I686744

(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 I686744 B**

(45)公告日： 中華民國 109 (2020) 年 03 月 01 日

(21)申請案號：106125587　(22)申請日： 中華民國 106 (2017) 年 07 月 28 日

(51)Int. Cl.：　*G06F9/44　(2018.01)*　*G06F12/02　(2006.01)*

(30)優先權：2016/07/29　美國　62/368,223

2017/03/21　美國　15/465,515

(71)申請人：美商高通公司 (美國) QUALCOMM INCORPORATED　(US)

美國

(72)發明人：德　薩柏瓦多庫馬 DE, SUBRATO KUMAR (US)；喬治　薩約桑德 GEORGE, SAJO SUNDER (IN)

(74)代理人：李世章

(56)參考文獻：

US	6681331B1	US	8566935B2
US	9178852B2	US	9235704B2
US	2002/0032804A1	US	2011/0082962A1
US	2012/0240230A1		

審查人員：朱明宗

申請專利範圍項數：22 項　圖式數：23　共 91 頁

(54)名稱

使用基於偏移的虛擬位址映射對目標應用功能的基於核心的偵測

(57)摘要

揭示用於偵測在計算設備上執行的應用軟體的高級功能的系統和方法。一種方法包括以下步驟：將用於應用軟體的應用特定虛擬位址映射表儲存在安全記憶體中。應用特定虛擬位址映射表包括在應用二進位碼中被映射到對應的目標應用功能的複數個虛擬位址偏移。回應於啟動應用軟體，產生用於將被執行的應用程序的實例的程序特定虛擬位址映射表。程序特定虛擬位址映射表使用應用特定虛擬位址映射表中的虛擬位址偏移來定義與目標應用功能相對應的實際虛擬位址。在應用代碼的執行期間，該方法基於程序特定虛擬位址映射表，來偵測與目標應用功能相對應的實際虛擬位址中的一或多個實際虛擬位址何時被執行。

Systems and methods are disclosed for detecting high-level functionality of an application executing on a computing device. One method comprises storing, in a secure memory, an application-specific virtual address mapping table for an application. The application-specific virtual address mapping table comprises a plurality of virtual address offsets in the application binary code mapped to corresponding target application functionalities. In response to launching the application, a process-specific virtual address mapping table is generated for an instance of an application process to be executed. The process-specific virtual address mapping table defines actual virtual addresses corresponding to the target application functionalities using the virtual address offsets in the application-specific virtual address mapping table. During execution of the application code, the method detects when one or more of the actual virtual addresses corresponding to the target application functionalities are executed based on the process-specific virtual address mapping table.

指定代表圖：

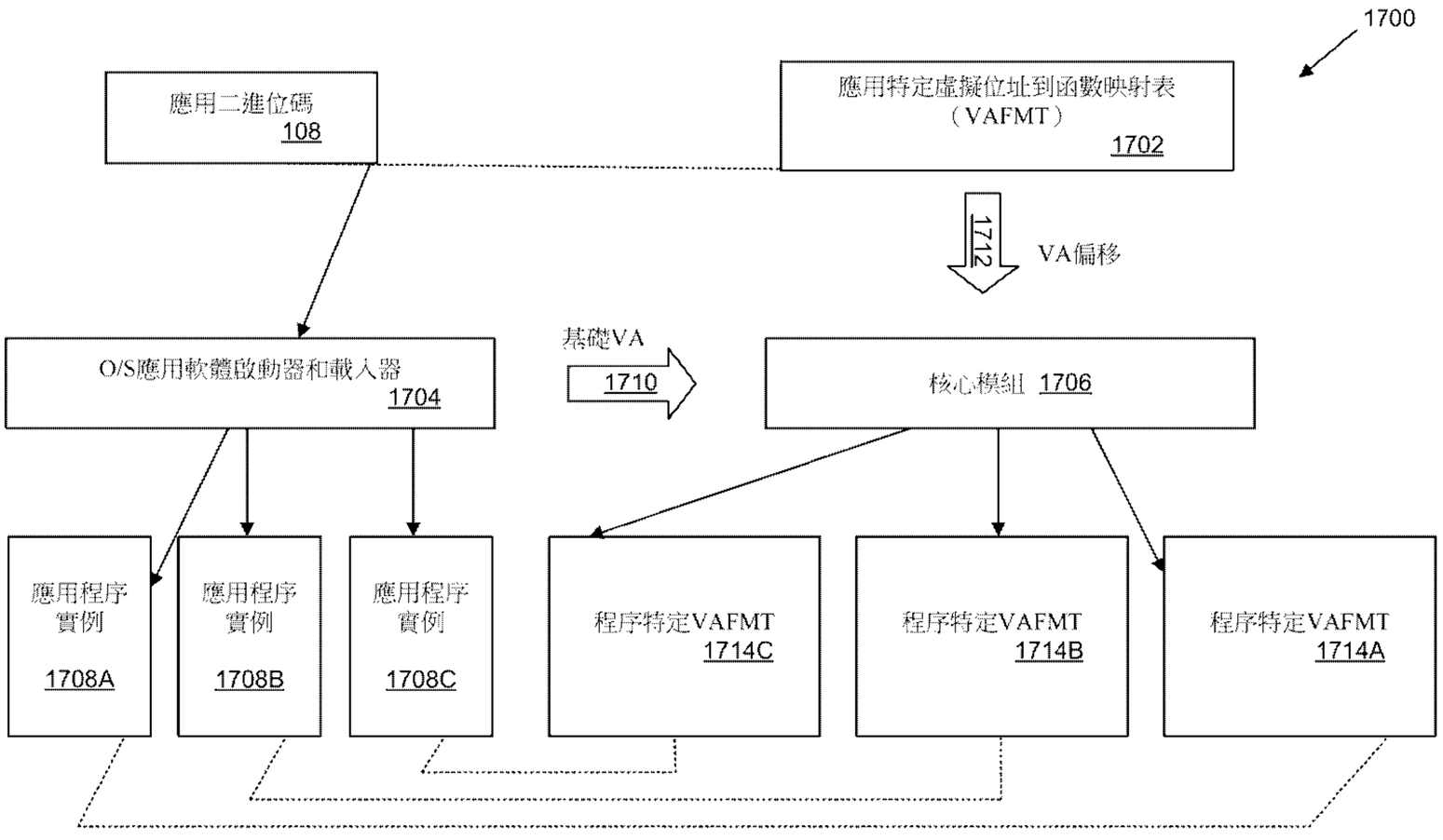


圖17

符號簡單說明：

108・・・應用二進位碼

1700・・・基於偏移的虛擬位址映射方案

1702・・・應用特定VAFMT

1704・・・O/S 應用軟體啟動器和載入器

1706・・・核心模組

1708A・・・應用程序實例

1708B・・・應用程序實例

1708C・・・應用程序實例

1710・・・基礎虛擬位址

1714・・・程序特定VAFMT

1714A・・・程序特定 VAFMT

1714B・・・程序特定 VAFMT

1714C・・・程序特定 VAFMT

專利案號：106125587

公告本

申請日：106年7月28日

I686744

IPC分類：*G06F 9/44* (2018.01)
G06F 12/02 (2006.01)

【發明摘要】

【中文發明名稱】使用基於偏移的虛擬位址映射對目標應用功能的基於核心的偵測

【英文發明名稱】KERNEL-BASED DETECTION OF TARGET APPLICATION FUNCTIONALITY USING OFFSET-BASED VIRTUAL ADDRESS MAPPING

【中文】

揭示用於偵測在計算設備上執行的應用軟體的高級功能的系統和方法。一種方法包括以下步驟：將用於應用軟體的應用特定虛擬位址映射表儲存在安全記憶體中。應用特定虛擬位址映射表包括在應用二進位碼中被映射到對應的目標應用功能的複數個虛擬位址偏移。回應於啟動應用軟體，產生用於將被執行的應用程序的實例的程序特定虛擬位址映射表。程序特定虛擬位址映射表使用應用特定虛擬位址映射表中的虛擬位址偏移來定義與目標應用功能相對應的實際虛擬位址。在應用代碼的執行期間，該方法基於程序特定虛擬位址映射表，來偵測與目標應用功能相對應的實際虛擬位址中的一或多個實際虛擬位址何時被執行。

【英文】

Systems and methods are disclosed for detecting high-level functionality of an application executing on a computing device. One method comprises storing, in a secure memory, an application-specific virtual address mapping table for an application. The application-specific virtual address mapping table comprises a plurality of virtual address offsets in the application binary code mapped to corresponding target application functionalities. In response to launching the

application, a process-specific virtual address mapping table is generated for an instance of an application process to be executed. The process-specific virtual address mapping table defines actual virtual addresses corresponding to the target application functionalities using the virtual address offsets in the application-specific virtual address mapping table. During execution of the application code, the method detects when one or more of the actual virtual addresses corresponding to the target application functionalities are executed based on the process-specific virtual address mapping table.

【指定代表圖】第（ 17 ）圖。

【代表圖之符號簡單說明】

108 應用二進位碼

1700 基於偏移的虛擬位址映射方案

1702 應用特定VAFMT

1704 O/S應用軟體啟動器和載入器

1706 核心模組

1708A 應用程序實例

1708B 應用程序實例

1708C 應用程序實例

1710 基礎虛擬位址

1714 程序特定VAFMT

1714A 程序特定VAFMT

1714B 程序特定VAFMT

1714C 程序特定VAFMT

申請案號：

【特徵化學式】

無

【發明說明書】

【中文發明名稱】使用基於偏移的虛擬位址映射對目標應用功能的基於核心的偵測

【英文發明名稱】KERNEL-BASED DETECTION OF TARGET APPLICATION FUNCTIONALITY USING OFFSET-BASED VIRTUAL ADDRESS MAPPING

【技術領域】

【0001】 本案依據專利法.119(e)主張於2016年7月29日提出申請的以及名稱為「Kernel-Based Detection of Target Application Functionality Using Virtual Address Mapping」的美國臨時專利申請案第62/368,223（高通案卷號163161P1）的優先權，故其以引用方式整體地併入本文。

【0002】 本案亦與以下申請案相關：於2016年8月23日提出申請的以及名稱為「Kernel-Based Detection of Target Application Functionality Using Virtual Address Mapping」美國專利申請案第15/245,037（案卷號163161U1），以及於2016年8月23日提出申請的以及名稱為「Updating Virtual Memory Addresses of Target Application Functionalities for an Updated Version of Application Binary Code」的美國專利申請案第15/245,041（案卷號163161U2）。

【0003】 本案係關於使用基於偏移的虛擬位址映射對目標應用功能的基於核心的偵測。

【先前技術】

【0004】 存在在硬體平臺上執行的各種高級應用軟體，該硬體平臺並不在系統或者平臺層處顯示出任何明顯的活動，因此並不提供偵測應用軟體執行的有用功能和行為資訊的時機。常見的實例是高級網頁瀏覽器應用軟體受危害。

【0005】 存在在硬體平臺上執行的各種高級應用軟體，該硬體平臺並不在系統或者平臺層處顯圖示任何明顯的活動，因此並不提供偵測應用軟體執行的有用功能和行為資訊的時機。常見的實例是高級網頁瀏覽器應用軟體在其在設備上執行期間受安全性漏洞（例如，跨站腳本）危害，安全性漏洞並不在系統和平臺級別處留下任何指示性蹤跡。經由探測系統庫、平臺、SOC硬體或者觀察設備級別活動無法決定此種活動正發生在高級應用軟體上。因此，為了對在設備上執行的各種協力廠商應用軟體具有更好的平臺級別控制，並且為了偵測該等正在執行的高級應用軟體的功能和行為活動中的一些，存在對開發如下機制的需求：該機制能夠實現將高級應用功能和行為表達並且傳送為平臺的HLOS或者核心能夠理解的形式。此舉將允許平臺對正在執行的應用軟體的行為具有更好的理解，並且允許平臺作出決策和採取動作，以處理正在執行的應用軟體的各種不同的情況。作為一個實例，可以使用該資訊來作出防止協力廠商網頁瀏覽器應用軟體上的網頁安全性漏洞的平臺級別決策。其他領域的示例性使用是：一旦

使用本案內容中的該等機制在HLOS或者核心層偵測到應用軟體的特定功能或者行為性質，平臺就作出如增加/減小各種SOC部件（DDR、匯流排、CPU、快取記憶體）的頻率或者引入高功率或者低功率模式的決策。通常，利用本案內容，平臺經由偵測和辨識出正被應用軟體執行的功能，來獲得對在設備上執行的各種協力廠商應用軟體進行各種控制的時機。此舉允許SOC和平臺供應商從平臺級別提供用於各種協力廠商應用軟體的更好的方案，該平臺原本對該等協力廠商應用軟體沒有控制。

【發明內容】

【0006】 揭示用於偵測在計算設備上執行的應用軟體的高級功能的系統、方法以及電腦程式。一種方法的一個實施例包括：將用於應用軟體的應用特定虛擬位址映射表儲存在計算設備上的安全記憶體中。該應用特定虛擬位址映射表包括該應用二進位碼中被映射到對應的目標應用功能的複數個虛擬位址偏移。回應於啟動該應用軟體，該方法產生用於將被執行的應用程序的實例的程序特定虛擬位址映射表。該程序特定虛擬位址映射表使用該應用特定虛擬位址映射表中的該等虛擬位址偏移來定義與該等目標應用功能相對應的實際虛擬位址。在用於該應用程序的該實例的該應用二進位碼的執行期間，該方法基於該程序特定虛擬位址映射表，來偵測與該等目標應用功能相對應的該等實際虛擬位址中的一或多個實際虛擬位址何時被執行。

【0007】 另一實施例是一種系統，其包括被配置為執行應用二進位碼的處理設備和高級作業系統（HLOS）。該HLOS包括應用特定虛擬位址映射表，其包括在該應用二進位碼中被映射到對應的目標應用功能的複數個虛擬位址偏移。該HLOS亦包括核心模組，其被配置為：回應於啟動該應用軟體，產生用於將被執行的應用程序的實例的程序特定虛擬位址映射表。該程序特定虛擬位址映射表使用該應用特定虛擬位址映射表中的該等虛擬位址偏移來定義與該等目標應用功能相對應的實際虛擬位址。該HLOS被配置為：在用於該應用程序的該實例的該應用二進位碼的執行期間，基於該程序特定虛擬位址映射表，來際虛擬位址中的一或多個實際虛擬位址何時被執行。

【圖式簡單說明】

【0008】 在各圖中，除非另外指出，否則類似的元件符號貫穿各個視圖代表類似的部分。對於具有諸如「102A」或者「102B」之類的字母字元名稱的元件符號而言，字母字元名稱可以對在同一圖中的兩個類似的部分或者元素進行區分。當意欲元件符號包含在所有圖中具有相同的元件符號的所有部分時，可以省略用於元件符號的字母字元名稱。

【0009】 圖1是用於使用安全記憶體中的虛擬位址映射來偵測目標應用功能的系統的實施例的方塊圖。

【0010】 圖2圖示目標應用功能到對應的應用二進位碼的示例性映射。

【0011】 圖3圖示虛擬位址到函數映射表（VAFMT）的示例性實施例。

【0012】 圖4是圖示用於偵測圖1的系統中的惡意程式碼活動的方法的實施例的流程圖。

【0013】 圖5圖示用於動態地辨識虛擬機器代碼空間的邊界的VAFMT的另一實施例。

【0014】 圖6圖示與VAFMT相結合地使用的辨識符到虛擬映射表（IVAMT）的實施例。

【0015】 圖7圖示與垃圾回收程序相結合地使用的VM代碼空間的部分。

【0016】 圖8圖示針對圖1的虛擬機器中的垃圾回收功能的示例性興趣點以及用於VAFMT中的功能興趣點的虛擬位址，該等虛擬位址用於在包含虛擬機器的應用二進位檔案的執行期間偵測垃圾回收活動的執行。

【0017】 圖9圖示用於虛擬機器堆的外部/內部邊界的虛擬位址的示例性映射。

【0018】 圖10是圖示用於在虛擬機器實施例中偵測圖1的系統中的惡意程式碼活動的方法的實施例的流程圖。

【0019】 圖11圖示包括用於特定緩衝分配器函數的虛擬位址的VAFMT的實施例，該等特定緩衝分配器函數用於決定被動態分配的緩衝器的虛擬位址，該等被動態分配的緩衝器包含特定資料結構類型的物件以及在該緩衝器中分配的物件的成員/欄位的值。

【0020】 圖12是圖示用於回應於接收到應用二進位碼的經更新的版本而自動地更新VAFMT的系統的實施例的組合方塊圖/流程圖。

【0021】 圖13圖示圖12的具有經更新的虛擬位址和中繼資料的VAFMT。

【0022】 圖14圖示圖12的VAFMT中的功能興趣點與偽二進位碼範本的示例性匹配。

【0023】 圖15圖示圖14的偽二進位碼範本與應用二進位碼的經更新的版本中的經匹配的區域的示例性匹配。

【0024】 圖16是圖示用於回應於接收到應用二進位碼的經更新的版本而更新VAFMT的方法的實施例的流程圖。

【0025】 圖17是用於使用基於偏移的虛擬位址映射來偵測目標應用功能的系統的實施例的方塊圖/流程圖。

【0026】 圖18圖示圖17中的應用特定VAFMT的示例性實施例。

【0027】 圖19圖示圖17中的程序特定VAFMT中的一個VAFMT的示例性實施例。

【0028】 圖20圖示應用特定URL緩衝器VAFMT的另一實施例。

【0029】 圖21圖示用於在圖20的應用特定URL緩衝器VAFMT中辨識的第一應用軟體的程序特定VAFMT的實施例。

【0030】 圖22圖示用於在圖20的應用特定URL緩衝器VAFMT中辨識的第二應用軟體的程序特定VAFMT的實施例。

【0031】 圖23是圖示用於使用基於偏移的虛擬位址映射來偵測目標應用功能的方法的實施例的流程圖。

【實施方式】

【0032】 「示例性」一詞在本文中用於意指「用作示例、實例或說明」。在本文中被描述為「示例性的」任何態樣未必被解釋為比其他態樣更佳或者有優勢。

【0033】 在該描述中，術語「應用軟體」亦可以包括具有可執行內容的檔案，例如：目標代碼、腳本、位元組代碼、標記語言檔案和補丁。另外，本文中所提及的「應用軟體」亦可以包括本質上不可執行的檔案，例如，可能需要開啟的文件或者需要存取的其他資料檔案。

【0034】 術語「內容」亦可以包括具有可執行內容的檔案，例如：目標代碼、腳本、位元組代碼、標記語言檔案和補丁。另外，本文中所提及的「內容」亦可以包括本質上不可執行的檔案，例如，可能需要開啟的文件或者需要存取的其他資料檔案。

【0035】 如該描述中使用的，術語「部件」、「資料庫」、「模組」、「系統」等意欲代表電腦相關實體，任一硬體、韌體、硬體和軟體的組合、軟體，或者執行中的軟體。例如，部件可以是但不限於在處理器上執行的程序、處理器、物件、可執行檔案、執行的執行緒、程式及/或電腦。

經由說明的方式，在計算設備上執行的應用軟體和計算設備皆可以是部件。一或多個部件可以位於程序及/或執行的執行緒內，並且部件可以被當地語系化在一個電腦上及/或分佈在兩個或更多個電腦之間。另外，該等部件可以從具有儲存在其上的各種資料結構的各個電腦可讀取媒體執行。部件可以經由本端及/或遠端程序的方式進行通訊，例如根據具有一或多個資料封包的信號（例如，來自一個部件的資料，該部件經由信號的方式與本端系統、分散式系統中及/或跨越諸如網際網路之類的具有其他系統的網路的另一部件互動）。

【0036】 圖1圖示用於從核心或者作業系統（O/S）層偵測應用二進位檔案的期望或者目標高級功能的系統100的實施例。如圖1的實施例中所示，系統100包括處理設備（例如，中央處理單元（CPU）102）、記憶體104和高級作業系統（HLOS）106。記憶體104儲存可以由CPU 102執行的一或多個應用軟體。記憶體104可以儲存與參考應用原始程式碼110相對應的應用二進位碼108，參考應用原始程式碼110與安裝在計算設備上的應用軟體相關聯。在該點上，系統100可以在任何期望的計算設備或者系統中實現，例如，包括個人電腦、膝上型電腦、工作站、伺服器，或者可攜式計算設備（PCD）（例如，蜂巢式電話、智慧型電話、可攜式數位助理（PDA）、可攜式遊戲控制台、導航設備、平板電腦、

可穿戴設備（例如，智慧手錶），或者其他電池供電的可攜式設備）。

【0037】 在一個實施例中，核心或者O/S層包括高級作業系統（HLOS）106。如圖1中所示，HLOS 106包括註冊應用軟體112的列表、安全記憶體（例如，可信區114）以及用於每個註冊應用軟體的應用二進位碼108的專門配置的虛擬位址映射表。註冊應用軟體112的列表辨識在系統100上安裝的、已經向HLOS 106註冊的以用於安全控制及/或支援的應用軟體。例如，應用軟體（例如，網頁應用軟體、瀏覽器應用軟體等）的應用二進位碼108可以向HLOS 106註冊，並且在列表112中進行辨識。如本領域中已知的，可信區114包括安全記憶體或者區域，其被配置為保證被載入到記憶體及/或被執行的代碼及/或資料在安全性、機密性、完整性等態樣受保護。用於註冊應用軟體的應用二進位碼108可以具有一或多個虛擬位址映射表，其由HLOS 106及/或可信區114中的演算法用於經由追蹤預定的虛擬位址點的執行來辨識期望或者目標高級應用功能。

【0038】 應當理解的是，可以將系統100應用於各種應用域，在該等應用域中，在核心層追蹤和偵測高級應用功能是有利的。例如，在一個示例性實施例中，核心可以控制決策，例如，回應於對正在執行的應用軟體的特定功能或者行為性質的偵測，增加及/或減小各種晶片上系統（SoC）部件（例如，中央處理單元（CPU）、快取記

憶體、雙倍資料速率（DDR）記憶體、一或多個匯流排等）的頻率，或者設置高功率及/或低功率模式以及啟用/禁用特定硬體特徵。以此種方式，HLOS 106和核心經由偵測和辨識出正被應用軟體執行的功能，而具有實現對在設備上執行的各種協力廠商應用軟體的各種控制的時機。應當理解的是，此舉可以允許SoC和平臺供應商從平臺/HLOS/核心級別提供用於各種協力廠商應用軟體的改良的方案，該平臺可能原本對該等協力廠商應用軟體沒有控制。

【0039】 在示例性應用域中，系統100可以提供針對網頁應用軟體、網頁瀏覽器、JavaScript（Java腳本）代碼等的惡意攻擊或者其他漏洞的即時安全性保護。如本領域中已知的，JavaScript是在許多網站和網頁應用軟體中使用的程式設計語言，基於JavaScript的攻擊是針對網路安全性的頭號威脅之一。隨著越來越多的網頁活動從桌上型電腦轉移到行動設備，JavaScript攻擊正變成對可攜式計算設備的主要威脅。

【0040】 大多數惡意JavaScript攻擊利用JavaScript語言的特性以及網頁標準和規範對漏洞的約束。經由惡意JavaScript的基於網頁的漏洞的常見實例係包括以下各項：跨站腳本（亦即，XSS/CSS）、跨站請求偽造（亦即，CSRF/XSRF）、偷渡下載、使用者意圖劫持、點擊劫持、分散式拒絕服務（DDoS）、JavaScript隱寫術以及各種形式的混淆JavaScript。

由於需要高級網頁行為和功能知識來嘗試偵測惡意行為，所以通常在瀏覽器軟體架構內構建當前網頁和JavaScript安全性方案。

【0041】 然而，HLOS、核心和設備平臺內的內置網頁安全性機制是受限的，因為基於網頁/JavaScript的漏洞可能沒有關於平臺活動(例如，系統撥叫、設備使用等)的可見的指示。許多基於網頁/JavaScript的攻擊是面向外部的，並且僅危害使用者的線上資產、活動、身份等。換言之，可能僅在網頁瀏覽器/應用軟體內偵測到可見的活動模式，並且因此針對網頁漏洞的大多數安全性機制幾乎總是構建在網頁瀏覽器應用軟體內。

【0042】 在該點上，系統100中的應用二進位碼108的示例性實施例可以包括網頁應用軟體、瀏覽器應用軟體或者在其中HLOS 106經由追蹤預定的虛擬位址點來偵測高級應用功能的其他應用軟體。如圖1中進一步所示，系統100亦可以包括位於可信區114中的一或多個惡意程式碼偵測演算法116。惡意程式碼偵測演算法116可以接收與虛擬位址點的執行以及在虛擬位址映射表中辨識的其相關聯的功能含義相關的資料。基於該資料，演算法116可以偵測例如惡意程式碼和行為、惡意JavaScript代碼和執行等，並且啟動用於解決安全性威脅或者以其他方式阻礙惡意攻擊的合適的方法。在一個實施例中，當偵測到安全性威脅時，系統100可以自動地解決威脅或者提示使用者進行合適的動作。

【0043】 如圖1的實施例中所示，由HLOS 106使用的虛擬位址映射表可以包括虛擬位址到函數映射表120以及辨識符到虛擬位址映射表122。應當理解的是，HLOS 106和映射表120和122包括整合平臺機制，經由該機制，系統100可以決定來自正在執行的應用二進位碼108的期望或者目標高級功能資訊。高級功能資訊可以由在可信區114中實現的演算法及/或模型（例如，惡意程式碼偵測演算法116）用於偵測惡意行為。

【0044】 如下文更詳細地描述的，系統100可以支援用於執行應用二進位碼108的兩種不同的執行模型。第一執行模型涉及本機二進位執行（例如，來自C/C++代碼）。第二執行模型涉及託管（managed）運行時間執行（例如，由虛擬機器118進行的執行）。在一個實施例中，虛擬機器118可以執行來自JavaScript源的動態即時（JIT）或者解釋代碼。在託管運行時間執行實施例中，虛擬機器118可以包括二進位碼108的部分，其中虛擬機器118在該二進位碼108內在該部分中執行。然而，應當理解的是，在其他實施例中，可以存在單獨的VM和二進位工作負載。

【0045】 在圖2-圖4中圖示本機二進位執行模型的示例性實施例。對於本機二進位執行而言，註冊應用軟體112的列表之每一者應用軟體具有對應的VAFMT 120，其由HLOS 106維護。VAFMT 120可以位於可信區114中。VAFMT 120包括不同的感興趣的虛擬位

址，其與其相關聯的高級功能相映射。在一個實施例中，每個相關聯的高級功能可以被表示為演算法116理解的巨集名稱。然而，應當理解的是，可以實現用於表示相關聯的高級功能的其他機制，例如包括指向演算法116中的函數或者函數名稱的指標，以使得在特定虛擬位址處偵測到的活動與演算法116中需要被觸發的功能直接對應。二進位圖像中的特定應用函數（以及函數內的特定點）的虛擬位址可以被稱為「興趣點」。在一個實施例中，虛擬位址興趣點可以包括在例如以下各項之內、起始處、結束處的點或者以下各項之間的多個特定點，或者用於對已知網頁/JavaScript攻擊的分析和偵測的其他合適的資訊：敏感源/宿常式、危險網頁應用程式設計介面（API）、特定網頁功能、緩衝器的起始/結束，或者攻擊者可以利用的任何其他物件。在其他實施例中，虛擬位址興趣點可以包括在JavaScript解譯器、即時（JIT）編譯器，或者運行時間環境（例如，用於儲存JavaScript原始程式碼、位元組代碼/JIT代碼的虛擬機器堆的分配/解除分配函數等）的實現中的點。

【0046】 圖2和圖3圖示VAFMT 120的示例性實施例。圖2圖示應用原始程式碼110內的某些期望或者目標功能點到應用二進位碼108內的對應的虛擬位址點的邏輯映射200。在圖2和圖3中，圖示虛擬位址，但是未圖示二進位目標代碼。在該實施例中，應用原始程式碼110包括用於「documentWrite（文件編寫）」函數的C++

代碼。原始程式碼中的點201被映射到二進位碼中的虛擬位址202。原始程式碼中的點203被映射到二進位碼中的虛擬位址204。原始程式碼中的點205被映射到二進位碼中的虛擬位址206。圖3圖示在VAFMT 120中的列302之下的二進位碼202、204和206中的的虛擬位址到代碼在彼等虛擬位址處表示的相應的功能含義的邏輯映射300。如圖3中所示，VAFMT 120可以包括複數個虛擬位址（列302）以及功能興趣點的對應描述（列304）。由二進位編碼點202表示的虛擬位址（0x3273fa94）被映射到與EVAL_FUNCTION相對應的功能點。由二進位編碼點204表示的虛擬位址（0x3473fac8）對應於表示DOCUMENT_WRITE_FUNCTION_START的功能興趣點。由二進位碼中的206表示的虛擬位址（0x3473fad4）被映射到具有巨集含義DOCUMENT_WRITE_1的功能點。

【0047】圖11圖示包括定製虛擬位址表的VAFMT 120的實施例，定製虛擬位址表具有用於特定緩衝分配器函數的虛擬位址，該等緩衝分配器函數可以用於決定動態分配的緩衝器(包括特定資料結構類型的物件(例如，類、結構體、聯合體））的起始和結束的虛擬位址。在緩衝器中分配的物件的成員/欄位的值可以使用偏移和長度欄位來決定，其中亦可以在該表中針對作為興趣點的特定欄位/成員來維護偏移和長度欄位。緩衝器分配函數的虛擬位址可以用於經由例如追蹤來自由分配器函數的虛擬位址

覆蓋的區域中的系統記憶體分配器函數的執行，來偵測所分配的緩衝器的大小和位址。一旦已知緩衝器起始和結束虛擬位址，偏移和長度欄位就可以用於決定用於特定資料結構類型的物件的特定成員/欄位的值。

【0048】 如圖1中虛線所示，應用原始程式碼110不需要儲存在系統100中。相反，其可以位於離線或者脫離設備的地方，並且可用作參考或者開原始程式碼。用於特定版本的參考原始程式碼可以用作參考和指導來決定瀏覽器或者網頁應用軟體的實際商業二進位檔案中的感興趣的虛擬位址。可以根據開源專案的相匹配的代碼修訂版/版本來編譯等效二進位檔案。經編譯的二進位檔案可以用作用於偵測基於該版本/修訂版的應用二進位檔案的期望或者目標虛擬位址以及函數/點的參考。可以使用類似的編譯器和連結器選項。此外，在應用代碼中的各個點處的中斷點可以用於對虛擬位址和其功能映射點的決定。二進位碼辨識和相似度提取方法可以用於經由使用來自用於開源專案的已知的、經編譯的函數的參考二進位檔案，來辨識給定應用二進位檔案中的功能。對於具有經稍微修改的版本的二進位檔案(或者來源於原始程式碼庫(source base）的二進位檔案，其具有與已知參考開源專案不同的一些原始程式碼）而言，可以編寫引動重要的網頁函數和API的測試代碼。來自各個測試用例的虛擬位址存取序列可以用於彙聚為目標虛擬位址點集合。應當理解的是，其他機制可以用於從應用二進位碼中提取功能。

【0049】 圖4是圖示用於偵測本機二進位執行模型中的惡意程式碼活動的方法400的實施例的流程圖。在方塊402處，產生用於應用軟體的VAFMT 120。如前述，VAFMT 120包括複數個感興趣的虛擬位址，該複數個感興趣的虛擬位址被映射到對應的高級應用功能。在方塊404處，可以在計算設備（例如，可攜式計算設備）上安裝應用軟體。在方塊406處，可以將應用軟體註冊用於由HLOS 106提供的安全性支援（例如，註冊應用軟體112）。在方塊408處，可以啟動應用軟體，並且作為回應，CPU 102可以執行應用二進位碼108。當註冊應用軟體112執行時，HLOS 106可以攔截應用軟體的執行程序（方塊410）。在方塊412處，HLOS 106可以使用對應的VAFMT 120來在功能興趣點被執行時偵測和記錄該等功能興趣點。在方塊414處，可以將所記錄的點提供給惡意程式碼偵測演算法116以偵測和解決惡意攻擊。惡意程式碼偵測演算法116可以包括基於簽名的演算法、模式匹配演算法或者採用機器學習或者其他技術。以此種方式，惡意程式碼偵測演算法116可以使用VAFMT 120來提供其作為輸入接收的虛擬位址的含義。

【0050】 由於VAFMT 120在HLOS 106的控制之下，由HLOS 106執行的應用二進位碼108的虛擬位址的任何轉換/隨機化（例如，位址空間佈局隨機化（ASLR））可以應用於VAFMT 120中的虛擬位址，以保持該等虛擬位址與正在執行的應用軟體的有效虛擬

位址同步。在一個實施例中，從JavaScript代碼以及利用VAFMT 120的應用軟體執行收集的資訊可以提供高級網頁/JavaScript功能資訊，其可以被提供給惡意程式碼偵測演算法116。在偵測到任何惡意行為（方塊416）之後，HLOS 106可以暫停應用軟體/渲染器/JavaScript程序，並且為使用者開啟對話方塊，該對話方塊就潛在的危險進行警告，並且詢問使用者用於繼續進行的指令。若使用者仍然想要繼續進行，則HLOS 106可以恢復瀏覽器程序。若使用者不想繼續進行，則HLOS 106可以請求使用者關閉標籤或者導覽到某個其他網站，或者HLOS 106可以結束用於該執行實例（瀏覽器標籤）的程序。

【0051】 當應用二進位碼110版本改變時，可以經由例如空中（OTA）更新來對VAFMT 120進行更新。該等更新確保HLOS 106準備好經更新的二進位檔案用於任何註冊應用軟體112。經更新的二進位檔案可以產生用於相同的興趣點的新的虛擬位址。

【0052】 應當理解的是，HLOS 106和映射表120和122亦可以被配置為支援涉及例如虛擬機器118（圖1）的託管運行時間執行模型。在該點上，上述整合平臺機制使得系統100能夠決定來自正在執行的應用二進位碼108的期望或者目標高級功能資訊。在圖5-圖10中圖示託管運行時間執行模型的示例性實施例。

【0053】 在涉及託管運行時間或者虛擬機器執行的實施例中，可以借助於另一表（例如，辨識符到位址映射表（IVAMT）122），從虛擬機器（VM）堆的不同部分中讀取JavaScript源及/或用於JavaScript源的位元組代碼/即時（JIT）二進位檔案。IVAMT 122包括用於VM堆的重要邊界的虛擬記憶體位址。其亦可以包括其他類型的條目，在該等條目中，可以維護用於虛擬機器118或者應用二進位108的各個功能點的虛擬位址。應當理解的是，IVAMT 122通常可以用於特定功能點的虛擬位址，其可以在應用軟體執行期間更新及/或動態地決定。在該點上，IVAMT 122可以將功能點映射到虛擬位址。在另一態樣，VAFMT 120可以將靜態定義的虛擬位址映射到功能含義。因此，在應用軟體執行期間VAFMT 120可以不改變，但是可以經由例如到計算設備的空中（OTA）更新來進行更新。亦應當理解的是，其他各種各樣的表可以與VAFMT 120和IVAMT 122相關聯。該等各種各樣的表可以包括各種巨集或者參數名稱，其映射到其不是虛擬位址的參數值或者設置。

【0054】 在圖9的實施例中，辨識用於示例性VM堆結構900的各個外部及/或內部邊界的虛擬記憶體位址901。如圖9中所示，VM堆結構900可以包括辨識各個外部及/或內部邊界的複數個資料欄位，其包括例如始於欄位912、至欄位914、代碼欄位902、映射欄位904、大物件欄位906、舊資料欄位908以及舊指標欄位910。

VM堆是VM託管記憶體區域，其被分配在本機系統堆中。如本領域中已知的，在VM堆中，VM執行例如對以下各項的抽象：記憶體管理、分配和解除分配代碼（例如，JavaScript源）、位元組代碼、中間代碼、JIT二進位檔案、在執行期間建立的物件以及用於程式的執行的所有其他相關聯的內務資訊以及內部資料結構（例如，JavaScript程式）。如圖9中進一步所示，根據VM所儲存的事物的類型，VM堆區域可以包括各個子區域（例如，910、908、906、904、902、912和914）。子區域912和914可以用於包含第一次建立的物件，並且任何垃圾回收活動互換來自子區域912至914的活動物件，並且反之亦然。在一個實施例中，子區域902可以用於保存JavaScript源、位元組代碼、中間代碼和JIT二進位/組合代碼。子區域904可以用於保存與由VM在程式（例如，JavaScript程式）的執行期間建立的物件相關聯的某些內部資料結構。子區域906可以用於保存比預定尺寸（例如，1 MB）大的任何種類的項（代碼、物件）。子區域908和910可以保存已經倖免於多個垃圾回收週期的物件和資料，其中子區域908關注具有常數值的物件，以及子區域910關注指向其他物件的的物件。

【0055】 在操作中，HLOS 106可以隨著針對VM堆的記憶體分配改變，而辨識並且動態地更新IVAMT 122中的虛擬記憶體位址901。應當理解的是，JavaScript虛擬機器118保存該堆中的源，直到函數是活動的為止。

託管運行時間或者虛擬機器執行模型可以涉及辨識來自VM堆的JavaScript源及/或位元組/JIT代碼。可以針對任何新的寫來追蹤具有JavaScript源的VM堆物件，並且可以辨識由虛擬機器118接收的新的JavaScript源。可以將所辨識的JavaScript源提供給可信區114中的演算法116，該演算法116從JavaScript代碼中提取各個特徵，並且使用該等特徵來偵測任何惡意行為。從JavaScript代碼中提取的特徵的實例係包括以下或者其他特徵：文件物件模型（DOM）修改以及敏感函數；評估的數量；字串的數量；腳本長度；字串修改函數；用於去混淆（de-obfuscation）的「內置」等。可信區115可以將所提取的特徵提供給惡意程式碼偵測演算法116，以決定任何惡意活動。

【0056】 在某些實施例中，當僅有JIT二進位/位元組代碼可用時，可以從JIT二進位/位元組代碼中提取特徵，並且隨後將特徵發送給惡意程式碼偵測演算法116。例如，HLOS 106可以維護表示高級JavaScript工件（artifact）的位元組代碼/JIT代碼序列的庫。可以記錄來自VM代碼空間中的JavaScript函數的位元組代碼/JIT代碼串流與該等工件的任何匹配，並且將其傳遞給惡意程式碼偵測演算法116，以對惡意特性進行決定。

【0057】 圖5和圖6圖示在託管運行時間或者虛擬機器執行期間使用的IVAMT 122和VAFMT 120的示例性實施例。圖5圖示與VM代碼空間的分配相關的目標功能

到對應的應用二進位碼108的邏輯映射500。在該實施例中，應用原始程式碼110包括用於「AllocateVMCodeSpace」函數的代碼。如圖5中所示，原始程式碼110中的第一點可以被映射到二進位碼108中的虛擬位址502。原始程式碼110中的第二點可以被映射到二進位碼108中的虛擬位址504。在示例性實現中，當VM在執行期間獲得其需要執行的新的JavaScript原始程式碼，並且決定在當前VM堆代碼空間中不存在太多空間（902）時，可以調用函數AllocateVMCodeSpace。該函數可以獲得新的JavaScript代碼的大小，並且決定VM堆代碼空間在大小上需要被增加的量，以使得VM可以保存JavaScript源、相關聯的位元組代碼或者中間代碼及/或JIT二進位檔案。基於所決定的大小，AllocateVMCodeSpace函數可以使用系統分配器函數（例如，mmap()、malloc()、calloc()或者realloc()），來增加本機平臺的堆中的VM堆代碼空間的所分配的空間。mmap()函數是相容POSIX的Unix系統調用，其將在從檔案描述符指定的其他物件的一偏移處起始(較佳地，在位址起始處）的位元組序列映射到記憶體中。mmap()函數返回物件被映射的實際地方。Malloc()、realloc()、calloc()和free()包括C標準庫中的用於以C/C++程式設計語言執行針對動態記憶體分配的手動記憶體管理的一組函數。可以將用於二進位碼108中的興趣點的虛擬位址502

和504直接放置在VAFMT 120中的列302中。由虛擬位址表示的不同興趣點的功能含義可以作為巨集名稱列在VAFMT 120的列304中。偵測演算法116（圖1）可以具有對由VAFMT 120的列304中的巨集所表示的功能的清楚的理解。針對VAFMT 120中的特定行的巨集名稱（列304中）可以明確地辨識當處理器（例如，CPU 102）執行應用軟體在虛擬位址點（列302中）處的二進位指令時正在被執行的功能。以此種方式，經由知曉執行統計結果、用於興趣點的虛擬位址的計數和分佈，偵測演算法116充分地理解正在由高級應用二進位檔案執行的功能。應當理解的是，映射可以直接在虛擬位址302與由巨集（304）表示並且由執行處理或者偵測的偵測演算法116理解的功能含義之間，從而消除知曉該虛擬位址興趣點處的實際二進位指令。

【0058】 利用虛擬位址和巨集含義表示的興趣點可以離線決定，並且隨後被填充於用於特定應用二進位檔案的VAFMT 120中。許多類型的應用軟體可以具有可用的匹配參考原始程式碼。例如，匹配參考原始程式碼可以可用於從普及的開源專案（例如，基於blink/Chromium的瀏覽器、基於Webkit的瀏覽器、安卓平臺中的各種虛擬機器（諸如Dalvik、ART、RenderScript））開發的常用應用軟體。對於具有可用匹配參考原始程式碼的應用軟體而言，各種離線機制可以用於決定用於商業應用二

進位檔案中的興趣點的虛擬位址，以用於原始程式碼中的用於彼等興趣點的對應運算式/語句。

【0059】 將對用於興趣點的虛擬位址的離線決定的示例性實施例進行描述。可以在匹配參考原始程式碼中辨識原始程式碼110中的實現感興趣的功能的某些重要且有用的函數。可以將原始程式碼110內的各個點手動地決定為形成將一起表示特定唯一的功能的唯一點集合。應當理解的是，此點集合可以等效於原始程式碼110內的用於該功能的取樣點集合，該取樣點集合唯一地表示完整的原始程式碼110的整體功能。可以對原始程式碼110進行編譯、組合以及連結到參考應用軟體，該參考應用軟體等效於實際的商業協力廠商應用軟體。二進位檔案（參考和商業協力廠商二者）皆可以源自於相同的原始程式碼110，並且使用類似的構建技術（例如，編譯、組合、連結）和工具鏈。如本領域已知的，開源應用軟體可以使用可免費獲得的GCC或者LLVM工具鏈。編譯器、組合器和連結器工具可以用於產生參考二進位應用軟體，並且可以記下與原始程式碼中的重要點相對應的虛擬位址點。由於用於興趣點的虛擬位址可以包括對二進位應用軟體從其構建（編譯、組合、連結）的原始程式碼110中的興趣點的直接映射，所以參考二進位檔案可以離線用於與商業二進位檔案進行比較，以辨識商業協力廠商二進位檔案中的虛擬位址興趣點。亦應當理解的是，其他離線或者其他技術可以用於決定商業協力廠商二進位檔案中的興趣點的虛擬

位址。在一個實施例中，圖2圖示原始程式碼110中的不同興趣點（201、203、205）可以如何直接被映射到二進位檔案108中的對應虛擬位址（202、204、206）。

【0060】 圖6圖示圖5中的VAFMT 120與示例性IVAMT 122之間的邏輯映射600。VAFMT 120包括二進位應用軟體中的固定且已知的興趣點的虛擬位址，該二進位應用軟體的執行是感興趣的並且正在被追蹤。每當二進位應用軟體改變時，可以更新該等虛擬位址。IVAMT 122 包括當二進位應用軟體執行時被建立或者更新的特定點的虛擬位址，其可以是動態的，並且表示動態項的虛擬位址（例如，運行時間緩衝器起始或者結束點）。VAFMT 120中的左側列（302）包括虛擬位址，而右側列（304）可以指示在該虛擬位址點處的在二進位碼108中存在的功能描述。以此種方式，VAFMT 120將虛擬位址映射到功能含義。通常，IVAMT 122包括相反的內容。在此種情況中，功能含義或者巨集名稱是已知的，並且系統決定在二進位應用軟體的執行實例中功能含義或者巨集名稱604被實現或者可用的虛擬位址602。IVAMT 122中的虛擬位址可以包括在運行時間被決定的動態值。對於動態分配的緩衝器（或者虛擬機器堆或者其子空間）的起始和結束被決定的情況而言，可以從VAFMT 120獲取用於二進位應用軟體中的正在進行動態的緩衝器/堆空間分配的函數內的興趣點的虛擬位址。該等函數的執行可以經由偵測VAFMT 120中的虛擬位

址的執行來決定。此外，緩衝器/堆空間分配的起始/結束虛擬位址可以經由偵測從該等函數引動的系統記憶體分配函數來決定。可以在IVAMT（122）中更新緩衝器/堆空間分配的該等決定的起始/結束虛擬位址。

【0061】 圖7圖示垃圾回收對VM堆代碼空間的影響以及可以如何在虛擬機器118的垃圾回收活動存在的情況下一貫地決定JavaScript源。應當理解的是，垃圾回收是託管運行時間或者虛擬機器的不可缺少的活動，因為對新物件的分配以及對無用（dead）（亦即沒有在使用中）物件的解除分配可以由運行時間或者虛擬機器118來明確地處理。從託管VM堆中取回（reclaim）無用（未使用的）物件的活動被稱為垃圾回收。在該點上，當取回不需要的腳本物件或者其他物件時，可以重新組織VM堆，並且將現有物件來回移動以及進行壓縮，以為新物件分配騰出空間。圖7圖示此種垃圾回收活動對VM堆代碼空間704a的影響。VM堆代碼空間704a包括JavaScript物件JS1、JS2、JS3、JS4。在垃圾回收事件之後，可以經由移除被垃圾回收器偵測為不需要的或者無用的JavaScript物件JS3，並且因此從VM堆代碼空間704b中取回（刪除），從而對該等JavaScript物件進行壓縮。然而，VM堆中的物件的任何此種移動（例如，移除、壓縮等）改變決定JavaScript物件位於何處的虛擬位址起始和結束位置。在示例性方法中，可以經由在每次垃圾回收活動之後，重新執行圖5和圖6中圖示的用於VM堆和該

堆內的各個空間（圖9）的虛擬位址決定機制，來改變虛擬位址，從而在腳本物件在垃圾回收期間被移動的情況下，利用新值來更新虛擬位址。如圖8中所示，核心可以追蹤在垃圾回收期間發生的物件移動以及該等物件移動的距離。經由追蹤物件移動的位址偏移，可以更新JavaScript物件在VM堆代碼空間中的起始和結束的虛擬位址值。以類似的方式，可以經由追蹤圖9中圖示的對VM堆的各個子空間的分配/解除分配/移動，來更新IVAMT 122中的用於VM堆的各個代碼空間的虛擬位址。

【0062】 圖10是圖示用於偵測託管運行時間或者虛擬機器執行模型中的惡意程式碼活動的方法1000的實施例的流程圖。應當理解的是，圖10中的方塊1002、1004、1006、1008和1010中表示的步驟或者功能通常可以與上文結合圖4的方法所描述的方塊402、404、406、408和410相對應。在方塊1012處，方法1000偵測用於VM堆分配器/解除分配器函數在被執行時的興趣點虛擬位址。如方塊1014處所示，當該執行被偵測到是在VM堆分配器/解除分配器函數內時，方法1000可以偵測進入核心的系統分配器/解除分配器函數的入口VM，並且記錄系統記憶體分配/解除分配。基於此，方法1000可以計算並且決定VM堆的起始/結束虛擬位址。經由實現用於VM堆的特定分配區域（例如，代碼空間、大物件空間等）的類似機制，可以決定用於VM堆內的特定子區域（例如，

代碼空間、大物件空間等）的起始/結束虛擬位址。如方塊1016處所示，一旦在方塊1014處決定用於儲存JavaScript原始程式碼物件的VM堆空間，方法1000就可以使用腳本物件頭部簽名/模式（具有二進位形式），來決定JavaScript物件在VM堆內的起始。JavaScript物件的長度可以是從頭部中提取的，並且用於提取整個JavaScript原始程式碼。如方塊1018處所示，JavaScript原始程式碼可以用於提取由偵測演算法116用於偵測例如惡意行為的感興趣的特定特徵。在方塊1020處，可以基於例如在方塊1018中從JavaScript源中提取的特徵，決定JavaScript代碼的惡意行為。

【0063】 如前述，VAFMT 120可以以離線方式初始地配置，並且被提供給計算系統100（圖1）。在一個實施例中，當使得應用二進位碼108的新版本可用於計算系統100時，VAFMT 120可以類似地以離線方式進行更新，並且經由例如通訊網路（被稱為「空中（OTA）更新」）被提供給計算系統100。對於被頻繁地更新的二進位應用軟體而言，以此種方式更新VAFMT 120可能是缺點。應當理解的是，在應用二進位碼108的經更新版本中的二進位碼的相對大的部分可能保持不變。VAFMT 120中辨識的功能興趣點304可以包括應用二進位碼108及/或二進位碼的可能逐個版本沒有改變的相對有限部分。

【0064】 例如，編譯器操作及/或設置可以不是經常改變，以及二進位碼中的各個模組可以維護在各模組之間類似或者預定的偏移。圖12-圖16圖示可以在計算系統100中實現的用於當安裝了應用二進位碼108的新的或者經更新的版本時自動地更新VAFMT 120中的虛擬位址的各種機制。

【0065】 應當理解的是，該等機制可以減少針對用於各種類型的應用軟體及/或用例的VAFMT 120的OTA更新的需求。例如，在網頁安全性應用軟體的背景下，該等機制可以消除針對用於對基於相同的原始程式碼庫的網頁瀏覽器應用軟體的最頻繁類型的更新中的許多更新的OTA更新的需求。現有的網頁瀏覽器應用軟體可以在每週或者每月的基礎上來更新二進位應用代碼。用於新二進位版本的虛擬位址可能改變，即使當原始程式碼還沒有針對與功能興趣點304相關的特定模組進行改變時。在此種情況中，在該應用軟體中的除了功能興趣點304之外的部分中存在原始程式碼改變或者在該應用軟體的其他部分中存取的變數類型和資料結構類型（例如，C++類、C-結構體、聯合體等）態樣存在改變的情況下，虛擬位址可能改變。此外，在編譯器、組合器和鏈路器選項中的某些種類的改變可能導致該應用軟體的其他部分中的虛擬改變。

【0066】 圖12圖示可以在計算系統100中實現的用於當安裝了應用二進位碼108的新的或者經更新的版本時

自動地更新VAFMT 120的示例性機制的實施例。如圖12中所示，可以利用中繼資料1200和一或多個偽二進位碼範本1202來增補VAFMT 120。如下文更詳細地描述的，中繼資料1200和偽二進位碼範本1202可以使得HLOS 106能夠在利用新版本更新應用二進位碼108時決定用於功能興趣點304的新虛擬位址302。

【0067】 應當理解的是，偽二進位碼範本1202包括操作陳述式序列，其將符號表示用於記憶體中的儲存位置以及用於本端變數的偽暫存器。偽二進位碼範本1202可以使用指示其目的的各種類別的偽暫存器。在一個實施例中，ArgumentReg#可以表示將引數傳遞給子常式的偽暫存器。ReturnReg可以包括當從子常式調用返回時的返回位址。ProgCounter可以包括由處理器的程式計數器指向的當前位址。ReturnValueReg#可以表示用於將來自子常式調用的值返回到調用器代碼的暫存器。操作可以包括處理器中具有可以是變數或者儲存位置的輸入和輸出的組合操作的接近表示（close representation）。例如，AddWord變數可以指示大小為4位元組或者1字的運算元的加法運算。LoadWord變數可以指示從具有預定大小（例如，4位元組或者1字）的記憶體中載入值。LoadByte變數可以指示從具有預定大小（例如，1位元組）的記憶體中載入值。branchEQ可以包括條件分支，其中若先前比較操作導致正在比較的運算元相等，則該條件分支進行分支到目標被作為運算元

而提供。定址模式或者位址計算可以獨立於載入或者儲存操作。在一個實施例中，利用基址暫存器和偏移的載入操作可以被分離為兩種操作：加法運算，其經由將常數偏移值加到偽暫存器上來計算最終位址；之後是實際的載入操作，其使用包含所計算的最終位址的偽暫存器。此舉可以完成以保存具有最通用形式的表示，因為經更新的應用二進位檔案可以使用各種形式的定址模式。作為常數的操作引數可以由對有效的常數範圍進行編碼所需要的位元數量表示。

【0068】 例如，常數「Const8bits」可以用作操作的運算元，其指示該運算元是可以由8位元編碼的任何有效值，並且因此，決定所允許的值的有效動態範圍。一些運算元可以是硬編碼常數（例如，「#8」指示值「8」）。直接分支操作的運算元可以被表示為從當前程式計數器的偏移（例如，「ProgCounter+#Const20bits」或者「ProgCounter+#12」）。偽二進位碼範本1202可以使用該等或者其他操作陳述式來實現感興趣的功能。應當理解的是，操作陳述式可以用於辨識新的經更新的二進位檔案中的區域，其經由例如匹配功能或者模組來實現提取功能。匹配模組被配置為理解偽二進位碼範本1202和應用軟體的實際二進位檔案的格式和表示二者。匹配模組可以在操作訊窗內執行逐個操作的比較，以偵測匹配或者使用控制資料流程和控制資料流程區域內的操作來進行比較。

【0069】 可以使用各種匹配技術。偽二進位碼範本1202中的操作陳述式可以使用靜態單賦值（SSA）表示，其中一次僅分配特定的偽暫存器變數，從而披露操作陳述式之間的真實依賴關係。SSA表示可以能夠實現應用軟體的經更新的二進位檔案中的功能區域的改良的匹配。術語「偽」代表以下事實：表示不是二進位可執行檔案並且不使用處理器的實際的組合指令、暫存器和定址模式，並且不被組合到二進位碼中。偽二進位碼範本1202提供功能參考，其中匹配模組使用其作為範本模式和指南來偵測應用軟體的經更新的二進位檔案中的感興趣的功能。應當理解的是，偽二進位碼範本1202的實際格式和表示是依賴的實現，並且可以使用各種其他替代方案。在其他實施例中，一些實現可以使用實際的組合指令表示，或者類似於二進位應用軟體在其上執行的CPU 102的組合表示的表示。

【0070】 如前述，HLOS 106可以維護註冊應用軟體112的列表。對於每個註冊應用軟體而言，HLOS 106維護包括用於功能興趣點304的虛擬位址302的表（例如，VAFMT 120、IVAMT 122）。如圖12中所示，VAFMT 120中的一或多個虛擬位址302可以與偽二進位碼範本1202相關聯。在圖12的實施例中，偽二進位碼範本1202與用於功能興趣點304的特定集合的虛擬位址302的集合相關聯，功能興趣點304的特定集合表示唯一功能（documentWrite函數）。偽二進位碼範本1202

包括一般等效於覆蓋documentWrite函數的二進位碼的偽代碼指令。在一個實施例中，偽二進位碼範本1202可以不使用處理器指令集架構（ISA），並且不需要被組合到實際的二進位碼中。偽二進位碼範本1202可以使用類似於組合操作的操作陳述式，並且使用偽暫存器和符號參考來進行儲存。儘管使用此種操作陳述式序列，但是偽二進位碼範本1202可以實現感興趣的功能（例如，在上文實例中的「documentWrite」函數的功能），其中其表示的該功能與在應用軟體的實際二進位檔案中實現的感興趣的功能（例如，documentWrite函數）相同或者等效。應當理解的是，計算系統100可以包括任何數量的偽二進位碼範本1202。不同的偽二進位碼範本1202的數量可以使得：在VAFMT 120中擷取的所有不同的功能（儘管不同的功能興趣點集合）皆具有至少一個代表性偽二進位碼範本1202，其用於當安裝新應用二進位碼時更新其覆蓋的函數點的虛擬位址。

【0071】 在一個實施例中，偽二進位碼範本1202可以包括通用形式的目標組合指令、一或多個偽暫存器，以及從通用基礎（例如，全域堆或者堆疊、符號/變數名稱）的記憶體存取偏移（其表示記憶體中的特定參考點）。中繼資料1200通常包括使用例如位元組偏移的無虛擬位址的表示。用於虛擬位址（0x3473fac8）的中繼資料1200包括位元組偏移（BASE2=BASE0+74709704）。用於虛擬位址（0x3473fad4）的中繼資料1200包括位元

組偏移（BASE2+12）。用於虛擬位址（0x3473fae8）的中繼資料1200包括位元組偏移（BASE2+32）。應當理解的是，該中繼資料可以形成與唯一地表示「document_write」功能的三個虛擬位址興趣點的集合相對應的唯一集合。

【0072】 偽二進位碼範本1202可以初始以離線方式產生，被提供給計算系統100，並且儲存在設備的安全儲存裝置中。應當理解的是，當在例如由功能興趣點304覆蓋的區域中的代碼及/或資料結構中存在明顯的改變時，可以僅需要更新偽二進位碼範本1202。該等類型的改變可以是相對不頻繁的(例如，每6個月一次)。可以經由OTA更新來實現該類型或者其他類型的更新。此舉可以能夠實現從例如每週/每月基礎的虛擬位址的OTA更新到僅在每6個月一次進行偽二進位碼範本1202的OTA更新的顯著減少。

【0073】 可以偵測用於現有的註冊應用軟體的新二進位版本的更新或者重新安裝。作為回應，中繼資料1200和偽二進位碼範本1202可以用於自動地更新VAFMT120。如圖12中所示，偽二進位碼範本1202可以用於對新應用軟體中的二進位碼的區域1206進行模式匹配，其中由偽二進位碼範本1202表示的功能興趣點304（並且因此該特定偽二進位碼範本表示的虛擬位址興趣點）位於該區域1206中。中繼資料1200可以用於關注於在應用二進位碼108的經更新的版本1204中搜尋區域1206。可以

進行初始嘗試，以經由使用來自用於唯一功能的功能興趣點304的原始基礎（BASE0）的相對OFFSET，對所關注的區域1206進行搜尋（例如，在基礎BASE2之前以及之後的預定百分比）。應當理解的是，在許多類型的頻繁更新中，該等相對偏移保持在附近。如圖12中進一步所示，當偵測到匹配時，可以從新二進位檔案中獲取新虛擬位址，並且可以對VAFMT 120進行更新以反映新虛擬位址。若一或多個功能興趣點304無法產生新二進位檔案中的匹配，則計算系統100可以啟動OTA更新，或者在其他實施例中，基於特定功能的重要性，從VAFMT 120中刪除特定的感興趣的功能以及相關聯的虛擬位址。

【0074】 圖13圖示來自圖12的具有經更新的虛擬位址的VAFMT 120（由灰色方塊表示）。與DOCUMENT_WRITE_FUNCTION_START興趣點304相對應的虛擬位址302已經被更新為新虛擬位址（0x3133b61c）。與DOCUMENT_WRITE_1興趣點304相對應的虛擬位址302已經被更新為新虛擬位址（0x3133b62c）。與DOCUMENT_WRITE_2興趣點304相對應的虛擬位址302已經被更新為新虛擬位址（0x3133b62c）。如圖12中進一步所示，亦可以對與虛擬位址相對應的中繼資料1200進行更新。如圖13中所示，用於新虛擬位址（0x3133b61c）的中繼資料1200已經被更新為「BASE2=BASE0+74709000」。此情形圖示在應用軟體的經更新的二進位檔案中的兩個感興

趣的功能之間（亦即，在「KERNEL_ALLOCATOR_FUNCTION」與「DOCUMENT_WRITE_FUNCTION」之間）的輕微相對位置改變。該改變可以是相對輕微的。例如，該改變可以是在該兩個感興趣的功能之間的74709704位元組的總原始距離中減少704位元組。因此，在已經以兩種感興趣的功能之間的基礎偏移中繼資料（亦即74709704位元組）之前和之後的某一容忍度關注了搜尋的情況下，經由使得搜尋區域變窄，而允許有效的匹配。用於新虛擬位址（0x3133b62c）的中繼資料1200已經被更新為BASE2+16。用於新虛擬位址（0x3133b640）的中繼資料1200已經被更新為BASE2+36。

【0075】圖14和圖15圖示與和DOCUMENT_WRITE函數相關的功能興趣點304的集合相關聯的偽二進位碼範本1202的示例性實施例。功能興趣點304的集合包括DOCUMENT_WRITE_FUNCTION_START模組、DOCUMENT_WRITE_1模組以及DOCUMENT_WRITE_2模組。如圖14中所示，在該集合中的功能興趣點304之每一者功能興趣點與特定偽代碼指令直接相關聯，特定偽代碼指令形成偽二進位碼範本1202內的「偽二進位指令興趣點」。基於經更新的應用二進位檔案中的與「偽二進位興趣點」直接匹配的特定二進位指令，偽二進位碼範本1202內的該等「偽二進位指

令興趣點」包括當前VAFMT 120中的虛擬位址興趣點與應用二進位檔案的經更新的版本中的新虛擬位址興趣點的一對一映射。如圖14中所示，DOCUMENT_WRITE_FUNCTION_START模組與保存前兩個調用器保存的偽暫存器（CallSave0、CallSave1）以及返回暫存器（ReturnReg）的「入堆疊」操作相關聯。其之後是AddWord操作，其計算隨後的LoadWord操作所需要的位址。AddWord操作將應當適合放入8位元的常數值與程式計數器相加，並且將結果保存在偽暫存器reg0中。隨後的LoadWord操作直接使用reg0中的位址作為要從其載入值的位址。在用於應用軟體的實際二進位檔案中，具有8位元常數的AddWord可以被直接包括在LoadWord指令中作為定址模式的一部分。「Const8bits」允許具有適合放入8位元的任何常數值的選項。將所載入的值保存在偽暫存器reg1中，並且將其用作將值載入在偽暫存器reg2中的第二LoadWord操作的位址。對於由DOCUMENT_WRITE_FUNCTION_START表示的功能興趣點而言，「入堆疊」操作是該偽二進位碼範本1202中的「偽二進位指令興趣點」。

【0076】 DOCUMENT_WRITE_1模組與邏輯左移16位元的值的操作相關聯，16位元的值被保存在偽暫存器（reg0）中並且保存在偽暫存器reg1中。隨後將其與常數值「4」相加，並且將得到的值保存在偽暫存器reg2

中，隨後該得到的值用作一位址，其中值從該位址被載入在偽暫存器（reg3）中。應注意的是，對於實際的二進位載入指令而言，定址模式可以直接執行與常數值4的加法，並且因此，AddWord和LoadWord可以由單載入指令表示。亦可以將reg3中的值加到程式計數器值（PC）上，以建立偽暫存器reg4中的最終位址，該最終位址是如下的位址：位元組值從該位址被載入到用於作為第一引數傳遞給所調用的常式的第一引數暫存器「ArgumentReg0」中。在其之後，存在去往處於一偏移（其是可以適合放入20位元的值）處的位址的直接分支。然而，在直接分支指令之前，存在AddWord指令，該AddWord指令保存在直接分支對應用軟體的不同部分進行控制之後要返回的位址（經由正確地設置ReturnReg）。「邏輯左移」操作是用於該偽二進位碼範本1202中的由DOCUMENT_WRITE_1表示的功能興趣點的「偽二進位指令興趣點」。

【0077】DOCUMENT_WRITE_2模組與AddWord操作相關聯，該AddWord操作將可以適合放入8位元的常數值與程式計數器相加，並且將結果保存在偽暫存器reg0中。隨後將偽暫存器reg0用作一位址，其中值從該位址被載入在偽暫存器（reg2）中。其之後是另一AddWord操作，該AddWord操作將偽暫存器（reg2）和程式計數器的當前值相加並且將結果保存在偽暫存器reg1中。隨後偽暫存器reg1用作一位址，其中

值從該位址被載入到ArgumentReg0中，ArgumentReg0用於經由直接分支指令將值傳遞給隨後的子常式調用。應注意的是，對於實際的二進位載入指令而言，定址模式可以直接執行與常數值的加法，並且因此，在應用軟體的實際二進位檔案中，AddWord和LoadWord可以由單載入指令表示。在LoadWord操作之後，存在去往處於一偏移（其是適合放入20位元的值）處的位址的直接分支。然而，在直接分支指令之前，存在AddWord指令，該AddWord指令保存在直接分支對應用軟體的不同部分進行控制之後要返回的位址(經由正確地設置ReturnReg）。對子常式的調用之後跟隨兩組比較和去往偽二進位碼範本1202內的附近位置的分支。比較皆是在第一子常式返回值暫存器（ReturnValueReg0）上完成的，以檢查由子常式返回的特定值（「0」和「1」），並且基於所返回的值，分別使用BranchEQ和BranchNE操作本端地進行分支。分支目標位址被提供為從當前程式計數器值的常數偏移。將Const8bits運算元與程式計數器相加的AddWord操作是用於該偽二進位碼範本1202中的由DOCUMENT_WRITE_2表示的功能興趣點的「偽二進位指令興趣點」。應注意的是，應用軟體的實際二進位檔案可以具有偽二進位碼範本中的該位址計算操作（AddWord）以及LoadWord操作，其匹配到單個實際二進位指令（如「ldr r1, [pc,#80]」），並且在此種

情況中，在「偽二進位指令興趣點」全部匹配或者作為其子部分匹配的實際二進位指令變成決定應用軟體的二進位檔案的新版本中的經更新的虛擬位址的指令。

【0078】 圖15圖示偽二進位碼範本1202中的偽代碼指令中的每一者與應用二進位碼108的經更新的版本1204中的所匹配的區域1206中的等效的對應二進位碼的匹配。在操作中，當偽二進位碼範本1202與區域1206匹配時，二進位碼中與功能興趣點304匹配的對應指令的虛擬位址變成新虛擬位址，並且在VAFMT 120中進行更新。可以基於新虛擬位址來計算新基礎和偏移，並且可以對中繼資料1200進行更新。

【0079】 圖16圖示在計算系統100中實現的用於當安裝應用二進位碼108的新的或者經更新的版本時自動地更新VAFMT 120的方法1600的實施例。在方塊1602處，可以將用於向HLOS 106註冊的應用軟體的虛擬位址映射表120儲存在計算系統100中，如前述。可以將VAFMT 120儲存在HLOS 106中的安全記憶體中。如圖12中所示，VAFMT 120可以包括複數個虛擬位址302的集合，其映射到用於註冊應用軟體的應用二進位碼108中的對應目標應用功能（功能興趣點304）的。回應於接收到應用二進位碼108的經更新的版本1204（決策方塊1604），可以決定與虛擬位址映射表120中的複數個虛擬位址302的集合中的一或多個集合相關聯的對應偽二進位碼範本1202（方塊1606）。如前述，在一個實

施例中，偽二進位碼範本1202連同初始VAFMT 120一起可以初始經由到系統100的空中（OTA）更新，或者經由下載代碼/日期並且將其安裝到系統100的任何其他方式，來獲取。該等偽二進位碼範本1202和VAFMT 120二者可以被儲存在系統100中可由HLOS 106和核心存取的位置中。實際的儲存位置是相互依賴的實現。各個級別的安全性保護或者安全記憶體配置可以被考慮用於儲存位置，此情形取決於實現選擇。當例如現有範本中的一或多個範本無法在應用軟體的經更新的二進位檔案中發現任何匹配時，可以對偽二進位碼範本1202進行更新。由於感興趣的區域中的應用代碼中的大規模改變或者上述其他種改變，可能發生不匹配。在此種情況期間，經更新的偽二進位碼範本1202和經更新的VAFMT 120可以是OTA下載的，並且被安裝在系統100中。在決策方塊1608處，偽二進位碼模組1202用於對應用二進位碼108的經更新的版本1204進行搜尋，並且將偽代碼指令與等效二進位指令進行匹配。當發現匹配時，在方塊1610處，決定與二進位指令相對應的新虛擬位址。在方塊1612處，可以利用新虛擬位址以及對應的經更新的基礎/偏移中繼資料1200，來對虛擬位址映射表120進行更新。

【0080】 如圖16中所示，可以針對所有不同的偽二進位碼範本1202，重複方塊1606、1608、1610和1612，直到所有的偽二進位碼範本1202被匹配並且VAFMT 120中的所有虛擬位址被更新為止。在決策方塊1611

處，方法1600可以決定所有偽二進位碼範本1202是否已經被處理。若「是」，方法1600可以在方塊1613處結束。若「否」，在方塊1606處，可以選擇新的偽二進位碼範本1202。在決策方塊1608處，當在應用軟體的經更新的二進位檔案中針對特定偽二進位碼範本1202辨識匹配的二進位序列時，方法1600可以重複到下一偽二進位碼範本1202，以進行匹配。若在某一重複處，在應用軟體的經更新的二進位檔案中不存在針對偽二進位碼範本1202的匹配，則首先決定是否可以從VAFMT 120中刪除感興趣的功能（由偽二進位碼範本1202表示）（決策方塊1607）。若可以刪除其（其可以由於不同的原因（包括功能的重要性為低）造成的），則可以從VAFMT 120中刪除用於該感興趣的功能的所有虛擬位址興趣點(方塊1605），並且重複繼續進行到方塊1606，以針對用於下一偽二進位碼範本1202的匹配進行搜尋。然而，若該功能（並且因此偽二進位碼範本1202）是重要的，並且不應當被刪除（方塊1609），則自動更新機制失敗，在此種情況中，可以執行用於虛擬位址及/或偽二進位碼範本1202的完整的空中（OTA）更新。此情形可以表示在應用軟體的經更新的二進位檔案中存在重大改變/修改的情況（例如，此情形可以以較低的頻率發生，6個月一次）。

【0081】 圖17-圖23圖示用於使用基於偏移的虛擬位址映射方案來偵測目標應用功能的系統和方法的各個實施例。通常，基於偏移的虛擬位址映射方案涉及使用虛擬

位址偏移來進行應用二進位碼108中的虛擬位址到對應的高級目標應用功能的映射。應當理解的是，對於實現對用於同一應用軟體的多個程序的同時執行的目標應用功能的偵測而言，基於偏移的虛擬位址映射可能是尤其有用的。在一個實施例中，目標應用功能可以是在多個瀏覽器標籤或者網頁瀏覽器應用軟體的實例的同時執行中偵測到的。此外，基於偏移的虛擬位址映射方案可以利用具有浮動的位址的動態共享庫。

【0082】 圖17圖示基於偏移的虛擬位址映射方案1700的示例性實施例的架構及/或操作。如圖17中所示，基於偏移的虛擬位址映射方案1700涉及由兩種不同類型的虛擬位址到函數映射表支援的兩階段方案：應用特定VAFMT 1702以及一或多個程序特定VAFMT 1714。每個註冊應用軟體112可以具有應用特定VAFMT 1702，其可以是針對對應的應用二進位碼108產生的。應用特定VAFMT 1702包括應用二進位碼108中的複數個虛擬位址偏移，其被映射到對應的目標應用功能。在該點上，應用特定VAFMT 1702包括虛擬位址偏移，而不是直接限定如前述的實際虛擬位址。應當理解的是，虛擬位址偏移限定虛擬位址範圍中的位置差。在一個實施例中，虛擬位址偏移可以限定相對於從應用二進位碼108的起始限定的基礎虛擬位址的位置差，或者在其他實施例中，目標應用功能之間的虛擬位址範圍中的相對差。

【0083】 如圖17中進一步所示，當載入應用軟體時，O/S應用軟體啟動器和載入器1704可以啟動應用軟體的兩個或者更多個實例或者與應用軟體相關聯的程序的兩個或者更多個實例（統稱為「應用程序實例」1708），其是同時執行的。例如，在應用軟體包括網頁瀏覽器的情況下，應用程序實例1708可以包括網頁瀏覽器的多個實例或者多個瀏覽器標籤。在圖17的實施例中，O/S應用軟體啟動器和載入器1704已經啟動三個應用程序實例1708a、1708b和1708c。對於每個應用程序實例1708而言，產生對應的程序特定VAFMT 1714。程序特定VAFMT 1714a是針對應用程序實例1708a產生的。程序特定VAFMT 1714b是針對應用程序實例1708b產生的。程序特定VAFMT 1714c是針對應用程序實例1708c產生的。

【0084】 如圖17的實施例中所示，核心模組1706回應於應用程序實例1708的啟動，可以建立對應的程序特定VAFMT 1714。程序特定VAFMT 1714是使用在應用特定VAFMT 1702中儲存的虛擬位址偏移（元件符號1712）以及由O/S應用軟體啟動器和載入器1704提供的基礎虛擬位址（元件符號1710）來產生的。例如，當啟動應用程序實例1708a時，O/S應用軟體啟動器和載入器1704可以提供應用程序實例1708a已經被載入的虛擬位址基礎。核心模組1706可以經由將虛擬位址偏移加到虛擬位址基礎上，來決定用於目標應用功能的實際虛擬位

址。將所計算的用於應用程序實例1708a的實際虛擬位址儲存在程序特定VAFMT 1714a中。當啟動應用程序實例1708b時，O/S應用軟體啟動器和載入器1704可以提供應用程序實例1708b已經被載入的虛擬位址基礎。核心模組1706可以經由將虛擬位址偏移加到虛擬位址基礎上，來決定用於目標應用功能的實際虛擬位址。將所計算的用於應用程序實例1708b的實際虛擬位址儲存在程序特定VAFMT 1714b中。當啟動應用程序實例1708c時，O/S應用軟體啟動器和載入器1704可以提供應用程序實例1708c已經被載入的虛擬位址基礎。核心模組1706可以經由將虛擬位址偏移加到虛擬位址基礎上，來決定用於目標應用功能的實際虛擬位址。將所計算的用於應用程序實例1708c的實際虛擬位址儲存在程序特定VAFMT 1714c中。

【0085】 以此種方式，程序特定VAFMT 1714a、1714b和1714c包括用於應用程序實例1708a、1708b和1708c的實際虛擬位址，其分別映射到應用二進位碼108中的目標應用功能。在應用程序實例1708a、1708b和1708c的同時執行期間，程序特定VAFMT 1714a、1714b和1714c分別用於以上述方式偵測目標應用功能。應當理解的是，上文結合圖1-圖16所描述的其他映射表（例如，IVAMT 122、「JavaScript原始程式碼列表表」等）的結構可以保持不變。該等映射表可以包括用於應用程序實例1708的唯一實例，其可以利用實際的

程序特定虛擬位址來初始化。在一個實施例中，可以在應用程序執行期間動態地初始化映射表。亦應當理解的是，對虛擬位址的任何程序特定調整（例如，針對諸如ASLR之類的活動等）可以是在程序特定VAFMT實例上並且針對於其他表（例如，IVAMT 122等）完成的，該等其他表是在程序運行時間期間動態地初始化的，因為該等調整是在核心控制之下。應用特定VAFMT 1702具有虛擬位址偏移，其可以不需要針對ASLR和其他活動進行調整。

【0086】 圖18圖示應用特定VAFMT 1702的示例性實施例。應當理解的是，應用特定VAFMT 1702可以以與VAFMT 120相同的方式進行配置，除了列1800定義虛擬位址偏移，而不是像在VAFMT 120中定義實際虛擬位址。在該點上，圖18圖示與應用二進位碼108中的代碼相關聯的虛擬位址偏移（列1800）到該代碼在彼等虛擬位址偏移處表示的相應的功能含義（在列1802中辨識的功能興趣點）的邏輯映射。應用特定VAFMT 1702可以類似地包括中繼資料（列1804），中繼資料與偽二進位碼範本1202相結合地使用，以使得HLOS 106能夠在利用新版本更新應用二進位碼108時，決定用於功能興趣點（列1802）的新虛擬位址偏移。

【0087】 圖19圖示程序特定VAFMT 1714的示例性實施例。程序特定VAFMT 1714可以包括列1802和1804，其以與應用特定VAFMT 1702相同的方式分別辨識功能興趣點和中繼資料。如圖19中所示，程序特定

VAFMT 1714可以包括列1900，其用於儲存用於對應的應用程序實例1708的實際虛擬位址，而不是應用特定VAFMT 1702中所辨識的虛擬位址偏移。核心模組1706可以使用在應用特定VAFMT 1702中儲存的虛擬位址偏移以及由O/S應用軟體啟動器和載入器1704提供的基礎虛擬位址，來決定列1900中儲存的用於實際虛擬位址的值。在圖19的實例中，可以從具有值0x30000000的基礎虛擬位址載入應用程序實例1708。核心模組1706可以接收該基礎虛擬位址值，並且作為回應，計算用於應用程序實例1708的實際虛擬位址。參照圖18中的應用特定VAFMT 1702中的第一行，EVAL_FUNCTION（列1802）可以具有虛擬位址偏移值0x373ea94（列1800）。為了計算EVAL_FUNCTION在應用程序實例1708中的實際虛擬位址，核心模組1706可以將基礎虛擬位址值（0x30000000）與虛擬位址偏移值（0x373ea94）相加。如圖19的第一行中所示，所計算的用於EVAL_FUNCTION的實際虛擬位址具有值0x3373ea94（值0x30000000和0x373ea94的總和）。在圖19的第二行中，所計算的用於DOCUMENT_WRITE_FUNCTION_START的實際虛擬位址具有值0x3473fac8（值0x30000000和0x473fac8的總和）。應當理解的是，用於圖19中的剩餘行的實際虛擬位址可以類似地根據等式1來計算並且被儲存在列1900中。

實際VA=基礎VA+虛擬位址偏移

等式1

【0088】 上文示例性實施例採用了加法運算來計算實際虛擬位址。然而，應當理解的是，在其他實施例中，可以根據例如用於計算的約定、用於特定作業系統/平臺的記憶體分配的方向（例如，朝向較高或者較低位址）等，經由將虛擬位址偏移從基礎虛擬位址中減去，來獲得實際虛擬位址。

【0089】 圖20圖示應用特定VAFMT 2000的另一實施例，應用特定VAFMT 2000包括使用虛擬位址偏移的URL緩衝器虛擬位址映射。應用特定VAFMT 2000通常與圖11中圖示的VAFMT 120相對應，除了該表儲存虛擬位址偏移，而不是實際虛擬位址。在該點上，應用特定版本包括定製虛擬位址偏移表，其具有用於特定緩衝器分配器函數的虛擬位址偏移，該等虛擬位址偏移可以用於決定被動態分配的緩衝器（其包括特定資料結構類型（例如，類、結構體、聯合體）的物件）的起始和結束的虛擬位址。圖20的URL緩衝器虛擬位址映射包括用於使用內置HTTPS堆疊的應用軟體的單獨的行（列2002）。第一行定義用於第一此種應用軟體（應用軟體-1）的URL緩衝器虛擬位址映射，並且第二行定義用於第二此種應用軟體（應用軟體-2）的URL緩衝器虛擬位址映射。列2004儲存應用軟體-1和應用軟體-2的虛擬位址偏移值，以用於函數執行例如URL資料結構分配。列2006、2008、

2010、2012、2014和2016與圖11中的列1104、1106、1108、1110、1112和1114直接對應。在該點上，應當理解的是，可以使用偏移和長度欄位來決定在緩衝器中分配的物件的成員/欄位的值，偏移和長度欄位亦可以是在用於作為興趣點的特定欄位/成員的表中維護的。緩衝器分配函數的虛擬位址可以用於經由例如追蹤來自由分配器函數的虛擬位址覆蓋的區域的系統記憶體分配器函數的執行，來偵測所分配的緩衝器的大小和位址。一旦已知緩衝器起始和結束虛擬位址，偏移和長度欄位就可以用於決定用於特定資料結構類型的物件的特定成員/欄位的值。

【0090】 圖21和圖22圖示分別針對應用軟體-1和應用軟體-2產生的程序特定VAFMT 2100和2200的實施例。使用圖20中的虛擬位址偏移值（列2004）以及應用軟體-1和應用軟體-2分別由OS應用軟體啟動器/載入器1704載入的基礎虛擬位址，來產生程序特定VAFMT 2100和2200。根據上文等式1而計算的用於應用軟體-1的實際虛擬位址被儲存在列2102中（圖21），而用於應用軟體-2的實際虛擬位址被儲存在列2202中。

【0091】 圖23是圖示用於使用上文結合圖17-圖22所描述的基於偏移的虛擬位址映射來偵測目標應用功能的方法2300的實施例的流程圖。在方塊2302處，產生用於應用軟體的應用特定VAFMT 1702。如前述，應用特定VAFMT 1702包括感興趣的複數個虛擬位址偏移，其被

映射到對應的高級應用功能。在方塊2304處，可以在計算設備（例如，可攜式計算設備）上安裝該應用軟體。在方塊2306處，可以對該應用軟體進行註冊，以用於由HLOS 106提供的安全性支援（例如，註冊應用軟體112）。在方塊2308處，可以啟動該應用軟體。回應於啟動該應用軟體，可以產生用於該應用軟體的實例或者應用程序實例1708的程序特定VAFMT 1714。程序特定VAFMT 1714使用在應用特定VAFMT 1702中儲存的虛擬位址偏移以及該應用軟體或者實例從其被載入的基礎虛擬位址，來定義高級應用功能的實際虛擬位址。應用二進位碼108可以開始執行。

【0092】 在方塊2310處，HLOS 106可以攔截應用軟體的正在執行的程序。在方塊2312處，HLOS 106可以使用程序特定VAFMT 1714來在功能興趣點被執行時偵測和記錄該等功能興趣點。在方塊2314處，可以將所記錄的點提供給惡意程式碼偵測演算法116，以偵測和解決惡意攻擊。惡意程式碼偵測演算法116可以包括基於簽名的演算法、模式匹配演算法，或者採用機器學習或者其他技術。如元件符號2318所示，可以針對多個應用程序實例，重複方塊2308、2310、2312、2314和2316，以使得可以針對同時執行的應用程序實例來偵測惡意程式碼。

【0093】 應當理解的是，可以將本文描述的方法步驟中的一或多個步驟作為電腦程式指令（例如，上述模組）儲

存在記憶體中。可以由任何適當的處理器與對應的模組結合或者合作來執行該等指令，以執行本文所描述的方法。

【0094】 在本說明書中描述的各程序或者各程序流程中的某些步驟自然而然地在其他步驟之前，以便本發明如所描述地運作。然而，本發明並不限於所描述的步驟的次序，若此種次序或者順序不改變本發明的功能。亦即，應認識到的是，在不脫離本發明的範疇和精神的情況下，一些步驟可以在其他步驟之前、之後或者與其並行地（與其基本上同時）執行。在一些實例中，可以在不脫離本發明的情況下，省略或者不執行某些步驟。此外，諸如「之後」、「隨後」、「接下來」等的詞並不意欲限制該等步驟的次序。該等詞僅用於引導讀者通讀示例性方法的描述。

【0095】 此外，一般技術者在程式設計時能夠毫無困難地基於例如本說明書中的流程圖以及相關聯的描述，編寫電腦代碼，或者辨識合適的硬體及/或電路，來實現所揭示的發明。

【0096】 因此，特定程式碼指令集或者詳細的硬體設備的揭示並不被視為對於充分地理解如何實現和使用本發明而言是必需的。在上文描述中並且結合可以圖示各個程序流程的圖，更加詳細地解釋了所發明的、所主張保護的電腦實現的程序的功能。

【0097】 在一或多個示例性態樣中，所描述的功能可以用硬體、軟體、韌體，或其任意組合來實現。若用軟體來實現，該等功能可以被儲存在電腦可讀取媒體上或作為電

腦可讀取媒體上的一或多個指令或代碼進行傳輸。電腦可讀取媒體包括電腦儲存媒體和通訊媒體二者，通訊媒體包括促進將電腦程式從一個地方傳輸到另一個地方的任何媒體。儲存媒體可以是能夠由電腦存取的任何可用媒體。經由舉例而非限制的方式，此種電腦可讀取媒體可以包括RAM、ROM、EEPROM、NAND快閃記憶體、NOR快閃記憶體、M-RAM、P-RAM、R-RAM、CD-ROM或其他光碟儲存、磁碟儲存或其他磁儲存設備，或者可以用於攜帶或儲存具有指令或資料結構形式的期望程式碼並且可以被電腦存取的任何其他媒體。

【0098】 另外，任何連接被適當地稱為電腦可讀取媒體。例如，若利用同軸電纜、光纖電纜、雙絞線、數位用戶線路（「DSL」）或無線技術（例如，紅外線、無線電和微波）從網站、伺服器或其他遠端源傳輸軟體，則同軸電纜、光纖電纜、雙絞線、DSL或無線技術（例如，紅外線、無線電和微波）被包括在媒體的定義中。

【0099】 如本文中所使用的，磁碟（disk）和光碟（disc）包括壓縮光碟（「CD」）、鐳射光碟、光碟、數位多功能光碟（「DVD」）、軟碟和藍光光碟，其中磁碟通常磁性地複製資料，而光碟則用鐳射來光學地複製資料。上述各項的組合亦應當包括在電腦可讀取媒體的範疇之內。

【0100】 對於一般技術者而言，在不脫離其精神和範疇的情況下，本發明涉及的替代實施例將變得顯而易見。因

此，儘管已經圖示並且詳細地描述了所選擇的態樣，但是將理解的是，可以在不脫離本發明的精神和範疇（如以下請求項所定義的）的情況下在其中進行各種替換和改變。

【符號說明】

【0101】

100 系統

102 中央處理單元（CPU）

104 記憶體

106 高級作業系統（HLOS）

108 應用二進位碼

110 參考應用原始程式碼

112 註冊應用軟體

114 可信區

116 惡意程式碼偵測演算法

118 虛擬機器

120 虛擬位址到函數映射表/VAFMT

122 辨識符到位址映射表（IVAMT）

200 邏輯映射

201 點

202 虛擬位址

203 點

204 虛擬位址

205 點

206 虛擬位址

300 邏輯映射

302 列

304 列

400 方法

402 方塊

404 方塊

406 方塊

408 方塊

410 方塊

412 方塊

414 方塊

416 方塊

500 邏輯映射

502 虛擬位址

504 虛擬位址

600 邏輯映射

602 虛擬位址

604 巨集名稱

704a VM堆代碼空間

704b VM堆代碼空間

900 VM堆結構

901 虛擬記憶體位址

902 代碼欄位/子區域

904 映射欄位/子區域

906 大物件欄位/子區域

908 舊資料欄位/子區域

910 舊指標欄位/子區域

912 始於欄位/子區域

914 至欄位/子區域

1000 方法

1002 方塊

1004 方塊

1006 方塊

1008 方塊

1010 方塊

1012 方塊

1014 方塊

1016 方塊

1018 方塊

1020 方塊

1104 列

1106 列

1108 列

1110 列

1112 列

1114 列

1200 中繼資料

1202 偽二進位碼範本

1204 經更新的版本

1206 所匹配的區域

1600 方法

1602 方塊

1604 決策方塊

1605 方塊

1606 方塊

1607 決策方塊

1608 決策方塊

1609 方塊

1610 方塊

1611 決策方塊

1612 方塊

1613 方塊

1700 基於偏移的虛擬位址映射方案

1702 應用特定VAFMT

1704 O/S應用軟體啟動器和載入器

1706 核心模組

1708A 應用程序實例

1708B 應用程序實例

1708C 應用程序實例

1710 基礎虛擬位址

1714 程序特定VAFMT

1714A 程序特定VAFMT

1714B 程序特定VAFMT

1714C 程序特定VAFMT

1800 列

1802 列

1804 列

1900 列

2000 應用特定VAFMT

2002 列

2004 列

2006 列

2008 列

2010 列

2012 列

2014 列

2016 列

2100 程序特定VAFMT

2102 列

2200 程序特定VAFMT

2202 列

2300 方法

2302 方塊

2304 方塊

2306 方塊

2308 方塊

2310 方塊

2312 方塊

2314 方塊

2316 方塊

2318 方塊

【生物材料寄存】

【0102】 國內寄存資訊(請依寄存機構、日期、號碼順序註記)

無

【0103】 國外寄存資訊(請依寄存國家、機構、日期、號碼順序註記)

無

【發明申請專利範圍】

【第1項】一種用於偵測在一計算設備上執行的一應用軟體的高級功能的方法，該方法包括以下步驟：

將用於一應用軟體的一應用特定虛擬位址映射表儲存在一計算設備上的一安全記憶體中，該應用特定虛擬位址映射表包括在應用二進位碼中被映射到該應用軟體的原始程式碼中相對應的目標應用功能的複數個虛擬位址偏移；

回應於啟動該應用軟體，產生用於將被執行的一應用程序的一實例的一程序特定虛擬位址映射表，該程序特定虛擬位址映射表使用該應用特定虛擬位址映射表中的該等虛擬位址偏移來定義與該等目標應用功能相對應的實際虛擬位址；

在用於該應用程序的該實例的該應用二進位碼的執行期間，基於該程序特定虛擬位址映射表，來偵測與該等目標應用功能相對應的該等實際虛擬位址中的一或多個實際虛擬位址被執行；及

將從該程序特定虛擬位址映射表中的該等實際虛擬位址偵測到的所執行的該等目標應用功能提供到一異常處理模組中，該異常處理模組被配置為偵測與用於該應用程序的該實例的該應用二進位碼的執行相關聯的一或多個異常或者行為，其中該異常處理模組包括

一惡意程式碼偵測演算法。

【第2項】 根據請求項1之方法，亦包括以下步驟：

產生用於該應用程序的另一實例的另一程序特定虛擬位址映射表，該應用程序的該另一實例將與該應用程序的其他實例被同時執行；

在用於該應用程序的該另一實例的該應用二進位碼的執行期間，基於該另一程序特定虛擬位址映射表，來偵測與該等目標應用功能相對應的該等實際虛擬位址中的一或多個實際虛擬位址何時被執行。

【第3項】 根據請求項1之方法，其中該等實際虛擬位址是使用用於該應用程序的該實例的一基礎虛擬位址以及該應用特定虛擬位址映射表中的該等虛擬位址偏移來決定的。

【第4項】 根據請求項1之方法，其中該安全記憶體位於一高級作業系統(high-level operating system，HLOS）中的一可信區中。

【第5項】 根據請求項1之方法，其中該應用軟體包括一安全網頁應用軟體和一網頁瀏覽器中的一項。

【第6項】 根據請求項1之方法，其中該應用二進位碼是作為本機（native）二進位碼來執行的。

【第7項】 一種用於偵測在一計算設備上執行的一應用軟體的高級功能的系統，該系統包括：

用於將用於一應用軟體的一應用特定虛擬位址映射表儲存在一計算設備上的構件，該應用特定虛擬位址映射表包括在應用二進位碼中被映射到該應用軟體的原始程式碼中相對應的目標應用功能的複數個虛擬位址偏移；

用於回應於啟動該應用軟體，產生用於將被執行的一應用程序的一實例的一程序特定虛擬位址映射表的構件，該程序特定虛擬位址映射表使用該應用特定虛擬位址映射表中的該等虛擬位址偏移來定義與該等目標應用功能相對應的實際虛擬位址；

用於在用於該應用程序的該實例的該應用二進位碼的執行期間，基於該程序特定虛擬位址映射表，來偵測與該等目標應用功能相對應的該等實際虛擬位址中的一或多個實際虛擬位址被執行的構件；及

用於將從該程序特定虛擬位址映射表中的該等實際虛擬位址偵測到的所執行的該等目標應用功能提供到一異常處理模組中的構件，該異常處理模組被配置為偵測與用於該應用程序的該實例的該應用二進位碼的執行相關聯的一或多個異常或者行為，其中該異常處理模組包括一惡意程式碼偵測演算法。

【第8項】 根據請求項7之系統，亦包括：

用於產生用於該應用程序的另一實例的另一程序特

定虛擬位址映射表的構件，該應用程序的該另一實例將與該應用程序的其他實例被同時執行；

用於在用於該應用程序的該另一實例的該應用二進位碼的執行期間，基於該另一程序特定虛擬位址映射表，來偵測與該等目標應用功能相對應的該等實際虛擬位址中的一或多個實際虛擬位址何時被執行的構件。

【第9項】 根據請求項 7 之系統，其中該等實際虛擬位址是使用用於該應用程序的該實例的一基礎虛擬位址以及該應用特定虛擬位址映射表中的該等虛擬位址偏移來決定的。

【第10項】 根據請求項 7 之系統，其中該用於儲存的構件位於一高級作業系統（high-level operating system，HLOS）中的一可信區中。

【第11項】 根據請求項 7 之系統，其中該應用軟體包括一安全網頁應用軟體和一網頁瀏覽器中的一項。

【第12項】 根據請求項 7 之系統，其中該應用二進位碼是作為本機（native）二進位碼來執行的。

【第13項】 一種電腦程式，其實施在一記憶體中並且包括一非暫態電腦可讀取媒體，該電腦可讀取媒體具有電腦可讀取程式碼實施於其中，該等電腦可讀取程式碼可由一處理器執行以用於偵測在一計算設備上執

行的一應用軟體的高級功能，該電腦程式包括被配置為進行以下操作的邏輯單元：

將用於一應用軟體的一應用特定虛擬位址映射表儲存在一計算設備上的一安全記憶體中，該應用特定虛擬位址映射表包括在應用二進位碼中被映射到該應用軟體的原始程式碼中相對應的目標應用功能的複數個虛擬位址偏移；

回應於啟動該應用軟體，產生用於將被執行的一應用程序的一實例的一程序特定虛擬位址映射表，該程序特定虛擬位址映射表使用該應用特定虛擬位址映射表中的該等虛擬位址偏移來定義與該等目標應用功能相對應的實際虛擬位址；

在用於該應用程序的該實例的該應用二進位碼的執行期間，基於該程序特定虛擬位址映射表，來偵測與該等目標應用功能相對應的該等實際虛擬位址中的一或多個實際虛擬位址被執行；及

將從該程序特定虛擬位址映射表中的該等實際虛擬位址偵測到的所執行的該等目標應用功能提供到一異常處理模組中，該異常處理模組被配置為偵測與用於該應用程序的該實例的該應用二進位碼的執行相關聯的一或多個異常或者行為，其中該異常處理模組包括一惡意程式碼偵測演算法。

【第14項】 根據請求項13之電腦程式，亦包括被配置為進行以下操作的邏輯單元：

產生用於該應用程序的另一實例的另一程序特定虛擬位址映射表，該應用程序的該另一實例將與該應用程序的其他實例被同時執行；

在用於該應用程序的兩個實例的該應用二進位碼的同時執行期間，基於該另一程序特定虛擬位址映射表，來偵測與該等目標應用功能相對應的該等實際虛擬位址中的一或多個實際虛擬位址何時被執行。

【第15項】 根據請求項13之電腦程式，其中該等實際虛擬位址是使用用於該應用程序的該實例的一基礎虛擬位址以及該應用特定虛擬位址映射表中的該等虛擬位址偏移來決定的。

【第16項】 根據請求項13之電腦程式，其中該安全記憶體位於一高級作業系統（high-level operating system，HLOS）中的一可信區中。

【第17項】 根據請求項13之電腦程式，其中該應用軟體包括一安全網頁應用軟體和一網頁瀏覽器中的一項。

【第18項】 根據請求項13之電腦程式，其中該應用二進位碼是作為本機（native）二進位碼來執行的。

【第19項】 一種用於偵測正在執行的一應用軟體的高

級功能的系統，該系統包括：

一處理設備，其被配置為執行應用二進位碼；及

一高級作業系統(high-level operating system，HLOS），其包括：

一應用特定虛擬位址映射表，其包括在應用二進位碼中被映射到該應用軟體的原始程式碼中相對應的目標應用功能的複數個虛擬位址偏移；及

一核心模組，其被配置為：回應於啟動該應用軟體，產生用於將被執行的一應用程序的一實例的一程序特定虛擬位址映射表，該程序特定虛擬位址映射表使用該應用特定虛擬位址映射表中的該等虛擬位址偏移來定義與該等目標應用功能相對應的實際虛擬位址；

該HLOS被配置為：在用於該應用程序的該實例的該應用二進位碼的執行期間，基於該程序特定虛擬位址映射表，來偵測與該等目標應用功能相對應的該等實際虛擬位址中的一或多個實際虛擬位址被執行；及

該HLOS將從該程序特定虛擬位址映射表中的該等實際虛擬位址偵測到的所執行的該等目標應用功能提供到一異常處理模組中，該異常處理模組被配置為偵測與用於該應用程序的該實例的該應用二進位碼的執行相關聯的一或多個異常或者行為，其中該異常處理

模組包括一惡意程式碼偵測演算法。

【第20項】 根據請求項19之系統，其中該HLOS亦被配置為：

產生用於該應用程序的另一實例的另一程序特定虛擬位址映射表，該應用程序的該另一實例將與該應用程序的其他實例被同時執行；及

在用於該應用程序的兩個實例的該應用二進位碼的同時執行期間，基於該另一程序特定虛擬位址映射表，來偵測與該等目標應用功能相對應的該等實際虛擬位址中的一或多個實際虛擬位址何時被執行。

【第21項】 根據請求項20之系統，其中該等實際虛擬位址是使用用於該應用程序的該實例的一基礎虛擬位址以及該應用特定虛擬位址映射表中的該等虛擬位址偏移來決定的。

【第22項】 根據請求項20之系統，其中該應用特定虛擬位址映射表被儲存在該HLOS中的一可信區中。

【發明圖式】

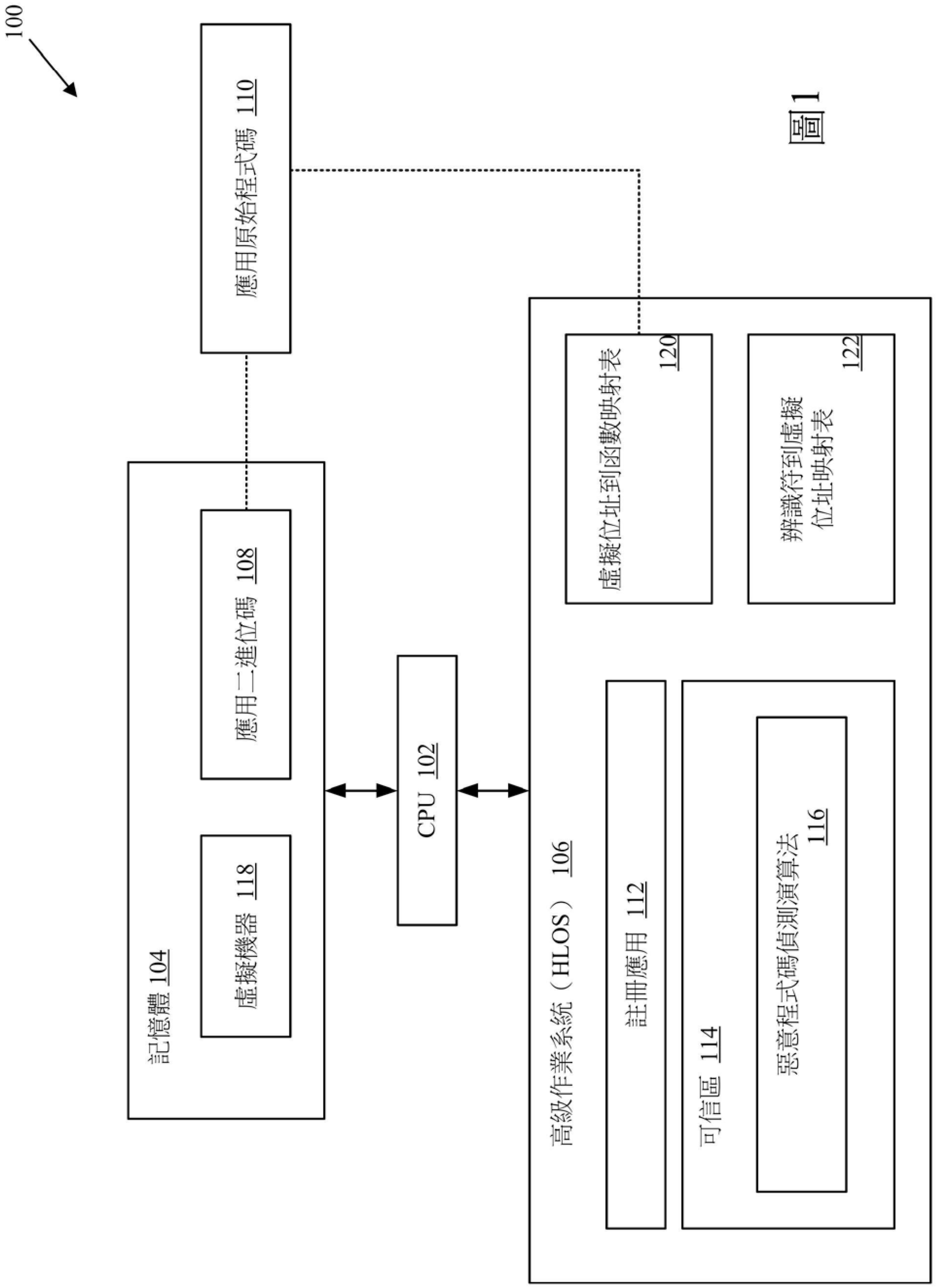

100
記憶體 104
虛擬機器 118
應用二進位碼 108
應用原始程式碼 110
CPU 102
高級作業系統（HLOS） 106
虛擬位址到函數映射表 120
辨識符到虛擬位址映射表 122
註冊應用 112
可信區 114
惡意程式碼偵測演算法 116

圖1

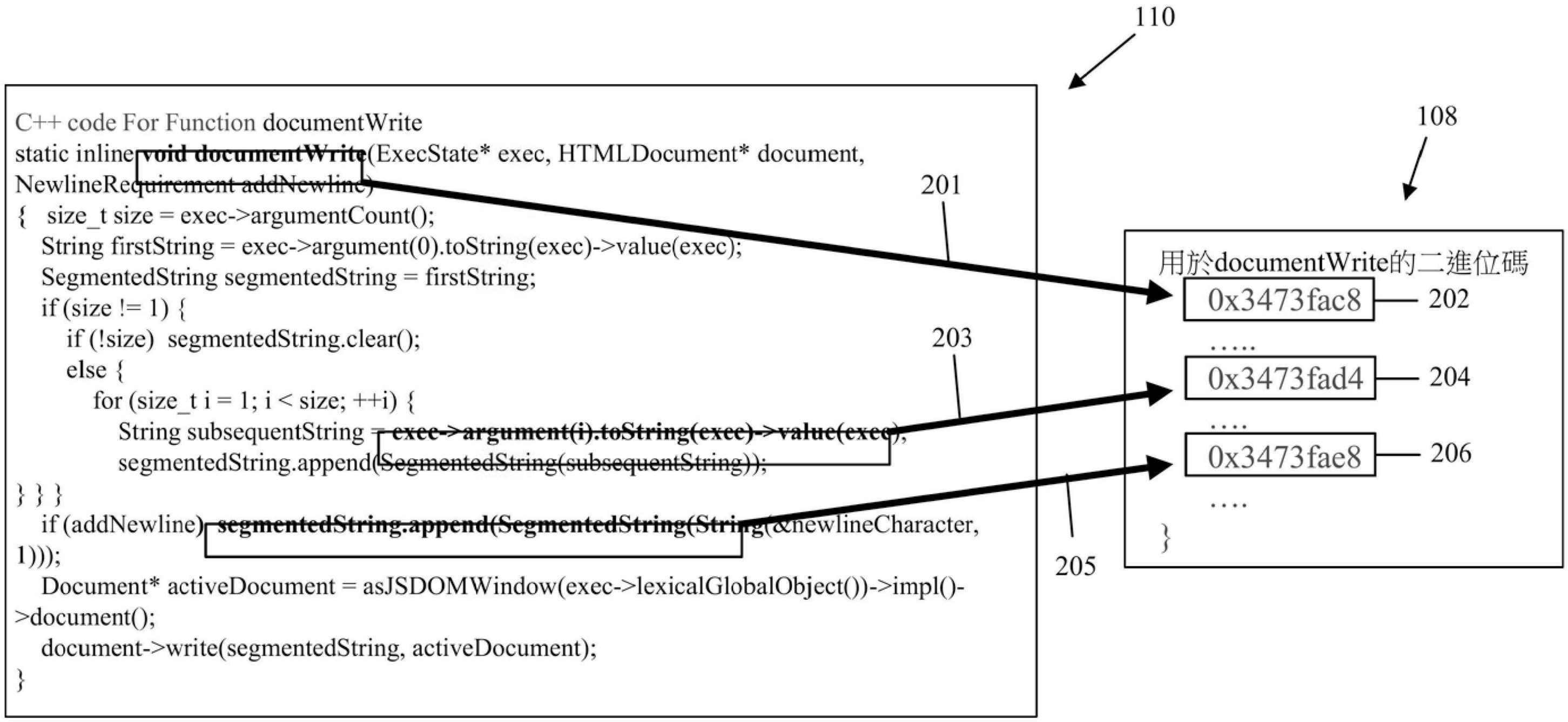

110
C++ code For Function documentWrite
static inline void documentWrite(ExecState* exec, HTMLDocument* document,
NewlineRequirement addNewline)
{ size_t size = exec->argumentCount();
String firstString = exec->argument(0).toString(exec)->value(exec);
SegmentedString segmentedString = firstString;
if (size != 1) {
if (!size) segmentedString.clear();
else {
for (size_t i = 1; i < size; ++i) {
String subsequentString = exec->argument(i).toString(exec)->value(exec);
segmentedString.append(SegmentedString(subsequentString));
} } }
if (addNewline) segmentedString.append(SegmentedString(String(&newlineCharacter,
1)));
Document* activeDocument = asJSDOMWindow(exec->lexicalGlobalObject())->impl()-
>document();
document->write(segmentedString, activeDocument);
}
201
203
205
108
用於documentWrite的二進位碼
0x3473fac8
202
0x3473fad4
204
0x3473fae8
206
}
200

圖2

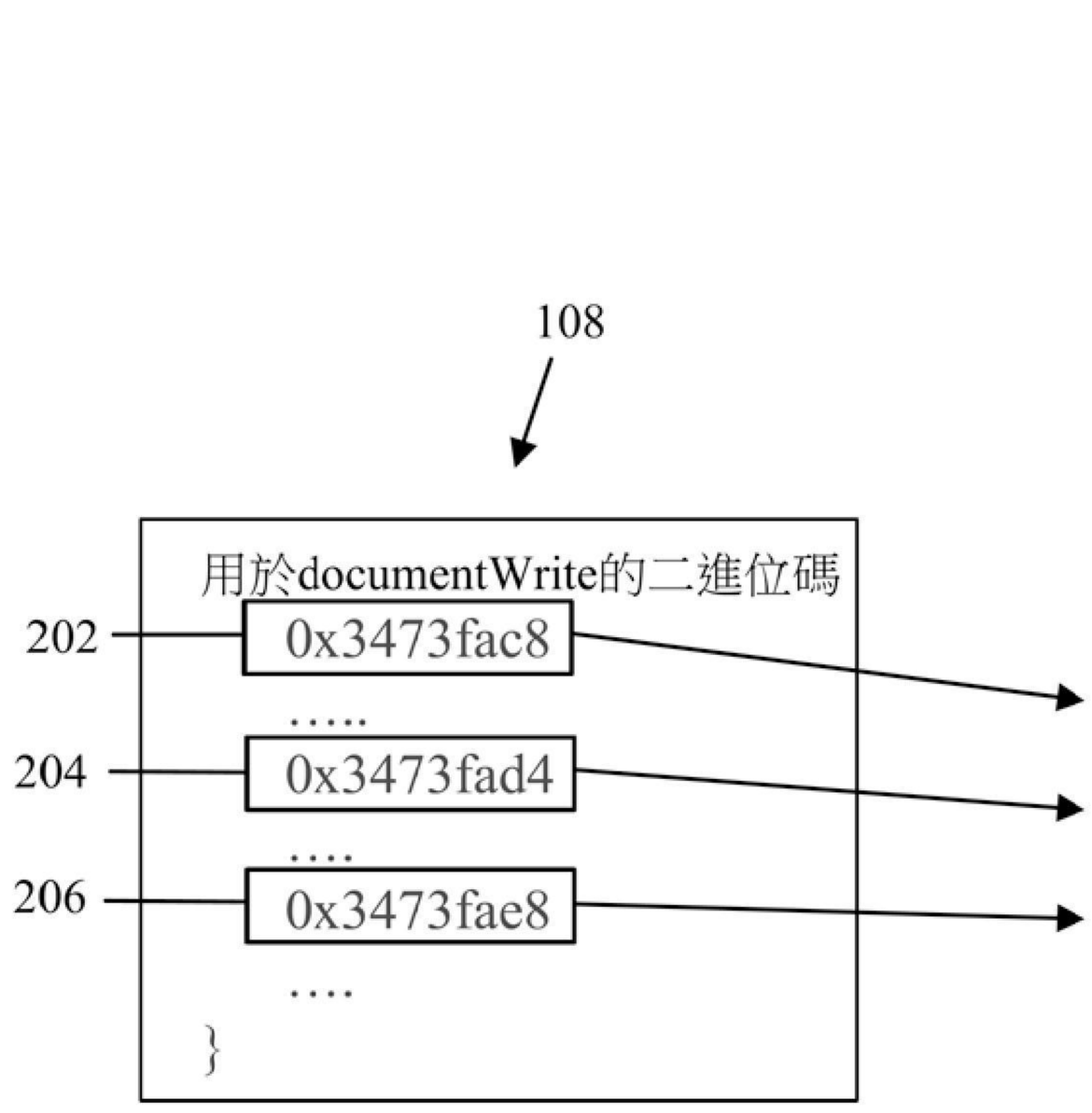

300
108
用於documentWrite的二進位碼
202
0x3473fac8
.....
204
0x3473fad4
....
206
0x3473fae8
....
}
虛擬位址到函數映射表 120
虛擬位址 302
功能興趣點 304
0x3273fa94
EVAL_FUNCTION
0x3473fac8
DOCUMENT_WRITE_FUNCTION_START
0x3473fad4
DOCUMENT_WRITE_1
0x3473fae8
DOCUMENT_WRITE_2
0x29b93420
ONCLICK_FUNCTION
0x59d782b4
DOCUMENT_COOKIE_FUNCTION
0x59d78264
SETTIMEOUT_FUNCTION_START

圖3

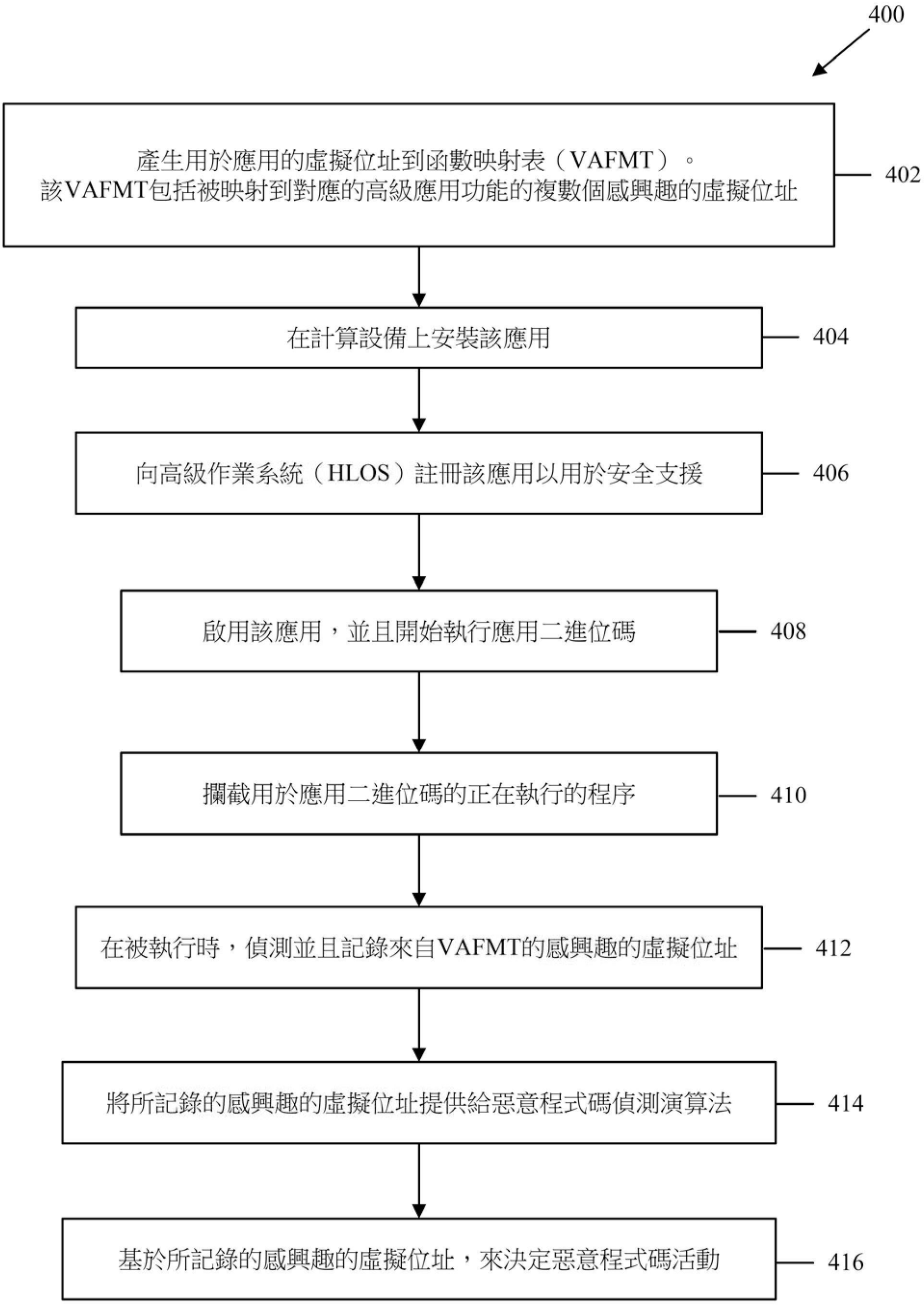
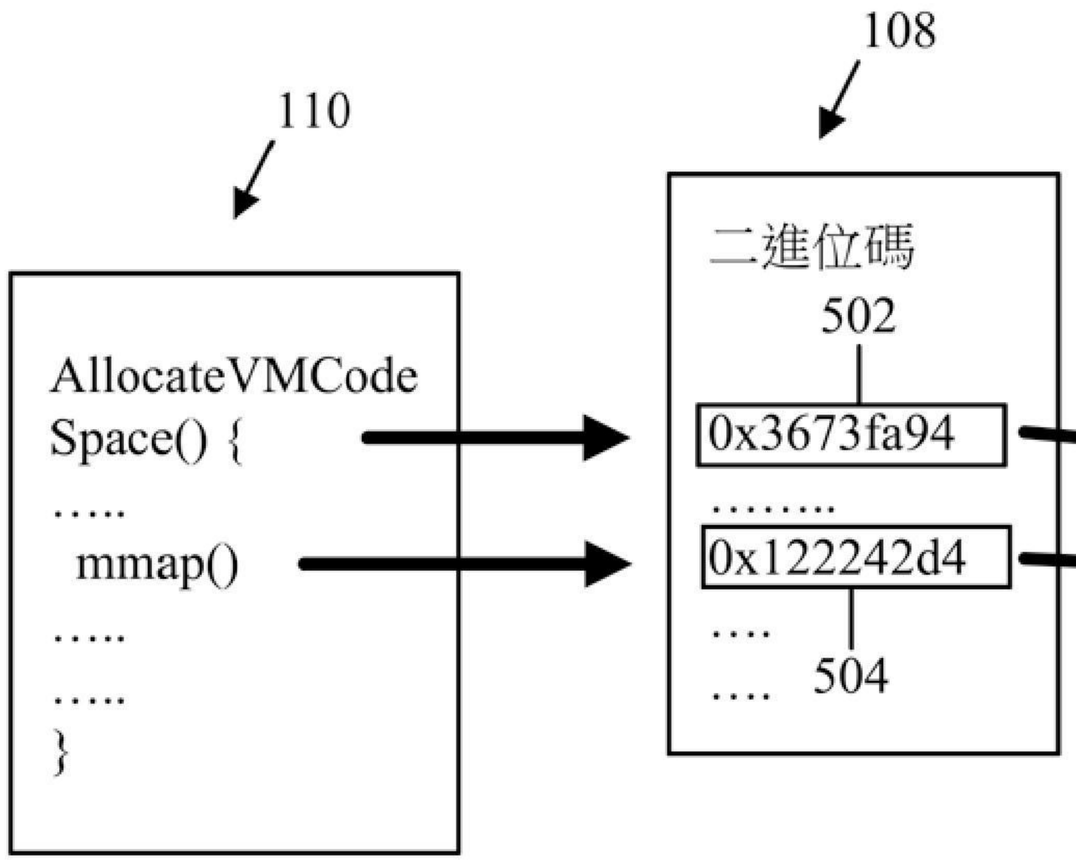

400
產生用於應用的虛擬位址到函數映射表（VAFMT）。
該VAFMT包括被映射到對應的高級應用功能的複數個感興趣的虛擬位址
402
在計算設備上安裝該應用
404
向高級作業系統（HLOS）註冊該應用以用於安全支援
406
啟用該應用，並且開始執行應用二進位碼
408
攔截用於應用二進位碼的正在執行的程序
410
在被執行時，偵測並且記錄來自VAFMT的感興趣的虛擬位址
412
將所記錄的感興趣的虛擬位址提供給惡意程式碼偵測演算法
414
基於所記錄的感興趣的虛擬位址，來決定惡意程式碼活動
416

圖4

圖5



500

虛擬位址到函數映射表 **120**	
虛擬位址 302	功能興趣點 304
0x3273fa94	EVAL_FUNCTION
0x3473fac8	DOCUMENT_WRITE_FUNCTION_START
0x3473fad4	DOCUMENT_WRITE_1
0x3473fae8	DOCUMENT_WRITE_2
0x29b93420	ONCLICK_FUNCTION
0x59d782b4	DOCUMENT_COOKIE_FUNCTION
0x59d78264	SETTIMEOUT_FUNCTION_START
0x3673fa94	VM_CODE_SPACE_ALLOCATOR
0x122242d4	KERNEL_ALLOCATOR_FUNCTION
0x3673fad4	VM_CODE_SPACE_DEALLOCATOR
0x122243e4	KERNEL_DEALLOCATOR_FUNCTION

圖6

600

虛擬位址到函數映射表 **120**	
虛擬位址 302	功能興趣點 304
0x3273fa94	EVAL_FUNCTION
0x3473fac8	DOCUMENT_WRITE_FUNCTION_START
0x3473fad4	DOCUMENT_WRITE_1
0x3473fae8	DOCUMENT_WRITE_2
0x29b93420	ONCLICK_FUNCTION
0x59d782b4	DOCUMENT_COOKIE_FUNCTION
0x59d78264	SETTIMEOUT_FUNCTION_START
0x3673fa94	VM_CODE_SPACE_ALLOCATOR
0x122242d4	KERNEL_ALLOCATOR_FUNCTION
0x3673fad4	VM_CODE_SPACE_DEALLOCATOR
0x122243e4	KERNEL_DEALLOCATOR_FUNCTION

辨識符到虛擬位址映射表 **122**	
巨集含義 604	虛擬位址 602
VM_CODE_SPACE_START	0x2fa2ca08
VM_CODE_SPACE_END	0x3473fa80
VM_LARGE_OBJ_SPACE_START	
VM_LARGE_OBJ_SPACE_END	
VM_NEWSPACE_START	0x3663fa80
VM_NEWSPACE_END	0x3663fbb8

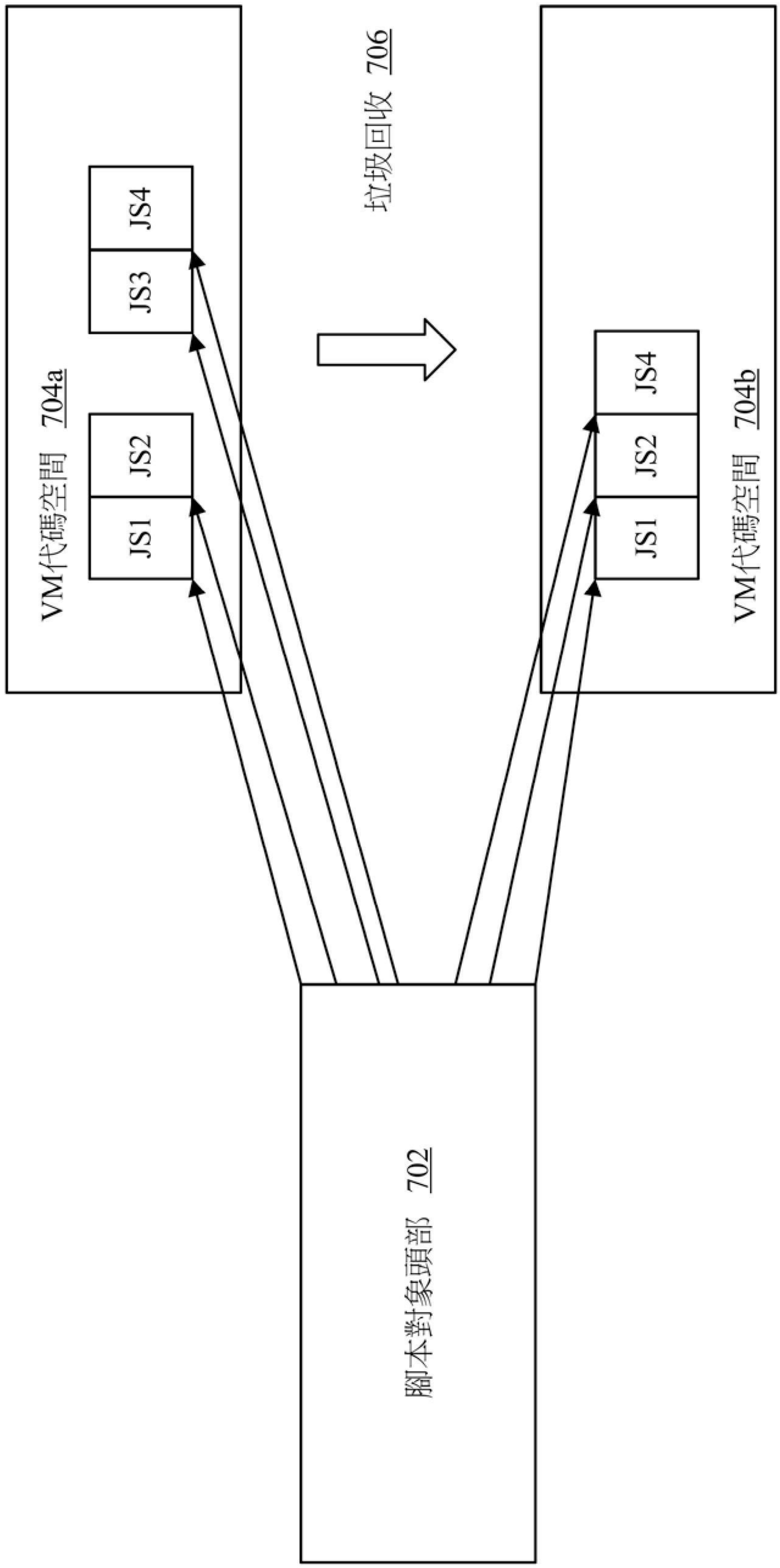

700
腳本對象頭部 702
垃圾回收 706
VM代碼空間 704a
JS1
JS2
JS3
JS4
VM代碼空間 704b
JS1
JS2
JS4

圖7

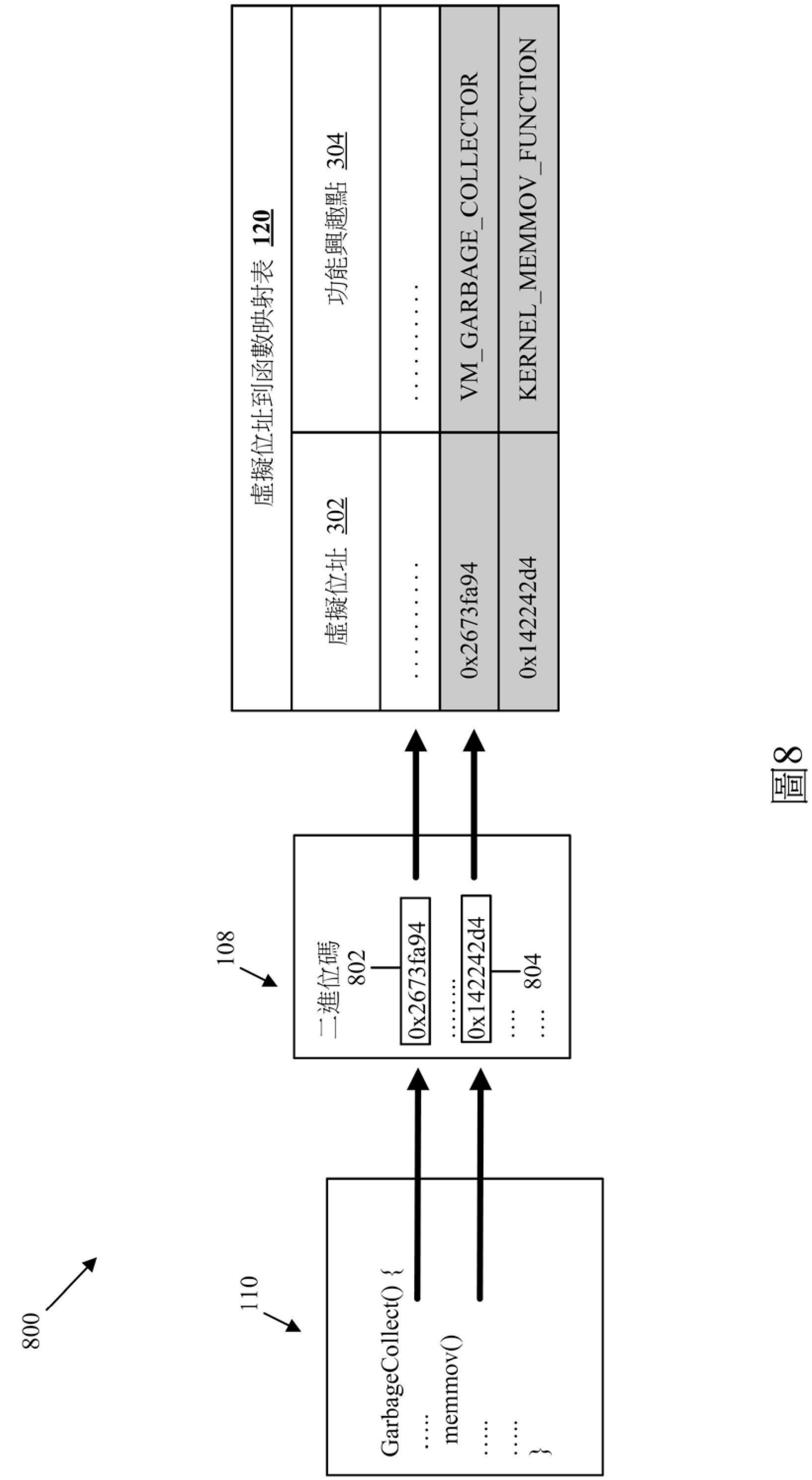

虛擬位址到函數映射表 120
虛擬位址 302
功能興趣點 304
0x2673fa94
VM_GARBAGE_COLLECTOR
0x142242d4
KERNEL_MEMMOV_FUNCTION
108
二進位碼
802
0x2673fa94
0x142242d4
804
800
110
GarbageCollect() {
memmov()
}

圖8

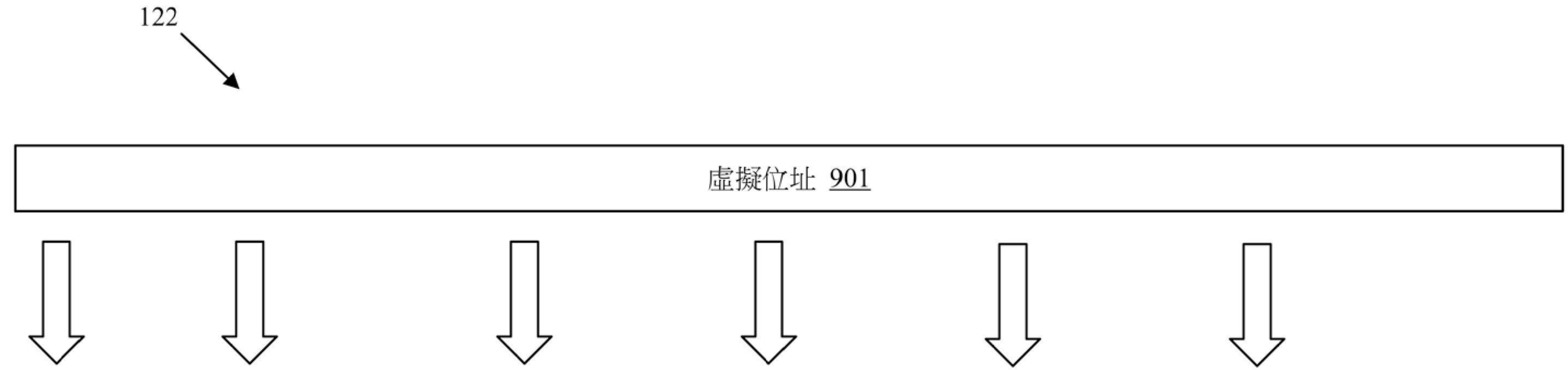

122
虛擬位址 901
始於 912
至 914
代碼 902
（JIT ASM二進位、元組代碼）
映射 904
（物件佈局資訊）
大對象 906
舊資料 908
（例如，字串）
舊指標 910
（例如，指向其他的物件）
900

圖9

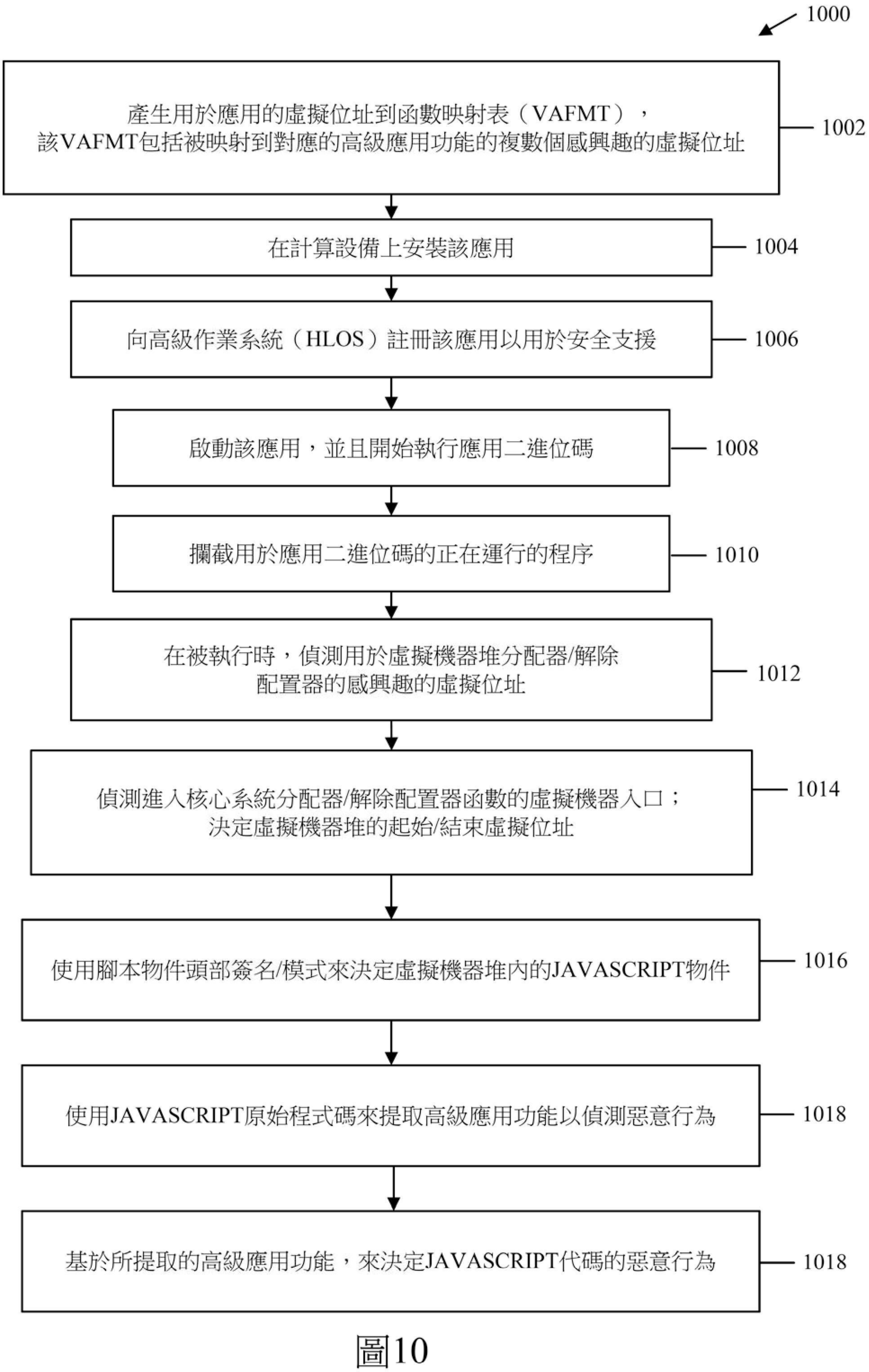

1000
產生用於應用的虛擬位址到函數映射表（VAFMT），
該VAFMT包括被映射到對應的高級應用功能的複數個感興趣的虛擬位址
1002
在計算設備上安裝該應用
1004
向高級作業系統（HLOS）註冊該應用以用於安全支援
1006
啟動該應用，並且開始執行應用二進位碼
1008
攔截用於應用二進位碼的正在運行的程序
1010
在被執行時，偵測用於虛擬機器堆分配器/解除
配置器的感興趣的虛擬位址
1012
偵測進入核心系統分配器/解除配置器函數的虛擬機器入口；
決定虛擬機器堆的起始/結束虛擬位址
1014
使用腳本物件頭部簽名/模式來決定虛擬機器堆內的JAVASCRIPT物件
1016
使用JAVASCRIPT原始程式碼來提取高級應用功能以偵測惡意行為
1018
基於所提取的高級應用功能，來決定JAVASCRIPT代碼的惡意行為
1018

圖10

120

1104

1112

具有偏移和長度的自訂虛擬位址映射表						
用於進行緩衝器或者資料結構分配的網頁/瀏覽器應用函數的虛擬位址 （離線/靜態地決定以及OTA更新） 1102	用於從進行緩衝器或者資料結構分配的應用函式撥叫的「核心系統分配器」的虛擬位址 （在應用的動態載入期間決定的）	緩衝器起始虛擬位址 （動態地決定） 1106	緩衝器結束虛擬位址 （動態地決定） 1108	所分配的緩衝器資料結構內的成員欄位/指標偏移 （離線/靜態地決定以及OTA更新） （可選） 1110	所分配的緩衝器資料結構內的成員欄位/指標的以位元組為單位的長度 （離線/靜態地決定以及OTA更新） （可選）	成員欄位是指標嗎 （離線/靜態地決定以及OTA更新） （可選） 1114
0x3473fa94	0x4473fa94	0x2fa2ca08	0x3473fa80	.....	.....	是/否
0x3473fac8	0x4473fa94	0x3663fa80	0x3663fbb8	.....	.....	是/否
.....		.....	.....			
.....		.....	.....			

圖11

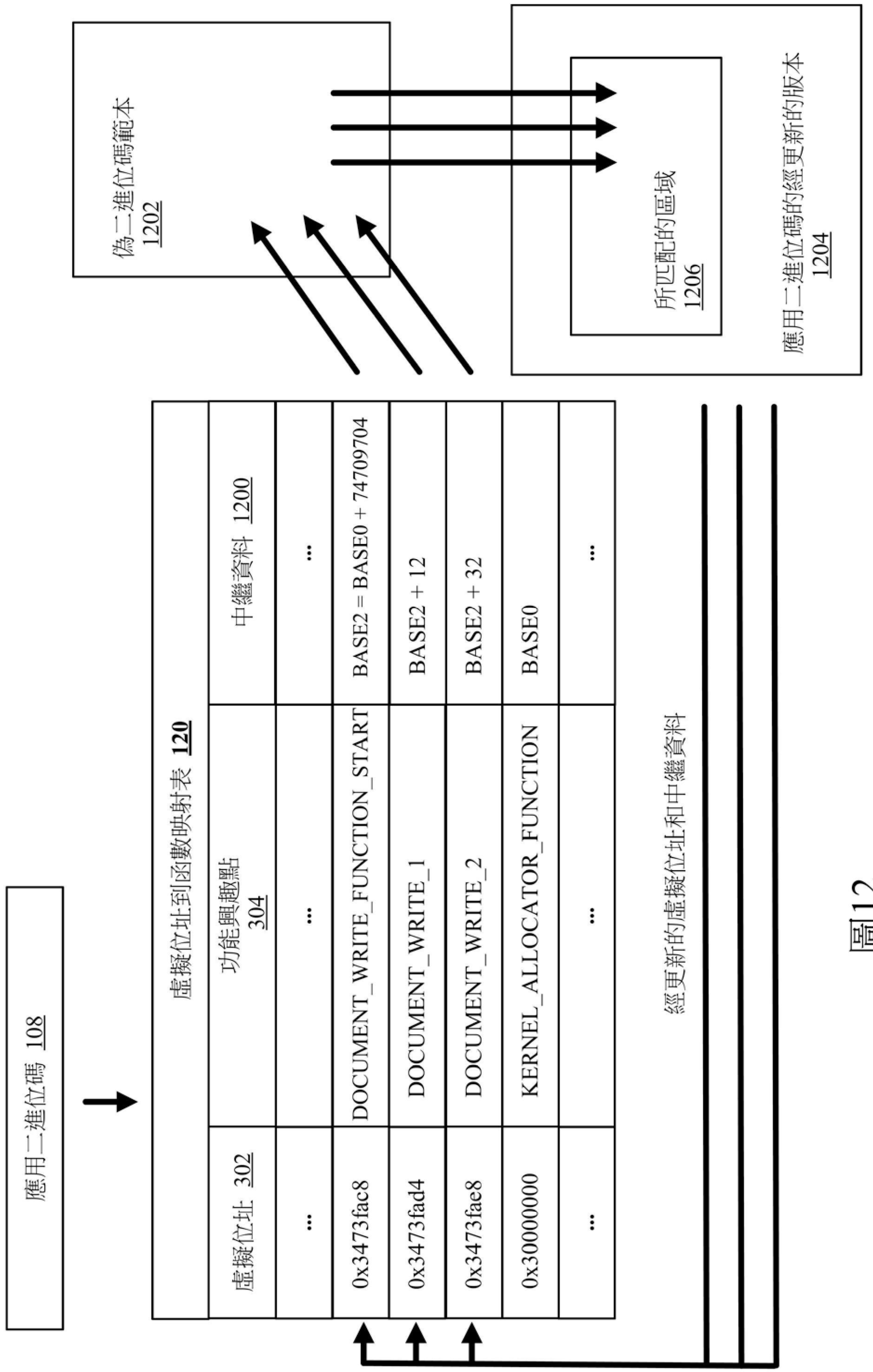

偽二進位碼範本
1202
所匹配的區域
1206
應用二進位碼的經更新的版本
1204
中繼資料 1200
...
BASE2 = BASE0 + 74709704
BASE2 + 12
BASE2 + 32
BASE0
...
虛擬位址到函數映射表 120
功能興趣點
304
虛擬位址 302
DOCUMENT_WRITE_FUNCTION_START
DOCUMENT_WRITE_1
DOCUMENT_WRITE_2
KERNEL_ALLOCATOR_FUNCTION
0x3473fac8
0x3473fad4
0x3473fae8
0x30000000
經更新的虛擬位址和中繼資料
應用二進位碼 108

圖12

虛擬位址到函數映射表 **120**		
虛擬位址 302	表示功能含義的巨集 304	使用位元組偏移的無虛擬位址的表示 1200
...	...	...
0x3133b61c	DOCUMENT_WRITE_FUNCTION_START	BASE2 = BASE0 + 74709000
0x3133b62c	DOCUMENT_WRITE_1	BASE2 + 16
0x3133b640	DOCUMENT_WRITE_2	BASE2 + 36
0x2cbfbe14	KERNEL_ALLOCATOR_FUNCTION	BASE0
...	...	...

圖13

虛擬位址到函數映射表
120

虛擬位址 302	表示功能含義的巨集 304
0x3473fac8	DOCUMENT_WRITE_FUNCTION_START
0x3473fad4	DOCUMENT_WRITE_1
0x3473fae8	DOCUMENT_WRITE_2
0x30000000	KERNEL_ALLOCATOR_FUNCTION

偽二進位碼範本 1202

```
Push   {callSave0, CallSave1, ReturnReg}
AddWord     reg0, ProgCounter, #Const8bits
LoadWord    reg1, [reg0]
LoadWord    reg2, [reg1]
.....
.....
LogicalShiftLeft   reg1, reg0, #16
AddWord     reg2, reg1, #4
LoadWord    reg3, [reg2]
AddWord     reg4, reg3, ProgCounter
LoadByte    ArgumentReg0, [reg4]
AddWord     ReturnReg, ProgCounter, #8
BranchDir   (ProgCounter + #Const20bits)
.....
.....
AddWord   reg0,  ProgCounter, #Const8bits
LoadWord  reg2, [reg0]
AddWord   reg1, reg2, ProgCounter
LoadWord  ArgumentReg0, [reg1]
AddWord   ReturnReg, ProgCounter, #8
BranchDir  (ProgCounter + #Const20bits)
Compare   ReturnValueReg0,  #0
BranchEQ  (ProgCounter + #12)
Compare   ReturnValueReg0,  #1
BranchNE   (ProgCounter + #Const5Bits)
.....
```

圖14

偽二進位碼範本 1202

```
Push   {callSave0, CallSave1, ReturnReg}
AddWord     reg0, ProgCounter, #Const8bits
LoadWord    reg1, [reg0]
LoadWord    reg2, [reg1]
.....
.....
LogicalShiftLeft   reg1, reg0, #16
AddWord     reg2, reg1, #4
LoadWord    reg3, [reg2]
AddWord     reg4, reg3, ProgCounter
LoadByte    ArgumentReg0, [reg4]
AddWord     ReturnReg, ProgCounter, #8
BranchDir   (ProgCounter + #Const20bits)
.....
.....
AddWord  reg0,  ProgCounter, #Const8bits
LoadWord  reg2, [reg0]
AddWord   reg1, reg2, ProgCounter
LoadWord  ArgumentReg0, [reg1]
AddWord   ReturnReg, ProgCounter, #8
BranchDir  (ProgCounter + #Const20bits)
Compare   ReturnValueReg0,  #0
BranchEQ  (ProgCounter + #12)
Compare   ReturnValueReg0,  #1
BranchNE   (ProgCounter + #Const5Bits)
.....
```

應用二進位檔案的經更新的版本
1204

```
3133b608:  mov          r0, r5
3133b60c:  mov          r1, r4
3133b610:  mov          r3, r6
3133b614:  ldmia.w   sp!, {r4, r5, r6, lr}
3133b618:  bx              r3
3133b61c:  push         {r4, r5, lr}
3133b620:  ldr          r4, [pc, #64]
3133b624   ldr          r4, [r4, #0]
3133b628:  ldr          r1, [pc, #60]
3133b62c:  lsl          r7, r1, #16
3133b630:  ldr          r3, [r7, #4]
3133b634:  add          r3, pc
3133b638:  ldrb         r0, [r3, #0]
3133b63c:  bl            314a8abc
3133b640:  ldr          r1, [pc, #80]
3133b644:  add          r1, pc
3133b648:  ldr          r0, [r1, #0]
3133b64c:  blx          314a6cbc
3133b650:  cmp          r0, #0
3133b654:  beq          3133b660
3133b658   cmp          r0, #1
3133b65c:  bne          3133b674
3133b660:  bl           313ca924
3133b664:  ldr           r3, [r0, #0]
3133b668:  mov           r0, #64
3133b66c:  ldr           r6, [r3, #0]
3133b670:  bl             3146e548
3133b674:  movs                r1, #0
3133b678:  movs    r2, #64  ; 0x40
.....
```

圖15

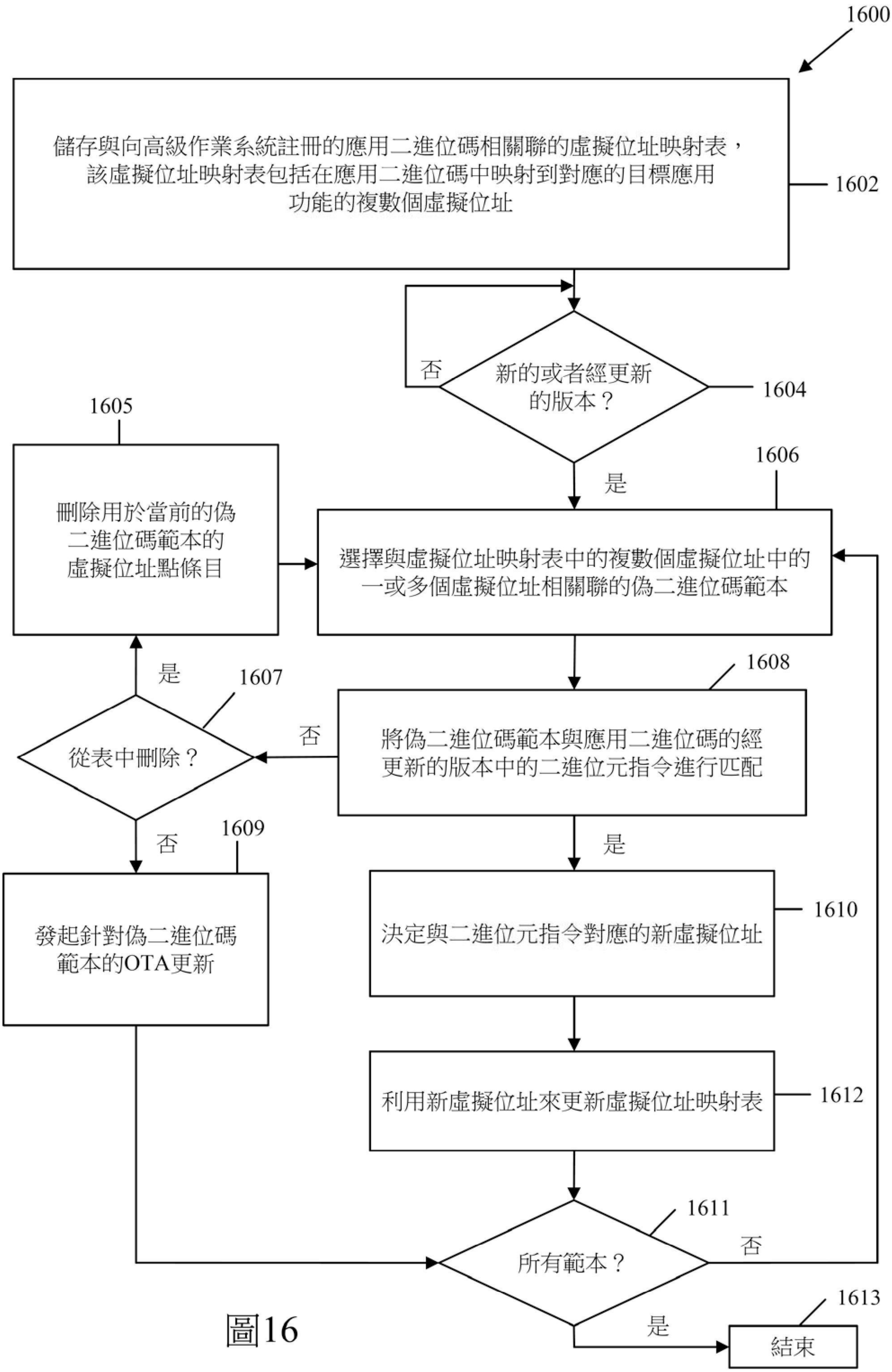

1600
儲存與向高級作業系統註冊的應用二進位碼相關聯的虛擬位址映射表，該虛擬位址映射表包括在應用二進位碼中映射到對應的目標應用功能的複數個虛擬位址
1602
新的或者經更新的版本？
否
1604
是
1605
刪除用於當前的偽二進位碼範本的虛擬位址點條目
1606
選擇與虛擬位址映射表中的複數個虛擬位址中的一或多個虛擬位址相關聯的偽二進位碼範本
是
1607
從表中刪除？
否
1608
將偽二進位碼範本與應用二進位碼的經更新的版本中的二進位元指令進行匹配
否
1609
是
發起針對偽二進位碼範本的OTA更新
決定與二進位元指令對應的新虛擬位址
1610
利用新虛擬位址來更新虛擬位址映射表
1612
所有範本？
1611
否
是
1613
結束

圖16

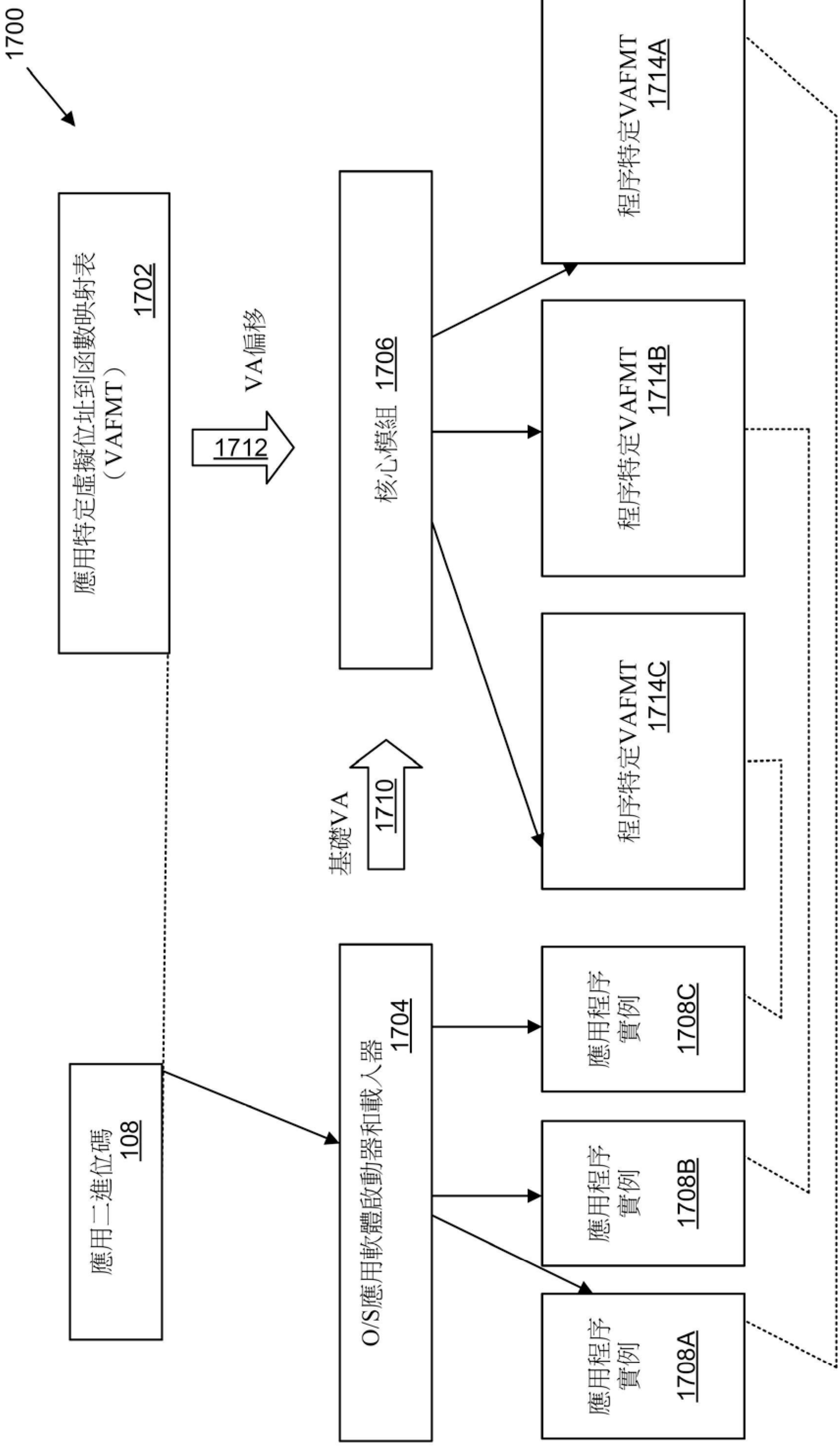

1700
應用特定虛擬位址到函數映射表（VAFMT）
1702
VA偏移
1712
核心模組 1706
程序特定VAFMT 1714A
程序特定VAFMT 1714B
程序特定VAFMT 1714C
基礎VA
1710
應用二進位碼 108
O/S應用軟體啟動器和載入器 1704
應用程序實例 1708C
應用程序實例 1708B
應用程序實例 1708A

圖17

應用特定VAFMT **1702**		
VA偏移 **1800**	功能點 **1802**	中繼資料 **1804**
0x373ea94	EVAL_FUNCTION	BASE1 = BASE0 + 57928340
0x473fac8	DOCUMENT_WRITE_FUNCTION_START	BASE2 = BASE0 + 74709704
0x473fad4	DOCUMENT_WRITE_1	BASE2 + 12
0x473fae8	DOCUMENT_WRITE_2	BASE2 + 32
0x1b93420	ONCLICK_FUNCTION	BASE3 = BASE0 + 28914720
0x1b934d4	ONCLICK_1	BASE3 + 180
0x9d78264	SETTIMEOUT_FUNCTION_START	BASE4 = BASE0 + 165118564
0x673fa94	VM_CODE_SPACE_ALLOCATOR	BASE5 = BASE0 + 108264084
0x673faD0	CALL_KERNEL_ALLOCATOR	BASE5 + 60
0x0000000	KERNEL_ALLOCATOR_FUNCTION	BASE0
0x673fbd4	VM_CODE_SPACE_DEALLOCATOR	BASE6 = BASE0 + 108264404
0x673fbf8	CALL_KERNEL_DEALLOCATOR	BASE6 + 36
0x22243e4	KERNEL_DEALLOCATOR_FUNCTION	BASE7 = BASE0 + 35800036

圖18

程序特定VAFMT **1714**		
實際VA **1900**	功能點 **1802**	中繼資料 **1804**
0x3373ea94	EVAL_FUNCTION	BASE1 = BASE0 + 57928340
0x3473fac8	DOCUMENT_WRITE_FUNCTION_START	BASE2 = BASE0 + 74709704
0x3473fad4	DOCUMENT_WRITE_1	BASE2 + 12
0x3473fae8	DOCUMENT_WRITE_2	BASE2 + 32
0x31b93420	ONCLICK_FUNCTION	BASE3 = BASE0 + 28914720
0x31b934d4	ONCLICK_1	BASE3 + 180
0x39d78264	SETTIMEOUT_FUNCTION_START	BASE4 = BASE0 + 165118564
0x3673fa94	VM_CODE_SPACE_ALLOCATOR	BASE5 = BASE0 + 108264084
0x3673faD0	CALL_KERNEL_ALLOCATOR	BASE5 + 60
0x30000000	KERNEL_ALLOCATOR_FUNCTION	BASE0
0x3673fbd4	VM_CODE_SPACE_DEALLOCATOR	BASE6 = BASE0 + 108264404
0x3673fbf8	CALL_KERNEL_DEALLOCATOR	BASE6 + 36
0x322243e4	KERNEL_DEALLOCATOR_FUNCTION	BASE7 = BASE0 + 35800036

圖19

應用特定URL緩衝器VAFMT 2000							
使用內置 HTTPS堆疊的應用軟體 2002	VA偏移 (進行URL資料結構分配的函數) 2004	用於「核心系統分配器」的VA (動態地決定) **2006**	URL緩衝器起始虛擬位址 (動態地決定) **2008**	URL緩衝器結束虛擬位址 (動態地決定) **2010**	所分配的緩衝器資料結構內的URL成員欄位/指標偏移(以位元組為單位) **2012**	所分配的緩衝器資料結構內的URL成員欄位/指標長度(以位元組為單位) **2014**	URL成員欄位是指標嗎? **2016**
應用軟體-1	0x473fa94						是/否
應用軟體-2	0x473fac8						是/否
....							

圖20

程序特定URL緩衝器VAFMT **2100**							
使用內置HTTPS堆疊的應用軟體 2002	VA偏移(進行URL資料結構分配的函數) **2102**	用於「核心系統分配器」的VA(動態地決定) **2006**	URL緩衝器起始虛擬位址(動態地決定) **2008**	URL緩衝器結束虛擬位址(動態地決定) **2010**	所分配的緩衝器資料結構內的URL成員欄位/指標偏移(以位元組為單位) **2012**	所分配的緩衝器資料結構內的URL成員欄位/指標長度(以位元組為單位) **2014**	URL成員欄位是指標嗎? **2016**
應用軟體-1	0x3473fa94	0x4473fa94	0x2fa2ca08	0x3473fa80	....	....	是/否

圖21

程序特定URL緩衝器VAFMT **2200**							
使用內置 HTTPS堆疊的應用軟體 2002	VA偏移 (進行URL資料 結構分配的 函數) **2202**	用於「核心系統 分配器」的VA (動態地決定) **2006**	URL緩衝器起 始虛擬位址 (動態地決定) **2008**	URL緩衝器 結束虛擬位址 (動態地決定) **2010**	所分配的緩衝器 資料結構內的 URL成員欄位/ 指標偏移(以 位元組為單位) **2012**	所分配的緩衝器 資料結構內的 URL成員欄位/ 指標長度(以 位元組為單位) **2014**	URL成員 欄位是 指標嗎? **2016**
應用軟體-2	0x2473fac8	0x1473fa94	0x2663fa80	0x2663fbb8	....	....	是/否

圖22

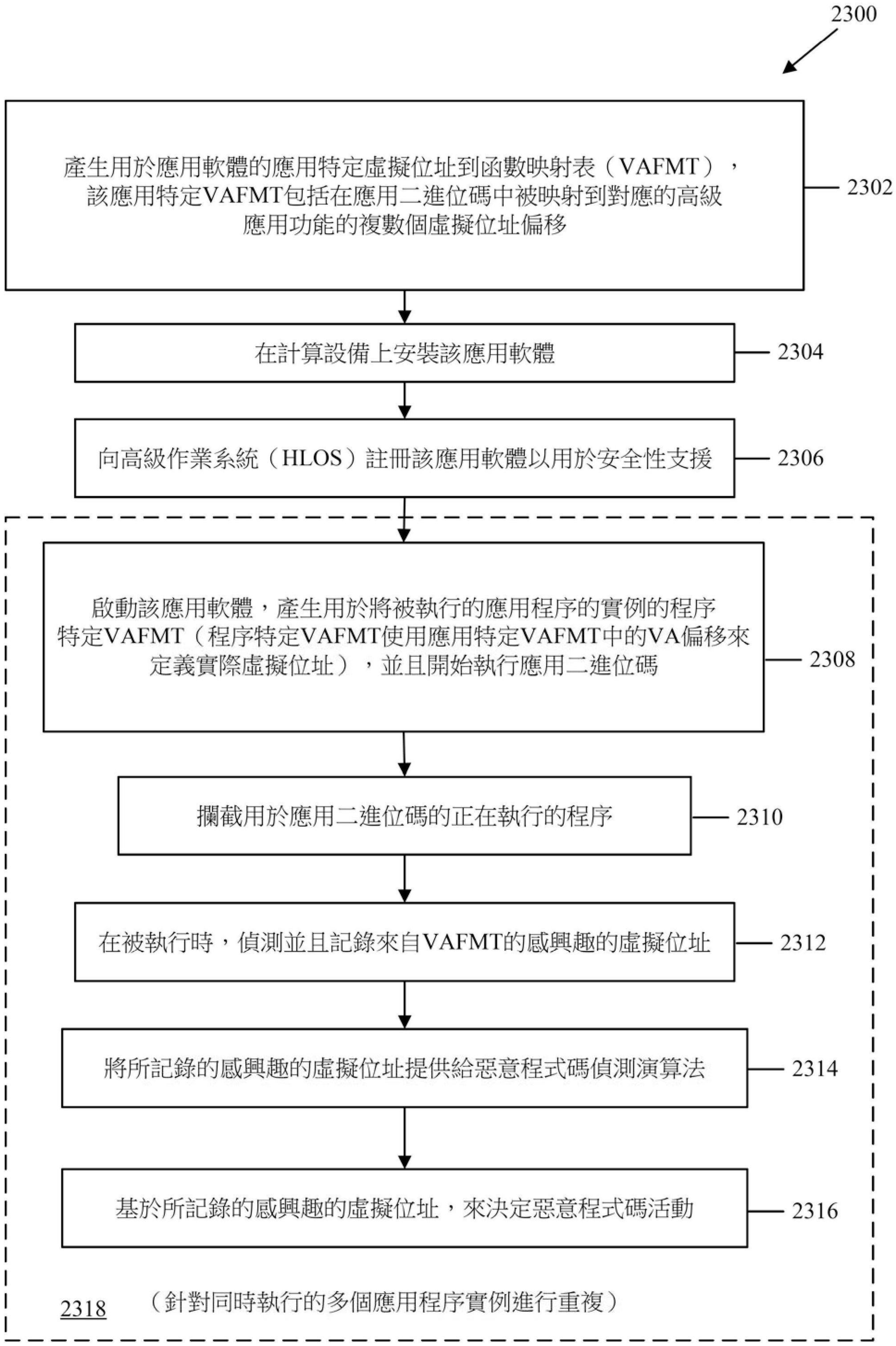

2300
產生用於應用軟體的應用特定虛擬位址到函數映射表（VAFMT），該應用特定VAFMT包括在應用二進位碼中被映射到對應的高級應用功能的複數個虛擬位址偏移
2302
在計算設備上安裝該應用軟體
2304
向高級作業系統（HLOS）註冊該應用軟體以用於安全性支援
2306
啟動該應用軟體，產生用於將被執行的應用程序的實例的程序特定VAFMT（程序特定VAFMT使用應用特定VAFMT中的VA偏移來定義實際虛擬位址），並且開始執行應用二進位碼
2308
攔截用於應用二進位碼的正在執行的程序
2310
在被執行時，偵測並且記錄來自VAFMT的感興趣的虛擬位址
2312
將所記錄的感興趣的虛擬位址提供給惡意程式碼偵測演算法
2314
基於所記錄的感興趣的虛擬位址，來決定惡意程式碼活動
2316
2318
（針對同時執行的多個應用程序實例進行重複）

圖23