201737059

(19)中華民國智慧財產局

(12)發明說明書公開本 (11)公開編號：TW 201737059 A

(43)公開日： 中華民國 106 (2017) 年 10 月 16 日

(21)申請案號：106106713 (22)申請日： 中華民國 106 (2017) 年 03 月 01 日

(51)Int. Cl.： *G06F9/06 (2006.01)* *G06F13/10 (2006.01)*

(30)優先權：2016/03/22 美國 15/076,936

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

(72)發明人：克里斯托鐸雷斯古 米哈 CHRISTODORESCU, MIHAI (US)；胡爾賈堤 迪那卡 DHURJATI, DINAKAR (IN)；伊斯蘭 纳伊姆 ISLAM, NAYEEM (US)

(74)代理人：陳長文

申請實體審查：無 申請專利範圍項數：28 項 圖式數：11 共 60 頁

(54)名稱

使用虛擬資源視圖之資料保護

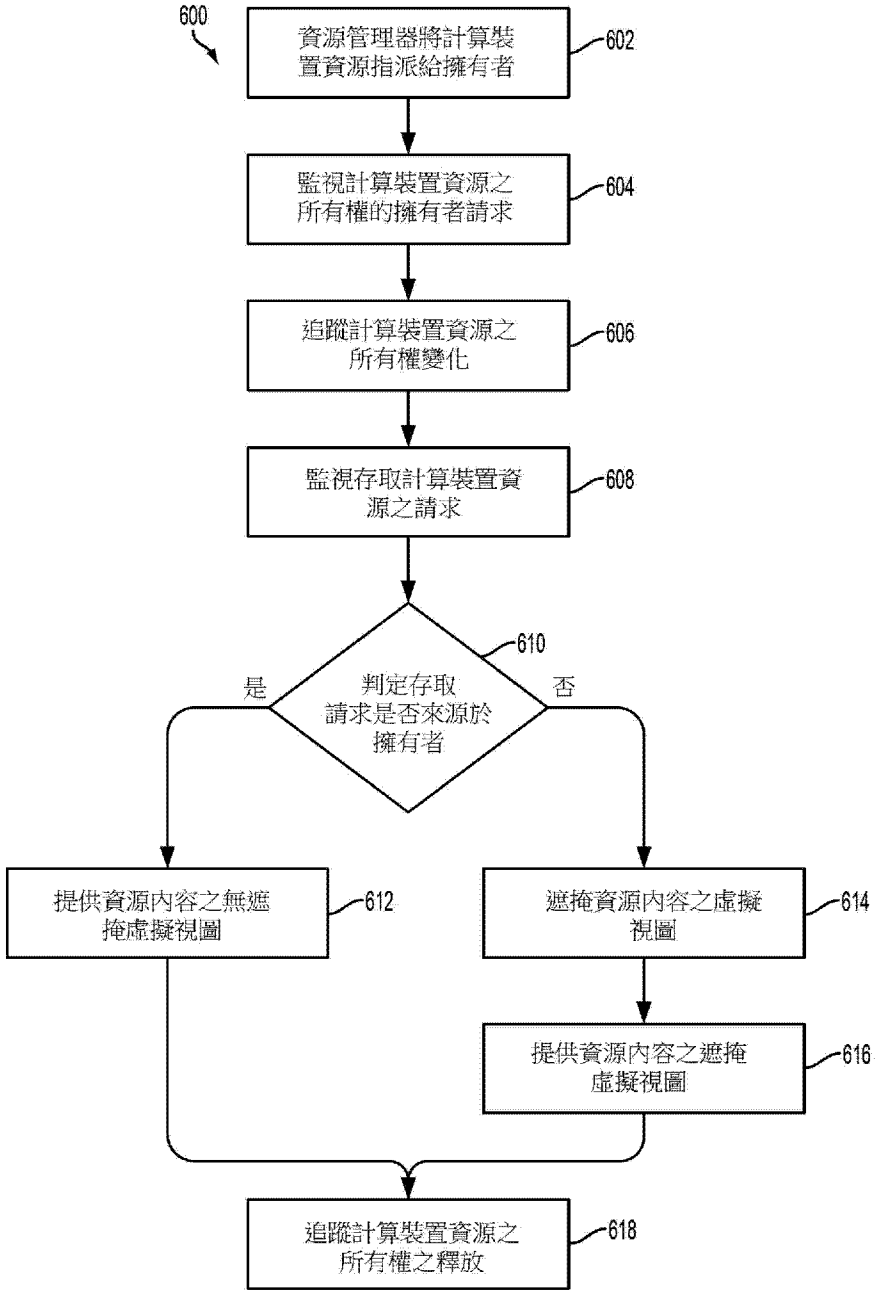
DATA PROTECTION USING VIRTUAL RESOURCE VIEWS

(57)摘要

實施例包括用於使用資源內容之虛擬視圖保護資料的計算裝置、系統及方法。一虛擬化介面監視器可監視一第一請求實體對存取一計算裝置資源之一請求且判定該第一請求實體是否為該計算裝置資源之一擁有者。一資料保護系統可回應於判定該第一請求實體係該計算裝置資源之該擁有者而將該計算裝置資源之資源內容之一無遮掩虛擬視圖提供至該第一請求實體。一資源內容密碼編譯裝置可回應於判定該第一請求實體係該計算裝置資源之一非擁有者而遮掩該計算裝置資源之該等資源內容的一虛擬視圖。該資料保護系統可將該計算裝置資源之資源內容之遮掩虛擬視圖提供至該第一請求實體。

Embodiments include computing devices, systems, and methods for protecting data using virtual views of resource contents. A virtualization interface monitor may monitor a request to access a computing device resource by a first requesting entity and determine whether the first requesting entity is an owner of the computing device resource. A data protection system may provide, to the first requesting entity, an unobscured virtual view of resource contents of the computing device resource in response to determining that the first requesting entity is the owner of the computing device resource. A resource content cryptographic device may obscure a virtual view of the resource contents of the computing device resource in response to determining that the first requesting entity is a non-owner of the computing device resource. The data protection system may provide, to the first requesting entity, the obscured virtual view of resource contents of the computing device resource.

指定代表圖：



【圖6】

符號簡單說明：

600・・・用於使用虛擬資源視圖保護資料之方法

602・・・區塊

604・・・區塊

606・・・區塊

608・・・區塊

610・・・判定區塊

612・・・區塊

614・・・區塊

616・・・區塊

618・・・區塊

20173705B
專利案號：106106713
201737059
申請日：106/03/01
IPC分類：G06F 9/06 (2006.01)
G06F 13/10 (2006.01)

【發明摘要】

【中文發明名稱】

使用虛擬資源視圖之資料保護

【英文發明名稱】

DATA PROTECTION USING VIRTUAL RESOURCE VIEWS

【中文】

實施例包括用於使用資源內容之虛擬視圖保護資料的計算裝置、系統及方法。一虛擬化介面監視器可監視一第一請求實體對存取一計算裝置資源之一請求且判定該第一請求實體是否為該計算裝置資源之一擁有者。一資料保護系統可回應於判定該第一請求實體係該計算裝置資源之該擁有者而將該計算裝置資源之資源內容之一無遮掩虛擬視圖提供至該第一請求實體。一資源內容密碼編譯裝置可回應於判定該第一請求實體係該計算裝置資源之一非擁有者而遮掩該計算裝置資源之該等資源內容的一虛擬視圖。該資料保護系統可將該計算裝置資源之資源內容之遮掩虛擬視圖提供至該第一請求實體。

【英文】

Embodiments include computing devices, systems, and methods for protecting data using virtual views of resource contents. A virtualization interface monitor may monitor a request to access a computing device resource by a first requesting entity and determine whether the first requesting entity is an owner of the computing device resource. A data protection system may provide, to the first requesting entity, an unobscured virtual view of resource contents of the computing

device resource in response to determining that the first requesting entity is the owner of the computing device resource. A resource content cryptographic device may obscure a virtual view of the resource contents of the computing device resource in response to determining that the first requesting entity is a non-owner of the computing device resource. The data protection system may provide, to the first requesting entity, the obscured virtual view of resource contents of the computing device resource.

【指定代表圖】

圖6

【代表圖之符號簡單說明】

600	用於使用虛擬資源視圖保護資料之方法
602	區塊
604	區塊
606	區塊
608	區塊
610	判定區塊
612	區塊
614	區塊
616	區塊
618	區塊

【發明說明書】

【中文發明名稱】

使用虛擬資源視圖之資料保護

【英文發明名稱】

DATA PROTECTION USING VIRTUAL RESOURCE VIEWS

【技術領域】

【先前技術】

在具有一或多個處理器及一或多個周邊裝置之任何電腦系統中，資源管理軟體以高權限執行。使用保護環模型化作為一實例，作業系統在環0中執行，具有對所有硬體之完全存取，且超管理器在環0以下執行，具有對所有硬體之完全存取。當資源管理器將一資源指派給一任務時(例如，當作業系統將一記憶體頁指派給一程序時)，資源管理器維持對資源之完全存取。維持對資源之完全存取使得資源管理器能夠稍後代表任務來管理資源。資源管理器亦可具有對資源之讀取/寫入存取，此可使得資源能夠實施資源管理。舉例而言，作業系統讀取指派給程序之記憶體頁，以重定位記憶體頁或將程序轉出記憶體。

資源管理器(包括作業系統、超管理器及TrustZone)係軟體之易損壞片段。歸因於資源管理器之固有複雜度，消除所有缺陷接近於不可能。利用資源管理器中之漏洞的攻擊可導致電腦系統之故障。由於資源管理器之高權限，攻擊者可具有對電腦系統之全面存取。因此，攻擊者有動機發現及利用資源管理器中之瑕疵。

【發明內容】

各種實施例之方法及設備提供用於使用資源內容之虛擬視圖保護資

料的設備及方法。各種實施例可包括一計算裝置之一虛擬化介面監視器，其監視一第一請求實體對存取一計算裝置資源之一請求。該虛擬化介面監視器可判定該第一請求實體是否為該計算裝置資源之一擁有者。該計算裝置之一資料保護系統可回應於判定該第一請求實體係該計算裝置資源之該擁有者，而將該計算裝置資源之資源內容之一無遮掩虛擬視圖提供至該第一請求實體。該資料保護系統可回應於判定該第一請求實體係該計算裝置資源之一非擁有者，而將該計算裝置資源之資源內容之一遮掩虛擬視圖提供至該第一請求實體。

在一些實施例中，資源內容密碼編譯裝置可判定該第一請求實體是否具有一認證功能，且回應於判定該第一請求實體具有一認證功能而判定用於該第一請求實體之一存取類型。資源內容密碼編譯裝置可回應於判定該第一請求實體係該計算裝置資源之一非擁有者，而基於該存取類型使用一遮掩位準來遮掩該計算裝置資源之資源內容之虛擬視圖。

在一些實施例中，存取類型可包括部分遮掩及遮掩。藉由回應於判定用於該第一請求實體之該存取類型為部分遮掩，使用同態加密對計算裝置資源之資源內容之虛擬視圖加密，資源內容密碼編譯裝置可基於該存取類型使用一遮掩位準來遮掩計算裝置資源之資源內容之虛擬視圖。資源內容密碼編譯裝置可回應於判定用於該第一請求實體之該存取類型為遮掩，而使用強加密對計算裝置資源之資源內容之虛擬視圖加密。

在一些實施例中，該虛擬化介面監視器可關於計算裝置資源之所有權變化對一虛擬化介面進行監視，且儲存與用於該第一請求實體的計算裝置資源之一虛擬資源識別符相關的該第一請求實體之一第一擁有者識別符。在此等實施例中，該第一擁有者識別符可指示該第一請求實體經授予

計算裝置資源之所有權且該虛擬資源識別符經映射至計算裝置資源之一實體資源識別符。

在一些實施例中，關於計算裝置資源之一所有權變化監視一虛擬化介面可包括監視一第二請求實體對計算裝置資源之所有權之一請求。

在一些實施例中，藉由將存取計算裝置資源之請求之一虛擬資源識別符與相關於計算裝置資源之一虛擬資源識別符的所儲存擁有者識別符進行比較，該虛擬化介面監視器可判定該第一請求實體是否為計算裝置資源之一擁有者。在存取計算裝置資源之請求的虛擬資源識別符與計算裝置資源之虛擬資源識別符匹配時，該虛擬化介面監視器可判定該第一請求實體係計算裝置資源之擁有者。

在一些實施例中，計算裝置資源之擁有者可包括一應用程式，且計算裝置資源之非擁有者可包括一資源管理器，包括一作業系統內核、一超管理器及一TrustZone中之一者。

各種實施例可包括經組態用於使用資源內容之虛擬視圖保護資料的計算裝置。該計算裝置可包括一資料保護系統，其包括一虛擬化介面監視器及一資源內容密碼編譯裝置。該計算裝置之一或多個處理器可用資料保護系統可執行指令、虛擬化介面監視器可執行指令及資源內容密碼編譯裝置可執行指令來組態以執行上文概述之實施例方法中之一或多者的操作。

各種實施例可包括經組態用於使用資源內容之虛擬視圖保護資料的計算裝置，其具有用於執行上文概述之實施例方法中之一或多者之功能的構件。

各種實施例可包括非暫時性處理器可讀儲存媒體，其上儲存有處理器可執行指令，該等指令經組態以使一計算裝置之一或多個處理器執行上

文概述之實施例方法中之一或多者的操作。

【圖式簡單說明】

併入本文中且構成本說明書之部分的隨附圖式說明各種實施例之實例實施例，且連同上文給出之一般描述及下文給出之詳細描述用以解釋申請專利範圍之特徵。

圖1為說明適用於實施一實施例之計算裝置的組件方塊圖。

圖2為說明適合於實施一實施例之實例多核心處理器的組件方塊圖。

圖3為適合於實施一實施例之資料保護系統的組件方塊圖。

圖4為根據一實施例之資源所有權表。

圖5為根據一實施例之存取請求憑證表。

圖6為說明用於使用虛擬資源視圖保護資料之一實施例方法的程序流程圖。

圖7為說明用於追蹤計算裝置資源之所有權之一實施例方法的程序流程圖。

圖8為說明用於使用憑證以用於將加密應用於資源內容之虛擬視圖之一實施例方法的程序流程圖。

圖9為說明適合於與各種實施例一起使用之一實例行動計算裝置的組件方塊圖。

圖10為說明適合於與各種實施例一起使用之一實例行動計算裝置的組件方塊圖。

圖11說明適合於與各種實施例一起使用之一實例伺服器的組件方塊圖。

【實施方式】

將參考隨附圖式來詳細地描述各種實施例。在任何可能之處，將貫穿圖式使用相同參考數字來指相同或相似部分。對特定實例及實施例之參考為出於說明之目的，且並不意欲限制申請專利範圍之範疇。

術語「計算裝置」及「行動計算裝置」在本文中可互換地使用，以指以下項中之任一個或全部：蜂巢式電話、智慧型電話、個人或行動多媒體播放器、個人資料助理(PDA)、膝上型電腦、平板電腦、可轉換之膝上型電腦/平板電腦(2合1電腦)、智慧筆記型電腦、超級本、迷你筆記型電腦、掌上型電腦、無線電子郵件接收器、具備多媒體網際網路能力之蜂巢式電話、行動遊戲控制台、無線遊戲控制器，及包括記憶體及多核心可程式化處理器之類似個人電子裝置。術語「計算裝置」可進一步指固定計算裝置，包括個人電腦、桌上型電腦、一體式電腦、工作站、超級電腦、大型電腦、嵌入型電腦、伺服器、本籍電影院電腦及遊戲控制台。各種實施例特別適用於具有有限記憶體及電池資源之行動計算裝置，諸如智慧型電話。然而，該等實施例大體上適用於複數個記憶體裝置及有限電力預算之任何電子裝置，其中減少處理器之電力消耗可延長行動計算裝置之電池工作時間。

實施例可包括用於將資源管理任務與資源管理器(諸如，作業系統，包括作業系統內核、超管理器及/或TrustZone)之高權限存取准許分離的方法、系統及裝置。對用以轉譯針對各種資源之存取請求的虛擬化介面的監視可用以區分擁有者應用程式存取與對資源之資源管理器存取。同一資源之不同視圖可經提供至擁有者應用程式及資源管理器。與存取請求相關的不同位準之資源內容保護可基於資源之存取者之計劃操作及資源資料之敏感性來提供。

資源可由資源管理器在不存取資源之內容(諸如，資源資料)的情況下進行管理(例如，移動、複製等)，而應用需要存取資源內容以實施各種程序。虛擬化介面可受監視以判定是否遮蔽來自資源管理器之資源內容，同時允許資源管理器實施管理功能，且同時允許資源擁有應用程式存取資源內容以實施程序。虛擬化介面監視器及資源內容密碼編譯裝置可實施於硬體中，該硬體經組態以區分對資源之擁有者應用程式存取及資源管理器存取且限制資源管理器對資源內容之存取。

虛擬化介面監視器可包括經組態以儲存及更新計算裝置系統之資源之所有權的資源所有權追蹤器。虛擬化介面監視器可經組態以判定對資源之存取請求是否由資源之擁有者應用程式或計算裝置系統之資源管理器發出。資源內容密碼編譯裝置可回應於存取請求係由資源管理器發出之判定而對資源之內容加密。資源內容密碼編譯裝置可回應於存取請求係由擁有者應用程式發出之判定而以未加密形式提供資源之內容。

資源管理器可將資源指派給應用程式。應用程式可請求資源之所有權，且虛擬化介面監視器可更新資源之擁有者。

資源管理器及資源之擁有者應用程式可被提供資源之不同虛擬表示。資源之每一虛擬表示可包括資源的虛擬記憶體位址至實體記憶體位址之不同映射。

虛擬化介面監視器可接收、偵測或攔截存取所擁有資源之請求。虛擬化介面監視器可藉由存取請求之虛擬記憶體位址來識別請求實體是否為資源管理器或資源擁有者應用程式。回應於判定請求實體係資源擁有者應用程式，資源內容密碼編譯裝置可為擁有者應用程式提供對資源內容之未加密虛擬表示之存取。回應於判定請求實體係資源管理器，資源內容密碼

編譯裝置可對資源之內容的虛擬表示加密且為資源管理器提供經加密虛擬表示之存取。

在一些實施中，資源內容密碼編譯裝置可基於請求實體之計劃操作及資源內容之敏感性來改變對資源內容之保護。資源內容密碼編譯裝置可支援不同類型之加密，諸如強加密及簽名要求，或部分同態加密。

憑證裝置可儲存及更新用於應用程式及資源管理器之編譯器憑證，從而闡述：編譯器保證某些操作藉由特定軟體組件執行。編譯器憑證可與指定加密類型相關。資源內容密碼編譯裝置可基於對請求實體之判定及各種資源擁有者應用程式、非擁有者應用程式及資源管理器的由憑證裝置維持之相關性而實施不同類型之加密。

圖1說明一系統，該系統包括適合於與各種實施例一起使用的與遠端計算裝置50通信之計算裝置10。計算裝置10可包括系統單晶片(SoC)12，其具有處理器14、記憶體16、通信介面18及儲存記憶體介面20。計算裝置10可進一步包括諸如有線或無線數據機之通信組件22、儲存記憶體24、用於建立至無線網路30之無線連接32的天線26，及/或用於連接到至網際網路40之有線連接44的網路介面28。處理器14可包括多種硬體核心中之任一者，例如數個處理器核心。

術語「系統單晶片」(SoC)在本文中用以指通常(但非獨占式地)包括硬體核心、記憶體及通信介面的一組互連電子電路。硬體核心可包括多種不同類型之處理器，諸如通用處理器、中央處理單元(CPU)、數位信號處理器(DSP)、圖形處理單元(GPU)、加速處理單元(APU)、輔助處理器、單核心處理器及多核心處理器。硬體核心可進一步體現其他硬體及硬體組合，諸如場可程式化閘陣列(FPGA)、特殊應用積體電路(ASIC)、其他可

程式化邏輯裝置、離散閘邏輯、電晶體邏輯、效能監視硬體、看門狗硬體及時間參考。積體電路可經組態以使得積體電路之組件駐存於單塊半導體材料(諸如，矽)上。SoC 12可包括一或多個處理器14。計算裝置10可包括多於一個的SoC 12，由此增加處理器14及處理器核心之數目。計算裝置10亦可包括不與SoC 12相關聯之處理器14。個別處理器14可為如下文參看圖2所描述之多核心處理器。處理器14可出於可與計算裝置10之其他處理器14相同或不同的特定目的而各自經組態。具有相同或不同組態的處理器14及處理器核心中之一或多者可分組在一起。處理器14或處理器核心之群組可被稱為多處理器叢集。

SoC 12之記憶體16可為經組態用於儲存資料及處理器可執行碼以供藉由處理器14存取的揮發性或非揮發性記憶體。計算裝置10及/或SoC 12可包括經組態以用於各種目的之一或多個記憶體16。在一實施例中，一或多個記憶體16可包括諸如隨機存取記憶體(RAM)或主記憶體之揮發性記憶體，或快取記憶體。此等記憶體16可經組態以暫時保持有限量的接收自資料感測器或子系統之資料。此等記憶體16可經組態以暫時保持向非揮發性記憶體請求、基於多種因素預想到未來存取而自非揮發性記憶體載入至記憶體16的資料及/或處理器可執行碼指令。此等記憶體16可經組態以暫時保持由處理器14產生且暫時儲存以供未來快速存取的中間處理資料及/或處理器可執行碼指令，無需儲存於非揮發性記憶體中。

記憶體16可經組態以至少暫時地儲存自另一記憶體裝置(諸如，另一記憶體16或儲存記憶體24)載入至記憶體16的資料及處理器可執行碼，以供由處理器14中之一或多者存取。載入至記憶體16之資料或處理器可執行碼可回應於藉由處理器14執行功能而予以載入。回應於功能之執行將資

料或處理器可執行碼載入至記憶體16可起因於對記憶體16的不成功或錯過的記憶體存取請求，此係因為所請求之資料或處理器可執行碼不位於記憶體16中。回應於錯過，可進行對另一記憶體16或儲存記憶體24之記憶體存取請求，以將所請求之資料或處理器可執行碼自另一記憶體16或儲存記憶體24載入至記憶體裝置16。回應於功能之執行而將資料或處理器可執行碼載入至記憶體16可起因於對另一記憶體16或儲存記憶體24之記憶體存取請求，且資料或處理器可執行碼可載入至記憶體16以供稍後存取。

通信介面18、通信組件22、天線26及/或網路介面28可一致工作以使得計算裝置10能夠經由無線連接32在無線網路30上通信及/或經由有線網路44與遠端計算裝置50通信。無線網路30可使用包括(例如)用於無線通信之射頻頻譜的多種無線通信技術實施，以為計算裝置10提供至網際網路40的連接，藉由該網際網路，該計算裝置可與遠端計算裝置50交換資料。

儲存記憶體介面20及儲存記憶體24可一致工作，以允許計算裝置10將資料及處理器可執行碼儲存於非揮發性儲存媒體上。儲存記憶體24可更類似記憶體16之實施例進行組態，其中儲存記憶體24可儲存資料或處理器可執行碼，以供藉由處理器14中之一或多者存取。非揮發性的儲存記憶體24可甚至在計算裝置10之電力已被切斷之後保留資訊。當電力恢復且計算裝置10重啟時，儲存於儲存記憶體24上之資訊可能可用於計算裝置10。儲存記憶體介面20可控制對儲存記憶體24之存取，且允許處理器14自儲存記憶體24讀取資料及將資料寫入至該儲存記憶體。

計算裝置10之組件中的一些或全部可以不同方式配置及/或組合，同時仍為必要功能提供服務。此外，計算裝置10可不受限於組件中之每一者

中的一者，且每一組件之多個個例可包括於計算裝置10之各種組態中。

圖2說明適合於實施一實施例之多核心處理器14。多核心處理器14可具有複數個均質的或異質的處理器核心200、201、202、203。處理器核心200、201、202、203可為均質的，此係因為單一處理器14之處理器核心200、201、202、203可經組態用於相同目的且具有相同或類似效能特性。舉例而言，處理器14可為通用處理器，且處理器核心200、201、202、203可為均質的通用處理器核心。替代地，處理器14可為圖形處理單元或數位信號處理器，且處理器核心200、201、202、203可分別為均質的圖形處理器核心或數位信號處理器核心。為了易於參考，術語「處理器」及「處理器核心」可在本文中互換地使用。

處理器核心200、201、202、203可為異質的，此係因為單一處理器14之處理器核心200、201、202、203可經組態用於不同目的及/或具有不同效能特性。此等異質處理器核心之異質性可包括不同指令集架構、管線、操作頻率等。此等異質處理器核心之一實例可包括被稱為「大小核(big.LITTLE)」架構之物，其中較慢的低功率處理器核心可與較強大的及功耗大之處理器核心耦接。在類似實施例中，SoC 12可包括數個均質的或異質的處理器14。

在圖2中所說明之實例中，多核心處理器14包括四個處理器核心200、201、202、203 (亦即，處理器核心0、處理器核心1、處理器核心2及處理器核心3)。為了易於解釋，本文中之實例可指圖2中所說明的四個處理器核心200、201、202、203。然而，圖2中所說明且本文中所描述之四個處理器核心200、201、202、203僅作為一實例而提供，而絕非意欲將各種實施例限於四核心處理器系統。計算裝置10、SoC 12或多核心處

理器14可個別地或以組合包括少於或多於本文中所說明且描述之四個處理器核心200、201、202、203的處理器核心。

圖3說明根據一實施例之資料保護系統。資料保護系統300可經組態以監視一計算裝置資源之一虛擬化介面，且藉由對資源內容之一些加密以及將資源內容之加密的及未加密的虛擬視圖提供至請求存取或使用資源的計算裝置10之不同組件(「請求組件」)來保護資源內容。資料保護系統300可包括虛擬化介面監視器302及資源內容密碼編譯裝置304。

虛擬化介面監視器302可經組態以追蹤計算裝置資源之所有權，諸如記憶體16之位址位置、儲存記憶體24之磁碟區塊及通信組件22之網路卡佇列識別符。資源之所有權可歸因於在計算裝置10上執行的應用程式312、作業系統306、超管理器308及/或TrustZone 310。

計算裝置資源之所有權的貢獻可由虛擬化介面監視器302以經組態以連結及/或配置多個資料的表或資料結構進行儲存。不限制揭露內容，為了易於解釋，本文中參考了由虛擬化介面監視器302儲存且在本文中參看圖4進一步進行描述的所有權表(圖中未示)。所有權表可將經組態以指示作業系統306、超管理器308、TrustZone 310及/或應用程式312中之一者的擁有者識別符(ID)與所擁有的計算裝置資源之虛擬資源識別符(諸如，虛擬位址)關聯。

計算裝置資源的至實體資源識別符映射(諸如，虛擬位址至實體位址映射)之不同虛擬資源識別符可用於潛在及實際擁有者，例如不同的潛在擁有者可使用映射至同一實體位址之不同虛擬位址。由於至實體資源識別符映射之不同虛擬資源識別符，虛擬化介面監視器302可使用對計算裝置資源之聲明或請求的虛擬資源識別符而將擁有者與所擁有之計算裝置資源

關聯。

虛擬化介面監視器302可接收、偵測或攔截指派記憶體資源管理器及計算裝置資源之實體指派所有權對計算裝置資源之所有權的聲明或請求。指派記憶體資源管理器可包括作業系統306、超管理器308及/或TrustZone 310。計算裝置資源之實體指派所有權可包括作業系統306、超管理器308、TrustZone 310及/或應用程式312。在一些實施例中，虛擬化介面監視器302可管理所有權表，以使得指示計算裝置資源之所有權的輸入項可在計算裝置資源之所有權有變化後被刪除或指示為無效。對於計算裝置資源之新擁有者，輸入項可添加或標記為有效。

在一些實施例中，虛擬化介面監視器302可追蹤指示資源存取請求者的所允許功能的憑證。功能之憑證可由功能之開發人員預先程式化或由執行於計算裝置10上之編譯器來識別。憑證可可適用於應用程式312、作業系統306、超管理器308及/或TrustZone 310之功能。在一些實施例中，需要實施認證功能的對資源內容之存取的類型可與憑證相關。

需要實施功能的存取之類型可指示功能需要對資源內容之完全、無遮掩存取、對資源內容之部分遮掩存取抑或對資源內容之遮掩存取。對資源內容之無遮掩存取可允許資源內容之視圖在儲存時無任何變化或操控而遮掩資源內容，且可允許對資源內容進行讀取及寫入。對資源內容之部分遮掩存取可允許資源內容之搜尋或算術操控，且可經由應用部分或完全同態加密(homomorphic encryption)來達成。對資源內容之遮掩存取可允許可執行而不對資源內容進行讀取或寫入存取的資源管理操作，且可經由應用強加密(strong encryption)及簽名要求來達成。

虛擬化介面監視器302可將功能憑證對存取計算裝置資源之請求者的

貢獻以經組態以連結及/或配置多個資料之表或資料結構進行儲存。在一些實施例中，虛擬化介面監視器302亦可儲存需要實施認證功能的存取之類型。不限制揭露內容，為了易於解釋，本文中參考了由虛擬化介面監視器302儲存且在本文中參看圖5進一步進行描述的憑證表(圖中未示)。

虛擬化介面監視器302可接收、偵測或攔截存取請求者對計算裝置資源之存取的請求。以類似於本文中所描述的追蹤計算裝置資源之所有權的方式，虛擬化介面監視器302可使用存取計算裝置資源之請求的虛擬資源識別符來判定請求實體是否為一擁有者。虛擬化介面監視器302可發現與存取計算裝置資源之請求的虛擬資源識別符相關的請求實體。在一些實施例中，虛擬化介面監視器302可使用所有權表，藉由將請求之虛擬資源識別符及請求實體識別符與所有權識別符進行比較來判定請求實體是否為一擁有者。在一些實施例中，虛擬化介面監視器302可使用請求實體識別符及/或存取計算裝置資源之請求的所請求之存取或功能而在憑證表中定位請求實體之功能憑證。虛擬化介面監視器302可識別與請求實體識別符及/或存取計算裝置資源之請求之功能憑證相關的存取之類型。在此等實施例中之任一者中，虛擬化介面監視器302可將儲存於所有權表及/或憑證表中的與存取計算裝置資源之請求相關的任何資料傳輸至資源內容密碼編譯裝置304。

資源內容密碼編譯裝置304可經組態以判定將應用於資源內容之虛擬視圖的遮掩之類型及/或位準，且回應於存取計算裝置資源之請求而提供資源內容之虛擬視圖。遮掩之類型及/或位準可包括加密之各種類型及位準。應用於計算裝置資源之虛擬視圖的加密可包括強加密及簽名要求，其用以向請求實體完全遮掩資源內容。應用於計算裝置資源之虛擬視圖的加

密可包括部分或完全的同態加密，其用以向請求實體遮掩資源內容，但允許請求實體搜尋或算術地操控由同態加密引起之密文。對密文之操作可產生經解密資源內容中之對應結果，但不允許請求實體讀取經解密資源內容。應用於計算裝置資源之虛擬視圖的加密可包括可由擁有者解密以允許擁有者存取資源內容之虛擬複本的加密。在一些實施例中，無加密可應用於計算裝置資源之虛擬視圖，從而允許擁有者存取資源內容之虛擬複本。

為判定將應用於資源內容之虛擬視圖的加密之類型及/或位準，資源內容密碼編譯裝置304可將接收自虛擬化介面監視器302之資料與加密之類型及/或位準關聯。接收自虛擬化介面監視器302之資料可包括(例如)擁有者識別符、請求實體識別符、請求實體是否為計算裝置資源之擁有者、功能憑證、存取之類型及/或虛擬資源識別符(諸如，虛擬位址)，或存取計算裝置資源之請求的對應實體位址。

資源內容密碼編譯裝置304可來自虛擬化介面監視器302之資料且識別與來自虛擬化介面監視器302之資料相關的加密之類型及/或位準。在一些實施例中，加密之類型及/或位準可作為存取資料之類型之部分由虛擬化介面監視器302提供。在一些實施例中，資源內容密碼編譯裝置304可使用接收自虛擬化介面監視器302之資料與加密之類型及/或位準之間的程式化相關性來判定加密之類型及/或位準。舉例而言，指示請求實體係擁有者之資料可與輕或無加密相關，而指示請求實體並非擁有者之資料可與強加密相關。類似地，指示所請求功能係非擁有者之認證功能之資料可與完全或部分的同態加密相關，且指示所請求功能係非擁有者之非認證功能之資料與強加密相關。

資料保護系統300可自計算裝置資源擷取所請求之資源內容，且資源

內容密碼編譯裝置304可將加密之類型及/或位準應用於所擷取之資源內容之虛擬視圖。資料保護系統300可將所請求之資源內容之遮掩或無遮掩虛擬視圖傳回至請求實體。

在一些實施例中，資料保護系統300可自計算裝置資源擷取所請求之資源內容，且虛擬化介面監視器302可基於用於存取計算裝置資源之請求的存取之類型而傳輸一信號。不同信號可觸發資源內容密碼編譯裝置304以將遮掩之類型及/或位準應用於所擷取資源內容之虛擬視圖。資料保護系統300可將所請求之資源內容之經加密或未加密的虛擬視圖傳回至請求實體。

如圖3中所說明，資料保護系統300可以硬體來實施。計算裝置10可執行軟體，包括作業系統306、超管理器308、TrustZone 310及/或應用程式312。計算裝置10可包括硬體組件，諸如記憶體16 (其可包括儲存頁表之隨機存取記憶體(RAM))、轉譯後援緩衝器314、處理器14 (其可包括CPU)及資料保護系統300。資料保護系統300可包括經組態以實施資料保護系統300之專用硬體或通用硬體，諸如SoC 12或處理器14。虛擬化介面監視器302可包括專用硬體或通用硬體，諸如處理器14或處理器核心200、201、202、203，及可包括緩衝器之記憶體16。資源內容密碼編譯裝置304可包括專用硬體或通用硬體，諸如處理器14、處理器核心200、201、202、203及加密引擎或硬體加速器，及可包括緩衝器之記憶體16。

圖4說明資料保護系統300可使用以儲存計算裝置資源之所有權之資料的所有權表400之一非限制性實例。各種實施可包括所有權資料之不同組合及排序，所有權資料包括擁有者識別符、虛擬資源識別符(諸如，虛擬位址)、實體資源識別符(諸如，實體位址)及有效性指示符。在一些實

施中，術語虛擬資源識別符及實體資源識別符可互換地使用。

實例所有權表400可包括擁有者識別符資料欄402及虛擬資源識別符資料欄404。如下文所進一步論述，所有權表400亦可包括可選有效性指示符資料欄406。所有權表400可包括多個列(例如，列408至414)，每一列表示計算裝置資源之不同所有權。

擁有者識別符資料欄402可包括用於計算裝置之每一擁有者或潛在擁有者的特有識別符。該等擁有者識別符可用以傳達作為計算裝置資源之擁有者的請求存取計算裝置資源之實體之身分。

虛擬資源識別符資料欄404可包括用於同一輸入項之相關擁有者或潛在擁有者的虛擬資源識別符(諸如，虛擬位址)，其例如根據虛擬位址至實體位址映射而映射至計算裝置資源之實體資源識別符，如在列408至414中。如所述，其他資料可用以將擁有者或潛在擁有者與計算裝置資源關聯，包括計算裝置資源之實體位址及實體計算裝置資源識別符。

在一些實施中，所有權表400僅包括用於計算裝置資源之當前擁有者的輸入項。在此等實施中，輸入項可回應於計算裝置資源之所有權之變化而自所有權表400移除。移除輸入項可涉及刪除、無效化或覆寫經移除輸入項。

在一些實施中，所有權表400可包括可選有效性指示符資料欄406，其可包括用於指示輸入項是否指示與同一輸入項之擁有者識別符相關聯之擁有者的計算裝置資源之當前所有權的值。包括可選有效性指示符資料欄406可允許儲存計算裝置資源之擁有者之過去、當前及潛在輸入項。包括指示計算裝置資源之當前所有權之值的輸入項可包括可選有效性指示符資料欄406中之指定值，諸如如列408、410及414中所說明之布林值「1」。

包括指示計算裝置資源之過去或潛在所有權之值的輸入項可包括可選有效性指示符資料欄406中之不同指定值，諸如如列412中所說明之布林值「0」。包括可選有效性指示符資料欄406之實施可回應於計算裝置資源之所有權的變化而保持非當前所有權之輸入項。包括可選有效性指示符之實施例可在計算裝置資源之所有權經取得時將新輸入項添加至所有權表400，或所有權表400可預先填入計算裝置資源及其潛在擁有者之可能組合中的一些或全部。在一些實施中，可存在所有權表400中之輸入項之數目的極限「N」，且輸入項可根據替換準則而移除以便添加當前或潛在所有權。

實例所有權表400說明在各種實施中可解釋之多種所有權情形。舉例而言，列408說明：由擁有者識別符「O1」指定之擁有者實體可擁有根據用於擁有者及計算裝置資源的虛擬資源識別符至計算裝置資源映射、由虛擬資源識別符「VA1」表示的計算裝置資源。在各種實施中，虛擬資源識別符「VA1」可為映射至擁有者及計算裝置資源之實體位址的虛擬位址。在不包括可選有效性指示符資料欄406之實施中，列408中存在資料可指示：由擁有者識別符「O1」指定之擁有者實體當前擁有由虛擬資源識別符「VA1」表示之計算裝置資源。當有效性指示符之值為「1」時，相同結果可指示於包括可選有效性指示符資料欄406之實例中。

進一步包括列410說明：列408之同一擁有者實體亦可擁有根據用於擁有者及計算裝置資源的虛擬資源識別符至計算裝置資源映射、由虛擬資源識別符「VA2」表示的計算裝置資源。

列412說明：由擁有者識別符「O2」指定之擁有者實體可為根據用於擁有者及計算裝置資源的虛擬資源識別符至計算裝置資源映射、由虛擬

資源識別符「VB1」表示的計算裝置資源之擁有者。然而，可選有效性指示符資料欄406中之有效性指示符值「0」可指示：由擁有者識別符「O2」指定之擁有者實體係由虛擬資源識別符「VB1」指示之計算裝置資源的過去或潛在擁有者，而非當前擁有者。在不包括可選有效性指示符資料欄406之一些實施中，列412可自所有權表400省略。

圖5說明資料保護系統300可使用以儲存計算裝置資源之過去、當前及/或潛在請求實體之功能憑證之資料的憑證表500之非限制性實例。各種實施可包括功能憑證資料之不同組合及排序，功能憑證資料包括請求實體識別符、憑證資料或憑證資料參考及存取類型。

在一些實施中，術語憑證資料及憑證資料參考可互換地使用。實例憑證表500包括請求實體識別符資料欄502及憑證資料欄504。如本文中進一步所論述，憑證表500亦可包括可選存取類型資料欄506。憑證表500可包括多個列(例如列508至514)，每一列表示計算裝置資源之請求實體的不同認證功能。

請求實體識別符資料欄502可包括針對計算裝置之每一請求實體或潛在請求實體的特有識別符。該等請求實體識別符可用以傳達請求存取計算裝置資源之實體之身分。

憑證資料欄504可包括至憑證儲存所在之位置的用於請求實體或請求實體之功能的憑證或參考(諸如，指標)。在一些實施中，憑證表500僅包括計算裝置資源之當前請求實體的輸入項。在此等實施中，輸入項可回應於計算裝置資源之所有權之變化而自憑證表500移除，使得請求存取各別所擁有計算裝置資源的擁有者不可在憑證表500中列出。移除輸入項可涉及刪除、無效化或覆寫經移除輸入項。

在一些實施中，憑證表500之輸入項可在作出對存取計算裝置資源之請求時添加，或憑證表500可預想填入潛在請求實體及其憑證之可能組合中的一些或全部。在一些實施中，即使計算裝置資源之所有權有變化，仍可保持輸入項。在將擁有者作為請求實體包括於憑證表500中的一些實施中，計算裝置資源之所有權可在對資源內容之虛擬視圖加密之前經確認。在一些實施中，可存在憑證表500中之輸入項之數目的極限「M」，且輸入項可根據替換準則而移除以便添加當前或潛在請求實體。

在一些實施中，憑證表500可包括可選存取類型資料欄506，其可包括用於指示請求實體所准許的對資源內容之存取之類型的值。包括可選存取類型資料欄506可允許較快加密，此係因為較少時間及資源可用在判定將使用之加密類型上。包括指示請求實體之存取類型之值及認證功能的輸入項可包括與加密之類型及/或位準相關之存取類型的識別符，或包括加密之類型及/或位準的識別符。可選存取類型資料欄506中之值可與認證功能及/或請求實體是否為擁有者相關。

在一些實施中，擁有者請求實體可關於認證功能或不論該功能而被授予對資源內容之無遮掩存取。列508說明亦作為所請求之計算裝置資源之擁有者的請求實體之實例。列510至514說明並非所請求之計算裝置資源之擁有者的請求實體。列510至514中之請求實體中之每一者之認證功能可與規定存取類型相關，該規定存取類型控制資料保護系統300可應用於提供至請求實體的所請求之資源內容之虛擬視圖的加密之類型及/或位準。舉例而言，列510指示：請求實體「R1」之憑證「CA2」可允許所請求之資源內容之虛擬視圖的僅部分遮掩。資料保護系統300可將完全或部分同態加密應用於由請求實體「R1」所作出之請求的所請求之資源內容

之虛擬視圖。類似地，列512及514指示：請求實體R2」及「RN」之憑證「CB1」及「CC1」分別可僅允許所請求之資源內容之虛擬視圖的遮掩。資料保護系統300可將強加密應用於由請求實體「R2」及「RN」所作出之請求的所請求之資源內容之虛擬視圖。

資料保護系統300之組件(虛擬化介面監視器302、資源內容密碼編譯裝置304)、所有權表400及憑證表500在各種實施中可以不同方式配置而不背離申請專利範圍之範疇。在一些實施中，所有權表400及憑證表500可組合、分裂成更多表，或包括經描述將包括於所有權表400及憑證表500中之另一者中的一或多個項目。

圖6說明根據各種實施例的用於使用虛擬資源視圖保護資料之方法600。方法600可在計算裝置中使用執行於通用硬體(諸如，處理器)上及/或實施資料保護系統、虛擬化介面監視器及/或資源內容密碼編譯裝置之專用硬體上的軟體來執行。

在區塊602中，計算裝置可執行資源管理器以將計算裝置資源之所有權指派給擁有者。如上文所論述，資源管理器可包括作業系統、超管理器及/或TrustZone，且擁有者可包括應用程式、作業系統、超管理器及/或TrustZone。將計算裝置資源之所有權指派給擁有者允許資源管理器在擁有者準備好取得計算裝置資源之所有權的情況下向擁有者授予所有權。舉例而言，計算裝置資源之所有權可指派給擁有者，但擁有者可在準備好取得計算裝置資源之所有權之前等待其他資源變得可用或其他程序完成。計算裝置資源之所有權之指派在所有權在一時間段未取得的情況下可到期，由此使得計算裝置資源可用於指派給其他擁有者。在一些實施例中，對計算裝置資源之所有權的指派可回應於對所有權之請求、所有權佇列中之下

一個擁有者、對直接信號或資源之可獲得性之廣播作出回應之第一擁有者，或用於基於各種準則(包括電力及效能參數)判定下一個擁有者之演算法。

在區塊604中，計算裝置可監視經指派擁有者對計算裝置資源之所有權的請求。在一些實施例中，計算裝置資源之經指派擁有者可請求計算裝置對計算裝置資源之所有權之指派的應答接受的所有權。在一些實施例中，對計算裝置資源之所有權的請求可發信至其他組件、系統及/或計算裝置資源之所有權的經指派擁有者之潛在擁有者。為監視經指派擁有者對於計算裝置資源之所有權之請求，計算裝置之組件(諸如，處理器、資料保護系統及/或虛擬化介面監視器)可接收、偵測或攔截計算裝置資源之所有權之請求。

在區塊606中，計算裝置可追蹤計算裝置資源之所有權之變化。計算裝置之組件(諸如，處理器、資料保護系統及/或虛擬化介面監視器)可使用對計算裝置資源之所有權的請求之資訊來判定作為計算裝置資源之擁有者的實體。為追蹤計算裝置資源之所有權，計算裝置可更新表或資料結構，諸如關於參看圖7之方法700進一步所描述的所有權表。

在區塊608中，計算裝置可監視任何實體、擁有者或非擁有者的存取計算裝置資源之請求。在一些實施例中，計算裝置資源之擁有者可請求存取計算裝置資源以讀取或寫入資源內容。在一些實施例中，非擁有者可正當地請求存取計算裝置資源，以實施資源內容之管理功能，諸如移動、複製或搜尋資源內容。然而，非擁有者的存取計算裝置資源之一些請求可藉由對非擁有者取得控制或有影響以達成對資源內容之存取的惡意演員(malicious actors)促使。為監視存取計算裝置資源之請求，計算裝置之組

件(諸如，處理器、資料保護系統及/或虛擬化介面監視器)可接收、偵測或攔截對存取計算裝置資源之請求。計算裝置可自存取計算裝置資源之請求抽取資訊，諸如目標在存取計算裝置資源之請求中的虛擬資源識別符。由此，計算裝置可監視計算裝置之虛擬化介面(其負責轉譯存取計算裝置資源之請求中所使用的計算裝置資源之虛擬資源識別符)，且回應該等請求。舉例而言，計算裝置可抽取計算裝置資源之虛擬位址且監視負責虛擬位址及實體位址轉譯之虛擬化介面。

在判定區塊610中，計算裝置可判定受監視的存取計算裝置資源之請求是否來源於目標在存取計算裝置資源之請求中的計算裝置資源之擁有者。不同實體(擁有者及非擁有者)對於同一計算裝置資源可使用不同的虛擬資源識別符至計算裝置資源映射。虛擬化介面可用以識別計算裝置之實體中之哪一個發出存取計算裝置資源之請求。

作為判定區塊610中之操作之部分，計算裝置之組件(諸如，處理器、資料保護系統及/或虛擬化介面監視器)可使用自存取計算裝置資源之請求抽取的資訊且將該資訊與所有權表中之資訊進行比較。在一些實施中，目標在存取計算裝置資源之請求中的虛擬資源識別符可與請求實體相關。相關可使用虛擬化介面映射作出，以識別可請求目標在存取計算裝置資源之請求中之虛擬資源識別符的實體。在一些實施中，經識別請求者可與可為所有權表中之擁有者識別符的雙倍之實體識別符相關。

在一些實施中，與存取計算裝置資源之請求相關的實體識別符及/或虛擬資源識別符可與所有權表中之相同類型之資訊的輸入項進行比較，以判定是否發現匹配。在一些實施中，所有權表可僅含有當前擁有者之輸入項，且匹配可指示請求者係擁有者，而不匹配可指示請求者係非擁有者。

在一些實施中，所有權表可包括計算裝置資源之過去、當前及/或潛在擁有者之輸入項，且來自所有權表之額外資訊(如有效性指示符)可經檢查以判定匹配是否亦指示請求者係擁有者或非擁有者。舉例而言，有效性指示符可指示匹配輸入項有效，從而指示請求者係擁有者。相反地，有效性指示符可指示匹配輸入項無效，從而指示請求者係非擁有者。

回應於判定受監視的存取計算裝置資源之請求來源於目標在存取計算裝置資源之請求中的計算裝置資源之擁有者(即，判定區塊610=「是」)，在區塊612中，計算裝置可提供回應於存取計算裝置資源之請求所提供的資源內容之無遮掩/未加密的虛擬視圖。針對規定虛擬資源識別符的存取計算裝置資源之請求可提示計算裝置將計算裝置資源之資源內容傳回至請求者。在一些實施中，計算裝置可經組態以提供資源內容作為虛擬視圖。因而，計算裝置可能夠保護資源內容免於在請求實體對資源內容之處理期間有缺陷或錯誤之情況下變得損壞。計算裝置亦可能夠藉由使用虛擬視圖而同時為多個實體提供資源內容之不同存取。在一些實施中，計算裝置資源之擁有者可受信任而未被用於資源內容之惡意存取，因此擁有者具備來自擁有者計算裝置資源之資源內容的無遮掩/未加密的虛擬視圖。在一些實施中，計算裝置之組件(包括處理器、資料保護系統及/或資源內容密碼編譯裝置)可在不遮掩/不加密虛擬視圖之情況下產生或傳遞資源內容之虛擬視圖。在一些實施中，計算裝置組件可被繞過，此係因為不需要遮掩/加密資源內容之虛擬視圖。

回應於判定受監視的存取計算裝置資源之請求來源於目標在存取計算裝置資源之請求中的計算裝置資源之非擁有者(即，判定區塊610=「否」)，在區塊614中，計算裝置可遮掩回應於存取計算裝置資源之請求

所提供的資源內容之虛擬視圖。計算裝置可判定用以遮掩資源內容之虛擬視圖的加密之類型及/或位準，如關於參看圖8之方法800進一步所描述。計算裝置之組件(包括處理器、資料保護系統及/或資源內容密碼編譯裝置)可遮掩資源內容之虛擬視圖，以保護資源內容免於經由非擁有者之惡意存取。在一些實施中，遮掩資源內容之虛擬視圖並不禁止非擁有者在不具有資源內容之清楚視圖的情況下實施合法存取及管理功能。在一實例中，資源內容在以區塊移動時可能無意義，此係因為資源內容無變化，僅該等資源內容之位置有變化，或移動資源內容之實體不必知道資源內容之資料的細節。在另一實例中，部分遮掩資源內容可允許對密文之某一搜尋及算術操控，其可足以藉由非擁有者提供必需回饋或無遮掩資源內容之對應變化而實施功能。

在區塊616中，計算裝置可提供資源內容之遮掩/經加密虛擬視圖。類似於區塊612中的提供無遮掩/未加密的虛擬視圖，計算裝置可將資源內容之虛擬視圖提供至請求實體。然而，提供至非擁有者之虛擬視圖經遮掩/經加密。

在區塊618中，計算裝置可追蹤所擁有之計算裝置資源的釋放。以類似於區塊604中的監視計算裝置資源之所有權之請求的方式，計算裝置可接收、偵測或攔截指示所擁有之計算裝置資源的釋放之信號。釋放信號可告知其他實體及計算裝置之組件：計算裝置資源可用於所有權。在一些實施例中，計算裝置之組件(諸如，處理器、資料保護系統及/或虛擬化介面監視器)可回應於釋放信號而更新所有權表。在一些實施例中，指示先前擁有者對計算裝置資源之所有權的輸入項可自所有權表移除或在所有權表中標記無效。

圖7說明根據各種實施例的用於追蹤計算裝置資源之所有權之方法700。方法700可在計算裝置中使用執行於通用硬體(諸如，處理器)上及/或實施資料保護系統、虛擬化介面監視器及/或資源內容密碼編譯裝置之專用硬體上的軟體來執行。

在判定區塊702中，計算裝置可判定輸入項是否存在於計算裝置資源之資料結構或表(諸如，所有權表)中。計算裝置之組件(諸如，處理器、資料保護系統及/或虛擬化介面監視器)可將存取計算裝置資源之請求之虛擬資源識別符與儲存於所有權表之輸入項中的對應資訊之值進行比較。具有存取計算裝置資源之請求之相同虛擬資源識別符的輸入項可指示針對計算裝置分量之輸入項存在。此外，由於不同擁有者可使用不同虛擬資源識別符而映射至同一計算裝置資源，因此具有虛擬資源識別符之輸入項可指示針對請求擁有者所擁有的計算裝置分量之輸入項存在。缺少具有存取計算裝置資源之請求之相同虛擬資源識別符的輸入項可指示針對計算裝置分量之輸入項不存在。然而，與存取計算裝置資源之請求具有相同虛擬資源識別符之輸入項的缺少可實際上指示請求計算裝置資源之所有權的當前擁有者在過去、當前或潛在地擁有之計算裝置組件之輸入項的缺少。由於不同擁有者可使用不同虛擬資源識別符映射至同一計算裝置資源，因此輸入項可針對計算裝置之其他過去、當前或潛在擁有者存在。在一些實施中，計算裝置亦可檢查供其他過去、當前或潛在擁有者使用的計算裝置組件之虛擬資源識別符。

回應於判定輸入不存在於計算裝置資源之所有權表中(即，判定區塊702=「否」)，在區塊710中，計算裝置可在計算裝置資源之所有權表中建立一輸入項。計算裝置之組件(諸如，處理器、資料保護系統及/或虛擬

化介面監視器)可將資料(包括計算裝置資源之所有權之請求的虛擬資源識別符及/或相關於虛擬資源識別符之經識別擁有者識別符)寫入至所有權表，以編輯現有輸入項或建立新輸入項。在一些實施中，現有輸入項可能陳舊或不再與計算裝置之資源之所有權的狀態相關且可被覆寫。

在一些實施例中，在可選區塊712中，計算裝置可將計算裝置資源之請求擁有者的新輸入項標記為有效，如本文中將更詳細描述。計算裝置可前進至監視任何實體的存取計算裝置資源之請求(在區塊608中)，如參看圖6所描述。

回應於判定輸入項存在於計算裝置資源之所有權表中(即，判定區塊702=「是」)，在判定區塊704中，計算裝置可判定計算裝置資源之請求擁有者是否與計算裝置資源之先前擁有者相同。如本文中所論述，計算裝置資源之過去、當前或潛在擁有者可藉由計算裝置資源之所有權之請求的虛擬資源識別符或相關擁有者識別符來識別。計算裝置之組件(諸如，處理器、資料保護系統及/或虛擬化介面監視器)可將計算裝置資源之所有權請求的資料與經識別輸入項進行比較，以判定請求擁有者是否與同一計算裝置資源之輸入項中所列出之擁有者相同。

回應於判定計算裝置資源之請求擁有者不與計算裝置資源之先前擁有者相同(即，判定區塊704=「否」)，在可選區塊708中，計算裝置可將具有不同擁有者之計算裝置資源的輸入項移除或標記無效。計算裝置之組件(諸如，處理器、資料保護系統及/或虛擬化介面監視器)可移除與計算裝置資源所有權請求相同之計算裝置資源的具有不同擁有者之任何輸入項。在一些實施例中，與計算裝置資源所有權請求相同之計算裝置資源的具有不同擁有者之輸入項可經維持，但藉由設定所有權表中之輸入項之有效性

指示符而標記為無效。同一計算裝置資源之其他輸入項可藉由該等輸入項之虛擬資源識別符及該等輸入項的同一計算裝置資源之各別映射來識別。

在區塊710中，計算裝置可關於計算裝置資源在所有權表中建立輸入項，且在可選區塊712中，計算裝置可將計算裝置資源之請求擁有者的新輸入項標記為有效，如本文中進一步描述。在區塊608中，計算裝置可監視任何實體的存取計算裝置資源之請求，如參看圖6所描述。

回應於判定計算裝置資源之請求擁有者與計算裝置資源之先前擁有者相同(即，判定區塊704=「是」)，在可選判定區塊706中，計算裝置可判定與計算裝置資源之請求擁有者相同的擁有者之輸入項是否有效。計算裝置之組件(諸如，處理器、資料保護系統及/或虛擬化介面監視器)可檢查同一計算裝置資源及擁有者的所有權表中之輸入項之有效性指示符之值。

回應於判定與計算裝置資源之請求擁有者相同的擁有者之輸入項有效(即，判定區塊706=「是」)，在區塊608中，計算裝置可監視任何實體的存取計算裝置資源之請求，如參看圖6所描述。

回應於判定計算裝置資源之相同擁有者之輸入項無效(即，判定區塊706=「否」)，在可選區塊712中，計算裝置可將計算裝置資源之相同擁有者之輸入項標記為有效。計算裝置之組件(諸如，處理器、資料保護系統及/或虛擬化介面監視器)可修改所有權表中之有效性指示符之值以指示輸入項有效而非無效。在區塊608中，計算裝置可監視任何實體的存取計算裝置資源之請求，如參看圖6所描述。

圖8說明用於使用憑證以用於將加密應用於資源內容之虛擬視圖之一實施例方法800。方法800可在計算裝置中使用執行於通用硬體(諸如，處理器)上及/或實施資料保護系統、虛擬化介面監視器及/或資源內容密碼編

譯裝置之專用硬體上的軟體來執行。

在區塊802中，計算裝置可判定非擁有者計算裝置資源存取請求者針對功能是否與憑證相關聯。如本文中所論述，非擁有者資源管理器及應用程式或非擁有者請求實體可對其並不擁有之計算裝置資源做出計算裝置資源存取請求。資源管理器及應用程式可經組態以執行藉由開發人員或藉由計算裝置之編譯器認證的功能。功能之憑證可指示對於非擁有者請求實體所允許的存取資源內容之位準。計算裝置之組件(包括處理器、資料保護系統及/或資源內容密碼編譯裝置)可判定輸入項是否存在於非擁有者請求實體之資料結構或表(諸如，憑證表)中。請求實體識別符可指示針對相關非擁有者請求實體的憑證表中之輸入項。缺少憑證表中之輸入項可指示請求實體未經認證。

回應於判定非擁有者請求實體與功能之憑證相關聯(即，判定區塊802=「是」)，在判定區塊804中，計算裝置可判定存取資源內容指定為部分遮掩抑或完全遮掩。計算裝置之組件(包括處理器、資料保護系統及/或資源內容密碼編譯裝置)可自與非擁有者請求實體相關之各別憑證或自憑證表中之非擁有者請求實體之一輸入項擷取存取類型。在一些實施中，憑證或憑證之參考可儲存於憑證表中之非擁有者請求實體之輸入項中。計算裝置可自憑證表或自憑證之參考之位置擷取憑證。自憑證之資料，計算裝置擷取非擁有者請求實體之存取。在一些實施中，憑證表可包括非擁有者請求實體之輸入項中的存取類型，且計算裝置可自憑證表中之對應輸入項擷取存取類型。如本文中所論述，存取類型可指定在將資源內容之虛擬視圖提供至非擁有者請求實體時所使用的加密之類型及/或位準或遮掩之位準。

回應於判定存取資源內容經指定為部分遮掩(即，判定區塊804=「部分」)，在區塊806中，計算裝置可遮掩資源內容之虛擬視圖/對其加密。計算裝置之組件(包括處理器、資料保護系統及/或資源內容密碼編譯裝置)可使用部分或完全同態加密來遮掩資源內容之虛擬視圖/對資源內容之虛擬視圖加密，部分或完全同態加密經組態以防止對資源內容之觀察、使用或操控，但允許對密文之搜尋或算術操控。如本文中所論述，非擁有者請求實體仍然可實施一些功能(搜尋或算術操控密文)而不存取資源內容，此導致如同對資源內容實施該等功能的類似結果。換言之，非擁有者請求實體可在不能夠讀取、寫入、操控或解譯資源內容之情況下實施特定功能，但仍然可產生類似於能夠讀取、寫入、操控或解譯資源內容之情況下之結果的結果。

回應於判定非擁有者請求實體不與功能之憑證相關聯(即，判定區塊802=「否」)，或回應於判定存取資源內容經指定為完全遮掩(即，判定區塊804=「完全」)，在區塊808中，計算裝置可遮掩資源內容之虛擬視圖/對虛擬視圖加密，如本文中進一步描述。計算裝置之組件(包括處理器、資料保護系統及/或資源內容密碼編譯裝置)可使用強加密來遮掩資源內容之虛擬視圖/對虛擬視圖加密，強加密經組態以防止對資源內容之觀察、使用或操控。如本文中所論述，非擁有者請求實體仍然可實施一些功能(諸如，管理功能)，不存取資源內容，但能夠存取具有資源內容的資料之不透明區塊。換言之，非擁有者請求實體可在不能夠讀取、寫入、操控或解譯資源內容之情況下實施特定功能。

如參看圖6所描述，在區塊616中，計算裝置可將資源內容之遮掩/經加密虛擬視圖提供至請求實體。

各種實施例(包括(但不限於)上文參看圖1至圖8所論述之實施例)可實施於廣泛多種計算系統中，該等計算系統可包括適合於與圖9中所說明之各種實施例一起使用的實例行動計算裝置。行動計算裝置900可包括耦接至內部記憶體906之處理器902。處理器902可為經指定用於一般或特定處理任務之一或多個多核心積體電路。內部記憶體906可為揮發性或非揮發性記憶體，且亦可為安全及/或加密記憶體，或不安全及/或未加密之記憶體，或其任何組合。可利用的記憶體類型之實例包括(但不限於)DDR、LPDDR、GDDR、WIDEIO、RAM、SRAM、DRAM、P-RAM、R-RAM、M-RAM、STT-RAM，及嵌入型動態隨機存取記憶體(DRAM)。

處理器902可耦接至行動計算裝置之顯示器912，其可具有或可不具有觸控螢幕能力。在一些實施中，顯示器912可為觸控螢幕面板912，諸如電阻性感測觸控螢幕、電容性感測觸控螢幕、紅外線感測觸控螢幕等。觸控螢幕顯示器912可耦接至觸控螢幕控制器904及處理器902。

行動計算裝置900可具有用於發送及接收通信、彼此耦接及/或耦接至處理器902的一或多個無線電信號收發器908 (例如，花生(Peanut)、藍芽、紫蜂(ZigBee)、Wi-Fi、RF無線電)及天線910。收發器908及天線910可與上文所提及之電路一起使用，以實施各種無線傳輸協定堆疊及介面。行動計算裝置900可包括蜂巢式網路無線數據機晶片916，其實現經由蜂巢式網路之通信且耦接至處理器。

行動計算裝置900可包括耦接至處理器902之周邊裝置連接介面918。周邊裝置連接介面918可單一地經組態以接受一種類型之連接，或可經組態以接受共同或專有的各種類型之實體及通信連接，諸如USB、FireWire、Thunderbolt或PCIe。周邊裝置連接介面918亦可耦合至經類似

地組態之周邊裝置連接埠(圖中未示)。

行動計算裝置900亦可包括用於提供音訊輸出之揚聲器914。行動計算裝置900亦可包括用於含有本文中所論述之組件之全部或一些的外殼920，其由塑膠、金屬或材料之組合建構。行動計算裝置900可包括耦接至處理器902之電源922，諸如一次性或可再充電電池。可再充電電池亦可耦接至周邊裝置連接埠以自行動計算裝置900外部之電源接收充電電流。行動計算裝置900亦可包括用於接收使用者輸入之實體按鈕924。行動計算裝置900亦可包括用於打開及關閉行動計算裝置900之電源按鈕926。

各種實施例(包括(但不限於)如上文參看圖1至圖8所論述之實施例)可實施於廣泛多種計算系統中，該等計算系統可包括多種行動計算裝置，諸如圖10中所說明之膝上型電腦1000。許多膝上型電腦包括充當電腦之指標裝置之觸控板觸控表面1017，且因此可接收類似於在配備有觸控螢幕顯示器及上文所描述之計算裝置上實施之彼等手勢的拖曳(拖曳)、捲動(scroll)及撥動(flick)手勢。膝上型電腦1000將通常包括耦接至揮發性記憶體1012及大容量非揮發性記憶體(諸如，快閃記憶體之磁碟機1013)的處理器1011。另外，電腦1000可具有用於發送及接收電磁輻射之一或多個天線1008，天線可連接至耦接至處理器1011之無線資料鏈路及/或蜂巢式電話收發器1016。電腦1000亦可包括耦接至處理器1011之軟碟驅動機1014及緊密光碟(CD)驅動機1015。在筆記型電腦組態中，電腦殼體包括觸控板1017、鍵盤1018及顯示器1019，其均耦接至處理器1011。計算裝置之其他組態可包括所熟知的耦接至處理器(例如，經由通用串列匯流排(USB)輸入端)之電腦滑鼠或軌跡球，其亦可結合各種實施例而使用。

各種實施例(包括(但不限於)上文參看圖1至圖8所論述之實施例)可實

施於廣泛多種計算系統中，該等計算系統可包括多種可購得之計算裝置(諸如，伺服器)中之任一者。實例伺服器1100說明於圖11中。此伺服器1100通常包括耦接至揮發性記憶體1102及大容量非揮發性記憶體(諸如，磁碟機1104)之一或多個多核心處理器組合件1101。如圖11中所說明，多核心處理器組合件1101可藉由插入至組合件之機架中而添加至伺服器1100。伺服器1100亦可包括耦接至處理器1101之軟碟驅動機、緊密光碟(CD)或DVD光碟驅動機1106。伺服器1100亦可包括耦接至多核心處理器組合件1101以用於建立與網路1105之網路介面連接的網路存取埠1103，該網路諸如耦接至其他廣播系統電腦及伺服器之區域網路、網際網路、公眾交換電話網路及/或蜂巢式資料網路(例如，CDMA、TDMA、GSM、PCS、3G、4G、LTE，或任何其他類型之蜂巢式資料網路)。

用於在可程式化處理器上執行以用於進行各種實施例之操作的電腦程式碼或「程式碼」可以諸如C、C++、C#、Smalltalk、Java、JavaScript、Visual Basic、結構化查詢語言(例如，交易SQL)、Perl之高階程式化語言或以各種其他程式化語言寫入。如本申請案中所使用的儲存於電腦可讀儲存媒體上之程式碼或程式可指機器語言程式碼(諸如，目標程式碼)，其格式可由處理器理解。

前述方法描述及程序流程圖係僅作為說明性實例而提供，且並不意欲要求或暗示必須以所呈現之次序執行各種實施例之操作。如將由熟習此項技術者瞭解，可以任何次序執行前述實施例中之操作的次序。諸如「此後」、「接著」、「隨後」等之詞並不意欲限制操作之次序；此等詞僅用以引導讀者閱讀方法之描述。此外，對呈單數形式之申請專利範圍元件之任何提及(例如，使用詞「一」或「該」)不應解釋為將元件限於單數形式。

結合各種實施例所描述的各種說明性邏輯區塊、模組、電路及演算法操作可實施為電子硬體、電腦軟體或兩者之組合。為了清楚地說明硬體與軟體之此互換性，已在上文中就各種說明性組件、區塊、模組、電路及操作之功能性對其加以大體描述。將此功能性實施為硬體或軟體視特定應用及強加於整個系統之設計約束而定。熟習此項技術者可針對每一特定應用而以不同方式實施所描述之功能性，但該等實施決策不應被解釋為引起脫離申請專利範圍之範疇。

藉由通用處理器、數位信號處理器(DSP)、特殊應用積體電路(ASIC)、場可程式化閘陣列(FPGA)或其他可程式化邏輯裝置、離散閘或電晶體邏輯、離散硬體組件或其經設計以執行本文中所描述之功能之任何組合，可實施或執行用以實施結合本文中所揭示之實施例所描述之各種說明性邏輯、邏輯區塊、模組及電路的硬體。通用處理器可為微處理器，但在替代方案中，處理器可為任何習知之處理器、控制器、微控制器或狀態機。處理器亦可實施為計算裝置之組合，例如，一DSP與一微處理器之組合、複數個微處理器、一或多個微處理器結合DSP核心或任何其他此組態。替代地，一些操作或方法可由特定於給定功能之電路來執行。

在一或多個實施例中，所描述功能可以硬體、軟體、韌體或其任何組合來實施。若以軟體來實施，則該等功能可作為一或多個指令或程式碼儲存於非暫時性電腦可讀媒體或非暫時性處理器可讀媒體上。本文中所揭示之方法或演算法之操作可體現於處理器可執行軟體模組中，處理器可執行軟體模組可駐存於非暫時性電腦可讀或處理器可讀儲存媒體上。非暫時性電腦可讀或處理器可讀儲存媒體可為可由電腦或處理器存取之任何儲存媒體。作為實例而非限制，此非暫時性電腦可讀或處理器可讀媒體可包括

RAM、ROM、EEPROM、FLASH記憶體、CD-ROM或其他光碟儲存裝置、磁碟儲存裝置或其他磁性儲存裝置，或可用於以指令或資料結構之形式儲存所要程式碼且可由電腦存取之任何其他媒體。如本文所使用之磁碟及光碟包括緊密光碟(CD)、雷射光碟、光學光碟、數位多功能光碟(DVD)、軟碟及藍光光碟，其中磁碟通常以磁性方式再現資料，而光碟用雷射以光學方式再現資料。以上各者之組合亦包括於非暫時性電腦可讀及處理器可讀媒體之範疇內。另外，方法或演算法之操作可作為程式碼及/或指令中之一者或任何組合或集合而駐存於可併入至電腦程式產品中之非暫時性處理器可讀媒體及/或電腦可讀媒體上。

提供對所揭示實施例之先前描述以使任何熟習此項技術者能夠製作或使用申請專利範圍。對此等實施例之各種修改將對熟習此項技術者顯而易見，且可在不脫離申請專利範圍之範疇的情況下將本文中所定義之一般原理應用於其他實施例。因此，本發明並不意欲受限於本文中展示之實施例，而應符合與以下申請專利範圍及本文中揭示之原理及新穎特徵一致的最廣範疇。

【符號說明】

10	計算裝置
12	系統單晶片(SoC)
14	處理器
16	記憶體
18	通信介面
20	儲存記憶體介面
22	通信組件

24	儲存記憶體
26	天線
28	網路介面
30	無線網路
32	無線連接
40	網際網路
44	有線連接
50	遠端計算裝置
200	處理器核心
201	處理器核心
202	處理器核心
203	處理器核心
300	資料保護系統
302	虛擬化介面監視器
304	資源內容密碼編譯裝置
306	作業系統
308	超管理器
310	TrustZone
312	應用程式
314	轉譯後援緩衝器
400	所有權表
402	擁有者識別符資料欄
404	虛擬資源識別符資料欄

406 可選有效性指示符資料欄

408 列

410 列

412 列

414 列

500 憑證表

502 請求實體識別符資料欄

504 憑證資料欄

506 可選存取類型資料欄

508 列

510 列

512 列

514 列

600 用於使用虛擬資源視圖保護資料之方法

602 區塊

604 區塊

606 區塊

608 區塊

610 判定區塊

612 區塊

614 區塊

616 區塊

618 區塊

700	用於追蹤計算裝置資源之所有權之方法
702	判定區塊
704	判定區塊
706	可選判定區塊
708	可選區塊
710	區塊
712	可選區塊
800	使用憑證以用於將加密應用於資源內容之虛擬視圖之方法
802	判定區塊
804	判定區塊
806	區塊
808	區塊
900	行動計算裝置
902	處理器
904	觸控螢幕控制器
906	內部記憶體
908	無線電信號收發器
910	天線
912	顯示器/觸控螢幕面板
914	揚聲器
916	蜂巢式網路無線數據機晶片
918	周邊裝置連接介面
920	外殼

922	電源
924	實體按鈕
926	電源按鈕
1000	膝上型電腦
1008	天線
1011	處理器
1012	揮發性記憶體
1013	磁碟機
1014	軟碟驅動機
1015	緊密光碟(CD)驅動機
1016	無線資料鏈路及/或蜂巢式電話收發器
1017	觸控板觸控表面
1018	鍵盤
1019	顯示器
1100	伺服器
1101	多核心處理器組合件
1102	揮發性記憶體
1103	網路存取埠
1104	磁碟機
1105	網路
1106	軟碟驅動機、緊密光碟(CD)或數位影音光碟(DVD)光碟驅動機

【發明申請專利範圍】

【第1項】

一種使用資源內容之虛擬視圖來保護資料之方法，其包含：

藉由一計算裝置之一虛擬化介面監視器來監視一第一請求實體對存取一計算裝置資源之一請求；

藉由該虛擬化介面監視器來判定該第一請求實體是否為該計算裝置資源之一擁有者；

回應於判定該第一請求實體係該計算裝置資源之該擁有者，藉由該計算裝置之一資料保護系統將該計算裝置資源之資源內容之一無遮掩虛擬視圖提供至該第一請求實體；及

回應於判定該第一請求實體係該計算裝置資源之一非擁有者，藉由該資料保護系統將該計算裝置資源之該等資源內容的一遮掩虛擬視圖提供至該第一請求實體。

【第2項】

如請求項1之方法，其進一步包含：

藉由一資源內容密碼編譯裝置來判定該第一請求實體是否具有一認證功能；

回應於判定該第一請求實體具有一認證功能，藉由該資源內容密碼編譯裝置來判定該第一請求實體之一存取類型；及

回應於判定該第一請求實體係該計算裝置資源之一非擁有者，藉由該計算裝置之一資源內容密碼編譯裝置，使用基於該存取類型之一遮掩位準而遮掩該計算裝置資源之該等資源內容之該等虛擬視圖。

【第3項】

如請求項2之方法，其中該存取類型包括部分遮掩及遮掩，且其中使用基於該存取類型之一遮掩位準而遮掩該計算裝置資源之該等資源內容之該等虛擬視圖包含：

回應於判定用於該第一請求實體之該存取類型為部分遮掩，藉由該資源內容密碼編譯裝置，使用同態加密對該計算裝置資源之該等資源內容之該等虛擬視圖加密；及

回應於判定用於該第一請求實體之該存取類型為遮掩，藉由該資源內容密碼編譯裝置，使用強加密對該計算裝置資源之該等資源內容之該等虛擬視圖加密。

【第4項】

如請求項1之方法，其進一步包含：

藉由該虛擬化介面監視器，關於該計算裝置資源之所有權變化對一虛擬化介面進行監視；及

藉由該虛擬化介面監視器來儲存與用於該第一請求實體的該計算裝置資源之一虛擬資源識別符相關的該第一請求實體之一第一擁有者識別符，其中該第一擁有者識別符指示該第一請求實體經授予該計算裝置資源之所有權且該虛擬資源識別符經映射至該計算裝置資源之一實體資源識別符。

【第5項】

如請求項4之方法，其中關於該計算裝置資源之一所有權變化對一虛擬化介面進行監視包含監視一第二請求實體對該計算裝置資源之所有權之一請求。

【第6項】

如請求項1之方法，其中判定該第一請求實體是否為該計算裝置資源之一擁有者包含：

藉由該虛擬化介面監視器，將存取該計算裝置資源之該請求的一虛擬資源識別符與相關於該計算裝置資源之一虛擬資源識別符的一所儲存擁有者識別符進行比較；及

在存取該計算裝置資源之該請求的該虛擬資源識別符與該計算裝置資源之該虛擬資源識別符匹配時，判定該第一請求實體係該計算裝置資源之該擁有者。

【第7項】

如請求項1之方法，其中：

該計算裝置資源之該擁有者係一應用程式；且

該計算裝置資源之該非擁有者為一資源管理器，包括一作業系統內核、一超管理器及一TrustZone中之一者。

【第8項】

一種計算裝置，其包含：

一資料保護系統，其包含一虛擬化介面監視器及一資源內容密碼編譯裝置，

其中該虛擬化介面監視器經虛擬化介面監視器可執行指令組態以執行包含以下各者之操作：

監視一第一請求實體對存取一計算裝置資源之一請求；及

判定該第一請求實體是否為該計算裝置資源之一擁有者，且

其中該資料保護系統經資料保護系統可執行指令組態以執行包含以下各者之操作：

回應於判定該第一請求實體係該計算裝置資源之該擁有者，將該計算裝置資源之資源內容之一無遮掩虛擬視圖提供至該第一請求實體；及

回應於判定該第一請求實體係該計算裝置資源之一非擁有者，將該計算裝置資源之該等資源內容的一遮掩虛擬視圖提供至該第一請求實體。

【第9項】

如請求項8之計算裝置，其中該資源內容密碼編譯裝置經資源內容密碼編譯裝置可執行指令組態以執行進一步包含以下各者之操作：

判定該第一請求實體是否具有一認證功能；

回應於判定該第一請求實體具有一認證功能，判定該第一請求實體之一存取類型；及

回應於判定該第一請求實體係該計算裝置資源之一非擁有者，遮掩該計算裝置資源之該等資源內容之一虛擬視圖。

【第10項】

如請求項9之計算裝置，其中該存取類型包括部分遮掩及遮掩，且其中該資源內容密碼編譯裝置經資源內容密碼編譯裝置可執行指令組態以執行操作，以使得使用基於該存取類型之一遮掩位準而遮掩該計算裝置資源之該等資源內容之該虛擬視圖包含：

回應於判定用於該第一請求實體之該存取類型為部分遮掩，使用同態加密對該計算裝置資源之該等資源內容之該虛擬視圖加密；及

回應於判定用於該第一請求實體之該存取類型為遮掩，使用強加密對該計算裝置資源之該等資源內容之該虛擬視圖加密。

【第11項】

如請求項8之計算裝置，其中該虛擬化介面監視器經虛擬化介面監視器可執行指令組態以執行進一步包含以下各者的操作：

關於該計算裝置資源之所有權變化對一虛擬化介面進行監視；及

儲存與用於該第一請求實體的該計算裝置資源之一虛擬資源識別符相關的該第一請求實體之一第一擁有者識別符，其中該第一擁有者識別符指示該第一請求實體經授予該計算裝置資源之所有權且該虛擬資源識別符經映射至該計算裝置資源之一實體資源識別符。

【第12項】

如請求項11之計算裝置，其中該虛擬化介面監視器經虛擬化介面監視器可執行指令組態以執行操作，以使得關於該計算裝置資源之一所有權變化對一虛擬化介面進行監視包含監視一第二請求實體對該計算裝置資源之所有權之一請求。

【第13項】

如請求項8之計算裝置，其中該虛擬化介面監視器經虛擬化介面監視器可執行指令組態以執行操作，以使得判定該第一請求實體是否為該計算裝置資源之一擁有者包含：

將存取該計算裝置資源之該請求的一虛擬資源識別符與相關於該計算裝置資源之一虛擬資源識別符的一所儲存擁有者識別符進行比較；及

在存取該計算裝置資源之該請求的該虛擬資源識別符與該計算裝置資源之該虛擬資源識別符匹配時，判定該第一請求實體係該計算裝置資源之該擁有者。

【第14項】

如請求項8之計算裝置，其進一步包含以通信方式連接至該資料保護系統的複數個處理器，且其中：

該計算裝置資源之該擁有者係在該複數個處理器中之一第一處理器上執行的一應用程式；且

該計算裝置資源之該非擁有者為在該複數個處理器中之一第二處理器上執行的一資源管理器，包括一作業系統內核、一超管理器及一TrustZone中之一者。

【第15項】

一種經組態用於使用資源內容之虛擬視圖來保護資料的計算裝置，其包含：

用於監視一第一請求實體對存取一計算裝置資源之一請求的構件；

用於判定該第一請求實體是否為該計算裝置資源之一擁有者的構件；

用於回應於判定該第一請求實體係該計算裝置資源之該擁有者，將該計算裝置資源之資源內容之一無遮掩虛擬視圖提供至該第一請求實體的構件；及

用於回應於判定該第一請求實體係該計算裝置資源之一非擁有者，將該計算裝置資源之資源內容的一遮掩虛擬視圖提供至該第一請求實體的構件。

【第16項】

如請求項15之計算裝置，其進一步包含：

用於判定該第一請求實體是否具有一認證功能的構件；及

用於回應於判定該第一請求實體具有一認證功能，判定該第一請求

實體之一存取類型的構件；及

用於回應於判定該第一請求實體係該計算裝置資源之一非擁有者，使用基於該存取類型之一遮掩位準而遮掩該計算裝置資源之該等資源內容之該等虛擬視圖的構件。

【第17項】

如請求項16之計算裝置，其中該存取類型包括部分遮掩及遮掩，且其中用於使用基於該存取類型之一遮掩位準而遮掩該計算裝置資源之該等資源內容之該等虛擬視圖的構件包含：

用於回應於判定用於該第一請求實體之該存取類型為部分遮掩，使用同態加密對該計算裝置資源之該等資源內容之該等虛擬視圖加密的構件；及

用於回應於判定用於該第一請求實體之該存取類型為遮掩，使用強加密對該計算裝置資源之該等資源內容之該等虛擬視圖加密的構件。

【第18項】

如請求項15之計算裝置，其進一步包含：

用於關於該計算裝置資源之所有權變化對一虛擬化介面進行監視的構件；及

用於儲存與用於該第一請求實體的該計算裝置資源之一虛擬資源識別符相關的該第一請求實體之一第一擁有者識別符，其中該第一擁有者識別符指示該第一請求實體經授予該計算裝置資源之所有權且該虛擬資源識別符經映射至該計算裝置資源之一實體資源識別符。

【第19項】

如請求項18之計算裝置，其中用於關於該計算裝置資源之一所有權

變化對一虛擬化介面進行監視的構件包含用於監視一第二請求實體對該計算裝置資源之所有權之一請求的構件。

【第20項】

如請求項15之計算裝置，其中用於判定該第一請求實體是否為該計算裝置資源之一擁有者的構件包含：

用於將存取該計算裝置資源之該請求的一虛擬資源識別符與相關於該計算裝置資源之一虛擬資源識別符的一所儲存擁有者識別符進行比較的構件；及

用於在存取該計算裝置資源之該請求的該虛擬資源識別符與該計算裝置資源之該虛擬資源識別符匹配時，判定該第一請求實體係該計算裝置資源之該擁有者的構件。

【第21項】

如請求項15之計算裝置，其中：

該計算裝置資源之該擁有者係一應用程式；且

該計算裝置資源之該非擁有者為一資源管理器，包括一作業系統內核、一超管理器及一TrustZone中之一者。

【第22項】

一種非暫時性處理器可讀儲存媒體，其上儲存有處理器可執行指令，該等指令經組態以使一計算裝置之一處理器執行包含以下各者之操作：

監視一第一請求實體對存取一計算裝置資源之一請求；

判定該第一請求實體是否為該計算裝置資源之一擁有者；

回應於判定該第一請求實體係該計算裝置資源之該擁有者，將該計

算裝置資源之資源內容之一無遮掩虛擬視圖提供至該第一請求實體；及

回應於判定該第一請求實體係該計算裝置資源之一非擁有者，將該計算裝置資源之資源內容的一遮掩虛擬視圖提供至該第一請求實體。

【第23項】

如請求項22之非暫時性處理器可讀儲存媒體，其中該等所儲存之處理器可執行指令經組態以使該處理器執行進一步包含以下各者之操作：

判定該第一請求實體是否具有一認證功能；

回應於判定該第一請求實體具有一認證功能，判定該第一請求實體之一存取類型；及

回應於判定該第一請求實體係該計算裝置資源之一非擁有者，使用基於該存取類型之一遮掩位準而遮掩該計算裝置資源之該等資源內容之一虛擬視圖。

【第24項】

如請求項23之非暫時性處理器可讀儲存媒體，其中該存取類型包括部分遮掩及遮掩，且其中該等所儲存之處理器可執行指令經組態以使該處理器執行操作，以使得使用基於該存取類型之一遮掩位準而遮掩該計算裝置資源之該等資源內容的該虛擬視圖包含：

回應於判定用於該第一請求實體之該存取類型為部分遮掩，使用同態加密對該計算裝置資源之該等資源內容之該虛擬視圖加密；及

回應於判定用於該第一請求實體之該存取類型為遮掩，使用強加密對該計算裝置資源之該等資源內容之該虛擬視圖加密。

【第25項】

如請求項22之非暫時性處理器可讀儲存媒體，其中該等所儲存之處

理器可執行指令經組態以使該處理器執行進一步包含以下各者之操作：

關於該計算裝置資源之所有權變化對一虛擬化介面進行監視；及

儲存與用於該第一請求實體的該計算裝置資源之一虛擬資源識別符相關的該第一請求實體之一第一擁有者識別符，其中該第一擁有者識別符指示該第一請求實體經授予該計算裝置資源之所有權且該虛擬資源識別符經映射至該計算裝置資源之一實體資源識別符。

【第26項】

如請求項25之非暫時性處理器可讀儲存媒體，其中該等所儲存之處理器可執行指令經組態以使該處理器執行操作，以使得關於該計算裝置資源之一所有權變化對一虛擬化介面進行監視包含監視一第二請求實體對該計算裝置資源之所有權之一請求。

【第27項】

如請求項22之非暫時性處理器可讀儲存媒體，其中該等所儲存之處理器可執行指令經組態以使該處理器執行操作，以使得判定該第一請求實體是否為該計算裝置資源之一擁有者包含：

將存取該計算裝置資源之該請求的一虛擬資源識別符與相關於該計算裝置資源之一虛擬資源識別符的一所儲存擁有者識別符進行比較；及

在存取該計算裝置資源之該請求的該虛擬資源識別符與該計算裝置資源之該虛擬資源識別符匹配時，判定該第一請求實體係該計算裝置資源之該擁有者。

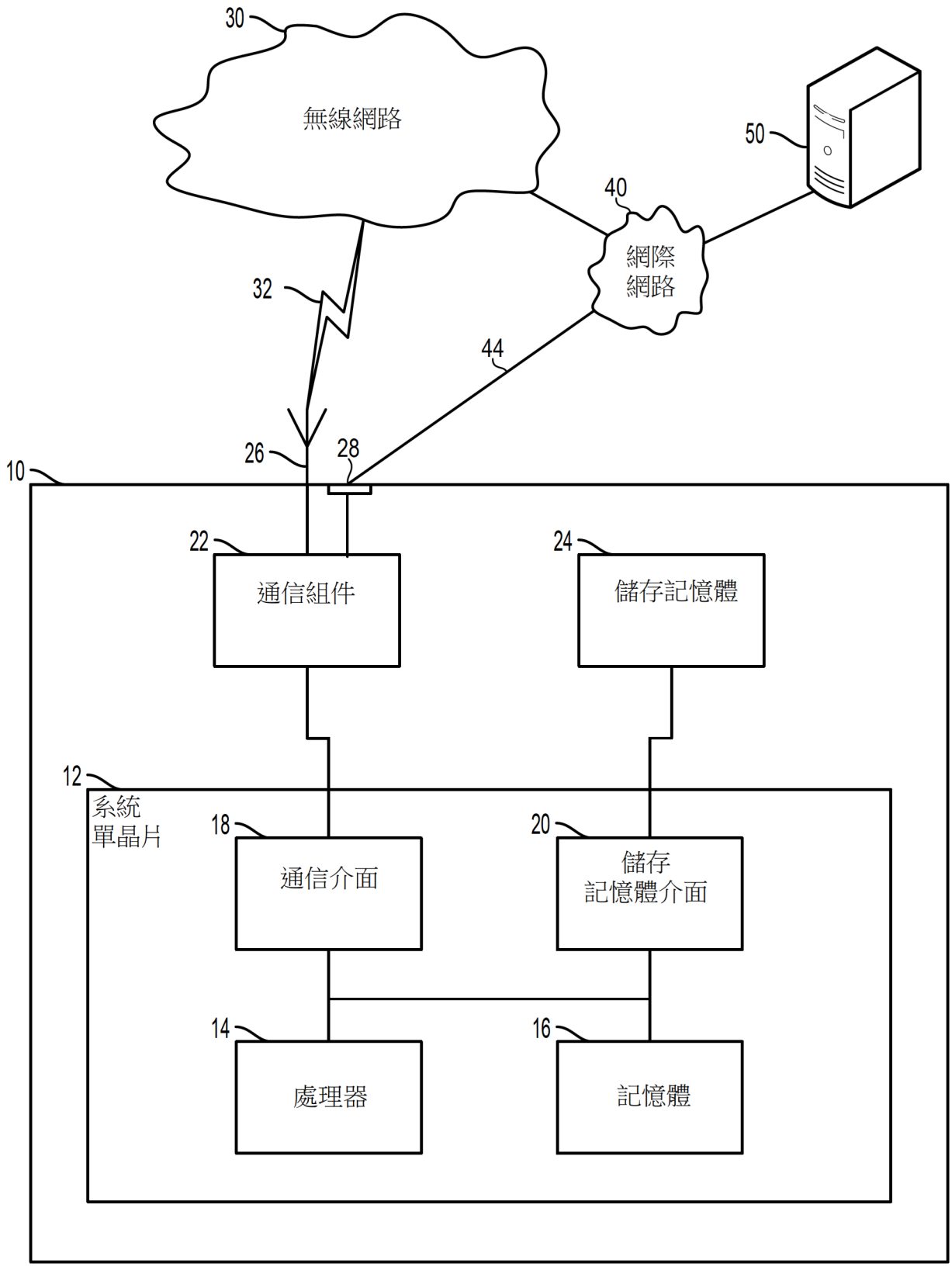
【第28項】

如請求項22之非暫時性處理器可讀儲存媒體，其中：

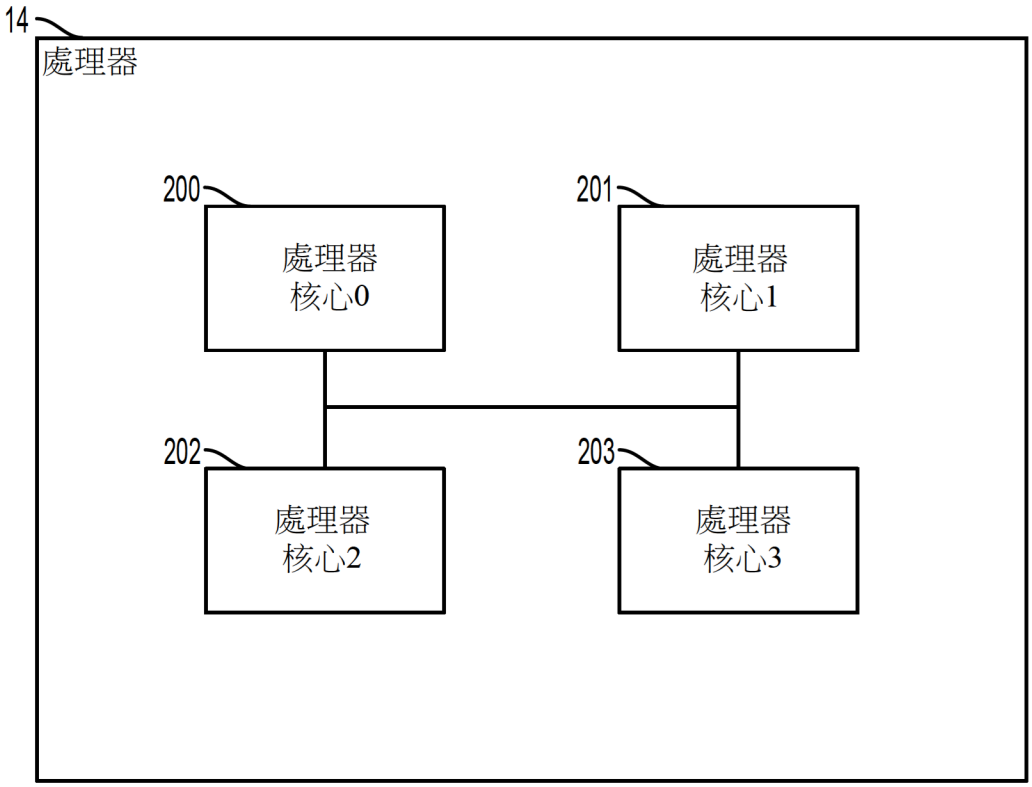
該計算裝置資源之該擁有者係一應用程式；且

該計算裝置資源之該非擁有者為一資源管理器，包括一作業系統內核、一超管理器及一TrustZone中之一者。

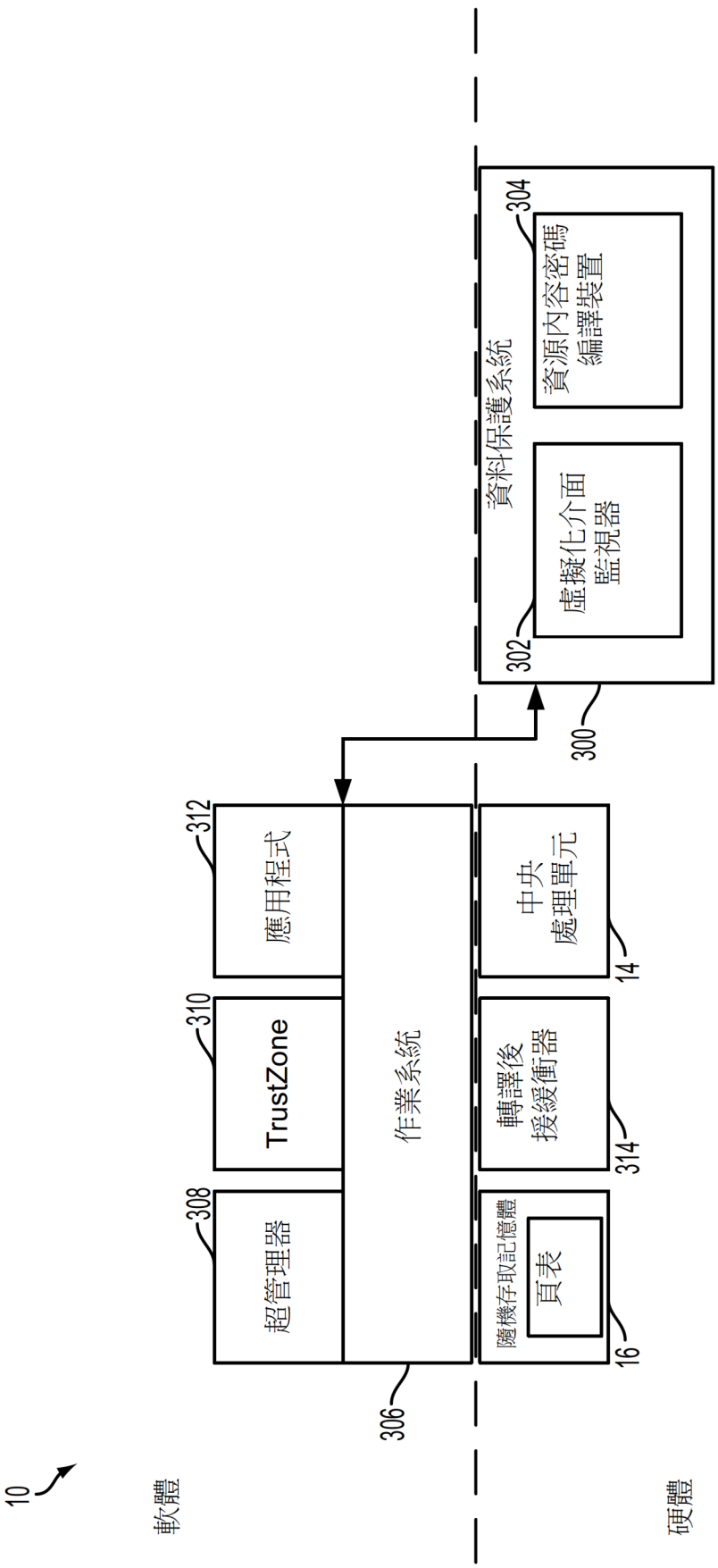
【發明圖式】


30
無線網路
50
40
網際
網路
32
44
26
28
10
22
通信組件
24
儲存記憶體
12
系統
單晶片
18
通信介面
20
儲存
記憶體介面
14
處理器
16
記憶體

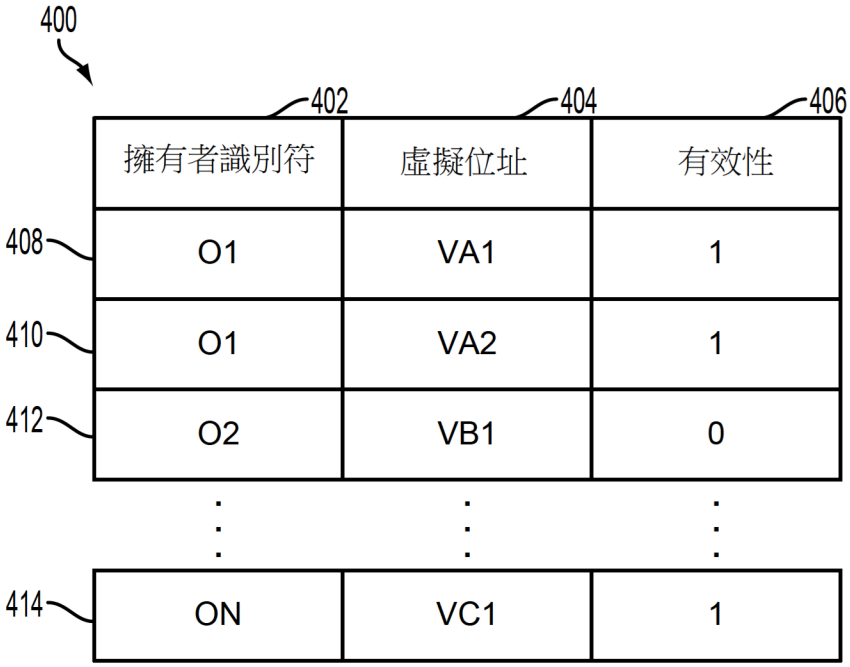
【圖1】



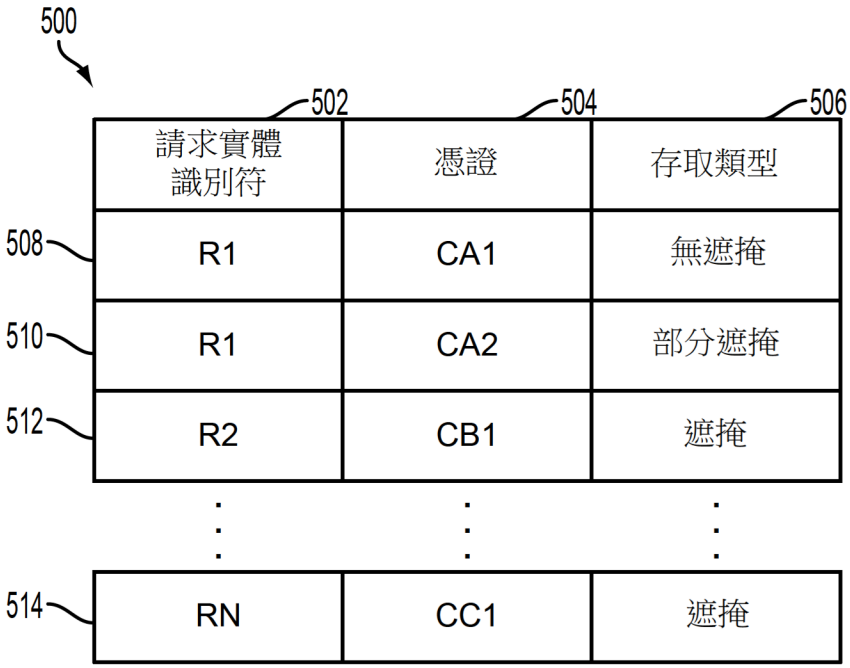
【圖2】


10
軟體
硬體
306
超管理器
308
TrustZone
310
應用程式
312
作業系統
隨機存取記憶體
頁表
16
轉譯後
援緩衝器
314
中央
處理單元
14
資料保護系統
304
資源內容密碼
編譯裝置
虛擬化介面
監視器
302
300

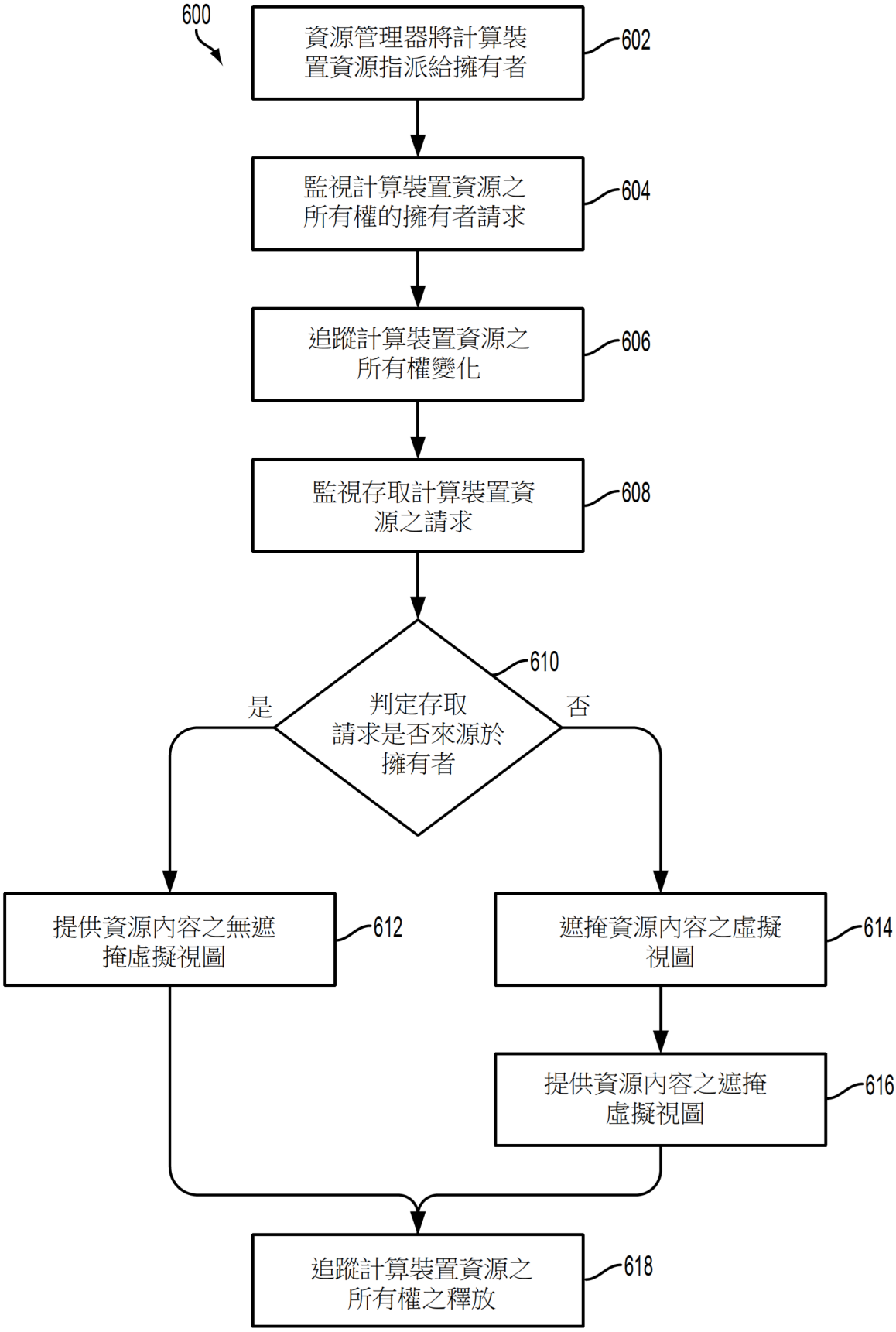
【圖3】


400
402
404
406
擁有者識別符
虛擬位址
有效性
408
O1
VA1
1
410
O1
VA2
1
412
O2
VB1
0
414
ON
VC1
1

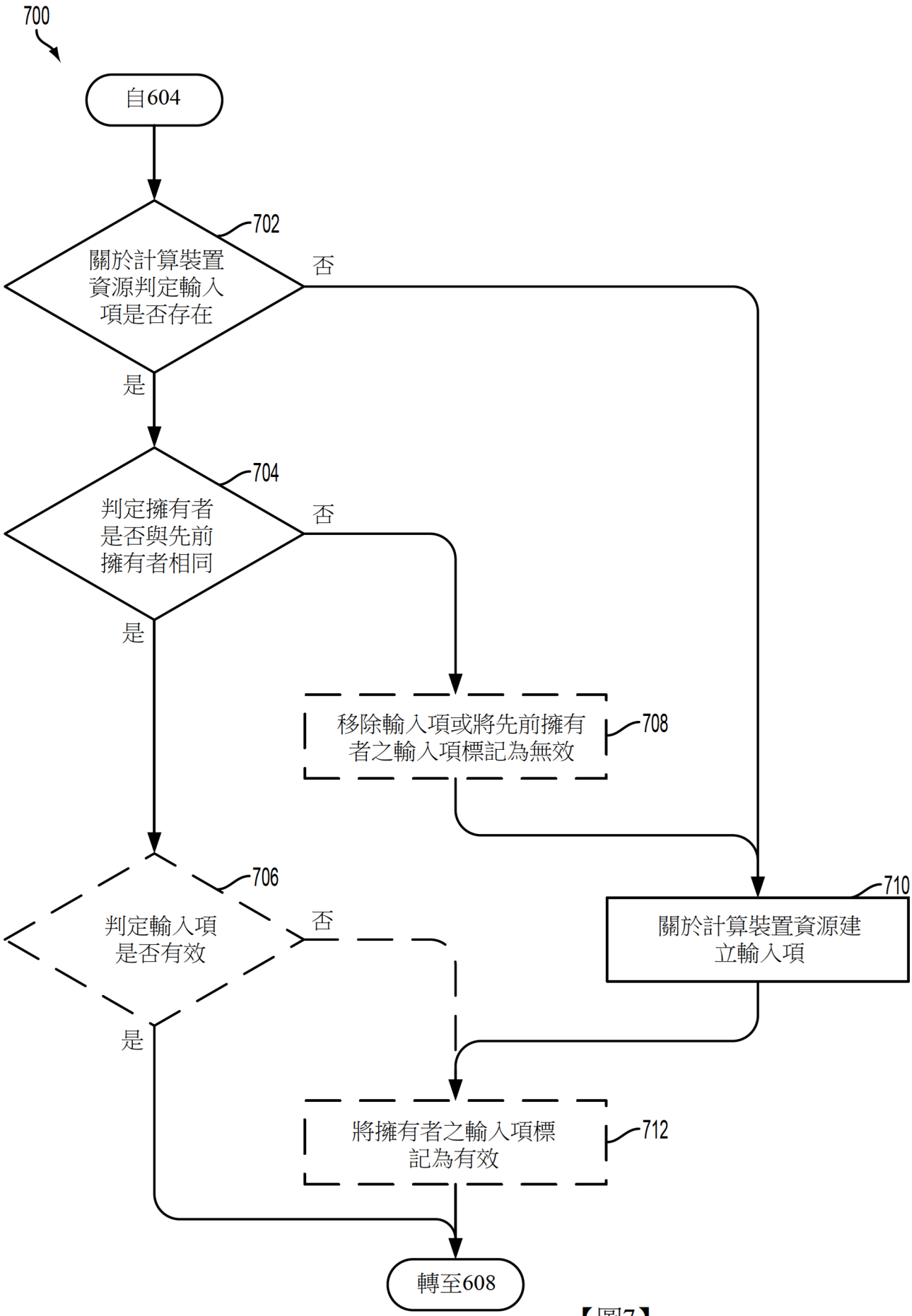
【圖4】


500
502
504
506
請求實體識別符
憑證
存取類型
508
R1
CA1
無遮掩
510
R1
CA2
部分遮掩
512
R2
CB1
遮掩
514
RN
CC1
遮掩

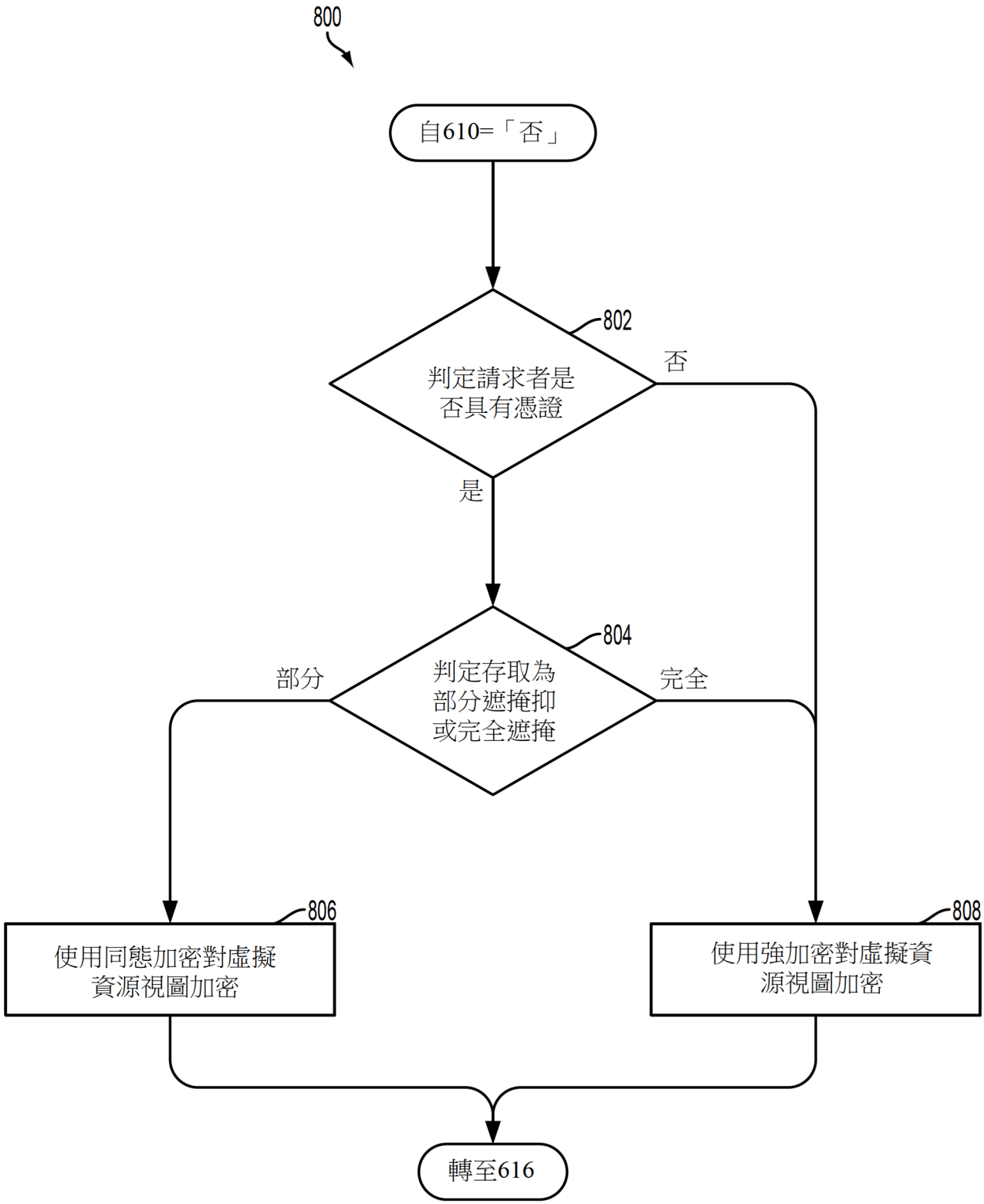
【圖5】


600
資源管理器將計算裝置資源指派給擁有者
602
監視計算裝置資源之所有權的擁有者請求
604
追蹤計算裝置資源之所有權變化
606
監視存取計算裝置資源之請求
608
判定存取請求是否來源於擁有者
610
是
否
提供資源內容之無遮掩虛擬視圖
612
遮掩資源內容之虛擬視圖
614
提供資源內容之遮掩虛擬視圖
616
追蹤計算裝置資源之所有權之釋放
618

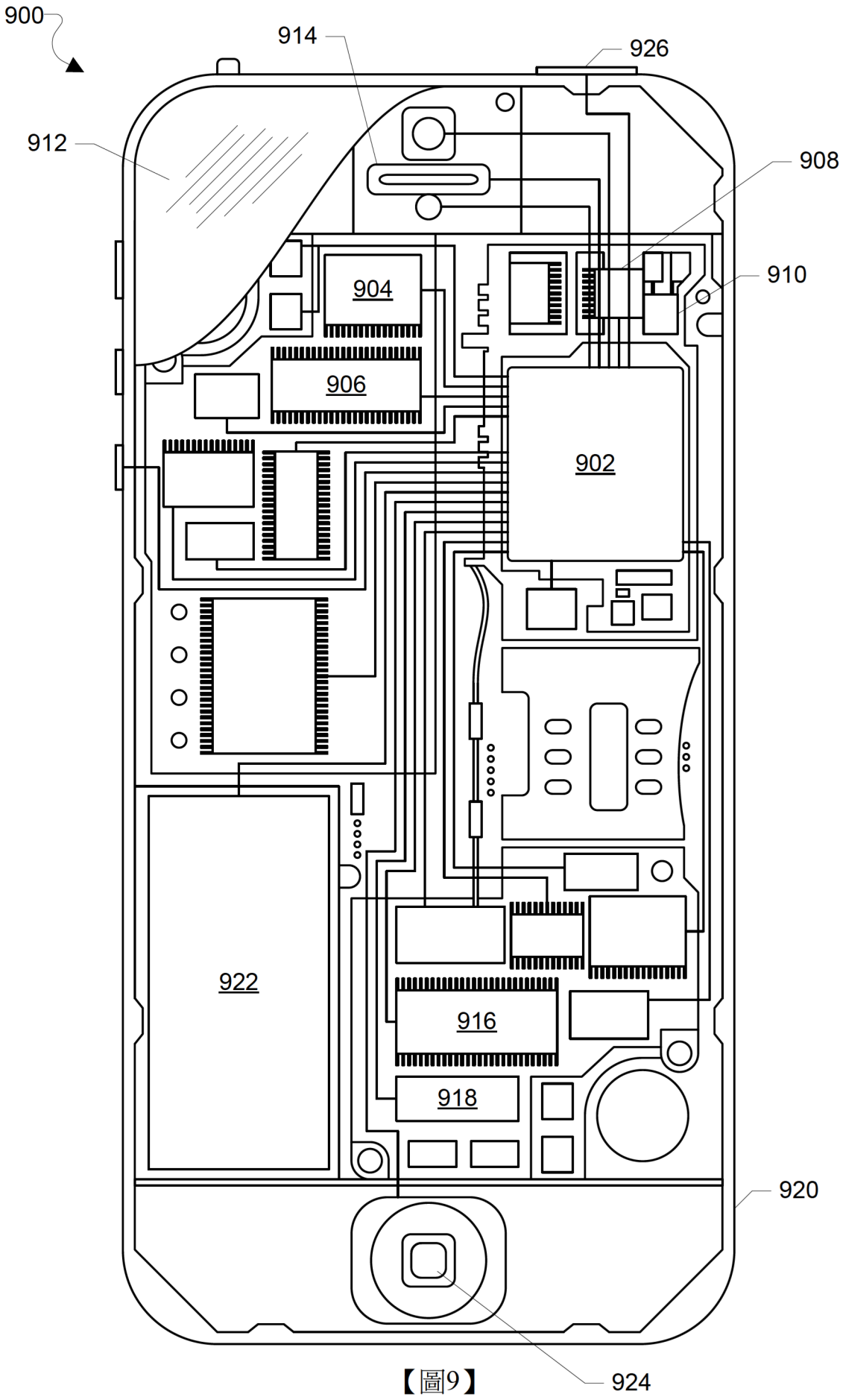
【圖6】


700
自604
702
關於計算裝置資源判定輸入項是否存在
否
是
704
判定擁有者是否與先前擁有者相同
否
是
移除輸入項或將先前擁有者之輸入項標記為無效
708
706
判定輸入項是否有效
否
是
710
關於計算裝置資源建立輸入項
將擁有者之輸入項標記為有效
712
轉至608

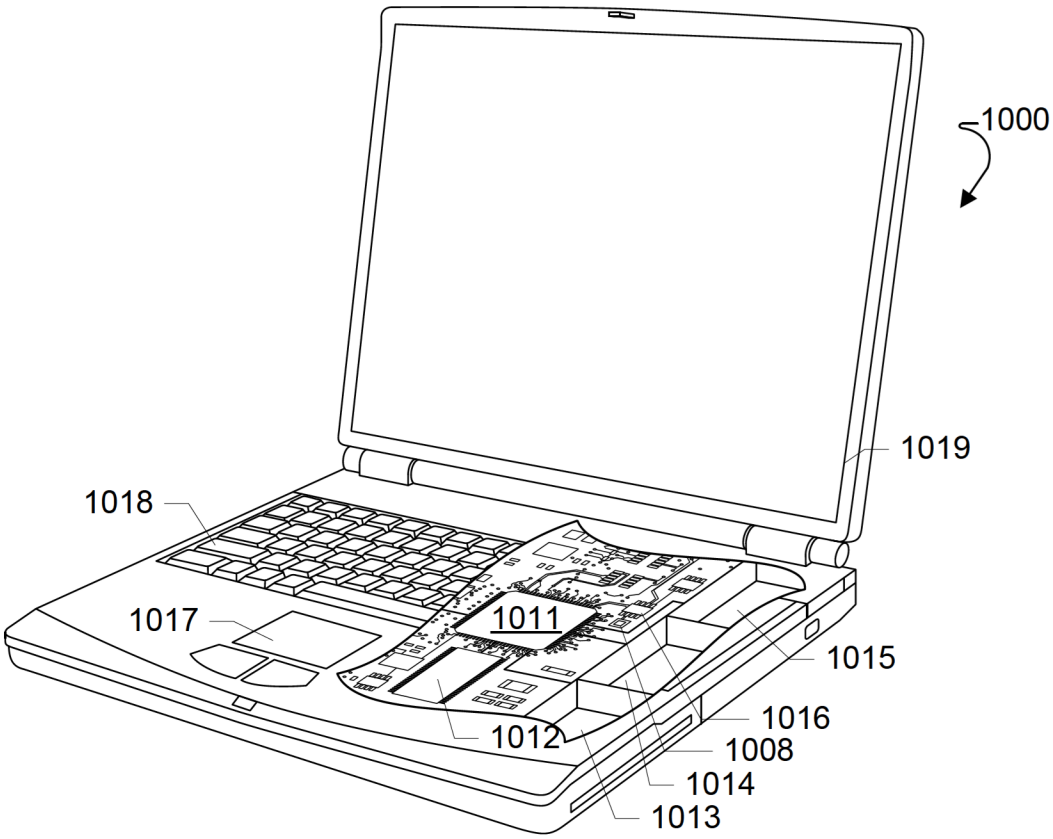
【圖7】


800
自610=「否」
802
判定請求者是否具有憑證
否
是
804
判定存取為部分遮掩抑或完全遮掩
部分
完全
806
使用同態加密對虛擬資源視圖加密
808
使用強加密對虛擬資源視圖加密
轉至616

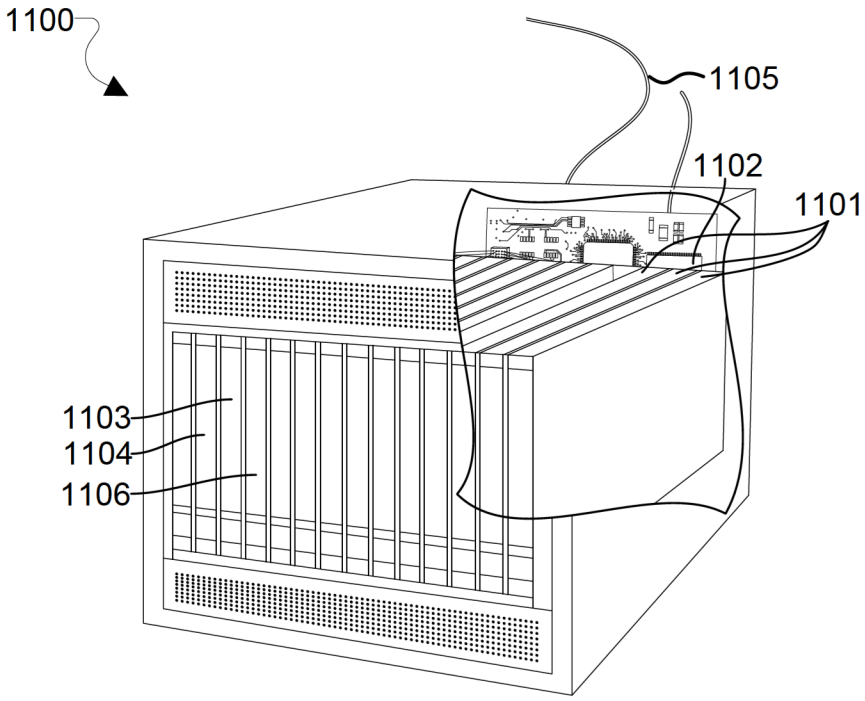
【圖8】



【圖9】


1000
1019
1018
1017
1011
1015
1016
1012
1008
1014
1013

【圖10】


1100
1105
1102
1101
1103
1104
1106

【圖11】