201937393

(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 201937393 A

(43)公開日： 中華民國 108 (2019) 年 09 月 16 日

(21)申請案號：108104320 (22)申請日： 中華民國 108 (2019) 年 02 月 01 日

(51)Int. Cl.： *G06F21/50 (2013.01)* *G06F21/56 (2013.01)*

(30)優先權：2018/02/02 美國 62/625,822

2018/02/26 美國 62/635,289

(71)申請人：美商多佛微系統公司 (美國) DOVER MICROSYSTEMS, INC. (US)

美國

美商查爾斯史塔克德拉普爾實驗室公司 (美國) THE CHARLES STARK DRAPER LABORATORY, INC. (US)

美國

(72)發明人：柏林 伊利 BOLING, ELI (US)；米爾本 史蒂芬 MILBURN, STEVEN (US)；沙利文 格雷戈里 T SULLIVAN, GREGORY T. (US)；薩瑟蘭德 安德魯 SUTHERLAND, ANDREW (US)；卡辛席諾 克里斯托弗 詹姆士 CASINGHINO, CHRISTOPHER JAMES (US)

(74)代理人：閻啟泰；林景郁

申請實體審查：無 申請專利範圍項數：35 項 圖式數：11 共 82 頁

(54)名稱

用於安全初始化的策略編輯之系統和方法

(57)摘要

本發明提供一種包括至少一個處理器之系統，該至少一個處理器經程式化以將一策略轉譯成策略程式碼，其中：該策略以一策略語言來提供；該策略程式碼呈不同於該策略語言之一程式設計語言；且該策略包括將一實體名稱映射至待與一目標系統中之一實體相關聯之一或多個詮釋資料符號之一陳述式，將對該實體執行該策略。

A system including at least one processor programmed to translate a policy into policy code, wherein: the policy is provided in a policy language; the policy code is in a programming language that is different from the policy language; and the policy includes a statement that maps an entity name to one or more metadata symbols to be associated with an entity in a target system against which the policy is to be enforced.

指定代表圖：

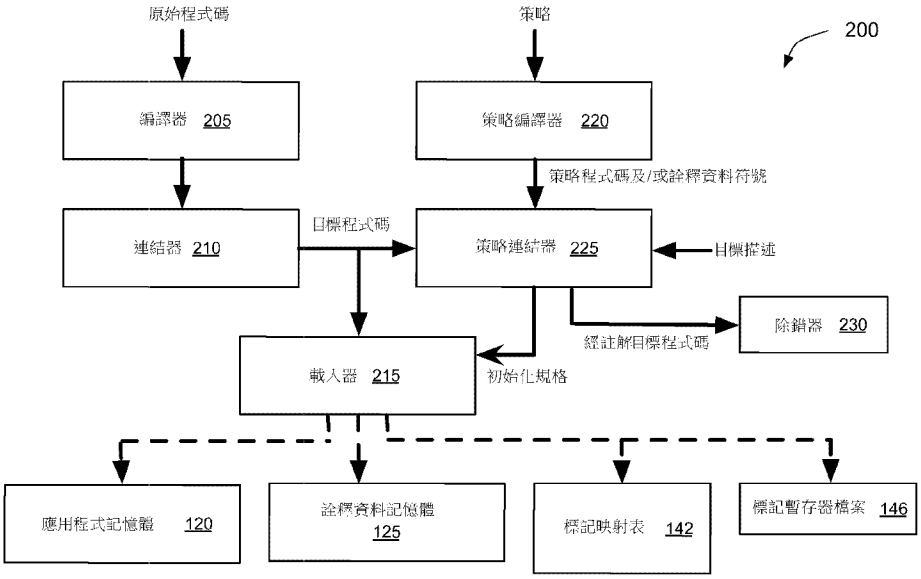


圖2

符號簡單說明：

120・・・應用程式記憶體

125・・・詮釋資料記憶體

142・・・標記映射表

146・・・標記暫存器檔案

200・・・軟體系統

205・・・編譯器

210・・・連結器

215・・・載入器

220・・・策略編譯器

225・・・策略連結器

230・・・除錯器

【發明說明書】

【中文發明名稱】　用於安全初始化的策略編輯之系統和方法

【英文發明名稱】　SYSTEMS AND METHODS FOR POLICY COMPILATION FOR SECURE INITIALIZATION

【技術領域】

【0001】　本申請案與用於安全初始化的策略編輯之系統和方法有關。

相關申請案

【0002】　本申請案依據35 U.S.C. § 119（e）主張2018年2月2日申請標題為「用於安全初始化之系統及方法（SYSTEMS AND METHODS FOR SECURE INITIALIZATION）」之具有代理人案號D0821.70000US00之美國臨時專利申請案第62/625,822號及2018年2月26日申請標題為「用於安全初始化之系統及方法（SYSTEMS AND METHODS FOR SECURE INITIALIZATION）」之具有代理人案號D0821.70000US01之美國臨時專利申請案第62/635,289號之權益，該等美國臨時專利申請案各自以全文引用之方式併入本文中。

【0003】　本申請案與以下申請案在同一天申請：

- 國際專利申請案第_____號，標題為「用於轉換用於詮釋資料處理之指令之系統及方法（SYSTEMS AND METHODS FOR TRANSFORMING INSTRUCTIONS FOR METADATA PROCESSING）」，具有代理人案號D0821.70001WO00，依據35 U.S.C. § 119（e）主張2018年2月2日申請標題為「用於指令集架構之間的轉譯的系統及方法（SYSTEMS AND METHODS FOR TRANSLATING BETWEEN INSTRUCTION SET ARCHITECTURES）」之具有代理人案號D0821.70001US00之美國臨時專利申請案第62/625,746號、2018年2

月26日申請標題為「用於轉換用於詮釋資料處理之指令之系統及方法（SYSTEMS AND METHODS FOR TRANSFORMING INSTRUCTIONS FOR METADATA PROCESSING）」之具有代理人案號D0821.70001US01之美國臨時專利申請案第62/635,319號，及2018年2月2日申請標題為「用於保護中斷服務常式條目之系統及方法（SYSTEMS AND METHODS FOR SECURING INTERRUPT SERVICE ROUTINE ENTRY）」之具有代理人案號D0821.70004US00之美國臨時專利申請案第62/625,802號之權益；及

- 國際專利申請案第_____號，標題為「用於快取後互鎖之系統及方法（SYSTEMS AND METHODS FOR POST CACHE INTERLOCKING）」，具有代理人案號D0821.70003WO00，依據35 U.S.C. § 119（e）主張2018年2月2日申請標題為「用於快取後互鎖之系統及方法（SYSTEMS AND METHODS FOR POST CACHE INTERLOCKING）」之具有代理人案號D0821.70003US00之美國臨時專利申請案第62/625,770號及2018年2月26日申請標題為「用於快取後互鎖之系統及方法（SYSTEMS AND METHODS FOR POST CACHE INTERLOCKING）」之具有代理人案號D0821.70003US01之臨時專利申請案第62/635,475號之權益。

【0004】 上文提及之申請案中之每一者以全文引用之方式併入本文中。

【先前技術】

【0005】 電腦安全性在社會各階層，自個人至企業至政府機構均已變為愈來愈迫切的問題。例如，在2015年，安全性研究人員識別出零日漏洞，其將允許攻擊者經由網際網路侵入Jeep Cherokee之機載電腦系統且控制車輛之儀錶盤功能、轉向、制動，及傳動。在2017年，WannaCry勒索軟體攻擊估計影響全球超過200,000台電腦，從而至少引起數億美元之經濟損失。值得注意地，該攻

擊嚴重破壞英國的若干國民健康服務醫院的操作。同一年，美國消費者信用報告機構艾可飛公司（Equifax）的資料外泄曝光人員資料，諸如全名、身分證號碼、出生日期、位址、駕駛執照號碼、信用卡號等。據報導該攻擊影響超過1億4千萬消費者。

【0006】 安全性專家一直與攻擊者進行追趕遊戲。一旦報告漏洞，安全性專家就爭相修補該漏洞。未能以及時方式修補漏洞（例如，歸因於對資源之較差管理及/或資源之缺乏）之個人及組織變為攻擊者之容易目標。

【0007】 一些安全性軟體監控電腦上及/或網路內之活動，且尋找可指示攻擊之形態。此方法無法防止惡意程式碼首先被執行。常常，在出現任何可疑形態時已經發生損壞。

【發明內容】

【0008】 根據至少一個態樣，提供一種系統。該系統包含至少一個處理器，該至少一個處理器經程式化以將策略轉譯成策略程式碼，其中該策略以策略語言來提供；該策略程式碼呈不同於該策略語言之程式設計語言；且該策略包含將實體名稱映射至待與目標系統中之實體相關聯之一或多個詮釋資料符號的陳述式，將對該實體執行該策略。

【0009】 在一些具體實例中，該至少一個處理器進一步經程式化以將該一或多個詮釋資料符號中之至少一個詮釋資料符號解析成二進位表示；該至少一個詮釋資料符號之該二進位表示包括於該策略程式碼中。

【0010】 在一些具體實例中，該至少一個處理器進一步經程式化以自描述該目標系統之目標描述來識別用以描述該目標系統之該實體之實體描述；且使用該實體描述以使該一或多個詮釋資料符號與該目標系統之該實體相關聯。

【0011】 在一些具體實例中，該目標描述包含被組織成複數個模組之複

數個實體描述。

【0012】 在一些具體實例中，該複數個模組包含對應於該目標系統之指令集架構（ISA）之至少一個指令集架構模組；且該至少一個ISA模組包含與該目標系統之該指令集架構相關聯之複數個ISA實體的實體描述。

【0013】 在一些具體實例中，該複數個模組包含對應於該目標系統之硬體晶片設計之至少一個系統單晶片（SOC）模組；且該至少一個SOC模組包含與該目標系統之該硬體晶片設計相關聯之複數個SOC實體的實體描述。

【0014】 在一些具體實例中，該複數個模組包含對應於該目標系統之作業系統之至少一個作業系統（OS）模組；且該至少一個OS模組包含與該目標系統之該作業系統相關聯之複數個OS實體的實體描述。

【0015】 在一些具體實例中，該複數個模組包含對應於該目標系統之至少一個使用者應用程式之至少一個使用者應用程式模組；且該至少一個使用者應用程式模組包含與該目標系統之該至少一個使用者應用程式相關聯之複數個使用者應用程式實體的實體描述。

【0016】 在一些具體實例中，該複數個模組包含至少一個類別模組；該至少一個類別模組包含至少一個類別實體之實體描述；且該至少一個類別實體對應於該目標系統中滿足一類別之一或多個界定準則的該類別的硬體及/或軟體實體。

【0017】 在一些具體實例中，該至少一個類別實體對應於該目標系統中與執行所選策略相關之類別的硬體及/或軟體實體。

【0018】 在一些具體實例中，該至少一個處理器進一步經程式化以將該類別實體闡述（elaborate）成複數個構成實體。

【0019】 在一些具體實例中，該複數個模組包含至少一個轉換模組；該至少一個轉換模組包含至少一個轉換實體之實體描述；且該至少一個轉換實體

對應於被應用至軟體程式碼之轉換以促進一或多個策略之執行。

【0020】 在一些具體實例中，該實體名稱具有根據階層式名稱空間之結構；且該至少一個處理器經程式化以使用該結構將該實體名稱映射至該一或多個詮釋資料符號。

【0021】 根據至少一個態樣，提供一種系統。該系統包含至少一個處理器，該至少一個處理器經程式化以將第一詮釋資料標籤及第二詮釋資料標籤兩者解析成詮釋資料之同一二進位表示，該第二詮釋資料標籤在語法上不同於該第一詮釋資料標籤但在語義上等效於該第一詮釋資料標籤。

【0022】 在一些具體實例中，該第一詮釋資料標籤及該第二詮釋資料標籤係基於同一組的一或多個詮釋資料符號。

【0023】 在一些具體實例中，該至少一個處理器進一步經程式化以執行指令而由此獲得執行結果；及將該執行結果儲存至記憶體位置；該系統進一步包含策略執行硬體，其經組態以；回應於接收到該指令藉由該至少一個處理器所執行之指示，評估一或多個規則以判定是否允許該指令，其中對該一或多個規則之評估回傳詮釋資料之該二進位表示；回應於判定允許該指令，判定由該一或多個規則所回傳的詮釋資料之該二進位表示之例項是否已經儲存；回應於判定詮釋資料之該二進位表示之例項未經儲存：將詮釋資料之該二進位表示儲存至硬體位置；且至少部分地藉由儲存自該記憶體位置至儲存有詮釋資料之該二進位表示之該硬體位置的映射而使詮釋資料之該二進位表示與該記憶體位置相關聯；及回應於判定詮釋資料之該二進位表示之例項已經儲存：至少部分地藉由儲存自該記憶體位置至已經儲存有詮釋資料之該二進位表示之硬體位置的映射而使詮釋資料之該二進位表示與該記憶體位置相關聯。

【0024】 在一些具體實例中，該記憶體位置包含應用程式記憶體中之位置；且儲存有詮釋資料之該二進位表示之該硬體位置包含與該應用程式記憶體

實體上分離之詮釋資料記憶體中之位置。

【0025】 在一些具體實例中，儲存有詮釋資料之該二進位表示之該硬體位置包含策略處理器之暫存器。

【0026】 在一些具體實例中，儲存有詮釋資料之該二進位表示之該硬體位置包含指令集架構（ISA）組態暫存器。

【0027】 在一些具體實例中，儲存有詮釋資料之該二進位表示之該硬體位置包含系統單晶片（SOC）組態暫存器。

【0028】 在一些具體實例中，該至少一個處理器經程式化以至少部分地藉由以下操作來判定該至少一個二進位表示之例項是否已經儲存：自該至少一個二進位表示以產生雜湊值；且使用該雜湊值來檢查雜湊表是否包括對應於該至少一個二進位表示之條目。

【0029】 在一些具體實例中，該至少一個處理器進一步經程式化以載入用於執行策略之一段策略程式碼；且該至少一個詮釋資料標籤係基於該策略程式碼中所指示之至少一個詮釋資料符號。

【0030】 在一些具體實例中，該至少一個處理器包含第一處理器及第二處理器；該第一處理器經組態以運行一段目標程式碼；且該第二處理器經組態以運行該段策略程式碼。

【0031】 根據至少一個態樣，提供一種系統。該系統包含至少一個處理器，該至少一個處理器經程式化以自應用程式記憶體載入第一值，其中該第一值與至少一個第一基元詮釋資料標籤相關聯；自該應用程式記憶體載入第二值，其中該第二值與至少一個第二基元詮釋資料標籤相關聯；以及至少部分地藉由對該第一值及該第二值執行操作而將該至少一個第一基元詮釋資料標籤及該至少一個第二基元詮釋資料標籤組合成複合詮釋資料標籤。

【0032】 在一些具體實例中，該至少一個處理器進一步經程式化以將該

應用程式記憶體之區域分配用於創建複合詮釋資料標籤；及自該應用程式記憶體之該區域載入該第一值與該第二值。

【0033】 在一些具體實例中，該第一值與該第二值相同。

【0034】 在一些具體實例中，該系統進一步包含策略執行硬體，其中對該第一值及該第二值執行之該操作致使該策略執行硬體評估一或多個規則；且對該一或多個規則之評估致使該策略執行硬體將該至少一個第一基元詮釋資料標籤及該至少一個第二基元詮釋資料標籤組合成該複合詮釋資料標籤。

【0035】 在一些具體實例中，載入該第一值致使該策略執行硬體自與第一應用程式記憶體位置相關聯之第一詮釋資料記憶體位置來讀取該第一基元詮釋資料標籤，該第一值係自該第一應用程式記憶體位置所載入；且載入該第二值致使該策略執行硬體自與第二應用程式記憶體位置相關聯之第二詮釋資料記憶體位置來讀取該第二基元詮釋資料標籤，該第二值係自該第二應用程式記憶體位置所載入。

【0036】 在一些具體實例中，對該第一值及該第二值執行之該操作產生第三值；且該第三值與該複合詮釋資料標籤相關聯。

【0037】 在一些具體實例中，該操作為始終產生預設值以作為該第三值之虛設操作。

【0038】 在一些具體實例中，對該第一值及該第二值執行之該操作包含第一操作；該至少一個處理器進一步經程式化以自該應用程式記憶體載入第四值；及至少部分地藉由對該第三值及該第四值執行第二操作而用該複合詮釋資料標籤來標記該第四值。

【0039】 在一些具體實例中，將該第三值儲存於第一輸入暫存器中；將該第四值儲存於第二輸入暫存器中；且對該第三值及該第四值執行之該第二操作致使該第四值被儲存於輸出暫存器中，且致使該輸出暫存器與該複合詮釋資

料標籤相關聯。

【0040】 在一些具體實例中，該至少一個處理器進一步經程式化以至少部分地藉由將該第四值自該輸出暫存器儲存至該應用程式記憶體中之位址，而使該應用程式記憶體中之該位址與該複合詮釋資料標籤相關聯。

【0041】 根據至少一個態樣，提供一種方法，其由先前態樣及具體實例中之任一者之系統來執行。

【0042】 根據至少一個態樣，提供至少一種電腦可讀取媒體，其上編碼有指令，該等指令在由至少一個處理器執行時致使該至少一個處理器執行如上文所定義之態樣及具體實例之方法。

【圖式簡單說明】

【0043】

圖1展示根據一些具體實例之用於執行策略之例示硬體系統100。

圖2展示根據一些具體實例之用於執行策略之例示軟體系統200。

圖3展示根據一些具體實例之用於確保載入器程式之安全之例示策略300。

圖4展示根據一些具體實例之由策略編譯器所輸出之例示策略程式碼400。

圖5示意性地展示根據一些具體實例之例示目標描述500。

圖6展示根據一些具體實例之已經藉由詮釋資料標籤所註解之例示組合程式碼600。

圖7展示根據一些具體實例之用於將可執行程式碼載入電腦系統中之例示程序700。

圖8展示根據一些具體實例之例示分隔策略800。

圖9展示根據一些具體實例之可藉由策略編譯器根據圖8之實例中之規則1所產生的例示策略程式碼900。

圖10展示根據一些具體實例之在通信規則情況下之例示策略程式碼1000。

圖11示意性地展示上面可實施本發明之任何態樣之例示電腦1100。

【實施方式】

【0044】 攻擊者所利用之許多漏洞追溯到資料及可執行指令混植（intermingle）於同一記憶體中之電腦架構設計。此混植允許攻擊者藉由將惡意程式碼偽裝為資料而將惡意程式碼注入至遠端電腦中。例如，程式可將緩衝區分配於電腦之記憶體中以儲存經由網路接收之資料。若該程式接收比該緩衝區可保存之資料更多的資料，但在將所接收的資料寫入至緩衝區中之前並未檢查該資料之大小，則所接收的資料之部分將超出緩衝區邊界寫入至鄰近記憶體中。攻擊者可利用此行為將惡意程式碼注入至鄰近記憶體中。若鄰近記憶體分配用於可執行程式碼，則惡意程式碼最終可由電腦執行。

【0045】 已經提出使得電腦硬體更具安全性意識之技術。例如，記憶體位置可與用於執行安全性策略之詮釋資料相關聯，且可檢查指令以符合安全性策略。例如，在給定待執行之指令之情況下，可檢查與指令相關聯之詮釋資料及/或與指令之一或多個運算元相關聯之詮釋資料以判定是否應接受指令。另外或替代地，適合的詮釋資料可與指令之輸出相關聯。

【0046】 圖1展示根據一些具體實例之用於執行策略之例示硬體系統100。在此實例中，硬體系統100包括主機處理器110，其可具有任何合適的指令集架構（instruction set architecture，ISA），諸如精簡指令集計算（reduced instruction set computing，RISC）架構或複雜指令集計算（complex instruction set computing，CISC）架構。主機處理器110可經由寫入互鎖112執行記憶體存取。寫入互鎖112可連接至系統匯流排115，其經組態以在諸如寫入互鎖112、應用程式記憶體120、詮釋資料記憶體125、唯讀記憶體（ROM）130、一或多個

周邊裝置135等各種組件之間傳送資料。

【0047】 在一些具體實例中，由主機處理器110操控（例如，修改、消耗及/或產生）之資料可儲存於應用程式記憶體120中。此類資料在本文中被稱作「應用程式資料」，區別於用於執行策略之詮釋資料。後者可儲存於詮釋資料記憶體125中。應瞭解，應用程式資料可包括由作業系統（OS）操控之資料、OS之指令、由一或多個使用者應用程式操控之資料，及/或該一或多個使用者應用程式之指令。

【0048】 在一些具體實例中，應用程式記憶體120及詮釋資料記憶體125可實體上分離，且主機處理器110可能無法存取詮釋資料記憶體125。以此方式，即使攻擊者成功將惡意程式碼注入至應用程式記憶體120中且致使主機處理器110執行惡意程式碼，詮釋資料記憶體125亦可能不受影響。然而，應瞭解，本發明之態樣不限於將應用程式資料及詮釋資料儲存於實體上分離之記憶體上。另外或替代地，詮釋資料可與應用程式資料儲存於同一記憶體中，且可使用實施有適合的保護方案的記憶體管理組件以防止執行於主機處理器110上之指令修改詮釋資料。另外或替代地，詮釋資料可與應用程式資料混植於同一記憶體中，且一或多個策略可用於保護詮釋資料。

【0049】 在一些具體實例中，可提供標記處理硬體140以確保藉由主機處理器110執行之指令符合一或多個策略。標記處理硬體140可包括任何合適的電路組件或電路組件之組合。例如，標記處理硬體140可包括將應用程式記憶體120中之位址映射至詮釋資料記憶體125中之位址之標記映射表142。例如，標記映射表142可將應用程式記憶體120中之位址X映射至詮釋資料記憶體125中之位址Y。此位址Y在本文中被稱作「詮釋資料標記」或僅被稱作「標記」。儲存於位址Y處之值在本文中亦被稱作「詮釋資料標記」或僅被稱作「標記」。

【0050】 在一些具體實例中，儲存於位址Y處之值又可為位址Z。此類間

接定址可重複任一合適次數，且最終可在詮釋資料記憶體125中產生用於儲存詮釋資料之資料結構。此類詮釋資料以及任何中間位址（例如，位址Z）在本文中亦被稱作「詮釋資料標記」或僅被稱作「標記」。

【0051】 應瞭解，本發明之態樣不限於將位址儲存於詮釋資料記憶體中之標記映射表。在一些具體實例中，標記映射表條目本身可儲存詮釋資料，使得標記處理硬體140能夠存取詮釋資料而無需執行記憶體操作。在一些具體實例中，標記映射表條目可儲存所選位元型樣，其中位元型樣之第一部分可對詮釋資料進行編碼，且位元型樣之第二部分可對詮釋資料記憶體中可儲存有其他詮釋資料之位址進行編碼。此可提供在速度與表達性之間的所需平衡。例如，標記處理硬體140能夠僅使用儲存於標記映射表條目本身中之詮釋資料來迅速檢查某些策略。對於較複雜規則情況下之其他策略，標記處理硬體140可存取儲存於詮釋資料記憶體125中之其他詮釋資料。

【0052】 再次參看圖1，藉由將應用程式記憶體位址映射至詮釋資料記憶體位址，標記映射表142可在應用程式資料與描述應用程式資料之詮釋資料之間創建相關性。在一個實例中，儲存於詮釋資料記憶體位址Y處且因此與儲存於應用程式記憶體位址X處之應用程式資料相關聯之詮釋資料可指示應用程式資料可為可讀取、可寫入及/或可執行的。在另一實例中，儲存於詮釋資料記憶體位址Y處且因此與儲存於應用程式記憶體位址X處之應用程式資料相關聯之詮釋資料可指示應用程式資料之類型（例如，整數、指標、16位元字組、32位元字組等）。取決於待執行策略，相關於該策略之任何合適詮釋資料可與一段應用程式資料相關聯。

【0053】 在一些具體實例中，詮釋資料記憶體位址Z可儲存於詮釋資料記憶體位址Y處。與儲存於應用程式記憶體位址X處之應用程式資料相關聯之詮釋資料可儲存於詮釋資料記憶體位址Z處，而不是詮釋資料記憶體位址Y處

（或外加詮釋資料記憶體之位址Y處）。例如，詮釋資料符號「RED」之二進位表示可儲存於詮釋資料記憶體位址Z處。藉由將詮釋資料記憶體位址Z儲存於詮釋資料記憶體位址Y中，儲存於應用程式記憶體位址X處之應用程式資料可標記為「RED」。

【0054】 以此方式，詮釋資料符號「RED」之二進位表示可僅儲存於詮釋資料記憶體125中一次。例如，若儲存於另一應用程式記憶體位址X'處之應用程式資料亦將被標記為「RED」，則標記映射表142可將應用程式記憶體位址X'映射至亦儲存有詮釋資料記憶體位址Z之詮釋資料記憶體位址Y'。

【0055】 此外，以此方式，可簡化標記更新。例如，若儲存於應用程式記憶體位址X處之應用程式資料在後續時間將被標記為「BLUE」，則詮釋資料記憶體位址Z'可寫入於詮釋資料記憶體位址Y處以替換詮釋資料記憶體位址Z，且詮釋資料符號「BLUE」之二進位表示可儲存於詮釋資料記憶體位址Z'處。

【0056】 因此，本發明人已認識且瞭解到，具有任何合適長度N之一系列詮釋資料記憶體位址可用於標記，包括N = 0 （例如，其中詮釋資料符號之二進位表示儲存於詮釋資料記憶體位址Y本身處）。

【0057】 在應用程式資料與詮釋資料之間的相關性（在本文中亦被稱作「標記」）可在任何合適的粒度級別及/或以可變粒度來進行。例如，可逐字組地進行標記。另外或替代地，記憶體中之一區域可映射至單一標記，使得該區域中之所有字組均與相同詮釋資料相關聯。此可有利地減小標記映射表142及/或詮釋資料記憶體125之大小。例如，相較於維持分別對應於位址範圍中之不同位址之多個標記，可針對整個位址範圍維持單一標記。

【0058】 在一些具體實例中，標記處理硬體140可經組態以將一或多個安全性規則應用至與指令相關聯之詮釋資料及/或與指令之一或多個運算元相關聯之詮釋資料，以判定是否應接受指令。例如，主機處理器110可提取及執行指

令，且可將執行指令之結果佇列至寫入互鎖112中。在將該結果寫回至應用程式記憶體120中之前，主機處理器110可將指令類型（例如，作業碼）、儲存有指令之位址、指令所提及之一或多個記憶體位址，及/或一或多個暫存器識別符發送至標記處理硬體140。此暫存器識別符可識別在執行指令時由主機處理器110所使用之暫存器，諸如用於儲存指令之運算元或結果之暫存器。

【0059】 在一些具體實例中，除了寫入指令或替代寫入指令，還可對破壞性讀取指令進行佇列。例如，嘗試存取破壞性讀取指令之目標位址之後續指令可佇列於非快取記憶體區域中。若判定應允許破壞性讀取指令且當判定應允許破壞性讀取指令時，則佇列指令可經載入以供執行。

【0060】 在一些具體實例中，可允許繼續進行破壞性讀取指令，且自目標位址讀取之資料可俘獲於緩衝區中。若判定應允許破壞性讀取指令且當判定應允許破壞性讀取指令時，則緩衝區中俘獲之該資料可捨棄。若判定不應允許破壞性讀取指令且當判定不應允許破壞性讀取指令時，則緩衝區中俘獲之該資料可恢復至該目標位址。另外或替代地，可藉由經緩衝資料為後續讀取服務。

【0061】 應瞭解，本發明之態樣不限於對已經藉由主機處理器所執行之指令（諸如已經被主機處理器之執行管線所引退之指令）來執行詮釋資料處理。在一些具體實例中，可在主機處理器之執行管線之前、期間及/或之後對指令執行詮釋資料處理。

【0062】 在一些具體實例中，在給定接收自主機處理器110之位址（例如，儲存有指令之位址或指令所提及之位址）之情況下，標記處理硬體140可使用標記映射表142來識別對應標記。另外或替代地，對於接收自主機處理器110之暫存器識別符，標記處理硬體140可自標記處理硬體140內之標記暫存器檔案146存取標記。

【0063】 在一些具體實例中，若應用程式記憶體位址並不具有標記映射

表142中之對應標記，則標記處理硬體140可將查詢發送至策略處理器150。該查詢可包括有疑慮之應用程式記憶體位址，且策略處理器150可回傳用於該應用程式記憶體位址之標記。另外或替代地，策略處理器150可針對包括該應用程式記憶體位址之位址範圍創建新標記映射條目。以此方式，可在與有疑慮之應用程式記憶體位址相關聯之標記映射表142中提供適合標記以供未來參考。

【0064】 在一些具體實例中，標記處理硬體140可將查詢發送至策略處理器150以檢查是否應允許藉由主機處理器110所執行之指令。該查詢可包括一或多個輸入，諸如指令之指令類型（例如，作業碼）、用於程式計數器之標記、用於提取指令之應用程式記憶體位址之標記（例如，程式計數器所針對之記憶體中之字組）、用於儲存有指令之運算元之暫存器之標記，及/或用於指令所提及之應用程式記憶體位址之標記。在一個實例中，該指令可為載入指令，且指令之運算元可為應用程式記憶體位址，應用程式資料將自該應用程式記憶體位址載入。該查詢尤其可包括用於儲存有應用程式記憶體位址之暫存器之標記以及用於應用程式記憶體位址本身之標記。在另一實例中，該指令可為算術指令，且可存在兩個運算元。該查詢尤其可包括用於儲存有第一運算元之第一暫存器之第一標記及用於儲存有第二運算元之第二暫存器之第二標記。

【0065】 亦應瞭解，本發明之態樣不限於每次對單一指令執行詮釋資料處理。在一些具體實例中，主機處理器之ISA中之多個指令可例如經由至策略處理器150之單一查詢作為指令束而共同被檢查。此查詢可包括更多輸入以允許策略處理器150檢查指令束中之所有指令。類似地，可經由至策略處理器150之單一查詢來檢查語義上可對應於多個操作之CISC指令，其中該查詢可包括足夠的輸入以允許策略處理器150檢查CISC指令內之所有構成操作。

【0066】 在一些具體實例中，策略處理器150可包括可組態處理單元，諸如微處理器、場可程式化閘陣列（FPGA），及/或任何其他合適的電路系統。

策略處理器150中可能已載入用以描述主機處理器110之允許操作之一或多個策略。回應於來自標記處理硬體140之查詢，策略處理器150可評估策略中之一或多者以判定是否應允許有疑慮之指令。例如，標記處理硬體140可將中斷信號以及關於有疑慮之指令（例如，如上文所描述）之一或多個輸入發送至策略處理器150。策略處理器150可將查詢之該等輸入儲存於工作記憶體中（例如，一或多個佇列中）以供立即或延遲處理。例如，策略處理器150可以某一合適的方式（例如，基於與每一查詢相關聯之優先權旗標）來優先化查詢之處理。

【0067】 在一些具體實例中，策略處理器150可評估一或多個輸入（例如，一或多個輸入標記）上之一或多個策略以判定是否應允許有疑慮之指令。若該指令未經允許，則策略處理器150可因此通知標記處理硬體140。若該指令經允許，則策略處理器150可計算一或多個輸出（例如，一或多個輸出標記）以回傳至標記處理硬體140。作為一個實例，該指令可為儲存指令，且策略處理器150可計算用於儲存有應用程式資料之應用程式記憶體位址之輸出標記。作為另一實例，該指令可為算術指令，且策略處理器150可計算用於暫存器之輸出標記，暫存器用於儲存執行該算術指令之結果。

【0068】 在一些具體實例中，策略處理器150可經程式化以執行外加關於評估策略之任務或替代關於評估策略之任務的一或多個任務。例如，策略處理器150可執行關於標記初始化、啟動載入、應用程式載入、對於詮釋資料記憶體125之記憶體管理（例如，廢料收集）、登入、除錯支援，及/或中斷處理之任務。此等任務中之一或多者可在背景下執行（例如，在為來自標記處理硬體140之查詢服務之間執行）。

【0069】 在一些具體實例中，標記處理硬體140可包括用於將一或多個輸入標記映射至決策及/或一或多個輸出標記之規則快取記憶體144。例如，至規則快取記憶體144中之查詢可類似地建構為至策略處理器150之查詢以檢查是否

應允許由主機處理器110所執行之指令。若存在快取命中，則規則快取記憶體144可輸出關於是否應允許指令之決策，及/或一或多個輸出標記（例如，如上文結合策略處理器150所描述）。可使用來自策略處理器150之查詢回應而在規則快取記憶體144中創建此映射。然而，如在一些具體實例中，一或多個映射可提前安置於規則快取記憶體144中，但此提前不是必要的。

【0070】 在一些具體實例中，規則快取記憶體144可用於提供效能增強。例如，在藉由一或多個輸入標記來查詢策略處理器150之前，標記處理硬體140可首先藉由該一或多個輸入標記來查詢規則快取記憶體144。在快取命中狀況下，標記處理硬體140可藉由來自規則快取記憶體144之決策及/或一或多個輸出標記繼續進行查詢，而無需查詢策略處理器150。此可提供顯著加速。在快取未命中狀況下，標記處理硬體140可查詢策略處理器150且將來自策略處理器150之回應安置於規則快取記憶體144中以供未來可能使用。

【0071】 在一些具體實例中，若標記處理硬體140判定應允許有疑慮之指令（例如，基於規則快取記憶體144中之命中或規則快取記憶體144中之未命中，隨後以來自策略處理器150指示未發現策略違反之回應），則標記處理硬體140可向寫入互鎖112指示執行指令之結果可寫回至記憶體。另外或替代地，標記處理硬體140可藉由一或多個輸出標記更新詮釋資料記憶體125、標記映射表142，及/或標記暫存器檔案146（例如，如接收自規則快取記憶體144或策略處理器150）。作為一個實例，對於儲存指令，詮釋資料記憶體125可藉由標記映射表142以經由位址轉譯而進行更新。例如，儲存指令所提及之應用程式記憶體位址可用於自標記映射表142查找詮釋資料記憶體位址，且接收自規則快取記憶體144或策略處理器150之詮釋資料可以該詮釋資料記憶體位址而儲存至詮釋資料記憶體125。作為另一實例，當待更新詮釋資料儲存於標記映射表142中之條目中（相較於儲存於詮釋資料記憶體125中）時，可更新標記映射表142

中之該條目。作為另一實例，對於算術指令，對應於由主機處理器110所用於儲存執行該算術指令之結果之暫存器之標記暫存器檔案146中之條目可藉由適合的標記進行更新。

【0072】 在一些具體實例中，若標記處理硬體140判定有疑慮之指令表示策略違反（例如，基於規則快取記憶體144中之未命中，隨後以來自策略處理器150指示已經發現策略違反之回應），則標記處理硬體140可向寫入互鎖112指示執行該指令之結果應被捨棄而非寫回至記憶體。另外或替代地，標記處理硬體140可將中斷發送至主機處理器110。回應於接收到該中斷，主機處理器110可切換至任何合適的違反處理程式碼。例如，主機處理器110可停止、重設、記錄該違反且繼續進行、對應用程式碼及/或應用程式資料執行完整性檢查、通知操作員等。

【0073】 在一些具體實例中，標記處理硬體140可包括一或多個組態暫存器。此暫存器可經由標記處理硬體140之組態介面（例如，藉由策略處理器150）進行存取。在一些具體實例中，標記暫存器檔案146可實施為組態暫存器。另外或替代地，可存在一或多個應用程式組態暫存器及/或一或多個詮釋資料組態暫存器。

【0074】 儘管實施細節展示於圖1中及論述於上文中，但應瞭解，本發明之態樣不限於使用任何特定組件或組件之組合，或不限於組件之任何特定配置。例如，在一些具體實例中，策略處理器150之一或多個功能性可由主機處理器110執行。作為實例，主機處理器110可具有不同操作模式，諸如用於使用者應用程式之使用者模式及用於作業系統之特許模式。策略相關程式碼（例如，標記、評估策略等）可與作業系統在相同特許模式下運行，或在不同特許模式下（例如，在對特權升級提供甚至更好保護之情況下）運行。

【0075】 圖2展示根據一些具體實例之用於執行策略之例示軟體系統

200。例如，軟體系統200可經程式化以產生可執行程式碼及/或將可執行程式碼載入至圖1中所展示之例示硬體系統100中。

【0076】 在圖2中所展示之實例中，軟體系統200包括軟體工具鏈，其具有編譯器205、連結器210，及載入器215。編譯器205可經程式化以將原始程式碼處理成可執行程式碼，其中原始程式碼可呈高階語言且可執行程式碼可呈低階語言。連結器210可經程式化以將由編譯器205所產生之多個目標檔案組合成單一目標檔案以藉由載入器215載入至記憶體（例如，在圖1之實例中之例示應用程式記憶體120）中。儘管未展示，但藉由連結器210所輸出之目標檔案可轉化成合適的格式且儲存於持久性儲存裝置，諸如快閃記憶體、硬碟、唯讀記憶體（ROM）等中。載入器215可自持久性儲存裝置擷取目標檔案，且將目標檔案載入至隨機存取記憶體（RAM）中。

【0077】 在一些具體實例中，編譯器205可經程式化以產生資訊以用於執行策略。例如，當編譯器205將原始程式碼轉譯成可執行程式碼時，編譯器205可產生關於資料類型、程式語義及/或記憶體佈局之資訊。作為一個實例，編譯器205可經程式化以標示在函式之一或多個指令與實施呼叫習知操作（例如，使一或多個參數自呼叫程式函式傳遞至被呼叫程式函式、使一或多個值自被呼叫程式函式返回至呼叫程式函式、儲存返回位址以指示當被呼叫程式函式將控制返回至呼叫程式函式時在呼叫程式函式之程式碼中在何處恢復執行等）之一或多個指令之間的邊界。例如，此類邊界可在初始化期間用於將某些指令標記為函式序言或函式結語。在運行時，可執行堆疊策略，使得當函式序言指令執行時，呼叫堆疊中之某些位置（例如，儲存返回位址之處）可標記為「訊框」位置，且當函式結語指令執行時，可移除「訊框」標記。堆疊策略可指示實施函式本體（相較於函式序言及函式結語）之指令僅讀取存取「訊框」位置。此可防止攻擊者覆寫返回位址且藉此獲得控制。

【0078】 作為另一實例，編譯器205可經程式化以執行例如控制流程分析以識別一或多個控制傳送點及各別目的地。此類資訊可用於執行控制流程策略。作為又一實例，編譯器205可經程式化以例如藉由應用諸如指標、整數、浮點數等類型標籤而執行類型分析。此類資訊可用於執行防止誤用（例如，使用浮點數作為指標）之策略。

【0079】 儘管圖2中未展示，但在一些具體實例中，軟體系統200可包括二進位分析組件，其經程式化以將由連結器210所產生之目標程式碼（相較於原始程式碼）用作輸入，且執行類似於由編譯器205所執行之彼等分析之一或多個分析（例如，控制流程分析、類型分析等）。

【0080】 在圖2之實例中，軟體系統200進一步包括策略編譯器220及策略連結器225。策略編譯器220可經程式化以將以策略語言編寫之策略轉譯成策略程式碼。例如，策略編譯器220可以C或某一其他合適的程式設計語言來輸出策略程式碼。另外或替代地，策略編譯器220可輸出策略所提及之一或多個詮釋資料符號。在初始化時，此詮釋資料符號可與一或多個記憶體位置、暫存器，及/或目標系統之其他機器狀態相關聯，且可解析成詮釋資料之二進位表示以被載入至該目標系統之詮釋資料記憶體或某一其他硬體儲存裝置（例如，暫存器）中。如上文所論述，詮釋資料之此二進位表示或儲存有該二進位表示之位置之指標有時在本文中被稱作「標記」。

【0081】 應瞭解，本發明之態樣不限於在載入時解析詮釋資料符號。在一些具體實例中，可（例如，在編譯時或在連結時）靜態地解析一或多個詮釋資料符號。例如，策略編譯器220可處理一或多個適用策略，且將由該一或多個策略所界定之一或多個詮釋資料符號解析成靜態界定二進位表示。另外或替代地，策略連結器225可將一或多個詮釋資料符號解析成靜態界定二進位表示，或儲存靜態界定二進位表示之資料結構之指標。本申請案發明人已認識且

瞭解到，靜態地解析詮釋資料符號可有利地減少載入時處理。然而，本發明之態樣不限於以任何特定方式解析詮釋資料符號。

【0082】 在一些具體實例中，策略連結器225可經程式化以處理目標程式碼（例如，如藉由連結器210之輸出）、策略程式碼（例如，如藉由策略編譯器220之輸出）及/或目標描述，以輸出初始化規格。該初始化規格可由載入器215用於安全地初始化具有一或多個硬體組件（例如，圖1中展示之例示硬體系統100）及/或一或多個軟體組件（例如作業系統、一或多個使用者應用程式等）之目標系統。

【0083】 在一些具體實例中，該目標描述可包括對複數個命名實體之描述。命名實體可表示目標系統之組件。作為一個實例，命名實體可表示硬體組件，諸如組態暫存器、程式計數器、暫存器檔案、計時器、狀態旗標、記憶體傳送單元、輸入/輸出裝置等。作為另一實例，命名實體可表示軟體組件，諸如函式、模組、驅動器、服務常式等。

【0084】 在一些具體實例中，策略連結器225可經程式化以搜索該目標描述以識別與策略有關之一或多個實體。例如，該策略可將某些實體名稱映射至對應詮釋資料符號，且策略連結器225可搜索該目標描述以識別具有彼等實體名稱之實體。策略連結器225可自該目標描述識別彼等實體之描述，且使用該等描述以藉由適合的詮釋資料符號來註解藉由連結器210所輸出之目標程式碼。例如，策略連結器225可將讀取標籤應用至可執行與可連結格式（Executable and Linkable Format，ELF）檔案之.rodata區段，將讀取標籤及寫入標籤應用至ELF檔案之.data區段，且將執行標籤應用至ELF檔案之.text區段。此類資訊可用於執行用於記憶體存取控制及/或可執行程式碼保護（例如，藉由檢查讀取、寫入及/或執行特權）之策略。

【0085】 應瞭解，本發明之態樣不限於將目標描述提供至策略連結器

225。在一些具體實例中，除了策略連結器225或替代策略連結器225，還可將目標描述提供至策略編譯器220。策略編譯器220可檢查該目標描述之誤差。例如，若策略中所提及之實體並不存在於該目標描述中，則可藉由策略編譯器220標示誤差。另外或替代地，策略編譯器220還可搜索該目標描述以搜索與待執行之一或多個策略相關的實體，且可產生僅包括對於相關實體之實體描述之經過濾目標描述。例如，策略編譯器220可使待執行策略之「init」陳述式中之實體名稱與該目標描述中之實體描述匹配，且可自該目標描述移除不具有對應「init」陳述式之實體描述。

【0086】 在一些具體實例中，載入器215可基於由策略連結器225所產生之初始化規格而初始化目標系統。例如，參考圖1之實例，載入器215可將資料及/或指令載入至應用程式記憶體120中，且可使用初始化規格以識別與載入至應用程式記憶體120中之該資料及/或指令相關聯之詮釋資料標籤。載入器215可將初始化規格中之詮釋資料標籤解析成各別二進位表示。然而，應瞭解，本發明之態樣不限於在載入時解析詮釋資料標籤。在一些具體實例中，詮釋資料標籤之範圍在策略連結期間可已知，且因此可在此時例如藉由策略連結器225來解析詮釋資料標籤。此可有利地減少初始化規格之載入時處理。

【0087】 在一些具體實例中，策略連結器225及/或載入器215可維持詮釋資料之二進位表示返回至詮釋資料標籤之映射。可例如藉由除錯器230使用此映射。例如，在一些具體實例中，可提供除錯器230以顯示初始化規格之人類可讀取版本，其可列出一或多個實體且針對每一實體，列出與實體相關聯之一組一或多個詮釋資料標籤。另外或替代地，除錯器230可經程式化以顯示藉由詮釋資料標籤所註解之組合程式碼，諸如藉由分解藉由詮釋資料標籤所註解之目標程式碼而產生之組合程式碼。此類組合程式碼之實例展示於圖6中且論述於下文。在除錯期間，除錯器230可在執行期間停止程式，且允許以人類可讀

取形式檢測實體及/或與實體相關聯之詮釋資料標記。例如，除錯器230可允許檢測策略違反中所涉及之實體及/或造成該策略違反之詮釋資料標記。除錯器230可使用詮釋資料之二進位表示返回至詮釋資料標籤之映射而進行此操作。

【0088】 在一些具體實例中，習知除錯工具可經擴展以允許審查與策略執行相關之問題，例如上文所述。另外或替代地，可提供獨立策略除錯工具。

【0089】 在一些具體實例中，載入器215可將詮釋資料標籤之二進位表示載入至詮釋資料記憶體125中，且可將在應用程式記憶體位址與詮釋資料記憶體位址之間的映射記錄於標記映射表142中。例如，載入器215可在標記映射表142中創建條目，其將應用程式記憶體120中儲存有指令之應用程式記憶體位址映射至與詮釋資料記憶體125中儲存有與指令相關聯之詮釋資料之詮釋資料記憶體位址。另外或替代地，載入器215可將詮釋資料儲存於標記映射表142本身中（相較於詮釋資料記憶體125），以允許存取而無需執行任何記憶體操作。

【0090】 在一些具體實例中，除標記映射表142之外或替代標記映射表142，載入器215可初始化標記暫存器檔案146。例如，標記暫存器檔案146可包括分別對應於複數個實體之複數個暫存器。載入器215可自初始化規格識別與實體相關聯之詮釋資料，且將詮釋資料儲存於標記暫存器檔案146中之各別暫存器中。

【0091】 再次參考圖1之實例，在一些具體實例中，載入器215可將策略程式碼（例如，如藉由策略編譯器220所輸出）載入至詮釋資料記憶體125中以供策略處理器150執行。另外或替代地，可提供分開的記憶體（圖1中未展示）以供策略處理器150使用，且載入器215可將策略程式碼及/或相關聯資料載入至分開的記憶體中。

【0092】 在一些具體實例中，詮釋資料標籤可以是基於多個詮釋資料符號。例如，實體可進行多個策略，且可因此與分別對應於不同策略之不同詮釋

資料符號相關聯。本申請案發明人已認識且瞭解到，可能需要藉由載入器215將同一組詮釋資料符號解析為同一二進位表示（其有時在本文中被稱作「典型」表示）。例如，詮釋資料標籤{A，B，C}及詮釋資料標籤{B，A，C}可藉由載入器215解析為同一二進位表示。以此方式，語法上不同但語義上相等之詮釋資料標籤可具有相同二進位表示。

【0093】 本申請案發明人已進一步認識且瞭解到，可能需要確保詮釋資料之二進位表示在詮釋資料儲存裝置中並不重複。例如，如上文所論述，圖1之實例中之例示規則快取記憶體144可將輸入標記映射至輸出標記，且在一些具體實例中，輸入標記可以是儲存有詮釋資料之二進位表示之詮釋資料記憶體位址，相較於二進位表示本身。本申請案發明人已認識且瞭解到，若詮釋資料之同一二進位表示儲存於兩個不同詮釋資料記憶體位址X及Y處，則規則快取記憶體144可能無法「辨別」詮釋資料記憶體位址Y，即使規則快取記憶體144已經儲存對於詮釋資料記憶體位址X之映射。此可能導致大量不必要的規則快取未命中，這會降低系統效能。

【0094】 此外，本申請案發明人已認識且瞭解到，在詮釋資料之二進位表示與其儲存位置之間的一對一對應性可有助於詮釋資料比較。例如，相較於比較詮釋資料之二進位表示，兩段詮釋資料之間的等同性可僅藉由比較詮釋資料記憶體位址而判定。此可引起顯著效能改良，尤其當二進位表示較大（例如，許多詮釋資料符號封裝於單一詮釋資料標籤中）時。

【0095】 因此，在一些具體實例中，載入器215可在儲存詮釋資料之二進位表示（例如，儲存至詮釋資料記憶體125中）之前檢查是否已經儲存有詮釋資料之二進位表示。若已經儲存有詮釋資料之二進位表示，而非再次將其儲存在不同儲存位置處，則載入器215可指代現有儲存位置。可在啟動時及/或在啟動之後載入程式時進行此檢查（在具有或不具有動態連結之情況下）。

【0096】 另外或替代地，可在由於評估一或多個策略（例如，藉由例示策略處理器150）而創建詮釋資料之二進位表示時執行類似檢查。若已經儲存有詮釋資料之二進位表示，則可使用提及之現有儲存位置（例如，安置於例示規則快取記憶體144中）。

【0097】 在一些具體實例中，載入器215可創建將雜湊值映射至儲存位置之雜湊表。在儲存詮釋資料之二進位表示之前，載入器215可使用雜湊函數以將詮釋資料之二進位表示減小為雜湊值，且檢查雜湊表是否已經含有與雜湊值相關聯之條目。若雜湊表含有與雜湊值相關聯之條目，則載入器215可判定已經儲存有詮釋資料之二進位表示，且可自該條目擷取關於詮釋資料之二進位表示之資訊（例如，詮釋資料之二進位表示之指標或該指標之指標）。若雜湊表並非已經含有與雜湊值相關聯之條目，則載入器215可儲存詮釋資料之二進位表示（例如，詮釋資料記憶體中之暫存器或位置），在雜湊表中創建與雜湊值相關聯之新條目，且將適合的資訊儲存於新條目中（例如，暫存器識別符、詮釋資料記憶體中詮釋資料之二進位表示之指標、該指標之指標等）。然而，應瞭解，本發明之態樣不限於使用雜湊表以用於追蹤已經儲存之詮釋資料之二進位表示。另外或替代地，可使用其他資料結構，諸如曲線圖資料結構、有序清單、無序清單等。可基於任何合適準則或準則之組合，諸如存取時間、記憶體用途等而選擇任何合適資料結構或資料結構之組合。

【0098】 應瞭解，上文引入且下文更詳細論述之技術可以多個方式中之任一者實施，由於技術不限於任何特定實施方式。本文中僅僅出於例示目的而提供實施細節之實例。此外，可個別地或以任何合適組合形式使用本文中所記載之技術，由於本發明之態樣不限於使用任何特定技術或技術之組合。

【0099】 例如，儘管本文中論述包括編譯器（例如，圖2之實例中之例示編譯器205及/或例示策略編譯器220）之實例，但應瞭解，本發明之態樣不限於

此。在一些具體實例中，軟體工具鏈可實施為解譯器。例如，可實施延遲初始化方案，其中一或多個預設符號（例如，「未初始化（UNINITIALIZED）」可在啟動時用於標記，且策略處理器（例如，圖1之實例中之例示策略處理器150）可評估一或多個策略及以即時方式解析該一或多個預設符號。

【0100】 本申請案發明人已認識且瞭解到，安全性策略之有效性可取決於當啟動目標系統時及/或當將應用程式載入至記憶體中以供執行時的適當標記。因此，本文中描述有用於描述及實現安全初始組態之技術。

【0101】 在一些具體實例中，可提供策略語言以用於描述在詮釋資料符號與跨越執行階段系統之各種實體（諸如硬體實體及/或軟體實體）之間的相關性。例如，策略語言可用於編寫將實體名稱映射至詮釋資料符號之策略。

【0102】 在一些具體實例中，實體名稱可僅識別系統組件，諸如本地端記憶體、晶片外記憶體、處理器暫存器檔案等。此等組件之實施細節可提供於目標描述中。例如，用於特定目標系統之目標描述可提供目標系統之實施細節，諸如暫存器檔案之大小、組態暫存器之索引數目，及/或待載入記憶體中之一段軟體程式碼之位址範圍。以此方式，將實體名稱映射至詮釋資料符號之策略可易於跨越不同目標系統再使用（例如，藉由組合策略與不同目標描述）。

【0103】 本申請案發明人已進一步認識且瞭解到，若攻擊者能夠控制載入器程式，則攻擊者能夠藉由使用載入器程式修改詮釋資料及/或策略程式碼之能力而阻止安全性策略。因此，在一些具體實例中，可提供確保載入器程式之安全之策略。

【0104】 圖3展示根據一些具體實例之用於確保載入器程式之安全之例示策略300。例如，策略300可以策略語言編寫，且可用於確保圖2之實例中之例示載入器215之安全。

【0105】 在圖3之實例中，策略300包括複數個區段。區段305可表明一或

多個詮釋資料符號，區段310可表明參考在區段305中所表明之一或多個詮釋資料符號之一或多個規則，且區段315可將一或多個實體名稱映射至區段305中所表明之一或多個詮釋資料符號。

【0106】 在一些具體實例中，在給定一種類型的指令（例如，作業碼）及與該指令相關聯之一或多個輸入詮釋資料符號之情況下，規則可指示是否應允許指令。另外或替代地，該規則可指示一或多個輸出詮釋資料符號。例如，該規則可指示若允許該指令，則一或多個輸出詮釋資料符號與執行該指令之結果相關聯。

【0107】 在一些具體實例中，可將一或多個規則應用至將資料及/或指令載入至應用程式記憶體中之載入器程式，及/或初始化詮釋資料記憶體中之對應詮釋資料。作為一個實例，可提供一或多個規則以有助於創建詮釋資料標記及/或標記與載入至應用程式記憶體中之該資料及/或指令之相關性。作為另一實例，可提供一或多個規則以保護載入器免於攻擊及誤用。例如，載入器程式碼可與指定詮釋資料標記（例如，「LoaderAllow」）相關聯。可禁止不具有該標記之指令存取與載入器相關聯之一或多個記憶體區域。

【0108】 在一些具體實例中，在本文中被稱作「詮釋資料調色板」之應用程式記憶體區域可經分配用於創建詮釋資料標記。此區域可如同畫家之具有複數種原色以按任何合適組合混合在一起的調色板。例如，儲存於應用程式記憶體120中之詮釋資料調色板中之每一字組可為零（或某一其他預設值），且字組之記憶體位置可與詮釋資料記憶體125中之基元詮釋資料標記相關聯。每一基元詮釋資料標記可對應於策略所提及之詮釋資料符號（例如，「Read」、「Write」、「Execute」、「LoaderAllow」、「LoaderCompose」、「LoaderApply」、「loadGrp」、「storeGrp」、「composeGrp」等）。另外或替代地，字組之記憶體位置可與經指定詮釋資料標記（例如，

「MetadataPalette」）相關聯以指示該位置在詮釋資料調色板區域內。

【0109】 在一些具體實例中，為了自兩個基元標記建構複合詮釋資料標記，載入器可經程式化以讀取儲存於分別對應於兩個基元標記之兩個詮釋資料調色板位置中之值，且對彼等值執行第一運算。來自詮釋資料調色板位置之讀數可使規則與待評估讀數相關聯，這可移除「MetadataPalette」標記。例如，儲存讀取自藉由{MetadataPalette，A}標記之位置之值的暫存器可標記為{A}。

【0110】 在一些具體實例中，讀取自兩個詮釋資料調色板位置之值可為零，第一運算可為按位元或運算，使得第一運算之結果亦為零。此「虛設」運算可使規則與待評估第一運算相關聯，這可引起新標記之創建及新標記與儲存結果之暫存器之相關性。例如構成{A}及{B}可導致暫存器被標記為{A，B}。

【0111】 在一些具體實例中，載入器可對第一運算之結果及讀取自待由複合標記所標記之應用程式記憶體位置之值執行第二運算，且將第二運算之結果寫回至待標記應用程式記憶體位置中。例如，第二運算亦可為按位元或運算，使得第二運算之結果與讀取自待標記應用程式記憶體位置之值相同。同樣，儘管第二運算為「虛設」，但執行第二運算可使規則與待評估第二運算相關聯，這可藉由複合標記（例如{A，B}）標記儲存第二運算之結果之暫存器。

【0112】 將結果寫回至記憶體可使規則與待評估寫入相關聯，這可藉由複合標記（例如，{A，B}）標記應用程式記憶體位置。

【0113】 返回至圖3之實例，策略300之區段310包括待按所示次序加以應用之五個規則。

- 第9行之規則指示允許具有「LoaderAllow」標記之載入指令讀取具有「MetadataPalette」標記之記憶體位置。當讀取記憶體位置時，除了移除「MetadataPalette」標記之外，儲存讀取自該記憶體位置之值之暫存器可與該記憶體位置具有相同標記。

• 第10行之規則指示允許具有「LoaderAllow」標記之儲存指令將儲存於暫存器中之任何值寫入至記憶體中之任何位置。寫入有該值之記憶體位置與標記相關聯，該標記和儲存該值之暫存器的標記相同。

• 第11行之規則指示並不允許不具有「LoaderAllow」標記之載入指令讀取具有「MetadataPalette」標記之任何記憶體位置（在此實例中，只有在第9行不適用時才抵達第11行）。

• 第12行之規則指示並不允許不具有「LoaderAllow」標記之儲存指令寫入具有「MetadataPalette」標記之任何記憶體位置（在此實例中，只有在第10行不適用時才抵達第12行）。

• 第13行之規則指示組成指令之結果具有一組一或多個標記，亦即兩個組之聯合，亦即第一組之第一運算元之一或多個標記及第二組之第二運算元之一或多個標記。

【0114】 在一些具體實例中，可認為某些指令類型（例如，作業碼）彼此足夠類似，且因此可出於執行策略目的而分組在一起。例如，可基於被稱作「loadGrp」之群組中之任何指令類型而觸發策略300之第9行，可基於被稱作「storeGrp」之群組中之任何指令類型而觸發策略300之第10行，等等。

【0115】 在一些具體實例中，策略語言可具有群組規格區段，其允許使用者界定任何一或多個指令之任何所需分組。策略連結器（例如，圖2之實例中之例示策略連結器225）可經程式化以使在處理目標程式碼時遇到之指令與由策略編譯器產生之初始化規格中指示之一或多個群組匹配。策略連結器225可接著藉由指示該等指令所屬之各別群組之詮釋資料標籤而註解該等指令。以此方式，策略編譯器可為ISA無關的，而使得ISA相依與策略連結器匹配。

【0116】 以下為RISC-V指令集架構中之一些指令類型之例示分組。應瞭解，僅僅出於說明目的而提供此等作業碼及作業碼群組。本發明之態樣不限於

使用任何特定ISA，或作業碼之任何特定分組。

- branchGrp(RS 1:op1, RS2:op2 ->)
  - beq, bne, blt, bge, bltu, bgeu
- immArithGrp(RS1:op1 -> RD:res)
  - addi, slli, slti, sltiu, xori, srli, srai, ori, andi, addiw, slliw, srliw, sraiw,
- arithGrp(RS1:op1, RS2:op2 -> RD:res)
  - add, sub, sll, slt, sltu, xor, srl, sra, or, and, addw, subw, sllw, srlw, sraw
- loadGrp(RS1:addr, MEM:mem -> RD:res)
  - lb, lh, lw, ld, lbu, lhu, lwu
- storeGrp(RS1:addr, RS2:val, MEM:mem -> MEM:mem)
  - sb, sh, sw, sd

【0117】 圖4展示根據一些具體實例之由策略編譯器輸出之例示策略程式碼400。例如，策略程式碼400可為藉由圖2之實例中之例示策略編譯器220來編譯圖3中展示之例示策略300之第12行之結果。

【0118】 在圖4之實例中，策略程式碼400之第405行可例如藉由檢查指令是否已與詮釋資料標籤「og_dover_riscv_storeGrp」相關聯而檢查輸入指令是否為儲存指令，其可指示該指令是否屬於儲存指令之群組。另外或替代地，可提供硬體區塊以將指令分類成諸如儲存、載入、算術、分支等群組。

【0119】 在一些具體實例中，策略程式碼400之第410行可檢查輸入指令是否正嘗試存取與「MetadataPalette」標記相關聯之記憶體位置。若如此，則可明確地回傳故障。否則，可回傳隱含故障，其可致使評估下一規則（例如，圖3中之第13行）。

【0120】 應瞭解，本發明之態樣不限於藉由將策略編譯成策略程式碼而實施策略。另外或替代地，可藉由程式化FPGA，及/或將規則直接載入至規則

快取記憶體中而實施策略（相較於由於執行策略程式碼而將規則載入至規則快取記憶體中）。

【0121】 返回至圖3之實例，策略300之區段315包括複數個陳述式，每一陳述式將實體名稱映射至一或多個詮釋資料符號。如下文所解釋，策略連結器（例如，圖2之實例中之例示策略連結器225）可使此陳述式中之實體名稱與表示待受保護系統組件之實體匹配，諸如作業系統之載入器程式之函式。關鍵字（例如，「init」）可用於指示由實體名稱所表示之實體將藉由遵循該實體名稱之一或多個詮釋資料符號進行初始化。例如，第16行可指示具有名稱「dover.Kernel.Code.ApplyTag.apply_tags_load_taga」之實體將藉由詮釋資料符號「LoaderAllow」進行初始化。

【0122】 如上文所論述，在一些具體實例中，實體名稱可僅識別諸如本地端記憶體、晶片外記憶體、處理器暫存器檔案等之系統組件。在給定待確保安全之特定目標系統之情況下，目標系統之一或多個組件之實施細節可提供於目標描述中。該目標描述可由策略連結器（例如，圖2之實例中之例示策略連結器225）用於藉由詮釋資料符號來註解目標程式碼。圖5示意性地展示根據一些具體實例之例示目標描述500。

【0123】 在一些具體實例中，目標描述500可包括分別對應於該目標系統之複數個組件之複數個命名實體之描述。實體描述可被組織成複數個模組。例如，在圖5中所展示之實例中，該目標描述500包括硬體實體模組510、軟體實體模組520、類別實體模組530、轉換實體模組540等。一些模組可包括複數個子模組。例如，硬體實體模組510可包括ISA實體模組512、系統單晶片（SOC）實體模組514等；軟體實體模組520可包括OS實體模組522、使用者應用程式實體模組524、建置系統實體模組526等；且類別實體模組530可包括軟體類別實體模組532、硬體類別實體模組534等。

【0124】 在一些具體實例中，各種模組可經選擇及組合以描述不同目標系統。例如，複數個不同ISA實體模組可為分別對應於不同ISA而可取用。類似地，複數個不同OS實體模組可為分別對應於不同作業系統而可取用。在給定特定目標系統之情況下，適合的ISA實體模組可選自可取用的ISA實體模組，且適合的OS實體模組可選自可取用的OS實體模組。可接著將所選模組組合成對於特定目標系統之目標描述。以此方式，針對一個目標系統製備之實體描述可易於再用於另一目標系統。

【0125】 命名實體可表示目標系統之硬體及/或軟體之任何態樣。實體之非限制性實例提供於下文中。

【0126】 在一些具體實例中，硬體實體模組510可描述晶片上之一或多個狀態元件，在啟動時針對該一或多個狀態元件初始化詮釋資料。此類狀態元件之實例包括但不限於以下各者。

- ISA實體模組512可包括基於該目標系統之指令集架構之一或多個實體。此類實體可表示具有待受保護之狀態資訊之硬體實施之態樣，諸如組態暫存器、程式計數器、暫存器檔案、計時器、狀態旗標等。
- SOC實體模組514可包括表示具有待受保護之狀態資訊之晶片級特徵之一或多個實體，諸如晶片上記憶體、組態暫存器、功能區塊、記憶體傳送單元、I/O裝置等。

【0127】 在一些具體實例中，軟體實體模組520可描述與執行階段軟體相關之一或多個狀態元件，在啟動時針對該一或多個狀態元件初始化詮釋資料。此類狀態元件之實例包括但不限於以下各者。

- OS實體模組522可包括表示作業系統特徵之一或多個實體，諸如函式、模組、驅動器、服務常式等。
- 使用者應用程式實體模組524可包括一或多個實體，諸如函式、模組、

驅動器、服務常式等。

• 建置系統實體模組526可包括表示具有可機器載入資料之建置系統特徵之一或多個實體，諸如具有可執行程式碼區段（例如，.text）、初始化資料區段（.data）等之可執行與可連結格式（ELF）檔案。

【0128】 本申請案發明人已認識且瞭解到，出於標記目的將某些硬體特徵及/或軟體特徵共同分組成一類可為有益的。例如，在初始化期間，呈一類別之所有硬體特徵及/或軟體特徵可與同一組一或多個詮釋資料符號相關聯。任何合適準則或準則之組合可用於界定類別實體。在一些具體實例中，類別實體模組530可包括類別實體之以下非限制性實例。

• 軟體類別實體模組532可包括分別表示所有函式之一或多個實體，所有函式具有與某一正規表達式匹配之名稱、所有軟體實體駐存於某一記憶體範圍中等。

• 硬體類別實體模組534可包括分別表示所有暫存器之一或多個實體，所有暫存器具有與某一正規表達式匹配之名稱、所有暫存器屬於某一類型（例如，所有組態暫存器）、所有暫存器在某一位址範圍內等。

• 表示滿足某一準則之所有硬體特徵及軟體特徵之實體，諸如具有以某一前綴開始之名稱。

• 表示與用於執行特定策略相關之所有硬體特徵及/或軟體特徵之實體。

【0129】 在一些具體實例中，類別實體可藉由策略連結器（例如，圖2之實例中之例示策略連結器225）被詳述為多個實體。作為一個實例，類別實體表達式可表示具有32個條目之暫存器檔案，且策略連結器225可將該表達式評估成32個表達式，各自表示各別暫存器。作為另一實例，類別實體表達式可表示八個組態暫存器，包含用於四個處理器模式中之每一者之在起始於某一位址（例如，0x1fc000）之16位元組邊界上對準之兩個組態暫存器。策略連結器225

可將該表達式評估成八個表達式，各自表示適合的位址處（例如，距起始位址16位元組之某一合適倍數之偏移）之各別組態暫存器。因此，類別實體可用於以緊湊方式描述目標系統中之重複結構。作為另一實例，類別實體表達式可包括型樣（例如，屬於特定程式庫之所有函式、晶片上所列舉的所有通用非同步接收器-發射器（UART）裝置等）之描述。策略連結器225可發現到該目標系統之所有實體與類別實體表達式中之型樣匹配。

【0130】 在圖5中所展示之實例中，該目標描述500之轉換實體模組540包括表示一或多個轉換之一或多個實體，其可在編譯之前或期間應用至軟體程式碼以促進更多策略中之一者之執行。例如，策略可指示應在執行一段程式碼之前滿足關於詮釋資料之某一條件。為了符合策略，一或多個指令可前置於該段程式碼（例如，經由編譯器修改及/或應用程式二進位重寫）。該一或多個經前置指令可被設計成不引起任何應用程式資料之改變（例如，NOP指令，或應用至輸入字組及常數0之邏輯或運算，由此返回輸入字組本身）。然而，執行該一或多個經前置指令可致使評估一或多個規則（例如，藉由例示標記處理硬體140），由此實現詮釋資料中之一或多個改變以滿足策略設定之條件。

【0131】 儘管命名實體之模組之實例展示於圖5中且論述於本文中，但應瞭解，本發明之態樣不限於使用任何特定模組，或根本不限於使用任何模組。並且應瞭解，可以任何合適方式創建目標描述。作為實例，實體可由使用者界定。作為另一實例，可提供軟體工具以自動地剖析硬體規格且提取硬體實體（例如程式計數器、組態暫存器等）。另外或替代地，可提供軟體工具以自動地剖析軟體原始程式碼且提取軟體實體（例如命名函式實體、可變實體等）。作為另一實例，一或多個實體可藉由編譯、連結及/或載入程序（例如執行階段堆疊及堆積樹、ELF區段等）及/或其他分析工具（例如流程圖）而界定。

【0132】 在一些具體實例中，階層式名稱空間可用於提供實體名稱，使

得每一實體可經唯一地識別。此可有助於自實體名稱至詮釋資料符號之映射（例如，如圖3之實例中之例示策略300之區段315中所示）。階層式實體名稱之實例提供於下文中。

- ISA實體
  - dover.riscv.User.PC
  - dover.riscv.User.Reg
- SOC實體
  - dover.SOC.IO.Flash
  - dover.SOC.CSR.MTVec
- OS實體
  - dover.Kernel.MemoryMap.UserStack
  - dover.Kernel.MemoryMap.UserHeap
  - dover.Kernel.MemoryMap.Default
  - dover.Kernel.Code.ElfSection. SHF_WRITE
  - dover.Kernel.Code.ElfSection.SHF_ALLOC
  - dover.Kernel. Code.ApplyT ag.my_function
- 執行階段程式庫實體
  - dover.Tools.RTL.memcpy

【0133】 在一些具體實例中，目標描述中之命名實體可具有描述如以硬體實現之實體之一或多個相關聯命名屬性。此類資訊可由策略連結器及/或載入器（例如，圖2之實例中之例示策略連結器225及/或載入器215）以用於安全地初始化目標系統。

【0134】 在一些具體實例中，可提供軟體工具以自動地剖析硬體規格且提取關於一或多個硬體實體之資訊（例如，暫存器檔案之大小、組態暫存器之

索引數目等）。所提取資訊可包括於目標描述中，例如作為與該一或多個硬體實體相關聯之一或多個屬性。

【0135】 在一些具體實例中，軟體實體可表示待載入至記憶體中之程式碼及/或資料之單元。可提供軟體工具以自動地分析軟體程式碼（例如，原始程式碼及/或目標程式碼）且提取關於一或多個軟體實體之資訊。所提取資訊可包括於目標描述中，例如作為與該一或多個軟體實體相關聯之一或多個屬性。作為實例，描述軟體實體之屬性可包括駐存有軟體實體之程式碼及/或資料之位址範圍。此位址範圍可依據偏移來提供，此偏移可用於在實際上將該程式碼及/或資料載入至記憶體中（例如，藉由圖2之實例中之例示載入器215）時判定絕對記憶體位址。

【0136】 另外或替代地，一或多個軟體實體之屬性可自一或多個構建程序符號表及/或使用一或多個二進位分析工具、程式碼分析工具，及/或基於編譯器之程式碼分析工具來提取。

【0137】 如上文所論述（例如，結合圖3之實例），在一些具體實例中，策略可經由「init」陳述式將實體名稱映射至對應詮釋資料符號。策略連結器（例如，圖2之實例中之例示策略連結器225）可經程式化以搜索目標描述以識別具有策略中所提及之實體名稱之實體。例如，對於策略中之每一「init」陳述式，策略連結器225可使「init」陳述式中之實體名稱與該目標描述中之實體匹配。若未發現匹配實體，則策略連結器225可輸出錯誤消息。若發現匹配實體，則策略連結器225可將「init」陳述式與實體結合。另外或替代地，策略連結器225可自該目標描述識別實體之描述，且可使用該描述以藉由來自「init」陳述式之一或多個詮釋資料符號來註解對應於實體之目標程式碼。

【0138】 在一些具體實例中，策略連結器225可將初始化規格格式化成適合於由載入器215使用之形式。例如，該初始化規格可經格式化以變為一或多

個二進位檔案，以便經由後段構建程序而流送至載入器215。然而，如在一些具體實例中，並不需要可將初始化規格單獨地提供至載入器215。

【0139】 再次參考圖2之實例，在一些具體實例中，策略連結器225可使詮釋資料標籤與藉由編譯器205所輸出之目標程式碼檔案中之指令及/或資料相關聯。（如上文所論述，詮釋資料標籤可提供對一或多個策略所提及之一組一或多個詮釋資料符號之緊湊編碼。）詮釋資料標籤與指令及/或資料之相關性可以任何合適方式進行。

【0140】 例如，ELF格式可允許在目標檔案內創建新區段以保存任意格式化之資料。可在目標檔案中添加用於詮釋資料之區段，且目標檔案中之每一程式碼或資料字組可具有詮釋資料區段中之對應詮釋資料標籤。以此方式，藉由策略連結器225進行之詮釋資料註解可傳遞通過連結器210且藉由連結器210加以聚合。另外或替代地，策略連結器225可使詮釋資料標籤與藉由編譯器205所輸出之目標程式碼檔案中之指令及/或資料相關聯。

【0141】 在一些具體實例中，策略連結器225可使用策略中之一或多個「init」陳述式（其將實體名稱映射至對應詮釋資料符號）、策略中所指示之指令之一或多個分組（例如，在群組規格區段中）、及/或目標規格中之一或多個實體描述，以創建用於目標程式碼檔案中之指令及/或資料之詮釋資料標籤。例如，策略連結器225可自策略之「init」陳述式識別實體名稱且使用實體名稱以查找該目標描述中之實體描述。策略連結器225可接著使用實體描述以定位目標程式碼檔案中之元件，且使適合的詮釋資料標籤與目標程式碼檔案中之該等指令及/或資料相關聯。

【0142】 圖6展示根據一些具體實例之已經藉由詮釋資料標籤所註解之例示組合程式碼600。例如，組合程式碼600可藉由分解藉由詮釋資料標籤所註解之目標程式碼（例如，具有添加之詮釋資料區段之目標程式碼檔案）而產生。

由於此類目標程式碼可能並非人類可讀取，因此本文中提供組合程式碼600以說明關於藉由詮釋資料標籤來註解目標程式碼之各種概念。此外，如上文所論述，除錯工具（例如，圖2中展示之例示除錯器230）可顯示藉由分解以詮釋資料標籤所註解之目標程式碼而產生之人類可讀取組合程式碼。

【0143】 在圖6之實例中，組合程式碼600包括分別對應於複數個指令之複數行。可將複數個標示插入至組合程式碼600中以標示某些函式開始之位置。例如，可插入標示605以指示「apply_md」函式開始之處，可插入標示610以指示「apply_md_compose_loop」函式開始之處，且可插入標示615以指示「apply_md_write_mem」函式開始之處。

【0144】 在一些具體實例中，組合程式碼600中之每一行可包括複數欄。例如，組合程式碼600可由目標檔案之摘錄產生，且最左欄可包括自目標檔案之起點偏移之位址（例如，如圖6中之620處所示之「424」）。接下來三欄可分別包括指令之碼字、助憶符，及一或多個參數（例如，如圖6中之625、630及635處所示之「0002a783」、「lw」，及「a5，0（t0）」）。最右欄可包括藉由策略連結器（例如，圖2之實例中之例示策略連結器225）所應用至指令之詮釋資料標籤。

【0145】 在一些具體實例中，藉由策略連結器所應用之詮釋資料標籤可基於策略中所表明之詮釋資料符號。例如，參考圖3之實例，詮釋資料符號「LoaderAllow」表明於例示策略300中。策略編譯器220可例如藉由添加前綴以指示策略名稱（例如，「dover.loader」）而自詮釋資料符號「LoaderAllow」建構階層式詮釋資料標籤。

【0146】 再次參考圖3之實例，策略300中之「init」陳述式將實體名稱「dover.Kernel.Code.ApplyTag.apply_tags_load_taga」映射至詮釋資料符號「LoaderAllow」。策略連結器225可使名稱

「dover.Kernel.Code.ApplyTag.apply_tags_load_taga」與實體及目標描述中之對應描述匹配，且可使用該描述以識別待藉由詮釋資料符號「LoaderAllow」所註解之目標程式碼中之一或多個指令。作為一個實例，實體描述可指示駐存於位址範圍0000 0424至0000 042f中之指令與實體相關聯，該實體與名稱「dover.Kernel.Code.ApplyTag.apply_tags_load_taga」相結合。作為另一實例，實體描述可指示在標示<apply_md>與下一標示之間的指令與實體相關聯，該實體與名稱「dover.Kernel.Code.ApplyTag.apply_tags_load_taga」相結合。策略連結器225可在軟體程式庫（例如，如由圖2之實例中之例示編譯器205及/或連結器210產生）中查找標示<apply_md>以識別位址範圍0000 0424至0000 042f。策略連結器225可接著分析在該範圍內所發現之指令，以判定是否應藉由額外詮釋資料來註解該等指令。例如，一或多個指令可係函式序言或函式結語之部分，且因而應藉由詮釋資料符號來註解以用於堆疊策略。

【0147】 在一些具體實例中，詮釋資料標籤可基於不同策略中所表明之複數個詮釋資料符號。例如，實體可進行多個不同策略且因此被提及於多個不同「init」陳述式中。儘管如此，單一詮釋資料標籤可應用至實體，且可隨後解析成二進位表示（例如，典型表示，如上文所論述）。以此方式，僅可維持一個詮釋資料記憶體位址，即使該實體將與多個詮釋資料符號相關聯。如此可減小標記映射表（例如，圖1之實例中之例示標記映射表142）之大小及/或處理時間（例如，藉由圖1之實例中之標記處理硬體140）。

【0148】 在一些具體實例中，用於儲存詮釋資料標籤之二進位表示之集合的詮釋資料記憶體之量可藉由建構詮釋資料標籤實際上使用到之二進位表示之表而減小。替代儲存二進位表示之集合，可將索引之集合儲存至表中。

【0149】 本申請案發明人已認識且瞭解到，可能需要使詮釋資料符號與指令合理地相關聯，以例如減小用於詮釋資料之儲存裝置之量及/或加速詮釋資

料處理。因此，在一些具體實例中，策略連結器225可經程式化以識別將使參考詮釋資料符號之一或多個規則觸發之指令，且僅將對應詮釋資料標籤應用至彼等指令。例如，參考圖3之實例，詮釋資料符號「LoaderAllow」在規則中被提及於第9及10行，且分別藉由群組「loadGrp」及「storeGrp」中之指令觸發彼等規則。因此，詮釋資料符號「LoaderAllow」與位址000 0424處之載入指令相關聯，但不與位址0000 0428處之算術指令或位址0000 042c處之分支指令相關聯，即使算術指令及分支指令與載入指令（亦即，「apply_md」函式）為同一軟體實體之部分。

【0150】 圖7展示根據一些具體實例之用於將可執行程式碼載入電腦系統中之例示程序700。例如，參考圖2之實例，程序700可由載入器215執行以將資料及/或指令載入至應用程式記憶體120中，及/或初始化詮釋資料記憶體125中之標記以用於資料及/或指令。

【0151】 在圖7之實例中，程序700包括兩個階段，啟動載入及動態載入。此等階段中之一者或兩者可由圖2之實例中之載入器215來執行。例如，載入器215可包括啟動載入器及動態載入器。在一些具體實例中，動態載入器可以是作業系統之一部分。然而，應瞭解，本發明之態樣不限於具有作為作業系統之一部分之動態載入器。

【0152】 在一些具體實例中，啟動載入器及動態載入器可由實體上分離之處理器來執行。例如，啟動載入器可藉由圖1之實例中之例示策略處理器150來執行，而動態載入器可藉由例示主機處理器110來執行。然而，應瞭解，本發明之態樣不限於以分開的處理器來執行啟動載入器及動態載入器。在一些具體實例中，啟動載入器及動態載入器兩者可以同一處理器來執行（例如，策略處理器150或主機處理器110）。

【0153】 本申請案發明人已認識且瞭解到，例如藉由將載入器程式碼載

入至與應用程式記憶體分離之記憶體中及/或使用分開的暫存器集合以用於執行載入器程式碼，具有用於載入器程式碼之分開的機器狀態可使得攻擊者存取或修改詮釋資料更為困難。例如，具有分開的機器狀態可使得攻擊者控制載入器程式碼更為困難。然而，應瞭解，相較於主機處理110，本發明之態樣不限於以策略處理器150執行載入器程式碼。在一些具體實例中，啟動載入器及/或動態載入器可以主機處理器110來執行，且可藉由載入器策略（例如，圖3中展示之例示策略300）確保安全。

【0154】 在一些具體實例中，載入器策略可限制將詮釋資料修改為以正確上下文執行之載入器程式碼之特權。作為一個實例，載入器策略可包括指示僅可載入合法二進位影像的一或多個規則，諸如與證明二進位資料來自有效源之詮釋資料符號相關聯之二進位資料。此詮釋資料符號可已經藉由另一程序附接至二進位資料，該程序已驗證二進位資料之完整性及/或真實性（例如，基於密碼編譯數位簽名）。作為另一實例，載入器策略可包括執行控制流程完整性的一或多個規則，使得程式執行可僅自OS程式碼中之特定點傳送至載入器程式碼。以此方式，載入器策略可防止惡意攻擊者程式碼載入非法二進位影像。

【0155】 另外或替代地，載入器策略還可包括一或多個規則，諸如載入器程式碼不可被修改或複製、載入器指令僅可以適當序列來執行等。

【0156】 返回至圖7，啟動載入器可在動作705處將作業系統之二進位影像載入至應用程式記憶體120中。另外或替代地，啟動載入器還可根據用於OS之初始化規格來初始化詮釋資料記憶體125中之標記。OS二進位影像及/或OS詮釋資料的初始化規格可擷取自持久性儲存裝置（例如，快閃記憶體、硬碟、ROM等）。如上文所述，OS詮釋資料的初始化規格可由策略連結器（例如，圖2之實例中之例示策略連結器225）基於OS二進位影像、用於適用OS之一或多個策略（例如，動態載入器策略）之經編譯程式碼，及/或目標描述而產生。

【0157】 在一些具體實例中，OS二進位影像及/或OS詮釋資料的初始化規格可以電子方式簽名，且可藉由對應於用於簽名之私用密鑰之公用密鑰進行分配。私用密鑰本身可未經分配。啟動載入器可使用公用密鑰以驗證OS二進位影像及/或OS詮釋資料的初始化規格尚未經修改。

【0158】 在動作710處，啟動載入器可將執行傳送至OS，這可完成啟動載入階段且開始動態載入階段。在動作715處，OS可在策略執行硬體之監督下執行，諸如圖1之實例中之例示寫入互鎖112、例示標記處理硬體140、例示策略處理器150，及/或例示詮釋資料記憶體125。

【0159】 在圖7中所展示之實例中，OS包括動態載入器。在動作720處，動態載入器可例如回應於使用者啟動使用者應用程式，而將使用者應用程式之二進位影像載入至應用程式記憶體120中。另外或替代地，動態載入器還可根據用於使用者應用程式之初始化規格來初始化詮釋資料記憶體125中之標記。使用者應用程式的二進位影像及/或使用者應用程式的詮釋資料的初始化規格可擷取自持久性儲存裝置（例如，快閃記憶體、硬碟、ROM等）。如上文所述，使用者應用程式的詮釋資料的初始化規格可由策略連結器（例如，圖2之實例中之例示策略連結器225）基於使用者應用程式的二進位影像、用於適用使用者應用程式之一或多個策略之經編譯程式碼，及/或目標描述而產生。

【0160】 在一些具體實例中，動態載入器可藉由觸發載入器策略之一或多個規則而初始化詮釋資料記憶體125中之標記，諸如圖3實例中之例示載入器策略300。例如，動態載入器可對應用程式記憶體120中之詮釋資料調色板區域執行某些操作，如上文結合圖3所述。此可觸發藉由處理硬體140及/或策略處理器150對載入器策略300之一或多個規則之評估，由此創建及應用複合標記。

【0161】 在一些具體實例中，使用者應用程式的二進位影像及/或使用者應用程式的詮釋資料的初始化規格可以電子方式簽名，且可藉由對應於用於簽

名之私用密鑰之公用密鑰進行分配。私用密鑰本身可未經分配。動態載入器可使用公用密鑰以驗證使用者應用程式的二進位影像及/或使用者應用程式的詮釋資料的初始化規格未經修改。另外或替代地，使用使用者應用程式的詮釋資料的初始化規格載入使用者應用程式的二進位影像還可觸發一或多個載入器策略規則。例如，該一或多個規則在經評估時可查找一或多個詮釋資料符號，以證明使用者應用程式的二進位影像及/或使用者應用程式的詮釋資料的初始化規格來自有效源。該一或多個詮釋資料符號可已經藉由已使用公用密鑰執行驗證之另一程序被附接至使用者應用程式的二進位影像及/或使用者應用程式的詮釋資料的初始化規格。

【0162】 由於OS及使用者應用程式可由不同供應商分配，因此用於簽名及驗證OS及使用者應用程式之公用-私用密鑰配對可以不同。

【0163】 在一些具體實例中，一旦經載入及標記，使用者應用程式可在策略執行硬體（例如，圖1之實例中之例示寫入互鎖112、例示標記處理硬體140、例示策略處理器150，及/或例示詮釋資料記憶體125）之監督下執行。

【0164】 在一些具體實例中，動態載入器亦可處置經終止應用程式之拆解及清除。例如，在動作725處，動態載入器可回應於使用者關閉使用者應用程式或停止電腦系統而自應用程式記憶體120移除使用者應用程式之二進位影像。在一些具體實例中，移除使用者應用程式之二進位影像可觸發藉由處理硬體140及/或策略處理器150對一或多個載入器策略規則之評估，這可引起標記映射表142中與經關閉使用者應用程式相關之所有條目之移除，及/或對應詮釋資料自詮釋資料記憶體125及/或標記暫存器檔案146之移除。在一些具體實例中，當同一標記可與不同使用者應用程式相關聯時，可移除標記映射表142中的任何位置處所不再提及之詮釋資料。

〈**例示策略**〉

完整性策略

【0165】 在一些具體實例中，完整性策略可使用資訊流以追蹤資料來自何處。例如，諸如串聯埠、乙太網埠、記憶體、ROM等資料源可藉由識別該資料源之詮釋資料標記進行標示。在傳送期間，該資料及任何導出資料可保留用於該資料源之標記。

【0166】 在一些具體實例中，策略規則可指示允許追蹤資訊之何種用途。例如，完整性策略可禁止使用來自晶片外源之資料進行任何控制流程決策，因此防止資料導向程式設計（Data Oriented Programming，DOP）攻擊。

【0167】 在一些具體實例中，經追蹤資料可藉由指示資料源之詮釋資料標記進行標示。當程式執行及操控該資料時，源標記可經由計算傳播使得任何導出資料保留源指示標記。

【0168】 在一些具體實例中，完整性策略可追蹤資訊流以限制資料之傳輸，例如以防止某些資料離開系統單晶片（SoC）。

【0169】 在一些具體實例中，完整性策略可檢查DOP保護之完整性。

【0170】 在一些具體實例中，完整性策略可偵測及/或防止某些資料之修改，例如確保韌體更新之安全。

安全性策略

【0171】 在一些具體實例中，安全性策略可維持詮釋資料以執行一或多個暫時系統屬性，諸如次序及協定狀態轉變。例如，在使用策略之情況下，可相對於參考狀態機來監控及檢查事件之定序。

【0172】 在一些具體實例中，系統程式碼之一或多個區段可藉由指示狀態轉變之詮釋資料進行標示。程式計數器（或另一合適的實體）可藉由可攜載系統狀態變數之環境詮釋資料進行標示。一或多個安全性策略可使用轉變以更新狀態變數，且檢查有效轉變。

上下文切換策略

【0173】 在一些具體實例中，上下文切換策略可允許OS中之特許程式碼執行上下文切換操作以在不同任務之間移動或處理上下文。切換上下文之程序可涉及將舊任務資料（例如，與經激發上下文相關聯之任務資料）保存至內核儲存裝置，及/或自內核儲存裝置載入新任務資料（例如，與經輸入上下文相關聯之任務資料）。本申請案發明人已認識且瞭解到，新任務資料之載入及/或舊任務資料之保存可違反正實行之策略之一或多個安全性屬性。因此，在一些具體實例中，可提供上下文切換策略來覆寫其他策略以允許進行上下文切換。

【0174】 在一些具體實例中，上下文切換策略可檢查出經執行程式碼上之詮釋資料來自OS上下文切換常式以用於在任務之間進行改變。上下文切換策略可在適當時機覆寫其他策略，且可允許來自OS上下文切換常式之程式碼將任務資料保存至內核記憶體，及/或恢復來自內核記憶體之任務資料，以及用於任務之各別詮釋資料。

【0175】 本申請案發明人已認識且瞭解到，在一些情況下，可不允許與一個任務相關聯之程式碼操控與另一任務相關聯之狀態。因此，在一些具體實例中，上下文切換策略可使用策略語言中之特殊全域關鍵字以允許上下文切換程式碼對經由詮釋資料與多於一個任務（例如，經暫停任務及上下文切換任務本身，或經恢復任務及上下文切換任務本身）相關聯之資料進行操作。

分隔策略

【0176】 在一些具體實例中，分隔策略可對任務之間的資訊流提供隔離及/或控制。此分隔化可例如用於軟體故障隔離方案，其中可防止受損分隔存取或損壞其他分隔。

【0177】 在一些具體實例中，分隔策略可將顏色指派至每一分隔且檢查出用於機器操作之詮釋資料始終具有一致的分隔顏色。例如，分隔顏色詮釋資

料可應用至任務資料、任務環境，及/或任務程式碼。此可使資料及程式碼與執行上下文相關聯。在一些具體實例中，分隔模型可具有一或多個機制以用於在任務之間切換，諸如即時作業系統（RTOS）上下文切換。另外或替代地，分隔策略還可指定在允許在分隔之間致能通信的分隔之間的資訊流。

【0178】 在一些具體實例中，分隔策略可對分隔之間的流提供明確策略控制。例如，分隔策略可在執行期間執行允許分隔A與分隔B共享資訊。

【0179】 在一些具體實例中，分隔策略可對資料提供一般化解密。例如，分隔策略可在執行期間執行允許某一類型之資料離開分隔。

【0180】 在一些具體實例中，分隔策略可使分隔與RTOS任務相關聯。例如，分隔策略可指派記憶體之所選區域用作資料之先進先出（FIFO）緩衝區以自分隔A傳送至分隔B。

【0181】 在一些具體實例中，分隔策略可提供運行於單一處理器上之執行環境之邏輯隔離。例如，分隔可包括完整執行上下文，其可包括記憶體中之程式碼及資料、硬體暫存器及指定環境（或程式計數器pc）暫存器以用於保存上下文識別符（例如，詮釋資料ID）。分隔策略可包括規則來確保執行上下文之所有部分（例如，程式碼、資料、暫存器等）共享用以識別分隔之單一共同詮釋資料ID。分隔內之執行可在每一分開的分隔內繼續正常進行。然而，可不允許一個分隔中之程式碼與來自另一分隔之資料交互，除非明確被規則允許。

【0182】 在一些具體實例中，分隔策略可在執行期間執行用於計算之輸入資料可僅屬於主動分隔，及/或計算之結果可藉由主動分隔之ID進行標註。類似地，將操作儲存至記憶體/自記憶體載入操作可僅發生在藉由適合的分隔ID標註該記憶體時。

【0183】 在一些具體實例中，可在分隔可在創建某一任務時與該任務相關聯之情況下提供多任務環境。每當OS在任務之間切換時，分隔ID可被改變以

與新分隔匹配。圖8展示根據一些具體實例之例示分隔策略800。在此實例中，分別針對複數個操作類型提供規則。每一規則可在被執行時執行對應類型之操作僅在所有輸入及輸出具有相同分隔ID時才可繼續進行。

【0184】 圖9展示根據一些具體實例之可藉由策略編譯器（例如圖2實例中之例示策略編譯器220）以自圖8實例中之規則1產生的例示策略程式碼900。

【0185】 在一些具體實例中，實施於RTOS上之基於任務之分隔策略可具有以下部分中之一或多者。

1）初始化任務程式碼及資料（藉由獨特ID詮釋資料來標註分隔）

2）開始RTOS排程器（經由排程器程式碼來保存ID）

3）協同式多任務上下文切換（在前一分隔與下一分隔之間切換ID）

4）搶先式多任務上下文切換（在前一分隔與下一分隔之間切換ID）

【0186】 在一些具體實例中，程式碼可在分隔之間共享，且可因此在步驟1）處未藉由分隔ID進行標註。然而，屬於不同分隔之資料可藉由各別分隔ID進行標註。以此方式，可甚至在分隔之間共享程式碼時維持資料隔離。

【0187】 在一些具體實例中，在啟動時，步驟1與步驟2可初始化用於RTOS之分隔及任務排程器。例如，圖8中展示之例示分隔策略800可包括將實體名稱「application.code.function.portstartscheduler」映射至詮釋資料符號「Cpt A」（用於分隔A）之以下「init」陳述式。

require: init application.code.function.portstartscheduler {Cpt A}

【0188】 在一些具體實例中，策略編譯器（例如，在圖2中展示之例示策略編譯器220）可基於以上「init」陳述式來產生階層式詮釋資料符號（例如，「Dover.Comparment.Cpt_A」）。

【0189】 在一些具體實例中，RTOS之目標描述可包括以下實體結合，其可使實體名稱「application.code.function.portstartscheduler」與函式符號

「xPortStartScheduler」結合。

name: application.code.function.portstartscheduler

elf_name: xPortStartScheduler

tag_all: true

kind: symbol

【0190】 在一些具體實例中，策略連結器（例如，在圖2中展示之例示策略連結器225）可使「init」陳述式中之實體名稱與實體結合中之實體名稱匹配，且可使階層式詮釋資料符號「Dover.Comparment.Cpt_A」與函式符號「xPortStartScheduler」提及之函式相關聯。

【0191】 在一些具體實例中，在正常操作期間，步驟3與步驟4可在將執行自一個任務傳送至另一任務時反覆地進行。例如，協同式多任務可在一個任務相對於另一任務產生執行時間時而同步地發生，而搶先式多任務可例如經由計時器中斷及暫停一個任務之執行以切換至另一任務之中斷服務常式（interrupt service routine，ISR）而非同步地發生。

【0192】 下文為用於以上實例中之四個步驟之例示偽碼。每一子步驟展示之註解可展示如何在該子步驟中更新詮釋資料ID。箭頭左側之ID可由右側之ID替換，其中標籤可如下：

0-未初始化ID

P-前一ID

N-下一ID

初始化分隔

分配堆疊記憶體

指派分隔id　　0 <- N

推動堆疊指標 N <- N

初始化暫存器 0 <- N

將程式計數器設定為任務條目 0 <- N

設定暫存器中之任務參數 0 <- N

返回

啟動排程器

初始化排程器資料結構

初始化計時器

恢復來自排程器資料結構之堆疊指標 P <- N

將pc恢復為epc P <- N

恢復暫存器 P <- N

彈出堆疊指標 N <- N

自中斷返回

協同式多任務上下文切換

停用中斷

推動堆疊指標 P <- P

保存暫存器 P <- P

保存排程器資料結構中之堆疊指標 P <- P

將返回位址保存為pc P <- P

呼叫排程器

恢復來自排程器資料結構之堆疊指標 P <- N

將pc恢復為epc P <- N

恢復暫存器　　P <- N

彈出堆疊指標　　N <- N

自中斷返回

搶先式多任務上下文切換

推動堆疊指標　　P <- P

保存暫存器　　P <- P

保存排程器資料結構中之堆疊指標　　P <- P

將epc保存為pc　　P <- P

呼叫排程器

恢復來自排程器資料結構之堆疊指標　　P <- N

將pc恢復為epc　　P <- N

恢復暫存器　　P <- N

彈出堆疊指標　　N <- N

自中斷返回

分隔間通信

【0193】 在一些具體實例中，為促進分隔之間的通信，可提供策略規則以在將資料發送至另一分隔時允許用於資料之分隔ID發生改變。此可藉由擴展分隔ID而進行，例如藉由添加與每一ID相關聯之權限。例如，替代「Cpt id」，「Read id」或「Write id」可用於指示與該ID相關聯之權限。

【0194】 在一些具體實例中，在使用權限之情況下，某些記憶體緩衝區可經標註為可由一個分隔讀取及可由另一分隔寫入。此可致能獨立進程與串流緩衝區（例如，Kahn進程網路）通信之固有程式設計樣式。

【0195】 圖10展示根據一些具體實例之在通信規則情況下之例示策略程

式碼1000。

即時排程

【0196】 在一些具體實例中，搶先式多任務上下文切換（例如，以上步驟4）可發生在目前執行任務之非同步中斷期間。本申請案發明人已認識且瞭解到，即時系統可對中斷延時敏感，且因此可能需要搶先式多任務上下文切換以及時地方式發生。由於允許P<-P或P<-N之規則可能尚未安置於規則快取記憶體中，因此規則快取未命中可發生在實施搶先式多任務上下文切換之ISR期間。在ISR期間規則快取未命中之可能性可損害一或多個即時潛時保證，這可影響應用程式之正確運行。因此，在一些具體實例中，可提供軟體機制以用於將規則預安置於快取記憶體中，及/或可提供硬體機制以用於防止收回ISR規則。此可保持確定性ISR效能。

【0197】 另外或替代地，硬體特徵還可提供於規則快取記憶體（例如，圖1之實例中之例示規則快取記憶體144）中以允許規則將規則之一或多個輸入轉送至規則之輸出。此轉送特徵可以任何合適方式實施，例如藉由提供一或多個指定標記值，該一或多個指定標記值在呈現於規則之輸出中時致使圖1之實例中之例示標記處理硬體140選擇一或多個輸入標記以用作一或多個輸出標記，從而替代該一或多個指定標記值。本申請案發明人已認識且瞭解到，一或多個轉送規則可用於降低規則快取記憶體144之空間要求。例如，轉送規則可用作藉由一或多個輸入標記加以參數化之規則。參考上文實例中之P<-P及P<-N狀況，單一規則可用於處置P及N之標記值之每個組合。以此方式，規則可經預安置而無需預先對P及N之所有可能標記值執行實例化。

例示電腦

【0198】 圖11示意性地展示上面可實施本發明之任何態樣之例示電腦1100。

【0199】 在圖11中所展示之具體實例中，電腦1100包括具有一或多個處理器之處理單元1101及可包括例如揮發性及/或非揮發性記憶體1102之非暫時性電腦可讀取儲存媒體。記憶體1102可儲存程式化處理單元1101以執行本文所述功能中之任一者的一或多個指令。除了系統記憶體1102，電腦1100亦可包括其他類型之非暫時性電腦可讀取媒體，諸如儲存裝置1105（例如，一或多個磁碟機）。儲存裝置1105亦可儲存一或多個應用程式及/或由應用程式（例如，軟體程式庫）使用之資源，該一或多個應用程式及資源可載入至記憶體1102中。

【0200】 電腦1100可具有一或多個輸出裝置及/或輸入裝置，如圖11中所說明的1106及1107。可例如使用此等裝置以呈現使用者介面。可用於提供使用者介面之輸出裝置之實例包括用於輸出之視覺呈現之印表機及顯示螢幕，及用於輸出之聽覺呈現之揚聲器及其他聲音產生裝置。可用於使用者介面之輸入裝置之實例包括鍵盤及指標裝置（例如，滑鼠、觸控板，及數位化平板）。作為另一實例，輸入裝置1107可包括用於俘獲音訊信號之麥克風，且輸出裝置1106可包括用於視覺再現之顯示螢幕，及/或用於聽覺再現已辨識文字之揚聲器。

【0201】 在圖11中所展示之實例中，電腦1100亦包括一或多個網路介面（例如，網路介面1110）以實現經由各種網路（例如，網路1120）之通信。網路之實例包括區域網路（例如，企業網路）及廣域網路（例如，網際網路）。此類網路可基於任何合適技術且根據任何合適協定進行操作，且可包括無線網路及/或有線網路（例如，光纖網路）。

【0202】 此外，本發明技術可按以下組態體現：

（1）一種包含至少一個處理器之系統，該至少一個處理器經程式化以：

將策略轉譯成策略程式碼，其中：

該策略以策略語言來提供；

該策略程式碼呈不同於該策略語言之程式設計語言；且

該策略包含將實體名稱映射至待與目標系統中之實體相關聯之一或多個詮釋資料符號的陳述式，將對該實體執行該策略。

（2）如（1）所述之系統，其中：

該至少一個處理器進一步經程式化以將該一或多個詮釋資料符號中之至少一個詮釋資料符號解析成二進位表示；

該至少一個詮釋資料符號之該二進位表示包括於該策略程式碼中。

（3）如（1）至（2）中任一項所述之系統，其中：

該至少一個處理器進一步經程式化以：

自描述該目標系統之目標描述來識別用以描述該目標系統之該實體之實體描述；及

使用該實體描述以使該一或多個詮釋資料符號與該目標系統之該實體相關聯。

（4）如（3）所述之系統，其中：

該目標描述包含被組織成複數個模組之複數個實體描述。

（5）如（1）至（4）中任一項所述之系統，其中：

該複數個模組包含對應於該目標系統之指令集架構（ISA）之至少一個指令集架構模組；且

該至少一個ISA模組包含與該目標系統之該指令集架構相關聯之複數個ISA實體的實體描述。

（6）如（1）至（4）中任一項所述之系統，其中：

該複數個模組包含對應於該目標系統之硬體晶片設計之至少一個系統單晶片（SOC）模組；且

該至少一個SOC模組包含與該目標系統之該硬體晶片設計相關聯之複數個SOC實體的實體描述。

（7）如（1）至（4）中任一項所述之系統，其中：

該複數個模組包含對應於該目標系統之作業系統（OS）之至少一個作業系統模組；且

該至少一個OS模組包含與該目標系統之該作業系統相關聯之複數個OS實體的實體描述。

（8）如（1）至（4）中任一項所述之系統，其中：

該複數個模組包含對應於該目標系統之至少一個使用者應用程式之至少一個使用者應用程式模組；且

該至少一個使用者應用程式模組包含與該目標系統之該至少一個使用者應用程式相關聯之複數個使用者應用程式實體的實體描述。

（9）如（1）至（4）中任一項所述之系統，其中：

該複數個模組包含至少一個類別模組；

該至少一個類別模組包含至少一個類別實體之實體描述；且

該至少一個類別實體對應於該目標系統中滿足類別之或多個界定準則的該類別的硬體及/或軟體實體。

（10）如（9）所述之系統，其中：

該至少一個類別實體對應於該目標系統中與執行所選策略相關之類別的硬體及/或軟體實體。

（11）如（9）所述之系統，其中：

該至少一個處理器進一步經程式化以將該類別實體闡述成複數個構成實體。

（12）如（1）至（4）中任一項所述之系統，其中：

該複數個模組包含至少一個轉換模組；

該至少一個轉換模組包含至少一個轉換實體之實體描述；且

該至少一個轉換實體對應於被應用至軟體程式碼之執行之轉換以促進一或多個策略。

（13）如（1）所述之系統，其中：

該實體名稱具有根據階層式名稱空間之結構；且

該至少一個處理器經程式化以使用該結構來將該實體名稱映射至該一或多個詮釋資料符號。

（14）一種包含至少一個處理器之系統，該至少一個處理器經程式化以：

將第一詮釋資料標籤及第二詮釋資料標籤兩者解析成詮釋資料之同一二進位表示，該第二詮釋資料標籤在語法上不同於該第一詮釋資料標籤但在語義上等效於該第一詮釋資料標籤。

（15）如（14）所述之系統，其中：

該第一詮釋資料標籤及該第二詮釋資料標籤係基於同一組的一或多個詮釋資料符號。

（16）如（14）至（15）中任一項所述之系統，其中：

該至少一個處理器進一步經程式化以：

執行指令而由此獲得執行結果；及

將該執行結果儲存至記憶體位置；

該系統進一步包含策略執行硬體，其經組態以：

回應於接收到該指令藉由該至少一個處理器所執行之指示，評估一或多個規則以判定是否允許該指令，其中該一或多個規則之評估回傳詮釋資料之該二進位表示；

回應於判定允許該指令，判定由該一或多個規則所回傳之詮釋資料之該二進位表示之例項是否已經儲存；

回應於判定詮釋資料之該二進位表示之例項未經儲存：

將詮釋資料之該二進位表示儲存至硬體位置；且

至少部分地藉由儲存自該記憶體位置至儲存有詮釋資料之該二進位表示之該硬體位置的映射而使詮釋資料之該二進位表示與該記憶體位置相關聯；及

回應於判定詮釋資料之該二進位表示之例項已經儲存：

至少部分地藉由儲存自該記憶體位置至已經儲存有詮釋資料之該二進位表示之硬體位置的映射而使詮釋資料之該二進位表示與該記憶體位置相關聯。

（17）如（14）至（16）中任一項所述之系統，其中：

該記憶體位置包含應用程式記憶體中之位置；且

儲存有詮釋資料之該二進位表示之該硬體位置包含與該應用程式記憶體實體上分離之詮釋資料記憶體中之位置。

（18）如（14）至（16）中任一項所述之系統，其中儲存有詮釋資料之該二進位表示之該硬體位置包含策略處理器之暫存器。

（19）如（14）至（16）中任一項所述之系統，其中儲存有詮釋資料之該二進位表示之該硬體位置包含指令集架構（ISA）組態暫存器。

（20）如（14）至（16）中任一項所述之系統，其中儲存有詮釋資料之該二進位表示之該硬體位置包含系統單晶片（SOC）組態暫存器。

（21）如（14）至（16）中任一項所述之系統，其中：

該至少一個處理器經程式化以至少部分地藉由以下操作來判定該至少一個二進位表示之例項是否已經儲存：

自該至少一個二進位表示以產生雜湊值；及

使用該雜湊值來檢查雜湊表是否包括對應於該至少一個二進位表示之條目。

（22）如（14）所述之系統，其中：

該至少一個處理器進一步經程式化以載入用於執行策略之一段策略程式

碼；且

該至少一個詮釋資料標籤係基於該策略程式碼中所指示之至少一個詮釋資料符號。

（23）如（22）所述之系統，其中：

該至少一個處理器包含第一處理器及第二處理器；

該第一處理器經組態以運行一段目標程式碼；且

該第二處理器經組態以運行該段策略程式碼。

（24）一種包含至少一個處理器之系統，該至少一個處理器經程式化以：

自應用程式記憶體載入第一值，其中該第一值與至少一個第一基元詮釋資料標籤相關聯；

自該應用程式記憶體載入第二值，其中該第二值與至少一個第二基元詮釋資料標籤相關聯；且

至少部分地藉由對該第一值及該第二值執行操作而將該至少一個第一基元詮釋資料標籤及該至少一個第二基元詮釋資料標籤組合成一複合詮釋資料標籤。

（25）如（24）所述之系統，其中：

該至少一個處理器進一步經程式化以將該應用程式記憶體之區域分配用於創建複合詮釋資料標籤；且

自該應用程式記憶體之該區域載入該第一值與該第二值。

（26）如（24）至（25）中任一項所述之系統，其中：

該第一值與該第二值相同。

（27）如（24）至（26）中任一項所述之系統，其進一步包含策略執行硬體，其中：

對該第一值及該第二值執行之該操作致使該策略執行硬體評估一或多個規

則；且

該一或多個規則之評估致使該策略執行硬體將該至少一個第一基元詮釋資料標籤及該至少一個第二基元詮釋資料標籤組合成該複合詮釋資料標籤。

（28）如（27）所述之系統，其中：

載入該第一值致使該策略執行硬體自與第一應用程式記憶體位置相關聯之第一詮釋資料記憶體位置來讀取該第一基元詮釋資料標籤，該第一值係自該第一應用程式記憶體位置所載入；且

載入該第二值致使該策略執行硬體自與第二應用程式記憶體位置相關聯之第二詮釋資料記憶體位置來讀取該第二基元詮釋資料標籤，該第二值係自該第二應用程式記憶體位置所載入。

（29）如（24）至（28）中任一項所述之系統，其中：

對該第一值及該第二值執行之該操作產生第三值；且

該第三值與該複合詮釋資料標籤相關聯。

（30）如（29）所述之系統，其中：

該操作為始終產生預設值作為該第三值之虛設操作。

（31）如（29）所述之系統，其中：

對該第一值及該第二值執行之該操作包含第一操作；

該至少一個處理器進一步經程式化以：

自該應用程式記憶體載入第四值；及

至少部分地藉由對該第三值及該第四值執行第二操作而用該複合詮釋資料標籤來標記該第四值。

（32）如（31）所述之系統，其中：

將該第三值儲存於第一輸入暫存器中；

將該第四值儲存於第二輸入暫存器中；且

對該第三值及該第四值執行之該第二操作致使該第四值被儲存於輸出暫存器中，且致使該輸出暫存器與該複合詮釋資料標籤相關聯。

（33）如（31）至（32）中任一項所述之系統，其中：

該至少一個處理器進一步經程式化以至少部分地藉由將該第四值自該輸出暫存器儲存至該應用程式記憶體中之位址而使該應用程式記憶體中之該位址與該複合詮釋資料標籤相關聯。

（34）一種方法，其由如先前組態中任一項所述之系統來執行。

（35）至少一種電腦可讀取媒體，其上編碼有指令，該等指令在由至少一個處理器執行時致使該至少一個處理器執行如（34）所述之方法。

【0203】 在已因此描述至少一個具體實例之若干態樣後，應瞭解，所屬技術領域中具有知識者將易於想到各種更改、修改及改良。此類更改、修改及改良意欲在本發明之精神及範圍內。因此，前文描述及圖式僅作為實例。

【0204】 本發明之上述具體實例可以任何眾多方式實施。舉例而言，具體實例可使用硬體、軟體或其組合來實施。當以軟體來實施時，軟體程式碼可執行於任何合適的處理器或處理器之集合上，無論提供於單一電腦中還是分配於多個電腦當中。

【0205】 並且，本文中所概述之各種方法或程序可經寫碼為可執行於一或多個處理器上以運行各種作業系統或平台中之任一者之軟體。此類軟體可使用多個合適的程式化語言及/或程式化工具來編寫，包括指令碼處理語言及/或指令碼處理工具中之任一者。在一些情況下，此類軟體可編譯為執行於系統框架或虛擬機器上之可執行機器語言程式碼或中間程式碼。另外或替代地，此類軟體可經解譯。

【0206】 本文所記載技術可實施為編碼有一或多個程式之非暫時性電腦可讀取媒體（或多個電腦可讀取媒體）（例如，電腦記憶體、一或多個軟碟、

CD、光碟、磁帶、快閃記憶體，以場可程式化閘陣列或其他半導體裝置之電路組態或其他非暫時性有形電腦儲存媒體），該一或多個程式在執行於一或多個處理器上時執行實施上文所論述之本發明之各種具體實例之方法。一或多個電腦可讀取媒體可為可傳輸的，使得其上儲存之一或多個程式可載入至一或多個不同電腦或其他處理器上以實施如上文所論述之本發明之各個態樣。

【0207】 術語「程式」或「軟體」在本文中用以指代任何類型之電腦程式碼或電腦可執行指令之集合，其可用於程式化一或多個處理器以實施如上文所論述之本發明之各個態樣。此外，應瞭解，根據此具體實例之一態樣，在被執行時執行本發明之方法的一或多個電腦程式無需駐存於單一電腦或處理器上，但可以模組化方式分配於多個不同電腦或處理器中以實施本發明之各個態樣。

【0208】 電腦可執行指令可呈許多形式，諸如由一或多個電腦或其他裝置執行的程式模組。程式模組可包括執行特定任務或實施特定抽象資料類型的常式、程式、物件、組件、資料結構等。在各種具體實例中，程式模組之功能性可視需要來組合或分配。

【0209】 並且，資料結構可以任何合適之形式儲存於電腦可讀取媒體中。出於說明簡單起見，資料結構可被展示為具有經由資料結構中之位置而相關的欄位。可同樣藉由將用於欄位之儲存裝置指派至電腦可讀取媒體中的在欄位之間傳達關係的位置而實現此類關係。然而，任何合適機制可用於在資料結構之欄位中之資訊之間建立關係，包括經由使用指標、標記或在資料元件之間建立關係之其他機制。

【0210】 本發明之各種特徵及態樣可單獨使用、以兩者或多於兩者之任何組合形式或以前述內容中所描述之具體實例中未特定論述之各種配置來使用，且因此不限於前述描述中所闡述的或圖式中所說明的組件之細節及配置。

舉例而言，一個具體實例中所描述之態樣可以任何方式與其他具體實例中所描述之態樣組合。

【0211】 並且，本文中所記載之技術可實施為方法，已經提供其實例。作為方法之部分所執行之動作可以任何合適的方式來排序。因此，可建構如下具體實例：其中動作以不同於所說明之次序的次序來執行，亦即，可包括同時執行一些動作，即使此等動作在例示具體實例中被展示為依序動作。

【0212】 在申請專利範圍中使用諸如「第一」、「第二」、「第三」等次序術語修飾請求項要素本身並不意謂一個請求項要素相對於另一請求項要素的任何優先順序、優先性或次序或執行方法動作之時間次序，而是僅用作標籤以區分具有某一名稱之一個請求項要素與具有相同名稱（但使用次序術語）之另一要素，以區分該等請求項要素。

【0213】 並且，本文中所使用之措辭及術語係出於描述之目的，且不應被視為限制性的。本文中對「包括」、「包含」、「具有」、「含有」、「涉及」及其變體的使用意謂涵蓋在其後所列出之項目及其等效物以及額外項目。

【符號說明】

【0214】

100：硬體系統

110：主機處理器

112：寫入互鎖

115：系統匯流排

120：應用程式記憶體

125：詮釋資料記憶體

130：唯讀記憶體

135：周邊裝置

140：標記處理硬體

142：標記映射表

144：規則快取記憶體

146：標記暫存器檔案

150：策略處理器

200：軟體系統

205：編譯器

210：連結器

215：載入器

220：策略編譯器

225：策略連結器

230：除錯器

300：策略

305、310、315：區段

400：策略程式碼

405、410：行

500：目標描述

510：硬體實體模組

512：ISA實體模組

514：系統單晶片（SOC）實體模組

520：軟體實體模組

522：OS實體模組

524：使用者應用程式實體模組

526：建置系統實體模組

530：類別實體模組

532：軟體類別實體模組

534：硬體類別實體模組

540：轉換實體模組

600：組合程式碼

605、610、615：標示

620：位址

625：碼字

630：助憶符

635：參數

800：分隔策略

900：策略程式碼

1000：策略程式碼

1100：電腦

1101：處理單元

1102：記憶體

1105：儲存裝置

1106：輸出裝置

1107：輸入裝置

1110：網路介面

1120：網路

201937393

【發明摘要】

【中文發明名稱】 用於安全初始化的策略編輯之系統和方法

【英文發明名稱】 SYSTEMS AND METHODS FOR POLICY COMPILATION FOR SECURE INITIALIZATION

【中文】

本發明提供一種包括至少一個處理器之系統，該至少一個處理器經程式化以將一策略轉譯成策略程式碼，其中：該策略以一策略語言來提供；該策略程式碼呈不同於該策略語言之一程式設計語言；且該策略包括將一實體名稱映射至待與一目標系統中之一實體相關聯之一或多個詮釋資料符號之一陳述式，將對該實體執行該策略。

【英文】

A system including at least one processor programmed to translate a policy into policy code, wherein: the policy is provided in a policy language; the policy code is in a programming language that is different from the policy language; and the policy includes a statement that maps an entity name to one or more metadata symbols to be associated with an entity in a target system against which the policy is to be enforced.

【指定代表圖】 圖2

【代表圖之符號簡單說明】

120：應用程式記憶體

125：詮釋資料記憶體

142：標記映射表

146：標記暫存器檔案

200：軟體系統

205：編譯器

210：連結器

215：載入器

220：策略編譯器

225：策略連結器

230：除錯器

【特徵化學式】

無

【發明申請專利範圍】

【第1項】一種包含至少一個處理器之系統，該至少一個處理器經程式化以：

將策略轉譯成策略程式碼，其中：

該策略以策略語言來提供；

該策略程式碼呈不同於該策略語言之程式設計語言；且

該策略包含將實體名稱映射至待與目標系統中之實體相關聯之一或多個詮釋資料符號之陳述式，將對該實體執行該策略。

【第2項】如請求項1所述之系統，其中：

該至少一個處理器進一步經程式化以將該一或多個詮釋資料符號中之至少一個詮釋資料符號解析成二進位表示；

該至少一個詮釋資料符號之該二進位表示包括於該策略程式碼中。

【第3項】如請求項1所述之系統，其中：

該至少一個處理器進一步經程式化以：

自描述該目標系統之目標描述來識別用以描述該目標系統之該實體之實體描述；及

使用該實體描述以使該一或多個詮釋資料符號與該目標系統之該實體相關聯。

【第4項】如請求項3所述之系統，其中：

該目標描述包含被組織成複數個模組之複數個實體描述。

【第5項】如請求項4所述之系統，其中：

該複數個模組包含對應於該目標系統之指令集架構（ISA）之至少一個指令集架構模組；且

該至少一個ISA模組包含與該目標系統之該指令集架構相關聯之複數個ISA

實體的實體描述。

【第6項】如請求項4所述之系統，其中：

該複數個模組包含對應於該目標系統之硬體晶片設計之至少一個系統單晶片（SOC）模組；且

該至少一個SOC模組包含與該目標系統之該硬體晶片設計相關聯之複數個SOC實體的實體描述。

【第7項】如請求項4所述之系統，其中：

該複數個模組包含對應於該目標系統之作業系統（OS）之至少一個作業系統模組；且

該至少一個OS模組包含與該目標系統之該作業系統相關聯之複數個OS實體的實體描述。

【第8項】如請求項4所述之系統，其中：

該複數個模組包含對應於該目標系統之至少一個使用者應用程式之至少一個使用者應用程式模組；且

該至少一個使用者應用程式模組包含與該目標系統之該至少一個使用者應用程式相關聯之複數個使用者應用程式實體的實體描述。

【第9項】如請求項4所述之系統，其中：

該複數個模組包含至少一個類別模組；

該至少一個類別模組包含至少一個類別實體之實體描述；且

該至少一個類別實體對應於該目標系統中滿足類別之一或多個界定準則之該類別的硬體及/或軟體實體。

【第10項】如請求項9所述之系統，其中：

該至少一個類別實體對應於該目標系統中與執行所選策略相關之一類別的硬體及/或軟體實體。

【第11項】如請求項9所述之系統，其中：

該至少一個處理器進一步經程式化以將該至少一個類別實體闡述成複數個構成實體。

【第12項】如請求項4所述之系統，其中：

該複數個模組包含至少一個轉換模組；

該至少一個轉換模組包含至少一個轉換實體之實體描述；且

該至少一個轉換實體對應於被應用至軟體程式碼之轉換，以促進一或多個策略之執行。

【第13項】如請求項1所述之系統，其中：

該實體名稱具有根據階層式名稱空間之結構；且

該至少一個處理器經程式化以使用該結構來將該實體名稱映射至該一或多個詮釋資料符號。

【第14項】一種包含至少一個處理器之系統，該至少一個處理器經程式化以：

將第一詮釋資料標籤及第二詮釋資料標籤兩者解析成詮釋資料之同一二進位表示，該第二詮釋資料標籤在語法上不同於該第一詮釋資料標籤但在語義上等效於該第一詮釋資料標籤。

【第15項】如請求項14所述之系統，其中：

該第一詮釋資料標籤及該第二詮釋資料標籤係基於同一組的一或多個詮釋資料符號。

【第16項】如請求項14所述之系統，其中：

該至少一個處理器進一步經程式化以：

執行指令而由此獲得執行結果；及

將該執行結果儲存至記憶體位置；

該系統進一步包含策略執行硬體，其經組態以：

回應於接收到該指令藉由該至少一個處理器來執行之指示，評估一或多個規則以判定是否允許該指令，其中該一或多個規則之評估回傳詮釋資料之該二進位表示；

回應於判定允許該指令，判定由該一或多個規則所回傳之詮釋資料之該二進位表示之例項是否已經儲存；

回應於判定詮釋資料之該二進位表示之例項未經儲存：

將詮釋資料之該二進位表示儲存至硬體位置；且

至少部分地藉由儲存自該記憶體位置至儲存有詮釋資料之該二進位表示之該硬體位置的映射，而使詮釋資料之該二進位表示與該記憶體位置相關聯；及

回應於判定詮釋資料之該二進位表示之例項已經儲存：

至少部分地藉由儲存自該記憶體位置至已經儲存有詮釋資料之該二進位表示之硬體位置的映射，而使詮釋資料之該二進位表示與該記憶體位置相關聯。

【第17項】如請求項16所述之系統，其中：

該記憶體位置包含應用程式記憶體中之位置；且

儲存詮釋資料之該二進位表示之該硬體位置包含與該應用程式記憶體實體上分離之詮釋資料記憶體中之位置。

【第18項】如請求項16所述之系統，其中儲存有詮釋資料之該二進位表示之該硬體位置包含策略處理器之暫存器。

【第19項】如請求項16所述之系統，其中儲存有詮釋資料之該二進位表示之該硬體位置包含指令集架構（ISA）組態暫存器。

【第20項】如請求項16所述之系統，其中儲存有詮釋資料之該二進位表示之該硬體位置包含系統單晶片（SOC）組態暫存器。

【第21項】如請求項16所述之系統，其中：

該至少一個處理器經程式化以至少部分地藉由以下操作來判定至少一個二進位表示之例項是否已經儲存：

自該至少一個二進位表示產生雜湊值；及

使用該雜湊值以檢查雜湊表是否包括對應於該至少一個二進位表示之條目。

【第22項】如請求項14所述之系統，其中：

該至少一個處理器進一步經程式化以載入用於執行策略之一段策略程式碼；且

該至少一個詮釋資料標籤係基於該策略程式碼中所指示之至少一個詮釋資料符號。

【第23項】如請求項22所述之系統，其中：

該至少一個處理器包含第一處理器及第二處理器；

該第一處理器經組態以運行一段目標程式碼；且

該第二處理器經組態以運行該段策略程式碼。

【第24項】一種包含至少一個處理器之系統，該至少一個處理器經程式化以：

自應用程式記憶體載入第一值，其中該第一值與至少一個第一基元詮釋資料標籤相關聯；

自該應用程式記憶體載入第二值，其中該第二值與至少一個第二基元詮釋資料標籤相關聯；及

至少部分地藉由對該第一值及該第二值執行操作而將該至少一個第一基元詮釋資料標籤及該至少一個第二基元詮釋資料標籤組合成複合詮釋資料標籤。

【第25項】如請求項24所述之系統，其中：

該至少一個處理器進一步經程式化以將該應用程式記憶體之區域分配用於創建複合詮釋資料標籤；且

自該應用程式記憶體之該區域載入該第一值與該第二值。

【第26項】如請求項25所述之系統，其中：

該第一值與該第二值相同。

【第27項】如請求項24所述之系統，其進一步包含策略執行硬體，其中：

對該第一值及該第二值執行之該操作致使該策略執行硬體評估一或多個規則；且

該一或多個規則之評估致使該策略執行硬體以將該至少一個第一基元詮釋資料標籤及該至少一個第二基元詮釋資料標籤組合成該複合詮釋資料標籤。

【第28項】如請求項27所述之系統，其中：

載入該第一值致使該策略執行硬體自與第一應用程式記憶體位置相關聯之第一詮釋資料記憶體位置來讀取該至少一個第一基元詮釋資料標籤，該第一值係自該第一應用程式記憶體位置所載入；且

載入該第二值致使該策略執行硬體自與一第二應用程式記憶體位置相關聯之第二詮釋資料記憶體位置來讀取該至少一個第二基元詮釋資料標籤，該第二值係自該第二應用程式記憶體位置所載入。

【第29項】如請求項24所述之系統，其中：

對該第一值及該第二值執行之該操作產生第三值；且

該第三值與該複合詮釋資料標籤相關聯。

【第30項】如請求項29所述之系統，其中：

該操作為始終產生預設值作為該第三值之虛設操作。

【第31項】如請求項29所述之系統，其中：

對該第一值及該第二值執行之該操作包含第一操作；

該至少一個處理器進一步經程式化以：

自該應用程式記憶體載入第四值；及

至少部分地藉由對該第三值及該第四值執行第二操作而用該複合詮釋資料標籤來標記該第四值。

【第32項】如請求項31所述之系統，其中：

將該第三值儲存於第一輸入暫存器中；

將該第四值儲存於第二輸入暫存器中；且

對該第三值及該第四值執行之該第二操作致使該第四值被儲存於輸出暫存器中，且致使該輸出暫存器與該複合詮釋資料標籤相關聯。

【第33項】如請求項32所述之系統，其中：

該至少一個處理器進一步經程式化以至少部分地藉由將該第四值自該輸出暫存器儲存至該應用程式記憶體中之位址，而使該應用程式記憶體中之該位址與該複合詮釋資料標籤相關聯。

【第34項】一種方法，其由如請求項1-33中任一項所述之系統來執行。

【第35項】至少一種電腦可讀取媒體，其上編碼有指令，該等指令在由至少一個處理器執行時致使該至少一個處理器執行如請求項34所述之方法。