I874839

(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 I874839 B**

(45)公告日： 中華民國 114 (2025) 年 03 月 01 日

(21)申請案號：111142532 (22)申請日： 中華民國 110 (2021) 年 09 月 23 日

(51)Int. Cl.： *G06F21/78 (2013.01)* *G06F9/46 (2006.01)*
G06F12/14 (2006.01) *H04L9/08 (2006.01)*

(30)優先權：2020/12/22 美國 17/131,716

(71)申請人：美商英特爾股份有限公司 (美國) INTEL CORPORATION (US)
美國

(72)發明人：瓦迪奧伯 安喬 VAHLDIEK-OBERWAGNER, ANJO LUCAS (DE)；莎西塔 拉維 SAHITA, RAVI L. (US)；維傑 孟那 VIJ, MONA (US)；伊利卡 拉梅庫馬 ILLIKKAL, RAMESHKUMAR (US)；斯坦納 麥可 STEINER, MICHAEL (US)；柯諾特 湯瑪斯 KNAUTH, THOMAS (DE)；庫維斯基 迪米崔 KUVAISKII, DMITRII (RU)；克許納庫瑪 蘇達 KRISHNAKUMAR, SUDHA (IN)；莫辛斯基 克萊斯多夫 ZMUDZINSKI, KRYSTOF C. (US)；史嘉拉塔 文森 SCARLATA, VINCENT (US)；麥金恩 法蘭西斯 MCKEEN, FRANCIS (US)

(74)代理人：林志剛

(56)參考文獻：

TW	202036351A	CN	107870788A
CN	110929266A	US	2017/0177417A1

審查人員：許人偉

申請專利範圍項數：7 項 圖式數：11 共 66 頁

(54)名稱

降低硬體可信執行環境的潛時的處理系統、方法、非暫態電腦可讀媒體及設備

(57)摘要

範例方法和系統旨在減少提供可信執行環境(TEE)的潛時。在 TEE 開始執行之前，初始化該 TEE 包含多個步驟。除了特定於工作負載的初始化之外，還會執行與工作負載無關的初始化，例如向 TEE 增加記憶體。在函數即服務(FaaS)環境中，TEE 大部分與工作負載無關，因此可以在接收該工作負載之前執行。在 TEE 初始化期間執行的某些步驟對於某些類別的工作負載是相同的。因此，TEE 初始化序列的共同部分可以在請求 TEE 之前執行。當為該類別中的工作負載請求 TEE 且為特定目的特殊化 TEE 的部分是已知時，執行初始化 TEE 的最後步驟。

Example methods and systems are directed to reducing latency in providing trusted execution environments (TEEs). Initializing a TEE includes multiple steps before the TEE starts executing. Besides workload-specific initialization, workload-independent initialization is performed, such as adding memory to the TEE. In function-as-a-service (FaaS) environments, a large portion of the TEE is workload-independent, and thus can be performed prior to receiving the workload. Certain steps performed during TEE initialization are identical for certain classes of workloads. Thus, the common parts of the TEE initialization sequence may be performed before the TEE is requested. When a TEE is requested for a

workload in the class and the parts to specialize the TEE for its particular purpose are known, the final steps to initialize the TEE are performed.

指定代表圖：

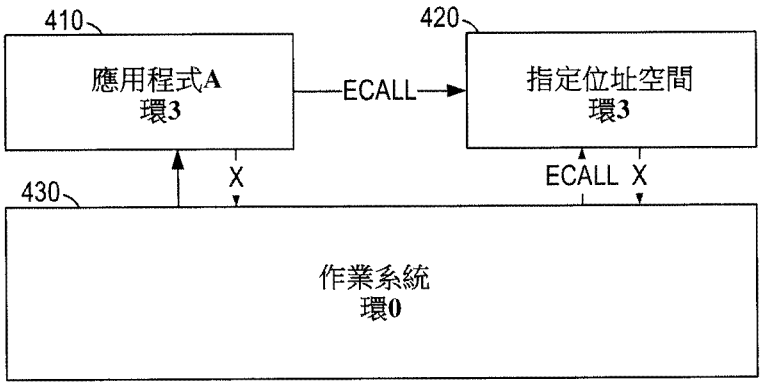
符號簡單說明：

400:方塊圖

410:應用程式

420:指定位址空間

430:作業系統



【圖 4】

專利案號：111142532

公告本

第 111142532 號

I874839

民國 112 年 12 月 15 日修正

【發明摘要】

【中文發明名稱】

降低硬體可信執行環境的潛時的處理系統、方法、非暫態電腦可讀媒體及設備

【英文發明名稱】

PROCESSING SYSTEM, METHOD, NON-TRANSITORY COMPUTER-READABLE STORAGE MEDIUM AND APPARATUS FOR REDUCING LATENCY OF HARDWARE TRUSTED EXECUTION ENVIRONMENTS

【中文】

範例方法和系統旨在減少提供可信執行環境(TEE)的潛時。在TEE開始執行之前，初始化該TEE包含多個步驟。除了特定於工作負載的初始化之外，還會執行與工作負載無關的初始化，例如向TEE增加記憶體。在函數即服務(FaaS)環境中，TEE大部分與工作負載無關，因此可以在接收該工作負載之前執行。在TEE初始化期間執行的某些步驟對於某些類別的工作負載是相同的。因此，TEE初始化序列的共同部分可以在請求TEE之前執行。當為該類別中的工作負載請求TEE且為特定目的特殊化TEE的部分是已知時，執行初始化TEE的最後步驟。

【英文】

Example methods and systems are directed to reducing latency in providing trusted execution environments (TEEs). Initializing a TEE includes multiple steps before the TEE starts executing. Besides workload-specific initialization, workload-independent initialization is performed, such as adding memory to the TEE. In function-as-a-service (FaaS) environments, a large portion of the TEE is workload-independent, and thus can be performed prior to receiving the workload. Certain steps performed during TEE initialization are identical for certain classes of workloads. Thus, the common parts of the TEE initialization sequence may be performed before the TEE is requested. When a TEE is requested for a workload in the class and the parts to specialize the TEE for its particular purpose are known, the final steps to initialize the TEE are performed.

【指定代表圖】圖4

【代表圖之符號簡單說明】

400:方塊圖

410:應用程式

420:指定位址空間

430:作業系統

【特徵化學式】無

第 111142532 號　　民國 112 年 12 月 15 日修正

【發明說明書】

【中文發明名稱】

降低硬體可信執行環境的潛時的處理系統、方法、非暫態電腦可讀媒體及設備

【英文發明名稱】

PROCESSING SYSTEM, METHOD, NON-TRANSITORY COMPUTER-READABLE STORAGE MEDIUM AND APPARATUS FOR REDUCING LATENCY OF HARDWARE TRUSTED EXECUTION ENVIRONMENTS

【技術領域】

【0001】本文揭露的標的大致涉及硬體可信執行環境(trusted execution environment；TEE)。具體而言，本揭露提出用於降低硬體TEE的潛時(latency)的系統和方法。

【先前技術】

【0002】處理器可以使用硬體特權層級來限制在裝置上運行的應用程式的記憶體存取。作業系統以更高的特權層級運行，且可以存取裝置的所有記憶體並為其他應用程式定義記憶體範圍。運行較低特權層級的應用程式只能存取作業系統定義的範圍內的記憶體，不能存取其他應用程式或作業系統的記憶體。然而，應用程式沒有針對惡意或破解的作業系統的保護。

【0003】TEE藉由處理器保護致能，確保加載在TEE內的編碼和資料不會被TEE外部執行的編碼存取。因此，TEE提供一個孤立的執行環境，在硬體層級上防止惡意軟體(包括作業系統)存取包含在TEE中的資料和編碼。

【圖式簡單說明】

【0004】一些實施例在所附圖式的圖中以範例而非限制的方式說明。

【0005】[圖1]是說明依據一些範例實施例的適用於使用TEE提供函數即服務(functions as a service)的伺服器的網路環境的網路圖。

【0006】[圖2]是依據一些範例實施例的適用於降低TEE的潛時的依據一些範例實施例的函數即服務伺服器的方塊圖。

【0007】[圖3]是習知技術的環狀記憶體保護的方塊圖。

【0008】[圖4]是依據一些範例實施例的適用於降低TEE的潛時的基於指定位址空間之記憶體保護的方塊圖。

【0009】[圖5]是依據一些範例實施例的適用於降低TEE潛時的資料庫簡圖的方塊圖。

【0010】[圖6]是依據一些範例實施例的在構建TEE中執行的一系列操作的方塊圖。

【0011】[圖7]是說明依據一些範例實施例的適用於初始化且提供對TEE的存取的方法的操作的流程圖。

【0012】[圖 8]是說明依據一些範例實施例的適用於初始化且提供對TEE的存取的方法的操作的流程圖。

【0013】[圖 9]是說明依據一些範例實施例的適用於初始化且提供對TEE的存取的方法的操作的流程圖。

【0014】[圖 10]是顯示用於計算裝置的軟體架構的範例的方塊圖。

【0015】[圖 11]是電腦系統的範例形式的機器的方塊圖，在該電腦系統中可以執行指令以使機器執行本文討論的任何一或多個方法。

【發明內容】及【實施方式】

【0016】範例方法及系統旨在降低提供TEE的潛時。在最一般的意義上，TEE是任何受信任的執行環境，無論該信任是如何獲得的。然而，如本文所使用的，TEE是藉由在一部分記憶體中執行編碼來提供的，該部分記憶體受保護免於被TEE之外的程序存取，即使那些程序在提升的特權層級上運行。範例TEE包含由Intel® Software Guard Extensions(SGX)建立的指定位址空間和由Intel® Trust Domain Extensions (TDX)建立的信賴網域。

【0017】TEE可用於藉由保護機密資訊免受TEE之外的所有軟體的影響來實現機密資訊的安全處理。TEE也可用於模組化程式設計，其中每個模組含有其自身功能性所需的一切，而不會暴露於其他模組引起的漏洞。舉例而言，針對一個TEE成功的編碼注入攻擊不會影響另一個

TEE的編碼。

【0018】全加密記憶體(total memory encryption；TME)保護記憶體中的資料不被旁路處理器存取。系統在啟動時在處理器內產生加密金鑰，並且決不將金鑰儲存在處理器之外。TME加密金鑰是一個短鑰，因為它不會跨重新啟動持續存在，並且永遠不會儲存在處理器之外。處理器寫入記憶體的所有資料都使用加密金鑰進行加密，並在從記憶體讀回時解密。因此，嘗試直接從記憶體中讀取資料而沒有處理器中介的基於硬體的攻擊將失敗。

【0019】多金鑰TME (MKTME))擴展TME以使用多個金鑰。可以使用TME的短鑰或使用軟體提供的金鑰對個別的記憶體頁面進行加密。這可以在基於軟體的攻擊方面提供比TME更高的安全性，因為攻擊者需要識別目標軟體正在使用的特定金鑰，而不是讓處理器自動解密攻擊軟體已獲得對其存取的任何記憶體。

【0020】初始化TEE需要多個步驟才能開始執行TEE，這會導致在重複建立和銷毀TEE的應用程式中出現潛時。除了特定於工作負載的初始化之外，還會執行與工作負載無關的初始化，例如向指定位址空間增加記憶體。在函數即服務(FaaS)環境中，TEE大部分與工作負載無關，因此可以在接收該工作負載之前執行。

【0021】FaaS平台提供執行應用程式邏輯但不儲存資料的雲端計算伺服器。與平台即服務(platform-as-a-service；PaaS)託管提供者相比，FaaS平台沒有持續運行

的伺服器程序。因此，與對PaaS主機的等效請求相比，對FaaS平台的初始請求可能需要更長的時間來處理，但具有降低閒置時間和更高可擴展性的優勢。如本文所述，降低處理初始請求的潛時提高了FaaS解決方案的吸引力。

【0022】對於某些類別的工作負載，在指定位址空間初始化期間執行的某些步驟是相同的。舉例而言，一類別中的每個指定位址空間都可以使用堆積記憶體。因此，可以在請求指定位址空間之前執行指定位址空間初始化序列的共同部分(例如，添加堆積記憶體)。當指定位址空間被請求用於該類別中的工作負載並且為特定目的特殊化指定位址空間的部分是已知的，執行初始化指定位址空間的最後步驟。如此降低了回應於對指定位址空間的請求而執行所有初始化步驟的潛時。

【0023】TEE可以針對特定工作負載提前初始化。該TEE被視為模板TEE。當請求工作負載的TEE時，將分叉模板TEE，並提供新副本作為請求的TEE。由於分叉現有的TEE比從頭建立新TEE更快，因此降低了潛時。

【0024】TEE可以針對特定工作負載提前初始化並標記為唯讀。該TEE被視為模板TEE。當請求工作負載的TEE時，將建立一個具有對模板TEE的唯讀存取的新TEE。只要模板TEE是唯讀的，多個TEE就可以安全地存取模板TEE。由於建立具有對模板TEE的存取的新TEE比從頭開始建立具有模板TEE的所有編碼和資料的新TEE更快，因此降低了潛時。

【0025】在一些範例實施例中，如本文所述，FaaS意象用於使用短鑰建立TEE。當請求FaaS的TEE時，會為短鑰分配存取控制的金鑰識別符，從而允許快速配置TEE作為回應。

【0026】藉由與初始化指定位址空間的現有方法相比，本文討論的方法和系統降低了潛時。潛時的降低可允許在TEE中額外的功能性被保護，以便使用更細粒度的TEE，或兩者兼有，從而提高系統安全性。當綜合考慮這些影響時，本文描述的一或多個方法可以消除對某些工作或資源的需求，否則這些工作或資源將涉及初始化TEE。相似地，可以減少一或多個機器、資料庫或網路所使用的計算資源。這種計算資源的範例包含處理器週期、網路流量、記憶體使用量、資料儲存容量、功率消耗和冷卻容量。

【0027】圖1是說明依據一些範例實施例的適用於使用TEE提供函數即服務的伺服器的網路環境100的網路圖。網路環境100包含函數即服務伺服器110A和110B、客戶端裝置120A和120B以及網路130。函數即服務伺服器110A、110B透過網路130向客戶端裝置120A、120B提供函數。客戶端裝置120A和120B可以是不同租戶的裝置，因此每個租戶都希望確保其他租戶無法存取他們的租戶特定資料和編碼。因此，函數即服務伺服器110A、110B可以為所提供的每個FaaS使用指定位址空間。

【0028】為了降低提供函數的潛時，可以使用本文描

述的用於降低TEE建立潛時的系統和方法。舉例而言，函數的TEE可以在客戶端裝置120請求函數之前由函數即服務伺服器110部分或全部建立。

【0029】函數即服務伺服器110A、110B以及客戶端裝置120A和120B每個都可以全部或部分地在電腦系統中實現，如下面關於圖9所描述的。函數即服務伺服器110A和110B可以合稱為函數即服務伺服器110或通常稱為函數即服務伺服器110。客戶端裝置120A和120B可以合稱為客戶端裝置120或通常稱為客戶端裝置120。

【0030】圖1中所示的任何機器、資料庫或裝置都可以在藉由軟體修改(例如，經組態或程式設計)後的通用電腦中實現，以作為專用電腦來執行本文描述的用於該機器、資料庫或裝置的函數。舉例而言，以下關於圖9討論能夠實現本文描述的任何一或多個方法的電腦系統。如本文所使用的，「資料庫」是資料儲存資源並且可以儲存結構化為正文檔案、表格、試算表、關連式資料庫(例如，物件關連式資料庫)、三重儲存、階層式資料儲存、文件導向的NoSQL資料庫、檔案儲存或其任何合適的組合的資料。資料庫可以是主記憶體資料庫。此外，圖1中所示的機器、資料庫或裝置中的任何兩或更多個可以組合成單一機器、資料庫或裝置，並且本文針對任何單一機器、資料庫或裝置描述的函數可以在多個機器、資料庫或裝置之間再細分。

【0031】函數即服務伺服器110和客戶端裝置120藉由

網路130連接。網路130可以是能夠在機器、資料庫和裝置之間或之中進行通訊的任何網路。因此，網路130可以是有線網路、無線網路(例如，行動或蜂巢式網路)或其任何合適的組合。網路130可以包含構成專用網路、公眾網路(例如，網際網路)或其任何合適的組合的一或多個部分。

【0032】圖2是依據一些範例實施例的適用於降低TEE的潛時的依據一些範例實施例的函數即服務伺服器110A的方塊圖。函數即服務伺服器110A被示為包含通訊模組210、應用程式的不信賴組件220、應用程式的信賴組件230、信賴網域模組240、引用指定位址空間250、共享記憶體260和專用記憶體270，所有經組態用於相互通訊(例如，透過匯流排、共享記憶體或開關)。本文所述的任何一或多個模組可以使用硬體(例如，機器的處理器)來實現。舉例而言，本文描述的任何模組可以由經組態用於針對該模組執行本文描述的操作的處理器來實現。此外，這些模組中的任何兩或更多個可以組合成單一模組，並且本文針對單一模組描述的函數可以在多個模組中細分。此外，根據各種範例實施例，本文描述為在單一機器、資料庫或裝置內實現的模組可以分散在多個機器、資料庫或裝置上。

【0033】通訊模組210接收發送到函數即服務伺服器110A的資料並從函數即服務伺服器110A傳輸資料。舉例而言，通訊模組210可以從客戶端裝置120A接收執行函數的請求。在執行該函數之後，該函數的結果由通訊模組

210提供給客戶端裝置120A。通訊模組210發送和接收的通訊可以由網路130作為中介。

【0034】不信賴組件220在指定位址空間之外執行。因此，如果作業系統或其他不信賴組件被破解，則不信賴組件220容易受到攻擊。信賴組件230在指定位址空間內執行。因此，即使作業系統或不信賴組件220被破解，信賴組件230的資料和編碼仍然是安全的。

【0035】信賴網域模組240建立和保護指定位址空間並且負責在不信賴組件220和信賴組件230之間轉換執行。可以將簽署的編碼提供給信賴網域模組240，其驗證該編碼自簽署以來沒有被修改過。簽署的編碼被加載到實體記憶體的部分中，該部分被標記為指定位址空間的一部分。此後，硬體保護防止不信賴的軟體對指定位址空間記憶體的存取、修改、執行或其任何合適的組合。可以使用僅對信賴網域模組240可用的金鑰來加密編碼。

【0036】一旦信賴組件230被初始化，不信賴組件220可以使用信賴網域模組240的從不信賴模式轉換到信賴模式的特殊處理器指令來調用信賴組件230的函數。信賴組件230執行參數驗證，如果參數有效則執行請求的函數，並透過信賴網域模組240將控制返回給不信賴組件220。

【0037】信賴網域模組240可以被實現為提供Intel® SGX、Intel® TDX、AMD®安全加密虛擬化環境(SEV)、ARM® TrustZone或其任何合適的組合的Intel®硬體處理器的一或多個組件。在Intel® SGX中，證明是第三方實體在

為該軟體提供機密和受保護資料之前建立軟體實體在受保護的Intel® SGX平台上運行的機制。證明依賴於平台產生準確反映指定位址空間簽章的憑證的能力，其中包含有關指定位址空間安全性屬性的資訊。Intel® SGX架構提供支持兩種證明形式的機制。有一種機制可以在同一平台上運行的指定位址空間之間建立基本判定，支持區域或平台內證明，而另一種機制為指定位址空間和遠端第三方之間的證明提供基礎。

【0038】引用指定位址空間250為指定位址空間(例如，信賴組件230)產生證明。證明是使用非對稱式加密並由內建處理器函數支持的唯一識別被證明的指定位址空間和主機(例如，函數即服務伺服器110A)的證據結構。該證明可以經由通訊模組210提供給客戶端裝置120，從而允許客戶端裝置120確認可信組件230沒有被破解。舉例而言，可以使用防止金鑰存取的硬體來製造帶有內建私密金鑰的處理器。使用該私密金鑰，證明結構可以由該處理器簽章，並且使用硬體製造商發布的相應公鑰，該簽章可以由客戶端裝置120確認。這允許客戶端裝置120確保遠端裝置(例如，函數即服務伺服器110A)上的指定位址空間實際上已被建立而沒有被篡改。

【0039】不信賴組件220和信賴組件230都可以存取和修改共享記憶體260，但只有信賴組件230可以存取和修改專用記憶體270。儘管在圖2中僅示出了一個不信賴組件220、一個信賴組件230和一個專用記憶體270，每個應用

程式可以具有多個信賴組件230，每個信賴組件具有相應的專用記憶體270，以及多個沒有存取任何專用記憶體270的不信賴組件220。此外，多個應用程式可以使用獨立的記憶體空間運行，因而使用獨立的共享記憶體260。在此上下文中，「共享」是指可被所有具有對記憶體空間(例如，應用程式及其作業系統)的存取的軟體和硬體存取的記憶體不一定可被系統上運行的所有應用程式存取。

【0040】圖3是習知技術的環狀記憶體保護的方塊圖300。方塊圖300包含應用程式310和320以及作業系統330。作業系統330在環0(Intel®和AMD®處理器)、例外層級1(ARM®處理器)或等效特權層級中執行處理器命令。應用程式310-320在環3(Intel®和AMD®處理器)、例外層級0(ARM®處理器)或等效特權層級中執行處理器命令。

【0041】硬體處理器阻止以較低特權層級執行的編碼存取作業系統定義的記憶體範圍之外的記憶體。因此，應用程式310的編碼不能直接存取作業系統330或應用程式320的記憶體(如圖3中的「X」所示)。作業系統330藉由預定義特定存取點(例如，藉由調用閘、Intel®處理器上的SYSENTER/SYSEXIT指令、AMD®處理器上的SYSCALL/SYSRET指令，或其任何合適的組合或同等物)向應用程式310-320揭露一些功能性。

【0042】由於作業系統330可以存取所有記憶體，因此應用程式310和320沒有針對惡意作業系統的保護。舉例而言，競爭者可以在運行應用程式310之前修改作業系統

以獲得對應用程式310的編碼和資料的存取，從而允許反向工程。

【0043】此外，如果應用程式能夠利用作業系統330中的漏洞並將其自身提升到作業系統的特權層級，則該應用程式將能夠存取所有記憶體。舉例而言，通常不能存取應用程式320的記憶體的應用程式310(如圖3中應用程式310和320之間的X所示)，在將自己提升為環0或例外層級1之後，將能夠存取應用程式320的記憶體。因此，如果使用者被誘騙運行惡意程式(例如，應用程式310)，則可以直接從記憶體存取使用者或應用程式提供者的私人資料(例如，應用程式320使用的銀行密碼)。

【0044】圖4是依據一些範例實施例的適用於降低TEE的潛時的基於指定位址空間之記憶體保護的方塊圖400。方塊圖400包含應用程式410、指定位址空間420及作業系統430。作業系統430在環0(Intel®和AMD®處理器)、例外層級1(ARM®處理器)或等效特權層級中執行處理器命令。應用程式410及指定位址空間420在環3(Intel®和AMD®處理器)、例外層級0(ARM®處理器)或等效特權層級中執行處理器命令。

【0045】作業系統430分配指定位址空間420的記憶體並向處理器指示要加載到指定位址空間420中的編碼和資料。然而，一旦實例化，作業系統430就不能存取指定位址空間420的記憶體。因此，即使作業系統430是惡意的或被破解的，指定位址空間420的編碼和資料仍然是安全

的。

【0046】指定位址空間420可以向應用程式410提供功能。作業系統430可以控制是否允許應用程式410調用指定位址空間420的函數(例如，藉由使用ECALL指令)。因此，惡意應用程式可能能夠藉由破解作業系統430來獲得調用指定位址空間420的函數的能力。儘管如此，硬體處理器將阻止惡意應用程式直接存取指定位址空間420的記憶體或編碼。因此，指定位址空間420中的編碼不能假設函數被正確地調用或由非攻擊者調用，但指定位址空間420中的編碼對參數檢查和其他內部安全性措施具有完全控制權，並且僅受其內部安全性漏洞的影響。

【0047】圖5是依據一些範例實施例的適用於降低TEE潛時的資料庫簡圖的方塊圖。資料庫簡圖500包含指定位址空間表格510。指定位址空間表格包含格式520的列530A、530B、530C及530D。

【0048】指定位址空間表格510的格式520包含指定位址空間識別符欄位、狀態欄位、唯讀欄位及模板識別符欄位。列530A-530D中的每一者儲存單一指定位址空間的資料。指定位址空間識別符是指定位址空間的唯一識別符。舉例而言，當指定位址空間被建立時，信賴網域模組240可以將下一個未使用的識別符分配給該建立的指定位址空間。狀態欄位指示指定位址空間的狀態，例如正在初始化(已建立但尚未準備好被使用)、已初始化(準備好被使用但尚未使用)、已分配(使用中)。唯讀欄位指示指定位址空間

是否為唯讀。模板識別符欄位含有另一個指定位址空間的指定位址空間識別符，該指定位址空間具有對其的唯讀存取。

【0049】因此，在圖5的範例中，在指定位址空間表格510中示出四個指定位址空間。一個指定位址空間正在初始化、兩個已初始化且一個已分配。列530A的指定位址空間0是唯讀指定位址空間並且用作列530B的指定位址空間1的模板。因此，處理器防止指定位址空間0被執行，但指定位址空間1可以存取指定位址空間0的資料和編碼。可以建立也使用指定位址空間0作為模板的其他指定位址空間，從而允許多個指定位址空間存取指定位址空間0的資料和編碼，而不會增加消耗的記憶體量。列530B-530D的指定位址空間1-3不是唯讀的，因此可以被執行。

【0050】圖6是依據一些範例實施例的藉由信賴網域模組240在構建TEE中執行的一系列操作的方塊圖600。如圖6所示，該系列操作包含ECREATE、EADD/EEXTEND、EINIT、EENTER及FUNCTION START。ECREATE操作建立指定位址空間。EADD操作將初始堆積記憶體增加到指定位址空間。可以使用EEXTEND操作增加額外的記憶體。EINIT操作初始化TEE以供執行。此後，不信賴組件220藉由請求信賴網域模組240執行EENTER操作將執行轉移到TEE。回應於FUNCTION START CALL，藉由執行TEE內的編碼來執行TEE的信賴FUNCTION。

【0051】如圖6所示，操作可以以至少兩種方式劃

分。一種劃分表明，ECREATE、EADD/EEXTEND和EINIT操作由主機應用程式(例如，不信賴組件220)執行，並且EENTER操作將控制權轉移到執行FUNCTION的TEE。另一個劃分表明，無論要增加到TEE的特定編碼和資料如何，都可以執行TEE的建立和為TEE分配堆積記憶體(「與工作負載無關的操作」)，而TEE 的初始化和隨後調用TEE函數取決於載入的特定編碼和資料(「與工作負載相關的操作」)。

【0052】在請求TEE之前，可以藉由執行與工作負載無關的操作來預初始化TEE池。如本文所使用的，預初始化TEE是在應用程式請求TEE之前為其發起至少一個操作的TEE。舉例而言，TEE可能在請求TEE之前由ECREATE操作建立。回應於接收到對TEE的請求，執行與工作負載相關的操作。藉由與在收到請求之前不執行與工作負載無關的操作的解決方案相比，潛時降低了。在一些範例實施例中，用於預初始化TEE的操作與接收對TEE的請求平行執行。舉例而言，可以開始TEE的ECREATE操作，並且在ECREATE操作完成之前，接收到對TEE的請求。因此，預初始化不是由在接收到對TEE的請求之前完成與工作負載無關的操作的特定時間量來定義的，而是由在接收到對TEE的請求之前開始與工作負載無關的操作來定義的。

【0053】對於FaaS環境，每個函數可以共享一個共用運行時間環境，該運行時間環境與工作負載無關，並且在執行與工作負載相關的操作之前被初始化。FaaS函數的啟

動時間是FaaS服務中的一個重要度量，因為較短的啟動時間可以提高服務的彈性。

【0054】圖7是說明依據一些範例實施例的適用於初始化且提供對TEE的存取的方法700的操作的流程圖。方法700包含操作710、720、730和740。作為範例而非限制，方法700可以由圖1的函數即服務伺服器110A執行，使用圖2至4中所示的模組、資料庫及結構。

【0055】在操作710，信賴網域模組240預初始化指定位址空間池。舉例而言，可以為指定位址空間池中的每個指定位址空間執行建立指定位址空間和向指定位址空間分配堆積記憶體的操作。在一些範例實施例中，指定位址空間池包含16至512個指定位址空間、16個指定位址空間、32個指定位址空間或128個指定位址空間。

【0056】在各種範例實施例中，指定位址空間池中的指定位址空間被部分預初始化或完全預初始化。完全預初始化的指定位址空間在請求指定位址空間之前至少執行了一個特定於工作負載的操作。部分預初始化的指定位址空間在請求指定位址空間之前只執行與工作負載無關的操作。預初始化的指定位址空間減少了任何指定位址空間的導出結果時間，但它們對於初始化占整體執行時間主要地位的短期暫時指定位址空間(例如，FaaS工作負載)特別有價值。

【0057】可以藉由分叉或複製模板指定位址空間來建立預初始化的指定位址空間。首先建立模板指定位址空

間，具有預初始化指定位址空間的所需狀態。然後為池中的每個預初始化的指定位址空間分叉或複製模板指定位址空間。在一些範例實施例中，模板指定位址空間本身就是池的一部分。在其他範例實施例中，模板指定位址空間是唯讀的、不可執行的，並且保留為模板以供之後使用。模板指定位址空間可以包含FaaS的記憶體內容和布局。

【0058】指定位址空間池中的每個指定位址空間都可以使用儲存在處理器中的金鑰對其記憶體進行加密。金鑰可以是短鑰(例如，TME短鑰)或具有可在處理器外部存取的金鑰識別符的金鑰。信賴網域模組240或MKTME模組可以產生金鑰並將其分配給指定位址空間。因此，金鑰本身永遠不會暴露在處理器之外。指定位址空間被分配了部分實體記憶體。源自指定位址空間的實體記憶體的記憶體存取請求與指定位址空間的金鑰識別符相關聯，因此與指定位址空間的金鑰相關聯。處理器不會將指定位址空間的金鑰應用於源自指定位址空間實體記憶體之外的記憶體存取。因此，不受信賴的應用程式或組件(例如，不信賴組件220)的記憶體存取僅可以接收指定位址空間的加密資料或編碼。

【0059】在一些範例實施例中，沒有金鑰識別符的不同短鑰(例如，MKTME金鑰)用於加密指定位址空間池中的每個指定位址空間。之後，當請求FaaS的指定位址空間時，會由信賴網域模組240為短鑰分配存取控制的金鑰識別符，從而允許快速提供指定位址空間作為回應。

【0060】在操作720，信賴網域模組240接收對指定位址空間的請求。舉例而言，應用程式的不信賴組件220可以將識別指定位址空間的資料作為請求的一部分提供給信賴網域模組240。識別指定位址空間的資料可以包含指向共享記憶體260中的位址的指標，該位址可由不信賴組件220存取。

【0061】該請求可以包含用於指定位址空間的預先計算的雜湊值並且指示含有用於指定位址空間的編碼和資料的共享記憶體260的一部分(例如，由位址識別的部分和包含在請求中的大小)。信賴網域模組240可以對二進制記憶體狀態(例如，請求中指示的共享記憶體260的部分)執行雜湊函數以確認該請求中提供的雜湊值與所計算的雜湊值匹配。如果雜湊值匹配，則信賴網域模組240已經確認所指示的記憶體實際上含有所請求的指定位址空間的編碼和資料，並且方法700可以繼續。如果雜湊值不匹配，則信賴網域模組240可以回傳錯誤值，防止被修改的記憶體被載入到指定位址空間中。

【0062】在一些範例實施例中，請求包含模板指定位址空間的識別符。信賴網域模組240建立具有唯讀權限的被請求的指定位址空間以存取模板指定位址空間。這允許被請求的指定位址空間讀取模板指定位址空間的資料並執行模板指定位址空間的函數，而無需修改模板指定位址空間的資料或編碼。因此，多個指定位址空間可以無衝突地存取模板指定位址空間，並且模板指定位址空間的資料和

編碼僅儲存一次(而不會為多個指定位址空間中的每一個各儲存一次)。因此，在建立存取指定位址空間期間更少記憶體被複製，從而減少了潛時。

【0063】在操作730，回應於接收到的請求，信賴網域模組240從預初始化的指定位址空間池中選擇指定位址空間。信賴網域模組240可以藉由基於識別隨請求接收的指定位址空間的資料對所選指定位址空間執行附加操作來修改所選指定位址空間，例如圖4中所示的特定於工作負載操作。附加操作可以包含將資料或編碼從請求中指示的共享記憶體260中的位址複製到分配給指定位址空間的專用記憶體270。

【0064】在一些範例實施例中，附加操作包含用新金鑰重新加密分配給指定位址空間的實體記憶體。舉例而言，預初始化步驟可能已經使用短鑰加密了指定位址空間的實體記憶體，並且可以使用用於指定位址空間之具有對應的唯一金鑰識別符的唯一金鑰來重新加密指定位址空間。在金鑰識別符是有限資源(例如，具有固定數量的可用金鑰識別符)的系統中，將短鑰用於預初始化的指定位址空間可能會增加指定位址空間池的最大大小(例如，高於固定數量的可用金鑰識別符)。額外的操作亦可包含為從模板TEE導出映射的編碼之該被選擇的TEE建立安全延伸分頁表(EPT)分頁。

【0065】信賴網域模組240回應於請求提供對所選指定位址空間的存取(操作740)。舉例而言，初始化的指定

位址空間的唯一識別符可以被回傳，可用作稍後對信賴網域模組240的請求(例如，EENTER命令)的參數，以在指定位址空間內執行函數。

【0066】之後，信賴網域模組240可以確定所選指定位址空間的執行完成(例如，回應於接收到指定位址空間退出指令)。分配給已完成指定位址空間的記憶體可能會被釋放。或者，已完成的指定位址空間的狀態可以恢復到預初始化的狀態，並且指定位址空間可以返回到池中。舉例而言，模板指定位址空間可以在指定位址空間上被複製，可以執行反向特定於工作負載操作的操作，在執行特定於工作負載操作之前執行指定位址空間的檢查點，並且在執行完成之後執行檢查點的恢復，或其任何合適的組合。

【0067】藉由與在接收對指定位址空間的請求(操作720)之前不執行指定位址空間的預初始化(操作710)的現有技術實施方式相比，減少了接收請求和提供存取(操作740)之間的延遲。潛時的降低可允許在指定位址空間中額外的功能性被保護，以便使用更細粒度的指定位址空間，或兩者兼有，從而提高系統安全性。此外，當客戶端裝置120藉由網路130調用指定位址空間時，在等待來自函數即服務伺服器110的回應時使用的客戶端裝置120的處理器週期減少，從而提高響應度並降低功率消耗。

【0068】圖8是說明依據一些範例實施例的適用於初始化且提供對TEE的存取的方法800的操作的流程圖。方

法800包含操作810、820、830和840。作為範例而非限制，方法800可以由圖1的函數即服務伺服器110A執行，使用圖2至4中所示的模組、資料庫及結構。

【0069】在操作810中，信賴網域模組240建立標記為唯讀的模板指定位址空間。舉例而言，指定位址空間可以被完整建立，將編碼和資料載入到專用記憶體270中。然而，由於模板指定位址空間是唯讀的，因此不能直接從不信賴組件220調用模板指定位址空間的函數。參考圖3的指定位址空間表格310，列330A示出唯讀模板指定位址空間。

【0070】在操作820，信賴網域模組240接收對指定位址空間的請求。舉例而言，應用程式的不信賴組件220可以將識別指定位址空間的資料作為請求的一部分提供給信賴網域模組240。識別指定位址空間的資料可以包含指向共享記憶體260中的位址的指標，該位址可由不信賴組件220存取。

【0071】在操作830，回應於接收到的請求，信賴網域模組240複製模板指定位址空間以建立所請求的指定位址空間。舉例而言，信賴網域模組240可以確定識別指定位址空間的資料指示所請求的指定位址空間用於與模板指定位址空間相同的編碼和資料。該確定可以基於指定位址空間編碼和資料的簽章、指定位址空間編碼和資料的訊息鑑別碼(MAC)、非對稱式加密或其任何合適的組合。

【0072】信賴網域模組240回應於請求提供對所選指

定位址空間的存取(操作840)。舉例而言，初始化的指定位址空間的唯一識別符可以被回傳，可用作稍後對信賴網域模組240的請求(例如，EENTER命令)的參數，以在指定位址空間內執行函數。

【0073】藉由與回應於接收到對指定位址空間的請求來建立指定位址空間(操作820)而不是複製模板指定位址空間來建立所請求的指定位址空間(操作830)的現有技術實現相比，減少了接收請求和提供存取(操作840)之間的延遲。潛時的降低可允許在指定位址空間中額外的功能性被保護，以便使用更細粒度的指定位址空間，或兩者兼有，從而提高系統安全性。此外，當客戶端裝置120藉由網路130調用指定位址空間時，在等待來自函數即服務伺服器110的回應時使用的客戶端裝置120的處理器週期減少，從而提高響應度並降低功耗。

【0074】圖9是說明依據一些範例實施例的適用於初始化且提供對TEE的存取的方法900的操作的流程圖。方法900包含操作910、920、930和940。作為範例而非限制，方法900可以由圖1的函數即服務伺服器110A執行，使用圖2至4中所示的模組、資料庫及結構。

【0075】在操作910，信賴網域模組240預初始化第一類別的第一指定位址空間池和第二類別的第二指定位址空間池。預初始化是完整的或部分的。對於完整初始化，池中的指定位址空間已完全準備好被使用並且已經載入指定位址空間的編碼和資料。因此，該類別的所有成員都是相

同的。對於部分初始化，池中的指定位址空間共享一或多個特性，例如使用的堆積記憶體的量。指定位址空間關於共享的特性進行初始化，但在預初始化期間並未載入指定位址空間的實際編碼和資料。此外，可以在稍後的步驟中執行進一步的客制化。因此，當執行部分初始化時，不同的指定位址空間可以是該類別的成員。

【0076】在操作920中，信賴網域模組240接收對第一類別指定位址空間的請求。舉例而言，應用程式的不信賴組件220可以將識別指定位址空間的資料作為請求的一部分提供給信賴網域模組240。識別指定位址空間的資料可以包含指向共享記憶體260中的位址的指標，該位址可由不信賴組件220存取。識別該類別指定位址空間的資料可以包含在指定位址空間或請求中。

【0077】在操作930，回應於接收到的請求，信賴網域模組240從用於第一類別的預初始化的指定位址空間池中選擇指定位址空間。信賴網域模組240可以藉由基於識別隨請求接收的指定位址空間的資料對所選指定位址空間執行附加操作來修改所選指定位址空間，例如圖4中所示的特定於工作負載操作。附加操作可以包含將資料或編碼從請求中指示的共享記憶體260中的位址複製到分配給指定位址空間的專用記憶體270。

【0078】信賴網域模組240回應於請求提供對所選指定位址空間的存取(操作940)。舉例而言，初始化的指定位址空間的唯一識別符可以被回傳，可用作稍後對信賴網

域模組240的請求(例如，EENTER命令)的參數，以在指定位址空間內執行函數。

【0079】藉由使用不同類別的不同池，可以將相似但需求相對較低的指定位址空間放入一個共用類別中進行部分預初始化，從而降低潛時，同時僅按其需求比例消耗資源。同時，高需求的指定位址空間可以完全預初始化，進一步降低潛時。

【0080】鑑於上述標的的實施方式，本案揭露以下所列的範例，其中範例的一個特徵單獨或範例的多個特徵結合起來，並且可選地，與一或多個進一步範例的一或多個特徵相組合，也是也落入本案的揭露範圍內的進一步範例。

【0081】範例1是一種提供可信執行環境(TEE)的系統，該系統包括：處理器；以及與該處理器耦接的儲存裝置，用於儲存指令，當該指令由該處理器執行時，使該處理器執行以下步驟：預初始化TEE池，該預初始化該TEE池中的每個TEE包含為該TEE分配該儲存裝置的記憶體；在該TEE池的該預初始化後，收到對TEE的請求；從該預先初始化的TEE池中選擇該TEE；以及回應於該請求，提供對該被選擇的TEE的存取。

【0082】在範例2中，範例1的標的包含，其中該指令進一步使該處理器執行以下步驟：在提供對該被選擇的TEE的存取之前，基於該請求中的資訊修改該被選擇的TEE。

【0083】在範例3中，範例2的標的包含，其中該修改該被選擇的TEE包括啟動該被選擇的TEE。

【0084】在範例4中，範例2-3的標的包含，其中該修改該被選擇的TEE包括將資料或編碼複製到分配給該TEE的記憶體。

【0085】在範例5中，範例2-4的標的包含，其中該修改該被選擇的TEE包括：分配加密金鑰給該被選擇的TEE；以及使用該加密金鑰加密分配給該TEE的該記憶體。

【0086】在範例6中，範例1-5的標的包含，其中：該TEE池的該預初始化包括將模板TEE的狀態複製到該TEE池的每個TEE。

【0087】在範例7中，範例1-6的標的包含，其中該指令進一步使該處理器執行以下步驟：基於確定該被選擇的TEE已完成執行，將該被選擇的TEE復原到模板TEE的狀態。

【0088】在範例8中，範例1-7的標的包含，其中該指令進一步使該處理器執行以下步驟：接收釋放該被選擇的TEE的請求；以及回應於釋放該被選擇的TEE的該請求，將該被選擇的TEE返回到該TEE池。

【0089】在範例9中，範例1-8的標的包含，其中該指令進一步使該處理器執行以下步驟：接收預先計算的雜湊值；確定二進制記憶體狀態的雜湊值；以及基於該確定的雜湊值和該預先計算的雜湊值，將該二進制記憶體狀態從

不安全的記憶體複製到該被選擇的TEE。

【0090】範例10是一種提供TEE的系統，該系統包括：處理器；以及與該處理器耦接的儲存裝置，用於儲存指令，當該指令由該處理器執行時，使該處理器執行以下步驟：預初始化TEE池；建立儲存在儲存裝置中的模板TEE並標記為唯讀；接收請求；以及回應於該請求：複製該模板TEE以建立TEE；以及提供存取至該建立的TEE。

【0091】在範例11中，範例10的標的包含，其中該模板TEE包括用於函數即服務(FaaS)的初始記憶體內容和布局。

【0092】在範例12中，範例10-11的標的包含，其中該處理器阻止該模板TEE的執行。

【0093】範例13是一種提供TEE的方法，該方法包括：藉由處理器預初始化TEE池，該預初始化該TEE池中的每個TEE包含為該TEE分配儲存裝置的記憶體；在該TEE池預初始化之後，藉由該處理器接收請求；以及回應於該請求：藉由該處理器，從該預先初始化的TEE池中選擇TEE；以及藉由該處理器，提供對該被選擇的TEE的存取。

【0094】在範例15中，範例14的標的包含，在提供對該被選擇的TEE的存取之前，基於該請求中的資訊修改該被選擇的TEE。

【0095】在範例16中，範例15的標的包含，其中修改該被選擇的TEE包括啟動被選擇的TEE。

【0096】在範例17中，範例15-16的標的包含，其中該修改該被選擇的TEE包括將資料或編碼複製到分配給該TEE的記憶體。

【0097】在範例18中，範例15-17的標的包含，其中該修改該被選擇的TEE包括：分配加密金鑰給該被選擇的TEE；以及使用該加密金鑰加密分配給該TEE的該記憶體。

【0098】在範例19中，範例14-18的標的包含，其中：該TEE池的該預初始化包括將模板TEE的狀態複製到該TEE池的每個TEE。

【0099】在範例20中，範例14-19的標的包含，基於確定該被選擇的TEE已完成執行，將該被選擇的TEE復原到模板TEE的狀態。

【0100】在範例21中，範例14-20的標的包含，接收釋放該被選擇的TEE的請求；以及回應於釋放該被選擇的TEE的該請求，將該被選擇的TEE返回到該TEE池。

【0101】在範例22中，範例14-21的標的包含，接收預先計算的雜湊值；確定二進制記憶體狀態的雜湊值；以及基於該確定的雜湊值和該預先計算的雜湊值，將該二進制記憶體狀態從不安全的記憶體複製到該被選擇的TEE。

【0102】範例23是一種提供可信執行環境(TEE)的方法，該方法包括：藉由處理器建立儲存在儲存裝置中的模板TEE並標記為唯讀；藉由處理器接收請求；並且回應於該請求：複製該模板TEE以建立TEE；以及提供對該建立

的TEE的存取。

【0103】在範例24中，範例23的標的包含，其中該模板TEE包括用於函數即服務(FaaS)的初始記憶體內容和布局。

【0104】在範例25中，範例23-24的標的包含，其中該處理器阻止該模板TEE的執行。

【0105】範例26是一種提供TEE的方法，該方法包括：藉由處理器使用第一加密金鑰加密資料和編碼；將加密的該資料和編碼儲存在儲存裝置中；藉由處理器接收請求；回應於該請求：分配第二加密金鑰給TEE；使用該第一加密金鑰對加密的該資料和編碼進行解密；使用該第二加密金鑰對解密後的該資料和編碼進行加密；以及提供對該TEE的存取。

【0106】範例27是一種非暫態電腦可讀媒體，具有用於使處理器藉由執行包括以下操作的操作來提供TEE的指令：預初始化TEE池，該預初始化該TEE池中的每個TEE，包含為該TEE分配儲存裝置的記憶體；在該TEE池的該預初始化後，收到對TEE的請求；從該預先初始化的TEE池中選擇該TEE；以及回應於該請求，提供對該被選擇的TEE的存取。

【0107】在範例28中，範例27的標的包含，其中該操作進一步包括：在提供對該被選擇的TEE的存取之前，基於該請求中的資訊修改該被選擇的TEE。

【0108】在範例29中，範例28的標的包含，其中修改

該被選擇的TEE包括啟動該被選擇的TEE。

【0109】在範例30中，範例28-29的標的包含，其中該修改該被選擇的TEE包括將資料或編碼複製到分配給該TEE的記憶體。

【0110】在範例31中，範例28-30的標的包含，其中該修改該被選擇的TEE包括：分配加密金鑰給該被選擇的TEE；以及使用該加密金鑰加密分配給該TEE的該記憶體。

【0111】在範例32中，範例27-31的標的包含，其中：該TEE池的該預初始化包括將模板TEE的狀態複製到該TEE池的每個TEE。

【0112】在範例33中，範例27-32的標的包含，其中該操作進一步包括：基於確定該被選擇的TEE已完成執行，將該被選擇的TEE復原到模板TEE的狀態。

【0113】在範例34中，範例27-33的標的包含，其中該操作進一步包括：接收釋放該被選擇的TEE的請求；以及回應於釋放該被選擇的TEE的該請求，將該被選擇的TEE返回到該TEE池。

【0114】在範例35中，範例27-34的標的包含，其中該操作進一步包括：接收預先計算的雜湊值；確定二進制記憶體狀態的雜湊值；以及基於該確定的雜湊值和該預先計算的雜湊值，將該二進制記憶體狀態從不安全的記憶體複製到該被選擇的TEE。

【0115】範例36是一種非暫態電腦可讀媒體，具有用

於使處理器藉由執行包括以下操作的操作來提供TEE的指令：建立儲存在儲存裝置中的模板TEE並標記為唯讀；接收請求；以及回應於該請求：複製該模板TEE以建立TEE；以及提供對該建立的TEE的存取。

【0116】在範例37中，範例36的標的包含，其中該模板TEE包括用於函數即服務(FaaS)的初始記憶體內容和布局。

【0117】在範例38中，範例36-37的標的包含，其中該操作進一步包括：防止該模板TEE的執行。

【0118】範例39是一種非暫態電腦可讀媒體，具有用於使處理器藉由執行包括以下操作的操作來提供TEE的指令：使用第一加密金鑰加密資料和編碼；將加密的該資料和編碼儲存在儲存裝置中；接收請求；回應於該請求：分配第二加密金鑰給TEE；使用該第一加密金鑰對加密的該資料和編碼進行解密；使用該第二加密金鑰對解密後的該資料和編碼進行加密；以及提供對該TEE的存取。

【0119】範例40是一種提供TEE的系統，該系統包括：儲存機構；以及處理機構用以：預初始化TEE池，該預初始化該TEE池中的每個TEE，包含為該TEE分配儲存機構的記憶體；接收對TEE的請求；從該預先初始化的TEE池中選擇該TEE；以及回應於該請求，提供對該被選擇的TEE的存取。

【0120】在範例41中，範例40的標的包含，其中，該處理機構進一步用以：在提供對該被選擇的TEE的存取之

前，基於該請求中的資訊修改該被選擇的TEE。

【0121】在範例42中，範例41的標的包含，其中修改該被選擇的TEE包括啟動被選擇的TEE。

【0122】在範例43中，範例41-42的標的包含，其中該修改該被選擇的TEE包括將資料或編碼複製到分配給該TEE的記憶體。

【0123】在範例44中，範例41-43的標的包含，其中該修改該被選擇的TEE包括：分配加密金鑰給該被選擇的TEE；以及使用該加密金鑰加密分配給該TEE的該記憶體。

【0124】在範例45中，範例40-44的標的包含，其中：該TEE池的該預初始化包括將模板TEE的狀態複製到該TEE池的每個TEE。

【0125】在範例46中，範例40-45的標的包含，其中，該處理機構進一步用以：基於確定該被選擇的TEE已完成執行，將該被選擇的TEE復原到模板TEE的狀態。

【0126】在範例47中，範例40-46的標的包含，其中，該處理機構進一步用以：接收釋放該被選擇的TEE的請求；以及回應於釋放該被選擇的TEE的該請求，將該被選擇的TEE返回到該TEE池。

【0127】在範例48中，範例40-47的標的包含，其中，該處理機構進一步用以：接收預先計算的雜湊值；確定二進制記憶體狀態的雜湊值；以及基於該確定的雜湊值和該預先計算的雜湊值，將該二進制記憶體狀態從不安全

的記憶體複製到該被選擇的TEE。

【0128】範例49是一種提供TEE的系統，該系統包括：儲存機構；以及處理機構用以：建立儲存在儲存機構中的模板TEE並標記為唯讀；接收請求；以及回應於該請求：複製該模板TEE以建立TEE；以及提供對該TEE的存取。

【0129】在範例50中，範例49的標的包含，其中該模板TEE包括用於函數即服務(FaaS)的初始記憶體內容和布局。

【0130】在範例51中，範例49-50的標的包含，其中該處理機構阻止該模板TEE的執行。

【0131】範例52是一種提供TEE的系統，該系統包括：儲存機構；以及處理機構用以：使用第一加密金鑰加密資料和編碼；將加密的該資料和編碼儲存在儲存機構中；接收請求；回應於該請求：分配第二加密金鑰給TEE；使用該第一加密金鑰對加密的該資料和編碼進行解密；使用該第二加密金鑰對解密後的該資料和編碼進行加密；以及提供對該TEE的存取。

【0132】範例53是一種包含指令的至少一種機器可讀媒體，當該指令由處理電路執行時，使該處理電路執行操作以實現範例1-52中的任一個。

【0133】範例54是一種包括用於實施範例1-52中任一個的機構的設備。

【0134】範例55是一種實施範例1-52中任何一個的系

統。

【0135】範例56是一種實施範例1-52中任何一個的方法。

【0136】圖10是顯示用於計算裝置的軟體架構1002的範例的方塊圖1000。架構1002可以與各種硬體架構結合使用，舉例而言，如本文所述。圖10僅是軟體架構的非限制性範例，並且可以實現許多其他架構以幫助本文描述的功能性。代表的硬體層1004被描繪並且可以代表例如任何上面提到的計算裝置。在一些範例中，硬體層1004可以根據圖10的電腦系統的架構來實現。

【0137】代表的硬體層1004包括具有相關聯的可執行指令1008的一或多個處理單元1006。可執行指令1008表示軟體架構1002的可執行指令，包含本文所述的方法、模組、子系統和組件等的實施方式，並且還可以包含也具有可執行指令1008的記憶體及/或儲存模組1010。硬體層1004還可以包括由表示硬體層1004的任何其他硬體的其他硬體1012指示的其他硬體，例如作為軟體架構1002的部分示出的其他硬體。

【0138】在圖10的範例架構中，軟體架構1002可被概念化為層的堆疊，其中每一層提供特定功能。舉例而言，軟體架構1002可以包含例如作業系統1014、程式館1016、框架/中介軟體1018、應用程式1020和表示層1044的層。在操作上，應用程式1020及/或層內的其他組件可以藉由軟體堆疊調用應用程式設計介面(API)呼叫1024，並存取

回應、回應於API呼叫1024而被示為訊息1026的回傳值等。所示的層在本質上具有代表性，且並非所有軟體架構都具有所有的層。舉例而言，一些行動或專用作業系統可能不提供框架/中介軟體層1018，而其他可能提供這樣的層。其他軟體架構可能包含額外的或不同的層。

【0139】作業系統1014可以管理硬體資源並提供公用服務。作業系統1014可以包含例如核心1028、服務1030和驅動程式1032。核心1028可以充當硬體和其他軟體層之間的抽象化層。舉例而言，核心1028可以負責記憶體管理、處理器管理(例如，排程)、組件管理、網路、安全性設定等。服務1030可以為其他軟體層提供其他公用服務。在一些範例中，服務1030包含中斷服務。中斷服務可以偵測到中斷的接收，並且作為回應，使架構1002暫停其當前處理並在存取中斷時執行中斷服務常式(ISR)。

【0140】驅動程式1032可負責控制底層硬體或與底層硬體介接。例如，驅動程式1032可以包含顯示驅動程式、相機驅動程式、藍牙®驅動程式、快閃記憶體驅動程式、串列通訊驅動程式(例如，通用序列匯流排(USB)驅動程式)、Wi-Fi®驅動程式、NFC驅動程式、音訊驅動程式、電源管理驅動程式等，具體取決於硬體組態。

【0141】程式館1016可以提供可以由應用程式1020及/或其他組件及/或層使用的共用基礎建設。程式館1016通常提供允許其他軟體模組以比直接與底層作業系統1014功能(例如，核心1028、服務1030及/或驅動程式1032)介接更

容易的方式執行任務的功能。程式館1016可以包含系統程式館1034(例如，C標準程式館)，其可以提供諸如記憶體分配函數、字串調處函數、數學函數等的函數。此外，程式館1016可以包括API程式館1036，例如媒體程式館(例如，支持各種媒體格式的呈現和調處的程式館，例如MPEG4、H.264、MP3、AAC、AMR、JPG、PNG格式)、繪圖程式館(例如，OpenGL框架，可用於在顯示器上呈現二維和三維圖形內容)、資料庫程式館(例如，可以提供各種關連式資料庫函數的SQLite)、網頁程式館(例如，可以提供網頁瀏覽功能的WebKit)等。程式館1016還可以包含多種其他程式館1038以向應用程式1020和其他軟體組件/模組提供許多其他API。

【0142】框架/中介軟體1018可以提供可以由應用程式1020及/或其他軟體組件/模組利用的更高層級的共用基礎建設。舉例而言，框架/中介軟體1018可以提供各種圖形使用者介面(GUI)函數、高階資源管理、高階定位服務等。框架/中介軟體1018可以提供可以由應用程式1020及/或其他軟體組件/模組使用的廣泛的其他API，其中一些可以特定於特定作業系統或平台。

【0143】應用程式1020包含內建應用程式1040及/或第三方應用程式1042。代表性內建應用程式1040的範例可以包含但不限於接觸應用程式、瀏覽器應用程式、書籍閱讀器應用程式、定位應用程式、媒體應用程式、訊息應用程式及/或遊戲應用程式。第三方應用程式1042可以包含

任何內建應用程式1040以及各式各樣的其他應用程式。在特定範例中，第三方應用程式1042(例如，由特定平台供應商以外的實體使用Android™或iOS™軟體開發套件(SDK)開發的應用程式)可以是在例如iOS™、Android™、Windows® Phone或其他行動計算裝置作業系統的行動作業系統上運行的行動軟體。在此範例中，第三方應用程式1042可以調用由例如作業系統1014的行動作業系統提供的API呼叫1024以促進本文描述的功能。

【0144】應用程式1020可以利用內建作業系統函數(例如，核心1028、服務1030及/或驅動程式1032)、程式館(例如，系統程式館1034、API程式館1036和其他程式館1038)、框架/中介軟體1018來建立與系統的使用者互動的使用者介面。替代地或附加地，在一些系統中，與使用者的互動可以透過表示層(例如表示層1044)發生。在這些系統中，應用程式/模組「邏輯」可以是單獨於和使用者互動的應用程式/模組的各個方面外。

【0145】一些軟體架構利用虛擬機器。在圖10的範例中，這由虛擬機器1048說明。虛擬機器建立一個軟體環境，其中應用程式/模組可以像在硬體計算裝置上執行一樣執行。虛擬機器由主機作業系統(作業系統1014)託管，並且通常(但不總是)具有虛擬機器監視器1046，其管理虛擬機器1048的操作以及與主機作業系統(即，作業系統1014)的介面。軟體架構在虛擬機器1048內執行，例如作業系統1050、程式館1052、框架/中介軟體1054、應用程

式1056及/或表示層1058。在虛擬機器1048內執行的這些軟體架構的層可以與先前描述的對應的層相同或可不同。

模組、組件及邏輯

【0146】某些實施例在本文中被描述為包含邏輯或多個組件、模組或機制。模組可以構成軟體模組(例如，體現在(1)非暫時性機器可讀媒體上或(2)在傳輸信號中的編碼)或硬體實現的模組。硬體實現的模組是能夠執行某些操作的有形單元，並且可以以某種方式組態或配置。在範例實施例中，一或多個電腦系統(例如，獨立的、客戶端或伺服器電腦系統)或一或多個硬體處理器可以由軟體(例如，應用程式或應用程式部分) 組態為運行以執行本文所述的某些操作的硬體實現的模組。

【0147】在各種實施例中，硬體實現的模組可以機械地或電子地實現。舉例而言，硬體實現的模組可以包括永久組態的專用電路或邏輯(例如，作為專用處理器，例如現場可程式設計邏輯閘陣列(FPGA)或特殊應用積體電路(ASIC))以執行某些操作。硬體實現的模組還可以包括由軟體臨時組態以執行某些操作的可程式設計邏輯或電路(例如，包含在通用處理器或另一個可程式設計處理器內)。應當理解，以機械方式、在專用和永久組態的電路中或在臨時組態的電路(例如，由軟體組態)中實現硬體實現的模組的決定可能受成本和時間考慮的驅動。

【0148】因此，用詞「硬體實現的模組」應理解為包

含有形實體，即實體構造、永久組態(例如，硬體化)或臨時或暫態組態(例如，被程式設計)為以某種方式操作及/或執行本文所描述的某些操作的實體。考慮到硬體實現的模組被臨時組態(例如，被程式設計)的實施例，每個硬體實現的模組都不需要在任何一個時間的實例上組態或實例化。舉例而言，在硬體實現的模組包括使用軟體組態的通用處理器的情況下，通用處理器可以在不同時間被組態為相應的不同硬體實現的模組。軟體可以相應地組態處理器，例如，以在一個時間實例構成特定的硬體實現的模組並且在不同的時間實例構成不同的硬體實現的模組。

【0149】硬體實現的模組可以向其他硬體實現的模組提供資訊並從其接收資訊。因此，所描述的硬體實現的模組可以被認為是通訊地耦接。在同時存在多個這樣的硬體實現的模組的情況下，可以透過信號傳輸(例如，透過連接硬體實現的模組的適當電路和匯流排)來實現通訊。在多個硬體實現的模組在不同時間被組態或實例化的實施例中，這些硬體實現的模組之間的通訊可以例如透過在具有對其的存取的多個硬體實現的模組的記憶體結構中儲存和檢索資訊來實現。舉例而言，一個硬體實現的模組可以執行一項操作，並將該操作的輸出儲存在與其通訊地耦接的記憶體裝置中。接著，另一個硬體實現的模組可以在稍後時間存取該記憶體裝置以檢索和處理儲存的輸出。硬體實現的模組還可以啟動與輸入或輸出裝置的通訊，並且可以對資源(例如，資訊集合)進行操作。

【0150】本文描述的範例方法的各種操作可以至少部分地由一或多個處理器執行，這些處理器被臨時組態(例如，藉由軟體)或永久組態為執行相關操作。無論是臨時組態的還是永久組態的，這樣的處理器都可以構成處理器實現的模組，這些模組運行而執行一或多個操作或函數。在一些範例實施例中，這裡提到的模組可以包括處理器實現的模組。

【0151】相似地，本文描述的方法可以至少部分地由處理器實現。舉例而言，一種方法的至少一些操作可以由一或多個處理器或處理器實現的模組來執行。某些操作的性能可以分散在一或多個處理器之中，不僅駐留在單一機器內，且部署在多個機器之中。在一些範例實施例中，一或多個處理器可以位於單一位置(例如，在家庭環境、辦公環境或伺服器場內)，而在其他實施例中，處理器可以分散在多個位置。

【0152】一或多個處理器還可操作以支持「雲端計算」環境中的相關操作的性能或作為「軟體即服務」(SaaS)。舉例而言，至少一些操作可以由一組電腦(作為包含處理器的機器的範例)執行，這些操作可藉由網路(例如，網際網路)和藉由一或多個適當的介面(例如，API)存取)。

電子設備和系統

【0153】範例實施例可以在數位電子電路中，或在電

腦硬體、韌體或軟體中，或在其組合中實現。範例實施例可以使用電腦程式產品來實現，例如，有形地體現在資訊載體中的電腦程式，例如，在機器可讀媒體中用於由資料處理設備執行或控制資料處理設備的操作，例如可程式化的處理器、電腦或多台電腦之資料處理設備。

【0154】電腦程式可以以任何形式的程式語言編寫，包含編譯或解譯語言，並且可以以任何形式部署，包含作為獨立程式或模組、副常式或適用於計算環境的其他單元。可以部署電腦程式以在一台電腦上或在一個站點或分散在多個站點並藉由通訊網路互連的多台電腦上執行。

【0155】在範例實施例中，操作可以由一或多個可程式設計處理器執行，該處理器執行電腦程式以藉由對輸入資料進行操作並產生輸出來執行函數。方法操作也可以由專用邏輯電路執行，並且示例實施例的設備可以實現為專用邏輯電路，例如FPGA或ASIC。

【0156】計算系統可以包含客戶端和伺服器。客戶端和伺服器通常彼此遠離並且通常透過通訊網路進行互動。客戶端和伺服器的關係是藉由在各自的電腦上運行並且彼此具有客戶端-伺服器關係的電腦程式而產生的。在部署可程式設計電腦系統的實施例中，應當理解硬體和軟體架構都是可考慮的。具體而言，應當理解，選擇在永久組態的硬體(例如，ASIC)中、在臨時組態的硬體(例如，軟體和可程式處理器的組合)中還是在結合永久和臨時組態的硬體中實現特定功能可能是一種設計選擇。以下列出在各

種範例實施例中可以部署的硬體(例如，機器)和軟體架構。

範例機器架構和機器可讀媒體

【0157】圖11是電腦系統1100的範例形式的機器的方塊圖，在該電腦系統中可以執行指令1124以使機器執行本文討論的任何一或多個方法。在替代實施例中，機器作為獨立裝置操作或可以連接(例如，網路連接)到其他機器。在網路連接部署中，機器可以在伺服器-客戶端網路環境中以伺服器或客戶端機器的能力操作，或作為同級間(或分散式)網路環境中的對等機器操作。機器可以是個人電腦(PC)、平板電腦、機上盒(STB)、個人數位助理(PDA)、行動電話、網路設備、網路路由器、開關或橋接器，或任何能夠執行指定該機器要採取的動作的指令(依序或其他方式)的機器。此外，雖然說明單一機器，但用詞「機器」還應被視為包含單獨或聯合執行一組(或多組)指令以執行任何一或多個本文所述的方法的任何機器的集合。

【0158】範例電腦系統1100包含處理器1102(例如，中央處理單元(CPU)、圖形處理單元(GPU)或兩者)、主記憶體1104和靜態記憶體1106，其藉由匯流排1108彼此通訊。電腦系統1100還可以包含視訊顯示單元1110(例如，液晶顯示器(LCD)或陰極射線管(CRT))。電腦系統1100還包含文數輸入裝置1112(例如，鍵盤或觸敏顯示螢幕)、使用者介面(UI)導航(或游標控制)裝置1114(例如，滑鼠)、

儲存單元1116、信號產生裝置1118(例如，揚聲器)及網路介面裝置1120。

機器可讀媒體

【0159】儲存單元1116包含機器可讀媒體1122，在其上儲存一或多組資料結構和指令1124(例如，軟體)，這些資料結構和指令1124(例如，軟體)由本文描述的任何一或多種方法或函數體現或使用。指令1124還可以在電腦系統1100執行其期間完全或至少部分地駐留在主記憶體1104內及/或處理器1102內，主記憶體1104和處理器1102也構成機器可讀媒體1122。

【0160】雖然在範例實施例中將機器可讀媒體1122顯示為單一媒體，用詞「機器可讀媒體」可以包含儲存一或多組指令1124或資料結構的單一媒體或多個媒體(例如，集中式或分散式資料庫及/或關聯的快取和伺服器)。用詞「機器可讀媒體」還應理解為包含能夠儲存、進行編碼或攜帶指令1124以供機器執行並且使機器執行本揭露的任何一或多種方法，或是能夠儲存、進行編碼或攜帶由此類指令1124利用或與此類指令1124相關聯的資料結構的任何有形媒體。因此，用詞「機器可讀媒體」應被視為包含但不限於固態記憶體，以及光學和磁性媒體。機器可讀媒體1122的具體範例包含非揮發性記憶體，包含範例半導體記憶體裝置，例如，可抹除可程式設計唯讀記憶體(EPROM)、電可抹除可程式設計唯讀記憶體(EEPROM)及

快閃記憶體裝置；磁碟，例如內部硬碟和可移磁碟；磁光碟；以及唯讀光碟(CD-ROM)和數位多函數光碟唯讀記憶體(DVD-ROM)碟。機器可讀媒體不是傳輸媒體。

傳輸媒體

【0161】指令1124還可以使用傳輸媒體在通訊網路1126上傳輸或接收。指令1124可以使用網路介面裝置1120和許多眾所周知的傳輸協定(例如，超文件傳送協定(HTTP))中的任何一種來傳輸。通訊網路的範例包含區域網路(LAN)、廣域網路(WAN)、網際網路、行動電話網路、簡易老式電話(POTS)網路和無線資料網路(例如WiFi和WiMax網路)。用詞「傳輸媒體」應被理解為包含能夠儲存、進行編碼或攜帶指令1124以供機器執行的任何無形媒體，並且包含數位或類比通訊信號或其他無形媒體以促進此類軟體的通訊。

【0162】儘管本文描述具體的範例實施例，但顯然可以對這些實施例進行各種修改和改變而不背離本揭露的更廣泛的精神和範圍。因此，說明書和圖式應被認為是說明而不是限制性的。形成其一部分的圖式藉由說明而非限制的方式示出可以實踐本標的的特定實施例。這些說明的實施例以充分的細節描述，使得本發明所屬技術領域中具有通常知識者能夠實踐本文所揭露的教導。可以利用其他實施例並從中導出其他實施例，從而可以在不背離本揭露的範圍的情況下進行結構和邏輯替換和改變。因此，此詳細

描述不應被理解為限制性意義，並且各種實施例的範圍僅由所附申請專利範圍以及這些申請專利範圍所享有的全部等同物範圍限定。

【0163】本發明標的的這些實施例可以在本文中單獨及/或共同地由用詞「發明」來引用，僅是為了方便，並且如果不止一個，則無意將本案的範圍自願限制到任何所揭露的單一發明或發明概念。因此，儘管這裡已經說明和描述具體實施例，但是應當理解，任何被計算為實現相同目的的配置都可以代替所示的具體實施例。本揭露旨在涵蓋各種實施例的任何和所有修改或變化。上述實施例的組合，以及本文未具體描述的其他實施例，對於本發明所屬技術領域中具有通常知識者在閱讀以上描述後將是顯而易見的。

【0164】本文討論的標的的一些部分可以根據演算法或對儲存為機器記憶體(例如，電腦記憶體)內的位元或二進制數位信號的資料的操作的符號表示來呈現。這樣的演算法或符號表示是資料處理領域中具有通常知識者用來將他們的工作的實質傳達給本領域的其他具有通常知識者的技術的範例。如本文所用，「演算法」是自洽的操作序列或導致期望結果的相似處理。在這種情況下，演算法和操作涉及實體量的實體調處。通常但並非必要地，這些量可以採取能夠被機器儲存、存取、傳輸、組合、比較或以其他方式調處的電、磁或光信號的形式。有時，主要出於常用的原因，使用諸如「資料」、「內容」、「位元」、

「值」、「元件」、「符號」、「字符」、「用詞」、「數字」、「數值」等字詞來指示此類信號是很便利的。然而，這些字詞只是便利的標籤，要與適合的實體量相關聯。

【0165】除非另有明確說明，否則本文使用例如「處理」、「運算」、「計算」、「確定」、「呈現」、「顯示」等字詞的討論可以指機器(例如，電腦)的動作或過程，其在一或多個記憶體(例如，揮發性記憶體、非揮發性記憶體或其任何合適的組合)、暫存器或接收、儲存、傳輸或顯示資訊的其他機器組件內操縱或轉換表示為實體(例如，電的、磁的或光學的)量的資料。此外，除非另有明確說明，本文使用的用詞「一」和「一個」在專利文獻中很常包含一或大於一個實例。最後，如本文所用，連接詞「或」指的是非排他性的「或」，除非另有明確說明。

【符號說明】

【0166】

100:網路環境

110:函數即服務伺服器

110A:函數即服務伺服器

110B:函數即服務伺服器

120:客戶端裝置

120A:客戶端裝置

120B:客戶端裝置

130:網路

210:通訊模組

220:不信賴組件

230:信賴組件

240:信賴網域模組

250:引用指定位址空間

260:共享記憶體

270:專用記憶體

300:方塊圖

310:應用程式

320:應用程式

330:作業系統

400:方塊圖

410:應用程式

420:指定位址空間

430:作業系統

500:資料庫簡圖

510:指定位址空間表格

520:格式

530A:列

530B:列

530C:列

530D:列

700:方法

710:操作

720:操作

730:操作

740:操作

800:方法

810:操作

820:操作

830:操作

840:操作

900:方法

910:操作

920:操作

930:操作

940:操作

1000:方塊圖

1002:軟體架構

1004:硬體層

1006:處理單元

1008:指令

1010:儲存模組

1012:其他硬體

1014:作業系統

1016:程式館

1018:框架/中介軟體

1020:應用程式

1024:應用程式設計介面呼叫

1026:訊息

1028:核心

1030:服務

1032:驅動程式

1034:系統程式館

1036:API程式館

1038:其他程式館

1040:內建應用程式

1042:第三方應用程式

1044:表示層

1046:虛擬機器監視器

1048:虛擬機器

1050:作業系統

1052:程式館

1054:框架/中介軟體

1056:應用程式

1058:表示層

1100:電腦系統

1102:處理器

1104:主記憶體

1106:靜態記憶體

1108:匯流排

1110:視訊顯示單元

1112:文數輸入裝置

1114:使用者介面導航裝置

1116:儲存單元

1118:信號產生裝置

1120:網路介面裝置

1122:機器可讀媒體

1124:指令

1126:通訊網路

【發明申請專利範圍】

【請求項1】一種處理系統，包括：

記憶體電路；以及

處理電路被配置以執行以下步驟：

分配該處理電路的資源以建立複數個可信執行環境(TEE)；

藉由向該記憶體電路中的相應的TEE分配隔離的記憶體空間並使該相應的TEE能夠在該處理電路上執行工作負載來初始化該複數個TEE中的每個該相應的TEE，其中，該複數個TEE中的每個該相應的TEE被初始化以支持複數個不同類型的工作負載的獨立排程和執行；

在該複數個TEE中的每個該相應的TEE初始化後，接收執行工作負載的請求；

使已初始化的該複數個TEE中的一個TEE回應該請求執行該工作負載；

為執行該工作負載的TEE分配加密金鑰；以及

使用該加密金鑰加密要執行該工作負載的該TEE的該記憶體空間，

其中，該複數個TEE被分配在複數個使用者之間，並且其中要執行該工作負載的TEE被隔離到該複數個使用者中的特定使用者，並且

其中，在該工作負載的執行期間，該複數個TEE中的其他TEE可用於為該複數個使用者中的其他使用者執行其他工作負載。

【請求項2】如請求項1的處理系統，其中該處理電路包含至少一圖形處理單元(GPU)，並且其中該複數個TEE中的每個該相應的TEE被配置為使用該至少一GPU的部分來執行該工作負載。

【請求項3】如請求項2的處理系統，其中該至少一GPU是單一GPU，並且其中該複數個TEE中的每個該相應的TEE在該單一GPU內受到保護和隔離。

【請求項4】一種建立可信執行環境(TEE)的方法，包括：

分配處理系統的處理電路的資源以建立複數個TEE；

初始化該複數個TEE中的每個相應的TEE，藉由(i)為該處理系統的記憶體電路中的該相應的TEE分配一隔離的記憶體空間，以及(ii)使該相應的TEE能夠在該處理電路上執行工作負載，其中，該複數個TEE中的每個該相應的TEE被初始化以支持複數個不同類型的工作負載的獨立排程和執行；

在該複數個TEE中的每個該相應的TEE被初始化之後，接收執行工作負載的請求；

使已初始化的該複數個TEE中的一個TEE回應該請求執行該工作負載；

分配加密金鑰給執行該工作負載的TEE；以及

使用該加密金鑰加密要執行該工作負載的該TEE的該記憶體空間，

其中該複數個TEE被分配在複數個使用者之間，並且

其中要執行該工作負載的TEE被隔離到該複數個使用者中的特定使用者，並且

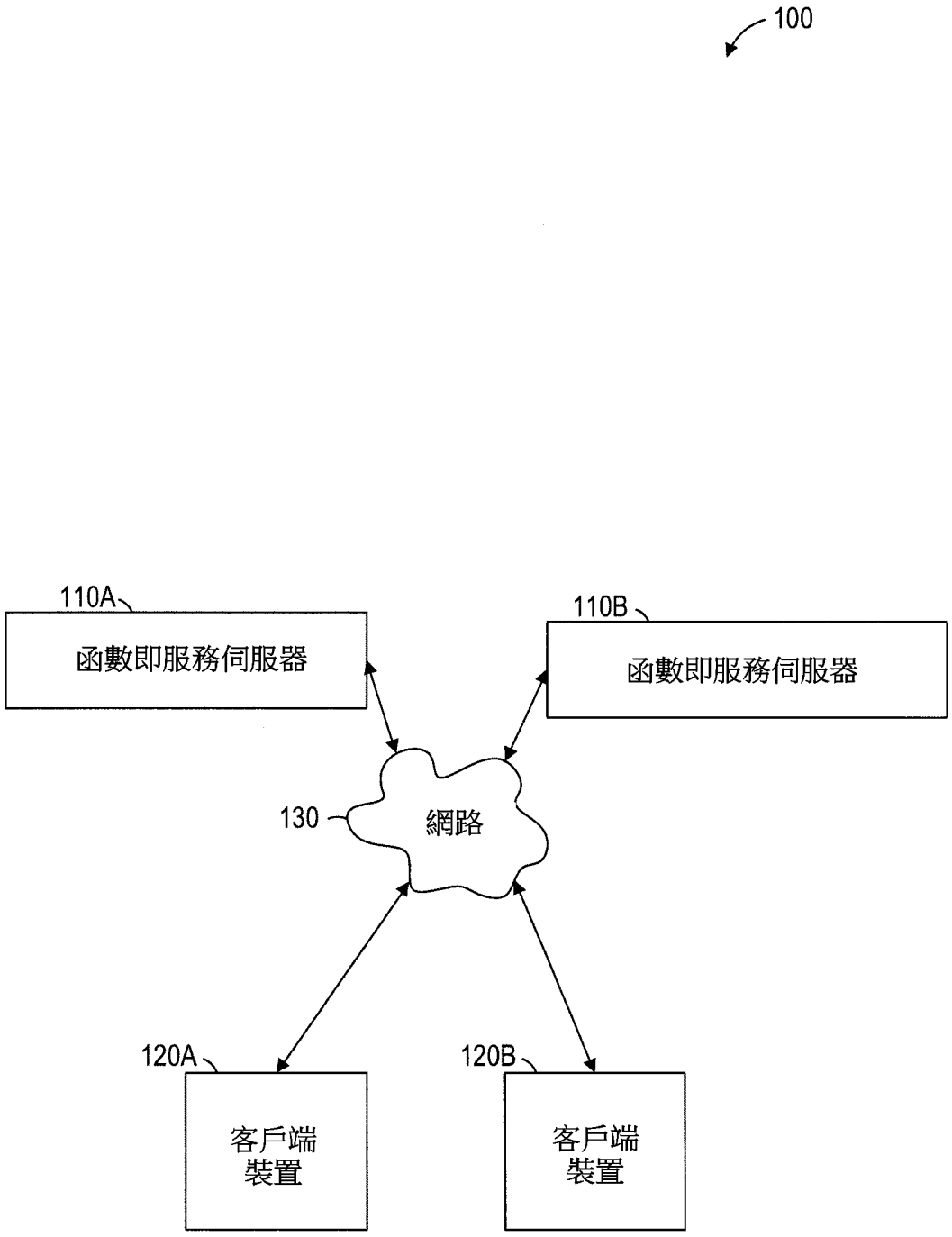
其中，在該工作負載的執行期間，該複數個TEE中的其他TEE可用於為該複數個使用者中的其他使用者執行其他工作負載。

【請求項5】如請求項4的方法，其中該處理電路包含至少一圖形處理單元(GPU)，並且其中該複數個TEE中的每個該相應的TEE被配置為使用該至少一GPU的部分來執行該工作負載。

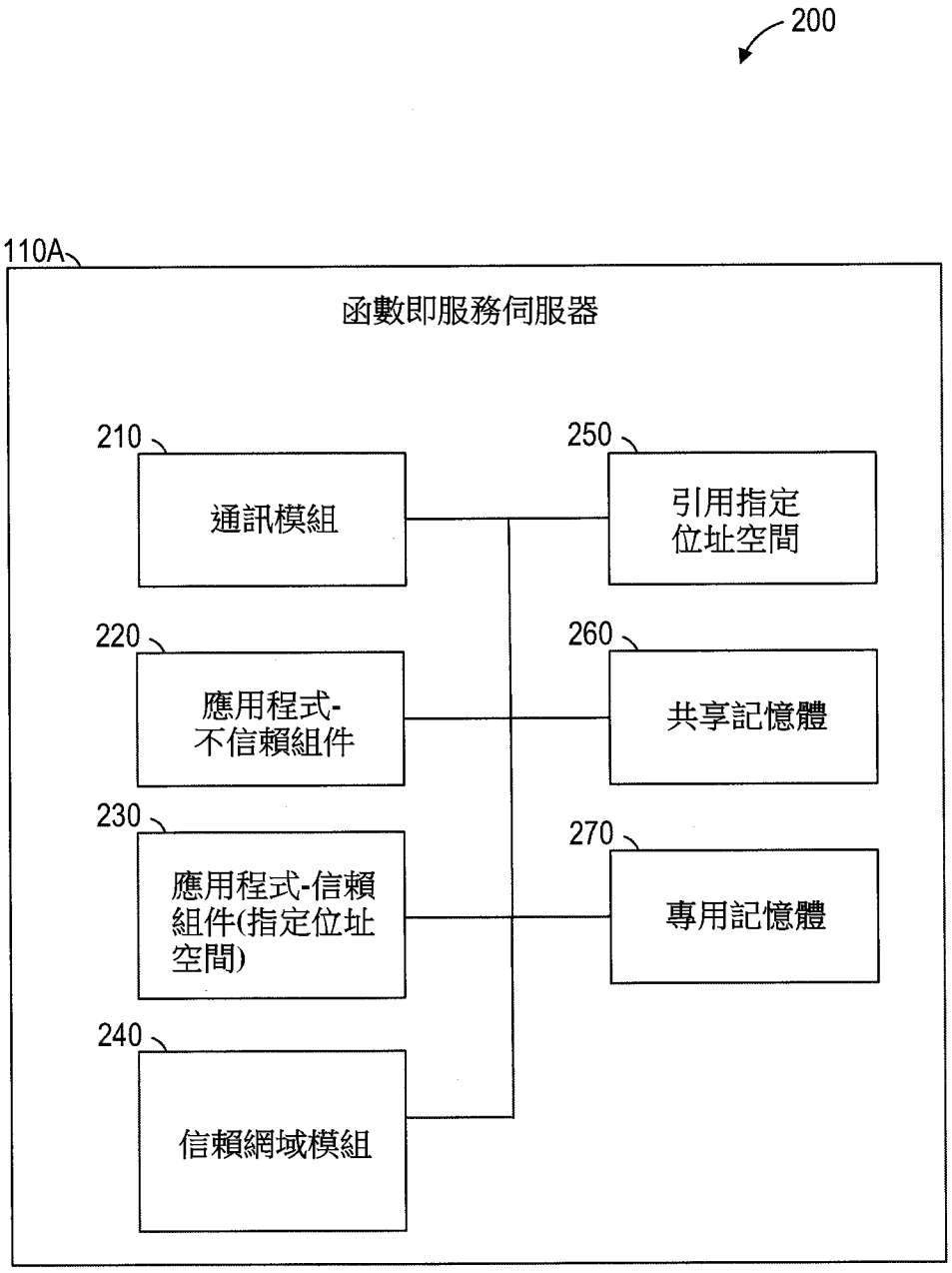
【請求項6】如請求項5的方法，其中該至少一GPU是單一GPU，並且其中該複數個TEE中的每個該相應的TEE在該單一GPU內受到保護和隔離。

【請求項7】一種非暫態電腦可讀媒體，能夠儲存指令，該指令被執行時使得處理電路執行如請求項4至6中任一項所述的方法。

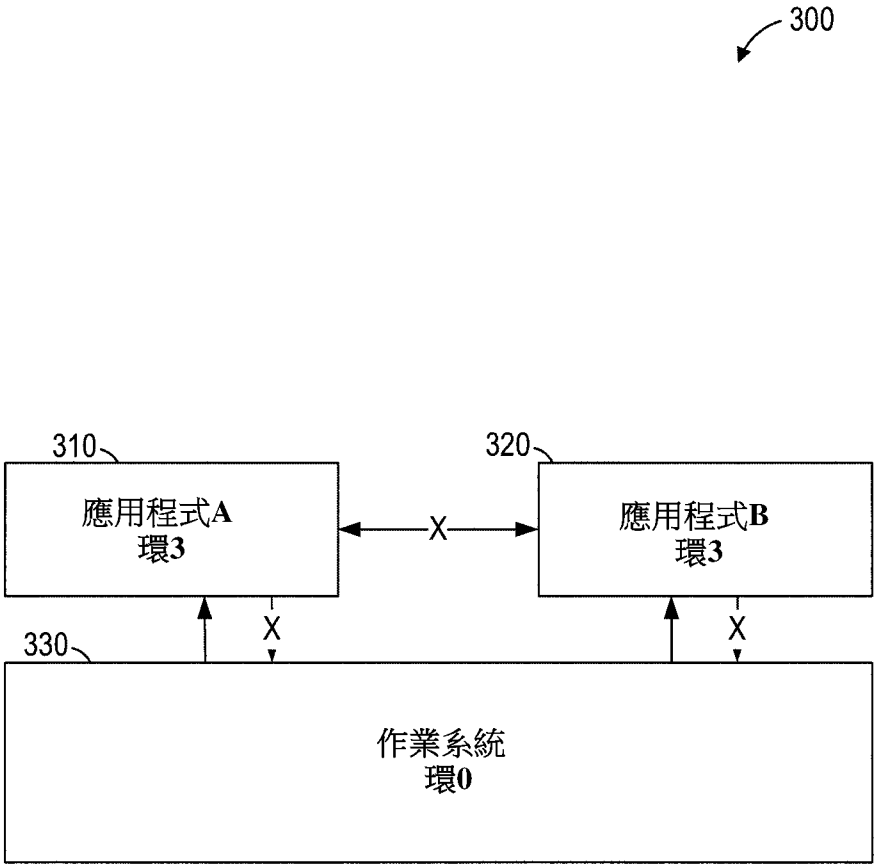
【發明圖式】


100
110A
函數即服務伺服器
110B
函數即服務伺服器
130
網路
120A
客戶端
裝置
120B
客戶端
裝置

【圖 1】

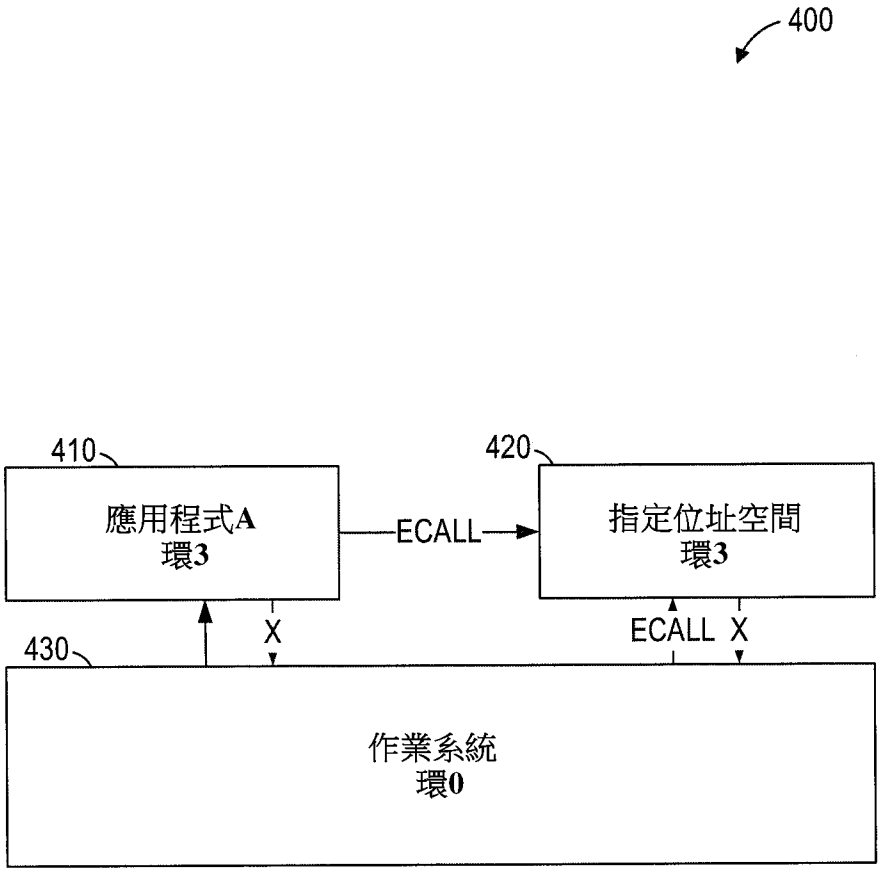

200
110A
函數即服務伺服器
210
通訊模組
250
引用指定
位址空間
220
應用程式-
不信賴組件
260
共享記憶體
230
應用程式-信賴
組件(指定位址
空間)
270
專用記憶體
240
信賴網域模組

【圖 2】

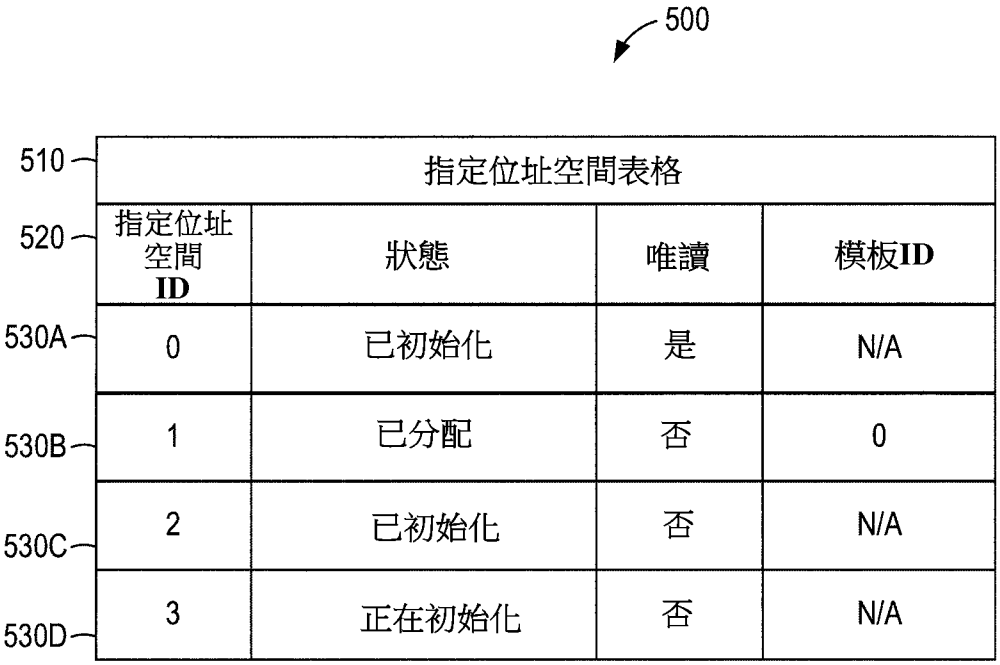


先前技術

【圖 3】

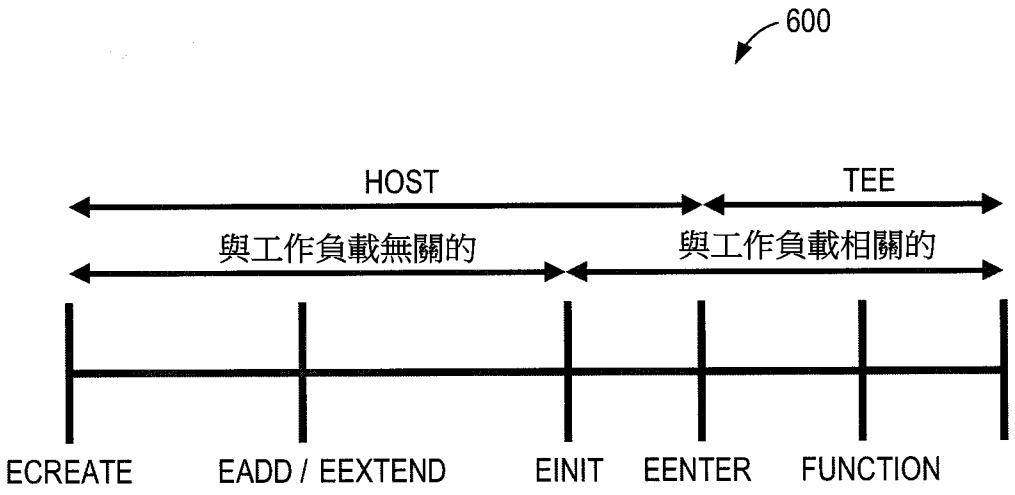


【圖 4】

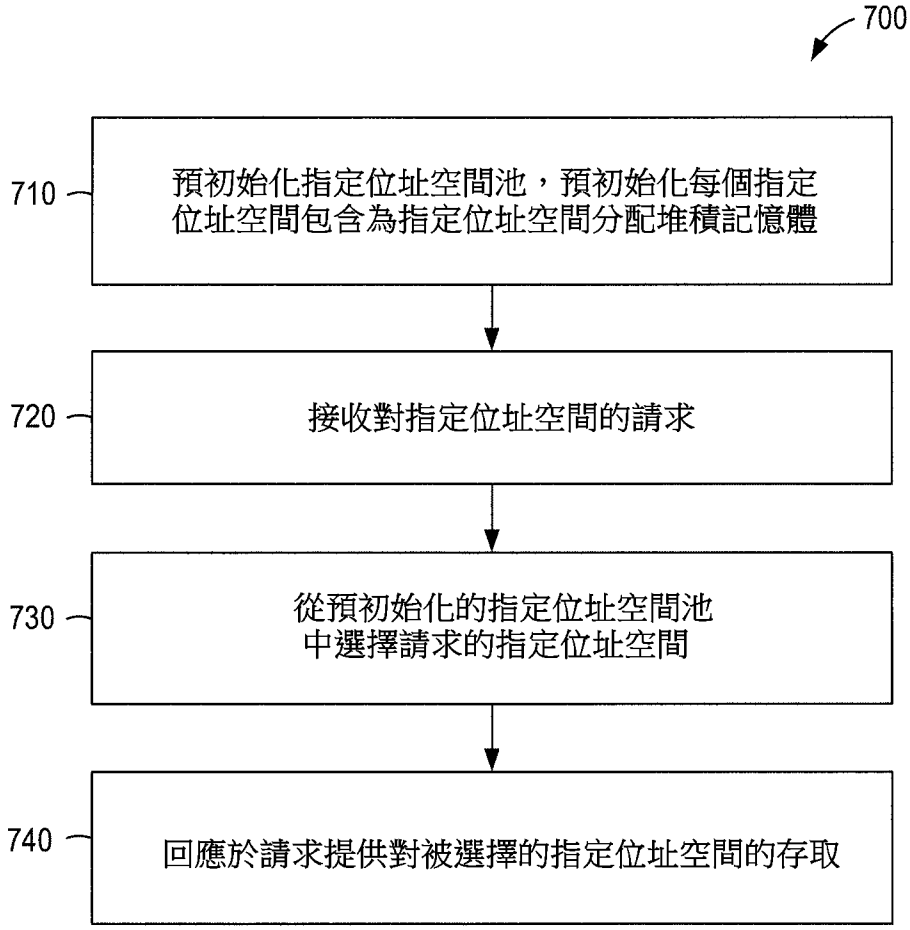


指定位址空間表格			
指定位址空間 ID	狀態	唯讀	模板ID
0	已初始化	是	N/A
1	已分配	否	0
2	已初始化	否	N/A
3	正在初始化	否	N/A

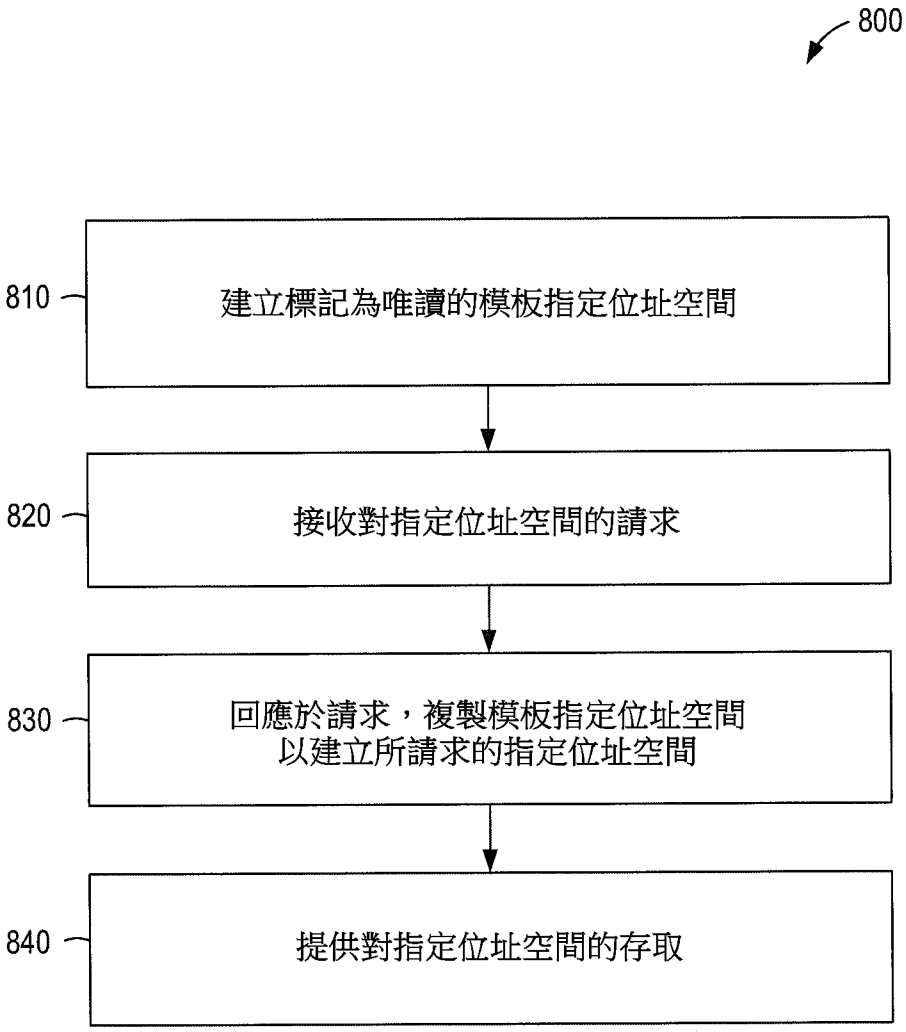
【圖 5】


600
HOST
TEE
與工作負載無關的
與工作負載相關的
ECREATE
EADD / EEXTEND
EINIT
EENTER
FUNCTION

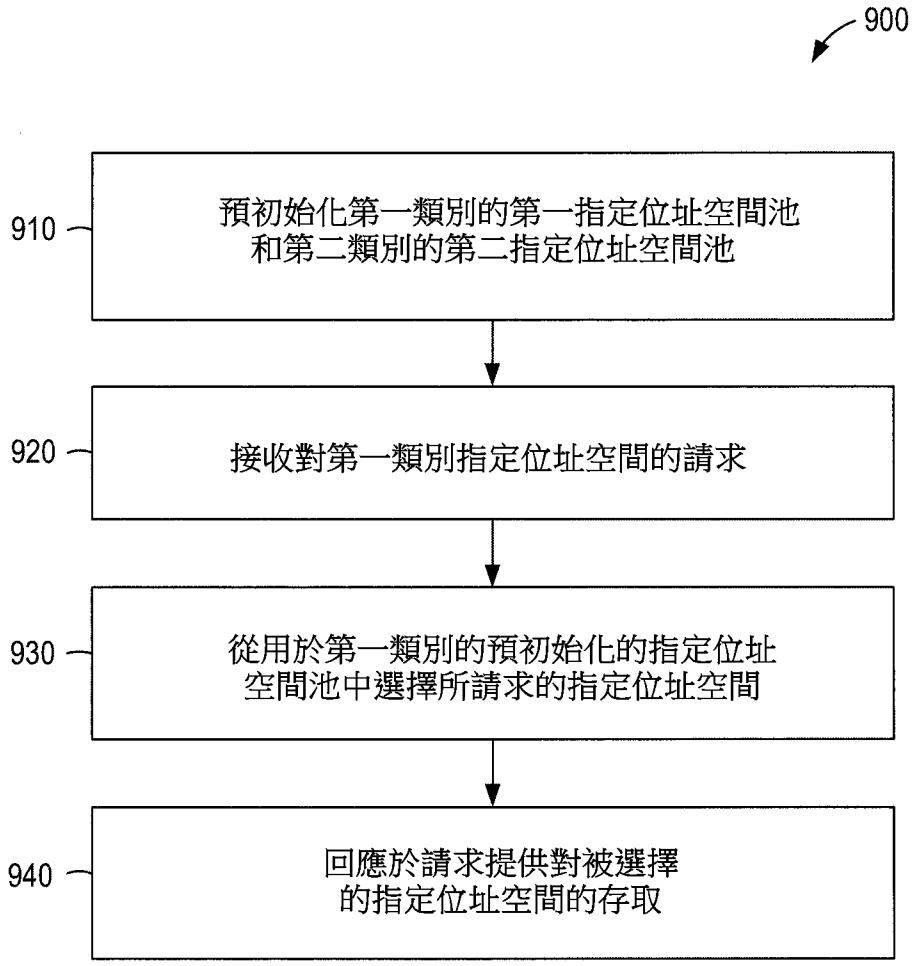
【圖 6】


700
710
預初始化指定位址空間池，預初始化每個指定位址空間包含為指定位址空間分配堆積記憶體
720
接收對指定位址空間的請求
730
從預初始化的指定位址空間池中選擇請求的指定位址空間
740
回應於請求提供對被選擇的指定位址空間的存取

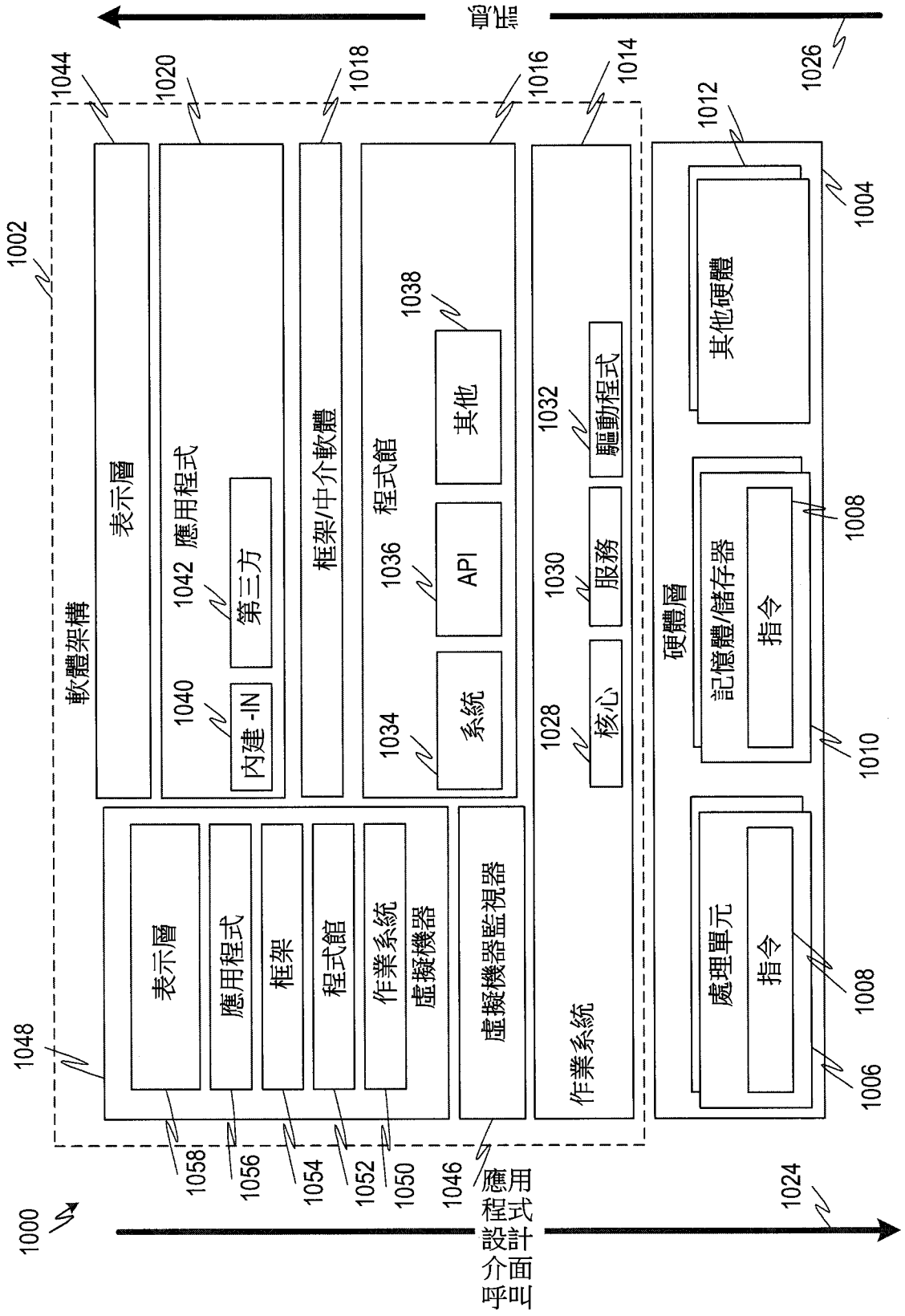
【圖 7】


800
810
建立標記為唯讀的模板指定位址空間
820
接收對指定位址空間的請求
830
回應於請求，複製模板指定位址空間
以建立所請求的指定位址空間
840
提供對指定位址空間的存取

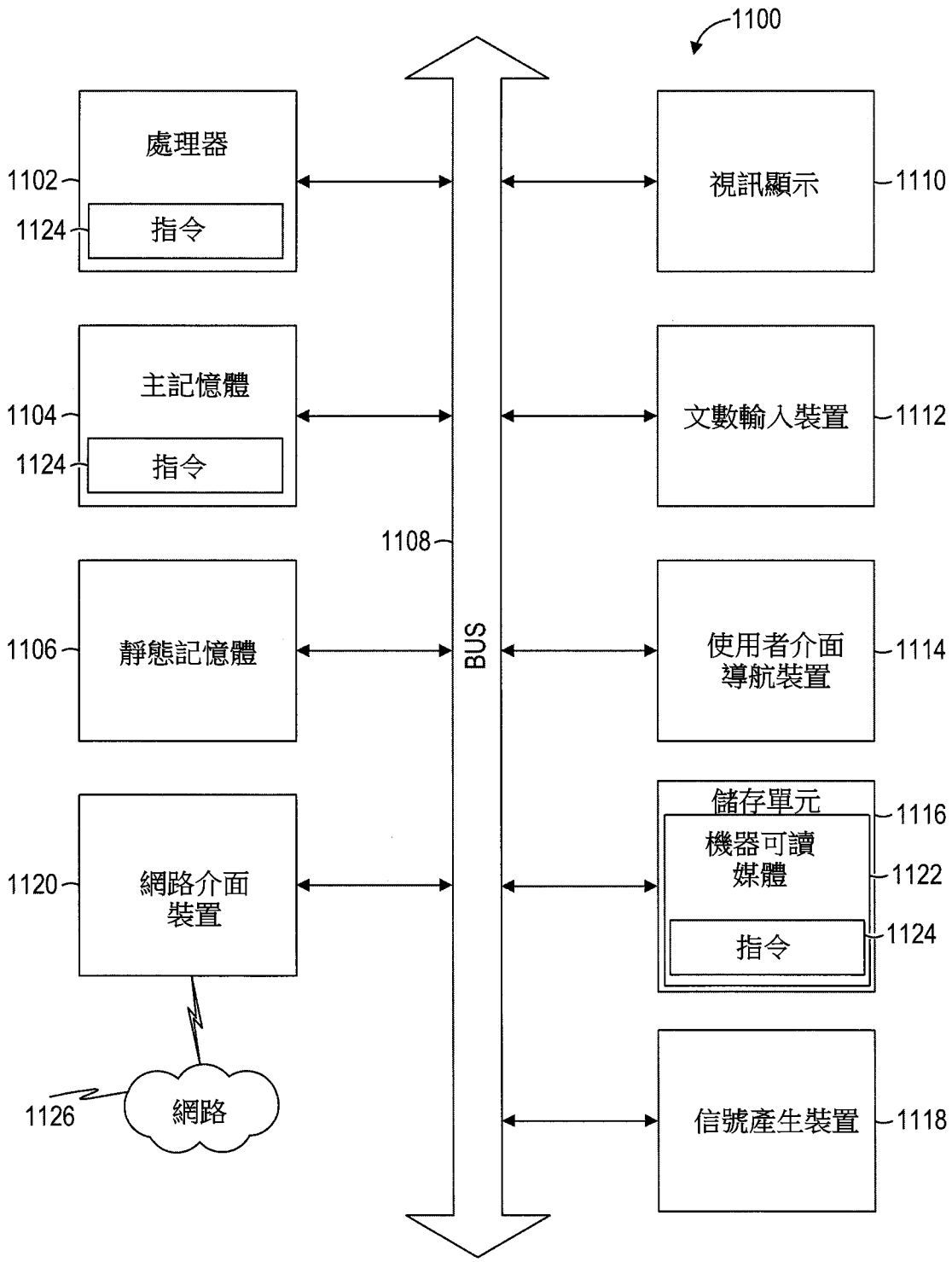
【圖 8】


900
910
預初始化第一類別的第一指定位址空間池
和第二類別的第二指定位址空間池
920
接收對第一類別指定位址空間的請求
930
從用於第一類別的預初始化的指定位址
空間池中選擇所請求的指定位址空間
940
回應於請求提供對被選擇
的指定位址空間的存取

【圖 9】


1000
1002
1004
1006
1008
1010
1012
1014
1016
1018
1020
1022
1024
1026
1028
1030
1032
1034
1036
1038
1040
1042
1044
1046
1048
1050
1052
1054
1056
1058
軟體架構
表示層
應用程式
內建 -IN
第三方
框架/中介軟體
程式館
系統
API
其他
作業系統
核心
服務
驅動程式
虛擬機器
虛擬機器監視器
表示層
應用程式
框架
程式館
作業系統
硬體層
處理單元
指令
記憶體/儲存器
指令
其他硬體
應用程式設計介面
匯流排

【圖 10】


1100
處理器
1102
指令
1124
主記憶體
1104
指令
1124
1108
BUS
靜態記憶體
1106
網路介面
裝置
1120
網路
1126
視訊顯示
1110
文數輸入裝置
1112
使用者介面
導航裝置
1114
儲存單元
1116
機器可讀
媒體
1122
指令
1124
信號產生裝置
1118

【圖 11】