IBM WebSphere Commerce

安全手冊

第 5.4 版

IBM WebSphere Commerce

安全手冊

第 5.4 版

注意事項：

在使用本書及其支援的產品之前，請先閱讀第 121 頁的『注意事項』的一般資訊。

第一版，第一次修訂（2002 年 5 月）。

本版適用於 IBM® WebSphere Commerce 5.4 版與其所有後續版次與修正層次，除非新版中另有提及。請確定您使用的是產品層次的正確版本。

請向 IBM 業務代表或向當地的 IBM 分公司訂購出版品。下列地點恕不供應。

IBM 歡迎您提供意見。請以下列任何一種方法傳送您的批評與建議：

1. 以電子郵件傳送至以下列出的其中一個網路 ID。如果您希望獲得答覆，請務必註明您的完整網路位址。

   Internet: torrcf@ca.ibm.com
   IBMLink: toribm(torrcf)

2. 如果要使用傳眞，請使用下列號碼：

   美國以及加拿大：416-448-6161
   其它國家：(+1)-416-448-6161

3. 郵件請寄到下列地址：

   IBM Canada Ltd. Laboratory B3/KB7/8200/MKM
   8200 Warden Avenue
   Markham, Ontario, Canada L6G 1C7

當您傳送資訊給 IBM 時，即授與 IBM 非獨占的資訊使用或公佈權利，IBM 不需對您負任何責任。

目錄

前言 v
本文件的導覽 v
持續進行的安全評估 vi
WebSphere Commerce 5.4 中的安全加強功能 . vi
網站管理者方面的加強功能 vi
系統管理者方面的加強功能 viii
WebSphere Commerce 程式設計人員方面的加強功能 viii
WebSphere Commerce Suite 5.1 Pro Edition 中的安全加強功能 ix
一般安全加強 ix
階段作業管理 x
鑑別 x
日誌記載 x
本書中的使用慣例 x
其它相關資訊的位置 xi

第 1 篇 WebSphere Commerce 安全模型 1

第 1 章 WebSphere Commerce 安全模型簡介. 3
概觀 3
何謂鑑別？. 3
何謂授權？. 3
何謂存取控制原則？. 3
何謂審核追蹤？ 4
何謂機密保護？ 4

第 2 章 鑑別 7
WebSphere Commerce 鑑別模型 7
檢核機制 9
鑑別機制 9
使用者登錄. 9
證明. 10
WebSphere Commerce 記號 10
WebSphere Application Server LTPA 記號 10
單一簽入 10
鑑別原則 11
帳戶原則 11
和鑑別有關的其它原則. 12
階段作業原則. 13

第 3 章 授權（存取控制） 15
組織階層 15
根組織 16
組織（賣方）. 17
組織（買方）. 17
職務. 18
網站作業 18
網站與內容開發 19
流程管理與營運 19
產品管理 20
銷售管理 20
行銷管理 21
組織管理 21
存取控制原則. 22
存取控制原則的元素 22
存取控制原則的概念 22
資源與原則的擁有權 28
存取控制原則的類型 28
存取控制的層次 30
存取控制如何防止越權動作 32
在執行使用者起始的動作前先檢查授權 . . 32
使用存取控制. 32
評估存取控制原則 32
組織階層 33
使用者 33
職務. 33
存取群組 33
文件. 34
評估標準原則. 34
評估範本原則. 36

第 2 篇 WebSphere Commerce 網站管理者的安全作業 39

第 4 章 強化網站安全 41
安全特性的檢視畫面 42
登入逾時 42
密碼無效 43
受密碼保護的指令 44

跨網站編寫 Script 的保護 44
啓用「登入逾時」 45
啓動「密碼無效」 46
啓用「受密碼保護的指令」 46
更新加密資料. 48
啓用「跨網站編寫 Script 的保護」 50
啓用「存取日誌記載」. 51
設置帳戶原則. 52
設置密碼原則. 53
設置帳戶鎖定原則 54
啓動安全檢查. 55
架構管理程式的「PDI 加密」欄位 56

第 5 章 啓用 WebSphere Application Server 安全特性 57
開始之前 57
使用 LDAP 使用者登錄來啓用安全特性 . . . 57
使用作業系統的使用者登錄來啓用安全特性 . . 62
停用 WebSphere Commerce EJB 安全特性 . . 63
WebSphere Commerce 安全部署選項 64

第 6 章 階段作業管理 67
Cookie 型階段作業管理 67
使用 cookie 進行階段作業管理 68
URL 重新編寫 69
使用 URL 重新編寫階段作業管理 70
撰寫 JSP 範本以進行 URL 重新編寫. . . 70

第 3 篇 系統管理者的安全作業. . . 73

第 7 章 設定與變更密碼. 75
使用者 ID、密碼與網址的簡要說明 76
變更架構管理程式密碼. 78
設定 IBM HTTP Server 管理者密碼 79
變更 SSL 金鑰檔密碼 79
產生 WebSphere Commerce 加密密碼. . . . 80
產生 Payment Manager 加密密碼 80

第 8 章 使用 IBM HTTP Server 啓用正式作業的 SSL. 83
關於安全特性. 83
建立正式用的安全金鑰檔 84
向憑證管理中心申請安全憑證 85
Equifax 使用者 85
VeriSign 使用者 85
接收正式金鑰檔並設爲現行金鑰檔 86
測試正式金鑰檔 86
Payment Manager 的 SSL 注意事項 87
在 IBM HTTP Server (iSeries) 中啓用 SSL . . 87
Payment Manager 搭配 SSL 一起使用 . . 88

第 9 章 在 IBM SecureWay Directory 伺服器 (LDAP) 中啓用 SSL 89
安裝 SecureWay 89
WebSphere Commerce 90

第 10 章 單一簽入 91
必備需求 91
啓用單一簽入. 91

第 4 篇 WebSphere Commerce 程式開發人員的安全作業 93

第 11 章 存取控制 95
瞭解存取控制. 95
WebSphere Application Server 中的資源保護概觀. 95
WebSphere Commerce 存取控制原則簡介 . 97
存取控制類型 105
存取控制的互動 107
可保護的介面 110
可分組介面 110
尋找存取控制的詳細資訊 111
施行存取控制 111
識別可保護的資源. 111
在 Enterprise Bean 中施行存取控制 . . . 112
在資料 Bean 中施行存取控制 113
在控制程式指令中施行存取控制 114
在檢視畫面中施行存取控制原則 116

第 5 篇 後記 119

注意事項 121
商標 123

前言

本文件說明 WebSphere Commerce 5.4 的安全特性以及如何架構這些特性。

其中將詳述一些 WebSphere Commerce 安全問題與特性，像是：鑑別、授權與存取控制原則。本文件的目的在於爲負責您網站安全的人員（像是：系統管理者或 WebSphere Commerce 網站管理者），提供一份綜合的文件說明，讓他們能夠確實地保護 WebSphere Commerce 正式網站。

本文件所擬定的適用對象爲最高的安全主管或 WebSphere Commerce 網站中的安全管理者。

請注意，本手冊中有許多章節是從 WebSphere Commerce 5.4 資訊庫中的其它文件衍生而來，像是：WebSphere Commerce 5.4 線上說明、*WebSphere Commerce 5.4 安裝手冊*與 *WebSphere Commerce 5.4 程式設計手冊*。*具體而言亦即：*

- 第 15 頁的第 3 章, 『授權（存取控制）』中的資訊亦會在 *WebSphere Commerce 5.4 存取控制手冊*中提及。
- 第 41 頁的第 4 章, 『強化網站安全』與第 67 頁的第 6 章, 『階段作業管理』中的資訊亦會在 WebSphere Commerce 5.4 線上說明中提及。第 57 頁的第 5 章, 『啓用 WebSphere Application Server 安全特性』中的資訊亦會在 *WebSphere Commerce 5.4 安裝手冊中提及*。
- 第 73 頁的第 3 篇, 『系統管理者的安全作業』中的資訊亦會在 *WebSphere Commerce 5.4 安裝手冊中提及*。
- 第 93 頁的第 4 篇, 『WebSphere Commerce 程式開發人員的安全作業』中的資訊亦會在 *WebSphere Commerce 5.4 程式設計手冊中提及*。

重要事項

本文件僅涵蓋和部署電子商務網站有關的 WebSphere Commerce 安全問題。而不提及和您作業系統漏洞有關的問題。您應向您的作業系統供應商查詢，以訂出用以保護您作業系統安全的適當對策。

本文件的導覽

本文件分成下列數篇：

- 第 1 頁的第 1 篇, 『WebSphere Commerce 安全模型』討論 WebSphere Commerce 安全模型，並提供 WebSphere Commerce 安全的概念性概觀。對於想大致瞭解 WebSphere Commerce 安全特性或想在 WebSphere Commerce 網站上規劃安全的人來說，此篇值得一讀。
- 第 39 頁的第 2 篇, 『WebSphere Commerce 網站管理者的安全作業』討論和網站安全有關的 WebSphere Commerce 網站管理作業。本篇極適合負責執行和網站安全有關之網站管理作業的人閱讀。
- 第 73 頁的第 3 篇, 『系統管理者的安全作業』討論和系統安全有關的 WebSphere Commerce 系統管理作業。本篇極適合負責執行系統管理作業並關心系統安全的人閱讀。
- 第 93 頁的第 4 篇, 『WebSphere Commerce 程式開發人員的安全作業』是從程式開發人員的立場來討論 WebSphere Commerce 存取控制。對於想瞭解存取控制概念，以便在程式碼中施行存取控制原則的人來說，此篇值得一讀。

持續進行的安全評估

WebSphere Commerce 產品線會透過獨立的 IBM 安全專家小組，持續進行安全分析。這些專家會從僅能透過瀏覽器存取 WebSphere Commerce 的使用者觀點，以及從具有較多許可權且在 WebSphere Commerce Server 執行的相同系統上具有帳戶的使用者觀點，來進行安全分析。我們將採用安全專家分析後的回覆，來提昇 WebSphere Commerce 的安全。

WebSphere Commerce 5.4 中的安全加強功能

下節列出相對於 WebSphere Commerce Suite 5.1，WebSphere Commerce 5.4 中具備的安全加強功能。這些加強功能大部份已用於 WebSphere Commerce Business Edition 5.1 版次中。一般而言，這些加強功能適用於：

- WebSphere Commerce 網站管理者
- 系統管理者
- WebSphere Commerce 程式開發人員

請注意，有時這些職務可以交換。

網站管理者方面的加強功能

以下是 WebSphere Commerce 5.4 中通常針對網站管理者所提供的加強功能：

存取控制

- **存取控制組織架構** -- 一項重要的加強功能是已在 WebSphere Commerce 5.4 中施行新的存取控制組織架構。這種新組織架構採用存取控制原則來

判斷給定使用者能否對給定的資源執行給定的動作。新存取控制組織架構提供的是細密的存取控制。它會結合使用 WebSphere Application Server 所提供的存取控制但不會予以取代。有關新存取控制組織架構的詳述，請參閱第 95 頁的第 11 章, 『存取控制』。

新存取控制組織架構在下列各方面強化了舊有的存取控制：

易於表達...
它能掌握眾多存取原則的意向。由於組織架構是共通的，因此它能處理紛雜的使用者群組、資源群組、動作群組與關係群組。

採階層性...
組織所擁有的存取控制原則亦適用於子組織。

可自訂...
存取控制原則和應用程式碼分開，因此可直接變更原則，而不需重新編譯程式碼。

精簡... 新組織架構調整得更好。存取控制原則的數目會隨商業程序數目（而非物件數）而增加。大部份的分組組織架構是以隱含條件爲依據，因此只要滿足條件，即適用於該原則。

- **跨網站編寫 Script** -- 使用 WebSphere Commerce 架構管理程式中的「跨網站編寫 Script 的保護」節點，以便一旦使用者要求中含有禁用的屬性或字元時，即予以拒絕。詳細說明請參閱第 41 頁的第 4 章, 『強化網站安全』。

鑑別

- **密碼的儲存** -- WebSphere Commerce 5.4 採用 SHA-1 雜湊法來加密單向雜湊的密碼並將之儲存在 WebSphere Commerce 資料庫中，而非原封不動地儲存密碼。這可確保包括網站或系統管理者在內的任何人皆無法解開密碼。
- **密碼無效** -- 使用 WebSphere Commerce 架構管理程式的「密碼無效」節點，以要求使用者在初次登入系統時變更密碼。詳細說明請參閱第 41 頁的第 4 章, 『強化網站安全』。
- **帳戶原則** -- 使用 WebSphere Commerce 管理主控台的「帳戶原則」頁面，爲您的網站設置帳戶原則，以定義使用中帳戶的相關原則。詳細說明請參閱第 41 頁的第 4 章, 『強化網站安全』。
- **密碼原則** -- 使用 WebSphere Commerce 管理主控台的「密碼原則」頁面，爲您的網站設置密碼原則，以控制使用者密碼選擇特性。詳細說明請參閱第 41 頁的第 4 章, 『強化網站安全』。

- **帳戶鎖定原則** -- 使用 WebSphere Commerce 管理主控台的「帳戶鎖定原則」頁面，爲您的網站設置帳戶鎖定原則，以降低危害使用者帳戶的機會。詳細說明請參閱第 41 頁的第 4 章, 『強化網站安全』。

授權

受密碼保護的指令 -- 使用 WebSphere Commerce 架構管理程式的「受密碼保護的指令」節點，要求使用者在進行一些會執行指定指令的要求時得輸入密碼。詳細說明請參閱第 41 頁的第 4 章, 『強化網站安全』。

加密資料

資料庫更新工具 -- 使用 WebSphere Commerce 架構管理程式的「資料庫更新工具」節點，更新 WebSphere® Commerce 資料庫中的加密資料（像是：密碼與信用卡資訊）與商家金鑰。詳細說明請參閱第 41 頁的第 4 章, 『強化網站安全』。

階段作業管理

登入逾時 -- 使用「登入逾時」節點，登出長期處於非作用中的使用者，並要求他們重新登入系統。此一加強功能是透過 WebSphere Commerce 架構管理程式來呼叫；詳細說明請參閱第 41 頁的第 4 章, 『強化網站安全』。

日誌記載

存取日誌記載 -- 啓用存取日誌記載特性，以迅速發現任何對 WebSphere Commerce 的安全威脅。此一加強功能是透過 WebSphere Commerce 架構管理程式來呼叫；詳細說明請參閱第 41 頁的第 4 章, 『強化網站安全』。

系統管理者方面的加強功能

以下是 WebSphere Commerce 5.4 中通常針對網站管理者所提供的加強功能：

- 其中一項重要的安全加強功能是讓您能夠將 WebSphere Commerce 管理工具架構成在非標準埠號上執行（例如：埠 8000 而非埠 443）。藉由限制存取此埠，您可以限制只有您的區域網路或企業內部網路才能存取管理工具。
- 從 WebSphere Commerce 管理主控台，使用啓動安全檢查頁面啓動安全程式，以檢查及刪除一些可能潛在安全暴露問題的 WebSphere Commerce 暫存檔。

WebSphere Commerce 程式設計人員方面的加強功能

重要的加強功能是已在 WebSphere Commerce 5.4 中施行新的存取控制組織架構。這種新組織架構採用存取控制原則來判斷給定使用者能否對給定的資源執行給定的動作。新存取控制組織架構提供的是細密的存取控制。它會結合使用 WebSphere Application Server 所提供的存取控制但不會予以取代。有關新存取控制組織架構的詳述，請參閱第 95 頁的第 11 章, 『存取控制』。

新存取控制組織架構在下列各方面強化了舊有的存取控制：

易於表達...

它能掌握眾多存取原則的意向。由於組織架構是共通的，因此它能處理紛雜的使用者群組、資源群組、動作群組與關係群組。

採階層性...

組織所擁有的存取控制原則亦適用於子組織。

可自訂...

存取控制原則和應用程式碼分開，因此可直接變更原則，而不需重新編譯程式碼。

精簡... 新組織架構調整得更好。存取控制原則的數目會隨商業程序數目（而非物件數）而增加。大部份的分組組織架構是以隱含條件爲依據，因此只要滿足條件，即適用於該原則。

WebSphere Commerce Suite 5.1 Pro Edition 中的安全加強功能

Commerce Suite 5.1 呈現了一個新的電子商務結構，並且完全重新編寫以 C++ 爲基礎的 Commerce Suite 4.1，除了仍含有舊版 WebSphere Commerce Suite 中的所有安全特性外，另外還新增一些安全加強功能。WebSphere Commerce 5.4 已沿用了這些加強功能。

Commerce Suite 5.1 依舊可保護舊版提供的 WebSphere Commerce Suite 管理者與購物者資源不受未獲授權者存取。

- 繼續支援存取控制特性，以確定在取得存取或提交敏感資訊前，WebSphere Commerce Suite 使用者皆已經過鑑別或處於 SSL 模式。
- 依循 Commerce Suite 4.1 的相同模型，爲群組指定 WebSphere Commerce Suite 指令，如此一來，唯有網站管理者或商店層次的管理者才能執行特定指令。

一般安全加強

由於 Commerce Suite 5.1 是以 Java™ 重新編寫，因而原來一些會導致以 C++ 寫成之軟體發生錯誤的安全問題皆已移除。因 Java 不會使用指標，而沒有緩衝區溢位問題，而這種緩衝區溢位問題是大部份以 C++ 寫成之軟體的安全漏洞之一。由於遵循業界標準 J2EE 規格，WebSphere Commerce Suite 採用嚴謹的檢查方式來確定伺服器不會執行蓄意之人所指定的惡劣陳述式。

WebSphere Commerce Suite 系統中已使用業界標準三重 DES 演算法（數據加密標準）來保護敏感資訊。內含三重 DES 演算法的套件皆經過數位簽章，因此一旦套件遭到竄改， WebSphere Commerce Suite 伺服器便不會啓動。

階段作業管理

為求取最大安全，WebSphere Commerce Suite 階段作業管理已使用一種獨特技術完全重新編寫，以確保 Cookie 不會遭竊。藉由使用只會行經 SSL（安全 Sockets 層次）且含一個加密時間戳記的鑑別 Cookie，重新編寫階段作業管理的設計可防範階段作業攔劫情況。

鑑別

WebSphere Commerce Suite 伺服器在執行期間所需的系統與應用程式密碼皆已使用商家指定的 12 位元金鑰加密，且儲存在 WebSphere Commerce Suite 架構檔中。而出現在 使用者 URL 輸入框中的敏感資訊亦經過加密，以保護購物者不會被擅自洩漏。

日誌記載

當初在設計 WebSphere Commerce Suite 日誌系統時已將安全視為重要考量，因此在預設的情況下，敏感資訊（如：購物者的密碼與信用卡資訊）不會記載於 WebSphere Commerce Suite 日誌檔中。

本書中的使用慣例

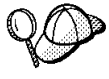
本書的使用慣例如下：

- **粗體字**表示指令或圖形式使用者介面（GUI）控制項，如：欄位名稱、圖示或功能表選項。
- 等寬字表示您必須輸入完全相同的文字範例以及檔名、目錄路徑與名稱。
- *斜體字*用以強調字眼。另外，以斜體字表示的名稱，必須以符合您系統的適當值取代之。當您看到下列任何名稱時，請按說明換成您的系統值：

  host_name
  : 您的 WebSphere Commerce Studio 機器的完整主電腦名稱（例如，ibm.com 是完整的名稱）。

  Windows

  drive 代表您安裝所提產品或元件的磁碟機代號（例如 C:）。



此圖示表示「要訣」- 此額外資訊有助您完成作業。

Windows 專指適用於 WebSphere Commerce for Windows NT® 與 Windows® 2000 的資訊。

AIX 專指適用於 WebSphere Commerce for AIX® 的資訊。

Solaris 專指適用於 WebSphere Commerce for Solaris™ 作業環境軟體的資訊。

400 專指適用於 WebSphere Commerce for IBM @server iSeries™ 400® （舊稱 AS/400®） 的資訊。

Linux 專指適用於 WebSphere Commerce for Linux 的資訊。

Professional 專指適用於 WebSphere Commerce Professional Edition 的資訊。

Business 專指適用於 WebSphere Commerce Business Edition 的資訊。

其它相關資訊的位置

WebSphere Commerce 5.4 產品的相關資訊，請見下列網站：

- Business
  http://ibm.com/software/webservers/commerce/wc_be/lit-tech-general.html
- Professional http://www.ibm.com/software/webservers/commerce/wcs_pro/lit-tech-general

Commerce Studio, Professional Developer 5.1 版 或舊版 WebSphere Commerce Studio 的相關資訊，請見下列網站：

http://www.ibm.com/software/webservers/commerce/commercestudio/lit-tech-general.html

第 1 篇 WebSphere Commerce 安全模型

本篇提供 WebSphere Commerce 安全的概念性概觀。

第 1 章 WebSphere Commerce 安全模型簡介

本章說明 WebSphere Commerce 安全模型與一些 WebSphere Commerce 安全概念。

概觀

本文件中的資訊在說明鑑別、授權、原則與機密性的觀念。

何謂鑑別？

鑑別是一種驗證使用者或應用程式和其所聲稱的身份是否一致的程序。在 WebSphere Commerce 系統中，除了訪客使用者外，凡是要存取系統的使用者與應用程式皆必須經過鑑別。使用者鑑別程序固定在 SSL 下執行。這可確保當使用者提交密碼時，使用網路竊聽程式的第三者無法從網路上*窺探*。在鑑別程序期間絕不會解密密碼，而會視同一般的安全事務。所有的使用者密碼皆經過雜湊，並使用 128 位元金鑰加密，做成所謂的*商家金鑰*。在安裝與架構 WebSphere Commerce 系統期間將會指定商家金鑰。

基於管理目的，WebSphere Commerce 系統有自己的密碼。這些密碼應定期隨 WebSphere Commerce 全網站的安全原則加以變更。有關變更 WebSphere Commerce 5.4 系統密碼的詳述，請參閱第 75 頁的第 7 章, 『設定與變更密碼』。

何謂授權？

授權爲一種判斷使用者可否對某資源執行特定作業的程序。授權與否取決於 WebSphere Commerce 資源的存取控制原則而定。在 WebSphere Commerce 系統中，下列兩個區域需要存取控制：

- 保護 WebSphere Commerce Enterprise JavaBeans™（EJB Bean）避免遭到未獲授權的存取。此程序將在第 57 頁的第 5 章, 『啓用 WebSphere Application Server 安全特性』中討論。
- 確保只有獲授權的人才可執行各種不同的 WebSphere Commerce 指令群。此程序將在第 95 頁的第 11 章, 『存取控制』中討論。

何謂存取控制原則？

假設您已定義出將參與您電子商務網站的組織與使用者，此時您可以透過一組原則來管理他們的活動，這種程序便稱爲*存取控制*。

存取控制原則是一種規則，其中說明哪個使用者或使用者群組有權在您網站中執行特定的活動。這些活動的範圍從登錄、管理拍賣、更新產品型錄、同意核准訂單，以及核准在操作與維護電子商務網站時所需的其它任何數以百計的活動。

原則用來授與使用者存取您的網站。除非使用者因一或多個存取控制原則而獲權執行其職責，否則使用者無權存取您網站中的任何功能。

WebSphere Commerce 5.4 的存取控制模型是以實施存取控制原則爲基礎。存取控制原則是透過存取控制「原則管理程式」實施。一般而言，當使用者嘗試存取受保護的資源時，存取控制原則管理程式會先判斷哪些存取控制原則適用該使用者，然後再依據適用的存取控制原則，來判斷使用者是否可以針對給定的資源執行所要求的作業。

何謂審核追蹤？

在運算環境中，*審核追蹤*相當於用來追蹤電腦活動的電子或書面日誌。舉例來說，員工有權存取公司網路中的某一部份（如：帳戶的應收帳款），但無權存取系統中的其它部份（如：薪資名冊）。如果該員工藉由鍵入密碼，企圖存取某個未獲授權的區段，則這項不當活動會記錄在審核追蹤中。

在電子商務系統中，審核追蹤用來記錄客戶活動。審核追蹤會記錄客戶和系統最初的聯絡，以及記錄後續的動作，像是：產品或服務的付款與遞送。公司可利用審核追蹤來回應任何詢問或抱怨。此外還可藉由審核追蹤來調整帳戶，以提供分析與歷史資訊進行未來的規劃與編列預算，並在一旦查稅時提供一份銷售記錄。

此外還可利用審核追蹤，來調查網際空間與網際網路上的電腦犯罪。如果要揭發個人對系統的惡意攻擊，調查人員可循著犯罪者所留下的審核追蹤追查下去。有時從事電腦犯罪活動的犯案者，會在其網際網路服務公司的活動日誌或者是聊天室日誌中，不經意地留下審核追蹤。

何謂機密保護？

機密保護是一種保護敏感資訊不會被無意的收件人解密的程序。在 WebSphere Commerce 系統中，當敏感資訊從使用者的瀏覽器遞至 WebSphere Commerce 伺服器時（以及從 WebSphere Commerce 伺服器遞回到使用者的瀏覽器時），便需要機密保護。如同第 83 頁的第 8 章, 『使用 IBM HTTP Server 啓用正式作業的 SSL』中所述，會使用「安全 Sockets 層次（SSL）」，爲此實務提供機密保護。

在階段作業管理區域中，亦相當需要機密保護。由於「超文字轉送通信協定 (HTTP)」爲無狀態式，因此通常會使用 *Cookie* 讓 WebSphere Commerce Server 能持續識別該使用者。如果此 Cookie 遭竊，則使用者帳戶可能會洩漏。這就是一般

所說的*階段作業攔劫*。WebSphere Commerce 則是利用第 67 頁的第 6 章, 『階段作業管理』中所說的 Cookie 規格獨特特性，來杜防階段作業攔劫情況。

第 2 章 鑑別

WebSphere Commerce 將鑑別視爲一種驗證提出要求之使用者或應用程式的身份的程序。本節詳述 WebSphere Commerce 鑑別的幾個方面。

WebSphere Commerce 鑑別模型

WebSphere Commerce 鑑別模型是以下列概念爲基礎：

- 檢核機制
- 鑑別機制
- 使用者登錄

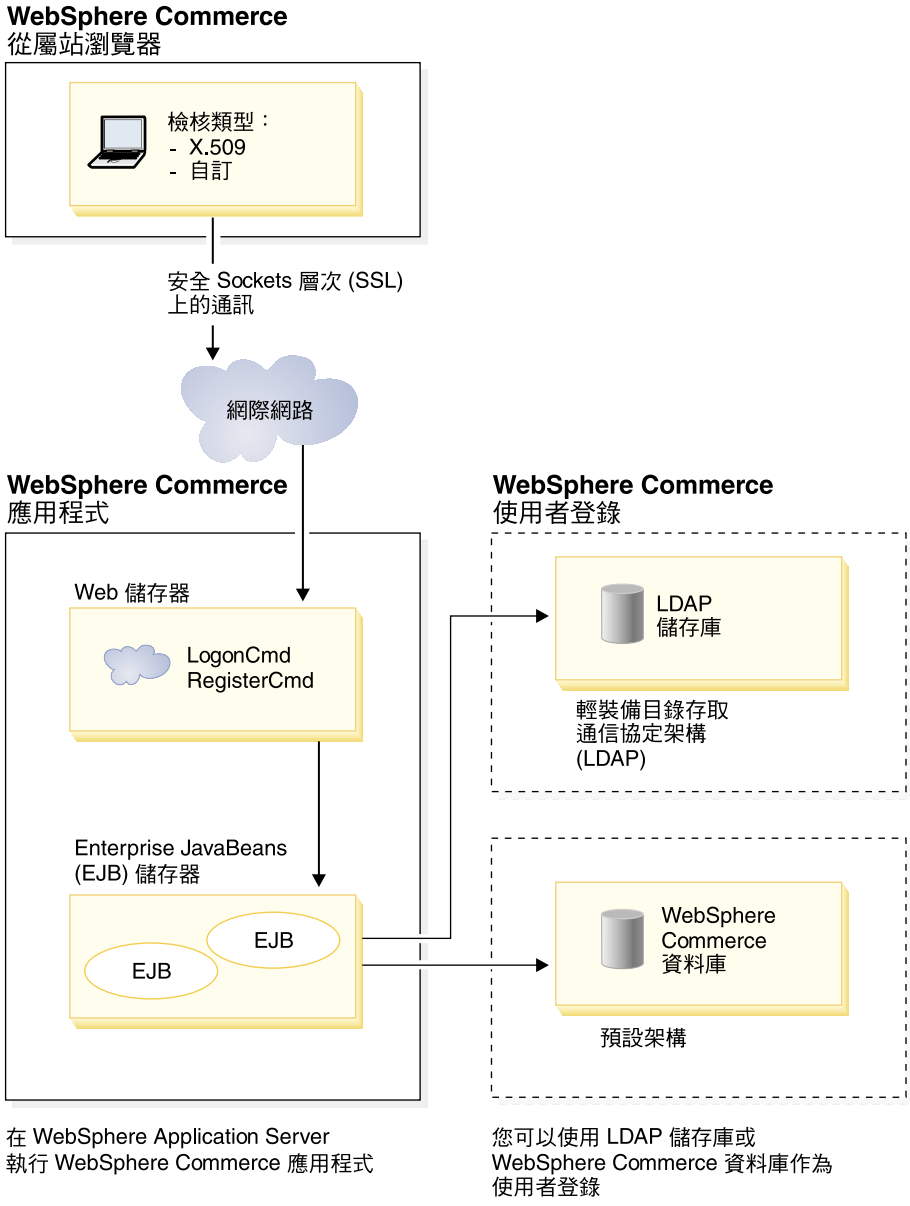


圖 1. WebSphere Commerce 5.4 安全模型

檢核機制

檢核機制訂出伺服器要如何檢核與擷取使用者的鑑別資料。WebSphere Commerce 5.4 支援如下的鑑別方法或檢核機制：

套表型或自訂鑑別

此種鑑別機制容許透過 HTML 頁面或 JSP 套表進行特定網站或商店登入。

憑證型鑑別（X.509 憑證）

憑證檢核機制隱含著將 Web 伺服器架構成透過 SSL 執行相互鑑別之意。這會要求從屬站提出憑證以建立連線。接著，將此憑證映射至使用者登錄。

鑑別機制

*鑑別機制*會以相關聯的使用者登錄來驗證使用者鑑別資料，以鑑別使用者。而在鑑別程序後，每當提出一次要求，WebSphere Commerce 5.4 即會發出和使用者有關的鑑別記號。當使用者登出或關閉瀏覽器時，即會終止。

憑證的查核

此程序是驗證 X.509 從屬站憑證是否是 Web 伺服器所信任的，且是否遵循 Web 伺服器的憑證原則。WebSphere Commerce 也會拿 WebSphere Commerce 資料庫來驗證 X.509 憑證。Web 伺服器會對憑證執行粗略的存取控制，而 WebSphere Commerce 會對憑證執行細密的存取控制。

LDAP 連結

此程序是驗證所提供的檢核資訊是否有效，其做法是執行 LDAP 連結作業以鑑別使用者。

資料庫連結

此程序是驗證在鑑別程序期間所提供的使用者 ID 與密碼是否有效（和儲存在 WebSphere Commerce 資料庫中的鑑別資訊相比對）。

使用者登錄

使用者登錄是一種儲存庫，其包含了使用者資訊以及使用者的鑑別資訊（例如：密碼）。主體（亦即，代表使用者登錄中的使用者本人或系統實體）提供的鑑別資訊可拿來和使用者登錄相驗證或查核。

WebSphere Commerce 5.4 支援以下列兩種使用者網域爲基礎的使用者登錄：LDAP 使用者登錄與 WebSphere Commerce 資料庫。

WebSphere Commerce 5.4 支援如下的 LDAP 提供者：

- IBM SecureWay® Directory Windows AIX Solaris Linux 400
- Netscape® Directory Server Windows AIX Solaris
- Windows 2000 Active Directory 2000

證明

WebSphere Commerce 5.4 Server 支援以查核證明（像是：憑證、記號、使用者 ID 和密碼配對）爲基礎的鑑別機制。證明將和支援這類架構的使用者登錄相驗證。

WebSphere Commerce 記號

WebSphere Commerce 使用安全鑑別 Cookie 來管理鑑別資料。鑑別 Cookie 只會行經 SSL，並且附有時間戳記，以達到最高的安全性。每當執行敏感的指令（例如，會要求使用者提供信用卡號碼的 DoPaymentCmd）時，即會在 SSL 連線下使用此 Cookie 來鑑別使用者。此 cookie 被盜取或被未鑑別使用者盜用的可能性不大。

第二個 Cookie 是在 SSL 或非 SSL 連線下流動於瀏覽器與伺服器間，而可用來在非 SSL 連線下驗證使用者。

WebSphere Application Server LTPA 記號

LTPA 記號爲一小段資料，內含決定使用者所要求資源之存取許可權時所需用到的使用者資訊。其含有鑑別資料與 WebSphere Application Server LTPA 伺服器的數位簽章。

就「WebSphere Application Server 小型認證機構」架構而言，是以內含使用者相關資訊的 LDAP 目錄做爲鑑別依據用的使用者登錄。資源伺服器會聯絡 WebSphere Application Server 安全伺服器，並指定 LTPA 做爲鑑別機制。它亦會提供要求的相關鑑別資料。接著，WebSphere Application Server 安全伺服器會向 LTPA 伺服器查核鑑別資料，並傳回一個 LTPA 記號。

單一簽入

HTTP 單一簽入的主要原理是跨多個 HTTP 要求保留使用者鑑別。其目標是在給定的信任網域中避免多次提示使用者提供安全證明，這類網域包括：

- 彼此合作但不同的 WebSphere Application Server 伺服器。
- 彼此合作的應用程式，像是 LDAP 伺服器、IBM SecureWay Directory Server。

在單一簽入 (SSO) 實務中，會使用 HTTP Cookie 將使用者的鑑別資訊傳達給相異的 Web 伺服器，以免使用者在每個新主從階段作業期間都得輸入一次鑑別資訊（假設採用基本鑑別）。

有關在 WebSphere Commerce 中施行單一簽入的步驟，請參閱第 91 頁的第 10 章, 『單一簽入』。

鑑別原則

鑑別原則爲一組規則，其套用在鑑別程序上以及套用在 WebSphere Commerce 所執行的鑑別資料驗證上。WebSphere Commerce 5.4 支援帳戶原則、和鑑別有關的其它原則以及階段作業原則；相關說明請見下列各節。

帳戶原則

下列各節說明 WebSphere Commerce 所提供的帳戶原則：

帳戶原則

WebSphere Commerce 管理主控台的「帳戶原則」頁面可讓您設置一個帳戶原則。帳戶原則用來定義和帳戶有關的原則，像是：密碼與帳戶鎖定原則。

一旦您建立帳戶原則後，您即可爲使用者指定原則。請注意，如果帳戶原則處於使用中（亦即，該帳戶原則已指定給使用者），則您無法刪除該帳戶原則。

有關建立帳戶原則的資訊，請參閱第 52 頁的『設置帳戶原則』。

另請參閱 WebSphere Commerce 線上說明中的 ″預設鑑別原則″ 參考主題。

帳戶鎖定原則

WebSphere Commerce 管理主控台的「帳戶鎖定原則」頁面可讓您針對 WebSphere Commerce 中的不同使用者職務設置帳戶鎖定原則。若有人對某個帳戶採取惡意動作，則帳戶鎖定原則會停用該使用者帳戶，以降低這些動作危及帳戶的機會。

帳戶鎖定原則會執行下列各項：

- 帳戶鎖定臨界值。在停用帳戶之前所能容許的無效登入嘗試次數。
- 連續登入失敗的延遲。在兩次嘗試登入失敗後，在這段期間將不容許使用者登入。在每次的連續登入失敗下，延遲會因所架構的時間延遲值（例如：10 秒）而增加。

有關建立帳戶鎖定原則的資訊，請參閱第 54 頁的『設置帳戶鎖定原則』。

密碼原則

WebSphere Commerce 管理主控台的「密碼原則」頁面可讓您控制使用者的密碼選擇，以定義其密碼的特性，確定該密碼符合您網站的安全原則。

此特性用以定義密碼必須遵循的屬性。密碼原則會實施下列條件：

- 使用者 ID 與密碼可否相符。
- 連續字元的出現次數上限。
- 任一字元的出現次數上限。
- 密碼的有效期限上限。
- 英文字母數目下限。
- 數值字元數目下限。
- 密碼長度下限。
- 使用者的前一個密碼可否重覆使用。

有關建立密碼原則的資訊，請參閱第 53 頁的『設置密碼原則』。

另請參閱 WebSphere Commerce 線上說明中的 ″預設鑑別原則″ 參考主題。

和鑑別有關的其它原則

下列各節說明 WebSphere Commerce 所提供的其它和鑑別有關的原則：

密碼無效

架構管理程式的「密碼無效」節點可讓您啓用或停用密碼無效特性。當啓用此特性時，一旦 WebSphere Commerce 使用者密碼過期，則會要求該使用者變更密碼。在此情況下，會將該使用者重新導向至一個要求其變更密碼的頁面。使用者將無法存取網站上的任何安全頁面，直到其變更密碼爲止。

有關「密碼無效」節點的資訊，請參閱第 46 頁的『啓動「密碼無效」』。

受密碼保護的指令

架構管理程式的「受密碼保護的指令」節點可讓您啓用或停用「受密碼保護的指令」特性。當啓用此特性時， WebSphere Commerce 會要求登入 WebSphere Commerce 的已登錄使用者先輸入密碼，才會繼續處理執行指定 WebSphere Commerce 指令的要求。

注意：當您架構受密碼保護的指令時，指令選單中的某些指令可讓一般或訪客使用者執行。因此當您將這類指令架構爲以密碼保護時，會導致一般或訪客使用者無法執行這些指令。因此，在將指令架構爲以密碼保護時，應該特別留意。

註: WebSphere Commerce 在可用指令清單中只會顯示被標爲**已鑑別**的指令，或在 `URLREG` 表格中設有 `https` 旗號的指令。

有關「受密碼保護的指令」節點的資訊，請參閱第 46 頁的『啓用「受密碼保護的指令」』。

階段作業原則

在 WebSphere Commerce 5.4 中，階段作業原則收錄在登入逾時原則中。

透過登入逾時原則，WebSphere Commerce 會使用「登入逾時」節點將長期處於非作用中的使用者登出，並要求他們重新登入系統。此一加強功能是透過 WebSphere Commerce 架構管理程式來呼叫；詳細說明請參閱第 45 頁的『啓用「登入逾時」』。

第 3 章 授權（存取控制）

WebSphere Commerce 將授權視爲一種驗證使用者或應用程式是否有足夠權限存取資源的程序。本章詳述 WebSphere Commerce 存取控制的幾個方面。

在 WebSphere Commerce 中，授權或存取控制是利用存取控制原則來達成。存取控制原則是一種規則，其中說明哪個使用者群組可對某組資源執行某組動作。WebSphere Commerce 會提供一組預設的存取控制原則。這些預設存取控制原則採 XML 格式指定，旨在滿足電子商務網站所需的眾多典型存取控制需求。爲了能瞭解 WebSphere Commerce 的存取控制元件，您必須先瞭解電子商務網站典型的組織階層。

組織階層

WebSphere Commerce 成員子系統中的使用者和組織實體會編到階層中。這種階層會模擬典型的組織階層，其中具有組織與組織單位項目，以及位於葉節點的使用者項目。階層中的最上層有一個虛擬的組織實體*根組織*。其它所有組織實體與使用者皆爲這個根組織的下代。在根組織下，可有一個賣方組織與數個買方組織；而這些組織下皆可有一或多個子組織。買方或賣方管理者是組織的領頭者，負責維護其組織。在賣方組織方面，每一個子組織中可有一或多家商店。商店管理者負責維護商店。下圖顯示企業消費型電子商務網站的組織階層。

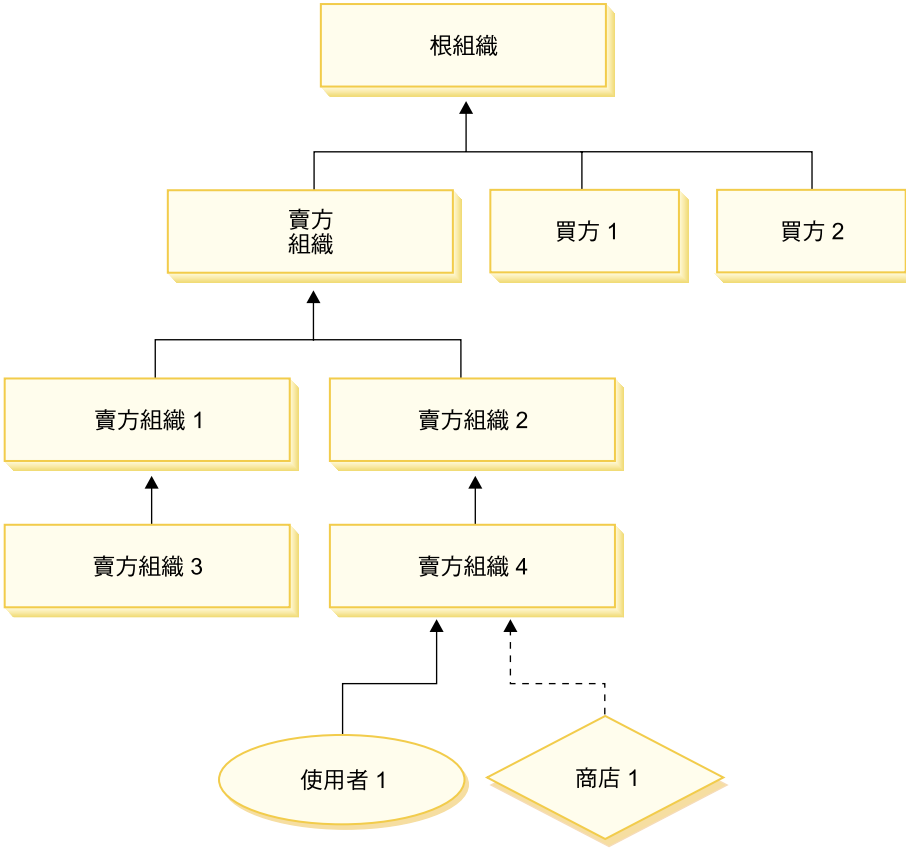


圖 2. 企業消費型商務（B2B）網站的組織階層

根組織

根組織位於組織階層中的最上層。網站管理者具有超級使用者存取權，而可執行 WebSphere Commerce 中的任何作業。網站管理者負責安裝、架構及維護 WebSphere Commerce 與相關的軟硬體。這個職務通常負責控制存取和授權（亦即，建立成員，並爲成員指定適當職務），並管理網站。網站管理者可指定職務給使用者，並指定該使用者是在哪個（些）組織中擔任職務。網站管理者必須指定密碼給每位管理者，以確保只有獲授權者能存取機密資訊。藉此可控制一些重要職責，像是：更新型錄或核准報價要求 (RFQ)。

註: 使用者可在其上層組織以外的組織中擔任職務。

在 WebSphere Commerce 網站中有一個賣方組織。在企業消費型商務（B2B）網站中，亦有一或多個買方組織。網站管理者可定義賣方組織（擁有商店）的存取控制原則，也可以爲商店的每一個買方組織定義存取控制原則。在大眾消費型商務（B2C）網站中，則沒有買方組織。大眾消費型商務（B2C）的客戶則被塑造成預設組織的成員。

組織（賣方）

在企業消費型商務（B2B）與大眾消費型商務（B2C）網站中，網站管理者可建立一個最上層的賣方。在這個賣方組織下，可建立其它子組織或組織單位。這些賣方端的組織實體皆可擁有一或多家商店。接著，網站管理者可爲賣方組織定義任何特殊的存取控制原則，並指定一個賣方管理者，以負責管理該組織。賣方管理者可根據該組織的相關存取控制原則，來登錄使用者並爲其指定不同的職務，以符合組織的商業需求。

賣方管理者的職責彙整如下：

- 建立可擁有商店的子組織。選擇性定義組織內需要核准的程序。只有企業消費型商務（B2B）網站才需要這個步驟。
- 指定職務給子組織。
- 建立使用者。
- 指定職務給使用者。

組織（買方）

在企業消費型商務（B2B）網站中，網站管理者可根據商業需求來建立一或多個買方組織。接著，網站管理者可爲買方組織定義任何特殊的存取控制原則，並指定一個買方管理者，以負責管理買方組織。買方管理者可根據該組織的相關存取控制原則，來登錄使用者並爲其指定不同的職務，以符合組織的商業需求。

買方管理者的職責彙整如下：

- 建立與管理買方組織中的子組織。選擇性定義組織內需要核准的程序。只有企業消費型商務（B2B）網站才需要這個步驟。
- 指定職務給子組織。
- 建立使用者。
- 指定職務給使用者。

註: 網站管理者可修改與管理買方組織的存取控制原則（若適當的話）。有關網站管理者的進一步資訊，請參閱第 18 頁的『網站管理者』。

職務

如同上述，WebSphere Commerce 會提供預設的職務組合。網站管理者必須先指定特定的職務給每一個組織，再爲使用者指定這些職務。組織只能擔任已指定給其上層組織的職務。同樣地，使用者只能擔任已指定給其上層組織的職務。

WebSphere Commerce 中的所有職務皆以組織範圍爲限。舉例來說，使用者爲組織 X 的產品經理。此使用者的上層組織本身也必須被指定爲「產品經理」職務。因而可設置存取控制原則，讓此使用者只能在組織 X 與其子組織的範圍中，執行產品管理作業。

註: 指定職務給使用者與組織是透過 MBRROLE 表格來完成。

WebSphere Commerce 所附的預設職務可分成下列幾類：

- 網站作業
- 網站與內容開發
- 行銷管理
- 產品管理
- 銷售管理
- 流程管理與營運管理
- 組織管理

網站作業

WebSphere Commerce 支援下列的技術作業職務：

- 網站管理者
- 商店管理者

網站管理者

網站管理者負責安裝、架構及維護 WebSphere Commerce 與相關的軟硬體。管理者要回應系統警告、警示和錯誤，以及診斷和解決系統問題。 這個職務通常要控制存取和授權（建立成員，並爲成員指定適當職務）、管理網站、監視網站效能及管理負荷平衡作業。網站管理者也可能要負責建立和維護多個伺服器架構，供測試、暫置和正式作業等不同開發階段使用。這個職務也要處理重要的系統備份及解決效能問題。

商店管理者

商店管理者負責管理商店資產及更新和公佈稅金、出貨和商店資訊的變更。商店管理者也可以管理組織的存取控制原則。商店管理者通常是商店開發團隊中的領

導人，是團隊中唯一有權公佈商店紀錄的職務（網站管理者也可以公佈商店紀錄）。商店管理者通常有非常豐富的 Web 知識，對於商店的商業程序有全盤的瞭解。

網站與內容開發

WebSphere Commerce 可支援商店程式開發人員網站與內容開發職務。

商店程式開發人員

商店程式開發人員負責建立 Java Server Pages 檔案及任何必要的自訂程式碼，且可以修改 WebSphere Commerce 中所含的任何標準功能。一旦建立好商店紀錄後，商店程式開發人員有權以手動方式或利用「商店設定檔」、「稅金」及「出貨」筆記本來變更商店紀錄。但他們無權將商店紀錄公佈到 WebSphere Commerce Server 中。

流程管理與營運

WebSphere Commerce 支援下列的流程管理與營運管理職務：

- 流通經理
- 營運經理
- 接單者
- 退貨管理者
- 裝箱員

流通經理

Business 流通經理（有時稱爲「貨運經理」）負責管理與協調從貨運公司到倉儲（以及到個別客戶）間的大量運輸或出貨。此職務負責確定公司所用的是最符合公司策略的最佳托運者以及最理想的價格。出貨是一項重要的客戶服務，且可能是線上商務是否成功的關鍵因素。

營運經理

B2C 此職務負責管理訂單處理、確定訂單的履行適當、付款已收到以及已出貨。「營運經理」可以搜尋客戶訂單、檢視明細、管理訂單資訊，以及建立和編輯退貨。

裝箱員

裝箱員負責從供貨中心揀取產品，並爲產品裝箱以運送給客戶。裝箱員也負責管理取貨券和裝箱單，這些是在訂單供貨期間用來確認產品的出貨。

接單者

接單者負責在供貨中心接收庫存，追蹤訂購產品的預期庫存記錄與臨時的收據，以及接收客戶所退回的退貨產品。

退貨管理者

退貨管理者負責管理退貨產品的處置。

- 列出退貨
- 列出退貨產品
- 處置退貨產品

產品管理

WebSphere Commerce 支援下列的產品管理職務：

- 買方（對賣方而言）
- 種類經理
- 產品經理或產品推銷經理

買方（對賣方而言）

買方負責購買銷售的商品。買方亦負責處理和供應商間的關係，並負責協商以便在交貨與付款選項等方面有利的條款下取得所要的產品。買方可以設定價格。庫存亦由買方負責管理，以決定所要購買的數量並確定庫存能適當補充。

種類經理

種類經理負責管理種類階層，像是：建立、修改以及刪除種類。種類階層中組織了商店所提供的產品或服務。種類經理亦負責管理產品、預期庫存記錄、供應商資訊、庫存以及退貨原因。

產品經理/產品推銷經理

Business 產品推銷或 B2C 產品經理負責追蹤客戶的交易、建議折扣，以及決定在線上商店中顯示、標價和銷售產品的最佳方式。

- 執行種類經理的所有作業
- 執行行銷經理的所有作業

銷售管理

WebSphere Commerce 支援下列的商業關係管理職務：

- 業務經理
- 帳戶代表
- 客戶服務主管

- 客戶服務代表

業務經理

業務經理負責獲得客戶並留住客戶，達成銷售預測目標，提供足以提高客戶生意的誘因，合約管理，設定計價條款，和產品經理一起建立庫存預測，以及配合行銷經理一同促銷。

帳戶代表

帳戶代表負責處理個人帳戶，並建立關係以及管理客戶服務問題。帳戶代表有權依照帳戶種類變更合約計價，商討合約，設定檔，以及分析獲利能力。

客戶服務主管

此職務負責存取所有的客戶服務工作。客戶服務主管負責管理客戶的詢問（像是客戶登錄、訂單、退貨與拍賣），並有權完成客戶服務代表無法存取的作業，像是：核准一些被系統拒絕的退貨記錄，以及通知客戶付款異常狀況（如：信用卡授權失敗）。

客戶服務代表

不論您的線上商務設計得多好，而能提供客戶自助性，總是有某類客戶或在某些情況下客戶（即使是相當熟悉 Web 運作的客戶）需要與專人聯絡。大部份的線上商務皆會提供電子郵件、傳眞或聯絡電話，讓客戶獲得直接的服務。客戶服務便負責處理客戶的所有查詢。

行銷管理

WebSphere Commerce 支援行銷經理的行銷管理職務。

行銷經理

行銷經理負責將行銷策略和品牌訊息傳遞給客戶。此職務負責監督、分析和瞭解客戶的行爲。此外，行銷經理亦負責針對目標銷售建立或修改客戶設定檔，並建立與管理活動與促銷。活動事件的規劃可由商家、行銷經理與產品推銷經理組成的團隊處理。

組織管理

WebSphere Commerce 支援下列的組織管理職務：

- 賣方管理者
- 買方管理者
- 買方核准者

賣方管理者
買方管理者負責管理賣方組織的相關資訊。賣方管理者負責建立與管理賣方組織中的子組織以及各類使用者（包括：指定適當的商業職務）。

買方管理者
買方管理者負責管理買方組織的相關資訊。他們負責建立與管理買方組織中的子組織，以及管理各類使用者（包括核准使用者作爲買方）。此外，亦可建立與管理其它買方端的職務（像是：買方核准者與其它的買方組織管理者）。

買方核准者
買方核准者爲買方組織中負責在提交訂單以便向賣方購買之前核准買方訂單的人。

存取控制原則

存取控制原則是授權使用者群組可對 WebSphere Commerce 中的一組資源執行一組動作。除非透過一或多項存取控制原則授權，否則使用者無權存取系統中的任何功能。爲了瞭解存取控制原則，您必須瞭解下列四大概念：使用者、動作、資源與關係。使用者爲使用系統的人。資源爲系統中需受保護的物件。動作是指使用者可對資源執行的活動。關係是指存在於使用者與資源間的選用條件。

存取控制原則的元素

存取控制原則是由四個元素組成：

存取群組
原則所適用的使用者群組。

動作群組
供使用者對資源執行的一組動作。

資源群組
由原則所控制的資源。資源群組可包括商業物件（像是合約或訂單），或一組相關指令（像是：具備某特定職務的使用者所能執行的所有指令）。

關係（選用）
每一種資源類別都可以有一組相關的關係。每一個資源可有一組使用者來達成每一種關係。舉例來說，原則中可指出唯有訂單的建立者才能修改該訂單。在此情況下，關係爲建立者，而其存在於使用者與訂單資源之間。

存取控制原則的概念

存取控制原則是授與使用者存取您的網站。除非使用者因一或多個存取控制原則而獲權執行其職責，否則使用者無權存取您網站中的任何功能。

每一個存取控制原則的格式如下：

```
AccessControlPolicy [AccessGroup,ActionGroup,ResourceGroup,Relationship]
```

存取控制原則中的元素會指出屬於特定存取群組的使用者，可針對屬於指定資源群組的資源，執行指定動作群組中的動作，但前提是使用者符合與資源之間的特定關係。只有在需要時才需指定關係。例如，`[AllUsers, UpdateDoc, doc, creator]` 表示只要使用者是文件的建立者，便能更新文件。

下列各節說明存取控制的概念資訊與相關術語。

成員群組

WebSphere Commerce 中的成員子系統可讓您建立成員群組，這是根據各種商業理由所分類出的使用者群組。您可以根據各種目的來分組，像是：存取控制目的、核准目的，以及行銷目的（如：計算折扣與價格、展示產品等）。「存取群組」成員群組類型 (-2) 是基於存取控制目的，「使用者群組」成員群組類型 (-1) 則是基於一般目的。成員群組和成員群組類型的連結是利用 MBRGRPUSG 表格來建立。

存取群組: 「存取群組」成員群組類型 (-2) 是基於存取控制目的來分類使用者。存取群組是存取控制原則中的一個元素，是由基於存取控制目的而明確定義出的使用者組成。存取群組中的成員準則通常是以職務、使用者所屬的組織或使用者登錄狀態爲基礎。例如，名爲**買方管理者**的存取群組，是由一群具備買方管理者職務的使用者組成。

WebSphere Commerce 含有一些預設職務，且每一種職務會對應至一個隱含參照該職務的預設存取群組。您可以根據使用者在網站中所提供的活動類型，將職務當成屬性以新增使用者到存取群組中。例如依預設，「賣方管理者」職務會有一個對應的**賣方管理者**存取群組。網站管理者可以利用 WebSphere Commerce 管理主控台來建立、維護以及刪除網站內的存取群組。買方管理者或賣方管理者可使用 WebSphere Commerce 的「組織管理主控台」，來指定職務給使用者，或明確指定使用者所屬的存取群組。存取群組可以是隱含、明確或兩者。

隱含的存取群組: 隱含的存取群組由一組準則定義而成。凡符合準則的人皆爲該群組中的成員。準則通常是以使用者的職務、上層組織或登錄狀態爲基礎。用來定義成員群組中之成員的隱含條件位於 MBRGRP 表格的 CONDITIONS 直欄中。使用會指定使用者屬性的隱含存取群組，可方便您授權存取權給相似的使用者，而不必明確指定與取消指定個別使用者。此外，當使用者的屬性變更時，也用不著更新群組的成員。您可爲存取群組指定簡單的準則，亦即，只要被指定有特定職務的人即可納入，不管該使用者是具備哪個組織中的職務。也可以指定複雜的準則，亦即，使用者必須具備某特定組織的某組職務中之一，才能隸屬該存取群組下。

明確的存取群組: 您可以明確在成員群組中新增或移除使用者。這兩種明確指定，可透過 MBRGRPMBR 表格來完成。明確的成員群組含有明確指定的使用者，而這些使用者不見得共用共通的屬性。此外，也可讓您將一些雛符合隱含定義群組列入條件但您卻不想列入的個人排除在外。

使用者群組: 「使用者群組」成員群組類型 (-1) 爲商家所定義出的一群使用者，而這些使用者具有共同的興趣。使用者群組很像是大型商店爲其常客或屬意的客戶提供的俱樂部。客戶成爲使用者群組中的一員後，在購買產品時，可享有特殊折扣及優惠。例如，如果市調顯示出高齡顧客不斷重覆購買旅遊書籍和行李箱，您就可以將這些客戶指定到稱爲**銀髮族旅遊俱樂部**的成員群組中。同樣地，您也可以建立一個使用者群組來酬謝一些老主顧。

動作

一般而言，動作爲一種針對資源執行的作業。在控制程式指令的職務型原則方面，動作通常爲**執行**，且資源指的是所要執行的指令。而在檢視畫面的職務型原則方面，動作爲檢視畫面的名稱，而資源是 com.ibm.commerce.commands.ViewCommand。若是資源層次型存取控制，則動作通常映射至 WebSphere Commerce 指令，且資源通常是指受保護 EJB (Enterprise Java Bean) 的遠端介面。舉例來說，對控制程式 com.ibm.commerce.order.objects.Order 資源執行控制程式指令 com.ibm.commerce.order.commands.OrderCancelCmd。 最後，**顯示**動作用以啓動資料 Bean 資源。

WebSphere Commerce 管理主控台可供網站管理者讓現有動作連結動作群組，但無法用來建立新動作。如果要建立新動作，可將之定義在 XML 檔中，然後再載入到資料庫。動作會儲存在 ACACTION 表格中。

動作群組

動作群組是相關動作的集合。像 AccountManage 群組即爲一種動作群組，其所含的指令如下：

- com.ibm.commerce.account.commands.AccountDeleteCmd
- com.ibm.commerce.account.commands.AccountSaveCmd

只有網站管理者才能建立、更新與刪除動作群組。這可透過 WebSphere Commerce 管理主控台與 XML 來完成。動作群組儲存在 ACACTGRP 表格中。動作與動作群組間的連結是在 ACACTACTGP 表格中建立。

資源種類

資源種類會參照一種資源類別，且受到存取控制的保護。資源必須施行「可保護」介面資訊。資源種類爲一些 Java 類別，像是：訂單、RFQ、拍賣等。資源爲

這些類別的案例。舉例來說，拍賣管理者 A 建立的 Auction1 即爲一種資源；而拍賣管理者 B 所建立的 Auction2 則爲另一種資源。這兩種資源皆隸屬於「拍賣」資源種類下。

註: 有關「可保護」介面的進一步資訊，請參閱 *IBM WebSphere Commerce 程式設計手冊*。

資源種類定義於 ACRESCGRY 表格中，爲了方便，有時會稱爲資源。網站管理者可使用 WebSphere Commerce 管理主控台，讓現有資源種類連結資源群組。新資源種類可使用 XML 來建立。

資源

資源爲系統中需受保護的任何物件。舉例來說， RFQ、拍賣、使用者和訂單都是 WebSphere Commerce 中一些需受保護的資源。每個資源都有一位擁有者。資源的擁有權用以判斷該資源所套用的是哪些存取控制原則。存取控制原則有一個擁有者，並且是組織實體。原則只會套用在擁有該原則之相同組織實體所擁有的資源上。而其上代組織實體所擁有的原則亦會套用在該資源上。

控制程式指令資源: 就控制程式指令的職務型存取控制而言，會建構原則，以便對控制程式指令資源進行執行動作。這些原則旨在限制唯有具備指定職務的使用者才能執行控制程式指令。這些原則的存取群組通常是一群具備某單一職務者（如：具備「產品經理」職務的產品經理）。而資源群組則是一組產品經理所能執行的控制程式指令。

在您對控制程式指令實施職務型存取控制時，必須決定出指令的擁有者。其做法是在指令中呼叫 getOwner() 方法（如果有施行的話）。由於通常不會施行此方法， WebSphere Commerce 執行時期會執行下列之一來評估出：

- 採用擁有目前指令環境定義中之商店的組織。
- 如果指令環境定義中沒有商店，則以根組織做爲擁有者。

資料 Bean 資源: 並非所有資料 Bean 都需要保護。在現有的 WebSphere Commerce 應用程式中，需要保護的資料 Bean 已施行必要的存取控制。 不過當您建立新資料 Bean 時，便會出現該保護哪些資源的問題。請根據您的應用程式來決定所要保護的資源。如果職務型存取控制不足以保護將顯示在檢視畫面上（對應至內含資料 Bean 的 JSP (Java Server Page) 的資訊，則應保護該資料 Bean（直接或間接）。

如果資料 Bean 需受到保護，而其可獨立存在，則應直接保護。如果資料 Bean 的存在與否取決於另一資料 Bean 的存在而定，則應委由另一資料 Bean 來保護。例如像 Order 資料 Bean 即爲直接保護的資料 Bean。而像 OrderItem 資料 Bean 則

爲間接保護的資料 Bean （因爲它隨 Order 資料 Bean 而存在）。有關如何保護資料 Bean 資源的進一步資訊，請參閱 *WebSphere Commerce 5.4 程式設計手冊*。

資料資源: 資料資源是指可操作的商業物件，像是：拍賣、訂單、RFQ 與使用者。這些通常是在 Enterprise Bean 層次下受到保護，不過只要其有施行「可保護」介面，也可保護任何類別。資料資源是透過資源層次存取控制檢查來保護。其通常的做法是在控制程式或作業指令的 getResources() 方法中傳回資料資源。進一步資訊請參閱 *WebSphere Commerce 5.4 程式設計手冊*。

資源群組

資源群組代表一組相關的資源。資源群組可包含商業物件，像是：合約或一組相關指令。在存取控制中，資源群組會指定存取控制原則授權存取的資源。

資源群組定義於 ACRESGRP 表格中。網站管理者可使用 WebSphere Commerce 管理主控台或 XML，來管理資源群組以及讓資源連結資源群組。

隱含的資源群組: 隱含的資源群組中定義了符合某組屬性的資源。這些屬性中必須有一個是 Java 類別名稱。其它屬性可包括狀態、商店 ID、價格等。例如，您可建立一個內含所有處於擱置狀態之訂單 (ORDERS.STATUS=P) 的隱含資源群組。隱含資源群組的用途是當有一群資源具有 Java 類別名稱以外的共通屬性時，則可使用隱含資源群組來集結這些將用於資源層次型原則中的資源。

隱含的資源群組是以 ACRESGRP 表格中的 CONDITIONS 直欄來定義。簡單的隱含資源群組可使用 WebSphere Commerce 管理主控台來建立。如果群組越來越複雜，則可使用 XML 來建立。

明確的資源群組: 當將一或多個資源種類連結某個資源群組時，即可稱爲明確的資源群組。這種連結是在 ACRESGPRES 表格中來完成。這種藉由列出其 Java 類別名稱，明確在群組中新增資源種類的方式，可讓您將不一定共用共通屬性的個別資源集結在一起。

關係

每一項資源可能具有某種相關的關係以及一組履行各關係的成員。舉例來說，所有資源都有一種*擁有者*關係，這個關係是由資源的擁有者履行。其它關係還可包括文件的收件人以及訂單的建立者。在決定哪些人可對特定資源案例執行某些動作方面，這些資源關係相當重要。例如，文件建立者無法刪除文件，但審核者卻可以。同樣地，檢視者只能讀取和核准文件，但卻不能轉遞文件或執行其它作業。

關係儲存在 ACRELATION 表格中，並可選擇性地使用 ACPOLICY 表格中的 ACRELATION_ID 直欄將之指定在存取控制原則中。在您評估要求使用者與資源間

必須存在關係的原則時，將會對資源呼叫 fulfills(Long Member, String relationship) 方法來評估之。如果比較這些關係和關係群組，這些關係有時可稱爲單純關係。

關係群組: 存取控制原則可指出使用者和所要存取的資源間必須存在某種特定關係，或者可指出使用者必須具備關係群組中的指定條件。在大部份情況下，使用一種關係即可。不過，如果需要複雜關係，則可改用關係群組。關係群組可讓您指定多重關係，且可以是一個關係鏈。這兩種皆可使用關係鏈概念來達成。關係鏈是一種概念，可用來傳達一種單純關係（直接存在於使用者與資源間），也可以用來傳達存在於使用者與資源間的一連串關係。 舉例來說，爲了傳達使用者必須在某個和資源間存在一種關係（非擁有者關係）的組織中擔任職務，則必須使用關係群組。在本例中，使用者與組織間存在職務關係，而組織與資源間亦存在一個關係。

比較關係與關係群組: 在大部份情況下，只使用一種關係應已足以符合您應用程式的存取控制需求，這是因爲在概念上，大部份關係是直接存在於使用者與資源間。舉例來說，原則中指出使用者必須是資源的建立者。不過，如果您想指定多重關係，則應使用關係群組。舉例來說，原則中指出使用者必須是資源的建立者或提交者。

如果要傳達使用者與資源間的關係鏈，亦必須使用關係群組。在關係鏈中，使用者與資源間沒有直接關係，舉例來說，使用者隸屬於訂單指定的買方組織。在此情況下，使用者和組織間存在一種下層關係，而該組織和訂單間存在一種買方關係。

關係鏈: 每一個關係群組由一或多個 RELATIONSHIP_CHAIN 開放條件組成，這些條件是依照 andListCondition 或 orListCondition 元素分組。關係鏈爲一系列一個以上的關係。關係鏈的長度取決於所含的關係數目而定。您可檢查關係鏈 XML 表示法中的 <parameter name= "X" value="Y"/> 項目數即可判定。以下是關係鏈的範例，其長度爲 1。

```
<openCondition name="RELATIONSHIP_CHAIN">
<parameter name="RELATIONSHIP"
value="aValue"/>
</openCondition>
```

對長度 1 的關係鏈而言， <parameter name="Relationship" value="something"> 元素指出使用者與資源間存在一個直接關係。 value 屬性爲一個字串，代表使用者與資源間的關係。此值亦必須對應至可保護資源中 fulfills() 方法的 relationship 參數。

當關係鏈的長度爲 2 時，則爲一連串的兩個關係。第一個 <parameter name= "X" value="Y"/> 元素是指使用者與組織實體之間。最後一個 <parmeter name= "X" value="Y"/> 元素是指組織實體與資源間。以下是關係鏈的範例，其長度爲 2。

```
<openCondition name=RELATIONSHIP_CHAIN">
<parameter name="aValue1" value="aValue2"/>
<parameter name="RELATIONSHIP" value="aValue3"/>
</openCondition>
```

aValue1 的可能值有 HIERARCHY 與 ROLE。HIERARCHY 代表成員階層中之使用者與組織實體間的階層關係。 ROLE 代表使用者在組織實體中所擔任的職務。

如果 aValue1 值爲 HIERARCHY，則可能值包括 child，亦即，會傳回在成員階層中使用者直屬其下的組織實體。 如果 aValue1 的值爲 ROLE，則可能值包含 ROLE 表格之 NAME 直欄中的任何有效值，亦即，會傳回現行使用者擔任職務所在的所有組織。

aValue3 項目爲一個字串，代表一或多個組織實體（從第一個參數與資源評估出）間的關係。此值對應至可保護資源中 fulfills() 方法的 relationship 參數。當評估 aValue1 參數的結果傳回一個以上的組織實體時，只要這些組織實體至少有一個符合 aValue2 參數所指定的關係，即符合 RELATIONSHIP_CHAIN 中的這個部份。

註: 如果關係群組是由一個只含單一參數元素的單一關係鏈構成，其相當於一個單純關係。在此情況下，可在原則中改用關係較好，而不使用關係群組。

資源與原則的擁有權

所有原則皆屬於某組織實體所擁有。所有存取控制也會有一個擁有者（通常是組織實體）；舉例來說，訂單是屬於擁有該商店（下單所在）之組織的。使用者也可以擁有資源，舉例來說，已登錄的使用者擁有本身的使用者登錄資訊。資源與存取控制原則的擁有權是決定該資源將套用哪些原則的重要關鍵。對給定資源而言，將會套用隸屬於其所屬組織實體下的原則，以及擁有者之上代組織實體的原則。

存取控制原則的類型

存取控制原則有下列兩種類型：

- 標準原則
- 範本原則

標準原則

標準原則會有一個固定的擁有者。舉例來說，假設某標準原則屬於賣方組織的，則該原則將只會套用在該賣方組織所擁有的資源上，以及套用在其下代組織實體

所擁有的資源上。由於根組織是 WebSphere Commerce 中其它所有組織的上代組織，因此依照定義，凡隸屬於根組織（成員 ID = -2001）下的原則，會套用在網站中的所有資源上。因而，根組織所擁有的標準原則有時可稱爲網站層次的原則。

而非隸屬於根組織下的標準原則，則稱爲組織層次的原則；這是因爲這類原則的套用範圍不是整個網站，而只會套用在原則擁有者所擁有或其任何下代組織實體所擁有的資源上。商店管理者可管理其本身之組織實體與其下代組織實體的原則。網站管理者則可修改所有原則。

範本原則

範本原則的擁有者爲動態的。範本原則是動態套用在擁有資源的組織實體與其上代組織實體上。舉例來說，假設根組織下有 10 個組織，且每一個組織皆想確定商店管理者只能修改其擔任職務所在之組織所擁有的資源。其設置方法有下列兩種：

1. 採用一項範本原則，以根據所要存取的資源，動態套用在這 10 個組織中的任何一個上。範本原則中的存取群組準則也可以動態。舉例來說，假設使用者試著存取組織 3 所擁有的資源，則範本原則的擁有者旋即變成組織 3，而存取群組亦隨而將本身限定在組織 3 範圍內，也就是說，使用者必須具備組織 3 的「商店管理者」職務才行。
2. 採用 10 項原則，這 10 個組織每一個各擁有一項原則。組織 1 的存取群組訂出使用者必須具備組織 1 的「商店管理者」職務。組織 2 的存取群組訂出使用者必須具備組織 2 的「商店管理者」職務，以此類推。

第一種處理方式的優點是，原則只有一份實體，但有 10 份邏輯。範本原則可供網站管理者管理。

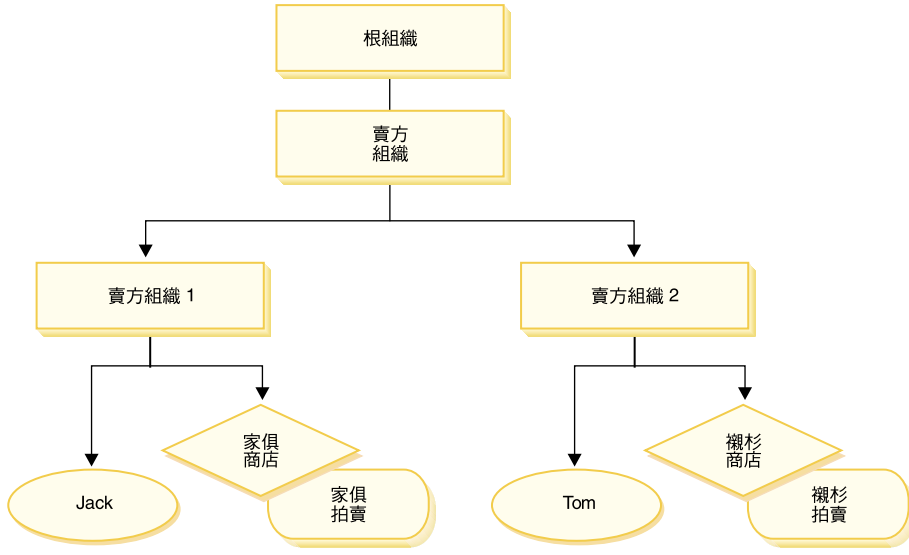
改寫範本原則: 範本原則的另一特性是，可針對指定的組織實體加以改寫。以上例來說，假設在 WebSphere Commerce 網站中新增了第 11 個組織，但這個最新的組織實體不想套用上述的範本原則，則其中一種做法是指定此範本原則。在此情況下，必須在 ACORGPOL 表格中新增項目，以指定範本原則的原則 ID 以及該第 11 個組織的組織實體 ID。當商店管理者在特定組織的環境定義下，刪除或更新範本原則時，則也可以透過 WebSphere Commerce 管理主控台來完成。

當改寫根組織之某些下代組織的範本原則時，範本原則仍會套用在根組織層次上。如果下代組織層次以較嚴苛的原則改寫範本原則時，您也應在根組織層次下改寫範本原則。改寫根組織之範本原則的唯一方法是透過資料庫，亦即執行下列 SQL：

```
insert into ACORGPOL (acpolicy_id, member_id) values ( (select acpolicy_id from
ACPOLICY where policyname = 'policyToOverride'), -2001)
```

存取控制的層次

WebSphere Commerce 中有兩個廣域的存取控制層次：指令層次（亦稱爲職務型）與資源層次（亦稱爲案例型）。



指令層次或職務型存取控制

指令層次型或職務型存取控制屬於粗略的存取控制。主要是判斷 "哪些人可執行哪些事"。在職務型存取控制下，您可以指出凡具備特定職務的使用者可執行某些指令。以「賣方可執行賣方指令」的存取控制原則爲例。在此原則中，其中一個賣方指令爲 `ModifyAuction` 指令。在上圖中，Jack 與 Tom 皆爲賣方，兩者皆可修改拍賣。

職務型存取控制是用在控制程式指令與檢視畫面上。此種存取控制類型不會考慮到指令所要執行的資料資源對象。它只會判斷該使用者能否執行特定的控制程式指令或檢視畫面。

此種存取控制層次爲必要的，並且由執行時期實施。所有控制程式指令必須受指令層次的存取控制保護。此外，凡是可直接呼叫的檢視畫面，或者可藉由另一個指令重新導向而啓動的檢視畫面（相對於藉由轉遞至檢視畫面而啓動）皆必須受指令層次的存取控制保護。

控制程式指令的指令層次型存取控制: 只要您執行控制程式指令，便必須有一則存取控制原則，以授與使用者對指令資源採取執行動作。資源爲控制程式指令的介

面名稱。而存取群組通常配合一個單一職務。舉例來說，您可以指出具備「帳戶代表」職務的使用者可執行 AccountRepresentativesCmdResourceGroup 資源群組中的任何指令。

檢視畫面的指令層次型存取控制: 如果檢視畫面是由 URL 直接呼叫，或者是由指令重新導向而來，則該檢視畫面必須有一項存取控制原則。且這類原則必須有一個 viewname（檢視畫面名稱），並當成動作指定在 ACACTION 表格中。接著，必須使用 ACACTACTGP 表格，讓此動作連結一個動作群組。然後，此動作群組必須在 ACPOLICY 表格中參照適當的指令層次型原則。

案例型或資源層次型存取控制

案例型或資源層次型存取控制原則可提供細膩的存取控制，主要是判斷哪些人可對哪些資源執行哪些指令。以上述的職務型存取控制原則範例（容許賣方修改拍賣）來說，可細膩調整成資源層次型存取控制，亦即，指出賣方可修改其組織（擔任職務所在）所擁有的拍賣。在30中，Jack 擔任「賣方組織 1」中的賣方職務， Tom 擔任「賣方組織 2」中的賣方職務。Jack 在家俱店中設立一項家俱拍賣。 Tom 在襯衫專賣店中建立一項襯衫拍賣。 Jack 可修改家俱拍賣，但*不能*修改襯衫拍賣。Tom 可修改襯衫拍賣，但*不能*修改家俱拍賣。

總結來說，系統會先進行指令層次的存取檢查。假設使用者能執行該指令，接著便會執行資源層次型存取控制原則，以判斷使用者能否存取考量中的資源。

資源層次型存取控制是套用在指令與資料 Bean 上。

指令的資源層次型存取控制: 在完成指令層次型存取控制檢查後，如果授與存取權，則在下列兩種情況之一下，將會進行資源層次檢查：

- 指令施行 getResources() -- 此方法指出針對現行動作而需要檢查的資源案例；此時的指令爲動作。 WebSphere Commerce 執行時期所實施的是現行使用者對 getResources() 所指的所有資源具備存取權。依預設，getResources() 會傳回空值，亦即，不會執行任何的資源層次檢查。
- 指令呼叫 checkIsAllowed(Object Resource, String Action) -- 假設指令撰寫者在執行時期呼叫 getResources() 時不知道需檢查哪些資源，則指令可視需要呼叫這個 checkIsAllowed() 方法，以判斷「現行動作/資源」對組是否經過授權。動作通常是現行指令的介面名稱。當呼叫此方法時，假設拒絕存取，則會擲出異常狀況：ECApplicationException(ECMessage._ERR_USER_AUTHORITY, ..)

資料 Bean 的資源層次型存取控制: 一如上述，檢視畫面是受指令層次型原則的保護，而這類原則通常是以職務爲基礎。舉例來說，指令層次型原則可訂出「賣方管理者」能存取特定檢視畫面。這通常還需進一步確定：JSP 中的資料 Bean 是指和使用者具備「賣方管理者」職務所在之組織有關的所有資料 Bean。其做法是讓所有需要保護（不論直接或間接）的資料 Bean 皆施行「委任者」介面。這些資

料 Bean 委任由主要（獨立的）資料 Bean 執行，由其轉而施行「可保護」介面。而主要資料 Bean 則委任給自己，因此將同時施行兩種介面。 接著，只要使用資料 Bean 管理程式的 activate() 方法呼叫資料 Bean， WebSphere Commerce 執行時期即會確定會有原則授與現行使用者有權對主要資料 Bean 資源執行 顯示動作。

存取控制如何防止越權動作

本節說明以原則爲基礎的存取控制如何運作，以確保使用者只能執行獲准的動作。

在執行使用者起始的動作前先檢查授權

*原則管理程式*爲一種存取控制元件，用以判斷現行使用者可否對指定的資源執行指定的動作。存取控制原則是以 XML 格式指定。在建立案例期間，會將預設原則載入到適當的資料庫表格中。當 WebSphere Commerce Application Server 啓動時，由於會將存取控制資訊快取到記憶體中，原則管理程式可在被呼叫時能迅速檢查使用者的授權情況。如果您透過 WebSphere Commerce 管理主控台（或藉由載入 XML 原則資料）變更資料庫中的存取控制資訊，則必須更新存取控制快取。其做法是在 WebSphere Commerce 管理主控台中更新存取控制登錄。重新啓動 WebSphere Commerce 的結果，亦會更新快取。

只要使用者試著執行受存取控制保護的動作時，即會執行存取控制檢查，以以確定該使用者已獲授權。「原則管理程式」會找出所有套用在擁有該資源之組織的存取控制原則。然後檢查這些原則，以評估該使用者是否有權對目標資源執行動作。只要至少找到一項此類原則，原則管理程式即授與存取權，否則即拒絕存取。

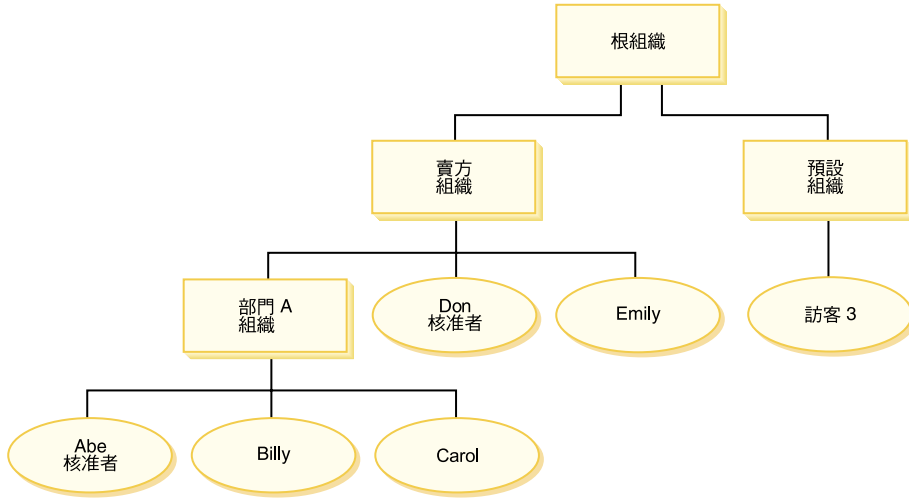
使用存取控制

有關自訂預設存取控制原則、自訂實務以及使用 XML 檔來自訂存取控制原則等作業的進一步資訊，請參閱「WebSphere Commerce 存取控制手冊」。

評估存取控制原則

本節可做爲您評估存取控制原則時的參考。在本節中，會提供一個實務給您，並以範例說明如何評估標準與範本存取控制原則。每一節的開頭爲相關原則的說明，然後是使用每一項原則的實務。有關標準與範本原則的進一步資訊，請參閱第 28 頁的『存取控制原則的類型』。

下圖顯示實務：



組織階層

從此圖中，您可看到網站中存在下列四個組織：

- 根組織
- 賣方組織
- 預設組織
- 部門 A 組織

如同您所看到的，根組織是賣方組織與預設組織的上一層。而賣方組織是部門 A 組織的上一層。

使用者

在此圖中，Don 與 Emily 登錄在賣方組織中。 Abe、Billy 與 Carol 登錄在部門 A 組織中。訪客 3 並未登錄，但基於存取控制目的，隱含隸屬在預設組織下。

職務

Don 在賣方組織中擔任核准者職務。Abe 在部門 A 組織中擔任核准者職務。

存取群組

本實務所用的存取群組如下：

- 已登錄的使用者：此群組隱含包含所有已登錄的使用者。
- 賣方的核准者：此群組隱含包含在賣方組織中擔任核准者職務的所有使用者。

- 部門 A 的核准者：此群組隱含包含在部門 A 組織中擔任核准者職務的所有使用者。

文件

文件物件是一個受保護的資源。文件的擁有者被定義成建有該文件的組織。

更新文件時的相關存取控制需求

以下是更新文件時的相關存取控制需求：

1. 已登錄的使用者可更新其所建立的文件。
2. 部門 A 的核准者可更新部門 A 所擁有的文件，但賣方所擁有的文件則不行。賣方組織的核准者則可更新同時部門 A 與賣方組織所擁有的文件。

評估標準原則

本節說明標準原則，並提供相關的評估實務。

和更新文件有關的存取控制原則

以下是和更新文件有關的原則格式以及存取控制原則：

原則格式：[存取群組，動作群組，資源群組，關係]

原則 1:

[已登錄的使用者，執行指令動作群組， 更新文件
資源群組，-]

此爲根組織所擁有的標準職務型原則。在此原則中，已登錄的使用者可執行更新文件指令。

原則 2:

[已登錄的使用者，更新文件動作群組，文件，建立者]

此爲根組織所擁有的標準資源層次型原則。在此原則中，已登錄的使用者只要是文件的建立者即可更新該文件。

原則 3:

[賣方的核准者，更新文件動作群組，文件，-]

此爲賣方組織所擁有的標準資源層次型原則。在此原則中，賣方的核准者可更新賣方所擁有的文件。

原則 4:

[部門 A 的核准者，更新文件動作群組，文件，-]

此爲部門 A 組織所擁有的標準資源層次型原則。在此原則中，部門 A 的核准者可更新部門 A 所擁有的文件。

實務

實務 1：Billy 想更新自己的文件: 以下是此實務的存取控制評估：

指令 - 層次檢查:

1. 由於未指定商店 ID，而將指令的擁有者設爲根組織。因此，只會使用根組織所擁有的原則來評估使用者是否具備指令層次的存取權：根組織擁有原則 1 與原則 2。
2. 原則 1 授與存取權；這是因爲 Billy 是「已登錄的使用者」存取群組中的成員，而他將對更新文件指令資源採取執行動作。

資源 - 層次檢查:

1. 更新文件指令指出文件資源受到保護。 Billy 的文件是屬於部門 A 所擁有。因此，只會套用部門 A 與其上代組織所擁有的原則：原則 1、2、3 與 4。
2. 原則 2 授與存取權；這是因爲 Billy 是「已登錄的使用者」存取群組中的成員，而他將對文件資源執行更新文件指令動作，且他和文件存在「建立者」關係。

由於 Billy 已通過指令層次與資源層次型存取控制檢查，因此他可更新自己的文件。

實務 2：Don 想更新 Carol 的文件: 以下是此實務的存取控制評估：

指令 - 層次檢查:

1. 由於未指定商店 ID，而將指令的擁有者設爲根組織。因此，只會使用根組織所擁有的原則來評估使用者是否具備指令層次的存取權：根組織擁有原則 1 與原則 2。
2. 原則 1 授與存取權；這是因爲 Don 是「已登錄的使用者」存取群組中的成員，而他將對更新文件指令資源採取執行動作。

資源 - 層次檢查:

1. 更新文件指令指出文件資源受到保護。 Carol 的文件是屬於部門 A 所擁有。因此，只會套用部門 A 與其上代組織所擁有的原則：原則 1、2、3 與 4。
2. 原則 4 授與存取權；這是因爲 Don 是「賣方的核准者」存取群組中的成員，而他將對文件資源執行更新文件指令動作。

由於 Don 已通過指令層次與資源層次型存取控制檢查，因此他可更新 Carol 的文件。

實務 3：Abe 想更新 Emily 的文件： 以下是此實務的存取控制評估：

指令 - 層次檢查：

1. 由於未指定商店 ID，而將指令的擁有者設爲根組織。因此，只會使用根組織所擁有的原則來評估使用者是否具備指令層次的存取權：根組織擁有原則 1 與原則 2。
2. 原則 1 授與存取權；這是因爲 Abe 是「已登錄的使用者」存取群組中的成員，而他將對更新文件指令資源採取執行動作。

資源 - 層次檢查：

1. 更新文件指令指出文件資源受到保護。 Emily 的文件是屬於賣方組織所擁有。因此，只會套用賣方組織與其上代組織所擁有的原則：原則 1、2 與 3。
2. 原則 3 未授與存取權；這是因爲 Abe 不是「賣方的核准者」存取群組中的成員。

雖然 Abe 通過指令層次檢查，但因未通過資源層次型存取控制檢查，因此他無法更新 Emily 的文件。

實務 4：訪客 3 想更新自己的文件： 以下是此實務的存取控制評估：

指令 - 層次檢查：

1. 由於未指定商店 ID，而將指令的擁有者設爲根組織。因此，只會使用根組織所擁有的原則來評估使用者是否具備指令層次的存取權：根組織擁有原則 1 與原則 2。
2. 原則 1 未授與存取權；這是因爲訪客 3 不是已登錄的使用者存取群組中的成員。

資源 - 層次檢查：

1. 由於指令層次檢查失敗，而不會執行資源層次檢查。

由於訪客 3 未通過指令層次檢查，而無法更新自己的文件。

評估範本原則

本範例是以先前的實務爲基礎。

和更新文件有關的存取控制原則

在評估範本原則時，仍會套用評估標準原則時所用的存取控制原則 1 與 2，不過標準原則 3 與 4 此時將換成範本原則 5。有關原則 1 與 2 的進一步資訊，請參閱第 34 頁的『評估標準原則』。

原則 5:

[組織的核准者，更新文件動作群組，文件，-]

此原則爲一種範本資源層次型原則。擁有文件之組織的核准者可更新文件。

我們另需要一個已參數化的新存取群組，以供此範本原則使用。此實務中所新增的存取群組如下：

- 組織的核准者：此群組隱含包含在 ? 組織中擔任核准者職務的所有使用者。（當於執行時期套用範本原則時， ? 參數會動態變成原則的擁有者）。

實務

下列實務只使用原則 1、2 與 5。

實務 1：Don 想更新 Carol 的文件: 以下是此實務的存取控制評估：

指令 - 層次檢查:

1. 由於未指定商店 ID，而將指令的擁有者設爲根組織。因此，只會使用根組織所擁有的原則來評估使用者是否具備指令層次的存取權：根組織擁有原則 1 與原則 2。在評估原則期間，範本原則會將擁有權動態轉給擁有資源的組織（接著是該組織的上代），因此亦會套用原則 5。
2. 原則 1 授與存取權；這是因爲 Don 是「已登錄的使用者」存取群組中的成員，而他將對更新文件指令資源採取執行動作。

資源 - 層次檢查:

1. 更新文件指令指出文件資源受到保護。 Carol 的文件是屬於部門 A 所擁有。因此，只會套用部門 A 與其上代組織所擁有的原則：原則 1、2。在評估原則期間，範本原則會將擁有權動態轉給擁有資源的組織（接著是該組織的上代），因此亦會套用原則 5。
2. 會先將範本原則 5 套用在擁有資源的組織：部門 A。在此情況下，原則 5 的實質行爲類似原則 5a：

   [部門 A 的核准者，更新文件動作群組，文件，-]
   部門 A 所擁有的標準資源層次型原則
3. 原則 5a 未授與存取權；這是因爲 Don 不是「部門 A 的核准者」存取群組中的成員。
4. 範本原則 5 接著將套用在部門 A 的上一層組織：賣方組織。在此情況下，原則 5 的實質行爲類似原則 5b：

   [賣方的核准者，更新文件動作群組，文件，-]
   賣方所擁有的標準資源層次型原則
5. 原則 5b 授與存取權；這是因爲 Don 是「賣方的核准者」存取群組中的成員，而他將對文件資源執行更新文件指令動作。

由於 Don 已通過指令層次與資源層次型存取控制檢查，因此他可更新 Carol 的文件。

實務 2：Abe 想更新 Emily 的文件: 以下是此實務的存取控制評估：

指令 - 層次檢查:

1. 由於未指定商店 ID，而將指令的擁有者設爲根組織。因此，只會使用根組織所擁有的原則來評估使用者是否具備指令層次的存取權：根組織擁有原則 1 與原則 2。在評估原則期間，範本原則會將擁有權動態轉給擁有資源的組織（接著是該組織的上代），因此亦會套用原則 5。
2. 原則 1 授與存取權；這是因爲 Abe 是「已登錄的使用者」存取群組中的成員，而他將對更新文件指令資源採取執行動作。

資源 - 層次檢查:

1. 更新文件指令指出文件資源受到保護。Emily 的文件是屬於賣方組織所擁有。因此，只會套用賣方與其上代組織所擁有的原則：原則 1、2。 在評估原則期間，範本原則會將擁有權動態轉給擁有資源的組織（接著是該組織的上代），因此亦會套用原則 5。
2. 會先將範本原則 5 套用在擁有資源的組織：賣方組織。在此情況下，原則 5 的實質行爲類似原則 5a：

   [賣方的核准者，更新文件動作群組，文件，-]
   賣方所擁有的標準資源層次型原則
3. 原則 5a 未授與存取權；這是因爲 Abe 不是「賣方的核准者」存取群組中的成員。
4. 範本原則 5 接著將套用在賣方組織的上一層組織：根組織。在此情況下，原則 5 的實質行爲類似原則 5b：

   [根組織的核准者，更新文件動作群組，文件，-]
   根組織所擁有的標準資源層次型原則
5. 原則 5b 未授與存取權；這是因爲 Abe 不是「根組織的核准者」存取群組中的成員。
6. 根組織沒有上一層組織，因此已完成範本原則 5 的評估。

雖然 Abe 通過指令層次檢查，但因未通過資源層次型存取控制檢查，因此他無法更新 Emily 的文件。

第 2 篇 WebSphere Commerce 網站管理者的安全作業

本篇說明通常可讓 WebSphere Commerce 網站管理者執行的安全作業。

第 4 章 強化網站安全

如果要強化您的 WebSphere Commerce 網站的安全性，您可以在 WebSphere Commerce 架構管理程式中啓用下列任何特性：

- 使用登入逾時節點，登出長期處於非作用中的使用者，並要求他們重新登入系統。詳細說明請參閱第 45 頁的『啓用「登入逾時」』。
- 使用密碼無效節點，要求使用者在初次登入系統時變更密碼。詳細說明請參閱第 46 頁的『啓動「密碼無效」』。
- 使用受密碼保護的指令節點，要求使用者在進行一些會執行指定指令的要求時得輸入密碼。詳細說明請參閱第 46 頁的『啓用「受密碼保護的指令」』。
- 使用資料庫更新工具節點，更新 WebSphere Commerce 資料庫中的加密資料（像是：密碼與信用卡資訊）與商家金鑰。詳細說明請參閱第 47 頁的『更新加密資料』。
- 使用跨網站編寫 Script 的保護節點，以便在一旦使用者要求中含有不容許的屬性或字元時，即予以拒絕。詳細說明請參閱第 48 頁的『啓用「跨網站編寫 Script 的保護」』。
- 啓用存取日誌記載特性，以迅速發現任何對 WebSphere Commerce 的安全威脅。詳細說明請參閱第 51 頁的『啓用「存取日誌記載」』。

此外，您可以從 WebSphere Commerce 管理主控台中的「安全」下拉功能表啓用下列特性：

- 使用帳戶原則頁面，爲您的網站設置帳戶原則，以定義使用中的帳戶相關原則。詳細說明請參閱第 52 頁的『設置帳戶原則』。
- 使用密碼原則頁面，爲您的網站設置密碼原則，以控制使用者密碼選擇特性（只適用以 WebSphere Commerce 資料庫做使用者鑑別）。詳細說明請參閱第 53 頁的『設置密碼原則』。
- 使用帳戶鎖定原則頁面，爲您的網站設置帳戶鎖定原則，以降低危害使用者帳戶的機會（只適用以 WebSphere Commerce 資料庫做使用者鑑別）。詳細說明請參閱第 54 頁的『設置帳戶鎖定原則』。
- 使用啓動安全檢查頁面啓動安全程式，以檢查及刪除一些可能含有潛在安全暴露問題的 WebSphere Commerce 暫存檔。詳細說明請參閱第 55 頁的『啓動安全檢查』。

相關概念的進一步說明，請參閱 WebSphere Commerce 線上說明中的下列主題：

- 架構管理程式

- WebSphere Commerce 架構檔
- 管理主控台
- 安全

相關作業的進一步說明，請參閱 WebSphere Commerce 線上說明中的下列主題：

- 啓動架構管理程式
- 開啓「管理主控台」

安全特性的檢視畫面

在您使用 WebSphere Commerce 的某些安全特性前，您必須先爲商店定義相關聯的檢視畫面，才能使用該特性。以下資訊說明如何爲下列定義檢視畫面：

- 登入逾時（請參閱『登入逾時』）
- 密碼無效（請參閱第 43 頁的『密碼無效』）
- 受密碼保護的指令（請參閱第 44 頁的『受密碼保護的指令』）
- 跨網站編寫 Script 的保護（請參閱第 44 頁的『跨網站編寫 Script 的保護』）

有關建立檢視畫面以及開發商店前端的一般資訊，請參閱*商店程式開發人員手冊*。

登入逾時

如果要使用「登入逾時」安全特性，您必須爲商店定義 LoginTimeoutErrorView 與 ReLogonFormView 檢視畫面。

LoginTimeoutErrorView

如果登入逾時資訊不正確，WebSphere Commerce 會將使用者的瀏覽器重新導向到這個檢視畫面中。當發生此情況時，很可能是有人竄改了 cookie。

表 1. LoginTimeoutErrorView 屬性

ECConstants.EC_LOGIN_TIMEOUT_ERROR_MSGCODE	1	有效時間值設定錯誤。
	2	登入時間值設定錯誤。
	3	有效或登入時間值設定錯誤。

ReLogonFormView

當使用者的階段作業過期後，這個檢視畫面會顯示在使用者面前。必須提供套表給使用者，以輸入使用者的登入 ID 與密碼。「提交」按鈕會呼叫 Logon 指令。另外應有一個「取消」按鈕，以便將使用者重新導向至另一頁面（在大部份情況下，通常是商店前端頁面）。

ReLogonFormView 沒有屬性。

表 2. ReLogonFormView 套表屬性

ECUserConstants.EC_UREG_LOGONID	使用者的登入 ID。
ECUserConstants.EC_UREG_LOGONPASSWORD	使用者的登入密碼。
ECUserConstants.EC_RELOGIN_URL	當提供的憑證無效時所要顯示的 URL。在大部份情況下，會是此檢視畫面的名稱。
ECConstants.EC_STORE_ID	商店的識別碼。
ECConstants.EC_URL	當輸入的憑證是另一使用者的時所要顯示的 URL。在大部份情況下，應爲商店首頁或是商店登入頁面中所用的相同 URL。

密碼無效

如果要使用「密碼無效」安全特性，您必須爲商店定義 ChangePassword 檢視畫面。

ChangePassword

這個檢視畫面是在使用者的密碼過期時顯示。應會提供套表給使用者，以輸入現行（已過期）的密碼與新密碼。「提交」按鈕會呼叫 ResetPassword 指令。另外應有一個「取消」按鈕，以便將使用者重新導向至另一頁面（在大部份情況下，通常是商店前端頁面）。

表 3. ChangePassword 屬性

ECConstants.EC_PASSWORD_EXPIRED_FLAG	**1**	使用者的密碼已過期。必須使用此屬性，以便在這個檢視畫面和密碼變更特性所用的檢視畫面相同時加以區別。密碼變更用的檢視畫面可由使用者呼叫，且在這兩種情況中指定給這個檢視畫面的 JSP 應該一樣。 JSP 應會尋找這個屬性，以決定要顯示哪一個檢視畫面。
	null	屬性不在 URL 中。這是一般的密碼變更行爲。
ECUserConstants.EC_UREG_LOGONID	現行使用者的登入 ID。	
ECConstants.EC_LOGIN_RETURN_URL	當密碼變更成功後要將瀏覽器重新導向至哪個 URL。此 URL 會傳給 ECConstants.EC_URL 名稱下的一個動作指令。	

表 4. ChangePassword 套表屬性

ECUserConstants.EC_UREG_LOGONID	使用者的登入 ID。現行登入 ID 已傳到檢視畫面中。
ECUserConstants.EC_UREG_LOGONPASSWORDOLD	舊密碼。
ECUserConstants.EC_UREG_LOGONPASSWORD	新密碼。
ECUserConstants.EC_UREG_LOGONPASSWORDVERIFY	新密碼驗證。
ECConstants.EC_URL	當密碼變更成功後要將使用者重新導向至哪個 URL。此值已傳到檢視畫面中。

表 4. ChangePassword 套表屬性 (繼續)

ECUserConstants.EC_RELOGIN_URL	當密碼變更失敗時要將瀏覽器重新導向至哪個 URL。

受密碼保護的指令

如果要使用「受密碼保護的指令」安全特性，您必須爲商店定義 PasswordReEnterErrorView 與 PasswordReEnterFormView 檢視畫面。

PasswordReEnterErrorView

在下列情況下將會使用這個檢視畫面：

- 使用者因未能提供正確的密碼而登出。
- 鑑別失敗。

在這兩種情況下，使用者應可透過現行頁面中的鏈結繼續另一頁面。

表 5. PasswordReEnterErrorView 屬性

ECConstants.EC_PASSWORD_REREQUEST _MSGCODE	**0**	當試著鑑別使用者時發生問題。
	null	屬性不在 URL 中。使用者因提供密碼失敗而登出。

PasswordReEnterFormView

當使用者試著執行受密碼保護的指令時，即會顯示此檢視畫面。應提供套表給使用者，以輸入密碼。應有兩個密碼輸入欄位。

表 6. PasswordReEnterFormView 屬性

ECConstants.EC_PASSWORD_REREQUEST _URL	當使用套表中的「提交」按鈕時所要執行的 URL。	
ECConstants.EC_PASSWORD_REREQUEST _MSGCODE	指定要出現在使用者面前之訊息的訊息代碼：	
	1	所輸入的密碼不相符。
	2	未輸入密碼。
	3	輸入的密碼不正確。

動作：URL 會當成如下的參數傳遞：

表 7. PasswordReEnterFormView 套表屬性

ECConstants.EC_PASSWORD_REREQUEST _PASSWORD1	第一個密碼。
ECConstants.EC_PASSWORD_REREQUEST _PASSWORD2	第二個密碼。

跨網站編寫 Script 的保護

如果要使用「跨網站編寫的 Script」安全特性，您必須爲商店定義 ProhibitedAttrsErrorView、ProhibitedCharacterErrorView 與 ProhibCharEncodingErrorView 檢視畫面。

ProhibitedAttrsErrorView

當因要求中含有禁止使用的屬性而不處理時，即會在使用者面前顯示此檢視畫面。

ProhibitedCharacterErrorView

當因要求中含有禁止使用的字元而不處理時，即會在使用者面前顯示此檢視畫面。

ProhibCharEncodingErrorView

和上述 ProhibitedCharacterErrorView 相同。

啓用「登入逾時」

註: 如果要在商店中使用「登入逾時」安全特性，您必須依照第 42 頁的『登入逾時』中所述，爲商店定義 LoginTimeoutErrorView 與 ReLogonFormView 檢視畫面。

架構管理程式中的「登入逾時」節點可讓您啓用或停用登入逾時特性。當啓用此特性時，只要 WebSphere Commerce 使用者長期處於非作用中，則會將之登出系統，並要求該使用者重新登入。如果該使用者登入成功，WebSphere Commerce 會執行該使用者所提的原始要求。如果該使用者登入失敗，系統會捨棄其原始要求，而使用者仍處於登出系統的狀態。

請注意，在 WebSphere Commerce 工具方面（像是：管理主控台、WebSphere Commerce Accelerator、商店服務等），登入逾時特性不會在使用者面前顯示重新登入頁面。相反地，它會關閉瀏覽器視窗，並讓使用者重新登入該工具。因此，在這些工具中，將不會處理使用者提交的原始要求。

若要啓用此特性請：

1. 啓動架構管理程式，並按照下列所示移至您案例的「登入逾時」節點：
   WebSphere Commerce > *host_name* > 案例清單 > *instance_name* > 案例內容 > 登入逾時
2. 若要啓用登入逾時特性，請按一下**啓用**勾選框。
3. 在「值」欄位中輸入登入逾時值（以秒計）。
4. 若要將變更套用在架構管理程式上，請按一下**套用**。
5. 一旦您順利更新案例的架構後，您會收到一則訊息，指出更新成功。
6. 從 WebSphere Application Server 管理主控台中，先停止再重新啓動 WebSphere Commerce Server 案例。

請注意，登入逾時值會以毫秒計儲存在 *instance*.xml 檔中，而您輸入於架構管理程式中的值則是以秒計。

啓動「密碼無效」

註: 如果要使用「密碼無效」安全特性，您必須依照第 43 頁的『密碼無效』中所述爲商店定義 ChangePassword 檢視畫面。

架構管理程式的「密碼無效」節點可讓您啓用或停用密碼無效特性。當啓動「密碼無效」時，一旦 WebSphere Commerce 使用者密碼過期，則會要求該使用者變更密碼。在此情況下，會將該使用者重新導向至一個要求其變更密碼的頁面。使用者將無法存取網站上的任何安全頁面，直到其變更密碼爲止。若要啓用此特性請：

1. 啓動架構管理程式，並按下列所示移至您案例的「密碼無效」節點：**WebSphere Commerce > *host_name* > 案例清單 > *instance_name* > 案例內容 > 密碼無效**
2. 若要啓動「密碼無效」特性，請按一下**啓用**勾選框。
3. 若要將變更套用在架構管理程式上，請按一下**套用**。
4. 一旦您順利更新案例的架構後，您會收到一則訊息，指出更新成功。
5. 從 WebSphere Application Server 管理主控台中，先停止再重新啓動 WebSphere Commerce Server 案例。

啓用「受密碼保護的指令」

註: 如果要使用「受密碼保護的指令」安全特性，您必須依照第 44 頁的『受密碼保護的指令』中所述，爲商店定義 PasswordReEnterErrorView 與 PasswordReEnterFormView 檢視畫面。

「架構管理程式」的「受密碼保護的指令」節點可讓您啓用或停用「受密碼保護的指令」特性。當啓用此特性時， WebSphere Commerce 會要求登入 WebSphere Commerce 的已登錄使用者先輸入密碼，才會繼續處理執行指定 WebSphere Commerce 指令的要求。

注意：當您架構受密碼保護的指令時，指令選單中的某些指令可讓一般或訪客使用者執行。因此當您將這類指令架構爲以密碼保護時，會導致一般或訪客使用者無法執行這些指令。因此，在將指令架構爲以密碼保護時，應該特別留意。

若要啓用此特性請：

1. 啓動架構管理程式，並按下列所示移至您案例的「受密碼保護的指令」節點：**WebSphere Commerce > *host_name* > 案例清單 > *instance_name* > 案例內容 > 受密碼保護的指令**
2. 在「一般」標籤中：
   a. 若要啓用「受密碼保護的指令」特性，請按一下**啓用**。
   b. 在「重試」欄位中輸入重試次數。（預設的重試次數爲 3 次。）
3. 在「進階」標籤中：
   a. 從「受密碼保護的指令清單」視窗中選取您想保護的 WebSphere Commerce 指令，並按一下**新增**。您所選的指令會列在「目前受密碼保護的指令清單」視窗中。
   b. 如果您想讓任何 WebSphere Commerce 指令沒有密碼保護，請在「目前受密碼保護的指令清單」視窗中選取指令，並按一下**移除**。
4. 若要將變更套用在架構管理程式上，請按一下**套用**。
5. 一旦您順利更新案例的架構後，您會收到一則訊息，指出更新成功。
6. 從 WebSphere Application Server 管理主控台中，先停止再重新啓動 WebSphere Commerce Server 案例。

註: WebSphere Commerce 在可用指令清單中只會顯示被標爲**已鑑別**的指令，或在 `URLREG` 表格中設有 `https` 旗號的指令。

更新加密資料

架構管理程式之「資料庫」節點中的「資料庫更新工具」可讓您更新所有加密資料（例如：密碼或信用卡號碼），以及給定案例之 WebSphere Commerce 資料庫的商家金鑰。若要使用工具請：

1. 啓動架構管理程式，並按下列所示移至特定的資料庫項目： **WebSphere Commerce > *host_name* > 案例清單 > *instance_name* > 案例內容 > 資料庫 > *database_name***
2. 以滑鼠右鍵按一下 *database_name*，並選取**執行資料庫更新工具**
   - 若選取**更新此案例的所有資料庫**，則會移轉所選案例之所有資料庫的加密資料。

     400 由於 iSeries 支援單一資料庫架構，此選項不適用於 iSeries。
   - 若選取**更新所選的資料庫**，則可讓您從下拉清單中選取資料庫，以移轉特定資料庫的加密資料（預設值）。
3. 請從「動作項目」框中選取您想執行的動作，並在「參數」欄位中填入必要資訊：

動作	參數	必要動作
變更商家金鑰	舊商家金鑰	請輸入您在建立目前之 WebSphere Commerce 案例時所用的現有商家金鑰。
	新商家金鑰	請輸入您的新商家金鑰。此爲架構管理程式重新加密目前所加密的資料時所要使用的十六進位號碼（共 16 碼）。「商家金鑰」必須最少有一個英文字母字元（a 至 f）以及一個數值字元（0 至 9）。 所有的英文和數值字元必須以小寫字母輸入；您不可以在同一列中輸入相同字元超過 4 次。

4. 請按一下**確定**，針對您所選的 WebSphere Commerce 資料庫或所有的 WebSphere Commerce 資料庫，執行資料庫更新工具。
5. 一旦您順利更新案例的架構後，您會收到一則訊息，指出更新成功。
6. 從 WebSphere Application Server 管理主控台中，先停止再重新啓動 WebSphere Commerce Server 案例。

啓用「跨網站編寫 Script 的保護」

註: 如果要在商店中使用「跨網站編寫的 Script」安全特性，您必須按照第 44 頁的『跨網站編寫 Script 的保護』中所述，爲商店定義 `ProhibitedAttrsErrorView`、`ProhibitedCharacterErrorView` 與 `ProhibCharEncodingErrorView` 檢視畫面。

「架構管理程式」的「跨網站編寫 Script 的保護」節點可讓您針對案例啓用或停用「跨網站編寫 Script 的保護」。若有啓用，則當使用者要求中含有不容許的屬性或字串時，「跨網站編寫 Script 的保護」即會拒絕該要求。您可在「架構管理程式」的這個節點中指定不容許的屬性與字串。您也可以將指令排除於跨網站編寫 Script 保護之外，方法是讓該特定指令的指定屬性值中含有禁止使用的字串。依預設，會停用「跨網站編寫 Script 的保護」。

警告：「跨網站編寫 Script 的保護」是一種限制特性，這個特性會根據架構來限制指令的執行。此特性不會檢查有哪些屬性或字串已被定義爲禁止使用，因此，當您架構禁止使用的屬性或字串時，請確定禁止的屬性不是指令需要使用的屬性。同時亦請確定禁止字串值不是通常要傳遞給指令的值。請在架構這個特性時，要極度小心。

若要啓用此特性請：

1. 啓動架構管理程式，並按下列所示移至您案例的「跨網站編寫 Script 的保護」節點： **WebSphere Commerce > *host_name* > 案例清單 > *instance_name* > 案例內容 > 跨網站編寫 Script 的保護**
2. 使用「一般」標籤，按如下所示啓用「跨網站編寫 Script 的保護」特性：
   a. 按一下**啓用**。
   b. 若要新增 WebSphere Commerce 指令不容許使用的屬性，請以滑鼠右鍵按一下「禁用屬性」表格，並選取**新增列**。鍵入您不容許使用的屬性。您可以在每一列只指定一個屬性。
   c. 如果要移除「禁用屬性」表格中的屬性，請標示並以滑鼠右鍵按一下表格中內含該屬性之行，並選取**刪除列**。
   d. 若要新增 WebSphere Commerce 指令不容許使用的字串，請以滑鼠右鍵按一下「禁用字元」表格，並選取**新增列**。請新增您不容許使用的字串。每一列只能指定一個字串。
   e. 如果要移除「禁用字元」表格中的字元，請標示並以滑鼠右鍵按一下表格中內含該字元之行，並選取**刪除列**。

   附註：依預設，禁用字元欄位中會指定下列字串。這些字串最常出現在惡意攻擊跨網站的 Script 的標籤中：
   - `<SCRIPT`
   - `<SCRIPT`
   - `<%` 與 `<%`

   .
3. 使用「進階」標籤，將 WebSphere Commerce 指令排除在跨網站編寫 Script 保護之外，方法依下列方式，容許該特定指令的指定屬性值可包含被禁止的字串：
   a. 從指令清單框中選取指令。
   b. 在「例外屬性清單」視窗中鍵入容許使用禁止字元的屬性清單（以逗點隔開），並按一下**新增**。
   c. 如果要移除指令與其屬性，請從「例外指令清單」視窗中選取所要指令，並按一下**移除**。

   您也可以選取特定屬性並按一下**移除**，以移除指令中的特定屬性。
4. 若要將變更套用在架構管理程式上，請按一下**套用**。
5. 一旦您順利更新案例的架構後，您會收到一則訊息，指出更新成功。
6. 從 WebSphere Application Server 管理主控台中，先停止再重新啓動 WebSphere Commerce Server 案例。

註:

1. 當指令被排除在跨網站編寫 Script 保護之外時，指定屬性的值將會使用 HTML 符號編碼制加以編碼。舉例來說，`cmd1?user=<Thomas>` 指令會編碼成 `ascmd1?user=&#60;Thomas&#62;`
2. 當您在禁用字元欄位中指定字串時，請注意下列幾點：
   - 字元順序可能因 URL 編碼標準，而將字串轉換成單一字元。舉例來說，`<%bb` 字串將轉換成 *<X* 字串，其中 *X* 爲單一字串，其十六進位表示值爲 HEX 'bb'（十進制 187）。在此情況下，當 `<%bb` 字串置於 URL 中傳遞時，「跨網站編寫 Script 的保護」將不會攫取到該字串。
   - 如果字元順序未遵循 URL 編碼標準，可能會造成字串轉換失敗。舉例來說，`<%gg` 字串將轉換失敗，因爲 HEX 'gg' 不是有效的十六進位值表示方式。在此情況下，不論是否啓用「跨網站編寫 Script 的保護」， `<%gg` 字串將造成異常狀況，而不會對內含這類字串的 URL 要求做出回應。

範例：請注意下列範例：

- 禁用字串：`<SCRIPT, <%`

  禁用屬性：`mycomment, description`

指令	狀態
cmd1?description=Available...	拒絕
cmd2?userid=Thomas...	接受
cmd3?mycomment=<SCRIPT>...	拒絕
cmd4?password=<%...%>...	拒絕

- 如果您希望 `cmd1` 指令的 `text` 屬性中能包含禁用字串 (`<SCRIPT, <%`)，但其它屬性則不行，如 `txt` 屬性，您可以排除 `cmd1` 並指定 `text` 作爲例外屬性。

指令	狀態
cmd1?text=<SCRIPT>...	接受
cmd1?text=<%...%>...	接受
cmd1?txt=<SCRIPT>...	拒絕
cmd1?txt=<%..%>...	拒絕

啓用「存取日誌記載」

若有啓用存取日誌記載特性，則系統會記載所有傳入 WebSphere Commerce Server 中的要求，或只記載造成存取違規的要求。存取違規像是：鑑別失敗、無充分權限執行指令，或重設的密碼有違您網站中的密碼規則。若有啓用，則「存取日誌記載」可讓 WebSphere Commerce 管理者迅速識別出對 WebSphere Commerce 系統的安全威脅。

一旦發生鑑別失敗或權限失效事件，即會將下列資訊記載到存取日誌檔資料庫表格 ACCLOGMAIN 與 ACCLOGSUB 中：

- 從屬站的主電腦名稱
- 執行該指令的執行緒 ID
- 從屬站的使用者 ID
- 發生事件的時間
- 所執行的指令
- 執行該指令的商店
- 執行該作業的資源
- 存取控制的檢查結果

如果要啓用存取日誌記載特性，請執行下列步驟：

1. 啓動架構管理程式。
2. 選取**主電腦名稱** > **案例** > **Instance_List**，然後開啓**元件**資料夾。
3. 選取 **AccessLoggingEventListener**。
4. 在「一般」畫面中，勾選**啓用元件**勾選框。
5. 選取「進階」畫面，並啓用**啓動**。
6. 按一下**套用**。
7. 結束架構管理程式。
8. 重新啓動 WebSphere Application Server。

如果要變更日誌檔大小，或要決定是否記載所有的要求，您必須針對位於 WebSphere Commerce 案例子目錄中的 WebSphere Commerce 案例，手動編輯 *instance*.xml 檔：

1. 在編輯程式中開啓您案例的 *instance*.xml 檔。
2. 找出下列節點，其位於 <LogSystem>/<activitylog> 節點中：

   ```
   <accessLogging cacheSize="aa" logAllRequests="bbbbb" />
   ```

   其中：

- *aa* 爲一個整數值，用以指出在將項目寫到資料庫中前，要記載到記憶體中的項目數上限。通常數目越高，則存取日誌記載方面的效能也越高。預設值爲 32。
- *bbbbb* 可爲 `true` 或 `false`。值 `true` 表示所有傳入的要求皆要記載。值 `false` 表示僅記載存取違規。如果要避免記載過多或不必要的記載，建議您採用值 `false`。只有在您懷疑網站上有鑑別問題或安全威脅時，才使用 `true`。預設值爲 `false`。

3. 在您完成更新後，請儲存您 WebSphere Commerce 案例的 *instance*.xml 檔。
4. 重新啓動 WebSphere Application Server。

在下列範例中，存取日誌記載特性會在記憶體中保留 3 個項目，一旦超過此數目，才會將項目記載到資料庫表格中。此外，它會記載所有傳入 WebSphere Commerce Server 中的要求：

```
<accessLogging cacheSize="3" logAllRequests="true" />
```

設置帳戶原則

WebSphere Commerce 管理主控台的「帳戶原則」頁面可讓您設置一個帳戶原則。依預設，此頁面會列出所有現有的帳戶原則，包括在預設情況下 WebSphere Commerce 所提供之任何預先定義的帳戶原則。帳戶原則用來定義和帳戶有關的原則，像是：密碼與帳戶鎖定原則。在此頁面中：

- 您可以按一下**新建**，建立新帳戶原則。
- 您可以選取清單中的原則，並按一下**變更**，以變更現有帳戶原則的特性。
- 您可以選取清單中的原則，並按一下**刪除**，以刪除現有的帳戶原則。

若要建立新的帳戶原則請：

1. 開啓管理主控台。
2. 從管理主控台的「安全」下拉式功能表中，按一下**帳戶原則**。
3. 在「帳戶原則」頁面中，按一下**新建**，以建立新帳戶原則。
4. 在「名稱」欄位中輸入帳戶原則的名稱（例如 `my_account_policy`）。
5. 從「密碼原則」功能表中，選取既存的密碼原則。
6. 從「帳戶鎖定原則」功能表中，選取一個既存的帳戶鎖定原則。
7. 按一下**確定**。

一旦您建立帳戶原則後，您即可爲使用者指定原則。請注意，如果帳戶原則處於使用中（亦即，某使用者被指定到該帳戶原則），則您無法刪除該帳戶原則。

另請參閱 WebSphere Commerce 線上說明中的 ″預設鑑別原則″ 參考主題。

設置密碼原則

WebSphere Commerce 管理主控台的「密碼原則」頁面可讓您控制使用者的密碼選擇，以定義其密碼的特性，確定該密碼符合您網站的安全原則。依預設，此頁面會列出所有現有的密碼原則，包括 WebSphere Commerce 所提供之任何預先定義的密碼原則。

密碼原則用以定義密碼必須遵循的屬性。密碼原則會強制執行下列條件：

- 使用者 ID 與密碼可否相符。
- 連續字元的出現次數上限。
- 任一字元的出現次數上限。
- 密碼的有效期限上限。
- 英文字母數目下限。
- 數值字元數目下限。
- 密碼長度下限。
- 使用者的前一個密碼可否重覆使用。
- 您可以按一下**新建**，建立新密碼原則。
- 您可以選取清單中的原則，並按一下**變更**，以變更現有密碼原則的特性。
- 您可以選取清單中的密碼原則，並按一下**刪除**，以刪除現有的原則。

若要建立新的密碼原則：

1. 開啓管理主控台。
2. 從管理主控台的「安全」下拉式功能表中，按一下**密碼原則**。
3. 在「密碼原則」頁面中，按一下**新建**，以建立新密碼原則。
4. 在「名稱」欄位中輸入密碼原則的名稱（例如 `my_password_policy`）。
5. 視需要更新下列各項，以便爲購物者修改預設值的任何值：
   - **使用者 ID 與密碼可否相符**？定義使用者 ID 與密碼可否相同。請從清單中選取是或否。
   - **單一字元連續出現的次數上限**。定義密碼中字元最多可連續出現幾次。最大值是連續 2 個字元。舉例來說，當您指定值 2 時，則使用者不能輸入密碼 `aaabc`。
   - **任一字元的出現次數上限**。定義同一字元最多可在密碼中出現幾次。最小值爲一個字元出現一次。舉例來說，當您指定值 2 時，則使用者不能輸入密碼 `abcaabc`。
   - **密碼的有效期限上限**。定義密碼最久可存在幾天。最小值爲 1 天。一旦過了此期限，將會提示使用者變更密碼。

- **英文字母數目下限**。定義密碼中最少需有多少個英文字母。最小值爲 0 個英文字母。
- **數值字元數目下限**。定義密碼中最少需有多少個數值字元。最小值爲 0 個數值字元。
- **密碼長度下限**。定義密碼的最小長度（以字元計）。最小值爲 1 個字元。
- **密碼可否重覆使用**？定義使用者的前一個密碼可否重覆使用。請從清單中選取是或否。

6. 按一下**確定**。

註:

1. 如果密碼原則處於使用中（亦即，某使用者被指定有該密碼原則），則您無法刪除該密碼原則。
2. 只有在以 WebSphere Commerce 資料庫來鑑別使用者時，才會實施密碼原則。

另請參閱 WebSphere Commerce 線上說明中的 ″預設鑑別原則″ 參考主題。

設置帳戶鎖定原則

WebSphere Commerce 管理主控台的「帳戶鎖定原則」頁面可讓您針對 WebSphere Commerce 中的不同使用者職務設置帳戶鎖定原則。依預設，此頁面會列出所有現有的帳戶鎖定原則，包括 WebSphere Commerce 所提供之任何預先定義的帳戶原則。若有人對某個帳戶採取惡意動作，則帳戶鎖定原則會停用該使用者帳戶，以降低這些動作危及帳戶的機會。

帳戶鎖定原則會執行下列各項：

- 帳戶鎖定臨界值。在停用帳戶之前所能容許的無效登入嘗試次數。
- 連續登入失敗的延遲。在兩次嘗試登入失敗後，在這段期間將不容許使用者登入。在每次的連續登入失敗下，延遲會因所架構的時間延遲值（例如：10 秒）而增加。

若要設定帳戶鎖定原則請：

1. 開啓管理主控台。
2. 從管理主控台的「安全」下拉式功能表中，按一下**帳戶鎖定原則**。
3. 「帳戶鎖定原則」頁面中會列出所有現有的帳戶鎖定原則。在此頁面中：
   - 您可以按一下**新建**，建立新原則。
   - 您可以選取清單中的原則，並按一下**變更**，以變更現有原則的特性。
   - 您可以選取清單中的原則，並按一下**刪除**，以刪除現有的原則。

若要建立新的帳戶鎖定原則，請在「帳戶鎖定原則」頁面中：

1. 在「名稱」欄位中輸入帳戶鎖定原則的名稱（例如 my_policy）。
2. 在「帳戶鎖定臨界值」欄位中輸入一個帳戶鎖定臨界值。例如，輸入 6（表示嘗試 6 次）。
3. 在「等待時間」欄位中輸入一個連續登入失敗的延遲時間（以秒計）。舉例來說，輸入 10（表示 10 秒）。
4. 按一下**確定**。

註:

1. 如果帳戶鎖定原則處於使用中（亦即，某使用者被指定到該帳戶鎖定原則），則您無法將之刪除。
2. 只有在以 WebSphere Commerce 資料庫來鑑別使用者時，才會實施帳戶鎖定原則。

啓動安全檢查

400 此特性不適用於 WebSphere Commerce for iSeries。

WebSphere Commerce 管理主控台的「啓動安全檢查」頁面可讓您以手動方式啓動安全程式，以檢查及刪除一些可能潛在安全曝露問題的 WebSphere Commerce 暫存檔。通常安全檢查程式採排定工作方式執行，且預設爲每月執行一次。

如果要呼叫安全檢查程式：

1. 開啓管理主控台。
2. 從管理主控台的「安全」下拉式功能表中，按一下**安全檢查程式**。
3. 在「啓動安全檢查」頁面中按一下**啓動**。

安全檢查的結果（包括程式所採取的所有動作）會寫到「安全檢查日誌」視窗以及位於下列 log 子目錄內的 sec_check.log 檔中：

NT *drive*:\WebSphere\Commerce\instances*instance_name*\log

2000 *drive*:\Program Files\WebSphere\Commerce\instances*instance_name*\log

AIX /usr/lpp/Commerce/instances/*instance_name*/log

Solaris /opt/WebSphere/Commerce/instances/*instance_name*/log

Linux /opt/WebSphere/Commerce/instances/*instance_name*/log

Windows 在非 Windows 平台上，WebSphere Commerce 將自動設定檔案許可權，讓未獲授權的使用者無法存取敏感檔案。而在 Windows 平台上，則必須按如下所示手動設定許可權。此程序可確保只有「管理者」群組對敏感檔案具備**讀取/寫入/執行權**：

1. 在「Windows 檔案總管」中以滑鼠右鍵按一下 *drive*:\WebSphere 資料夾。
2. 按一下**內容**與**安全**。依預設， "Everyone" 群組對此資料夾擁有**全部**的許可權。
3. 按一下**新增**。
4. 會出現視窗（選取使用者、電腦...）。在此視窗中，請選取**管理者**群組。

   註: 附註：此處可能有點不明確，因爲您可能會看到**管理者**變成使用者，但您必須新增「管理者」群組，而非「管理者」使用者。

   按一下**新增**，然後按一下**確定**。
5. 在「安全」標籤中，已新增「管理者」群組中。您必須移除 "Everyone"。請選取 **Everyone**，並取消勾選「容許可繼承的許可權.... 」勾選框。
6. 在出現的「安全」視窗中按一下**移除**。

架構管理程式的「PDI 加密」欄位

在您架構 WebSphere Commerce 案例時，建議您選取「PDI 加密」勾選框。啓用「PDI 加密」欄位時，表示 ORDPAYINFO 與 ORDPAYMTHD 表格中的資訊應該加密。藉由選取這個勾選框，可以加密格式將付款資訊儲存在 WebSphere Commerce 資料庫中。

第 5 章 啓用 WebSphere Application Server 安全特性

本章說明如何在 WebSphere Application Server 中啓用安全特性。啓用 WebSphere Application Server 安全特性可避免所有 Enterprise JavaBean 元件曝露，讓外人有機會從遠端呼叫。

註: Windows AIX Solaris Linux 如果您有啓用 WebSphere Application Server 安全特性，您的機器最好能符合下列需求：

- 機器記憶體最少有 1 GB。
- 資料堆大小最少有 384 MB（以供 WebSphere Commerce 應用程式使用）。

開始之前

在您開始啓用安全特性前，您得先瞭解您要啓用安全特性的 WebSphere Application Server 是如何驗證使用者 ID。WebSphere Application Server 可使用 LDAP 或作業系統的使用者登錄來作爲 WebSphere Application Server 使用者登錄。

Windows AIX Solaris Linux 有關執行 WebSphere Application Server 安全特性所需的最新 eFix，請前往 WebSphere Commerce 網站參考最新的 WebSphere Commerce 5.4 README 文件；其網址爲：

Business

```
http://www.ibm.com/software/webservers/commerce/wc_be/lit-tech-general.html
```

Professional

```
http://www.ibm.com/software/webservers/commerce/wc_pe/lit-tech-general.html
```

使用 LDAP 使用者登錄來啓用安全特性

Windows 當您以 LDAP 作爲 WebSphere Application Server 使用者登錄時，如果要啓用 WebSphere Application Server 安全特性，請以具備管理權限的使用者登入系統，並執行下列步驟。

400 當您以 LDAP 作爲 WebSphere Application Server 使用者登錄時，如果要啓用 WebSphere Application Server 安全特性，請登入系統，並執行下列步驟。

AIX Solaris Linux 當您以 LDAP 作爲 WebSphere Application Server 使用者登錄時，如果要啓用 WebSphere Application Server 安全特性，請以 wasuser 登入系統，並執行下列步驟。

1. 啓動 WebSphere Application Server 管理伺服器，並開啓「WebSphere Application Server 管理主控台」。
2. 在「主控台」中，修改通用安全設定，方法如下：
   a. 從「主控台」功能表選取**安全中心**。
   b. 在「一般」標籤中，選取**啓用安全**。
   c. 在**鑑別**標籤中，選取「小型認證機構（LTPA）」。填妥 LTPA 設定，如果您不想使用此功能，請取消勾選**啓用單一簽入**勾選框。視您所用的目錄伺服器類型而定，按如下所示填妥 **LDAP 設定**標籤：

Windows AIX Solaris Linux 400

表 8. SecureWay 使用者

欄位名稱	定義	範例值	附註
安全伺服器 ID	使用者 ID	*user_ID*	• 不得爲 LDAP 管理者。 • 請勿使用設爲 cn=xxx 的使用者。 • 請確定此使用者的物件類別和「LDAP 進階內容」視窗之「使用者過濾程式」欄位中指定的物件類別相容。
安全伺服器密碼	使用者密碼	*password*	
目錄類型	LDAP 伺服器類型	SecureWay	
主電腦	LDAP 伺服器的主電腦名稱	*hostname.domain.com*	
埠	LDAP 伺服器所用之埠		此欄位爲選用的
基本識別名稱	要在其下進行搜尋的識別名稱	o=ibm,c=us	
連結識別名稱	搜尋時要連結目錄的識別名稱		此欄位爲選用的
連結密碼	連結識別名稱的密碼		此欄位爲選用的

Windows

表 9. Netscape 使用者

欄位名稱	定義	範例值	附註
安全伺服器 ID	使用者 ID	*user_ID*	• 不得爲 LDAP 管理者。 • 請勿使用設爲 cn=xxx 的使用者。 • 請確定此使用者的物件類別和「LDAP 進階內容」視窗之「使用者過濾程式」欄位中指定的物件類別相容。
安全伺服器密碼	使用者密碼	*password*	
目錄類型	LDAP 伺服器類型	Netscape	
主電腦	LDAP 伺服器的主電腦名稱	*hostname.domain.com*	
埠	LDAP 伺服器所用之埠		此欄位爲選用的
基本識別名稱	要在其下進行搜尋的識別名稱	o=ibm	
連結識別名稱	搜尋時要連結目錄的識別名稱		此欄位爲選用的
連結密碼	連結識別名稱的密碼		此欄位爲選用的

Windows

表 10. Domino™ 使用者

欄位名稱	定義	範例值	附註
安全伺服器 ID	簡短名稱/使用者 ID	*user_ID*	請確定此使用者的物件類別和 「LDAP 進階內容」視窗之「使用者過濾程式」欄位中指定的物件類別相容。
安全伺服器密碼	使用者密碼	*password*	
目錄類型	LDAP 伺服器類型	Domino 5.0	

表 10. Domino™ 使用者 (繼續)

欄位名稱	定義	範例值	附註
主電腦	LDAP 伺服器的主電腦名稱	*hostname.domain.com*	
埠	LDAP 伺服器所用之埠		此欄位爲選用的
基本識別名稱	要在其下進行搜尋的識別名稱		此欄位爲選用的
連結識別名稱	搜尋時要連結目錄的識別名稱		此欄位爲選用的
連結密碼	連結識別名稱的密碼		此欄位爲選用的

Windows

表 11. 作用中的目錄使用者

欄位名稱	定義	範例值	附註
安全伺服器 ID	sAMAccountName	*user_ID*	• 任何一般使用者的使用者登入名稱。 • 請勿使用設爲 cn=xxx 的使用者。 • 請確定此使用者的物件類別和「LDAP 進階內容」視窗之「使用者過濾程式」欄位中指定的物件類別相容。
安全伺服器密碼	使用者密碼	*password*	
目錄類型	LDAP 伺服器類型	作用中的目錄	
主電腦	LDAP 伺服器的主電腦名稱	*hostname.domain.com*	
埠	LDAP 伺服器所用之埠		此欄位爲選用的
基本識別名稱	要在其下進行搜尋的識別名稱	CN=users, DC=domain1, DC=domain2, DC=com	

表 11. 作用中的目錄使用者 (繼續)

欄位名稱	定義	範例值	附註
連結識別名稱	搜尋時要連結目錄的識別名稱	CN=*user_ID*, CN=users, DC=domain1, DC=domain2, DC=com	*user_ID* 值爲顯示名稱。不一定得和使用者登入名稱相同。
連結密碼	連結識別名稱的密碼	*bind_password*	應和「安全伺服器密碼」相同。

d. Windows 400 重新啓動 WebSphere Application Server 管理伺服器，然後重新開啓 WebSphere Application Server 管理主控台。

e. 在**職務映射**標籤中，選取 WCS 應用程式伺服器，並按一下**編輯映射...** 按鈕。

   1) 選取「WCSSecurity 職務」，並按一下**選取...** 按鈕。

   2) 勾選「選取使用者/群組」勾選框，並新增您在步驟（第 58 頁的2c）中所輸入的使用者 ID。

f. 按一下**完成**。

3. 關閉「管理主控台」，然後停止再重新啓動 WebSphere Application Server 管理伺服器。今後，每當您開啓「WebSphere Application Server 管理主控台」，將會提示您輸入安全伺服器 ID 與密碼。

4. 開啓 WebSphere Commerce 架構管理程式，並選取**案例 > *instance_name* > 案例內容 > 安全**，然後按一下**啓用**勾選框。將會提示您輸入您在步驟（第 58 頁的2c）中所輸入的使用者名稱與密碼。請按一下**套用**，然後結束架構管理程式。

5. 停止再重新啓動 WebSphere Application Server 管理伺服器。

使用作業系統的使用者登錄來啓用安全特性

Windows 400 如果您是以作業系統之使用者驗證特性作爲 WebSphere Application Server 使用者登錄時，如果要啓用 WebSphere Application Server 安全特性，請以具備管理權限的使用者登入，並執行下列步驟。

AIX Solaris Linux 如果要以作業系統做爲使用者登錄，WebSphere Application Server 必須當成 root 執行。請將 WebSphere Application Server 當成 root 執行，並執行下列步驟。

1. AIX Solaris Linux 以 root 登入。

2. AIX Solaris Linux 在以 root 登入後，啓動 WebSphere Application Server，然後啓動 WebSphere Application Server 管理主控台：

```
export DISPLAY=fully_qualififed_host_name:0.0
cd WAS_HOME/bin
./startupServer.sh &
./adminclient.sh remote_WAS_host_name port
```

其中 *fully_qualififed_host_name* 爲您存取 WebSphere Application Server 管理主控台 時所用的電腦名稱，*remote_WAS_host_name* 爲 WebSphere Application Server 的完整主電腦名稱， port 爲您存取 WebSphere Application Server 時所經由之埠（預設埠爲 2222）。

3. 在 WebSphere Application Server 管理主控台 中，依下列方式修改通用安全設定：
   a. 從「主控台」功能表選取**安全中心**。
   b. 在「一般」標籤中，選取**啓用安全**勾選框。
4. 選取**鑑別**標籤，並選取**本端作業系統**圓鈕。
5. 在**安全伺服器 ID** 欄位中輸入您的安全伺服器 ID。按如下所示輸入使用者名稱：

欄位名稱	範例值	附註
使用者 ID	*user_ID*	Windows 這是您用來登入且具備作業系統管理專用權的使用者 ID。如果機器隸屬於某個網域，請使用完整的使用者 ID。例如 DomainXYZ\user_id。請確定這個帳戶有存在於網域伺服器中，且爲管理者群組中的成員。 AIX Solaris Linux 爲 root 或具備 root 權限的使用者 ID。 400 iSeries 中的使用者 ID 應具備 *SECOFR 權限。
安全伺服器密碼	*password*	此爲您用以登入而具備作業系統管理專用權之使用者的密碼。

6. Windows 400 重新啓動 WebSphere Application Server 管理伺服器，然後重新開啓 WebSphere Application Server 管理主控台。
7. 在**職務映射**標籤中，選取 WC 企業應用程式，並按一下**編輯映射...** 按鈕。
   a. 選取 WCSecurityRole，並按一下**選取...** 按鈕。
   b. 選取「選取使用者/群組」勾選框，在「搜尋」欄位中輸入您在步驟 第 62 頁的5 中所用的使用者 ID，並按一下**搜尋**。從「可用的使用者/群組」清單中選取該使用者，並按一下**新增**，以將之新增到「所選的使用者/群組」清單中。然後按一下每個畫面中的**確定**，直到您結束「安全中心」爲止。
8. 開啓 WebSphere Commerce 架構管理程式並選取**案例清單 → *instance_name* → 案例內容 → 安全**，並選取**啓用安全**勾選框。選取**作業系統使用者登錄**作爲鑑別模式，然後輸入您在步驟第 62 頁的5中所輸入的使用者名稱和密碼。請按一下**套用**，然後結束架構管理程式。
9. 停止再重新啓動 WebSphere Application Server 管理伺服器。今後，每當您開啓 WebSphere Application Server 管理主控台，將會提示您輸入安全伺服器 ID 與密碼。

停用 WebSphere Commerce EJB 安全特性

WebSphere Commerce Business Edition 可讓您停用 EJB 安全特性。如果要停用 WebSphere Commerce EJB 安全特性，請執行下列步驟：

1. 啓動 WebSphere Application Server 管理主控台。
2. 按一下**主控台 → 安全中心...**，然後在**一般**標籤中取消選取**啓用安全**勾選框。
3. 開啓 WebSphere Commerce 架構管理程式，並選取**案例清單 → *instance_name* → 案例內容 → 安全**，並清除**啓用安全**勾選框。
4. 結束 WebSphere Application Server 管理主控台。
5. 停止再重新啓動 WebSphere Application Server 管理伺服器。

WebSphere Commerce 安全部署選項

WebSphere Commerce 支援各種安全部署架構。下表說明您可使用的安全部署選項。

表 12. 單一機器的安全情況

有啓用 WebSphere Application Server 安全特性。	• 以作業系統作爲 WebSphere Application Server 登錄。 • 以資料庫作爲 WebSphere Commerce 登錄。
	• 以 LDAP 作爲 WebSphere Application Server 登錄。 • 以 LDAP 作爲 WebSphere Commerce 登錄。
	• 以 LDAP 作爲 WebSphere Application Server 登錄。
停用 WebSphere Application Server 安全特性，且您的 WebSphere Commerce 網站有防火牆保護。	• 不需要 WebSphere Application Server 登錄。 • 以資料庫作爲 WebSphere Commerce 登錄。
	• 不需要 WebSphere Application Server 登錄。 • 以 LDAP 作爲 WebSphere Commerce 登錄。

表 13. 多部機器的安全情況

有啓用 WebSphere Application Server 安全特性。恆部署 LDAP。	• 以 LDAP 作爲 WebSphere Application Server 登錄。 • 以 LDAP 作爲 WebSphere Commerce 登錄。
	• 以 LDAP 作爲 WebSphere Application Server 登錄。 • 以資料庫作爲 WebSphere Commerce 登錄。 • 您需要設置 LDAP，並在 LDAP 登錄中加上一個管理項目。

表 13. 多部機器的安全情況 (繼續)

停用 WebSphere Application Server 安全特性，且您的 WebSphere Commerce 網站有防火牆保護。	• 以資料庫作爲 WebSphere Commerce 登錄。 • 不需要 WebSphere Application Server 登錄。 • 不支援單一簽入。
	• 以 LDAP 作爲 WebSphere Application Server 登錄。 • 不需要 WebSphere Application Server 登錄。

註: 如果您是在防火牆的保護下操作您的 WebSphere Commerce 網站，則可停用 WebSphere Application Server 安全特性。只有在您確定防火牆後並無惡意的應用程式執行時，才適合停用 WebSphere Application Server 安全特性。

第 6 章 階段作業管理

Web 瀏覽器和電子商務網站利用 HTTP 來通信。由於 HTTP 是無狀態的通信協定（每個指令都個別執行，不需要知道先前的任何指令），因而必須有一種方法可管理瀏覽器端和伺服器端之間的階段作業。

WebSphere Commerce 支援 Cookie 型和 URL 重新編寫這兩種階段作業管理方式。管理者可以選擇只支援 Cookie 型的階段作業管理，或同時支援 Cookie 型及 URL 重新編寫兩種階段作業管理。如果 WebSphere Commerce 只支援 Cookie 型階段作業管理，則購物者的瀏覽器必須能接受 Cookie。如果同時採用 Cookie 型和 URL 重新編寫特性，WebSphere Commerce 會先試著利用 Cookie 來管理階段作業；如果購物者的瀏覽器設定爲不接受 Cookie，則會使用 URL 重新編寫特性。

Cookie 型階段作業管理

當使用 Cookie 型階段作業管理時，Web 伺服器會傳送含有使用者資訊的訊息（Cookie) 到瀏覽器。當使用者試圖存取特定頁面時，會將這個 Cookie 送回伺服器。在送回 Cookie 之後，伺服器便能認出使用者，並從階段作業資料庫中擷取使用者的階段作業，因而能夠維護使用者的階段作業。當使用者登出或關閉瀏覽器時，Cookie 型階段作業便告結束。 Cookie 型階段作業管理不但安全，而且具有效能上的好處。 Cookie 型階段作業管理相當安全，這是因爲它採用只會行經 SSL 的識別標籤。 Cookie 型階段作業管理可提供顯著的效能優點，因爲 WebSphere Commerce 快取機制只支援 Cookie 型階段作業，而不支援 URL 重新編寫特性。建議購物者階段作業採用 Cookie 型階段作業管理。

如果您沒有使用 URL 重新編寫特性，且您想確定使用者已在他們的瀏覽器上啓用 cookie，請勾選架構管理程式之「階段作業管理」頁面上的 **Cookie 接受度測試**。這會通知購物者如果其瀏覽器不支援 Cookie，或者其停用了 Cookie，則其瀏覽器必須能支援 Cookie 才能瀏覽 WebSphere Commerce 網站。

由於安全因素，cookie 型的階段作業管理會使用兩種 cookie 類型：

- 非安全階段作業 Cookie

  用以管理階段作業資料。其中包含建構 cookie 時的階段作業 ID、協調的語言、目前的商店以及購物者偏好的貨幣。這個 Cookie 可利用瀏覽器和伺服器之間的 SSL 或非 SSL 連線來傳送。非安全階段作業 cookie 有兩種類型：

  – WebSphere Application Server 階段作業 Cookie 是以 Servlet HTTP 階段作業標準爲基礎。WebSphere Application Server cookie 會存留在記憶體中，在

多節點佈署中則存留在資料庫中。進一步資訊請搜尋 WebSphere Application Server InfoCenter（http://www.ibm.com/software/webservers/appserv/infocenter.html）中的「階段作業管理」。

– WebSphere Commerce 階段作業 Cookie 屬於 WebSphere Commerce 的內部項目，而不會留存在資料庫中。

如果要選取要使用的 cookie 類型，請在架構管理程式的「階段作業管理」頁面中，針對 **Cookie 階段作業管理程式**參數選取 WCS 或 WAS。

- 安全鑑別 Cookie

  用以管理鑑別資料。鑑別 Cookie 會串流通過 SSL 且會加上時間戳記，以達到最高的安全性。每當執行敏感的指令（例如，會要求使用者提供信用卡號碼的 DoPaymentCmd）時，即會以此 Cookie 來鑑別使用者。此 cookie 被盜取或被未鑑別使用者盜用的可能性不大。每當使用 Cookie 型的階段作業管理時，WebSphere Commerce 就會產生鑑別碼 Cookie。

如果要檢視安全頁面，則必須同時用到階段作業和鑑別程式碼 Cookie。

若發生 Cookie 錯誤，即會在下列情況下呼叫 CookieErrorView：

- 使用者從另一個位置使用相同的登入 ID 登入。
- Cookie 已損壞或被擅改過，或兩者皆是。
- 如果 Cookie 接受設爲 ″true″ 但使用者的瀏覽器不支援 cookie。

使用 cookie 進行階段作業管理

如果要在 WebSphere Commerce 中使用 Cookie，請執行下列步驟：

1. 開啓架構管理程式。
2. 選取**案例**，再開啓**階段作業管理**資料夾。
3. 選取適當的階段作業值。
   - Cookie 接受度測試

     請選取這個勾選框，檢查客戶的瀏覽器對於只支援 Cookies 的網站，接不接受其 Cookies。

   - Cookie 階段作業管理程式

     選取是否要由 WebSphere Commerce 或 WebSphere Application Server 來管理 Cookie。預設值爲 WebSphere Commerce。

     – WebSphere Application Server 階段作業 Cookie 是以 Servlet HTTP 階段作業標準爲基礎。WebSphere Application Server cookie 會存留在記憶體中，在多節點佈署中則存留在資料庫中。進一步資訊請搜尋 WebSphere

Application Server InfoCenter
（http://www.ibm.com/software/webservers/appserv/infocenter.html）
中的「階段作業管理」。

– WebSphere Commerce 階段作業 Cookie 屬於 WebSphere Commerce 的內部項目，而不會留存在資料庫中。

4. 按一下**進階**標籤。選取適當的階段作業值。
   - Cookie 路徑

     這個欄位通常不應改變。指定 Cookie 的路徑，它是 Cookie 所應傳送之 URL 的子集。
   - Cookie 有效期

     此欄位不應改變。Cookie 的預設值是在瀏覽器關閉時到期。
   - Cookie 網域

     這個欄位通常不應改變。指定網域限制型樣。網域是指定應該看到 Cookie 的伺服器。依預設， Cookie 只會傳回給當初發出它們的 WebSphere Commerce Server。在預設的情況下，Cookies 只會傳回儲存它們的主電腦。指定網域名稱型樣會取代它。型樣必須起始於一點，且必須包含至少兩點。型樣只對應第一點之後的一個項目。舉例來說，".ibm.com" 爲有效的，且和 a.ibm.com 與 b.ibm.com 吻合，但不同於 www.a.ibm.com。如果需要領域型樣的詳細資料，請參閱 Netscape 的 Cookie 規格和 RFC 2109。
5. 按一下**套用**。
6. 關閉架構管理程式。
7. 從 WebSphere Application Server 管理主控台中，先停止再重新啓動案例。

URL 重新編寫

當使用 URL 重新編寫時，所有傳回瀏覽器或重新導向的鏈結都會附加一個階段作業 ID。當使用者按一下這些鏈結時，從屬站要求會將 URL 重新編寫的形式傳送到伺服器中。 Servlet 引擎會辨識 URL 中的階段作業 ID，並將它儲存起來，以取得這位使用者的適當物件。如果要使用 URL 重新編寫，鏈結不能使用 HTML 檔（副檔名爲 .html 或 .htm 的檔案）。如果要使用 URL 重新編寫，必須使用 JSP 檔作爲顯示之用。當購物者登出時，以 URL 重新編寫的階段作業即屬過期。

註: WebSphere Commerce 快取與 URL 重新編寫不能交互運作。如果您啓用 URL 重新編寫，則必須停用 WebSphere Commerce 快取元件。

使用 URL 重新編寫階段作業管理

如果要指定應該如何管理階段作業，請執行下列動作：

1. 開啓「架構管理程式」。
2. 選取**案例**，再開啓**階段作業管理**資料夾。
3. 選取適當的階段作業值。

   啓用 URL 重新編寫。選取這個勾選框時，則會在階段作業管理中使用 URL 重寫特性。

   Cookie 階段作業管理程式。選取 WebSphere Application Server。
4. 按一下**套用**。
5. 關閉架構管理程式。
6. 從 WebSphere Application Server 管理主控台中，先停止再重新啓動案例。

撰寫 JSP 範本以進行 URL 重新編寫

如果您要利用 URL 重新編寫特性來維護階段作業狀態，請勿在純 HTML 檔中，將鏈結併入 Web 應用程式的部份。這是一項必要的限制，因爲在純文字 HTML 檔中不能使用 URL 編碼。如果要使用 URL 重新編寫特性來維護狀態，使用者在階段作業期間要求的每個頁面都必須有 Java 直譯器所能瞭解的程式碼。如果您的 Web 應用程式和網站中使用者有可能在階段作業期間存取的部份中有這些純 HTML 檔，請將它們轉換成 JSP 檔。這會影響應用程式寫出器，因爲利用 URL 重新編寫特性來維護階段作業不同於利用 Cookie 來維護階段作業，它要求應用程式中每個 JSP 範本在 <A> 標籤的每個 HREF 屬性上，都採用 URL 編碼。如果應用程式中有一或多個 JSP 範本沒有呼叫 encodeURL(String url) 或 encodeRedirectURL(String url) 方法，便可能會遺失階段作業。

撰寫鏈結

當使用 URL 重新編寫時，所有傳回瀏覽器或重新導向的鏈結都必須附加一個階段作業 ID 給它們。舉例來說，在網頁中將下列鏈結：

```
<a href="store/catalog">
```

重新編寫成：

```
<a href="store/catalog;$jsessionid$DA32242SSGE2">
```

當使用者按一下這個鏈結時，從屬站要求會將 URL 重新編寫的形式傳送到伺服器中。Servlet 引擎會將 ;$jsessionid$DA32242SSGE2 視爲階段作業 ID 並加以儲存，以便取得此使用者的適當 HttpSession 物件。

下列範例說明如何在 JSP 檔中內嵌 Java 程式碼：

```
<%
 response.encodeURL ("/store/catalog");
%>
```

如果要重新編寫您要傳回給瀏覽器的 URL，請在 JSP 範本中呼叫 encodeURL() 方法，再將 URL 傳到輸出串流。舉例來說，下列 JSP 範本（沒有使用 URL 重新編寫特性）含有：

```
out.println("<a href=\"/store/catalog\">catalog</a>")"
```

將之換成：

```
out.println("<a href=\"");
out.println(response.encodeURL ("/store/catalog"));
out.println("\">catalog</a>");
```

如果要重新編寫您要重新導向的 URL，請呼叫 encodeRedirctURL() 方法。比方說，如果您的 JSP 範本有：

```
response.sendRedirect (response.encodeRedirectURL ("http://myhost/store/catalog"));
```

encodeURL() 與 encodeRedirectURL() 方法爲 HttpServletResponse 物件的一部份。在這兩種情況下，這些呼叫都會在進行 URL 編碼之前，檢查有沒有配置好 URL 重新編寫。如果沒有配置的話，它會傳回原來的 URL。

撰寫套表: 如果要撰寫套表並提交，請在套表範本的 ACTION 標籤中呼叫 response.encodeURL("Logon");。例如：

```
String strLoginPost = response.encodeURL("Logon");
<FORM NAME="Logon" METHOD="post" ACTION= <%= strLoginPost %> >
...
</FORM>
```

編寫第一頁: 入口頁（通常是首頁）無法含有頁框。如果您想在商店中使用頁框，您可以一個無頁框的頁面作爲商店的入口頁，且讓其中內含一條通往商店的鏈結。不過，假設商店有使用頁框，而有客戶未先經由入口頁，而逕自透過頁框來存取這些頁面，則可能會遺失其階段作業。如果客戶使用**上一步**按鈕（只含頁框）回到入口頁並重新整理入口頁，客戶同樣會遺失其階段作業。當重新整理入口頁時，會給予客戶一個新的階段作業 ID。因此您必須使用可回到入口頁的鏈結，來取代**上一步**按鈕，以免發生此種階段作業遺失型態。

第 3 篇 系統管理者的安全作業

本篇說明通常可讓您網站上之系統管理者（而不一定得是 WebSphere Commerce 網站管理者）執行的安全作業。

第 7 章 設定與變更密碼

WebSphere Commerce 中的大部份元件都使用經過作業系統查核的使用者 ID 與密碼。有關變更這些密碼的資訊，請參閱您的作業系統文件。本章說明如何針對不是透過作業系統來查核使用者 ID 與密碼的 WebSphere Commerce 元件，設定與變更密碼。

使用者 ID、密碼與網址的簡要說明

WebSphere Commerce 環境管理需要使用多個使用者 ID。以下說明這些使用者 ID 及其必備權限。對於 WebSphere Commerce 使用者 ID，其預設密碼會在下面提供。

Windows 使用者 ID

您的 Windows 使用者 ID *必須*具有管理者權限。如果您使用 DB2®，則使用者 ID 與密碼必須遵循下列規則：

- 長度不能超過 8 個字元。
- 只能包含字元 A 到 Z、a 到 z、0 到 9、@、#、$ 和 _。
- 不能以底線（_）爲開頭。
- 使用者 ID 不論是大小寫，或以大小寫混合組成，均不能爲下列各項：USERS、ADMINS、GUESTS、PUBLIC、LOCAL。
- 使用者 ID 不論是大小寫，或以大小寫混合組成，均不能以下列各項做爲開頭： IBM、SQL、SYS。
- 使用者 ID 不能和任何 Windows 服務程式名稱相同。
- 使用者 ID 必須定義在本端機器中，且隸屬於本端管理者的群組。
- 使用者 ID *必須爲部份作業系統*的進階使用者權限。

您可在未具有*作爲作業系統的一部份*的進階使用者權限下進行安裝，不過，DB2 安裝程式將無法驗證您指定的管理伺服器帳戶是否正確。建議您安裝 DB2 時所用的任何使用者帳戶皆具備此種進階使用者權限。

重要事項

如果您的 Windows 使用者 ID *沒有*管理者權限，或長度超過 8 個字元，或者未定義在本端機器中，您將會收到發生問題的通知，且無法繼續進行安裝。

如果您使用 DB2，您將以這個使用者 ID 做爲 DB2 資料庫使用者名稱（資料庫使用者登入 ID）。

如果您需要建立符合上述準則的使用者 ID，您可以在 Windows 的線上說明中，尋找有關如何建立 Windows 使用者 ID 的資訊。

iSeries 使用者設定檔 400

在您安裝與架構 WebSphere Commerce 時，經常會用到與提到下列兩個 iSeries 使用者設定檔：

- 一個是您所建立的使用者設定檔；這個使用者設定檔用以安裝 WebSphere Commerce，且會存取架構管理程式。如果要安裝與架構 WebSphere Commerce，您必須使用 iSeries 的 USRCLS(*SECOFR) 使用者設定檔或使用 QSECOFR 使用者設定檔。如果您需要建立使用者設定檔，請參閱 iSeries 版的 *WebSphere Commerce 5.4 安裝手冊*。
- 另一個使用者設定檔是您在建立 WebSphere Commerce 案例時由「架構管理程式」所建。這個使用者設定檔亦稱爲 "案例使用者設定檔"。每當您建立 WebSphere Commerce 案例時，「架構管理程式」即會建立 USRCLS(*USER) 使用者設定檔。如果您需要建立使用者設定檔，請參閱 iSeries 版的 *WebSphere Commerce 5.4 安裝手冊*。

架構管理程式的使用者 ID

架構管理程式工具的圖形式介面，可讓您修改 WebSphere Commerce 的架構方式。預設的架構管理程式使用者 ID 和密碼爲 `webadmin` 與 `webibm`。

Windows AIX Solaris Linux 您可從 WebSphere Commerce 機器或從和 WebSphere Commerce 相同網路中的任何機器來存取架構管理程式。

400 在 iSeries方面，您可從位於和您 iSeries 伺服器相同的 Windows 機器中來存取架構管理程式。

IBM HTTP Server 使用者 ID Windows AIX Solaris Linux

如果您使用 IBM HTTP Server，您可以開啓 Web 瀏覽器，然後鍵入以下網址來存取 Web 伺服器的首頁：

http://*host_name*

如果您有自訂過 Web 伺服器，您可能需要在主電腦名稱之後加上您的 Web 伺服器首頁名稱。

WebSphere Commerce 案例管理者

「案例管理者」的使用者 ID 和密碼適用於下列 WebSphere Commerce 工具：

- WebSphere Commerce Accelerator. 如果要從執行 Windows 作業系統的遠端機器來存取 WebSphere Commerce Accelerator，請開啓您的 Internet Explorer Web 瀏覽器，並輸入下列網址：

  https://*host_name*:8000/accelerator

- WebSphere Commerce 管理主控台. 如果要從執行 Windows 作業系統的遠端機器來存取 WebSphere Commerce 管理主控台，請開啓您的 Internet Explorer Web 瀏覽器，並輸入下列網址：

  https://*host_name*:8000/adminconsole

- 商店服務。您可以開啓 Web 瀏覽器並且鍵入以下的網址來存取您的「商店服務」頁面：

  https://*host_name*:8000/storeservices

預設案例管理者使用者 ID 爲 wcsadmin，預設密碼爲 wcsadmin。

註: wcsadmin 使用者 ID 絕不可以移除，而且恆具有案例管理者權限。WebSphere Commerce 會要求您所用的使用者 ID 和密碼必須遵循下列規則：

- 密碼長度至少有 8 個字元。
- 密碼中必須至少含有一個數值。
- 密碼中同一個字元不能出現超過 4 次。
- 密碼中同一個字元不同連著出現 3 次。

Payment Manager 管理者

當您安裝 Payment Manager 時，WebSphere Commerce 管理者 ID wcsadmin 會自動具有 Payment Manager 管理者職務。按 *WebSphere Commerce 5.4 安裝手冊中的指示，將 Payment Manager 領域類別切換爲 WCSRealm（如果尚未如此做的話）*。

Payment Manager 管理者職務可讓使用者 ID 控制和管理 Payment Manager。

附註： 400

- 請勿刪除登入使用者 ID wcsadmin 或重新命名，也不要變更 wcsadmin 預先指定的 Payment Manager 職務，這是因爲如此會導致和 Payment Manager 整合有關的 WebSphere Commerce 功能無法運作。
- 如果您指定 Payment Manager 職務給某位 WebSphere Commerce 管理者，且在稍後要刪除此管理者的登入使用者 ID 或重新命名，您必須在將其刪除或重新命名該使用者 ID 前，先移除此管理者的 Payment Manager 職務。

重要事項

Payment Manager 已經將 Payment Manager 「管理者」職務預先指定給其他兩個管理 ID：

- ncadmin
- admin

如果要防止使用者無意間取得此項 Payment Manager 管理者職務，您可以：

1. 使用「WebSphere Commerce 管理主控台」，在 WebSphere Commerce 中建立上述管理 ID。
2. 在「Payment Manager 使用者介面」中，選取**使用者**。
3. 移除這兩個管理 ID 的 Payment Manager 管理者職務。

您應該記住 Payment Manager 案例密碼，因爲您需要這個密碼才能啓動、停止或刪除 Payment Manager 案例。您也需要這個密碼，才能新增卡匣到 Payment Manager 案例中。如果 Payment Manager 案例是由 WebSphere Commerce 架構管理程式所建立， Payment Manager 案例密碼和 WebSphere Commerce 案例登入密碼就是一樣的，後者也叫做案例使用者設定檔密碼。如果 Payment Manager 案例是使用 **CRTPYMMGR** 指令從 iSeries 階段作業建立，或是從 iSeries「作業頁面」建立，系統會提示您提供密碼。

變更架構管理程式密碼

當您啓動架構管理程式後，您可以變更架構管理程式密碼；方法是在您輸入使用者 ID 和密碼的視窗中按一下**修改**。

Windows AIX Solaris Linux 另外一種變更架構管理程式使用者 ID 或密碼的方法，是切換到 WebSphere Commerce 安裝路徑下的 bin 子目錄，並在指令視窗中鍵入下列指令：

```
config_env
java com.ibm.commerce.config.server.PasswordChecker -action [action type]
   -pwfile [password file] -userid [user ID]
   -password [userid password] [-newpassword [new userid password]]
```

其中 action type 是 Add、Check、Delete 或 Modify。這些參數的說明如下：

pwfile
將儲存密碼之檔案的路徑。預設路徑爲 WebSphere Commerce 安裝路徑下的 bin 子目錄。此參數是必要的。

userid
輸入您要新增、檢查、刪除或修改的使用者 ID。此參數是必要的。

password
輸入您要建立、檢查、刪除或修改的密碼。此參數必須和 userid 參數一起使用。此參數是必要的。

newpassword
使用此參數來變更特定使用者 ID 的密碼。此參數必須和 userid與 password 參數一起使用。當您指定動作類型 Modify 時，需指定此參數。

設定 IBM HTTP Server 管理者密碼

Windows AIX Solaris Linux 如果要設定 IBM HTTP Server 管理者密碼，

1. 切換至您機器上的 IBM HTTP Server 安裝目錄。
2. 鍵入以下指令：

   Windows `htpasswd -b conf\admin.passwd user password`

   AIX Solaris Linux `htpasswd -b conf/admin.passwd user password` 其中 *user* 和 *password* 是指您希望有 IBM HTTP Server 管理權限的使用者 ID 和密碼。

現在您已成功設定 IBM HTTP Server 管理密碼。

變更 SSL 金鑰檔密碼

Windows AIX Solaris Linux 如果您使用 IBM HTTP Server，請依照下列步驟來變更您的 SSL 金鑰檔密碼。

1. Windows 按一下**「開始」功能表 → 程式集 → IBM HTTP Server → 金鑰管理公用程式**。

2. 從**金鑰資料庫檔**功能表中選取**開啓**。
3. 切換至您機器上之 IBM HTTP Server 安裝路徑下的 ssl 子目錄。金鑰檔（副檔名爲 .kdb）應位於此資料夾中。若非如此，請依照第 83 頁的第 8 章, 『使用 IBM HTTP Server 啓用正式作業的 SSL』中的指示建立新的金鑰檔。
4. 從**金鑰資料庫檔**功能表中選取**變更密碼**。會出現「變更密碼」視窗。
5. 輸入新密碼，並啓用**將密碼隱藏在檔案中**。
6. 按一下**確定**。您的密碼應已變更。

現在您已順利變更 SSL 金鑰檔管理密碼。

產生 WebSphere Commerce 加密密碼

Windows AIX Solaris Linux WebSphere Commerce 可讓您產生加密密碼。如果要產生加密密碼，請執行下列步驟：

1. 移至 WebSphere Commerce 安裝目錄下的 bin 子目錄。
2. 從指令行執行以下的 Script：

   Windows `wcs_password.bat password SALT merchant_key`

   AIX Solaris Linux `./wcs_password.sh password SALT merchant_key` 其中

   - *password* 爲純文字的密碼。
   - *SALT* 爲一個隨機字串，用來產生密碼。您可在要更新其密碼之特定使用者的 USERREG 資料庫表格的 SALT 直欄中找到。
   - *merchant_key* 爲您在建立案例期間所輸入的商家金鑰。

400 在 iSeries 方面，如果要變更購物者的加密密碼，請使用 CHGWCSPWD 指令。有關執行此指令的詳述，請參閱 F1 線上說明。

產生 Payment Manager 加密密碼

WebSphere Commerce 可讓您產生 Payment Manager 的加密密碼。如果要產生加密密碼，請執行下列步驟：

1. 移至 WebSphere Commerce 安裝目錄下的 bin 子目錄。
2. 從指令行執行以下的 Script：

   Windows `wcs_pmpassword.bat password SALT`

   AIX Solaris Linux `./wcs_pmpassword.sh password SALT`

   其中：

   - *password* 爲純文字的密碼。

- *SALT* 爲一個隨機字串，用來產生密碼。您可在要更新其密碼之特定使用者的 USERREG 資料庫表格的 SALT 直欄中找到。

400 在 iSeries 方面，如果要產生 Payment Manager 的加密密碼，請使用 CRTWCSPMPW 指令。有關執行此指令的詳述，請參閱 F1 線上說明。

第 8 章 使用 IBM HTTP Server 啓用正式作業的 SSL

400 本節不適用於 iSeries 平台。有關 iSeries 資訊，請參閱第 87 頁的『在 IBM HTTP Server (iSeries) 中啓用 SSL』。

在您建立使用 IBM HTTP Server 的 WebSphere Commerce 案例後，即會啓用「安全 Sockets 層次 (SSL)」以供測試用。在您向購物者開放網站之前，您必須遵循本章的步驟，啓用正式作業 SSL。

關於安全特性

IBM HTTP Server 使用加密技術，爲您的商務交易提供安全的環境。加密是將網際網路上的資訊交易亂數化，使其在接收者解除亂數化之前無法閱讀。傳送者使用一種運算型樣或金鑰將交易亂數化（加密），接收者則使用解密金鑰。這些金鑰是供安全 Socket 層次（SSL）通信協定使用。

您的 Web 伺服器會使用一套鑑別程序，來驗證和您進行商務者的身份（亦即確定他們的身份）。此動作需要取得由具公信力的第三者（稱爲憑證管理中心，CA）簽發的憑證。對於 IBM HTTP Server 的使用者而言，憑證管理中心可以是 Equifax® 或 VeriSign® Inc.。此外也有其它適用的憑證管理中心。

如果要建立正式金鑰檔時，您必須完成下列步驟：

1. 建立正式安全金鑰檔。
2. 向憑證管理中心申請安全憑證。
3. 將您的正式金鑰檔設爲目前的金鑰檔。
4. 接收憑證，並測試正式金鑰檔。

這些步驟的詳細說明如下。

註:

1. 如果您已在使用憑證管理中心簽發的正式金鑰檔，可略過這些步驟。請在閱讀本章後判斷是否可以略過。
2. 當您在執行這些步驟時，您的瀏覽器可能會顯示有關安全方面的訊息。請仔細檢視每一則訊息中的資訊，然後決定如何繼續進行下一步。

建立正式用的安全金鑰檔

如果要建立正式安全金鑰檔，請在 Web 伺服器機器上執行下列步驟：

1. 停止 IBM HTTP Server。
2. 在您的機器中將目錄切換至 IBM HTTP Server 安裝子目錄下的 conf 子目錄。
3. 建立一份 httpd.conf 備份。
4. 在文字編輯器中開啓 httpd.conf。
5. 請確定埠 443 的下列各行已取消註解：

   - Windows

     ```
     #LoadModule ibm_ssl_module modules/IBMModuleSSL128.dll
     #Listen 443#Listen 443#<VirtualHost host.some_domain.com:443>
     #SSLEnable
     #</VirtualHost>
     #SSLDisableKeyfile "drive:/WebSphere/HTTPServer/ssl/keyfile.kdb"
     #SSLV2Timeout 100
     #</VirtualHost>
     #SSLDisable
     ```

   - AIX Solaris Linux

     ```
     #LoadModule ibm_ssl_module modules/IBMModuleSSL128.dll
     #AddModule mod_ibm_ssl.c
     #Listen 443#<VirtualHost host.some_domain.com:443>
     #SSLEnable
     #</VirtualHost>
     #SSLDisableKeyfile "keyfile"
     #SSLV2Timeout 100
     #</VirtualHost>
     #SSLDisable
     ```

     其中 *keyfile* 爲下列之一：

     AIX /usr/HTTPServer/ssl/keyfile.kdb

     Solaris /opt/IBMHTTPD/ssl/keyfile.kdb

     Linux /opt/IBMHTTPServer/ssl/keyfile.kdb

6. 請確定埠 8000 的下列各行已取消註解：
   a. #Listen 8000
   b. #<VirtualHost host.some_domain.com:8000>。在此行中，您也必須換成您完整的主電腦名稱。
   c. #SSLEnable
   d. #</VirtualHost>

註: 建議您使用防火牆軟體來防堵外來存取您架構給 WebSphere Commerce 工具之埠（預設埠爲 8000）。相關做法請參閱您網站所用之防火牆軟體的文件。

7. 儲存變更。
8. 爲了確定您 `httpd.conf` 檔中沒有語法錯誤，請在機器上切換至 IBM HTTP Server 安裝目錄下的 `bin` 子目錄，然後執行下列指令：

   AIX Solaris Linux `./apachectl configtest`

   Windows `apachectl configtest`
9. 啓動 IBM HTTP Server。

向憑證管理中心申請安全憑證

如果要驗證您在上一步驟中建立的安全金鑰檔，您需要向憑證管理中心（CA）（像是 Equifax 或 VeriSign）取得憑證。憑證包含伺服器的公開金鑰、伺服器憑證的相關識別名稱，以及憑證的序號和有效期限。

如果您要使用其它的憑證管理中心，請直接聯絡他們以瞭解申請程序。

Equifax 使用者

如果要向 Equifax 取得安全伺服器憑證時，請參考下列網址，並依照提供的指示進行：

`http://www.equifax.com`

您應會在 2 到 4 個工作天內，經由電子郵件收到 Equifax 的安全伺服器憑證。

VeriSign 使用者

如果要向 VeriSign 取得安全伺服器憑證時，請參考下列 URL，並依照提供的指示進行：

`http://www.verisign.com`

AIX 雖然您是針對 IBM HTTP Server 執行這些程序，請循著 **Internet Connection Secure Server** (ICSS) 鏈結進行。請依照提供的指示進行。 當您收到憑證時，請依照上一節的說明，建立正式金鑰檔（如果您尚未建立的話）。

Solaris 雖然您是針對 IBM HTTP Server 執行這些程序，請遵循 **Internet Connection Secure Server** (ICSS) 的鏈結進行。後續頁次會指出這些程序適用於 OS/2® 與 AIX 平台。這些指示亦適用於 Solaris 軟體。

請依照提供的指示進行。 在您提交要求後，您應會在三到五個工作天內收到您的憑證。當您收到時，請依照上一節的說明，建立正式金鑰檔（如果您還尚未建立的話）。

接收正式金鑰檔並設為現行金鑰檔

在您收到憑證管理中心的憑證後，您必須讓 Web 伺服器使用您的正式金鑰檔。請執行下列步驟：

1. 將您從憑證管理中心收到的 *certificatename*.kdb、 *certificatename*.rdb 與 *certificatename*.sth 檔，複製到您機器上之 IBM HTTP Server 安裝路徑下的 ssl 子目錄中；其中 *certificatename* 爲您在憑證申請中提供的憑證名稱。
2. 開啓金鑰管理公用程式。
3. 開啓 *certificatename*.kdb 檔，並在出現提示時輸入密碼。
4. 選取**個人憑證**並按一下**接收**。
5. 按一下**瀏覽**。
6. 選取您收到憑證管理中心的檔案後用以儲存這些檔案的資料夾。選取 *certificatename*.txt 檔，並按一下**確定**。
7. 此時，**個人憑證**清單框中應會列出 VeriSign *certificatename* 憑證或 Equifax *certificatename* 憑證。
8. 結束金鑰管理公用程式。
9. 在您的機器中將目錄切換至 IBM HTTP Server 安裝路徑下的 conf 子目錄。
10. 建立一份 httpd.conf 備份。
11. 在文字編輯器中開啓 httpd.conf。
12. 確定您在步驟（第 84 頁的5）中列出之行未加上備註。
13. 找出 Keyfile "*keyfile path name*" 控制指令，然後變更路徑名稱而指向您在上述步驟中所建立的檔案。
14. 停止並重新啓動 IBM HTTP Server。

測試正式金鑰檔

如果要測試正式金鑰，請執行下列步驟：

1. 使用您的瀏覽器前往下列 URL：

   https://*host_name*

   註:

   a. 如果您已自訂了您的 Web 伺服器，您可能需要在主電腦名稱後鍵入 Web 伺服器的首頁名稱。

b. 確定您所鍵入的是 https，而不是 http。

如果您的金鑰定義正確，您將會看到數個關於您新憑證的訊息。

2. 如果您要接受此憑證，請在**新網站憑證**畫面中選取**永遠接受此憑證（直到過期為止）**圓鈕。
3. 在您的 Web 瀏覽器中，將您的快取和 Proxy（或 socks）伺服器設定值回復成其原始狀態。

現在您已在您的伺服器中啓用了 SSL。

Payment Manager 的 SSL 注意事項

依預設，WebSphere Commerce 與 Payment Manager 間的通信會經由 SSL。不過，如果您是按如下直接啓動 Payment Manager 使用者介面：

http://*host_name*/webapp/Paymentmanager/

則您是使用非 SSL 通信方式來呼叫 Payment Manager 。爲了確保會經由 SSL 通信，您應使用

https://*host_name*/webapp/Paymentmanager/

或在下列目錄中將 indexSSL.html 檔更名爲 index.html：

- Windows *WAS_HOME*\installedApps\IBM_PaymentManager.ear\PaymentManager.war
- AIX Solaris

Linux *WAS_HOME*/installedApps/IBM_PaymentManager.ear/PaymentManager.war

此方法可讓您繼續使用 **http://***host_name*/webapp/Paymentmanager/ 目錄，且更名後的 index.html 將重新導向至 https (SSL)。

在 IBM HTTP Server (iSeries) 中啓用 SSL

400 本節適用於 iSeries 平台。

SSL 爲一種安全通信協定。SSL 可確保在從屬站與伺服器間傳輸的資料保有私密性。它可讓從屬站鑑別伺服器的身份，以及讓伺服器鑑別從屬站的身份。

數位式憑證爲一種電子文件，用以鑑別網際網路中涉及安全交易的伺服器與從屬站。數位式憑證的發卡機構稱爲「憑證管理中心 (CA)」。在企業內部網路環境中，iSeries 系統可扮演 CA 角色負責發出伺服器與從屬站憑證，並扮演以 iSeries CA 或網際網路 CA（像是 VeriSign®）所發憑證鑑別過的伺服器角色。 作爲 Web 伺服器的 IBM HTTP Server for iSeries 也可以架構成會要求出示從屬站憑證，以鑑別啓用 SSL 功能的從屬站。

有關如何在 IBM HTTP Server for iSeries 上啓用 SSL 的詳細資訊，請見下列網址：

```
www.ibm.com/software/webservers/commerce/servers/lit-tech-os400.html
```

尤其是請查看**提示與秘訣**區段。

Payment Manager 搭配 SSL 一起使用

如果您在建立 WebSphere Commerce 案例後建立系統憑證商店，您必須同時授與 Payment Manager 案例與 WebSphere Commerce 案例對系統憑證商店的存取權。舉例來說，下列指令將授與 Payment Manager 案例對 V5R1 系統的必要存取權：

```
CHGAUT OBJ('/QIBM/UserData/ICSS/Cert/Server') USER(QPYMSVR) DTAAUT(*RX)
CHGAUT OBJ('/QIBM/UserData/ICSS/Cert/Server/DEFAULT.KDB') USER(QPYMSVR) DTAAUT(*R)
```

下列指令將授與 WebSphere Commerce 對 V5R1 系統的必要存取權：

```
CHGAUT OBJ('/QIBM/UserData/ICSS/Cert/Server') USER(QEJBSVR) DTAAUT(*RX)
CHGAUT OBJ('/QIBM/UserData/ICSS/Cert/Server/DEFAULT.KDB') USER(QEJBSVR) DTAAUT(*R)
```

如果您選擇要使用 Payment Manager 案例，您必須同時將 WebSphere Commerce 案例與 Payment Manager 案例架構成信任發出數位憑證的遠端憑證管理中心。若要建立兩個遠端應用程式間的信任關係，請參考下列的高階程序：

1. 在 WebSphere Commerce 機器上，使用「數位憑證管理程式」匯出伺服器的憑證管理中心。
2. 將憑證檔轉送到 Payment Manager 機器上。
3. 在 Payment Manager 機器上，使用「數位憑證管理程式」來匯入 WebSphere Commerce Server 的憑證管理中心。
4. 將 Payment Manager 應用程式伺服器架構成信任所匯入的 WebSphere Commerce Server 憑證管理中心。
5. 在 Payment Manager 機器上，使用「數位憑證管理程式」匯出伺服器的憑證管理中心。
6. 將憑證檔轉送到 WebSphere Commerce 機器上。
7. 在 WebSphere Commerce 機器上，使用「數位憑證管理程式」匯入 Payment Manager 伺服器的憑證管理中心。
8. 將 WebSphere Commerce 應用程式伺服器架構成信任所匯入之 Payment Manager 伺服器的憑證管理中心。

詳細資訊請參閱下列網址，並查看**提示與秘訣**：

```
www.ibm.com/software/webservers/commerce/servers/lit-tech-os400.html
```

第 9 章 在 IBM SecureWay Directory 伺服器 (LDAP) 中啓用 SSL

下列步驟是爲 IBM SecureWay Directory 伺服器與 WebSphere Commerce 架構 SSL 安全特性。

安裝 SecureWay

如果要安裝 IBM SecureWay Directory 伺服器請：

1. 根據 SecureWay Directory 伺服器產品的安裝指示，安裝 IBM SecureWay Directory 伺服器。請確定您有安裝 GSKit 元件。
2. 在安裝完成後，呼叫 IBM 金鑰管理程式，（位於 Windows 上的 *drive*:\Program Files\IBM\GSK4\bin\gsk4ikm.exe 中）。
3. 建立一個新 CMS 金鑰資料庫檔案。確定您有選出**隱藏密碼於檔案中**（例如 ldap_key.kdb）。
4. 建立一份自簽式憑證。
5. 將憑證壓縮成以 Base64 編碼的 ASCII 資料資料類型。
6. 建立新 SSLight 金鑰資料庫類別（例如 keyring.class）。
7. 在**簽章者的憑證**區段中，新增您在步驟 5 中所建的憑證檔案。
8. 開啓瀏覽器並前往下列位址：http://hostname/ldap
9. 按一下**安全 --> SSL --> 設定**，並進行下列的變更：
   - SSL 狀態：SSL 啓用或僅 SSL
   - 鑑別方法：伺服器鑑別
   - 安全埠：636
   - 金鑰資料庫的路徑和檔案名稱：

     AIX Solaris Linux /Keys/ldap_key.kdb

     Windows *drive*:\Keys\ldap_key.kdb
   - 金鑰標籤：*your_label*（憑證的標籤）
10. 按一下**更新**，並重新啓動 SecureWay。

WebSphere Commerce

如果要將 WebSphere Commerce 安裝成搭配 SecureWay 使用，您必須修改 *instance*.xml 檔：

```
java.naming.security.ssl.keyring = keyring
'keyring' 為 SSLight 金鑰資料庫類別的名稱 (keyring.class)
此類別檔應置於 WAS 中的類別路徑內。

java.naming.security.ssl.authentication = ibm
'ibm' 為您在建立 SSLight 金鑰資料庫類別時所指定的密碼。

java.naming.security.protocol = ssl
LdapPort = 636
```

```
<MemberSubSystem name="Member SubSystem"
                     ProfileDataStorage="LDAP"
                     AuthenticationMode="LDAP">
  <Directory LdapAdminDN="cn=root"
                 LdapAuthenticationMode="SIMPLE"
                 LdapTimeOut="0"
                 LdapVersion="3"
                 EntryFileName="WC_Install_Dir/xml/ldap/ldapentry.xml"
                 LdapPort="636"
                 SingleSignOn="0"
                 LdapAdminPW="EaDPFd9VAf0="
                 LdapHost="yazhuang.torolab.ibm.com"
                 MigrateUsersFromWCSdb="ON"
                 JNDIEnvPropName1="java.naming.security.ssl.keyring"
                 JNDIEnvPropValue1="keyring"
                 JNDIEnvPropName2="java.naming.security.ssl.authentication"
                 JNDIEnvPropValue2="ibm"
                 JNDIEnvPropName3="java.naming.security.protocol"
                 JNDIEnvPropValue3="ssl"
                 display="false"
                 LdapType="SECUREWAY" />
</Membersubsystem>
```

重新啓動 WebSphere Commerce。

第 10 章 單一簽入

本章說明如何爲 WebSphere Commerce 設定單一簽入。

必備需求

如果要啓用單一簽入，您必須符合下列需求：

- 已安裝並架構好一個現有的 LDAP 伺服器。如果要架構 LDAP 伺服器，請參閱 *IBM WebSphere Commerce 5.4 版附加軟體手冊*。
- 必須安裝及架構 WebSphere Commerce 以使用 LDAP。
- 必須啓用 WebSphere Application Server 安全特性。如果要啓用 WebSphere Application Server 安全特性，請參閱第 57 頁的第 5 章, 『啓用 WebSphere Application Server 安全特性』。

啓用單一簽入

限制

單一簽入在與 WebSphere Commerce 一起使用時，有幾個主要的限制。這些限制包括：

- LTPA Cookie 可能會經過不同的 Web 伺服器埠。
- 您可能需要修改 `ldapentry.xml` 檔案，並且新增物件類別 `ePerson`。 這是 `ldapocs` 元素的屬性。
- 您需要修改 `instance.xml`，並確定已針對 LDAP 元件中的使用者進行移轉。
- 參與單一簽入架構的機器必須使系統時鐘同步。
- 只有在可讀取並可發出 WebSphere Application Server 小型認證機構 (LTPA) 記號的應用程式間才支援單一簽入。

若要啓用單一簽入，您必須執行下列步驟：

1. 在 WebSphere Application Server 中啓用單一簽入。相關資訊請搜尋 WebSphere Application Server InfoCenter 中的 "single sign-on"，網址如下：

   ```
   http://www.ibm.com/software/webservers/appserv/doc/v40/ae
   /infocenter/index.html
   ```

選取**單一簽入：WebSphere Application Server**，並完成下列各段：

- **為 WebSphere Application Server 架構 SSO**。
  - **修改 WebSphere Application Server 的安全設定**。

    註: 您大可忽略詳述如何填寫 LDAP 欄位的步驟。
  - **將 LTPA 金鑰匯出到檔案中**。

2. 在您的 WebSphere Commerce 機器上，啓動「WebSphere Commerce 架構管理程式」。
3. 如果要架構**成員子系統**節點，請執行下列步驟：
   a. 展開 **WebSphere Commerce** → *host_name* → **案例清單** → *instance_name* → **案例內容** → **成員子系統**。
   b. 在**鑑別模式**下拉功能表中，選取 **LDAP**。
   c. 啓用**單一簽入**勾選框。
   d. 在**主電腦**欄位中，輸入 LDAP 伺服器的完整主電腦名稱。
   e. 在**管理者識別名稱**欄位中，輸入管理者的識別名稱。這個名稱應該和您的 LDAP 伺服器上使用的名稱相同。
   f. 在**管理者密碼**欄位中，輸入管理者的密碼。這個密碼應該和您的 LDAP 伺服器上使用的密碼相同。在**確認密碼**欄位中確認密碼。
   g. 填入每一個剩餘的欄位。
   h. 按一下**套用**，然後按一下**確定**。
4. 重新啓動 WebSphere Application Server。

第 4 篇 WebSphere Commerce 程式開發人員的安全作業

本篇說明必須透過 WebSphere Commerce 程式設計來執行的安全作業。通常這些作業是由 WebSphere Commerce 程式設計師來執行。

第 11 章 存取控制

瞭解存取控制

WebSphere Commerce 應用程式的存取控制模型有下列三個主要概念：使用者、動作與資源。使用者爲使用系統的人。資源爲在應用程式中維護或由應用程式維護的實體。舉例來說，資源可以是產品、文件或訂單。而代表人員的使用者設定檔亦爲資源。動作是指使用者可對資源執行的活動。存取控制是電子商務應用程式中的元件，用以決定給定的使用者是否能對給定的資源執行給定的動作。

在 WebSphere Commerce 應用程式中，存取控制有兩個主要層次。存取控制的第一個層次由 WebSphere Application Server 執行。在此層面中，WebSphere Commerce 使用 WebSphere Application Server 來保護 Enterprise Bean 與 Servlet。存取控制的第二個層次則爲 WebSphere Commerce 中細密的存取控制系統。

WebSphere Commerce 存取控制組織架構採用存取控制原則來判斷給定使用者能否對給定的資源執行給定的動作。這種存取控制組織架構提供的是細密的存取控制。它會結合使用 WebSphere Application Server 所提供的存取控制但不會予以取代。

WebSphere Application Server 中的資源保護概觀

以下的 WebSphere Commerce 資源由 WebSphere Application Server 的存取控制保護：

- 實體 Bean
  這些 Bean 仿造了電子商務應用程式中的物件。它們屬於分散式物件，可供遠端從屬站存取。
- JSP 範本
  WebSphere Commerce 在顯示頁面上採用了 JSP 範本。每一個 JSP 範本可含有一或多個會從實體 Bean 中擷取資料的資料 Bean。從屬站可藉由撰寫 URL 要求來要求 JSP 頁面。
- 控制程式與檢視畫面指令
  從屬站可藉由撰寫 URL 要求來要求控制程式與檢視畫面指令。此外，顯示頁面中可藉由使用 JSP 檔名稱或檢視畫面名稱（視 VIEWREG 表格中的登錄而定），以包含移往另一個頁面的鏈結。

一般而言會將 WebSphere Commerce server 架構成使用如下的 Web 路徑：

- `/webapp/wcs/stores/servlet/*`
  用於送往「要求 Servlet」的要求方面。
- `/webapp/wcs/stores/*.jsp`
  用於送往 JSP Servlet 的要求方面。

下圖是就上述的 Web 路徑架構，顯示要求在存取 WebSphere Commerce 資源時可能的遵循途徑。

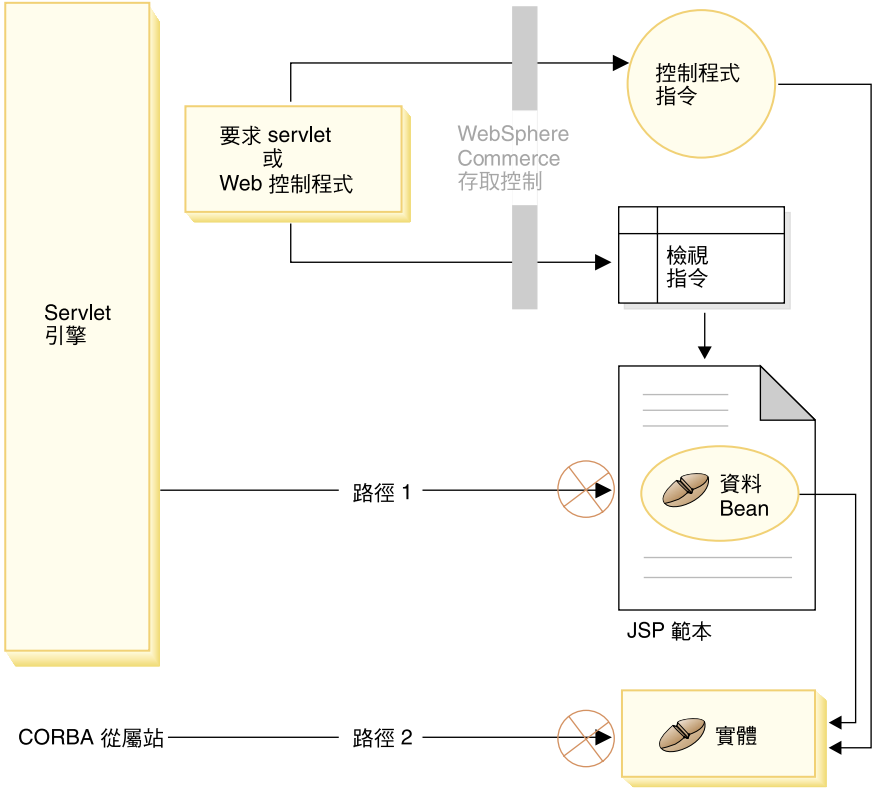


圖 3.

所有合格的要求應導向到「要求 Servlet」，再由「要求 Servlet」將之導向到 Web 控制程式。Web 控制程式會針對控制程式指令與檢視畫面施行存取控制。不過上述的 Web 路徑卻可讓某些蓄意的使用者有機會直接存取 JSP 範本（路徑 1）與實體 Bean（路徑 2）。爲了讓這些蓄意攻擊無法得逞，在執行期間必須將之拒絕在外。

您可以使用下列一種方法，以防直接存取 JSP 範本與實體 Bean：

WebSphere Application Server 安全特性

WebSphere Application Server 提供一種安全特性。當使用此方法時，會將所有的 Enterprise Bean 方法與 JSP 範本架構成只能由系統身份呼叫之。如果要存取這些 WebSphere Commerce 資源，則必須先將 URL 要求引導至將系統身份設爲現行執行緒的「要求 Servlet」處，然後再將之傳遞給 Web 控制程式。接著 Web 控制程式會先確定呼叫端具有必要的權限，然後才將要求傳遞給對應的控制程式指令或檢視畫面。任何試著直接存取 JSP 範本與實體 Bean （亦即未使用 Web 控制程式）的動作，都會遭 WebSphere Application Server 安全元件拒絕。

有關將 WebSphere Application Server 架構爲保護 WebSphere Commerce 資源的說明，請參閱 *WebSphere Commerce 安裝手冊*。有關 WebSphere Application Server 中之安全的說明，請參閱 WebSphere Application Server 文件中的「系統管理」主題。

有關爲自訂 Enterprise Bean 架構 WebSphere Application Server 安全特性方法的資訊，請參閱 *WebSphere Commerce 5.4 程式設計手冊中的「將新 Enterprise Bean 組譯到企業應用程式中」與「將已修改的 Enterprise Bean 組譯到企業應用程式中」*。

防火牆保護

當 WebSphere Commerce Server 在防火牆後面執行時，網際網路從屬站將無法直接存取實體 Bean。當您使用此方法時，是由頁面中所含的資料 Bean 來提供 JSP 範本的保護。資料 Bean 是由資料 Bean 管理程式所啓動。資料 Bean 管理程式會偵測 JSP 範本是否由檢視畫面指令所轉遞。若不是由檢視畫面指令轉遞，則會擲出異常狀況，並拒絕該項 JSP 範本要求。

WebSphere Commerce 存取控制原則簡介

WebSphere Commerce 存取控制模型是以施行存取控制原則爲基礎。存取控制原則容許存取控制規則和商業邏輯程式碼分開，因而不用將存取控制陳述式硬寫在程式碼中。例如，您不必包含如下的程式碼：

```
if (user.isAdministrator())
   then {}
```

存取控制原則是透過存取控制原則管理程式實施。一般而言，當使用者嘗試存取受保護的資源時，存取控制原則管理程式會先判斷該受保護的資源有哪些存取控制原則適用，然後再依據適用的存取控制原則，來判斷使用者能否存取所要的資源。

存取控制原則是一種 4 變數值組型的原則，且儲存在 ACPOLICY 表格中。每一個存取控制原則的格式如下：

```
AccessControlPolicy [UserGroup, ActionGroup, ResourceGroup, Relationship]
```

4 變數值組型存取控制原則中的元素會指出屬於特定使用者群組的使用者，可針對屬於指定資源群組的資源，執行指定動作群組中的動作，但前提是使用者得符合該資源的相關關係或關係群組中指定的條件。例如，[AllUsers, UpdateDoc, doc, creator] 表示只要使用者是文件的建立者，便能更新文件。

使用者群組爲一種特定的成員群組類型，其定義在 MBRGRP 資料庫表格中。使用者群組必須連結成員群組類型 -2。值 -2 代表存取群組，且定義在 MBRGRPTYPE 表格中。使用者群組與成員群組類型間的連結關係儲存在 MBRGRPUSG 表格中。

使用者與特定使用者群組間的成員關係可明確或隱含指出。當 MBRGRPMBR 表格中有指出使用者隸屬於某特定成員群組時，即屬明確指定。而如果使用者符合 MBRGRPCOND 表格中的陳述條件（例如，執行「產品經理」職務的所有使用者），即屬隱含指定。另外，亦可能存在合併條件（例如，執行「產品經理」職務並擔任該職務至少 6 個月的所有使用者）或明確排除。

大部份用以將使用者納入使用者群組中的條件，是以使用者執行某特定職務爲基礎。舉例來說，某存取控制原則可指出容許擔任「產品經理」職務的所有使用者執行型錄管理作業。在此情況下，凡在 MBRROLE 表格中被指定爲「產品經理」職務的使用者，即隱含納於使用者群組中。

有關成員群組子系統的進一步資訊，請參閱 WebSphere Commerce 線上說明。

ActionGroup 元素出自 ACACTGRP 表格。動作群組會參照某個明確指定的動作群。動作清單儲存在 ACACTION 表格中，而每個動作和其動作群組間的關係則儲存在 ACACTACTGP 表格中。例如像 ″OrderWriteCommands″ 動作群組即爲一種動作群組。此動作群組中含有下列各種用以更新訂單的動作：

- com.ibm.commerce.order.commands.OrderDeleteCmd
- com.ibm.commerce.order.commands.OrderCancelCmd
- com.ibm.commerce.order.commands.OrderProfileUpateCmd
- com.ibm.commerce.order.commands.OrderUnlockCmd
- com.ibm.commerce.order.commands.OrderScheduleCmd
- com.ibm.commerce.order.commands.ScheduledOrderCancelCmd
- com.ibm.commerce.order.commands.ScheduledOrderProcessCmd
- com.ibm.commerce.order.commands.OrderItemAddCmd
- com.ibm.commerce.order.commands.OrderItemDeleteCmd
- com.ibm.commerce.order.commands.OrderItemUpdateCmd
- com.ibm.commerce.order.commands.PayResetPMCmd

資源群組是一種將特定資源類型集結在一起的機制。資源與群組資源間的成員關係可用下列兩種方法之一指定：

- 使用 ACRESGRP 表格中的條件直欄
- 使用 ACRESGPRES 表格

在大部份情況下，要讓資源連結資源群組使用 ACRESGPRES 表格即可。當使用此方法時，資源是以其 Java 類別名稱定義在 ACRESCGRY 表格中。然後透過 ACRESGPRES 連結表格將這些資源連結適當的資源群組（ACRESGRP 表格）。如果單使用 Java 類別名稱尚不足以定義資源群組的成員（例如，如果您需要依照資源的屬性，進一步限制此類別的物件），您可使用 ACRESGRP 表格的條件直欄完整定義資源群組。請注意，如果要依照屬性來分組資源，則資源亦必須施行「可分組」介面。

下圖舉例說明資源分組的指定。在本例中，資源群組 10023 含有 ACRESGPRES 表格中所有和其連結的資源。資源群組 10070 則以 ACRESGRP 表格中的 Conditions 欄位直欄定義出。此資源群組中含有「訂單」遠端介面的案例，其狀態爲 "Z"（代表共用的需求項目清單）。

註: 有關 ACRESGRP 表格之 Conditions 直欄的 XML 資訊，請參閱 *WebSphere Commerce 存取控制手冊*。

ACRESGRP

AcResGrp_Id	GrpName	條件
10023	AccountRepresentatives CmdResourceGroup	空值
10070	SharedRequisitionList ResourceGroup	<profile> <andListCondition> <simpleCondition> <variable name="Status"/> <operator name="="/> <value data="Z"/> </simpleCondition> <simpleCondition> <variable name="classname"/> <operator name="="/> <value data="com.ibm.commerce.order.objects.Order"/> </simpleCondition> </andListCondition> </profile>

ACRESGRPES

AcResGrp_Id	AcResCgry_Id
10023	10246
10023	10247
10023	10248
10023	10249
10023	10250

ACRESCGRY

AcResCgry_Id	ResClassname
10246	com.ibm.commerce.contract.commands.ContractCreateCmd
10247	com.ibm.commerce.contract.commands.ContractCreateCmd
10248	com.ibm.commerce.contract.commands.ContractCreateCmd
10249	com.ibm.commerce.contract.commands.ContractCreateCmd
10250	com.ibm.commerce.contract.commands.ContractCreateCmd

圖 4.

ACACTGRP、ACRESGRP 與 ACRELGRP 表格中的 MEMBER_ID 直欄值應爲 -2001（根組織）。

存取控制原則可選擇性地包含 Relationship 或 RelationshipGroup 元素做爲其第四個元素。

如果您的存取控制原則使用 Relationship 元素，則其出自 ACRELATION 表格。相反地，如果其包含 RelationshipGroup 元素，則其出自 ACRELGRP 表格。請注

意，不一定要包含這兩者，但如果要包含則只能擇一。ACRELGRP 表格中的 RelationshipGroup 規格會比 ACRELATION 表格中的 Relationship 資訊優先採用。

ACRELATION 表格用以指出存在於使用者與資源間的關係類型。例如，關係類型可爲：creator（建立者）、submitter（提交者）與 owner（擁有者）。而會用到 relationship 元素的情況像是：用來確定訂單的建立者恆可更新訂單。

ACRELGRP 表格用以指定可連結特定資源的關係群組類型。關係群組是由一或多個關係鏈組成的群組。關係鏈爲一系列一個以上的關係。 舉例來說，關係群組可指出使用者必須是資源的建立者，且隸屬於資源中所參照的買方組織實體。

關係群組（或關係）規格是存取控制原則中的一個選用部份。通常是在您建有自己的指令且未限制這些指令僅供某些職務使用時使用。在這些情況下，您可能會想在使用者與資源間設立一項關係。一般而言，如果指令被限制只有某些職務才能使用，通常是透過存取控制原則的 UserGroup 元素來達到此目的，而非使用 Relationship 元素。

存取控制原則另一項重要的概念是存取控制原則*擁有者*的概念。存取控制原則擁有者是擁有該存取控制原則的組織實體。知道存取控制原則擁有者很重要，這是因爲存取控制原則僅適用於存取控制原則擁有者所擁有的資源。

存取控制原則管理程式會針對考量中的每一項資源，套用擁有組織實體（或在成員階層中其上層組織實體）所擁有的存取控制原則，直到找到授與許可權的原則爲止，或檢查完所有原則而沒有授與許可權爲止。

請注意下圖所示的成員階層。

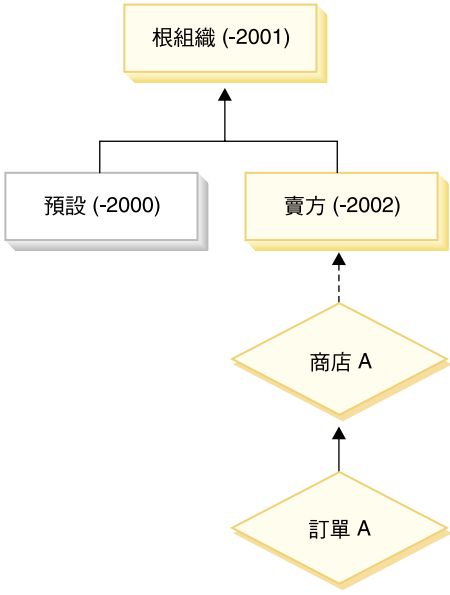


圖 5.

在資源 “OrderA” 方面，可套用「賣方」或「根組織」所擁有的任何存取控制原則。只要存取控制原則管理程式找到這些組織所擁有且會授與使用者許可權的一項原則（根據存取控制原則中的四項元素），即會立即停止搜尋存取控制原則。不過，如果找不到這些組織所擁有，且會授與使用者對受保護資源執行動作的存取控制原則，則會拒絕存取。

關係群組

關係群組可讓您指定多重關係。關係可以是使用者與該資源間的直接關係，也可以是間接讓使用者連結資源的一個關係鏈。

註： 在下列和關係群組有關的各節中，要強調的是 WebSphere Commerce Professional Edition 中的可用組織只有：RootOrganization、DefaultOrganization 與 SellerOrganization。凡提及其它組織的範例則僅適用於 WebSphere Commerce Business Edition。

比較關係與關係群組： 存取控制原則可指出使用者和所要存取的資源間必須存在某種特定關係，或者可指出使用者必須具備關係群組中的指定條件。

在大部份情況下，當您指定關係時，應符合您應用程式的存取控制需求。不過，如果因該原則使得您必須指定一種不是直接存在於使用者與資源間的關係，而實際上是存在於使用者與資源間的一連串關係，則您必須使用資源群組。

舉例來說，如果您必須在使用者與買方組織間指定一項連結，而其中的關係要求使用者必須擔任該組織的某個特定職務，或該使用者必須是買方組織的成員，則您必須用到關係群組與關係鏈。

如果您純粹只想直接在使用者與該資源間設立一項連結，您可使用一個單純關係。舉例來說，當您想指出該使用者必須是資源的建立者時。

如果您組合了多個單純關係（舉例來說，使用者必須是建立者或提交者），便成爲一種關係鏈，且您必須使用關係群組。如果您使用的是 WebSphere Commerce Professional Edition 或 WebSphere Commerce Business Edition，便可能出現此種單純關係組合現象。

關係群組的一般資訊: 關係鏈爲一系列一個以上的關係。 關係鏈的長度取決於所含的關係數目而定。您可檢查關係鏈 XML 表示法中的 `<parameter name="aName" value="aValue" />` 元素數即可判定。

只有最後的 `<parameter name="Relationship" value="aValue" />` 元素才必須由資源的 fulfills() 方法處理。其餘的則由存取控制原則管理程式內部處理。

當關係鏈的長度爲 2 時，第一個 `<parameter name="aName" value="aValue" />` 元素是位於使用者與組織實體之間。最後的 `<parameter name="aName" value="aValue" />` 元素是位於組織實體與資源之間。

如果您需要定義關係群組，必須藉由在 XML 檔中定義關係群組資訊來完成。您可以修改 `defaultAccessControlPolicies.xml` 檔，或建立自己的 XML 檔。有關建立這些 XML 型資訊的進一步資訊，請參閱 *WebSphere Commerce 存取控制手冊*。

下列各節顯示各種不同關係群組類型的範例。

由單一關係鏈組成的關係群組: Business 您可能需在存取控制原則中指出使用者所隸屬的組織實體必須是資源的 BuyingOrganizationalEntity。因此，您必須建立一個由單一關係鏈（長度 2）組成的關係群組。關係鏈的長度之所以爲 2 是因爲其由兩個個別的關係組成。第一個關係位於使用者與其上層組織實體間。使用者在該關係中屬於 ″下層″。在第二個關係方面，存取控制原則管理程式會檢查上層組織實體和資源間有否執行 BuyingOrganizationalEntity 關係。換句話說，如果它是資源的買方組織實體，則會傳回 ″true″。

下列 XML 片段取自 `defaultAccessControlPolicies.xml` 檔，顯示如何定義此種關係群組類型：

```
<RelationGroup Name="MemberOf->BuyerOrganizationalEntity"
     OwnerID="RootOrganization">
 <RelationCondition><![CDATA[
  <profile>
```

```
    <openCondition name="RELATIONSHIP_CHAIN">
     <parameter name="HIERARCHY" value="child"/>
     <parameter name="RELATIONSHIP" value="BuyingOrganizationalEntity"/>
    </openCondition>
  </profile>
 ]]></RelationCondition>
</RelationGroup>
```

Business 另舉一例，使用者在組織實體（爲該資源的買方組織實體）中必須擔任「帳戶代表」職務。同樣地，這會用到一個由單一關係鏈（長度 2）組成的關係群組。關係鏈中的第一個部份將找出使用者在其中擔任「帳戶代表」職務的所有組織實體。接著存取控制原則管理程式會針對此組組織實體，檢查其中是否至少有一個有和資源間執行 BuyingOrganizationalEntity 關係。換句話說，如果其中有一個是資源的買方組織實體，則會傳回 ″true″。

下列 XML 片段取自 defaultAccessControlPolicies.xml 檔，顯示如何定義此種關係群組類型：

```
<RelationGroup Name="AccountRep->BuyerOrganizationalEntity"
     OwnerID="RootOrganization">
 <RelationCondition><![CDATA[
  <profile>
    <openCondition name="RELATIONSHIP_CHAIN">
            <parameter name="ROLE" value="Account Representative"/>
     <parameter name="RELATIONSHIP" value="BuyingOrganizationalEntity"/>
    </openCondition>
  </profile>
 ]]></RelationCondition>
</RelationGroup>
```

由多個關係鏈組成的關係群組： 您可以撰寫一個由多個關係鏈組成的關係群組。如果要如此做，您必須指出使用者必須符合所有的關係鏈（亦即，*AND* 情況），或者至少必須符合其中一個關係鏈（亦即，*OR* 情況）。

Business 爲了示範此種關係類型，下列 XML 片段指出使用者必須是資源的建立者，且該使用者亦必須隸屬於資源中指定的 BuyingOrganizationalEntity。第一個關係鏈指出使用者必須是資源的建立者，且長度爲 1。第二個關係鏈指出使用者必須隸屬於資源中指定的 BuyingOrganizationalEntity，且長度爲 2。

```
<RelationGroup Name="Creator_And_MemberOf->BuyerOrganizationalEntity"
     OwnerID="RootOrganization">
 <RelationCondition><![CDATA[
  <profile>
   <andListCondition>
    <openCondition name="RELATIONSHIP_CHAIN">
     <parameter name="RELATIONSHIP" value="creator" />
    </openCondition>
    <openCondition name="RELATIONSHIP_CHAIN">
     <parameter name="HIERARCHY" value="child"/>
```

```
    <parameter name="RELATIONSHIP" value="BuyingOrganizationalEntity"/>
   </openCondition>
  </andListCondition>
 </profile>
]]></RelationCondition>
</RelationGroup>
```

如果不是 *AND* 情況，亦即您要求使用者必須符合這兩個關係鏈中的一個，則 <andListCondition> 標籤應改爲 <orListCondition> 標籤。

Professional Business 爲了示範一個可用於 WebSphere Commerce Professional Edition（以及 WebSphere Commerce Business Edition）中的關係群組，在此假設有一個關係群組指出使用者是資源的建立者或提交者。請見下列 XML 片段。

```
<RelationGroup Name="Creator_Or_Submitter"
     OwnerID="RootOrganization">
  <RelationCondition><![CDATA [
 <profile>
     <orListCondition>
   <openCondition name="RELATIONSHIP_CHAIN">
          <parameter name="RELATIONSHIP"value="creator"/>
   </openCondition>
   <openCondition name="RELATIONSHIP_CHAIN">
          <parameter name="RELATIONSHIP"value="submitter"/>
   </openCondition>
     </orListCondition>
 </profile>
]]></RelationCondition>
</RelationGroup>
```

存取控制類型

存取控制有兩種類型，這兩種類型皆以原則爲基礎：指令層次的存取控制與資源層次的存取控制。

指令層次（亦稱爲「職務型」）的存取控制採用廣泛的原則類型。您可以指出凡具備特定職務的使用者可執行某些指令類型。舉例來說，您可以指定具備「帳戶代表」職務的使用者可執行 AccountRepresentativesCmdResourceGroup 資源群組中的任何指令。或者，以下圖所述的另一原則爲例，指出所有商店管理者可對 StoreAdminCmdResourceGrp 指定的任何資源執行 ExecuteCommandAction 群組中指定的任何動作。

註: MBRGRPCOND 表格之 Conditions 直欄的 XML 資訊是在您使用管理主控台來設置存取群組時產生。有關使用管理主控台來設置存取群組的詳細資訊，請參閱 WebSphere Commerce 線上說明。

ACPOLICY

PolicyName	Member_Id	MbrGrp_Id	AcActGrp_id	AcResGrp_Id	AcRelGrp_Id
StoreAdministrators ExecuteStoreAdmin CmdResourceGroup	-2001	-8	10052	10018	空值

MBRGRP

MbrGrp_Id	MbrGrpName
-8	StoreAdministrators

MBRGRPCOND

MbrGrp_Id	Conditions
-8	<profile> <simpleCondition> <variable name="role"/> <operator name="="/> <value data="商店管理者" /> </simpleCondition> </profile>

ACACTGRP

AcActGrp_Id	GroupName
10052	ExecuteCommandActionGroup

ACRESGRP

AcResGrp_Id	GrpName
10018	StoreAdminCmdResourceGroup

圖 6.

指令層次的存取控制原則恆有 ExecuteCommandActionGroup 以作爲控制程式指令的動作群組。就檢視畫面而言，資源群組恆爲 ViewCommandResourceGroup。

所有控制程式指令必須受指令層次的存取控制保護。此外，凡是可直接呼叫的檢視畫面，或者可藉由另一個指令重新導向而啓動的檢視畫面（相對於藉由轉遞至檢視畫面而啓動）皆必須受指令層次的存取控制保護。

指令層次的存取控制不會考慮到指令所要執行的資源對象。它只會判斷該使用者能否執行特定的指令。假設使用者能執行該指令，接著便會套用資源層次的存取控制原則，以判斷使用者能否存取考量中的資源。

假設某商店管理者試著執行某項管理作業。第一層的存取控制檢查會判斷該使用者能否執行特定的商店管理指令。一旦它判斷出該使用者確能如此做時（因爲商

店管理者能執行 storeAdminCmds 群組中的指令），即可呼叫資源層次的存取控制原則。此原則可能指出：商店管理者能執行管理作業的商店，僅限於該使用者在其中扮演商店管理者職務之組織所擁有的商店。

總結來說，在指令層次的存取控制中，「資源」爲指令本身，而「動作」純爲執行指令（換句話說，案例化指令物件）。存取控制檢查會判斷使用者能否執行指令。相對地，在資源層次的存取控制中，「資源」可爲指令或 Bean 所存取之任何可保護的資源，而「動作」則爲指令本身。

存取控制的互動

本節以互動圖解來說明在 WebSphere Commerce 存取控制原則組織架構下存取控制如何運作。

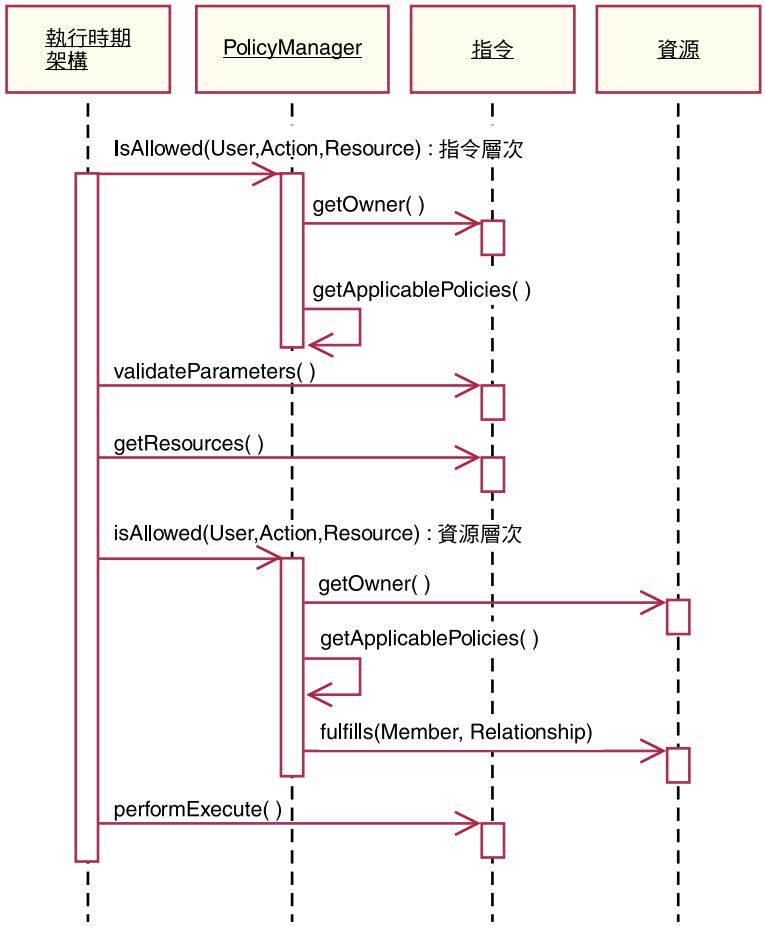


圖 7.

上圖顯示存取控制*原則管理程式*所執行的動作。存取控制原則管理程式是一種存取控制元件，會判斷現行使用者能否對指定資源執行指定動作。它是藉由搜尋資源擁有者與其上層組織所擁有的原則來作出判斷。只要至少有一項原則授與存取，即授與許可權。

下列說明上述互動圖中的各項動作。且從圖中的上到下依序說明。

1. `isAllowed()`
   執行期間元件判斷使用者對於控制程式指令或檢視畫面是否具備指令層次的存取權。
2. `getOwner()`
   存取控制原則管理程式判斷指令層次資源的擁有者。就預設施行而言，會傳

回指令環境定義中的商店 (storeId) 擁有者的成員識別碼 (memberId)。如果指令環境定義中沒有商店識別碼，則會傳回根組織 (-2001)。

3. getApplicablePolicies()
   存取控制原則管理程式根據指定的使用者、動作與資源，來尋找與處理適用的原則。
4. validateParameters()
   起始參數的檢查與解析。
5. getResources()
   傳回一個存取向量（即「資源/動作」對的向量）。

   假設未傳回任何項目，則不會執行資源層次的存取控制檢查。如有資源應受保護，則應會傳回一個存取向量（由「資源/動作」對組成）。

   每一項*資源*皆爲可保護物件（即施行 com.ibm.commerce.security.Protectable 介面的物件）的案例。在眾多情況下，資源爲一種存取 Bean。

   存取 Bean 不見得施行 com.ibm.commerce.security.Protectable 介面，不過只要其對應的 Enterprise Bean 受到保護，仍可進行存取控制檢查（相關資訊請參閱第 112 頁的『在 Enterprise Bean 中施行存取控制』）。

   *動作*爲一種字串，代表對資源所執行的作業。在大部份情況下，動作爲指令的介面名稱。
6. isAllowed()
   執行期間元件判斷使用者對於 getResources() 指定的所有「資源/動作」對組是否具備資源層次的存取權。
7. getOwner()
   資源傳回其擁有者的 memberId。這是判斷要套用哪些原則。只會套用資源擁有者與其上層組織所擁有的原則。
8. getApplicablePolicies()
   存取控制原則管理程式搜尋適用的原則，並加以套用。如果每個「資源/動作」對至少找到一項原則可授與使用者存取資源的許可權，則授與存取，否則則拒絕存取。
9. fulfills()
   如果適用的原則有指定關係群組，則會檢查資源，看看該成員是否符合指定的資源關係。
10. performExecute()
    指令的商業邏輯。

可保護的介面

若要讓資源受 WebSphere Commerce 存取控制原則保護，其關鍵因素在於資源必須施行 com.ibm.commerce.security.Protectable 介面。此介面最常搭配 Enterprise Bean 與資料 Bean 使用，但只有這些需要保護的特定 Bean 才需施行此介面。

在「可保護」介面下，資源必須提供下列兩個關鍵方法：getOwner() 與 fulfills(Long member, String relationship)。

存取控制原則爲組織或組織實體所擁有。 getOwner 方法會傳回可保護資源之擁有者的 memberId。在存取控制原則管理程式判斷出資源擁有者後，亦會取得成員階層中該擁有者之每一個上層的 memberId。所有隸屬於原始 getOwner 要求中之擁有者的存取控制原則，以及隸屬於擁有者之上層的所有存取控制原則皆會套用。

適用於指定擁有者的存取控制原則，以及適用於成員階層中擁有者之任何上層的存取控制原則皆會套用。

只有在給定成員符合所要的資源關係時，fulfills 方法才會傳回 true。通常成員爲單一使用者，不過也可以是一個組織。如果您在存取控制原則中有使用關係群組，則會是組織。

可分組介面

存取控制原則的應用將隨資源群組而定。您可根據屬性（像是：類別名稱、訂單狀態或 storeId 值）來進行資源分組。

如果您爲了套用存取控制原則，而依屬性（而非其類別名稱）來分組資源，則其必須施行 com.ibm.commerce.grouping.Groupable 介面。

下列的程式碼片段顯示「可分組」介面：

```
Groupable interface {
Object getGroupingAttributeValue (String attributeName, GroupContext context)
}
```

舉例來說，假設您要施行一項僅套用於處於擱置狀態（status = P（擱置））的訂單之原則， Order 實體 Bean 的遠端介面會施行「可分組」介面，且 attributeName 值會設爲 "status"。

通常很少使用「可分組」介面。

尋找存取控制的詳細資訊

有關 WebSphere Commerce 存取控制模型的詳細資訊，請參閱 *WebSphere Commerce 存取控制手冊*。此手冊會提供存取控制的詳細概觀，並說明如何使用管理主控台來建立或修改原則、動作群組與資源群組。

施行存取控制

本節說明如何以自訂程式碼來施行存取控制。

識別可保護的資源

一般而言，Enterprise Bean 與資料 Bean 可能是您想保護的資源。不過，並非所有的 Enterprise Bean 與資料 Bean 皆應保護。在現有的 WebSphere Commerce 應用程式中，需要保護的資源已施行可保護介面。不過當您建立新 Enterprise Bean 與資料 Bean 時，便會出現該保護哪些資源的問題。請根據您的應用程式來決定所要保護的資源。

如果指令在 `getResources` 方法中傳回 Enterprise Bean，則該 Enterprise Bean 必須加以保護，這是因爲存取控制原則管理程式會對該 Enterprise Bean 呼叫 getOwner 方法。如果對應的資源層次存取控制原則中有指定關係，亦會呼叫 `fulfills` 方法。

如果您針對自己所有的 Enterprise Bean 與資料 Bean 施行可保護介面（因而讓資源受到保護）您的應用程式可能會要求許多原則。原則越多，效能可能降低，且原則管理亦趨複雜。

主要資源與相依資源有理論上的區分。*主要資源*可獨立存在。*相依資源*則必須在其相關主要資源存在時才存在。舉例來說，在 out-of-the-box WebSphere Commerce 應用程式碼中， Order 實體 Bean 爲可保護的資源，OrderItem 實體 Bean 則不是。其原因在於 OrderItem 的存在與否端視 Order 而定 -- Order 爲主要資源，而 OrderItem 爲相依資源。如果使用者應具備 Order 的存取權，則亦應具備訂單中各項目的存取權。

同樣地，User 實體 Bean 爲可保護的資源，但 Address 實體 Bean 則不是。在此情況中，地址的存在與否端視使用者而定，因此只要能夠存取該使用者，便應能夠存取該地址。

主要資源應受保護，但相依資源通常不需保護。如果使用者能存取主要資源，在預設的情況下，該使用者也應能存取其相依資源。

在 Enterprise Bean 中施行存取控制

如果您建立的新 Enterprise Bean 需要受存取控制原則保護，您必須執行下列步驟：

1. 建立新 Enterprise Bean，並確定它是從 com.ibm.commerce.base.objects.ECEntityBean 延伸而來。
2. 確定 Bean 的遠端介面是 com.ibm.commerce.security.Protectable 介面的延伸。
3. 如果和 Bean 互動的資源是依屬性（而非資源的 Java 類別名稱）分組，則 Bean 的遠端介面亦必須是 com.ibm.commerce.grouping.Groupable 介面的延伸。
4. Enterprise Bean 類別中含有下列方法的預設施行：
   - getOwner
   - fulfills
   - getGroupingAttributeValue

   請改寫任何您要的方法。您至少需改寫 getOwner 方法。
   下列程式碼片段顯示這些方法的預設施行。

```
*************************************************************************
public Long getOwner() throws Exception, java.rmi.RemoteException
{
      return null;
}
*************************************************************************
*************************************************************************
public boolean fulfills(Long member, String relationship)
  throws Exception, java.rmi.RemoteException
{
      return false;
}
*************************************************************************
*************************************************************************
public Object getGroupingAttributeValue(String attributeName,
   GroupingContext context) throws Exception, java.rmi.RemoteException
{
      return null;
}
*************************************************************************
```

以下是這些方法的範例施行，其以 OrderBean Bean 爲基礎：

```
*************************************************************************
public Long getOwner() throws Exception, java.rmi.RemoteException
{
   com.ibm.commerce.common.objects.StoreEntityAccessBean storeEntAB = new
   com.ibm.commerce.common.objects.StoreEntityAccessBean();
   storeEntAB.setInitKey_storeEntityId(getStoreEntityId().toString());
   return storeEntAB.getMemberIdInEJBType();
}
*************************************************************************
```

```
*****************************************************************************
public boolean fulfills(Long member, String relationship)
  throws Exception, java.rmi.RemoteException
   {
if (relationship.equalsIgnoreCase("creator"))
      {
         return member.equals(getMemberId());
      }
      else if (relationship.equalsIgnoreCase (
         com.ibm.commerce.base.helpers.EJBConstants.
         SAME_ORGANIZATIONAL_ENTITY_AS_CREATOR_RELATION)) {
            com.ibm.commerce.user.objects.UserAccessBean creator = new
               com.ibm.commerce.user.objects.UserAccessBean();
            creator.setInitKey_MemberId(getMemberId().toString());
            com.ibm.commerce.user.objects.UserAccessBean ab = new
               com.ibm.commerce.user.objects.UserAccessBean();
            ab.setInitKey_MemberId(member.toString());
            if (ab.getParentMemberId().equals(creator.getParentMemberId()))
     return true;
          }
      return false;
}
*****************************************************************************
*****************************************************************************
public Object getGroupingAttributeValue(String attributeName,
   GroupingContext context) throws Exception
   {
      if (attributeName.equalsIgnoreCase("Status"))
         return getStatus();
      return null;
   }
*****************************************************************************
```

5. 建立（或重建）Enterprise Bean 的存取 Bean 與產生的程式碼。

在資料 Bean 中施行存取控制

如果您想保護某個資料 Bean，則可由存取控制原則直接或間接保護。如果資料 Bean 受直接保護，則會有一個套用在該特定資料 Bean 的存取控制原則。如果資料 Bean 受間接保護，則是委由有套用存取控制原則的另一資料 Bean 來保護。

如果您想建立一個直接由存取控制原則保護的新資料 Bean，則資料 Bean 必須執行下列步驟：

1. 施行 `com.ibm.commerce.security.Protectable` 介面。在此情況下， Bean 必須提供 `getOwner()` 與 `fulfills(Long member, String relationship)` 方法的施行。這些應施行於 Bean 的遠端介面上。

   當資料 Bean 施行「可保護」介面時，資料 Bean 管理程式會呼叫 `isAllowed` 方法，以根據目前的存取控制原則，判斷使用者是否具備適當的存取控制專用權。下列程式碼片段說明 `isAllowed` 方法：

   ```
   IsAllowed(Context, "Display", protectable_databean);
   ```

2. 如果和 Bean 互動的資源是依屬性（而非資源的 Java 類別名稱）分組，則 Bean 必須施行 com.ibm.commerce.grouping.Groupable 介面。
3. 施行 com.ibm.commerce.security.Delegator 介面。此介面是以下列程式碼片段來說明：

```
Interface Delegator {
Protectable getDelegate();
}
```

註: 如果要直接保護，getDelegate 方法應傳回資料 Bean 本身（亦即，資料 Bean 基於存取控制而委任給自己）。

哪些資料 Bean 應直接保護以及哪些資料 Bean 應間接保護的區別，和主要與相依資源間的區別類似。如果資料 Bean 物件可獨立存在，則應直接保護。如果資料 Bean 的存在與否取決於另一資料 Bean 的存在而定，則應委由另一資料 Bean 來保護。

例如像 Order 資料 Bean 即爲直接保護的資料 Bean。而像 OrderItem 資料 Bean 則爲間接保護的資料 Bean。

如果您想建立一個由存取控制原則間接保護的新資料 Bean，則資料 Bean 必須執行下列：

1. 施行 com.ibm.commerce.security.Delegator 介面。此介面是以下列程式碼片段來說明：

```
Interface Delegator {
Protectable getDelegate();
}
```

註: getDelegate 傳回的資料 Bean 必須施行「可保護」介面。

如果資料 Bean 未施行「委任者」介面，則會在沒有存取控制原則保護下移入資料。

在控制程式指令中施行存取控制

在您建立新控制程式指令時，新指令的施行類別應由 com.ibm.commerce.commands.ControllerCommandImpl 類別延伸而來，且其介面應由 com.ibm.commerce.command.ControllerCommand 介面延伸而來。

就控制程式指令的指令層次原則來說，會以指令的介面名稱做爲資源。如果要保護資源，則必須施行「可保護」介面。根據 WebSphere Commerce 程式設計模型，可藉由讓指令的介面從 com.ibm.commerce.command.ControllerCommand 介面延伸而來，以及讓指令的施行從 com.ibm.commerce.commands.ControllerCommandImpl 延伸而來來達成此項。ControllerCommand 介面是從

com.ibm.commerce.command.AccCommand 介面延伸而來，而此介面又是從可保護延伸而來。AccCommand 介面是指令所應執行的最小介面，以便受指令層次型存取控制保護。

如果指令會存取應受保護的資源，請建立一個 AccessVector 類型的專用案例變數，以放置資源。然後改寫 getResources 方法，這是因爲方法的預設施行是傳回空值，因而不會進行任何資源檢查。

在新 getResources 方法中，您應傳回指令所能執行的資源陣列或「資源/動作」對陣列。如果未明確指定動作，將會執行指令介面名稱的預設動作。

此外，建議您由方法來判斷是否必須案例化資源，或者可否使用內含資源參照的現有案例變數。檢查資源物件是否存在，有助提昇系統效能。必要時，您可在新控制程式指令的 performExecute 方法中使用相同的 getResources 方法。

下列是 getResources 方法的範例：

```
private AccessVector resources = null;

public AccessVector getResources() throws ECException {

   if (resources == null) {
      OrderAccessBean orderAB = new OrderAccessBean();
      orderAB.setInitKey_orderId(getOrderId().toString());
      resouces = new AccessVector(orderAB);
      }
   return resources;
}
```

以 OrderItemUpdate 指令爲例。此指令的 getResources 方法會傳回「訂單」與「使用者」可保護的物件。如果未指定動作，將預設爲 OrderItemUpdate 指令的介面。

getResources 方法所傳回的資源可能有多個。如果發生此情況，當執行動作時，必須能夠找到容許使用者存取所有指定資源的原則。假設使用者有權存取三個資源中的兩個，則動作不見得能繼續進行（三個全需要）。

如果您需要檢查控制程式指令中的其它參數或解析其中的參數，您可以使用 validateParameters() 方法。此爲選用方法。

其它的資源層次檢查

當呼叫控制程式指令中的 getResources 方法時，不一定都會判斷所有需要保護的資源。

必要時，作業指令也可施行 getResources 方法，以傳回指令所能執行的資源清單。

另一種呼叫資源層次檢查的方法是，使用 checkIsAllowed(Object resource, String action) 方法直接呼叫存取控制原則管理程式。此方法適用於任何延伸自 com.ibm.commerce.command.AbstractECTargetableCommand 類別的類別。舉例來說，下列類別是延伸自 AbstractECTargetableCommand 類別：

- com.ibm.commerce.command.ControllerCommandImpl
- com.ibm.commerce.command.DataBeanCommandImpl

checkIsAllowed 方法亦適用於延伸自 com.ibm.commerce.command.AbstractECCommand 類別的類別。舉例來說，下列類別延伸自 AbstractECCommand 類別：

- com.ibm.commerce.command.TaskCommandImpl

下列是 checkIsAllowed 方法的用法：

```
void checkIsAllowed(Object resource, String action)
   throws ECException
```

一旦不容許現行使用者對指定資源執行指定的動作，此方法即會擲出 ECApplicationException。如果授與存取權，則方法只會傳回。

“create” 指令的存取控制

由於在指令中 getResources 方法是在 performExecute 方法之前呼叫，您必須針對尚未建立之資源的存取控制採取不同的方式。舉例來說，假設您有 WidgetAddCmd，getResources 方法無法傳回即將建立的資源。在此情況下，getResources 方法應會傳回資源的建立者。舉例來說，指令由指令 factory 所建立的，訂單建於商店中，使用者則建於組織中。

指令層次之存取控制的預設施行

在指令層次的存取控制方面，getOwner() 方法的預設施行會傳回商店擁有者的 memberId（如果有指定 storeId 的話）。如果未指定 storeId，則會傳回根組織的 memberId（memberId = -2001）。

就 getResources() 方法的預設施行而言，是傳回 null。

就 validateParameters() 的預設施行而言，則不執行任何動作。

在檢視畫面中施行存取控制原則

檢視畫面的資源層次存取控制是由資料 Bean 管理程式所執行。在下列情況下將會呼叫資料 Bean 管理程式：

1. 當 JSP 範本含有 <useBean> 標籤，且屬性清單中沒有資料 Bean 時。
2. 當 JSP 範本含有下列的啓動方法時：

   ```
   DataBeanManager.activate(xyzDatabean, request);
   ```

註: 任何必須保護的資料 Bean（不論直接或間接）皆必須施行「委任者」介面。凡受直接保護的資料 Bean 將委任給自己，因而亦必須施行「可保護」介面。而受間接保護的資料 Bean 則應委任給施行「可保護」介面的資料 Bean。

下列情況下將會略過存取控制檢查（不過不建議您如此做）：

1. 如果 JSP 範本直接呼叫存取 Bean，而非使用資料 Bean 時。
2. 如果 JSP 範本直接呼叫資料 Bean 的 populate() 方法時。

如果控制程式指令的結果會轉遞至檢視畫面（使用 ForwardViewCommand），則不會對檢視畫面執行指令層次的存取控制。再者，如果控制程式指令將移入資料的資料 Bean（用於檢視畫面中）置於回應內容的屬性清單中，並轉遞給檢視畫面，則 JSP 範本可直接存取資料，而不需透過資料 Bean 管理程式。不過 JSP 範本中得使用 `<useBean>` 標籤。此方法可讓 JSP 範本更有效率，這是因爲它可針對使用者透過控制程式指令而有權存取的資源（資料 Bean），略過對這些資源冗餘的資源層次存取控制檢查。

第 5 篇 後記

注意事項

本資訊是針對 IBM 在美國所提供之產品與服務開發出來的。

而在其他國家中，IBM 不見得有提供本書中所提的各項產品、服務、或功能。要知道在您所在之區是否可用到這些產品與服務時，請向當地的 IBM 服務代表查詢。凡提及 IBM 產品、程式或服務項目時，亦不表示只可用 IBM 的產品、程式或服務項目。只要未侵犯 IBM 的智慧財產權，任何功能相當的產品、程式或服務都可以取代 IBM 的產品、程式或服務。不過，其他非 IBM 產品、程式、或服務在運作上的評價與驗證，其責任屬於使用者。

本書在提及任何 IBM 授權程式時，不表示或暗示只可以使用 IBM 授權程式。 只要未侵犯 IBM 的智慧財產權，任何功能相等的產品、程式或服務，都可以取代 IBM 的產品、程式或服務。其它產品、程式或服務在運作上的評價與驗證，除非 IBM 特別指示，其責任屬於使用者。

IBM 可能已經申請與本書有關（包括本書的主題內容）的各項專利權，或者具有正在審理中的專利權申請書。本書使用者並不享有前述專利之任何授權。您可以用書面方式來查詢授權，來函請寄到：

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

如果要查詢有關二位元組（DBCS）資訊的授權事宜，請聯絡您國家的 IBM 智慧財產部門，或者用書面方式寄到：

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106, Japan

下列段落若與該國之法律條款抵觸，即視爲不適用：

IBM 就本書僅提供「交附時之現況」保證，而並不提供任何明示或默示之保證，如默示保證書籍之適售性或符合客戶之特殊使用目的；有些地區在某些固定的交易上並不接受明示或默示保證的放棄聲明，因此此項聲明不見得適用於您。

本書可能會有技術上或排版印刷上的訛誤。因此，IBM 會定期修訂；並將修訂後的內容納入新版中。同時，IBM 得隨時改進並 (或) 變動本出版品中所提及的產品及 (或) 程式。

本資訊中任何對非 IBM 網站的敘述僅供參考，IBM 對該網站並不提供保證。該 Web 站上的資料，並非本 IBM 產品所用資料的一部分，因使用該 Web 站造成之損害，由 貴客戶自行負責。

IBM 得以各種適當的方式使用或散布由 貴客戶提供的任何資訊，而無需對您負責。

本程式的獲授權者若希望取得相關資料，以便使用下列資訊者可洽詢 IBM。其下列資訊指的是：（1）獨立建立的程式與其他程式（包括此程式）之間更換資訊的方式 （2）相互使用已交換之資訊方法。若有任何問題請聯絡：

IBM Canada Ltd.
Office of the Lab Director
8200 Warden Avenue
Markham, Ontario
L6G 1C7
Canada

上述資料之取得有其特殊要件，在某些情況下必須付費方得使用。

IBM 基於雙方之「IBM 客戶合約」、「IBM 國際程式授權合約」（或任何同等合約）條款，提供本資訊中所述的授權程式與其所有適用的授權資料。

任何此處涵蓋的執行效能資料都是在一個受控制的環境下決定出來的。因此，若在其他作業環境下，所得的結果可能會大大不同。有些測定已在開發階段系統上做過，不過這並不保證在一般系統上會出現相同結果。再者，有些測定可能已透過推測方式評估過。但實際結果可能並非如此。本書的使用者應依自己的特定環境，查證適用的資料。

本書所提及之非 IBM 產品資訊，取自產品的供應商，或其公佈的聲明或其他公開管道。IBM 並未測試過這些產品，也無法確認這些非 IBM 產品的執行效能、相容性、或任何對產品的其他主張是否完全無誤。如果您對非 IBM 產品的性能有任何的疑問，請逕向該產品的供應商查詢。

有關 IBM 未來動向的任何陳述，僅代表 IBM 的目標而已，並可能於未事先聲明的情況下有所變動或撤回。

此資訊僅供規劃用。因此在產品尚未上市前此資訊仍有變更的可能。

本書中的範例包含了用於日常商業活動的資料及報告。爲了盡可能詳細，範例中涵蓋了個人、公司、品牌及產品的名稱。這些名稱全部都是虛構的，如果與眞實公司企業的名稱和地址雷同，純屬巧合。

本產品中提到的信用卡影像、商標和商品名稱只限於已取得信用卡商標的擁有者授權可以接受以該信用卡付款的商家使用。

商標

下列詞彙爲 IBM 公司在美國及（或）其他國家的商標或註冊商標：

400	AIX	AS/400
DB2	IBM	iSeries
OS/2	SecureWay	WebSphere

Domino 是 Lotus Development 公司與（或） IBM 公司在美國與（或）其它國家中的註冊商標。

Netscape 是 Netscape Communications 公司在美國和其他國家的註冊商標。

Solaris、Solaris Operating Environment、Java、JavaBeans 以及所有與 Java 相關的商標與標誌爲 Sun Microsystems, Inc. 的商標或註冊商標。

VeriSign 和 VeriSign 標誌是 VeriSign, Inc. 的商標和服務標誌，或其註冊商標和服務標誌。

UNIX 是 The Open Group 在美國以及其他國家內的註冊商標。

Windows、Windows NT 和 Windows 標誌是 Microsoft Corporation 在美國及（或）其他國家的商標。

其它公司、產品或服務名稱可能是其他者的商標或服務標記。

讀者意見表

爲使本書盡善盡美，本公司極需您寶貴的意見；懇請您使用過後，撥冗填寫下表，惠予指教。

請於下表適當空格內，填入記號（∨）；我們會在下一版中，作適當修訂，謝謝您的合作!

評估項目	評 估 意 見		備 註
正 確 性	內容說明與實際程序是否符合	□是□否	
	參考書目是否正確	□是□否	
一 致 性	文句用語及風格，前後是否一致	□是□否	
	實際畫面訊息與本書所提之畫面訊息是否一致	□是□否	
完 整 性	是否遺漏您想知道的項目	□是□否	
	字句、章節是否有遺漏	□是□否	
術語使用	術語之使用是否恰當	□是□否	
	術語之使用，前後是否一致	□是□否	
可 讀 性	文句用語是否通順	□是□否	
	有否不知所云之處	□是□否	
內容說明	內容說明是否詳盡	□是□否	
	例題說明是否詳盡	□是□否	
排版方式	本書的形狀大小，版面安排是否方便使用	□是□否	
	字體大小，顏色編排，是否有助於閱讀	□是□否	
目錄索引	目錄內容之編排，是否便於查考	□是□否	
	索引語錄之排定，是否便於查考	□是□否	
	※評估意見爲 "否" 者，請於備註欄說明。		

其他： (篇幅不夠時，請另紙說明。)

上述改正意見，一經採用，本公司有合法之使用及發佈權利，特此聲明。

註： 您也可將寶貴的意見以電子郵件寄至 NLSC01@tw.ibm.com，謝謝。

IBM WebSphere Commerce
安全手冊

第 5.4 版

折疊線

台北市 110 基隆路一段 206 號

大臺灣國際商業機器股份有限公司
中華研發中心
軟體國際部 啟

廣告回信
台灣北區郵政管理局
登記證
北台字第 0587 號
（免貼郵票）

寄件人 姓名：
地址：

寄

折疊線

讀者意見表