I470625

(19)中華民國智慧財產局

(12)發明說明書公告本 **(11)證書號數：TW I470625 B**

(45)公告日： 中華民國 104 (2015) 年 01 月 21 日

(21)申請案號：101128038 (22)申請日： 中華民國 95 (2006) 年 02 月 14 日

(51)Int. Cl.： *G11B20/10 (2006.01)* *G06F21/00 (2013.01)*

(30)優先權：2005/02/14 日本 2005-036621

(71)申請人：松下電器產業股份有限公司 (日本) PANASONIC CORPORATION (JP)
日本

(72)發明人：列區杉寧 葛蔓諾 LEICHSENRING, GERMANO (BR)；金丸智一 KANAMARU, TOMOKAZU (JP)

(74)代理人：惲軼群；陳文郎

(56)參考文獻：

TW 200412579A JP 2004-302973A

US 6584495B1

審查人員：林坤隆

申請專利範圍項數：2 項 圖式數：18 共 72 頁

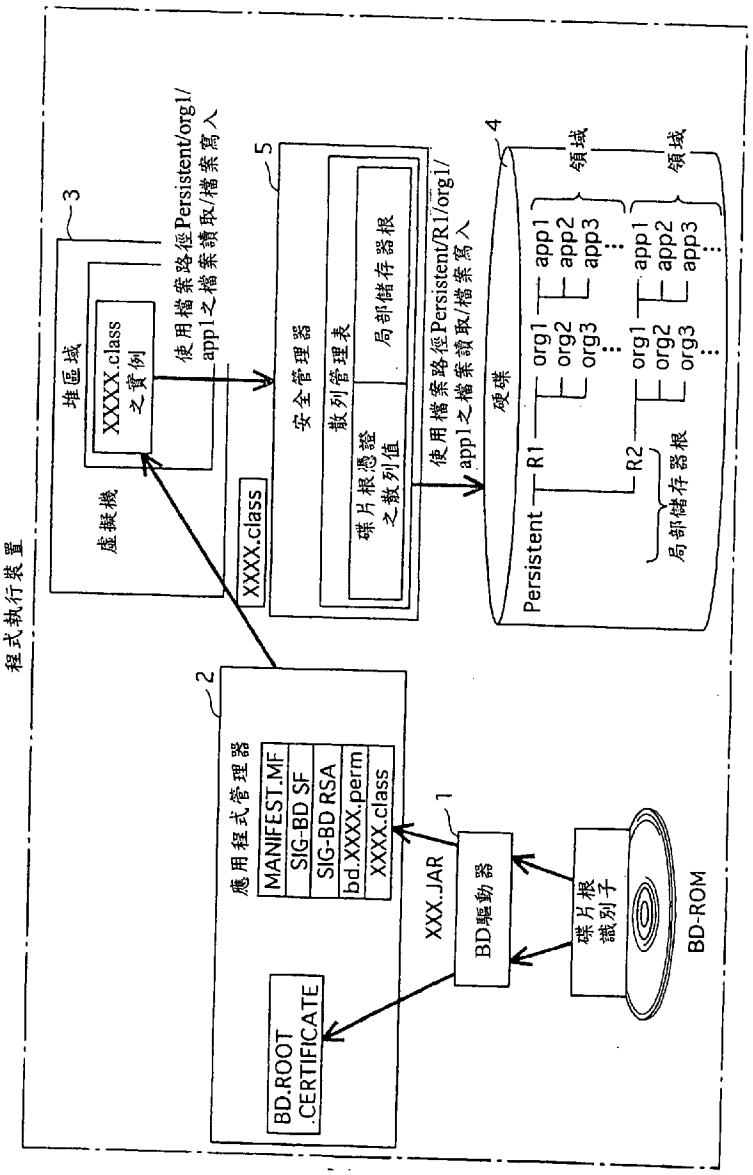
(54)名稱

應用程式執行裝置、應用程式執行方法

(57)摘要

於 BD-ROM 記錄碟片根憑證，且該碟片根憑證係將從根憑證機構頒布之根憑證分配該媒體者。又，應用程式管理器從碟片根憑證取得散列值，使用該散列值，判定應用程式之正當性。當判定為正當時，虛擬機便執行應用程式。局部儲存器具有複數領域，安全管理器將存在於局部儲存器之複數領域中對應所取得之散列者分配至應用程式。

第 6 圖



1・・・BD 驅動器

2・・・應用程式管理器

3・・・虛擬機

4・・・硬碟

5・・・安全管理器

I470625

第101128038號申請案 修正替換 102.2.7

公告本

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： 101128038

※ 申請日期： 95.2.14 ※IPC 分類： G11B 20/10 (2006.01)
G06F 21/00 (2013.01)

原申請案號： 95104913

一、發明名稱：（中文/英文）

應用程式執行裝置、應用程式執行方法

二、中文發明摘要：

於BD-ROM記錄碟片根憑證，且該碟片根憑證係將從根憑證機構頒布之根憑證分配該媒體者。又，應用程式管理器從碟片根憑證取得散列值，使用該散列值，判定應用程式之正當性。當判定為正當時，虛擬機便執行應用程式。局部儲存器具有複數領域，安全管理器將存在於局部儲存器之複數領域中對應所取得之散列者分配至應用程式。

三、英文發明摘要：

四、指定代表圖：

(一)本案指定代表圖為：第（ 6 ）圖。

(二)本代表圖之元件符號簡單說明：

1…BD驅動器
2…應用程式管理器
3…虛擬機
4…硬碟
5…安全管理器

五、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

六、發明說明：

【發明所屬之技術領域】

發明領域

本發明係有關於一種屬於對應用程式之資源分配技術領域者。

【先前技術】

發明背景

資源分配技術係指一種屬於將具有平台之記憶裝置(局部儲存器)內之區域作為資源分配給應用程式之技術的發明。為有系統管理從世界各組織提供之各種應用程式，歐洲方面之數位傳送接收裝置之MHP(Multimedia Home Platform)規定局部儲存器之目錄構造而可在如下述之統一樣式之檔案路徑存取。

檔案路徑：Root/組織ID/appID

在此，組織ID係指將作為應用程式之供給來源之組織顯示為同義之識別子，appID係將應用程式顯示為同義之識別子。

實現以上之區域分配時，作為MHP之機器使用根憑證，判定應用程式之正當性。以下，就在機器(MHP)進行之應用程式正當性檢查及對應用程式之區域分配作說明。

製作應用程式之製作者將應用程式交接給機器時，除了將根憑證附加於應用程式外，亦將應用程式傳送至機器。此根憑證為與分配至機器固有之根憑證相同者，機器接收附加了根憑證之應用程式，以判定附加於此應用程式

之根憑證與分配至機器之根憑證之相同性。若有相同性時，便將對應該應用程式供給來源之組織的組織用目錄分配給該應用程式，使應用程式進行該目錄內之檔案之存取。

適當控制應用程式之存取權限之技術記載於非專利文獻1。

非專利文獻1：「JAVA(註冊商標)Security」Scott Oaks著，O'Reilly發行，May 2001，ISBN 0-596-00157

然而，在上述習知技術中，設置對應應用程式供給來源之組織之區域，將對應該組織之目錄下之區域分配至要求存取之應用程式。因此，應用程式執行裝置分發至世界各地，從世界各組織提供應用程式時，需世界各組織之組織ID不重複之線索。這是因為若不如此，屬於某組織之應用程式便可自由存取供其他組織用之目錄，而無法保護應用程式利用之資料之機密性。由於需要此線索，故世界各組織便需要分配唯一之組織ID之第3者機關，參與應用執行裝置之標準化之製造者必須對此機關之設立經營確保資本或人材。這對參與應用程式執行裝置標準化之製造者造成極大之負擔。然而，一旦其他組織可自由存取供自身組織用之目錄時，便產生自身組織之應用程式用之資料為其他組織盜用、任意使用之可能性。在裝置方面，若放任此種非法行為，便經常發生製作應用程式之製作者猶豫對裝置提供應用程式之情形。如此一來，便無法期待在裝置運作之應用程式之充實化，而有因應用程式之不足，而封閉應用程式執行裝置普及之路之虞。

又，在MHP中，將分配給裝置之根憑證用於應用程式之正當性判定。當分配至裝置之根憑證為不懷好意者揭露時，分配給機器之數位憑證為製造之製造源更新為最新者。當有此數位憑證之更新時，附加有舊憑證之應用程式便無法正確判斷正當性，而不充許局部儲存器存取。當然，如在MHP利用之應用程式般，若應用程式為僅於播放時利用即可之一次性者，由於不斷傳送新之應用程式，故此種處理或許便已足夠。然而，若應用程式進行有關於DVD-Video內容、BD-ROM內容等有關於記錄於碟片之電影作品之處理時，需不斷再生舊電影作品時，亦要求進行有關該電影作品之處理之應用程式正確進行動作。因此，因數位憑證之更新，而導致應用程式無法動作是決不希望發生。即，習知技術有根憑證揭露時，動作保障不徹底之問題。

【發明內容】

發明概要

本發明第1目的在於提供一種即使不需以世界性標準進行不產生重複之組織ID之管理，亦可提高為從各組織供給之應用程式所利用之檔案之機密性的應用程式執行裝置。

本發明第2目的在於提供一種即使根憑證揭露時，亦可實現高標準之動作保障之應用程式執行裝置。

為達成上述第1、第2目的，本發明應用程式執行裝置係從記錄有碟片根憑證及應用程式之碟片媒體讀取應用程

式，以執行者，該碟片根憑證係該碟片媒體之製作者將由根憑證機構頒布之根憑證分配給該碟片媒體者，該應用程式執行裝置具有從碟片根憑證取得散列值，使用該散列值，判定應用程式之正當性之管理機構、當管理機構判定為正當時，執行應用程式之執行機構、具有複數領域之記憶機構及將對應存在於記憶機構內之複數領域中取得之散列值者分配給應用程式者。

由於本發明應用程式執行裝置具有上述技術項事項(1)，故於局部儲存器內部存在複數領域，將各領域分配至根憑證之各散列值。且該等領域下，依各組織作成各應用程式之區域時，在世界性標準組織不為唯一亦可。在稱為“領域”之封閉世界中，由於可區別複數領織便足夠，故不需使組織ID在世界性標準為唯一之值，而不需第3者機關所作之管理。即使不進行組織ID不重複之管理，亦可在1個平台使從世界中組織提供之應用程式動作，且提高作為應用程式之讀取/寫入對象之檔案之機密性。

即使不需第3者機關之管理，亦可去除使製作業者猶豫是否提供應用程式之障壁，而提高應用程式利用之檔案之獨立性、機密性，故可對電影製作者、電影發行者、播放機構、出版者、計算機軟體開發公司等呼籲提供應用程式執行裝置用應用程式。藉此，可謀求應用程式之豐富化，而可充實裝置用應用程式，而對作為碟片媒體再生裝置之應用程式執行裝置之普及更有助益。

又，根憑證是分配給記憶機構內之領域而非裝置本

體。對某一碟片媒體提供之應用程式若對應該碟片媒體之碟片根憑證時，只要該碟片媒體裝設於應用程式執行裝置，必可保障運作。當然並非碟片根憑證無揭露之可能性，此時，使該碟片媒體無法使用或僅更新該碟片媒體之碟片根憑證即可，而對其他碟片提供之應用程式如前述使用碟片根憑證即可，故可實現確實之動作保障。

如此，不需以世界性標準管理組織ID，且可將以往之各應用程式之保障維持在高標準，故本發明之應用程式執行裝置對執行有關電影作品之處理之應用程式之應用程式執行裝置的世界性標準化有極大之助益。

又，任意於上述應用執行裝置之技術性事項(1)增加以下之技術性事項(2)(3)~，使應用程式執行裝置為具體之結構，可更發揮效果。在本申請案中，將該等技術性事項區分為申請專利範圍第1項以下之附屬形式而記載。

技術性事項(2)於碟片媒體記錄第1數位憑證鏈，前述管理機構所作之正當性判定包含檢查從前述第1數位憑證鏈中之根憑證所取得之散列值與從前述碟片根憑證中所取得之散列值是否一致，前述領域具有複數組織區域，前述分配機構所作之分配包含當散列值一致時，允許應用程式利用應用程式所分配之領域中之複數組織區域中對應記載於第1數位憑證鏈中之葉憑證的組織ID。

當於應用程執行裝置附加上述技術性事項時，便可利用使用習知憑證機構之商業模組，而無法非法利用第1應用程式分配至第2應用程式之資源。此非法利用之防止藉複數

組織共用相同之碟片根憑證而進行，而無將根憑證保持於應用程式內之情形，故可維持將應用程式執行裝置之憑證更新時之動作互換。

技術性事項(3)作為前述應用程式之供給來源之組織接受從其他組織提供區域利用之權限，前述碟片媒體更記錄有具有顯示作為區域利用權限之提供者之組織的提供者組織ID及顯示作為區域利用權限之接受者之組織之接受者組織ID的身份碼資訊，前述管理機構更進行前述資訊之正當性之確認，前述分配機構所作之分配包含當確認前述資訊之正當性時，允許應用程式利用分配至應用程式之領域中之複數組織區域中對應提供者組織ID者。

技術性事項(4)為前述身份碼資訊具有從提供者組織固有之根憑證取得之散列值及接受者組織固有之根憑證取得之散列值，前述管理機構所作之身份碼資訊之正當性判定包含檢查從碟片根憑證取得之散列值與從接受者組織固有之根憑證取得之散列值是否一致及檢查記載於前述第1數位憑證鏈中之葉憑證之組織ID與身份碼資訊所示之接受者組織ID是否一致。

若於應用程式執行裝置附加上述技術性事項時，對應用程式執行裝置重複進行各種碟片媒體之裝設、退出，於該等複數碟片媒體分配各碟片根1憑證時，當對應各應用程式之碟片根憑證不同時，記錄於某一記錄媒體之第1應用程式亦可存取分配至記錄於其他媒體之第2應用程式之領域。如此，應用程式記錄於各碟片媒體，當所分配之碟片

根憑證不同時，應用程式可共有複數領域。藉此，可提高製作者相互間之連帶關係、協調性。

技術性事項(5)為於前述碟片媒體記錄有第2數位憑證鏈，前述管理機構所作之身份碼資訊之正當性判定包含從前述第2數位憑證鏈中之根憑證取得散列值，檢查該散列值與從前述提供者組織固有之根憑證取得之散列值是否一致及檢查記載於前述第2數位憑證中之葉憑證之組織ID與提供者組織ID是否一致。

當於應用程式執行裝置附加上述技術性事項時，可防止身份碼資訊之竄改，且當身份碼無資訊時，便無法至供其他應用程式用之領域進行存取，故可防止非法之存取。

技術性事項(6)前述身份碼資訊具有檔案列表，前述分配機構所作之組織區域之利用允許包含於前述應用程式存取存在於組織區域下存在之檔案中顯示於檔案列表者。

若於應用程式執行裝置附加上述技術性事項時，可以細小粒度進行資訊之存取，而可抑制應用程式之不妥造成之資料之破壞風險。

技術性事項(7)前述身份碼資訊更具有顯示檔案之存取方法之存取資訊，前述分配機構所作之組織區域利用允許包含使前述應用程式以存取資訊所示之存取方法存取存在於組織區域下之檔案中顯示於檔案列表者。

當於應用程式執行裝置附加上述技術性事項時，即使有使用資訊之應用程式之存取時，亦可抑制應用程式之不妥造成之資料之破壞風險。

技術性事項(8)於碟片媒體記錄有第1數位憑證鏈，前述管理機構所作之正當性判定包含檢查從前述第1數位憑證鏈內之根憑證取得之散列值與從前述碟片根憑證取得之散列值是否一致，前述執行機構所作之應用程式之執行於散列值一致時進行。

當於應用程式執行裝置附加上述技術性事項時，可防止濫用過程間通信(Interprocess Communication、IPC)之攻擊，而使安全性提高。

圖式簡單說明

第1(a)圖係顯示BD-ROM之檔案、目錄結構者。

第1(b)圖係顯示Java(TM)歸檔檔案302中之構造之一例者。

第2(a)圖係顯示Credential之資料構造之一例者。

第2(b)圖係顯示Credential之具體一例者。

第3(a)圖係例示顯示在BD-ROM中，根憑證如何分配者。

第3(b)圖係例示顯示在MHP中，根憑證如何分配者。

第4圖係顯示無權限提供時之SIG-BD.RSA、SIB-BD.SF、BD.ROOT.CERTIFICATE、MANIFEST.MF之相互關係者。

第5圖係顯示無權限提供時之SIG-BD.RSA、SIB-BD.SF、BD.ROOT.CERTIFICATE、MANIFEST.MF、bd.XXXX.perm之相互關係者。

第6圖係顯示本實施形態之應用程式執行裝置之機能

結構之塊圖者。

第7圖係顯示應用程式管理器2所作之Java(TM)歸檔檔案302內之類別檔案之應用程式的啟動程序之流程圖。

第8圖係顯示應用程式管理器2所作之Credential之簽章認證程序之流程圖。

第9圖係顯示應用程式管理器2保持之管理資訊之一例者。

第10圖係顯示應用程式管理器2保持之管理資訊之一例者。

第11圖係顯示Java(TM)應用程式利用硬碟4時之處理程序之流程圖。

第12圖係顯示安全管理器5所作之局部儲存器名稱之取得程序詳細內容之流程圖。

第13圖係顯示安全管理器5保持之散列管理表之一例者。

第14圖係顯示安全管理器5之組織ID之取得函數之詳細內容的流程圖。

第15圖係顯示安全管理器5之檔案讀取函數之詳細內容之流程圖。

第16圖係顯示安全管理器5之檔案讀取函數之詳細內容之流程圖。

第17圖係顯示安全管理器5之檔案寫入函數之詳細內容之流程圖。

第18圖係顯示安全管理器5之檔案寫入函數之詳細內

容之流程圖。

【實施方式】

用以實施發明之最佳形態

以下，參照圖式，說明本發明之實施形態

(第1實施形態)

以下，就本發明應用程式執行裝置之實施形態作說明。首先，針對應用程式執行裝置，就提供應用程式之記錄媒體作說明。在本實施形態中，此記錄媒體選擇BD-ROM為題材。這是由於BD-ROM之應用程式進行有關上述之電影作品之處理。第1(a)圖係顯示BD-ROM之檔案、目錄構造者。於本圖之第1段顯示BD-ROM。BD-ROM與DVD或CD等其他光碟同樣地具有從內周往外周呈螺旋狀之記錄區域。第2段顯示此記錄區域。如第2段所示，記錄區域具有於內周之「讀入區域」及外周之「讀出區域」間可記錄邏輯資料之「邏輯位址空間」。又，於讀入內側有稱為BCA(Burst Cutting Area)之僅可以驅動器讀取之特別區域。由於此區域無法從應用程式讀取，故經常用於著作權保護技術等。

「邏輯位址空間」記錄有以檔案系統資料(容量)為前頭之影像資料、含有檔案及其相關資料之Java(TM)歸檔檔案302等資料。檔案系統係指UDF(Universal Disk Format)或ISO9660等，可使用目錄、檔案構造讀取如一般之個人電腦同樣地記錄之邏輯資料。第3段顯示BD-ROM之目錄、檔案構造。此目錄、檔案構造係在根目錄(ROOT)之下，置放

BDDATA目錄者。於目錄BDDATA記錄以下之2種檔案。

(A)BD.ROOT.CERTIFICATE：碟片根憑證301

碟片根憑證301係指製作此BD-ROM之製作者將從根憑證機構頒佈之根憑證分配給BD-ROM者。碟片根憑證301為以諸如X.509之形式標號。X.509之規格由國際電信電話諮詢委員會發行，記載於CCITT Recommendation X.509 (1988),"The Directory-Authentication Framework"。將此根憑證記錄於可搬型記錄媒體使根憑證曝露之可能性高，在DVD中，此分配因有根憑證曝露之危險性而未導入。然而，於BD-ROM採用較DVD更高度之著作權保護技術，此著作權保護技術之採用係趁"於BD-ROM分配固有之根憑證"之想法導入之便。BD-ROM之碟片根憑證301之導入應留意有以上之背景。

(B)XXX.JAR：Java(TM)歸檔檔案302

此以記載於http：//java(TM).sun.com/j2se/1.4.2/docs/guide/jar/jar.html之規格為準。Java(TM)歸檔檔案302係將ZIP檔案形式特別化成Java(TM)者，可藉市面販售之ZIP展開軟體確認其內容。在此，「XXX」為可變，擴張子「JAR」為固定。

Java(TM)歸檔檔案302將複數檔案以目錄構造之形式儲存。第1(b)圖係顯示Java(TM)歸檔檔案302中之構造之一例者。

此構造係於根目錄下存在XXXX.class，於META-INF目錄存在檔案NAINFEST.MF、檔案SIG-BD.SF、檔案

SIG-BD.RSA、檔案bd.XXXX.perm者。以下，將就該等檔案個別說明。

(i)XXXX.class：類別檔案401

類別檔案401係儲存有定義可在虛擬機上執行之Java(TM)應用程式之構造體之類別檔案401。

以此類別檔案401定義之Java(TM)應用程式為經由Xlet介面，藉應用程式執行裝置之應用程式管理器控制之Java(TM)xlet。Xlet介面具有稱為“loaded”、“paused”、“active”、“destroyed”之4個狀態。

(ii)MANIFEST.MF：清單檔案402

清單檔案402係對應數位憑證者，其為記載Java(TM)歸檔檔案302之屬性、Java(TM)歸檔檔案302內之類別檔案401及資料檔案之散列值者。Java(TM)歸檔檔案302之屬性有作為類別檔案401之實例而給予Java(TM)應用程式之應用程式ID、為執行Java(TM)302而應最先執行之類別檔案401名稱。當上述2個Java(TM)歸檔檔案302之屬性不存在時，不執行為Java(TM)歸檔檔案302中之類別檔案401。

(iii)SIG-BD.SF：簽章檔案403

簽章檔案403係記載清單檔案402之散列值之檔案。

(iv)SIG-BD.RSA：數位簽章檔案404

數位簽章檔案404係記載「數位憑證鏈」、簽章檔案403之「簽章資訊」之檔案。

對簽章檔案403之「簽章資訊」係藉對檔案403施行簽章處理而得。該等簽章處理使用對應數位簽章檔案404內之

數位憑證鏈之公鑰的私鑰。

「數位憑證鏈」係指具有第1個憑證(根憑證)簽署第2個憑證，同樣地第n個憑證簽署第n+1個憑證之形式之複數憑證群。將數位憑證鏈之最後憑證稱為「葉憑證」。藉利用此結構，從根憑證依序保障下個憑證，而可保障至數位憑證鏈之最後一個憑證。

「根憑證」儲存與存在於BD.ROOT.CERTIFICATE檔案之碟片根憑證301相同之憑證。

「葉憑證」記載有組織ID。簽章檔案403以PKCS#7之形式儲存。PKCS#7為儲存簽章及1個以上之數位憑證之檔案形式，記載於由IETF(Internet Engineering Task Force)發行之RFC2315。RFC2315可從http：//www.ietf.org/rfc/rfc2315.txt參考。

通常此數位憑證鏈為1個，而當有後述之權限提供時，此數位憑證鏈便製作2個。將該2個數位憑證鏈稱為第1數位憑證鏈、第2數位憑證鏈。第1數位憑證鏈之根憑證顯示接受權限提供之組織之碟片根憑證，葉憑證顯示接受權限提供之組織之組織ID。第2數位憑證鏈之根憑證顯示提供權限之組織之碟片根憑證，葉憑證顯示提供權限之組織之組織ID。另一方面，當無權限之提供時，數位憑證鏈僅為1個(第1數位憑證鏈)。

清單檔案402、簽章檔案403、數位簽章檔案404之詳細內容記載於Java(TM)歸檔檔案之規格。清單檔案402、簽章檔案403、數位簽章檔案404利用於進行簽章處理及簽章認

證處理。最後，可以數位憑證簽署作為Java(TM)歸檔檔案302中之類檔案401之實例的Java(TM)應用程式或允許請求檔案405。之後，將清單檔案402、簽章檔案403、數位簽章檔案404總稱為「數位憑證之簽章」。

(v)bd.XXXX.perm：允許請求檔案405

允許請求檔案405為儲存應將哪個允許給予將執行之Java(TM)應用程式之資訊之檔案。具體為儲存以下之資訊。

(A)Credential(數位信用憑證)

(B)過程間通信之允計資訊

之後，就(A)Credential作說明。"Credential"係指用以將屬於某一組織之組織目錄內之檔案共有化之資訊。此共有化係藉將利用屬於某一組織之應用程式用檔案提供給屬於其他組織之應用程式。因此，Credential包含顯示提供權限之組織之提供者組織ID及顯示接受權限之組織識別之接受者組織ID。

第2(a)圖顯示Credential之資料構造之一例。Credential由從根憑證機構頒佈給提供者組織之根憑證之散列值501、分配給提供者組織之提供者組織ID502、從根憑證機構頒佈給接受者之接受者根憑證之散列值503，分配給接受者組織之接受者組織ID504、接受者應用程式ID505及提供檔案列表506構成。提供檔案列表506儲存1個以上之提供檔案名稱507及存取方法508(可讀取、可寫入)之資訊。為使Credential有效，而必須簽章。Credential之簽章可與數位簽章檔案404同樣地使用PKCS#7之方式。

第2(b)圖顯示Credential具體一例者。本圖之Credential係對檔案「4/5/scores.txt」給予讀取允許，對檔案「4/5/etc/settings.txt」藉Credential給予讀寫允許。

接著，就(B)過程間通信之允許資訊作說明。1個Java(TM)歸檔檔案302所含之Java(TM)應用程式通常不允許與其他Java(TM)歸檔檔案302所含之Java(TM)應用程式之通信(過程間通信)。僅於給予允許請求檔案405過程間通信之允許時，方可進行過程間通信。

以上為關於允許請求檔案405之說明。接著，就根憑證更詳細說明。

第3(a)圖為例示顯示在BD-ROM，根憑證如何分配者。本圖之第3段顯示機器(應用程式執行裝置)及裝設於該機器之BD-ROM，第2段顯示製作該等機器及BD-ROM之業者(BD-ROM之製作者、機器之製造業者)。第1段顯示管理根憑證之根憑證機構。

在本圖中，BD-ROM之製作者從根憑證機構接受根憑證之頒布(f1)，將所頒布之根憑證作為碟片根憑證301而分配給BD-ROM，且將該根憑證儲存於BD.ROOT.CERTIFICATE後，寫入BD-ROM(w1)。另一方面，製作Java(TM)歸檔檔案302時，將該根憑證及顯示組織ID之葉憑證收錄於SIG-BD.SF，而包含於Java(TM)歸檔檔案302內。

雖不為本發明實施形態之說明，但為進行對比，而就MHP之根憑證之分配作說明。

第3(b)圖係顯示在MHP中，根憑證如何分配者。在MHP中，製造機器之製造業者從根憑證機構接受根憑證之頒布(f2)，該製造業者將該根憑證分配給機器(w2)。另一方面，播放內容之製作業者將該根憑證及顯示自身組織ID之葉憑證添附於定義應用程式之類別檔案，且送入機器。比較該等圖式可知在MHP中，將分配至機器之根憑證分配給BD-ROM，從分配至該BD-ROM之根憑證形成憑證鏈。

Java(TM)檔案302不是從BD-ROM而是從WWW伺服器下載，而寫入應用程式執行裝置內之記憶裝置之情形亦相同。此下載以記錄於BD-ROM之內容之更新為目的，在此下載中，使與收錄於BD.ROOT.CERTIFICATE而以碟片根憑證301寫入之根憑證具同一性之根憑證儲存於BD-ROM而包含於Java(TM)歸檔檔案。如此進行，將以記錄於BD-ROM之內容更新為目的之Java(TM)歸檔檔案302以下載供給應用程式執行裝置時，亦藉使用分配至BD-ROM之碟片根憑證301，使應用程式執行裝置確認Java(TM)歸檔檔案302之正當性。

第4圖係顯示無權限提供時之SIG-BD.RSA、SIB-BD.SF、BD.ROOT.CERTIFICATE、MANIFEST.MF之相互關係者。本圖之箭號d1係顯示該等檔案內部構成之資訊要件中具同一性者。無權限之提供時，BD.ROOT.CERTIFICATE內之根憑證(碟片根憑證301)為與SDG-BD.RSA之第1數位憑證鏈內之根憑證具同一性者。

MANIFEST.MF簽署類別檔案XXXX.class，SIG-BD.SF

包含從MAINFEST.MF算出之散列值，SIG-BD.RSA包含從SIG-BD.SF算出之散列值(箭號h1)，藉確認該等簽章是否正確，判定該等圖所示之同一性，應用程式執行裝置可判斷Java(TM)歸檔檔案302是否正當或為加以竄改者。由於為無權限提供之假設，故在本圖中，顯示bd.XXXX.perm。

第5圖係顯示無權限提供時之SIG-BD.RSA、SIB-BD.SF、BD.ROOT.CERTIFICATE、MANIFEST.MF、bd.XXXX.perm之相互關係者。本圖之箭號d1~d6顯示該等檔案內部構造之資訊要件中具同一性者。當有權限之提供時，BD-.ROOT.CERTIFICATE內之根憑證(碟片根憑證)為與SDG-BD.RSA之第1數位憑證鏈內之根憑證具同一性者(箭號d1)。另一方面，當有權限之提供時，由於BD.ROOT.CERTIFICATE內之碟片根憑證301為接受者所有，故bd.XXXX.perm之Credential之接受者憑證與BD.ROOT.CERTIFICATE內之根憑證具有同一性(箭號d2)。又，Credential之接受者組織ID與第1數位憑證鏈之葉之組織ID具同一性(箭號d3)。

bd.XXXX.perm之Credential之提供者組織之根憑證與SIG-BD.RSA內之第2數位憑證鏈之根憑證具同一性(箭號d4)。又，Credential之提供者組織ID與SIG-BD.RSA之第2數位憑證鏈之葉之組織ID具同一性(箭號d5)。Credential之接受者應用程式ID與在bd.XXXX.perm中存在於Credential以外之部份之應用程式ID具同一性(箭號d6)。

MAINFEST.MF包含從類別檔案XXXX.class算出之散

列值，SIG-BD.SF包含從MAINFEST.MF算出之散列值，SIG-BD.RSA包含從SIG-BD.SF取得之散列值(箭號h1)，藉確認該等簽章是否正確，判定該等圖所示之同一性，應用程式執行裝置可判斷Java(TM)歸檔檔案302是否正當或為加以竄改者。雖預先判斷，但在本實施形態中，將根憑證之同一性與對該等根憑證算出之散列值加以比較，判斷該等散列值是否一致。散列值之算出進行一次即可，將所算出者記憶於記憶體等而加以利用為一般所進行者。從根憑證算出散列值或取出儲存於記憶體之散列值稱為散列值之「取得」。

以上為有關BD-ROM之說明。接著，就本發明應用程式執行裝置之內部結構作說明。

本實施形態之應用程式執行裝置於具備CPU、ROM、RAM、硬碟驅動器、BD-ROM驅動器、AV解碼器、輸入輸出機器等之電腦系統將安裝Java(TM)2Micro_Edition(J2ME)Personal Basis Profile(PBP1.0)及Globally Executable MHP specification(GEM1.0.2)for package media targets全部安裝，而構成Java(TM)平台，藉於此Java(TM)平台設置以下所示之機能性構成要件，而可工業化生產。

第6圖係顯示本實施形態之應用程式執行裝置之機能結構之塊圖者。應用程式執行裝置以BD驅動器1、應用程式管理器2、虛擬機3、硬碟4、安全管理器5構成。

(BD驅動器1)

BD驅動器1進行BD-ROM之載入/卸除，以執行

BD-ROM內之資料存取。於BD-ROM驅動器1載入/卸除BD-ROM時，BD驅動器1將此主旨通知應用程式管理器2。

(應用程式管理器2)

應用程式管理器2為在虛擬機3內之堆區域內動作之系統應用程式，以執行應用程式發信。“應用程式發信”係指在GEM1.0.2規定之MHP(Multimedei Home Platform)中，以“服務”為生存區間而進行應用程式之啟動、執行之控制。本實施形態之應用程式管理器2以BD-ROM之“標題”取代此“服務”作為生存區域，實現應用程式之啟動、執行之控制。在此，“標題”為記錄於BD-ROM之影像、聲音資料之再生單位，而同義地分配於應用程式管理表(AMT)。

當使應用程式啟動時，應用程式管理器2判定將啟動之應用程式是否為正當者。此判定程式如下述。若BD-ROM載入時，確認稱為/BDDATA/BD.ROOT.CERTIFICATE之檔案之存在。當檔案存在時，應用程式管理器2從BD-ROM讀取該碟片根憑證301，將之保持於記憶體。之後，讀取Java(TM)歸檔檔案302，認證存在於此Java(TM)歸檔檔案302之簽章。若此認證正確，應用程式管理器2便於虛擬機3內讀取存在於BD-ROM上之Java(TM)歸檔檔案302中之類別檔案401，於堆區域生成此類別檔案401之實例，以啟動Java(TM)應用程式。

(虛擬機3)

虛擬機3為由從BD-ROM讀取類別檔案之使用者類別載入器、將對應類別檔案之實例作為Java(TM)應用程式儲

存之堆記憶體、執行緒、Java(TM)堆疊(stack)構成之Java(TM)應用程式之執行主體。在此，執行緒為執行Java(TM)應用程式之方法(method)之邏輯執行主體，令局部變數或儲存於運算元堆疊之引數為運算元而進行運算，將運算結果儲存為局部變數或運算元堆疊。執行緒所作之方法執行係藉將構成方法之位元組碼轉換為CPU之本機碼後，並於CPU發行而進行。有關此本機碼轉換由於脫離本案之著眼點，故省略說明。若Java(TM)歸檔檔案302內存在允許請求檔案405時，必須於清單檔案402中代入Java(TM)應用程式之正確之散列值，方可執行該Java(TM)應用程式。為判定該散列值，虛擬機3將顯示將執行之Java(TM)應用程式儲存於哪個Java(TM)歸檔檔案302之資訊保持於記憶體上。藉參照該允許請求檔案405，虛擬機3確認應用程式管理器2保持之過程間通信之允許，對Java(TM)應用程式提供過程間通信之機能。

(硬碟4)

硬碟4為藉使用來自Java(TM)IO Package之方法，而可存取之局部儲存器。此局部儲存器具有多數領域。在此，領域係指對應各碟片根憑證301之目錄(圖中之R1、R2)，於該等目錄下，儲存各組織之目錄(圖中之org1、org2、org3)。組織之每一應用程式之目錄(圖中之org1/app1,org1/app2,org1/app3...)為與MHP相同者。即，在局部儲存器中，為將規定於MHP之各組織之每一應用程式之目錄(圖中之org1/app1,org1/app2,org1/app3...)配置於對

應根憑證之目錄(圖中之R1、R2)下的結構。如此進行，可與MHP之儲存方式維持互換。在此，用以存取之局部儲存器之目錄構造之檔案路徑中，至對應根憑證之部份為止(圖中之Root/R1,ROOt/R2)稱為“局部儲存器根”。

(安全管理器5)

安全管理器5保持顯示複數從根憑證算出之散列值與區部儲存器路徑之組合之散列管理表，當從應用程式要求檔案之讀取/寫入時，就對應要求端之根憑證算出散列值，從散列管理表選擇對應如此算出之散列值之局部儲存器根。將如此算出之局部儲存器根編入檔案路徑。又，依Credential，置換對應檔案路徑之組織ID之目錄。如此，應用程式之檔案路徑之記述可保持與MHP規定者互換。

之後，就應用程式管理器2、安全管理器5之具體軟體之安裝作說明。應用程式管理器2作成如第7圖所示之程式，使CPU執行，而可安裝於應用程式執行裝置。

第7圖係顯示應用程式管理器2所作之Java(TM)歸檔檔案302內之類別檔案401之應用程式之啟動程序的流程圖。應用程式管理器2確認Java(TM)歸檔檔案302中是否存在SIG-BD.SF、SIG-BD.RSA、bd.XXXX.perm(SA01)。若皆不存在時，便有Java(TM)應用程式遭竄改之可能性，而不進行Java(TM)應用程式之執行(SA04)。

上述3個檔案皆存在時，則利用MAINFEST.MF、SIG-BD.SF.RSA，對bd.XXXX.perm及Java(TM)應用程式進行簽章認證(SA03)。當簽章認證失敗時，記憶無有效之

bd.XXXX.perm，使虛擬機3執行具有允許之預設之類別檔案401。

當簽章認證成功時，判定存在於第1數位憑證鏈之憑證與BD.ROOT.CERTIFICATE內之碟片根憑證301之同一性(SA05)。若各根憑證不同時，便判斷Java(TM)歸檔檔案302為非法，而不進行Java(TM)應用程式之執行(SA04)。

當各根憑證具同一性時，確認第1數位憑證鏈之葉憑證內是否存在組織ID(SA06)。當組織ID不存在時，便判斷Java(TM)檔案302為非法，而不進行Java(TM)應用程式之執行(SA04)。

當組織ID存在時，確認bd.XXXX.perm中是否存在Credential(SA07)。若不存在時，便前進至步驟SA10。

當Credential存在時，便認證Credential(SA08)。認證處理之詳細內容後述之。當Credential有多數時，該步驟對各Credential進行。

當Credential之認證即使有一個失敗時(SA09為No)時，亦判斷Java(TM)歸檔檔案302為非法，而不執行Java(TM)應用程式(SA04)。

當Credential之認證皆成功時或Credential不存在時，記憶存在於bd.XXXX.perm、組織ID與MAINFEST.MF內之應用程式ID，使虛擬機讀入記載於MAINFEST.MF且為應最先執行之類別檔案401，而執行作為此實例之Java(TM)應用程式。

參照第8圖，說明應用程式管理器2認證Credential之流

程。第8圖係顯示應用程式管理器2所作之Credential之簽章認證程序之流程圖。

首先，確認接受者憑證之散列值503是否與BD.ROOT.CERTIFICATE之碟片根憑證301一致(SY01)。若不一致時，認證失敗(SY02)。

確認接受者組織ID504與記載於第1數位憑證鏈之葉憑證之組織ID是否一致(SY03)。若不一致，則認證失敗(SYO2)。

確認接受者應用程式ID505與記載於bd.XXXX.perm內之Credential以外之處的應用程式ID是否一致(SY04)。若不一致，則認證失敗(SYO2)。確認Credential之提供檔案之名稱前頭是否與提供者組織ID一致(SY05)。若不一致，則認證失敗(SYO2)。

確認SIG-BD.RSA之簽章資訊之正當性(SYO6)。當簽章資訊不正當時，有Credential遭竄改之可能性，而認證失敗(SY02)。

若簽章資訊正當時，確認第2數位憑證鏈之根憑證之散列值與Credential之提供者根憑證之散列值之同一性(SY07)。若不一致時，則Credential非法，認證失敗(SY02)。

確認第2數位憑證鏈之葉憑證之組織ID與Credential之提供者組織ID是否一致(SY08)。若不一致，則Credential為非法，認證失敗(SY02)。

當所有之確認成功時，認證便成功(SY09)。

第9圖係顯示本發明應用程式執行裝置中，應用程式管

理器2保持之管理資訊之一例者。以表之形式管理碟片根憑證301、執行之Java(TM)歸檔檔案302之「Jar檔案名稱」、「組織ID」、「應用程式ID」、「過程間通信」及「Credential」。

第10圖係顯示本發明應用程式執行裝置中，應用程式管理器2保持之管理資訊中之Credential表之一行的一例者。Credential表由「提供者根憑證之散列值」501、「提供者組織ID」502、「提供者檔案列表」506構成。此「提供者檔案列表」506記載有提供檔案名稱507、提供者存取方法508。

當將允許給予Java(TM)歸檔檔案302時，虛擬機3於Java(TM)應用程式執行前，進行以下之處理。虛擬機3確認MAINFEST.MF之Java(TM)應用程式之散列值與Java(TM)應用程式之實際之散列是否一致，若不一致時，便不執行。

Java(TM)應用程式以虛擬機3執行。參照第11圖，說明於典型之Java(TM)應用程式欲利用局部儲存器時進行之處理程序。

第11圖係顯示Java(TM)應用程式利用硬碟4時之處理程序之流程圖。

Java(TM)應用程式取得虛擬局部儲存器根(SC01)。在此，虛擬局部儲存器根係指以MHP之形式，指定作為存取標的之檔案之檔案路徑，以/Root或/Storage/Root之名稱表現。此虛擬局部儲存器根僅謀求與MHP之檔案路徑之形式的互換，在硬碟4之檔案存取時，該局部儲存器名稱轉換為依根憑證決定之局部儲存器根。

接著，Java(TM)應用程式取得組織ID(SC02)。組織ID為諸如「4」之數字。

Java(TM)應用程式組合局部儲存器根之名稱與組織ID，指定要讀取之檔案名稱，進行對檔案之輸入輸出(SC03)。舉例言之，局部儲存器根之名稱為「/persistent/0003」、組織ID為「7」、要讀取之檔案之相對路徑為「8/scores.txt」時，便可從「/persistent/0003/7/8/scores.txt」之檔案路徑，指定檔案。

Java(TM)應用程式為進行第11圖之處理，安全管理器5對Java(TM)提供以下之函數呼叫。

(A)局部儲存器根之取得

(B)組織ID之取得

(C)檔案之讀取

(D)檔案之寫入

參照第12圖，說明Java(TM)應用程式之「局部儲存器根之取得」函數呼叫處理之流程圖。

首先，安全管理器5於呼叫端之Java(TM)應用程式確認是否有bd.XXXX.perm(SD01)。是否有bd.XXXX.perm係從虛擬機3取得儲存有以Java(TM)應用程式作為實例之類別檔案401之Java(TM)歸檔檔案302，而可從應用程式管理器2取得。若無bd.XXXX.perm時，便拒絕「局部儲存器根之取得」(SD02)。

若有bd.XXXX.perm時，便從應用程式管理器2取得碟片根憑證301之散列值(SD03)。安全管理器5確認散列管理

表(後述)後，確認碟片根憑證301之散列值是否已登錄(SD04)。若已登錄時，便將對應碟片根憑證301之散列值之局部儲存器根歸還Java(TM)應用程式(SD05)。

若於散列管理表未登錄碟片根憑證301之散列值時，安全管理器5於管理表追加新之登錄(SD06)。於該登錄記載碟片根憑證301之散列值與在表內同義之局部儲存器根。將於散列管理表新登錄之登錄歸還Java(TM)應用程式(SD07)。

參照第13圖，顯示安全管理器5保持之散列管理表之一例。散列管理表存在根憑證之散列值1301及局部儲存器根1302。本圖之局部儲存器根之「/0001」、「0003」分別指第6圖之目錄名稱/R1、/R2。該等局部儲存器根1302與根憑證之散列值1301一對一對應。因此，對位於具有相同碟片根憑證301之BD碟片之Java(TM)歸檔檔案302中之類別檔案401之實例之Java(TM)應用程式歸還相同之局部儲存器根1302，對位於具有不同碟片根憑證301之BD-ROM之Java(TM)歸檔檔案302中之類別檔案401之實例之Java(TM)應用程式，歸還不同之局部儲存器根1302。

參照第14圖，說明「組織ID之取得」函數呼叫之流程圖。首先，安全管理器5確認呼叫端之Java(TM)應用程式是否有bd.XXXX.perm(SF01)。若無bd.XXXX.perm時，由於無法確認組織ID，便拒絕「組織ID之取得」(SF02)。若有bd.XXXX.perm時，從應用程式管理器2取得對應Java(TM)應用程式之組織ID，而將之歸還Java(TM)應用程式(SF03)。

「檔案讀取」函數呼叫係將要讀取之檔案名稱之全路

徑作為參數而從Java(TM)應用程式傳送至安全管理器5。此全路徑為組織ID/appID/之形式者，應用程式以與存取MHP之局部儲存器內之檔案相同之程序，存取應用程式執行裝置內之檔案。

若檔案存取成功時，安全管理器5將資料歸還Java(TM)應用程式。參照第15圖及第16圖，說明「檔案讀取」函數呼叫之流程圖。

首先，安全管理器5確認呼叫端之Java(TM)應用程式是否有bd.XXXX.perm(SH01)。若無bd.XXXX.perm時，便拒絕「檔案讀取」(SH02)。

若有bd.XXXX.perm時，便從應用執行程式管理器2取得碟片根憑證301之散列值(SH03)。

安全管理器確認散列管理表，取得對應碟片根憑證301之散列值之局部儲存器根1302(SH04)。

接著，判定指定檔案名稱之全路徑之前頭之名稱是否與虛擬局部儲存器根之名稱一致(SH05)。此為檢查是否以與裝置相關之形式(在此為具有與MHP互換之形式)指定存取標的檔案者，當一致時，便將根名稱轉換為對應碟片根憑證之形式之局部儲存器根(SH13)。若不一致時，便拒絕存取(SH02)。

在此，轉換前後全路徑如下。

應用程式指定之全路徑：

/虛擬局部儲存器根/指定組織ID/指定路徑

SH05之轉換後之路徑：

/局部儲存器根/指定組織ID/指定路徑

之後，安全管理器5分解檔案名稱之全路徑(SH06)。由於檔案名稱之全路徑利用「局部儲存器根11302+"/"+指定組織ID+"/"+指定路徑」之形式，故檔案名稱之全路徑可分解為局部儲存器根1302、指定組織ID及指定路徑。無法分解時，便拒絕讀取(SH02)。

安全管理器5從應用程式管理器2取得呼叫端之Java(TM)應用程式之組織ID(SH07)。然後，嘗試是否可從應用程式管理器2取得指定組織ID與提供者組織ID502一致之Credential(SH10)。當可取得Credential時，便拒絕存取(SH02)。

當可取得Credential時，來自Java(TM)應用程式之指定路徑存在於Credential之提供檔案名稱506，確認是否已允許以提供存取方法507讀取(SH11)。若允許時，安全管理器5便取得位於Credential內之提供者根憑證之散列值501(SH12)。

若不允許時，安全管理器5便確認指定組織ID與Java(TM)應用程式之組織ID是否一致(SH08)。若一致時，依Java(TM)應用程式指定之全路徑，從硬碟讀取檔案，而將之歸還應用程式(SH09)。若不一致時，便拒絕讀取(SH02)

安全管理員5確認散列管理表，確認提供者根憑證之散列值501是否已登錄(SH13)。若已登錄時，取得對應提供者根憑證之散列值之局部儲存器根1302，確定作為提供者局部儲存器根(SH14)。

若於散列管理表未登錄提供者根憑證之散列值501時，安全管理器5便於散列管理表追加新之登錄(SH15)。於該登錄記載提供者根憑證之散列值501及在表內同義之局部儲存器根11302。

確定將於散列管理表新登錄之行之局部儲存器根1302作為提供者局部儲存器根(SH16)。

於確定提供者局部儲存器根後，安全管理器5將檔案名稱之全路徑中之局部儲存器根1302置換為提供者局部儲存器根(SH17)。

安全管理器5從硬碟4讀取置換後之檔案名稱之全路徑之檔案，而將之歸還Java(TM)應用程式(SH18)。

以上為有關檔案讀取之說明。接著，就檔案寫入作說明。

「檔案寫入」函數呼叫時將要寫入之檔案名稱之全路徑與要寫入之資料作為參數而從Java(TM)應用程式傳送至安全管理器5。成功時，安全管理器5便將資料寫入至檔案。參照第17圖及第18圖，說明「檔案寫入」函數呼叫之流程圖。

首先，安全管理器5確認呼叫端之Java(TM)應用程式是否有bd.XXXX.perm(SI01)。若無bd.XXXX.perm時，便拒絕「檔案寫入」(SI02)。

若有bd.XXXX.perm時，便從應用執行程式管理器2取得碟片根憑證301之散列值(SI03)。

安全管理器確認散列管理表，取得對應碟片根憑證301

之散列值之局部儲存器根1302(SI04)。

接著，判定指定檔案名稱之全路徑之前頭之根名稱是否與虛擬局部儲存器根之名稱一致(SI05)。當一致時，便將根名稱轉換為局部儲存器根(SI13)。若不一致時，便拒絕存取(SI02)。

在此，轉換前後全路徑如下。

應用程式指定之全路徑：

/虛擬局部儲存器根/指定組織ID/指定路徑

SI05之轉換後之路徑：

/局部儲存器根/指定組織ID/指定路徑

之後，安全管理器5分解檔案名稱之全路徑(SI06)。由於檔案名稱之全路徑利用「局部儲存器根1302+"/"+指定組織ID+"/"+指定路徑」之形式，故檔案名稱之全路徑可分解為局部儲存器根1302、指定組織ID及指定路徑。無法分解時，便拒絕寫入(SI02)。

安全管理器5從應用程式管理員2取得呼叫端之Java(TM)應用程式之組織ID(SI07)。然後，嘗試是否可從應用程式管理器2取得指定組織ID與提供者組織ID502一致之Credential(SI10)。當無法取得時，便拒絕寫入(SI02)。

當可取得時，來自Java(TM)應用程式之指定路徑以Credential之提供檔案名稱506存在，確認是否已允許以提供存取方法507讀取(SI11)。若不允許時，安全管理器5便確認指定組織ID與Java(TM)應用程式之組織ID是否一致(SI08)。若一致時，依Java(TM)應用程式指定之全路徑，將

資料寫入檔案(SI09)。若不一致時，便拒絕寫入(SI02)

若可確認允許寫入時，安全管理器5取得位於Credential內之提供者根憑證之散列值501(SI12)。

安全管理器5確認散列管理表，確認提供者根憑證之散列值501是否已登錄(SI13)。若已登錄時，取得對應提供者根憑證之散列值之局部儲存器根1302，確定作為提供者局部儲存器根(SI14)。

若於散列管理表未登錄提供者根憑證之散列值501時，安全管理器5便於散列管理表追加新之行(SI15)。於該行記載提供者根憑證之散列值501及在表內同義之局部儲存器根1302。

確定將於散列管理表新登錄之行之局部儲存器根1302作為提供者局部儲存器根(SI16)。

於確定提供者局部儲存器根後，安全管理器5將檔案名稱之全路徑中之局部儲存器根1302置換為提供者局部儲存器根(SI17)。

安全管理器5寫入置換後之檔案名稱之全路徑之檔案(SI18)。

如以上，根據本實施形態，由於局部儲存器內部存在分配至各根憑證之散列值之目錄，故該等目錄之下依各組織作成各應用程式之區域時，在世界性標準組ID不為唯一亦可。在稱為"區域"之封閉世界中，由於可區別複數組織便足夠，故不需使組織ID在世界性標準為唯一之值，而不需第3者機關所作之管理。

又，由於根憑證是分配給記憶機構內之領域而非裝置本體，只要BD-ROM裝設於應用程式執行程式，必可保障運作。當然並非碟片根憑證無曝露之可能性，此時，使BD-ROM無法使用或僅更新該BD-ROM之碟片根憑證即可，而對提供給其他BD-ROM之應用程式如前述使用碟片根憑證即可，故可實現確實之動作保障。

如此，不需以世界性標準管組織ID，且可將以往之各應用程式之保障維持在高標準，故本發明之應用程式執行裝置對執行有關電影作品之處理之應用程式之應用程式執行裝置的世界性標準化有極大之助益。

(備註)

以下，在本案申請之時間點就申請人所知之最佳實施形態作了說明，而以下所示之技術性標題可增加進一步之改良或變更實施。應注意依各實施形態所示者實施或是否實施該等之改良或變更皆是任意，是依實施者之主觀進行。

(Java(TM)歸檔檔案302之選擇)

當影像等資料共存於BD-ROM時，可選擇根據影像再生之事件(章2之再生開始等)指定之Java(TM)歸檔檔案302或對應使用者畫面上選擇之Java(TM)歸檔檔案302。

亦有數位憑證鏈由一個憑證構成之情形。此時，根憑證及葉憑證皆為相同之憑證。

(允許之種類)

若為具有更豐富之功能之應用程式執行裝置時，於bd.XXXX.perm包含其他種類之允許亦可。於

bd.XXXX.perm中包含複數數位憑證312亦可。

(組織ID)

依實施形態，組織ID記載於BD-ROM上之不同檔案。此時，不需拒絕「組織ID之取得」，而歸還以其他方法確定之組織ID亦可。

(檔案之讀取/寫入)

在第15圖、第16圖、第17圖、第18圖中以檔案之讀取為中心作說明，同樣地亦可從Java(TM)應用程式於目錄存取。於目錄存取時，亦有於檔案名稱之全路徑無指定之情形。

又，在第15圖及第16圖中以讀取檔案全體之函數呼叫作說明，同樣地取得部份檔案或進行典型之檔案存取亦可。

第11圖所示之控制流程為一例，亦有因Java(TM)應用程式之製作而大為不同之情形。

(與其他方式之併用)

本方式可與於檔案存取允許方式(例如經常用於UNIX(註冊商標)之使用者、群組、世界存取模組)併用。例如併用本方式與第2方式而決定以下之優先度亦可。

(A)在步驟SH06中無法於全路徑分解時，或在步驟SH10中，數位信用憑證不存在時，利用第2方式之存取控制。

(B)在步驟SH09中，利用第2方式之存取控制。

(C)其他以本方式優先。

(散列值)

本實施形態之散列值係利用SHA-1或MD5等之保全散

列函數之結果的值。保全散列函數具有發現具相同之散列值之不同資料在實質上不可能的特徵。

(根憑證之散列值)

本實施形態之根憑證之散列值不需從根憑證全體算出，至少僅從根憑證中所含之公鑰算出亦可。用於儲存於MAINFEST.MF、SIB-BD.SF、SIG-BD.RSA中之散列值之計算的保全散列函數可由碟片製作者明確選擇。

在本實施形態中，bd.XXXX.perm中之數位信用憑證中，以提供者根憑證之散列值501及用於接受者根憑證之散列值503之計算之保全散列函數固定為連接接對象，而於bd.XXXX.perm中之數位信用憑證中明示提供者根憑證之散列值501及接受者根憑證之散列值503之計算的保全散列函數亦可。

(根憑證之比較)

步驟SA05之根憑證之比較亦可進行根憑證是否相同之比較、根憑證中所含之公鑰是否相同之比較。又，其他之方式為忽視數位簽章檔案中之第1個憑證(根憑證)，而確認接續根憑證之第2個憑證是否根據碟片根憑證301簽章亦可。由於不論使用何種方式，碟片根憑證301皆可保障數位簽章檔案中之第2個憑證，故在安全觀點上之效果相同。

步驟SA05之比較以防止濫用應用程式間通信之攻擊為主要目的。濫用應用程式間通信之攻擊假設為嘗試利用以下所作之攻擊用BD-ROM。

1.從攻擊對象之碟片製作者製作之正當BD-ROM讀取

根據數位憑證簽章之攻擊對象之Java(TM)歸檔檔案302。

2.作成用以攻擊之Java(TM)歸檔檔案302，根據數位憑證進行簽章。

3.將用以與攻擊對象之Java(TM)歸檔檔案302攻擊之Java(TM)歸檔檔案302記錄於攻擊用BD-ROM。

用以攻擊之Java(TM)歸檔檔案302與攻擊對象之Java(TM)歸檔檔案302皆根據數位憑證簽章，皆利用不同之根憑證。在應用程式執行裝置中，對位於2個Java(TM)歸檔檔案302之Java(TM)應用程式給予過程間通信之允許時，用以攻擊之Java(TM)歸檔檔案302可對攻擊對象之Java(TM)歸檔檔案302進行非法之過程間通信，攻擊對象之Java(TM)歸檔檔案302對自身利用之記憶區域可進行攻擊對象之碟片製作者不預期之動作。

為防止上述攻擊，在步驟SA05中需進行根憑證之比較。又，亦可防止利用因步驟SA05之改變而不同之根憑證之Java(TM)應用程式間之過程間通信。此時，於1個BD-ROM具有複數碟片根憑證301亦可。

(局部儲存器之名稱取得函數)

在實施形態中，局部儲存器之名稱取得函數之步驟SC01中，暫時將為具有與MHP互換之形式之全路徑的虛擬局部儲存器名稱歸還應用程式後，在SH05、SI05中，轉換為應用程式執行裝置之局部儲存器名稱，而在局部儲存器名稱之名稱取得函數之步驟SC01中，將記述於散列管理表之局部儲存器名稱直接歸還至Java(TM)應用程式，而省略

從虛擬局部儲存器名稱轉換為局部儲存器名稱。

(標題)

當製造應用程式執行裝置作為BD-ROM再生裝置時，宜於應用程式執行裝置設置依BD-ROM之裝設、使用者操作、裝置之狀態選擇標題之“模組管理器”。BD-ROM再生裝置內之解碼器依此“模組管理器”所作之標題選擇，進行根據播放列表資訊之AVClip再生。

應用程式管理器2於“模組管理器”進行標題之選擇時，使用對應前一個標題之AMT對應目前標題之AMT，進行發信。此發行進行以下之控制，即，使記載於對應前一個標題之AMT而未記載於對應目前標題之AMT之應用程式之動作結束，使未記載於對應前一個標題之AMT而記載於對應目前標題之AMT之應用程式之動作開始。然後，每次進行此應用程式發信時，宜進行使用上述碟片根憑證之認證。

(BD-BOX)

將長篇之電影作品或群組物之電影作品記錄於複數BD-ROM，構成所謂之BD-BOX時，宜於該等BD-ROM分配同一碟片根憑證301。如此，於複數BD-ROM分配同一碟片根憑證時，根據應用程式亦有在碟片交換前後運作者。如此，將在碟片交換前後運作之應用程式稱為“碟片邊界應用程式”。在此，應用程式管理器2宜於進行BD-ROM交換時，讀取新裝設之BD-ROM之碟片根憑證301，確認與定義該碟片邊界應用程式之Java(TM)歸檔檔案302內之碟片根憑證

301之同一性。然後，若有同一性時，便使碟片邊界應用程式繼續，若無同一性時，便強制結束碟片邊界應用程式。如此進行，可在BD-ROM交換前後，僅使正當之應用程式運作。

(Credential)

・Credential宜構成在複數XML文書中，取出以特定之標籤包圍之部份，而將該等結合。

・將以提供者組織之葉憑證(公鑰)簽署Credential資料之Credential的值作為Credential之簽章資訊，而記載於bd.XXXX.perm中亦可。

・在進行「權限之提供」時，bd.XXXX.perm為複數亦可，宜記述SIG-BD.GF之哪一個葉憑證用於與哪一個Credential對照之資訊。

・Credential之作法為於bd.XXXX.perm中寫入提供者檔案名稱，而從寫入其他檔案之值算出Credential之實體亦可。

・然後，將該等全部組合，以於bd.XXXX.perm取得用以界定提供者檔案、葉憑證之資訊、簽章資訊。

(局部儲存器)

在本實施形態中，局部儲存器為裝置組裝型之硬碟，若為安全之記錄媒體，亦可採用可搬型者。例如亦可採用SD記憶卡。

(應安裝之封包)

於執行應用程式執行裝置時，宜將以下之BD-J Extention安裝於應用程式執行裝置。BD-J Extention為將超

越GEM[1.02]之功能給予Java(TM)平台而具有業經特別化之各種封包。提供給BD-J Extention之封包具有以下者。

· org.bluray.media

此封包提供應於Java(TM)Media Frame Work追加之特殊功能。於此封包追加角度、聲音、字幕之選擇的控制。

· org.bluray.ti

此封包包含將GEM[1.02]之"服務"標示為"標題"而運作之API、自BD-ROM詢問標題資訊之機構或選擇新標題之機構。

· org.bluray.application

此封包包含用以管理應用程式之生存空間之API。亦包含詢問執行應用程式時之發信所需之資訊。

· org.bluray.ui

此封包包含將供於BD-ROM特別化之關鍵事件用之常數定義，以實現與影像再生之同步之類別。

· org.bluray.vfs

此封包為不受資料之所在地所限，而使資料無縫再生，而將記錄於BD-ROM上之內容(on-disc內容)與未記錄於BD-ROM上之local storage上之內容(off-disc內容)結合之機構(Binding Scheme)。

Binding Scheme係指使BD-ROM上之內容(AVClip、字幕、BD-J應用程式)與local storage上之相關內容具關聯者。此Binding Scheme不受內容之所在地所限，而可實現無縫再生。

(局部儲存器之存取)

舉例言之，確認於檔案路徑「/Persistent/1/1/streams/是否存在所期之檔案係藉使用java(TM).io之exits()方法而執行。以下顯示所期之檔案為O.m2ts時之java(TM).io之exits()方法之使用例。

例：

new java(TM).io.File("/Presistent/1/1/streams/0.2mts").exists()；

(允許請求檔案)

允許請求檔案亦可決定是否允許以下之功能。

・網路連接之利用

・BD-ROM之存取

・BD-ROM之其他標題之選擇

・其他平台之執行控制

(影像、聲音)

在第1(a)圖所示之BD-ROM之構造中，於ROOT目錄之下設置BDMV目錄，於此目錄記錄為MPEG2-TS形式之AV串流之AVClip或規定此再生路徑之播放列表資訊亦可。然後，為進行透過播放列表資訊之再生，記述Java(TM)應用程式亦可。

當播放列表資訊儲存於稱為00001.mpls之檔案時，Java(TM)應用程式依JMF程式管，生成JMF播放器實例。JMF A"BD：//00001.mpls"係命令使PL再生之播放器實例生成之方法。A.play為命令JMF播放器實例再生之方法。

(BD-ROM內容)

記錄於BD-ROM之應用程式為構成電影作品者，若非於安裝於局部儲存器而供利用之應用程式，而是以記錄於BD-ROM之狀態供利用之應用程式時，為構成電影作品以外者亦可。例如亦可為構成遊戲軟體之應用程式。又，在本實施形態中，碟片媒體可選擇以BD-ROM為題材，只要為可搬體且為已進行著作權保護之記錄媒體，採用其他記錄媒體亦可。

(Virtual Package)

亦可使安全管理器5執行生成Virtual Package之處理。Virtual Package係指藉將記錄於BD-ROM等唯讀型之記錄媒體之數位串流及記錄於硬碟等可改寫型記錄媒體之數位串流動態組合，而構築虛擬封包，而謀求唯讀型記錄媒體之內容擴大之技術。記錄於BD-ROM之數位串流為構成電影作品之本篇者，若記錄於硬碟之數位串流為構成電影作品之續篇時，藉構築上述Virtual Package，可將BD-ROM上之本編與硬碟上之續篇處理為1個長篇電影作品而供再生。

此藉安全管理器5生成Virtual Package資訊而進行。Virtual Package係指將BD-ROM之容量管理資訊擴大之資訊。在此，容量管理資訊為規定存在於某一記錄媒體上之目錄檔案構造之資訊，由有關目錄之目錄管理資訊及有關檔案之檔案管理資訊構成。Virtual Package資訊係指藉於顯示BD-ROM之構造之容量管理資訊追加新之檔案管理資訊，而謀求BD-ROM之目錄檔案構造之擴大者。藉此Virtual

Package資訊之生成，應用程式以與存取BD-ROM相同之感覺，可存取局部儲存器之每一碟片根憑證之領域之每一組織的區域。

(控制程序之實現)

由於各實施形態中引用流程圖說明之控制程序或功能性構成要件之控制程序使用硬體資訊而具體實現，故可稱為利用自然法則之技術性思想之創作，而滿足"程式發明"之成立要件。

・本發明之程式之生產形態

本發明之程式為電腦可執行之執行形式的程式(目標程式)，由使電腦執行實施形態所示之流程圖之各步驟或功能性構成要件之各程序之1個以上之程式碼構成。在此，程式碼如處理器之本機碼或JAVA位元組碼般有各種種類。程式碼之各步驟之實現有各種態樣。利用外部函數，可實現各步驟時，呼叫此外部函數之呼叫文即為程式碼。又，諸如實現1個步驟之程式碼有屬於各目標程式之情形。在限制命令種類之RISC處理器中，藉組合算術運算命令、邏輯運算命令或分歧命令等，實現流程圖之步驟。

本發明之程式可如以下作成。首先，軟體開發者使用程式語言，記載實現各流程圖或功能性構成要件之原始程式。在記述時，軟體開發者依程式語言之句法結構，使用類別構造體、變數、陣列變數或外部函數之呼叫，記述具體實現各流程圖或功能性構成要件之原始程式。

所記述之原始程式作為檔案而給予編繹器。編繹器將

該等原始程式翻譯而生成目標程式。

編繹器所作之翻譯由句法結構解析、最適當化、資源分割、碼生成之過程構成。在句法結構解析中，進行原始程式之字句解析、句法結構解析及意思解析，將原始程式轉換為中間程式。在最適當化中，對中間程式，進行基本區塊化、控制流程解析、資料流程解析之作業。在資源分割中，為謀求對作為目標之處理器之命令組之適合，而將中間程式中之變數分割於作為目標之處理器具有之暫存器或記憶體。在碼生成中，將中間程式內之各中間命令轉換為程式碼而獲得目標程式。

當生成目標程式時，程式員對該等啟動鏈接器。鏈接器將該等目標程式及相關之程式館程式分配至記憶體空間，將該等結合成1個而生成載入模組。如此生成之載入模組為以電腦之讀取為前提者，使電腦執行各流程圖所示之處理程序或功能性構成要件之處理程序者。經由以上之處理，可作成本發明之程式。

・本發明之程式之使用形態

本發明之程式可如以下使用。

(i)作為組裝程式之使用

將本發明之程式作為組裝程式而使用時，將相當於程式之載入模組與基本輸入輸出程式(BIOS)及各種中間軟體(操作系統)一同寫入命令ROM。藉將此命令ROM組裝入控制部，使CPU執行，可將本發明之程式作為應用程式執行裝置之控制程式使用。

(ii)作為應用程式之使用

應用程式執行裝置為硬碟內藏模組時，基本輸入輸出程式(BIOS)組裝於命令ROM，各中間軟體(操作系統)預載於硬碟。從硬碟使系統啟動之啟動ROM設於應用程式執行裝置。

此時，經由可搬型記錄媒體或網路僅將載入模組供給應用程式執行裝置，而安裝於硬碟作為1個應用程式。如此，應用程式執行裝置進行啟動ROM之自我啟動，使操作系統啟動，且作為1個應用程式而使CPU執行該應用程式，而使用本發明之程式。

在硬碟模組之應用程式執行裝置中，由於可將本發明之程式作為1個應用程式來使用，故本發明之程式可以單體讓渡、貸與或經由網路提供。

(應用程式管理器2~安全管理器5)

應用程式管理器2~安全管器5可以1個系統LIS實現。

系統LSI係指於高密度基板上安裝裸晶片而封裝者。藉於高密度基板上安裝複數個裸晶片而封裝，使複數個裸晶片具有如1個LSI之外形構造者亦包含於系統LSI(此種系統LSI稱為多晶片模組)。在此，著眼於封包種類之系統LSI有QFP(四平包)、PGA(針腳柵格陣列)之類別。QFP為於封包之4側面安裝有針腳之系統LSI。PGA為於底面全體安裝有多數針腳之系統LSI。

該等針腳扮演作為與其他電路之介面之角色。由於系統LSI之針腳存在此介面之角色，故藉於系統LSI之該等針

腳連接其他電路，系統LSI可發揮應用程式執行裝置之核心之角色。

於系統LSI封裝之由“前端部”、“後端部”、“數位處理部”構成。“前端部”係將類比信號數位化之部份，“後端部”係將數位處理結果所得之資料類比化而輸出之部份。

在各實施形態中，以內部構成圖顯示之各構成要件安裝於該數位處理部內。

如之前“作為組裝程式之使用”所記述，於命令ROM寫入相當於程式之載入模組、基本輸入輸出程式(BIOS)、各種中間軟體(操作系統)。在本實施形態中，由於特別創作者為相當於此程式之載入模組之部份，故藉將儲存有相當於程式之載入模組之命令ROM作為裸晶片封裝，可生產本發明之系統LSI。

有關具體之安裝宜使用Soc安裝或SiP安裝。SoC(System on chip)封裝係於1個晶片上燒成複數電路之技術。SiP(System in Package)封裝係將複數晶片以樹脂等形成1個封包之技術。經由以上之過程，本發明之系統LSI可以各實施形態所示之應用程式執行裝置之內部構成圖為基礎而作成。

又，如上述進行而生成之積體電路依積體度之不同，有稱為IC、LSI、超級LSI、極端(ultra)LSI。

再者，亦可將各記錄應用程式執行裝置之構成要件之部份或全部作為1個晶片而構成。積體電路化不限於上述Soc封裝、SiP封裝，亦可以專用電路或泛用程序實現。於

LSI製造後，可利用可進行程式之FPGA(Field Programmable Gate Array)、可再構成LSI內部之電路胞元之連接或設定之可重組態微處理器。進而，若有因半導體技術之進步或衍生之技術置換為LSI之積體電路化之技術時，當然亦可利用該技術，進行功能區塊之積體電路化。例如，可因應生物技術。

本發明之應用程式執行裝置於上述實施形態揭示內部結構，可清楚明白依此內部結構可量產，故在本質上可利用在工業上。由此可知，本發明之應用程式執行裝置具有產業上之可利用性。

【圖式簡單說明】

第1(a)圖係顯示BD-ROM之檔案、目錄結構者。

第1(b)圖係顯示Java(TM)歸檔檔案302中之構造之一例者。

第2(a)圖係顯示Credential之資料構造之一例者。

第2(b)圖係顯示Credential之具體一例者。

第3(a)圖係例示顯示在BD-ROM中，根憑證如何分配者。

第3(b)圖係例示顯示在MHP中，根憑證如何分配者。

第4圖係顯示無權限提供時之SIG-BD.RSA、SIB-BD.SF、BD.ROOT.CERTIFICATE、MANIFEST.MF之相互關係者。

第5圖係顯示無權限提供時之SIG-BD.RSA、SIB-BD.SF、BD.ROOT.CERTIFICATE、MANIFEST.MF、

bd.XXXX.perm之相互關係者。

第6圖係顯示本實施形態之應用程式執行裝置之機能結構之塊圖者。

第7圖係顯示應用程式管理器2所作之Java(TM)歸檔檔案302內之類別檔案之應用程式的啟動程序之流程圖。

第8圖係顯示應用程式管理器2所作之Credential之簽章認證程序之流程圖。

第9圖係顯示應用程式管理器2保持之管理資訊之一例者。

第10圖係顯示應用程式管理器2保持之管理資訊之一例者。

第11圖係顯示Java(TM)應用程式利用硬碟4時之處理程序之流程圖。

第12圖係顯示安全管理器5所作之局部儲存器名稱之取得程序詳細內容之流程圖。

第13圖係顯示安全管理器5保持之散列管理表之一例者。

第14圖係顯示安全管理器5之組織ID之取得函數之詳細內容的流程圖。

第15圖係顯示安全管理器5之檔案讀取函數之詳細內容之流程圖。

第16圖係顯示安全管理器5之檔案讀取函數之詳細內容之流程圖。

第17圖係顯示安全管理器5之檔案寫入函數之詳細內

容之流程圖。

第18圖係顯示安全管理器5之檔案寫入函數之詳細內容之流程圖。

【主要元件符號說明】

1…BD驅動器

2…應用程式管理器

3…虛擬機

4…硬碟

5…安全管理器

301…碟片根憑證

302…Java(TM)歸檔檔案

401…類別檔案

402…清單檔案

403…簽章檔案

404…數位簽章檔案

405…允許請求檔案

501…提供者根憑證之散列值

502…提供者組織ID

503…接受者根憑證之散列值

504…接受者組織ID

505…接受者應用程式ID

506…提供檔案列表

507…提供檔案名稱

508…存取方法

1301…根憑證之散列值

1302…局部儲存器根

七、申請專利範圍：

1. 一種應用程式執行裝置，係從記錄有碟片根憑證、第1根憑證、應用程式、提供者組織之提供者組織ID、葉憑證、及與前述葉憑證相關之第2根憑證的記錄媒體，讀出應用程式而執行者，且前述提供者組織係對前述應用程式提供利用成為對象之檔案的權限者，前述葉憑證係包含與前述提供者組織ID相同之組織ID者，

其中前述碟片根憑證係將從根憑證機構頒佈之第3根憑證分配給該記錄媒體者，

該應用程式執行裝置具有：

管理機構，係藉由判斷前述碟片根憑證和前述第1根憑證是否相同，而判定應用程式之正當性者；

執行機構，係當前述管理機構判定為正當時，執行前述應用程式；

記憶機構，係包含藉由使用了前述第2根憑證之散列值及前述提供者組織ID之檔案路徑所特定之記憶領域者；

又，前述執行中之應用程式指定包含前述提供者組織ID之檔案路徑，而要求向前述記憶領域之存取時，變換至如下述之檔案路徑，並給予前述應用程式利用檔案之權限，該檔案係藉由前述已變換之檔案路徑所特定之記憶領域之成為對象的檔案，而前述檔案路徑係使用了包含和前述已指定之提供者組織ID相同組織ID之葉憑證相關的第2根憑證之散列值、及前述已指定之提供者組織

ID者。

2. 一種應用程式執行方法，係使電腦執行者，該電腦係具有包含用檔案路徑來特定之記憶領域的記憶機構，且構成為可從記錄有碟片根憑證、第1根憑證、應用程式、提供者組織之提供者組織ID、葉憑證、及與前述葉憑證相關之第2根憑證的記錄媒體讀出應用程式者，且前述提供者組織係對應用程式提供利用成為對象之檔案的權限者，前述葉憑證係包含與前述提供者組織ID相同之組織ID者，

其中前述碟片根憑證係將從根憑證機構頒佈之第3根憑證分配給該記錄媒體者，

該應用程式執行方法使前述電腦執行下列步驟：

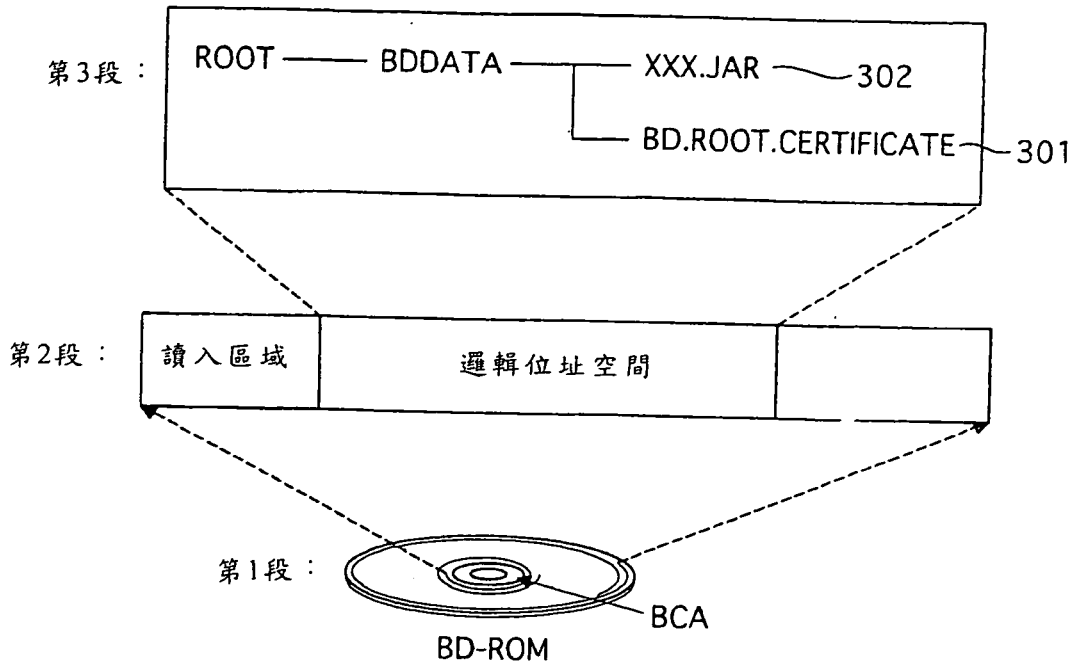
第1步驟，係藉由判斷前述碟片根憑證和前述第1根憑證是否相同，而判定應用程式之正當性者；

第2步驟，係於前述第1步驟判定為正當時，執行應用程式；

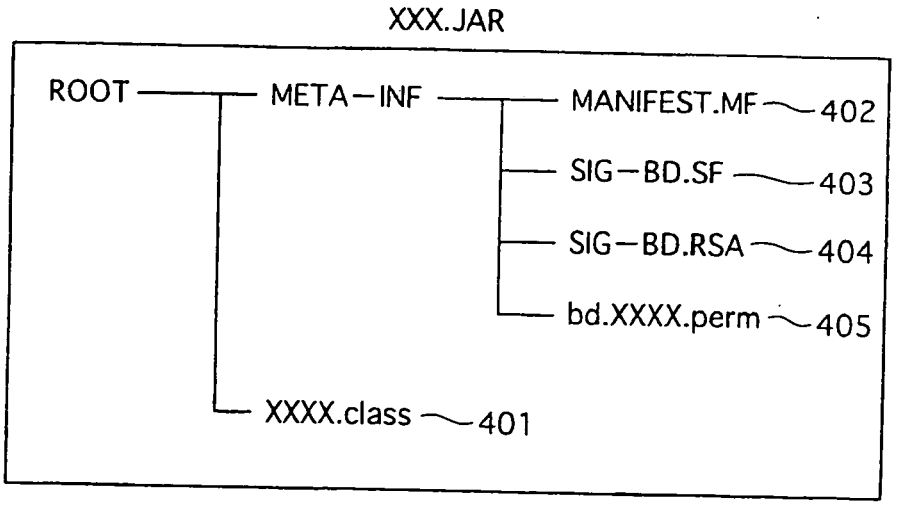
第3步驟，係當前述執行中之應用程式指定包含前述提供者組織ID之檔案路徑，而要求向前述記憶領域之存取時，變換至如下述之檔案路徑，並給予前述應用程式利用檔案之權限，該檔案係藉由前述已變換之檔案路徑所特定之記憶領域之成為對象的檔案，而前述檔案路徑係使用了包含和前述已指定之提供者組織ID相同組織ID之葉憑證相關的第2根憑證之散列值、及前述已指定之提供者組織ID者。

第 1 圖

(a)

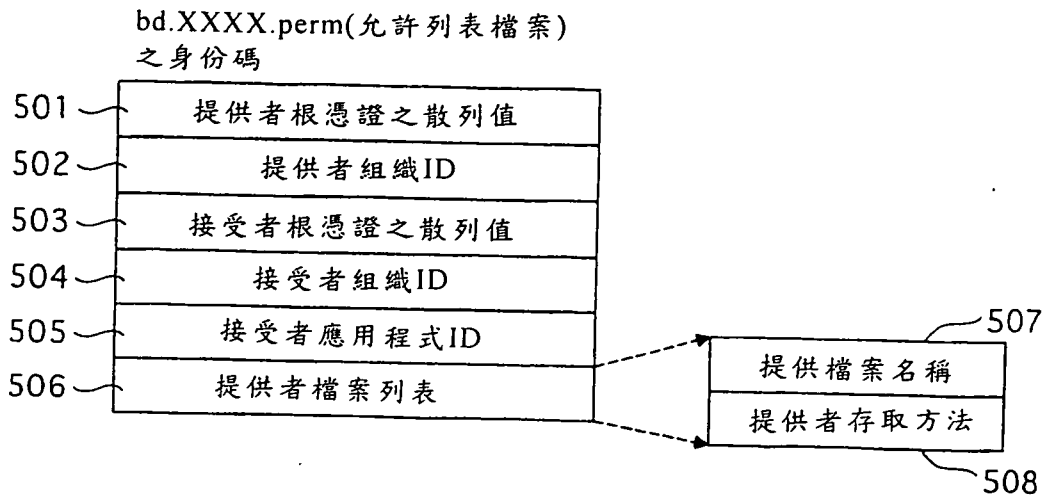

第3段：
ROOT
BDDATA
XXX.JAR
302
BD.ROOT.CERTIFICATE
301
第2段：
讀入區域
邏輯位址空間
第1段：
BCA
BD-ROM

(b)

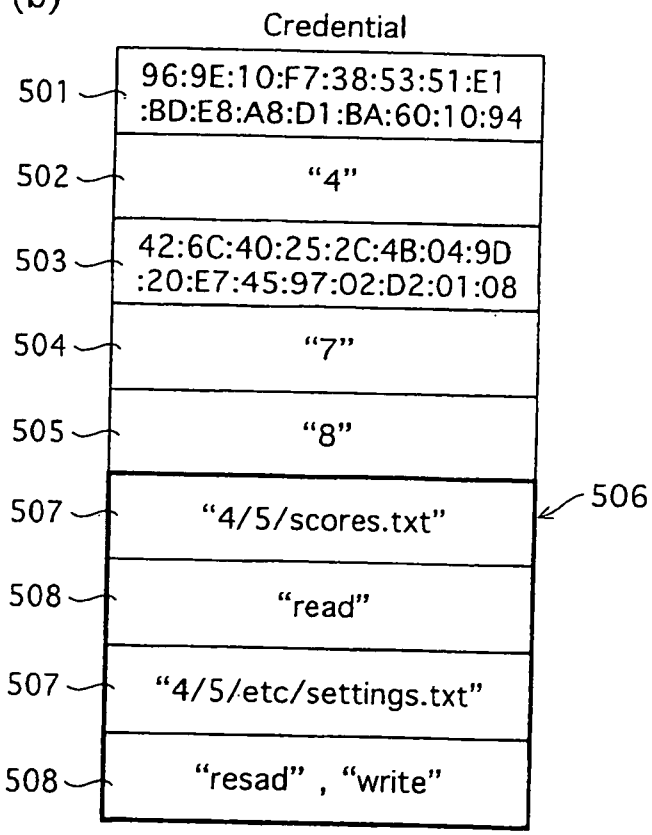

XXX.JAR
ROOT
META-INF
MANIFEST.MF
402
SIG-BD.SF
403
SIG-BD.RSA
404
bd.XXXX.perm
405
XXXX.class
401

第 2 圖

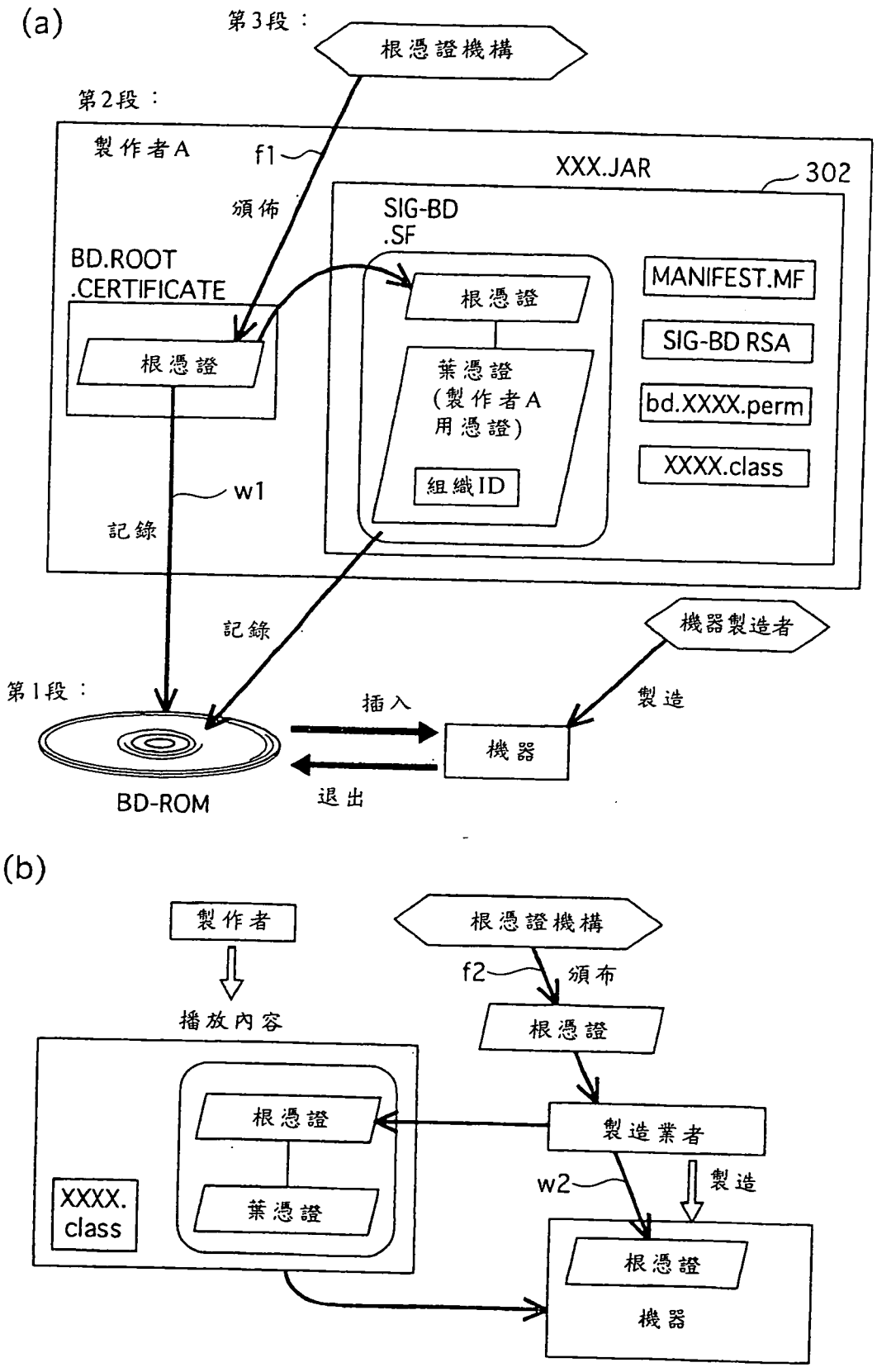
(a)


bd.XXXX.perm(允許列表檔案)
之身份碼
501
提供者根憑證之散列值
502
提供者組織ID
503
接受者根憑證之散列值
504
接受者組織ID
505
接受者應用程式ID
506
提供者檔案列表
507
提供檔案名稱
提供者存取方法
508

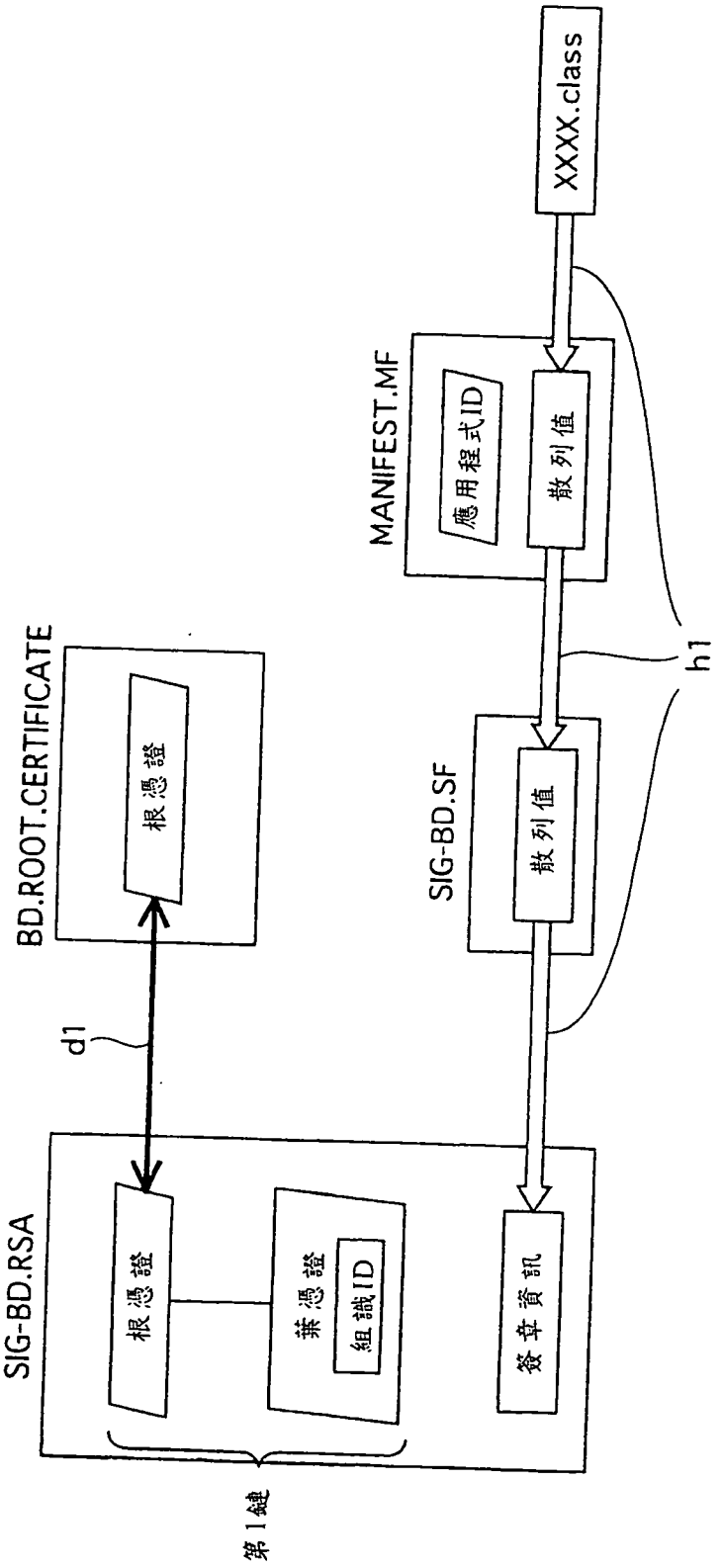
(b)


Credential
501
96:9E:10:F7:38:53:51:E1
:BD:E8:A8:D1:BA:60:10:94
502
"4"
503
42:6C:40:25:2C:4B:04:9D
:20:E7:45:97:02:D2:01:08
504
"7"
505
"8"
507
"4/5/scores.txt"
506
508
"read"
507
"4/5/etc/settings.txt"
508
"resad" , "write"

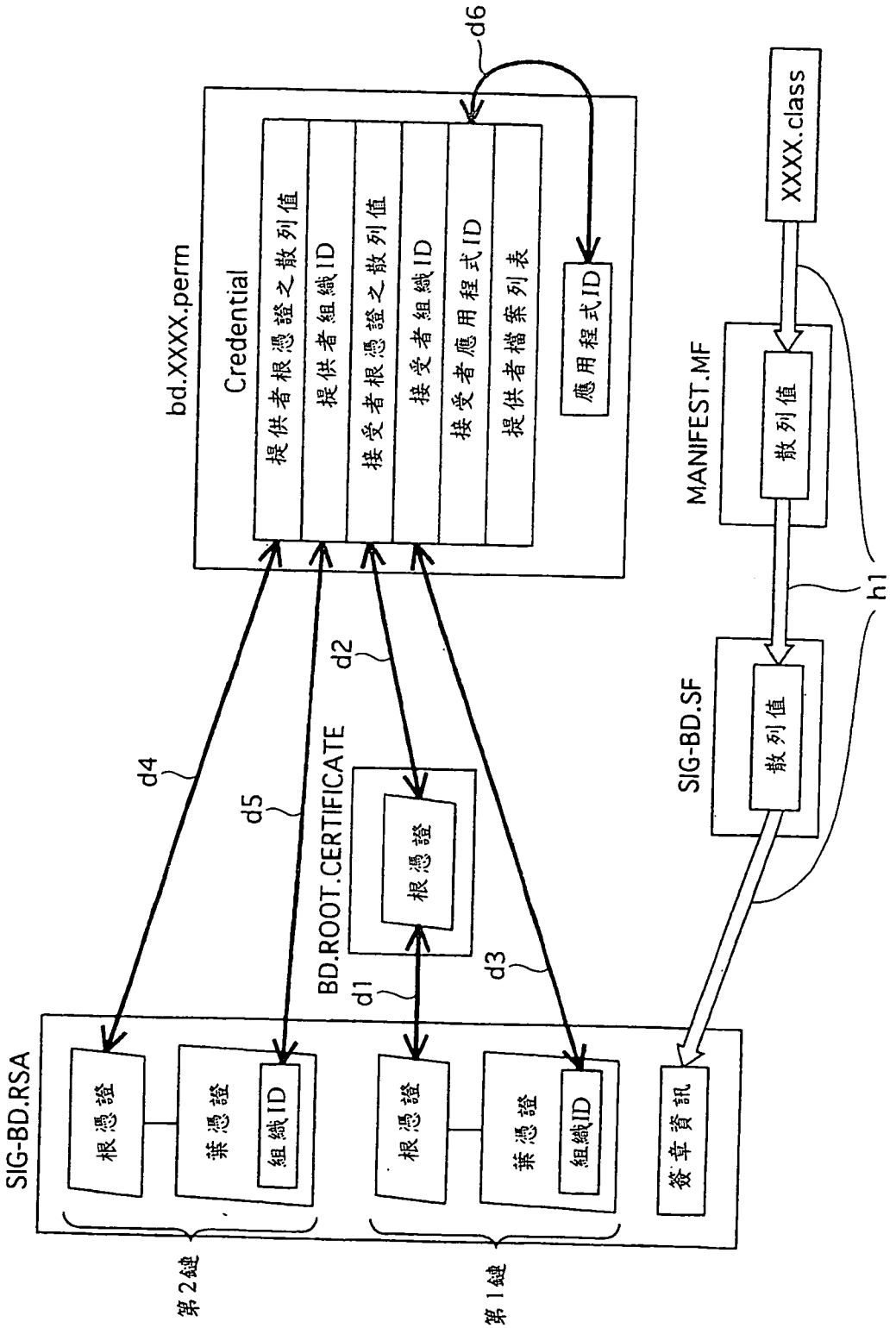
第 3 圖


(a)
第3段：
根憑證機構
第2段：
製作者A
f1
頒佈
XXX.JAR
302
SIG-BD
.SF
BD.ROOT
.CERTIFICATE
根憑證
根憑證
葉憑證
(製作者A
用憑證)
組織ID
MANIFEST.MF
SIG-BD RSA
bd.XXXX.perm
XXXX.class
w1
記錄
記錄
機器製造者
第1段：
插入
製造
機器
BD-ROM
退出
(b)
製作者
播放內容
根憑證機構
f2
頒布
根憑證
根憑證
葉憑證
XXXX.
class
製造業者
w2
製造
根憑證
機器

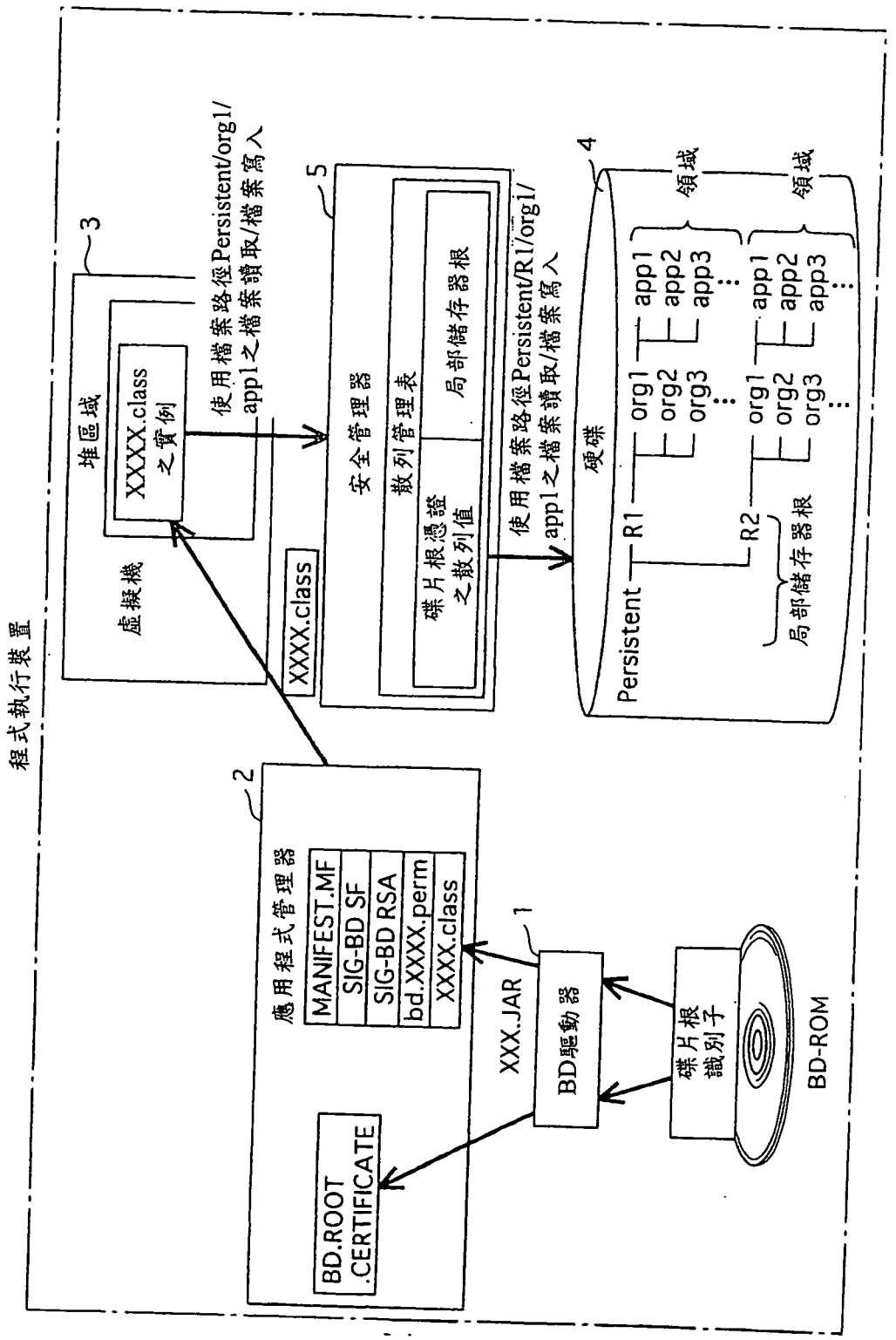
第 4 圖


XXXX.class
MANIFEST.MF
應用程式ID
散列值
h1
SIG-BD.SF
散列值
BD.ROOT.CERTIFICATE
根憑證
d1
SIG-BD.RSA
根憑證
葉憑證
組織ID
簽章資訊
第1鏈

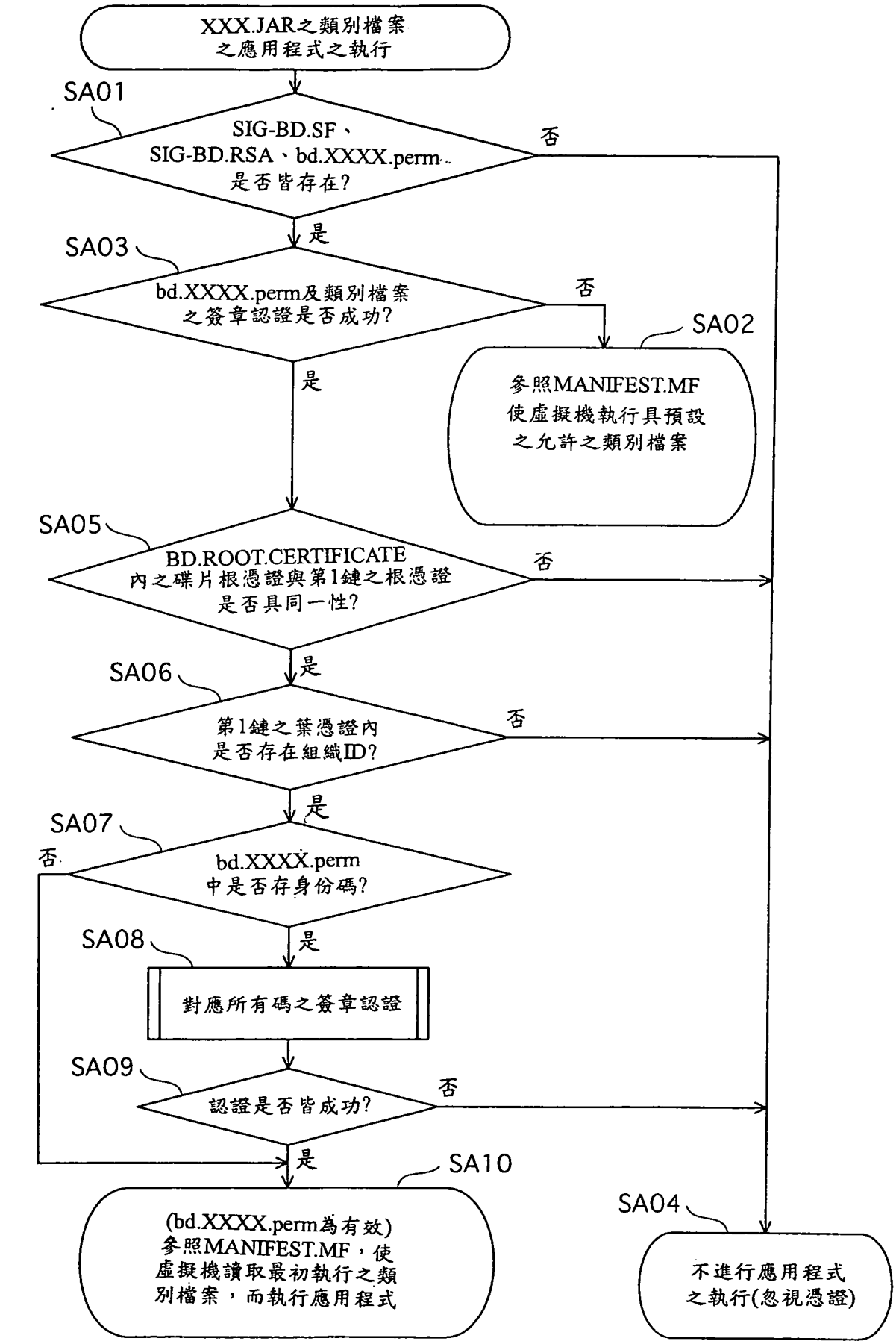
第 5 圖


bd.XXXX.perm
Credential
提供者根憑證之散列值
提供者組織ID
接受者根憑證之散列值
接受者組織ID
接受者應用程式ID
提供者檔案列表
應用程式ID
d6
XXXX.class
MANIFEST.MF
散列值
h1
SIG-BD.SF
散列值
d2
d4
d5
BD.ROOT.CERTIFICATE
根憑證
d1
d3
SIG-BD.RSA
根憑證
葉憑證
組織ID
根憑證
葉憑證
組織ID
簽章資訊
第2鍵
第1鍵

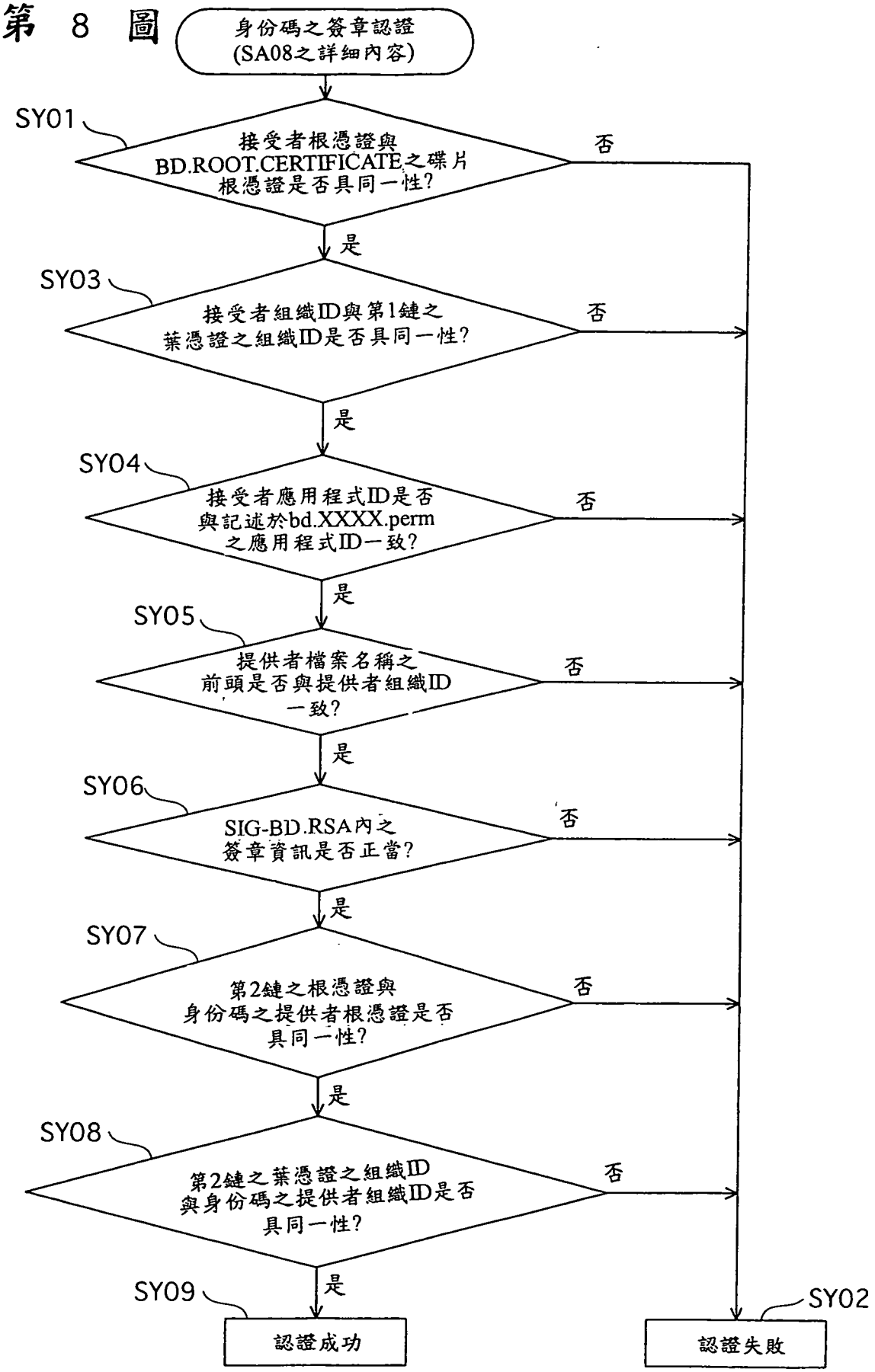
第 6 圖


程式執行裝置
虛擬機
堆區域
XXXX.class
之實例
3
使用檔案路徑Persistent/org1/
app1之檔案讀取/檔案寫入
XXXX.class
5
安全管理器
散列管理表
碟片根憑證
之散列值
局部儲存器根
使用檔案路徑Persistent/R1/org1/
app1之檔案讀取/檔案寫入
4
硬碟
Persistent
R1
R2
org1
org2
org3
app1
app2
app3
領域
局部儲存器根
2
應用程式管理器
MANIFEST.MF
SIG-BD SF
SIG-BD RSA
bd.XXXX.perm
XXXX.class
BD.ROOT
.CERTIFICATE
XXX.JAR
1
BD驅動器
碟片根
識別子
BD-ROM

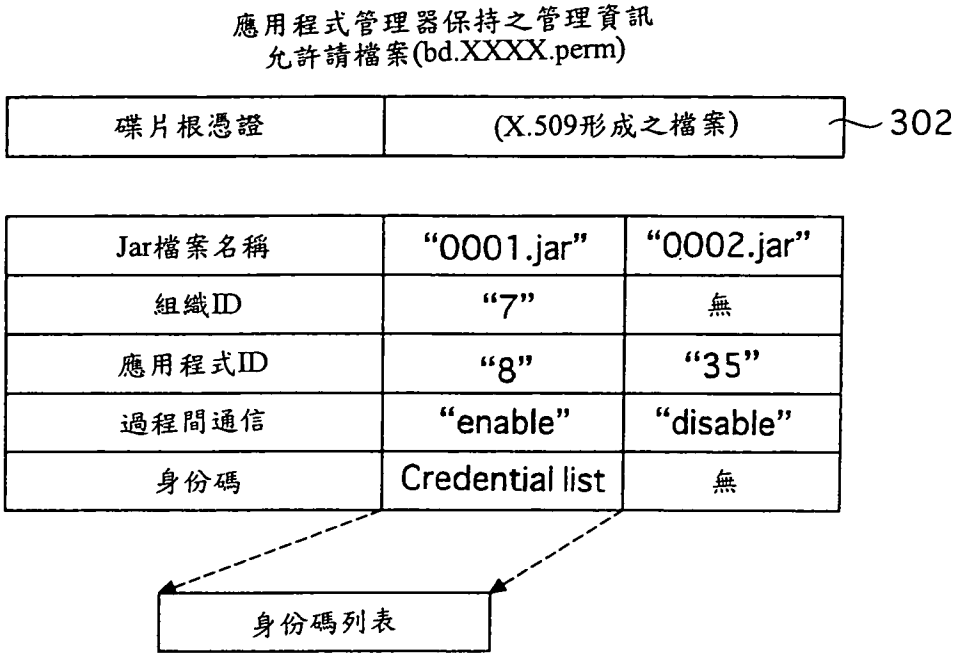
第 7 圖


XXX.JAR之類別檔案
之應用程式之執行
SA01
SIG-BD.SF、
SIG-BD.RSA、bd.XXXX.perm
是否皆存在?
否
是
SA03
bd.XXXX.perm及類別檔案
之簽章認證是否成功?
否
SA02
參照MANIFEST.MF
使虛擬機執行具預設
之允許之類別檔案
是
SA05
BD.ROOT.CERTIFICATE
內之碟片根憑證與第1鏈之根憑證
是否具同一性?
否
是
SA06
第1鏈之葉憑證內
是否存在組織ID?
否
是
SA07
否
bd.XXXX.perm
中是否存身份碼?
是
SA08
對應所有碼之簽章認證
SA09
認證是否皆成功?
否
是
SA10
(bd.XXXX.perm為有效)
參照MANIFEST.MF，使
虛擬機讀取最初執行之類
別檔案，而執行應用程式
SA04
不進行應用程式
之執行(忽視憑證)

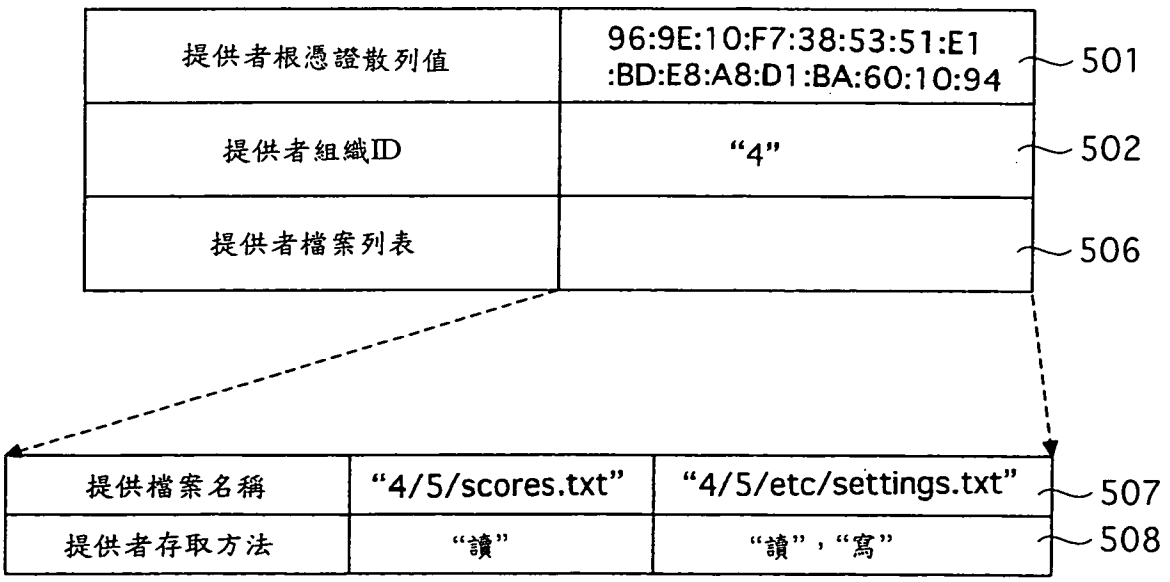
第 8 圖


身份碼之簽章認證
(SA08之詳細內容)
SY01
接受者根憑證與
BD.ROOT.CERTIFICATE之碟片
根憑證是否具同一性?
否
是
SY03
接受者組織ID與第1鏈之
葉憑證之組織ID是否具同一性?
否
是
SY04
接受者應用程式ID是否
與記述於bd.XXXX.perm
之應用程式ID一致?
否
是
SY05
提供者檔案名稱之
前頭是否與提供者組織ID
一致?
否
是
SY06
SIG-BD.RSA內之
簽章資訊是否正當?
否
是
SY07
第2鏈之根憑證與
身份碼之提供者根憑證是否
具同一性?
否
是
SY08
第2鏈之葉憑證之組織ID
與身份碼之提供者組織ID是否
具同一性?
否
是
SY09
認證成功
SY02
認證失敗

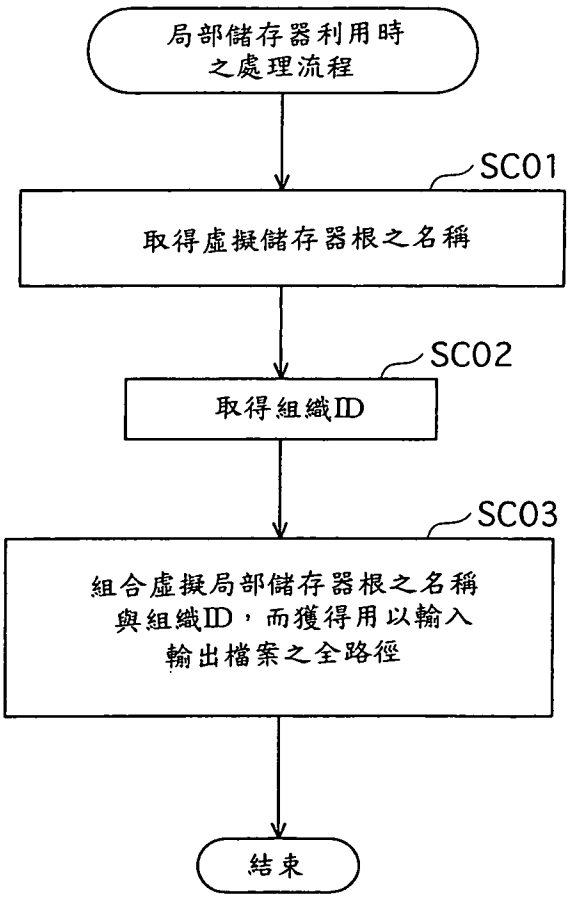
第 9 圖


應用程式管理器保持之管理資訊
允許請檔案(bd.XXXX.perm)
碟片根憑證
(X.509形成之檔案)
302
Jar檔案名稱
"0001.jar"
"0002.jar"
組織ID
"7"
無
應用程式ID
"8"
"35"
過程間通信
"enable"
"disable"
身份碼
Credential list
無
身份碼列表

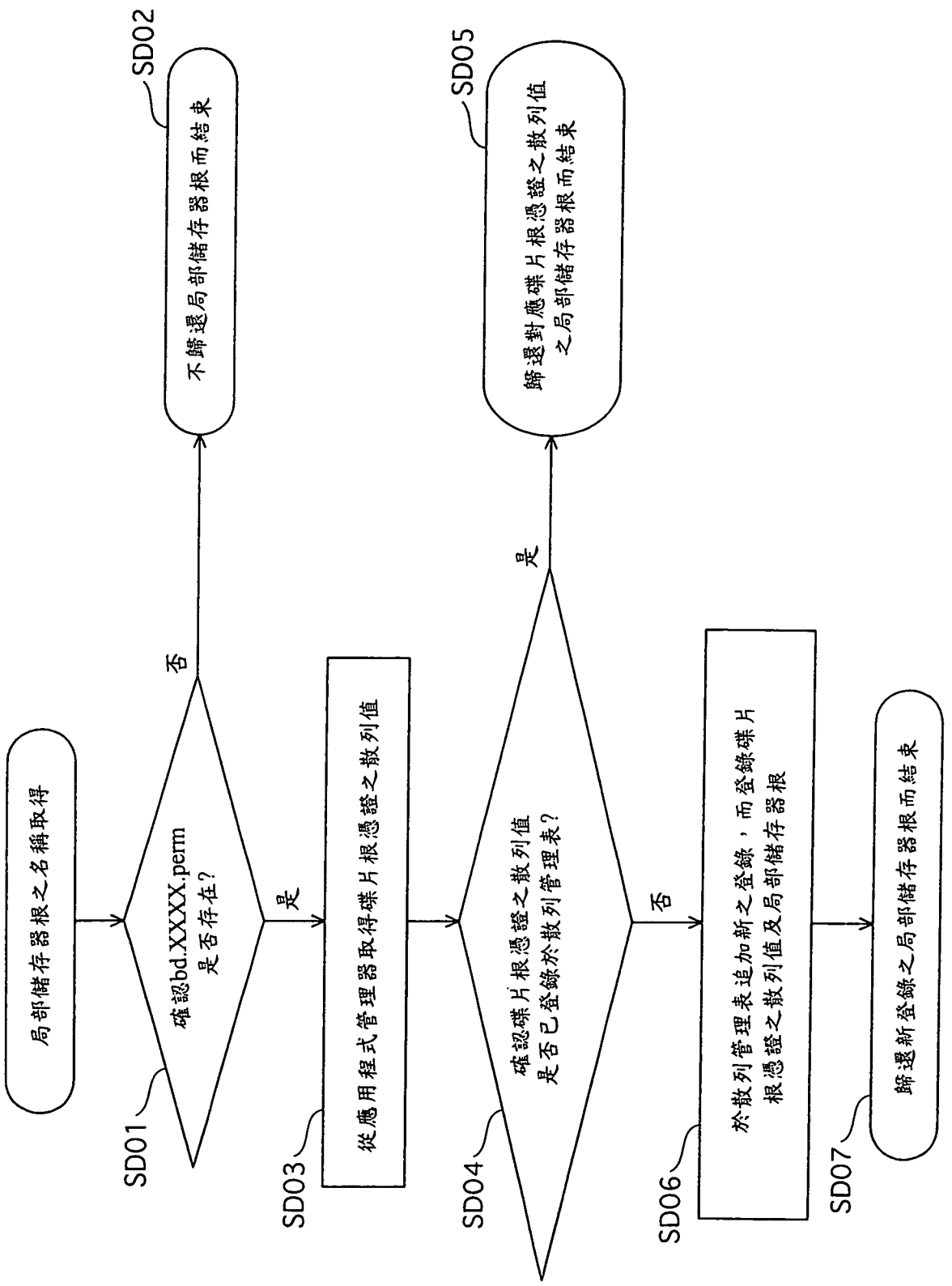
第 10 圖


提供者根憑證散列值
96:9E:10:F7:38:53:51:E1
:BD:E8:A8:D1:BA:60:10:94
501
提供者組織ID
"4"
502
提供者檔案列表
506
提供檔案名稱
"4/5/scores.txt"
"4/5/etc/settings.txt"
507
提供者存取方法
"讀"
"讀"，"寫"
508

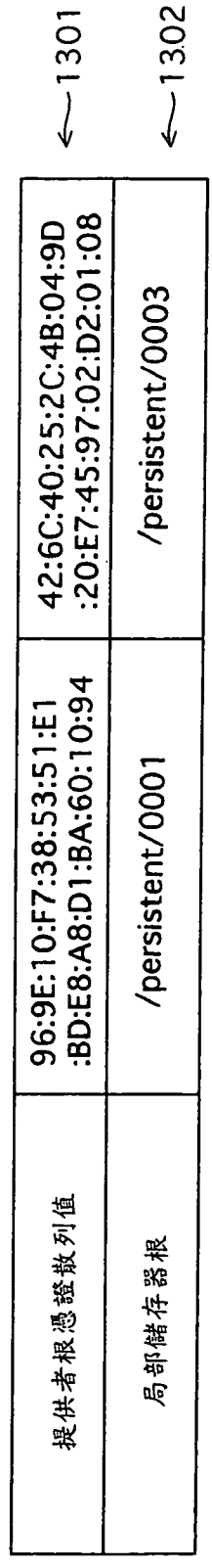
第 11 圖


局部儲存器利用時
之處理流程
SC01
取得虛擬儲存器根之名稱
SC02
取得組織ID
SC03
組合虛擬局部儲存器根之名稱
與組織ID，而獲得用以輸入
輸出檔案之全路徑
結束

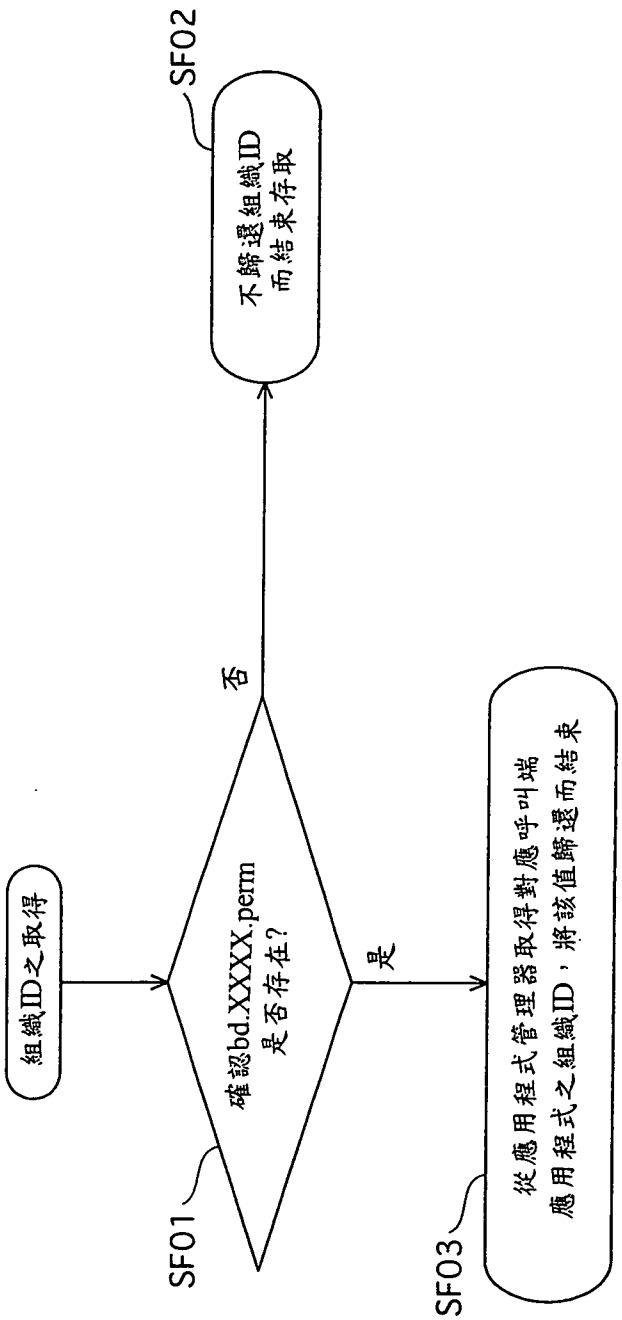
第 12 圖


局部儲存器根之名稱取得
確認bd.XXXX.perm
是否存在?
SD01
否
不歸還局部儲存器根而結束
SD02
是
從應用程式管理器取得碟片根憑證之散列值
SD03
確認碟片根憑證之散列值
是否已登錄於散列管理表?
SD04
是
歸還對應碟片根憑證之散列值
之局部儲存器根而結束
SD05
否
於散列管理表追加新之登錄，而登錄碟片
根憑證之散列值及局部儲存器根
SD06
歸還新登錄之局部儲存器根而結束
SD07

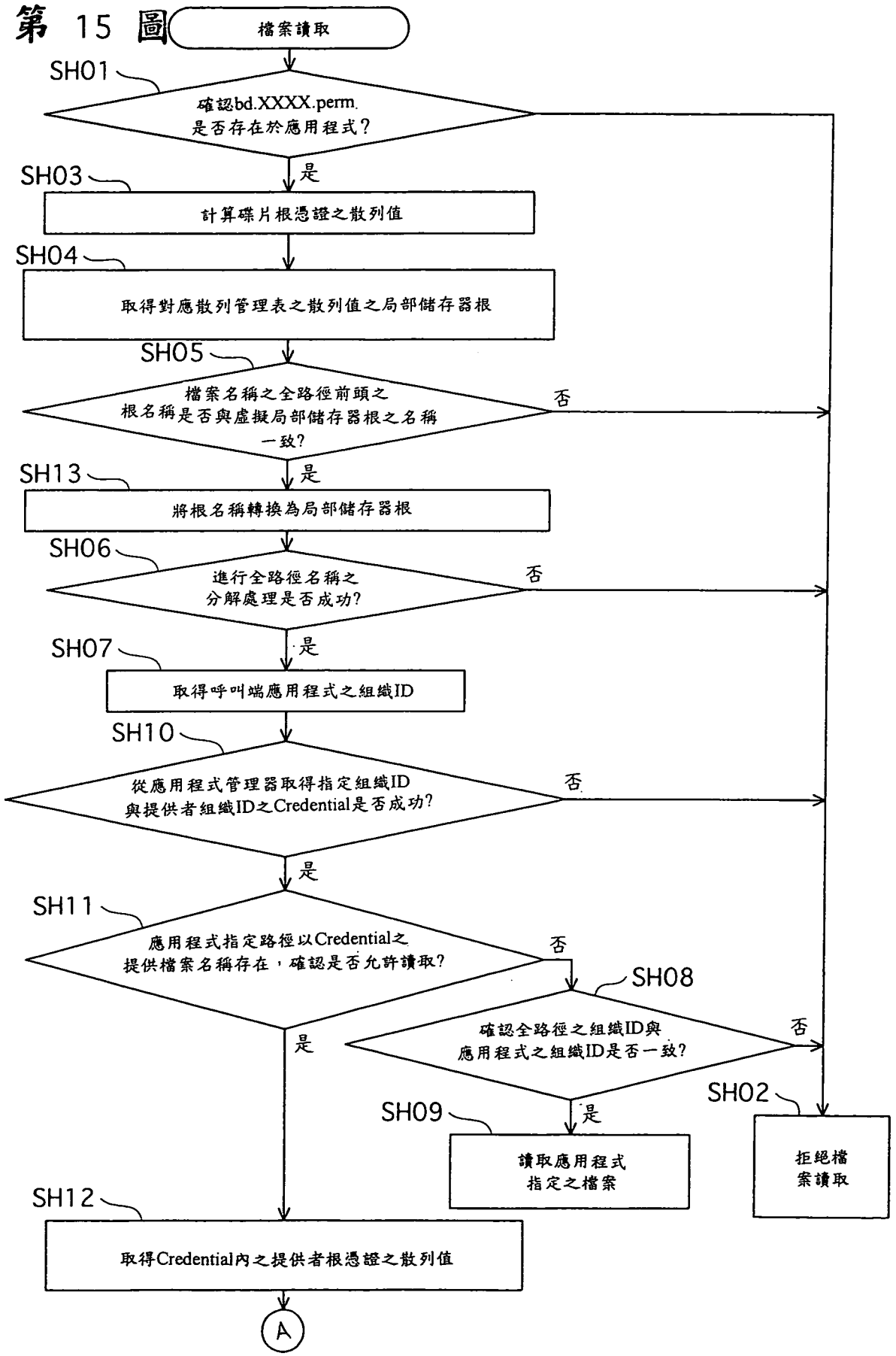
第 13 圖


安全管理器保持之散列管理表
提供者根憑證散列值
局部儲存器根
96:9E:10:F7:38:53:51:E1
:BD:E8:A8:D1:BA:60:10:94
/persistent/0001
42:6C:40:25:2C:4B:04:9D
:20:E7:45:97:02:D2:01:08
/persistent/0003
1301
1302

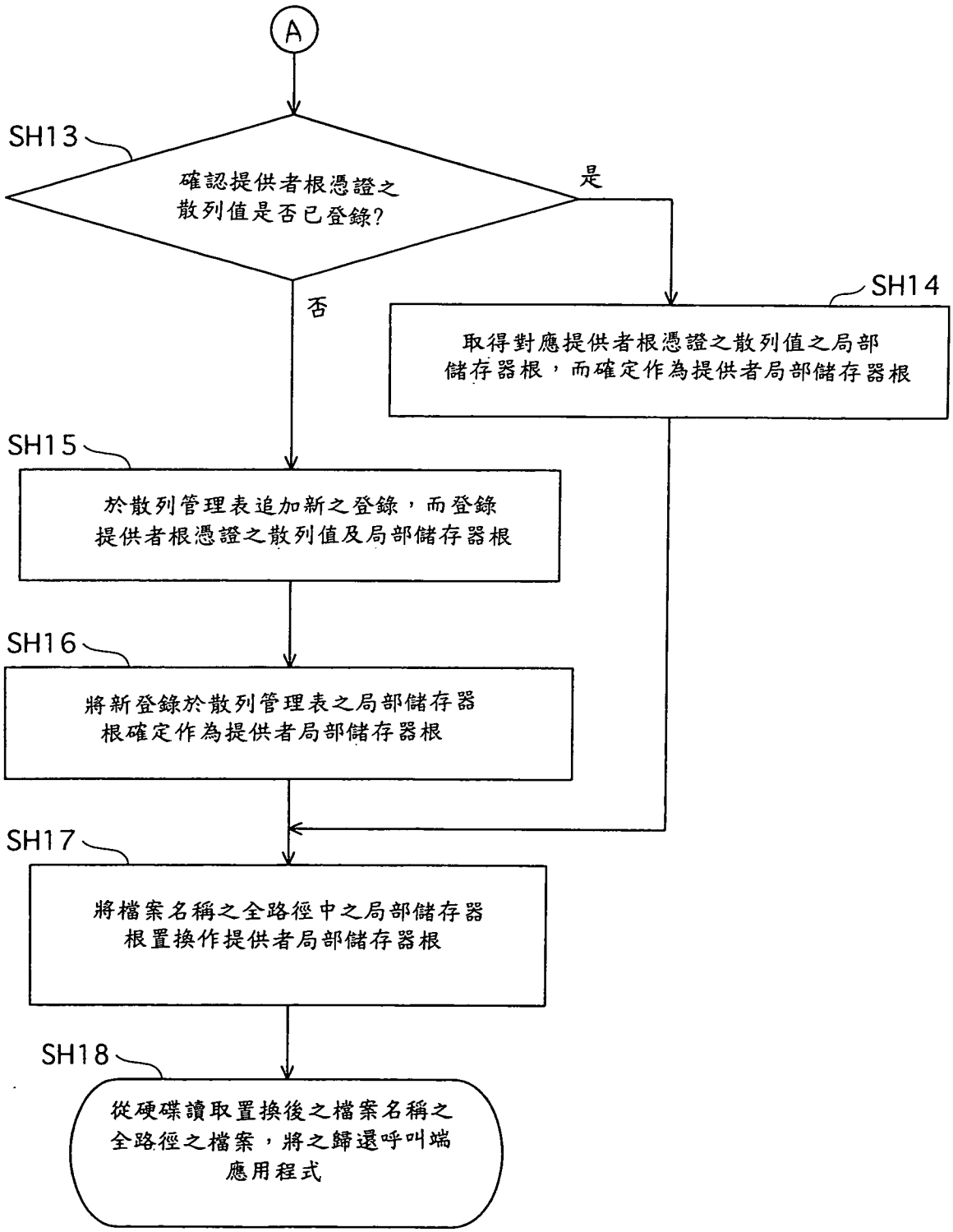
第 14 圖


組織ID之取得
確認bd.XXXX.perm
是否存在?
SF01
否
SF02
不歸還組織ID
而結束存取
是
SF03
從應用程式管理器取得對應呼叫端
應用程式之組織ID，將該值歸還而結束

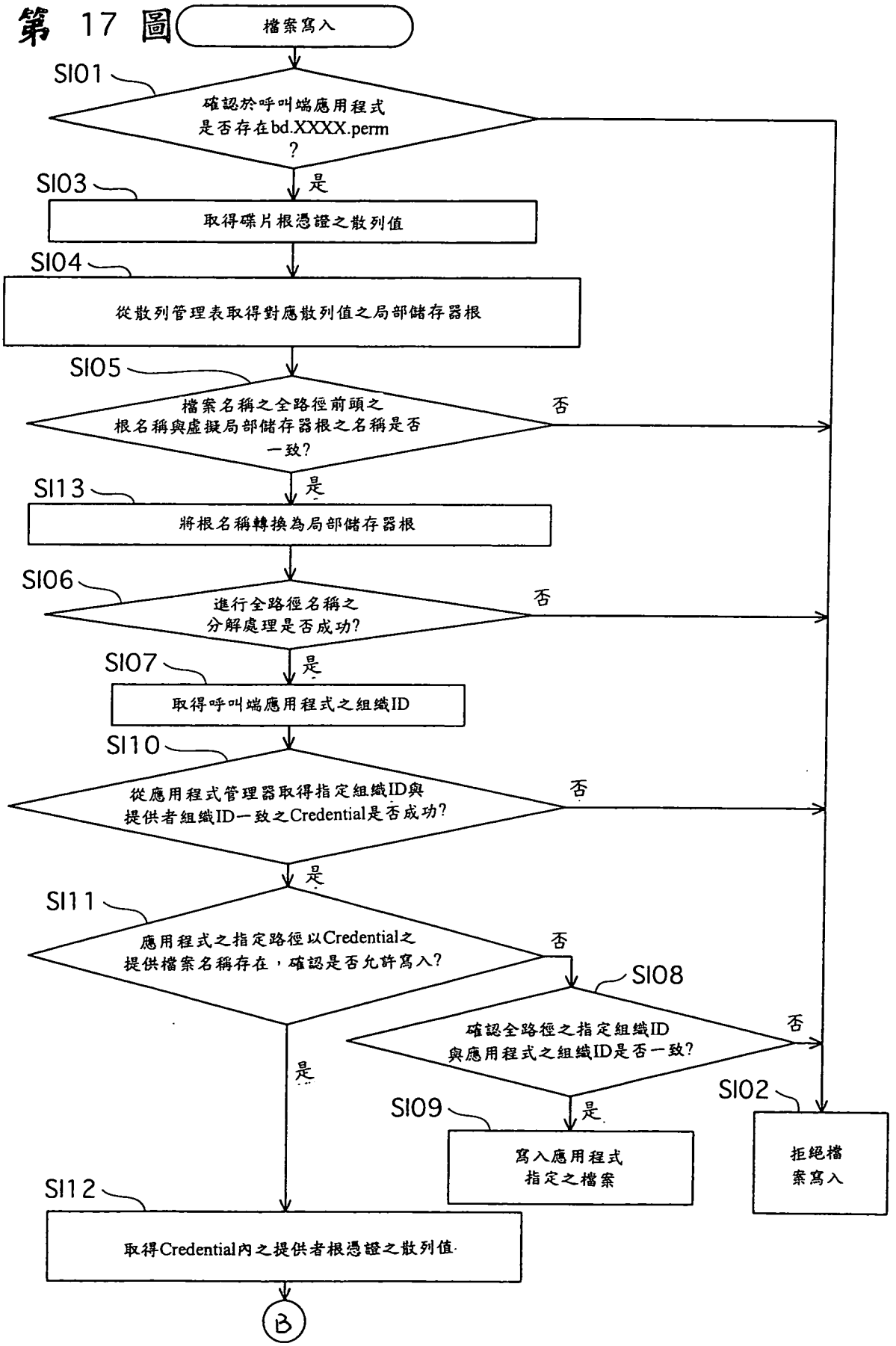
第 15 圖


檔案讀取
SH01
確認bd.XXXX.perm.
是否存在於應用程式?
是
否
SH03
計算碟片根憑證之散列值
SH04
取得對應散列管理表之散列值之局部儲存器根
SH05
檔案名稱之全路徑前頭之
根名稱是否與虛擬局部儲存器根之名稱
一致?
否
是
SH13
將根名稱轉換為局部儲存器根
SH06
進行全路徑名稱之
分解處理是否成功?
否
是
SH07
取得呼叫端應用程式之組織ID
SH10
從應用程式管理器取得指定組織ID
與提供者組織ID之Credential是否成功?
否
是
SH11
應用程式指定路徑以Credential之
提供檔案名稱存在，確認是否允許讀取?
否
SH08
確認全路徑之組織ID與
應用程式之組織ID是否一致?
否
是
SH09
讀取應用程式
指定之檔案
SH02
拒絕檔
案讀取
是
SH12
取得Credential內之提供者根憑證之散列值
A

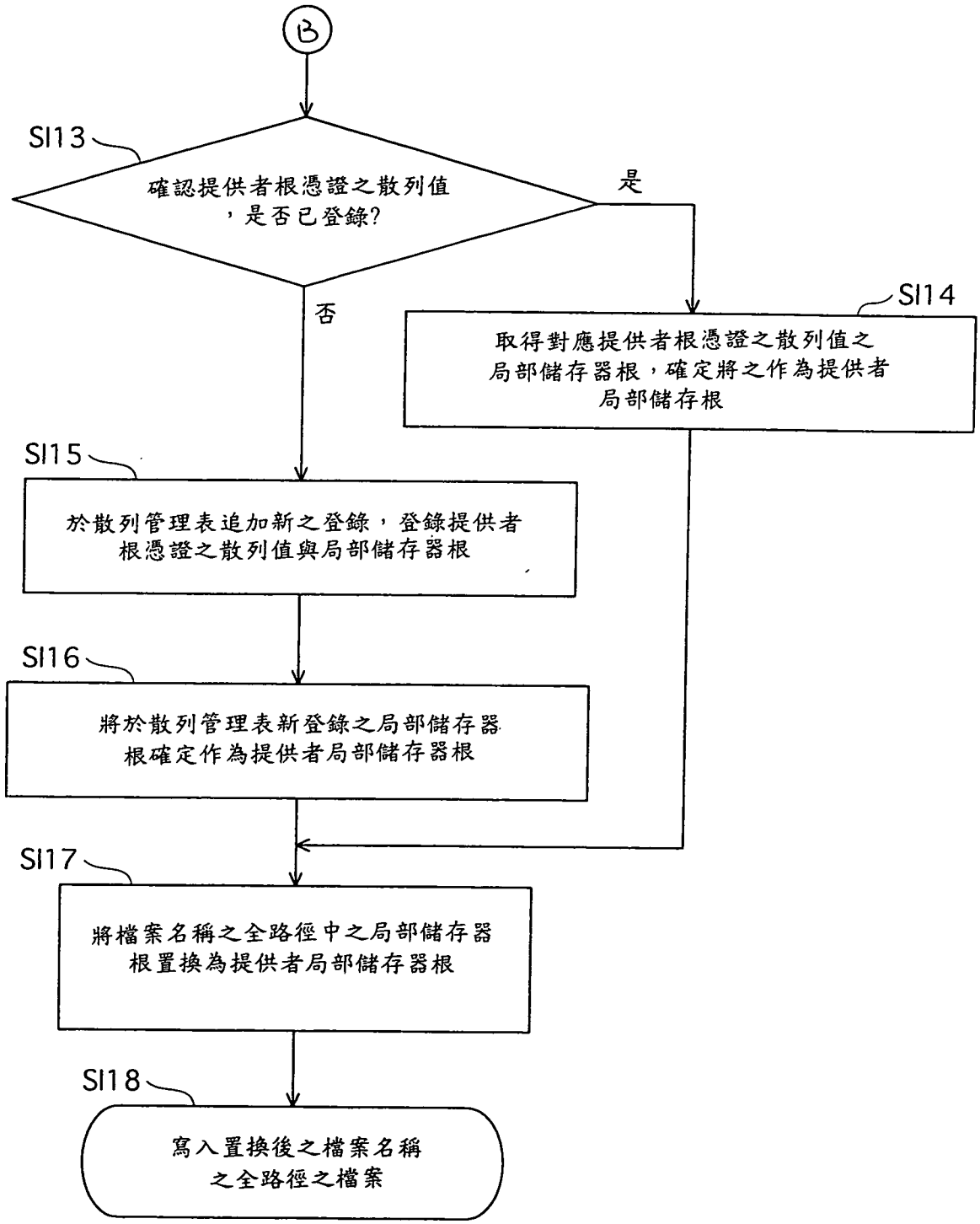
第 16 圖


A
SH13
確認提供者根憑證之散列值是否已登錄?
是
否
SH14
取得對應提供者根憑證之散列值之局部儲存器根，而確定作為提供者局部儲存器根
SH15
於散列管理表追加新之登錄，而登錄提供者根憑證之散列值及局部儲存器根
SH16
將新登錄於散列管理表之局部儲存器根確定作為提供者局部儲存器根
SH17
將檔案名稱之全路徑中之局部儲存器根置換作提供者局部儲存器根
SH18
從硬碟讀取置換後之檔案名稱之全路徑之檔案，將之歸還呼叫端應用程式

第 17 圖


檔案寫入
S101
確認於呼叫端應用程式是否存在bd.XXXX.perm?
是
否
S103
取得碟片根憑證之散列值
S104
從散列管理表取得對應散列值之局部儲存器根
S105
檔案名稱之全路徑前頭之根名稱與虛擬局部儲存器根之名稱是否一致?
是
否
S113
將根名稱轉換為局部儲存器根
S106
進行全路徑名稱之分解處理是否成功?
是
否
S107
取得呼叫端應用程式之組織ID
S110
從應用程式管理器取得指定組織ID與提供者組織ID一致之Credential是否成功?
是
否
S111
應用程式之指定路徑以Credential之提供檔案名稱存在，確認是否允許寫入?
是
否
S108
確認全路徑之指定組織ID與應用程式之組織ID是否一致?
是
否
S109
寫入應用程式指定之檔案
S102
拒絕檔案寫入
S112
取得Credential內之提供者根憑證之散列值
B

第 18 圖


B
SI13
確認提供者根憑證之散列值，是否已登錄?
是
否
SI14
取得對應提供者根憑證之散列值之局部儲存器根，確定將之作為提供者局部儲存根
SI15
於散列管理表追加新之登錄，登錄提供者根憑證之散列值與局部儲存器根
SI16
將於散列管理表新登錄之局部儲存器根確定作為提供者局部儲存器根
SI17
將檔案名稱之全路徑中之局部儲存器根置換為提供者局部儲存器根
SI18
寫入置換後之檔案名稱之全路徑之檔案