於由在該第一執行狀態中執行的一指令篡改的至少一個經硬化1階轉譯表項；

當一反別名性質對該目標記憶體區域指定時，該記憶體管理電路系統經組態以回應於偵測到該目標1階轉譯表項或用以定位該目標1階轉譯表項的另一1階轉譯表項係未受該轉譯硬化機制保護的一未硬化轉譯表項而拒絕該記憶體存取請求；及

在該處理電路系統的至少一個操作狀態中，該記憶體管理電路系統經組態以回應於判定該記憶體存取請求係該GCS記憶體存取請求而該反別名性質未對該目標記憶體區域指定而拒絕該記憶體存取請求。

【請求項2】如請求項1之設備，其中該記憶體管理電路系統經組態以支援二階段位址轉譯，其中該1階位址映射包含從該目標虛擬位址至一目標中間位址的一映射，且從該目標虛擬位址至該目標實體位址的該位址映射亦取決於從該目標中間位址至該目標實體位址的一2階位址映射，該目標實體位址係藉由一2階轉譯表結構中的一目標2階轉譯表項對該目標中間位址指定，該2階轉譯表結構可使用可由在該第二執行狀態中的該處理電路系統執行的一指令設定的一2階基底位址存取。

【請求項3】如請求項2之設備，其中該目標2階轉譯表項指定該反別名性質是否對該目標記憶體區域指定。

【請求項4】如請求項2及3中任一項之設備，其中，對於儲存在對應於一給定中間位址的一給定記憶體區域的一給定1階轉譯表項，用於指定該給定1階轉譯表項是否係一經硬化1階轉譯表項的該轉譯硬化資訊包括由對應於該給定中間位址的一對應2階轉譯表項指定的2階權限資訊。

【請求項5】如請求項4之設備，其中各經硬化1階轉譯表項包含一1階轉譯表項，對於該1階轉譯表項，儲存其的該給定記憶體區域由該對應2階轉譯表項的該2階權限資訊指示為下列一者：

一唯讀記憶體區域，禁止對於其的寫入請求；及

一部分唯讀記憶體區域，對於其，容許一限制性寫入請求類型子集之對該部分唯讀記憶體區域的寫入請求且禁止該限制性子集以外的寫入請求類型之對該部分唯讀記憶體區域的該等寫入請求，該限制性寫入請求類型子集包含由該記憶體管理電路系統產生的至少一後設資料更新寫入請求以更新一轉譯表項中的存取追蹤後設資料。

【請求項6】如請求項5之設備，其中該2階權限資訊具有用於指示該唯讀記憶體區域及該部分唯讀記憶體區域二者的編碼。

【請求項7】如請求項4之設備，其中該2階權限資訊指定該給定記憶體區域是否係一部分唯讀記憶體區域，對於其，容許一限制性寫入請求類型子集之對該部分唯讀記憶體區域的寫入請求且禁止該限制性子集以外的寫入請求類型之對該部分唯讀記憶體區域的該等寫入請求，該限制性寫入請求類型子集包含由該記憶體管理電路系統產生的至少一後設資料更新寫入請求以更新一轉譯表項中的存取追蹤後設資料；且

該記憶體管理電路系統經組態以支援該第一轉譯表結構的各1階轉譯表項具有指定該1階轉譯表項是否係與未指定為一受保護項的未受保護1階轉譯表項相比對其的更新受限制的一受保護項的一編碼，該限制性寫入請求類型子集包

括允許更新一未受保護1階轉譯表項但禁止更新一受保護1階轉譯表項的至少一位元子集的一寫入請求類型。

【請求項8】如請求項7之設備，其包含受保護項檢查電路系統，其回應於該處理電路系統執行用於請求對一給定記憶體系統位置的一更新的一受保護項檢查類型的讀取-檢查-寫入指令而：

從該給定記憶體系統位置讀取資料，

檢查從該給定記憶體系統位置讀取的該資料是否具有與指定為一受保護項的一1階轉譯表項一致的一值，及

回應於判定從該給定記憶體系統位置讀取的該資料具有與指定為一受保護項的一1階轉譯表項一致的一值，防止回應於該讀取-檢查-寫入指令而更新該1階轉譯表項的一更新受限制位元子集；

該限制性寫入請求類型子集包括回應於該受保護項檢查類型的讀取-檢查-寫入指令而發布的一寫入請求。

【請求項9】如請求項7及8中任一項之設備，其中該轉譯硬化資訊包含指示一給定1階轉譯表項是否指定為該受保護項的資訊，且該記憶體管理電路系統經組態以在由該對應2階轉譯表項指定的該2階權限資訊指定該給定記憶體區域係該部分唯讀記憶體區域時，將一未受保護1階轉譯表項視為一未硬化1階轉譯表項。

【請求項10】如請求項7至9中任一項之設備，其中各經硬化1階轉譯表項包含下列一者：

一1階轉譯表項，用於其的該給定記憶體區域由該2階權限資訊指示為禁止對於其之寫入請求的一唯讀記憶體區域；及

一1階轉譯表項，其經指定為一受保護項，用於其的該給定記憶體區域由該2階權限資訊指示為該部分唯讀記憶體區域。

【請求項11】如前述請求項中任一項之設備，其中該處理電路系統的該至少一個操作狀態包含在其中將一GCS轉譯硬化檢查啟用控制參數設定成一啟用狀態的一操作狀態，該啟用狀態指示GCS記憶體存取請求將受該反別名性質是否對該目標記憶體區域指定的一檢查。

【請求項12】如前述請求項中任一項之設備，其中該記憶體管理電路系統經組態以回應於判定該記憶體存取請求係該GCS記憶體存取請求及判定該1階權限資訊未指定對應於該目標虛擬位址的該記憶體區域係該GCS區域而拒絕該記憶體存取請求。

【請求項13】如前述請求項中任一項之設備，其中該限制性GCS存取類型指令子集包含一返回狀態推入指令以控制該處理電路系統將基於指示在該處理電路系統的一或多個暫存器中的資訊而獲得的返回狀態資訊推入至該GCS資料結構。

【請求項14】如前述請求項中任一項之設備，其中該限制性GCS存取類型指令子集包含一返回狀態移出指令以控制該處理電路系統將返回狀態資訊從該GCS資料結構移出。

【請求項15】如前述請求項中任一項之設備，其包含至少一個GCS指標暫存器以儲存指示該受防護控制堆疊資料結構的一位址的一堆疊指標。

【請求項16】如前述請求項中任一項之設備，其中將指定該目標記憶體區域是否係該GCS區域的該1階權限資訊指定在由該目標1階轉譯表項所參考的一權限間接暫存器的一欄位中。

【請求項17】一種方法，其包含：

在複數個執行狀態的一者中執行指令；及

回應於指定對應於待存取的一目標記憶體區域的一目標虛擬位址的一記憶體存取請求而將該目標虛擬位址轉譯成一目標實體位址，其中從該目標虛擬位址至該目標實體位址的一映射至少取決於由一1階轉譯表結構中的一目標1階轉譯表項對該目標虛擬位址指定的一1階位址映射，該1階轉譯表結構可使用可由在一第一執行狀態中的該處理電路系統執行的一指令設定的一1階基底位址存取；其中：

至少當該記憶體存取請求係一寫入請求時，回應於判定該等下列條件二者皆獲得滿足而拒絕該記憶體存取請求：

由該目標1階轉譯表項指定的1階權限資訊指定該目標記憶體區域係用於儲存用於保護用於從一函數呼叫或例外返回的返回狀態資訊的一受防護控制堆疊(GCS)資料結構的一GCS區域；及

該記憶體存取請求係由一限制性GCS存取類型指令子集的一者所觸發的一GCS記憶體存取請求以外的一請求；

一轉譯硬化機制，其支援至少基於可由在具有比該第一執行狀態更大特權的一第二執行狀態中執行的一指令設定的轉譯硬化資訊定義由該轉譯硬化機制

保護以免於由在該第一執行狀態中執行的一指令篡改的至少一個經硬化1階轉譯表項；及

該方法包含：

當一反別名性質對該目標記憶體區域指定時，回應於偵測到該目標1階轉譯表項或用以定位該目標1階轉譯表項的另一1階轉譯表項係未受該轉譯硬化機制保護的一未硬化轉譯表項而拒絕該記憶體存取請求；及

在該處理電路系統的至少一個操作狀態中，回應於判定該記憶體存取請求係該GCS記憶體存取請求而該反別名性質未對該目標記憶體區域指定而拒絕該記憶體存取請求。

【請求項18】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：

處理程式邏輯，以模擬該目標碼之指令在複數個執行狀態的一者中的執行；及

記憶體管理程式邏輯，以回應於指定對應於待存取的一目標記憶體區域的一目標虛擬位址的一記憶體存取請求而將該目標虛擬位址轉譯成一經模擬目標實體位址，其中從該目標虛擬位址至該經模擬目標實體位址的一映射至少取決於由一1階轉譯表結構中的一目標1階轉譯表項對該目標虛擬位址指定的一1階位址映射，該1階轉譯表結構可使用可由經模擬成在一第一執行狀態中執行的一指令設定的一1階基底位址存取；其中：

至少當該記憶體存取請求係一寫入請求時，該記憶體管理程式邏輯經組態以回應於判定該等下列條件二者皆獲得滿足而拒絕該記憶體存取請求：

由該目標1階轉譯表項指定的1階權限資訊指定該目標記憶體區域係用於儲存用於保護用於從一函數呼叫或例外返回的返回狀態資訊的一受防護控制堆疊(GCS)資料結構的一GCS區域；及

該記憶體存取請求係由一限制性GCS存取類型指令子集的一者所觸發的一GCS記憶體存取請求以外的一請求；

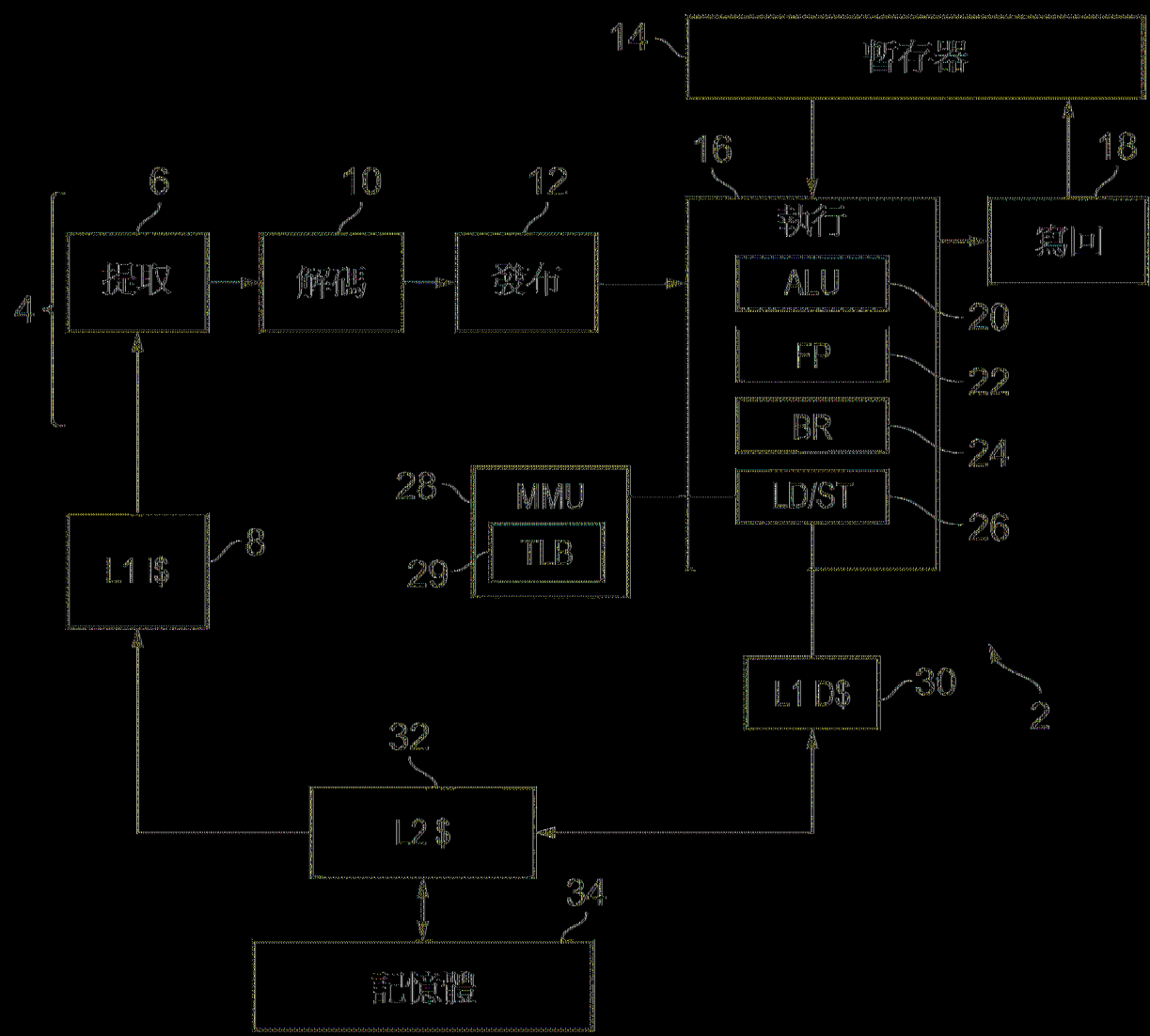
該記憶體管理程式邏輯經組態以支援一轉譯硬化機制，該轉譯硬化機制用於至少基於可由經模擬成在具有比該第一執行狀態更大特權的一第二執行狀態中執行的一指令設定的轉譯硬化資訊定義由該轉譯硬化機制保護以免於由經模擬成在該第一執行狀態中執行的一指令篡改的至少一個經硬化1階轉譯表項；

當一反別名性質對該目標記憶體區域指定時，該記憶體管理程式邏輯經組態以回應於偵測到該目標1階轉譯表項或用以定位該目標1階轉譯表項的另一1階轉譯表項係未受該轉譯硬化機制保護的一未硬化轉譯表項而拒絕該記憶體存取請求；及

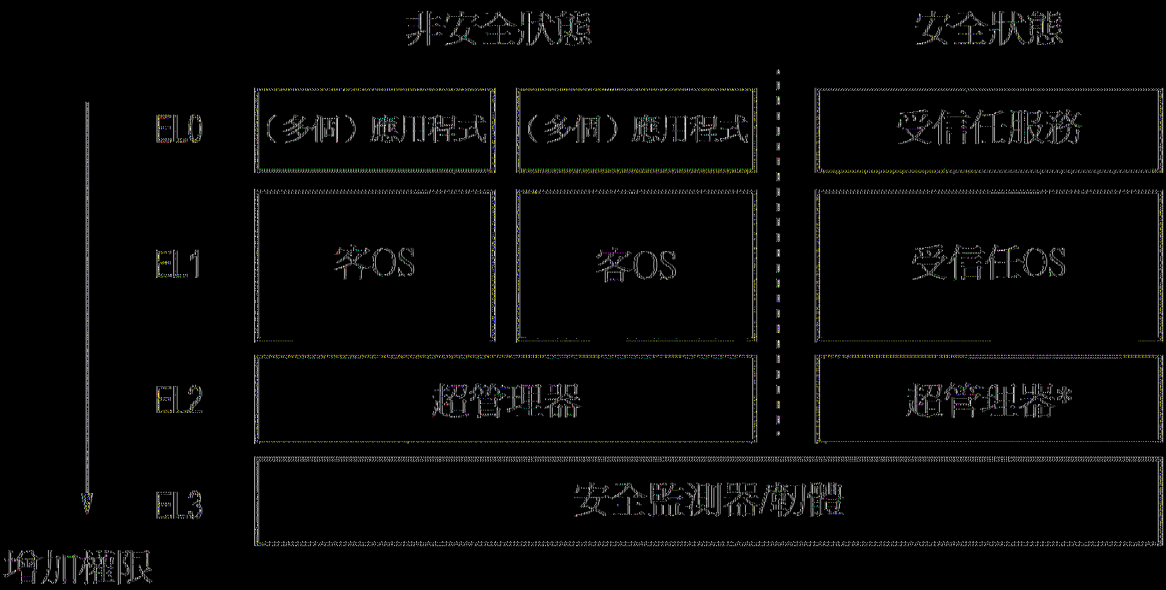
在該處理電路系統的至少一個操作狀態中，該記憶體管理電路系統經組態以回應於判定該記憶體存取請求係該GCS記憶體存取請求而該一反別名性質未對該目標記憶體區域指定而拒絕該記憶體存取請求。

【請求項19】一種儲存媒體，其儲存如請求項18的電腦程式。

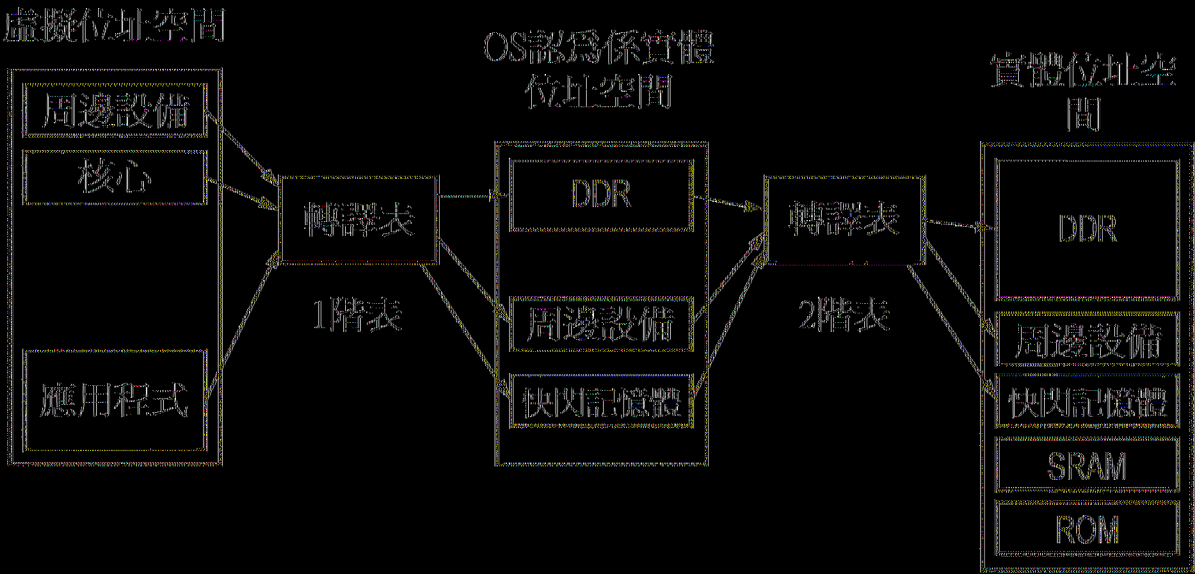
|(發明圖式)|



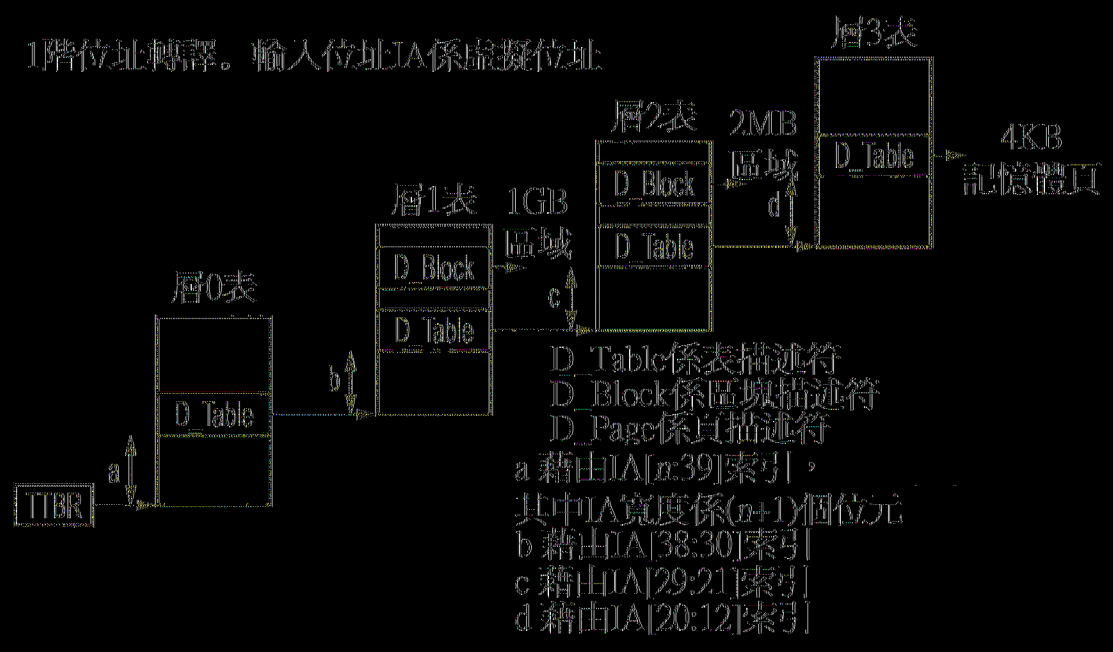
|(圖1)|



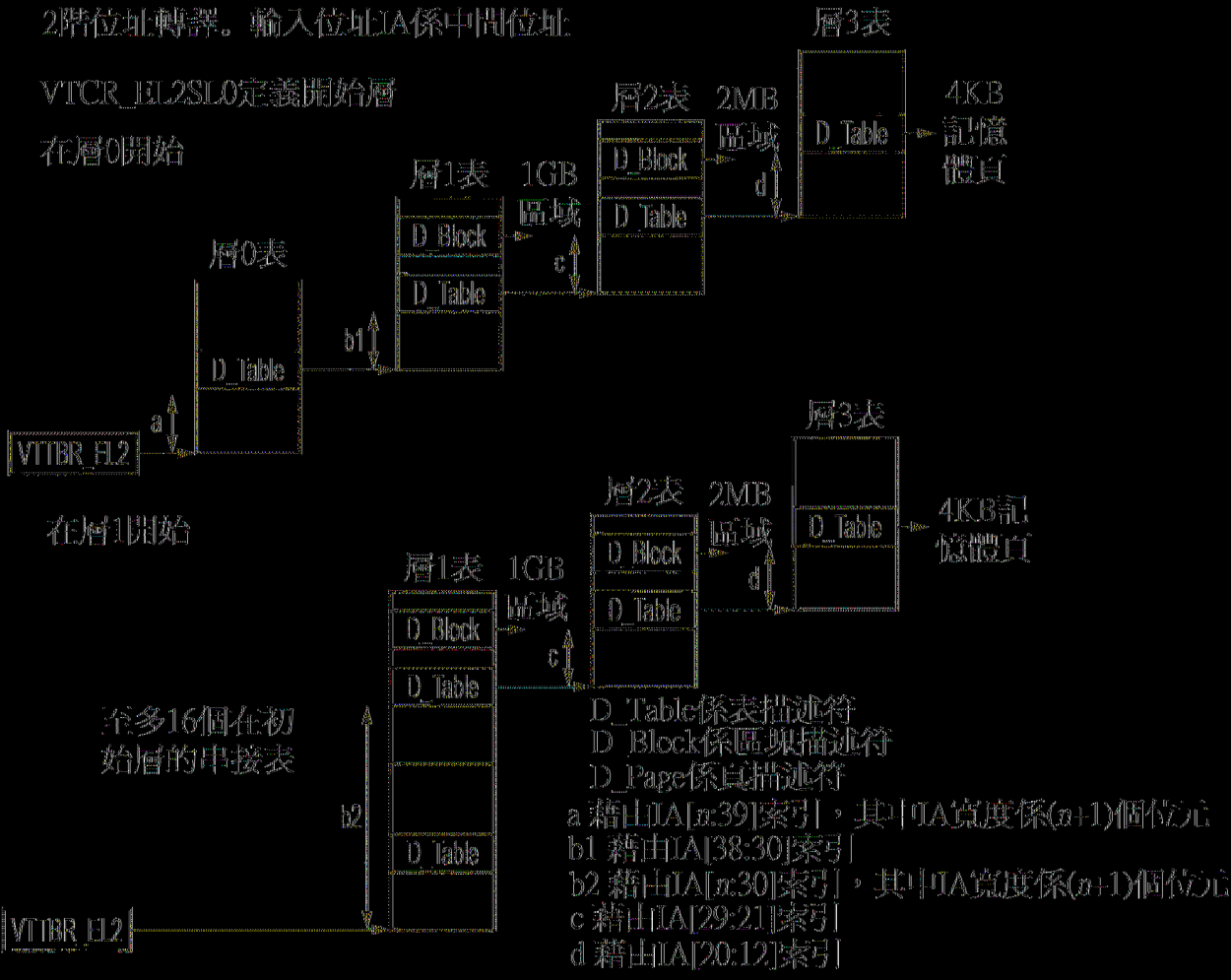
[(圖2)]



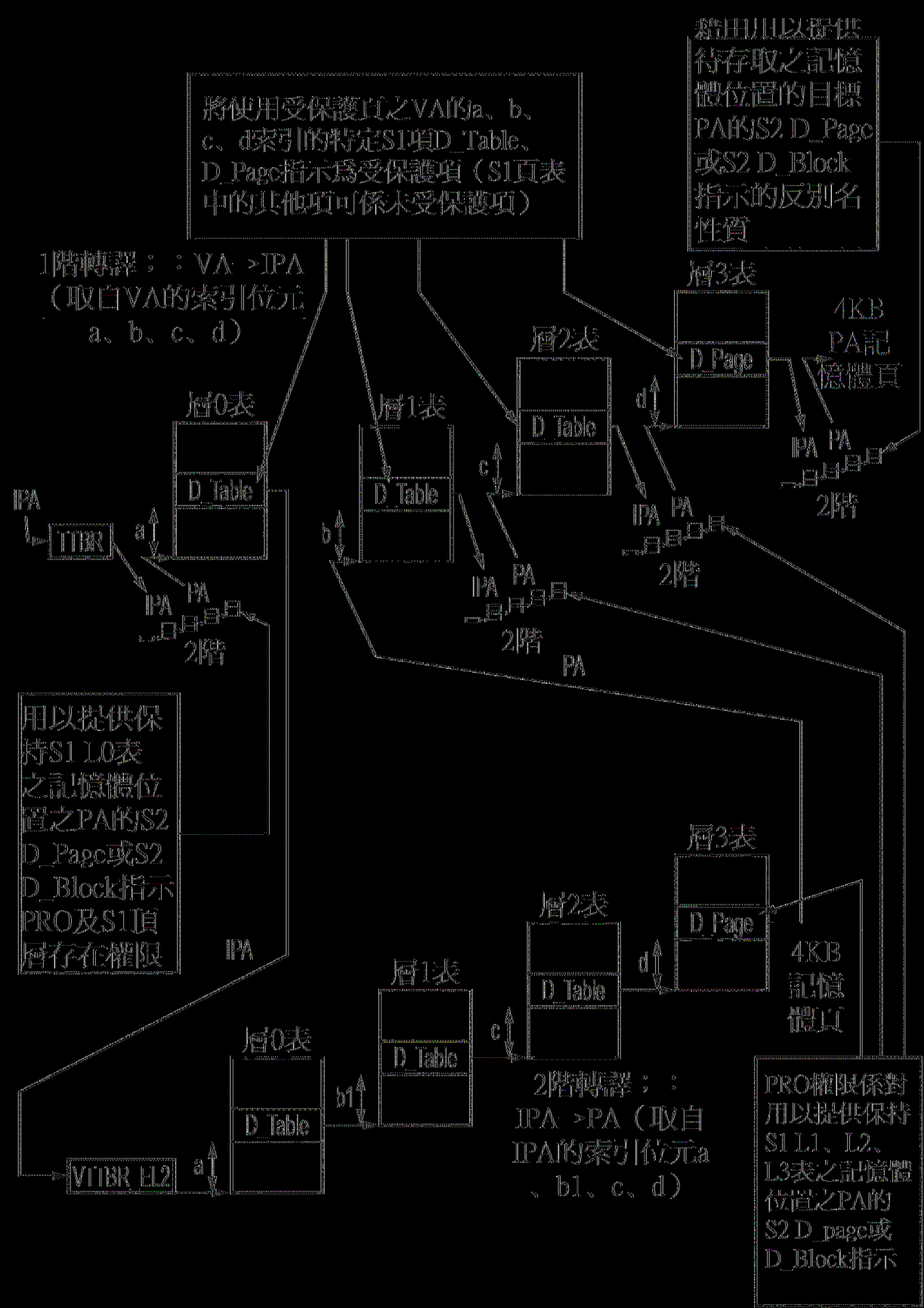
[(圖3)]



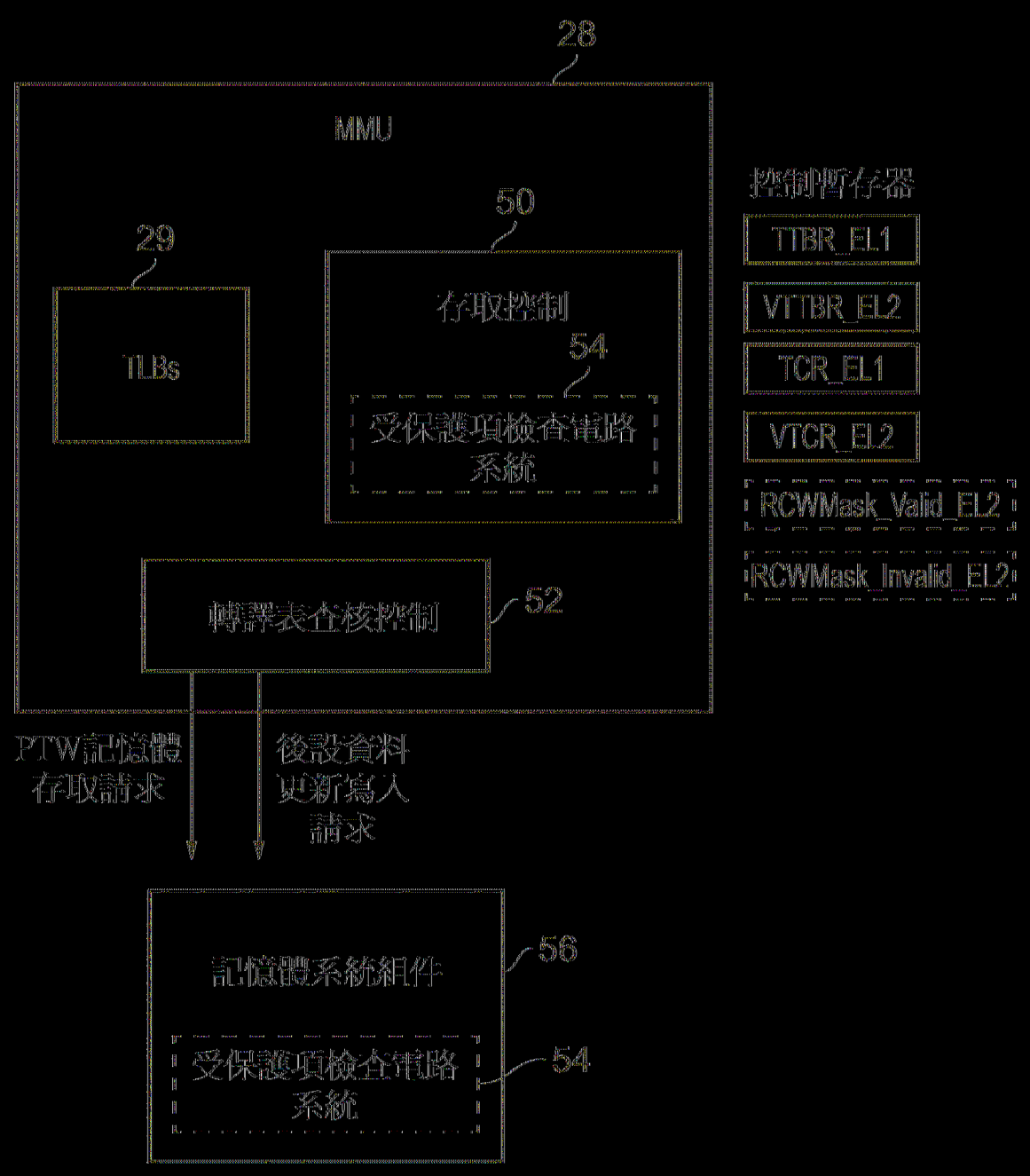
|(圖4)|



(圖5)

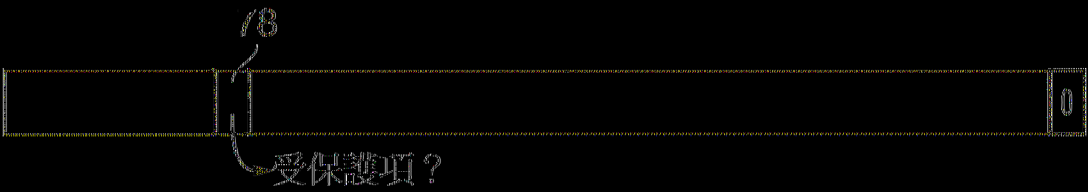


(圖6)



(圖7)

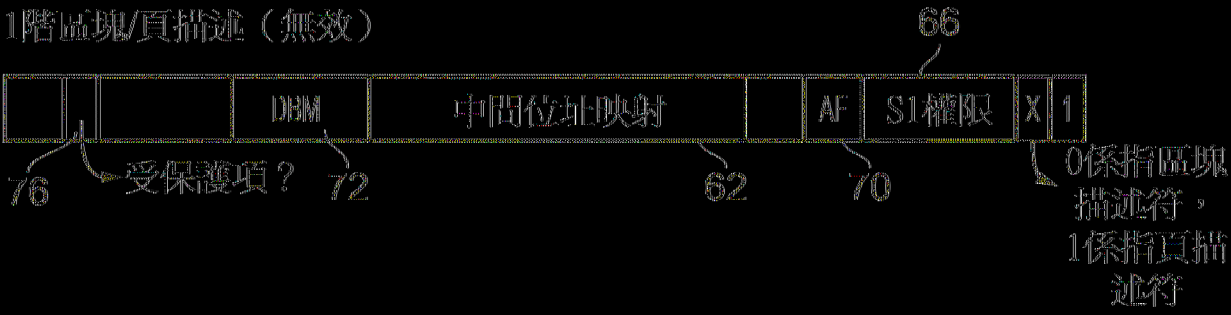
1階描述 (無效)



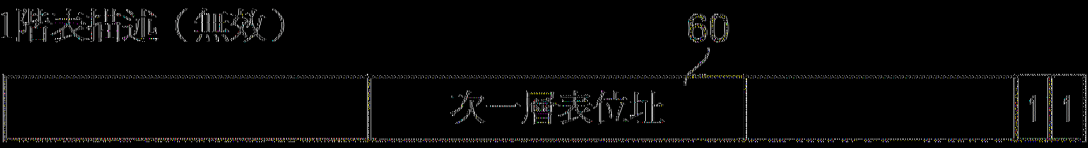
1階表描述 (無效) L0、L1、或L2



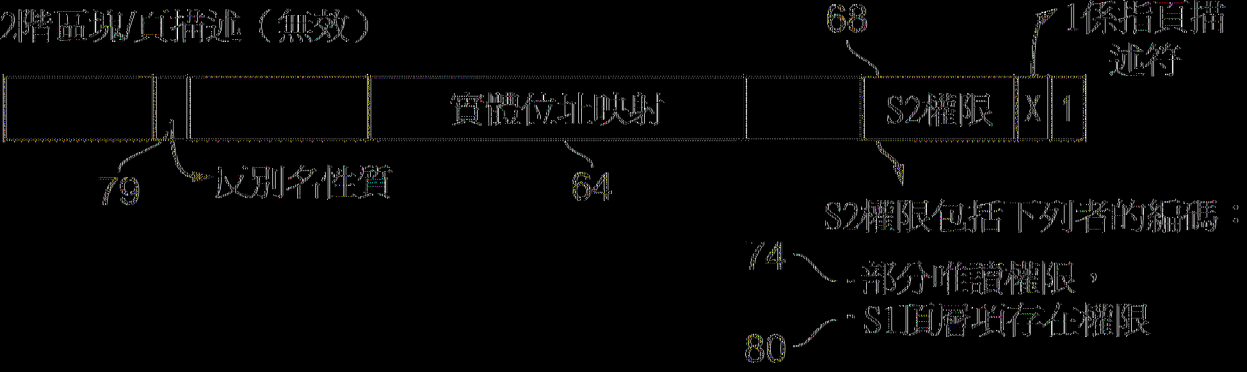
1階區塊/頁描述 (無效)



1階表描述 (無效)



2階區塊/頁描述 (無效)



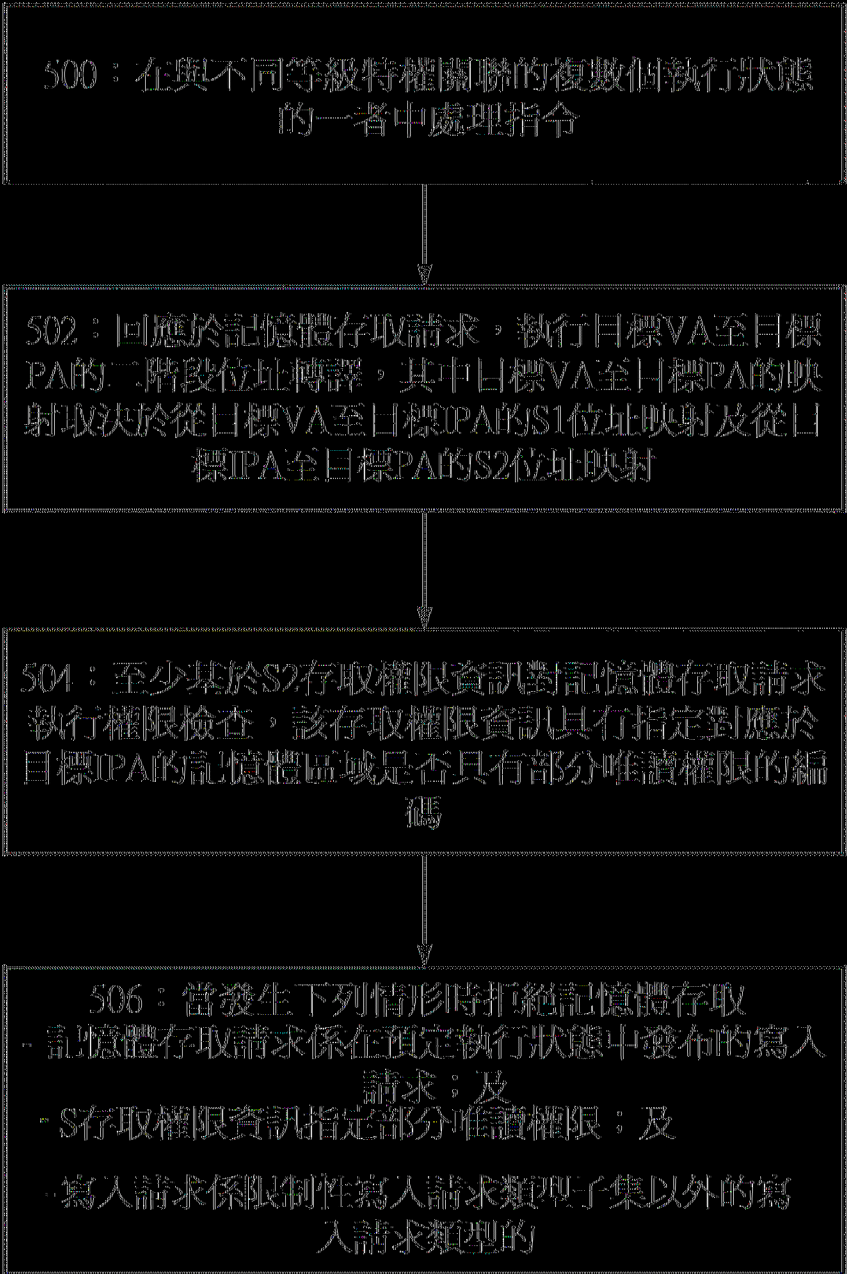
[圖8]

回應於不同的寫入請求類型，對於由S2權限標記為部分唯讀之記憶體區域的寫入存取控制：

當在EL1發布寫入時，容許寫入至部分唯讀區域的限制性寫入請求類型子集

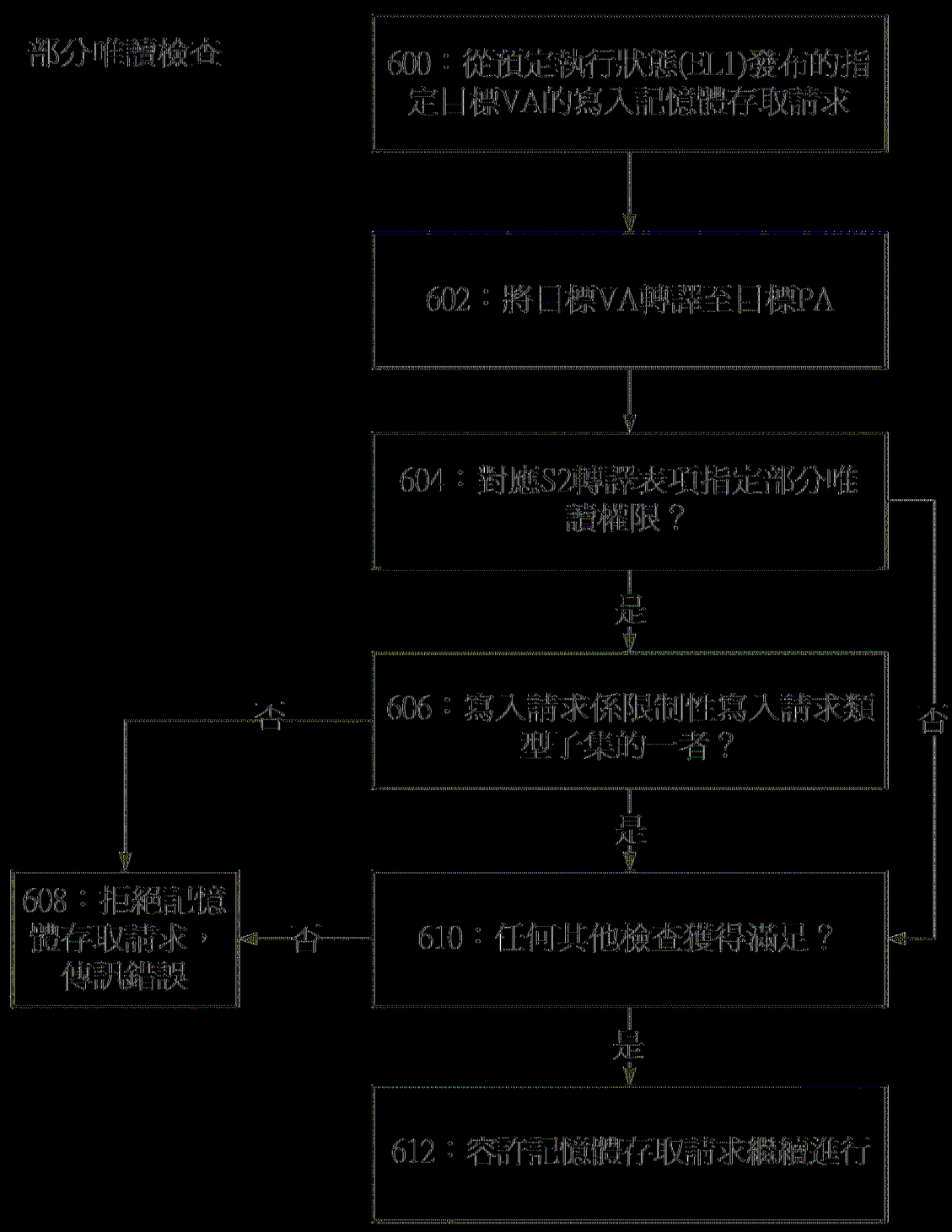
容許寫入至部分唯讀區域的寫入請求類型	禁止寫入至部分唯讀區域的寫入請求類型
(可選的) 回應於在EL2或EL3執行的儲存指令而發布的寫入請求 (若在EL0或EL1執行，包括禁止寫入至部分唯讀區域的至少一種類型的儲存) 在EL1執行的預定類型的轉譯表項更新指令，例如： ● 當通過受保護項檢查時，在EL1執行的受保護項檢查類型的RCW指令。	回應於在EL0 EL1執行的至少一種類型的儲存指令 (例如，ISA的大部分儲存指令) 而發布的寫入請求
由MMU產生以更新轉譯表項中的存取追蹤後設資料 (例如，AF、當DBM設定時的寫入權限) 的後設資料更新寫入請求	

[(圖9)]

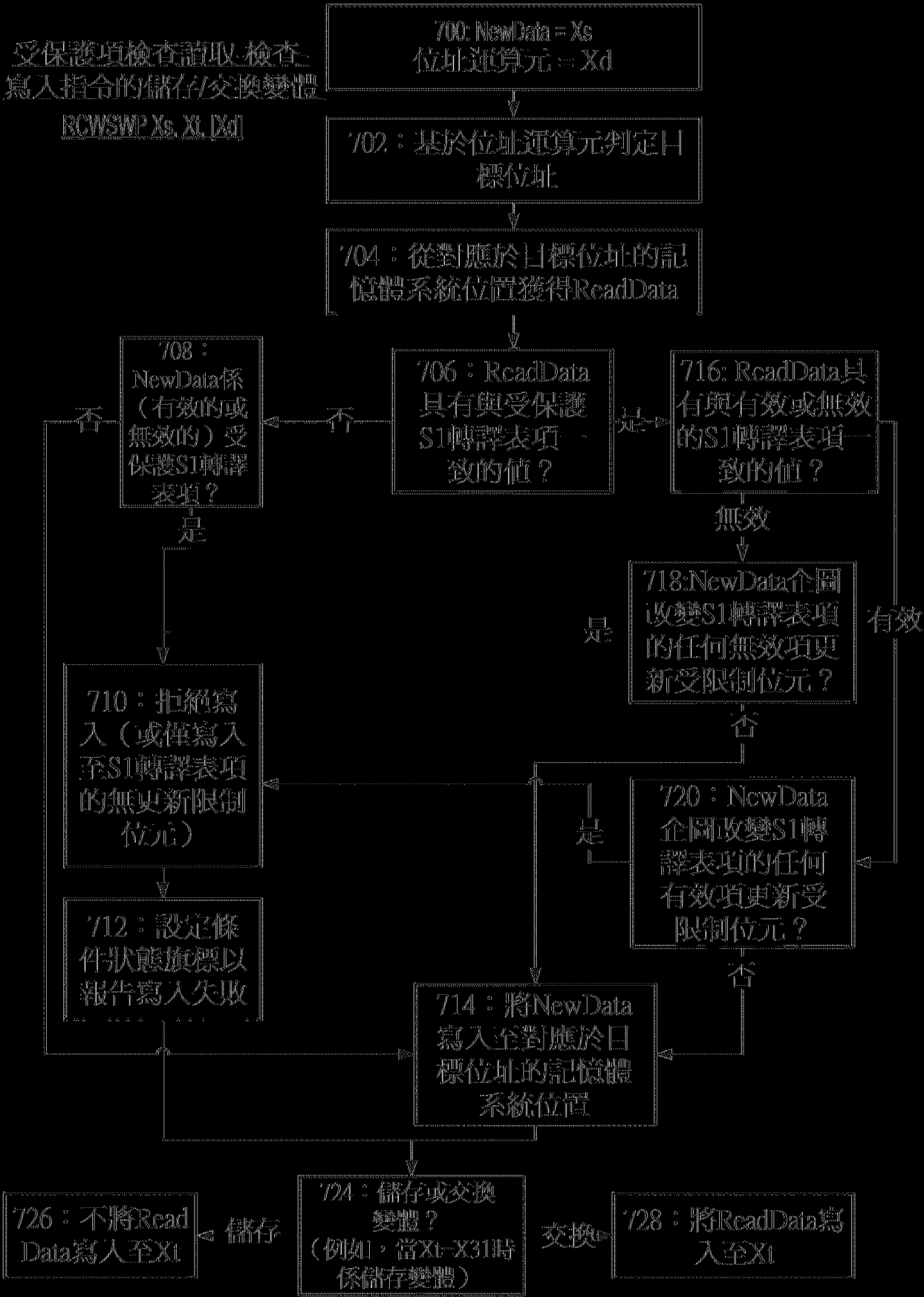


〔圖10〕

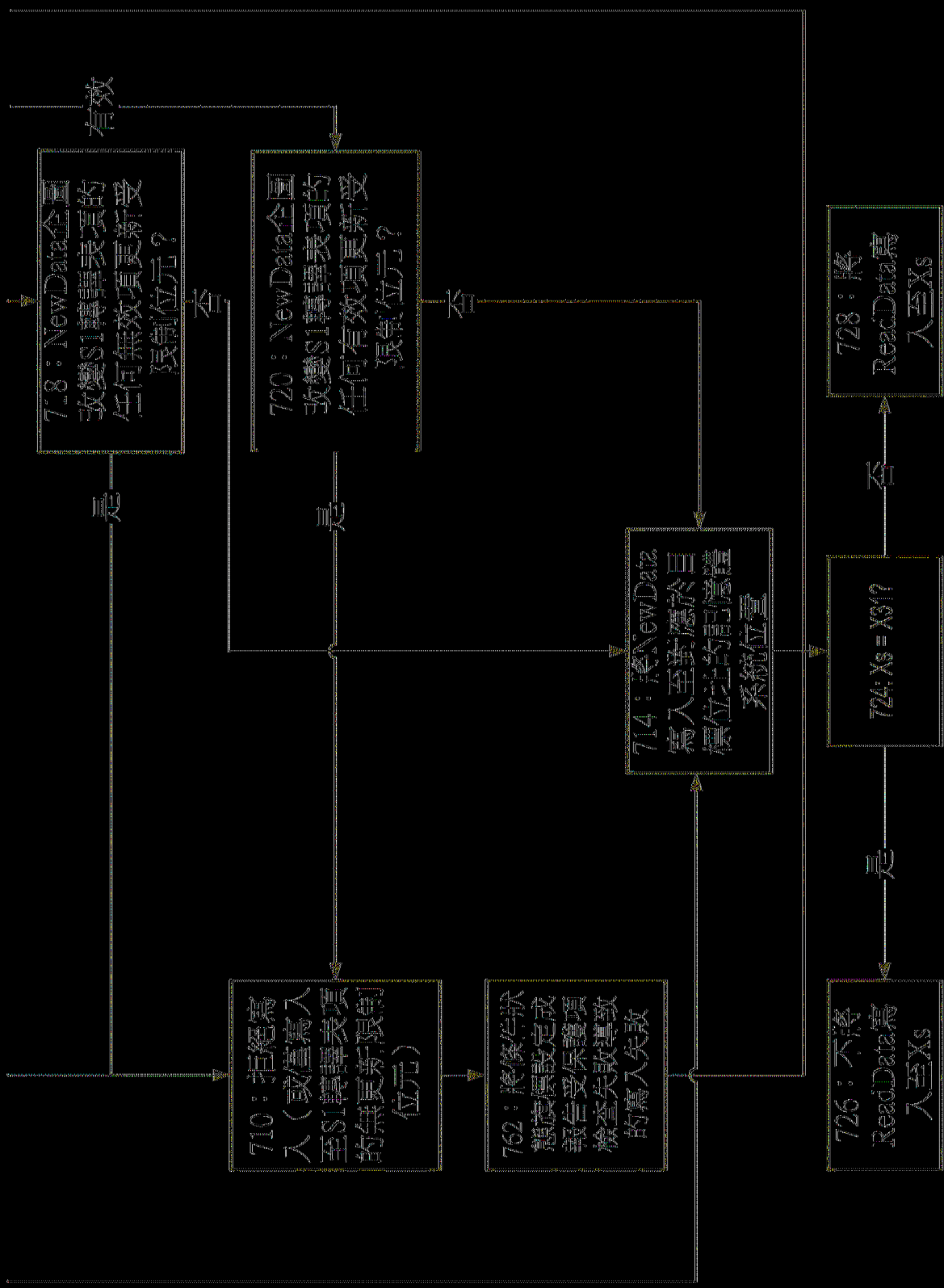
部分唯讀檢查



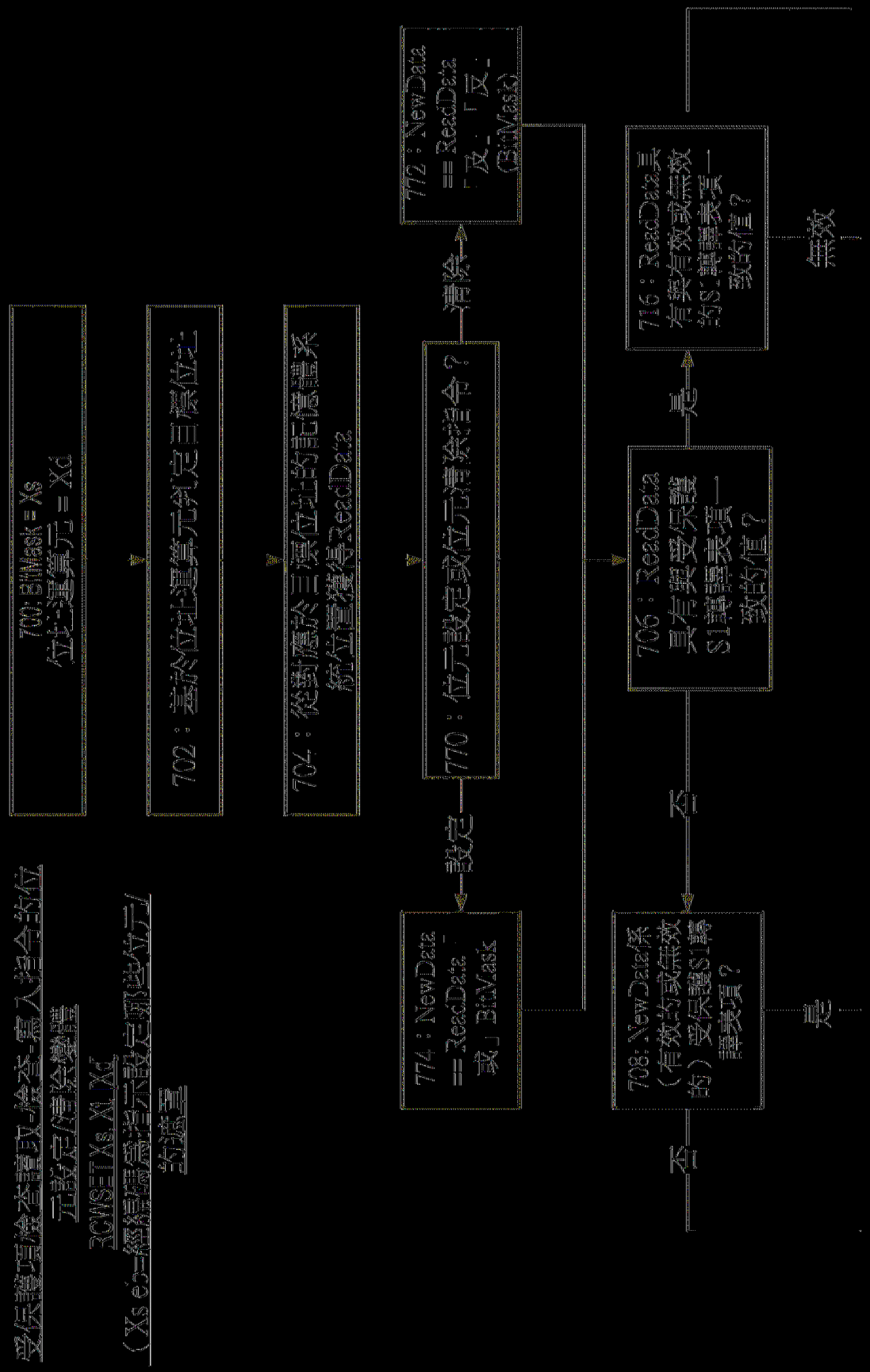
[圖11]



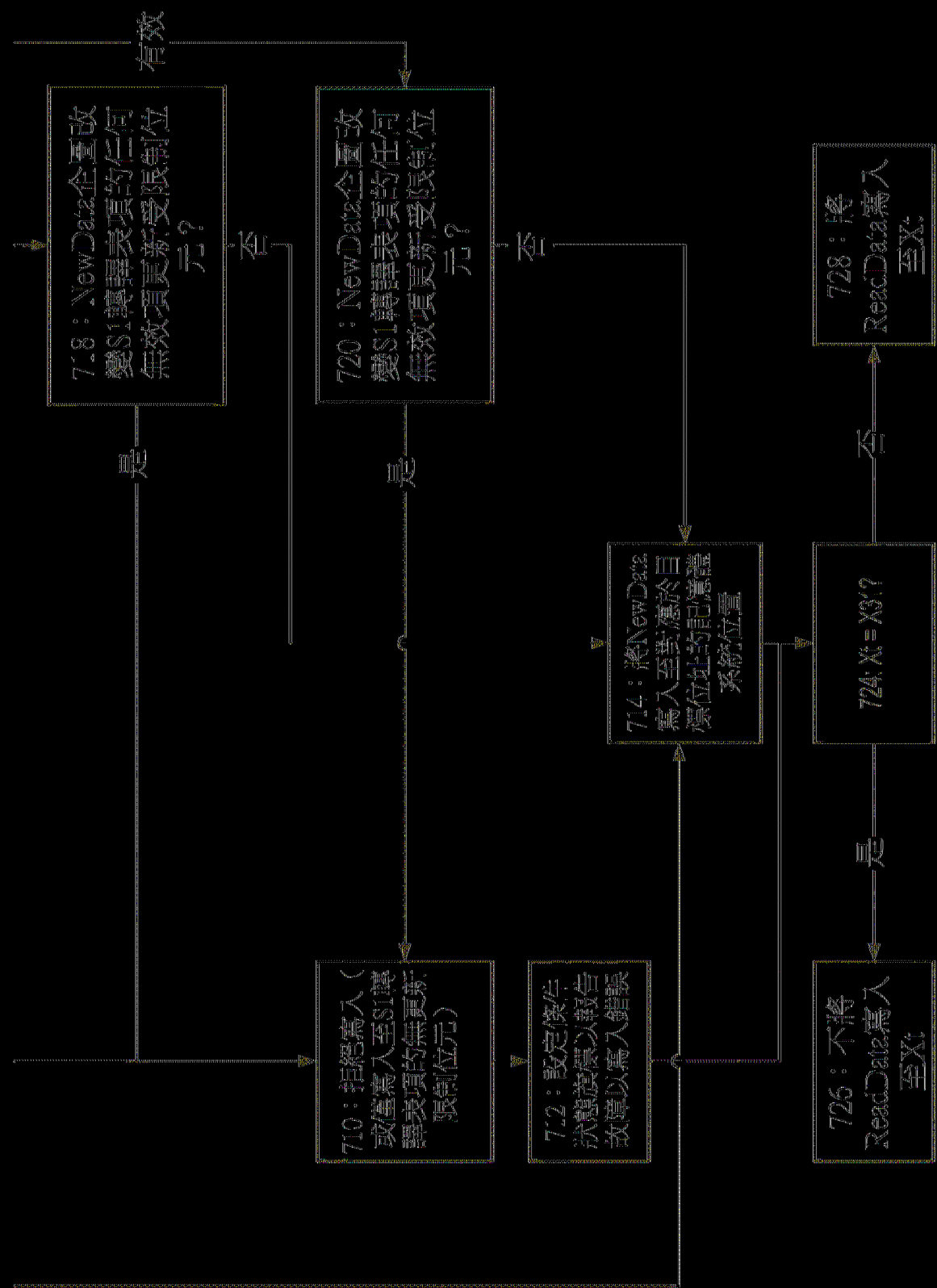
〔圖12〕



[(圖13 (續))]

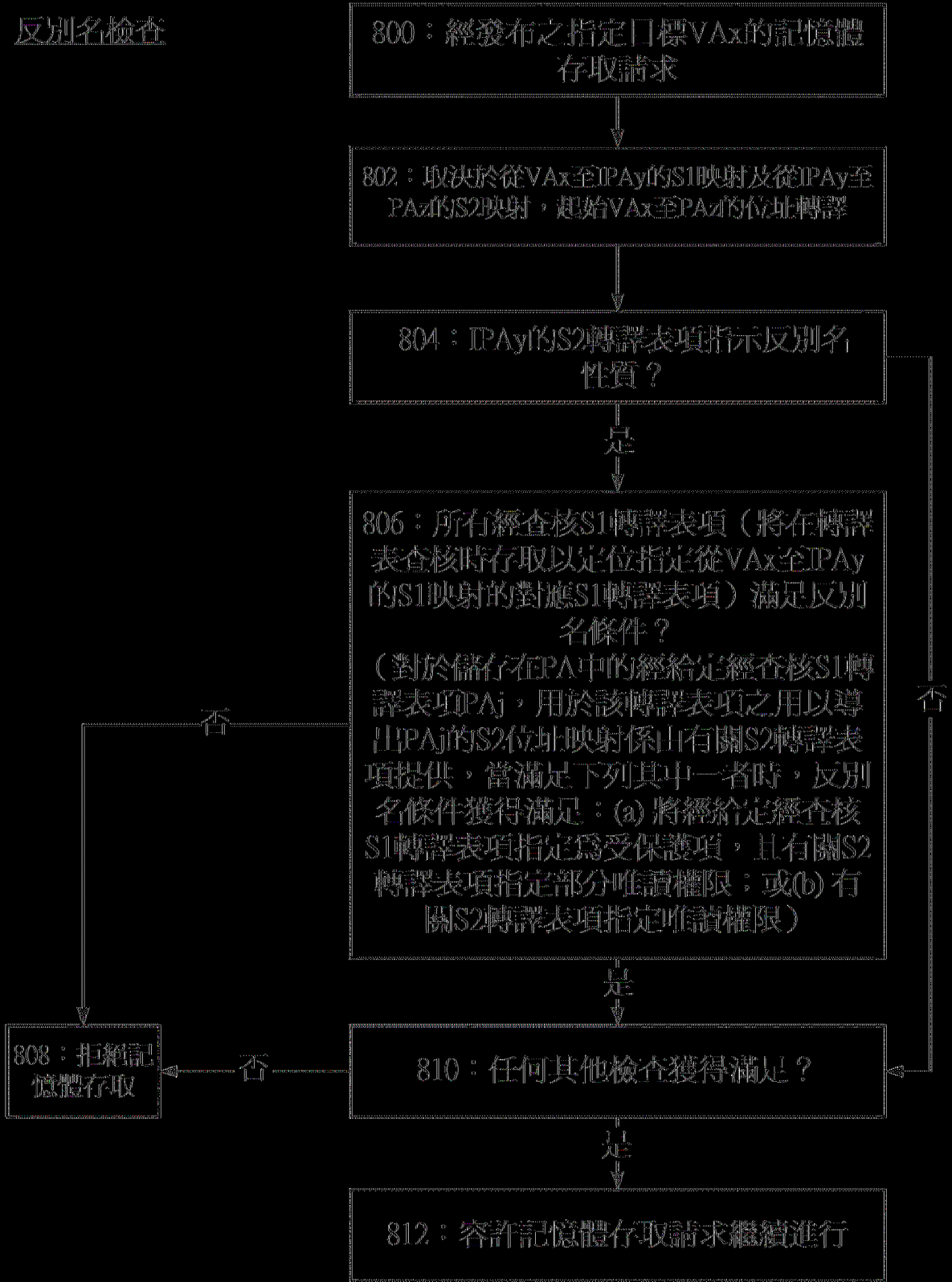


(圖14)

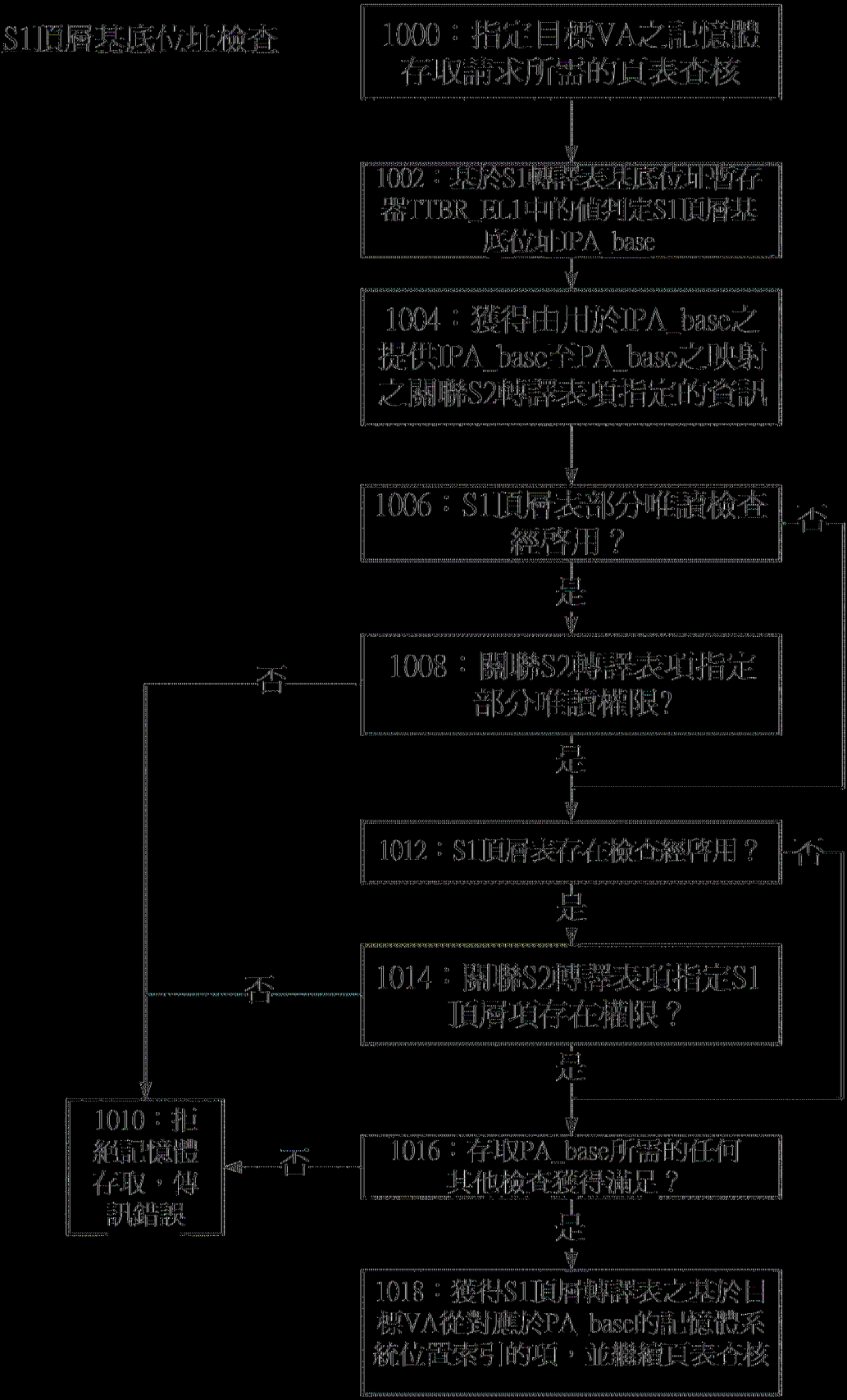


(圖14 (續))

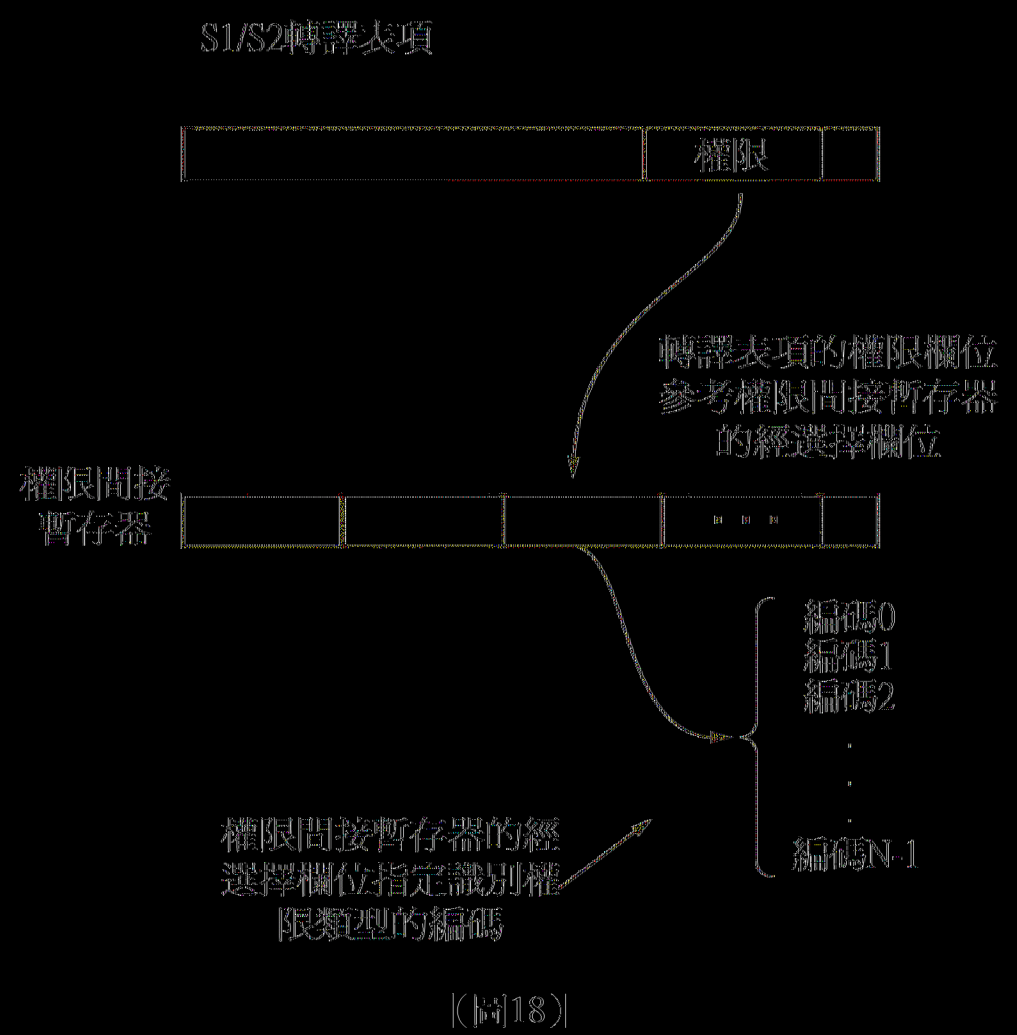
反別名檢查

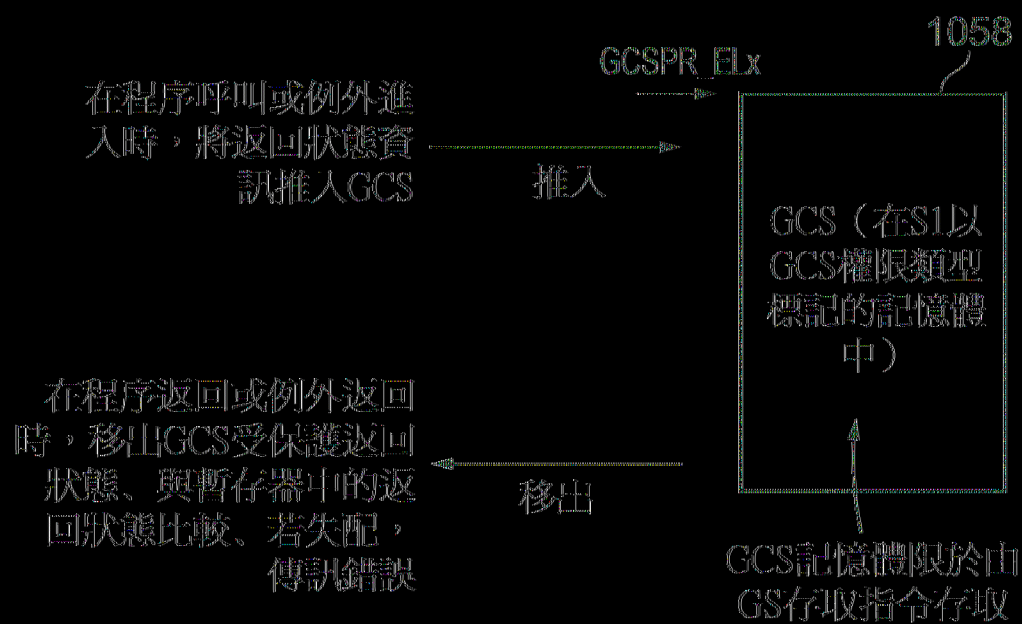


〔圖16〕

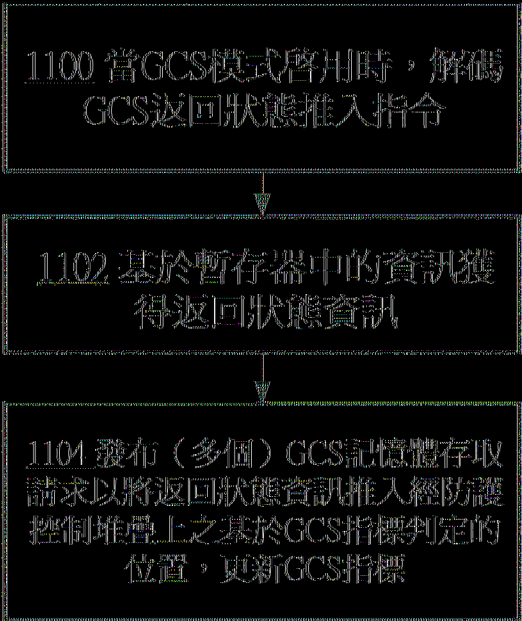


[(圖17)]

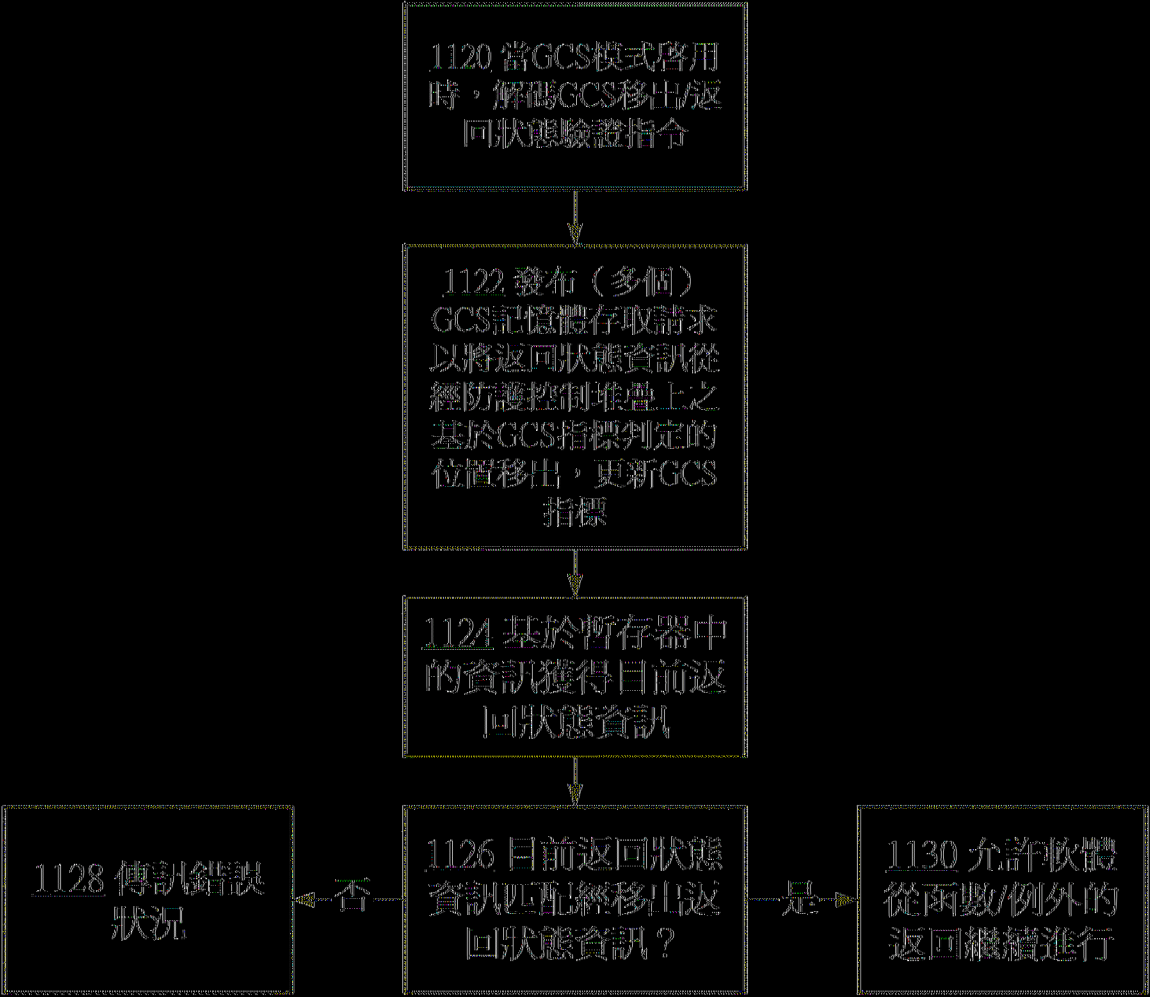




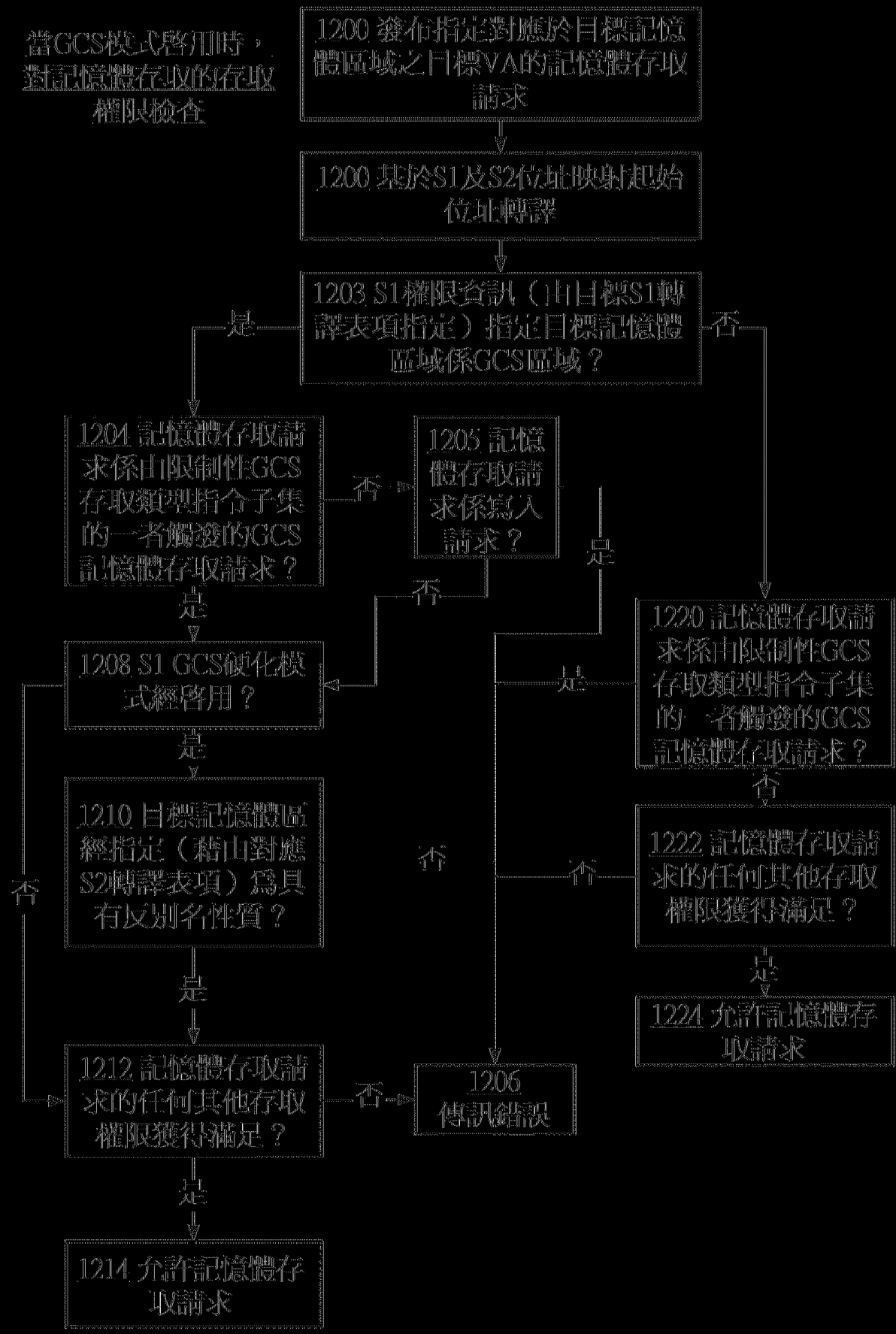
[(圖21)]



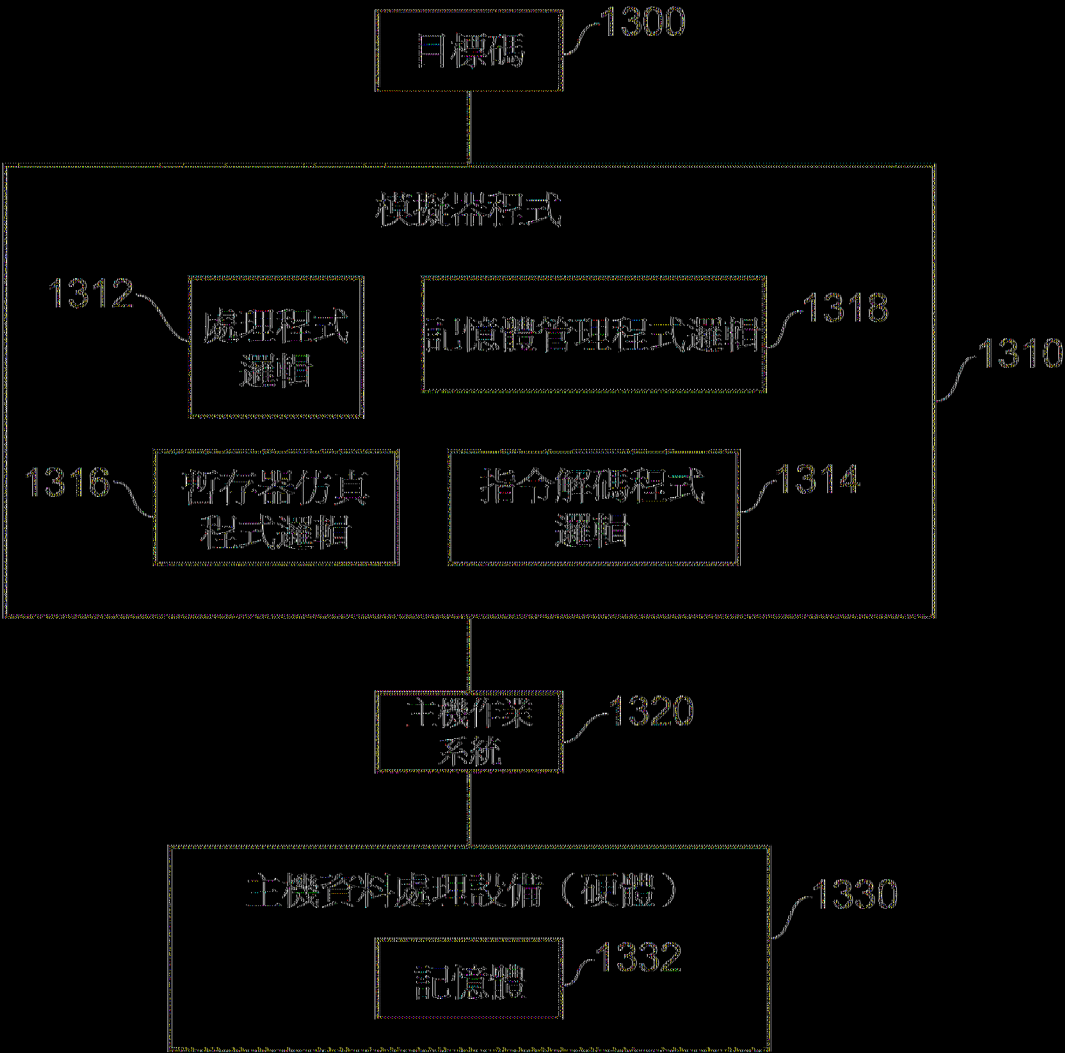
[(圖22)]



[(圖23)]



〔圖24〕



|(圖25)|