申請日期：	IPC分類
申請案號：	

(以上各欄由本局填註)

發明專利說明書

一、發明名稱	中 文	
	英 文	
二、發明人(共6人)	姓 名(中文)	4.梅森，卡爾頓 基斯 5.瑞迪，亞結庫馬 卡卡拉 6.凡卡塔拉馬帕，維許瓦納特
	姓 名(英文)	4.MASON, Carlton Keith 5.REDDY, Ajaykumar Karkala 6.VENKATARAMAPPA, Vishwanath
	國 籍(中英文)	4.美國 US 5.美國 US 6.美國 US
	住居所(中 文)	4.美國78727奧斯汀市巴瑞克小灣12602號 5.美國德州78717奧斯汀市奧羅小灣15512號 6.美國德州78717奧斯汀市弗里契路8704號
	住居所(英 文)	4.12602 Barricks Cove, Austin, Texas 78727 USA 5.15512 Omro Cove, Austin, Texas 78717 USA 6.8704 Fritsch Drive, Austin, Texas 78717 USA
三、申請人(共1人)	名稱或姓 名(中文)	
	名稱或姓 名(英文)	
	國 籍(中英文)	
	住居所(營業所)(中 文)	
	住居所(營業所)(英 文)	
	代表人(中文)	
	代表人(英文)	

一、本案已向

國家(地區)申請專利	申請日期	案號	主張專利法第二十四條第一項優先權
美國 US	2002/09/19	10/246,909	有

二、□主張專利法第二十五條之一第一項優先權:

申請案號:

無

日期:

三、主張本案係符合專利法第二十條第一項□第一款但書或□第二款但書規定之期間

日期:

四、□有關微生物已寄存於國外:

寄存國家:

寄存機構: 無

寄存日期:

寄存號碼:

□有關微生物已寄存於國內(本局所指定之寄存機構):

寄存機構:

寄存日期: 無

寄存號碼:

□熟習該項技術者易於獲得,不須寄存。

五、發明說明 (1)

一、【發明所屬之技術領域】

本發明係相關但非限於應用伺服器安全管理系統與工具領域。

二、【先前技術】

應用伺服器是一種在例如企業內部網路或網際網路的分散式網路內經由電腦或計算機平台所執行的伺服器程式，並且提供商業邏輯運作以作為一種應用或服務。像國際商業機器(IBM)、微軟公司(Microsoft Corporation)、以及昇陽微系統(Sun Microsystems)等公司所提供的套裝軟體就適用於在一些廣泛且多樣化的硬體平台上開發、管理、佈署、並執行應用伺服器，該硬體平台包括但不限於個人電腦、網路伺服器、大型電腦主機、以及工作站，並得以廣泛且多樣化的作業系統為標的，其作業系統包括但不限於UNIX、Linux、IBM's AIX、OS/2、以及OS/390、微軟的視窗軟體、以及昇陽的Solaris。IBM提供一種廣為人知且廣泛使用稱為WebSphere的應用伺服器組。

應用伺服器可以用例如"C"的高階語言(HLLs)，或是利用昇陽微系統的JAVA可攜式語言，或是其組合來撰寫。部分的應用邏輯可以在Enterprise Java Beans("EJB")，動態連結程式庫("DLL")，程式物件，應用小程式(applets)，以及伺服小程式servelets中實現，並依其設計方法與所使用的語言來開發應用伺服器程式。

五、發明說明 (2)

典型的應用伺服器需與用戶端的電腦與電腦處理流程配合，例如經由網路瀏覽器與遠端終端機的電腦處理流程而與使用者形成界面，藉以提供所需的功能或服務。一般在用戶端電腦與電腦處理之間的傳輸協定(protocol)包括但不限定於超文件傳輸協定(HTTP)、傳輸控制協定/網際網路傳輸協定(TCP/IP)、安全套件層(SSL)、以及檔案傳輸協定(FTP)。用戶端與應用伺服器配合的電腦處理包括但不限定於獨立的(例如獨立於瀏覽器之外)用戶端程式、超文件標示語言(HTML)資源、瀏覽器擴充或外掛式裝置、可擴充標示語言(XML)資源、繪圖與多媒體物件(例如TIFF、GIF、JPEG、AVI等等)、Java伺服器網頁(JSP)、動態伺服器網頁(ASP)、個人家庭網頁(PHP)、Java模組、與Java Beans。

應用伺服器能夠與其他例如檔案系統與資料庫的系統資源產生互動，而能夠讀取、儲存、創造以及複製資料等。這些系統資源可以經由例如存在本身電腦快取記憶體中的應用伺服器來直接管理，或是由其他可存取的伺服器來管理。

應用伺服器也時常和安全性授權與驗證的伺服器共同合作以確認使用者的身分，以及該使用者是否擁有許可或優先權以執行其請求的動作，並存取資源或其所需的資料等等。

五、發明說明 (3)

應用伺服器和這些授權與驗證電腦處理之間溝通的傳輸協定，就如同與其他系統資源之間一樣，可以包括任何前述所列的用戶端通訊之傳輸協定，並且通常包括其他由業者自訂規格的傳輸協定，就如同Java Version 2 Enterprise Edition(J2EE)介面與通訊模式以及Common Object Request Broker Architecture(CORBA)。

工業界有許多使用CORBA的實例，包括IBM的SOM與DSOM架構、網景公司的開放式網路環境(ONE)、昇陽的RMI、以及微軟的COM與DCOM架構。這些架構能允許用戶端應用程式物件去"發掘"其他可能有用或有需要的程式物件的存在，並可藉以完成一件任務或服務。有一種物件需求仲介(ORB)能讓用戶端傳送出請求特定功能的訊息就是一個這種架構之下的組件。此時ORB就可以轉遞給ORB所知能夠提供合乎用戶端所需功能的伺服器。之後用戶端與伺服器之間就產生互動以決定予使用者適當的介面，使得用戶端得以使用伺服器所提供的程式物件。

CORBA架構的特定使用項目就是定義在可互通物件參照表(IOR)。IOR所提供的物件參照獨立於該物件所常駐的平台，並且與ORB的使用無關。

當這些分散物件應用的型態漸趨複雜，有許多的應用

五、發明說明（4）

管理系統就被導入市場中了。應用管理包括控制與監視一個應用從其安裝到設定，在整個使用生命週期期間包括量化分析的資料蒐集並調整達到最大的效率與反應速度。可為應用管理系統所接受的模式通常是一種管理員-代理人(manager-agent)模式。該應用負責提供特定資訊給管理系統、對於從管理系統代理人而來的資訊請求行為做出反應、並與管理系統代理人做溝通。通常管理系統代理人與被管理的應用程式會在同一硬體平台上運作。

管理系統與一個或多個代理人之間做溝通，而代理人本身再與被管理的應用程式接觸。管理系統與其代理人之間可以使用一種自訂的傳輸協定做溝通，或者也可以使用一種開放式的傳輸協定例如簡單網路管理協定(SNMP)或是利用Java延伸管理技術(JMX)。一些市場上可取得的管理系統是例如Tivoli的管理環境(Tivoli's Management Environment)以及IBM的WebSphere管理應用程式。

圖3顯示出一種使用JMX Management Bean，或稱Mbeans作為管理系統的實施例。Mbeans是一種可經由標準JMX界面取得的物件，並可提供設計者將特殊應用管理介面展現出來的能力。JMX伺服器（JMX MBeanServer）33執行應用伺服器管理物件（Application Server MBean）34，而應用伺服器管理物件就是負責將應用伺服器的介面顯示給管理應用程式。同樣地，JMX伺服器33也可執行應用管理

五、發明說明 (5)

物件（Application MBean）35，而其中應用管理物件可將該應用程式(32)的特殊管理介面顯示給管理應用程式(37)。JMX伺服器(33)也提供了許多必須的轉接器(36)以連接一個或多個管理系統給該應用程式使得應用程式管理員的管理工具能被運用並與該應用程式連結。

目前IBM WebSphere應用伺服器的版本中，有一個管理伺服器是與所有受其管制的管理需求接觸的中心點。保護此管理伺服器僅需要將應用伺服器設定成安全等級的用戶，但該應用伺服器無須被設定為安全等級的伺服器。就如同使用者物件不允許出現在管理伺服器上一樣，管理伺服器物件也不允許出現在應用伺服器上，此方法某些時候符合技術上的需要。

然而，應用程式的發展已經逐漸包括管理上的功能並且已經可以在應用伺服器上使用管理物件，物件級安全(而非伺服器等級的安全)是必要的但傳統架構(legacy architectures)並不支援。在一些系統中，所有的應用程式處理皆包括需受到保護的管理資源，雖然使用者的資源可能需要也可能不需要受到保護。在目前伺服器等級安全的安全架構之下，若使者物件安全是無作用的，則管理物件安全也是無作用的。對於實際上無須受保護的使用者物件安全而言，對應用到這些使用者物件的電腦處理要求身分確認與授權將導致不需要且不受歡迎的效能損失。若該

五、發明說明（6）

系統內定取消安全設定包括管理資源的安全設定，則該系統將會不必要且不情願地經由管理功能暴露出安全上的缺口。因此，技術上對於一種能提供物件級安全架構的應用伺服器系統或方法就產生了需求，該應用伺服器含有使用者物件與管理物件。

三、【發明內容】

此處提供的流程與機制允許對於管理物件與指定的物件之安全機制得以個別地宣告啟動或不啟動，而不論在一個安全網域內的應用伺服器對伺服器為基礎之使用者物件安全機制的啟動與否。特別是在以IBM WebSphere Application Server產品為基礎的應用環境中，在相同的流程中為維護管理上的安全性時，此方式具有讓使用者安全性失效的能力。

為維護在其他應用伺服器上使用者物件的安全性並經由該安全的網域確保全球管理物件的安全時，客戶（例如應用伺服器擁有人與操作員）得選擇性地在一個安全的網域內於一些應用伺服器中取消使用者物件安全。管理安全與內部系統管理等等的管理功能也因此可以由使用者安全性中分離並加以控管。

當使用此處揭露的流程與機制時，用戶端電腦處理流程並不會察覺一應用物件是屬於使用者物件或是管理物件

五、發明說明 (7)

而僅會察覺每一個物件使否需要實行安全性檢查動作。同時我們的流程也允許宣告以分類和封包所保護的物件之定義。

一般而言，為實現一個應用伺服器物件級安全的可架構性，一CORBA架構會被採用，其ORB會將IOR's作為分享物件而傳輸到名稱伺服器。受保護物件的IOR's，例如管理物件都設有一標籤組件以作為使用此項服務的安全性說明。而如使用者物件的未受保護物件之IOR's，則該物件傳輸無須標籤組件。在任何特定物件傳輸時，有一IOR攔檢器會被啟動。此IOR攔檢器會載入一個列出需受保護的管理物件或管理封包的符號描述檔案。當整體性安全於該安全網域中啟動時，此種方式能使載明的單一物件、單獨物件的列表、或物件的封包皆受到保護。

只要是在符號描述檔案中的物件，IOR's在傳輸時都會有附安全性標籤的部位。稍後，當用戶端拾取此一附標籤的IOR時，該用戶就會知道該伺服器釋出此種請求時的安全性要求。倘若IOR未設有標籤，則不需任何安全防衛手段即可請求該伺服器的服務。針對這些無安全性的物件，用戶端將不會送出任何使用者安全資訊給應用伺服器也不會保護對應用伺服器的傳輸，因而使得使用者物件的效能獲得改善並避免了對使用者物件不必要的保護。

五、發明說明（8）

一般而言，有兩種型態的旗標被用以設定網域中的物件級安全：(a)一種整體(網域等級管理安全)安全性旗標，以及(b)一個或多個的應用伺服器安全性旗標。前者係維護網域等級的安全，後者則針對個別的應用伺服器。整體安全性旗標決定了經由此網域的所有管理物件是否受到保護。這些管理物件通常也列在前述的符號描述檔案之中。而每一應用伺服器安全性旗標僅會啟動或停止該相關應用伺服器上使用者物件的安全防護，但不影響該伺服器上管理者物件的安全性。

四、【實施方式】

本發明更可被視為存在已知例如個人電腦、網路伺服器、以及網路瀏覽器的計算機平台上企業伺服器軟體的一種特徵、延伸、或改良。這些一般的計算機平台可能包括個人電腦、工作站、大型電腦、及想像得到能夠攜帶的計算機平台，例如個人數位助理(PDA)、可上網無線電話、以及其他樣式的個人資訊管理(PIM)裝置。

因此，檢視一個計算機平台的一般化架構是很重要的，該平台可以橫跨許多不同的應用範圍，從高階的網路或企業伺服器平台到個人電腦、攜帶型PDA或可上網無線電話。

如圖1，呈現一個一般化的架構包括一個中央處理單元

五、發明說明 (9)

1(CPU)，中央處理單元原則上是由一個微處理器2與隨機存取記憶體(RAM)4以及唯讀記憶體(ROM)所組成。通常該CPU(1)也設有快取記憶體3以及可程式化快閃唯讀記憶體6。微處理器與各種不同CPU記憶體間的介面7
通常是利用一種內部的匯流排，但也可以用一種更一般化或工業標準化的匯流排。

許多計算機平台也設有一個或更多的儲存裝置9，例如硬碟機(HDD)、軟碟機、光碟機(CD、CD-R、CD-RW、DVD、DVD-R等)、以及特定規格磁片與磁帶機(例如Iomega Zip與Jaz，Addonics SuperDisk等)。此外，一些儲存裝置也可以在電腦網路上取得。

許多計算機平台依其原始設計功能也設有一個或多個通訊介面10。例如一部個人電腦通常設有一個高速串列埠(RS-232，RS-422等)、一個增強型並列埠(EPP)、以及一個或更多的泛用串列匯流排(USB)埠。該計算機平台亦得設有一內部區域網路(LAN)介面，例如乙太網路卡、以及其他高速介面，例如高效能串列匯流排IEEE-1394。

無線電話與無線上網PDA的計算機平台亦得設有一附天線之無線電射頻介面。在一些實例中，該計算機平台亦得設有一紅外線資料傳輸(IrDA)介面。

五、發明說明 (10)

計算機平台亦常設有一個或數個內部擴充槽11，例如工業標準架構ISA、增強型工業標準架構EISA、週邊零件連接介面PCI、或是為其他額外硬體例如音效卡、記憶卡、以及圖形加速卡所設的特殊介面。

此外，許多的單元例如膝上型電腦以及PDA's也設有一個或更多的外部擴充槽12能讓使用者輕易地安裝與除去擴充的硬體裝置，例如PCMCIA卡、SmartMedia卡、以及如可拆式硬碟機、光碟機、和軟碟機等各種不同之特殊模組。

通常，儲存裝置9、溝通介面10、內部擴充槽11以及外部擴充槽12皆是經由一個如ISA、EISA或PCI的標準或工業開放式匯流排架構8連接CPU1。在一些實例中，該匯流排得為特殊規格設計。

一個計算機平台通常設有一個或多個鍵盤或袖珍鍵盤16、滑鼠或指標裝置17、以及/或觸控銀幕顯示器18的使用者輸入裝置。以個人電腦為例，一個完整的鍵盤上通常也設有一個滑鼠或是像軌跡球或軌跡點的指標裝置。以可上網無線電話為例，一個簡單的袖珍鍵盤並得設有一個或多個的特殊功能鍵。以PDA為例，通常會附有一個觸控式面版18並具備手寫辨識能力。

此外，該計算機平台通常設有一個麥克風19，例如可

五、發明說明 (11)

上網無線電話的麥克風或是個人電腦上的麥克風。此麥克風可供作簡易的回報播送裝置與語音訊號，亦得用以輸入使用者選擇項，例如網站的語音導航或運用語音辨識功能來做自動撥號。

許多的計算機平台也配備有照相裝置100，例如一個固定式數位相機或全動態影像數位像機。

一個或多個顯示器13的使用者輸出裝置通常皆與大部分的計算機平台一起提供。顯示器13有許多型式，包括陰極射線管(CRT)、薄膜平面電晶體(TFT)陣列、簡單的一組發光二極體(LED)，或液晶顯示(LCD)指示器。

一個或多種揚聲器14以及/或傳聲裝置15通常也與計算機平台結合。此揚聲器14得用以重新產生聲音與音樂，例如無線電話的揚聲器或是個人電腦的揚聲器。傳聲裝置15得以是簡單的警告聲發音器或蜂鳴器，常見於如PDA與PIM等特定裝置上。

使用者輸出入裝置得直接經由特殊匯流排結構與/或介面而與CPU1連接(8'，8")，或得經由一個或多種如ISA，EISA，PCI等等的工業開放匯流排連接。

該計算機平台亦設有一個或多個軟體與韌體101程式以

五、發明說明 (12)

實現此計算機平台所要的功能。

圖2對於計算機平台範圍內的軟體與韌體101之一般化結構有更詳盡的說明。一個或多個作業系統(OS)原應用程式23得於該計算機平台上提供，例如文書處理器、電子表單、多功能聯繫管理(contact management utilities)、通訊錄、月曆、郵件用戶、簡報、財務與簿記等程式。

此外，一個或更多可攜式或獨立裝置程式亦得以使用，這些例如爪哇描述語言與程式必須由特定平台的原始作業系統的翻譯器25加以翻譯。

通常，計算機平台亦設有某種網路瀏覽器或小型瀏覽器26，而得以包括一個或多個擴充瀏覽器例如外掛式瀏覽器27。

該計算機裝置通常設有一作業系統20，例如Microsoft Windows、UNIX、IBM OS/2、LINUX、MAC OS、或其他特定的平台作業系統。其他較小型的裝置如PDA與無線電話亦得以配置其他種類的作業系統如即時作業系統(RTOS)或Palm Computing's PalmOS。

一組基本輸出入功能(BIOS)與硬體裝置驅動程式21也常用來使得該作業系統20與程式能連接並控制該計算機平

五、發明說明 (13)

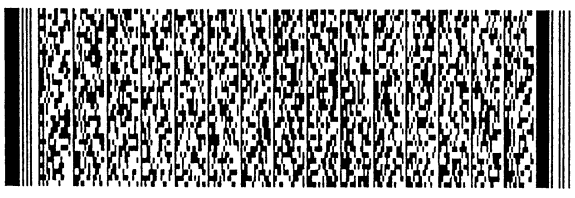
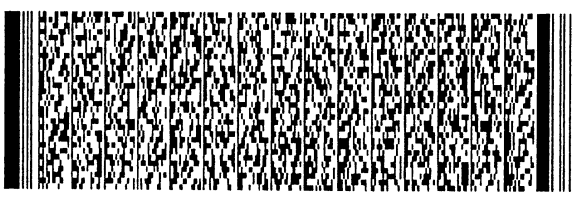
台上所提供的特定硬體功能。

此外，許多計算機平台也常一起提供一個或更多的內建韌體程式22，這些程式可以藉由電路板中的或內建的微處理器來執行以作為週邊裝置的一部份，週邊裝置例如一個微控制器或硬碟裝置，一個通訊處理器，網路介面卡，音效卡或繪圖卡。

圖1與圖2本身對於各種硬體零組件與各種不同計算機平台的軟體與韌體程式已有一般性的描述，其計算機平台包括但不限定於個人電腦、PDA、PIM、可上網電話以及其他家電用品如網路電視(WebTV)。現在我們可將注意力集中到本發明所揭露關於在這樣一個計算機平台上軟體與韌體導入的較佳流程與方法。對熟知此項技藝人士而言，應可接受以下方法與流程最好以硬體功能性來加以理解，無論是部份或整體觀之皆不脫離本發明之精神與範圍。

現在我們可將注意力轉到本發明方法之描述與其相關之組件。在一可能的實施例中，可視為Java Beans的集合或群聚，其存取與修改特定系統檔案與資源如以下章節的詳細敘述，不過亦得以整合到現存如網路伺服器套件的軟體中而不脫離本發明之精神與範圍。

在一個簡化的實施例中，在以OMG介面定義語言(IDL)

五、發明說明 (14)

定義的物件中導入CORBA架構，物件分散在伺服器與用戶端之間，物件請求仲介(ORB)被用以協調尋找與使用所得到的物件與服務。IDL編譯器完成了CORBA的聯繫並產生用戶分株與伺服器的輪廓並映照出從該伺服器環境到用戶端的每一個物件服務。用戶與伺服器之間以及伺服器之間的通訊協定是用General Inter-ORB Protocol(GIOP)與Inter-ORB Protocol(IIOP)，IIOP能完成GIOP在傳輸控制協定/網際網路傳輸協定(TCP/IP)上的傳輸。可互通物件參考(IOR)提供了不同平台與不同ORB導入物件的參考。在CORBA架構內會提供一個名稱伺服器以便將每一個CORBA物件連接到一個公開名稱。

更進一步來看此實施例中，利用到一個Enterprise Java Bean(EJB)程式設計模型以使物件介面與伺服器的導入皆符合Java的定義。物件是分散的，故可由遠端存取，且包括遠端方法調用(RMI)在內的Java通訊協定也會被使用到。本實施例是使用IBM WebSphere應用伺服器產品而得以完成，該產品是架構在IMB企業伺服器並執行AIX或Linux的作業系統。由於目前WebSphere的版本僅支援RMI-IIOP，用戶端不得使用Java RMI傳輸協定中的RMI-JRMP格式。而在使用其他網路應用環境的實施例中，此一限制就不需要了。同樣地，Java名稱伺服器(JNDI)也被用做此實施例中的名稱伺服器。

五、發明說明 (15)

儘管一般的CORBA與EJB的原理、傳輸協定、程式設計方法與功能於此技藝中為普遍習知，且儘管WebSphere產品廣為使用而其本身亦廣為熟悉，習知此項技術之人仍可認知到本發明得以其他程式設計方法、傳輸協定、計算機平台、作業系統架構與網路應用伺服器產品來實現而不脫離本發明之精神與範圍。例如，一些具備潛在能力得以實現本發明的應用伺服器，包括Oracle's 9i產品、BEA Systems WebLogic平台、Sun Microsystem的ONE應用伺服器、Hewlett-Packard的應用伺服器以及JBoss。以作業系統而言，Unix、Linux、Novell的Netware、IBM的AIX與OS/2、Sun Microsystem的Solaris、Hewlett-Packard的HP-UX以及微軟的視窗軟體亦得以任意地利用在不同的實施例中。

圖4根據本發明表示出一個用戶系統43與多重應用伺服器41，42之間的交互作用與關係40，包括一個管理節點代理人47與名稱伺服器46。該應用伺服器41，42、管理節點代理人47與名稱伺服器46就是提供應用給用戶系統43的網域45的一部份。

當應用請求出現時，在一個IOR攔檢器載入後，特定的初始化程序即行展開，並給予從每一個應用伺服器41，42傳輸412，413，414，415，416到名稱伺服器46的分享物件做參考，使分享物件得以被用戶43尋得。

五、發明說明（16）

當物件正被傳輸到名稱伺服器時，有一個IOR攔檢器會檢驗每一個物件。在ORB創造IOR的期間內，對每一個組件，所有的IOR攔檢器都會被啟用一次。這些IOR攔檢器的目的是在IOR加上標籤組件，用以增加額外的資訊以允許該伺服器傳出資訊並完成該項服務。之後該資訊即得以被需用到此項服務的用戶所讀取。對一個受到安全防護的伺服器而言，置於該標籤組件上的資訊得含有參數，該參數包括該伺服器所注意的安全套接層(SSL)的指示資訊、用戶端必須使用何種SSL與該伺服器連接、該伺服器支援何種安全機制、用戶必須提供何種必要資訊(例如使用者名稱、密碼、認證等等)、以及該伺服器屬於何種領域讓用戶端能提醒使用者所登入的伺服器是屬於何種領域等等。若安全防護未啟動，則IOR不會加上任何標籤組件。

當IOR攔檢器載入時，該攔檢器會載入一個類似文件檔並含有需要受到保護的管理物件之等級與封裝名稱的檔案，即便在應用伺服器上的其他使用者物件皆未受保護的狀態之下。管理物件得為管理員視為需永遠受到保護的物件，無論應用伺服器上的使用者物件是安全或不安全。例如圖中，應用伺服器1(41)提供皆受到安全保護的使用者物件與管理物件。因此，安全的IOR就能傳送412，413到名稱伺服器46。然而，應用伺服器2(42)提供不需受保護的使用者物件403，因此這些使用者物件403所產生的不安全IOR就

五、發明說明 (17)

會被傳送到名稱伺服器46，同時在同一伺服器42上，對安全保護的管理物件所產生的安全的IOR也會一併傳送。

如此則能允許客戶以伺服器為基礎的取消伺服器的安全性，而無需與管理上的安全性妥協。當管理員修改應用伺服器的安全性時，整體的(例如整個網域的安全)安全防護仍必須保持啟動狀態。在取消特定應用伺服器的安全性並啟動整體安全防護的情況下，IOR攔檢器會載入一個無論使用者物件狀態為何皆須保持安全性的等級與封裝的列表(如同文件檔案)，並決定對每一被保護的管理物件而言是否必要以及何種標籤組件需要傳送。而使用者物件並不是此保持安全的封裝或等級名單上的一員，因此有一種宣告的方法可供管理員修改該網域中需保持的安全性等級。就其本身而言，使用者物件並不包括在該列表中，也因此其IOR's不會收到標籤組件；而管理物件包括在該列表中，若其被視為有安全上的敏感性則其IOR's會收到標籤組件。無論是使用者物件或管理物件的所有物件都會加到由名稱伺服器46所負責的命名區間。如此可產生一個以等級為基礎並可宣告設定的物件安全體系。

由於使用此一協定與流程，當一個用戶端物件405 請求使用從一個安全防護完全啟動的伺服器如應用伺服器1(41)而來的物件時，所有用戶端43與該物件400，401之間的交換事務407都會在安全的狀態下進行。當該用戶物件

五、發明說明 (18)

405查詢406應用伺服器上的物件之名稱伺服器46的IOR's時，其將會接收到標籤。亦即暗示所有的物件400，401皆受安全保護且必須被安全地使用407。一個認證與授權的流程得以被安全地用來410提供安全性服務，如由標籤所表示的安全性服務、或由例如WebSpher的認證引擎與授權引擎、或者藉由管理節點47與一個或多個的管理物件402所提供的安全性服務。

當一個用戶端電腦處理試圖使用未啟動使用者物件安全機制的應用伺服器2(42)所提供的使用者物件403時，查詢406的行為將不會產生能被用戶端電腦處理流程接收到的標籤，也因此當與使用者物件403不安全地互動408時不會有任何安全機制的流程被啟動。因此，與這些使用者物件403之間的溝通與互動408得以在匿名(無認證或身分證明)以及/或完全透明(無傳輸保護)的狀態下進行。然而當使用到由應用伺服器2(42)所提供的管理者物件404時，該查詢的行為將會收到標籤並使管理節點釋出安全機制的功能，例如WebSpher的授權引擎與認證引擎。因此，當管理者物件404仍保持安全的情形下，應用伺服器2成功地容許在無安全機制的狀態下讓用戶端利用使用者物件403，也暗示了原有效能的提昇(例如用戶端不請求認證、伺服器不請求授權、不產生憑證與儲存等等)。

為更容易理解圖4，以粗箭號(寬箭號)加斜線表示不安

五、發明說明 (19)

全的通訊或互動(如408)，而無斜線的寬箭號則表示安全的通訊或互動(如407，410，411)。同樣地，細箭號(如412，413，414，415，416)則表示傳送加了標籤組件的安全物件之IORs，而粗體線的箭頭則表示傳送未加標籤組件的不安全物件之IORs。

總括並檢視此新流程，無論有無標籤組件，在IOR's適當的產生之後，當用戶端請求一個不安全也無認證的使用者物件時，該用戶物件會查詢IOR、接收IOR、且ORB也會呼叫一個或多個請求攔檢器，包括一個安全請求攔檢器。由於該IOR不包括標籤組件，因此無須認證與SSL即可產生一個TCP/IP的請求。此允許了在無憑證、認證或授權的情況下利用使用者物件。然而，使用任何管理物件或受保護的使用者物件都會觸發認證與授權的流程以及安全通訊(如SSL)的使用，即使這些受保護的物件與未受保護的使用者物件處於同一網域內。

圖5透過圖表描繪出前述附標籤組件的分享物件之IOR's傳輸的流程。在伺服器或應用程式啟動後51就會存取或載入52管理分類描述檔500，並對每一個分享物件53釋出54IOR攔檢器。無論是直接指定或是屬於特定套件中的一部份，若該物件屬於管理等級55則其所傳送57的IOR都會附有安全標籤。若該物件不屬於管理等級則通常56該物件IOR的傳輸不會附有安全標籤。對所有的分享物件與其IOR's的傳

五、發明說明（20）

輸時，此一檢查動作會一再重複。

圖6透過圖表描繪出前述用戶端請求一個分享物件或服務的流程60。其IOR會依所需的服務而受查詢61且其所接收的IOR也會受檢62看看是否有安全標籤。若63其認為請求與使用此項服務時的認證、授權、以及/或傳輸保護是必須的，則會採取一些必要的措施以取得認證、授權以及/或建立一個連到該應用伺服器的安全通訊連結。否則該項服務得被請求與使用而無須安全措施。

更進一步而言，根據此一使用WebSphere平台的實施例，一個從使用者物件而來的的授權引擎也會特別供作管理物件的授權引擎。WebSphere管理授權引擎提供一個以角色為基礎的授權模型或流程。因為使用者物件有一個個別的授權引擎，任何J2EE皆得被用作使用者物件安全機制。由於我們個別的使用者物件安全旗標與管理物件旗標(例如整體安全旗標)的獨特用途，該系統得以不同的授權與認證引擎分別定義與管理使用者物件與管理物件的安全性。此方式允許設定三種安全模式：

(a) 當應用伺服器的安全機制啟動且整體安全機制也啟動時，在網域內的已知伺服器上的所有(使用者與管理)物件皆受到安全保護。

(b) 當應用伺服器的安全機制未啟動但整體安全機制啟動時，在特定伺服器上僅有使用者物件是不安全的但管理物

五、發明說明 (21)

件仍保持安全狀態；且

(c) 當整體安全機制未啟動時，在網域內的所有伺服器上的所有物件(使用者物件與管理物件)皆不受安全保護。

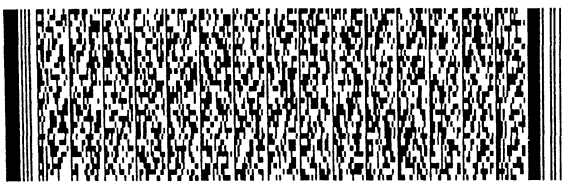
圖4的實施例中使用WebSphere與CORBA，該用戶端物件405與使用者物件400，403是Enterprise Java Beans (EJB's)，而管理物件401，402，與404是Java Management MBeans。其他合適的物件導向程式語言亦得任意使用。

本技術之背景、揭露的總結、摘要、以及詳細說明皆已提供包括不同實施例的選擇，以及特別查詢了特定的應用伺服器產品、作業系統、計算機平台、程式設計方法、以及通訊傳輸協定等。對於熟知此項技術之人而言，可容易地認知到此處所提供的細節僅為本發明之說明與理解，本發明的範圍並不限於這些實施例的細節而是由其後的申請專利範圍來界定。

例如，此揭露範圍已描述出一個實施例與其中使用CORBA、IIOP、與IOR的細節，並用以描述本發明的物件級安全流程與機制。本發明亦可應用到其他安全傳輸協定與物件模型，包括但不限定於網路伺服器安全機制。在一個網路伺服器安全模型中，訊息傳遞與物件函式呼叫皆經由簡單物件存取協定(SOAP)訊息來傳遞而非IIOP安全傳輸協定，並且該服務也由網路服務定義語言(WSDL)與網路服務

五、發明說明 (22)

端點語言(WSEL)來描述而非使用IDL。同樣地，通用描述探索與整合(UDDI)在網路服務模型中的使用也已取代CORBA的CosNaming，後者提供API以查閱IOR，同時前者提供一組API以查閱一個商業入口網站與網路伺服器入口網站。因此，在本實施例揭露的範圍中，吾等已使用IOR作為一種機制以傳達一個物件請求中的物件種類資訊，並得以利用任意的物件模型與相對應的傳輸協定來實現，例如在一網路服務UDDI物件登錄中提供物件種類資訊。



圖式簡單說明

五、【圖示簡單說明】

以下詳細敘述與在此所呈現的圖樣將使本發明完整的揭露。

圖1描述一種一般化的計算機平台架構，例如個人電腦、伺服器電腦、個人數位助理、可上網的無線電話、或其他以處理器為基礎的裝置。

圖2表示一種一般化的軟體與韌體與圖1的一般化架構結合。

圖3顯示一種典型的管理系統與應用之安排。

圖4以下是本發明之流程與其互動的示範實施例。

圖5通過圖表描述分享物件在導入的IIOP模型中傳送出含標籤組件的IOR之流程。

圖6通過圖表描述在導入的IIOP模型中，用戶請求一個分享物件或伺服器的流程。

圖示元件符號說明

1	中央處理單元	2	處理器
3	快取記憶體	4	隨機存取記憶體
5	唯讀記憶體	6	快閃唯讀記憶體
9	儲存裝置	10	溝通介面
11	內部擴充槽	12	以及外部擴充槽
13	顯示器	14	揚聲器
15	傳聲裝置	16	鍵盤
17	滑鼠/指標	18	觸控面板

圖式簡單說明

19 麥克風　　100 攝影裝置

101 軟體與韌體　　20 作業系統

21 基本輸出入功能與硬體裝置驅動程式

22 內建韌體程式　　23 應用程式

24 可攜式程式

25 特定平台的原始作業系統的翻譯器

26 瀏覽器　　27 外掛式瀏覽器

30 伺服器運作圖　　31 應用伺服器

32 應用程式　　33 JMX伺服器

34 應用伺服器管理物件　　35 應用管理物件

36 轉換器　　37 管理應用程式

40 用戶系統與多重應用伺服器之間作用與關係

41 多重應用伺服器　　42 多重應用伺服器

43 用戶系統　　45 網域

46 名稱伺服器　　47 管理節點代理人

400 使用者物件　　401 管理者物件

402 管理者物件　　403 使用者物件

404 管理者物件　　405 用戶物件

406 查詢　　407 交換事務

408 互動　　410 互動

411 互動

412，413，414，415，416 傳輸

50 物件系統

51 伺服器或應用程式啟動

圖式簡單說明

52 存取或載入管理分類描述檔

53 對每一個分享物件

54 對每一個分享物件釋出IOR攔檢器

55 是否屬管理等級

56 物件IOR的傳輸不附有安全標籤

57 所傳送的IOR都會附有安全標籤

58 是否有更多物件

59 結束

500 管理分類描述檔

60 用戶端請求一個分享物件或服務的流程

61 依所需的服務查詢IOR

62 檢查接收的IOR看是否有安全標籤

63 安全上是否需要利用服務

64 未經授權直接運用物件

65 執行安全性功能

66 使用傳輸保護及安全的物件

六、申請專利範圍

1. 一種用於分散式計算機網域的方法，包括：

分散式之一管理物件（distributing administrative objects）與一使用者物件（user objects）到一或多個應用伺服器；

針對管理物件的網域級安全定義一整體安全旗標；

以介面連接一或多個應用伺服器安全旗標（security flags）到前述分散式之該管理物件；以及

藉由設定在三種模式之一之一用戶端電腦協同合作的一應用伺服器執行一或多個安全性計算，其中一第一模式係當該整體安全旗標與前述連結之該應用伺服器安全旗標皆啟動時，則該使用者物件與該管理物件皆會受到保護，一第二模式是該使用者物件的使用不經安全性計算但該管理物件仍會受到保護，其中該整體安全旗標會啟動而前述之連結該應用伺服器安全旗標則不啟動，一第三模式是該使用者物件與該管理物件的使用不經安全性計算，其中該整體安全旗標不會啟動。

2. 如申請專利範圍第1項之方法，其中前述執行安全性計算的步驟包含提供一個別的安全性計算給該管理物件與該使用者物件。

3. 如申請專利範圍第1項之方法，其中前述該應用伺服器安全旗標與該管理物件介面的步驟包含選自一傳輸附標籤組件的COBRA IOR之群組給該應用伺服器的該使用者物件，

六、申請專利範圍

其中該應用伺服器之使用者物件安全機制是啟動的，同時亦在UDDI登錄上提供一組物件型態給該應用伺服器的該使用者物件，其中該應用伺服器之使用者物件安全機制是啟動的。

4. 如申請專利範圍第3項之方法，該方法更進一步包括存取受保護物件的一宣告列表。

5. 如申請專利範圍第1項之方法，該方法包括提供一WebSphere應用伺服器。

6. 如申請專利範圍第1項之方法，該方法包括提供如Enterprise Java Bean之一用戶端電腦處理。

7. 如申請專利範圍第1項之方法，該方法包括提供如Enterprise Java Beans之該使用者物件。

8. 如申請專利範圍第1項之方法，該方法包括提供如Mbeans之該管理物件。

9. 如申請專利範圍第1項之方法，該方法包括實行選自認證、授權、以及傳輸保護之一表單中之該安全性計算。

10. 如申請專利範圍第1項之方法，該方法包括利用選自簡

六、申請專利範圍

藉由設定在三種模式之一之一用戶端電腦協同合作的應用伺服器執行一或多個安全性的計算，其中一第一模式是當該整體安全旗標與該應用伺服器安全旗標皆啟動，則該使用者物件與該管理物件皆會受到保護，前述一第二模式是該使用者物件的使用不經安全性計算但該管理物件仍會受到保護，其中該整體安全旗標會啟動而前述的連結應用伺服器安全旗標則不啟動，一第三模式是該使用者物件與該管理物件的使用不經安全性計算，其中該整體安全旗標不會啟動。

24. 如申請專利範圍第23項之系統，其中該安全性計算包含一個別的安全性計算給該管理物件與該使用者物件。

25. 如申請專利範圍第23項之系統，其中連結該管理物件介面的該應用伺服器安全旗標包含選自傳輸附標籤組件的COBRA IOR群組之物件種類指示給該應用伺服器的該使用者物件，其中該應用伺服器之該使用者物件安全機制是啟動的，同時亦在UDDI登錄上提供一組物件型態給該應用伺服器的該使用者物件，其中該應用伺服器使用者物件安全機制是啟動的。

26. 如申請專利範圍第23項之系統，該系統進一步包含一受保護物件的宣告列表已決定IOR或UDDI的登錄入口必須修改以啟動該使用者物件安全。

六、申請專利範圍

27. 如申請專利範圍第23項之系統，該系統包含一WebSphere應用伺服器。

28. 如申請專利範圍第23項之系統，該系統包含一Enterprise Java Beans的用戶端電腦處理流程。

29. 如申請專利範圍第23項之系統，該系統包含一Enterprise Java Beans使用者物件。

30. 如申請專利範圍第23項之系統，該系統包含一MBeans管理物件。

31. 如申請專利範圍第23項之系統，該系統包含選自認證、授權、以及傳輸保護之一表單之該安全性計算。

32. 如申請專利範圍第23項之系統，該系統包含一選自簡單物件存取協定與Inter-ORB傳輸協定群組的安全傳輸協定。

33. 如申請專利範圍第23項之系統，該系統包括選自IDL與網路服務定義語言加上網路服務端點語言和介面定義語言的群組之一服務描述模型。

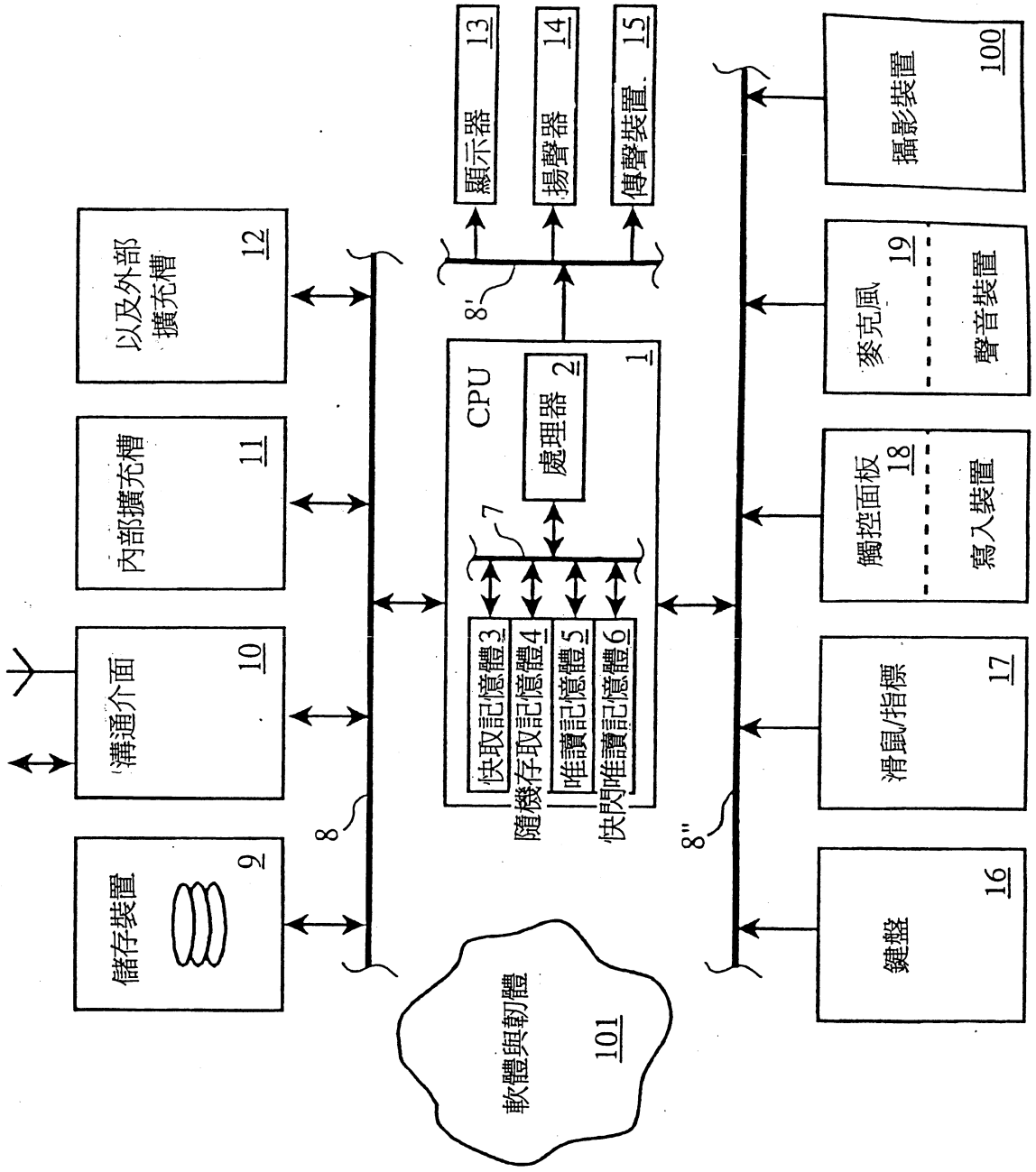

儲存裝置
9
溝通介面
10
內部擴充槽
11
以及外部擴充槽
12
8
軟體與韌體
101
CPU
處理器
2
1
7
快取記憶體3
隨機存取記憶體4
唯讀記憶體5
快閃唯讀記憶體6
8'
顯示器
13
揚聲器
14
傳聲裝置
15
8"
鍵盤
16
滑鼠/指標
17
觸控面板
18
寫入裝置
麥克風
19
聲音裝置
攝影裝置
100

圖 1

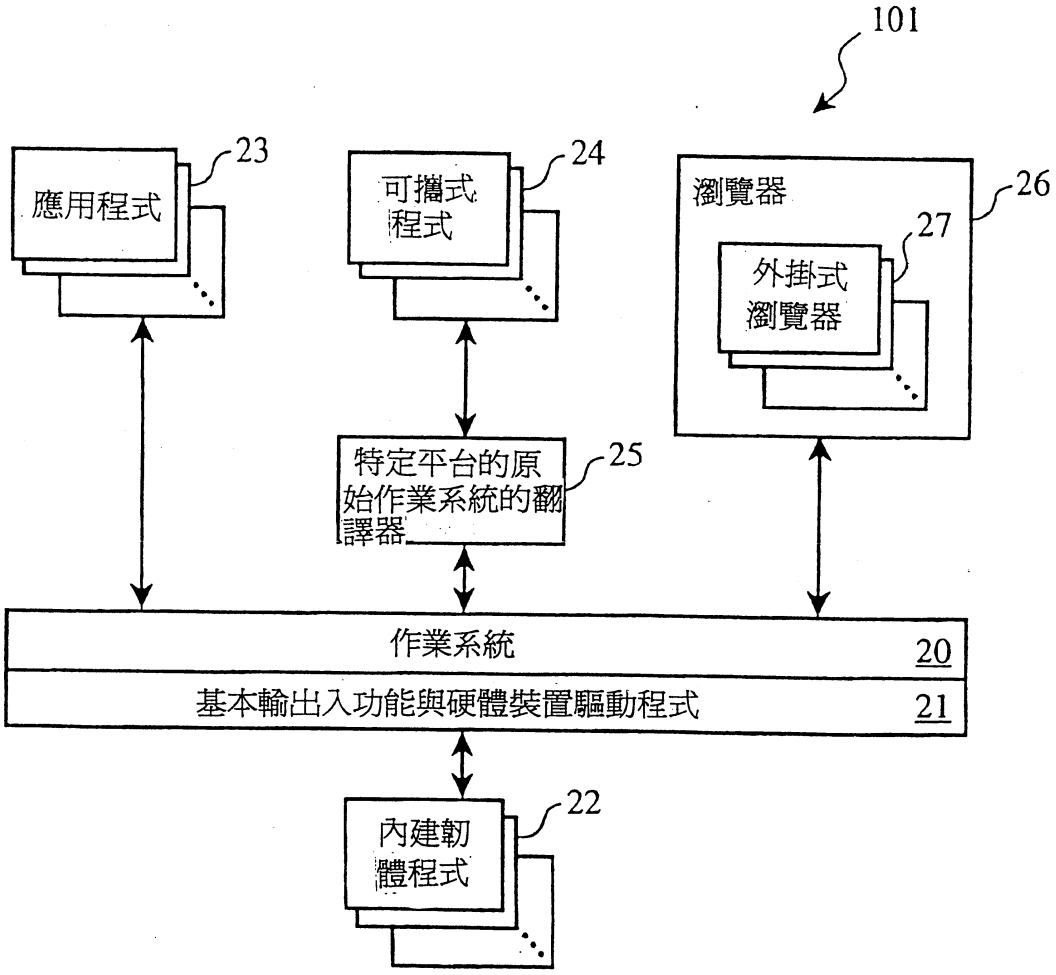

101
應用程式
23
可攜式程式
24
瀏覽器
26
27
外掛式瀏覽器
特定平台的原始作業系統的翻譯器
25
作業系統
20
基本輸出入功能與硬體裝置驅動程式
21
內建韌體程式
22

圖 2

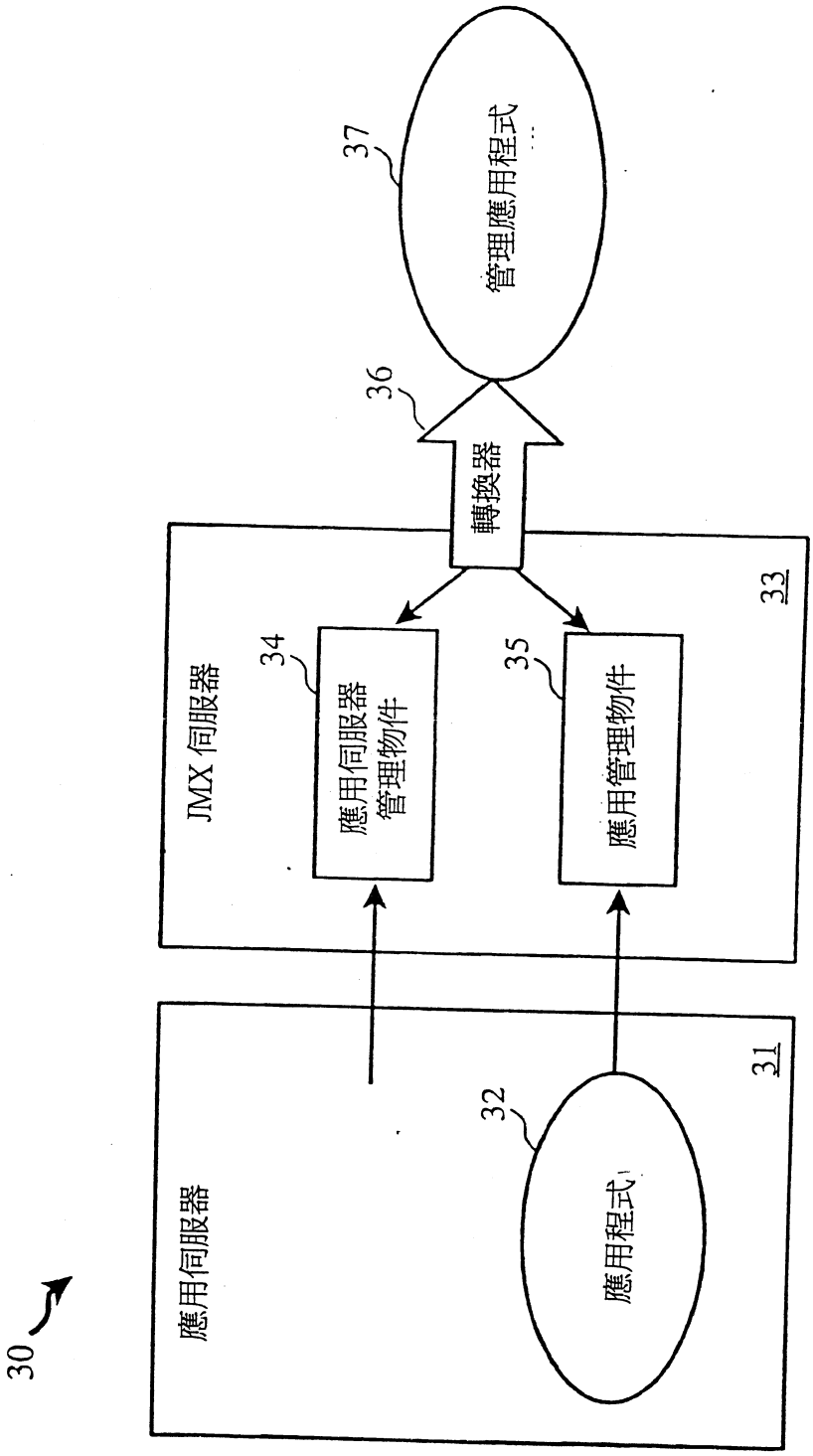

30
應用伺服器
31
32
應用程式
JMX 伺服器
33
34
應用伺服器管理物件
35
應用管理物件
轉換器
36
37
管理應用程式

圖 3

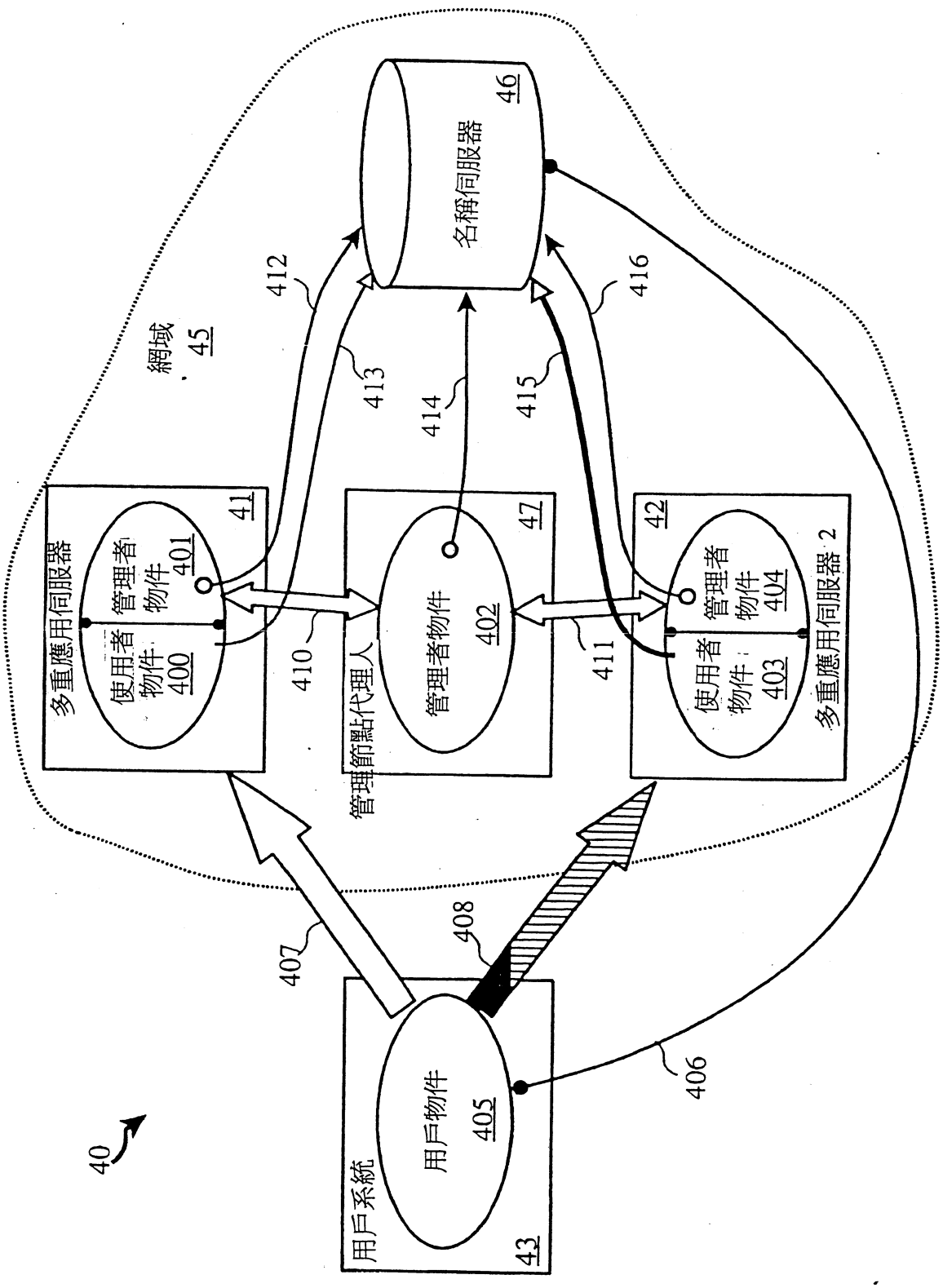

40
網域
45
名稱伺服器
46
412
413
414
415
416
多重應用伺服器
41
使用者物件 400
管理者物件 401
管理節點代理人
47
管理者物件 402
410
411
42
管理者物件 404
使用者物件 403
多重應用伺服器 2
用戶系統
43
用戶物件 405
407
408
406

圖 4

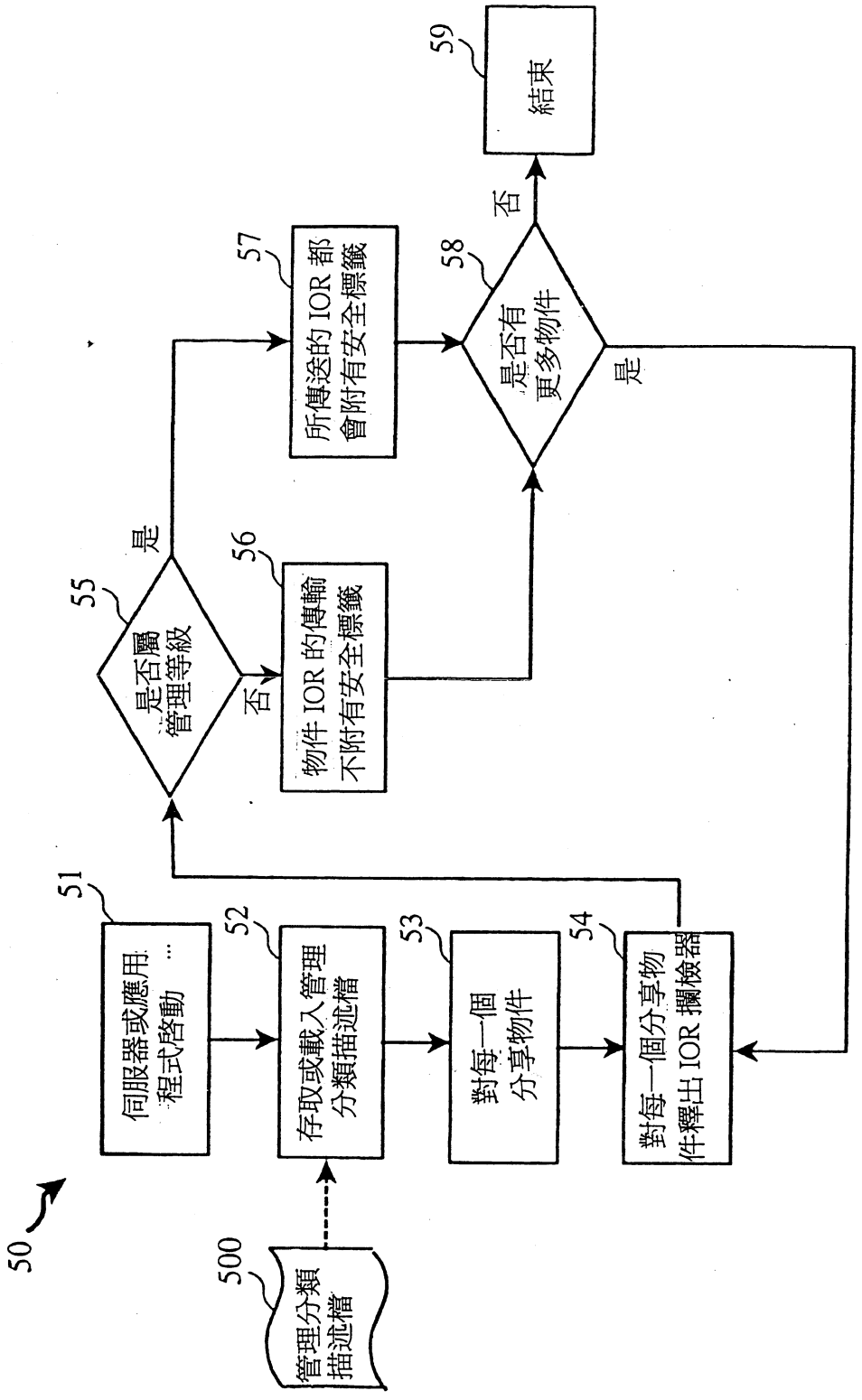

50
500
管理分類描述檔
51
伺服器或應用程式啓動
52
存取或載入管理分類描述檔
53
對每一個分享物件
54
對每一個分享物件釋出 IOR 攔檢器
55
是否屬管理等級
是
否
56
物件 IOR 的傳輸不附有安全標籤
57
所傳送的 IOR 都會附有安全標籤
58
是否有更多物件
是
否
59
結束

圖 5

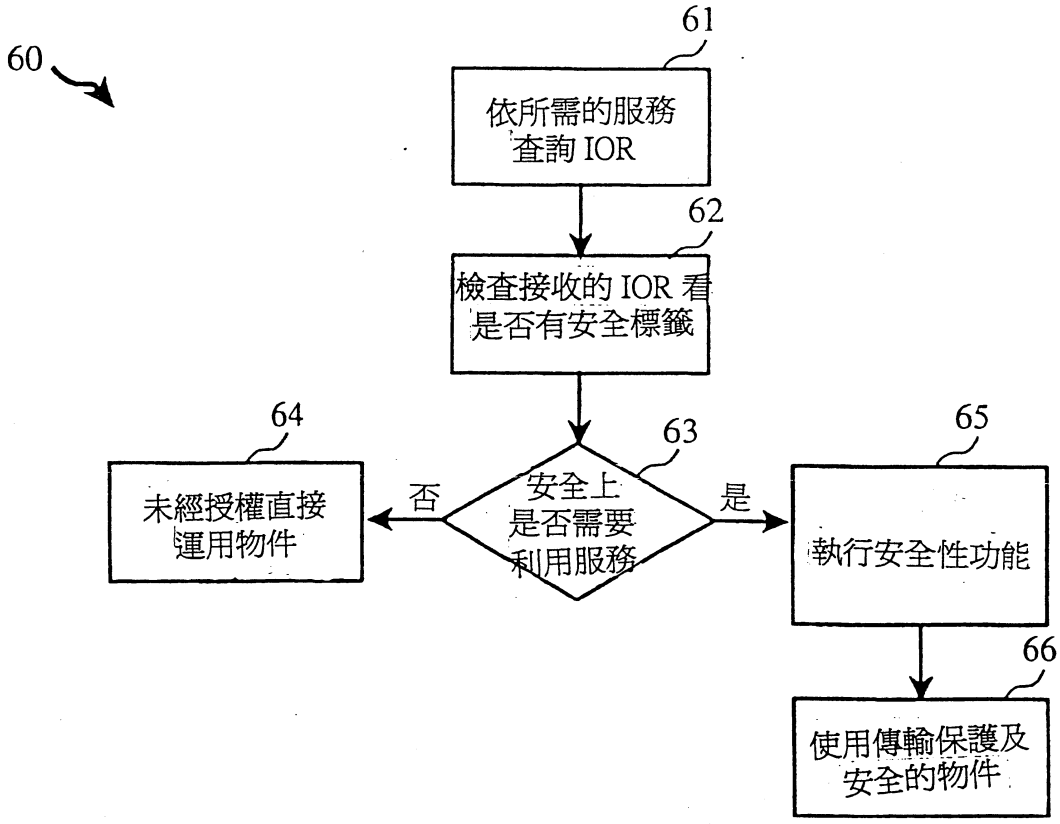

60
61
依所需的服務
查詢 IOR
62
檢查接收的 IOR 看
是否有安全標籤
63
安全上
是否需要
利用服務
否
是
64
未經授權直接
運用物件
65
執行安全性功能
66
使用傳輸保護及
安全的物件

圖 6

六、指定代表圖

（一）、本案代表圖為：第____2____圖

（二）、本案代表圖之元件代表符號簡單說明：

20 作業系統　　21 基本輸出入功能與硬體裝置驅動程式

22 內建韌體程式　23 應用程式

24 可攜式程式　　25 特定平台的原始作業系統的翻譯器

26 瀏覽器　　27 外掛式瀏覽器

公告本

年 月 日(更)正替換頁

I273811

申請日期： 92.7.21	IPC分類
申請案號： 92119802	H04L 9/32 (2006.01)

(以上各欄由本局填註)

發明專利說明書

一、發明名稱	中文	分散式計算網域之應用伺服器物件級安全方法及系統
	英文	METHOD AND SYSTEM OF APPLICATION SERVER OBJECT-LEVEL SECURITY FOR DISTRIBUTED COMPUTING DOMAINS
二、發明人(共6人)	姓名(中文)	1.柏克，彼得　丹尼爾 2.趙，清雲 3.鍾，海維
	姓名(英文)	1.BIRK, Peter Daniel 2.CHAO, Ching-Yun 3.CHUNG, Hyen Vui
	國籍(中英文)	1.美國 US 2.美國 US 3.愛爾蘭 IE
	住居所(中文)	1.美國德州78727奧斯汀市狩獵林路1925號 2.美國德州78750奧斯汀市粗石路11518號 3.美國德州78681-3457圓石市牧師河路8619號
	住居所(英文)	1.1925 Chasewood Dr., Austin, Texas 78727 USA 2.11518 Rustic Rock Drive, Austin, Texas 78750 USA 3.8619 Priest River Drive, Round Rock, Texas 78681-3457 USA
三、申請人(共1人)	名稱或姓名(中文)	1.萬國商業機器公司
	名稱或姓名(英文)	1.INTERNATIONAL BUSINESS MACHINES CORPORATION
	國籍(中英文)	1.美國 US
	住居所(營業所)(中文)	1.美國紐約州10504亞芒克市新奧爾察德路　(本地址與前向貴局申請者相同)
	住居所(營業所)(英文)	1.New Orchard Road, Armonk, NY 10504, USA
	代表人(中文)	1.傑羅 羅森梭
	代表人(英文)	1.Gerald Rosenthal

四、中文發明摘要　(發明名稱：分散式計算網域之應用伺服器物件級安全方法及系統)

本發明之應用伺服器上的物件得以不同分類加以定義以取得不同等級的安全保護，如同對使用者物件與管理物件的定義。網域級的安全機制得以針對管理物件加以強化，而對於使用者物件安全機制則針對網域中的每一應用伺服器做個別的設定。在COBRA架構中，以網域為基礎的分享物件之IOR皆必須受到保護，例如一個管理物件在IOR的產生以及傳輸到名稱伺服器期間，其IOR必定設有標籤組件。稍後當用戶使用IOR時，該用戶必須根據前述標籤組件實行必要的安全措施如認證、授權、以及傳輸保護。

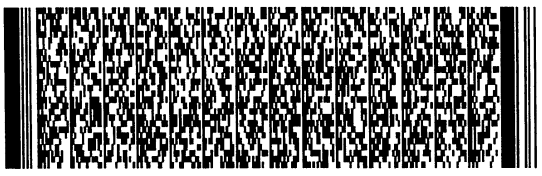
五、英文發明摘要　(發明名稱：METHOD AND SYSTEM OF APPLICATION SERVER OBJECT-LEVEL SECURITY FOR DISTRIBUTED COMPUTING DOMAINS)

Objects on application servers may be defined into classes which receive different levels of security protection, such as definition of user objects and administrative objects. Domain-wide security may be enforced on administrative objects, which user object security may be configured separately for each application server in a domain. In a CORBA architecture, IOR's for

四、中文發明摘要 （發明名稱：分散式計算網域之應用伺服器物件級安全方法及系統）

五、英文發明摘要 （發明名稱：METHOD AND SYSTEM OF APPLICATION SERVER OBJECT-LEVEL SECURITY FOR DISTRIBUTED COMPUTING DOMAINS）

shared objects which are to be secured on a domain-wide basis, such as administrative objects, are provided with tagged components during IOR creation and exporting to a name server. Later, when the IOR is used by a client, the client invokes necessary security measures such as authentication, authorization and transport protection according to the tagged components.



六、申請專利範圍

單物件存取協定與Inter-ORB傳輸協定群組之一安全傳輸協定。

11. 如申請專利範圍第1項之方法，該方法包括利用選自IDL與網路服務定義語言加上網路服務端點語言和介面定義語言群組之一服務描述模型（service description model）。

12. 一種用在分散式計算機網域之具有一軟體編碼之電腦可讀取記錄媒體，該軟體的實行步驟包括：

分送一管理物件與一使用者物件到一或多個應用伺服器；

定義一整體安全旗標給該管理物件的一網域級安全；以介面連接一或多個應用伺服器安全旗標到前述分散式之該管理物件；以及

藉由設定在三種模式之一的一用戶端電腦協同合作之一應用伺服器執行一或多個安全性的計算，其中第一個模式是假若該整體安全旗標與前述之該應用伺服器安全旗標皆啟動，則該使用者物件與該管理物件皆會受到保護，前述一第二模式是使用者物件的使用不經安全性計算但該管理物件仍會受到保護，其中該整體安全旗標會啟動而該應用伺服器安全旗標則不啟動，一第三模式是該使用者物件與該管理物件的使用不經安全性計算，其中該整體安全旗標不會啟動。

六、申請專利範圍

13. 如申請專利範圍第12項之記錄媒體，其中前述執行安全性計算的該軟體包含提供個別的該安全性計算給該管理物件與該使用者物件。

14. 如申請專利範圍第12項之記錄媒體，其中該應用伺服器安全旗標與該管理物件介面包含該軟體以及選自傳輸附標籤組件的COBRA IOR之群組給該應用伺服器的該使用者物件，其中該應用伺服器之該使用者物件安全機制是啟動的，同時亦在UDDI登錄上提供一組物件型態給該應用伺服器的該使用者物件，其中該應用伺服器該使用者物件安全機制是啟動的。

15. 如申請專利範圍第14項之記錄媒體，該記錄媒體進一步包含存取受一保護物件的宣告列表之一軟體。

16. 如申請專利範圍第12項之記錄媒體，該記錄媒體包含一個WebSphere應用伺服器。

17. 如申請專利範圍第12項之記錄媒體，該記錄媒體包含一Enterprise Java Beans的用戶端電腦處理流程。

18. 如申請專利範圍第12項之記錄媒體，該記錄媒體包含Enterprise Java Beans使用者物件。

六、申請專利範圍

19. 如申請專利範圍第12項之記錄媒體，該記錄媒體包含一MBeans管理物件。

20. 如申請專利範圍第12項之記錄媒體，該記錄媒體包含實行選自認證、授權、以及傳輸保護之一表單之安全性計算的一軟體。

21. 如申請專利範圍第12項之記錄媒體，該記錄媒體包含利用一選自簡單物件存取協定與Inter-ORB傳輸協定群組的安全傳輸協定之一軟體。

22. 如申請專利範圍第12項之記錄媒體，該記錄媒體包含利用一選自IDL與網路服務定義語言加上網路服務端點語言(WSEL)和介面定義語言的群組之一服務描述模型。

23. 一位於一個分散式計算機網域內之物件級安全系統，包括：

一或多個管理物件與一或多個使用者物件分散在一或多個應用伺服器之間；

在一網路化的計算機網域等級中，一整體安全旗標定義該管理物件之安全性；

一或多應用伺服器安全旗標與前述分散的該管理物件之一介面相連結；以及