200901034

發明專利說明書

（本說明書格式、順序及粗體字，請勿任意更動，※記號部分請勿填寫）

※ 申請案號：97117382

※ 申請日期：97/05/12　　※IPC 分類：G06F 9/44 (2006.01)

一、發明名稱：（中文/英文）

在安全環境控制處理器執行之裝置

Apparatus for Controlling Processor Execution in a Secure Environment

二、申請人：（共 1 人）

姓名或名稱：（中文/英文）

艾柯斯達科技公司 / EchoStar Technologies L.L.C

代表人：（中文/英文）

約翰 甘迺迪 / John T Kennedy

住居所或營業所地址：（中文/英文）

美國科羅拉多州英格塢市英凡尼斯東圓環 90 號

90 Inverness Circle East, Englewood, 80112 CO, USA

國　籍：（中文/英文）

美國 / USA

三、發明人：（共 1 人）

姓　名：（中文/英文）

威廉 麥克 比爾斯 / William Michael BEALS

國　籍：（中文/英文）

美國 / USA

四、聲明事項：

☐ 主張專利法第二十二條第二項☐第一款或☐第二款規定之事實，其事實發生日期為：　年　月　日。

☑ 申請前已向下列國家（地區）申請專利：

【格式請依：受理國家（地區）、申請日、申請案號　順序註記】

☑ 有主張專利法第二十七條第一項國際優先權：

1. 美國；2007/05/11；60/917,582
2.
3.
4.
5.

☐ 無主張專利法第二十七條第一項國際優先權：

☐ 主張專利法第二十九條第一項國內優先權：

【格式請依：申請日、申請案號　順序註記】

☐ 主張專利法第三十條生物材料：

☐ 須寄存生物材料者：

國內生物材料 【格式請依：寄存機構、日期、號碼　順序註記】

國外生物材料 【格式請依：寄存國家、機構、日期、號碼　順序註記】

☐ 不須寄存生物材料者：

所屬技術領域中具有通常知識者易於獲得時，不須寄存。

九、發明說明：

【發明所屬之技術領域】

本文描述之本發明之各種具體例以各種方式關於用於在安全環境中控制一或多個處理器的執行之裝置、系統、及程序。另外，此等各種具體例之實施可包括在無線及非無線電視接收設備(諸如由電纜、衛星、電信、無線、及/或其他音訊、視訊、及/或資料服務提供者所提供之設備)中控制處理器執行。

本申請案主張2007年5月11日提出主題為“在安全環境中控制處理器執行之裝置、系統及方法(APPARATUS, SYSTEM AND METHOD FOR CONTROLLING PROCESSOR EXECUTION IN A SECURE ENVIRONMENT)”的美國臨時申請案第60/917,582號之權利，該案藉此以全文引用方式併入。

【先前技術】

無

【發明內容】

本文描述之各種具體例係關於用於建立並實施安全計算環境以執行軟體部分之裝置、系統、及方法。更特定言之，一具體例提供在提供對計算環境資源之限制存取之環境中執行軟體部分的安全處理器。

在另一具體例中，一種用於提供安全計算環境之系統包括(但不限於)一安全處理器、一上下文管理器、及一信任向量驗證器。該安全處理器可被組態成為執行具有相關聯

上下文（其為（例如）軟體所限制於之特定操作環境）之軟體程式及/或常式中之一些或全部。軟體可包括（例如）方法、子程式、常式、整個應用程式、或者一或多個軟體應用程式之任何部分。在至少一具體例中，軟體可限制於一或多個上下文。

在又一具體例中，一種用於在安全操作環境中控制安全處理器之執行之方法包括一請求一上下文交換的安全處理器。在一具體例中，該上下文交換為針對不同軟體部分至新上下文之切換。在一具體例中，一上下文管理器接收該上下文交換請求。在其他具體例中，該上下文管理器載入一信任向量驗證器中之一信任向量描述符。在至少一具體例中，上下文管理器重設安全處理器。在其他具體例中，該信任向量驗證器基於載入之信任向量描述符來控制安全處理器對一或多個資源之存取。

一種電腦可讀媒體被描述，其具有一用於控制一安全處理器之執行的編碼資料結構。該資料結構可包括關於界定用於該安全處理器之操作環境的一或多個上下文之資料。另外，一上下文可包括一識別一給定上下文之欄位、一安全處理器可存取的記憶體之一或多個區域之一表示、及一安全處理器可存取的一或多個硬體資源之一表示。同樣地，執行資料結構之一電腦系統根據一硬體信任向量來判定該安全處理器是否可存取一硬體資源。

此概述經提供以引入下文在「實施方式」中進一步描述的簡化形式之概念之選定。此概述不欲識別所主張之標的

物的關鍵特徵或本質特徵，亦不欲用以限制所主張之標的物的範疇。

【實施方式】

後文中參考所附圖式描述一些具體例。若干圖式中之相同數字表示相同元件。

本揭示現將參考隨附圖式較為充分地描述一些具體例，其中僅展示可能具體例中之一些。然而，其他態樣可以許多不同形式被具體化且不應被解釋為限於本文陳述之具體例。本說明書中所陳述之具體例係關於涉及受信任微處理器計算之方法及系統。該計算可(例如)發生於預訂衛星電視系統中。其他具體例亦可包括(例如，但不限於)有線電視、無線電視、有線或無線電訊系統、音訊/視訊/資料分布系統、任何內容傳遞服務、及/或其他計算環境。

在圖 1 所示之具體例中，一計算環境 100 可包括一由虛線 102 表示之安全計算或操作環境。安全計算或操作環境 102 可包括一安全中央處理單元(“CPU”)或處理器 104、一上下文管理器 106、及一信任向量驗證器 108。另外，處理器 104、上下文管理器 106、及信任向量驗證器 108 中之每一者可彼此直接或間接通訊。安全處理器 104 可為任何類型之通用處理器，且可在需要時被特別設計而為安全的。在諸具體例中，上下文管理器 106 及信任向量驗證器 108 可為用於本發明之具體例中的特別設計之硬體設備、軟體模組、或硬體與軟體之組合。

在一具體例中，安全處理器 104 操作以執行至少三個基

本動作：執行一軟體程式中之一數學函數或邏輯運算，移動資料至記憶體中之不同位置或自該等不同位置移動資料以保持用於一軟體程式中之資料，及/或進行決策且跳至一軟體程式中之新指令。為了完成此等工作，安全處理器 104 可包括算術或邏輯單元(arithmetic or logic unit, ALU)(未圖示)、暫存器 124、記憶體 122、及內部或外部記憶體或者其他資料儲存器 126。ALU 執行數學函數或邏輯運算。暫存器 124 保持關於由安全處理器 104 所執行之操作的資訊或資料。舉例而言，一資料暫存器可保持用於由 ALU 所完成之數學運算中之資料值；記憶體暫存器可保持記憶體 126 中資料所儲存之位址。記憶體 126 一般由臨時或以其他方式保持且/或儲存資料的一或多個硬體設備、結構、或組件組成。在一具體例中，記憶體包括保持由安全處理器 104 規律存取之資料的快取記憶體 122 及一或多個其他記憶體 126。快取記憶體 122 為整合於安全處理器 104 內之記憶體區、直接連接至安全處理器 104 之記憶體、或易於由安全處理器 104 存取或與安全處理器 104 介面連接的記憶體 126 之區。在另一具體例中，記憶體 126 可包括一記憶體管理單元(memory management unit, MMU)128，其控制資料自記憶體 126 之讀取及至記憶體 126 之寫入。記憶體 126 可由保持資料的一或多個類型之記憶體組成，例如，隨機存取記憶體(random access memory, RAM)、唯讀記憶體(read only memory, ROM)、硬碟機、光學儲存器、或者一或多個其他記憶體技術。熟習此項技

術者將認識到安全處理器 104 不限於關於計算系統之闡述，而是可包括此項技術中已知的其他組件及功能。另外，本文中之計算系統闡述經提供以簡化關於本發明之具體例的闡述，且本發明不應限於本文描述之計算系統。

在執行上文提及之三個動作的程序中，安全處理器 104 執行軟體之部分。此等軟體部分一般組合以形成一軟體程式或應用程式來完成大規模工作。一般而言，軟體部分為由安全處理器 104 所執行之一或多個指令。在後文中可將軟體部分稱為軟體常式，子常式或模組。在執行軟體部分時，安全處理器 104 可產生稱為堆疊(未圖示)之抽象資料類型。堆疊可為例如快取記憶體 122 或記憶體 126 之記憶體中的一組記憶體位址，安全處理器 104 分別向該等記憶體位址儲存資料或指令或者自其讀取資料或指令。舉例而言，在將一資料項或一指令儲存至堆疊中時，安全處理器 104 可在暫存器 124 中記錄一堆疊指標(stack pointer)，該堆疊指標為記憶體中資料或指令所儲存之位址。資料可在兩個或兩個以上軟體部分之間共用，且為了促進此共用，可將資料儲存於堆疊中且向軟體部分提供堆疊指標。

在各種具體例中，安全處理器 104 在包括(例如)軟體、記憶體 122/126、及資源 120 之組合的操作環境中執行各種軟體部分。安全處理器 104 可被組態成為執行、介面連接、且/或利用軟體、記憶體、資源、及其類似物來執行給定操作。為了防止且/或最小化惡意或以其他方式不合需要之代碼之引入，提供促進對安全處理器 104 之操作環

境的控制之系統、方法、裝置、及其類似物。

在至少一具體例中，一安全操作環境102可由一或多個“上下文”來指定。一上下文藉由指定安全處理器104被允許執行之彼等指令、功能、及/或操作而界定操作環境之界限。舉例而言，一軟體應用程式可包含四個指令。一上下文可指定安全處理器104可執行此等四個指令中之一第一者、此等指令中之一或多者、此等指令中之全部、其組合、或其類似物。亦即，一上下文可建立排除未指定指令不被執行之容許的環境。舉例而言，若安全處理器104試圖執行並非四個指令中之一者的指令，則識別出一異常且防止安全處理器104執行該其他指令。

在另一例子中，一上下文可允許一安全處理器僅存取記憶體位址1至20。若安全處理器嘗試存取記憶體位址40，則識別出一異常且防止安全處理器104存取記憶體位址40。

在又一例子中，一上下文可指定安全處理器104僅被允許存取硬碟機。若安全處理器104嘗試存取使用者介面設備，則識別出一異常且防止安全處理器104存取使用者介面。

在各種具體例中，上下文管理器106及信任向量驗證器108建立並實施上下文。上下文管理器106操縱上下文之改變。兩個或兩個以上軟體部分各自具有相關聯之上下文。在執行一第一軟體部分時，一第一上下文用以界定安全操作環境。同樣，在安全處理器104執行一第二軟體部

分時，一不同的第二上下文用以界定不同安全操作環境。為了在軟體部分之間進行切換，上下文管理器建立與待執行之新軟體部分相關聯的新上下文。在建立新上下文之程序中，新軟體部分在適合於彼軟體部分之操作環境中執行。將由新軟體部分造成的自上下文之偏差係識別為安全異常。因此，在需要時針對每一軟體部分設定安全操作環境來控制安全處理器 104 操作。

如上文所提及，各種具體例亦可包括實施上下文之信任向量驗證器 108。信任向量驗證器 108 虛擬及/或實體地定位於(在資料信號流中)安全處理器 104 與一給定系統之其他虛擬或實體組件(諸如資源 120 及記憶體 126)之間。藉由信任向量驗證器 108 之置放，信任向量驗證器 108 可被組態成為截取安全處理器 104、資源 120、及/或記憶體 126 之間及/或其中間的通訊。在諸具體例中，信任向量驗證器 108 可載有資訊，該資訊界定給定上下文，且信任向量驗證器 108 比較該資訊與安全處理器 104 進行之動作。若一動作不與信任向量驗證器 108 中之載入資訊比較，則該動作在彼上下文中不被允許。不與載入資訊比較的動作處於所允許上下文之外。信任向量驗證器 108 將此等動作識別為異常且防止該等動作發生。舉例而言，信任向量驗證器 108 自安全處理器 104 接收用於存取記憶體 126 之請求，信任向量驗證器 108 判定該請求在目前上下文內是否被允許，且若該請求不被允許，則信任向量驗證器 108 識別該異常且防止對記憶體 126 之存取。

安全處理器 104 亦可被組態成為在第一軟體部分與第二軟體部分之執行之間進行週期性切換。在一具體例中，在於不同軟體部分之間切換執行之前，可執行一或多個步驟以確保系統 100 之安全性。舉例而言，安全處理器 104 可清除快取記憶體 122 及/或 MMU 128，且儲存指向堆疊中之資料的指標。安全處理器 104 可向上下文管理器 106 傳送用於上下文交換 110 之請求(亦即，用以改變為新的預定上下文之請求)。在諸具體例中，上下文管理器 106 向安全處理器 104 發送一重設 112 以對其進行重設，且向信任向量驗證器 108 發送一指令 114 以自記憶體 126 或可由信任向量驗證器 108 所存取之其他安全記憶體(未圖示)載入與所要上下文相關聯之信任向量描述符。在諸具體例中，理想地重設導致安全處理器 104 之一或多個內部狀態的清除。應瞭解，該清除減小將惡意軟體被引入安全處理器 104 之風險。重設可包括清除安全處理器 104 之一個、多個、或全部狀態之任何方法。在另一具體例中，安全處理器 104 可在重設期間被組態成使得所有狀態資訊均為不可操作且不可用的。

更具體言之，對於至少一具體例，安全處理器 104 可藉由執行啟動或硬體重設操作而完成重設功能。該啟動可(例如)在安全處理器 104 於新上下文中執行一或多個指令之前發生。應瞭解，該啟動可為需要軟體之重新載入的軟體啟動，或需要安全處理器 104 及/或一或多個其他組件之電力關閉及開啟的硬體啟動。對於每一具體例理想但

並非必要地，軟體及硬體啟動均抹除儲存於快取記憶體122、暫存器124、及/或記憶體126中之資料及/或指令中之一些(若非全部)。在諸具體例中，一或多個通常已知之方法可用以抹除快取記憶體122、暫存器124、及/或記憶體126中之資料及/或指令中之一些或全部。舉例而言，所儲存之記憶體位址可藉由在先前儲存之資料上寫入新資料而刪除。因此，安全處理器104可被組態成為抹除或以其他方式使得對於第一上下文有用而對於第二上下文並非所要之不可用資料及/或指令。

在至少一具體例中，自一上下文至另一者，安全處理器104不保持任何狀態資訊。亦即，安全處理器可被組態成為不保持任何先前上下文或軟體之任何知識。

如圖1所示，信任向量驗證器108經由通訊路徑116與安全處理器104通訊。在一具體例中且通常為了防止安全異常，信任向量驗證器108可被組態成為向安全處理器104發送硬體中斷121。在接收到硬體中斷121之後，安全處理器104如下文結合圖3所闡述而重設，且/或啟動或重新啟動至另一上下文中。此另一上下文可為預定或即時判定的。在另一具體例中，信任向量驗證器108可被組態成為在回應於安全異常之請求至新上下文之上下文交換的同時處理目前上下文中之安全異常。

在各種具體例中，信任向量驗證器108可被組態並載入有資訊，該資訊使得信任向量驗證器108能夠實施任何給定上下文。此資訊可永久地載入，在上下文交換之前載

入，在安全處理器之重設期間載入，在重設安全處理器104之後載入及/或在另一時間載入。舉例而言，載入資訊可包括自記憶體126或另一安全記憶體(未圖示)載入之一或多個信任向量描述符。在需要時，該記憶體126可被組態成使得其僅可由信任向量驗證器108存取。在其他具體例中，信任向量驗證器108可包括且/或能夠存取一或多個專用或共用記憶體設備，諸如ROM、EEPROM、硬碟機、或其類似物。此記憶體可被組態成為在需要時持久地包含一或多個信任向量描述符。在至少一具體例中，信任向量描述符界定：安全處理器104可執行之軟體程式、常式、及/或指令。信任向量描述符亦可被組態成為界定安全處理器104如何、何時可存取、控制、利用、傳送(等等)資源及/或可存取、控制、利用、傳送(等等)哪些資源。同樣地，信任向量描述符可界定安全處理器104可存取哪一記憶體126或122，及安全處理器104可於上下文中起始、執行、及完成之其他動作。

信任向量描述符之一具體例展示於圖2中。在此具體例中，信任向量描述符包括至少一信任向量描述符202，且可包括多個信任向量描述符202、204、或206。信任向量描述符可儲存於(例如)信任向量表(trust vector table, TVT)資料結構200或任何其他所要資料結構中。如上文參考圖1所提及，在載入或以其他方式表示一信任向量描述符202用於由信任向量驗證器108使用時，新的上下文被建立且管理安全處理器104之操作。

如圖 2 所描繪之具體例進一步所展示，每一信任向量描述符 202、204、及 206 可界定不同上下文，且因此可具有不同資料。在諸具體例中，信任向量描述符 202、204、及 206 之每一區段中的資料為特定類型。每一信任向量描述符 202、204 及、206 可包含一或多個其他資料欄位，但不限於所描述之資料欄位。信任向量描述符 202、204 及、206 可由上下文識別(ID)欄位 208 識別。在其他具體例中，每一信任向量描述符 202、204、及 206 可包括關於代碼開始位址 210、代碼結束位址 212、密鑰號碼 214、目標 CPU 及向量號碼(#)216、擦拭類型 218、硬體信任向量描述符 220、記憶體資料區域 222、CPU 啟動位址 224、信任向量描述符簽名 226、及代碼簽名 228 之資料欄位。

代碼開始位址 210 及代碼結束位址 212 識別代碼之哪一部分待鑑定且接著由安全處理器 104 執行(圖 1)。應瞭解有用於識別待執行之代碼的部分之其他方法，例如，代碼開始位址及代碼之長度。舉例而言，代碼開始位址 210 及代碼結束位址 212 可表示包含所要代碼的記憶體之一或多組之多個非連續區域。該等區域可進一步(例如)由兩個或兩個以上開始及結束位址表示。

在至少一具體例中，信任向量描述符 202、204、206 可包括用以驗證待執行的軟體及/或其部分之確實性之密鑰號碼及/或其他參考資訊。參考資訊可包括(例如)用以鑑定代碼的代碼之指紋(識別)、用以鑑定代碼的代碼之簽名、及/或對用以驗證代碼之簽名之密鑰的參考。另外，

在具有多個密鑰之具體例中，密鑰號碼 214 可指定使用哪一密鑰來驗證所產生之簽名且藉此鑑定軟體部分。應瞭解，此驗證可(例如)藉由比較所產生之簽名與信任描述符簽名 226 及/或代碼簽名 228 而發生。

若系統具有多個處理器，則目標 CPU 欄位 216 提供關於使用哪一處理器之指定符。如將結合圖 4 所闡述，軟體部分可在一或多個安全處理器上執行。向量號碼欄位 216 提供關於信任向量描述符 202 之指定符。

如結合圖 6 所論述，擦拭類型欄位 218 提供關於如何擦拭軟體部分之資訊，亦即，證明軟體部分之確實性。舉例而言，若軟體部分被鑑定或被擦拭過一次，則擦拭類型欄位 218 可包括“初始”擦拭之指定符。其他類型之擦拭方法包括(但不限於)：“連續”擦拭，藉此在操作的同時連續擦拭軟體部分，及“從不”，其不需要軟體部分之任何擦拭。在其他具體例中，可使用其他擦拭方法。

硬體信任向量描述符欄位 220 可用以界定上下文中之資源存取。更具體言之，硬體信任向量描述符 220 識別安全處理器 104(圖 1)可在操作期間介面連接、通訊等等的諸如周邊設備或內部組件之彼等資源，而該等操作於一給定信任向量描述符 202、204、206 所界定之上下文內執行。在一具體例中，硬體信任向量描述符 220 可為位元映射或位元陣列，其中陣列之每一位元表示特定類型之硬體。舉例而言，硬體信任向量描述符 220 可呈現為“0101”。設定為“1”之第一位元可表示處理器可存取

硬碟機控制器。設定為“0”之第二位元可表示處理器不可存取智慧卡。設定為“1”之第三位元及設定為“0”之第四位元可表示處理器可存取 I/O 埠但不可存取視訊控制器。硬體信任向量描述符 220 中的位元之數目可隨安全處理器所用於之具體例而變化且可為四個以下或四個以上位元。應瞭解，硬體信任向量描述符 220 之其他具體例可被使用。舉例而言，除了由硬體信任向量 220 識別之資源之外，信任向量描述符 220 可被組態使得給定實施內之所有資源均可用安全處理器。其他具體例亦為可能的，且包括於所附加或於後文所加入之申請專利範圍的範疇內。

記憶體資料區域欄位 222 亦可用以界定上下文中之資源存取，且進一步界定安全處理器 104(圖 1)可存取(例如)以自記憶體讀取資料及/或將資料寫入記憶體的記憶體 126(圖 1)中之位址空間。關於硬體信任向量 220，記憶體資料區域欄位 222 可基於開始及停止位址而藉由指定位址將位址空間指定為鄰近區塊及/或其他。又，可以肯定(亦即，可存取之位址空間)、異常(亦即，除所識別之位址空間外均可存取)、或其他方式來表示位址空間。因此，應瞭解記憶體資料區域欄位 222 可識別可讀取及/或寫入可執行資料的位址。包含於一或多個未界定位址中的資料同樣可表示為不可執行，以致若安全處理器嘗試執行來自禁止資料區域之代碼且/或利用來自禁止資料區域之資料，則安全異常將發生。

在一具體例中，將可存取記憶體 126(圖 1)之一或多個

部分與其他軟體部分共用。另外，每一軟體部分可在一或多個上下文中執行。在該具體例中，一軟體部分可能需要將資料傳遞至另一軟體部分，但該兩個軟體部分不在同一上下文中執行。記憶體資料區域欄位 222 可被組態成為藉由使用(例如)用以識別位址空間之異常方法來支援此情形。同樣地，在另一具體例中，記憶體資料區域欄位 222 可包括(對於藉此指定之記憶體的任何或每一區域)表示待包括於一或多個擦拭操作中的記憶體之區域之共同或單獨擦拭位元。

如針對本文描述之至少一具體例所描述，當安全處理器 104(圖 1)交換上下文時，安全處理器可重設並啟動至新的上下文中。參考圖 2，CPU 啟動位址欄位 224 提供啟動安全處理器 104(圖 1)所在的記憶體 126(圖 1)中之位址。在一具體例中，啟動位址 224 為快閃記憶體中之偏移。在其他具體例中，啟動位址 224 為 ROM 位址、RAM 位址、或記憶體 126 之其他位址。在一具體例中，每一上下文可具有唯一的啟動位址 224。

信任向量描述符 202、204、及 206 亦可包括簽名欄位 226。簽名欄位 226 提供用於驗證每一信任向量描述符 202、204、206 中的例如私密密鑰之資料值。信任向量描述符之驗證可在指導信任向量驗證器 108(圖 1)載入一給定信任向量描述符之前或之後發生。另外，簽名欄位 226 可被組態成為提供用於驗證給定信任向量描述符的欄位 208 至 228 中之資料中之一些或全部中的簽名。另外，應

瞭解，如結合圖 6 所闡述，給定軟體部分中之一些，無給定軟體部分或給定軟體部分之全部可被擦拭，或在允許安全處理器 104(圖 1)執行給定軟體部分中之一些或全部之前被鑑定。

在本發明之至少一具體例中，信任向量描述符亦可被組態成為包括代碼簽名欄位 228，而代碼簽名欄位 228 提供用於驗證給定軟體代碼部分(在由安全處理器執行給定軟體代碼部分之前)中之資料。應瞭解，任何類型之數位簽名可用作簽名 226 及/或代碼簽名 228。舉例而言，數位簽名可使用私密及公用密鑰系統，諸如描述於 1994 年 5 月 19 日之 Digital Signature Standard (DSS), Federal Information Processing Standard Publication 186 中的彼等鑑定方法，該文件關於其所教示之全部內容且特別關於其對於數位簽名、私密密鑰系統及公用密鑰系統之使用的教示而以全文引用方式併入本文中。

一展示程序 300 之具體例的流程圖展示於圖 3A 及圖 3B 中，程序 300 係用於交換上下文 301 且用於管理安全異常 309。上下文交換程序可由上下文管理器、安全處理器、及/或安全處理器與上下文管理器之組合執行。如圖 3A 所示，目前由安全處理器 104(圖 1)所執行之上下文被儲存(操作 303)。在至少一具體例中，安全處理器 104(圖 1)在上下文交換發生之前儲存指向堆疊之指標，將任何所需資料儲存至記憶體 126(圖 1)，且完成任何“清除”功能。儲存操作可在上下文交換之前(如圖 3A 所示)、按需

求、以規律間隔、在根據需要之基礎上、及/或以其他方式發生。上下文交換程序亦可包括上下文交換請求之傳送(操作 302)。此請求通常自安全處理器發送至上下文管理器，且可在請求上下文交換之前或之後發生，且可在多種環境中發生。

舉例而言，安全處理器 104(圖 1)可在導致安全處理器需要在不同的或第二上下文下執行第二軟體部分之情形發生時執行第一軟體部分。為了促使第二軟體部分之執行，安全處理器 104(圖 1)可被組態成為將交換上下文之請求傳送至上下文管理器 106(圖 1)—如在圖 3A 中由操作 302 所示。上下文交換請求可包括(例如)安全處理器 104(圖 1)希望交換至的上下文 202(圖 2)之上下文 ID 208(圖 2)。上下文交換請求可視所使用之特定實施或具體例而包含額外或其他資訊。

如圖 3A 進一步所展示，上下文交換程序可包括重設安全處理器 104(操作 304)。亦即，安全處理器可由上下文管理器在接收到由安全處理器所傳送之上下文交換請求之後重設。安全處理器重設滿意地抹除安全處理器快取記憶體 122、MMU 128、暫存器 124、記憶體、或其類似物中之任何資料，且自安全處理器 104(圖 1)清除先前軟體狀態。又，應瞭解各種具體例可包括在不完成請求操作 302 及/或儲存操作 303 的情況下的重設操作 304。

如圖 3A 進一步所展示，上下文交換程序亦可包括將信任向量載入信任向量驗證器(操作 306)。在需要時，上下

文管理器 106(圖 1)將諸如描述符 202(圖 2)之信任向量描述符載入信任向量驗證器 106(圖 1)。如上文關於本發明之特定具體例所描述，信任向量驗證器可預載有處於非動作狀態中之描述符。因此，應易於瞭解，對於任何給定具體例，信任向量驗證器之載入可為可選及/或非必要的。

上下文交換程序亦包括致能新上下文(操作 308)，使得載入至信任向量驗證器中或在必要時針對動作狀態以其他方式表示之軟體部分準備好配合新上下文而使用。在一些具體例中，信任向量描述符 202(圖 2)可藉由相對於所產生之簽名比較儲存於信任向量描述符 202(圖 2)中之簽名 226(圖 2)來鑑定。此鑑定在將描述符載入信任向量驗證器 108 之前或之後發生。同樣地，待於新上下文下所執行之軟體部分可藉由相對於所產生之簽名比較代碼簽名 228(圖 2)而鑑定。鑑定信任向量描述符及軟體部分結合圖 6 在下文較為詳細地被描述。信任向量描述符 202 及軟體部分之載入滿意地組態安全處理器用於在新上下文中之軟體的執行。

用於管理安全異常 309 之程序的具體例展示於圖 3B 中。對於至少此具體例，一資源請求由信任向量驗證器 108(圖 1)自安全處理器 104(圖 1)接收。在資源請求之接收(操作 310)時，信任向量驗證器比較該請求與目前的動作信任向量描述符，且判定請求是否符合描述符(操作 312)。舉例而言，信任向量驗證器可比較一請求記憶體位址與目前動作信任向量描述符中之授權記憶體資料區域

222(圖 2)的清單。

當請求符合目前動作信任向量描述符時，信任向量驗證器允許通訊在安全處理器與資源之間發生(操作 316)。舉例而言，信任向量驗證器將資源請求 118(圖 1)傳遞至適當資源 120(圖 1)。

當請求不符合信任向量描述符時，可觸發安全異常(操作 320)，其導致安全處理器之重設(操作 330)。在至少一具體例中，信任向量驗證器向安全處理器發送硬體中斷或重設指令，(諸如指令 121(圖 1))。另外，對於至少一具體例，整個晶片組而非僅僅安全處理器可在安全異常發生時被重設。

該程序可進一步包括最近觸發之安全異常是否為安全異常發生之第二次發生的任選判定(操作 322)。當最近觸發之安全異常不為第二次安全異常時，可指導信任向量驗證器等待預定或即時判定之時間週期(操作 326)。另外且對於至少一具體例，信任向量驗證器可被程式化以警告安全處理器，其將在給定等待時間週期期滿後被重設。應瞭解在等待週期期間，安全處理器可完成額外處理動作且/或請求額外資源。在等待週期期滿時，安全處理器即被重設(操作 330)。

在至少一具體例中，安全處理器之重設可在至少兩個單獨的情形下發生。第一，安全處理器 104(圖 1)可藉由上下文管理器 106(圖 1)回應於上下文交換而重設。上下文交換重設抑制可能插入系統 100(圖 1)中之任何惡意代碼

存取與另一上下文相關聯之狀態資訊。第二，安全處理器104可在無論何時信任向量驗證器108(圖1)回應於一或多個安全異常，起始安全處理器104(圖1)及/或任何支援電路之硬體重設或硬體啟動時被重設。在此情形下，安全異常硬體重設防止惡意代碼完成在目前上下文中未被授權之程序。因此，應瞭解上下文交換及安全異常可起始促使安全處理器、記憶體、資源、及其類似物之安全且/或授權使用之重設，且提供針對該等組件之不安全且/或未授權使用的某一程度之保護。

包括安全操作環境402之具體例的設備400之具體例之方塊圖展示於圖4中。設備400可為(例如)衛星電視轉換設備。在至少一具體例中，設備400可包括控制電子426，控制電子426可進一步包括(但不限於)安全操作環境402、主處理器環境404、記憶體406、周邊介面408、及資料儲存介面410(在(諸如)由硬碟機434提供外部資料儲存時使用)中之一或多者。更具體言之，安全操作環境402可包括第一安全操作環境412及第二安全操作環境418，而第一安全操作環境412包括第一安全處理器414及第一信任向量驗證器416，且第二安全操作環境418包括第二安全處理器420及第二信任向量驗證器422。安全操作環境之其他具體例可包括單一安全處理器、多個安全處理器、單一向量驗證器、多個向量驗證器、單一操作環境、或多個操作環境。第一安全操作環境412及第二操作環境418亦可可操作地連接至一或多個共同或專用上下

文管理器 424。因此，應瞭解環境、處理器、向量驗證器、及上下文管理器之各種組合可被使用。

如圖 4 進一步所展示，控制電子 426 亦可包括系統匯流排 432。至及自匯流排之通訊可如圖 4 所示為直接的，且/或經由一或多個獨立或整合之匯流排主控器(bus master)或其類似物。舉例而言，安全處理器 414/420 可包括匯流排主控器。

信任向量驗證器 416、422、及 430 滿意地被組態成為分別自安全處理器傳達通訊至系統匯流排 432/自系統匯流排 432 傳遞通訊至安全處理器。另外，應瞭解一或多個安全處理器(例如，安全處理器 414 及 420)可被組態成為執行控制電子 426 之相同(平行)或不同功能或工作。舉例而言，處理器 414 可被組態成為處理顯示資料及使用者命令，而處理器 420 被組態成為處理安全功能，例如，解密視訊信號、驗證使用者觀看權、及與電視轉換設備 400 之其他組件相互作用。

包括安全處理器 414 及 420、信任向量驗證器 416 及 422、及上下文管理器 424 之安全操作環境 402 可提供於一或多個積體電路或分離的離散組件中。舉例而言，處理器 414 及 420 可分別與信任向量驗證器 416 及 422 組合為單一積體電路或兩個單獨的積體電路(亦即，針對每一安全操作環境 412 及 418 之一積體電路)。

另外，安全處理器 414 及 420、信任向量驗證器 416 及 422、上下文管理器 424、及/或其他組件可提供於硬體及

/或軟體之任何所要組合中。舉例而言，上下文管理器 424 可為包括一或多個程序之軟體模組。同樣地，包括一或多個邏輯組件之硬體電路可被使用。

控制電子 426 亦可包括一或多個揮發性及/或非揮發性記憶體組件 406。該等記憶體設備之例子包括(但不限於)隨機存取記憶體及快閃記憶體。

安全處理器 414 及 420 及/或上下文管理器 424 亦可或者替代地連接至一或多個共同或單獨記憶體組件或者記憶體範圍(未圖示)。記憶體組件(其可為安全的)可用以儲存(例如)TVT 200(圖 2)及/或對應於一或多個上下文之一或多個信任向量描述符 202(圖 2)。同樣，記憶體組件可被組態成為儲存用於一計算簽名與信任向量描述符及/或軟體部分之參考簽名之比較中的一計算雜湊。

可將上下文記憶體範圍、參考簽名、及信任向量描述符儲存於不安全記憶體 406 中。舉例而言，可將上下文記憶體範圍、參考簽名、及/或信任向量描述符儲存於可重寫及揮發性記憶體中，諸如隨機存取記憶體(RAM)、動態 RAM (DRAM)、靜態 RAM (SRAM)、或快閃記憶體。在至少一具體例中，上下文管理器 424 可藉由使用指標、記憶體位址、或類似參考而與記憶體 406 通訊。

在至少一具體例中，安全處理器 414 及 420 以及信任向量驗證器 416、422、及 430 可為通用處理器。安全處理器亦可包括(但不限於)快取記憶體及記憶體管理單元(MMU)。安全處理器亦可在需要時執行指令取出、資料讀

取/寫入、I/O讀取/寫入、及其他功能與常式。

一或多個信任向量驗證器416、422、及430利用一或多個位址檢查器來在安全處理器414及420與系統匯流排432、記憶體406、周邊介面408、資料儲存介面410、及/或控制電子426之其他組件之間傳達存取。另外，信任向量驗證器416、422、及430防止自處理器414、420、或428至系統匯流排432之直接連接，及藉由其延伸至記憶體406、周邊介面408、或硬碟機介面410之連接。藉由充當處理器與匯流排之間的閘道管理器(gatekeeper)，信任向量驗證器可控制並促使安全處理器與其他系統組件之間的連接及/或隔離。

信任向量驗證器可視其所用於之具體例而被組態成為在任何給定時間處理一或多個上下文。同樣，信任向量驗證器416可被組態成為位址檢查器，以儲存並驗證對於給定上下文之有效記憶體範圍。此資訊可(例如)儲存為信任向量描述符中之個別項。熟習此項技術者將認識到處理上下文資料之其他方式為可能的，且在於本發明之各種具體例之範疇內。

信任向量驗證器可被組態成為在無論何時一或多個處理器存取請求在有效範圍外之判定係達到時藉由以信號通知、以旗標表示、安全異常、或其他方式作出回應。同樣地，信任向量驗證器可被組態成為驗證針對記憶體406之任何範圍的存取模式，諸如讀取、讀取/寫入、及寫入。舉例而言，信任向量驗證器416可被組態，使得在由安全

處理器 414 接收到寫入請求時，其判定資料記憶體範圍是否為針對各別上下文之有效範圍，及資料記憶體範圍是否允許寫入存取。舉例而言，若寫入存取不被允許，則信任向量驗證器 416 可被組態成為以旗標表示一安全異常。

在各種具體例中，用以儲存程式代碼或資料之記憶體範圍可為鄰近或非鄰近的。舉例而言，記憶體範圍可為一或多個位址及一或多個自-至位址之長度的形式。同樣地，記憶體範圍可利用一或多個記憶體組件或設備。舉例而言，記憶體範圍可在結合有三個 EEPROM 記憶體組件之利用兩個 DDR-SDRAM 記憶體組件、一個 DDR-SDRAM 記憶體組件、及/或實際及/或虛擬記憶體及/或資料儲存設備之其他組合。該等設備可接近或遠離給定控制電子。

進一步參考圖 4，信任向量描述符亦可用以部分或全部地授權對應於一或多個上下文之周邊組件。舉例而言，信任向量描述符可授權經由周邊介面 408 對智慧卡 436、遙控器 438、電視、及/或其他周邊裝置中之一或多者的存取。該一或多個周邊裝置可藉由項指標及周邊範圍而表示於(例如)信任向量表中。範圍可以一或多個自-至位址之形式表示。如結合圖 2 所闡述，位元映射可用以授權上下文之信任向量描述符內的周邊裝置，例如，將位元映射“0101B”解譯為授權周邊組件一(1)及三(3)。

在圖 4 所示之具體例中，上下文管理器 424 負責管理安全處理器 414 及 420 上之安全上下文交換。在一具體例中，在初始階段期間(亦即，在電視轉換器設備 400 之啟

動程序期間)，上下文管理器 424 自記憶體 406 接收一或多個上下文之信任向量描述符。在將信任向量描述符載入上下文管理器 424 之前，信任向量描述符之完整性可藉由鑑定信任向量描述符而驗證。舉例而言，信任向量描述符之完整性可藉由使用雜湊函數來計算一摘錄、藉由密鑰對該摘錄簽名以產生一計算簽名、且比較該計算簽名與參考簽名 226(圖 2)而驗證。在此例子中，若計算簽名與參考簽名之比較不匹配，則可產生安全異常或者可警告控制電子 426，且上下文管理器 424 將不能夠致能軟體。

在至少一具體例中，信任向量驗證器 416 及 422 可將信任向量描述符限制於記憶體 406 之特定範圍。舉例而言，在初始階段啟動程序期間及在信任向量驗證器 416 及 422 自上下文管理器 424 接收到一或多個命令之前，一或多個信任向量描述符可自記憶體 406 之特定界定之範圍且不自記憶體之其他範圍載入。

在其他具體例中，列於信任向量描述符中的儲存於自區域 210(圖 2)至區域 212(圖 2)之記憶體範圍中之代碼亦可針對該一或多個上下文而被鑑定。同樣，上下文管理器 424 可儲存用於針對進一步上下文驗證之鑑定中的計算雜湊。

如針對至少一具體例結合圖 3 所闡述，安全處理器 414 及 420 可藉由向上下文管理器 424 傳輸信號(例如，對上下文交換之請求)而改變上下文。上下文管理器 424 在接收到一或多個信任向量描述符之表示時，驗證對應於該一

或多個上下文的程式記憶體範圍之確實性。一旦上下文記憶體範圍得到驗證，上下文管理器 424 通知記憶體 406 之範圍之對應於所驗證之上下文的信任向量驗證器 416 及 422，以用於載入信任向量描述符。在一具體例中，在初始化時、連續地、隨機地、根據排程、或回應於某一事件來驗證記憶體 406 之程式記憶體範圍及資料記憶體範圍之參考簽名。

對應於一或多個上下文的記憶體 406 之範圍及參考簽名可被封裝且/或儲存於不安全位置。舉例而言，可將對應於一或多個上下文的記憶體 406 之範圍及參考簽名封裝於定義標頭(definition header)中。另外，不對稱密鑰可用以導出簽名。然而，應瞭解安全儲存之對稱密鑰可亦用以導出簽名。

再次參考圖 4，控制電子 404 可包括主處理器操作環境 404，而主處理器操作環境 404 進一步包括主處理器 428 及主信任向量驗證器 430。在至少一具體例中，主處理器環境 404 可用以執行(例如)使用者介面及其他軟體常式。通常，此常式不需要與由安全處理器 414 及 416 所執行之常式有相同的安全等級。

另外，不能夠執行上下文交換之特定程序(諸如 Linux 作業系統)通常由主處理器 428 而非安全處理器 414 執行。另外，主環境可被組態成為包括信任向量驗證器 430，而信任向量驗證器 430 被組態成為傳達由主處理器對一或多個資源之存取。另外，可將上下文管理器自主環境排

除，且藉此消除由主處理器進行之上下文交換。

圖 5 提供用於至少一具體例中之設備的方塊圖。如圖所示，此設備 500 包括一安全操作環境 502，而安全操作環境 502 具有一安全處理器 410 及一上下文管理器 424。另外，此設備包括一主處理環境 404，而主處理環境 404 包含一主處理器 512。安全處理器 410 及主處理器 512 經由匯流排 432 而互連。信任向量驗證器 504、506、及 508 連接至匯流排 432，且被組態成為傳達安全處理器 510 及/或主處理器 512 的對一或多個資源之存取請求。信任向量驗證器 504、506、及 508 可被組態成為相對於安全處理器 410 非同步操作。更具體言之，在初始階段(例如，啟動序列)期間，以關於特定上下文(或更特定言之，關於安全水準)的記憶體 406 之範圍，上下文管理器 424 載入信任向量驗證器 504、506、及 508。此上下文接著可用於處理器與資源之間的所有通訊，直至上下文改變被執行且新信任向量描述符被載入至一或多個向量驗證器中。因此，應瞭解安全處理器經由其相關聯之上下文管理器判定其自身及主處理器所利用的向量驗證器之組態。

在另一具體例中，個別組件可具有一個以上信任向量驗證器，且一個以上安全處理器可存取相同驗證器模組。舉例而言，在多安全處理器組態中，每一組件之多個信任向量驗證器允許每一組件之兩個或兩個以上上下文之進一步非同步處理。在又一具體例中，無需由信任向量驗證器 504、506、及 508 傳達之另一連接的情況下或除該另一連

接以外，一或多個組件單獨連接至系統匯流排 432。

現參考圖 6，用於為軟體部分、信任向量描述符、或資料擦拭或鑑定記憶體範圍之程序 600 針對本發明之至少一具體例被展示。如圖所示，產生指定用於鑑定之局部資料的雜湊(操作 610)。舉例而言，控制電子 426(圖 4)判定記憶體範圍之雜湊值或其他類似值。

雜湊以一密鑰簽名，且藉此產生一計算簽名(操作 612)。在至少一具體例中，參考雜湊可以公共密鑰簽名，以產生該計算簽名。計算簽名被儲存用於比較(操作 613)。

如圖 6 進一步所展示，鑑定程序可包括擷取一參考簽名(操作 614)。對於至少一具體例，上下文管理器 106(圖 1)擷取信任向量資料結構之簽名欄位 226(圖 2)或代碼簽名欄位 228(圖 2)之參考簽名。然而，應瞭解參考簽名可自不同資料結構擷取或自另一組件接收。舉例而言，上下文管理器可自安全記憶體擷取簽名。在至少一具體例中，先前雜湊藉由私密密鑰簽名，以產生參考簽名。

如圖 6 進一步所展示，鑑定程序可包括比較該計算簽名與參考簽名(操作 616)。亦即，上下文管理器 106(圖 1)可以數學方式比較藉由用公共密鑰對雜湊簽名而產生的計算簽名與自信任向量資料結構所擷取之參考簽名。應瞭解，計算簽名與參考簽名之比較可藉由逐位元比較或其他計算程序完成。若該等簽名比較，則鑑定軟體部分、信任向量描述符、或資料。

鑑定程序視情況包括判定鑑定程序是否連續(操作

618)。在至少一具體例中，上下文管理器 106(圖 1)判定在信任向量描述符中之擦拭類型資料欄位 218(圖 2)的設定。舉例而言，若在擦拭類型資料欄位 218 中設定連續擦拭類型位元，則上下文管理器 106(圖 1)判定該鑑定為連續的。應瞭解，上下文管理器 106(圖 1)可藉由檢查連同軟體部分、信任向量描述符、或資料所發送之標頭中的數值，藉由擷取記憶體之另一部分中的設定，或藉由自另一組件擷取指令而判定鑑定之類型。

若鑑定為連續的，則圖 6 所示的鑑定程序之另一具體例可視情況包括等待一時間之週期以對相同一軟體部分、信任向量描述符、或資料執行另一鑑定(操作 620)。在至少一具體例中，上下文管理器 106(圖 1)等待預定時間週期，且接著完成對相同軟體部分、信任向量描述符、或資料之另一鑑定。預定時間週期可為係一秒之小部分、數秒、數分鐘、數小時、數日等等的任何時間週期。在至少一具體例中，上下文管理器 106(圖 1)中之計時器對預定時間週期進行計數。在達到設定界限時，再次執行鑑定程序。

根據以上內容，一具體例包括用於在安全計算環境中執行軟體之系統。該系統包括被組態成為在自第一軟體部分向第二軟體部分切換執行時請求自第一上下文至第二上下文之上下文交換的安全處理器。該系統進一步包括與安全處理器通訊之上下文管理器，其被組態成為接收所請求之上下文交換且起始上下文交換。該系統進一步包括與安

全處理器及上下文管理器通訊之信任向量驗證器，其被組態成為在來自上下文管理器之命令時載入信任向量描述符。

在至少一具體例中，上下文管理器回應於上下文交換以起始安全處理器之重設。

在至少一具體例中，上下文管理器使信任向量描述符與第二上下文相關聯。

在至少一具體例中，信任向量驗證器根據信任向量描述符控制由安全處理器對一或多個資源之存取。

在至少一具體例中，系統包括與上下文管理器通訊之第二安全處理器。第二安全處理器執行一或多個其他軟體部分，且被組態成為在自第三軟體部分向第四軟體部分切換執行時請求自第三上下文至第四上下文之上下文交換。系統亦包括與第二安全處理器及上下文管理器通訊之第二信任向量驗證器，其被組態成為在來自上下文管理器之命令時載入第二信任向量描述符。信任向量驗證器被組態成為根據第二信任向量描述符控制由第二安全處理器對一或多個資源之存取。

在至少一具體例中，系統包括被組態成為在靜態上下文中執行軟體部分之主處理器。系統亦包括與主處理器通訊之主信任向量驗證器，其被組態成為在靜態上下文中載入信任向量描述符，且控制由主處理器對一或多個資源之存取。

在至少一具體例中，系統包括與主信任向量驗證器通訊

之匯流排主控器，其被組態成為在靜態上下文中執行操作。

在至少一具體例中，於靜態上下文中所執行之軟體部分為作業系統。

另一具體例包含用於在安全計算環境中執行軟體之系統。該系統包括兩個或兩個以上安全處理器，其中每一安全處理器被組態成為在自第一軟體部分向另一軟體部分切換執行時請求自第一上下文至另一上下文之上下文交換。系統進一步包括與兩個或兩個以上安全處理器中之每一者通訊的上下文管理器，其被組態成為接收由兩個或兩個以上安全處理器中之至少一者所請求的上下文交換。回應於所接收之請求，上下文管理器起始請求安全處理器之重設，且使另一請求之上下文與第一信任向量描述符相關聯，該第一信任向量描述符被組態用於控制對至少一資源之存取中。上下文管理器進一步起始至另一請求之上下文的交換。系統亦包括被組態成為在靜態上下文中執行作業系統之主處理器。系統亦包括複數個信任向量驗證器，其中每一信任向量驗證器與安全處理器中之至少一者及主處理器通訊。信任向量驗證器被組態成為載入與所請求之上下文相關聯的第一信任向量描述符、或被組態用於控制由主處理器對一或多個資源之存取中的主信任向量描述符。

在至少一具體例中，安全處理器中之一者被組態成為在自第一軟體部分向第二軟體部分切換執行時請求自第一

上下文至第二上下文之第一上下文交換。

在至少一具體例中，安全處理器中之一者被組態成為在自第三軟體部分向第四軟體部分切換執行時請求自第三上下文至第四上下文之第二上下文交換。

在至少一具體例中，第二軟體部分與第四軟體部分實質上為類似的。

另一具體例包含用於在接收到用以交換至用於一軟體部分之上下文之請求時在安全操作環境中執行軟體之方法。該方法包括載入組態用於控制處理器之操作及重設處理器中的信任向量描述符。

在至少一具體例中，信任向量描述符界定由處理器對一或多個周邊設備之存取，且信任向量驗證器控制由處理器對該或該等周邊設備之存取。

在至少一具體例中，信任向量描述符包含位元映射。

在至少一具體例中，該方法進一步包括鑑定軟體部分。

在至少一具體例中，鑑定操作包括產生軟體部分之雜湊，對所產生之雜湊簽名以產生一計算簽名，擷取一參考簽名及比較參考簽名與計算簽名。若簽名為相同的，則該方法進一步包括允許軟體部分之執行。

在至少一具體例中，該方法包括等待一時間週期及執行軟體部分之第二鑑定。

在至少一具體例中，第二鑑定在軟體鑑定為連續時發生。

在至少一具體例中，該方法包括自安全處理器接收一資

源請求及判定資源請求是否符合信任向量描述符。若資源請求不符合信任向量描述符，則該方法包括觸發一安全異常及重設安全處理器。

在至少一具體例中，該方法進一步包括判定安全異常是否為第二安全異常。若安全異常並非為第二安全異常，則該方法包括在重設安全處理器之前等待一時間週期。若安全異常為第二安全異常，則該方法進一步包括重設安全處理器而不等待該時間週期。

一具體例為包括安全處理器之裝置，該安全處理器組態成為請求至用於軟體部分之一上下文之上下文交換，且藉由產生軟體部分之雜湊而鑑定軟體部分。安全處理器進一步組態成為對該產生雜湊簽名以產生一計算簽名，擷取一參考簽名且比較參考簽名與計算簽名。若簽名相同，則安全處理器允許軟體部分之執行。該裝置亦包括上下文管理器，該上下文管理器組態成為接收該請求上下文交換，載入信任向量驗證器中之信任向量描述符且重設安全處理器。該裝置亦包括信任向量驗證器，該信任向量驗證器組態成為自安全處理器接收資源請求，且判定資源請求是否符合信任向量描述符。信任向量驗證器亦被組態成為在資源請求不符合信任向量描述符之情況下觸發一安全異常，且判定安全異常是否為第二安全異常。若安全異常並非第二安全異常，則信任向量驗證器在重設安全處理器之前等待一時間週期。然而，若安全異常為第二安全異常，則信任向量驗證器重設安全處理器而不等待該時間週期。

另一具體例包含具有一編碼資料結構之電腦可讀媒體，該編碼資料結構執行於一電腦系統上用於控制安全處理器之執行。資料結構包含一或多個上下文，其中每一上下文包含識別上下文之上下文識別欄位、表示記憶體之安全處理器可存取區域的記憶體資料區域、及表示安全處理器可存取硬體資源之硬體信任向量。該電腦系統被組態成為基於硬體信任向量來判定安全處理器是否可存取硬體資源。

在至少一具體例中，硬體信任向量為識別對於安全處理器所允許的存取類型之位元映射。

在至少一具體例中，資料結構包括代碼開始位址欄位。

在至少一具體例中，資料結構包括代碼結束位址欄位。

在至少一具體例中，資料結構包括密鑰號碼欄位、目標處理器欄位、向量號碼欄位、擦拭類型欄位、處理器啟動位址欄位、信任向量描述符簽名欄位、及代碼簽名欄位

在至少一具體例中，代碼開始位址欄位及代碼結束位址欄位界定在上下文中所執行之軟體部分的程式記憶體範圍。

在至少一具體例中，該擦拭類型欄位表示軟體部分之鑑定是否連續。

另一具體例為包含安全處理器及電腦可讀媒體之電腦系統。電腦可讀媒體包括具有一或多個上下文用於由安全處理器所執行之編碼資料結構。每一上下文包含上下文識別欄位、表示安全處理器可存取哪些硬體資源之硬體信任

向量、一代碼開始位址欄位、一代碼結束位址欄位、及一處理器啟動位址欄位。代碼開始位址欄位及代碼結束位址欄位界定在上下文中所執行之軟體部分的程式記憶體範圍。該電腦系統被組態成為基於硬體信任向量來判定安全處理器是否可存取硬體資源。

在至少一具體例中，上下文包含目標處理器欄位。

另一具體例包含用於保護計算系統免於惡意軟體攻擊之方法。該方法包括載入一信任向量描述符，該信任向量描述符界定上下文。該方法進一步包括接收惡意軟體及嘗試執行惡意軟體中之指令。該方法進一步包括識別該指令對於上下文為異常，防止指令執行及重設安全處理器。

在至少一具體例中，該方法包括接收用於惡意軟體之上下文交換。

在至少一具體例中，該方法包括識別惡意軟體。

在至少一具體例中，識別惡意軟體進一步包括產生惡意軟體之雜湊，自雜湊產生一計算簽名，擷取一參考簽名及比較計算簽名與參考簽名。若計算簽名與參考簽名不相同，則該方法進一步包括防止指令執行。

在至少一具體例中，該方法包括識別信任向量描述符。

在至少一具體例中，將指令儲存於在上下文中不可存取之記憶體區域中。

在至少一具體例中，該指令嘗試周邊設備或在上下文中不可存取之記憶體位置的存取。

雖然許多例示性態樣及具體例已在上文被論述，但熟習

此項技術者將認識到其特定修改、排列、添加、及子組合。因此，意欲將以下所附申請專利範圍及後文所引入之申請專利範圍說明為包括處於其真實精神及範疇內的所有該等修改、排列、添加、及子組合。

【圖式簡單說明】

圖 1 為用於本文描述的本發明之至少一具體例中之計算環境之方塊圖。

圖 2 為用於至少一具體例中之信任向量表之一具體例的簡化資料結構圖。

圖 3A 及圖 3B 為用於改變計算環境中之上下文且保持該計算環境之方法的具體例之流程圖。

圖 4 為用於至少一具體例中之設備的方塊圖。

圖 5 為用於另一具體例中之設備的方塊圖。

圖 6 為用於鑑定軟體代碼或資料之記憶體區域之方法的流程圖，該方法用於本文描述之本發明之至少一具體例中且/或配合該至少一具體例而使用。

【主要元件符號說明】

100 計算環境
102 虛線/安全計算或操作環境
104 安全中央處理單元(“CPU”)或安全處理器
106 上下文管理器
108 信任向量驗證器
110 上下文交換
112 重設
114 指令
116 通訊路徑
118 資源請求

120 資源
121 硬體中斷
122 快取記憶體
124 暫存器
126 資料儲存器/記憶體
128 記憶體管理單元(MMU)
200 信任向量表(TVT)資料結構
202 信任向量描述符
204 信任向量描述符
206 信任向量描述符
208 上下文識別(ID)欄位
210 代碼開始位址
212 代碼結束位址
214 密鑰號碼
216 目標CPU及向量號碼(#)/目標CPU欄位/向量號碼欄位
218 擦拭類型/擦拭類型欄位
220 硬體信任向量描述符/硬體信任向量描述符欄位
222 記憶體資料區域/記憶體資料區域欄位
224 CPU啟動位址/CPU啟動位址欄位
226 信任向量描述符簽名/簽名欄位
228 代碼簽名/代碼簽名欄位
300 程序
301 交換上下文
302 請求操作
303 儲存操作
304 重設操作
306 操作
308 操作
309 管理安全異常
310 操作
312 操作
316 操作
320 操作
322 操作
326 操作

330 操作
400 電視轉換設備
402 安全操作環境
404 主處理器環境
406 記憶體
408 周邊介面
410 資料儲存介面；安全處理器
412 第一安全操作環境
414 第一安全處理器
416 第一信任向量驗證器
418 第二安全操作環境
420 第二安全處理器
422 第二信任向量驗證器
424 上下文管理器
426 控制電子
428 主處理器
430 主信任向量驗證器
432 系統匯流排
434 硬碟機
436 智慧卡
438 遙控器
500 設備
502 安全操作環境
504 信任向量驗證器
506 信任向量驗證器
508 信任向量驗證器
512 主處理器
600 程序
610 操作
612 操作
613 操作
614 操作
616 操作
618 操作
620 操作

五、中文發明摘要：

本文描述之各種具體例係關於用於在一安全計算環境(100)中執行軟體之裝置。可使用一安全處理器(104)，且被組態成為在自一第一軟體部分向一第二軟體部分切換執行時請求一自一第一上下文至一第二上下文之上下文交換。一可與該安全處理器通訊之上下文管理器(106)可被組態成為接收並啟始一所請求之上下文交換。一可與該安全處理器及該上下文管理器通訊之信任向量驗證器(108)可被組態成為在接收到來自上下文管理器之命令時載入一信任向量描述符。

六、英文發明摘要：

Various embodiments described herein relate to apparatus for executing software in a secure computing environment (100). A secure processor (104) can be used and configured to request a context swap from a first context to a second context when switching execution from a first portion of software to a second portion of software. A context manager (106), which can be in communication with the secure processor, can be configured to receive and initiate a requested context swap. A trust vector verifier (108), which can be in communication with the secure processor and the context manager, can be configured to load a trust vector descriptor upon command from a context manager.

十、申請專利範圍：

1.一種裝置，其包含：

一安全處理器(104)，其可操作以執行軟體指令之第一及第二部分，且進一步可操作以產生在一與該等軟體指令之該第一部分相關聯的第一上下文與一與該等軟體指令之該第二部分相關聯的第二上下文之間所切換之一請求；

第一離散電路(106)，以通訊方式耦接至該安全處理器，該第一離散電路接收該請求，且在該第一上下文與該第二上下文之間起始一上下文切換，該第二上下文與一上下文識別符相關聯；及

第二離散電路(108)，以通訊方式耦接至該安全處理器及該第一離散電路，該第二離散電路可操作以基於該上下文識別符而在該安全處理器與至少一與該安全處理器相關聯之資源(120)之間傳達存取。

2.如申請專利範圍第1項之裝置，其中，該第二上下文與一信任向量描述符相關聯，且其中該第二離散電路回應於一來自該第一離散電路之命令而載入該信任向量描述符。

3.如申請專利範圍第2項之裝置，其中，該第二離散電路可操作以基於該信任向量描述符而在該安全處理器與該至少一資源之間傳達該存取。

4.如申請專利範圍第1項之裝置，其中，該第一離散電路回應於該請求以起始該安全處理器之一重設。

5.如申請專利範圍第1項之裝置，其中，該資源包含記

憶體(126)，且其中該第二離散電路在該安全處理器與該記憶體之間傳達存取。

6.如申請專利範圍第1項之裝置，其中，該資源包含至少一周邊設備(408)，且其中該第二離散電路在該安全處理器與該至少一周邊設備之間傳達存取。

7.一種裝置，其包含：

一主處理器(512)，其可操作以在一靜態上下文中執行第一軟體指令；

一安全處理器(410)，其可操作以執行第二軟體指令之第一及第二部分，且進一步可操作以產生在一與該等第二軟體指令之該第一部分相關聯的第一上下文與一與該等第二軟體指令之該第二部分相關聯的第二上下文之間所切換之一請求；

第一離散電路(424)，以通訊方式耦接至該安全處理器，該第一離散電路接收該請求，且在該第一上下文與該第二上下文之間起始一上下文切換，該第二上下文與一上下文識別符相關聯；

一匯流排(432)，其以通訊方式耦接至該主處理器及該安全處理器；

至少一資源(406、408、434、436)，其經由該匯流排以通訊方式耦接至該主處理器及該安全處理器；及

第二離散電路(504、506、508)，其以通訊方式耦接至該匯流排，且可操作以基於該上下文識別符傳達由該安全處理器及該主處理器對該至少一資源之存取。

8.如申請專利範圍第 7 項之裝置，其中，該第二上下文與一信任向量描述符相關聯，且其中該第二離散電路回應於一來自該第一離散電路之命令而載入該信任向量描述符，該第二離散電路可操作以基於該信任向量描述符來傳達由該主處理器及該安全處理器對該至少一資源之該存取。

9.如申請專利範圍第 7 項之裝置，其中，該第一離散電路回應於該請求以起始該安全處理器之一重設。

10.如申請專利範圍第 7 項之裝置，其中，該資源包含記憶體(406)，且其中該第二離散電路傳達由該主處理器及該安全處理器對該記憶體之存取。

11.如申請專利範圍第 7 項之裝置，其中，該資源包含至少一周邊設備(434)，且其中該第二離散電路傳達由該主處理器及該安全處理器對該至少一周邊設備之存取。

12.如申請專利範圍第 7 項之裝置，其中，該至少一周邊設備包含一硬碟機。

13.一種裝置，其包含：

一第一安全處理器(414)，其可操作以執行軟體指令之第一及第二部分，且進一步可操作以產生在一與該等軟體指令之該第一部分相關聯的第一上下文與一與該等軟體指令之該第二部分相關聯的第二上下文之間切換之一第一請求；

一第二安全處理器(420)，其可操作以執行該等軟體指令之第三及第四部分，且進一步可操作以產生在一與該等

軟體指令之該第三部分相關聯的第三上下文與一與該等軟體指令之該第四部分相關聯的第四上下文之間切換之一第二請求；

一離散上下文管理器電路(424)，以通訊方式耦接至該第一及該第二安全處理器，該離散上下文管理器電路接收該第一請求且在該第一上下文與該第二上下文之間起始一第一上下文切換，該第二上下文與一第一上下文識別符相關聯，且其進一步接收該第二請求且在該第三上下文與該第四上下文之間起始一第二上下文切換，該第四上下文與一第二上下文識別符相關聯；

一第一離散信任向量驗證器電路(416)，以通訊方式耦接至該第一安全處理器及該離散上下文管理器電路，該第一離散信任向量驗證器電路可操作以基於該第一上下文識別符在該安全處理器與至少一與該第一安全處理器相關聯之資源(406、408、434、436)之間傳達存取；及

一第二離散信任向量驗證器電路(422)，以通訊方式耦接至該第二安全處理器及該離散上下文管理器電路，該第二離散信任向量驗證器電路可操作以基於該第二上下文識別符在該第二安全處理器與該至少一資源之間傳達存取。

14.如申請專利範圍第13項之裝置，其中，該第二上下文與一第一信任向量描述符相關聯，且其中該第一離散信任向量驗證器回應於一來自該離散上下文管理器之命令而載入該第一信任向量描述符，其中該第一離散信任向量

驗證器電路可操作以基於該第一信任向量描述符在該第一安全處理器與該至少一資源之間傳達該存取。

15.如申請專利範圍第13項之裝置，其中，該第一離散信任向量驗證器電路回應於該請求以產生一起始該安全處理器之一重設的信號。

16.如申請專利範圍第13項之裝置，進一步包含：

一主處理器(428)，其可操作以在一靜態上下文中執行第二軟體指令；及

一主信任向量驗證器電路(430)，以通訊方式耦接至該主處理器，該主信任向量驗證電路(430)自該離散上下文管理器接收一命令以載入一信任向量描述符，且基於該信任向量描述符在該靜態上下文中傳達由該主處理器對該至少一資源之存取。

17.如申請專利範圍第16項之裝置，其中，該至少一資源包含一可由該第一安全處理器、該第二安全處理器、及該主處理器所存取之記憶體(406)。

18.如申請專利範圍第16項之裝置，其中，該至少一資源包含一可由該第一安全處理器、該第二安全處理器、及該主處理器所存取之周邊設備(434)。

19.如申請專利範圍第17項之裝置，其中，該等第二軟體指令包含一在該靜態上下文中所執行之作業系統。

20.如申請專利範圍第19項之裝置，其中，該作業系統可以一電視接收器而操作。

十一、圖式：

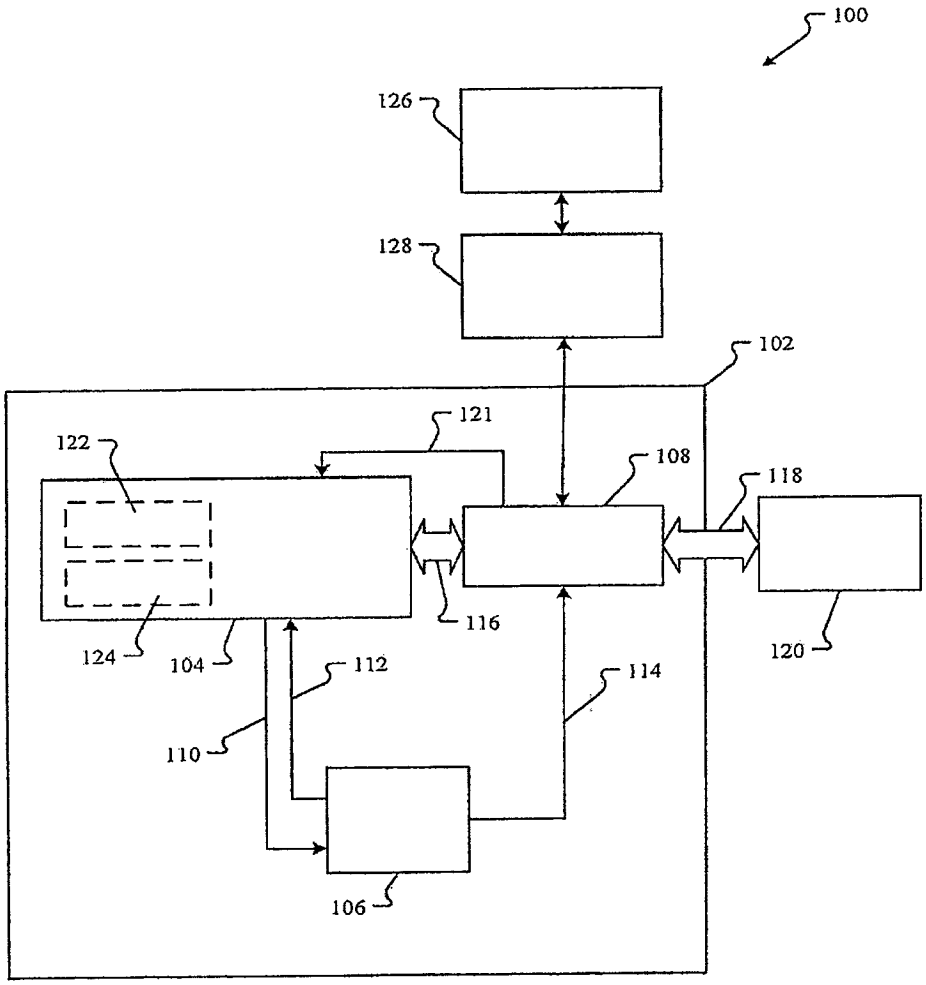


圖 1

200901034

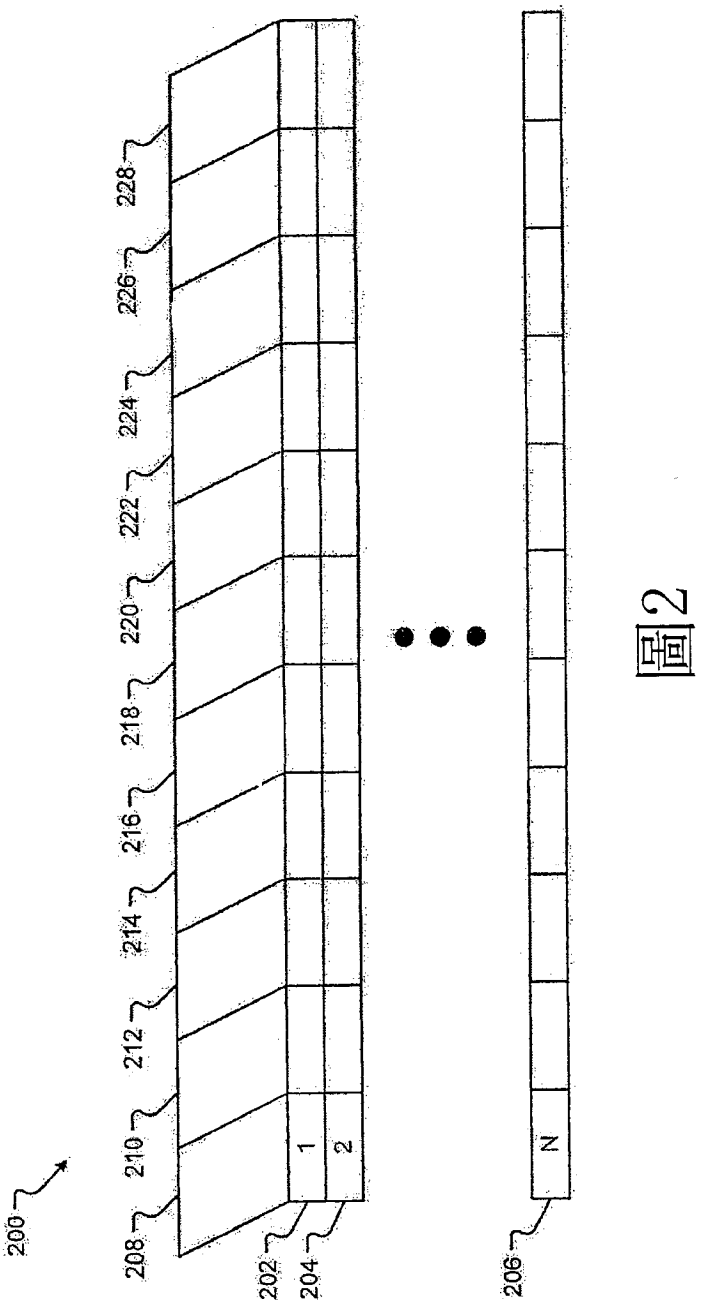


圖2

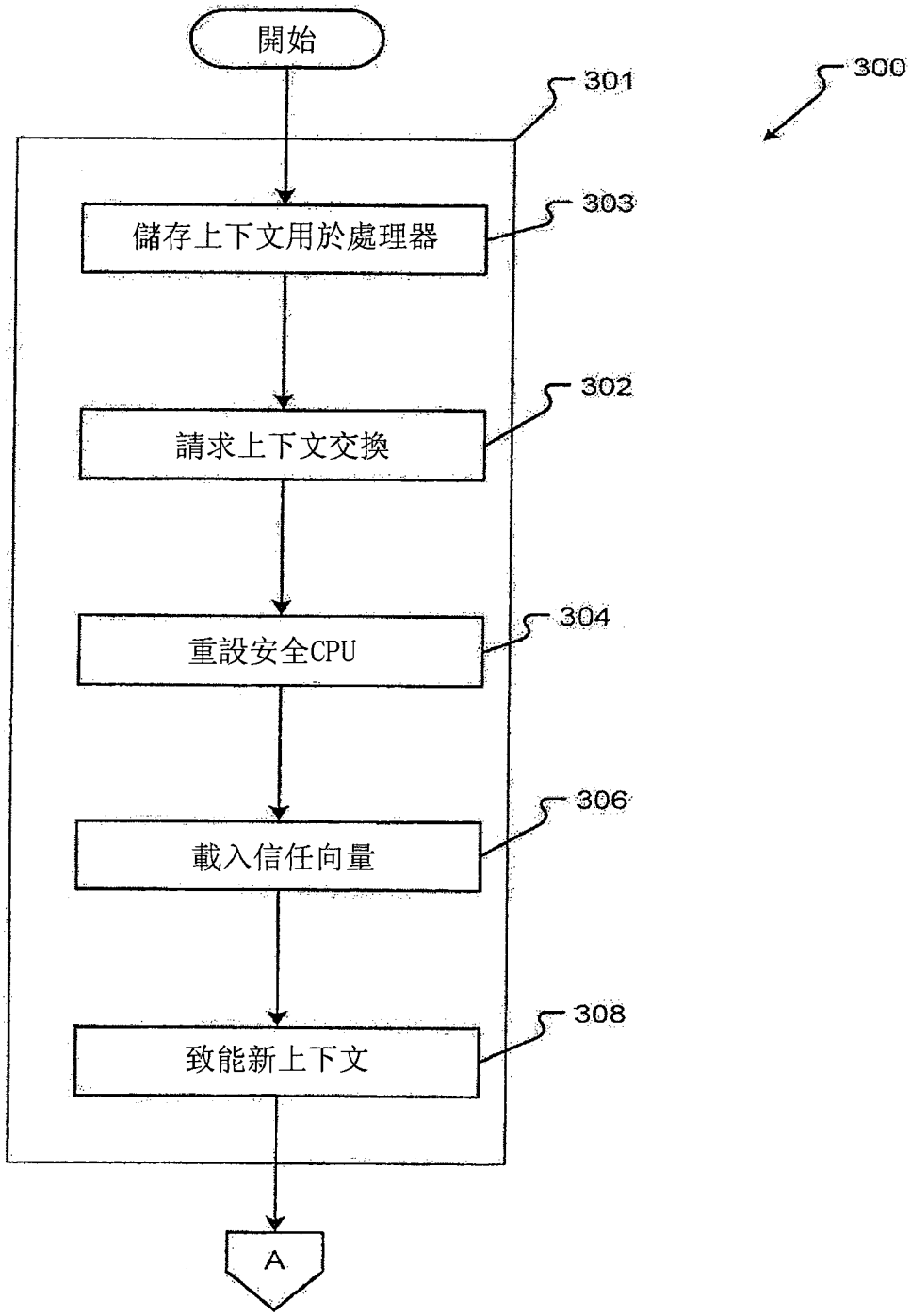

開始
300
301
303
儲存上下文用於處理器
302
請求上下文交換
304
重設安全CPU
306
載入信任向量
308
致能新上下文
A

圖3A

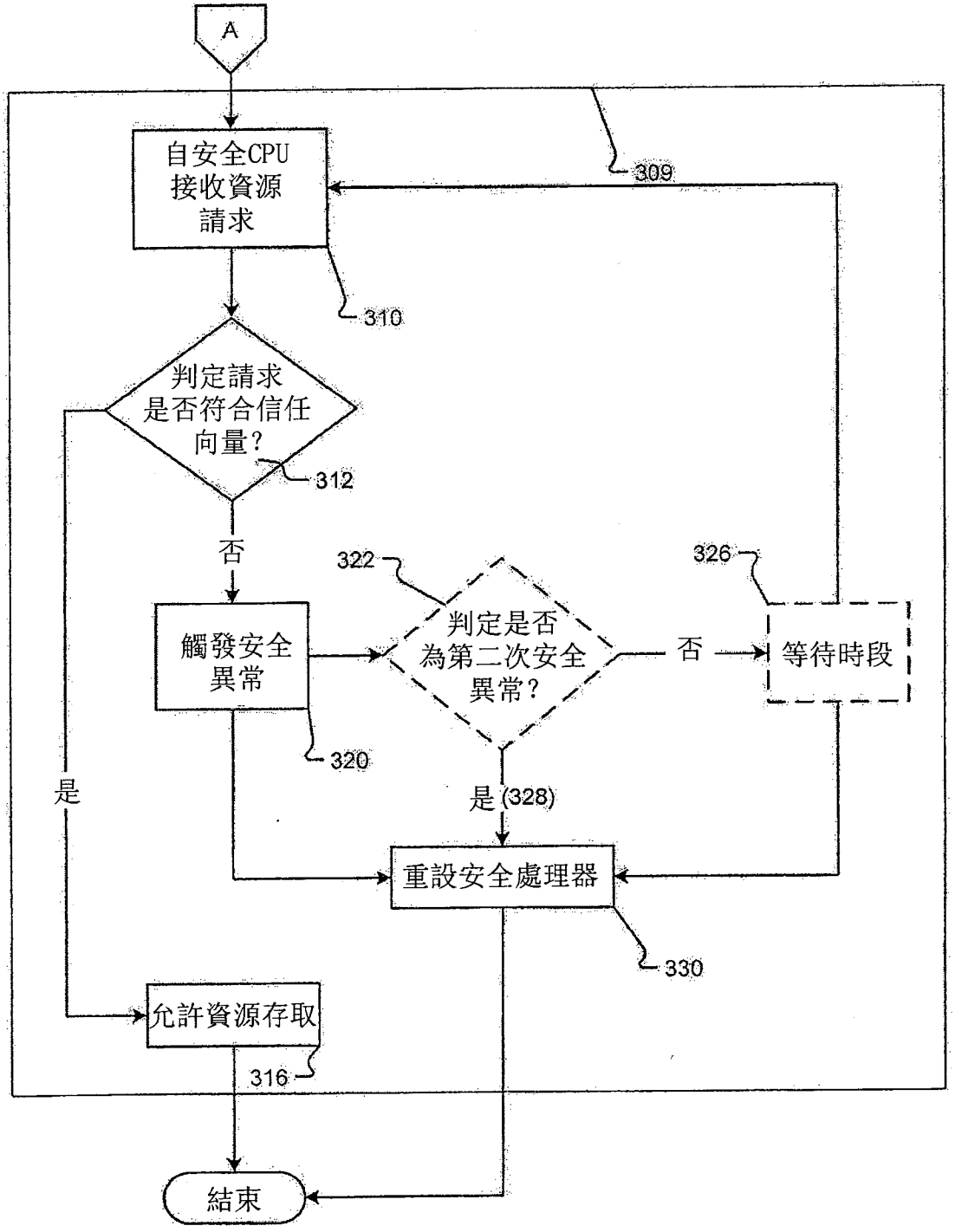
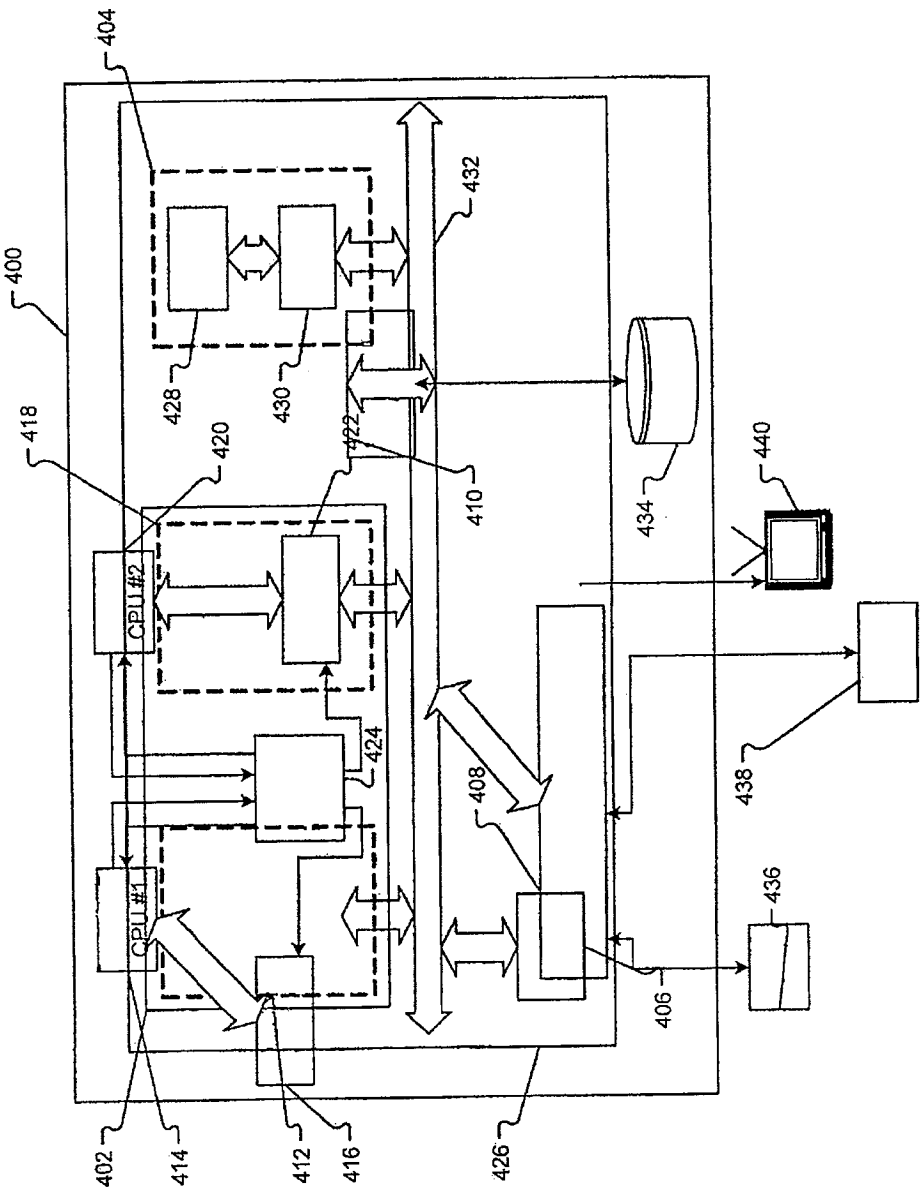

A
自安全CPU
接收資源
請求
309
310
判定請求
是否符合信任
向量?
312
否
是
322
判定是否
為第二次安全
異常?
否
326
等待時段
觸發安全
異常
320
是 (328)
重設安全處理器
330
允許資源存取
316
結束

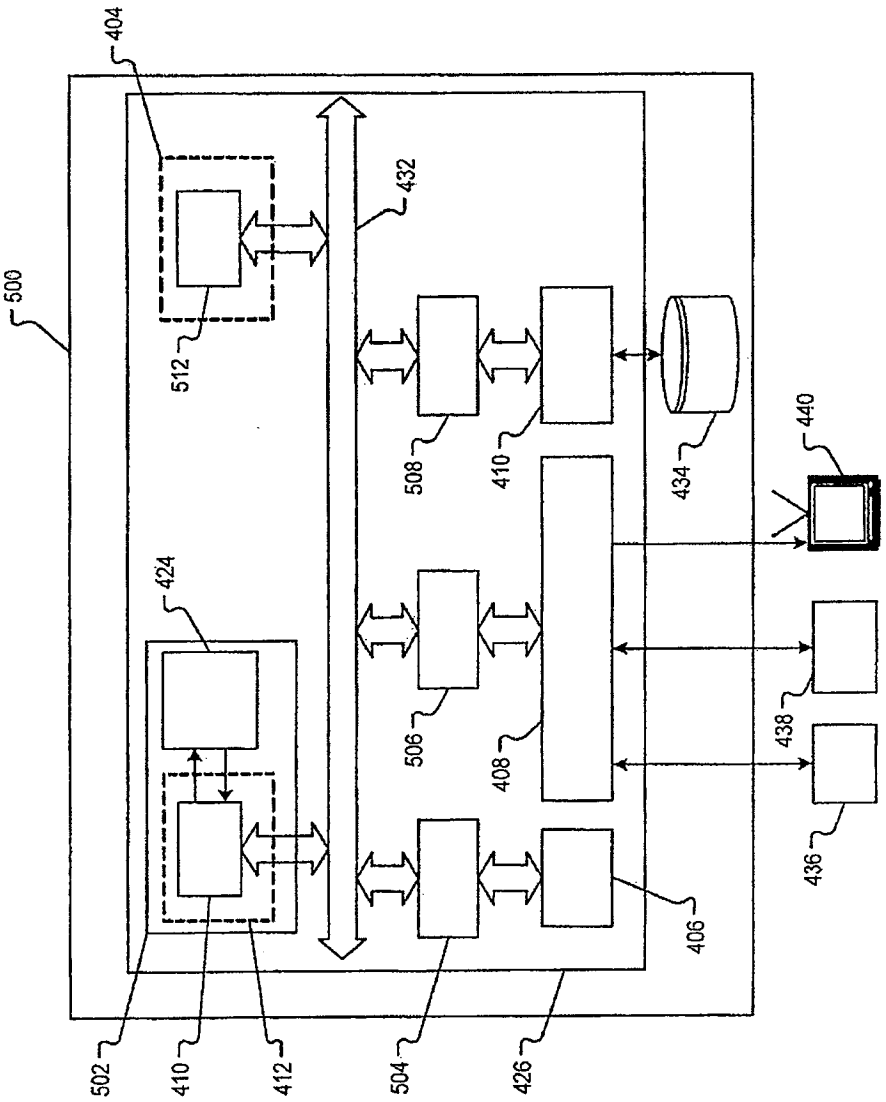
圖3B

圖 4


404
400
432
428
430
422
410
418
420
434
440
CPU #2
424
408
438
CPU #1
436
406
402
414
412
416
426

200901034

圖 5



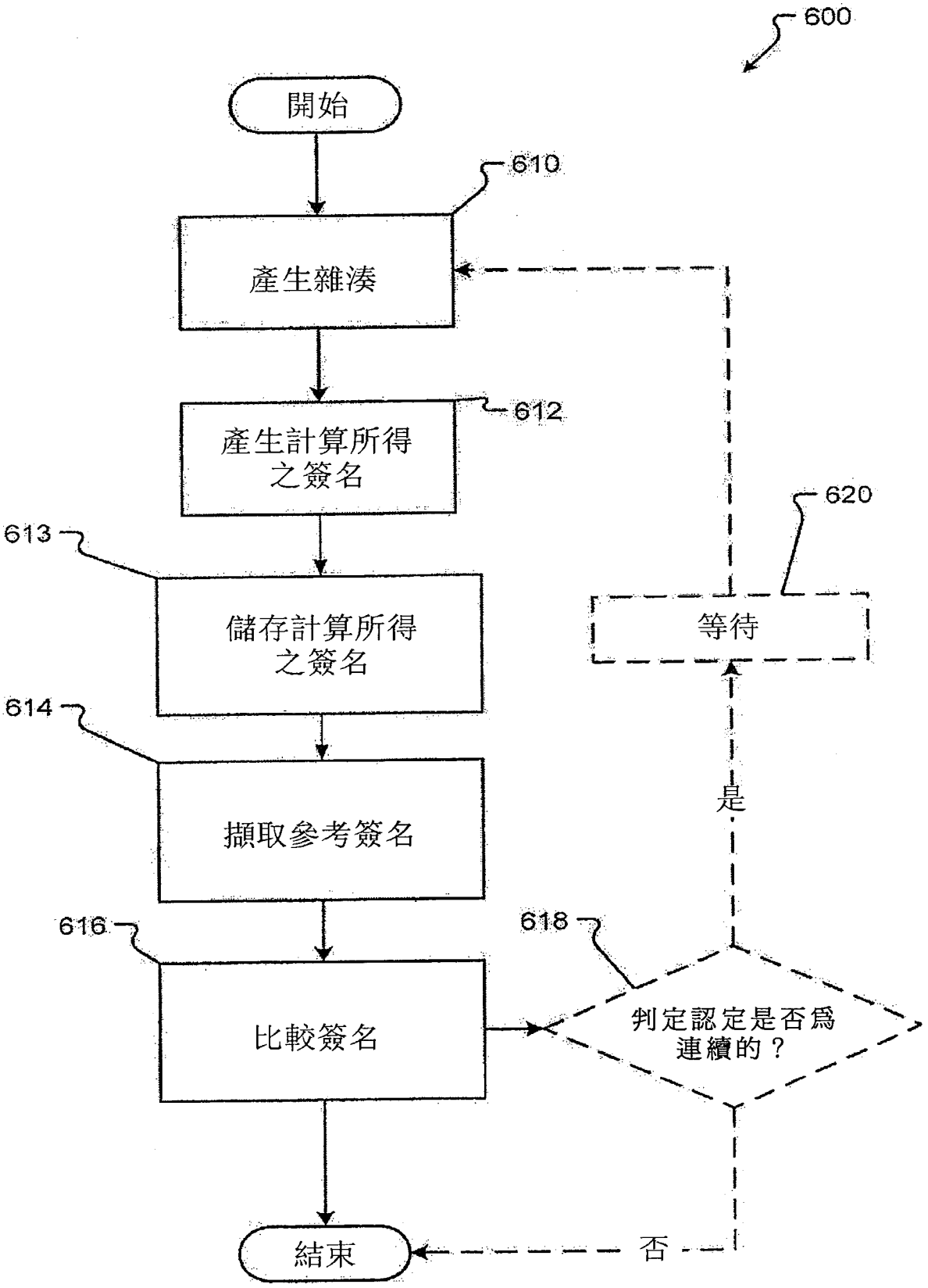

600
開始
610
產生雜湊
612
產生計算所得之簽名
613
儲存計算所得之簽名
614
擷取參考簽名
616
比較簽名
618
判定認定是否爲連續的？
620
等待
是
否
結束

圖6

七、指定代表圖：

(一)本案指定代表圖為：第（ 1 ）圖。

(二)本代表圖之元件符號簡單說明:

100 計算環境
102 虛線/安全計算或操作環境
104 安全中央處理單元(“CPU”)或處理器
106 上下文管理器
108 信任向量驗證器
110 上下文交換
112 重設
114 指令
116 通訊路徑
118 資源請求
120 資源
121 硬體中斷
122 快取記憶體
124 暫存器
126 資料儲存器/記憶體
128 記憶體管理單元(MMU)

八、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

無