eserver

iSeries

iSeries 安全保護要訣及工具

版本 5

SC40-1899-07

iSeries

iSeries 安全保護要訣及工具

版本 5

SC40-1899-07

請注意

使用此資訊及其支援的產品之前，請先閱讀第 145 頁的『注意事項』中的資訊。

第八版 (2004 年 4 月)

| 此版本適用於 IBM Operating System/400 版本 5 版次 3 修正層次 0 (產品編號 5722-SS1)，以及所有後續版次與修訂
| 版，除非新版中另有指示。此版本並非適用於所有的精簡指令集電腦 (RISC) 機型和 CISC 機型。

此版本取代 SC40-0195-06。

目錄

圖 vii

表 ix

關於保護 iSeries 安全的要訣及工具 (SC40-1899-07) xi
本書的讀者對象 xi
如何使用本資訊 xii
先決條件與相關資訊 xii
如何傳送您的意見 xii

第 1 篇 iSeries 安全的基本功能 . . . 1

第 1 章 iSeries 安全的基本元素. 3
安全層次. 3
整體設定. 4
使用者設定檔 4
群組設定檔 4
資源安全. 5
限制程式功能 5
安全審核. 6
範例：系統安全屬性報告 7

第 2 章 iSeries 安全性精靈與 eServer 安全規劃程式. 9
安全精靈. 9
eServer 安全規劃程式 11

第 3 章 控制交談式登入. 13
設定密碼規則 13
密碼層次 14
規劃密碼層次變更 14
變更公開的密碼 18
設定登入值 19
變更登入錯誤訊息 20
排定使用者設定檔的可用性 20
移除非作用中的使用者設定檔 21
自動停用使用者設定檔 21
自動移除使用者設定檔 22
避免預設密碼 22
監督登入及密碼活動 23
儲存密碼資訊 23

第 4 章 配置 iSeries 使用安全性工具程式 25
安全地操作安全性工具程式 25
避免檔案衝突. 25
儲存安全性工具程式 25
安全指令的指令和功能表 26
「安全工具」功能表選項 26
使用「安全批次」功能表 28
自行設定安全的指令 31
配置系統安全指令所設定的值 32
「取消公用權限」指令的功能 34

第 2 篇 iSeries 安全的進階功能. . . 37

第 5 章 以物件權限來保護資訊資產 . . . 39
增強物件權限. 39
功能表安全性. 39
功能表存取控制的限制. 40
以物件安全性增強功能表存取控制 40
範例：建立轉移環境 40
使用檔案庫安全來補充功能表安全 42
配置物件所有權 42
系統指令和程式的物件權限 43
審核安全功能. 43
分析使用者設定檔 44
分析物件權限. 45
檢查已改變的物件 45
分析採用權限的程式 46
管理審核日誌及異動日誌接收器. 46

第 6 章 管理權限 49
監督物件的公用權限 49
管理新物件的權限 49
監督授權清單. 50
使用授權清單. 51
存取「iSeries 領航員」中的原則. 52
監督物件的專用權限 52
監督對輸出及工作佇列的存取 53
監督特殊權限. 53
監督使用者環境. 54
管理服務工具. 55

第 7 章 使用邏輯分割區安全性 (LPAR) 57
管理邏輯分割區的安全性 57

第 8 章 iSeries 作業主控台 59
作業主控台安全概觀 60
主控台裝置鑑別. 60
使用者鑑別 60
資料私密性 60
資料完整性 60
使用具有 LAN 連接的作業主控台 61
保護具有 LAN 連接的作業主控台 61
使用作業主控台設定精靈 61

第 9 章 偵測可疑的程式. 63
防止電腦病毒的侵襲 63
監督沿用權限的使用 64

限制沿用權限的使用 65
防止新程式使用沿用的權限 66
監督觸發程式的使用 67
檢查隱藏程式 68
評估登記的跳出程式 69
檢查排定的程式 70
限制儲存和復置功能 70
檢查在受保護檔案庫內的使用者物件 71

第 10 章 防止及偵測駭客入侵 73
實體安全性 73
監督使用者設定檔活動 73
物件簽署 74
監督子系統說明 74
自動啓動工作登錄 75
工作站名稱及工作站類型 75
工作佇列登錄 75
遞送登錄 76
通訊登錄及遠端位置名稱 76
預先啓動工作登錄 76
工作及工作說明 76
架構的異動程式名稱 77
架構的 TPN 要求 78
監督安全事件的方法 79

第 3 篇 應用程式及網路通訊 81

第 11 章 使用 整合檔案系統 來保護檔案 83
整合檔案系統 安全方法 83
根 (/)、QOpenSys 及使用者定義的檔案系統 84
權限的工作方式 84
列印專用權限物件 (PRTPVTAUT) 指令 87
列印公用授權的物件 (PRTPUBAUT) 指令 87
限制存取 QSYS.LIB 檔案系統 88
保護目錄安全 89
新物件的安全 89
使用建立目錄指令 89
使用 API 來建立目錄 89
使用 open() 或 creat() API 來建立串流檔 . . . 90
使用 PC 介面來建立物件 90
QFileSvr.400 檔案系統 90
網路檔案系統 (NFS) 90

第 12 章 保護 APPC 通訊安全. 93
APPC 專用辭彙 93
APPC 通訊的基本元素 93
範例：基本 APPC 階段作業 94
限制 APPC 階段作業 94
APPC 使用者存取目標系統 95
用來傳送有關使用者資訊的系統方法 95
區分網路安全責任的選項 96
工作之使用者設定檔的目標系統分派 96
顯示站透通選項 97
避免非預期的裝置分派 98
控制遠端指令及批次工作 98
評估 APPC 配置. 99
APPC 裝置的相關參數 99
APPC 控制器的參數 101
線路說明的參數. 102

第 13 章 保護 TCP/IP 通訊安全. . . . 105
防止 TCP/IP 處理 105
TCP/IP 安全性元件 105
使用封包規則來保護 TCP/IP 傳輸的安全 . . . 106
HTTP PROXY 伺服器 106
虛擬專用網路 (VPN) 106
Secure Sockets Layer (SSL) 107
保護 TCP/IP 環境的安全. 107
控制自動啓動的 TCP/IP 伺服器 108
使用 SLIP 的安全注意事項 109
控制撥入 SLIP 連接 109
控制撥出階段作業 111
使用點對點通訊協定的安全注意事項 112
使用啓動程式通訊協定伺服器的安全注意事項 . . . 113
防止 BOOTP 存取. 113
保護 BOOTP 伺服器的安全. 114
使用 DHCP 伺服器的安全注意事項 114
防止 DHCP 存取 114
保護 DHCP 伺服器的安全 115
使用 TFTP 伺服器的安全注意事項 116
防止 TFTP 存取 116
保護 TFTP 伺服器的安全 116
使用 REXEC 伺服器的安全注意事項. 117
防止 REXEC 存取. 117
保護 REXEC 伺服器的安全. 118
使用 RouteD 的安全注意事項 118
使用 DNS 伺服器的安全注意事項. 119
防止 DNS 存取. 119
保護 DNS 伺服器的安全. 119
使用 HTTP Server for iSeries 的安全注意事項 . . 120
防止 HTTP 存取 120
控制對 HTTP 伺服器的存取 121
將 SSL 與 IBM HTTP Server for iSeries 搭配使用的安全注意事項 124
LDAP 的安全注意事項 125
LPD 的安全性注意事項 125
防止 LPD 存取. 125
控制 LPD 存取. 126
SNMP 的安全注意事項 126
防止 SNMP 存取 126
控制 SNMP 存取 127
INETD 伺服器的安全注意事項 127
限制 TCP/IP 漫遊的安全注意事項. 128

第 14 章 保護工作站存取的安全 131
防止工作站病毒. 131
保護工作站資料存取的安全 131
具有工作站存取的物件權限 132
應用程式管理 132
搭配使用 SSL 和 iSeries Access for Windows 133
iSeries 領航員 安全性. 133
防止 ODBC 存取 134

工作站階段作業密碼的安全注意事項 134
保護伺服器不受遠端指令及程序影響 135
保護工作站不受遠端指令及程序影響 136
閘道伺服器 136
無線 LAN 通訊. 137

第 15 章 安全跳出程式 139

第 16 章 網際網路瀏覽器的安全注意事項 141

風險：工作站損壞 141
風險：透過對映磁碟機來存取 iSeries 目錄 141
風險：信任已簽章 Applet 142

第 17 章 相關資訊 143

注意事項. 145

商標 146

索引 149

圖

1. 系統安全屬性報告範例 7
2. 進度表設定檔啓動顯示畫面 - 樣本 21
3. 授權清單的專用權限報告 50
4. 顯示授權清單物件報告 50
5. 使用者資訊報告：範例 1 54
6. 使用者資訊報告：範例 2 54
7. 列印使用者設定檔-使用者環境範例 55
8. 使用系統登記資訊 - 範例 69
9. APPC 裝置說明 - 報告樣本 99
10. 配置清單報告 - 範例 100
11. APPC 控制器說明 - 報告樣本 102
12. APPC 線路說明 - 報告樣本 103
13. 使用閘道伺服器的 iSeries 系統 137

表

1. 密碼系統值 13
2. IBM 所提供之設定檔的密碼 18
3. 專用服務工具的密碼 19
4. 登入系統值 19
5. 登入錯誤訊息 20
6. 使用者設定檔工具指令 26
7. 安全審核的工具指令 27
8. 安全報表的指令 29
9. 自行設定系統的指令 32
10. CFGSYSSEC 指令所設定的值 32
11. RVKPUBAUT 指令來設定其公用權限的指令 34
12. 由 RVKPUBAUT 指令來設定其公用權限的指令 34
13. 加密結果 59
14. 使用沿用權限 (USEADPAUT) 範例 65
15. 系統提供的跳出程式 68
16. 使用者設定檔活動的跳出點 73
17. TPN 要求的程式和使用者 78
18. APPC 架構中的安全值 95
19. APPC 安全值及 SECURELOC 值如何一起工作 96
20. 預設使用者參數的可能值 97
21. 範例透通登入要求 97
22. TCP/IP 指令決定要啓動哪些伺服器 108
23. TCP/IP 伺服器的自動啓動值 108
24. 跳出程式樣本來源 139

關於保護 iSeries 安全的要訣及工具 (SC40-1899-07)

在企業組織中，電腦所扮演的角色日新月異，因此，對於舊日所習以為常的許多層面，資訊技術的經理人員、軟體開發人員、安全管理人員和審核人員都必須改採一種全新的觀念和作法。其中包括對於 iSeries 安全問題的考量。

現今的系統所提供的許多新功能迥異於傳統的會計應用程式系統。使用者可使用多種新的方式來進入系統，例如：LAN、撥接線路、無線通訊，以及各種類型的網路。通常他們根本不會看到登入顯示畫面。許多企業組織也試圖透過專用網路或網際網路，使自己成為一個『延伸性的企業』。

於是，系統似乎忽然有了一組全新的門窗設施。系統負責人和安全管理者也必須開始關心，在這個快速變化的環境中，應該如何保護資訊資產。

本資訊提供使用 iSeries 安全特性，以及建立有安全考量的操作程序時的實用建議。本資訊中的建議，適用於一般安全保護基本要求及漏洞的安裝。本資訊不提供 iSeries 可用安全特性的完整說明。若要了解其它選項，或需要更完整的背景資訊，請查閱第 143 頁的第 17 章, 『相關資訊』中的出版品。

本資訊同時說明如何設定並使用安全性工具，這些工具是 OS/400 的一部份。第 25 頁的第 4 章, 『配置 iSeries 使用安全性工具程式』及第 26 頁的『安全指令的指令和功能表』提供關於安全性工具的參考資料。本資訊提供使用工具的範例。

本書的讀者對象

負責處理系統安全事項的**安全主管**或**安全管理者**。這個責任通常包括下列作業：

- 設置和管理使用者設定檔
- 在系統層面設定與安全相關的值
- 管理物件權限
- 執行和監督安全原則

如果您負責一或多個 iSeries 系統的安全性管理，則需要本資訊。本資訊中的指令假設如下：

- 您瞭解基本的 iSeries 作業程序，如登入和使用指令。
- 您瞭解 iSeries 安全保護的基本元素，例如：安全層次、安全系統值、使用者設定檔，以及物件安全。

  註: 第 3 頁的第 1 章, 『iSeries 安全的基本元素』提供這些元素的概略敘述。如果您不熟悉這些基本元素，請先閱讀 iSeries 資訊中心中的*基本安全性與規劃*主題。請參閱第 xii 頁的『先決條件與相關資訊』，取得詳細資訊。
- 您已啓動系統的安全程序，並至少將安全層次 (QSECURITY) 系統值設定為 30。

IBM® 會不斷強化 iSeries 的安全性功能。若要獲取這些加強功能的優點，您應定期地評估您的版次目前可用之累積的修正程式套裝軟體。請查看它是否包含與安全性相關的修正程式。

如何使用本資訊

如果您的系統尚未設置使用安全保護工具，或您是針對較早的版次來安裝「OS/400 的安全性工具箱」，請執行下列動作：

1. 開始閱讀第 9 頁的第 2 章, 『iSeries 安全性精靈與 eServer 安全規劃程式』。它說明如何使用這些特性以選取建議的安全性工具程式，以及如何開始使用它們。
2. 若需要更基礎性的安全資訊，您可以參考 iSeries™ 資訊中心的「安全性參考」資訊。

附註

本資訊有*許*多要訣可以保障 iSeries 安全。但您的系統可能只需要某些範圍內的保護程序。使用本資訊可讓您瞭解可能的安全漏洞，及其對應方法。之後，再將您的精力集中於對您的系統最重要的部份。

先決條件與相關資訊

請使用「iSeries 資訊中心」作爲您查閱 iSeries 技術資訊的起點。

您可以兩種方式存取資訊中心：

- 從下列的網站存取：

  `http://www.ibm.com/eserver/iseries/infocenter`
- 從 *iSeries 資訊中心*, SK3T-0191-04 CD-ROM。這個 CD-ROM 會隨新的 iSeries 硬體或 IBM Operating System/400 軟體升級訂單附送。您也可以從 IBM Publications Center 訂購 CD-ROM：

  `http://www.ibm.com/shop/publications/order`

iSeries 資訊中心包含全新與更新的 iSeries 資訊，例如軟硬體安裝、Linux、WebSphere®、 Java™、高可用性、資料庫、邏輯分割區、CL 指令，以及系統應用程式程式設計介面 (API) 等。此外，它提供了通告器和搜尋器，可協助規劃、疑難排解，以及配置 iSeries 硬體和軟體。

在每一張新的硬體訂單上，您會收到 *iSeries 設定與操作 CD 標籤*, SK3T-0194-02. 此 CD-ROM 中包含 IBM @server IBM e(logo)server iSeries Access for Windows 以及 EZ-Setup 精靈。 iSeries Access Family 提供了強大的用戶端與伺服器功能，可將 PC 連接到 iSeries 伺服器。 EZ-Setup 精靈可以將 iSeries 的許多設定作業自動化。

如何傳送您的意見

您的意見對於我們提供最精確及高品質的資訊有很大的幫助。如果您對本書或任何其他 iSeries 文件有任何意見，請填寫本書最後面的讀者意見表。

- 如果您要郵寄意見表，請使用背面印有地址的讀者意見表。如果您從美國以外的國家郵寄讀者意見表，您可以將意見表利用郵資已付的信件，送交當地 IBM 分公司或 IBM 業務代表。
- 如果您要以傳眞來傳送意見，請使用下列號碼：
  - 美國、加拿大及波多黎各：1-800-937-3430
  - 其它國家：(+1)+507+253-51*92

- 如果您要以電子郵件來傳送意見，請使用下列電子郵件位址：
  - 對書籍的意見：

    RCHCLERK@us.ibm.com
  - iSeries 資訊中心的意見：

    RCHINFOC@us.ibm.com

請記得在郵件中加入下列資訊：
- 書籍名稱或「iSeries 資訊中心」主題。
- 書籍的出版品編號。
- 您有意見的書籍的頁次或主題。

第 1 篇 iSeries 安全的基本功能

第 1 章 iSeries 安全的基本元素

本主題簡要地說明共同作業以提供 iSeries 安全的基本元素。在本書中的其它部份提供進一步的要訣，讓您使用這些安全元素來配合您的組織需求。

安全層次

您可以設定安全層次 (QSECURITY) 系統值來選擇系統所要執行的安全程度。系統提供的安全層次有五種：

層次 10：
系統不強制執行任何安全措施。不需要任何密碼。如果使用者登入時，系統中沒有指定的使用者設定檔，則系統會建立一個。

注意:

從 V4R3 開始，以及在其後續版本中，您不能將 QSECURITY 系統值設定為 10。假設您系統目前安全層次為 10，當您安裝版本 4 版次 3 時，系統將維持層次 10。若您將安全層次變更為其它值，您便無法再變更回層次 10。由於層次 10 不提供任何安全性保護，IBM 不建議您使用安全層次 10。對於安全層次 10 所發生的任何問題，**IBM 不提供支援服務，除非該問題也發生在更高的安全層次**。

層次 20：
系統需要有使用者 ID 和密碼才能登入。安全層次 20 通常也稱為**登入安全**。依預設，所有使用者對於所有物件都有存取權，因為所使用者都具有 *ALLOBJ 特殊權限。

層次 30：
系統需要有使用者 ID 和密碼才能登入。使用者必須擁有使用物件的權限，因為依照預設值，使用者沒有任何權限。這稱為**資源安全**。

層次 40：
系統需要有使用者 ID 和密碼才能登入。除了資源安全之外，系統會提供**整合性保護**功能。整合保護功能 (例如驗證作業系統的介面參數) 的目的，是要保護您的系統和系統中的物件，以免受到有經驗之系統使用者的擅用。對於大部份的安裝作業而言，層次 40 是建議的安全層次。當您收到新的 iSeries 系統而其版次為 R4R5 或更新的版次時，安全層次設定為 40。

層次 50：
系統需要有使用者 ID 和密碼才能登入。系統會強迫執行層次 40 的資源安全與整合性保護，但會新增**加強整合性保護**，例如限制系統狀態程式與使用者狀態程式之間的訊息處理。安全層次 50 的目的，是針對具有較高安全性需求的 iSeries 系統。

註: 層次 50 是 C2 資格認定（以及 FIPS-140 資格認定）的必要層次。

iSeries Security Reference 一書的第 2 章提供有關安全層次及如何從一個安全層次移至另一個安全層次之資訊的說明。

整體設定

您的系統中具有整體設定值，可影響工作進入系統的方式，以及系統使用者所見到的系統外觀。這些設定值包括下列項目：

安全系統值：

安全系統值是用來控制系統上的安全性。這些值可分成四個群組：
- 一般安全系統值
- 其它與安全相關的系統值
- 控制密碼的系統值
- 控制審核的系統值

本書中有許多主題討論特定系統值的安全實作方式。*iSeries Security Reference* 一書的第 3 章說明所有與安全相關的系統值。

網路屬性：

網路屬性控制系統在網路中參與其它系統的方式 (或選擇不參與)。您可以在 *Work Management* 一書中找到網路屬性的詳細資訊。

子系統說明與其它工作管理元素：

工作管理元素決定進入系統的工作數目，以及工作所執行的環境。本資訊有許多主題討論某些工作管理值的安全實作方式。*Work Management* 一書提供有完整的資訊。

通訊配置：

您的通訊配置也會影響工作進入系統的方式。本資訊中許多主題所提供的建議，可在系統參與網路時，協助您保護系統。

使用者設定檔

每個系統使用者都**必須**要有一個使用者設定檔。在使用者可以登入之前，您必須建立使用者設定檔。使用者設定檔也可用來控制如 DASD 及主儲存體傾出等服務工具的存取。請參閱第 55 頁的『管理服務工具』，取得詳細資訊。

使用者設定檔是個有力且富於彈性的工具。它會控制使用者所能執行的動作，並自行設定使用者所見到的系統狀態。*iSeries Security Reference* 一書說明使用者設定檔中所有的參數。

群組設定檔

群組設定檔是一種特殊類型的使用者設定檔。您可以使用一個設定檔來定義使用者群組的權限，而不必個別地提供權限給每個使用者。當您使用複製設定檔功能來建立個別的使用者設定檔時，您都可以使用群組設定檔來作爲型樣，或是在使用「iSeries 領航員」時，您可以使用安全原則功能表來編輯您的使用者權限。

iSeries Security Reference 一書的第 5 章和第 7 章提供規劃和使用群組設定檔的詳細資訊。

資源安全

系統資源安全可讓您定義哪些人可以使用物件，以及如何使用這些物件。存取物件的功能稱為**權限**。當您設定物件權限時，您可能需要小心，在不提供瀏覽及變更系統的權限下，提供足夠的權限給使用者來執行他們的工作。物件權限可提供特定物件許可權給使用者，並可指定使用者可對該物件執行的動作。物件資源可經由特定的詳細使用者權限來限制，如新增記錄或變更記錄。系統資源可讓使用者存取特定之系統定義的權限子集：*ALL、*CHANGE、*USE 以及 *EXCLUDE。

檔案、程式、檔案庫和目錄是需要資源安全保護的最常見系統物件，但對於系統中的任何個別物件，您也可以指定權限。

第 5 章, 『以物件權限來保護資訊資產』說明在系統中設置物件權限的重要性。*iSeries Security Reference* 的第 5 章說明設定資源安全的選項。

限制程式功能

限制存取程式功能可以在您沒有 iSeries 物件以保護程式安全時，提供安全措施來保護程式。在 V4R3 加入限制存取程式功能支援以前，您會透過建立授權清單或其它物件，以及檢查物件的權限來控制程式功能的存取活動，以保護程式。現在，您可以使用程式功能之存取限制，以更簡單的方式來控制應用程式、應用程式組件或程式內功能的存取活動。

您可以利用兩種方式，經由「iSeries 領航員」來管理使用者對於應用程式功能的存取活動。第一個方式是使用「應用程式管理」支援：

1. 在包含您要變更其存取設定之功能的系統上按一下滑鼠右鍵。
2. 選取**應用程式管理**。
3. 如果您是在管理系統上，請選取**區域設定**。否則，請繼續下一步。
4. 選取一個可管理的功能。
5. 如果適用的話，請選取**預設存取**。藉由選取它，您可以依照預設值，容許所有使用者存取此功能。
6. 如果適用的話，請選取**所有物件存取**。藉由選取它，您可以容許所有具有所有物件系統權限的所有使用者存取此功能。
7. 如果適用的話，請選取**自訂**。請使用**自訂存取**對話框上的**新增**及**移除**按鈕，來新增或移除**允許存取**及**拒絕存取**清單中的使用者或群組。
8. 如果適用的話，請選取**移除自訂**。藉由選取它，您將刪除所選功能的任何自訂存取。
9. 按一下**確定**來關閉**應用程式管理**對話框。

第二個管理使用者存取的方法，包含「iSeries 領航員」的「使用者和群組」支援：

1. 在「iSeries 領航員」中，展開**使用者與群組**。
2. 選取**所有使用者**、**群組**或**群組以外的使用者**來顯示使用者與群組的清單。
3. 在使用者或群組上按一下滑鼠右鍵，並選取**內容**。
4. 按一下**功能**。
5. 按一下**應用程式**標籤。
6. 使用此頁來變更使用者或群組的存取設定。

7. 按一下**確定**兩次來關閉**內容**對話框。

請參閱第 133 頁的『iSeries 領航員 安全性』，取得「iSeries 領航員」安全問題的詳細資訊。

如果您是應用程式的設計者，您可以使用程式功能 API 的限制存取來執行下列動作：

- 登記功能
- 取回功能的相關資訊
- 定義哪些人可使用該功能，哪些人不行
- 檢查使用者能否使用該功能

註: 此支援**不能**取代資源安全。限制程式功能的存取並不會阻止使用者從另一介面存取資源（像是檔案或程式）。

要在應用程式中使用此支援，在安裝應用程式時，應用程式提供者必須登記功能。登記的函數會對應到應用程式中某些功能的程式碼區塊。使用者執行應用程式時，應用程式會先呼叫 API 再呼叫程式碼區塊。API 會呼叫檢查使用 API，查看該使用者功能。假設容許該使用者使用登記的功能，則會執行程式碼區塊。假設不容許該使用者使用功能，則會阻止使用者執行程式碼區塊。

註: API 在登記資料庫 (WRKREGINF) 中包含登記的 30 個字元功能 ID。雖然功能 API 的限制存取權要使用的功能 ID 沒有相連結的跳出程式，但跳出程式還是必要的。若要在登錄中登錄任何項目，您**必須**提供一個跳出程式格式名稱。若要這樣做，「登錄功能 API」會建立一個虛擬格式名稱，然後在所有已經登錄的功能使用此虛擬格式名稱。因為這是一個虛擬的格式名稱，所以並不會呼叫任何跳出程式程式。

系統管理者可指定哪些人可存取功能，哪些人不行。管理者可使用 API 來管理程式功能的存取，或使用「iSeries 領航員」應用程式管理 GUI 來管理。*iSeries 系統 API 參照*一書提供有關限制存取程式功能 API 的資訊。有關控制功能的存取的資訊，請參閱第 133 頁的『iSeries 領航員 安全性』。

安全審核

人們基於下述理由審核其系統安全：

- 評估安全性規劃是否完整。
- 確定所規劃的安全性控制適當且可行。這類的審核通常由安全主管來執行，並當作每日安全性管理的一部份。它也可由內部或外部的審核員，當成定期的安全性複查的一部份，但有時會更為詳細。
- 確定系統安全在系統環境變更時仍穩定。影響安全性之變更的部份範例如下：
  - 由系統使用者建立的新物件
  - 進入系統的新使用者
  - 物件所有權的變更（未調整授權）
  - 責任的變更（變更使用者群組）
  - 暫時的權限（未適時撤回）
  - 安裝新產品

- 爲未來事件作準備，諸如安裝新的應用程式、移動到較高的安全層次或設置通訊網路。

此處所說明的技術適用於所有上述的狀況。審核的事項及頻率取決於您組織的大小及安全性需求。

安全性審核包括使用系統上的指令和存取日誌資訊。您可以建立一個特殊的設定檔，由其他人用來進行您系統的安全性審核。審核員設定檔需要 *AUDIT 特殊權限才能變更系統的審核性質。本章所建議的部份審核作業需要具有 *ALLOBJ 及 *SECADM 特殊權限的使用者設定檔。當審核期間結束時，將審核員設定檔的密碼設定爲 *NONE。

有關安全性審核的更多明細，請參閱 *Security Reference* 一書的第 9 章。

範例：系統安全屬性報告

圖 1 顯示來自「列印系統安全屬性 (PRTSYSSECA)」指令的輸出範例。報表顯示安全相關系統值的設定值，以及正常安全性基本要求下爲系統所建議的網路屬性。它還顯示您系統上目前的設定值。

註: 報表上的*現行值*一欄，會顯示您的系統上目前的設定。以此設定與建議值相比較以了解安全性的問題所在。

```
系統安全屬性

系統值
名稱            現行值                    建議值
QALWOBJRST      *NONE                     *NONE
QALWUSRDMN      *ALL                      QTEMP
QATNPGM         QEZMAIN   QSYS            *NONE
QAUDENDACN      *NOTIFY                   *NOTIFY
QAUDFRCLVL      *SYS                      *SYS
QAUDCTL         *AUDLVL                   *AUDLVL   *OBJAUD
QAUDLVL         *SECURITY                 *AUTFAIL  *CREATE
                                          *DELETE   *SECURITY
                                          *SAVRST   *NOQTEMP
```

圖 1. 系統安全屬性報告範例 (1/4)

```
QAUTOCFG        0                         0
QAUTORMT        1                         0
QAUTOVRT        9999                      0
QCMNRCYLMT      0 0                       0 0
QCRTAUT         *CHANGE                   檔案庫層次的控制。
QCRTOBJAUD      *NONE                     檔案庫層次的控制。
QDEVRCYACN      *DSCMSG                   *DSCMSG
QDSCJOBITV      120                       120
QDSPSGNINF      1                         1
QINACTITV       60                        60
QINACTMSGQ      *ENDJOB                   *ENDJOB
QLMTDEVSSN      0                         1
QLMTSECOFR      0                         1
QMAXSGNACN      2                         3
QMAXSIGN        3                         3
```

圖 1. 系統安全屬性報告範例 (2/4)

```
QPWDEXPITV       60                 60
QPWDLMTAJC       1                  1
QPWDLMTCHR       *NONE              AEIOU@$#
QPWDLMTREP       1                  2
QPWDLVL          0
QPWDMAXLEN       8                  8
QPWDMINLEN       6                  6
QPWDPOSDIF       1                  1
QPWDRQDDGT       1                  1
QPWDRQDDIF       0                  1
QPWDVLDPGM       *NONE              *NONE
QRETSVRSEC       0                  0
QRMTIPL          0                  0
QRMTSIGN         *FRCSIGNON         *FRCSIGNON
QSECURITY        50                 50
QSHRMEMCTL       1                  0
QSRVDMP          *DMPUSRJOB         *NONE
QUSEADPAUT       *NONE              CRTAUTL AUTL(QUSEADPAUT) AUT(*EXCLUDE)
                                    CHGOBJOWN OBJ(QUSEADPAUT) OBJTYPE(*AUTL)
                                    CHGSYSVAL SYSVAL(QUSEADPAUT) VALUE(QUSEADPAUT)
QVFYOBJRST       1                  3
```

圖 1. 系統安全屬性報告範例 (3/4)

```
系統安全屬性

網路屬性
名稱             現行值             建議值
DDMACC           *OBJAUT             *REJECT
JOBACN           *FILE               *REJECT
PCSACC           *OBJAUT             *REJECT
```

圖 1. 系統安全屬性報告範例 (4/4)

第 2 章 iSeries 安全性精靈與 eServer 安全規劃程式

iSeries 伺服器「安全精靈」和「eServer 安全規劃程式」兩個工具，可以協助您決定要在 iSeries 伺服器中運用的安全值。使用「iSeries 領航員」中的「iSeries 伺服器安全精靈」，將可以根據您選定的回答，產生反映您的安全需求的報告。接著您可以使用它來配置您的系統安全。

請使用「iSeries 安全精靈」或「eServer 安全規劃程式」，來協助您規劃及實施 iSeries 伺服器的基本安全原則。這兩種工具的目標，是讓您更容易在系統上實施及管理安全性。OS/400® 中所提供的精靈，會問您許多關於伺服器環境的高階問題，並根據您的答案提供一組精靈可以立即套用到您系統的建議。

「eServer 安全規劃程式」是「安全精靈」的線上版本。它可以讓您根據安全需求選取選項，然後提供一份報表，建議您需要哪些特性來保護您的網站安全。

「eServer 安全規劃程式」是精靈的網路型版本。它提供在您的系統上實施安全措施的建議，與精靈的功能相同。不過，顧問無法套用建議。反之，它會根據您回覆給顧問的答案，產生一份系統安全值及其它您應該在系統上套用的其它屬性清單。

安全精靈

決定要為企業採用哪些 iSeries 安全系統值是頗令人困擾的。假設您是 iSeries 伺服器安全施行的新手，或 iSeries 伺服器的執行環境最近有變更，則「安全精靈」可協助您做決定。

精靈是什麼？
- 精靈是一種工具，可讓初學者在系統上使用來安裝或配置事物。
- 精靈會詢問問題以從使用者取得資訊。每一個問題的回應會決定下一個要詢問的問題為何。
- 當精靈問完所有的問題以後，使用者便會見到完成的對話框。接著使用者會按下**完成**按鈕，以安裝或配置該項目。

安全精靈目標

「安全精靈」的目標是基於使用者回應來配置下列項目。
- 安全相關的系統值與網路屬性。
- 監督系統的安全相關報表
- 產生「管理者資訊報表」以及「使用者資訊報表」：
  – 「管理者資訊報表」含有建議的安全設定，以及實施這些建議前應當遵循的程序。
  – 「使用者資訊報表」含有可用於企業安全政策的資訊。例如，此報告含有密碼組合規則。
- 提供系統上各種安全相關項目的建議設定值。

「安全精靈」目標
- 「安全精靈」的目標是：
  – 根據使用者對精靈問題的回答決定系統安全設定值，然後建置適當的設定值。
  – 精靈會產生詳細的資訊報表，包括下列各項。

- 說明精靈建議的報表。
- 詳細說明在實行之前應該遵循的程序的報表。
- 列有要分送給系統使用者的相關資訊的報表。
- 這些項目會在您的系統上實施基本安全政策。
- 精靈會建議您排程以定期執行審核異動記載報告。排程之後，這些報表有助於：
  - 確保遵循安全政策。
  - 確保只在您的同意下變更政策。
  - 排定報告的時程表，以監督您系統中的安全相關事件。
- 此精靈可讓您儲存建議，或套用部份或全部建議到系統中。

註: 「安全精靈」在同一個系統上可以使用一次以上，讓可能擁有舊安裝的使用者來檢視他們的現行安全設定。「安全精靈」從 V3R7 系統 (開始引進「iSeries 領航員」) 以上即可使用。

若要使用「iSeries 領航員」，您的 Windows® 95/NT PC 上必須安裝 IBM iSeries Access for Windows，並且該 PC 上要有 iSeries 伺服器連線。「精靈」的使用者必須連接 iSeries 伺服器。使用者的使用者 ID 必須具有 *ALLOBJ、 *SECADM、*AUDIT 和 *IOSYSCFG 特殊權限。關於 Windows 95/NT PC 與 iSeries 系統連接的說明，請參閱資訊中心中的 IBM iSeries Access for Windows 主題 (詳細請參閱第 xii 頁的『先決條件與相關資訊』)。

若要**存取安全精靈**，請執行下列步驟：

1. 在「iSeries 領航員」中，展開您的伺服器。
2. 在**安全**上按一下滑鼠右鍵，並選取**配置**。
   - 當使用者啓動「iSeries 領航員」的**安全**選項時，會傳送一個要求到 iSeries 伺服器以檢查使用者的特殊權限。
   - 萬一使用者沒有必要的特殊權限 (*ALLOBJ, *AUDIT, *IOSYSCFG, *SECADM)，他們將無法看見**配置**選項，且無法存取「安全精靈」。
3. 假設使用者有必要的權限：
   - 擷取先前的精靈回應。
   - 擷取現有的安全設定值。

「安全精靈」會提供您三個歡迎光臨螢幕的其中之一。您會見到哪個螢幕，取決於下面中哪一項條件存在：

- 精靈未曾針對目標 iSeries 伺服器執行。
- 這個精靈先前曾執行過，而安全變更已延緩實施。
- 這個精靈先前曾執行過，而安全變更已開始實施。

如果不是使用「iSeries 領航員」，您還是可以取得安全需求規劃的協助。「eServer 安全規劃程式」是「安全精靈」的線上版本，不過兩者有一個差異存在。「安全顧問」不會自動配置您的系統。它只能根據您的回答，產生一份安全選項的建議報表。若要存取「eServer 安全規劃程式」，請至「eServer 資訊中心」：

`http://publib.boulder.ibm.com/eserver/`

eServer 安全規劃程式

「eServer 安全規劃程式」是「安全精靈」的線上版本。它會提出和「安全精靈」相同的問題，並根據您的回答產生相同的建議。這兩個工具的主要差異在於：

- 「eServer 安全規劃程式」**不會**--
  - 產生報告。
  - 比較現行設定值與建議設定值。
  - 自動設定任何系統值。
- 您無法從「eServer 安全規劃程式」套用建議。

「eServer 安全規劃程式」會產生一個 CL 程式，供您根據本身的需要剪貼與編輯，將安全配置自動化。您也可從「eServer 安全規劃程式」直接鏈結到 iSeries 伺服器文件。此文件會提供系統值或報告的相關資訊，協助您判斷該設定是否適合您的環境。

若要存取「eServer 安全規劃程式」，請將網際網路瀏覽器指向下列 URL：

`http://publib.boulder.ibm.com/eserver/`

第 3 章 控制交談式登入

如果您考慮讓使用者在進入您的系統時受到限制，您可以由顯而易見的「登入」顯示畫面來開始著手。您可以使用下列選項，讓其他人比較不容易使用「登入」顯示畫面來登入您的系統。

設定密碼規則

若要保護您的系統登入安全，可以執行下列動作：

- 設定一個原則，說明不能使用可有可無的密碼，同時也不能共用密碼。
- 設定系統值可協助您強化這個作用。表 1 顯示建議您使用的系統值設定。

表 1 中之值的組合相當具有限制性，它的目的是要明顯降低通常碼流於可有可無的可能性。不過，您的使用者可能會覺得選取符合這些限制的密碼很困難，很容易使人感到挫折與不便。

請您考慮為使用者提供下列資料：

1. 一份密碼基準列示。
2. 無效密碼的範例。
3. 如何構想好密碼的建議事件。

執行「配置系統安全 (CFGSYSSEC)」指令來設定這些值。使用「列印系統安全屬性 (PRTSYSSECA)」指令來列印這些系統值的現行設定。

iSeries Security Reference 書籍的第三章。第 32 頁的『配置系統安全指令所設定的值』提供有關 CFGSYSSEC 指令的資訊。

表 1. 密碼系統值

系統值名稱	說明	建議值
QPWDEXPITV	系統使用者必須每隔多久變更他們的密碼。您可以在使用者設定檔中，指定不同的值給個別使用者。	60 (天)
QPWDLMTAJC	系統是否不容許使用相同的相鄰字元。	1 (是)
QPWDLMTCHR	密碼不可使用的字元。[2]	AEIOU#$@
QPWDLMTREP	系統是否不容許在密碼中重複出現相同字元。	2 (不容許連續)
QPWDLVL	使用者設定檔密碼限制為 10 個字元，還是最多 128 個字元。	0[3]
QPWDMAXLEN	密碼中的最大字元數。	8
QPWDMINLEN	密碼中的最小字元數。	6
QPWDPOSDIF	密碼中的每一個字元，是否都必須不同於舊有密碼之相同位置的字元。	1 (是)
QPWDRQDDGT	密碼是否至少必須有一個數值字元。	1 (是)
QPWDRQDDIF	使用者重新使用相同密碼必須等待的時間。[2]	5 或以下 (到期間隔) [1]
QPWDVLDPGM	呼叫哪些跳出程式來驗證新指定的密碼。	*NONE

表 1. 密碼系統值 (繼續)

<table>
<tr><th>系統值名稱</th><th>說明</th><th>建議值</th></tr>
<tr><td colspan="3">

註:

1. QPWDEXPITV 系統值指定您必須多久變更一次密碼，例如，每隔 60 天。這是**到期間隔**。QPWDRQDDIF 系統值指定在您可以使用同一個密碼之前，必須經過多少個到期間隔。*iSeries Security Reference* 一書的第 3 章提供這些系統值如何共同作業的詳細資訊。
2. 未強制 QPWDLMTCHR 於密碼層次 2 或 3。詳細請參閱『密碼層次』。
3. 請參照『規劃密碼層次變更』以判定密碼層次符合您的需求。

</td></tr>
</table>

密碼層次

從作業系統的 V5R1 開始，QPWDLVL 系統值提供更多的密碼安全性。在先前的版次中，限制使用者密碼不得超過 10 個字元，且須取自受限制的字元範圍。現在，使用者可選取最多可達 128 個字元的密碼，取決於其系統所設定的密碼層次。密碼層次為：

- **層次 0**：系統是以這個層次出貨。在層次 0，密碼長度不得超過 10 個字元，且只能為 A-Z、0-9、#、@、$ 及 _ 字元。層次 0 的密碼比較高層次之密碼安全性低。
- **層次 1**：規則與密碼層次 0 相同，但不儲存 iSeries Support for Windows Network Neighborhood (此後稱為 iSeries NetServer) 的密碼。
- **層次 2**：密碼在此層次是安全的。這個層次可以作為測試之用。若密碼等於或小於 10 個字元，就會儲存給層次 0 或 1 的使用者，並使用字集作為層次 0 或 1 密碼。此層次的密碼 (或密碼詞組) 具有下列性質：
  - 最大長度可達 128 個字元。
  - 可由任何可用的鍵盤字元所組成。
  - 不可全部都為空白；會自密碼尾端除去空白。
  - 區分大小寫。
- **層次 3**：此層次的密碼極為安全，並利用最進階的加密演算法。此層次的密碼與層次 2 的密碼具有相同的性質。不會在此層次儲存 iSeries NetServer 的密碼。

只有在網路上的每一個系統均符合此基準，才使用密碼層次 2：

- 作業系統是 V5R1 或以上的版本
- 密碼層次設為 2 或 3

同樣地，使用者必須使用相同的密碼層次登入。密碼層次是全域的；使用者無法自行選擇他們認為安全的密碼層次。

規劃密碼層次變更

變更密碼層次應謹慎規劃。若未確實地規劃密碼層次變更，可能導致其他系統作業失敗，或使用者可能無法登入系統。在變更 QPWDLVL 系統值之前，請確定您已使用 SAVSECDTA 或 SAVSYS 指令儲存您的安全性資料。若您有現行的備份，假設您要返回較低的密碼層次，則您將可重設所有使用者設定檔的密碼。

當密碼層次 (QPWDLVL) 系統值設定為 2 或 3 時，您在系統及與系統有介面連接之用戶端上使用的產品可能會有問題。任何的產品或用戶端都以加密的形式將密碼傳送

給系統，而非以使用者在登入螢幕中鍵入的文字傳送，因此產品或用戶端必須升級為使用 QPWDLVL 2 或 3 的新密碼加密規則。傳送加密的密碼即為一般所知的**密碼替代**。

密碼替代可用來防止密碼在透過網路傳輸期間被抓取。由舊版用戶端產生的密碼替代，不支援 QPWDLVL 2 或 3 的新演算法，就算是正確的字元仍無法接受。這也套用到任何 iSeries 對 iSeries 同層級存取，它利用加密的值讓系統彼此鑑別。

因為某些受影響的產品 (如 Java 工具箱) 是被當成中介軟體來提供。納入前版產品的非 IBM 產品將無法正常運作，必須等到它們使用介體的更新版重新建置後才能正常運作。

由上述狀況及其他實務可知，在變更 QPWDLVL 系統值之前謹慎規劃的必要性。

將 QPWDLVL 由 0 變更到 1 的注意事項

密碼層次 1 可讓不需與 Windows 95/98/ME AS/400® Client Support for Windows Network Neighborhood (iSeries NetServer) 產品通訊的系統，自系統中將 iSeries NetServer 密碼移除。從系統消除不必要的加密密碼會增加系統整體的安全性。

在 QPWDLVL 1，所有現行及 V5R1 版本前的密碼替代和密碼鑑別機制都將繼續運作。除了需要 iSeries NetServer 密碼的功能和服務之外，將會有一個極小的潛在斷層。

將 QPWDLVL 由 0 或 1 變更到 2 的注意事項

密碼層次 2 引進區分大小寫且長度最多可達 128 個字元的密碼用法 (也稱為密碼詞組)，且提供回復到 QPWDLVL 0 或 1 的最大能力。

與系統的密碼層次無關，每當變更密碼或使用者登入系統時，便會建立密碼層次 2 及 3 的密碼。當系統仍為密碼層次 0 或 1 時，建立層次 2 及 3 的密碼，可協助您為變更至密碼層次 2 或 3 作準備。

在變更 QPWDLVL 為 2 之前，您應使用 DSPAUTUSR 或 PRTUSRPRF TYPE(*PWDINFO) 指令，來尋找沒有可在密碼層次 2 使用之密碼的使用者設定檔。根據這些指令找到的設定檔，您可能希望使用下列其中一項機制來將密碼層次 2 及 3 的密碼新增到設定檔。

- 使用 CHGUSRPRF 或 CHGPWD CL 指令或 QSYCHGPW API 來變更使用者設定檔的密碼。這將造成系統變更在密碼層次 0 及 1 可用的密碼；且系統還會建立兩組相同之區分大小寫的密碼，該密碼可在密碼層次 2 及 3 使用。密碼皆為大寫及皆為小寫的版本是為密碼層次 2 及 3 所建立的。

  例如，變更密碼為 C4D2RB4Y 導致系統產生 C4D2RB4Y 及 c4d2rb4y 密碼層次 2 的密碼。
- 以清楚呈現文字之密碼的機制登入系統 (不使用密碼替代)。若密碼有效且使用者設定檔中沒有可在密碼層次 2 及 3 使用的密碼，則系統會建立兩組相同且區分大小寫的密碼，並可在密碼層次 2 及 3 使用。密碼皆為大寫及小寫的版本是為密碼層次 2 及 3 所建立的。

每當使用者設定檔沒有可用於密碼層次 0 及 1 的密碼，或當使用者嘗試透過使用密碼替代的產品登入時，則沒有可用於密碼層次 2 或 3 的密碼將會是一個問題。在這些情況下，使用者在密碼層次變更為 2 時，將無法登入。

若使用者設定檔沒有可用於密碼層次 2 及 3 的密碼，而使用者設定檔有可用於密碼層次 0 及 1 的密碼，且使用者透過傳送清楚呈現文字密碼的產品登入，則系統會驗證密碼層次 0 的密碼，並為使用者設定檔建立兩個密碼層次 2 的密碼 (如上所述)。後續的登入將會依密碼層次 2 的密碼驗證。

若用戶端／服務尚未更新為使用新密碼（密碼詞組）替代架構，則任何使用密碼替代的用戶端／服務將無法在 QPWDLVL 2 正確運作。管理者應檢查用戶端／服務是否尚未更新為必要的新密碼替代架構。

使用密碼替代的用戶端／服務包括：

- TELNET
- iSeries Access
- iSeries 主電腦伺服器
- QFileSrv.400
- iSeries NetServer 列印支援
- DDM
- DRDA®
- SNA LU6.2

我們強烈建議在變更至 QPWDLVL 2 之前應先儲存安全性資料。如此可幫助您在必要時轉移回 QPWDLVL 0 或 1。

我們建議在尚未於 QPWDLVL 2 進行某些測試前，不要先行變更如 QPWDMINLEN 及 QPWDMAXLEN 等系統值。這將有助於必要時轉移回 QPWDLVL 1 或 0。然而，QPWDVLDPGM 系統值在系統允許 QPWDLVL 變更為 2 之前，必須指定為 *REGFAC 或 *NONE。因此，若您使用密碼驗證程式，您會希望使用 ADDEXITPGM 指令，寫入一個可為 QIBM_QSY_VLD_PASSWRD 跳出程式登錄的新程式。

QPWDLVL 2 仍支援 iSeries NetServer 密碼，因此需要使用 iSeries NetServer 密碼的任何功能／服務仍可正確運作。

一旦管理者在 QPWDLVL 2 順利執行系統之後，便可開始變更密碼系統值為使用較長的密碼。然而，管理者需要明白較長的密碼將有下列效果：

- 若指定大於 10 個字元的密碼，則會清除密碼層次 0 及 1。若系統返回密碼層次 0 或 1，此使用者設定檔將無法登入。
- 若密碼中有特殊字元或並非遵循簡式物件名稱的撰寫規則 (區分大小寫除外)，則會清除密碼層次 0 及 1。
- 若指定大於 14 個字元的密碼，則會清除使用者設定檔的 iSeries NetServer 密碼。
- 密碼系統值僅套用於新密碼層次 2 值，且不會套用於系統產生的密碼層次 0 及 1 的密碼，或 iSeries NetServer 密碼值 (若有產生的話)。

將 QPWDLVL 由 2 變更到 3 的注意事項

在 QPWDLVL 2 執行系統一段時間之後，管理者可考慮提升到 QPWDLVL 3，以將密碼安全性保護放至最大。

在 QPWDLVL 3，會清除所有的 iSeries NetServer 密碼，因此系統在不需使用 iSeries NetServer 密碼之後，才能將系統移動到 QPWDLVL 3。

在 QPWDLVL 3，會清除所有密碼層次 0 及 1 的密碼。管理者可使用 DSPAUTUSR 或 PRTUSRPRF 指令來尋找沒有密碼層次 2 或 3 密碼的使用者設定檔。

變更到較低的密碼層次

在可能時回復到較低的 QPWDLVL 值，並不是完全不麻煩的作業。一般而言，這應是從低的 QPWDLVL 值到較高的 QPWDLVL 值的單向旅程。然而，仍有些情況必須復原較低的 QPWDLVL 值。

下列章節將會逐一討論需要回到較低之密碼層次的作業。

將 QPWDLVL 由 3 變更到 2 的注意事項: 此變更十分簡單。一旦設定 QPWDLVL 為 2，管理者需要決定使用者設定檔是否要有 iSeries NetServer 密碼，或密碼層次 0 或 1 的密碼，若有此需要，請變更使用者設定檔的密碼為允許的值。

此外，密碼系統值必須變更回 iSeries NetServer 及密碼層次 0 或 1 密碼相容的值 (若需要這些密碼)。

將 QPWDLVL 由 3 變更到 1 或 0 的注意事項: 因為有潛在有極高的可能會對系統造成問題 (就像因為已清除密碼層次 0 及 1 的密碼，將造成無人可登入的情況)，所以不會直接支援此項變更。若要從 QPWDLVL 3 變更為 QPWDLVL 1 或 0，系統必須先進行中間變更為 QPWDLVL 2。

將 QPWDLVL 由 2 變更到 1 的注意事項: 在變更 QPWDLVL 到 1 之前，管理者應使用 DSPAUTUSR 或 PRTUSRPRF TYPE(*PWDINFO) 指令來尋找沒有密碼層次 0 或 1 的密碼之使用者設定檔。若使用者設定檔在變更 QPWDLVL 後需要密碼，管理者應確定已使用下列其中一種機制，建立設定檔的密碼層次 0 及 1 之密碼：

- 使用 CHGUSRPRF 或 CHGPWD CL 指令或 QSYCHGPW API 來變更使用者設定檔的密碼。這將造成系統變更在密碼層次 2 及 3 可用的密碼；且系統還建立在密碼層次 0 及 1 可用的一個相同但大寫的密碼。只有符合下列狀況，系統才能建立密碼層次 0 及 1 的密碼：
  - 密碼長度等於或小於 10 個字元。
  - 可將密碼轉換為大寫的 EBCDIC 字元、A-Z、0-9、@、#、$ 及底線。
  - 密碼並非以數字或底線字元開頭。

  例如，變更密碼為 RainyDay 將導致系統產生一個密碼層次 0 及 1 的密碼 RAINYDAY。但將密碼值變更為「Rainy Days In April」，則系統會清除密碼層次 0 及 1 的密碼 (因為密碼太長且中間有空白)。

  若無法建立密碼層次 0 或 1 的密碼，並不會產生訊息或指示。
- 以清楚呈現文字之密碼的機制登入系統 (不使用密碼替代)。若為有效的密碼，且使用者設定檔沒有可用於密碼層次 0 及 1 的密碼，則系統會建立一個在密碼層次 0 及 1 可用的一個相同但大寫的密碼。只有符合上述的狀況，系統才能建立密碼層次 0 及 1 的密碼。

然後管理者可將 QPWDLVL 變更為 1。當變更為 QPWDLVL 1 生效時 (下一次 IPL)，會清除所有的 iSeries NetServer 密碼。

將 QPWDLVL 由 2 變更到 0 的注意事項: 與 QPWDLVL 由 2 變更為 1 的注意事項相同，但當變更生效時會保留所有的 iSeries NetServer 密碼。

將 QPWDLVL 由 1 變更到 0 的注意事項: 在變更 QPWDLVL 為 0 之後，管理者應使用 DSPAUTUSR 或 PRTUSRPRF 指令來尋找任何沒有 iSeries NetServer 密碼的使用者設定檔。若使用者設定檔需要 iSeries NetServer 密碼，則可透過以清楚呈現文字的機制，變更使用者密碼或登入來建立它。

然後管理者可將 QPWDLVL 變更為 0。

變更公開的密碼

您可以執行下列動作，來關閉某些可能存在於系統的 iSeries 伺服器已知進入點。

__ 步驟 1. 確定沒有使用者設定檔仍擁有預設密碼 (等於使用者設定檔名稱)。您可以使用「分析預設密碼 (ANZDFTPWD)」指令。(請參閱第 22 頁的『避免預設密碼』。)

__ 步驟 2. 嘗試使用表 2 中所示的使用者設定檔和密碼的組合來登入您的系統。這些密碼是公開的，任何人試圖進入您的系統時，首先會選擇這些密碼。如果您可以登入，請使用「變更使用者設定檔 (CHGUSRPRF)」指令，將密碼變更為建議值。

__ 步驟 3. 啓動「專用服務工具 (DST)」，並嘗試以表 2 中所示的密碼來登入。請參照「iSeries 資訊中心 --> 安全性 --> 服務工具」。請參閱第 xii 頁的『先決條件與相關資訊』，以獲得存取「iSeries 資訊中心」的資訊。

__ 步驟 4. 如果您可以使用下列中的任何參數來登入 DST，則應變更密碼。「iSeries 資訊中心 --> 安全性 --> 服務工具」提供了如何變更服務工具使用者 ID 和密碼的詳細指示。請參閱第 xii 頁的『先決條件與相關資訊』，以獲得存取「iSeries 資訊中心」的資訊。

__ 步驟 5. 最後，請確定如果您只在「登入」畫面中按下 Enter 鍵，而不輸入使用者 ID 和密碼，即無法登入。請嘗試多個不同的顯示畫面。如果您未在「登入」顯示畫面輸入資訊，而仍然可以登入，請執行下列動作：

- 變更至安全層次 40 或 50 (QSECURITY 系統值)。

  註: 當您增加至安全層次 40 或 50 時，應用程式的執行方式可能會不同。
- 變更交談式子系統的所有工作站登錄，以指向指定 USER(*RQD) 的工作說明。

表 2. IBM 所提供之設定檔的密碼

使用者 ID	密碼	建議值
QSECOFR	QSECOFR[1]	一個並非可有可無的值，只讓安全管理者知道。**記下您選取的密碼，並將它儲存在安全的地方。**
QSYSOPR	QSYSOPR	*NONE[2]
QPGMR	QPGMR	*NONE[2]
QUSER	QUSER	*NONE[2, 3]
QSRV	QSRV	*NONE[2]
QSRVBAS	QSRVBAS	*NONE[2]

表 2. IBM 所提供之設定檔的密碼 (繼續)

使用者 ID	密碼	建議值

註:

1. 系統出貨時，QSECOFR 的*設定密碼到期*值會設為 *YES。您第一次登入新系統時，必須變更 QSECOFR 密碼。
2. 系統需要這些使用者設定檔來執行系統功能，但您不應該讓使用者透過這些設定檔來登入。以 V3R1 或以後的版次來安裝的新系統，這個密碼的出貨值是 *NONE。

   當您執行 CFGSYSSEC 指令時，系統會將這些密碼設定為 *NONE。
3. 如果要使用 TCP/IP 來執行 iSeries Access for Windows，必須啓用 QUSER 使用者設定檔。

表 3. 專用服務工具的密碼

DST 層次	使用者 ID	密碼	建議值
基本功能	11111111	11111111	一個並非可有可無的值，只讓安全管理者知道。[2]
完整功能	22222222	22222222[3]	一個並非可有可無的值，只讓安全管理者知道。[2]
安全功能	QSECOFR	QSECOFR[3]	一個並非可有可無的值，只讓安全管理者知道。[2]
服務功能	QSRV	QSRV[3]	一個並非可有可無的值，只讓安全管理者知道。[2]

註:

1. 只有 PowerPC® AS (RISC) 版次的作業系統需要使用者 ID。
2. 如果您的客戶服務代表必須使用這個使用者 ID 和密碼，在客戶服務代表離開後，請將這個密碼的值變更為新的值。
3. 服務工具使用者設定檔在第一次使用後便到期。

註: 僅可以鑑別的裝置來變更 DST 密碼。亦適用於所有密碼與對應的使用者 ID 為相同時。有關鑑別的裝置之資訊，請參閱「iSeries 資訊中心」中的「作業主控台」設定資訊。

設定登入值

表 4 顯示設定之後，可讓未獲授權的使用者更難於登入系統的若干值。如果您執行 CFGSYSSEC 指令，它會將這些系統值設定為建議值。您可以在 *iSeries Security Reference* 一書的第 3 章，找到這些系統值的詳細資訊。

表 4. 登入系統值

系統值名稱	說明	建議設定
QAUTOCFG	系統是否會自動配置新裝置。	0 (否)
QAUTOVRT	如果沒有可用的裝置時，系統將自動建立的虛擬裝置說明數目。	0
QDEVRCYACN	在發生錯誤後又重新連接裝置時，系統將執行哪些動作。[1]	*DSCMSG
QDSCJOBITV	在結束已切斷的工作之前，系統要等待多久。	120

表 4. 登入系統值 (繼續)

系統值名稱	說明	建議設定
QDSPSGNINF	當使用者登入時，系統是否會顯示先前的登入活動的相關資訊。	1 (是)
QINACTITV	當交談工作在不作用的狀態時，系統要等多久才採取動作。	60
QINACTMSGQ	在到達 QINACTITV 時間期間之後，系統會執行什麼動作。	*ENDJOB
QLMTDEVSSN	系統是否容許一個使用者同時在多個工作站登入。	1 (是)
QLMTSECOFR	具有 *ALLOBJ 或 *SERVICE 特殊權限的使用者是否只能在特定的工作站登入。	1 (是)[2]
QMAXSIGN	連續不正確登入嘗試 (使用者設定檔或密碼不正確) 的最大次數。	3
QMAXSGNACN	在到達 QMAXSIGN 限制之後，系統會執行什麼動作。	3 (停用使用者設定檔和裝置)

註:

1. 在明確指定階段作業的裝置說明之後，系統可以切斷再重新連接 TELNET 階段作業。
2. 如果您將系統值設定為 1 (是) ，您將需要明確地授與使用者對於裝置的 *ALLOBJ 或 *SERVICE 特殊權限。執行這個動作的最簡單方法，是提供 QSECOFR 使用者設定檔對於特定裝置的 *CHANGE 權限。

變更登入錯誤訊息

在電腦駭客順利侵入某個系統後，他們通常會想要取得相關訊息。例如，當「登入」顯示畫面出現密碼不正確的錯誤訊息時，駭客們即可以假設使用者 ID 是正確的。不過，您可以使用「變更密碼說明 (CHGMSGD)」指令，變更兩個登入錯誤訊息的文字來阻擾這些駭客。表 5 顯示建議使用的文字。

表 5. 登入錯誤訊息

訊息 ID	出貨文字	建議文字
CPF1107	CPF1107 - 使用者設定檔的密碼不正確。	登入資訊不正確。 **註:** 請勿在訊息文字中併入訊息 ID。
CPF1120	CPF1120 - 使用者 XXXXX 不存在。	登入資訊不正確。 **註:** 請勿在訊息文字中併入訊息 ID。

排定使用者設定檔的可用性

您可以讓某些使用者設定檔只能在一天中的某些時刻或一星期中的某幾天使用。例如，如果有某個設定檔專為安全審核人員而設置，您可以只在審核人員排定工作的時間才啓用這個使用者設定檔。您也可以使用 *ALLOBJ 特殊權限，在不工作的時間內停用使用者設定檔 (包括 QSECOFR 使用者設定檔)。

您可以使用「變更啓動進度表登錄 (CHGACTSCDE)」指令，將使用者設定檔設置為自動啓用和停用。對於您要排入進度表的每個使用者設定檔，您都可以建立一個登錄，用來定義使用者設定檔的進度表。

例如，如果您只要在早上 7 點到晚上 10 點之間，讓 QSECOFR 設定檔成爲可用狀態，您可以在 CHGACTSCDE 顯示畫面中鍵入下列內容：

```
                              變更啓動進度表登錄 (CHGACTSCDE)

請鍵入選項，然後按 Enter 鍵。

使用者設定檔 . . . . . . . . . . . > QSECOFR       名稱
啓用時間 . . . . . . . . . . . . . > '7:00'        時間, *NONE
停用時間 . . . . . . . . . . . . . > '22:00'       時間, *NONE
天數 . . . . . . . . . . . . . . . > *MON          *ALL, *MON, *TUE, *WED...
                                   > *TUE
                                   > *WED
                                   > *THU
              + 尚有其餘值         > *FRI
```

圖 2. 進度表設定檔啓動顯示畫面 - 樣本

事實上，您可以只在每天極有限的時數內，讓 QSECOFR 設定檔成爲可用狀態。大部份的系統功能，您都可以使用另一個 *SECOFR 類別的使用者設定檔來執行。如此即可避免讓駭客取得公開的使用者設定檔。

您可以使用「顯示審核異動記載登錄 (DSPAUDJRNE)」指令，定期地列印 CP (變更設定檔) 審核異動記載登錄。您可以使用這些登錄來驗證系統是否根據您的計劃進度來啓用和停用使用者設定檔。

另一個檢查是否根據排定的進度表來停用使用者設定檔的方法，是使用「列印使用者設定檔 (PRTUSRPRF)」指令。當您將報告類型指定爲 *PWDINFO 時，報告中會包括每個選定之使用者設定檔的狀態。例如，如果您定期地停用具有 *ALLOBJ 特殊權限的所有使用者設定檔，您可以排定在設定檔停用後，立即執行下列指令：

```
PRTUSRPRF TYPE(*PWDINFO) SELECT(*SPCAUT) SPCAUT(*ALLOBJ)
```

移除非作用中的使用者設定檔

您的系統應該只包含必要的使用者設定檔。如果某個使用者已離開，或轉任企業內的其它工作，因而不再需要其使用者設定檔，請除去該使用者設定檔。如果某個使用者長期不在職，請停用 (停止) 其使用者設定檔。不必要的使用者設定檔，有可能讓他人在未獲授權的情況下進入您的系統。

自動停用使用者設定檔

您可以使用「分析設定檔活動 (ANZPRFACT)」指令，定期地停用不作用時間已達指定天數的使用者設定檔。您在使用 ANZPRFACT 指令時，指定系統所要尋找的不作用天數。系統會尋找上次的使用日期、復置日期，以及使用者設定檔的建立日期。

在您指定好 ANZPRFACT 指令的值以後，系統會排定一項每週執行一次的工作，在 1 a.m. 執行 (從第一次指定這個值之後的第二天開始)。這個工作會檢查所有設定檔，並停用不作用的設定檔。除非您要變更不作用的天數，否則您不需要重新使用 ANZPRFACT 指令。

您可以使用「變更作用設定檔列示 (CHGACTPRFL)」指令，讓某些設定檔不受 ANZPRFACT 指令的影響。 CHGACTPRFL 指令可建立一個無法停用的使用者設定檔列示，不論這些設定檔不作用的時間有多長，ANZPRFACT 指令都無法停用它們。

當系統執行 ANZPRFACT 指令時，它會在審核異動記載中，寫入每個停用的使用者設定檔的 CP 登錄。您可以使用 DSPAUDJRNE 指令來列出新停用的使用者設定檔。

註: 只有當 QAUDCTL 値指定 *AUDLVL 且 QAUDLVL 系統値指定 *SECURITY 時，系統才會寫入審核登錄。

另一個檢查是否根據排定的進度表來停用使用者設定檔的方法，是使用「列印使用者設定檔 (PRTUSRPRF)」指令。當您將報告類型指定為 *PWDINFO 時，報告中會包括每個選定之使用者設定檔的狀態。

自動移除使用者設定檔

您可以使用「變更到期日進度表登錄 (CHGEXPSCDE)」指令來管理使用者設定檔的除去或停用程序。如果您知道某個使用者將長期不在職，您應該排定除去或停用他的使用者設定檔。

您第一次使用 CHGEXPSCDE 指令時，它會建立一個工作進度表登錄，在每天的午夜過後 1 分鐘執行。這個工作會查看 QASECEXP 檔，判斷當天是否有排定要除去的使用者設定檔。

您可以使用 CHGEXPSCDE 指令來停用或刪除使用者設定檔。如果您選擇要刪除某個使用者設定檔，您必須指定對於使用者所擁有的物件，系統將會執行什麼動作。在您排定要刪除某個使用者設定檔之前，您必須先搜尋使用者所擁有的物件。例如，如果使用者擁有沿用權限的程式，則是否要讓這些程式沿用新擁有者的所有權？或新擁有者是否擁有超過所需的權限 (例如特殊權限) ？您也許需要建立一個具有特殊權限的新使用者設定檔，使它擁有需要沿用權限的程式。

如果您要刪除使用者設定檔，您也必須了解，是否會發生任何應用程式的問題。例如，是否會有任何工作說明將使用者設定檔指定為預設使用者？

您可以使用「顯示到期日進度表 (DSPEXPSCD)」指令來顯示排定要停用或除去的設定檔列示。

您可以使用「顯示授權使用者 (DSPAUTUSR)」指令來列出系統中的所有使用者設定檔。再使用「刪除使用者設定檔(DLTUSRPRF)」指令來刪除過時的設定檔。

安全注意事項：: 您可以將某個使用者設定檔的狀態設定為 *DISABLED 來停用它。您停用使用者設定檔時，它即成為無法進行交談式的使用。您不能使用停用的使用者設定檔來進行登入，或將您的工作變更至停用的使用者設定檔。在已停用的使用者設定檔之下，仍可以執行批次工作。

避免預設密碼

當您建立新的使用者設定檔時，依預設，會建立和使用者設定檔同名的密碼。這時，如果有人知道您的設定檔命名原則，且知道企業組織內有新人加入，則他便有了進入系統的機會。

當您建立新使用者設定檔時，請考慮指定唯一且非可有可無的密碼來取代預設的密碼。例如在概述您的安全原則的 『歡迎光臨系統』 信函，秘密地告訴新使用者密碼。要求使用者將使用者設定檔設定為 PWDEXP(*YES)，在第一次登入時變更密碼。

您可以使用「分析預設密碼 (ANZDFTPWD)」指令來對您系統中的所有使用者設定檔進行預設密碼的檢查。 當您列印報告時，您可以選擇指定系統應該在密碼和使用者設定檔名稱相同時採取動作 (例如停用使用者設定檔)。 ANZDFTPWD 指令會列出一份列示，其中包括它找到的設定檔以及所採取的任何動作。

註: 在您的系統中，密碼會以單向加密的方式來儲存。它們無法被解密。系統會將指定的密碼加密，再將其與儲存的密碼比較，猶如您登入系統時所執行的密碼檢查。如果您正在審核權限失效 (*AUTFAIL)，系統會針對每個*沒有*預設密碼的使用者設定檔，寫入一項 PW 審核日誌登錄 (針對執行 V4R1 或更早版次的系統)。 從 V4R2 開始，當您執行 ANZDFTPWD 指令時，系統不會寫入 PW 審核日誌登錄。

監督登入及密碼活動

如果您擔心未獲授權而企圖進入您的系統的嘗試，您可以使用 PRTUSRPRF 指令來協助監督登入和密碼活動。

以下是使用這個報告的若干建議事項：

- 判斷某些使用者設定檔的密碼到期日間隔是否超出系統值，以及是否調整較長的到期間隔。例如，在報告中，USERY 的密碼到期間隔是 120 天。
- 定期執行這份報告，以監督未順利完成登入的嘗試。有些企圖侵入您的系統的使用者可能知道，您的系統經過若干失敗的嘗試後會採取行動。這些可能的侵入者可在每個晚上嘗試低於 QMAXSIGN 值的次數，避免讓您注意到這些嘗試。不過，如果您在每天一早執行這個報告，並注意某些設定檔是否常常出現失敗的登入嘗試，便會懷疑是否發生問題。
- 識別許久未使用或未變更密碼的使用者設定檔。

儲存密碼資訊

爲支援某些網路功能和通訊需求，iSeries 伺服器提供一個安全的方法，讓您儲存可解密的密碼。您的系統使用這些密碼來執行若干作業，例如，建立與另一個系統之間的 SLIP 連接。(第 111 頁的『安全性和撥出階段作業』說明儲存密碼的這個使用方式。)

iSeries 伺服器將這些特殊密碼儲存在一個安全的區域，任何使用者程式或介面都無法存取這個區域。只有明確取得權限的系統功能可以設定這些密碼並擷取它們。

例如，當您將儲存的密碼用於撥出的 SLIP 連接時，您使用建立配置檔 (WRKTCPPTP) 的系統指令來設定密碼。您必須擁有 *IOSYSCFG 才能使用指令。在撥出程序期間，會使用一個特殊編碼的連接 script 來擷取並解密這個密碼。使用者看不到解密後的的密碼，也不會出現任何工作日誌中。

作爲一個安全管理者，您必須決定可解密的密碼是否要儲存在系統中。您使用「保留伺服器安全資料 (QRETSVRSEC)」系統值來指定這個項目。預設值爲 0 (否)。因此，除非您明確地設定了這個系統值，否則您的系統不會儲存可解密的密碼。

如果您有儲存密碼的網路或通訊需求，您應該設定適當的原則，並瞭解您的通訊伙伴的原則和操作。例如，當您使用 SLIP 與另一個 iSeries 伺服器通訊時，兩個系統都應該考慮設置特殊的使用者設定檔，用以建立階段作業。在系統中，特殊設定檔的權限應該受到限制。當對等系統會損害儲存的密碼時，這可以限制您的系統所可能受到的影響。

第 4 章 配置 iSeries 使用安全性工具程式

本資訊說明如何設定您的系統來使用 OS/400 之一部份的安全性工具程式。在您安裝好 OS/400 時，安全性工具程式即已備妥，可供使用。以下主題提供安全性工具程式之作業程序的建議事項。

安全地操作安全性工具程式

當您安裝 OS/400 時，關聯於安全性工具程式的物件都是安全的。如果要安全地操作安全性工具程式，請避免對任何安全性工具程式物件做任何變更。

以下是安全性工具程式物件的安全設定和需求：

- 安全性工具程式程式和指令在 QSYS 產品檔案庫中。在出貨時，指令和產品的公用權限是 *EXCLUDE。許多安全性工具程式指令都會在 QUSRSYS 檔案庫內建立檔案。在系統建立這些檔案時，檔案的公用權限是 *EXCLUDE。

  產生變更報告之資訊所在的檔案，名稱開頭為 QSEC。用來管理使用者設定檔之資訊所在的檔案，名稱開頭為 QASEC。這些檔案都含有系統的機密資訊。因此，您不應該變更檔案的公用權限。
- 安全性工具程式使用您的一般系統設置來導引列印的輸出。這些報告都含有系統的機密資訊。 如果要將輸出導引至產品輸出佇列，請對將執行安全性工具程式之使用者的使用者設定檔或工作說明進行適當的變更。
- 由於所具備的安全功能，也由於會存取系統中的許多物件，安全性工具程式指令需要 *ALLOBJ 特殊權限。有些指令也需要 *SECADM、*AUDIT 或 *IOSYSCFG 特殊權限。如果要確定能順利執行指令，當您使用安全性工具程式時，應該登入為安全主管。因此，您應該不需要授與任何安全性工具程式指令的專用權限。

避免檔案衝突

許多安全性工具程式報告指令都會建立可用來列印報告變更版本的資料庫檔案。第 26 頁的『安全指令的指令和功能表』說明每個指令的檔案名稱。您每次只能從一個工作執行一個指令。大部份指令現在都可以勾選實施這個項目。如果您在某個工作尚未完成它的執行過程之前執行另一個指令，則您會收到一則錯誤訊息。

許多列印工作都屬於執行時間較長的工作。當您提出以批次方式來執行報告，或將它們新增到工作排程器時，您需要小心避免檔案衝突。例如，您可以使用不同的選項基準來列印兩種版本的 PRTUSRPRF 報告。如果您提出以批次方式來執行報告，您應該使用每次只執行一個工作的工作佇列，以確定能連續執行報告工作。

如果您在使用工作排程器，您必須讓兩個工作有足夠的間隔，使第一個版本結束後，才會開始第二個工作。

儲存安全性工具程式

每當您執行「儲存系統 (SAVSYS)」指令或「儲存」功能表中用來執行 SAVSYS 指令的選項時，都會儲存安全性工具程式程式。

安全性工具程式檔案在 QUSRSYS 檔案庫內。您應該將這個檔案庫當作正常作業程序來儲存。QUSRSYS 檔案庫含有系統中許多授權程式的資料。請參閱「資訊中心」，取得關於儲存 QUSRSYS 檔案庫的指令和選項的詳細資訊。

安全指令的指令和功能表

本節說明安全工具的指令和功能表。有關如何使用指令的範例散見本資訊中。

安全工具的可用功能表有兩個：

- 以交談方式來執行指令的 SECTOOLS (安全工具) 功能表。
- 以批次方式來執行報表的 SECBATCH (提出或排定以批次方式來執行安全報表) 功能表。SECBATCH 功能表有兩個部份。功能表的第一部份使用「提出工作 (SBMJOB)」指令來提出以批次方式來立即處理的報表。

  功能表的第二部份使用「新增工作排程登錄 (ADDJOBSCDE)」指令。您使用它來排定依照指定的日期和時間來定期執行安全報表。

「安全工具」功能表選項

表 6 說明這些功能表選項與相關的指令：

表 6. 使用者設定檔工具指令

功能表 [1] 選項	指令名稱	說明	使用的資料庫檔案
1	ANZDFTPWD	使用「分析預設密碼」指令對密碼等於使用者設定檔名稱的使用者設定檔進行報表，並採取動作。	QASECPWD[2]
2	DSPACTPRFL	使用「顯示作用中的設定檔列示」指令顯示或列印免除 ANZPRFACT 處理之使用者設定檔的列示。	QASECIDL[2]
3	CHGACTPRFL	使用「變更作用設定檔列示」指令，在 ANZPRFACT 指令的免除列示中新增和除去使用者設定檔。在作用設定檔列示中的使用者設定檔會成爲永久作用 (直到您從列示中除去設定檔爲止)。在作用設定檔列示中的設定檔，不論其不作用的時間有多久，ANZPRFACT 指令都不會停用它。	QASECIDL[2]
4	ANZPRFACT	使用「分析設定檔活動」指令停用不作用時間已達指定天數的使用者設定檔。在您使用 ANZPRFACT 指令來指定天數之後，系統會在夜間執行 ANZPRFACT 工作。 您可以使用 CHGACTPRFL 指令來免除對於使用者設定檔的停用。	QASECIDL[2]
5	DSPACTSCD	使用「顯示設定檔啓動排程」指令顯示或列印啓用或停用特定使用者設定檔之排程的相關資訊。您可以使用 CHGACTSCDE 指令來建立排程。	QASECACT[2]
6	CHGACTSCDE	使用「變更啓動排程登錄」指令讓某個使用者設定檔只在一週或一天內的特定時間登入。對於您排定其排程的每個使用者設定檔，系統都會建立啓用和停用時間的工作排程登錄。	QASECACT[2]

表 6. 使用者設定檔工具指令 (繼續)

功能表 ¹ 選項	指令名稱	說明	使用的資料庫檔案
7	DSPEXPSCD	使用「顯示到期日排程」指令顯示或列印系統中排定將要停用或除去的設定檔列示。您可以使用 CHGEXPSCDE 指令來設置到期的使用者設定檔。	QASECEXP²
8	CHGEXPSCDE	使用「變更到期日排程登錄」指令排定除去某個使用者設定檔。您可以暫時性地除去它 (停用)，也可以從系統中刪除它。這個指令使用在每天 00:01 (午夜過後 1 分鐘) 執行的工作排程登錄。這個工作會查看 QASECEXP 檔，判斷是否有設置爲當天到期的使用者設定檔。 使用 DSPEXPSCD 指令可以顯示排定到期的使用者設定檔。	QASECEXP²
9	PRTPRFINT	使用「列印設定檔內部」指令列印一份報表，報表會提供使用者設定檔所含之登錄數的相關資訊。藉由登錄數，可判斷使用者設定檔的大小。	

註:

1. 選項爲 SECTOOLS 功能表的選項。
2. 這個檔案在 QUSRSYS 檔案庫內。

您可以在功能表中向下翻頁，查看其它選項。表 7 說明要進行安全審核的功能表選項和相關指令：

表 7. 安全審核的工具指令

功能表 ¹ 選項	指令名稱	說明	使用的資料庫檔案
10	CHGSECAUD	使用「變更安全審核 (CHGSECAUD)」指令可以設置安全審核，並變更控制安全審核的系統值。當您執行 CHGSECAUD 指令時，如果沒有安全審核 (QAUDJRN) 異動記載的話，系統會予以建立。 CHGSECAUD 指令提供的選項，使得 QAUDLVL (審核層次) 系統值的設定更爲簡易。您可以指定 *ALL 來啓動所有可能的審核層次設定。您也可以指定 *DFTSET 來啓動最常使用的設定值 (*AUTFAIL、*CREATE、*DELETE、*SECURITY 和 *SAVRST)。 **註:** 如果您使用安全工具來設置審核，請務必規劃審核異動記載接收器的管理作業。否則，您可能很快就會在磁碟使用上發生問題。	
11	DSPSECAUD	使用「使用安全審核」指令顯示安全審核異動記載和控制安全審核之系統值的相關資訊。	

註:

1. 選項爲 SECTOOLS 功能表的選項。

使用「安全批次」功能表

以下是 SECBATCH 功能表的第一部份：

```
SECBATCH          提出或排定批次執行的安全報表
                                                                     系統：
請選取下列項目之一：

  提出批次執行的報表
     1. 沿用物件
     2. 審核異動記載登錄
     3. 授權清單權限
     4. 指令權限
     5. 指令專用權限
     6. 通訊安全
     7. 目錄權限
     8. 目錄專用權限
     9. 文件權限
    10. 文件專用權限
    11. 檔案權限
    12. 檔案專用權限
    13. 資料夾權限
```

當您選取這個功能表的選項時，您會看到「提出工作 (SBMJOB)」顯示畫面。如果您要變更指令的預設選項，您可以按下*要執行的指令*行的 F4。

要查看「排定批次報表」時，請在 SECBATCH 功能表上向下翻頁。透過使用這部份的功能表選項，您可以執行若干動作，例如，設置您的系統來定期執行報表的變更版本。您可以向下翻頁，查看其餘的功能表選項。當您選取這部份的功能表選項時，您會看到「新增工作排程登錄 (ADDJOBSCDE)」顯示畫面。

您可以將您的游標放在*要執行的指令*行，再按 F4 (提示) ，選擇不同的報表設定。您應該指定有意義的工作名稱，以便在您顯示工作排程登錄時能夠辨識它們。

「安全批次」功能表選項

第 29 頁的表 8 說明要安全報表的功能表選項和相關指令：

當您執行安全報表時，系統只會列印符合您指定的選取基準和工具的選取基準的相關資訊。例如，指定使用者設定檔名稱的工作說明與安全相關。因此，只有在工作說明的公用權限不是 *EXCLUDE，*以及*如果工作說明指定在 USER 參數內的使用者設定檔名稱時，工作說明 (PRTJOBDAUT) 報表才會列印指定的檔案庫。

同樣地，當您列印子系統資訊 (PRTSBSDAUT 指令) 時，只有在子系統說明擁有指定使用者設定檔的通訊登錄時，系統才會列印子系統的相關資訊。

如果特定報表列印的資訊比您所預期的少，請詳閱線上解說資訊，找出報表的選取基準。

表 8. 安全報表的指令

功能表 ¹ 選項	指令名稱	說明	使用的資料庫檔案
1, 40	PRTADPOBJ	使用「列印沿用物件」指令列印沿用指定的使用者設定檔之權限的物件列示。您可以指定單一設定檔、同屬設定檔名稱 (例如所有以 Q 為首的設定檔) ，或系統中的所有設定檔。 這份報表有兩個版本。完整的報表會列出符合選取基準的所有沿用物件。變更的報表會列出目前在系統中的沿用物件和前次執行報表時在系統中的沿用物件之間的差異。	QSECADPOLD[2]
2, 41	DSPAUDJRNE	使用「顯示審核異動記載登錄」指令顯示或列印安全審核異動記載中之登錄的相關資訊。您可以選取特定的登錄類型、特定使用者和某個時間期間。	QASYxxJ4[3]
3, 42	PRTPVTAUT *AUTL	當您對 *AUTL 物件使用「列印專用權限」指令時，您會收到系統中之所有授權清單的列示。報表中包括取得列示權限的使用者和使用者所擁有的列示權限。使用這個資訊可協助您分析系統中之物件權限的來源。 這個報表有三個版本。完整報表會列出系統中的所有權限列示。變更的報表會列出前次執行報表後，又發生過的權限附加和變更。刪除的報表會列出前次執行報表後，其授權清單權限遭到刪除的使用者。 當您列印完整報表時，您可以選擇列印每個授權清單所保護的物件列示。系統會針對每個授權清單來建立個別的報表。	QSECATLOLD[2]
6, 45	PRTCMNSEC	使用「列印通訊安全」指令列印會影響系統通訊之物件的安全相關設定。這些設定會影響使用者和工作進入您系統的方式。 這個指令可產生兩份報表：一份報表顯示系統中之配置清單的設定值，一份報表列出線路說明、控制器和裝置說明的安全相關參數。在這些報表中，每一份都會有完整版本和變更版本。	QSECCMNOLD[2]
15, 54	PRTJOBDAUT	使用「列印工作說明權限」指令列印指定使用者設定檔並擁有非 *EXCLUDE 之公用權限的工作說明之列示。報表會顯示工作說明中所指定之使用者設定檔的特殊權限。 這份報表有兩個版本。完整的報表會列出符合選取基準的所有工作說明物件。變更的報表會列出目前在系統中的工作說明物件和前次執行報表時在系統中的工作說明物件之間的差異。	QSECJBDOLD[2]

表 8. 安全報表的指令 (繼續)

功能表 [1] 選項	指令名稱	說明	使用的資料庫檔案
請參閱附註 4	PRTPUBAUT	使用「列印公用授權物件」指令列印公用權限不是 *EXCLUDE 的物件列示。您在執行指令時，會指定該報表的物件類型和檔案庫。使用 PRTPUBAUT 指令可以列印系統中之每個使用者所能存取之物件的相關資訊。 這份報表有兩個版本。完整的報表會列出符合選取基準的所有物件。變更的報表會列出目前在系統中的指定物件和前次執行報表時在系統中的物件 (相同檔案庫，相同類型) 之間的差異。	QPBxxxxxx[5]
請見附註 5。	PRTPVTAUT	使用「列印專用權限」指令列印指定的檔案庫中，指定類型之物件的專用權限列示。使用這個報表可協助您判斷物件權限的來源。 這個報表有三個版本。完整的報表會列出符合選取基準的所有物件。變更的報表會列出目前在系統中的指定物件和前次執行報表時在系統中的物件 (相同檔案庫，相同類型) 之間的差異。刪除的報表會列出前次列印報表後，其物件權限遭到刪除的使用者。	QPVxxxxxx[5]
24, 63	PRTQAUT	使用「列印佇列報表」指令列印系統中的輸出佇列和工作佇列的安全設定。這些設定可控制哪些使用者可檢視和變更輸出佇列或工作佇列中的變更。 這份報表有兩個版本。完整的報表會列出符合選取基準的所有輸出佇列和工作佇列物件。變更的報表會列出目前在系統中的輸出佇列和工作佇列物件和前次執行報表時在系統中的輸出佇列和工作佇列物件之間的差異。	QSECQOLD[2]
25, 64	PRTSBSDAUT	使用「列印子系統說明」指令列印系統中之子系統說明的安全相關通訊登錄。這些設定控制工作可如何進入您的系統，以及工作的執行方式。只有在報表擁有指定使用者設定檔名稱的通訊登錄時，報表才會列印子系統說明。 這份報表有兩個版本。完整的報表會列出符合選取基準的所有子系統說明物件。變更的報表會列出目前在系統中的子系統說明物件和前次執行報表時在系統中的子系統說明物件之間的差異。	QSECSBDOLD[2]
26, 65	PRTSYSSECA	使用「列印系統安全屬性」指令列印安全相關系統值和網路屬性的列示。報表會顯示現行值和建議值。	
27, 66	PRTTRGPGM	使用「列印觸發程式」指令列印系統中之資料庫檔案的相關觸發程式列示。 這份報表有兩個版本。完整報表會列出每個指定並符合您的選取基準的觸發程式。變更的報表會列出前次執行報表後，又指定過的觸發程式。	QSECTRGOLD[2]

表 8. 安全報表的指令 (繼續)

功能表 [1] 選項	指令名稱	說明	使用的資料庫檔案
28, 67	PRTUSROBJ	使用「列印使用者物件」指令，列印檔案庫中的使用者物件 (不是 IBM 提供的物件) 清單。您可以使用這份報表來列出檔案庫列示系統部份中之檔案庫 (如 QSYS) 內的使用者物件列示。 這份報表有兩個版本。完整的報表會列出符合選取基準的所有使用者物件。變更的報表會列出目前在系統中的使用者物件和前次執行報表時在系統中的使用者物件之間的差異。	QSECPUOLD[2]
29, 68	PRTUSRPRF	使用「列印使用者設定檔」指令分析符合指定的基準的使用者設定檔。您可以根據特殊權限、使用者類別，或特殊權限與使用者類別的不符，來選取使用者設定檔。您可列印權限資訊、環境資訊、密碼資訊或密碼層次資訊。	
30, 69	PRTPRFINT	使用「列印設定檔內部」指令列印一份報表，此報表會提供有關登錄數的內部資訊。	
31, 70	CHKOBJITG	使用「檢查物件整合性」指令判斷是否在未使用編譯器的情況下變更了可操作的物件 (例如程式)。這個指令可協助您偵測出將病毒引入系統的企圖，以及變更程式來執行未獲授權之指示的企圖。*iSeries Security Reference* 一書提供關於 CHKOBJITG 指令的詳細資訊。	

註:

1. 選項為 SECBATCH 功能表的選項。
2. 這個檔案在 QUSRSYS 檔案庫內。
3. xx 是兩個字元的日誌登錄類型。例如，AE 日誌登錄的模型輸出檔是 QSYS/QASYAEJ4。型號輸出檔的說明，請參閱 *iSeries Security Reference* 一書的「附錄 F」。
4. SECBATCH 功能表含有安全管理者所關切之物件類型的選項。例如，使用選項 11 或 50，對 *FILE 物件執行 PRTPUBAUT 指令。一般選項 (18 與 57) 則可用來指定物件類型。
5. SECBATCH 功能表含有安全管理者所關切之物件類型的選項。例如，使用選項 12 或 51，對 *FILE 物件執行 PRTPVTAUT 指令。一般選項 (19 與 58) 則可用來指定物件類型。
6. 檔案名稱中的 xxxxxx 是物件類型。例如，公用權限的程式物件檔案稱為 QPBPGM，專用權限則為 QPVPGM。檔案位在 QUSRSYS 檔案庫內。

   在檔案中，已列印報表的每個檔案庫都會有一個成員。成員名稱和檔案庫名稱相同。

自行設定安全的指令

第 32 頁的表 9 說明可用來自行設定系統中之安全的指令。這些指令在 SECTOOLS 功能表中。

表 9. 自行設定系統的指令

功能表 [1] 選項	指令名稱	說明	使用的資料庫檔案
60	CFGSYSSEC	使用「配置系統安全」指令可將安全相關系統值設定為建議值。指令也會設置系統中的安全審核。『配置系統安全指令所設定的值』說明執行所執行的動作。 **註:** 如果要取得針對您的情況而設定的安全建議，請執行「iSeries 安全精靈」或「iSeries 安全顧問」，而不要執行這個指令。請參閱第 9 頁的第 2 章,『iSeries 安全性精靈與 eServer 安全規劃程式』，以取得這些工具的詳細資訊。	
61	RVKPUBAUT	使用「取消公用權限」指令可針對系統中的安全相關指令，將公用權限設定為 *EXCLUDE。第 34 頁的『「取消公用權限」指令的功能』列出 RVKPUBAUT 指令所執行的動作。	

註:

1. 選項為 SECTOOLS 功能表的選項。

配置系統安全指令所設定的值

表 10 列出執行 CFGSYSSEC 指令時所執行的系統值。CFGSYSSEC 指令執行一個稱為 QSYS/QSECCFGS 的程式。

表 10. CFGSYSSEC 指令所設定的值

系統值名稱	設定	系統值說明
QALWOBJRST	*NONE	是否可以復置系統狀態程式和沿用權限的程式
QAUTOCFG	0 (否)	自動配置新裝置
QAUTOVRT	0	如果沒有可用的裝置時，系統將自動建立的虛擬裝置說明數目。
QDEVRCYACN	*DSCMSG (切斷與訊息的連接)	重新建立通訊時的系統動作
QDSCJOBITV	120	系統對切斷的工作採取動作之前的時間期間。
QDSPSGNINF	1 (是)	使用者是否會看到登入資訊顯示畫面
QINACTITV	60	系統對不作用的交談式工作採取動作之前的時間期間。
QINACTMSGQ	*ENDJOB	系統對不作用的工作採取的動作
QLMTDEVSSN	1 (是)	是否將使用者限制為每次只能使用一個裝置來登入。
QLMTSECOFR	1 (是)	是否將 *ALLOBJ 和 *SERVICE 使用者限制於特定的裝置
QMAXSIGN	3	容許連續失敗的登入嘗試次數
QMAXSGNACN	3 (兩者)	到達 QMAXSIGN 限制時，系統是否要停用工作站或使用者設定檔。
QRMTSIGN	*FRCSIGNON	系統如何處理遠端 (透通或 TELNET) 登入嘗試。
QRMTSVRATR	0 (Off)	容許遠端分析系統。
QSECURITY 第 33 頁的 1	50	執行的安全層次
QVFYOBJRST	3 (復置時驗證簽章)	復置時驗證物件
QPWDEXPITV	60	使用者多久必須變更一次密碼
QPWDMINLEN	6	密碼的最小長度

表 10. CFGSYSSEC 指令所設定的值 (繼續)

系統值名稱	設定	系統值說明
QPWDMAXLEN	8	密碼的最大長度
QPWDPOSDIF	1 (是)	新密碼的每個位置是否都必須不同於舊密碼的相同位置
QPWDLMTCHR	請參閱註 2	密碼所不容許使用的字元
QPWDLMTAJC	1 (是)	密碼是否禁止使用相鄰的數字
QPWDLMTREP	2 (不能連續重複)	密碼是否禁止使用重複的字元
QPWDRQDDGT	1 (是)	密碼是否至少必須有一個數字
QPWDRQDDIF	1 (32 獨特的密碼)	可重複某個密碼之前，必須經過多少個獨特的密碼。
QPWDVLDPGM	*NONE	系統呼叫來驗證密碼的使用者跳出程式

註:

1. 如果您正執行值 40 (或以下) 的 QSECURITY，在您變更爲較高的安全層次前，請先複查 *iSeries Security Reference* 一書的第 2 章中的資訊。
2. 限制的字元儲存在訊息檔 QSYS/QCPFMSG 的訊息 IDXB302 中。它們出貨時是 AEIOU@$#。您可以使用「變更訊息說明 (CHGMSGD)」指令來變更限制的字元。QPWDLMTCHR 系統值不使用於密碼層次 2 或 3。

CFGSYSSEC 指令也可將下列 IBM 所提供之使用者設定檔的密碼設定爲 *NONE：

QSYSOPR

QPGMR

QUSER

QSRV

QSRVBAS

最後，CFGSYSSEC 指令會使用「變更安全審核 (CHGSECAUD)」指令，設置安全審核。CFGSYSSEC 指令會開啓動作與物件審核，同時會在 CHGSECAUD 指令指定一組要對審核的預設動作。

自訂程式

如果您的安裝作業不適合其中的某些設定，您可以建立您自己的程式版本來處理指令。請執行下列作業：

__ 步驟 1. 使用「擷取 CL 來源 (RTVCLSRC)」指令來複製您使用 CFGSYSSEC 指令時所執行之程式的來源。要擷取的程式是 QSYS/QSECCFGS。當您擷取它時，請給它*另一個名稱*。

__ 步驟 2. 編輯程式來執行您的變更。之後，再編譯它。在您編譯時，您並不置換 IBM 所提供的 QSYS/QSECCFGS 程式。您的程式應該有另一個名稱。

__ 步驟 3. 使用「變更指令 (CHGCMD)」指令來變更 CFGSYSSEC 指令的「處理指令的程式 (PGM)」參數。請將 PGM 值設爲您的程式名稱。例如，如果您在 QGPL 檔案庫中建立一個稱爲 MYSECCFG 的程式，您應該鍵入下列指令：

```
CHGCMD CMD(QSYS/CFGSYSSEC) PGM(QGPL/MYSECCFG)
```

註: 若您變更 QSYS/QSECCFGS 程式，IBM 無法保證或默許程式的可靠性、有用性、效能或功能。在特定目的下的任何銷售可能與適用性，IBM 也一概明確否認任何隱含的保證。

「取消公用權限」指令的功能

您可以使用「取消公用權限 (RVKPUBAUT)」指令，針對某一組指令或程式，將公用權限設定為 *EXCLUDE。RVKPUBAUT 指令執行一個稱為 QSYS/QSECRVKP 的程式。在出貨時，QSECRVKP 會取消表 11 所列出之指令的公用權限 (將公用權限設定為 *EXCLUDE) 和 表 12 所列出的應用程式介面 (API)。當您的系統到達時，這些指令和 API 會將它們的公用權限設定為 *USE。

表 11 列出的指令和表 12 列出的 API 在您系統上執行的功能，都可能提供造成災害的機會。作為一個安全管理者，您應該明確地授權給執行這些指令和程式的使用者，而不能讓所有系統使用者都能使用它們。

您在執行 RVKPUBAUT 指令時，指定含有指令的檔案庫。預設值為 QSYS 檔案庫。如果您的系統中有多種國家語言，您必須針對每個 QSYSxxx 檔案庫來執行指令。

表 11. RVKPUBAUT 指令來設定其公用權限的指令

ADDAJE	CHGJOBQE	RMVCMNE
ADDCFGLE	CHGPJE	RMVJOBQE
ADDCMNE	CHGRTGE	RMVPJE
ADDJOBQE	CHGSBSD	RMVRTGE
ADDPJE	CHGWSE	RMVWSE
ADDRTGE	CPYCFGL	RSTLIB
ADDWSE	CRTCFGL	RSTOBJ
CHGAJE	CRTCTLAPPC	RSTS36F
CHGCFGL	CRTDEVAPPC	RSTS36FLR
CHGCFGLE	CRTSBSD	RSTS36LIBM
CHGCMNE	ENDRMTSPT	STRRMTSPT
CHGCTLAPPC	RMVAJE	STRSBS
CHGDEVAPPC	RMVCFGLE	WRKCFGL

表 12 的 API 全在 QSYS 檔案庫中：

表 12. 由 RVKPUBAUT 指令來設定其公用權限的指令

QTIENDSUP
QTISTRSUP
QWTCTLTR
QWTSETTR
QY2FTML

當您執行 RVKPUBAUT 指令時，系統會將根目錄的公用權限設定為 *USE (除非它已經是 *USE 或以下)。

自訂程式

如果您的安裝作業不適合其中的某些設定，您可以建立您自己的程式版本來處理指令。請執行下列作業：

__ 步驟 1. 使用「擷取 CL 來源 (RTVCLSRC)」指令來複製您使用 RVKPUBAUT 指令時所執行之程式的來源。要擷取的程式是 QSYS/QSECRVKP。當您擷取它時，請給它*另一個名稱*。

__ 步驟 2. 編輯程式來執行您的變更。之後，再編譯它。在您編譯時，您並不置換 IBM 所提供的 QSYS/QSECRVKP 程式。您的程式應該有另一個名稱。

__ 步驟 3. 使用「變更指令 (CHGCMD)」指令來變更 RVKPUBAUT 指令的「處理指令的程式 (PGM)」參數。請將 PGM 值設爲您的程式名稱。例如，如果您在 QGPL 檔案庫中建立一個稱爲 MYRVKPGM 的程式，您應該鍵入下列指令：

```
CHGCMD CMD(QSYS/RVKPUBAUT) PGM(QGPL/MYRVKPGM)
```

註: 若您變更 QSYS/QSECRVKP 程式，IBM 無法保證或默許程式的可靠性、有用性、效能及功能。在特定目的下的任何銷售可能與適用性，IBM 也一概明確否認任何隱含的保證。

第 2 篇 iSeries 安全的進階功能

第 5 章 以物件權限來保護資訊資產

作爲一個安全管理者，您面臨的挑戰，是要在保護企業組織資產的同時，不干擾系統使用者的作業。您必須確定讓使用者擁有足夠的權限可執行他們的工作，但又不會有過多的權限來瀏覽整個系統，以及執行未獲授權的變更程序。

安全要訣

嚴格的權限會造成不利的結果。當權限的限制過於嚴格時，有時會導致使用者彼此共用密碼。

OS/400 作業系統提供整合性的物件安全。使用者必須使用系統所提供的介面才能存取物件。例如，如果您要存取資料庫檔案，您必須使用針對資料庫檔案之存取的指令或程式。您不能使用存取佇列或工作日誌的指令。

每當您使用某個系統介面來存取物件時，系統都會驗證您是否擁有該介面所需要之物件的權限。物件權限是個有力且富於彈性的工具，可用來保護您系統中的資產。作爲一個安全管理者，您面臨的挑戰，是設置一套您能夠管理和維護的有效物件安全架構。

增強物件權限

每當您試圖要存取物件時，作業系統都會檢查您是否擁有該物件的權限。不過，如果系統所設定的安全層次 (QSECURITY 系統值) 是 10 或 20，則每個使用者都自動擁有存取每個物件的權限，因爲每個使用者設定檔都擁有 *ALLOBJ 特殊權限。

物件權限要訣： 如果您不確定是否使用了物件權限，請檢查 QSECURITY (安全層次) 系統值。如果 QSECURITY 是 10 或 20，代表您未使用物件安全性。

您必須先進行規劃和準備，才能變更至安全層次 30 或以上。否則，您的使用者可能無法存取他們所需要的資訊。

資訊中心中的**基本系統安全與規劃**主題已提供一個方法，讓您分析應用程式，並決定該如何設定物件安全性。如果您未執行物件安全程序，或如果您的物件安全架構已過期或過於複雜，您可以閱讀本主題作爲開始。

功能表安全性

iSeries 伺服器原來是 S/36 和 S/38 的衍生產品。在某一段時間裡，許多 iSeries 伺服器的安裝即是 S/36 或 S/38 的安裝作業。爲了控制使用者所能執行的動作，在這些早期系統上，安全管理者通常使用一種技術，稱爲**功能表安全性**或**功能表存取控制**。

功能表存取控制表示，當使用者登入時，他會看見一個功能表：使用者只能執行功能表中所列出的功能。使用者不能進入系統的指令行來執行功能表所未列出的任何功能。理論上，安全管理者不必擔心物件的權限問題，因爲功能表和程式會控制使用者能夠執行哪些動作。

iSeries 伺服器提供幾種使用者設定檔選項，以輔助功能表存取控制，您可以使用：
- **起始功能表** (INLMNU) 參數，控制使用者登入後第一個看到的功能表。
- **起始程式** (INLPGM) 參數，在使用者看到功能表之前執行一個設置程式。您也可以使用 INLPGM 參數來限制使用者只能執行單一程式。
- **限制功能** (LMTCPB) 參數，限制使用者只能執行一組有限的指令。它也會防止使用者在「登入」顯示畫面指定另一組起始程式或功能表。(LMTCPB 參數只會限制從指令行輸入的指令。)

功能表存取控制的限制

近幾年來，電腦和電腦使用者已經歷大幅度的變更。如今，使用者已有許多工具，如查詢程式和試算表等，可以自行完成若干程式設計，而不再需要 IS 部門。有些工具，例如 SQL 或 ODBC，可提供檢視資訊和變更資訊的功能。要在功能表結構內使用這些工具，非常困難。

目前，固定功能 (『綠色螢幕』) 的工作站已逐漸被淘汰，改用個人電腦和網路中電腦對電腦的系統。如果您的系統參與某個網路，則使用者將可進入您的系統，而不需經過登入顯示畫面或功能表。

作爲一個執行功能表存取控制的安全管理者，您會面對兩個基本問題：
- 如果您順利限制使用者對於功能表的使用，使用者可能會很不高興，因爲您限制了他們使用新型工具的能力。
- 如果您未順利加以限制，則原來功能表存取控制所要保護的重要機密資訊，可能會面臨危險。當您的系統參與某個網路時，您執行功能表存取控制的能力會降低。例如，LMTCPB 參數只適用於在交談式階段作業的指令行中輸入的指令。對於通訊階段作業所提出的要求 (如 PC 檔案轉送、FTP，或遠端指令等) 而言，LMTCPB 參數沒有作用。

以物件安全性增強功能表存取控制

隨著可用來連接系統之新選項的增加，可實施的 iSeries 伺服器安全架構，也將無法只依賴於功能表的存取控制。本主題提供一些建議，協助您移轉至物件安全環境來補充您的功能表存取控制。

資訊中心中的*基本系統安全與規劃*主題說明一種用來分析使用者執行您的現行應用程式時所必須擁有的物件權限的技術。然後，您可將使用者指定給某個群組，並提供該群組適當的權限。這個方式非常合理，合乎邏輯。不過，如果您的系統已運作了許多年，擁有許多應用程式，則分析應用程式和設置物件權限的作業會顯得有點強迫的意味。

物件權限要訣： 您的現行功能表和程式擁用者權限的程式結合起來，可讓您進行功能表存取控制範圍以外的移轉。請務必保護沿用權限的程式，以及擁有這些程式的使用者設定檔。

在您逐步分析您的應用程式和物件之時，您的現行功能表或許可協助您設置轉移環境。以下範例使用「訂購登錄 (OEMENU)」功能表和相關的檔案與程式。

範例：建立轉移環境

這個範例由下列假設和需求開始：
- 所有檔案都在檔案庫 ORDERLIB 中。

- 您不知道所有檔案的名稱。您也不知道對於各不同的檔案，功能表需要什麼權限。
- 功能表及其所呼叫的程式都在檔案庫 ORDERPGM 中。
- 您要讓每個可登入您系統的使用者，都可以檢視所有訂購檔、客戶檔和項目檔內的資訊 (例如使用查詢或試算表)。
- 只有現行登入功能表為 OEMENU 的使用者可以變更這些檔案。同時，他們必須使用功能表中的程式來執行這個動作。
- 安全管理者以外的系統使用者沒有 *ALLOBJ 或 *SECADM 特殊權限。

請執行下列步驟來變更這個功能表存取控制環境，以符合查詢需求：

__ 步驟 1. 建立一份使用者列示，這些使用者的起始功能表是 OEMENU。

您可以使用「列印使用者設定檔 (PRTUSRPRF *ENVINFO)」指令來列出系統中之每個使用者設定檔的環境。報告中包括起始功能表、起始程式，以及現行檔案庫。第 55 頁的圖 7 顯示一份報告範例。

__ 步驟 2. 確定 OEMENU 物件 (它可能是 *PGM 物件或 *MENU 物件) 是某個未用於登入的使用者設定檔所擁有。使用者設定應該在停用狀態，或擁有密碼 *NONE。在這個範例中，假設 OEOWNER 擁有 OEMENU 程式物件。

__ 步驟 3. 確定擁有 OEMENU 程式物件的使用者設定檔不是一個群組設定檔。您可以使用下列指令：

```
DSPUSRPRF USRPRF(OEOWNER) TYPE(*GRPMBR)
```

__ 步驟 4. 變更 OEMENU 程式，以沿用 OEOWNER 使用者設定檔的權限。(使用 CHGPGM 指令，將 USRPRF 參數變更為 *OWNER。)

註: *MENU 物件不能沿用權限。如果 OEMENU 是一個 *MENU 物件，則您不能執行下列動來調整這個範例：

- 建立程式來顯示功能表。
- 對於使用者選取 OEMENU 功能表選項時所執行的程式使用沿用權限。

__ 步驟 5. 鍵入下兩個指令，將 ORDERLIB 中之所有檔案的公用權限設定為 *USE：

```
RVKOBJAUT OBJ(ORDERLIB/*ALL) OBJTYPE(*FILE) USER(*PUBLIC)
     AUT(*ALL)
GRTOBJAUT OBJ(ORDERLIB/*ALL) OBJTYPE(*FILE) USER(*PUBLIC)
   AUT(*USE)
```

請記住，如果您選取 *USE 權限，則使用者可以使用 PC 檔案轉送或 FTP 來複製檔案。

__ 步驟 6. 鍵入下列指令來提供擁有功能表程式 *ALL 權限的設定檔：

```
GRTOBJAUT OBJ(ORDERLIB/*ALL) OBJTYPE(*FILE) USER(OEOWNER)
     AUT(*ALL)
```

對於多數應用程式而言，檔案的 *CHANGE 權限已經足夠。不過，您的應用程式可以執行需要 *CHANGE 以上之權限的功能，例如清除實體檔案成員。最後，您應該分析您的應用程式，並只提供應用程式所需要的最基本權限。不過，在轉移期間，藉由沿用 *ALL 權限，您可以避免發生權限不足而導致應用程式失效的情形。

__ 步驟 7. 鍵入下列指令來限制對於訂購檔案庫中之程式的權限：

```
GRTOBJAUT OBJ(ORDERPGM/*ALL) OBJTYPE(*PGM) USER(*PUBLIC)
   AUT(*EXCLUDE)
```

__ 步驟 8. 鍵入下列指令來提供 OEOWNER 設定檔權限給檔案庫中的程式：

```
GRTOBJAUT OBJ(ORDERPGM/*ALL) OBJTYPE(*PGM) USER(OEOWNER)
   AUT(*USE)
```

__ 步驟 9. 鍵入下列指令，提供功能表程式的權限給您在步驟 1 中識別的每個使用者：

```
GRTOBJAUT OBJ(ORDERPGM/OEMENU) OBJTYPE(*PGM)
     USER(user-profile-name) AUT(*USE)
```

當您完成這些步驟時，所有未明確排除的系統使用者都可以存取 (不含變更) QRDERLIB 檔案庫中的檔案。擁有 OEMENU 程式之權限的使用者都能夠使用功能表中的程式來更新 ORDERLIB 檔案庫中的檔案。現在，只有擁有 OEMENU 程式之權限的使用者可以變更這個檔案庫中的檔案。物件安全和功能表安全的組合可以保護這些檔案。

當您針對含有使用者資料的所有檔案庫完成類似的步驟後，您已建立起一個用來控制資料庫更新作業的簡單架構。這個方法可防止系統使用者未使用核准的功能表和程式，而擅自更新資料庫檔案。同時，如果使用者擁有確定支援工具，或使用已鏈接的其它系統或 PC，則他們也可以檢視、分析和複製資料庫檔案。

物件權限要訣： 當您的系統參與某個網路時，*USE 權限可提供超出您所預期的權限。例如，使用 FTP 時，如果您擁有檔案的 *USE 權限，您可以將檔案複製到另一個系統 (包括 PC) 中。

使用檔案庫安全來補充功能表安全

如果要存取檔案庫內的物件，您必須同時擁有物件和檔案庫的權限。多數作業都會要求檔案庫的 *EXECUTE 權限或 *USE 權限。

視您的情況而定，您也許可以使用檔案庫權限來作爲簡單的物件安全保護方式。例如，假設對於「訂購登錄」功能表的範例而言，每個擁有「訂購登錄」功能表權限的使用者都可以使用 ORDERPGM 檔案庫內的所有程式。您不需要保護個別程式的安全，您可以將 ORDERPGM 檔案庫的公用權限設定爲 *ESCLUDE。之後，再將檔案庫的 *USE 權限授與特定的使用者設定檔，這樣，它們便可以使用檔案庫內的程式。(這假設程式的公用權限 *USE 或以上。)

檔案庫權限可以是管理物件權限的簡單而有效的方法。不過，您必須確定您熟悉所要保護的檔案庫內容，以免提供了不當的物件存取權。

配置物件所有權

系統中之物件的所有權是物件安全架構中的重要成份。依預設，物件的擁有者擁有物件的 *ALL 權限。*iSeries Security Reference* 一書的第 5 章提供規劃物件所有權的建議和範例。以下簡單提出幾個要訣：

- 一般而言，群組設定檔不應該擁有物件。如果某個群組設定檔擁有物件，則在未明確排除群組成員的情況下，所有群組成員都會擁有物件的 *ALL 權限。
- 如果您使用沿用權限，請考慮擁有程式的使用者設定檔是否也擁有應用程式物件，例如檔案。您可能不希望讓執行沿用權限之程式的使用者也擁有檔案的 *ALL 權限。

如果您使用的是「iSeries 領航員」，在經由使用安全**原則**功能完成變更後，即能完成此項。相關資訊請參照 iSeries 資訊中心 (詳細資訊請參閱第 xii 頁的『先決條件與相關資訊』)。

系統指令和程式的物件權限

以下是您限制 IBM 所提供之物件的權限時，相關的若干建議事項：

- 當您的系統中有多種國家語言時，其中也會有多個系統 (QSYS) 檔案庫。在您的系統中，每個國家語言都會有一個 QSYSxxxx 檔案庫。如果您使用物件權限來控制系統指令的存取，請記得為系統 QSYS 檔案庫和每個 QSYSxxx 檔案庫中的指令提供安全保護。
- System/38™ 檔案庫所提供的指令，其功能有時會和您要限制的指令相同。請務必限制 QSYS38 檔案庫內的對等指令。
- 如果您擁有 System/36™ 環境，您可能需要限制其它程式。例如，QY2FTML 程式提供 System/36 的檔案轉送。

審核安全功能

本節說明審核系統上安全效用的技術。人們基於下述理由審核其系統安全：

- 評估安全性規劃是否完整。
- 確定所規劃的安全性控制適當且可行。這類的審核通常由安全主管來執行，並當作每日安全性管理的一部份。它也可由內部或外部的審核員，當成定期的安全性複查的一部份，但有時會更為詳細。
- 確定系統安全在系統環境變更時仍穩定。影響安全性之變更的部份範例如下：
  - 由系統使用者建立的新物件
  - 進入系統的新使用者
  - 物件所有權的變更（未調整授權）
  - 責任的變更（變更使用者群組）
  - 暫時的權限（未適時撤回）
  - 安裝新產品
- 為未來事件作準備，諸如安裝新的應用程式、移動到較高的安全層次或設置通訊網路。

說明於本章的技術適用於這所有的狀況。審核的事項及頻率取決於您組織的大小及安全性需求。本章的目的在於討論有哪些可用的資訊、取得的管道及需要它的原因，而非提供審核頻率的指引。

本資訊有三部份：

- 可規劃及審核的安全性項目核對清單。
- 設置及使用系統提供之審核日誌的資訊。
- 蒐集系統安全資訊之其他可用的技術。

安全性審核包括使用 iSeries 系統上的指令和存取系統日誌資訊。您可能想建立一個特殊的設定檔，由某人用來進行您系統的安全性審核。審核員設定檔需要 *AUDIT 特殊權限，以變更您系統的審核性質。本章所建議的部份審核作業需要具有 *ALLOBJ 及 *SECADM 特殊權限的使用者設定檔。請確定當審核期間結束時，您將審核員設定檔的密碼設定為 *NONE。

有關安全性審核的更多明細，請參閱 *Security Reference* 一書的第 9 章。

分析使用者設定檔

您可使用「顯示授權使用者 (DSPAUTUSR) 指令，顯示或列印系統上全部使用者的完整清單。清單可依照設定檔名稱或群組設定檔名稱來排序。以下為群組設定檔順序的範例：

```
                        顯示授權使用者

密碼
群組        使用者        最近        無
設定檔      設定檔        變更日期    密碼      本文
DPTSM
             ANDERSOR    08/04/0x            Roger Anders
             VINCENTM    09/15/0x            Mark Vincent
DPTWH
             ANDERSOR    08/04/0x            Roger Anders
             WAGNERR     09/06/0x            Rose Wagner
QSECOFR
             JONESS      09/20/0x            Sharon Jones
             HARRISOK    08/29/0x            Ken Harrison
*NO GROUP
             DPTSM       09/05/0x    X       市場行銷
             DPTWH       08/13/0x    X       倉庫
             RICHARDS    09/05/0x            Janet Richards
             SMITHJ      09/18/0x            John Smith
```

列印選定的使用者設定檔

您可使用「顯示使用者設定檔 (DSPUSRPRF)」指令來建立您可使用查詢工具處理的輸出檔。

```
DSPUSRPRF USRPRF(*ALL) +
          TYPE(*BASIC) OUTPUT(*OUTFILE)
```

您可使用查詢工具來建立輸出檔的各種分析報告，例如：

- 同時具有 *ALLOBJ 及 *SPLCTL 特殊權限之所有使用者的清單。
- 依使用者設定檔欄位 (如起始程式或使用者類別) 排序之所有使用者的清單。

您可建立查詢程式來自輸出檔產生不同的報告。例如：

- 以選取欄位 UPSPAU 不等於 *NONE 的記錄，列出具有特殊權限的所有使用者設定檔。
- 以選取*限制功能*欄位 (在模型資料庫輸出檔中稱為 UPLTCP) 等於 *NO 或 *PARTIAL 的記錄，列出可輸入指令的所有使用者。
- 列出具有特殊起始功能表或起始程式的所有使用者。
- 以查看最近登入日期欄位，列出非作用中的使用者。

檢查大型使用者設定檔

具有大量權限的使用者設定檔，不規則的遍及大部份系統上，反映出安全性規劃的不足。以下為尋找大型使用者設定檔及評估它們的方法：

1. 使用「顯示物件說明 (DSPOBJD)」指令來建立包含系統上所有使用者設定檔資訊的輸出檔：

```
DSPOBJD OBJ(*ALL) OBJTYPE(*USRPRF) +
        DETAIL(*BASIC) OUTPUT(*OUTFILE)
```

2. 建立一個查詢程式，依列出每一個使用者設定檔的名稱及大小，並依據大小以降序順序排列。
3. 列印最大的使用者設定檔之詳細資訊，並評估權限及擁有的物件，以了解它們是否適當：

```
DSPUSRPRF USRPRF(user-profile-name) +
          TYPE(*OBJAUT) OUTPUT(*PRINT)
DSPUSRPRF USRPRF(user-profile-name) +
          TYPE(*OBJOWN) OUTPUT(*PRINT)
```

   部份 IBM 提供的使用者設定檔非常大，是因爲它們擁有許多的物件。通常不需要列印及分析它們。然而，您應檢查採用 IBM 所提供使用者設定檔之權限的程式，該使用者設定檔具有 *ALLOBJ 特殊權限，例如 QSECOFR 及 QSYS。

有關安全性審核的更多明細，請參閱 *Security Reference* 一書的第 9 章。

分析物件權限

您可使用下列方法以判定何者具有系統檔案庫的權限：

1. 使用 DSPOBJD 指令列示系統上所有的檔案庫：

```
DSPOBJD OBJ(QSYS/*ALL) OBJTYPE(*LIB) ASPDEV(*ALLAVL) OUTPUT(*PRINT)
```

   註: 在獨立的輔助儲存體儲存區 (ASP) 中不是 AVAILABLE 狀態的檔案庫，將無法利用這個指令來顯示。
2. 使用「顯示物件權限 (DSPOBJAUT)」指令以列出特定檔案庫的權限：

```
DSPOBJAUT OBJ(QSYS/library-name) OBJTYPE(*LIB) +
          ASPDEV(asp-device-name) OUTPUT(*PRINT)
```

3. 使用「顯示檔案庫 (DSPLIB)」指令以列出檔案庫中的物件：

```
DSPLIB LIB(QSYS/library-name) ASPDEV(asp-device-name) OUTPUT(*PRINT)
```

您可使用這些報告來判定檔案庫中的內容，以及何者可存取檔案庫。若有需要，您還可使用 DSPOBJAUT 指令來檢視檔案庫中所選取物件的權限。

檢查已改變的物件

您可使用「檢查物件整合性 (CHKOBJITG)」指令來尋找已改變的物件。改變的物件通常表示有人試圖要亂弄您的系統。在某人有下述情況後，您可執行此指令：

- 復置程式到您的系統
- 已使用專用服務工具 (DST)

當您執行此指令時，系統會建立包含任何潛伏的整合性問題之資訊的資料庫檔案。您可檢查由一個設定檔、數個不同設定檔或所有設定檔所擁有的物件。您可尋找物件領域遭改變的物件。您還可以重新計算程式驗證值以尋找類型爲 *PGM、*SRVPGM、*MODULE 及 *SQLPKG 且已遭改變的物件。

CHKOBJITG 程式的執行需要 *AUDIT 特殊權限。因該指令所執行的掃描及計算，使此指令的執行時間較長。您應在系統不忙碌時執行此指令。

註: 擁有許多具有多個專用權限之物件的設定檔會變得很大。擁有者設定檔的大小影響顯示和使用所屬物件權限以及儲存或復置設定檔時的效能。同時也會影響系統

作業。若要防止影響效能或系統作業，請分送物件的所有權到多個設定檔。**請勿將所有的物件都指定到一個擁有者設定檔**。

分析採用權限的程式

採用具有 *ALLOBJ 特殊權限之使用者權限的程式會有安全性曝露之處。可使用下列方法來尋找及檢測這類的程式：

1. 針對每一個具有 *ALLOBJ 特殊權限的使用者，請使用「顯示沿用程式 (DSPPGMADP)」指令列出沿用使用者權限的程式：

   ```
   DSPPGMADP USRPRF(user-profile-name) +
             OUTPUT(*PRINT)
   ```

   註: 主題第 44 頁的『列印選定的使用者設定檔』顯示列出具有 *ALLOBJ 權限之使用者的方法。

2. 使用 DSPOBJAUT 指令來判定授權何人可使用每一個沿用程式，以及程式的公用權限爲何：

   ```
   DSPOBJAUT OBJ(library-name/program-name) +
           OBJTYPE(*PGM) ASPDEV(library-name/program-name) +
             OUTPUT(*PRINT)
   ```

3. 檢測原始程式碼及程式說明以評估下列事項：
   - 程式的使用者在沿用的設定檔下執行時是否無法使用超過權限的功能，例如使用指令行。
   - 程式採用的最小權限層次是否爲功能之所需。使用程式失效的應用程式可使用物件及程式的相同擁有者設定檔來設計。當沿用程式擁有者的權限時，使用者具有應用程式物件的 *ALL 權限。在許多情況下，擁有者設定檔不需要任何的特殊權限。

4. 請使用 DSPOBJD 指令來驗證最近的程式變更：

   ```
   DSPOBJD OBJ(library-name/program-name) +
           OBJTYPE(*PGM) ASPDEV(library-name/program-name) +
           DETAIL(*FULL)
   ```

管理審核日誌及異動日誌接收器

QSYS/QAUDJRN 是專門用於安全性審核的審核日誌。物件不應登載於審核日誌。確定控制不應使用審核日誌。不應將使用者登錄傳送到使用「傳送日誌登錄 (SNDJRNE)」指令或「傳送日誌登錄 (QJOSJRNE)」API 的日誌。

特殊鎖定保護用來確定系統可將審核登錄寫入審核日誌。當審核爲作用中時 (QAUDCTL 系統值非 *NONE)，系統仲裁工作 (QSYSARB) 會保留 QSYS/QAUDJRN 日誌上的鎖定。當審核爲作用中時，您無法在審核日誌上執行以下的特定作業：

- DLTJRN 指令
- ENDJRNxxx 指令
- APYJRNCHG 指令
- RMVJRNCHG 指令
- DMPOBJ 或 DMPSYSOBJ 指令
- 移動日誌
- 復置日誌
- 使用權限的作業，如 GRTOBJAUT 指令

- WRKJRN 指令

記錄於安全性日誌登錄中的資訊說明於 *Security Reference* 一書中。審核日誌中所有的安全性登錄都有一個日誌碼 T。除了安全性登錄之外，系統登錄也會出現在日誌 QAUDJRN 中。這些是具有日誌碼 J 的登錄，它們與在起始程式載入 (IPL) 及日誌接收器上執行的一般作業有關 (例如，保存接收器)。

如果日誌或其目前的接收器發生損壞，導致無法登載審核登錄，QAUDENDACN 系統值會判定系統應採取的動作。損壞日誌或日誌接收器的回復與其他日誌相同。

您可能想要系統管理日誌接收器的變更。當您建立 QAUDJRN 日誌時請指定 MNGRCV(*SYSTEM)，或將日誌變更爲該值。若您指定 MNGRCV(*SYSTEM)，當接收器達到其臨界值大小時，系統會自動分離接收器，並建立及附加新的日誌接收器。這樣稱爲**系統變更-日誌管理**。請參閱「iSeries 資訊中心 --> 系統管理 -> 日誌管理 -> 本端日誌管理 -> 管理日誌」，以獲得詳細資訊。請參閱第 xii 頁的『先決條件與相關資訊』，以獲得存取「iSeries 資訊中心」的資訊。

第 6 章 管理權限

您可以使用一組安全報告來協助追蹤系統中的權限設置狀態。當您開始執行這些報告時，您可以列印每一樣內容 (例如，所有檔案或所有程式的權限)。

在您建立好您的基礎資訊後，您可以定期執行變更的報告版本。變更的版本可協助您識別出需要注意的系統安全變更。例如，您可以執行會顯示每週檔案公用權限的報告。您可以只要求變更過的報告版本。它會顯示系統中每個人都可使用的新檔案，以及前次報告後又變更過公用權限的現有檔案。

您可以使用兩個功能表來執行安全工具：

- 使用 SECTOOLS 功能表可透過交談方式來執行程式。
- 使用 SECBATCH 功能表可透過批次方式來執行程式。SECBATCH 功能表有兩個部份：一部份將工作立即提交給工作佇列，另一部份將工作安排在工作排定程式中。

如果您正在使用「iSeries 領航員」，請遵循下列步驟來執行安全工具：

1. 在「iSeries 領航員」中，展開「伺服器 --> **安全性**」。
2. 在**原則**上按一下滑鼠右鍵，並選取**探勘**來顯示您可以建立及管理的原則清單。

監督物件的公用權限

為能簡單和效能同時兼顧，大部份的系統設置都是讓多數使用者能夠使用多數物件。只在具安全性、安全敏感性的特定物件上，才會明確拒絕使用者存取，並不需要針對每個物件來明確地授權給每個使用者。少數具有高度安全需求的系統則採用相反的方式，只以「必須知道」為根據，來授與物件的權限。這些系統在建立物件時，多半將公用權限設為 *EXCLUDE。

iSeries 是一個以物件為基礎的系統，具有許多不同類型的物件。多數的物件類型不包含敏感性資訊，或不執行與安全相關的功能。作為具有一般安全需要之 iSeries 系統的安全管理者，您也許應該將重心放在需要保護的物件上。對於其它物件類型，您可以只將公用權限設定為應用程式夠用即可，對於多數物件類型而言，這個權限是 *USE。

您可以使用「列印公用權限 (PRTPUBAUT)」指令來列印公共使用者所能存取之物件的相關資訊。(所謂**公共使用者**，意指任何擁有登入權限，而未擁有某個物件之明確權限的使用者。) 當您使用 PRTPUBAUT 指令時，您可以指定您要檢查的物件類型，以及檔案庫或目錄。您可以使用 SECBATCH 和 SECTOOLS 功能表的選項，針對通常會有安全問題的物件類型，來列印其「公用授權物件報告」。您可以定期地列印這份報告的變更版本，檢查需要特別注意的物件。

管理新物件的權限

OS/400 提供的功能可協助您管理系統中之新物件的權限和所有權。當使用者建立新物件時，系統會決定下列事項：

- 誰將擁有這個物件
- 物件的公用權限為何
- 物件是否有任何專用權限

- 物件要放在何處 (哪個檔案庫或目錄)
- 是否要審核對於物件的存取作業

系統會使用系統值、檔案庫參數和使用者設定檔參數來完成這些決定。*iSeries Security Reference* 一書的第 5 章 『指定新物件的權限和所有權』 提供可用選項的若干範例。

您可以使用 PRTUSRPRF 指令來列印會影響新物件之所有權和權限的使用者設定檔參數。第 54 頁的圖 5 顯示這份報告的範例。

監督授權清單

您可以使用授權清單，將安全需求相似的物件分成一組。在概念上，授權清單中可包含使用者及其所擁有之物件權限的列示，這些物件即是列示要保護其安全的物件。授權清單提供一種有效的方法，讓您管理系統中之類似物件的權限。不過，在某些情況中，它會使物件權限的追蹤變得較為困難。

您可以使用「列印專用權限 (PRTPVAUT)」指令來列印授權清單權限的相關資訊。圖 3 顯示一份報告範例。

```
                                   專用權限 (完整報告)
SYSTEM4
授權                                                           列示  -----------物件------------  ------------資料------------
列示         擁有者      主群組      使用者      權限         管理  作業 管理 存在   改變 參照 讀取  新增 更新 刪除   執行
LIST1        QSECOFR     *NONE       *PUBLIC     *EXCLUDE
LIST2        BUDNIKR     *NONE       BUDNIKR     *ALL          X     X    X     X      X    X    X     X    X    X      X
                                     *PUBLIC     *CHANGE             X                             X     X    X    X      X
LIST3        QSECOFR     *NONE       *PUBLIC     *EXCLUDE
LIST4        CJWLDR      *NONE       CJWLDR      *ALL          X     X    X     X      X    X    X     X    X    X      X
                                     GROUP1      *ALL                X    X     X      X    X    X     X    X    X      X
*PUBLIC                 *EXCLUDE
```

圖 3. 授權清單的專用權限報告

這份報告顯示的資訊和「編輯授權清單 (EDTAUTL)」顯示畫面相同。報告的好處是它將所有授權清單的相關資訊放在一起。例如，如果您要設置新物件群組的安全，您可以快速掃瞄報告，查看這些物件中是否有符合您的要求的現存授權清單。

您可以列印報告的變更版本，查看新的授權清單，或前次列印後又變更過其中之權限的授權清單。您也擁有列印每個授權清單所保護之物件列示的選項。圖 4 顯示一份授權清單的報告範例：

```
                      顯示授權清單物件
授權清單 . . . . . . . . . . . . . . :   CUSTAUTL
檔案庫 . . . . . . . . . . . . . . . :     QSYS
擁有者 . . . . . . . . . . . . . . . :   AROWNER
主群組 . . . . . . . . . . . . . . . :   *NONE


物件          檔案庫        類型        擁有者        主群組        文字
CUSTMAS       CUSTLIB       *FILE       AROWNER       *NONE
CUSTORD       CUSTORD       *FILE       OEOWNER       *NONE
```

圖 4. 顯示授權清單物件報告

您可以使用這份報告來掌握若干狀況，例如，瞭解授權清單中新增某個使用者的結果 (該使用者將取得哪些權限)。

使用授權清單

「iSeries 領航員」提供了一些安全性功能，這些功能的設計目的是為輔助您開發安全性規劃及原則，並將系統配置為符合貴公司需求。其中一項可用的功能是授權清單的使用。

授權清單有下列特性。
- 授權清單群組物件和類似的安全性基本要求。
- 在概念上，授權清單包含使用者和群組，以及對清單保障之物件的權限。
- 每一個使用者和群組對清單保障的物件可有不同的權限。
- 權限的提供是依清單的方法，而非個別的使用者和群組。

可使用授權清單執行的作業如下。
- 建立授權清單。
- 變更授權清單。
- 新增使用者和群組。
- 變更使用者許可權。
- 顯示受保護的物件。

若要使用此功能，請執行下列步驟。
1. 從「iSeries 領航員」展開「伺服器 --> 安全性」。您將看見**授權清單**及**原則**。
2. 在**授權清單**上按一下滑鼠右鍵，並選取**新授權清單**。**新增授權清單**可讓您執行下列事項。
   - **使用**：可存取物件屬性及物件的用法。供檢視用，不變更物件。
   - **變更**：可變更物件的內容 (有部份例外)。
   - **全部**：允許物件上的所有作業，擁有者所限制者除外。使用者或群組可控制的存在、指定物件的安全、變更物件及執行物件上的基本功能。使用者或群組也可變更物件的所有權。
   - **排除**：禁止物件上的所有作業。具有許可權的使用者和群組皆不得存取物件或執行物件的作業。指定具有公用權限者不允許使用物件。

當使用授權清單時，您將要授與物件及資料的許可權。以下為您可選擇的物件許可權。
- **作業**：提供查閱物件說明的許可權，並依使用者或群組對物件的許可權來決定該如何使用物件。
- **管理**：提供許可權以指定物件的安全性、移動或更名物件及新增資料庫檔案的成員。
- **存在性**：提供許可權以控制物件的存在性及所有權。使用者或群組可刪除物件、釋放物件的儲存體、執行物件的儲存及復置，以及轉送物件的所有權。若使用者或群組具有特殊的儲存許可權，則使用者或群組不需存在性許可權。
- **變更** (僅適用於資料庫檔案及 SQL 資料包)：提供變更物件屬性所需的許可權。若使用者或群組在資料庫檔案上具有此許可權，則使用者或群組可新增及除去觸發程式、新增及除去參照和唯一限制，以及變更資料庫檔案的屬性。若使用者或群組在 SQL 資料包上具有此許可權，則使用者或群組可變更 SQL 資料包的屬性。目前使用的許可權僅適用於資料庫檔案及 SQL 資料包。
- **參照** (僅適用於資料庫檔案及 SQL 資料包)：提供從另一個物件參照一項物件所需的許可權，如在該物件上的作業可能由其他物件所限制。若使用者或群組在實體檔上具有此許可權，則使用者或群組可在身為父節點的實體檔中新增參照限制。目前已使用的許可權僅適用於資料庫檔案。

以下為您可選擇的資料許可權。
- **讀取**：提供取得及顯示物件內容所需的許可權，如檢視檔案中的記錄。
- **新增**：提供新增物件中之登錄的許可權，如新增訊息佇列中的訊息或新增檔案中的記錄。
- **更新**：提供變更物件中登錄的許可權，如變更檔案中的記錄。
- **刪除**：提供自物件除去登錄的許可權，如自訊息佇列中除去訊息或刪除檔案中的記錄。
- **執行**：提供執行程式、服務程式或 SQL 資料包所需的許可權。使用者可在檔案庫或目錄中尋找物件。

若要取得建立或編輯授權清單之每一個程序的資訊，請使用「iSeries 領航員」中可用的線上說明。

存取「iSeries 領航員」中的原則

您可以使用「iSeries 領航員」來檢視及管理 iSeries 伺服器的原則。「iSeries 領航員」有五種原則範圍：

- **審核原則**
  這可讓您設定特定動作及存取系統上特定資源的監督功能。
- **安全原則**
  這可讓您指定與系統安全相關的安全層次及額外選項。
- **密碼原則**
  這可讓您指定系統的密碼層次。
- **復置原則**
  這可讓您指定如何將特定物件復置在系統上。
- **登入原則**
  這可讓您指定使用者登入系統的方式。

若要使用「iSeries 領航員」來檢視或變更原則，請遵循下列步驟：

1. 從「iSeries 領航員」展開「伺服器 --> **安全性**」。
2. 在**原則**上按一下滑鼠右鍵，並選取**探勘**來顯示您可以建立及管理的原則清單。請參閱「 iSeries 領航員」說明，以取得這些原則的說明。

監督物件的專用權限

SECBATCH 功能表選項：

12 *立即提出* **41** *使用工作排程器*

您可以使用「列印專用權限 (PRTPVAUT)」指令來列印指定的檔案庫中，指定類型之物件的所有專用權限列示。

您可以使用這份報告來協助偵測物件的新權限。它也可以協助您避免讓專用權限架構變得過於複雜而變得難以理解。

監督對輸出及工作佇列的存取

有時安全管理者會在執行對於檔案存取的重要保護工作之後，到了要列印檔案內容時，又忘了曾做過什麼事。iSeries 伺服器爲您提供保護機密之輸出佇列及工作佇列的功能。在您保護輸出佇列之後，未獲授權的使用者即無法對它執行作業，例如檢視或複製待印的機密排存檔。在您保護工作佇列之後，未獲授權的使用者即完全無法將機密性的工作重新引導至非機密性的輸出佇列，也無法取消工作。

SECBATCH 功能表選項：

24，立即提出63，*使用工作排定程式*

「資訊中心」中的*基本系統安全與規劃*以及 *iSeries Security Reference* 書籍都說明了如何保護您的輸出佇列和工作佇列。

您可以使用「列印佇列權限 (PRTQAUT)」指令來列印系統中的工作佇列和輸出佇列的安全設定。之後，您可以對列印機密資訊的列印工作進行評估，並確定它們會前往受保護的輸出佇列和工作佇列。

對於您覺得具有安全敏感性的輸出佇列和工作佇列，您可以比較您的安全設定和 *iSeries Security Reference* 一書「附錄 D」中的資訊。「附錄 D」的表格說明執行不同的輸出佇列和工作佇列功能時，需要哪些設定。

監督特殊權限

當系統中的使用者擁有不必要的特殊權限時，您費心建立的物件權限架構可能會失去作用。當使用者設定檔擁有 *ALLOBJ 特殊權限時，物件權限不具任何意義。擁有 *SPLCTL 特殊權限的使用者可以查看系統中的任何排存檔，不論您費多少心思來保護您的輸出佇列都一樣。具有 *JOBCTL 特殊權限的使用者可以影響系統的作業和重新導入的工作。具有 *SERVICE 特殊權限的使用者，不須透過作業系統，即可使用服務工具來存取資料。

SECBATCH 功能表選項：

29 可以立即提出 68 *可以使用工作排程器*

您可以使用「列印使用者設定檔 (PRTUSRPRF)」指令來列印系統中之使用者設定檔的特殊權限和使用者類別的相關資訊。當您執行報告時，會有幾個選項：
- 所有使用者設定檔
- 具有特定特殊權限的使用者設定檔
- 具有特定使用者類別的使用者設定檔
- 使用者類別和特殊權限不符的使用者設定檔。

第 54 頁的圖 5 顯示一份內容爲所有使用者設定檔的特殊權限的報告範例：

```
                                                                                                          使用者設定檔資訊
報告類型 . . . . . . . . . . . . :   *AUTINFO
選取依據 . . . . . . . . . . . . :   *SPCAUT
特殊權限 . . . . . . . . . . . . :   *ALL
------------------特殊權限------------------
                                *IO                                                                          群組
使用者    群組        *ALL  *AUD  SYS  *JOB  *SAV  *SEC  *SER  *SPL  使用者                      群組          權限          限制
設定檔    設定檔       OBJ   IT   CFG   CTL   SYS   ADM  VICE   CTL  類別        擁有者      權限          類型          功能
USERA     *NONE        X     X     X    X     X     X     X     X    *SECOFR     *USRPRF    *NONE         *PRIVATE      *NO
USERB     *NONE                         X     X                      *PGMR       *USRPRF    *NONE         *PRIVATE      *NO
USERC     *NONE        X     X     X    X     X     X     X     X    *SECOFR     *USRPRF    *NONE         *PRIVATE      *NO
USERD     *NONE                                                      *USER       *USRPRF    *NONE         *PRIVATE      *NO
```

圖 5. 使用者資訊報告：範例 1

除了特殊權限之外，報告中還顯示下列資訊：

- 使用者設定檔是否具有限制的功能。
- 使用者或使用者的群組是否擁有使用者所建立的新物件。
- 對於使用者所建立的新物件，使用者群組會自動收到的權限為何。

圖 6 顯示特殊權限和使用者類別不符的報告範例：

```
                                                        使用者設定檔資訊
報告類型 . . . . . . . . . . . . :   *AUTINFO
選取依據 . . . . . . . . . . . . :   *MISMATCH
--------------------------------特殊權限-------------
                                *IO                                                                          群組
使用者    群組        *ALL  *AUD  SYS  *JOB  *SAV  *SEC  *SER  *SPL  使用者                      群組          權限          限制
設定檔    設定檔       OBJ   IT   CFG   CTL   SYS   ADM  VICE   CTL  類別        擁有者      權限          類型          功能
USERX     *NONE         X                X     X                 X   *SYSOPR     *USRPRF    *NONE         *PRIVATE      *NO
USERY     *NONE                                      X               *USER       *USRPRF    *NONE         *PRIVATE      *NO
USERZ                                                X               *USER       *USRPRF    *NONE         *PRIVATE      *NO
          QPGMR                          X     X
```

圖 6. 使用者資訊報告：範例 2

關於圖 6，請注意下列事項：

- USERX 擁有系統操作員 (*SYSOPR) 使用者類別，但擁有 *ALLOBJ 和 *SPLCTL 特殊權限。
- USERY 擁有使用者 (*USER) 使用者類別，但擁有 *SECADM 特殊權限。
- USERZ 擁有使用者 (*USER) 類別和 *SECADM 特殊權限。您也會看到 USERZ 是 QPGMR 群組的一個成員具有 *JOBCTL 和 *SAVSYS 特殊權限。

您可以定期執行這些報告來協助監督使用者設定檔的管理作業。

監督使用者環境

使用者設定檔的功能之一，是為使用者定義一個環境，包括輸出輸出佇列、起始功能表，以及工作說明。使用者的環境會影響使用者所看到的系統狀態，同時在某個程度上，也會決定使用者所能執行的動作。使用者必須擁有使用者設定檔所指定之物件的權限。不過，如果您的權限架構在進行中，或是不夠嚴格，則使用者設定檔所定義的使用者環境可能會產生您不願見到的結果。以下是若干範例：

SECBATCH 功能表選項：

29 *可以立即提出* **68** *可以使用工作排程器*

- 使用者的工作說明所指定的使用者設定檔，其權限可能會超過使用者。
- 使用者可能會有不具指令行的起始功能表。不過，使用者的岔斷要求鍵處理程式可提供指令行。
- 使用者可能取得執行機密報告的權限。但使用者的輸出所導向的輸出佇列，可能是不該看到該報告的使用者所能使用的輸出佇列。

您可以使用「列印使用者設定檔 (PRTUSRPRF)」指令的 *ENVINFO 選項，協助您監督定義給系統使用者的環境。圖 7 顯示一份報告範例：

```
                                                                                          使用者設定檔資訊
報告類型 . . . . . . . . . . . . :   *ENVINFO
選取依據 . . . . . . . . . . . . :   *USRCLS
                              起始           起始              工作           訊息          輸出           岔斷要求
使用者         現行           功能表/        程式/             說明/          佇列/         佇列/          程式/
設定檔         檔案庫         檔案庫         檔案庫            檔案庫         檔案庫        檔案庫         檔案庫
AUDSECOFR      AUDITOR        MAIN           *NONE             QDFTJOBD       QSYSOPR         *WRKSTN        *SYSVAL
                              *LIBL                            QGPL            QSYS
USERA          *CRTDFT        OEMENU         *NONE             QDFTJOBD       USERA           *WRKSTN        *SYSVAL
                              *LIBL                            QGPL            QUSRSYS
USERB          *CRTDFT        INVMENU        *NONE             QDFTJOBD       USERB           *WRKSTN        *SYSVAL
                              *LIBL                            QGPL            QUSRSYS
USERC          *CRTDFT        PAYROLL        *NONE             QDFTJOBD       USERC           PAYROLL        *SYSVAL
                              *LIBL                            QGPL            QUSRSYS         PRPGMLIB
```

圖 7. 列印使用者設定檔-使用者環境範例

管理服務工具

服務工具是用來配置、管理以及服務您的伺服器。服務工具可以從專用服務工具 (DST) 或系統服務工具 (SST) 存取。需要服務工具使用者 ID 來存取 DST、SST，以及使用 iSeries 領航員功能來使用邏輯分割區 (LPAR) 管理和硬碟機管理。

即使 OS/400 尚未載入，當「授權內碼」啟動時，DST 就可以使用了。SST 是從 OS/400 得到的。下表說明 DST 與 SST 之間的基本差異。

特性	DST	SST
如何存取	在手動 IPL 時經由主控台作實體存取，或在控制面板上選取 21 選項。	使用 QSRV 登入的能力，或利用下列授權經由交談式作業存取： • 授權給 STRSST (啓動 SST) CL 指令。 • 服務特殊權限 (*SERVICE) 或全部物件特殊權限 (*ALLOBJ)。 • 使用 SST 的功能專用權。

何時可用	即使當伺服器僅具備有限功能時仍可用。存取 DST 不需要 OS/400。	當 OS/400 啟動後可用。存取 SST 需要 OS/400。
如何鑑別	需要服務工具使用者 ID 和密碼。	需要服務工具使用者 ID 和密碼。

請參閱「iSeries 資訊中心 --> 安全性 --> 服務工具」，以獲得關於使用服務工具來執行下列作業的相關資訊：

- 以 DST 存取服務工具
- 以 SST 存取服務工具
- 以「iSeries 領航員」存取服務工具
- 建立服務工具使用者 ID
- 變更服務工具使用者 ID 的功能專用權
- 變更服務工具使用者 ID 的說明
- 顯示服務工具使用者 ID
- 啓用或停用服務工具使用者 ID
- 刪除服務工具使用者 ID
- 使用 SST 或 DST 來變更服務工具使用者 ID 和密碼
- 使用 STRSST 來變更您的服務工具使用者 ID 密碼
- 使用變更服務工具使用者 ID (QSYCHGDS) API 來變更服務工具使用者 ID 和密碼
- 重設 QSECOFR OS/400 使用者設定檔密碼
- 重設 QSECOFR 服務工具使用者 ID 和密碼
- 儲存服務工具安全資料
- 復置服務工具安全資料
- 建立 QSECOFR 服務工具使用者 ID 的自身版本
- 配置 DST 的服務工具伺服器
- 配置 OS/400 的服務工具伺服器
- 透過 DST 監視服務功能的使用
- 透過 OS/400 安全性審核日誌來監視服務工具的使用

請參閱第 xii 頁的『先決條件與相關資訊』，以獲得存取「iSeries 資訊中心」的資訊。

第 7 章 使用邏輯分割區安全性 (LPAR)

從下列實例中可以證明，在單一 iSeries 伺服器上開啓多重邏輯分割區有很多好處。

- **維護獨立的系統**：將部份資源 (磁碟儲存單位、處理器、記憶體及 I/O 裝置) 專用於一個分割區，使其可以達到軟體的邏輯隔離。如果經過適當地配置，邏輯分割區也具有部份的硬體失效容差。在單一機器上無法一起執行的交談式及批次工作負荷可加以隔離，並在不同的分割區有效的執行。
- **合併**：一個在邏輯上分割的系統，可以減少企業所需的 iSeries 伺服器系統數量。您可將數個系統合併爲一個單一的邏輯分割系統。這可消除對額外設備的需求及費用。當需求變更時，您可將資源自一個邏輯分割區移位至另一個。
- **建立一個生產及測試的混合環境**：您可以建立一個生產及測試的組合環境。您可在主分割區建立一個單一的產品分割區。有關多重分割區，請參閱下列的*建立多重產品分割區環境*。

  邏輯分割區不是測試分割區就是產品分割區。產品分割區執行您主要的商業應用程式。產品分割區的失敗對企業運作是極大的阻礙，且會浪費時間及金錢。測試分割區測試軟體。當非預期的測試分割區失敗時，將不會造成正常作業的瓦解。
- **建立一個多重生產分割區環境**：您應只將多重生產分割區建立在您的次要分割區。在此狀況下，您指定主分割區來進行分割區管理。
- **熱備份**：若將次要分割區抄寫到同一系統中的另一個邏輯分割區，在分割失敗期間切換到備份，可使不方便性降到最低。此種配置也會將長時間的儲存視窗作用縮至最小。當其他的邏輯分割區仍繼續執行產品作業時，您可使備份分割區離線並儲存之。使用這種熱備份策略需要特殊的軟體。
- **整合叢集**：使用 OptiConnect/400 以及可用性高的應用程式軟體，您的分割系統將可當作整合叢集來執行。您可使用整合叢集來保護您的系統，使在次要分割區內部不會有許多未預期的失敗。

註: 當設置次要分割區時，還需要製作卡位置的額外注意事項。若您爲主控台所選取的「輸入/輸出處理器(IOP)」也具有 LAN 卡，且 LAN 卡不是要與「作業主控台」併用，則它將以主控台來啓動，且您可能無法以原有的用途來使用它。使用「作業主控台」的相關資訊，請參閱第 59 頁的第 8 章, 『iSeries 作業主控台』。

本主題的詳細資訊請參照 iSeries 資訊中心中的「邏輯分割區」。

管理邏輯分割區的安全性

您在分割的系統中所執行之與安全性相關的作業，與在沒有邏輯分割區的系統上執行的相同。然而，當您建立邏輯分割區時，您便使用多個獨立的系統。因此，您將在每一個邏輯分割區上執行相同的作業，而不像在沒有邏輯分割區的系統上只執行一次。

以下是處理邏輯分割區之安全性時應注意的一些基本規則：

- 以一次一個邏輯分割區的方式新增使用者到系統。您得新增使用者到您要他們存取的每一個邏輯分割區。
- 限制使用主分割區專用服務工具 (DST) 及系統服務工具 (SST) 之有權限使用人員的數量。如需 DST 與 SST 的相關資訊，請參照 iSeries 資訊中心中的「使用 iSeries 領航員、DST 以及 SST 來管理邏輯分割區」主題。請參照第 55 頁的『管理服務工具』，以取得使用服務工具使用者設定檔控制分割區活動之存取的資訊。

註: 使用「iSeries 領航員」存取 LPAR 功能之前，必須先起始設定「服務工具伺服器 (STS)」。請參閱「iSeries 資訊中心 --> 安全性 --> 服務工具」以獲得相關資訊。請參閱第 xii 頁的『先決條件與相關資訊』，以獲得存取「iSeries 資訊中心」的資訊。

- 次要分割區無法查看或使用主記憶體及另一個邏輯分割區的硬碟機。
- 次要分割區僅可查看其擁有的硬體資源。
- 主分割區可在 DST 及 SST 的「使用系統分割區」顯示畫面中，查看所有的硬體資源。
- 主分割區作業系統仍僅可查看其本身可用的資源。
- 系統主控台畫面控制器卡分割區。當您將畫面模式設爲「安全」時，在 SST 的「使用分割區狀態」顯示畫面中不會執行任何動作。若要在系統主控台畫面強制 DST，則您必須將模式變更爲「手動」。
- 當您將次要分割區的作業模式設定爲安全時，則是以下列的方法限制其「使用分割區狀態」的用法：
  – 您僅可在次要分割區上使用 DST 來變更分割區狀態；您無法使用 SST 來變更分割區狀態。
  – 您僅可從主分割區使用 DST 或 SST 的「使用分割區狀態」顯示畫面上，強制次要分割區上的 DST。
  – 您僅可使用主分割區上的 DST，將次要分割區模式從安全變更爲任何其他的值。

一旦次要分割區模式不再爲安全，則使用次要分割區上的 DST 及 SST 皆可變更分割區狀態。

有關 iSeries 伺服器安全性的詳細資訊，請參照「安全性參考」手冊及 iSeries 資訊中心的「基本系統安全及規劃頁」。

第 8 章 iSeries 作業主控台

作業主控台可讓您使用您的 PC 來存取及控制您的 iSeries 伺服器。「作業主控台」包括對遠端 PC 撥入無主控台裝置的 iSeries 伺服器支援，讓遠端 PC 成為主控台。當使用作業主控台時，請注意下列事項：

- 您可在作業主控台上執行任何您可在傳統主控台上執行的作業。例如，具有 *SERVICE 或 *ALLOBJ 特殊權限的使用者設定檔就算在停用狀態，仍可登入作業主控台階段作業。
- 作業主控台使用「服務工具使用者設定檔」及密碼，啓用到 iSeries 伺服器的連線。這使得變更您的「服務工具使用者設定檔」及密碼更為重要。駭客可能熟悉預設的「服務工具使用者設定檔」使用者 ID 及密碼，且可能會用它們試圖以遠端主控台階段作業來存取您的 iSeries 伺服器。請參閱第 18 頁的『變更公開的密碼』及第 22 頁的『避免預設密碼』，以取得密碼的秘訣。
- 若要在使用「遠端主控台」時保護您的資訊，請使用 Windows 撥號網路設定的回電選項。
- 當設置次要分割區時，還需要製作卡位置的額外注意事項。若您為主控台所選取的「輸入／輸出處理器(IOP)」也具有 LAN 卡，且 LAN 卡不是要與「作業主控台」併用，則它將啓動來供主控台，且您可能無法以原有的用途來使用它。

在 V5R1 中，將作業主控台強化為可透過區域網路 (LAN) 啓用主控台活動。已強化的鑑別及資料加密提供主控台程序的網路安全性。若要使用具有 LAN 連接的作業主控台，則強烈地建議您應安裝下列產品：

- 在您的 iSeries 伺服器上，安裝「密碼存取提供者」5722-AC2 或 5722-AC3
- 用戶端密碼化，您「作業主控台」PC 上的 5722-CE2 或 5722-CE3

為了將主控台資料加密，iSeries 伺服器必須安裝一種「密碼存取提供者」產品，**且** PC 必須安裝一種「用戶端加密碼」產品。

註: 若未安裝密碼的產品，將不會加密任何資料。

下表彙總可用產品的加密結果：

表 13. 加密結果

在您的 iSeries 伺服器上，安裝的「密碼存取提供者」	**您「作業主控台」 PC 上的「用戶端加密」**	**結果資料加密**
無	無	無
5722-AC2	5722-CE2	56 位元
5722-AC2	5722-CE3	56 位元
5722-AC3	5722-CE2	56 位元
5722-AC3	5722-CE3	128 位元

有關設置及管理 iSeries 作業主控台的其餘資訊，請參閱「iSeries 資訊中心」。

作業主控台安全概觀

作業主控台安全性由下列項目組成：

- 主控台裝置鑑別
- 使用者鑑別
- 資料專用性
- 資料完整性

具有直接連通性的作業主控台，因它的點對點連線，故具有隱含的裝置鑑別、資料專用性及資料完整性。登入主控台顯示器必須有使用者鑑別的安全功能。

主控台裝置鑑別

主控台裝置鑑別可確認實體裝置為主控台。具有直接連通性的作業主控台使用一個類似雙軸主控台的實體連線。使用直接連線的作業主控台，其實際上的安全保障類似雙軸連線，用以控制對實體主控台裝置的存取。

具有 LAN 連接的作業主控台使用 Securd Sockets Layer (SSL) 的版本，其支援裝置及使用者鑑別，但未使用憑證。對於這種形式的連線，裝置鑑別是根據服務工具裝置設定檔。另請參閱第 61 頁以取得進一步的詳細資料。

使用者鑑別

使用者鑑別提供主控台裝置使用者的保證。使用者鑑別相關的所有項目都是相同的，與主控台類型無關。

資料私密性

資料私密性提供主控台資料僅供所需接受者讀取的機密性。具有直接連通性的作業主控台使用類似於雙軸主控台或 LAN 連接的安全網路連線，來保護主控台資料。使用直接連線的作業主控台具有與雙軸連線相同的資料私密性。若實體連線是安全的，則主控台資料也會受保護。

若安裝了適當的的密碼化產品 (ACx 及 CEx)，則具有 LAN 連接的作業主控台會使用安全網路連線。主控台階段作業是根據安裝在 iSeries 伺服器上的密碼化產品及執行「作業主控台」的 PC，儘可能使用最強的加密法。

註: 若未安裝密碼化產品，將不會加密任何資料。

資料完整性

資料完整性提供主控台資料未變更接受者路徑的機密性。具有直接連通性的作業主控台使用類似於雙軸主控台或 LAN 連接的安全網路連線，來保護主控台資料。使用直接連線的作業主控台具有與雙軸連線相同的資料完整性。若實體連線是安全的，則主控台資料也會受保護。

若安裝了適當的的密碼化產品 (ACx 及 CEx)，則具有 LAN 連接的作業主控台會使用安全網路連線。主控台階段作業是根據安裝在 iSeries 伺服器上的密碼化產品及執行「作業主控台」的 PC，儘可能使用最強的加密法。

註: 若未安裝密碼化產品，將不會加密任何資料。

使用具有 LAN 連接的作業主控台

註: 任何的「作業主控台」都可以是主控台，但僅有基於 LAN 配置者使用服務工具使用者設定檔。

iSeries 伺服器附於 QCONSOLE 的預設服務工具裝置設定檔，並具有 QCONSOLE 的預設密碼。具有 LAN 連接的作業主控台將在每一個順利完成的連線期間變更密碼。請參閱『使用作業主控台設定精靈』，取得詳細資訊。

關於 iSeries 具有 LAN 連接的作業主控台的其餘資訊，請參閱「資料中心」中的主題：配置具有 LAN 連接的「作業主控台」。

保護具有 LAN 連接的作業主控台

使用具有 LAN 連接的作業主控台時，建議下列的項目：

- 以主控台屬性建立另一個服務工具裝置設定檔，並將設定檔資訊儲存在安全的位置。
- 在您的 iSeries 伺服器上，安裝「密碼存取提供者」5722-AC2 或 5722-AC3，以及在您的作業主控台 PC 上安裝「用戶端密碼化」5722-CE2 或 5722-CE3。
- 選擇一個不平常的服務裝置資訊密碼。
- 以您保護雙軸主控台或具有直接連通性之作業主控台相同的方式來保護作業主控台。

使用作業主控台設定精靈

當使用具有 LAN 連接的作業主控台時，設定精靈將新增 PC 所需的資訊。設定精靈要求服務工具裝置設定檔、服務工具裝置設定檔密碼及保護服務工具裝置設定檔資訊的密碼。

註: 使用服務工具裝置設定檔資訊密碼來鎖定及解除鎖定 PC 上的服務工具裝置設定檔資訊 (服務工具裝置設定檔及密碼)。

當建立網路連接時，作業主控台設定精靈將提示您輸入存取已加密之服務工具裝置設定檔及密碼的服務裝置資訊密碼。還會提示您輸入有效的服務工具使用者識別及密碼。

第 9 章 偵測可疑的程式

在近年來的電腦發展趨勢中，系統中往往會有來源不可信的程式，或執行不明功能的程式。例如：

- 個人電腦的使用者有時會從其它 PC 使用者取得程式。如果這部 PC 連接於您的 iSeries 系統，則這個程式可能會影響到您的 iSeries 伺服器。
- 連接於網路的使用者也可以取得程式，例如，從公佈欄下載程式。
- 駭客活動日益猖獗。他們往往會公佈他們的方法和結果。而這也會讓守法的程式設計師跟著學壞。

這些趨勢已創造出一種電腦安全問題，稱為**電腦病毒**。病毒是一種程式，它能夠變更其它程式，使該程式中含有它自己的副本。之後，我們便說，這個被變更的程式感染了病毒。此外，病毒也可以執行其它作業來佔用系統資源或摧毀資料。

iSeries 伺服器的架構提供了若干防止感染病毒的保護措施。『防止電腦病毒的侵襲』提供這方面的說明。對於執行未獲授權之功能的程式，iSeries 伺服器的安全管理者應該格外注意。本章的其餘主題說明意圖不良者所可能使用的方法，他們透過這些方法來設置有害的程式，並在您的系統中執行這些程式。這些主題也提供若干要訣，讓您防止執行未獲授權之功能的程式。

安全要訣

物件權限永遠是您的第一線保護。如果您對於物件的保護沒有完善的規劃，您的系統將門戶洞開，無絲毫自我防衛的能力。本資訊說明獲授權的使用者，如何利用您物件權限架構中的漏洞。

防止電腦病毒的侵襲

在受病毒感染的電腦中，有一個程式會造成其它程式的改變。和其它類型的電腦架構比起來，在 iSeries 以物件為基礎的架構中，災害製造者比較不容易製造和散播這類型的病毒。在 iSeries 伺服器中，您使用特定指令和指示，針對每個物件類型來執行作業。您不能使用檔案指令來變更可操作的程式物件 (這正是大部份病毒的作為)。您也無法輕易地建立一個程式來變更另一個程式物件。要達到這個目的，需要很可觀的時間、精力和練習，並且還需要若干通常無法取得的工具和文件。

不過，隨著可加入開放系統環境的各種新 iSeries 伺服器功能的逐漸出現，iSeries 伺服器中某些以物件為基礎的保護功能也不再適用。例如，透過整合檔案系統 (IFS)，使用者可直接操作目錄內的某些物件，例如串流檔。

此外，雖然 iSeries 伺服器架構使得病毒難以在 iSeries 伺服器程式之間傳播，但這個架構無法讓 iSeries 伺服器不會成為病毒的攜帶者。作為檔案伺服器，iSeries 伺服器可儲存許多 PC 使用者所共用的程式。而這些程式中，可能會有某個程式帶有病毒，而 iSeries 伺服器並未偵測出來。如果要防止這類型的病毒感染 iSeries 所連接的 PC，您必須使用 PC 病毒掃瞄軟體。

iSeries 伺服器中的若干功能，可防止使用者利用具有指標功能的低階語言來改變可操作的物件程式：

- 如果您的系統執行安全層次 40 或以上，則整合保護功能中，包括防止對於程式物件的變更。例如，您無法順利執行含有暫停執行 (受保護) 之機器指令的程式。
- 程式驗證值的目的，是要在您復置程式且該程式儲存 (或將會變更) 於另一個系統時，用以提供保護。 *iSeries Security Reference* 一書的第 2 章說明安全層次 40 和以上的整合保護功能。

  註: 程式驗證值並不簡單，但在評估復置到系統的程式時，不能因此而掉以輕心。

此外，還有若干工具可協助您偵測系統中是否介入了改變過的程式：

- 您可以使用「檢查物件整合性 (CHKOBJITG)」指令來掃瞄符合搜尋值的物件 (可操作的物件) ，以確定這些物件未被改變。這和病毒掃瞄功能相似。
- 您可以使用安全審核功能來監督已變更或復置的程式。權限層次系統值的 *PGMFAIL、*SAVRST 和 *SECURITY 等值可提供審核記錄，協助您偵測出將病毒型程式引入系統的企圖。*iSeries Security Reference* 一書的第 9 章和附錄 F 提供關於審核值和審核異動記載登錄的詳細資訊。
- 您可以使用「變更程式 (CHGPGM)」指令的「強迫建立 (FRCCRT)」參數來重新建立已復置系統中的任何程式。系統會使用程式範本來重新建立程式。如果程式物件在編譯好後又變更過，系統會重新建立變更過的物件，並予以置換。如果程式範本含有暫停執行 (受保護) 的指令，則系統無法順利重新建立程式。
- 您可以使用 QFRCCVNRST (復置時強制轉換) 系統值，趁著將程式復置到系統時重新建立它。系統會使用程式範本來重新建立程式。這個系統值提供程式用來重新建立的多種選項。
- 您可使用 QVFYOBJRST (復置時驗證物件) 系統值來防止沒有數位簽章或不具有效數位簽章之程式的復置。當數位簽章無效時，表示自程式開發者簽章後程式已變更。API 可讓您簽章您自己的程式、儲存檔案及串流檔。

有關簽章及其如何保護系統免於侵入的資訊，請參閱第 74 頁的『物件簽署』。

監督沿用權限的使用

在 iSeries 伺服器中，您可以建立一個程式，讓它沿用程式擁有者的權限。這表示執行該程式的任何使用者都和擁有該程式的使用者設定檔具有相同的權限 (專用權限和特殊權限)。

如果您能正確地使用沿用權限，它會是一個非常有價值的安全工具。例如第 40 頁的『以物件安全性增強功能表存取控制』所說明的，如何結合沿用權限和功能表來協助您跨越功能表存取控制。您可以使用沿用權限來保護您的重要檔案，讓您未核可的應用程式，無法在仍容許查詢這些檔案時，變更這些檔案。

作爲一個安全管理者，您應該確定以正確的方式來使用沿用的權限：

- 被程式沿用權限的使用者設定檔，應該只有剛好足以執行必要功能的權限，不能有過度的權限。當使用者設定檔擁有 *ALLOBJ 特殊權限或重要物件時，如果程式要沿用這個使用者設定檔的權限，您必須格外小心。
- 沿用權限的程式應該有其特定而有限的功能，並且不應該提供指令登錄功能。
- 沿用權限的程式應該受到恰當的安全保護。

- 沿用權限的過度使用，可能會對系統效能造成負面的影響。如果您要避免發生效能的問題，請詳閱 *iSeries Security Reference* 一書的第 5 章，其中有關於沿用權限之使用的權限檢查流程圖和建議事項。

SECBATCH 功能表選項：

1，*立即提出* **40，使用工作排定程式**

您可以使用「列印沿用物件 (PRTADPOBJ)」指令 (SECTOOLS 功能表中的選項 21)，協助您監督系統中沿用的權限的使用。

這份報告會顯示指定使用者設定檔的特殊權限、沿用該使用者設定檔權限的程式、以及使用設定檔權限的 ASP 裝置。在您建立好資訊基礎後，您可以定期地列印沿用之物件報表的變更版本。它會列出沿用權限的新程式，以及前次執行報表後又變更過並沿用權限的程式。

如果您懷疑系統中發生沿用權限誤用的情況，您可以將 QAUDLVL 系統值設定為 *PGMADP。在這個值產生作用後，每當使用或結束沿用權限的程式時，系統都會建立一個審核異動記載登錄。登錄中包括啓動程式的使用者名稱和程式名稱。

限制沿用權限的使用

在執行 iSeries 程式時，程式可依照以下兩個方式，透過沿用的權限來存取物件：

- 程式本身可以沿用其擁有者的權限。這是在程式或服務程式的「使用者設定檔 (USRPRF)」參數中指定的。
- 程式可以使用 (繼承) 仍在工作呼叫堆疊中之前一個程式的權限。即使程式本身沒有沿用權限，它也可以繼續先前程式的沿用權限。程式或服務程式的「使用沿用權限 (USEADPAUT)」參數可以控制程式是否繼承程式堆疊中之先前程式的沿用權限。

以下範例說明使用先前程式的沿用權限如何作業。

假設 ICOWNER 使用者設定檔擁有 ITEM 檔的 *CHANGE 權限，並且 ITEM 檔的公用權限是 *USE。沒有任何其它使用者設定檔擁有 ITEM 檔的明確定義的權限。表 14 顯示三個使用 ITEM 檔之程式的屬性：

表 14. 使用沿用權限 (USEADPAUT) 範例

程式名稱	程式擁有者	USRPRF 值	USEADPAUT 值
PGMA	ICOWNER	*OWNER	*YES
PGMB	ICOWNER	*USER	*YES
PGMC	ICOWNER	*USER	*NO

範例 1 - 沿用權限：

1. 「使用者 A」執行 PGMA 程式。
2. PGMA 程式試圖以更新功能來開啓 ITEM 檔。

結果：嘗試順利完成。「使用者 A」擁有 ITEM 檔的 *CHANGE 權限，因為 PGMA 沿用了 ICOWNER 的權限。

範例 2 - 使用沿用權限：

1. 「使用者 A」執行 PGMA 程式。
2. PGMA 程式呼叫 PGMB 程式。
3. PGMB 程式試圖以更新功能來開啓 ITEM 檔。

結果：嘗試順利完成。雖然 PGMB 程式未沿用權限 (*USRPRF 是 *USER)，仍容許使用先前的沿用權限 (*USEADPAUT 是 *YES)。PGMA 程式仍在程式堆疊中。因此，「使用者 A」取得 ITEM 檔的 *CHANGE 存取權，因爲 PGMA 沿用了 ICOWNER 的權限。

範例 3 - 未使用沿用權限：

1. 「使用者 A」執行 PGMA 程式。
2. PGMA 程式呼叫 PGMC 程式。
3. PGMC 程式試圖以更新功能來開啓 ITEM 檔。

結果：權限失效。PGMC 程式未沿用權限。PGMC 程式也不容許使用先前程式的沿用權限。雖然 PGMA 仍在呼叫堆疊中，但未使用它的沿用權限。

防止新程式使用沿用的權限

將沿用權限傳遞至堆疊中較後面的程式，可讓內行的程式設計師有機會建立「特洛依木馬」。「特洛依木馬」程式可以透過堆疊中較前面的程式來取得破壞行動所需要的權限。如果要防止發生這個情況，您可以限制哪些使用者可以建立程式，並使用先前程式的沿用權限。

當您建立好新的程式時，系統會自動將 USEADPAUT 參數設爲 *YES。如果您不要程式繼承沿用的權限，您必須使用「變更程式 (CHGPGM)」指令或「變更服務程式 (CHGSRVPGM)」指令，將 USEADPAUT 參數設定爲 *NO。

您可以使用授權清單和「使用沿用權限 (QUSEADPAUT)」系統值，來控制哪些使用者可以建立程式並繼承沿用的權限。當您指定 QUSEADPAUT 系統值中的授權清單名稱時，系統會使用這個授權清單來判斷如何建立新的程式。

當使用者建立程式或服務程式時，系統會檢查使用者的授權清單權限。如果使用者擁有 *USE 權限，則新程式的 USEADPAUT 參數會設爲 *YES。如果使用者沒有 *USE 權限，則 USEADPAUT 參數會設爲 *NO。使用者的授權清單權限不能來自沿用的權限。

您在 QUSEADPAUT 系統值內指定的授權清單也會控制使用者是否可使用 CHGxxx 指令來設定程式或服務程式的 USEADPAUT 值。

註:

1. 您不需要呼叫您的授權清單 QUESADPAUT。您可以不同的名稱建立權限清單。之後，再對 QUSEADPAUT 系統值指定該授權清單。請在這個範例的指令中，代換爲您的授權清單名稱。
2. QUSEADPAUT 系統值不會影響您系統中現有的程式。使用 CGHPGM 指令或 CHGSRVPGM 指令，對現存的程式設定 USEADPAUT 參數。

較嚴格的環境： 如果您要在多數使用者建立新程式時，讓 USEADPAUT 參數設爲 *NO，請執行下列動作：

1. 如果要將授權清單的公用權限設爲 *EXCLUDE，請鍵入下列指令：

```
CHGAUTLE AUTL(QUSEADPAUT) USER(*PUBLIC)
   AUT(*EXCLUDE)
```

2. 如果要設置特定使用者，讓他們在建立程式時使用先前程式的沿用權限，請鍵入下列指令：

```
ADDAUTLE AUTL(QUSEADPAUT) USER(user-name)
   AUT(*USE)
```

較不嚴格的環境： 如果您要在多數使用者建立新程式時，讓 USEADPAUT 參數設為 *YES，請執行下列動作：

1. 保留授權清單公用權限的設定 *USE。
2. 如果要防止特定使用者，不讓他們在建立程式時使用先前程式的沿用權限，請鍵入下列指令：

```
ADDAUTLE AUTL(QUSEADPAUT)
   USER(user-name) AUT(*EXCLUDE)
```

監督觸發程式的使用

DB2® UDB 提供結合觸發程式及資料庫檔案的功能。在高功能資料庫管理程式之間，觸發程式功能非常普遍。

您將觸發程式關聯於資料庫檔案時，會指定觸發程式的執行時間。例如，您可設置客戶訂購檔，讓它在每次有新記錄加入檔案時，執行觸發程式。當客戶的未清餘額超出信用額度時，觸發程式可列印一份傳送給客戶的提示信函，並傳送一則訊息給信用管理程式。

不論是提供應用程式功能，或是管理資訊，觸發程式都是一種具有極高效能的方式。對於意圖不軌的使用者而言，他可以使用觸發程式所提供的功能，在您的系統中建立『特洛依木馬』。其中可能會藏有破壞性的程式，等到系統資料庫檔案出現某些事件時，即會發動攻擊。

註: 特洛依木馬是一個歷史典故，它是一座大型的中空木馬，裡面藏了許多希臘士兵。當木馬被帶進特洛依城時，裡面的士兵便爬出木馬，展開與特洛依人的戰鬥。在電腦世界裡，隱藏破壞性功能的程式，也常稱為「特洛依木馬」。

SECBATCH 功能表選項：

27，*立即提出* **66**，*使用工作排定程式*

在系統休眠時，會限制新增觸發程式到資料庫檔案的功能。如果您的物件權限管理非常謹慎，一般的使用者不會有足夠的權限來新增觸發程式到資料庫檔案。(*iSeries Security Reference* 一書的「附錄 D」說明所有指令需要的權限，包括「新增實體檔觸發程式 (ADDPFTRG)」指令。)

您可以使用「列印觸發程式 (PRTTRGPGM)」指令來列印一份特定檔案庫或所有檔案庫中之所有觸發程式的列示。

您可以使用起始報表來評估已存在於系統中的任何觸發程式。之後，您可以定期列印報表，查看系統是否新增了新的觸發程式。

在您評估觸發程式時，請考慮下列事項：

- 誰建立觸發程式？您可以使用「顯示物件說明 (DSPOBJD)」指令來判斷。
- 程式執行哪些動作？您必須查看來源程式，或與程式建立者討論，才能形成判斷。例如，觸發程式是否會檢查誰是使用者？觸發程式也可能正在等待特定的使用者 (QSECOFR)，以便取得對資源的存取權。

在建立好基礎資訊後，您可以定期列印變更的報表，監督系統中所新增的新觸發程式。

檢查隱藏程式

要將特洛依木馬引入您系統中，觸發程式不是唯一的方式。觸發程式是**跳出程式**的一個例子。當發生特定事件時，例如在觸發程式的情況中出現檔案更新，系統會執行關聯於該事件的跳出程式。

表 15 說明您系統中所可能有的跳出程式例子。對於這些跳出程式，您應該使用和觸發程式相同的方法來評估其用法和內容。

註: 表 15 不是所有可能的跳出程式之完整列示。

.

表 15. 系統提供的跳出程式

程式名稱	程式執行時機
使用者在 DDMACC 網路屬性中指定的名稱。	使用者試圖開啓您系統上的 DDM 檔案或進行 DRDA 連線時。
使用者在 PCSACC 網路屬性中指定的名稱。	使用者試圖使用 Original Client 的 Client Access™ 功能來存取您系統上的物件時。
使用者在 QPWDVLDPGM 系統值中指定的名稱。	使用者執行「變更密碼」功能時。
使用者在 QRMTSIGN 系統值中指定的名稱。	使用者試圖從遠端系統，以交談方式來登入。
QSYS/QEZUSRCLNP	執行自動清除功能時。
使用者在 CHGBCKUP 指令的 EXITPGM 參數中指定的名稱。	在您使用「作業輔助」備份功能時。
使用者在 CRTPRDLOD 中指定的名稱。	在儲存、復置或刪除以這個指令來建立的產品之前或之後。
使用者在 CHGMSGD 指令的 DFTPGM 參數中指定名稱。	如果將預設程式指定給某個訊息，則系統會在發出訊息時執行程式。由於一般系統上的大量訊息說明，因此很難監督預設程式的使用情況。如果要防止公共使用者新增訊息的預設程式，請考慮將訊息檔 (*MSGF 物件) 的公用權限設定為 *USE。
使用者在 STREML3270 指令的 FKEYPGM 參數中指定的名稱。	在 3270 裝置模擬階段作業期間，使用者按下某個功能鍵之時。當跳出程式結束時，系統會返回對於 3270 裝置模擬階段作業的控制。
使用者在效能監督指令的 EXITPGM 參數中指定的名稱。	處理下列指令所收集的資料：STRPFRMON、ENDPFRMON、ADDPFRCOL 和 CHGPFRCOL。 程式在資料收集完成時執行。
使用者在 RCVJRNE 指令的 EXITPGM 參數中指定的名稱。	用於自指定日誌及日誌接收器讀取每一個日誌登錄或日誌登錄群組。
使用者在 QTNADDCR API 中指定的名稱。	在 COMMIT 或 ROLLBACK 作業期間。

表 15. 系統提供的跳出程式 (繼續)

程式名稱	程式執行時機
使用者在 QHFRGFS API 中指定的名稱。	如果要執行檔案系統功能。
使用者在印表機裝置說明的 SEPPGM 參數中指定的名稱。	決定要在排存檔或列印工作之前或之後的分隔頁上列印的內容。
QGPL/QUSCLSXT	在關閉資料庫檔案，容許擷取檔案用法資訊之時。
使用者在邏輯檔案的 FMTSLR 參數中指定的名稱。	當記錄寫入資料庫檔案，而記錄格式名稱不包括在高階語言程式內之時。選取器程式會將收到的記錄當作輸入，決定所使用的記錄格式，並將它傳回資料庫中。
使用者在 QATNPGM 系統值、使用者設定檔的 ATNPGM 參數，或 SETATNPGM 指令的 PGM 參數中指定的名稱。	當使用者按下「岔斷要求」鍵時。
使用者在 TRCJOB 指令的 EXITPGM 參數中指定的名稱。	在啓動「追蹤工作」程序之前。

對於可讓您指定跳出程式的指令，您應該確定指令的預設值未被變更來指定跳出程式。您也應該讓這些指令的公用權限不足以變更指令預設值。CHGCMDDFT 指令需要對於指令的 *OBJMGT 權限。您不需要使用 *OBJMGT 權限來執行指令。

評估登記的跳出程式

您可以使用系統登記功能來登記發生特定事件時所應執行的跳出程式。如果要列出系統中的系統登記資訊，請鍵入 `WRKREGINF OUTPUT(*PRINT)` 。圖 8 顯示一份報告範例：

```
                        使用系統登記資訊
跳出程式 . . . . . . . . . . . . . . . . :   QIBM_QGW_NJEOUTBOUND
跳出程式格式 . . . . . . . . . . . . . . :   NJEO0100
登記的跳出程式 . . . . . . . . . . . . . :   *YES
容許取消登錄 . . . . . . . . . . . . . . :  *YES
跳出程式最大數目 . . . . . . . . . . . . :  *NOMAX
跳出程式現行數目 . . . . . . . . . . . . :  0
新增作業前置處理 . . . . . . . . . . . . :  *NONE
  檔案庫 . . . . . . . . . . . . . . . . :
  格式 . . . . . . . . . . . . . . . . . :
除去作業前置處理 . . . . . . . . . . . . :  *NONE
  檔案庫 . . . . . . . . . . . . . . . . :
  格式 . . . . . . . . . . . . . . . . . :
擷取作業前置處理 . . . . . . . . . . . . :  *NONE
  檔案庫 . . . . . . . . . . . . . . . . :
```

圖 8. 使用系統登記資訊 - 範例

報告會顯示系統中的每個跳出程式目前是否有已登記的跳出程式。當跳出程式有已登記的跳出程式時，您可以從 WRKREGINF 的顯示版本中選取選項 8 (顯示程式) ，以顯示程式的相關資訊：

```
                      使用系統登記資訊

請鍵入選項，然後按 Enter 鍵。
5=顯示跳出程式            8=使用跳出程式


                             跳出程式
Opt  跳出程式                   格式         已登記    文字
     QIBM_QGW_NJEOUTBOUND   NJE00100     *YES     網路工作登錄離埠 ex
8    QIBM_QHQ_DTAQ          DTAQ0100     *YES     原始資料佇列伺服器
     QIBM_QLZP_LICENSE      LICM0100     *YES     原始授權管理伺服器
     QIBM_QMF_MESSAGE       MESS0100     *YES     原始訊息伺服器
     QIBM_QNPS_ENTRY        ENTR0100     *YES     網路列印伺服器 - 登錄
     QIBM_QNPS_SPLF         SPLF0100     *YES     網路列印伺服器 - 排存
     QIBM_QNS_CRADDACT      ADDA0100     *YES     新增 CRQ 說明活動
     QIBM_QNS_CRCHGACT      CHGA0100     *YES     變更 CRQ 說明活動
```

請使用和其它跳出程式和觸發程式相同的方法來評估這些跳出程式。

檢查排定的程式

iSeries 提供許多方法，使您可稍後執行排定的工作，包括工作排程器。這些方法通常都不代表安全上的漏洞，因爲排定工作的使用者必須擁有相同的必要權限，才能提出批次執行的工作。

不過，您應該定期地檢查排定在未來執行的工作。因爲，如果已離職的員工心懷不平，他可能會使用這個方法來排定執行災難性的工作。

限制儲存和復置功能

大部份使用者不需要在您的系統中儲存和復置物件。儲存指令可用來將您企業組織的重要資產複製到媒體或另一個系統中。大部份的儲存指令都支援在未存取媒體或儲存/復置裝置的情況下，將可傳送至另一個系統的檔案儲存到另一個系統中 (使用 SNDNETF 檔案指令)。

復置指令可用來將未獲授權的物件，例如程式、指令和檔案，復置到您的系統中。您也可以在未存取媒體或儲存/復置裝置的情況下，使用儲存檔來復置資訊。您可以使用 SNDNETF 指令或 FTP 功能來復置另一個系統中的儲存檔。

以下是在您的系統中限制儲存和復置作業的建議事項：

- 控制哪些使用者擁有 *SAVSYS 特殊權限。*SAVSYS 特殊權限可讓使用者在沒有必要的物件權限時，也能儲存及復置物件。
- 控制實體存取以儲存及復置裝置。
- 限制對於儲存和復置指令的存取。當您安裝 OS/400 授權程式時，RSTxxx 指令的公用權限是 *EXCLUDE。SAVxxx 指令的公用權限是 *USE。請考慮將 SAVxxx 指令的公用權限變更爲 *EXCLUDE。小心限制您授與 RSTxxx 指令權限的使用者。
- 使用 QALWOBJRST 系統值以限制系統狀態程式、採用權限的程式及有驗證錯誤之物件的復置。
- 使用 QVFYOBJRST 系統值來控制您系統上正簽章物件的復置。
- 使用 QFRCCVNRST 系統值，控制在系統上所復置特定物件的重建。

- 使用安全審核來監督復置作業。在 QAUDLVL 系統值內併入 *SAVRST，並定期地列印復置作業所建立的審核記錄。 (*iSeries Security Reference* 一書的第 9 章和「附錄 F」提供審核登錄作業的詳細資訊。)

檢查在受保護檔案庫內的使用者物件

每個 iSeries 伺服器工作都有一份檔案庫清單。如果物件名稱未指定檔案庫名稱時，檔案庫列示會決定系統搜尋物件的次序。例如，當您呼叫未指定所在位置的程式時，系統會依照次序來搜尋您的檔案庫列示，並執行它找到的第一份程式。

iSeries Security Reference 一書提供關於檔案庫列示和不具檔案庫名稱的呼叫程式 (**未完整定義的呼叫**) 之安全漏洞的詳細資訊。它也提供若干建議事項，協助您控制檔案庫列示的內容和變更系統檔案庫列示的能力。

為讓您的系統正確執行，某些系統檔案庫 (如 QSYS 和 QGPL) 必須在每個工作的檔案庫列示中。您應該使用物件權限來控制哪些使用者可將程式加入這些檔案庫中。這有助於限止使用者利用檔案庫列示較後部份的檔案庫中之程式的名稱，將偽裝的程式放在較前面的某個檔案庫內。

您也應該評估哪些使用者擁有 CHGSYSLIBL 指令的權限，並監督安全審核異動記載中的 SV 記錄。居心不良的使用者可檔案庫列示中，將某個檔案庫放在 QSYS 前面，使其它使用者執行未獲授權但和 IBM 所提供之指令同名的指令。

SECBATCH 功能表選項：

28，*立即提出* **67**，*使用工作排定程式*

您可以使用「列印使用者物件 (PRTUSROBJ)」指令，來列印指定之檔案庫中的使用者物件 (不是 IBM 建立的物件) 的清單。之後，您可以評估列示中的程式，判斷是哪個使用者建立它們，以及它們能執行哪些功能。

非程式的使用者物件，當它們在系統檔案庫之內時，也代表一種安全上的漏洞。例如，如果某個程式將機密資料寫入檔案中，但未適當地限定檔案名稱，此時，這個程式很可能會受到欺騙，並在系統檔案庫內開啓該檔案的虛假版本。

第 10 章 防止及偵測駭客入侵

這部份的資訊蒐集各種協助您偵測潛在安全性漏洞及惡作劇的要訣。

實體安全性

您的主機是企業的一項重要資產，同時也是系統的潛在門戶。主機內的某些元件體機可能非常小，但價值則非常昂貴。您應該將主機放在管制良好的地方，防止他人取走有價值的主機元件。

主機有一個控制面板，可在工作站之外執行基本功能。例如，您可以使用控制面板來執行下列動作：

- 停止系統。
- 啓動系統。
- 載入作業系統。
- 啓動服務功能。

所有這些功能可能會干擾您的使用者。它們也都代表潛在的系統安全漏洞。您可以使用系統所附送的鑰匙鎖來控制容許執行這些活動的時機。若要防止他人使用控制台，請將鑰匙鎖置於「安全」的位置，取出鑰匙，將之存放在安全的地方。

註:

1. 如果您需要在系統中執行遠端 IPL 或執行遠端診斷，則鑰匙鎖可能需要選取其它設定。iSeries 資訊中心提供鑰匙鎖設定值的相關資訊 (詳細資訊請參閱第 xii 頁的『先決條件與相關資訊』)。
2. 並非所有機型都附有鑰匙鎖，以它為標準配備特性。

監督使用者設定檔活動

使用者設定檔可爲您的系統提供登錄。使用者設定檔內的參數會決定使用者的環境和使用者的安全特性。作爲一個安全管理者，您必須控制和審核系統中的使用者設定檔所發生的變更。

您可以設置安全審核，讓系統記錄使用者設定檔所發生的變更。您可以使用 DSPAUDJRNE 指令來列印這些變更的報告。

您可以建立跳出程式來評估對於使用者設定檔的要求動作。表 16 顯示可用於使用者設定檔指令的跳出程式。

表 16. 使用者設定檔活動的跳出點

使用者設定檔指令	跳出點名稱
建立使用者設定檔 (CRTUSRPRF)	QIBM_QSY_CRT_PROFILE
變更使用者設定檔 (CHGUSRPRF)	QIBM_QSY_CHG_PROFILE
刪除使用者設定檔 (DLTUSRPRF)	QIBM_QSY_DLT_PROFILE
復置使用者設定檔 (RSTUSRPRF)	QIBM_QSY_RST_PROFILE

您的跳出程式可執行若干作業，例如，尋找可能會讓使用者執行未授權之程式版本的變更。這些變更可能會指定不同的工作說明，或是新的現行檔案庫。根據跳出程式收到的資訊，您的跳出程式可能會通知訊息佇列，也可能採取某些動作 (如變更或停用使用者設定檔)。

iSeries Security Reference 一書提供關於使用者設定檔動作之跳出程式的詳細資訊。

物件簽署

如果有人可略過您的安全性預防措施，將擅改的資料導入您的系統，則您所作的任何安全性預防措施都不具意義。iSeries 伺服器擁有許多內建的功能，可以避免讓任何篡改軟體載入到您的系統，並偵測系統中任何這類已存在的軟體。新增在 V5R1 的一項技術就是物件簽章。

物件簽署是 iSeries 伺服器應用密碼的概念，也就是所謂的「數位簽章」。這個理念是因而產生的：一旦軟體的生產者在準備好將軟體交給客戶時，對軟體進行「簽章」。此簽章不保證軟體執行任何特定的功能。然而，它提供證明軟體是來自生產者的簽章，且該軟體在生產及簽章後未經變更。若軟體已藉由網際網路傳輸或儲存在您認為已遭修改的媒體上時，這就更為重要。

使用數位簽章對可載入您系統的軟體提供更多的控制，並可讓您在萬一載入它後，有更大的能力可以偵測到變更。新的系統值「驗證物件復置 (QVFYOBJRST)」提供您設定限制原則的機制，此原則需要所有載入系統的軟體，都經過已知軟體來源的簽章。您也可選擇更開放的原則並簡化簽章的驗證。

所有 OS/400 軟體、選項的軟體，以及 iSeries 伺服器授權程式都已經由系統可靠來源簽署。這些簽章可以協助系統維持其完整性，而且當修訂程式套用到系統時都會先檢查它們，以確保該修訂程式來自系統可靠來源，同時也確保它在過程中不會變更。這些簽章也可在軟體在系統上時加以檢查。CHKOBJITG (檢查物件完整性) 指令已擴充除了為檢查系統上物件之其他完整性特性之外還檢查簽章。此外，「數位憑證管理程式」也有可用來檢查物件上簽章的畫面，包括作業系統中的物件。

一旦作業系統經簽章後，您可使用數位簽章來保護您企業中重要軟體的完整性。您可購買由軟體提供者簽章的軟體，或是簽章您已購買或撰寫的軟體。然後在您安全原則中指定期地使用 CHKOBJITG 或「數位憑證管理程式」來驗證軟體上的簽章仍為有效，亦即物件在簽章後未遭變更。您進一步可能需要在系統復置時，所有的軟體必須經由您或已知來源簽章。但因為大部分 iSeries 伺服器軟體都不是由 IBM 所開發，所以尚未簽署，這對您的系統而言可能有所限制。新的數位簽章支援提供您決定保護軟體完整性程度的彈性。

保護軟體的數位簽章只是數位憑證的一種用法。您可在資訊中心中的「數位憑證管理」主題中，找到有關管理數位憑證的相關資訊 (詳細資料請參閱第 xii 頁的『先決條件與相關資訊』)。

監督子系統說明

當您啓動 iSeries 伺服器中的子系統時，系統會建立一個工作環境，讓您進入系統並執行作業。子系統說明負責定義環境的狀態。因此，子系統說明可提供機會給居心不良的使用者。災害製造者可能會使用子系統說明來自動建立程式，或造成不需要使用者設定檔即可登入的情況。

當您執行「取消公用權限 (RVKPUBAUT)」指令時，系統會將子系統說明指令的公用權限設為 *EXCLUDE。這可避免讓未取得特定授權的使用者 (以及沒有 *ALLOBJ 特殊權限的使用者) 變更或建立子系統說明。

以下主題提供複查目前存在於系統中之子系統說明的建議事項。您可以使用「使用子系統說明 (WRKSBSD)」指令來建立所有子系統說明的清單。當您從清單中選取 5 (顯示) 時，您會看到您選取之系統說明的功能表。它會顯示子系統環境各個部份的列示。

您選取選項來查看各部份的詳細資料。請使用「變更子系統說明 (CHGSBSD)」指令來變更功能表中的前兩個項目。如果要變更其它項目，請針對登錄類型來使用適當的新增、除去或變更指令。例如，如果要變更工作站登錄，請使用「變更工作站登錄 (CHGWSE)」指令。

Work Management 一書提供關於子系統說明之使用的詳細資訊。它也列出 IBM 所提供之子系統說明的出貨值。

自動啓動工作登錄

自動啓動工作登錄包含工作說明的名稱。工作登錄可包含會導致執行程式或指令的要求資料 (RQSDTA)。例如，RQSDTA 可能是 `CALL LIB1/PROGRAM1`。每當子系統啓動時，系統都會執行檔案庫 LIB1 中的程式 PROGRAM1。

請查看您的自動啓動工作登錄和相關的工作說明。請確定您瞭解當啓動子系統時，將自動執行之任何程式的功能。

工作站名稱及工作站類型

當子系統啓動時，它會配置它的工作站名稱登錄和工作站類型登錄中所列出的所有未配置的工作站。當使用者登入時，使用者會登入到已配置工作站的子系統。

工作站登錄會顯示在該工作站中啓動某個工作時，將會使用哪個工作說明。工作登錄可包含會導致執行程式或指令的要求資料。例如，RQSDTA 參數可能是 `CALL LIB1/PROGRAM1`。每當使用者登入該子系統的某個工作站時，系統都會執行 LIB1 中的 PROGRAM1。

請查看您的工作站登錄和相關的工作說明。確定沒有任何人新增或更新任何登錄來執行您並不知道的程式。

工作站登錄也可能會指定預設的使用者設定檔。對特定子系統配置而言，這可讓某些使用者只需要按下 Enter 鍵即可登入。如果系統的安全層次 (QSECURITY 系統值) 小於 40，您應該複查預設使用者的工作站登錄。

工作佇列登錄

當子系統啓動時，它會配置子系統說明中所列出的任何未配置的工作佇列。工作佇列登錄並不提供任何直接的安全漏洞。不過，它們會使某些使用者有機會讓工作在非預期的環境中執行，而變更了系統的效能。

您應該定期地複查子系統說明中的工作佇列登錄，以確定批次工作是在您預期的場合中執行。

遞送登錄

遞送登錄負責定義工作進入子系統後所執行的動作。子系統會使用所有工作類型的遞送登錄：批次、交談和通訊工作。遞送登錄指定的事項如下：

- 工作類別。和工作佇列登錄一樣，工作的相關類別可影響它的效能，但並不代表安全上的漏洞。
- 啓動工作時所執行的程式。請查看遞送登錄，並確定沒有任何人新增或更新任何登錄來執行您並不知道的程式。

通訊登錄及遠端位置名稱

當通訊工作進入您的系統時，系統會使用作用子系統的通訊登錄和遠端位置名稱登錄，來決定如何執行通訊工作。請查看這些登錄的下列事項：

- 所有子系統都能夠執行通訊工作。如果您要用於通訊的子系統不在作用中，則試圖進入系統的工作可能會在符合需求的另一個子系統說明中找到一個登錄。您需要查看所有子系統說明中的登錄。
- 含有工作說明的通訊登錄。工作說明可能含有執行指令或程式的要求資料。請查看您的通訊登錄及其相關工作說明，以確定您瞭解工作將如何啓動。
- 通訊登錄也會指定一個系統在某些情況下所將使用的預設使用者設定檔。請確定您瞭解預設設定檔的角色。如果您的系統含有預設設定檔，您應該確定它們是具有最低權限的設定檔。請參閱第 12 章,『保護 APPC 通訊安全』，取得預設使用者設定檔的詳細資訊。

  您可以使用「列印子系統說明 (PRTSBSDAUT)」指令來識別用以指定使用者設定檔名稱的通訊登錄。

預先啓動工作登錄

您可以使用預先啓動的工作登錄來針對某些類型的工作備妥子系統，讓系統的啓動更快速。在啓動子系統或需要子系統之時，可以啓動預先啓動工作。預先啓動工作登錄指定的事項如下：

- 要執行的程式

  預設使用者設定檔

  工作說明

以上這些，都提供了潛在的安全漏洞。您應該確定預先啓動的工作登錄只執行已授權的預期功能。

工作及工作說明

工作說明含有可在使用工作說明時執行特定程式的要求資料和遞送資料。當工作說明在要求資料參數中指定某個程式時，系統即會執行這個程式。當工作說明指定遞送資料時，系統即會執行與遞送資料相符之遞送登錄中所指定的程式。

系統會使用交談和批次工作的工作說明。對於交談式工作而言，工作站登錄會指定其工作說明。工作站登錄值通常是 *USRPRF，因此程式會使用使用者設定檔中指定的工作說明。對於批次工作而言，您在提出工作時指定工作說明。

您應該定期地複查工作說明，以確定它們並未執行非預期的程式。您也應該使用物件權限來防止對於工作說明的變更。使用 *USE 權限即足以透過工作說明來執行工作。一般的使用者不需要工作說明的 *CHANGE 權限。

SECBATCH 功能表選項：

15 *立即提出* **54** *使用工作排定程式*

工作說明也可以指定哪個工作應該在哪個使用者設定檔之下執行。使用安全層次 40 或以上時，您必須擁有工作說明和其中所指定的使用者設定檔的 *USE 權限。使用在 40 以下的安全層次時，您只需要有工作說明的 *USE 權限。

您可以使用「列印工作說明權限 (PRTJOBDAUT)」指令來列印指定使用者設定檔並擁有公用權限 *USE 的工作說明之列示。

報表顯示工作說明中所指定之使用者設定檔的特殊權限。報表包含使用者設定檔所擁有之任何群組設定檔的特殊權限。您可以使用下列指令來顯示使用者設定檔的專用權限：

```
DSPUSRPRF USRPRF(設定檔名稱) TYPE(*OBJAUT)
```

工作說明指定執行工作時所使用的檔案庫列示。如果某個使用者可變更使用者的檔案庫列示，則使用者可以執行不同檔案庫中之非預期版本的程式。您應該定期地複查您系統的工作說明中所指定的檔案庫列示。

最後，您應該確定「提出工作 (SBMJOB)」指令和「建立使用者設定檔 (CRTUSRPRF)」指令的預設值未受到變更，並指向非預期的工作說明。

架構的異動程式名稱

有些通訊要求會傳送特定類型的信號給您的系統。由於對系統而言，異動程式的名稱是 APPC 架構的一部份，故此要求稱為**架構異動程式名稱 (TPN)**。顯示站透通要求即是架構 TPN 的一個範例。架構 TPN 是與功能通訊的常見方式，且未必會出現安全上的漏洞。不過，架構 TPN 可能讓外人找到進入您系統的入口。

有些 TPN 不會在要求中傳送設定檔。如果要求與預設使用者為 *SYS 的通訊登錄發生關聯，則可能在您的系統中起始這個要求。不過，*SYS 設定檔只能執行系統功能，不會執行使用者應用程式。

如果您不想讓架構 TPN 以預設設定檔執行，您可以將通訊登錄中的預設使用者 *SYS 變更為 *NONE。第 78 頁的『架構的 TPN 要求』會列出結構 TPN 和其相關的使用者設定檔。

如果您完全不讓特定的 TPN 在您的系統中執行，請執行下列動作：

1. 變更接受多個程式的 CL 程式。程式不應該執行任何功能。它應該只擁有參數的「宣告 (DCL)」陳述式，然後結束。
2. 新增 TPN 遞送登錄到擁有通訊登錄的每個子系統或遠端位置名稱登錄。遞送登錄應該指定下列事項：
   - *比較值* (CMPVAL) 的值等於起始位置為 37 之 TPN (請參閱「架構的 TPN 要求」) 的程式名稱。

- *要呼叫的程式* (PGM) 的值等於您在步驟 第 77 頁的1 中建立的程式名稱。這可防止 TPN 找到另一個遞送登錄，例如 *ANY。

若干 TPN 在 QCMN 子系統中已有它們自己的遞送登錄。它們是基於效能上的理由而加入的。

架構的 TPN 要求

表 17. TPN 要求的程式和使用者

TPN 要求	程式	使用者設定檔	說明
X'30F0F8F1'	AMQCRC6A	*NONE	訊息佇列
X'06F3F0F1'	QACSOTP	QUSER	APPC 登入異動程式
X'30F0F2D1'	QANRTP	QADSM	ADSM/400 APPC 配置
X'30F0F1F9'	QCNPCSUP	*NONE	共用資料夾
X'07F0F0F1'	QCNTEDDM	QUSER	DDM
X'07F6C4C2'	QCNTEDDM	QUSER	遠端 SQL-DRDA1
X'30F0F7F7'	QCQNRBAS	QSVCCS	SNA CC_Server
X'30F0F1F4'	QDXPRCV	QUSER	DSNX-PC 接收者
X'30F0F1F3'	QDXPSEND	QUSER	DSNX-PC 傳送者
X'30F0F2C4'	QEVYMAIN	QUSER	ENVY**/400 伺服器
X'30F0F6F0'	QHQTRGT	*NONE	PC 資料佇列
X'30F0F8F0'	QLZPSERV	*NONE	Client Access 授權管理程式
X'30F0F1F7'	QMFRCVR	*NONE	PC 訊息接收者
X'30F0F1F8'	QMFSNDR	*NONE	PC 訊息傳送者
X'30F0F6F6'	QND5MAIN	QUSER	APPN 5394 工作站控制器
DB2DRDA	QCNTEDDDM	QUSER	DB2DRDA
APINGD	QNMAPINGD	QUSER	APINGD
X'30F0F5F4'	QNMEVK	QUSER	系統管理公用程式
X'30F0F2C1'	QNPSERVR	*NONE	PWS-I 網路列印伺服器
X'30F0F7F9'	QOCEVOKE	*NONE	交互系統日曆
X'30F0F6F1'	QOKCSUP	QDOC	目錄投影
X'20F0F0F7'	QOQSESRV	QUSER	DIA 版本 2
X'20F0F0F8'	QOQSESRV	QUSER	DIA 版本 2
X'30F0F5F1'	QOQSESRV	QUSER	DIA 版本 2
X'20F0F0F0'	QOSAPPC	QUSER	DIA 版本 1
X'30F0F0F5'	QPAPAST2	QUSER	S/36--S/38 透通
X'30F0F0F9'	QPAPAST2	QUSER	印表機透通
X'30F0F4F6'	QPWFSTP0	*NONE	共用資料夾類型 2
X'30F0F2C8'	QPWFSTP1	*NONE	Client Access 檔案伺服器
X'30F0F2C9'	QPWFSTP2	*NONE	Windows** Client Access 檔案伺服器
X'30F0F6F9'	QRQSRVX	*NONE	遠端 SQL 收歛伺服器
X'30F0F6F5'	QRQSRV0	*NONE	遠端 SQL，不確定
X'30F0F6F4'	QRQSRV1	*NONE	遠端 SQL，不確定

表 17. TPN 要求的程式和使用者 (繼續)

TPN 要求	程式	使用者設定檔	說明
X'30F0F2D2'	QSVRCI	QUSER	SOC/CT
X'21F0F0F8'	QS2RCVR	QGATE	SNADS FS2 接收者
X'21F0F0F7'	QS2STSND	QGATE	SNADS FS2 傳送者
X'30F0F1F6'	QTFDWNLD	*NONE	PC 轉送功能
X'30F0F2F4'	QTIHNPCS	QUSER	TIE 功能
X'30F0F1F5'	QVPPRINT	*NONE	PC 虛擬列印
X'30F0F2D3'	QWGMTP	QWGM	Ultimedia Mail/400 伺服器
X'30F0F8F3'	QZDAINIT	QUSER	PWS-I 資料存取伺服器
X'21F0F0F2'	QZDRCVR	QSNADS	SNADS 接收者
X'21F0F0F1'	QZDSTSND	QSNADS	SNADS 傳送者
X'30F0F2C5'	QZHQTRG	*NONE	PWS-I 資料佇列伺服器
X'30F0F2C6'	QZRCSRVR	*NONE	PWS-I 遠端指令伺服器
X'30F0F2C7'	QZSCSRVR	*NONE	PWS-I 中央伺服器

監督安全事件的方法

安全的設置無法一次完成。您需要持續地評估系統和安全失效情況的變化。之後，再調整您的安全環境，回應您發現的情況。

安全報告可協助您監督系統中所發生的安全相關變化。以下是可協助您偵測安全失效或漏洞的其它系統功能：

- 安全審核是一套強大的工具，可用來觀察發生於系統中的各種安全相關事件。例如，您可以設置系統，讓它在每次使用者開啓特定資料庫檔案來進行更新時，都會寫入一筆審核記錄。您可以審核對於系統值的所有變更。您可以審核在使用者復置物件時所發生的動作。

  iSeries Security Reference 一書的第 9 章提供關於安全審核功能的完整資訊。您可以使用「變更安全審核 (CHGSECAUD)」指令，在系統中設置安全審核。 您也可以使用「顯示審核異動日誌登錄 (DSPAUDJRNE)」指令，從安全審核日誌中列印選取的資訊。
- 您可以建立 QSYSMSG 訊息佇列，來擷取重要的系統操作員訊息。在標準的一個工作天內，QSYSOPR 訊息佇列會收到許多訊息，這些訊息的重要性各不相同。有時候，由於 QSYSOPR 訊息佇列中的訊息太多，可能會忽略重要的安全相關訊息。

  如果您在系統的 QSYS 檔案庫中建立 QSYSMSG 訊息佇列，系統會自動將特定的重要訊息引導至 QSYSMSG 訊息佇列中，而非 QSYSOPR 訊息佇列。

  您可以建立程式來監督 QSYSMSG 訊息佇列，您也可以使用岔斷模式，將它指定給您自己，或指定給另一個可信的使用者。

第 3 篇 應用程式及網路通訊

第 11 章 使用 整合檔案系統 來保護檔案

整合檔案系統提供多種方法來讓您儲存並檢視 iSeries 伺服器上的資訊。整合檔案系統是 OS/400 作業系統的一部份，可支援串流輸入和輸出作業。它提供類似 (且相容於) 個人電腦作業系統和 UNIX® 作業系統的儲存體管理方法。

隨著 整合檔案系統 的引進，使用者便可以從階層式目錄結構的角度來看待系統中的所有物件。不過，在多數情況中，使用者會針對特定檔案系統，以最通行方式來看待其中的物件。例如，「傳統的」iSeries 物件是在 QSYS.LIB 檔案系統中。使用者通常會從檔案庫的角度來看待這些物件。至於 QDLS 檔案系統中的物件，使用者會從資料夾內之文件的角度來看待它。根 (/)、QOpenSys 和使用者定義的檔案系統會呈現階層式 (巢狀) 的目錄結構。

作爲一個安全管理者，您必須知道下列事項：

- 您的系統中使用哪些檔案系統
- 每個檔案系統所特有的安全特性

以下主題針對整合檔案系統的安全程序，提供若干一般性的注意事項。

整合檔案系統 安全方法

根檔案系統的作用是當作 iSeries 伺服器上所有其它檔案系統的保護傘 (或是基礎)。它從最高層次提供對於系統中之所有物件的整合性觀點。可以存在 iSeries 伺服器上的其它檔案系統會依據每一個檔案系統的基礎，提供不同的物件管理及整合的方法。例如，QOPT (光學) 檔案系統可讓 iSeries 應用程式及伺服器 (包括 iSeries Access for Windows 檔案伺服器) 存取位於 iSeries 伺服器上的光碟機。同樣地，QFileSvr.400 檔案系統則可讓應用程式存取位於遠端 iSeries 伺服器上的整合檔案系統資料。QLANSrv 檔案伺服器則容許存取 Integrated xSeries Server for iSeries 或網路中其它相連的伺服器所儲存的檔案。

每個檔案系統的安全方法，決定於在該檔案系統下所能使用的資料。例如 QOPT 檔案系統不會提供物件層次的安全程序，因爲目前沒有在 CD-ROM 中寫入權限資訊的技術。對於 QFileSvr.400 檔案系統而言，存取控制發生在遠端系統上 (實際儲存和管理檔案的所在)。對於類似 QLANSrv 的檔案系統而言，「Integrated xSeries Server for iSeries」負責提供存取控制。雖然安全模式各有不同，但許多檔案系統都支援透過整合檔案系統指令，例如「變更權限 (CHGAUT)」和「變更擁有者 (CHGOWN)」，來對存取控制進行一致性的管理。

這裡有一些與整合檔案系統安全每一處相關的秘訣。整合檔案系統的目的是儘可能地遵循 POSIX 標準。如此會導致一些有趣的行爲，其中 iSeries 伺服器權限會與 POSIX 許可權混合在一起：

1. 不要移除使用者對他自己所擁有目錄的專用權限，即使使用者是經由公用權限、群組或授權清單獲得授權。當使用標準 iSeries 伺服器安全性模型中的檔案庫或資料夾時，移除擁有者的專用權限將會減少儲存作爲使用者設定檔的權限資訊數量，但不會影響其它作業。可是，因爲 POSIX 標準定義目錄的許可權繼承方式，新建目錄的擁有者對該目錄將具有的物件權限，將與父代的擁有者對其父代之所有相同，即使新建目錄的擁有者對此父代具有其它的專用權限。這可能難以理解，所以這裡舉出

一個範例：「使用者 A」擁有目錄 /DIRA，但是「使用者 A」的專用權限已經移除。「使用者 B」對 /DIRA 具有專用權限。「使用者 B」建立了目錄 /DIRA/DIRB。因爲「使用者 A」沒有 /DIRA 的物件權限，「使用者 B」將沒有 /DIRA/DIRB 的物件權限。若沒有進一步動作變更「使用者 B」的物件權限，「使用者 B」將無法更名或刪除 /DIRA/DIRB。使用 O_INHERITMODE 建立具有 open() API 的檔案亦然。假使「使用者 B」建立一個檔案 /DIRA/FILEB，「使用者 B」對它將沒有物件權限，「也」沒有資料權限。「使用者 B」將無法寫入新檔案。

2. 大部份的實體檔案系統並不接受沿用權限。這包括 Root (/)、QOpenSys、QDLS 和使用者定義的檔案系統。
3. 任何物件都是由建立該物件的使用者設定檔擁有，即使使用者設定檔的 OWNER 欄位設在 *GRPPRF。
4. 許多檔案系統作業需要對路徑的每一個元件都具有 *RX 資料權限，包括根 (/) 目錄。發生權限問題時，請確定要檢查使用者對根目錄本身的授權。
5. 顯示或擷取現行工作目錄（DSPCURDIR、 getcwd() 等等）需要對路徑中的每一個元件都具有 *RX 資料權限。然而，變更現行工作目錄（CD、chdir() 等等）只需要具有每個元件的 *X 資料權限。因此，使用者可以變更現行工作目錄到一定的路徑，然後卻無法顯示該路徑。
6. COPY 指令是用以複製物件。除了擁有者，新檔案的權限設定值將會和原來的一樣。然而，CPYTOSTMF 指令的用途只是要複製資料。使用者並無法控制新檔案的權限設定值。建立者/擁有者將具有 *RWX 資料權限，但群組和公用權限將會是 *EXCLUDE。使用者必須使用另一個方法（CHGAUT、 chmod() 等等）來指定想要的權限。
7. 使用者必須是物件的擁有者或具有 *OBJMGT 物件權限，才能擷取該物件的權限資訊。這會發生在某些非預期的地方，像是 COPY，它必須在來源物件上擷取權限資訊，才能在目標物件上設定相等的權限。
8. 當變更物件的擁有者或群組，使用者不僅要有適當的物件權限，也要具有新擁有者/群組使用者設定檔的 *ADD 資料權限，以及舊擁有者/群組設定檔的 *DELETE 資料權限。這些資料權限與檔案系統資料權限並無關連。這些資料權限可以使用 DSPOBJAUT 指令來顯示，也可使用 EDTOBJAUT 指令來變更。這也會出乎意料地發生在 COPY 指令嘗試設定新物件群組 ID 的時候。
9. MOV 指令更可能造成令人困惑的權限錯誤，特別是在從某個實體檔案系統移動到另一個、或在執行資料轉換的時候。在這些情況中，移動實際上變成一種複製以及刪除的作業。因此，除了其它特定的 MOV 注意事項以外，COPY 指令（請參閱上述 7 和 8）和 RMVLNK 指令的所有相同的權限注意事項都可以影響 MOV 指令。

下列章節說明數種代表性檔案系統的一些注意事項。關於 iSeries 伺服器上特定檔案系統的詳細資訊，需要查閱使用檔案系統之授權程式的文件。

根 (/)、QOpenSys 及使用者定義的檔案系統

以下是根、QOpenSys 和使用者定義的檔案系統的安全考量。

權限的工作方式

根、QOpenSys 以及使用者定義的檔案系統，提供 iSeries 伺服器、PC 以及 UNIX** 混合功能，可以用於物件管理以及安全保護。當您從 iSeries 伺服器階段作業 (WRKAUT 及 CHGAUT) 使用整合檔案系統指令時，您可以設定所有正常的 iSeries 伺服器物件權限。其中包括與 Spec 1170 (UNIX 型的作業系統) 相容的 *R、*W 和 *X 權限。

註: 根、QOpenSys 和使用者定義的檔案系統具有相同的功能。不過，QOpenSys 檔案系統大小寫有別。根檔案系統則不區分大小寫。使用者定義的檔案系統，在定義時，可以區分大小寫。由於這些檔案系統有相同的安全特性，在下列主題中，您可以假設這些檔案系統的名稱可以互換。

當您以管理者的身份使用 PC 階段作業來存取根檔案系統時，您可以設定 PC 所使用的物件屬性來限制某些類型的存取行為：
- 系統
- 隱藏
- 保存
- 唯讀

這些 PC 屬性是加入到 iSeries 伺服器物件權限值，而不是取代。

當使用者試圖存取根檔案系統內的物件時，OS/400 會針對該物件來執行所有的物件權限值和屬性。例如，假設某個物件的唯讀屬性設為開啓。PC 使用者無法透過 iSeries Access 介面刪除物件。擁有固定功能工作站的 iSeries 伺服器使用者也不能刪除物件，即使具有 *ALLOBJ 特殊權限的 iSeries 伺服器使用者也不行。在可以刪除物件之前，必須先由授權使用者使用 PC 功能，將唯讀屬性值重設為關閉。同樣地，PC 使用者也可能沒有足夠的 OS/400 權限，無法變更與 PC 相關的物件安全屬性。

在 iSeries 伺服器上執行的 UNIX 類型應用程式，會使用類似 UNIX 的應用程式設計介面 (API) 來存取根檔案系統中的資料。透過具有 UNIX 特性的 API，應用程式可以識別並維護下登記全資訊：
- 物件擁有者
- 群組擁有者 (iSeries 伺服器主群組權限)
- 讀取 (檔案)
- 寫入 (變更內容)
- 執行 (執行程式或搜尋目錄)

系統將這些資料權限對映到現有的 iSeries 伺服器物件及資料權限：
- 讀取 (*R) = *OBJOPR 和 *READ
- 寫入 (*W) = *OBJOPR、*ADD、*UPD、*DLT
- 執行 (*X) = *OBJOPR 和 *EXECUTE

其它物件權限 (*OBJMGT、*OBJEXIST、*OBJALTER 和 *OBJREF) 概念，在 UNIX 類型的環境中不存在。

不過，根檔案系統內的所有這些物件都擁有這些物件權限。當您使用 UNIX 型的 API 來建立物件時，這個物件會繼承親項目錄的這些權限，並產生下列結果：
- 新物件的擁有者和親項目錄擁有者的物件權限相同。
- 新物件的主群組和親項目錄主群組的物件權限相同。
- 新物件的公共使用者和親項目錄公共使用者的物件權限相同。

新物件的擁有者、主群組和公共使用者的資料權限，在 API 上，都由模式參數來指定。當所有物件權限都設為 ’on’ 時，您取得的權限模式和 UNIX 型的環境相同。除非您不要 POSIC 的模式，否則，您最好保留它們的 ’on’ 設定。

當您執行的應用程式使用具有 UNIX 特性的介面時，不論 UNIX 類型的應用程式是否能夠「看到」這些應用程式，系統都會執行所有物件權限。例如，系統會執行授權清單的權限，即使在 UNIX類型的作業系統中沒有授權清單的概念也一樣。

當您擁有混合應用程式的環境時，如果某個環境內的某些權限變更後會岔斷另一個環境內的應用程式，您必須確定未變更這些權限。

使用根 (/)、QOpenSys 以及使用者定義檔案系統的安全

藉由使用整合檔案系統，iSeries 伺服器也能提供一組新的指令，來處理多重檔案系統中的物件。這個指令集包括用來處理安全程序的指令：

- 變更審核 (CHGAUD)
- 變更權限 (CHGAUT)
- 變更擁有者 (CHGOWN)
- 變更主群組 (CHGPGP)
- 顯示權限 (DSPAUT)
- 使用權限 (WRKAUT)

這些指令用來將基礎資料和物件權限分組為具有 UNIX 特性的權限子集：

***RWX** 讀取/寫入/執行
***RW** 讀取/寫入
***R** 讀取
***WX** 寫入/執行
***W** 寫入
***X** 執行

此外，您也可以用 UNIX 型的 API 來處理安全。

根目錄的公用權限

當您的系統出貨時，根目錄的公用權限是 *ALL (所有物件權限和所有資料權限)。這個設定可以提供符合 UNIX 類型應用程式，以及典型 iSeries 伺服器使用者預期的彈性和相容性。具有指令行能力的 iSeries 伺服器使用者，可以僅使用 CRTLIB 指令就可以在 QSYS.LIB 檔案系統中建立一個新的檔案庫。通常在典型 iSeries 伺服器上的權限都會允許這種做法。同樣地，在使用根檔案系統的出貨值之時，一般使用者也可以在根檔案系統中建立新的目錄 (就好像您可以在 PC 中建立一個新的檔案)。

作為一個安全管理者，您必須教育您的使用者，如何才能適當地保護他們所建立的物件。當使用者建立一個檔案庫時，檔案庫的公用權限不應該是 *CHANGE (預設值)。使用者應該根據檔案庫的內容，將公用權限設定為 *USE 或 *EXCLUDE。

如果您的使用者需要在根 (/)、QOpenSys 或使用者定義的檔案系統中建立新的目錄，您會有幾個安全選項：

- 您可以教育您的使用者，讓他們在建立新目錄時置換預設的權限。預設值是繼承直接親項目錄的權限。如果是在根目錄中建立新目錄，依預設，公用權限的預設值是 *ALL。
- 您可以在根目錄下，建立一個「主要」次目錄。針對該主要目錄，將公用權限設定為適合於您的企業需求的設定值。之後，指示使用者在這個主要次目錄中建立任何新的個人目錄。他們的新目錄將會繼承它的權限。
- 您可以考慮變更根目錄的權限，防止使用者在該目錄中建立物件。(除去 *W、*OBJEXIST、*OBJALTER、*OBJREF 和 *OBJMGT 權限。) 不過，您必須評

估，這個變更是否會讓應用程式發生問題。例如，您可能會有具有 UNIX 特性的應用程式，它們預期能夠刪除根目錄中的物件。

列印專用權限物件 (PRTPVTAUT) 指令

「列印專用權限 (PRTPVTAUT)」指令可讓您列印指定的檔案庫、資料夾或目錄中指定的類型之物件的所有專用權限報表。此報表會列出指定的類型的所有物件，以及獲授權使用該物件的使用者。此方法可用來檢查物件的不同權限來源。

此指令會列印 3 份選取的物件的報表。第 1 份報表 (完整報表) 含有每一選取的物件的所有專用權限。假設先前曾針對指定的檔案庫、資料夾或目錄中指定的物件執行 PRTPVTAUT 指令，則第 2 份報表 (變更報表)會列出選取的物件的專用權限的新增與變更。「變更報表」會印出選取的類型的新物件，現存物件的新權限或對現存物件的現存權限的變更。假設您先前未針對指定的檔案庫、資料夾或目錄中指定的物件執行 PRTPVTAUT 指令，則不會產生「變更報表」。假設先前曾執行此指令，但未變更物件的權限，則會列印「變更報表」，只是其中不列出任何物件。

第 3 份報表 (刪除報表) 會列出先前執行 PRTPVTAUT 指令以來，自指定的物件中刪除的任何私用授權的使用者的。被刪除的任何物件或被當作私用授權的使用者除去的任何使用者會列在「刪除報表」中。假設先前未執行 PRTPVTAUT 指令，將不會產生「刪除報表」。假設先前曾執行此指令，但未針對物件執行刪除作業，則會列印「刪除報表」，只是其中不列出任何物件。

限制：您必須擁有 *ALLOBJ 特殊權限才能使用此指令。

範例：

這個指令會針對 PAYROLLLIB 中的所有檔案物件來建立完整、變更和刪除的報表：

```
PRTPVTAUT OBJTYPE(*FILE) LIB(PAYROLLLIB)
```

這個指令會針對 garry 目錄中的所有串流檔案物件來建立完整、變更和刪除的報表：

```
PRTPVTAUT OBJTYPE(*STMF) DIR(/GARRY) SCHSUBDIR(*NO)
```

這個指令會針對起始於 garry 目錄的子目錄結構中的所有串流檔案物件來建立完整、變更和刪除的報表：

```
PRTPVTAUT OBJTYPE(*STMF) DIR(/GARRY) SCHSUBDIR(*YES)
```

列印公用授權的物件 (PRTPUBAUT) 指令

「列印公用授權的物件 (PRTPUBAUT)」指令可讓您列印沒有公用權限 *EXCLUDE 的指定的物件的報表。以 *PGM 物件來說，唯有不具 *EXCLUDE 公用權限，且可讓使用者呼叫的程式 (此程式為使用者網域，或系統安全層次 (QSECURITY 系統值) 為 30 或以下) 才會列在報表中。此方法可用來檢查系統中每位使用者皆獲授權存取的物件。

此指令會列印出兩份報表。第 1 份報表 (完整報表) 讓您列印沒有公用權限 *EXCLUDE 的指定的物件報表。第 2 份報表 (變更報表) 會列出先前執行 PRTPUBAUT 指令時，尚具 *EXCLUDE 公用權限 (或尚不存在)，而如今已無 *EXCLUDE 公用權限的物件。假設您先前未針對指定的檔案庫、資料夾或目錄中指定的物件執行 PRTPUBAUT 指令，則不會產生「變更報表」。假設先前曾執行此指令，但新增的物件皆擁有 *EXCLUDE 公用權限，則會印出「變更報表」，只是其中不會列出任何物件。

限制：您必須具 *ALLOBJ 特殊權限才能使用此指令。

範例：

這個指令會針對沒有 *EXCLUDE 公用權限的檔案庫 GARRY 其中的所有檔案物件來建立完整和變更的報表：

```
PRTPUBAUT OBJTYPE(*FILE) LIB(GARRY)
```

這個指令會針對起始於 garry 目錄的不具 *EXCLUDE 公用權限的子目結構錄其中的所有串流檔案物件來建立完整、變更和刪除的報表：

```
PRTPUBAUT OBJTYPE(*STMF) DIR(GARRY) SCHSUBDIR(*YES)
```

限制存取 QSYS.LIB 檔案系統

由於根檔案系統是一個如傘般具有籠罩性的檔案系統，因此 QSYS.LIB 檔案系統會出現在根目錄之內，成爲一個次目錄。因此，任何存取您 iSeries 伺服器的 PC 使用者，都可以用一般的 PC 指令及動作來操作儲存在 iSeries 伺服器檔案庫 (QSYS.LIB 檔案系統) 的物件。例如，PC 使用者可以將 QSYS.LIB 物件 (例如具有重資料檔的檔案庫) 拉到碎紙機中。

在您學習第 84 頁的『根 (/)、QOpenSys 及使用者定義的檔案系統』時，系統會執行所有物件權限，而不論介面是否能看到它。因此，如果使用者沒有物件的 *OBJEXIST 權限，即無法刪除物件。不過，如果您的 iSeries 以功能表存取安全爲依據，而不是物件安全，則 PC 使用者很可能會在 QSYS.LIB 檔案系統中找到可刪除的物件。

隨著系統之使用和所提供之不同存取方法的擴充，您很快會發現功能表存取安全不夠用。第 39 頁的第 5 章, 『以物件權限來保護資訊資產』討論以物件安全來補充功能表存取控制的方針。不過，透過根檔案系統目錄結構，iSeries 伺服器也提供一個簡單的方法可以來避免 QSYS.LIB 檔案系統的存取。您可以使用 QPWFSERVER授權清單來控制哪些使用者可以透過根目錄來存取 QSYS.LIB 檔案系統。

當使用者的 QPWFSERVER 授權清單權限是 *EXCLUDE 時，使用者無法從根目錄結構來進入 QSYS.LIB 目錄。當使用者的權限是 *USE 時，使用者可以進入目錄。在使用者擁有進入目錄的權限後，使用者試圖針對 QSYS.LIB 檔案系統內之物件執行的任何動作，都適用一般的物件權限。換言之，QPWFSERVER 授權清單權限的作用，是當作整個 QSYS.LIB 檔案系統的門戶。對於具有 *EXCLUDE 權限的使用者而言，這個門是鎖著的。對於具有 *USE 權限 (或任何較高的權限) 的使用者而言，這個門是開放的。

在多數情形中，使用者不需要使用目錄介面來存取 QSYS.LIB 檔案系統內的物件。您可能會想把 QPWFSERVER 權限列示的公用權限設定爲 *EXCLUDE。請記住，授權清單的權限可開啓 QSYS.LIB 檔案系統內之所有檔案庫的門戶，包括使用者檔案庫。如果有使用者反對排除，您可以在個別的基礎上評估他們的需求。如果適當，您可以明確地授與個別使用者授權清單的權限。不過，您必須確定使用者擁有 QSYS.LIB 檔案系統內之物件的適當權限。否則，使用者可能會不小心刪除物件或整個檔案庫。

註:

1. 在您的系統出貨時，QPWFSERVER 權限列示的公用權限是 *USE。
2. 如果您明確地授權給個別的使用者，授權清單只會以 iSeries Access 檔案服務、NetServer 檔案服務及 iSeries 伺服器間的檔案服務來控制存取。使用者若是透過 FTP、ODBC 與其它網路，他還是可以存取相同的目錄。

保護目錄安全

如果要存取根檔案系統內的某個物件，您會透過該物件的完整路徑來進行讀取。如果要搜尋某個目錄，您必須擁有該目錄的 *X (*OBJOPR 和 *EXECUTE) 權限。例如，假設您要存取下列物件：

```
/companya/customers/custfile.dat
```

您必須具有 companya 目錄及 customers 目錄的 *X 權限。

在使用根檔案系統時，您可以建立物件的符號鏈接。在概念上，符號鏈接是路徑名稱的別名。和完整路徑名稱比起來，它通常比較短，比較好記。不過，符號鏈接不會建立通往物件的不同實體路徑。使用者仍必須有物件之實體路徑內的每個目錄和次目錄的 *X 權限。

對於根檔案系統內的物件而言，目錄安全程序的使用方式和 QSYS.LIB 檔案系統內的檔案庫安全程序相同。例如，您可以將某個目錄的公用權限設定為 *EXCLUDE，避免公共使用者存取該目錄樹內的任何物件。

新物件的安全

當您在根檔案系統內建立新物件時，您用來建立新物件的介面會決定它的權限。例如，如果您使用 CRTDIR 指令和它的預設值，則新目錄會繼承親項目錄的所有權限特性，包括專用權限、主群組權限，以及授權清單的關聯性。以下各段說明，如何決定各介面類型的權限。

權限來源為直接的親項目錄，而不是目錄樹內較高層的目錄。因此，作為一個安全管理者，您必須從兩個角度來檢視指定給階層中之目錄的權限：

- 對於目錄樹中之物件的存取，權限有何影響 (如檔案庫權限)。
- 對於新建立的物件，權限有何影響 (如檔案庫的 CRTAUT 值)。

建議: 您可以提供一個起始目錄 (例如，/home/usrxxx) 給在整合檔案系統中工作的使用者，之後，再設定適當的安全 (如 PUBLIC *EXCLUDE)。如此一來，使用者在其起始目錄下建立的任何目錄，都會繼承權限。

以下是不同介面之權限繼承的說明：

使用建立目錄指令

當您使用 CRTDIR 指令來建立新的次目錄時，您有兩個指定權限的選項：

- 您可以指定公用權限 (資料權限、物件權限，或兩者)。
- 您可以指定 *INDIR 給資料權限、物件權限，或兩者。當您指定 *INDIR 給資料權限和物件權限時，系統會將親項目錄的所有權限資訊完整複製到新物件中，包括權限列示、主群組、公用權限和專用權限。(系統不會複製 QSYS 設定檔或 QSECOFR 設定檔所擁有的物件專用權限。)

使用 API 來建立目錄

您在使用 mkdir() API 來建立目錄時，指定擁有者、主群組和公用等資料權限 (使用 *R、*W 和 *X 的權限對映)。系統使用上層目錄中的資訊來設定擁有者、主群組及公用的物件權限。

由於 UNIX 類型的作業系統沒有物件權限概念，因此 mkdir() API 不支援指定物件權限。如果您要不同的物件權限，您可以使用 iSeries 伺服器指令 (CHGAUT)。不過，當您除去某些物件權限時，具有 UNIX特性的應用程式不會依照您預期的方式來作業。

使用 open() 或 creat() API 來建立串流檔

當您使用 creat() API 來建立串流檔案時，您可以指定擁有者、主群組和公共使用者的資料權限 (使用 UNIX 型的 *R、*W 和 *X 權限)。系統使用上層目錄中的資訊來設定擁有者、主群組及公用的物件權限。

您也可以在使用 open() API 來建立串流檔時，指定這些權限。另一個情況時，當您使用 open() API時，您可以指定讓物件繼承親項目錄的所有權限。這稱爲**繼承模式**。您指定繼承模式後，系統會建立與親項權限完全相符的權限，包括權限列示、主群組、公用權限和專用權限。這個選項的作用，和在 CRTDIR 指令中指定 *INDIR 一樣。

使用 PC 介面來建立物件

當您使用 PC 應用程式在根檔案系統中建立物件時，系統會自動繼續親項目錄的所有權限。其中包括權限列示、主群組、公用權限和專用權限。在您建立物件時，PC 應用程式沒有任何指定權限的對等項。

QFileSvr.400 檔案系統

使用 QFileSvr.400 檔案系統時，iSeries 系統 (SYSTEMA) 的使用者 (USERX) 可以存取另一個相連 iSeries 系統 (SYSTEMB) 中的資料。USERX 有一個和 Client Access 介面相同的介面。遠端 iSeries 伺服器 (SYSTEMB) 會顯示爲一個目錄，而其所有檔案系統則顯示爲子目錄。

當 USERX 試圖使用這個介面來存取 SYSTEMB 時，SYSTEMA 會將 USERX 的使用者設定檔名稱和加密的密碼傳送到 SYSTEMB。SYSTEMB 中必須有相同的使用者設定檔和密碼，否則 SYSTEMB 會拒絕該要求。

如果 SYSTEMB 接受要求，對 SYSTEMB 而言，USERX 和任何 Client Access 使用者沒有不同。相同的權限檢查規則適用於 USERX 所嘗試的任何動作。

作爲一個安全管理者，您必須知道 QFileSvr.400 檔案系統代表另一個通往您的系統的可能門戶。您不能假設您已透過顯示站透通，將遠端使用者限制於交談式的登入。如果您已執行 QSERVER子系統，並且您的系統連接於另一個 iSeries 系統，則遠端使用者可以像是在執行 Client Access 的本端 PC 中般地存取您的系統。大體上，您的系統會有一個需要執行 QSERVER 子系統的連接。好的物件權限架構非常重要，這也是一個原因。

網路檔案系統 (NFS)

「網路檔案系統 (NFS)」提供與實作 NFS 的系統之間的存取功能。NFS 是一個工業標準方法，用來在網路化之系統的使用者間共用資料。大部份主要的作業系統 (包括 PC 作業系統) 都提供 NFS。對 UNIX 系統而言，NFS 是存取資料的主要方法。iSeries 伺服器可以當作一個 NFS 用戶端以及一個 NFS 伺服器。

當您是執行 NFS 伺服器功能之 iSeries 系統的安全管理者時，您必須瞭解和管理 NFS 安全的各個方面。以下是建議和注意事項：

- 您必須使用 STRNFSSVR 指令來明確地啓動 NFS 伺服器功能。請控制哪些人擁有使用這個指令的權限。
- 您匯出目錄或物件時，使它們能夠提供給 NFS 用戶端使用。因此，您擁有特定的控制，可以掌握系統中的哪些部份可以提供給網路中的 NFS 用戶端使用。
- 當您匯出時，您可以指定哪些用戶端可以存取這些物件。您使用系統名稱或 IP 位址來識別用戶端。用戶端可以是個別 PC 或是整個 iSeries 伺服器，或是 UNIX 系統。在 NFS 的語彙中，用戶端 (IP 位址)稱爲**機器**。
- 在您匯出時，您可以針對可存取匯出之目錄或物件的每個機器，指定唯讀存取或讀寫存取。在多數情況中，您會提供唯讀存取。
- NFS 不提供密碼的保護。它的設計目的，是要在可信的系統共用區內，提供對於資料的共用。當使用者要求存取時，伺服器會收到使用者的 `uid`。以下是若干 `uid` 注意事項：
  - iSeries 伺服器嘗試以相同 `uid` 來尋找使用者設定檔。如果找到相符的 `uid`，它會使用使用者設定檔的資格證明 (credential)。資格證明是一個 NFS 語彙，用來描述對於使用者權限的使用。這與其它 iSeries 伺服器應用程式中的設定檔交換類似。
  - 當您匯出目錄或物件時，您可以指定是否要透過具有根權限的設定檔來核可存取。在 iSeries 伺服器上的 NFS 伺服器，使根權限等於 *ALLOBJ 特殊權限。如果您指定不容許使用根權限，則 NFS使用者即使具有 `uid`，且對應於擁有 *ALLOBJ 特殊權限的使用者設定檔，也無法在這個設定檔之下存取物件。相反地，如果容許匿名存取的話，則要求器會對映到匿名的設定檔。
  - 當您匯出目錄或物件時，您可以指定是否接受匿名要求。所謂匿名要求，意指要求的 `uid` 與您系統中的所有 `uid` 都不相符。如果您選擇容許匿名要求，系統會將匿名的使用者對映至 IBM 所提供的 QNFSANON 使用者設定檔。這個使用者設定檔沒有任何特殊權限或明確權限。(在匯出時，您可以依照需要，指定不同的使用者設定檔給匿名的要求。)
- 當您的 iSeries 伺服器加入到 NFS 網路時 (或是使用依靠 `uids` 的 UNIX 系統的任何網路)，您可能需要自行管理您自己的 `uids`，而不是讓系統自動指派。您需要與網路中之其它系統的 `uid` 進行調整。

  您可能會發現需要變更 `uid` (甚至包括 IBM 所提供的使用者設定)，才能與網路中的其它系統相容。有程式可以使變更使用者設定檔的 `uid` 變得更簡單。(當您變更某個使用者設定檔的 `uid` 時，必須同時變更該設定檔在根目錄或 QOpenSrv 目錄中所擁有之所有物件的 `uid`。) QSYCHGID 程式會自動變更使用者設定檔及其所擁有之所有物件中的 `uid`。如何使用此程式的資訊，請參閱 *iSeries 系統 API 參照*手冊。

第 12 章 保護 APPC 通訊安全

當您的系統在網路中參與其它系統時，系統同時對外開放了一組新的門窗。身爲安全管理者，您必須知道，在 APPC 環境中有哪些選項可用來控制進入您系統的通道。

「高級程式對程式通訊」是一種通訊方式，電腦 (包括個人電腦) 可用它來互相通訊。顯示站透通、分散式資料管理以及 iSeries Access for Windows 都可以使用 APPC 通訊。

以下主題提供的基本資訊是有關 APPC 通訊如何作業，以及如何設置適當的安全程序。這些主題主要集中在 APPC 配置的安全相關元素。如果要調整這個範例來配合您的情況，您必須與通訊網路的管理人員一起作業，也可能必須與應用程式的提供者一起作業。使用這個資訊來作爲基礎，可協助您了解 APPC 所能運作的各種安全考量和選項。

安全永遠無法『平白獲得』。如果有人建議您，讓網路的安全程序寬鬆一些，實際上會讓網路的管理變得更加困難。例如，本資訊不強調 APPN® (進階點對點網路®)，因爲沒有 APPN 會更容易瞭解並管理安全性。然而，在沒有 APPN 時，網路管理者必須手動建立 APPN 自動建立的配置資訊。

PC 也使用通訊

將 PC 連接到您的 iSeries 伺服器的許多方法都依靠通訊，如 APPC 或 TCP/IP。當您閱讀下列主題時，請務必同時考慮連接到其它系統和 PC 時的安全考量。在您規劃網路保護措施時，請確定您並未負面地影響到系統所連接的 PC。

APPC 專用辭彙

APPC 提供的功能，可讓某個系統中的使用者在另一個系統中執行作業。發出要求的系統稱爲：

- **來源系統**
- **區域系統**
- **用戶端**

接收要求的系統稱爲：

- **目標系統**
- **遠端系統**
- **伺服器**

APPC 通訊的基本元素

從安全管理者的角度來看，在某個系統的使用者 (SYSTEMA) 可在另一個系統 (SYSTEMB) 中執行有意義的作業之前，必須先發生下列動作：

- 來源系統 (SYSTEMA) 必須提供通往目標系統 (SYSTEMB) 的路徑。這個路徑稱爲 **APPC 階段作業**。
- 目標系統必須識別使用者，並將使用者連結到使用者設定檔。目標系統必須支援來源系統的加密演算法 (相關資訊請參閱第 14 頁的『密碼層次』)。

- 目標系統必須以適當的環境來為使用者啓動一項工作（工作管理值）。

以下主題討論這些元素以及它們與安全程序的關聯。防止 APPC 使用者違反安全程序，主要是由目標系統的安全管理者負責。不過，當兩個系統的安全管理者一起作業時，APPC 安全程序的管理作業會變得比較簡單。

範例：基本 APPC 階段作業

在 APPC 環境中，當一個系統上的使用者或應用程式要求存取另一個系統時，兩個系統會建立一個階段作業。為建立這個階段作業，系統必須鏈接兩個相符的 APPC 裝置說明。 在 SYSTEMA 裝置說明中的「遠端位置名稱 (RMTLOCNAME)」參數必須符合 SYSTEMB 裝置說明中的「區域位置名稱 (LCLLOCNAME)」參數，反之亦然。

如果要讓兩個系統共同建立一個 APPC 階段作業，SYSTEMA 和 SYSTEMB 的 APPC 裝置說明必須有相同的位置密碼。兩者必須同時指定 *NONE，或指定相同的值。

如果密碼的值不是 *NONE，則會以加密的形式來儲存和傳送它們。如果密碼相符，系統會建立一個階段作業。如果密碼不符，則會拒絕使用者的要求。當系統指定位置密碼來建立階段作業時，這稱為**安全連結**。

註: 並非所有電腦系統都能支援「安全連結」功能。

限制 APPC 階段作業

如果您是來源系統的安全主管，您可以使用物件權限來控制哪些使用者可嘗試存取其它系統。請將 APPC 裝置說明的公用權限設定為 *EXCLUDE，並提供 *CHANGE 權限給特定的使用者。您可以使用 QLMTSECOFR 系統值，讓具有 *ALLOBJ 特殊權限的使用者無法使用 APPC 通訊。

如果您是目標系統的安全主管，另可使用 APPC 裝置的權限，防止使用者在系統上啓動 APPC 階段作業。不過，您必須知道哪個使用者 ID 會嘗試存取 APPC 裝置說明。第 95 頁的『APPC 使用者存取目標系統』說明 iSeries 伺服器如何將使用者 ID 與要求 APPC 階段作業相結合。

註: 您可以使用「列印公用授權的物件 (PRTPUBAUT *DEVD)」指令和「列印專用權限 (PRTPVTAUT *DEVD)」指令，來找出在您的系統中擁有裝置說明權限的使用者。

當您的系統使用 APPN 時，如果系統選擇的路徑沒有現存的裝置可用，則它會自動建立一個新的 APPC 裝置。限制存取使用 APPN 之系統上的 APPC 裝置之方法之一，就是建立一份授權清單。授權清單含有應該已取得 APPC 裝置權限的使用者列示。之後，您再使用「變更指令預設 (CHGCMDDFT)」指令來變更 CRTDEVAPPC 指令。請將 CRTDEVAPPC 指令的「權限 (AUT)」參數預設值設定為您所建立的授權清單。

註: 如果您的系統語言不是英文，您必須在 QSYSxxxx 檔案庫內，變更系統中每個國家語言的指令預設。

您可以使用 APPC 裝置說明中的「位置密碼 (LOCPWD)」參數，來驗證對您的系統提出階段作業要求的另一個系統 (代表某個使用者或應用程式) 的身份。位置密碼可協助您偵測出冒充的系統。

當您使用位置密碼時，您必須與網路中其它系統的安全管理者合作。您也必須控制哪些使用者可以建立或變更 APPC 裝置說明和配置清單。系統要求有 *IOSYSCFG 特殊權限，才能使用指令來處理 APPC裝置和配置清單。

註: 當您使用 APPN 時，位置密碼是儲存在 QAPPNRMT 配置清單中，而不是在裝置說明中。

APPC 使用者存取目標系統

當系統建立 APPC 階段作業時，它們會建立一個路徑，讓提出要求的使用者可以抵達目標系統的門口。接著再由其它元素決定使用者必須執行哪些動作，才能取得進入其它系統的方法。

以下主題說明決定 APPC 使用者如何取得目標系統方法的元素。

用來傳送有關使用者資訊的系統方法

APPC 架構提供三種方法，將來源系統的使用者安全資訊傳送到目標系統。這些方法稱爲**架構安全值**。表 18 顯示這些方法：

註: *APPC Programming* 一書提供關於架構安全值的詳細資訊。

表 18. APPC 架構中的安全值

架構的安全值	傳送到目標系統的使用者 ID	傳送到目標系統的密碼
無	否	否
相同	是[1]	請參閱附註 2。
程式	是	是[3]

註:

1. 如果目標系統指定 SECURELOC(*YES) 或 SECURELOC(*VFYENCPWD)，則來源系統會傳送使用者 ID。
2. 使用者未在要求中輸入密碼，因爲來源系統已驗證密碼。對於 SECURELOC(*YES) 和 SECURELOC(*NO) 而言，來源系統不會傳送密碼。對於 SECURELOC(*VFYENCPWD) 而言，來源系統會取出儲存的加密密碼，並加以傳送 (依加密的形式)。
3. 如果來源及目標系統都支援密碼加密，則系統會以加密格式傳送密碼。否則，不會予以加密。

使用者所要求的應用程式會決定架構安全值。例如，SNADS 固定會使用 SECURITY(NONE)。DDM 會使用 SECURITY(SAME)。當使用顯示站透通時，使用者會使用 STRPASTHR 指令的參數來指定安全值。

在所有情形中，目標系統都會選擇是否要接受具有來源系統所指定之安全值的要求。在某些情形中，目標系統可能會完全拒絕要求。在其它情形中，目標系統可能會強迫使用另一個安全值。例如，當使用者在 STRPASTHR 指令中同時指定使用者 ID 和密碼時，要求會使用 SECURITY(PGM)。不過，如果目標系統的 QRMTSIGN 系統值是 *FRCSIGNON，則會出現「登入」顯示畫面。當使用 *FRCSIGNON 設定時，系統固定會使用 SECURITY(NONE)，這等於使用者未在 STRPASTHR 指令中輸入使用者 ID 和密碼。

註:

1. 在傳送資料前，來源和目標系統會先協定安全值。當目標系統指定 SECURELOC(*NO) 而要求為 SECURITY(SAME) 之時，例如，目標系統通知來源系統使用 SECURITY(NONE)，此時，來源系統不會傳送使用者 ID。
2. 當目標系統上的使用者密碼已經過期時，目標系統會拒絕階段作業的要求。這只適用於傳送密碼的連接要求，包括：
   - 類型 SECURITY(PROGRAM) 的階段作業要求。
   - 類型 SECURITY(SAME) 的階段作業要求 (當 SECURELOC 值是 *VFYENCPWD 時)。

區分網路安全責任的選項

當您的系統參與某個網路時，您必須決定是否要相信其它系統，讓它們來驗證想要進入您的系統的使用者。您會相信 SYSTEMA 真能確保「使用者 A」確實是「使用者 A」(或 QSECOFR 確實是 QSECOFR) 呢？或是會讓使用者重新提供使用者 ID 和密碼？

目標系統 APPC 裝置說明的「安全位置 (SECURELOC)」參數可用來指定來源系統是否為安全 (可信) 位置。

當兩個系統都執行支援 *VFYENCPWD、SECURELOC(*VFYENCPWD) 的版次時，則當應用程式使用 SECURITY(SAME) 時會提供額外的保護。雖然要求者未在要求中輸入密碼，來源系統仍會取出使用者的密碼，並將它附在所傳送的密碼中。如果要讓要求順利完成，使用者必須在兩個系統中擁有相同的使用者 ID 和密碼。

當目標系統指定 SECURELOC(*VFYENCPWD) 而來源系統不支援這個值時，目標系統會以 SECURITY(NONE) 來處理要求。

表 19 顯示架構安全值和 SECURELOC 值如何一起作業：

表 19. APPC 安全值及 SECURELOC 值如何一起工作

來源系統	**目標系統**	
架構的安全值	**SECURELOC 值**	**工作的使用者設定檔**
無	任意	預設使用者[1]
相同	*NO	預設使用者[1]
	*YES	和來源系統的要求者相同的使用者設定檔名稱。
	*VFYENCPWD	和來源系統的要求者相同的使用者設定檔名稱。使用者必須在兩個系統中擁有相同的密碼。
程式	任意	來源系統的要求所指定的使用者設定檔。

註:

1. 預設的使用者由子系統說明中的通訊登錄來決定。『工作之使用者設定檔的目標系統分派』有這方面的說明。

工作之使用者設定檔的目標系統分派

當使用者要求另外一個系統中的 APPC 工作時，這個要求會關聯於某個模式名稱。模式名稱可能來自使用者的要求，也可能是來源系統的網路屬性預設值。

目標系統會使用這個模式名稱和 APPC 裝置名稱來決定工作的執行方式。目標系統會搜尋與 APPC裝置名稱和模式名稱最符合之通訊登錄的作用中子系統。

通訊登錄會指定，對於 SECURITY(NONE) 要求，系統將會使用哪個使用者設定檔。以下是子系統說明中的通訊登錄範例：

```
                          顯示通訊登錄

子系統說明：              QCMN            狀態：     ACTIVE

                          工作                       預設          最多
裝置          模式        說明           檔案庫      使用者        作用中
*ALL          *ANY        *USRPRF                    *SYS          *NOMAX
*ALL          QPCSUPP     *USRPRF                    *NONE         *NOMAX
```

表 20 顯示通訊登錄中之預設使用者參數的可能值：

表 20. 預設使用者參數的可能值

值	結果
***NONE**	沒有可用的預設使用者。如果來源系統的要求中未提供使用者 ID，則不會執行工作。
***SYS**	只會執行 IBM 所提供的程式 (系統工作)。不會執行任何使用者應用程式。
user-name	如果來源系統未傳送使用者 ID，則會使用這個使用者設定檔來執行工作。

您可以使用「列印子系統說明 (PRTSBSDAUT)」指令來列印所有擁有通訊登錄且登錄具有預設使用者設定檔的子系統。

顯示站透通選項

顯示站透通是使用 APPC 通訊的應用程式範例。您可以使用顯示站透通來登入經由網路而連接於您的系統的另一個系統。

表 21 顯示透通要求 (STRPASTHR 指令) 以及目標系統之處理方式的範例。對於顯示站透通而言，系統會使用 APPC 通訊的基本元素和遠端登入 (QRMTSIGN) 系統值。

註: 「顯示站透通」要求已不再透過 QCMN 或 QBASE 子系統來遞送。從 V4R1 開始，它們是透過 QSYSWRK 子系統來遞送。在 V4R1 之前，您可以認爲，如果沒有啓動 QCMD 或 QBASE 子系統，「顯示站透通」即無法工作。但現在的情況已經不同。您可以將 QPASTHRSVR 系統值變更爲 0，強迫「顯示站透通」使用 QCMN (如果 QBASE 在作用中，也可以使用它)。

表 21. 範例透通登入要求

STRPASTHR 指令的值		**目標系統**		
使用者 ID	**密碼**	**SECURELOC 值**	**QRMTSIGN 值**	**結果**
*NONE	*NONE	任意	任意	使用者必須登入目標系統。
使用者設定檔名稱	未輸入	任意	任意	要求失效。

表 21. 範例透通登入要求 (繼續)

<table>
<tr><th colspan="2">STRPASTHR 指令的值</th><th colspan="3">目標系統</th></tr>
<tr><th>使用者 ID</th><th>密碼</th><th>SECURELOC 值</th><th>QRMTSIGN 值</th><th>結果</th></tr>
<tr><td rowspan="7">*CURRENT</td><td rowspan="7">未輸入</td><td>*NO</td><td>任意</td><td>要求失效</td></tr>
<tr><td rowspan="3">*YES</td><td>*SAMEPRF</td><td rowspan="2">交談工作使用和來源系統的使用者設定檔相同的使用者設定檔名稱來啓動。密碼不會傳送到遠端系統。使用者設定檔名稱必須存在於目標系統中。</td></tr>
<tr><td>*VERIFY</td></tr>
<tr><td>*FRCSIGNON</td><td>使用者必須登入目標系統。</td></tr>
<tr><td rowspan="3">*VFYENCPWD</td><td>*SAMEPRF</td><td rowspan="2">交談工作使用和來源系統的使用者設定檔相同的使用者設定檔名稱來啓動。來源系統擷取使用者的密碼，並將它傳送至遠端系統。使用者設定檔名稱必須存在於目標系統中。</td></tr>
<tr><td>*VERIFY</td></tr>
<tr><td>*FRCSIGNON</td><td>使用者必須登入目標系統。</td></tr>
<tr><td rowspan="3">*CURRENT (或工作的現行使用者名稱)</td><td rowspan="3">已輸入</td><td rowspan="3">任意</td><td>*SAMEPRF</td><td rowspan="2">交談工作使用和來源系統的使用者設定檔相同的使用者設定檔名稱來啓動。密碼會傳送到遠端系統。使用者設定檔名稱必須存在於目標系統中。</td></tr>
<tr><td>*VERIFY</td></tr>
<tr><td>*FRCSIGNON</td><td>使用者必須登入目標系統。</td></tr>
<tr><td rowspan="3">使用者設定檔名稱（不同於工作的現行使用者設定檔的名稱）</td><td rowspan="3">已輸入</td><td rowspan="3">任意</td><td>*SAMEPRF</td><td>要求失效。</td></tr>
<tr><td>*VERIFY</td><td>交談工作使用和來源系統的使用者設定檔相同的使用者設定檔名稱來啓動。密碼會傳送到遠端系統。使用者設定檔名稱必須存在於目標系統中。</td></tr>
<tr><td>*FRCSIGNON</td><td>一個以指定的使用者設定檔名稱開始的交談式工作。密碼會傳送至目標系統。使用者設定檔名稱必須存在於目標系統中。</td></tr>
</table>

避免非預期的裝置分派

當作用裝置失效時，系統會試圖讓它復原。在某些情況中，當連接被岔斷時，另一個使用者有可能意外地重新建立已失效的階段作業。例如，假設「使用者 A」關閉了某個工作站的電源，但並未登出。「使用者 B」可能會在開啓工作站的電源後，在未登入的情況下，重新啟動「使用者 A」的階段作業。

如果要防止出現這種情況，您可以將「裝置 I/O 錯誤動作 (QDEVRCYACN)」系統值設定為 *DSCMSG。當裝置失效時，系統會結束使用者的工作。

控制遠端指令及批次工作

有許多選項可協助您控制系統中可執行哪些遠端指令和工作，其中包括：

- 如果您的系統使用 DDM，您可以限制對於 DDM 檔案的存取權，來防止使用者從另一個系統使用「提出遠端指令 (SBMRMTCMD)」指令。如果要使用 SBMRMTCMD，使用者必須能夠開啓 DDM 檔案。您也必須限制建立 DDM 檔案的能力。
- 您可以指定一個跳出程式來提供給 DDM 要求存取 (DDMACC) 系統值。在跳出程式中，您可以先評估所有 DDM 要求，然後才核可執行它們。
- 您可以使用網路工作動作 (JOBACN) 網路屬性來防止提出網路工作，或防止自動執行它們。
- 您可以從子系統說明中除去 PGMEVOKE 遞送登錄，明確地指定可在通訊環境中執行哪些程式要求。 PGMEVOKE 遞送登錄可讓要求者指定執行的程式。當您從子系統說明 (例如 QCMN 子系統說明) 中除去這個遞送登錄時，您需要加入必須順利執行的通訊要求的遞送登錄。

  第 78 頁的『架構的 TPN 要求』依據 IBM 所提供的應用程式來列出通訊要求的程式名稱。對於您所要核可的每個要求，您可以加入一個遞送登錄，讓它的比較值和程式名稱都和程式名稱相等。

  當您使用這個方法時，您必須瞭解系統中的工作管理環境，以及系統中所發生的通訊要求類型。如果可能，您應該測試所有通訊要求類型，確定在您變更遞送登錄後，它們都能夠正常作業。當通訊要求找不到可用的遞送登錄時，您會收到一則 CPF1269 訊息。另一個替代方案 (比較不會出錯，但有效性會稍微低些) 是將系統所不執行之異動程式的公用權限設定爲 *EXCLUDE。

  註: *Work Management* 一書提供關於遞送登錄和系統如何處理程式啓動要求的詳細資訊。

評估 APPC 配置

您可以使用「列印通訊安全 (PRTCMNSEC)」指令或功能表選項來列印 APPC 配置中與安全相關的各個值。以下主題說明列印報告的相關資訊。

APPC 裝置的相關參數

圖 9 顯示裝置說明的「通訊資訊報告」範例。第 100 頁的圖 10 顯示配置清單的報告範例。報告後面是對於報告欄位的說明。

```
                                  通訊資訊 (完整報告)
SYSTEM4
物件類型 . . . . . . . . . . . :   *DEVD

物件          物件          裝置             安全        位置      APPN       單一        預先建立      SNUF
名稱          類型          種類             位置        密碼      功能     階段作業     階段作業    程式啓動

CDMDEV1       *DEVD         *APPC            *NO         *NO       *NO        *YES        *NO
CDMDEV2       *DEVD         *APPC            *NO         *NO       *NO        *YES        *NO
```

圖 9. APPC 裝置說明 - 報告樣本

```
                    顯示配置清單                                        頁次      1
                              SYSTEM4  12/17/95  07:24:36
配置清單 . . . . . . . . . . . . . . :   QAPPNRMT
配置清單類型 . . . . . . . . . . . . :   *APPNRMT
文字 . . . . . . . . . . . . . . . . :
---------------------APPN 遠端位置---------------------

遠端       遠端        區域       遠端       控制點      安全
位置       網路 ID     位置       控制點     網路 ID     位置
SYSTEM36  APPN      SYSTEM4   SYSTEM36  APPN       *NO
SYSTEM32  APPN      SYSTEM4   SYSTEM32  APPN       *NO
SYSTEMU   APPN      SYSTEM4   SYSTEM33  APPN       *YES
SYSTEMJ   APPN      SYSTEM4   SYSTEMJ   APPN       *NO
SYSTEMR2  APPN      SYSTEM4   SYSTEM1   APPN       *NO
------------------------------APPN 遠端位置------------------------------

遠端       遠端        區域         單一                      區域       預先建立
位置       網路 ID     位置       階段作業        交談數      控制點     階段作業
SYSTEM36  APPN      SYSTEM4    *NO             10      *NO        *NO
SYSTEM32  APPN      SYSTEM4    *NO             10      *NO        *NO
```

圖 10. 配置清單報告 - 範例

安全位置欄位

安全位置 (SECURELOC) 欄位指定區域系統是否相信遠端系統，讓它代表區域系統來執行密碼的驗證作業。SECURELOC 欄位只適用於使用 SECURITY(SAME) 值的應用程式，例如 DDM 和使用 CPI 通訊 API 的應用程式。

SECURELOC(*YES) 會讓區域系統暴露在遠端系統的可能缺點之下。存在於兩個系統的任何使用者，都可以呼叫區域系統的程式。這一點特別危險，因爲所有 iSeries 系統中的 QSECOFR (安全主管) 使用者設定檔都擁有 *ALLOBJ 特殊權限。如果網路中某個系統對於 QSECOFR 密碼的保護工作做得不好，則所有將該系統視爲安全位置的系統，都會陷入危險之中。

當您使用 SECURELOC(*VFYENCPWD) 時，您的系統比較不會暴露於未妥善保護密碼之其它系統的缺點之下。當使用者要求使用 SECURITY(SAME) 的應用程式時，他也必須在兩個系統中擁有相同的使用者 ID 和密碼。SECURELOC(*VFYENCPWD) 需要適用於全網路的密碼管理原則，因此，在所有系統中，使用者都必須有相同的密碼。

註: SECURELOC(*VFYENCPWD) 只在執行 V3R2、V3R7 或 V4R1 的系統之間，才受到支援。如果目標系統指定 SECURELOC(*VFYENCPWD)，而來源系統不支援這個功能，則會將這個要求當作 SECURITY(NONE) 來處理。

如果系統指定 SECURELOC(*NO)，則使用 SECURITY(SAME) 的應用程式將需要預設的使用者來執行程式。預設使用者由該要求的相關裝置說明和模式來決定。(請參閱第 96 頁的『工作之使用者設定檔的目標系統分派』。)

位置密碼欄位

位置密碼欄位決定兩個系統是否要交換密碼，以驗證提出要求的系統是否爲冒充的系統。第 94 頁的『範例：基本 APPC 階段作業』提供有位置密碼的詳細資訊。

APPN 功能欄位

APPN 功能 (APPN) 欄位指定遠端系統是否可支援進階網路功能，或只能使用單一跳躍點連接。APPN(*YES) 的意義如下：

- 如果遠端系統是一個網路節點，則遠端系統可將區域系統連接到其它系統。這稱爲**中間節點遞送**。它表示系統中的使用者可以使用遠端系統來作爲通往較大網路的路徑。
- 如果區域系統是一個網路節點，則遠端系統可以使用區域系統來連接到其它系統。遠端系統的使用者可以使用您的系統來作爲通往較大網路的路徑。

註: 您可以使用 DSPNETA 指令來判斷某個系統是網路節點或終端節點。

單一階段作業欄位

單一階段作業 (SNGSSN) 欄位指定遠端系統是否可以使用同一個 APPC 裝置說明來同時執行多個階段作業。通常會使用 SNGSSN(*NO)，因爲使用它，便不需要爲同一個遠端系統建立多個裝置說明。例如，PC 的使用者通常會需要多個 5250 模擬階段作業來用於檔案伺服器和列印伺服器功能。當使用 SNGSSN(*NO) 時，您可以只使用一個裝置說明來提供這個功能給 iSeries 系統中的 PC。

SNGSSN(*NO) 表示您必須依賴 PC 使用者和其它 APPC 使用者側重安全考量的作業程序。如果遠端系統的使用者啓動未獲授權的階段作業，並使用現存階段作業的相同裝置說明，則您的系統將很容易受到這個遠端系統使用者的侵犯。(這個作法有時也稱爲**挾帶**。)

預先建立階段作業欄位

單一階段作業裝置的預先建立 (PREESTSSN) 階段作業欄位控制遠端系統第一次接觸區域系統時，區域系統是否要啓動和遠端系統之間的階段作業。PREESTSSN(*NO) 表示區域系統會等到應用程式要求建立與系統之間的階段作業時，才會啓動階段作業。PREESTSSN(*YES) 則可以將應用程式完成連接所需要的時間縮到最小。

PREESTSSN(*YES) 可避免讓系統切斷不再使用的撥接線路。應用程式或使用者必須明確地轉斷線路。PREESTSSN(*YES) 會延長區域系統可能受到階段作業之挾帶侵犯的時間。

SNUF 程式啓動欄位

SNUF 程式啓動欄位指定是否要讓遠端系統啓動區域系統中的程式。*YES 表示遠端系統使用者啓動並執行區域系統中的程式時，區域系統的物件權限架構必須足以保護物件。

APPC 控制器的參數

第 102 頁的圖 11 顯示控制器說明的「通訊資訊報告」範例。報告後面是對於報告欄位的說明。

通訊資訊 (完整報告)

SYSTEM4
物件類型 . . . . : *CTLD

物件名稱	物件類型	控制器種類	自動建立	撥接式控制器	呼叫方向	APPN功能	CP階段作業	切斷計時器	刪除秒數	裝置名稱
CTL01	*CTLD	*APPC	*YES	*YES	*DIAL	*YES	*YES	0	1440	AARON
CTL02	*CTLD	*APPC	*YES	*YES	*DIAL	*YES	*YES	0	1440	BASIC
CTL03	*CTLD	*APPC	*YES	*YES	*DIAL	*YES	*YES	0	1440	*NONE

圖 11. APPC 控制器說明 - 報告樣本

自動建立欄位

在線路說明中，自動建立 (AUTOCRTCTL) 欄位指定在進入的要求找不到相符的控制器說明時，區域系統是否要自動建立一個控制器說明。在控制器說明中，自動建立 (AUTOCRTDEV) 欄位指定在進入的要求找不到相符的裝置說明時，區域系統是否要自動建立一個裝置說明。

對於具有 APPN 功能的控制器而言，自動建立欄位沒有作用。不論您如何設定自動建立欄位，在必要時，系統都會自動建立裝置說明。

當您對線路說明指定 *YES 時，任何可以存取該線路的使用者都能連接到您的系統。其中包括透過橋接器和路由器來連接的站台。

控制點階段作業欄位

對於具有 APPN 功能的控制器而言，控制點階段作業 (CPSSN) 欄位控制系統是否要自動建立與遠端系統間的 APPC 連接。系統會使用 CP 階段作業來和遠端系統交換網路資訊和狀態。APPN 網路節點間之最新資訊的交換特別重要，它可使網路運轉得更順暢。

當您指定 *YES 時，不會自動切斷閒置的撥接線路。這會讓您的系統較容易受到挾帶階段作業的侵犯。

切斷計時器欄位

對於 APPC 控制器而言，切斷計時器欄位指定控制器停用 (沒有作用中的階段作業) 多久之後，系統會切斷與遠端系統之間的線路。這個欄位有兩個值。第一個值指定控制器起始連接之後，作用時間會持續多久。第二個值決定從控制器結束最後一個階段作業後，到系統切斷線路之前，系統所要等待的時間。

只有當撥接切斷 (SWTDSC) 欄位為 *YES 時，系統才會使用切斷計時器。

您將這些值設得愈大，系統受到挾帶階段作業侵犯的可能性也愈高。

線路說明的參數

第 103 頁的圖 12 顯示線路說明的「通訊資訊報告」範例。報告後面是對於報告欄位的說明。

```
                                通訊資訊 (完整報告)

物件類型 . . . . . . . . . . . . :   *LIND
自動
物件            物件           線路            自動          刪除       自動       自動
名稱            類型           種類            建立          秒數       回答       撥號
LINE01          *LIND          *SDLC           *NO             0        *NO        *NO
LINE02          *LIND          *SDLC           *NO             0        *YES       *NO
LINE03          *LIND          *SDLC           *NO             0        *NO        *NO
LINE04          *LIND          *SDLC           *NO             0        *YES       *NO
```

圖 12. APPC 線路說明 - 報告樣本

自動回答欄位

自動回答 (AUTOANS) 欄位指定撥接線路是否要接受進入的呼叫，而不需要操作員的介入。

當您指定 *YES 時，系統比較不安全，因為它會變得比較容易存取。如果在您指定 *YES 時，要將安全漏洞的可能縮到最小，您應該在不需要使用線路時轉斷線路。

自動撥號欄位

自動撥號 (AUTODIAL) 欄位指定撥接線路是否可送出呼叫，而不需要操作員的介入。當您指定 *YES 時，區域使用者即使沒有通訊線路和數據機的實際存取權，也可以連接到其它系統。

第 13 章 保護 TCP/IP 通訊安全

TCP/IP (傳輸控制通訊協定/網際網路通訊協定) 是一種常用的通訊方法，所有類型的電腦都可用它來互相通訊。在 『資訊高速公路』 中，TCP/IP 應用程式爲人所熟知，並且被廣泛地使用。

本章提供下列要訣：

- 防止 TCP/IP 應用程式在您的系統上執行。
- 當容許 TCP/IP 應用程式在您的系統上執行時，保護您的系統資源。

「iSeries 資訊中心 --> 網路功能 --> TCP/IP」網站是關於所有 TCP/IP 應用程式資訊的完整來源。*SecureWay®: iSeries 及 Internet* (iSeries 資訊中心 --> 安全性 --> SecureWay) 說明將 iSeries 伺服器連接到網際網路 (超大型 TCP/IP 網路) 或內部網路時的安全注意事項。請參閱第 xii 頁的『先決條件與相關資訊』，以獲得存取「iSeries 資訊中心」的資訊。

請記得 iSeries 伺服器支援許多可用的 TCP/IP 應用程式。當您決定要讓某個 TCP/IP 應用程式在您的系統上執行時，您也可以同時啓用其它 TCP/IP 應用程式。作爲一個安全管理者，您必須知道 TCP/IP 應用程式的範圍，以及這些應用程式所具有的安全作用。

防止 TCP/IP 處理

TCP/IP 伺服器工作在 QSYSWRK 子系統中執行。您要使用「啓動 TCP/IP (STRTCP)」指令，在系統上啓動 TCP/IP。如果您不要執行任何 TCP/IP 處理或應用程式，請勿使用 STRTCP 指令。您的系統出貨時，STRTCP指令的公用權限設定爲 *EXCLUDE。

如果您懷疑某個擁有指令存取權的使用者在啓動 TCP/IP (例如，在下班時間)，您可以設置對於 STRTCP 指令的物件審核。每當使用者執行指令時，系統就會寫入一筆審核日誌登錄。

TCP/IP 安全性元件

您可以利用各種 TCP/IP 安全性元件的優點，它們可以提高網路的安全性並增加彈性。雖然其中有些技術也可以在防火牆產品中找到，但是這些適用於 OS/400 的 TCP/IP 安全性元件，並非爲了當作防火牆使用而提供。不過，在某些情況下，您可以使用其中的某些特性，而用不著另購個別防火牆產品。此外，這些 TCP/IP 特性也可以在已使用防火牆的環境中，提供額外的安全。

可利用下列的元件增強 TCP/IP 安全性：

- 封包規則
- HTTP Proxy 伺服器
- VPN (虛擬專用網路)
- SSL (secure sockets layer)

使用封包規則來保護 TCP/IP 傳輸的安全

封包規則 (是 IP 過濾及網址轉換 (NAT) 的組合) 的功能有如保護您的內部網路對抗侵入者的防火牆。IP 過濾可讓您控制哪些 IP 傳輸可以出入您的網路。基本上，它會根據您定義的規則來過濾封包，藉以保護您的網路。另一方面，NAT 可讓您將未登錄的專用 IP 位址隱藏在一組登錄的 IP 位址背後。如此可幫助您保護內部網路與外部網路相隔離。NAT 也有助於減緩 IP 位址的消耗問題，因為許多專用位址可以利用一小組登錄的位址作代表。請參閱「iSeries 資訊中心」，以獲得相關資訊。

HTTP PROXY 伺服器

HTTP PROXY 伺服器隨附於 IBM HTTP Server for iSeries 伺服器。HTTP 伺服器是 OS/400 的一部份。虛擬伺服器會接收 Web 瀏覽器的 HTTP 要求，並將它重送給 Web 伺服器。接收到這些要求的 Web 伺服器只知道虛擬伺服器的 IP 位址，而無從得知真正發出這些要求之 PC 的名稱或位址。虛擬伺服器可處理 HTTP、FTP、Gopher，與 WAIS 的 URL 要求。

虛擬伺服器會快取所有虛擬伺服器使用者所要求且傳回的網頁。因此，當使用者要求某網頁時，虛擬伺服器會先檢查快速記憶體中有否該網頁。若有，則 虛擬伺服器會傳回快取的網頁。透過快取網頁的使用，虛擬伺服器可加快網頁的服務，因此消除 Web 伺服器的潛在耗時要求。

虛擬伺服器也可以記載所有 URL 要求，以供追蹤。然後，您可以複查這些日誌，監督網路資源的使用與濫用情況。

您可使用 IBM HTTP 伺服器中的 HTTP 虛擬支援來合併 Web 存取。PC 用戶端存取的 Web 伺服器看不到這些 PC 用戶端的位址；這些 Web 伺服器只知道虛擬伺服器的 IP 位址。此外，網頁快取特性也可以降低通訊頻寬需求與防火牆工作負荷。請參閱 IBM HTTP Server for iSeries 首頁，以取得詳細資訊：
http://www-1.ibm.com/servers/eserver/iseries/software/http/index.html

虛擬專用網路 (VPN)

虛擬專用網路 (VPN) 可讓貴公司安全地在現有公用網路組織架構上 (例如網際網路) 延伸專用企業內部網路。使用 VPN，貴公司可以控制網路傳輸，同時提供重要的安全特性，例如鑑別及資料隱密性。

OS/400 VPN 是「iSeries 領航員」的選用安裝元件，也是 OS/400 的圖形式使用者介面 (GUI)。它可讓您建立任何主電腦及閘道組合之間的點對點路徑。OS/400 VPN 使用鑑別方法、加密演算法，及其它預防措施，以確保連線兩端之間所傳送資料的安全。

VPN 是在 TCP/IP 層通訊堆疊模型的網路層上執行。尤其是 VPN 會使用 IP 安全架構 (IPSec) 開放組織架構。IPSec 提供網際網路的基本安全性功能，並且提供具有彈性的建置區塊，您可以用來建立既堅固又安全的虛擬專用網路。

VPN 也提供「階層 2 通道通訊協定 (L2TP) VPN」解決方案。L2TP 連線 (亦稱為虛擬線路) 藉由讓公司網路伺服器管理分派給遠端使用者的 IP 位址，提供了具成本效率的遠端使用者存取方式。當您使用 IPSec 來保護 L2TP 連線時，它會進一步地為您的系統或網路提供安全的存取。

瞭解 VPN 對您整個網路所造成的影響是很重要的。適當的規劃及施行是順利執行的重要因素。您應複查「iSeries 資訊中心」內的 VPN 主題，以確定您瞭解 VPN 如何工作，

以及使用 VPN 的方式。詳細資訊，請參閱「iSeries 資訊中心 --> 安全性 --> 虛擬專用網路」。請參閱第 xii 頁的『先決條件與相關資訊』，以獲得存取「iSeries 資訊中心」的資訊。

Secure Sockets Layer (SSL)

Secure Sockets Layer (SSL) 已經成為一項工業標準，可讓應用程式在未受保護的網路上 (例如網際網路) 進行安全的通訊階段作業。SSL 通訊協定會在用戶端與伺服器應用程式之間，建立一個安全連線，並提供通訊階段作業一端或兩端的鑑別。SSL 也提供了用戶端與伺服器應用程式之間所交換資料的隱密性及完整性。詳細資訊，請參閱 「iSeries 資訊中心 -> 安全性 --> Secure Sockets Layer (SSL)」。請參閱第 xii 頁的『先決條件與相關資訊』，以獲得存取「iSeries 資訊中心」的資訊。

保護 TCP/IP 環境的安全

這個主題提供一般性的建議，協助您採取步驟來減少在 TCP/IP 環境中暴露系統安全漏洞的可能。這些步驟適用於您的整個 TCP/IP 環境，不適用於後面的主題中所討論的特定應用程式。

- 當您撰寫 TCP/IP 埠的應用程式時，請確定讓該應用程式受到適當的安全保護。您應該假設會有外來人員試圖侵入該埠來存取該應用程式。內行的外來者可能會嘗試使用 TELNET 來侵入該應用程式。
- 監督系統中對於 TCP/IP 埠的使用情形。關聯於 TCP/IP 埠的某個使用者應用程式可能會在使用者 ID 或密碼之外，提供 『非法途徑』 來進入您的系統。您系統中某個具有足夠權限的使用者，可將應用程式關聯到 TCP 或 UDP 埠。
- 如果您是安全主管，您應該知道有一種電腦駭客所使用的技術，稱為 *IP 詐騙*。TCP/IP 網路中的每個系統都有一個 IP 位址。每個使用「IP 詐騙」技術的人都會設置一個系統 (通常稱為一個 PC)，假裝是一個現存的 IP 位址，或是可信的 IP 位址。於是，冒充者便偽裝成您常常連接的系統，來建立與您的系統間的連接。

  如果您在系統上執行 TCP/IP，而您的系統參與未受實際保護的網路 (所有非撥接線路以及預先定義的鏈接)，您將很容易受到「IP 詐騙」的侵入。如果要保護您的系統，讓它不會受到 『詐騙客』的侵犯，請您著手實施本章的建議，例如登入保護和物件安全程序。您也應該確保您的系統設定有合理的輔助記憶體限制。這可防止詐騙客利用郵件或排存檔來氾濫您的系統，造成系統的癱瘓。

  此外，您應該定期地監督系統中的 TCP/IP 活動。如果您偵測到「IP 詐騙」，您應該找出 TCP/IP 設置中的弱點，再加以調整。
- 對於您的企業內部網路 (不必與外界直接連接的系統所組成的網路)，請使用可重複使用的 IP位址。可重複使用的位址，它的目的是要在專用網路之內使用。網際網路供應中樞不會遞送 IP 位址可重複使用的分封。因此，可重複使用的位址可在您的防火牆內，多提供一層安全保護。

  iSeries 資訊中心 --> 網路功能 --> TCP/IP 網站提供 IP 位址指定方式及其範圍的相關資訊，同時還提供關於 TCP/IP 的安全資訊。
- 如果您正考量系統與網際網路或企業內部網路的連線問題，請詳閱「 *SecureWay：iSeries 與網際網路」*中的安全資訊 (iSeries 資訊中心 --> 安全性 --> SecureWay)。請參閱第 xii 頁的『先決條件與相關資訊』，以獲得存取「iSeries 資訊中心」的資訊。

控制自動啓動的 TCP/IP 伺服器

如果您是安全主管，您必須控制在啓動 TCP/IP 時，會自動啓動哪些 TCP/IP 應用程式。啓動 TCP/IP 的指令有兩個。對於每一個指令，系統都有不同的方法，可用來決定要啓動哪些應用程式 (伺服器)。

表 22 顯示這兩個指令和它們的安全建議事項。表 23 顯示伺服器的預設自動啓動值。如果要變更伺服器的自動啓動值，請使用該伺服器的 CHGxxxA (變更 xxx屬性) 指令。例如，TELNET 的指令是 CHGTELNA。

表 22. TCP/IP 指令決定要啓動哪些伺服器

指令	伺服器啓動的項目	安全建議事項
啓動 TCP/IP (STRTCP)	系統會啓動每個指定 AUTOSTART(*YES) 的伺服器。表 23 顯示每個 TCP/IP 伺服器的出貨值。	• 小心指定 *IOSYSCFG 特殊權限，以控制哪些使用者可變更自動啓動設定。 • 小心控制哪些使用者擁有使用 STRTCP 指令的權限。指令的預設公用權限是 *EXCLUDE。 • 設置「變更 *server-name* 屬性」指令 (例如 CHGTELNA) 的物件審核，以監督試圖變更伺服器之 AUTOSTART 值的使用者。
啓動 TCP/IP 伺服器 (STRTCPSVR)	您使用參數來指定要啓動哪些伺服器。這個指令的出貨預設值是啓動所有伺服器。	• 使用「變更指令預設 (CHGCMDDFT)」指令，將 STRTCPSVR 指令設置爲只啓動一個特定伺服器。這不會禁止使用者啓動其它伺服器。不過，變更指令預設後，使用者比較不會意外啓動所有伺服器。例如，使用下列指令，設定預設值爲只啓動 TELNET 伺服器：`CHGCMDDFT CMD(STRTCPSVR) NEWDFT('SERVER(*TELNET)')` **註:** 在變更預設值後，您只可以指定一個單一伺服器。請選擇一個您經常使用的伺服器，或最不會產生安全漏洞的伺服器 (例如 TFTP)。 • 小心控制哪些人擁有使用 STRTCPSVR 指令的權限。指令的預設公用權限是 *EXCLUDE。

下表包含 TCP/IP 伺服器的自動啓動值。如需每一部伺服器的相關資訊，請參閱「 iSeries 資訊中心」 (**網路功能 --> TCP/IP**)。請參閱第 xii 頁的『先決條件與相關資訊』，以獲得存取「iSeries 資訊中心」的詳細資訊。

表 23. TCP/IP 伺服器的自動啓動值

伺服器	預設值	您的值
TELNET	AUTOSTART(*YES)	
FTP (檔案轉送通訊協定)	AUTOSTART(*YES)	
BOOTP (啓動程式通訊協定)	AUTOSTART(*NO)	
TFTP (一般檔案轉送通訊協定)	AUTOSTART(*NO)	
REXEC (遠端執行伺服器)	AUTOSTART(*NO)	
RouteD (路由常駐程式)	AUTOSTART(*NO)	
SMTP (簡易郵件轉送通訊協定)	AUTOSTART(*YES)	
POP (郵局通訊協定)	AUTOSTART(*NO)	
HTTP (超文字轉送通訊協定) [1]	AUTOSTART(*NO)	
ICS (網際網路連線伺服器)[1]	AUTOSTART(*NO)	
LPD (印表常駐程式)	AUTOSTART(*YES)	

表 23. TCP/IP 伺服器的自動啓動值 (繼續)

伺服器	預設值	您的值
SNMP (Simple Network Management Protocol (SNMP))	AUTOSTART(*YES)	
DNS (網域名稱系統)	AUTOSTART(*NO)	
DDM	AUTOSTART(*NO)	
DHCP (動態的主電腦配置通訊協定)	AUTOSTART(*NO)	
NSMI	AUTOSTART(*NO)	
INETD	AUTOSTART(*NO)	
註: 1. 利用 IBM HTTP Server for iSeries 伺服器，您會使用 CHGHTTPA 指令來設定 AUTOSTART 值。		

使用 SLIP 的安全注意事項

iSeries 伺服器 TCP/IP 支援包括「序列介面線路通訊協定 (SLIP)」。 SLIP 可提供低成本的點對點連接。SLIP 使用者可以和 LAN 或 WAN 中的系統建立點對點的連接來連接 LAN 或 WAN。

SLIP 執行於非同步的連接。您可以使用 SLIP 來建立與 iSeries 伺服器之間的撥接式連接。例如，您可以使用 SLIP，從您的 PC 撥接到 iSeries 系統。在建立好連接後，您可以使用 PC 中的 TELNET 應用程式來連接到 iSeries TELNET 伺服器。或者，您也可以使用 FTP 應用程式，在兩個系統之間轉送檔案。

您的系統出貨時，其中沒有任何 SLIP 配置。因此，如果您不要在系統中執行 SLIP (和撥接式 TCP/IP)，請勿配置任何 SLIP 的配置設定檔。如果您要建立 SLIP 配置，您可以使用「使用 TCP/IP 點對點 (WRKTCPPTP)」指令。您必須擁有 *IOSYSCFG 特殊權限，才能使用 WRKTCPPTP 指令。

如果您要在系統中執行 SLIP，您可以建立一或多個 SLIP (點對點) 配置設定檔。您可以使用下列作業模式來建立配置設定檔：
- 撥入 (*ANS)
- 撥出 (*DIAL)

以下主題討論如何設置 SLIP 配置設定檔的安全程序。

註: **使用者設定檔**是一種可讓使用者登入的 iSeries 伺服器物件。每個 iSeries 伺服器工作都必須有使用者設定檔才能執行。**配置設定檔**儲存用來建立與 iSeries 系統之 SLIP 連線的資訊。當您啓動與 iSeries 伺服器的 SLIP 連接時，您只是建立一個鏈接。您尚未登入或啓動 iSeries 伺服器工作。因此，您不一定需要使用者設定檔，才能啓動與 iSeries 伺服器的 SLIP 連接。不過，如後面的討論將說明，SLIP 配置設定檔可能需要有使用者設定檔，才能決定是否容許建立連接。

控制撥入 SLIP 連接

在使用者可透過 SLIP 來建立撥入連接以通向您的系統之前，您必須先啓動 SLIP *ANS 配置設定檔。如果要建立或變更 SLIP 配置，您可以使用「使用 TCP/IP 點對點 (WRKTCPPTP)」指令。如果要啓動配置設定檔，您可以使用「啓動 TCP/IP 點對點 (STRTCPPTP)」指令，或使用 WRKTCPPTP 顯示畫面的選項。當您的系統出貨時，

STRTCPPTP 和 ENDTCPPTP 指令的公用權限是 *EXCLUDE。您必須擁有 *IOSYSCFG 特殊權限，才能使用新增、變更和刪除 SLIP 配置設定檔的選項。如果您是一個安全主管，您可以使用指令權限和特殊權限來判斷，哪個使用者可設置您的系統以容許建立撥入連接。

保護撥入 SLIP 連接的安全

如果您要驗證撥入您的系統的系統，您可以要求提出要求的系統傳送使用者 ID 和密碼。之後，您的系統即可驗證這個使用者 ID 和密碼。如果使用者 ID 和密碼無效，您的系統可以拒絕這個階段作業要求。

如果要設置撥入驗證，請執行下列動作：

__ 步驟 1. 建立一個提出要求的系統可用它來建立連接的使用者設定檔。要求者所傳送的使用者 ID 和密碼必須符合這個使用者設定檔的名稱和密碼。

註: 如果要讓系統執行密碼驗證，QSECURITY 系統值必須設為 20 或以上。

如果要進行其它保護措施，您可能會想特別建立使用者設定檔，以此來建立 SLIP 連接。在系統中，使用者設定檔應該擁有有限的權限。如果這些設定檔專用來建立 SLIP 連接，不用於任何其它功能，您可以在使用者設定檔中設定下列值：

- 起始功能表 (INLMNU) *SIGNOFF
- 起始程式 (INLPGM) *NONE
- 限制功能 (LMTCPB) *YES

這些值可防止任何使用者透過使用者設定檔，以交談的方式來進行登入。

__ 步驟 2. 建立一份系統的授權清單，以便在要求者試圖建立 SLIP 連接時進行檢查。

註: 您在建立或變更 SLIP 設定檔時，在*系統存取授權清單*欄位中指定這個授權清單。 (請參閱步驟 4。)

__ 步驟 3. 使用「新增權限登錄 (ADDAUTLE)」指令，將步驟 1 所建立的使用者設定檔加到授權清單中。您可以為每個點對點配置設定檔各建立一個唯一的授權清單，您也可以建立一個讓許多配置設定檔共用的授權清單。

__ 步驟 4. 使用 WRKTCPPTP 指令來設置 TCP/IP 點對點 *ANS 設定檔，讓設定檔擁有下列特性：

- 配置設定檔必須使用一個連接對話 script，其中包括使用者驗證功能。使用者驗證功能包括接受要求者送來的使用者 ID 和密碼，並加以驗證。系統出貨時，附有許多對話 script 樣本提供有這個功能。
- 配置設定檔必須指定步驟 2 所建立之授權清單的名稱。授權清單中必須有連接對話 script 所收到的使用者 ID。

請記住，撥入安全的設置值會受到撥入系統的安全措施和功能的影響。如果您需要使用者 ID 和密碼，則提出要求之系統的連接對話 script 必須傳送該使用者 ID 和密碼。有些系統，例如 iSeries 伺服器，會提供一個安全方法來儲存使用者 ID 和密碼。(第 111 頁的『安全性和撥出階段作業』說明這個方法。) 其它系統則將使用者 ID 和密碼儲存在 script 中，而任何知道 script 在系統中之位置的使用者，都有可能存取這個 script。

由於您的通訊伙伴可能擁有不同的安全措施和功能，因此，您可以針對要求端的不同配置環境來建立不同的配置設定檔。您可以使用 STRTCPPTP 指令來設置您的系統，使

它接受某個特定配置設定檔的階段作業。例如，您可以只在一天中的某些時間，針對某些配置設定檔來啓動階段作業。您可以使用安全審核來記錄相關使用者設定檔的活動。

防止撥入使用者存取其它系統

根據您的系統和網路配置，啓動 SLIP 連接的使用者也許不必登入您的系統，即可存取您網路中的另一個系統。例如，使用者可建立一個 SLIP 連接來通往您的系統。之後，使用者可以建立一個 FTP 連接來通往您網路中另一個不容許撥入的系統。

您可以在配置設定檔的*容許 IP 資料包轉遞*欄位中指定 N (否) ，來防止 SLIP 使用者存取您網路中的其它系統。如此可防止使用者在登入您的系統前，先存取您的網路。不過，在使用者順利登入您的系統後，資料包轉遞值即不再有用。它不會限制使用者的功能，讓他們無法使用 iSeries 系統中的 TCP/IP 應用程式 (如 FTP 或 TELNET) 來建立與網路中其它系統的連線。

控制撥出階段作業

在使用者可使用 SLIP 來建立以您的系統爲起點的撥出連接之前，您必須先啓動 SLIP *DIAL 配置設定檔。如果要建立或變更 SLIP 配置，您可以使用 WRKTCPPTP 指令。如果要啓動配置設定檔，您可以使用「啓動 TCP/IP 點對點 (STRTCPPTP)」指令，或使用 WRKTCPPTP 顯示畫面的選項。當您的系統出貨時，STRTCPPTP 和 ENDTCPPTP 指令的公用權限是 *EXCLUDE。您必須擁有 *IOSYSCFG 特殊權限，才能使用新增、變更和刪除 SLIP 配置設定檔的選項。如果您是一個安全主管，您可以使用指令權限和特殊權限來判斷，哪個使用者可設置您的系統以容許建立撥出連接。

安全性和撥出階段作業

iSeries 系統中的使用者可以建立撥出連接來通往需要驗證使用者的系統。iSeries 伺服器中的連接對話 Script 必須傳送使用者 ID 和密碼給遠端系統。iSeries 伺服器會提供一個安全的方法來儲存這個密碼。在連接對話 script 中，不需要儲存密碼。

註:

1. 雖然您的系統會以加密的形式來儲存連接密碼，但在傳送這個密碼之前，系統會先予以解密。和 FTP 和 TELNET 密碼一樣，SLIP 密碼是以未加密的方式來傳送的 (『以清楚的方式』)。不過，它和 FTP 和 TELNET 仍有不同，在系統建立 TCP/IP 模式之前，會先傳送 SLIP 密碼。

   由於 SLIP 是以非同步的模式來使用點對點連接，因此，在傳送未加密的密碼時，它的安全漏洞與 FTP 和 TELNET 密碼不同。當網路傳送未加密的 FTP 和 TELNET 密碼時，可將它們當作 IP 通訊來傳送，因此，它們很容易受到電子循跡追蹤的侵犯。至於 SLIP 密碼的傳輸，它的安全程度和兩個系統間的電話連接相同。
2. 用來儲存 SLIP 連接對話 script 的預設檔案是 QUSRSYS/QATOCPPSCR。這個檔案的公用權限是 *USE，它會防止任何公共使用者變更預設連接對話 script。

當您建立連接設定檔來提供給需要驗證的遠端階段作業時，請執行下列動作：

__ 步驟 1. 確定「保留伺服器安全資料 (QRETSVRSEC)」系統值是 1 (是)。這個系統值用來決定可解密的密碼是否可儲存在系統中的受保護區內。

__ 步驟 2. 使用 WRKTCPPTP 指令來建立配置設定檔，讓設定檔擁有下列特性：

- 對於配置設定檔的模式，指定 *DIAL。

- 對於*遠端服務存取名稱*，指定遠端系統所預期的使用者 ID。例如，如果您要連接到另一個 iSeries 伺服器，則指定該 iSeries 伺服器中的使用者設定檔名稱。
- 對於*遠端服務存取密碼*，指定遠端系統預期適用於這個使用者 ID 的密碼。在您的 iSeries 伺服器中，這個密碼依可解密的形式，儲存在受保護的區域內。您指定給配置設定檔的名稱和密碼關聯於 QTCP 使用者設定檔。這些名稱和密碼無法透過任何使用者指令或介面來存取。只有已登記的系統程式可以存取這個密碼資訊。

  註: 請記住，當您儲存 TCP/IP 配置檔時，不會儲存連接設定檔的密碼。如果要儲存 SLIP 密碼，您需要使用「儲存安全資料 (SAVSECDTA)」指令來儲存 QTCP 使用者設定檔。
- 對於連接對話 script，指定一個傳送使用者 ID 和密碼的 script。系統出貨時，附有許多對話 script 樣本提供有這個功能。當系統執行 script 時，系統會取出密碼，予以解密，再將它傳送到遠端系統。

使用點對點通訊協定的安全注意事項

您可以將點對點通訊協定 (PPP) 當作 TCP/IP的一部份來使用。PPP 是點對點連接的工業標準，可對透過 SLIP 來使用的項目提供額外的功能。

使用 PPP 時，您的 iSeries 伺服器可使用高速連接直接通往「網際網路服務提供者」，或通往企業內部網路或企業外部網路中的其它系統。遠端 LAN 可以很有彈性地建立與 iSeries 伺服器之間的撥接連線。

請記住，PPP 和 SLIP 一樣，可提供網路連接來聯絡您的 iSeries 伺服器。基本上，PPP 連接會將要求者帶到您的系統門口。和 TELNET 或 FTP 一樣，要求者仍需要有使用者 ID 和密碼才能進入您的系統，並連接到 TCP/IP 伺服器。以下是這個新連接功能的安全注意事項：

註: 您在 IBM iSeries Access for Windows 工作站中使用 iSeries 領航員來配置 PPP。

- PPP 提供使用專用連接的功能 (同一個使用者固定使用同一個 IP 位址)。由於使用專用位址，因此，有受到「IP 詐騙」的可能 (冒充的系統偽裝成具有已知 IP 位址的可信系統)。不過，PPP 所提供的加強型身份驗證功能，可協助您免於受到「IP 詐騙」的侵犯。
- 使用 PPP 時，正如同使用 SLIP，您會建立擁有使用者名稱和相關密碼的連接設定檔。然而，與 SLIP 不同的是使用者不需具備有效的使用者設定檔及密碼。使用者名稱及密碼與使用者設定檔無關。相反地，會在 PPP 鑑定中使用驗證列示。此外，PPP 也不需要連接 Script。身份驗證 (交換使用者名稱和密碼) 是 PPP 架構的一部份，發生在比 SLIP 低的層面。
- 使用 PPP 時，您擁有使用 CHAP (盤查交握身份驗證通訊協定) 的選項。您不需要擔心竊聽者追蹤密碼的行為，因為 CHAP 會對使用者名稱和密碼進行加密處理。

  只有當兩端都擁有 CHAP 支援時，您的 PPP 連接才會使用 CHAP。在兩個數據機互相交換信號以設置通訊期間，兩個系統會進行協定。例如，如果 SYSTEMA 支援 CHAP 而 SYSTEMB 不支援，則 SYSTEMA 可以拒絕階段作業，或同意使用未加密的使用者名稱和密碼。同意使用未加密的使用者名稱和密碼，稱為向下協定。向下協定的決定是一個配置選項。例如，如果在您的企業內部網路中，您知道您的所有

系統都具有 CHAP 功能，您應該配置您的連接設定檔，使它不會向下協定。但在您的系統正要撥出的公用網路中，您可能會想要向下協定。

PPP 的連接設定檔可提供指定有效 IP 位址的功能。例如，您可以針對某個特定使用者，指示您所預期的特定位址或位址範圍。這個功能和加密密碼的功能合起來，可針對詐騙的行爲提供進一步的保護。

如果您要針對詐騙和挾帶，爲作用中的階段作業提供其它保護，您可以配置 PPP 來依照指定的間隔重複盤查。例如，當 PPP 階段作業作用時，您的 iSeries 伺服器可以針對使用者和密碼來盤查其它系統。它會每 15分鐘執行一次，以確定這是相同的連接設定檔。(一般使用者不會知道這個重複盤查的活動。系統會在一般使用者所見到的層次以下交換名稱和密碼。)

使用 PPP 時，遠端 LAN 可能會建立撥入連接來通往您的 iSeries 伺服器和您的擴充網路。在這個環境中，可能需要開啓 IP 轉遞。使用 IP 轉遞時，侵入者可以在您的網路中遊蕩。不過，PPP 擁有很強的保護 (例如密碼和 IP 位址驗證的加密)。這會讓侵入者很難著手建立網路連接。

如果需要 PPP 的詳細資訊，請參閱「iSeries 資訊中心」。

使用啓動程式通訊協定伺服器的安全注意事項

| 啓動程式通訊協定 (BOOTP) 提供一種動態的方法，用來將工作站關聯於伺服器，並指
| 定工作站 IP 位址和起始程式載入 (IPL) 來源。

BOOTP 是一個 TCP/IP 通訊協定，無媒體工作站 (用戶端) 用它來要求含有網路中某個伺服器之起始程式碼的檔案。BOOTP 伺服器以通用的 BOOTP 伺服器埠 67 來接收。在收到某個用戶端要求時，伺服器會尋找定義給該用戶端的 IP 位址，並傳回一則回答給該用戶端，附有用戶端的 IP 位址和載入檔的名稱。然後，用戶端會起始一個 TFTP 要求，向伺服器要求載入檔。用戶端硬體位址及 IP 位址間的對映，會保留在 iSeries 伺服器的 BOOTP 表格中。

防止 BOOTP 存取

如果您不要讓任何 Thin Client 連接到您的網路，您不需要在您的系統中執行 BOOTP 伺服器。它可以用在其它裝置，但這些裝置所偏好的解決方案是使用 DHCP。請執行下列動作來防止執行 BOOTP 伺服器：

__ 步驟 1. 如果要在啓動 TCP/IP 時，防止自動執行 BOOTP 伺服器工作，請鍵入下列字串：

```
CHGBPA AUTOSTART(*NO)
```

註:

1. AUTOSTART(*NO) 是預設值。
2. 第 108 頁的『控制自動啓動的 TCP/IP 伺服器』提供控制自動啓動哪些 TCP/IP 伺服器的詳細資訊。

__ 步驟 2. 若要避免某人將使用者應用程式 (例如 Socket 應用程式)，與系統通常用來執行 BOOTP 的連接埠連結起來，請執行下列動作：

註: 由於 DHCP 和 BOOTP 使用相同的埠號，因此這會抑制 DHCP 所使用的埠。如果您要使用 DHCP，請勿限制這個埠。

__ 步驟 a. 鍵入 `GO CFGTCP`，以顯示「配置 TCP/IP」功能表。

__ 步驟 b. 選取選項 4 (使用 TCP/IP 埠限制)。

__ 步驟 c. 在「使用 TCP/IP 埠限制」顯示畫面中，指定選項 1 (新增)。

__ 步驟 d. 對於較低的埠範圍，指定 `67`。

__ 步驟 e. 對於較高的埠範圍，指定 `*ONLY`。

註:

1. 埠限制在您下次啓動 TCP/IP 時生效。如果您設定埠限制時 TCP/IP 在作用中，您應該先結束 TCP/IP，再重新啓動。
2. RFC1700 提供通用埠號指定的相關資訊。

__ 步驟 f. 對於通訊協定，指定 `*UDP`。

__ 步驟 g. 請在使用者設定檔欄位中指定系統中受保護的使用者設定檔。(受保護的使用者設定檔是未擁有沿用權限之程式的使用者設定檔，且沒有其它使用者所知道的密碼。) 將埠限制於特定使用者後，您會自動排除所有其它使用者。

保護 BOOTP 伺服器的安全

BOOTP 伺服器不提供對於您的 iSeries 系統的直接存取功能，因此具有較少的安全漏洞。作爲一個安全管理者，主要關心的是確定讓正確的資訊關聯於正確的 Thin Client。換言之，災害的製造者可能會改變 BOOTP 表格，並導致 Thin Client 作業不正常，或沒有影響。

如果要管理 BOOT 伺服器和 BOOTP 表格，您必須擁有 *IOSYSCFG 特殊權限。您必須小心地控制在您的系統中擁有 *IOSYSCFG 特殊權限的使用者設定檔。

使用 DHCP 伺服器的安全注意事項

動態的主電腦配置通訊協定 (DHCP) 提供一個架構，讓您傳送配置資訊給 TCP/IP 網路中的主電腦。對於您的用戶端工作站而言，DHCP 可提供類似於自動配置的功能。用戶端工作站中啓用 DHCP 的程式會播送對於配置資訊的要求。如果您的 iSeries 伺服器正在執行 DHCP 伺服器，則伺服器會回應這個要求，並送出從屬工作站所需要的資訊，讓它能夠正確地配置 TCP/IP。

您可以使用 DHCP，讓第一次連接到您的 iSeries 伺服器的使用者能更容易建立連接。因爲，這可讓使用者不必輸入 TCP/IP 配置資訊。您也可以使用 DHCP 來減少次網路中所需要的內部 TCP/IP 位址的數目。DHCP 伺服器可以將 IP 位址 (來源爲它的 IP 位址儲存池) 暫時配置給作用中的使用者。

對於 Thin Client 而言，您可以使用 DHCP 來取代 BOOTP。DHCP 提供的功能比 BOOTP 多，並且可支援 Thin Client 和 PC 的動態配置。

防止 DHCP 存取

如果您不讓任何使用者在您的系統中使用 DHCP 伺服器，請執行下列動作：

1. 如果要在啓動 TCP/IP 時，防止自動執行 DHCP 伺服器工作，請鍵入下列字串：

   ```
   CHGDHCPA AUTOSTART(*NO)
   ```

   註:

   1. AUTOSTART(*NO) 是預設值。

2. 第 108 頁的『控制自動啓動的 TCP/IP 伺服器』提供控制自動啓動哪些 TCP/IP 伺服器的詳細資訊。

2. 若要避免某人將使用者應用程式 (例如 Socket 應用程式)，與系統通常用來執行 DHCP 的連接埠連結起來，請執行下列動作：

   a. 鍵入 GO CFGTCP，以顯示「配置 TCP/IP」功能表。

   b. 選取選項 4 (使用 TCP/IP 埠限制)。

   c. 在「使用 TCP/IP 埠限制」顯示畫面中，指定選項 1 (新增)。

   d. 對於較低的埠範圍，指定 67。

   e. 對於較高的埠範圍，指定 68。

      註:

      1. 埠限制在您下次啓動 TCP/IP 時生效。如果您設定埠限制時 TCP/IP 在作用中，您應該先結束 TCP/IP，再重新啓動。

      2. RFC1700 提供通用埠號指定的相關資訊。

   f. 對於通訊協定，指定 *UDP。

   g. 請在使用者設定檔欄位中指定系統中受保護的使用者設定檔。(受保護的使用者設定檔是未擁有沿用權限之程式的使用者設定檔，且沒有其它使用者所知道的密碼。) 將埠限制於特定使用者後，您會自動排除所有其它使用者。

保護 DHCP 伺服器的安全

以下是您在 iSeries 系統中執行 DHCP 時，有關安全性的注意事項：

- 限制擁有管理 DHCP 之權限的使用者數目。管理 DHCP 需要下列權限：
  - *IOSYSCFG 特殊權限
  - 下列檔案的 *RW 權限：

    ```
    /QIBM/UserData/OS400/DHCP/dhcpsd.cfg
    /QIBM/UserData/OS400/DHCP/dhcprd.cfg
    ```

- 評估您的 LAN 實際上的可存取程度。外來者是否可以很容易地使用膝上型電腦進入您的位置，並實際地連接到您的 LAN？如果出現這個安全漏洞，則 DHCP 可提供一個建立用戶端 (硬體位址) 列示的功能，列示中包括 DHCP伺服器所將配置用戶端。當您使用這個特性時，您會犧牲 DHCP 提供給您的網路管理者的若干生產能力上的好處。不過，您可以防止系統配置來路不明的工作站。
- 如果可能，請使用可重複使用的 IP 位址儲存池 (不是爲了網際網路而設計的)。這有助於避免讓網路外的工作站從伺服器取得可用的配置資訊。
- 如果您需要其它安全保護，請使用 DHCP 跳出程式。以下是跳出程式及其功能的概觀。*iSeries AS/400 System API Referenc* 說明如何使用這些跳出程式。

  埠登錄 每當系統從埠 67 (DHCP 埠) 讀到資料分封時，都會呼叫您的跳出程式。您的跳出程式會收到完整的資料分封。它可以決定系統要處理或捨棄這個分封。當現存的 DHCP 螢幕顯示特性不符合您的需求時，您可以使用這個跳出程式。

  位址指定
  每當 DHCP 正式指定位址給用戶端時，系統會呼叫您的跳出程式。

  位址釋放
  每當 DHCP 正式釋放一個位址，並將它放回位址儲存池時，系統會呼叫您的跳出程式。

使用 TFTP 伺服器的安全注意事項

簡易檔案轉送通訊協定 (TFTP) 提供基本的檔案轉送功能，不進行使用者的身份驗證。TFTP 可以處理 啓動程式通訊協定 (BOOTP) 或 動態的主電腦配置通訊協定 (DHCP)。

用戶端一開始就會連接到 BOOTP 伺服器或 DHCP 伺服器。 BOOTP 伺服器或 DHCP 伺服器會以用戶端的 IP 位址和載入檔的名稱來回應。然後，用戶端會起始一個 TFTP 要求，向伺服器要求載入檔。當用戶端完成載入檔的下載作業時，它會結束 TFTP 階段作業。

防止 TFTP 存取

如果您不要讓任何 Thin Client 連接到您的網路，您不需要在您的系統中執行 TFTP 伺服器。請執行下列動作來防止執行 TFTP 伺服器：

__ 步驟 1. 如果要在啓動 TCP/IP 時，防止自動執行 TFTP 伺服器工作，請鍵入下列字串：

```
CHGTFTPA AUTOSTART(*NO)
```

註:

1. AUTOSTART(*NO) 是預設值。
2. 第 108 頁的『控制自動啓動的 TCP/IP 伺服器』提供控制自動啓動哪些 TCP/IP 伺服器的詳細資訊。

__ 步驟 2. 若要避免讓某人將使用者應用程式 (例如 Socket 應用程式)，與系統通常用來執行 TFTP 的連接埠連結起來，請執行下列動作：

__ 步驟 a. 鍵入 `GO CFGTCP`，以顯示「配置 TCP/IP」功能表。

__ 步驟 b. 選取選項 4 (使用 TCP/IP 埠限制)。

__ 步驟 c. 在「使用 TCP/IP 埠限制」顯示畫面中，指定選項 1 (新增)。

__ 步驟 d. 對於較低的埠範圍，指定 `69`。

__ 步驟 e. 對於較高的埠範圍，指定 `*ONLY`。

註:

1. 埠限制在您下次啓動 TCP/IP 時生效。如果您設定埠限制時 TCP/IP 在作用中，您應該先結束 TCP/IP，再重新啓動。
2. RFC1700 提供通用埠號指定的相關資訊。

__ 步驟 f. 對於通訊協定，指定 `*UDP`。

__ 步驟 g. 請在使用者設定檔欄位中指定系統中受保護的使用者設定檔。(受保護的使用者設定檔是未擁有沿用權限之程式的使用者設定檔，且沒有其它使用者所知道的密碼。) 將埠限制於特定使用者後，您會自動排除所有其它使用者。

保護 TFTP 伺服器的安全

依預設，TFTP 伺服器所提供對於您的 iSeries 系統的存取非常有限。特別配置提供 Thin Client 的起始碼。如果您是安全主管，您應該知道 TFTP 伺服器的下列特性：

- TFTP 伺服器不需要身份驗證 (使用者 ID 和密碼)。所有 TFTP 工作都在 QTFTP 使用者設定檔之下執行。QTFTP 使用者設定檔沒有密碼。因此，它無法用於交談式登入。QTFTP 使用者設定檔沒有任何特殊權限，也未明確取得系統資源的權限。它使用公用權限來存取 Thin Client 所必須使用的資源。

- 當 TFTP 伺服器到達時，會配置為存取 Thin Client 資訊所在的目錄。您必須擁有 *PUBLIC 或 QTFTP 權限，才能讀取或寫入該目錄。如果要寫入該目錄，您必須在 CHGTFTPA 指令的「容許檔案寫入」參數中指定 *CREATE。如果要寫入既有的檔案，您必須在 CHGTFTPA 指令的「容許檔案寫入」參數中指定 *REPLACE。*CREATE 可讓您置換現存的檔案或是建立新檔案。*REPLACE 僅能讓您置換現存的檔案。

  除非您使用「變更 TFTP 屬性 (CHGTFTPA)」指令來明確地定義目錄，否則 TFTP 無法存取任何其它目錄。因此，如果有區域或遠端使用者試圖針對您的系統來啟動 TFTP 階段作業，使用者存取資訊或造成損壞的能力，都將非常有限。
- 如果您選擇要配置 TFTP 伺服器，以提供處理 Thin Client 以外的其它服務，您可以定義一個跳出程式來評估並授權每個 TFTP 要求。TFTP 伺服器會提供一個要求驗證跳出程式，類似於可用於 FTP 伺服器的跳出程式。如需詳細資訊，請參閱 iSeries 資訊中心 --> 網路功能 --> TCP/IP --> TFTP。請參閱第 xii 頁的『先決條件與相關資訊』，以獲得存取「iSeries 資訊中心」的資訊。

使用 REXEC 伺服器的安全注意事項

遠端執行伺服器 (REXEC) 會接收和執行 REXEC 用戶端所發出的指令。REXEC 用戶端通常是支援傳送 REXEC 指令的一個 PC 或 UNIX 應用程式。這個伺服器所提供的支援，類似於對 FTP 伺服器使用 RCMD (遠端指令) 次指令時所使用的功能。

防止 REXEC 存取

如果不讓您的 iSeries 伺服器接受 REXEC 用戶端所發出的指令，請執行下列動作來防止執行 REXEC 伺服器：

__ 步驟 1. 如果要在啓動 TCP/IP 時，防止自動執行 REXEC 伺服器工作，請鍵入下列字串：

```
CHGRXCA AUTOSTART(*NO)
```

註:

1. AUTOSTART(*NO) 是預設值。
2. 第 108 頁的『控制自動啓動的 TCP/IP 伺服器』提供控制自動啓動哪些 TCP/IP 伺服器的詳細資訊。

__ 步驟 2. 若要避免讓某人將使用者應用程式 (例如 Socket 應用程式)，與系統通常用來執行 REXEC 的連接埠連結起來，請執行下列動作：

__ 步驟 a. 鍵入 `GO CFGTCP`，以顯示「配置 TCP/IP」功能表。

__ 步驟 b. 選取選項 4 (使用 TCP/IP 埠限制)。

__ 步驟 c. 在「使用 TCP/IP 埠限制」顯示畫面中，指定選項 1 (新增)。

__ 步驟 d. 對於較低的埠範圍，指定 `512`。

__ 步驟 e. 對於較高的埠範圍，指定 `*ONLY`。

__ 步驟 f. 對於通訊協定，指定 `*TCP`。

__ 步驟 g. 請在使用者設定檔欄位中指定系統中受保護的使用者設定檔。(受保護的使用者設定檔是未擁有沿用權限之程式的使用者設定檔，且沒有其它使用者所知道的密碼。) 將埠限制於特定使用者後，您會自動排除所有其它使用者。

註:

1. 埠限制在您下次啓動 TCP/IP 時生效。如果您設定埠限制時 TCP/IP 在作用中，您應該先結束 TCP/IP，再重新啓動。
2. RFC1700 提供通用埠號指定的相關資訊。

保護 REXEC 伺服器的安全

以下是您在系統中執行遠端執行伺服器時，相關的注意事項：

- REXCD 要求包括使用者 ID、密碼，以及要執行的指令。正常的 iSeries 伺服器身份驗證和權限檢查適用情況：
  – 使用者設定檔和密碼的組合必須有效。
  – 系統強制爲使用者設定檔使用*限制功能* (LMTCPB) 値。
  – 使用者必須取得指令和指令所使用之所有資源的權限。
- REXEC 伺服器所提供的跳出程式類似於 FTP 伺服器所能使用的跳出程式。您可以使用「驗證」跳出程式來評估指令，並判斷是否容許執行該指令。如需相關資訊，請參閱 iSeries 資訊中心 --> 網路功能 --> TCP/IP --> REXEC。請參閱第 xii 頁的『先決條件與相關資訊』，以獲得存取「iSeries 資訊中心」的資訊。
- 當您選擇要執行 REXEC 伺服器時，您的執行作業不涉及您在系統中所擁有的任何功能表存取控制。您必須確定您的物件權限架構足以保護您的資源。

使用 RouteD 的安全注意事項

路由常駐程式 (RouteD) 伺服器提供在 iSeries 伺服器中的「遞送資訊通訊協定 (RIP)」支援。在遞送通訊協定中，RIP 的使用最爲廣泛。它是一個「內部閘道通訊協定」，可協助 TCP/IP 遞送匿名系統內的 IP 分封。

RouteD 的目的，是要讓可信網路內的系統互相更新最新的遞送資訊，來增加網路通訊的效率。當您執行 RouteD 時，您的系統可以收到其它參與的系統所送出的，有關傳輸 (分封) 遞送方式的更新內容。因此，如果駭客能夠存取您的 RouteD 伺服器，駭客可能會利用它，並透過可追蹤或修改這些分封的系統來重新遞送您的分封。以下是有關 RouteD 安全的建議事項：

- iSeries 伺服器會使用 RIPv1，它不提供任何驗證路由器身份的方法。它的目的是要在可信網路之內使用。如果您的系統所在的網路中有 ″不可信″ 的系統，您不應該執行 RouteD 伺服器。如果要確定不會自動啓動 RouteD 伺服器，請鍵入下列字串：

  ```
  CHGRTDA AUTOSTART(*NO)
  ```

  註:

  1. AUTOSTART(*NO) 是預設値。
  2. 第 108 頁的『控制自動啓動的 TCP/IP 伺服器』提供控制自動啓動哪些 TCP/IP 伺服器的詳細資訊。
- 請確定您可以控制哪些人能變更 RouteD 配置，他們需要有 *IOSYSCFG 特殊權限。
- 如果您的系統參與多個網路 (如企業內部網路和網際網路)，您可以將 RouteD 伺服器配置爲只和安全網路互相傳送和接收更新內容。

使用 DNS 伺服器的安全注意事項

網域名稱系統 (DNS) 伺服器提供主電腦名稱和 IP 位址之間來回轉換的功能。在 iSeries 伺服器中，DNS 伺服器的目的，是要提供內部安全網路 (企業內部網路) 的位址轉換功能。

防止 DNS 存取

如果您不讓任何使用者在您的系統中使用 DNS 伺服器，請執行下列動作：

1. 如果要在啓動 TCP/IP 時，防止自動執行 DNS 伺服器工作，請鍵入下列字串：

   ```
   CHGDNSA AUTOSTART(*NO)
   ```

   註:

   1. AUTOSTART(*NO) 是預設值。
   2. 第 108 頁的『控制自動啓動的 TCP/IP 伺服器』提供控制自動啓動哪些 TCP/IP 伺服器的詳細資訊。
2. 若要避免讓某人將使用者應用程式 (例如 Socket 應用程式)，與系統通常用來執行 DNS 的連接埠連結起來，請執行下列動作：
   a. 鍵入 GO CFGTCP，以顯示「配置 TCP/IP」功能表。
   b. 選取選項 4 (使用 TCP/IP 埠限制)。
   c. 在「使用 TCP/IP 埠限制」顯示畫面中，指定選項 1 (新增)。
   d. 對於較低的埠範圍，指定 53。
   e. 對於較高的埠範圍，指定 *ONLY。

      註:

      1. 埠限制在您下次啓動 TCP/IP 時生效。如果您設定埠限制時 TCP/IP 在作用中，您應該先結束 TCP/IP，再重新啓動。
      2. RFC1700 提供通用埠號指定的相關資訊。
   f. 對於通訊協定，指定 *TCP。
   g. 請在使用者設定檔欄位中指定系統中受保護的使用者設定檔。(受保護的使用者設定檔是未擁有沿用權限之程式的使用者設定檔，且沒有其它使用者所知道的密碼。) 將埠限制於特定使用者後，您會自動排除所有其它使用者。
   h. 重複 *UDP（使用者資料圖）通訊協定的步驟 2c 到 2g。

保護 DNS 伺服器的安全

以下是您在 iSeries 系統中執行 DNS 時，有關安全性的注意事項：

- DNS 伺服器所提供的，是對於 IP 位址和名稱的轉換功能。它不提供對於 iSeries 系統中之物件的任何存取功能。當外來者存取您的 DNS 伺服器時，您的風險是，伺服器會提一個簡便的途徑，讓外來者可以察看網路的拓樸內涵。您的 DNS 可能會使駭客省下不少精力，即可取得潛在目標的位址。不過，您的 DNS 並不會提供協助他們侵入目標系統的資訊。
- 通常您會將 iSeries DNS 伺服器用在企業內部網路。因此，您不需要限制對於 DNS 的查詢功能。不過，您可能會有某些情況，例如，在企業內部網路內有若干次網路。您可能不想讓另一個次網路的使用者查詢您 iSeries 伺服器的 DNS。DNS 的安全選項可讓您限制對於主要網域的存取。您可以使用「iSeries 領航員」來指定 DNS 伺服器所應回應的 IP 位址。

另一個安全選項可讓您指定哪些次要伺服器可從您的主要 DNS 伺服器中複製資訊。當您使用這個選項時，您的伺服器會接受您明確列出的次要伺服器所發出的區域轉送要求 (要求複製資訊)。

- 請務必小心限制變更 DNS 伺服器之配置檔的功能。有些使用者可能會有動機不善的作為，例如，變更您的 DNS 檔，讓它指向在您網路之外的 IP 位址。他們可能會摸擬您網路內的伺服器，並透過訪問伺服器的使用者，順利存取機密資訊。

使用 HTTP Server for iSeries 的安全注意事項

HTTP 伺服器提供全球資訊網瀏覽器用戶端，可存取 iSeries 伺服器多媒體物件，例如 HTML (超文字標示語言) 文件。此外，其也支援*共用閘道介面 (CGI)* 規格。應用程式設計師可撰寫 CGI 程式，擴充伺服器的功能。

管理者可以使用 網際網路連線伺服器 或 IBM HTTP Server for iSeries 在相同的 iSeries 伺服器上同時執行多個伺服器。每個執行中的伺服器都稱為**伺服器案例**。每個伺服器案例都有一個唯一的名稱。管理者可控制要啓動哪些案例，以及每個案例執行的動作。

註: 當您使用 Web 瀏覽器來配置或管理下列中的任何項目時，您必須已在執行 HTTP 伺服器的 *ADMIN 案例：

- Firewall for iSeries
- 網際網路連線伺服器
- 網際網路連線安全伺服器
- IBM HTTP Server for iSeries

使用者 (網站造訪者) 絕不會看到 iSeries 伺服器「登入」顯示畫面。不過，iSeries 伺服器管理者必須使用 HTTP 指引定義所有 HTML 文件和 CGI 程式，以明確授權之。此外，管理者也可以針對部份或全部要求，設置資源安全和使用者鑑定 (使用者 ID 和密碼)。

駭客的攻擊可能會使您的 Web 伺服器陷於拒絕服務的情況。您的伺服器可以計量某用戶端要求的逾時來偵測出拒絕服務的攻擊。如果伺服器未收到用戶端送來的要求，則您的伺服器會判定有拒絕服務的攻擊在進行中。這出現的時機，是在用戶端起始連接到您的伺服器之後。伺服器的預設值是偵測和宣告攻擊。

防止 HTTP 存取

如果您*不*想讓任何人透過程式存取您的系統，您應該防止 HTTP 伺服器執行。請執行下列作業：

__ 步驟 1. 如果要在啓動 TCP/IP 時，防止自動執行 HTTP 伺服器工作，請鍵入下列字串：

```
CHGHTTPA AUTOSTART(*NO)
```

註:

1. AUTOSTART(*NO) 是預設值。
2. 第 108 頁的『控制自動啓動的 TCP/IP 伺服器』提供控制自動啓動哪些 TCP/IP 伺服器的詳細資訊。

__ 步驟 2. 依預設，HTTP 伺服器工作使用 QTMHHTTP 使用者設定檔。如果不要啓動 HTTP 伺服器，請將 QTMHHTTP 使用者設定檔的狀態設定爲 *DISABLED。

控制對 HTTP 伺服器的存取

執行 HTTP 伺服器的主要目的，是要讓來訪者存取您 iSeries 系統中的網站。您可以想像某個使用者拜訪您的網站，猶如某個消費者在翻看商業雜誌中的廣告。來訪者並不知道您的網站所執行的軟硬體，例如您使用哪種類型的伺服器，您的伺服器實際所在的位置爲何。通常，您也不要在可能的來訪者和您的網站之間，佈置任何障礙物 (例如「登入」顯示畫面)。不過，您可以限制對於某些文件的存取，或是對於您的網站所提供之 CGI 程式的存取。

您也可以讓單一的 iSeries 系統提供多個邏輯網站。例如，您的 iSeries 系統可能會支援企業的多個分支單位，它們各有不同的客戶群。對於各個企業分支單位，您需要一個完全獨立的單一網站，來提供給來訪的使用者。此外，您可以提供內部的網站 (企業內部網路)，提供關於您的企業的機密資訊。

作爲一個安全管理者，您需要做的是，保護網站的內容，同時確定您的安全措施不會對您的網站價值造成負面的影響。此外，您必須確定，HTTP 活動不會使您的系統或網路陷入危險之中。下列主題提供使用此程式時的安全建議事項。

管理注意事項

以下是管理您網際網路伺服器的若干安全注意事項。

- 您使用 Web 瀏覽器和 *ADMIN 案例來執行某些設置和配置功能。至於某些功能，例如建立在伺服器中建立額外的案例，您*必須*使用 *ADMIN 伺服器。
- 管理首頁 (*ADMIN 伺服器的首頁) 的預設 URL 公佈在提供瀏覽器管理功能之產品的說明文件中。因此，駭客可能會知道預設的 URL，並將之公佈於駭客論壇，就好像將 IBM 所提供之使用者設定檔的預設密碼公開公佈一樣。您可以避免讓自己暴露在這個漏洞之下，方法如下：
  - 只在您需執行管理功能時，才執行 HTTP 伺服器的 *ADMIN 案例。不要讓 *ADMIN 案例始終在執行的狀態中。
  - 爲 *ADMIN 案例啓動 SSL 支援 (透過「數位認證管理程式」)。*ADMIN 會透過 HTTP 保護指示來要求使用者 ID 和密碼。當您使用 SSL 時，會將您的使用者 ID 與密碼 (以及出現在管理表格中有關係您的配置的所有其它資訊) 加密。
  - 使用防火牆可防止使用者從網際網路存取 *ADMIN 伺服器，也可以隱藏您在 URL 中的系統和網域名稱。
- 當您執行管理功能時，您必須使用具有 *IOSYSCFG 特殊權限的使用者設定檔來登入。您可能也需要系統中之特定物件的權限，例如：
  - 含有您的 HTML 文件和 CGI 程式的檔案庫或指示。
  - 您計劃要予以交換，使它出現在伺服器指示之內的任何使用者設定檔。
  - 您的指示所使用之任何目錄的「存取控制列示 (ACL)」。
  - 用來建立和維護使用者 ID 和密碼的驗證列示物件。

  使用 *ADMIN 伺服器和 TELNET 時，您可以利用遠端方式來執行管理功能，例如，透過網際網路的連線。您必須知道，當您透過公用鏈接 (網際網路) 來執行管理作業時，可能會將有力的使用者 ID 和密碼暴露在循跡追蹤之下。之後，"循跡追蹤者" 可以使用這個使用者 ID 和密碼，經由 TELNET 或 FTP 等方式來嘗試存取您的系統。

註:

1. 使用 TELNET 時，「登入」顯示畫面的處理方式和任何其它顯示畫面沒有不同。雖然您鍵入密碼時，螢幕中不會出現這個密碼，但系統傳輸時不會對它進行任何加密或編碼的程序。
2. 當使用 *ADMIN 伺服器時，會對密碼進行編碼，但不會加密。編碼的架構是一個工業標準，因此，駭客集團對它具有充分掌握的能力。雖然臨時性的 ″循跡追蹤者″ 不容易瞭解編碼的狀況，但追蹤老手可能會有密碼的解碼工具。

安全要訣

如果您想透過網際網路來進行遠端管理，您應該搭配使用 *ADMIN 案例和 SSL，對您的傳輸進行加密。不使用不安全的應用程式，如 V4R4 之前的 TELNET (從 V4R4 開始，TELNET 可以支援 SSL)。如果您使用透過*信賴的*使用者的企業內部網路的 *ADMIN 伺服器，您也許可放心使用此伺服器來管理。

- HTTP 指示是您伺服器中的所有活動的基礎。出貨的配置提供預設「歡迎光臨」頁的伺服能力。在伺服器管理者定義伺服器的指示之前，用戶端無法檢視「歡迎光臨」頁以外的任何文件。如果要定義指示，您可以使用 Web 瀏覽器和 *ADMIN 伺服器，也可以使用「使用 HTTP 配置 (WRKHTTPCFG)」指令。兩個方法都需要 *IOSYSCFG 特殊權限。當您將 iSeries 伺服器連接到網際網路時，評估和控制企業組織內有多少使用者擁有 *IOSYSCFG 特殊權限，是一件非常重要的事。

保護資源

IBM HTTP server for iSeries 含有 HTTP 指引，可提供伺服器所使用之資訊資產的詳細控制。您可以使用指引來控制 Web 伺服器服務 HTML 檔案和通用閘道介面 (CGI) 程式之 URL 的目錄、與其他使用者設定檔交換、以及要求資源的鑑別。

註: 資訊中心中的「Web 服務」提供可用的 HTTP 指引，以及使用方式的完整說明。以下是使用這個支援的若干建議和注意事項：

- HTTP 伺服器以 ″明確的權限″ 作爲基礎來開始作業。如果某個要求在指示中沒有明確的定義，則伺服器不會接受這個要求。換言之，除非 URL 已 (依名稱或同屬方式) 定義於指示之中，否則伺服器會立即拒絕這個 URL 的任何要求。
- 您可以透過保護指令，要求使用者先提供使用者 ID 和密碼，才接受使用者對您某些或全部資源的要求。
  - 當使用者 (用戶端) 要求受保護的資源時，伺服器會盤查瀏覽器，要求它提供使用者 ID 和密碼。瀏覽器會提示使用者輸入使用者 ID 和密碼，然後再將資訊傳送給伺服器。有些瀏覽器會儲存使用者 ID 和密碼，並隨著後續的要求來自動傳送它們。如此使用者便不需要爲某個要求，重複輸入相同的使用者 ID 和密碼。

    由於某些瀏覽器會儲存使用者 ID 和密碼，因此，當使用者透過 iSeries 伺服器「登入」顯示畫面或路由器來進入您的系統時，將會有相同的使用者教學作業。無人式的瀏覽器階段作業代表一種潛在的安全漏洞。
  - 在系統處理使用者 ID 和密碼的方式（由保護指令指定）上，您有下列 3 種選擇：
    1. 您可以使用一般 iSeries 伺服器使用者設定檔和密碼驗證。這是最常用來保護企業內部網路 (安全網路) 中之資源的方式。

2. 您可以建立「網際網路使用者」：使用者可以被驗證，但在 iSeries 伺服器中沒有使用者設定檔。網際網路使用者是透過一種稱為「驗證清單」的 iSeries 伺服器物件來施行的。驗證列示物件含有專門定義來使用特定應用程式的使用者和密碼的列示。

   您決定要以什麼方式來提供網際網路使用者 ID 和密碼 (例如透過應用程式，或管理者回應電子郵件要求) ，以及如何管理這些網際網路使用者。您可以使用 HTTP 伺服器以瀏覽器為基礎的介面來進行這個設定。

   對非安全網路 (網際網路) 而言，網際網路使用者所提供的整體性保護，比一般使用者設定檔和密碼為佳。專用的使用者 ID 和密碼組可以建立內建的限制來控制使用者所能執行的動作。使用者 ID 和密碼不能用於一般登入 (例如 TELNET 或 FTP)。此外，您的一般使用者 ID 和密碼也不會成為線路循跡追蹤的對象。

3. 輕裝備目錄存取通訊協定 (LDAP) 是一個目錄服務通訊協定，可用來透過「傳輸控制通訊協定 (TCP)」存取目錄。可讓您在該目錄中儲存資訊並查詢之。目前所採用的 LDAP 支援方式，是作為使用者鑑別的一個選項。

註:

1. 當瀏覽器傳送使用者 ID 和密碼時 (不論是針對使用者設定檔或網際網路使用者) ，會對它們進行編碼，但不會予以加密。編碼的架構是一個工業標準，因此，駭客集團對它具有充分掌握的能力。雖然臨時性的 ″循跡追蹤者″ 不容易瞭解編碼的狀況，但追蹤老手可能會有密碼的解碼工具。
2. iSeries 伺服器會將驗證物件儲存在受保護的系統區域內。您必須透過定義好的系統介面 (API) 和適當權限，才能存取它。

– 您可以使用「數位憑證管理程式 (DCM)」建立您自己的企業內部網路「認證中心」。「數位憑證」會自動連結認證和擁有者的使用者設定檔。認證所擁有的授權與許可同於相關的設定檔。

• 當伺服器接受要求後，一般 iSeries 伺服器資源安全即取得控制。要求資源的使用者設定檔，必須擁有資源 (例如含有 HTML 文件的資料夾和實體檔案) 的權限。以預設值來說，工作是執行於 QTMHHTTP 使用者設定檔之下。您可以使用指引交換至另一個使用者設定檔。之後，系統會使用這個使用者設定檔權限來存取物件。以下是這個支援的若干注意事項：

  – 當您的伺服器提供多個邏輯網站時，交換使用者設定檔特別有用。您可為每個網站將不同的使用者設定檔與指引相關，之後即可使用一般 iSeries 伺服器資源安全程序來保護每個站台的文件。

  – 您可以結合交換使用者設定檔和驗證物件的功能。伺服器會使用唯一的使用者 ID 和密碼 (不同於您的一般使用者 ID 和密碼) 以評估起始要求。在伺服器驗證過使用者的身份後，系統會交換到另一個使用者設定檔，並利引的資源安全。因此，使用者不會知道真的使用者設定檔名稱，無法嘗試以其它方式 (FTP) 來使用它。

• 有些 HTTP 伺服器要求需要在 HTTP 伺服器執行程式。例如，可在您的系統中存取資料的程式。在程式可以執行之前，伺服器管理者必須先將要求 (URL) 對映至符合 CGI 使用者介面標準的特定使用者定義程式。以下是 CGI 程式的若干注意事項：

  – 和處理 HTML 文件一樣，您可以使用 CGI 程式的保護指示。因此，您可以在執行程式前，要求使用者 ID 和密碼。

  – 依預設，所有 CGI 程式都是在 QTMHHTP1 使用者設定檔之下執行的。在執行程式前，您可以交換至另一個使用者設定檔。因此，您可以針對您的通用閘道介面 (CGI) 程式所存取的資源，設置一般 iSeries 伺服器資源安全程序。

– 作爲一個安全管理者，您應該先進行安全複查，然後才授權在您的系統中使用任何 CGI 程式。您應該知道程式的來源，以及這個 CGI 程式所要執行的功能。您也應該監督用來執行 CGI 程式之使用者設定檔的功能。您也應該以 CGI 程式來進行測試，以判斷各種情況，例如，您是否可以存取某個指令行。請謹慎處理 CGI 程式，如同處理沿用權限的程式一般。
– 此外，您也必須評估哪些敏感性物件可能會有不當的公用權限。在少數情形中，設計不良的 CGI 程式會讓內行但行事不正的使用者試圖遊蕩到您的系統。
– 使用特定的使用者檔案庫 (如 CGILIB) 來保留您的所有 CGI 程式。請使用物件權限來控制哪些使用者可在這個檔案庫內放置新物件，哪些使用者可執行這個檔案庫內的程式。請使用指示來限制 HTTP 伺服器，讓它執行這個檔案庫內的 CGI 程式。

註: 如果您的伺服器提供多個邏輯網站，您可以針對每個站台的 CGI 程式來設置個別的檔案庫。

其它安全注意事項

以下是其它安全注意事項：

- HTTP 可提供對於您的 iSeries 系統的唯讀存取。HTTP 伺服器要求不能更新或刪除您系統中的資料。不過，您可能會有擁有更新資料的 CGI 程式。此外，您可啓用 Net.Data® 通用閘道介面程式來存取您的 iSeries 伺服器資料庫。系統使用 Script（類似跳出程式）來評估對 Net.Data 程式的要求。因此，系統管理者可控制 Net.Data 程式所採取的動作。
- HTTP 伺服器會提供一個存取日誌，您可以用它來監督經過伺服器的存取活動，包括進行中的和已完成的存取活動。

將 SSL 與 IBM HTTP Server for iSeries 搭配使用的安全注意事項

IBM HTTP Server for iSeries 可爲您的 iSeries 伺服器提供安全的 Web 連線。**安全網站**表示在用戶端和伺服器之間的傳輸 (兩個方向) 是經過加密處理的。這些加密過的傳輸，不會受到循跡追蹤者的偵查，試圖擷取或改變傳輸內容的使用者也無法著力。

註: 請記住，安全網站只適用於用戶端和伺服器之間的資訊傳輸安全。其用意並非爲了降低駭客侵犯您系統的可能性。不過，對駭客透過循跡追蹤而輕易取得的資訊，它當然也會加以限制。

資訊中心裡的 SSL 和 Webserving (HTTP) 主題中有安裝、配置和管理加密處理的完整資訊。這些主題概述伺服器特性和使用伺服器的若干注意事項。

當安裝下列中的任何授權程式時，網際網路連線伺服器 便可以提供 HTTP 和 HTTPS 支援：

- 5722-NC1
- 5722-NCE

當安裝有這些選項時，產品稱爲 Internet Connection 安全伺服器。

IBM HTTP Server for iSeries (5722-DG1) 同時提供 HTTP 及 HTTPS 兩種支援。您必須安裝下列中的任何加密產品，來能使用 SSL：

- 5722-AC2
- 5722-AC3

以加密處理為基礎的安全程序有下列幾項需求：

- 傳送者和接收者 (伺服器和用戶端) 都必須「瞭解」加密的機制，並具有加密和解密的能力。HTTP 伺服器需要啓用 SSL 的用戶端。(通行的 Web 瀏覽器多半都啓用 SSL)。iSeries 加密授權程式可支援多種工業標準加密方法。當用戶端想要建立安全階段作業時，伺服器和用戶端會進行協商，找出兩者都能支援的最佳加密方法。
- 傳輸內容必須讓竊取者無法進行解密。因此，使用加密方法的兩方，各需擁有一份彼此才知道的加密/解密**私用鑰匙**。如果您希望擁有一個安全的*外部*網站，就應該使用獨立的認證中心 (CA)，建立並發行數位憑證給使用者與伺服器。認證權限即所謂信賴的一方。

加密程序可保護所傳輸之資訊的機密性。不過，對於敏感性資訊 (如財務資訊) 而言，除了機密性以外，您還需要整合性和確實性。換言之，用戶端和 (選用) 伺服器必須彼此相信 (透過獨立的參照) ，並且必須確定傳輸內容沒有被改變。認證權限（CA）所提供的數位簽署，可提供眞實性和完整性的保證。透過對於伺服器認證 (以及選用的用戶端的認證) 的數位簽署之驗證，SSL 通訊協定可提供這個確實性。

加密和解密的程序需要一些處理時間，會對傳輸的效能造成若干影響。因此，iSeries 伺服器會提供同時執行安全和不安全程式的能力。您可以使用不安全的 http 伺服器來提供不需要安全保護的文件，例如您的產品型錄。這些文件的 URL，開頭為 `http://`。您可以用 HTTP 伺服器來處理敏感性資訊，例如客戶輸入信用卡資訊的表格。此程式可提供 URL 以 `http://` 或 `https://` 為首的文件。

提示

基於網際網路上的禮貌，您應讓用戶端知道何時保障或不保障傳輸安全，尤其是當您的網站只針對某些文件使用安全伺服器時更應如此。

請記住，加密程序要求兩端都必須是安全用戶端和安全伺服器。安全瀏覽器 (HTTP 用戶端) 的使用已日漸普及。

LDAP 的安全注意事項

「輕裝備目錄存取通訊協定 (LDAP)」安全特性包括「Secure Sockets Layer (SSL)」、「存取控制清單」及 CRAM-MD5 密碼加密。在 V5R1 中，已新增 Kerberos 連線及安全性審核支援，以增強 LDAP 安全性。

這些主題的詳細資訊，請參閱「iSeries 資訊中心 --> 網路功能 -> TCP/IP -> 目錄服務 (LDAP)」。請參閱第 xii 頁的『先決條件與相關資訊』，以獲得存取「iSeries 資訊中心」的資訊。

LPD 的安全性注意事項

LPD (行式印表機常駐程式) 提供的功能，可將印表機輸出分散到您的系統上。系統不會執行 LPD 的任何登入處理。

防止 LPD 存取

如果您不要任何使用者透過 LPD 存取您的系統，您應該防止 LPD 伺服器執行。請執行下列作業：

__ 步驟 1. 如果要在啓動 TCP/IP 時，防止自動執行 LDP 伺服器工作，請鍵入下列字串：

```
CHGLPDA AUTOSTART(*NO)
```

註:

1. AUTOSTART(*YES) 是預設值。
2. 第 108 頁的『控制自動啓動的 TCP/IP 伺服器』提供控制自動啓動哪些 TCP/IP 伺服器的詳細資訊。

__ 步驟 2. 若要避免讓某人將使用者應用程式 (例如 Socket 應用程式)，與系統通常用來執行 LPD 的連接埠連結起來，請執行下列動作：

__ 步驟 a. 鍵入 `GO CFGTCP`，以顯示「配置 TCP/IP」功能表。

__ 步驟 b. 選取選項 4 (使用 TCP/IP 埠限制)。

__ 步驟 c. 在「使用 TCP/IP 埠限制」顯示畫面中，指定選項 1 (新增)。

__ 步驟 d. 對於較低的埠範圍，指定 `515`。

__ 步驟 e. 對於較高的埠範圍，指定 `*ONLY`。

註:

1. 埠限制在您下次啓動 TCP/IP 時生效。如果您設定埠限制時 TCP/IP 在作用中，您應該先結束 TCP/IP，再重新啓動。
2. RFC1700 提供通用埠號指定的相關資訊。

__ 步驟 f. 對於通訊協定，指定 `*TCP`。

__ 步驟 g. 請在使用者設定檔欄位中指定系統中受保護的使用者設定檔。(受保護的使用者設定檔是未擁有沿用權限之程式的使用者設定檔，且沒有其它使用者所知道的密碼。) 將埠限制於特定使用者後，您會自動排除所有其它使用者。

__ 步驟 h. 重複 *UDP 通訊協定的步驟 2c 到 2g。

控制 LPD 存取

如果您要讓 LPD 用戶端存取您的系統，您必須瞭解下登記全考量：

- 如果要防止使用者以無用的物件來淹沒您的系統，請務必設定輔助儲存體儲存區 (ASP) 的適當臨界值限制。您可以使用系統服務工具 (SST) 或專用服務工具 (DST) 來顯示和設定 ASP 的臨界值。*備份及回復*一書提供關於 ASP 臨界值的詳細資訊。
- 您可以使用輸出佇列的權限來限制哪些使用者可將排存檔傳送到您的系統。 沒有使用者 ID 的 LDP 使用者使用 QTMPLPD 使用者設定檔。您只能提供少量輸出佇列的存取權給這個使用者設定檔。

SNMP 的安全注意事項

iSeries 伺服器可在網路中當成一個簡易網路管理通訊協定 (SNMP) 代理程式。 SNMP 可提供用來管理網路環境中之閘道、路由器和主電腦的方法。SNMP 代理程式會收集系統的相關資訊，並執行遠端 SNMP 網路管理者所要求的功能。

防止 SNMP 存取

如果您不要任何使用者透過 SNMP 存取您的系統，您應該防止 SNMP伺服器執行。請執行下列作業：

__ 步驟 1. 如果要在啓動 TCP/IP 時，防止自動執行 SNMP 伺服器工作，請鍵入下列字串：

```
CHGSNMPA AUTOSTART(*NO)
```

註:

1. AUTOSTART(*YES) 是預設值。
2. 第 108 頁的『控制自動啓動的 TCP/IP 伺服器』提供控制自動啓動哪些 TCP/IP 伺服器的詳細資訊。

__ 步驟 2. 若要避免讓某人將使用者應用程式 (例如 Socket 應用程式)，與系統通常用來執行 SNMP 的連接埠連結起來，請執行下列動作：

__ 步驟 a. 鍵入 `GO CFGTCP`，以顯示「配置 TCP/IP」功能表。

__ 步驟 b. 選取選項 4 (使用 TCP/IP 埠限制)。

__ 步驟 c. 在「使用 TCP/IP 埠限制」顯示畫面中，指定選項 1 (新增)。

__ 步驟 d. 對於較低的埠範圍，指定 `161`。

__ 步驟 e. 對於較高的埠範圍，指定 `*ONLY`。

註:

1. 埠限制在您下次啓動 TCP/IP 時生效。如果您設定埠限制時 TCP/IP 在作用中，您應該先結束 TCP/IP，再重新啓動。
2. RFC1700 提供通用埠號指定的相關資訊。

__ 步驟 f. 對於通訊協定，指定 `*TCP`。

__ 步驟 g. 請在使用者設定檔欄位中指定系統中受保護的使用者設定檔。(受保護的使用者設定檔是未擁有沿用權限之程式的使用者設定檔，且沒有其它使用者所知道的密碼。) 將埠限制於特定使用者後，您會自動排除所有其它使用者。

__ 步驟 h. 重複 *UDP 通訊協定的步驟 2c 到 2g。

控制 SNMP 存取

如果您要讓 SNMP 管理程式存取您的系統，您必須瞭解下列的安全注意事項：

- 某些可透過 SNMP 來存取您的網路的使用者，可收集您的網路的相關資訊。您使用別名和網域名稱伺服器來隱藏的資訊，有意入侵的使用者將可以透過 SNMP 來加以存取。此外，入侵者也可能使用 SNMP 來改變您的網路配置，並瓦解您的通訊。
- SNMP 必須透過共用區名稱才能進行存取。在概念上，共用區名稱和密碼相近。共用區名稱並不進行加密處理。因此，它很容易成爲循跡追蹤的對象。使用「新增 SNMP 社區 (ADDCOMSNMP)」指令，將管理員網際網路位址 (INTNETADR) 參數，設爲一或多個特定的 IP 位址，而非 *ANY。您也可以將 ADDCOMSNMP 或 CHGCOMSNMP 指令的 OBJACC 參數設爲 *NONE，以防止共用區的管理者存取任何 MIB 物件。這只是要暫時執行以拒絕共用區內之成員的存取權，而不要移除共用區。

INETD 伺服器的安全注意事項

INETD 伺服器和大部份 TCP/IP 伺服器不同，它不爲伺服器提供單一服務。相反地，它提供管理者能夠自訂的各種雜項服務。因此，INETD 伺服器有時也稱爲「超級伺服器」。INETD 伺服器有下列內建服務：

- time

- daytime
- echo
- discard
- changed

這些服務可以支援 TCP 和 UDP。如果是 UDP，echo、 time、daytime 和 changed 等服務都會接收 UDP 封包，再將封包傳回給來源者。Echo 伺服器會回應它收到的封包，time 和 daytime 伺服器會產生特定格式的時間並將它傳回，changed 伺服器會產生可列印 ASCII 字元的封包並將它傳回。

這些 UDP 服務的本性，會使系統容易受到「拒絕服務」的攻擊。例如，假設您有兩套 iSeries 伺服器：SYSTEMA 和 SYSTEMB。心懷不軌的程式設計師會以 SYSTEMA 的來源位址和時間伺服器的 UDP 埠號碼來僞造 IP 標頭和 UDP 標頭。之後，它可以將該封包傳送到 SYSTEMB 的時間伺服器上，使它將時間傳回給 SYSTEMA，而這又會回應至 SYSTEMB，並繼續下去，藉此產生一個連續的迴路來耗用兩個系統的 CPU 資源和網路頻寬。

因此，您應該在您的 iSeries 系統上，將這類風險列入考量，只在安全網路上執行這類服務。INETD 伺服器的原始狀態是啓動 TCP/IP 時不自動啓動。您可以配置是否要在啓動 INETD 時啓動這些服務。依預設，TCP 和 UDP 時間伺服器都會在您啓動 INETD 伺服器時啓動。

INETD 伺服器有兩個配置檔：

```
/QIBM/UserData/OS400/inetd/inetd.conf
/QIBM/ProdData/OS400/inetd/inetd.conf
```

這些檔案會決定在啓動 INETD 伺服器時，啓動哪些程式。他們也會判斷在 INETD 啓動這些程式時，要在哪一個使用者設定檔之下執行。

註: 在 proddata 中的配置檔絕對不能修改。每當重新載入系統時，都會置換這個檔案。如果在版次升級期間**未**更新這個檔案，則客戶的配置變更只應該放在 userdata 目錄樹的檔案中。

如果心懷不軌的程式設計師能夠存取這些檔案，他可能會將它們配置成在啓動 INETD 時，啓動任何程式。因此，這些檔案的保護便顯得格外重要。依預設，它們需要有 QSECOFR 權限才能進行變更。您不應該降低存取它們時所需要權限。

註: 不修改 ProdData 目錄中的配置檔。每重新載入系統時，都會置換這個檔案。如果在版次更新期間未更新這個檔案，則客戶的配置變更只應該放在 UserData 目錄樹的檔案中。

限制 TCP/IP 漫遊的安全注意事項

如果您的系統和網路相連，您可以限制使用者透過 TCP/IP 應用程式來漫遊於網路之中的功能。要達到這個目的，方法之一，是限制對於下列 TCP/IP 指令的存取：

註: 這些指令可能會存在於系統內的多個檔案庫中。至少在 QSYS 和 QTCP 檔案庫中，會有這些指令。請務必找出每一個指令，並加以保護。

- STRTCPFTP
- FTP
- STRTCPTELN

- TELNET
- LPR
- SNDTCPSPLF
- RUNRMTCMD (REXEC 用戶端)

使用者的可能目標取決於下列各個項目：

- 在 TCP/IP 主電腦表中的登錄。
- 在 TCP/IP 遞送表中的 *DFTROUTE 登錄。當使用者的目標是不明的網路時，這可讓使用者輸入下個中繼點系統的 IP 位址。使用者可透過這個預設路徑來通往或聯絡遠端的網路。
- 遠端名稱伺服器配置。這個支援可讓網路中的另一個伺服器尋找使用者的主電腦名稱。
- 遠端系統表格。

您必須控制哪些使用者可新增登錄到這些表格中，以及變更您的配置。您也必須瞭解表格登錄和配置的隱藏內涵。

請您務必瞭解，可存取 ILE C 編譯器的內行使用者能夠建立一個可連接到 TCP 或 UDP 埠的 socket 程式。您可以限制對於 QSYSINC 檔案庫中之下列 socket 介面檔的存取，來使這個意圖便得更為困難。

- SYS
- NETINET
- H
- ARPA
- socket 與 SSL

在服務程式方面，您可以藉由限制下列服務程式的使用，來限制 socket 與 SSL 應用程式 (已經過編譯) 的使用。

- QSOSRV1
- QSOSRV2
- QSOSKIT(SSL)
- QSOSSLSR(SSL)

服務程式在出貨時具備公用權限 *USE，但您可將此權限變更為 *EXCLUDE (或其它值)。

第 14 章 保護工作站存取的安全

在您的系統使用者中，有許多人都備有個人電腦 (PC)，用來作爲他們的工作站。他們使用的工具在 PC 中執行，他們也使用 PC 來連接 iSeries 伺服器。

將 PC 連接到 iSeries 伺服器的大部份方法，都能提供超過工作站模擬所能提供的功能。此 PC 像是 iSeries 的顯示器，可提供給使用者交談式的登入階段作業。此外，對 iSeries 伺服器而言，此 PC 也好像是另一部電腦，可提供類似檔案轉送和遠端程序呼叫等功能。

作爲一個 iSeries 伺服器安全管理者，您必須知道下列事項：

- 連接於系統的 PC 使用者所能使用的功能
- PC 使用者所能存取的 iSeries 伺服器資源

如果您尚未針對這些功能準備好您的 iSeries 伺服器安全架構，您可以不執行進階 PC 功能 (例如檔案轉送和遠端程序呼叫)。也許您的遠端目標是要在保護系統資訊的同時，容許執行進階 PC 功能。下列主題說明與 PC 存取相關的若干安全論題。

防止工作站病毒

本資訊將建議安全管理者防堵 PC 病毒的方法。

保護工作站資料存取的安全

有些 PC 用戶端軟體使用共用資料夾來儲存伺服器上的資訊。如果要存取 iSeries 資料庫檔案，PC 使用者必須擁有一組有限且定義良好的介面。透過多數用戶端/伺服器軟體的檔案轉送功能，PC 使用者可以在伺服器和 PC 之間複製檔案。透過資料庫存取功能，例如 DDM 檔、遠端 SQL，或 ODBC 驅動程式，PC 使用者可以存取伺服器中的資料。

在這個環境中，您可以建立程式來攔截和評估 PC 使用者存取伺服器資源的要求。當要求使用 DDM檔時，您在分送式資料管理存取 (DDMACC) 網路屬性中指定跳出程式。對於某些 PC 檔案轉送方法，您使用「用戶端要求存取 (PCSACC)」網路屬性來指定跳出程式。您也可以指定 PCSACC(*REGFAC) 來使用登記功能。當要求使用其它伺服器功能來存取資料時，您可以使用 WRKREGINF 指令來登記這些伺服器功能的跳出程式。

不過，跳出程式可能很難設計，它們很難落實。跳出程式無法作爲物件權限的取代方案，物件權限的設計是要保護您的物件，讓它免受任何來源的未獲授權的存取。

有些用戶端軟體，例如 IBM iSeries Access for Windows，使用整合檔案系統來儲存和存取 iSeries 伺服器中的資料。透過整合檔案系統，PC 使用者能很容易地使用伺服器。物件權限會變得更爲重要。透過整合檔案系統，具有足夠權限的使用者可以將伺服器檔案庫當作一個 PC 目錄來檢視。簡單的移動和複製指令，可立即將資料從 iSeries 伺服器檔案庫移到 PC 目錄中，反之亦然。系統會自動變更資料格式。

註:

1. 您可以使用授權清單來控制 QSYS.LIB 檔案系統中之物件的使用。請參閱第 88 頁的『限制存取 QSYS.LIB 檔案系統』，取得詳細資訊。

2. 第 83 頁的第 11 章, 『使用 整合檔案系統 來保護檔案』提供關於整合檔案系統之安全主題的詳細資訊。

整合檔案系統的力量在於它的簡單性，不論對使用者或軟體開發者都一樣。透過單一介面，使用者可使用多個環境內的物件。PC 使用者不需要特殊軟體或 API 即可存取物件。相反地，PC 使用者可以使用熟悉的 PC 指令或 『點按』 功能來直接使用物件。

對於所有連接 PC 的系統而言，尤其是對於有用戶端軟體使用整合檔案系統的系統而言，好的物件權限架構非常重要。由於安全機制整合到 OS/400 產品中，因此，任何存取資料的要求都會經過權限檢查程序。權限檢查適用於任何來源的要求，也適用於使用任何方法的資料存取。

具有工作站存取的物件權限

當您設置物件權限時，您需要評估該權限提供給 PC 使用者的內容爲何。例如，當使用者擁有檔案的 *USE 權限時，使用者即可以檢視或列印檔案中的資料。使用者不能變更檔案中的資訊，或刪除檔案。對於 PC 使用者而言，檢視和『讀取』沒有不同，它們都會提供足夠的權限，讓使用者在 PC上建立檔案副本。但這可能不是您想要的。

對於某些重要檔案，您可能必須將公用權限設定爲 *EXCLUDE，來防止使用者下載它們。之後，您可以提供另一個方法，讓使用者在伺服器中『檢視』檔案，例如使用採用權限的功能表和程式。

另一個防止下載的選項，是使用 PC 使用者啓動伺服器 (交談式登入以外的功能) 功能時所執行的跳出程式。您可以使用「變更網路屬性 (CHGNETA)」指令，在 PCSACC 網路屬性中指定一個跳出程式。您也可以使用「使用系統登記資訊 (WRKREGINF)」指令來登記跳出程式。至於所用的方法，視 PC 如何存取您系統中的資料以及 PC 使用哪個用戶端程式而定。跳出程式 (QIBM_QPWFS_FILE_SERV) 適用於 iSeries Access 以及 Net Server 存取 IFS。此無法防止採用其它機制 (像是 FTP 或 ODBC) 從 PC 存取。

通常，PC 軟體也會提供上載的功能，因此使用者可以將 PC 的資料複製到伺服器資料庫檔案。如果您尚未正確設置您的權限架構，PC 使用者可能會以 PC 中的資料來覆蓋掉檔案中的所有資料。請謹慎指定 *CHANGE 權限。請詳閱 *iSeries Security Reference* 一書中的「附錄 D」，以瞭解檔案作業所需要的權限。

iSeries 資訊中心 提供關於 PC 功能的權限和跳出程式之使用的詳細資訊。詳細請參閱第 xii 頁的『先決條件與相關資訊』。

應用程式管理

「應用程式管理」是「iSeries 領航員」(iSeries 伺服器的圖形式使用者介面 (GUI)) 的一項選用性安裝元件。「應用程式管理」可讓系統管理者在特定的伺服器上，控制使用者和群組可以使用的功能或應用程式。這包括控制經由用戶端存取其伺服器的使用者可以使用的功能。值得注意的是，如果您從 Windows 用戶端存取伺服器，則 iSeries 伺服器使用者而非 Windows 使用者決定可供管理的功能。

如需「iSeries 領航員應用程式管理」的完整文件，請參照 iSeries 資訊中心 -> 連線到 iSeries --> 連接方式 --> iSeries 領航員 (../html/as400/v5r2/ic2924/info/rzaj3/rzaj3overview.htm)。

原則管理

原則是管理者在用戶端 PC 上配置軟體時可使用的工具。原則可以在 PC 上限制使用者可以存取的功能和應用程式爲何。原則也可以建議或命令由某些使用者或某些 PC 使用的配置。

註: 「原則」未提供伺服器資源的控制。原則不是伺服器安全性的取代。原則可用來影響 iSeries Access 自特定的 PC 由特定的使用者存取伺服器的方法。然而，它們不會變更透過其它機制存取伺服器資源的方法。

原則是儲存在檔案伺服器上。每當使用者登入其 Windows 工作站時，便從檔案伺服器下載套用至 Windows 使用者的原則。原則會先套用到登錄，而後使用者才能在工作站上執行動作。

Microsoft® 原則對應用程式管理

iSeries Access Express 支援兩種不同的策略，以便於在網路內部實施管理控制：Microsoft 系統原則與「iSeries 領航員應用程式管理」。在判斷何種策略最適合您的需求時，請考慮下列項目。

Microsoft 系統原則

原則由 PC 驅動，而非依據特定的 OS/400 版次。原則可套用到 PC 和 Windows 使用者。這表示使用者參照 Windows 使用者設定檔，而非伺服器使用者設定檔。原則也可以用來「配置」以及限制。一般而言，原則比「應用程式管理」更詳細因而更能提供保證，且提供更大範圍的功能。這是因爲到伺服器連線不需判定使用者是否可使用功能。實施原則比實施「應用程式管理」更爲複雜，因爲必須使用 Microsoft 系統原則編輯器，且 PC 必須個別配置以下載原則。

iSeries 領航員應用程式管理

「應用程式管理」關聯的使用者設定檔的資料，而非 Microsoft 系統原則關聯 Windows 設定檔。雖然需要 V4R3 或更新版 OS/400 產品的 iSeries 伺服器才能使用「應用程式管理」，但有些功能只能在 V4R4 或更新版本使用。「應用程式管理」使用「iSeries 領航員」的圖形式使用者介面來管理，使用起來比原則編輯器簡單。「應用程式管理資訊」可套用到使用者，而無論其從何種 PC 登入。您可以限制「iSeries 領航員」內的特殊功能。如果您要限制的所有功能都是啓用「應用程式管理」的，而且如果使用的 OS/400 版本支援「應用程式管理」的話，您就可以考慮使用「應用程式管理」。

搭配使用 SSL 和 iSeries Access for Windows

如需將 iSeries Access Express 和 SSL 搭配使用的相關資訊，請參考 iSeries 資訊中心主題 *Secure Sockets Layer 管理*、*保護 iSeries Access Express 以及「iSeries 領航員」的安全*、*iSeries Developer Kit for Java 以及 Java 主題下的 iSeries Java 工具箱*。您也可在系統所提供的 CD 上查閱此資訊。

iSeries 領航員 安全性

「iSeries 領航員」爲使用 iSeries Access 的使用者提供了一種很容易使用的伺服器介面。隨著每個 OS/400 新版次的推出，使用者可透過「iSeries 領航員」來使用的伺服器功能將會愈來愈多。這種易於使用的介面可提供許多好處，包括降低技術支援成本，改善系統給人的印象。它也可以提供許多安全上的盤查。

作爲一個安全管理者，您不再能依賴使用者的無知來保護您的資源。「iSeries 領航員」讓許多功能暴露在使用者的面前，並且垂手可得。您必須確定您已針對您的安全需求，設計並實作了適用於使用者設定檔和物件安全的安全原則。

IBM e(logo)server iSeries Access for Windows V4R4 與更新的版本提供了下列方法，可用來控制使用者透過「iSeries 領航員」來執行的功能：

- 選擇性安裝
- 應用程式管理
- Windows NT® 系統原則支援

「iSeries 領航員」被套裝成多個元件，您可以個別安裝它們。因此，您可以只安裝您要的功能。「應用程式管理」可讓管理者控制使用者或群組能夠透過「iSeries 領航員」來存取的功能。「應用程式管理」將應用程式組織成下列各種類：

iSeries 領航員
包括「iSeries Navigator 領航員」和任何插入項。

用戶端應用程式
包括所有其它的用戶端應用程式，其中的 iSeries Access 提供用戶端上透過「應用程式管理」所管理的功能。

主應用程式
包括完全常駐於您的伺服器的所有應用程式，並提供透過「應用程式管理」來管理的功能。

您可以使用選擇性安裝、「應用程式管理」和原則來限制使用者所能存取的「iSeries 領航員」功能。不過，它們都不適用於資源安全。

從 V4R4 開始，IBM e(logo)server iSeries Access for Windows 也支援使用 Windows NT 的「系統原則編輯器」來控制特定 PC 用戶端所能支援的功能, 而不論是誰在使用這個 PC。

請參閱 iSeries 資訊中心以取得選擇性安裝、「應用程式管理」和「原則管理」的詳細資訊。本書的第 5 頁的『限制程式功能』一節也有應用程式管理的相關討論。

防止 ODBC 存取

「開放資料庫連接 (ODBC)」是一個工具，PC 應用程式可用它來存取 iSeries 資料，如同存取 PC 中的資料一般。ODBC 程式設計師可讓資料的實際位置，針對 PC 應用程式的使用者而成爲透明的。關於 ODBC 安全注意事項的詳細資訊，請到「iSeries Access for Windows ODBC security」資訊 (/rzaii/rzaiiodbc09.HTM)，其位於「iSeries 資訊中心」內。

工作站階段作業密碼的安全注意事項

一般而言，當 PC 使用者啓動連接軟體 (例如 iSeries Access) 時，使用者會對伺服鍵入一次使用者ID 和密碼。密碼會被加密，並儲存到 PC 記憶體中。每當使用者對同一個伺服器建立新的階段作業時，PC即會自動傳送使用者 ID 和密碼。

有些用戶端/伺服器的軟體所提供的選項，也可以讓您略過交談式階段作業的「登入」顯示畫面。當使用者啓動交談式 (5250 模擬) 階段作業時，軟體會傳送使用者 ID 和加密的密碼。如果要支援這個選項，伺服器的 QRMTSIGN 系統值必須設定爲 *VERIFY。

當您選取容許略過「登入」顯示畫面時，您必須考慮到安全上的代價。

安全漏洞：對於 5250 模擬或任何其它類型的交談式階段作業而言，「登入」顯示畫面和任何其它顯示畫面相同。雖然鍵入密碼時，不會出現在螢幕中，但如同任何其它資料欄位一樣，密碼會透過鏈接，以未加密的形式來傳送。對於某些鏈接類型而言，這會讓潛在的入侵者取得監督鏈接的機會，並偵測到使用者 ID和密碼。使用電子設備來監督鏈接，通常也稱為**循跡追蹤**。從 V4R4 開始，您可以使用 Secure Sockets Layer (SSL)，將 iSeries Access 和 iSeries 伺服器之間的通訊加密。這可以保護您的資料和密碼，免於受到循跡追蹤的侵擾。

當您選擇略過「登入」顯示畫面選項時，在傳送之前 PC 會加密密碼。加密程序可降低使用者利用循跡追蹤來竊取密碼的可能。不過，您必須確定您的 PC 使用者執行可作業的安全程序。如果無人的 PC 與 iSeries 系統之間有作用中的階段作業，則其它使用者有可能在不需要知道使用者 ID 和密碼的情況下，啓動另一個階段作業。當系統長期不作用時，應該將 PC設置為鎖定，這些 PC 需要有密碼才能回復階段作業。

即使您未選擇略過「登入」顯示畫面，擁有作用階段作業的無人 PC 仍然是一個安全上的漏洞。使用者可以透過 PC 軟體來啓動伺服器階段作業並存取資料，同樣不需要知道使用者 ID 和密碼。5250 模擬的漏洞則又大些，因為使用者啓動階段作業和開始存取資料時，所需要的知識更少。

您也必須教育使用者，讓他們知道切斷 iSeries Access 階段作業連線的影響。許多使用者假設 (合邏輯，但不正確) 切斷選項會完全停止他們與伺服器的連接。事實上，當使用者選取切斷選項時，伺服器會將使用者的階段作業 (使用權限) 轉給另一個使用者。然而，用戶端與伺服器的連接仍在開啓狀態中。另一個使用者可以進入未受保護的 PC 並存取伺服器資源，而不需要輸入使用者 ID 和密碼。

對於需要切斷其階段作業的使用者，您可以提供兩個建議給他們：

- 務必讓他們的 PC 擁有需要密碼的鎖定功能。這可讓不知道密碼使用者無法使用無人的 PC。
- 若要完全切斷階段作業，請登出 Windows 或重新啓動 PC。這可以結束與 iSeries 的階段作業。

您也必須教導使用者，讓他們知道使用 iSeries Access for Windows 時可能有的潛在安全風險。當使用者指定 UNC (通用命名慣例) 來識別某個 iSeries 資源時，Win95 或 NT 用戶端會建立一個網路連接來鏈接伺服器。由於使用者指定 UNC，因此，使用者不會看到它成為對映的「網路驅動器」。通常，使用者甚至不會知道網路連接的存在。不過，在無人的 PC 上，這個網路連接代表一個安全上的漏洞，因為伺服器會出現在 PC 的目錄樹之中。如果使用者的階段作業擁有有力的使用者設定檔，則這個無人的 PC 可能會將伺服器資源暴露出來。針對前面的例子，補救之道，在於讓使用者了解風險，請他們務必使用 PC 鎖定功能。

保護伺服器不受遠端指令及程序影響

如果內行的 PC 使用者擁有 iSeries Access 這類的軟體，他不需要透過「登入」顯示畫面，便可以在伺服器中執行指令。下列是可供 PC 使用者執行伺服器指令的各種方法。您的用戶端/伺服器軟體會判斷您的 PC 使用者所能使用的方法。

- 使用者可開啓一個 DDM 檔案，並使用遠端指令來執行指令。

- 某些軟體，例如 iSeries Access 最佳化用戶端，可透過「分散式程式呼叫 (DPC) API」來提供遠端指令功能，而不需要使用 DDM。
- 某些軟體，例如遠端 SQL 和 ODBC，不需要透過 DDM 或 DPC，即可提供遠端指令功能。

對於使用 DDM 來提供遠端指令支援的用戶端/伺服器軟體而言，您可以用 DDMACC 網路屬性來徹底禁絕遠端指令。對於使用其它伺服器支援的用戶端/伺服器軟體而言，您可以登記伺服器的跳出程式。如果您要讓使用者執行遠端指令，您必須確定您的物件權限架構足以保護您的資料。使用遠端指令功能時，使用者等於擁有了指令行。此外，當 iSeries 透過 DDM 接收到遠端指令時，系統不會執行使用者設定檔「有限的功能 (LMTCPB)」設定。

保護工作站不受遠端指令及程序影響

IBM iSeries Access for Windows 提供在 PC 接收遠端指令的功能。您可以在伺服器中使用「執行遠端指令 (RUNRMTCMD)」指令，而在連接的 PC 上執行程序。RUNRMTCMD 功能是一項有力工具，可提供給系統管理者和解說站的人員使用。不過，它也提供了使用者有意或無意地毀損 PC 資料的機會。

PC 和 iSeries 伺服器並沒有相同的物件權限功能。針對 RUNRMTCMD 指令的問題，您的最佳保護方針，是小心限制擁有指令存取權的系統使用者。IBM iSeries Access for Windows 提供的功能，可讓您登記哪些使用者可在特定 PC 中執行遠端指令。當連接是透過 TCP/IP 之時，您可以使用用戶端的性質控制畫面來控制遠端指令的存取。您可以透過使用者 ID 或遠端系統名稱來授權使用者。當連接是透過 SNA 時，某些用戶端軟體的功能，可讓您針對交談來設置安全程序。當使用其它用戶端軟體時，您只需要選擇是否要設置進入指令功能。

對於每個用戶端軟體和連接類型的組合 (例如 TCP/IP 或 SNA) 而言，您需要檢查所連接之 PC 的每個進入指令的潛在可能。您可以搜尋『進入指令』或『RUNRMTCMD』來檢閱用戶端文件。請準備好向您的 PC 使用者和網路管理者建議配置用戶端以容許或禁止這個功能的正確 (安全) 方法。

閘道伺服器

您的系統可以透過在 iSeries 系統和 PC 之間的中間伺服器或閘道伺服器來參與網路。例如，您的 iSeries 系統可能會連接於有 PC 伺服器的 LAN，且該伺服器也連接於若干 PC。這個情況下的安全問題，決定於閘道伺服器中所執行之軟體的功能。第 137 頁的圖 13 顯示閘道伺服器配置的範例：

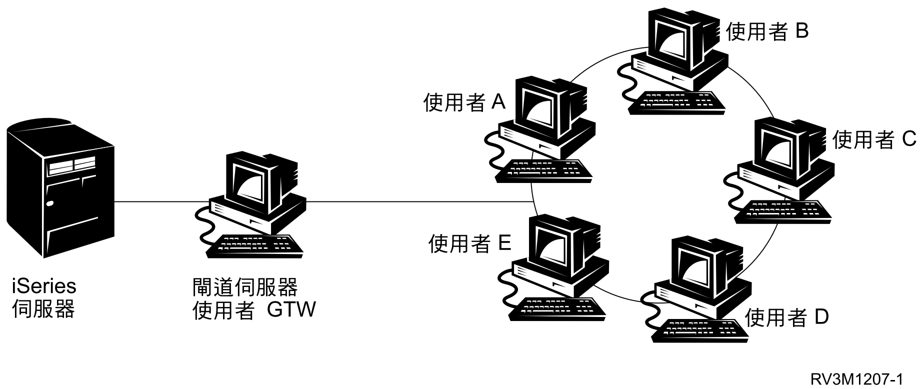

圖 13. 使用閘道伺服器的 iSeries 系統

在使用某些軟體時，您的 iSeries 系統不會知道閘道伺服器的下游有哪些使用者 (例如「使用者 A」或「使用者 C」)。伺服器會以單一使用者 (USERGTW) 來登入系統。它會使用「使用者 GTW」使用者 ID 來處理下游使用者的所有要求。對伺服器而言，USERA 的要求有如使用者 USERGTW 所發出的要求。

如果是這個情況，您必須透過閘道伺服器來執行安全維護作業。您必須瞭解和管理閘道伺服器的安全功能。從 iSeries 伺服器的角度來看，每個使用者都和閘道伺服器用來啓動階段作業的使用者 ID 擁有相同的權限。您可以將它等同於在沿用權限並提供指令行的程式中作業。

在使用其它軟體時，閘道伺服器會將個別使用者的要求傳送到 iSeries 伺服器。iSeries 伺服器會知道 USERA 正在要求對於特定物件的存取權。對於系統而言，閘道幾乎是透通的。

如果您的系統所在的網路有閘道伺服器，您必須評估要提供多少權限給閘道伺服器所使用的使用者 ID。您也必須瞭解下列事項：
- 閘道伺服器所執行的安全機制。
- 對於您的 iSeries 系統，將會出現多少下游使用者。

無線 LAN 通訊

有些用戶端可能以「iSeries 無線 LAN」來與您的系統進行無線式通訊。「iSeries 無線 LAN」使用射頻通訊技術。作爲一個安全管理者，您應該知道「iSeries 無線 LAN」產品的下登記全特性：
- 這些無線 LAN 產品使用分頻技術。政府從前也使用這個技術來保護無線電發射的安全。對於想要以電子方式來監督資料傳輸的使用者而言，這些傳輸猶如噪音一般，而不像是實際的傳輸。
- 無線連接有三個安全相關配置參數：
  - 資料速率 (兩個可能的資料速率)
  - 頻率 (五個可能的頻率)
  - 系統 ID (8 百萬個可能的 ID)

  這些配置元素的組合，可提供八千萬個可能的配置，面對這個情況，駭客猜對配置的可能極爲渺茫。

- 和使用其它通訊方法一樣，無線通訊的安全狀況也會受到用戶端裝置之安全狀況的影響。系統 ID 資訊和其它配置參數都在用戶端裝置的某個檔案中，並且應該受到保護。
- 如果無線裝置遺失或被偷，當未獲授權的使用者試圖使用遺失或偷來的裝置來存取您的系統時，一般的伺服器安全措施，例如登入密碼和物件安全，都可以提供保護。
- 如果無線用戶端裝置遺失或被偷，您應該考慮變更所有使用者、存取點和系統的系統 ID 資訊。您可以將這個情況想像成遺失整串的鑰匙並變更門板上的鎖頭。
- 您可以將伺服器分割成各自擁有唯一系統 ID 的用戶端群組。當某個裝置遺失或被偷時，這會讓影響受到限制。只有在您可以將某群使用者限制於安裝作業的特定部份之內時，才可以使用這個方法。
- 和有線的 LAN 技術不同，無線的 LAN 技術具有專利。因此，對這些無線 LAN 產品而言，不會有公共的電子循跡追蹤者。循跡追蹤者是一個電子裝置，會對傳輸作業進行未獲授權的監督。

第 15 章 安全跳出程式

有些 iSeries 伺服器功能可提供跳出程式，讓您的系統能夠執行使用者建立的程式，來執行其它檢查和驗證。例如，您可以設置您的系統，讓它在每次有人試圖開啓系統中的 DDM 時執行跳出程式。您可以使用系統登記功能來指定在特定狀況下執行的跳出程式。

許多 iSeries 出版品中都有執行安全功能的跳出程式範例。表 24 提供一份列示，其中有這些跳出程式的範例，以及程式範例的來源。

表 24. 跳出程式樣本來源

跳出程式的類型	目的	範例來源
密碼驗證	QPWDVLDPGM 系統值可指定一個程式名稱，或指出 QIBM_QSY_VLD_PASSWRD 跳出程式的登錄驗證程式，來針對 QPWDxxx 系統值所不處理的其餘基本要求檢查新密碼。您使用這個程式時，應該小心地監督，因爲它會接收未加密的密碼。這個程式**不應該**將密碼儲存在檔案中，或將它們傳送到另一個程式。	• *An Implementation Guide for iSeries Security and Auditing，GG24-4200* • *iSeries Security Reference*, SC41-5302-07
PC Support/400 或 Client Access 存取[1]	您可以在網路屬性的「用戶端要求存取 (PCSACC)」參數中指定這個程式名稱來控制下列功能： • 虛擬印表機功能 • 檔案轉送功能 • 共用資料夾「類型 2」功能 • 用戶端存取訊息功能 • 資料佇列 • 遠端 SQL 功能	*An Implementation Guide for iSeries Security and Auditing，GG24-4200*
「分送式資料管理 (DDM)」存取	您可以在網路屬性的「DDM 要求存取 (DDMACC)」參數中指定這個程式名稱來控制下列功能： • 共用資料夾「類型 0」和「類型 1」功能 • 「提出遠端指令」功能	*An Implementation Guide for iSeries Security and Auditing，GG24-4200*
遠端登入	您可以在 QRMTSIGN 系統中指定參數來控制哪些使用者可自動從該位置登入 (透通)。	*An Implementation Guide for iSeries Security and Auditing，GG24-4200*
iSeries Access[1] 的「開放式資料庫連接 (ODBC)」	控制下列 ODBC 功能： • 是否容許執行 ODBC。 • 容許對 iSeries 資料庫檔案執行哪些功能。 • 容許使用哪些 SQL 陳述式。 • 可擷取資料庫伺服器物件的哪些相關資訊。 • 容許執行哪些 SQL 型錄功能。	無可用項目。
QSYSMSG 岔斷處理程式	您可以建立一個程式來監督 QSYSMSG 訊息佇列，並根據訊息類型來採取適當的動作 (例如通知安全管理者)。	*An Implementation Guide for iSeries Security and Auditing，GG24-4200*

表 24. 跳出程式樣本來源 (繼續)

跳出程式的類型	**目的**	**範例來源**
TCP/IP	許多 TCP/IP 伺服器 (例如 FTP、TFTP、TELNET 和 REXEC) 都可提供跳出程式。您可以新增跳出程式來處理登入並驗證使用者要求，例如，取出或放入特定檔案的要求。您也可以使用這些跳出程式，在您的系統中提供匿名的 FTP。	『TCP/IP 使用者跳出程式』於 *iSeries System API Reference* 一書中
使用者設定檔變更	您可以針對下列使用者設定檔指令來建立跳出程式： CHGUSRPRF CRTUSRPRF DLTUSRPRF RSTUSRPRF	• *iSeries Security Reference*, SC41-5302-07 • 『TCP/IP 使用者跳出程式』於 *iSeries System API Reference* 一書中

註:

1. 可在 iSeries「資訊中心」找到本主題的其餘資訊。請參閱第 xii 頁的『先決條件與相關資訊』，取得詳細資訊。

第 16 章 網際網路瀏覽器的安全注意事項

您組織中的許多 PC 使用者在他們的工作站中擁有工作站。他們可能會連接到網際網路。他們也可能會連接到您的伺服器。以下是 PC 和您的伺服器的若干安全注意事項。

風險：工作站損壞

您的使用者所前往的網頁，可能是一個相關的「程式」，如 Java Applet、Active-X 控制項，或其它類型的外掛程式。雖然並不多見，但在 PC 上執行這類型的「程式」時，有可能損壞 PC 中的資訊。作為一個安全主管，請考慮使用下列方式來保護您企業組織中的 PC：

- 瞭解您的使用者所擁有的各種瀏覽器的安全選項。例如，對某些瀏覽器而言，您可以控制 Java Applet 在瀏覽器外所擁有的存取 (Java 限制的作業環境稱為 *Sandbox*)。這可避免讓 Applet 損壞了 PC 中的資料。

  註: 對 Active-X 和其它登入而言，並不存在此沙箱概念和其相關的安全限制。
- 建議您的使用者使用某些瀏覽器設定值。也許您沒有足夠的時間或資源，可確定使用者是否遵循您的建議。因此，您必須教育他們，讓他們知道不當的設定具有潛在的風險。
- 考慮標準化所使用的瀏覽器，讓他們能夠擁有您需要的安全選項。
- 指示您的使用者，當出現與特定網站有關的任何可疑行為或症狀時，務必要通知您。

風險：透過對映磁碟機來存取 iSeries 目錄

假設一台 PC 以 IBM iSeries Access for Windows 階段作業連接到您的伺服器。階段作業會設定對映的驅動器來鏈接 iSeries 整合檔案系統。例如，PC 的 **G** 磁碟機對映到網路中 SYSTEM1 伺服器的整合檔案系統。

現在，假設同一個 PC 使用者擁有瀏覽器，可存取網際網路。這個使用者要求某個網頁，而該網頁在執行具危險性的「程式」，例如 Java Applet 或 Active-X 控制。您可以想像，程式可能會嘗試清除 PC G 磁碟機中的所有內容。

有關對映的磁碟機所可能受到的損害，您可以有幾個保護的方法：

- 您最重要的保護對象，是伺服器中的資源安全。對伺服器而言，Java Applet 或 Active-X 控制和建立 PC 階段作業的使用者一樣。您必須小心管理哪些 PC 使用者可取得伺服器的權限。
- 請建議您的 PC 存取使用者，讓他們將瀏覽器設定為無法存取對映的磁碟機。這適用於 Java Applet，但不適用於不具 Sandbox 概念的 Active-X 控制。
- 請教育您的使用者，讓他們知道在同一個階段作業中，同時連接於伺服器和網際網路所可能具有的危險。此外，您的 PC 使用者 (如 Windows 95 用戶端) 也必須知道，即使表面上已經結束 iSeries Access 階段作業，但磁碟機的對映關係仍然存在。

風險：信任已簽章 Applet

您的使用者可能已遵循您的建議，並設置他們的瀏覽器來防止 Applet 寫入任何 PC 驅動器。不過，您的 PC 使用者也必須知道，*已簽章 Applet* 可改寫他們的瀏覽器設定。

已簽章 Applet 擁有相關的數位簽名，用以建立它的身份驗明。當使用者存取的 Web 頁中有已簽章 Applet 時，使用者會看到一則訊息。訊息中會有這個 Applet 的簽章說明 (簽章人和簽章時間)。當您的使用者接受這個 Applet 時，使用者即會授權給這個 Applet ，容許它置換瀏覽器的安全設定。即使瀏覽器的預設值不容許，已簽章 Applet 仍然可以寫入 PC 的區域磁碟機中。這個已簽章 Applet 也可以寫入位於伺服器的對應磁碟機，因爲對 PC 而言，這些磁碟機和區域磁碟機沒有不同。

對於來自您伺服器中的 Java Applet，您可能需要使用已簽章 Applet。不過，一般而言，您應該指示您的使用者，不要接受來路不明的已簽章 Applet。

第 17 章 相關資訊

手冊

- *APPC Programming*, SC41-5443-00 說明 iSeries 系統的進階程式間通訊 (APPC) 支援。本書引導您開發使用 APPC 的應用程式，並定義 APPC 通訊的通訊環境。其中包括應用程式的注意事項、配置需求和指令、APPC 的問題管理，以及一般性的網路注意事項。請參閱 iSeries 資訊中心 CD-ROM。
- *AS/400 網際網路安全性：保護您的 AS/400 使其免於來自網際網路上的危害* 紅皮書，SG24-4929 討論安全性議題，以及將 iSeries 連接至網際網路的相關風險。書中提供 TCP/IP 應用程式的範例、建議事項、要訣和技術。
- *備份及回復*, SC40-0814-07 提供關於規劃備份及回復策略、從您的系統保存資訊、以及回復您系統的資訊。請參閱 iSeries 資訊中心。也可在 iSeries 資訊中心中找到這些主題的相關資訊。請參閱第 xii 頁的『先決條件與相關資訊』，取得詳細資訊。
- *CL Programming*, SC41-5721-06，提供對於可外部說明之檔案進行資料說明規格 (DDS) 編碼的詳細說明。這些檔案是實體、邏輯、顯示、列印和交互系統通訊功能 (ICF) 檔。請參閱 iSeries 資訊中心。
- 在「資訊中心」(詳細資訊請參閱第 xii 頁的『先決條件與相關資訊』) 的 CL 主題提供所有 iSeries 控制語言 (CL) 及其 OS/400 指令的說明。OS/400 指令是用來要求 Operating System/400® (5722-SS1) 授權程式的功能。與其它授權程式相關的所有非 OS/400 CL 指令，包括各種語言及公用程式在內，都會在支援這些授權程式的書籍中說明。
- *Implementing iSeriesSecurity，第三版，作者爲* Wayne Madden 與 Carol Woodbury。Loveland, Colorado: 29th Street Press, a division of Duke Communications International, 1998. 提供規劃、設置和管理 iSeries 安全的準則和實際建議事項。

  ISBN 訂購號碼：

  1-882419-78-2
- 關於 HTTP 伺服器的詳細資訊，請參閱下列 URL：

  `http://www.ibm.com/eserver/iseries/software/http/docs/doc.htm`
- *iSeries Security Reference*, SC41-5302-07，提供關於安全系統值、使用者設定檔、資源安全性和安全審核的完整資訊。這個手冊不說明特定授權程式、語言和公用程式的安全性。請參閱 iSeries 資訊中心。
- 在「資訊中心」的「基本系統作業」主題，提供部份主要概念以及 iSeries 基本操作所需作業的資訊。請參閱第 xii 頁的『先決條件與相關資訊』，取得詳細資訊。
- 「資訊中心」說明如何使用及配置 TCP/IP，以及其它 TCP/IP 應用程式，如 FTP、SMTP 及 TELNET。請參閱第 xii 頁的『先決條件與相關資訊』，取得詳細資訊。
- *OS/400 的 TCP/IP 檔案伺服器支援 Installation and User's Guide*, SC41-0125，提供檔案伺服器支援授權程式服務項目的簡介資訊、安裝指示和設定程序。它說明產品所能使用的功能，包括與其它系統合用的範例和提示。
- *Trusted Computer Systems Evaluation Criteria* DoD 5200.28.STD，說明電腦系統可信層次的基準。TCSEC 是美國政府的出版品。您可以向下列單位取得副本：

Office of Standards and Products
National Computer Security Center
Fort Meade, Maryland 20755-6000 USA
Attention: Chief, Computer Security Standards

- 「資訊中心」包含 iSeries 上關於「系統管理」及「工作管理」的各種不同主題。這些主題中包含效能資料集合、系統值管理及儲存體管理。存取「資訊中心」的詳細資訊，請參閱第 xii 頁的『先決條件與相關資訊』。「工作管理」SC41-5306-03 提供關於如何建立及變更工作管理環境的資訊。請參閱 iSeries 資訊中心。

除了「資訊中心」主題及「補充手冊」外，您也可以從下列資源中獲得協助：

- **IBM SecureWay**
  IBM SecureWay 為 IBM 的各類安全性產品提供一種共同的品牌，這些產品包括硬體、軟體、諮詢及服務，協助客戶保障其資訊技術安全。不論是解決個別客戶的需求，或建立整體企業解決方案，IBM SecureWay 產品為企業提供規劃、設計、應用及操作安全解決方案時所需要的專業。如需 IBM SecureWay 產品的相關資訊，請造訪 IBM SecureWay 首頁：

  `http://www.ibm.com/secureway`

- **服務產品**
  安裝新的硬體或軟體可以大大地提升您的效率及公司作業。但它也會造成公司混亂及停頓的威脅，並且也會對您珍貴的內部資源造成龐大的負擔。IBM Global Services 提供與 iSeries 安全性相關的服務。下列網站可讓您搜尋 iSeries 服務的完整清單：

  `http://www.as.ibm.com/asus`

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 不見得有提供本資訊中所提的各項產品、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。本書在提及 IBM 的產品、程式或服務時，不表示或暗示只能使用 IBM 的產品、程式或服務。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。

在這本書或文件中可能包含著 IBM 所擁有之專利或專利申請案。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 LicensingIBM Corporation
| 500 Columbus Avenue
| Thornwood, NY 10594-1785
| U.S.A.

若要查詢有關二位元組 (DBCS) 資訊的特許權限事宜，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 CorporationLicensing
| 2-31 Roppongi 3-chome, Minato-ku
| Tokyo 106, Japan

下列段落若與當地之法令抵觸，則不適用之： IBM 僅以「現狀」提供本出版品，而不爲任何明示或默示之保證 (包括但不限於產品未涉侵權、可售性或符合特定效用的保證。) 倘若干地區在特定交易中並不許可相關明示或默示保證之棄權聲明，則於該等地區之特定交易，此項聲明不適用之。

本資訊中可能包含技術上或排版印刷上的錯誤。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) 變動本書中所提及的產品及 (或) 程式。

本資訊中任何對非 IBM 網站的敘述僅供參考，IBM 對該等網站並不提供保證。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。

| 當您提供資訊給 IBM 時，您即授權予 IBM 以其認爲適當的方式來使用或分送資訊，
| 而不必對您負起任何責任。

本程式之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 Corporation
| Software Interoperability Coordinator, Department 49XA
| 3605 Highway 52 N

Rochester, MN 55901
U.S.A.

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」或任何同等合約之條款，提供本資訊中所說的授權程式與其所有適用的授權資料。

此間所含之任何效能資料，皆是得自控制的環境之下；因此不同作業環境之下所得的結果，可能會有很大的差異。部份測量可能是在開發中的系統上執行，因此不保證可以從一般的系統獲致相同的結果。甚至有部份的測量，是利用插補法而得的估計值，其實際結果可能會有所不同。本書的使用者應根據其特有的環境，驗證出適用的資料。

本書所提及之非 IBM 產品資訊，係一由產品的供應商，或其出版的聲明或其他公開管道取得。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。

本資訊僅供規劃用途。所提及的產品發行之前，本書內含的資訊有變動的可能。

本資訊包含日常商業活動所用的資料及報告範例。為了提供完整的說明，這些範例包括個人、公司、廠牌和產品的名稱。這些名稱全屬虛構，若與任何公司的名稱和住址雷同，純屬巧合。

著作權授權：

本書包含原始語言的範例應用程式，用以說明各種作業平台上的程式設計技術。您可以基於研發、使用、銷售或散佈符合作業平台 (用於執行所撰寫的範例程式) 之應用程式設計介面的應用程式等目的，以任何形式複製、修改及散佈這些範例程式，而無需付費給 IBM。但這些範例皆未經過完整的測試。因此，IBM 不擔保或默示保證這些程式的可靠性、可用性或功能。您可以基於研發、使用、銷售或散佈符合 IBM 應用程式設計介面的應用程式等目的，以任何形式複製、修改及散佈這些範例程式，而無需付費給 IBM。

若您檢視本資訊的電子檔，圖片及彩色圖例可能不會顯示。

商標

下列術語是 IBM 公司在美國及 (或) 其它國家的商標。

Advanced Peer-to-Peer Networking
APPN
AS/400
DB2
DRDA
e (logo)
IBM

iSeries
Net.Data
Operating System/400
OS/400
PowerPC
SecureWay
System/36
System/38
400

| ActionMedia、LANDesk、MMX、Pentium 及 ProShare 是 Intel Corporation 在美國及
| (或) 其它國家的商標或註冊商標。

Microsoft、Windows、Windows NT 以及 Windows 標誌是 Microsoft Corporation 在美國及 (或) 其它國家的商標。

Java 以及所有與 Java 有關的商標是 Sun Microsystems, Inc. 在美國及 (或) 其它國家的商標。

UNIX 是 The Open Group 在美國及 (或) 其它國家的商標。

其他公司、產品及服務名稱，可能是第三者的商標或服務標誌。

索引

索引順序以中文字，英文字，及特殊符號之次序排列。

〔一劃〕

一般檔案轉送通訊協定 (TFTP)
  安全要訣 116
  限制埠 116

〔三劃〕

下載
  必要的權限 132
上載
  必要的權限 132
大的使用者設定檔 44
子系統說明
  列印安全相關參數 29
  安全相關值 74
  安全要訣
    工作佇列登錄 75
    工作站名稱登錄 75
    工作站類型登錄 75
    自動啓動工作登錄 75
    通訊登錄 76
    預先啓動工作登錄 76
    遠端位置名稱登錄 76
    遞送登錄 76
  通訊登錄
    預設使用者 97
    模式 97
  監督安全相關值 74
  遞送登錄
    除去 PGMEVOKE 登錄 99
工作佇列
  列印安全相關參數 30
  監督存取 53
工作佇列登錄
  安全要訣 75
工作站名稱登錄
  安全要訣 75
工作站類型登錄
  安全要訣 75
工作排程器
  評估程式 70
工作說明
  列印安全相關參數 29
  列印使用者設定檔的 54
  安全要訣 76
工作，APPC
  指定使用者設定檔 96
已中斷的工作逾時間隔 (QDSCJOBITV) 系統值
  建議設定 19
  CFGSYSSEC 指令所設定的值 32
已簽章 Applet，信任 142

〔四劃〕

不作用的工作逾時間隔 (QINACTITV) 系統值
  建議設定 19
  CFGSYSSEC 指令所設定的值 32
中間節點遞送 101
內容
  安全工具 26
公用權限
  列印 30
  使用 RVKPUBAUT 指令取消 34
  取消 31
  監督 49
公共使用者
  定義 49
公開的密碼
  變更 18
分析
  使用者設定檔 44
    依據使用者類別 29
    依據特殊權限 29
  物件權限 45
  程式失效 46
分析設定檔活動 (ANZPRFACT) 指令
  建立免除使用者 26
  建議使用 21
  說明 26
分析預設密碼 (ANZDFTPWD) 指令
  建議使用 23
  說明 26
分送程式呼叫 API 135
分割區，邏輯 57
分隔頁
  跳出程式 68
切斷計時器參數 102
日誌接收器，審核
  儲存體臨界值 47

〔五劃〕

以物件爲基礎的系統
  防止電腦病毒的侵襲 63
以物件爲基礎的系統 *(繼續)*
  潛在安全問題 39
出版品
  相關 143
加密
  密碼
    PC 階段作業 134
加強整合性保護
  安全層次 (QSECURITY) 50 3
功能表
  安全工具 26
功能表存取控制
  以物件權限來補充 40
  功能表存取限制 40
  使用者設定檔參數 39
  說明 39
  轉移環境 40
功能表安全
  以物件權限來補充 40
  功能表存取限制 40
  使用者設定檔參數 39
  說明 39
  轉移環境 40
功能，審核安全性 43
可使用指令
  使用者報表 44
可疑的程式，偵測 63
未完整定義的呼叫 71
用戶端系統
  定義 93
用戶端要求存取 (PCSACC) 網路屬性
  使用跳出程式 68
  限制 PC 資料存取 131
  跳出程式樣本來源 139
目標系統
  定義 93
目錄，保護 89

〔六劃〕

列印
  公用授權物件 30
  列印安全相關工作佇列參數 30
  列印安全相關輸出佇列參數 30
  安全相關子系統說明值 29
  安全相關通訊設定 29
  系統安全屬性 7
  系統值 29
  沿用物件資訊 29
  非 IBM 物件的列示 29
  授權清單資訊 29, 50

列印 *(繼續)*
網路屬性 29
審核異動記載登錄 29
觸發程式 29
列印子系統說明 (PRTSBSDAUT) 指令
建議使用 97
說明 29
列印工作說明權限 (PRTJOBDAUT) 指令
建議使用 77
說明 29
列印公用授權物件 (PRTPUBAUT) 指令 87
建議使用方式 94
說明 30
列印公用授權物件 (PRTPUBAUT) 指令，列印 87
列印佇列權限 (PRTQAUT) 指令
說明 30
列印系統安全屬性 (PRTSYSSECA) 指令
建議使用 13
說明 29
範例輸出 7
列印使用者物件 (PRTUSROBJ) 指令
建議使用 71
說明 29
列印使用者設定檔 (PRTUSRPRF) 指令
不符的範例 54
特殊權限範例 54
密碼資訊 21, 23
說明 29
環境資訊範例 55
列印沿用物件 (PRTADPOBJ) 指令
說明 29
列印專用權限 (PRTPVTAUT) 指令
建議使用 94
授權清單 29, 50
說明 30
列印專用權限物件 (PRTPVTAUT) 指令 87
列印通訊安全 (PRTCMNSEC) 指令
說明 29
範例 99, 103
列印觸發程式 (PRTTRGPGM) 指令
說明 29
印表常駐程式 (LDP)
安全要訣 125
防止自動啓動伺服器 126
限制埠 126
說明 125
印表機裝置說明
分隔頁跳出程式 68
回復
審核日誌損壞 47
回轉作業
跳出程式 68
存取
控制 39
存取 QSYS.LIB 檔案系統，限制 88
安全工具
內容 26
功能表 26
指令 26
安全位置 (SECURELOC) 參數 100
圖解 94
說明 96
*VFYENCPWD (驗證加密密碼) 值 96, 100
安全和 iSeries 領航員 133
安全性工具程式
保護安全 25
保護輸出 25
指令權限 25
儲存 25
檔案 25
檔案衝突 25
安全性功能，審核 43
安全性屬性
列印 7
安全性，LP 57
安全性，實體 73
安全的基本元素 3
安全值
設定 31
安全值，架構
使用 SECURELOC (安全位置) 參數 96
說明 95
應用程式範例 95
安全連結 94
安全跳出程式，使用 139
安全精靈 9
安全網站 124
安全審核
使用建議
物件審核 105
概觀 79
CP (變更設定檔) 異動記載登錄 21, 22
SV (系統值) 異動記載登錄 71
*PGMADP 審核層次 65
*PGMFAIL 值 64
*SAVRST 值 64
*SECURITY 值 64
設定 27
復置作業 71
簡介 6, 43
顯示 27
安全審核異動記載
列印登錄 29
安全層次 10
物件權限 39
安全層次 10 *(繼續)*
移轉來源 39
安全層次 20
物件權限 39
移轉來源 39
安全層次 (QSECURITY) 系統值
說明 3
CFGSYSSEC 指令所設定的值 32
安全，整合檔案系統方式 83
自行設定
安全值 31
自動回答 (AUTOANS) 欄位 103
自動建立控制器 (AUTOCRTCTL) 參數 102
自動配置 (QAUTOCFG) 系統值
建議設定 19
CFGSYSSEC 指令所設定的值 32
自動控制啓動的 TCP/IP 伺服器 108
自動清除
跳出程式 68
自動虛擬裝置配置 (QAUTOVRT) 系統值
建議設定 19
CFGSYSSEC 指令所設定的值 32
自動撥號 (AUTODIAL) 欄位 103

〔七劃〕

位置密碼
APPN 95
位置密碼 (LOCPWD) 參數 94
伺服器
定義 93
作用設定檔列示
變更 26
作業主控台
加密法 59
使用 59
使用者設定檔 59
使用者鑑別 60
服務工具使用者設定檔 59
直接連通性 60
設定精靈 61
裝置鑑別 60
資料完整性 60
資料專用性 60
遠端主控台 59
LAN 連接 60
完整
審核 (QAUDJRN) 日誌接收器 47
岔斷要求程式
列印使用者設定檔的 54
跳出程式 68
序列介面線路通訊協定 (SLIP)
保護撥入的安全 110
保護撥出安全 111
控制 109

序列介面線路通訊協定 (SLIP) *(繼續)*
說明 109
系統用來傳送使用者相關資訊的方法 95
系統值
列印與安全相關 7, 29
安全
設定 31
保留伺服器安全資料 (QRETSVRSEC)
說明 23
設定指令 31
登入
建議 19
簡介 4
CHGSYSLIBL (系統檔案庫列示)
保護 71
QALWOBJRST (容許物件復置)
建議使用 70
CFGSYSSEC 指令所設定的值 32
QAUDCTL (審核控制)
變更 27
顯示 27
QAUDLVL (審核層次)
變更 27
顯示 27
QAUTOCFG (自動配置)
建議設定 19
CFGSYSSEC 指令所設定的值 32
QAUTOVRT (自動虛擬裝置配置)
建議設定 19
CFGSYSSEC 指令所設定的值 32
QDEVRCYACN (裝置復原動作)
建議設定 19
預防安全漏洞 98
CFGSYSSEC 指令所設定的值 32
QDSCJOBITV (已中斷的工作逾時間隔)
建議設定 19
CFGSYSSEC 指令所設定的值 32
QDSPSGNINF (顯示登入資訊)
建議設定 19
CFGSYSSEC 指令所設定的值 32
QINACTITV (不作用的工作逾時間隔)
建議設定 19
CFGSYSSEC 指令所設定的值 32
QINACTMSGQ (非作用中工作訊息佇列)
建議設定 19
CFGSYSSEC 指令所設定的值 32
QLMTSECOFR (限制安全主管)
建議設定 19
CFGSYSSEC 指令所設定的值 32
QMAXSGNACN (達到登入嘗試次數時的動作)
CFGSYSSEC 指令所設定的值 32
QMAXSIGN (最大登入嘗試次數)
建議設定 19
CFGSYSSEC 指令所設定的值 32
系統值 *(繼續)*
QPWDEXPITV (密碼到期間隔)
建議設定 13
CFGSYSSEC 指令所設定的值 32
QPWDLMTAJC (密碼限制相鄰字元)
建議設定 13
CFGSYSSEC 指令所設定的值 32
QPWDLMTCHR (密碼限制字元)
建議設定 13
CFGSYSSEC 指令所設定的值 32
QPWDLMTREP (密碼限制重複字元)
建議設定 13
CFGSYSSEC 指令所設定的值 32
QPWDLMTREP (密碼需要位置差異)
建議設定 13
CFGSYSSEC 指令所設定的值 32
QPWDLVL (密碼層次)
建議設定 13
QPWDMAXLEN (密碼最大長度)
建議設定 13
CFGSYSSEC 指令所設定的值 32
QPWDMINLEN (密碼最小長度)
建議設定 13
CFGSYSSEC 指令所設定的值 32
QPWDRQDDGT (密碼需要數值字元)
建議設定 13
CFGSYSSEC 指令所設定的值 32
QPWDRQDDIF (密碼的必要差異)
建議設定 13
CFGSYSSEC 指令所設定的值 32
QPWDVLDPGM (密碼驗證程式)
使用跳出程式 68
建議設定 13
跳出程式樣本來源 139
CFGSYSSEC 指令所設定的值 32
QRETSVRSEC (保留伺服器安全資料)
用於 SLIP 撥出 111
QRMTSIGN (容許遠端登入)
使用跳出程式 68
跳出程式樣本來源 139
CFGSYSSEC 指令所設定的值 32
*FRCSIGNON 值的影響 95
QSECURITY (安全層次)
說明 3
CFGSYSSEC 指令所設定的值 32
QUSEADPAUT (使用沿用權限) 66
系統訊息 (QSYSMSG) 訊息佇列
建議使用 79
跳出程式樣本來源 139
系統配置 (*IOSYSCFG) 特殊權限
APPC 配置指令的需要 95
系統檔案庫列示 (QSYSLIBL) 系統值
保護 71
系統變更日誌管理支援 47
系統，QFileSvr.400 檔案 90
系統，限制存取 QSYS.LIB 檔案 88
系統，根 (/)、 QOpenSys 以及使用者定義檔案的安全 86
系統，網路檔案 90
防止
TCP/IP 登錄 105
防止與偵測駭客入侵 73
防止撥入使用者存取其它系統 111

〔八劃〕

使用 API 來建立目錄 89
使用 open() 或 creat() API 來建立串流檔 90
使用 PC 介面來建立物件 90
使用子系統說明 (WRKSBSD) 指令 75
使用系統登記資訊 (WRKREGINF) 指令
跳出程式 69
使用沿用權限 (QUSEADPAUT) 系統值 66
使用沿用權限 (USEADPAUT) 參數 65
使用者
APPC 工作 95
使用者物件
在受保護的檔案庫內 71
使用者設定檔
大的，找出 44
不符的特殊權限和使用者類別 54
分析
依據使用者類別 29
依據特殊權限 29
以查詢分析 44
功能表存取控制 39
永久作用列示
變更 26
列印
特殊權限 53
環境 55
請參閱 報表
自動除去 22
防止被停用 21
指定給 APPC 工作 96
除去不作用 21
停用
自動 21
停用的 (*DISABLED) 狀態 22
排定到期日 22
排定停用 20
排定啓動 20
處理不作用 21
報表
可使用指令的使用者 44
具有特殊權限的使用者 44
非作用中 44
選定的 44
預設密碼 22
監督 73

使用者設定檔 *(繼續)*
監督使用者類別 54
監督特殊權限 53
監督環境設定 54
審核
授權使用者 44
檢查預設密碼 26
簡介 4
顯示到期日進度表 22
使用者環境
監督 54
使用者類別
分析指定 29
與特殊權限不符 54
使用者，系統用來傳送相關資訊的方法 95
來源
安全跳出程式 139
來源系統
定義 93
具有 LAN 連接的作業主控台
使用 61
設定精靈
服務工具裝置設定檔 61
服務工具裝置設定檔密碼 61
變更密碼 61
到期日
使用者設定檔
設定進度表 22, 26
顯示排程 26
取消
公用權限 31
取消公用權限 (RVKPUBAUT) 指令
明細 34
建議使用 75
說明 31
受保護的檔案庫
檢查使用者物件 71
所有權，物件 42
服務工具
使用者設定檔 (服務工具) 55
服務工具伺服器 (STS)
邏輯分割區 57
服務工具使用者設定檔
服務工具使用者設定檔 (DST) 55
DST 管理 55
服務工具裝置設定檔
保護 61
密碼 61
預設密碼 61
屬性
主控台 61
變更密碼 61
注意事項 145
沿用的權限
列印物件列示 29
限制 65
沿用的權限 *(繼續)*
監督使用情況 64
沿用權限的程式
限制 65
監督使用情況 64
物件
列印
沿用的權限 29
非 IBM 29
權限來源 29
改變
檢查 45
管理新物件的權限 49
權限來源
列印列示 50
物件所有權 42
物件整合性
審核 45
物件簽章
簡介 74
物件權限
工作佇列 53
公用 49
分析 45
安全性工具程式 指令 25
安全層次 10 或 20 39
沿用的 64
限制 65
監督 64
特殊 53
國家語言 43
開始 40
新物件 49
概觀 39
當執行時 39
補充功能表存取控制 40
對於復置指令的存取 70
對於儲存指令的存取 70
監督 49, 52
管理 49
輸出佇列 53
檔案庫安全 42
簡介 5
轉移環境 40
顯示 45
PC 使用者的資料存取 132
*SAVSYS (儲存系統) 特殊權限 70
控制 70
物件，新的安全 89
非作用中
使用者
報表 44
非作用中工作訊息佇列 (QINACTMSGQ) 系統值
建議設定 19
CFGSYSSEC 指令所設定的值 32
信任已簽章 Applet 142
「保留伺服器安全性資料 (QRETSVRSEC)」系統值
用於 SLIP 撥出 111
說明 23
保護
防止電腦病毒 63
TCP/IP 埠應用程式 107
保護 APPC 通訊 93
保護目錄安全 89
保護安全
安全性工具程式 25
TCP/IP 通訊 105

〔九劃〕

建立目錄指令 89
建立產品載入 (CRTPRDLOD) 指令
跳出程式 68
建議
密碼系統值 13
登入系統值 19
指令
取消公用權限 31
指令，CL
安全工具 26
啓動排程 26
傳送日誌登錄 (SNDJRNE) 46
檢查物件整合性 (CHKOBJITG)
說明 45
顯示使用者設定檔 (DSPUSRPRF)
使用輸出檔 44
顯示物件說明 (DSPOBJD)
使用輸出檔 44
顯示物件權限 (DSPOBJAUT) 45
顯示授權使用者 (DSPAUTUSR)
審核 44
顯示採用程式 (DSPPGMADP)
審核 46
顯示檔案庫 (DSPLIB) 45
ADDPFRCOL (新增效能集合)
跳出程式 68
ANZDFTPWD (分析預設密碼)
建議使用 23
說明 26
ANZPRFACT (分析設定檔活動)
建立免除使用者 26
建議使用 21
說明 26
CFGSYSSEC (配置系統安全)
建議使用 13
說明 31
CHGACTPRFL (變更作用設定檔列示)
建議使用 21
說明 26

指令，CL *(繼續)*
CHGACTSCDE (變更啓動進度表登錄)
建議使用 20
說明 26
CHGBCKUP (變更備份)
跳出程式 68
CHGEXPSCDE (變更到期日進度表登錄)
建議使用 22
說明 26
CHGMSGD (變更訊息說明)
跳出程式 68
CHGPFRCOL (變更效能集合)
跳出程式 68
CHGSECAUD (變更安全審核)
建議使用 79
說明 27
CHGSYSLIBL (變更系統檔案庫情單)
限制存取 71
CHKOBJITG (檢查物件整合性)
建議使用 64
說明 29, 45
CRTPRDLOD (建立產品載入)
跳出程式 68
DSPACTPRFL (顯示作用設定檔列示)
說明 26
DSPACTSCD (顯示作用排程)
說明 26
DSPAUDJRNE (顯示審核異動記載登錄)
建議使用 79
說明 29
DSPAUTUSR (顯示授權使用者)
審核 44
DSPEXPSCD (顯示到期日進度表)
建議使用 22
說明 26
DSPLIB (顯示檔案庫) 45
DSPOBJAUT (顯示物件權限) 45
DSPOBJD (顯示物件說明)
使用輸出檔 44
DSPPGMADP (顯示採用程式)
審核 46
DSPSECAUD (顯示安全審核)
說明 27
DSPUSRPRF (顯示使用者設定檔)
使用輸出檔 44
ENDPFRMON (結束效能監督程式)
跳出程式 68
PRTADPOBJ (列印沿用物件)
說明 29
PRTCMNSEC (列印通訊安全)
說明 29
範例 99, 103
PRTJOBDAUT (列印工作說明權限)
建議使用 77
指令，CL *(繼續)*
PRTJOBDAUT (列印工作說明權限) *(繼續)*
說明 29
PRTPUBAUT (列印公用授權物件)
建議使用 94
說明 29
PRTPVTAUT (列印專用權限)
建議使用 94
授權清單 29, 50
說明 30
PRTQAUT (列印佇列權限)
說明 30
PRTSBSDAUT (列印子系統說明)
建議使用方式 97
說明 29
PRTSYSSECA (列印系統安全屬性)
建議使用 13
說明 29
範例輸出 7
PRTTRGPGM (列印觸發程式)
說明 29
PRTUSROBJ (列印使用者物件)
建議使用 71
說明 29
PRTUSRPRF (列印使用者設定檔)
不符的範例 54
特殊權限範例 54
密碼資訊 21, 23
說明 29
環境資訊範例 55
RCVJRNE (接收異動記載登錄)
跳出程式 68
RUNRMTCMD (執行遠端指令)
限制 136
RVKPUBAUT (取消公用權限)
明細 34
建議使用 75
說明 31
SBMRMTCMD (提出遠端指令)
限制 98
SETATNPGM (設定岔斷要求程式)
跳出程式 68
SNDJRNE (傳送日誌登錄) 46
STREML3270 (啓動 3270 顯示器模擬)
跳出程式 68
STRPFRMON (啓動效能監督)
跳出程式 68
STRTCP (啓動 TCP/IP)
限制 105
TRCJOB (追蹤工作)
跳出程式 68
WRKREGINF (使用系統登記資訊)
跳出程式 69
WRKSBSD (使用子系統說明) 75
指令，iSeries 400 建立目錄 89
指令，列印公用授權物件 (PRTPUBAUT) 87
指令，列印專用權限物件 (PRTPVTAUT) 87
指定
APPC 工作的使用者設定檔 96
架構安全值
使用 SECURELOC (安全位置) 參數 96
說明 95
應用程式範例 95
架構的異動程式名稱
IBM 所提供者的列示 78
相關出版品 143
限制
功能
使用者報表 44
沿用的 65
請參閱 控制
限制 APPC 階段作業 94
限制存取 QSYS.LIB 檔案系統 88
限制安全主管 (QLMTSECOFR) 系統值
建議設定 19
CFGSYSSEC 指令所設定的值 32

〔十劃〕

個人電腦
請參閱 PC (個人電腦)
容許物件復置 (QALWOBJRST) 系統值
建議使用 70
CFGSYSSEC 指令所設定的值 32
容許遠端登入 (QRMTSIGN) 系統值
使用跳出程式 68
跳出程式樣本來源 139
CFGSYSSEC 指令所設定的值 32
*FRCSIGNON 值的影響 95
挾帶 101
效能集合
跳出程式 68
根 (/)、QOpenSys 以及使用者定義檔案系統的安全 86
根 (/)、QOpenSys 和使用者定義檔案系統 84
根目錄的公用權限 86
根目錄，公用權限 86
特洛依木馬
說明 67
檢查 68
繼承沿用的權限 66
特殊權限
分析指定 29
使用者報表 44
監督 53
與使用者類別不符 54

特殊權限 *(繼續)*
*SAVSYS (儲存系統)
控制 70
病毒
防止 63
定義 63
偵測 45
掃描 45, 64
iSeries 伺服器保護機制 64
病毒掃瞄程式 64
記錄格式選項程式 (FMTSLR) 參數 68
訊息
跳出程式 68
CPF1107 20
CPF1120 20
訊息佇列 (MSGQ) 參數 54
起始功能表 (INLMNU) 參數 54
起始程式 (INLPGM) 參數 54
追蹤工作 (TRCJOB) 指令
跳出程式 68
配置系統安全 (CFGSYSSEC) 指令
建議使用 13
說明 31
配置檔，TCP/IP
限制存取 107
除去
不作用的使用者設定檔 21
使用者設定檔
自動 22, 26
PGMEVOKE 遞送登錄 99

〔十一劃〕

停用
使用者設定檔 20
自動 21, 26
影響 22
偵測可疑的程式 63
動作，審核 46
動態的主電腦配置通訊協定 (DHCP)
安全要訣 114
限制埠 115
區域系統
定義 93
參考書目 143
國家語言支援
物件權限 43
執行遠端指令 (RUNRMTCMD) 指令
限制 136
密碼
加密
PC 階段作業 134
必要差異 (QPWDRQDDIF) 系統值
建議設定 13
CFGSYSSEC 指令所設定的值 32
密碼 *(繼續)*
到期間隔 (QPWDEXPITV) 系統值
建議設定 13
CFGSYSSEC 指令所設定的值 32
限制字元 (QPWDLMTCHR) 系統值
建議設定 13
CFGSYSSEC 指令所設定的值 32
限制相鄰字元 (QPWDLMTAJC) 系統值
建議設定 13
CFGSYSSEC 指令所設定的值 32
限制重複字元 (QPWDLMTREP) 系統值
建議設定 13
CFGSYSSEC 指令所設定的值 32
設定規則 13
最大長度 (QPWDMAXLEN) 系統值
建議設定 13
CFGSYSSEC 指令所設定的值 32
最小長度 (QPWDMINLEN) 系統值
建議設定 13
CFGSYSSEC 指令所設定的值 32
單向加密 23
預設 22
監督活動 23
需要位置差異 (QPWDPOSDIF) 系統值
建議設定 13
CFGSYSSEC 指令所設定的值 32
需要數值字元 (QPWDRQDDGT) 系統值
建議設定 13
CFGSYSSEC 指令所設定的值 32
儲存 23
檢查預設 26
變更 18
變更 IBM 所提供的 18
驗證程式 (QPWDVLDPGM) 系統值
建議設定 13
CFGSYSSEC 指令所設定的值 32
QPGMR (程式設計師) 使用者設定檔 33
QSRV (服務) 使用者設定檔 33
QSRVBAS (基本服務) 使用者設定檔 33
QSYSOPR (系統操作員) 使用者設定檔 33
QUSER (使用者) 使用者設定檔 33
密碼必要差異 (QPWDRQDDIF) 系統值
CFGSYSSEC 指令所設定的值 32
密碼層次
規劃 14
設定 14
簡介 14
變更 14, 15, 16, 17, 18
密碼驗證程式 (QPWDVLDPGM) 系統值
使用跳出程式 68
跳出程式樣本來源 139
專用服務工具 (DST)
密碼 19
專用權限
監督 52
專用權限物件 (PRTPVTAUT) 指令，列印 87
強迫
建立程式 64
強迫建立 (FRCCRT) 參數 64
控制
子系統說明 74
存取
資訊 39
對於復置指令 70
對於儲存指令 70
來自 PC 的資料存取 131
沿用的權限 64, 65
密碼 13
排定的程式 70
復置功能 70
登入 13
結構異動程式名稱 77
開放式資料庫連接 (ODBC) 134
跳出程式 68
管理者網際網路位址 (INTNETADR) 參數 127
遠端指令 98, 135
儲存功能 70
檔案庫列示變更 71
觸發程式 67
APPC 階段作業 94
APPC 裝置說明 94
PC (個人電腦) 131
System/36 檔案轉送 43
TCP/IP
配置檔 107
登錄 105
跳出 128
*SAVSYS (儲存系統) 特殊權限 70
控制自動啓動的 TCP/IP 伺服器 108
控制撥入 SLIP 連線 109
控制器說明
列印安全相關參數 29
控制點階段作業 (CPSSN) 參數 102
接收異動記載登錄
跳出程式 68
接收異動記載登錄 (RCVJRNE)
跳出程式 68
掃描
物件改變 45
授權清單
列印權限資訊 29, 50
控制使用沿用權限 66
監督 50
採用程式
顯示 46

排定
使用者設定檔
到期日 22, 26
停用 20
啓動 20, 26
啓用
使用者設定檔
自動 26
啓動
使用者設定檔 20, 26
透通工作 97
啓動 3270 顯示器模擬 (STREML3270) 指令
跳出程式 68
啓動 TCP/IP (STRTCP) 指令
限制 105
啓動效能監督 (STRPFRMON) 指令
跳出程式 68
啓動程式通訊協定 (BOOTP)
安全要訣 113
限制埠 113
清除，自動
跳出程式 68
現行檔案庫 (CURLIB) 參數 54
略過登入
潛在安全問題 135
異動記載登錄
接收
跳出程式 68
傳送 46
CP (變更設定檔)
建議使用 21, 22
規定
請參閱 控制
規劃密碼層次變更
遞減密碼層次 17, 18
遞增密碼層次 15
變更密碼層次
規劃層次變更 14, 15
變更密碼層次 (0 到 1) 15
變更密碼層次 (0 到 2) 15
變更密碼層次 (1 到 0) 18
變更密碼層次 (1 到 2) 15
變更密碼層次 (2 到 0) 17
變更密碼層次 (2 到 1) 17
變更密碼層次 (2 到 3) 16
變更密碼層次 (3 到 0) 17
變更密碼層次 (3 到 1) 17
變更密碼層次 (3 到 2) 17
QPWDLVL 變更 14, 15
設定
安全值 31
安全審核 27
系統值 31
網路屬性 31
設定岔斷要求程式 (SETATNPGM) 指令
跳出程式 68
設定檔
以查詢分析 44
使用者 44
大的，找出 44
可使用指令的使用者報表 44
非作用中報表 44
特殊權限使用者報表 44
選定的報表 44
設定檔，使用者
請參閱 使用者設定檔
設定檔，群組
請參閱 群組設定檔
通訊協定 (SNMP)， 簡易網路管理 126
通訊登錄
安全要訣 76
預設使用者 97
模式 97
通訊，APPC 基本元素 93
通訊，保護 APPC 93
通訊, APPC
請參閱 APPC (高級程式對程式通訊’)
通訊,，TCP/IP
請參閱 TCP/IP 通信
連線， 控制撥入 SLIP 109
透通工作
啓動 97
透過對映磁碟機存取 iSeries 400 目錄 141
透過對映磁碟機到 iSeries 400 目錄，存取 141

〔十二劃〕

備份列示
跳出程式 68
最大值
大小
審核 (QAUDJRN) 日誌接收器 47
最大登入嘗試次數 (QMAXSIGN) 系統值
建議設定 19
CFGSYSSEC 指令所設定的值 32
單一階段作業 (SNGSSN) 參數 101
單向加密 23
報表
所有檔案庫 45
選定的使用者設定檔 44
檔案庫內容 45
復置功能
控制 70
監督 64
復置指令
限制存取 70
循跡追蹤 135
提出
安全報表 28
提出遠端指令 (SBMRMTCMD) 指令
限制 98
無線通訊 137
登入
控制 13
略過 135
設定系統值 19
監督嘗試 23
「登入」顯示畫面
變更錯誤訊息 20
登入安全
定義 3
登記的跳出程式
評估 69
程式
強迫建立 64
採用權限功能
審核 46
排定的
評估 70
隱藏
檢查 68
請參閱 觸發程式
程式失效
審核 46
程式沿用 (*PGMADP) 審核層次 65
程式驗證值 64
程式，使用安全跳出 139
結束效能監督程式 (ENDPFRMON) 指令
跳出程式 68
結構異動程式名稱
安全要訣 77
評估
排定的程式 70
登記的跳出程式 69
進階的程式間通訊 (APPC)
請參閱 APPC (高級程式對程式通訊)
開放式資料庫連接 (ODBC)
控制存取 134
跳出程式樣本來源 139
階段作業， APPC 的基礎 94

〔十三劃〕

傳送
異動記載登錄 46
傳送日誌登錄 (SNDJRNE) 指令 46
搭配使用 SSL 和 iSeries Access Express 133
新物件
管理權限 49
新物件的安全 89
新物件，安全 89

新增效能集合 (ADDPFRCOL) 指令
跳出程式 68
群組設定檔
簡介 4
裝置復原動作 (QDEVRCYACN) 系統值
建議設定 19
預防安全漏洞 98
CFGSYSSEC 指令所設定的值 32
裝置說明
列印安全相關參數 29
裝置說明，APPC
請參閱 APPC 裝置說明
資料庫檔案
用法資訊跳出程式 68
防止進行 PC 存取 131
資源安全
定義 3
限制存取
簡介 5
簡介 5
路由常駐程式 (RouteD)
安全要訣 118
跳出程式
分隔頁 68
用戶端要求存取 (PCSACC) 網路屬性 68, 139
印表機裝置說明 68
回轉作業 68
自動清除 (QEZUSRCLNP) 68
岔斷要求程式 68
系統登記功能 69
來源 139
建立產品載入 (CRTPRDLOD 指令) 68
容許遠端登入 (QRMTSIGN) 系統值 68, 139
效能集合 68
格式選項 68
訊息說明 68
密碼驗證程式 (QPWDVLDPGM) 系統值 68, 139
接收異動記載登錄 68
備份列示 (CHGBCKUP 指令) 68
評估 68
開放式資料庫連接 (ODBC) 139
資料庫檔案用法 68
確定作業 68
檔案系統功能 68
變更訊息說明 (CHGMSGD 指令) 68
邏輯檔案格式選項 68
3270 模擬功能鍵 68
DDM 要求存取 (DDMACC) 網路屬性 68, 139
QATNPGM (岔斷要求程式) 系統值 68
QHFRGFS API 68
跳出程式 *(繼續)*
QTNADDCR API 68
QUSCLSXT 程式 68
RCVJRNE 指令 68
SETATNPGM (設定岔斷要求程式) 指令 68
STREML3270 (啓動 3270 顯示器模擬) 指令 68
TRCJOB (追蹤工作) 指令 68
遊蕩，TCP/IP
限制 128
達到登入嘗試次數時的動作 (QMAXSGNACN) 系統值
建議設定 19
CFGSYSSEC 指令所設定的值 32
閘道伺服器
安全問題 136
電腦病毒
防止 63
定義 63
掃描 64
iSeries 伺服器保護機制 64
預先建立階段作業 (PREESTSSN) 參數 101
預設使用者
針對結構 TPN 77
通訊登錄
可能值 97

〔十四劃〕

實體安全 73
對映磁碟機，存取 iSeries 400 目錄 141
監督
子系統說明 74
工作佇列 53
公用權限 49
使用者設定檔
變更 73
使用者環境 54
沿用的權限 64, 65
物件整合性 45
物件權限 45
特殊權限 53
密碼活動 23
專用權限 52
授權清單 50
排定的程式 70
復置功能 64, 70
登入活動 23
程式失效 46
新物件的權限 49
輸出佇列 53
儲存功能 64, 70
觸發程式 67
權限 49
管理
子系統說明 74
工作佇列 53
公用權限 49
使用者環境 54
沿用的權限 64, 65
特殊權限 53
專用權限 52
授權清單 50
排定的程式 70
復置功能 64, 70
新物件的權限 49
審核異動記載 46
輸出佇列 53
儲存功能 64, 70
觸發程式 67
權限 49
管理者網際網路位址 (INTNETADR) 參數
限制 127
管理通訊協定 (SNMP)， 簡易網路 126
精靈, 安全 9
網域名稱系統 (DNS)
安全要訣 119
限制埠 119
網路工作動作 (JOBACN) 網路屬性 99
網路檔案系統 (NFS) 90
網路屬性
列印與安全相關 7, 29
設定指令 31
DDMACC (DDM 要求存取)
使用跳出程式 68, 99
限制 PC 資料存取 131
限制遠端指令 136
跳出程式樣本來源 139
JOBACN (網路工作動作) 99
PCSACC (用戶端要求存取)
使用跳出程式 68
限制 PC 資料存取 131
跳出程式樣本來源 139
網際網路連線安全伺服器 (ICSS)
安全要訣 124
說明 124
網際網路連線伺服器 (ICS)
安全要訣 120
防止自動啓動伺服器 120
說明 120
輕裝備目錄存取通訊協定 (LDAP)
安全特性 125
遠端工作
防止 98
遠端位置名稱登錄
安全要訣 76
遠端系統
定義 93
遠端指令
防止 98, 135

遠端指令 *(繼續)*
限制以 PGMEVOKE 登錄 99
遠端執行伺服器 (REXECD)
安全要訣 117
限制埠 117
遞送登錄
安全要訣 76
除去 PGMEVOKE 登錄 99

〔十五劃〕

審核
物件整合性 45
物件權限 45
程式失效 46
審核 (QAUDJRN) 日誌
系統登錄 47
接收器儲存體臨界值 47
損壞 47
管理 46
審核日誌損壞 47
審核安全功能 43
審核動作 46
審核控制 (QAUDCTL) 系統值
變更 27
顯示 27
審核異動記載
列印登錄 29
審核層次 (QAUDLVL) 系統值
變更 27
顯示 27
審核，安全
使用建議
物件審核 105
概觀 79
CP (變更設定檔) 異動記載登錄 21, 22
SV (系統值) 異動記載登錄 71
*PGMADP 審核層次 65
*PGMFAIL 值 64
*SAVRST 值 64
*SECURITY 值 64
撥入使用者存取其它系統，防止 111
數位簽章
簡介 74
模式
通訊登錄 97
確定作業
跳出程式 68

〔十六劃〕

整合性
檢查
說明 45
整合保護
安全層次 (QSECURITY) 40 3
整合檔案系統 83
潛在安全問題 131
整合檔案系統，安全 83
整體設定 4
輸出佇列
列印安全相關參數 30
列印使用者設定檔的 54
監督存取 53
駭客入侵、防止與偵測 73

〔十七劃〕

儲存
安全性工具程式 25
密碼 23
儲存功能
控制 70
監督 64
儲存指令
限制存取 70
儲存體
臨界值
審核 (QAUDJRN) 日誌接收器 47
檔案
安全性工具程式 25
檔案用法
跳出程式 68
檔案系統、根 (/)、QOpenSys 以及使用者定義 84
檔案系統功能
跳出程式 68
檔案系統，QFileSvr.400 90
檔案系統，Root (/)、QOpenSys 以及 使用者定義的安全 86
檔案系統，限制存取 QSYS.LIB 88
檔案系統，網路 90
檔案系統，整合 83
檔案庫
報表
內容 45
所有檔案庫 45
檔案庫列示
潛在安全問題 71
檔案庫安全 42
檔案轉送
限制 43
PC (個人電腦) 131
檔案轉送通訊協定 (FTP)
跳出程式樣本來源 139
檢查
改變的物件 45
物件整合性 29, 64
說明 45
預設密碼 26
檢查 *(繼續)*
隱藏程式 68
檢查物件整合性 (CHKOBJITG) 指令
建議使用 64
說明 29, 45
避免
安全性工具程式檔案衝突 25
隱藏程式
檢查 68
點對點 (PPP) 通訊協定
安全注意事項 112

〔十八劃〕

瀏覽器的安全注意事項 141
瀏覽器，安全注意事項 141
簡易網路管理 通訊協定 (SNMP) 126
簡單網路管理通訊協定 (SNMP)
安全要訣 126, 127
防止自動啓動伺服器 127
限制埠 127

〔十九劃〕

簽章物件 74
識別
APPC 使用者 95

〔二十劃〕

觸發程式
列出全部 29
評估使用情況 68
監督使用情況 67

〔二十一劃〕

顧問, 安全 11

〔二十二劃〕

權限
工作佇列 53
公用 49
安全性工具程式 指令 25
安全層次 10 或 20 39
沿用的 64
限制 65
監督 64
審核 46
特殊 53
國家語言 43
開始 40
新物件 49

權限 *(繼續)*
概觀 39
當執行時 39
補充功能表存取控制 40
對於復置指令的存取 70
對於儲存指令的存取 70
監督 49, 52
管理 49
輸出佇列 53
檔案庫安全 42
簡介 5
轉移環境 40
PC 使用者的資料存取 132
*SAVSYS (儲存系統) 特殊權限 70
控制 70
權限，物件
請參閱 物件、

〔二十三劃〕

變更
公開的密碼 18
安全審核 27
作用設定檔列示 26
登入錯誤訊息 20
IBM 所提供的密碼 18
uid 91
變更安全審核 (CHGSECAUD) 指令
建議使用 79
說明 27
變更作用設定檔列示 (CHGACTPRFL) 指令
建議使用 21
說明 26
變更系統檔案庫列示 (CHGSYSLIBL) 指令
限制存取 71
「變更到期日進度表登錄 (CHGEXPSCDE)」指令
建議使用 22
說明 26
變更效能集合 (CHGPFRCOL) 指令
跳出程式 68
變更訊息說明 (CHGMSGD) 指令
跳出程式 68
「變更啟動進度表登錄 (CHGACTSCDE)」指令
建議使用 20
說明 26
變更備份 (CHGBCKUP) 指令
跳出程式 68
邏輯分割區，安全性 57
邏輯檔案
記錄格式選項跳出程式 68
顯示
安全審核 27
顯示 *(繼續)*
使用者設定檔
作用設定檔列示 26
到期日排程 26
專用權限 77
啟動排程 26
物件權限 45
授權使用者 44
採用程式 46
群組設定檔成員 41
QAUDCTL (審核控制) 系統值 27
QAUDLVL (審核層次) 系統值 27
顯示安全審核 (DSPSECAUD) 指令
說明 27
顯示作用排程 (DSPACTSCD) 指令
說明 26
顯示使用者設定檔 (DSPUSRPRF) 指令
使用輸出檔 44
「顯示到期日進度表 (DSPEXPSCD)」指令
建議使用 22
說明 26
顯示物件說明 (DSPOBJD) 指令
使用輸出檔 44
顯示物件權限 (DSPOBJAUT) 指令 45
顯示授權列示物件報告 50
顯示授權使用者 (DSPAUTUSR) 指令
審核 44
顯示授權使用者 (DSPAUTUSR) 顯示 44
顯示採用程式 (DSPPGMADP) 指令
審核 46
顯示登入資訊 (QDSPSGNINF) 系統值
建議設定 19
CFGSYSSEC 指令所設定的值 32
顯示審核異動記載登錄 (DSPAUDJRNE) 指令
建議使用 79
說明 29
顯示檔案庫 (DSPLIB) 指令 45
驗證加密密碼 (*VFYENCPWD) 值 96, 100
驗證物件復置 (QVFYOBJRST) 系統值
建議使用 70
驗證值 64

〔數字〕

3270 裝置模擬
跳出程式 68

A

ADDPFRCOL (新增效能集合) 指令
跳出程式 68
ANZDFTPWD (分析預設密碼) 指令
建議使用 23
ANZDFTPWD (分析預設密碼) 指令 *(繼續)*
說明 26
ANZPRFACT (分析設定檔活動) 指令
建立免除使用者 26
建議使用 21
說明 26
API，使用 the open() 或 creat() 建立串流檔 90
API，建立目錄 89
APPC 使用者取得目標系統的方法 95
APPC 通訊的基本元素 93
APPC 通訊， 基本元素 93
APPC (進階的程式間通訊)
安全要訣 93
指定使用者設定檔 96
架構安全值
使用 SECURELOC (安全位置) 參數 96
說明 95
應用程式範例 95
限制階段作業 94
區分安全責任 96
基本元素 93
專用辭彙 93
控制器說明
切斷計時器參數 102
安全相關參數 101
AUTOCRTDEV (自動建立裝置) 參數 102
CPSSN (控制點階段作業) 參數 102
啟動透通工作 97
評估配置 99, 103
階段作業 94
裝置說明
以 APPN 來保護安全 94
以物件權限來限制 94
安全位置 (SECURELOC) 參數 100
安全角色 94
安全相關參數 99
APPN (APPN 功能) 參數 101
LOCPWD (位置密碼) 參數 94
PREESTSSN (預先建立階段作業) 參數 101
SECURELOC (安全位置) 參數 94, 96
SNGSSN (單一階段作業) 參數 101
SNUF 程式啟動欄位 101
遠端指令 99
限制以 PGMEVOKE 登錄 99
線路說明 102
安全相關參數 102
AUTOANS (自動回答) 欄位 103
AUTODIAL (自動撥號) 欄位 103
識別使用者 95
APPC 階段作業的基礎 94

APPC 階段作業，限制 94
APPN 功能 (ANN) 參數 101
AUTOANS (自動回答) 欄位 103
AUTOCRTCTL (自動建立控制器) 參數 102
AUTODIAL (自動撥號) 欄位 103

B

BOOTP (啓動程式通訊協定)
安全要訣 113
限制埠 113

C

CFGSYSSEC (配置系統安全) 指令
建議使用 13
說明 31
CHGACTPRFL (變更作用設定檔列示) 指令
建議使用 21
說明 26
CHGACTSCDE (變更啓動進度表登錄) 指令
建議使用 20
說明 26
CHGBCKUP (變更備份) 指令
跳出程式 68
CHGEXPSCDE (變更到期日進度表登錄) 指令
建議使用 22
說明 26
CHGMSGD (變更訊息說明) 指令
跳出程式 68
CHGPFRCOL (變更效能集合) 指令
跳出程式 68
CHGSECAUD (變更安全審核) 指令
建議使用 79
說明 27
CHGSYSLIBL (系統檔案庫列示) 系統值
保護 71
CHGSYSLIBL (變更系統檔案庫列示) 指令
限制存取 71
CHKOBJITG (檢查物件整合性) 指令
建議使用 64
說明 29, 45
CP (變更設定檔) 異動記載登錄
建議使用 21, 22
CPF1107 訊息 20
CPF1120 訊息 20
CPSSN (控制點階段作業) 參數 102
CRTPRDLOD (建立產品載入) 指令
跳出程式 68

D

DDMACC (DDM 要求存取) 網路屬性
使用跳出程式 68, 99
限制 PC 資料存取 131
限制遠端指令 136
跳出程式樣本來源 139
DHCP (動態的主電腦配置通訊協定)
安全要訣 114
限制埠 115
DNS (網域名稱系統)
安全要訣 119
限制埠 119
DSPACTPRFL (顯示作用設定檔列示) 指令
說明 26
DSPACTSCD (顯示作用排程)指令
說明 26
DSPAUDJRNE (顯示審核異動記載登錄) 指令
建議使用 79
說明 29
DSPAUTUSR (顯示授權使用者) 指令
審核 44
DSPEXPSCD (顯示到期日進度表) 指令
建議使用 22
說明 26
DSPLIB (顯示檔案庫) 指令
使用 45
DSPOBJAUT (顯示物件權限) 指令
使用 45
DSPOBJD (顯示物件說明) 指令
使用輸出檔 44
DSPPGMADP (顯示沿用程式) 指令
審核 46
DSPSECAUD (顯示安全審核) 指令
說明 27
DSPUSRPRF (顯示使用者設定檔) 指令
使用輸出檔 44
DST (專用服務工具)
密碼 19

E

ENDPFRMON (結束效能監督程式) 指令
跳出程式 68
eServer 安全規劃程式 9, 11

F

FMTSLR (記錄格式選項程式) 參數 68
FRCCRT (強迫建立) 參數 64
FTP (檔案轉送通訊協定)
跳出程式樣本來源 139

I

IBM 所提供的設定檔
變更密碼 18
ICS (網際網路連線伺服器)
安全要訣 120
防止自動啓動伺服器 120
說明 120
ICSS (網際網路連線安全伺服器)
安全要訣 124
說明 124
INETD 127
INTNETADR (管理者網際網路位址) 參數
限制 127
iSeries 400 建立目錄指令 89
iSeries Access
防止 PC 病毒 131
防止遠端指令 136
物件權限 132
限制遠端指令 135
密碼加密 134
控制資料存取 131
略過登入 135
資料存取方法 131
閘道伺服器 136
潛在安全問題 131
整合檔案系統的蘊涵 131
檔案轉送 131
PC 上的病毒 131
iSeries Access Express, 使用 SSL 133
iSeries Access for Windows
搭配 SSL 133
iSeries 安全精靈 9
iSeries 領航員, 安全 133

J

JOBACN (網路工作動作) 屬性 99

L

LOCPWD (位置密碼) 參數 94
LP 安全性 57
LPD (印表常駐程式)
安全要訣 125
防止自動啓動伺服器 126
限制埠 126
說明 125

O

ODBC (開放式資料庫連接)
控制存取 134
跳出程式樣本來源 139

P

PC (個人電腦)
防止 PC 病毒 131
防止遠端指令 136
物件權限 132
限制遠端指令 135
密碼加密 134
控制資料存取 131
略過登入 135
資料存取方法 131
閘道伺服器 136
潛在安全問題 131
整合檔案系統的蘊涵 131
檔案轉送 131
PC 上的病毒 131
PCSACC (用戶端要求存取) 網路屬性
使用跳出程式 68
限制 PC 資料存取 131
跳出程式樣本來源 139
PREESTSSN (預先建立階段作業) 參數 101
PRTADPOBJ (列印沿用物件) 指令
說明 29
PRTCMNSEC (列印通訊安全) 指令
說明 29
範例 99, 103
PRTJOBDAUT (列印工作說明權限) 指令
建議使用 77
說明 29
PRTPUBAUT (列印公用授權物件) 指令
建議使用 94
說明 29
PRTPVTAUT (列印專用權限) 指令
建議使用 94
授權清單 29, 50
說明 30
PRTQAUT (列印佇列權限) 指令
說明 30
PRTSBSDAUT (列印子系統說明) 指令
建議使用 97
說明 29
PRTSYSSECA (列印系統安全屬性) 指令
建議使用 13
說明 29
範例輸出 7
PRTTRGPGM (列印觸發程式) 指令
說明 29
PRTUSROBJ (列印使用者物件) 指令
建議使用方式 71
說明 29
PRTUSRPRF (列印使用者設定檔) 指令
不符的範例 54
特殊權限範例 54
密碼資訊 21, 23
說明 29
PRTUSRPRF (列印使用者設定檔) 指令 *(繼續)*
環境資訊範例 55

Q

QALWOBJRST (容許物件復置) 系統值
建議使用 70
CFGSYSSEC 指令所設定的值 32
QAUDCTL (審核控制) 系統值
變更 27
顯示 27
QAUDJRN (審核) 日誌
系統登錄 47
接收器儲存體臨界值 47
損壞 47
管理 46
QAUDLVL (審核層次) 系統值
變更 27
顯示 27
QAUTOCFG (自動配置) 系統值
建議設定 19
CFGSYSSEC 指令所設定的值 32
QAUTOVRT (自動虛擬裝置配置) 系統值
建議設定 19
CFGSYSSEC 指令所設定的值 32
QCONSOLE
預設密碼 61
QDEVRCYACN (裝置復原動作) 系統值
建議設定 19
預防安全漏洞 98
CFGSYSSEC 指令所設定的值 32
QDSCJOBITV (已中斷的工作逾時間隔) 系統值
建議設定 19
CFGSYSSEC 指令所設定的值 32
QDSPSGNINF (顯示登入資訊) 系統值
建議設定 19
CFGSYSSEC 指令所設定的值 32
QEZUSRCLNP 跳出程式 68
QFileSvr.400 檔案系統 90
QHFRGFS API
跳出程式 68
QINACTITV (不作用的工作逾時間隔) 系統值
建議設定 19
CFGSYSSEC 指令所設定的值 32
QINACTMSGQ (不作用的工作訊息佇列) 系統值
建議設定 19
CFGSYSSEC 指令所設定的值 32
QLMTSECOFR (限制安全主管) 系統值
建議設定 19
CFGSYSSEC 指令所設定的值 32
QMAXSGNACN (達到登入嘗試次數時的動作) 系統值
建議設定 19
CFGSYSSEC 指令所設定的值 32
QMAXSIGN (最大登入嘗試次數)
建議設定 19
QMAXSIGN (最大登入嘗試次數) 系統值
CFGSYSSEC 指令所設定的值 32
QPGMR (程式設計師) 使用者設定檔
CFGSYSSEC 指令所設定的密碼 33
QPWDEXPITV (密碼到期間隔) 系統值
建議設定 13
CFGSYSSEC 指令所設定的值 32
QPWDLMTAJC (密碼限制相鄰字元) 系統值
建議設定 13
CFGSYSSEC 指令所設定的值 32
QPWDLMTCHR (密碼限制字元) 系統值
建議設定 13
CFGSYSSEC 指令所設定的值 32
QPWDMAXLEN (密碼最大長度) 系統值
建議設定 13
CFGSYSSEC 指令所設定的值 32
QPWDMINLEN (密碼最小長度) 系統值
建議設定 13
CFGSYSSEC 指令所設定的值 32
QPWDPOSDIF (密碼需要位置差異) 系統值
建議設定 13
CFGSYSSEC 指令所設定的值 32
QPWDRQDDGT (密碼需要數值字元) 系統值
建議設定 13
CFGSYSSEC 指令所設定的值 32
QPWDRQDDIF (密碼必要差異) 系統值
建議設定 13
CFGSYSSEC 指令所設定的值 32
QPWDVLDPGM (密碼驗證程式) 系統值
使用跳出程式 68
建議設定 13
跳出程式樣本來源 139
CFGSYSSEC 指令所設定的值 32
QPWFSERVER 88
QRETSVRSEC (保留伺服器安全資料) 系統值
用於 SLIP 撥出 111
說明 23
QRMTSIGN (容許遠端登入) 系統值
使用跳出程式 68
跳出程式樣本來源 139
CFGSYSSEC 指令所設定的值 32
*FRCSIGNON 值的影響 95
QSECURITY (安全層次) 系統值
說明 3
CFGSYSSEC 指令所設定的值 32

QSRV (服務) 使用者設定檔
CFGSYSSEC 指令所設定的密碼 33
QSRVBAS (基本服務) 使用者設定檔
CFGSYSSEC 指令所設定的密碼 33
QSYS38 (System/38) 檔案庫
限制指令 43
QSYSCHID (變更 uid) API 91
QSYSMSG (系統訊息) 訊息佇列
建議使用 79
跳出程式樣本來源 139
QSYSOPR (系統操作員) 使用者設定檔
CFGSYSSEC 指令所設定的密碼 33
QSYS.LIB 檔案系統，限制存取 88
QTNADDCR API
跳出程式 68
QUSCLSXT 程式 68
QUSEADPAUT (使用沿用權限) 系統值 66
QUSER (使用者) 使用者設定檔
CFGSYSSEC 指令所設定的密碼 33
QVFYOBJRST (驗證物件復置)
系統值 74
QVFYOBJRST (驗證物件復置) 系統值
建議使用 70

R

RCVJRNE (接收異動記載登錄)
跳出程式 68
REXECD (遠端執行伺服器)
安全要訣 117
限制埠 117
RouteD (路由常駐程式)
安全要訣 118
RUNRMTCMD (執行遠端指令) 指令
限制 136
RVKPUBAUT (取消公用權限) 指令
明細 34
建議使用 75
說明 31

S

SBMRMTCMD (提出遠端指令) 指令
限制 98
SECBATCH (提出批次報表) 功能表
提出報表 28
Secure Sockets Layer (SSL)
搭配 iSeries Access for Windows 133
SECURELOC (安全位置) 參數 100
圖解 94
說明 96
*VFYENCPWD (驗證加密密碼) 值 96, 100
SECURE(NONE)
說明 95
SECURE(PROGRAM)
說明 95
SECURE(SAME)
說明 95
SECURITY(NONE)
QRMTSIGN 系統值使用 *FRCSIGNON 值 95
SETATNPGM (設定岔斷要求程式) 指令
跳出程式 68
SLIP (序列介面線路通訊協定)
保護撥入的安全 110
保護撥出安全 111
控制 109
說明 109
SNDJRNE (傳送日誌登錄) 指令 46
SNGSSN (單一階段作業) 參數 101
SNMP (簡單網路管理通訊協定)
安全要訣 126, 127
防止自動啓動伺服器 127
限制埠 127
SNUF 程式啓動欄位 101
SSL
搭配 iSeries Access for Windows 133
STRPFRMON (啓動效能監督) 指令
跳出程式 68
STRTCP (啓動 TCP/IP) 指令
限制 105
STS (服務工具伺服器)
邏輯分割區 57
SV (系統值) 異動記載登錄
建議使用 71
System/36 檔案轉送
限制 43
System/38 (QSYS38) 檔案庫
限制指令 43

T

TCP/IP
點對點 (PPP) 通訊協定
安全注意事項 112
TCP/IP 通信
安全保障要訣 105
防止登錄 105
保護埠應用程式 107
限制
配置檔 107
跳出 128
遊蕩 128
管理者網際網路位址 (INTNETADR) 參數 127
STRTCP 指令 105
網際網路連線安全伺服器 (ICSS)
安全要訣 124
TCP/IP 通信 *(繼續)*
網際網路連線安全伺服器 (ICSS) *(繼續)*
說明 124
網際網路連線伺服器 (ICS)
安全要訣 120
防止自動啓動伺服器 120
說明 120
BOOTP (啓動程式通訊協定)
安全要訣 113
限制埠 113
DHCP (動態的主電腦配置通訊協定)
安全要訣 114
限制埠 115
DNS (網域名稱系統)
安全要訣 119
限制埠 119
FTP (檔案轉送通訊協定)
跳出程式樣本來源 139
LPD (印表常駐程式)
安全要訣 125
防止自動啓動伺服器 126
限制埠 126
說明 125
REXECD (遠端執行伺服器)
安全要訣 117
限制埠 117
RouteD (路由常駐程式)
安全要訣 118
SLIP (序列介面線路通訊協定)
保護撥入的安全 110
保護撥出安全 111
控制 109
說明 109
SNMP (簡單網路管理通訊協定)
安全要訣 126, 127
防止自動啓動伺服器 127
限制埠 127
TFTP (一般檔案轉送通訊協定)
安全要訣 116
限制埠 116
TFTP (一般檔案轉送通訊協定)
安全要訣 116
限制埠 116
TRCJOB (追蹤工作) 指令
跳出程式 68

U

uid
變更 91
USEADPAUT (使用沿用權限) 參數 65

W

WRKREGINF (使用系統登記資訊) 指令
跳出程式 69
WRKSBSD (使用子系統說明) 指令 75

〔特殊字元〕

(PRTPUBAUT) 指令，列印公用授權物件 87
(PRTPVTAUT) 指令，列印專用權限物件 87
(QVFYOBJRST) 驗證復置物件系統值
復置系統值
復置系統值 (QVFYOBJRST) 64
數位簽章 64
(SNMP)， 簡易網路管理通訊協定 126
*IOSYSCFG (系統配置) 特殊權限
APPC 配置指令的需要 95
*PGMADP (程式沿用) 審核層次 65
*SAVSYS (儲存系統) 特殊權限
控制 70
*VFYENCPWD (驗證加密密碼) 值 96, 100

讀者意見表

為使本書盡善盡美，本公司極需您寶貴的意見；懇請您閱讀後，撥冗填寫下表，惠予指教。

請於下表適當空格內，填入記號 (v) ；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	
	實際產品介面訊息與本書中所提是否一致	□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，版面安排是否方便閱讀	□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，是否便於查找	□是□否	
	索引語錄之排定，是否便於查找	□是□否	
	※評估意見為 "否" 者，請於備註欄提供建議。		

其他： (篇幅不夠時，請另外附紙說明。)

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。

iSeries 安全保護要訣及工具
版本 5

SC40-1899-07

折疊線

105 台北市敦化南路一段 2 號 4 樓

臺灣國際商業機器股份有限公司
大中華研發中心 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 00176 號
(免貼郵票)

寄件人
姓名：
地址：

寄

折疊線

Printed in Denmark by IBM Danmark A/S

SC40-1899-07