



(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 I804388 B

(45)公告日：中華民國 112 (2023) 年 06 月 01 日

(21)申請案號：111126947

(22)申請日：中華民國 111 (2022) 年 07 月 19 日

(51)Int. Cl. : G06F9/06 (2006.01)

G06F9/46 (2006.01)

(30)優先權：2021/12/03 美國

17/457,446

(71)申請人：美商萬國商業機器公司(美國) INTERNATIONAL BUSINESS MACHINES CORPORATION (US)

美國

(72)發明人：里奇丹拿 塞德瑞 LICHTENAU, CEDRIC (DE)；朗 雅各布 克里斯托弗 LANG, JAKOB CHRISTOPHER (DE)；帕斯 依柏克哈德 PASCH, EBERHARD (DE)；伯翠格 克里斯汀 BORNTRAEGER, CHRISTIAN (DE)

(74)代理人：陳長文

(56)參考文獻：

US 2012/0147937A1

US 2016/0124719A1

US 2016/0234019A1

US 2017/0140153A1

US 2018/0268130A1

審查人員：何偉權

申請專利範圍項數：25 項 圖式數：2 共 32 頁

(54)名稱

在處理單元之處理器核心上操作安全碼區段

(57)摘要

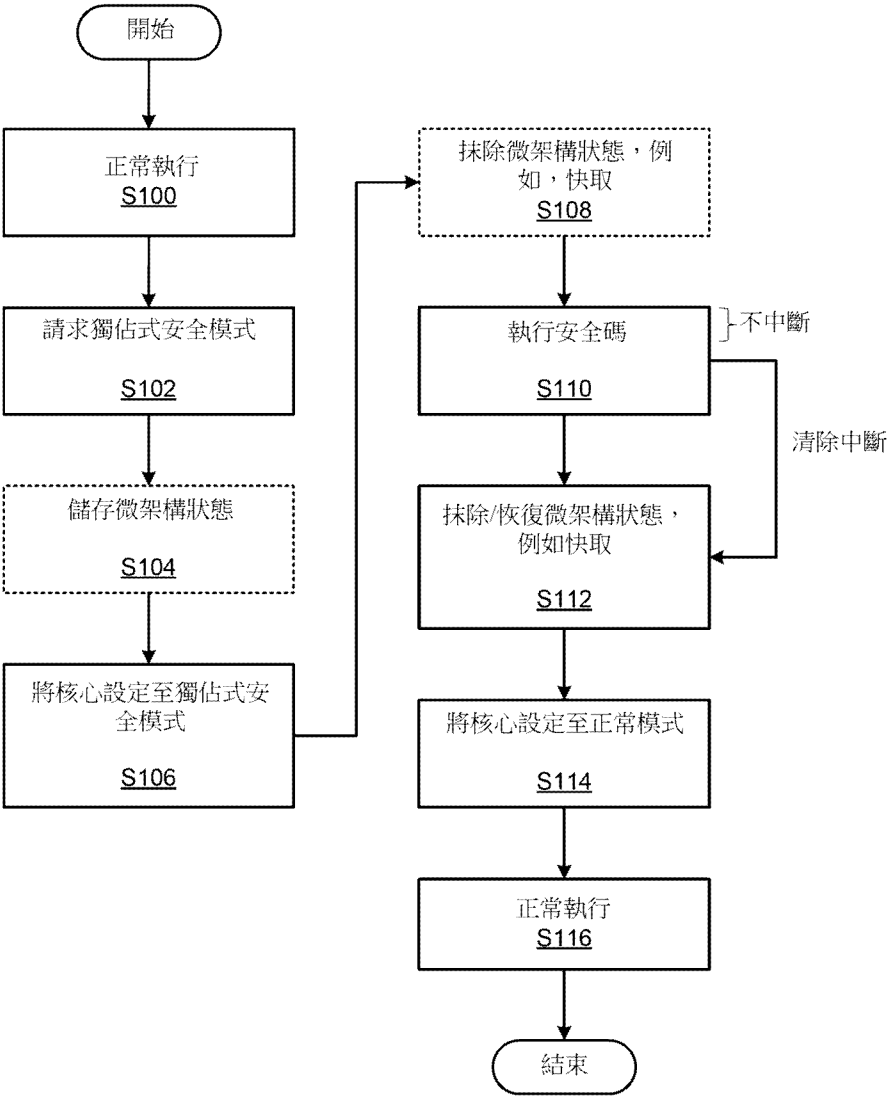
本發明係關於一種在一處理單元上之一處理器核心上操作一安全碼區段之電腦實施方法、電腦系統及電腦程式產品，其中該處理單元經組態具有至少一個處理器核心。該方法包含請求在該至少一個處理器核心上獨佔式安全執行該程式碼之一安全碼區段。該方法亦包含設定該至少一個處理器核心以獨佔式安全執行該安全碼區段。該方法進一步包含在該至少一個處理器核心上不中斷地執行該安全碼區段。此外，該方法包含自該至少一個處理器核心抹除一實體處理器核心之一架構狀態及一非架構狀態。最後，該方法包含將該至少一個處理器核心設定至第一執行模式以用於執行該至少一個處理器核心上之程式碼。

A computer-implemented method, a computer system and a computer program product operate a secure code segment on a processor core of a processing unit, wherein the processing unit is configured with at least one processor core. The method comprises requesting exclusive secure execution of a secure code segment of the program code on the at least one processor core. The method also comprises setting the at least one processor core to exclusive secure execution for the secure code segment. The method further comprises executing the secure code segment on the at least one processor core uninterruptably. In addition, the method comprises wiping an architected state and a non-architected state of a physical processor core from the at least one processor core. Lastly, the method comprises setting the at least one processor core to the first execution mode for executing program code on the at least one processor core.

指定代表圖：

符號簡單說明：

- S100:步驟
- S102:步驟
- S104:步驟
- S106:步驟
- S108:步驟
- S110:步驟
- S112:步驟
- S114:步驟
- S116:步驟



【圖1】



I804388

【發明摘要】

【中文發明名稱】

在處理單元之處理器核心上操作安全碼區段

【英文發明名稱】

OPERATING A SECURE CODE SEGMENT ON A PROCESSOR
CORE OF A PROCESSING UNIT

【中文】

本發明係關於一種在一處理單元上之一處理器核心上操作一安全碼區段之電腦實施方法、電腦系統及電腦程式產品，其中該處理單元經組態具有至少一個處理器核心。該方法包含請求在該至少一個處理器核心上獨佔式安全執行該程式碼之一安全碼區段。該方法亦包含設定該至少一個處理器核心以獨佔式安全執行該安全碼區段。該方法進一步包含在該至少一個處理器核心上不中斷地執行該安全碼區段。此外，該方法包含自該至少一個處理器核心抹除一實體處理器核心之一架構狀態及一非架構狀態。最後，該方法包含將該至少一個處理器核心設定至第一執行模式以用於執行該至少一個處理器核心上之程式碼。

【英文】

A computer-implemented method, a computer system and a computer program product operate a secure code segment on a processor core of a processing unit, wherein the processing unit is configured with at least one processor core. The method comprises requesting exclusive secure execution of a secure code segment of the program code on the at least one processor core. The method also comprises setting the at least one

processor core to exclusive secure execution for the secure code segment. The method further comprises executing the secure code segment on the at least one processor core uninterruptably. In addition, the method comprises wiping an architected state and a non-architected state of a physical processor core from the at least one processor core. Lastly, the method comprises setting the at least one processor core to the first execution mode for executing program code on the at least one processor core.

【指定代表圖】

圖1

【代表圖之符號簡單說明】

S100:步驟

S102:步驟

S104:步驟

S106:步驟

S108:步驟

S110:步驟

S112:步驟

S114:步驟

S116:步驟

【發明說明書】

【中文發明名稱】

在處理單元之處理器核心上操作安全碼區段

【英文發明名稱】

OPERATING A SECURE CODE SEGMENT ON A PROCESSOR
CORE OF A PROCESSING UNIT

【技術領域】

【0001】 本發明大體上係關於資料處理系統，詳言之，係關於一種用於在一處理單元之一處理器核心上操作一安全碼區段的電腦實施方法、電腦系統、電腦程式產品及資料處理系統。

【先前技術】

【0002】 多執行緒處理器可包括複數個可同時執行的硬體執行緒。多執行緒處理器之一個實例可為同時多執行緒(SMT)處理器。在同時多執行緒處理中，來自超過一個執行緒的指令可同時在任何給定指令管線級中執行。因此，同時多執行緒處理可允許執行多個獨立執行緒以更好地利用處理器架構提供之資源。同時多執行緒處理可使虛擬機之各處理器向應用程式呈現為稱作執行緒之 n 處理器。

【0003】 來自雲端中或在現場之不同客戶的處理或執行緒可在虛擬機(VM)上或在容器上虛擬化，且可在相同實體核心上執行。請求在單執行緒模式中執行執行緒係常見的。

【0004】 用於執行安全多執行緒之管線的一個實施可為用於執行指令之積體電路，該積體電路包括：處理器管線，其經組態以使用該處理器管線之執行單元同時執行來自兩個或更多個執行緒之指令；及執行緒危險

電路，其經組態以偵測第一執行緒之指令已指定為敏感指令，且回應於該敏感指令的偵測，當處理器管線之執行單元正執行該敏感指令時，使用處理器管線之執行單元阻止執行緒而非第一執行緒之指令的執行。

【0005】 在此實施中，僅單個的指令可經保護，從而驗證執行緒的架構狀態係孤立的，而不可視為非架構狀態。

【0006】 可針對所有安全工作永久地保留核心，但若不進行全時間段的安全工作，則此舉可能在效果上降低整個處理器效能。此外，若電腦系統上之大部分工作請求安全環境來執行，則其不靈活。

【發明內容】

【0007】 提出一種用於在處理單元之處理器核心上操作安全碼區段之電腦實施方法，其中該處理單元經組態具有至少一個處理器核心，該至少一個處理器核心用於運行用於在該至少一個處理器核心上執行程式碼之第一執行模式，且在該至少一個處理器核心上執行操作指令之程式碼。該方法至少包含：(i)請求在該至少一個處理器核心上獨佔式安全執行該程式碼之安全碼區段；(ii)設定該至少一個處理器核心以獨佔式安全執行該安全碼區段；(iii)在該至少一個處理器核心上不中斷地執行該安全碼區段；(iv)自該至少一個處理器核心抹除實體處理器核心之架構狀態及非架構狀態；(v)將該至少一個處理器核心設定至用於在該至少一個處理器核心上執行程式碼的該第一執行模式。

【0008】 根據所提出的方法，安全碼區段可在至少最小時間及最小操作指令計數下請求獨佔式安全上下文。此包含，在硬體控制下，至少安全地將實體核心設定至獨佔式安全模式，在最小時間段及/或操作指令數目下不中斷地執行，且最後當在初始時間段及/或操作指令數目後完成安

全碼區段或採取任何中斷時，自快取儲存器或暫存器或記憶體至少抹除實體核心之架構狀態及非架構狀態。

【0009】 有利地，可避免處理器核心中之不同碼區段之間的干擾。可減少碼區段之執行期間的故障數目。此外，藉由處理器核心中之安全碼區段之安全操作中所提出的方法可有利地增強電腦系統的效能。

【0010】 由於本發明之一實施例，另外地或替代地，在將處理器核心設定至獨佔式安全模式之前，至少可儲存實體處理器核心之架構狀態及非架構狀態。因此，可能在完成安全碼區段的執行之後，恢復實體處理器核心之架構狀態及非架構狀態以便繼續程式碼的正常執行。

【0011】 由於本發明之一實施例，另外地或替代地，在將處理器核心設定至第一執行模式之前，至少可恢復實體處理器核心之架構狀態及非架構狀態。因此，在完成安全碼區段的執行之後，恢復實體處理器核心之架構狀態及非架構狀態以便繼續程式碼的正常執行。

【0012】 由於本發明之一實施例，另外地或替代地，可在執行安全碼區段之前，尤其自實體處理器核心之至少一個快取儲存器抹除該實體處理器核心的非架構狀態。藉由此方式，在執行安全碼區段的情況下可能不會出現對已存在資料的干擾。

【0013】 由於本發明之一實施例，另外地或替代地，可藉由處理單元之硬體以硬體受控方式執行實體處理器核心非架構狀態的抹除。有利地，可降低隨後抹除不足之軟體故障的風險。

【0014】 由於本發明之一實施例，另外地或替代地，處理器核心之第一執行模式可為同時多執行緒處理模式。同時多執行緒處理允許執行多個獨立執行緒以更好地利用處理器架構提供的資源，且為尋常處理器核心

之正常執行模式。

【0015】 由於本發明之一實施例，另外地或替代地，安全碼區段之不中斷的執行可界定為最小時間段及/或最小數目的指令。因此，可保證安全碼區段之不受干擾的執行以實現有效處理。

【0016】 由於本發明之一實施例，另外地或替代地，安全碼區段之不中斷的執行可藉由狀態機控制。狀態機可證明為控制安全碼區段之不中斷之執行的一種有效方式。

【0017】 由於本發明之一實施例，另外地或替代地，可在安全碼區段之執行期間阻止中斷。有利地，可在最小時間量及/或操作指令數目下無干擾地執行安全碼區段。

【0018】 由於本發明之一實施例，另外地或替代地，在執行安全碼區段之後自至少一個處理器核心抹除架構狀態及非架構狀態可藉由中斷請求起始。因此，可自執行安全碼區段用剩餘資料無干擾地達成在第一執行狀態中之程式碼的進一步正常執行。

【0019】 由於本發明之一實施例，另外地或替代地，可在虛擬機上或在容器上實施操作指令。在雲端中或在現場之不同客戶之相同實體核心上執行的處理或執行緒可有利地在虛擬機上或在容器上虛擬化。

【0020】 此外，提出一種用於在處理單元之處理器核心上操作安全碼區段的電腦系統，其中該處理單元經組態具有至少一個處理器核心。該電腦系統包含至少一個具有至少一個處理器核心之處理器單元，該處理器核心經組態以執行用於在該至少一個處理器核心上執行程式碼之第一執行模式，且在該至少一個處理器核心上執行操作指令之程式碼。該電腦系統經組態以執行一方法，其至少包含： (i)請求在該至少一個處理器核心上

獨佔式安全執行程式碼之安全碼區段；(ii)設定該至少一個處理器核心以獨佔式安全執行該安全碼區段；(iii)在該至少一個處理器核心上不中斷地執行該安全碼區段；(iv)自該至少一個處理器核心抹除實體處理器核心之架構狀態及非架構狀態；(v)將該至少一個處理器核心設定至用於在該至少一個處理器核心上執行程式碼的該第一執行模式。

【0021】 在所提出之電腦系統上執行安全碼區段可請求獨佔式安全上下文之至少最小時間及/或操作指令之最小計數。此包含，在硬體控制下，至少安全地將實體核心設定至獨佔式安全模式，在最小時間及/或操作指令數目下不中斷地執行，且最後當在初始時間段及/或操作指令數目後完成安全碼區段或採取任何中斷時，自實體核心之快取儲存器或暫存器或記憶體至少抹除架構狀態及非架構狀態。

【0022】 有利地，可避免處理器核心中之不同碼區段之間的干擾。可減少碼區段之執行期間的故障數目。此外，藉由處理器核心中之安全碼區段之安全操作的所提出方法可有利地增強電腦系統的效能。

【0023】 由於本發明之一實施例，另外地或替代地，電腦系統可經組態在將處理器核心設定至獨佔式安全模式之前至少儲存實體處理器核心之架構狀態及非架構狀態。因此，有可能在完成安全碼區段的執行之後，恢復實體處理器核心之架構狀態及非架構狀態以便繼續程式碼的正常執行。

【0024】 由於本發明之一實施例，另外地或替代地，電腦系統可經組態以在將處理器核心設定至第一執行模式之前，至少恢復實體處理器核心之架構狀態及非架構狀態。因此，在完成安全碼區段的執行之後，可恢復實體處理器核心之架構狀態及非架構狀態以便繼續程式碼的正常執行。

【0025】 由於本發明之一實施例，另外地或替代地，電腦系統可經組態以在執行安全碼區段之前，尤其自實體處理器核心之至少一個快取儲存器抹除該實體處理器核心的非架構狀態。藉由此方式，在執行安全碼區段的情況下可能不會出現對已存在資料的干擾。

【0026】 由於本發明之一實施例，另外地或替代地，電腦系統可經組態以藉由處理單元之硬體以硬體受控方式抹除實體處理器核心之非架構狀態。有利地，可降低由於抹除不足造成軟體故障的風險。

【0027】 由於本發明之一實施例，另外地或替代地，處理器核心之第一執行模式可為同時多執行緒處理模式。同時多執行緒處理允許執行多個獨立執行緒以更好地利用處理器架構提供的資源，且為尋常處理器核心之正常執行模式。

【0028】 由於本發明之一實施例，另外地或替代地，電腦系統可經組態以在最小時間段及/或最小指令數目下不中斷地執行安全碼區段。因此，可保證安全碼區段之不受干擾的執行以實現有效處理。

【0029】 由於本發明之一實施例，另外地或替代地，安全碼區段之不中斷執行可由狀態機控制。狀態機可證明為控制安全碼區段之不中斷執行的一種有效方式。

【0030】 由於本發明之一實施例，另外地或替代地，電腦系統可經組態以在執行安全碼區段期間阻止中斷。有利地，可在最小時間量及/或操作指令數目下無干擾地執行安全碼區段。

【0031】 由於本發明之一實施例，另外地或替代地，在執行安全碼區段之後自至少一個處理器核心抹除架構狀態及非架構狀態可藉由中斷請求起始。因此，可自執行安全碼區段用剩餘資料無干擾地達成在第一執行

狀態中之程式碼的進一步正常執行。

【0032】 由於本發明之一實施例，另外地或替代地，可在虛擬機上或在容器上實施操作指令。在雲端中或在現場之不同客戶之相同實體核心上執行的處理或執行緒可有利地在虛擬機上或在容器上虛擬化。

【0033】 此外，提出一種用於在處理單元之處理器核心上操作安全碼區段的有利電腦程式產品，其中該處理單元經組態具有至少一個處理器核心。該電腦系統包含至少一個具有至少一個處理器核心之處理器單元，該處理器核心經組態以執行用於在該至少一個處理器核心上執行程式碼之第一執行模式，且在該至少一個處理器核心上執行操作指令之程式碼。

【0034】 該電腦程式產品包含電腦可讀儲存媒體，其具有隨其實施之程式指令，該等程式指令可由該電腦系統執行以使得該電腦系統執行一種方法，該方法包含：(i)請求在該至少一個處理器核心上獨佔式安全執行程式碼之安全碼區段；(ii)設定該至少一個處理器核心以獨佔式安全執行該安全碼區段；(iii)在該至少一個處理器核心上不中斷地執行該安全碼區段；(iv)自該至少一個處理器核心抹除實體處理器核心之架構狀態及非架構狀態；(v)將該至少一個處理器核心設定至用於在該至少一個處理器核心上執行程式碼的該第一執行模式。

【0035】 另外，提出一種用於執行資料處理程式之資料處理系統，其包含用於執行上文所描述之方法的電腦可讀程式指令。

【圖式簡單說明】

【0036】 本發明以及上文所提及及其他目標及優點可自實施例之以下實施方式中最佳地理解，但不限於本實施例。

【0037】 圖1描繪根據本發明之一實施例之用於在處理單元之處理

器核心上操作安全碼區段的電腦實施方法的流程圖。

【0038】 圖2描繪根據本發明之用於執行方法之資料處理系統的一實例實施例。

【實施方式】

【0039】 在諸圖中，用相同元件符號來指代相同元件。該等圖僅為示意性表示，其不意欲描繪本發明之特定參數。此外，該等圖意欲僅描繪本發明之典型具體實施例，且因此不應被視為限制本發明之範疇。

【0040】 本文所描述之說明性實施例提供一種用於在處理單元之處理器核心上操作安全碼區段的電腦系統，其中該處理單元經組態具有至少一個處理器核心。該電腦系統包含至少一個具有至少一個處理器核心之處理器單元，該處理器核心經組態以執行用於在該至少一個處理器核心上執行程式碼之第一執行模式，且在該至少一個處理器核心上執行操作指令之程式碼。

【0041】 說明性實施例可進一步用於一種方法，其至少包含：(i)請求在該至少一個處理器核心上獨佔式安全執行程式碼之安全碼區段；(ii)設定該至少一個處理器核心以獨佔式安全執行該安全碼區段；(iii)在該至少一個處理器核心上不中斷地執行該安全碼區段；(iv)自至少一個處理器核心抹除架構狀態及非架構狀態；(v)將至少一個處理器核心設定至第一執行模式以用於執行在至少一個處理器核心上之程式碼。

【0042】 圖1描繪根據本發明之一實施例之用於在處理單元216 (如圖2中所描繪)之處理器核心上操作安全碼區段的電腦實施方法的流程圖。

【0043】 該處理單元216經組態具有至少一個處理器核心，該至少一個處理器核心用於運行用於作為正常執行在至少一個處理器核心上執行

程式碼之第一執行模式。

【0044】 處理器核心之第一執行模式可為同時多執行緒處理模式。同時多執行緒處理允許執行多個獨立執行緒以更好地利用處理器架構提供的資源，且為尋常處理器核心之正常執行模式。

【0045】 可在虛擬機上或在容器上實施操作指令。在雲端中或在現場之不同客戶之相同實體核心上執行的處理或執行緒可有利地在虛擬機上或在容器上虛擬化。

【0046】 在步驟S100中，在第一執行模式中，在至少一個處理器核心上執行操作指令之程式碼。

【0047】 在步驟S102中，請求獨佔式安全模式以在至少一個處理器核心上獨佔式安全執行程式碼之安全碼區段。

【0048】 視情況，在步驟S104中，在將處理器核心設定至獨佔式安全模式之前，可至少儲存實體處理器核心之架構狀態及非架構狀態。因此，有可能在完成安全碼區段的執行之後，恢復實體處理器核心之架構狀態及非架構狀態以便繼續程式碼的正常執行。

【0049】 接下來，在步驟S106中，設定至少一個處理器核心以獨佔式安全執行安全碼區段。

【0050】 亦視情況，在步驟S108中，可在執行安全碼區段之前抹除實體處理器核心之非架構狀態。特定言之，可自實體處理器核心之至少一個快取儲存器或自暫存器或自記憶體抹除非架構狀態。抹除實體處理器核心之非架構狀態可藉由處理單元216之硬體以硬體受控方式執行。有利地，可降低由於抹除不足造成軟體故障的風險。藉由此方式，在執行安全碼區段的情況下可能不會出現對已存在資料的干擾。

【0051】 接著，在步驟S110中，在至少一個處理器核心上執行安全碼區段。在最小時間段及/或最小指令數目下不中斷地執行安全碼區段。可藉由狀態機控制安全碼區段之不中斷執行。狀態機可證明為控制安全碼區段之不中斷執行的一種有效方式。

【0052】 可在安全碼區段執行期間阻止任何中斷。因此，可保證安全碼區段之不受干擾的執行以實現有效處理。有利地，可在最小時間量及/或操作指令數目下無干擾地執行安全碼區段。

【0053】 在完成安全碼區段之執行後，在步驟S112中，可尤其自至少一個處理器核心之至少一個快取儲存器或自暫存器或自記憶體抹除架構狀態及非架構狀態。在執行安全碼區段之後自至少一個處理器核心抹除架構狀態及非架構狀態可藉由中斷請求起始。因此，可自執行安全碼區段用剩餘資料無干擾地達成在第一執行狀態中之程式碼的進一步正常執行。

【0054】 視情況，在步驟S112中，若在步驟S104中儲存該架構狀態及非架構狀態，則在將處理器核心設定至第一執行模式之前，可至少恢復實體處理器核心之架構狀態及非架構狀態。因此，在完成安全碼區段的執行之後，可恢復實體處理器核心之架構狀態及非架構狀態以便繼續程式碼的正常執行。

【0055】 接著，在步驟S114中，將至少一個處理器核心設定至第一執行模式以用於執行該至少一個處理器核心上之程式碼，以便在步驟S116中繼續正常執行。

【0056】 現參考圖2，其展示資料處理系統210之實例的示意圖。資料處理系統210僅為合適的資料處理系統之一個實例，且並不意欲暗示對本文中所描述之本發明之實施例的使用或功能性之範疇的任何限制。無論

如何，資料處理系統210能夠經實施及/或執行上文所闡述之功能性中之任一者。

【0057】 在資料處理系統210中，存在電腦系統/伺服器212，其可與眾多其他通用或專用計算系統環境或組態一起操作。可能適合與電腦系統/伺服器212一起使用之熟知計算系統、環境及/或組態之實例包括但不限於：個人電腦系統、伺服器電腦系統、精簡型用戶端、複雜型用戶端、手持型或膝上型電腦裝置、多處理器系統、基於微處理器之系統、機上盒、可程式化消費型電子裝置、網路PC、小型電腦系統、大型電腦系統及包括以上系統或裝置中之任一者的分散式雲端計算環境，以及其類似者。

【0058】 電腦系統/伺服器212可在由電腦系統執行之電腦系統可執行指令(諸如程式模組)的一般上下文中描述。通常，程式模組可包括執行特定任務或實施特定抽象資料類型之常式、程式、物件、組件、邏輯、資料結構等。可在分散式雲端計算環境中實踐電腦系統/伺服器212，其中由經由通信網路而鏈接之遠端處理裝置執行任務。在分散式雲端計算環境中，程式模組可位於包括記憶體儲存裝置的本端及遠端電腦系統儲存媒體兩者中。

【0059】 如圖2中所展示，資料處理系統210中之電腦系統/伺服器212係以通用計算裝置之形式展示。電腦系統/伺服器212之組件可包括但不限於一或多個處理器或處理單元216、系統記憶體228及匯流排218，該匯流排將包括系統記憶體228之多種系統組件耦接至處理單元216。

【0060】 匯流排218表示任何數種類型之匯流排結構中之一或多者，包括記憶體匯流排或記憶體控制器、周邊匯流排、加速圖形埠及使用

多種匯流排架構中之任一者之處理器或本端匯流排。作為實例而非限制，此類架構包括工業標準架構(ISA)匯流排、微通道架構(MCA)匯流排、增強型ISA (EISA)匯流排、視訊電子標準協會(VESA)本端匯流排及周邊組件互連(PCI)匯流排。

【0061】 電腦系統/伺服器212通常包括多種電腦系統可讀媒體。此類媒體可為可由電腦系統/伺服器212存取之任何可用媒體，且其包括揮發性及非揮發性媒體兩者、抽取式及非抽取式媒體兩者。

【0062】 系統記憶體228可包括呈揮發性記憶體之形式的電腦系統可讀媒體，諸如隨機存取記憶體(RAM) 230及/或快取記憶體232。電腦系統/伺服器212可進一步包括其他抽取式/非抽取式、揮發性/非揮發性電腦系統儲存媒體。僅作為實例，可提供儲存系統234以用於自非抽取式、非揮發性磁性媒體(未展示，且通常稱為「硬碟」)讀取及寫入至非抽取式、非揮發性磁性媒體。儘管未展示，但可提供用於自抽取式、非揮發性磁碟(例如，「軟碟」)讀取及寫入至抽取式、非揮發性磁碟之磁碟機，及用於自抽取式、非揮發性光碟(諸如，CD-ROM、DVD-ROM或其他光學媒體)讀取及寫入至抽取式、非揮發性光碟之光碟機。在此等情況下，各者可藉由一或多個資料媒體介面連接至匯流排218。如下文將進一步描繪及描述，記憶體228可包括具有經組態以執行本發明之實施例之功能的一組(例如，至少一個)程式模組的至少一個程式產品。

【0063】 作為實例而非限制，具有一組(至少一個)程式模組242之程式/公用程式240以及作業系統、一或多個應用程式、其他程式模組及程式資料可儲存於記憶體228中。作業系統、一或多個應用程式、其他程式模組及程式資料或其某種組合中之各者可包括網路連接環境之實施。程式模

組242通常執行如本文中所描述之本發明之實施例的功能及/或方法。

【0064】 電腦系統/伺服器212亦可與以下各者通信：諸如鍵盤、指標裝置、顯示器224等之一或多個外部裝置214；使得使用者能夠與電腦系統/伺服器212互動之一或多個裝置；及/或使得電腦系統/伺服器212能夠與一或多個其他計算裝置通信的任何裝置(例如，網路卡、數據機等)。此通信可經由輸入/輸出(I/O)介面222發生。再另外，電腦系統/伺服器212可經由網路適配器220與諸如區域網路(LAN)、通用廣域網路(WAN)及/或公用網路(例如，網際網路)之一或多個網路通信。如所描繪，網路適配器220經由匯流排218與電腦系統/伺服器212之其他組件通信。應理解，儘管未展示，但可結合電腦系統/伺服器212使用其他硬體及/或軟體組件。實例包括但不限於：微碼、裝置驅動器、冗餘處理單元、外部磁碟機陣列、RAID系統、磁帶驅動器及資料歸檔儲存系統等。

【0065】 本發明可為一種系統、一種方法及/或一種電腦程式產品。電腦程式產品可包括(多個)電腦可讀儲存媒體，其上具有電腦可讀程式指令以使得處理器執行本發明之態樣。

【0066】 電腦可讀儲存媒體可為有形裝置，其可保持及儲存指令以供指令執行裝置使用。電腦可讀儲存媒體可為例如但不限於電子儲存裝置、磁性儲存裝置、光學儲存裝置、電磁儲存裝置、半導體儲存裝置或前述各者之任何合適組合。電腦可讀儲存媒體之更特定實例之非窮盡性清單包括以下各者：攜帶型電腦磁片、硬碟、隨機存取記憶體(RAM)、唯讀記憶體(ROM)、可擦除可程式化唯讀記憶體(EPROM或快閃記憶體)、靜態隨機存取記憶體(SRAM)、攜帶型緊密光碟唯讀記憶體(CD-ROM)、數位化通用光碟(DVD)、記憶棒、軟性磁碟、機械編碼裝置(諸如打孔卡片或

其上記錄有指令之凹槽中的凸起結構)及前述各者之任何合適組合。如本文中所使用，不將電腦可讀儲存媒體本身理解為暫時信號，諸如無線電波或其他自由傳播之電磁波、經由波導或其他傳輸媒體傳播之電磁波(例如，經由光纖電纜傳遞之光脈衝)，或經由導線傳輸之電信號。

【0067】 本文中所描述之電腦可讀程式指令可自電腦可讀儲存媒體下載至各別計算/處理裝置或經由網路(例如，網際網路、區域網路、廣域網路及/或無線網路)下載至外部電腦或外部儲存裝置。網路可包含銅傳輸纜線、光傳輸光纖、無線傳輸、路由器、防火牆、交換器、閘道器電腦及/或邊緣伺服器。每一計算/處理裝置中之網路適配器或網路介面自網路接收電腦可讀程式指令且轉遞電腦可讀程式指令以用於儲存於各別計算/處理裝置內之電腦可讀儲存媒體中。

【0068】 用於執行本發明之操作的電腦可讀程式指令可為組譯程式指令、指令集架構(ISA)指令、機器指令、機器相關指令、微碼、韌體指令、狀態設定資料或以一或多種程式設計語言之任何組合撰寫的原始碼或目標碼，該一或多種程式設計語言包括諸如Smalltalk、C++或其類似者的物件導向式程式設計語言，及諸如「C」程式設計語言或類似程式設計語言之習知程式設計語言。電腦可讀程式指令可完全在使用者之電腦上執行、部分地在使用者之電腦上執行、作為獨立套裝軟體執行、部分地在使用者之電腦上執行且部分地在遠端電腦上執行或完全在遠端電腦或伺服器上執行。在後一種情境中，遠端電腦可經由任何類型之網路(包括區域網路(LAN)或廣域網路(WAN))連接至使用者之電腦，或可連接至外部電腦(例如，經由使用網際網路服務提供者之網際網路)。在一些實施例中，電子電路(包括例如可程式化邏輯電路、場可程式化閘陣列(FPGA)或可程式

化邏輯陣列(PLA))可藉由利用電腦可讀程式指令之狀態資訊來個人化電子電路而執行電腦可讀程式指令，以便執行本發明之態樣。

【0069】 本文參考根據本發明之實施例之方法、設備(系統)及電腦程式產品之流程圖說明及/或方塊圖描述本發明之態樣。應理解，可藉由電腦可讀程式指令實施流程圖說明及/或方塊圖中之每一區塊以及流程圖說明及/或方塊圖中之區塊之組合。

【0070】 可將此等電腦可讀程式指令提供至通用電腦、專用電腦或其他可程式化資料處理設備之處理器以製造機器，以使得經由電腦或其他可程式化資料處理設備之處理器執行之指令建立用於實施一或多個流程圖及/或方塊圖區塊中所指定之功能/動作之構件。亦可將此等電腦可讀程式指令儲存於電腦可讀儲存媒體中，該等指令可指導電腦、可程式化資料處理設備及/或其他裝置以特定方式起作用，使得其中儲存有指令之電腦可讀儲存媒體包含製品，該製品包括實施一或多個流程圖及/或方塊圖區塊中所指定之功能/動作之態樣的指令。

【0071】 電腦可讀程式指令亦可載入至電腦、其他可程式化資料處理設備或其他裝置上，以使一系列操作步驟在該電腦、其他可程式化設備或其他裝置上執行以產生電腦實施之程序，使得在該電腦、其他可程式化設備或其他裝置上執行之指令實施一或多個流程圖及/或方塊圖區塊中所指定之功能/動作。

【0072】 諸圖中之流程圖及方塊圖說明根據本發明之各種實施例之系統、方法及電腦程式產品之可能實施之架構、功能性及操作。就此而言，流程圖或方塊圖中之各區塊可表示指令之模組、區段或部分，其包含用於實施經指定邏輯功能之一或多個可執行指令。在一些替代實施中，區

塊中所提及之功能可不按諸圖中所提及之次序發生。舉例而言，視所涉及之功能性而定，連續展示之兩個區塊實際上可實質上同時執行，或該等區塊有時可以相反次序執行。亦將注意，可藉由執行指定功能或動作或執行專用硬體及電腦指令之組合的基於專用硬體之系統實施方塊圖及/或流程圖說明之各區塊，及方塊圖及/或流程圖說明中之區塊之組合。

【0073】 已出於說明目的呈現本發明之各種實施例之描述，但該描述並不意欲為詳盡的或限於所揭示之實施例。在不脫離所描述具體實例之範圍及精神的情況下，許多修改及變化對一般熟習此項技術者而言將顯而易見。本文中所使用的術語經選擇以最佳解釋實施例的原理、實際應用或對市場中發現之技術的技術改良，或使得其他一般熟習此項技術者能夠理解本文中所揭示之實施例。

【0074】 在以下編號項中闡明本發明之另外例示性實施例：

【0075】 編號項1：一種用於在一處理單元(216)之一處理器核心上操作一安全碼區段之電腦實施方法，其中該處理單元(216)經組態具有至少一個處理器核心，該至少一個處理器核心用於運行用於在該至少一個處理器核心上執行程式碼之一第一執行模式，且在該至少一個處理器核心上執行操作指令之程式碼，該方法至少包含：

(i)請求在該至少一個處理器核心上獨佔式安全執行該程式碼之安全碼區段；

(ii)設定該至少一個處理器核心以獨佔式安全執行該安全碼區段；

(iii)在該至少一個處理器核心上不中斷地執行該安全碼區段；

(iv)自該至少一個處理器核心抹除實體處理器核心之架構狀態及非架構狀態；

(v)將該至少一個處理器核心設定至用於在該至少一個處理器核心上執行程式碼的該第一執行模式。

【0076】 編號項2：根據編號項1之方法，其進一步在將該處理器核心設定至一獨佔式安全模式之前，至少儲存該實體處理器核心之該架構狀態及該非架構狀態。

【0077】 編號項3：根據編號項1或編號項2之方法，其進一步在將該處理器核心設定至該第一執行模式之前，至少恢復該實體處理器核心之該架構狀態及該非架構狀態。

【0078】 編號項4：根據編號項1至3中任一項之方法，其進一步在執行該安全碼區段之前，自該實體處理器核心之至少一個快取儲存器抹除該實體處理器核心之該非架構狀態。

【0079】 編號項5：根據編號項4之方法，其中抹除該實體處理器核心之該非架構狀態係藉由該處理單元(216)之硬體以硬體受控方式執行。

【0080】 編號項6：根據編號項1至5中任一項之方法，其中用於在該處理器核心上執行程式碼之該第一執行模式為同時多執行緒處理模式。

【0081】 編號項7：根據編號項1至6中任一項之方法，其中在該至少一個處理器核心上不中斷地執行該安全碼區段係在最小時間段及/或最小指令數目下界定。

【0082】 編號項8：根據編號項1至7中任一項之方法，其中在該至少一個處理器核心上不中斷地執行該安全碼區段係由狀態機控制。

【0083】 編號項9：根據編號項1至8中任一項之方法，其中在該安全碼區段執行期間阻止中斷。

【0084】 編號條項10：根據編號條項1至9中任一項之方法，其中在

執行該安全碼區段後自該至少一個處理器核心抹除該實體處理器核心之該架構狀態及該非架構狀態係藉由中斷請求起始。

【0085】 編號項11：根據編號項1至10中任一項之方法，其中操作指令實施於虛擬機或容器上。

【0086】 編號項12：一種用於在一處理單元(216)之一處理器核心上操作一安全碼區段之電腦系統(212)，其中該處理單元(216)經組態具有至少一個處理器核心，該電腦系統(212)包含至少一個具有至少一個處理器核心之處理器單元(216)，該處理器核心經組態以執行用於在該至少一個處理器核心上執行程式碼之第一執行模式，且在該至少一個處理器核心上執行操作指令之程式碼，其中該電腦系統(212)經組態以執行根據編號項1至11中任一項之方法，其至少包含：

(i)請求在該至少一個處理器核心上獨佔式安全執行該程式碼之安全碼區段；

(ii)設定該至少一個處理器核心以獨佔式安全執行該安全碼區段；

(iii)在該至少一個處理器核心上不中斷地執行該安全碼區段；

(iv)自該至少一個處理器核心抹除實體處理器核心之架構狀態及非架構狀態；

(v)將該至少一個處理器核心設定至用於在該至少一個處理器核心上執行程式碼的該第一執行模式。

【0087】 編號項13：根據編號項12之電腦系統，其經組態以在將該處理器核心設定至獨佔式安全模式之前至少儲存該實體處理器核心之該架構狀態及該非架構狀態。

【0088】 編號項14：根據編號項12或編號項13之方法，其經組態以

在將該處理器核心設定至該第一執行模式之前，至少恢復該實體處理器核心之該架構狀態及該非架構狀態。

【0089】 編號項15：根據編號項12至14中任一項之電腦系統，其經組態以在執行該安全碼區段之前自該實體處理器核心之至少一個快取儲存器抹除該實體處理器核心之該非架構狀態。

【0090】 編號項16：根據編號項12至15中任一項之電腦系統，其經組態以藉由該處理單元之硬體以硬體受控方式抹除該實體處理器核心之該非架構狀態。

【0091】 編號項17：根據編號項12至16中任一項之電腦系統，其中用於在該處理器核心上執行編碼之該第一執行模式為同時多執行緒處理模式。

【0092】 編號項18：根據編號項12至17中任一項之電腦系統，其經組態以在最小時間段及/或最小指令數目下在該至少一個處理器核心上不中斷地執行該安全碼區段。

【0093】 編號項19：根據編號項12至18中任一項之電腦系統，其中在該至少一個處理器核心上不中斷地執行該安全碼區段係由狀態機控制。

【0094】 編號項20：根據編號項12至19中任一項之電腦系統，其經組態以在執行該安全碼區段期間阻止中斷。

【0095】 編號條項21：根據編號條項12至20中任一項之電腦系統，其中在執行該安全碼區段後自該至少一個處理器核心抹除該實體處理器核心之該架構狀態及該非架構狀態係藉由中斷請求起始。

【0096】 編號項22：根據編號項12至21中任一項之電腦系統，其中操作指令實施於虛擬機或容器上。

【0097】 編號項23：一種用於在一處理單元(216)之處理器核心上操作一安全碼區段之電腦程式產品，其中該處理單元(216)經組態具有至少一個處理器核心，該至少一個處理器核心用於運行用於在該至少一個處理器核心上執行程式碼之第一執行模式，且在該至少一個處理器核心上執行操作指令之程式碼，該電腦程式產品包含電腦可讀儲存媒體，該電腦可讀儲存媒體具有隨其實施之程式指令，該等程式指令藉由電腦系統(212)執行以使得該電腦系統(212)執行根據編號項1至11中任一項之方法，該方法包含：

(i)請求在該至少一個處理器核心上獨佔式安全執行該程式碼之安全碼區段；

(ii)設定該至少一個處理器核心以獨佔式安全執行該安全碼區段；

(iii)在該至少一個處理器核心上不中斷地執行該安全碼區段；

(iv)自該至少一個處理器核心抹除實體處理器核心之架構狀態及非架構狀態；

(v)將該至少一個處理器核心設定至用於在該至少一個處理器核心上執行程式碼的該第一執行模式。

【0098】 編號項24：一種用於執行資料處理程式(240)之資料處理系統(210)，該資料處理程式包含用於執行根據編號項1至11中任一項之方法的電腦可讀程式指令。

【0099】 編號項25：一種用於執行用於在處理單元之處理器核心上操作一安全碼區段之指令之積體電路，其中該處理單元經組態具有至少一個處理器核心，該電腦系統包含至少一個具有至少一個處理器核心之處理器單元，該處理器核心經組態以執行用於在該至少一個處理器核心上執行

程式碼之第一執行模式，且在該至少一個處理器核心上執行操作指令之程式碼，其中該積體電路經組態以執行根據編號項1至11中之任一項的方法，該方法至少包含：

(i)請求在該至少一個處理器核心上獨佔式安全執行該程式碼之安全碼區段；

(ii)設定該至少一個處理器核心以獨佔式安全執行該安全碼區段；

(iii)在該至少一個處理器核心上不中斷地執行該安全碼區段；

(iv)自該至少一個處理器核心抹除實體處理器核心之架構狀態及非架構狀態；及

(v)將該至少一個處理器核心設定至用於在該至少一個處理器核心上執行程式碼的該第一執行模式。

【符號說明】

【0100】

210:資料處理系統

212:電腦系統

214:外部裝置

216:處理單元

218:匯流排

220:網路適配器

222:輸入/輸出(I/O)介面

224:顯示器

228:系統記憶體

230:隨機存取記憶體

232:快取記憶體

234:儲存系統

240:程式/公用程式

242:程式模組

S100:步驟

S102:步驟

S104:步驟

S106:步驟

S108:步驟

S110:步驟

S112:步驟

S114:步驟

S116:步驟

【發明申請專利範圍】

【請求項1】

一種用於在一處理單元之一處理器核心上操作一安全碼區段之電腦實施方法，其中該處理單元經組態具有至少一個處理器核心，該至少一個處理器核心用於運行用於在該至少一個處理器核心上執行程式碼之一第一執行模式，且在該至少一個處理器核心上執行操作指令之一程式碼，該方法至少包含：

請求在該至少一個處理器核心上獨佔式安全執行該程式碼之一安全碼區段；

設定該至少一個處理器核心以獨佔式安全執行該安全碼區段；

在該至少一個處理器核心上不中斷地執行該安全碼區段；

自該至少一個處理器核心抹除一實體處理器核心之一架構狀態及一非架構狀態；及

將該至少一個處理器核心設定至用於在該至少一個處理器核心上執行程式碼之該第一執行模式。

【請求項2】

如請求項1之電腦實施方法，其進一步包含：

在將該處理器核心設定至一獨佔式安全模式之前，至少儲存該實體處理器核心之該架構狀態及該非架構狀態。

【請求項3】

如請求項1之電腦實施方法，其進一步包含：

在將該處理器核心設定至該第一執行模式之前，至少恢復該實體處理器核心之該架構狀態及該非架構狀態。

【請求項4】

如請求項1之電腦實施方法，其進一步包含：

在執行該安全碼區段之前自該實體處理器核心之至少一個快取儲存器抹除該實體處理器核心之該非架構狀態。

【請求項5】

如請求項4之電腦實施方法，其中抹除該實體處理器核心之該非架構狀態係藉由該處理單元之硬體以一硬體受控方式執行。

【請求項6】

如請求項1之電腦實施方法，其中用於在該處理器核心上執行程式碼之該第一執行模式為一同時多執行緒處理模式。

【請求項7】

如請求項1之電腦實施方法，其中在該至少一個處理器核心上不中斷地執行該安全碼區段係在一最小時間段及一最小指令數目下界定。

【請求項8】

如請求項1之電腦實施方法，其中在該至少一個處理器核心上不中斷地執行該安全碼區段係藉由一狀態機控制。

【請求項9】

如請求項1之電腦實施方法，其中在執行該安全碼區段期間阻止一中斷。

【請求項10】

如請求項1之電腦實施方法，其中在執行該安全碼區段後自該至少一個處理器核心抹除該實體處理器核心之該架構狀態及該非架構狀態係藉由一中斷請求起始。

【請求項11】

如請求項1之電腦實施方法，其中操作指令實施於一虛擬機或一容器上。

【請求項12】

一種用於在一處理單元之一處理器核心上操作一安全碼區段之電腦系統，其中該處理單元經組態具有至少一個處理器核心，該電腦系統包含至少一個具有至少一個處理器核心之處理器單元，該處理器核心經組態以運行用於在該至少一個處理器核心上執行程式碼之一第一執行模式，且在該至少一個處理器核心上執行操作指令之一程式碼，其中該電腦系統經組態以執行一方法，該方法至少包含：

請求在該至少一個處理器核心上獨佔式安全執行該程式碼之一安全碼區段；

設定該至少一個處理器核心以獨佔式安全執行該安全碼區段；

在該至少一個處理器核心上不中斷地執行該安全碼區段；

自該至少一個處理器核心抹除一實體處理器核心之一架構狀態及一非架構狀態；及

將該至少一個處理器核心設定至該第一執行模式以用於在該至少一個處理器核心上執行程式碼。

【請求項13】

如請求項12之電腦系統，其經組態以在將該處理器核心設定至一獨佔式安全模式之前，至少儲存該實體處理器核心之該架構狀態及該非架構狀態。

【請求項14】

如請求項12之電腦系統，其經組態以在將該處理器核心設定至該第一執行模式之前，至少恢復該實體處理器核心之該架構狀態及該非架構狀態。

【請求項15】

如請求項12之電腦系統，其經組態以在執行該安全碼區段之前自該實體處理器核心之至少一個快取儲存器抹除該實體處理器核心之該非架構狀態。

【請求項16】

如請求項15之電腦系統，其經組態以藉由該處理單元之硬體以一硬體受控方式抹除該實體處理器核心之該非架構狀態。

【請求項17】

如請求項12之電腦系統，其中用於在該處理器核心上執行程式碼之該第一執行模式為一同時多執行緒處理模式。

【請求項18】

如請求項12之電腦系統，其經組態以在一最小時間段及一最小指令數目下不中斷地執行該至少一個處理器核心之該安全碼區段。

【請求項19】

如請求項12之電腦系統，其中該在該至少一個處理器核心上不中斷地執行該安全碼區段係由一狀態機控制。

【請求項20】

如請求項12之電腦系統，其經組態以在執行該安全碼區段期間阻止一中斷。

【請求項21】

如請求項12之電腦系統，其中在執行該安全碼區段後自該至少一個處理器核心抹除該實體處理器核心之該架構狀態及該非架構狀態係藉由一中斷請求起始。

【請求項22】

如請求項12之電腦系統，其中操作指令實施於一虛擬機或一容器上。

【請求項23】

一種用於在一處理單元之一處理器核心上操作一安全碼區段之電腦程式產品，其中該處理單元經組態具有至少一個處理器核心，該至少一個處理器核心用於運行用於在該至少一個處理器核心上執行程式碼之一第一執行模式，且在該至少一個處理器核心上執行操作指令之一程式碼，

該電腦程式產品包含一電腦可讀儲存媒體，其具有隨其實施之程式指令，該等程式指令可由一電腦系統執行以使得該電腦系統執行一方法，該方法包含：

請求在該至少一個處理器核心上獨佔式安全執行該程式碼之一安全碼區段；

設定該至少一個處理器核心以獨佔式安全執行該安全碼區段；

在該至少一個處理器核心上不中斷地執行該安全碼區段；

自該至少一個處理器核心抹除一實體處理器核心之一架構狀態及一非架構狀態；及

將該至少一個處理器核心設定至用於在該至少一個處理器核心上執行程式碼的該第一執行模式。

【請求項24】

一種用於執行一資料處理程式之資料處理系統，該資料處理程式包含用於執行如請求項1之電腦實施方法的電腦可讀程式指令。

【請求項25】

一種用於在一處理單元之一處理器核心上執行操作一安全碼區段的指令之積體電路，其中該處理單元經組態具有至少一個處理器核心，該積體電路包含至少一個具有至少一個處理器核心之處理器單元，該處理器核心經組態以運行用於在該至少一個處理器核心上執行程式碼之一第一執行模式，且在該至少一個處理器核心上執行操作指令之一程式碼，其中該積體電路經組態以執行一方法，該方法至少包含：

請求在該至少一個處理器核心上獨佔式安全執行該程式碼之一安全碼區段；

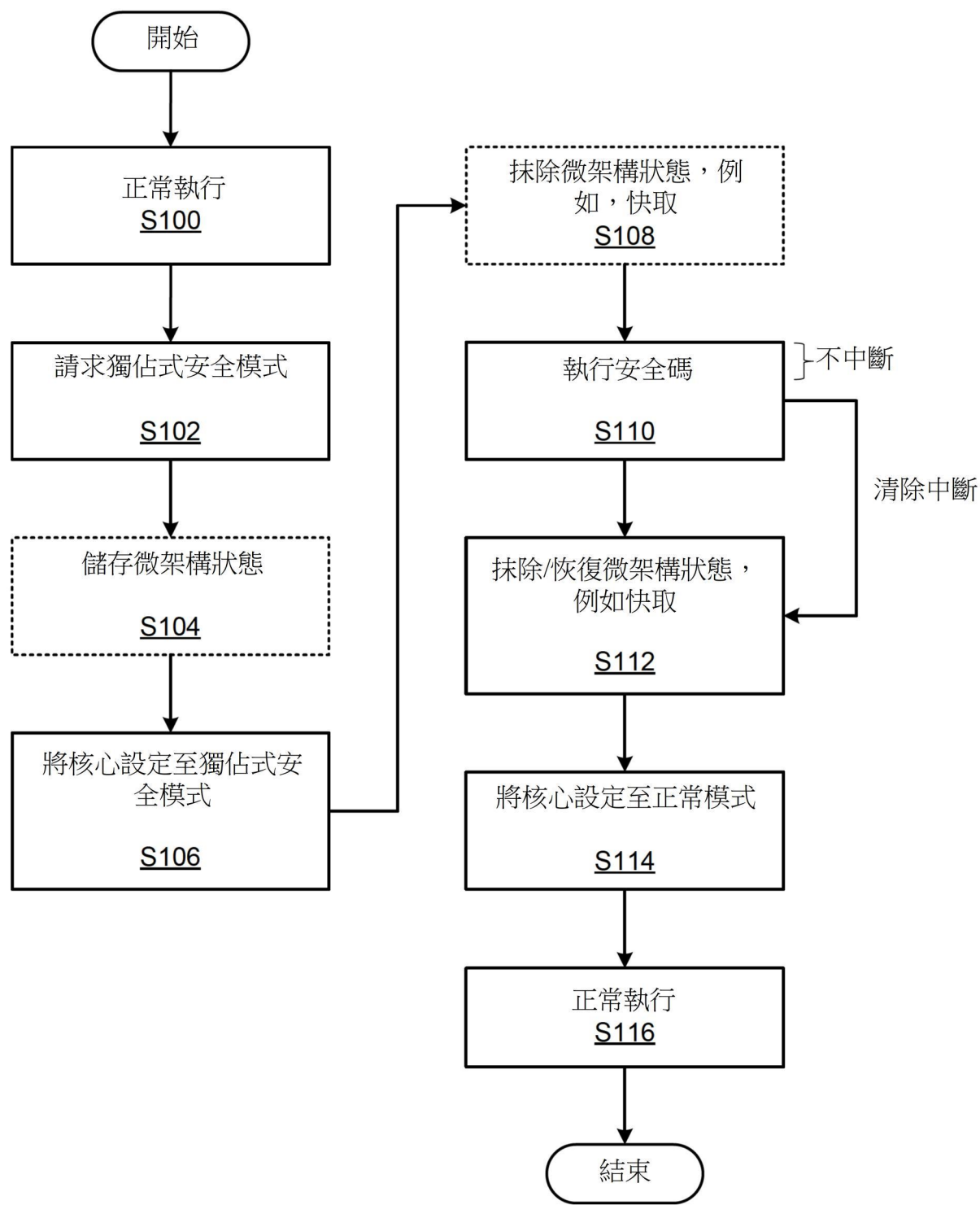
設定該至少一個處理器核心以獨佔式安全執行該安全碼區段；

在該至少一個處理器核心上不中斷地執行該安全碼區段；

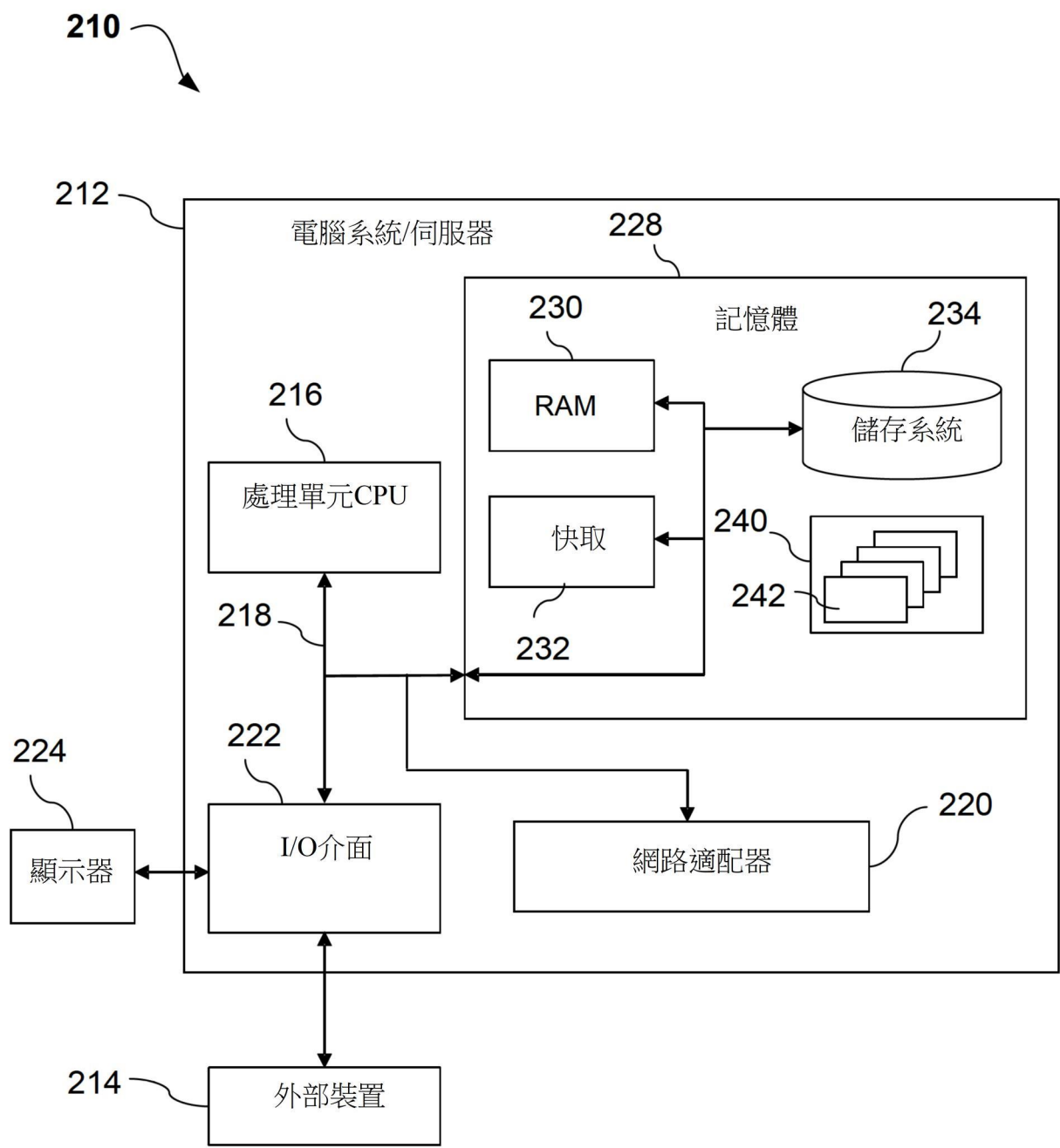
自該至少一個處理器核心抹除一實體處理器核心之一架構狀態及一非架構狀態；及

將該至少一個處理器核心設定至用於在該至少一個處理器核心上執行程式碼的該第一執行模式。

【發明圖式】



【圖1】



【圖2】