「個人資料」高度安全維護時代－談「特殊權限帳號」管理之重要性

邱靖峰 / 財金資訊公司安控部資源控管組高級工程師

一、前言

企業組織為發展業務，建立各項業務應用系統，且每一系統各有所屬的作業系統及資料庫系統；而隨著網際網路及雲端運算的蓬勃發展，為因應網路存取與安全防護的需求，各種功能的設備亦日趨多元。爰為有效控管該等應用系統、作業系統、資料庫及設備的使用者存取權限，管理單位必須建立使用者與管理者的帳號，並經由控管存取權限的方式，限制各類使用者的存取範圍，以保護系統資源，避免未經授權不當存取的風險。使用者必須依規定申請核可後，才能取得使用者帳號。

一般而言，「特殊權限帳號」(Privileged account) 包含最高權限帳號 (例如：Unix 作業系統的 root、Windows 作業系統的 administrator、資料庫系統的 sa 等)、權限管理 (授權) 帳號及變更帳號。「特殊權限帳號」通常具有較高的權限，可異動帳號與存取權限、存取資料庫內部資料、進行應用系統變更，或是變更系統、網路或設備的組態參數等；萬一管理不當，可能會影響業務正常營運，危害資料安全。面對多元發展且持續增加的系統與設備，帳號權限管理作業日趨複雜且繁重，如何有效管理倍數成長的「特殊權限帳號」，更成為企業組織的重要課題。

二、特殊權限帳號之安全風險

一般使用者與個人帳號間存在一對一的對應關係，可從帳號識別對應的使用者，再由帳號的軌跡紀錄找出所有使用紀錄，進行後續追蹤分析，如此，帳號維護管理作業較為容易。不過，如果系統與使用者眾多，也會成為帳號管理人員的沉重負擔。

另一方面，「特殊權限帳號」常會有多人共用的情形，不易從軌跡紀錄分辨、識別真正的使用者，也難以區分使用者真正的執行紀錄，這是企業組織各項系統中都可能存在的問題。

以下說明帳號管理作業常會遭遇的難題：

(一) 多樣化之帳號權限管理

由於各種作業系統 (例如：Windows、Linux、IBM AIX、zOS 等) 與資料庫系統 (例如：Oracle、MS SQL Server、MySQL 等) 各有不同的帳號權限管理方式，帳號管理人員不僅要熟悉多種系統，而且必須因應各系統的

限制，分別設定或調整管理政策。例如：針對以下常見的密碼管理原則，設定適當的管理強度或標準：

1. 密碼的歷程紀錄
2. 密碼的最長使用期限
3. 密碼的最短使用期限
4. 密碼的最小長度
5. 密碼的複雜度要求
6. 使用可還原的加密方式存放密碼

然而，每一種系統或設備可以設定的密碼管理原則不盡相同，可能無法貫徹企業組織的要求，達到一致的管理強度或標準。

(二) 「特殊權限帳號」之風險

「特殊權限帳號」如遭不當使用，可能造成系統故障或資料洩漏。作業系統的最高權限帳號經常有多人共同使用的情況，因此不易分辨真正的使用者，也無法正確區分使用者的執行軌跡紀錄，這是管理共用帳號常見的棘手問題。

另外，一般網路、資安或磁碟機之類的設備，帳號權限管理的功能設計通常比較簡單，可設定的參數條件較少，未必能完整滿足密碼複雜度、密碼使用期限、存取權限等各種要求，增加帳號管理作業的困難度。

(三) 應用程式帳號之風險

應用系統的帳號權限管理功能可能因無統一規範，或者來自不同開發廠商及人員等因素，而各有其特定的管理方式，授權與執行軌跡紀錄的內容格式與記錄方式亦各不相同。帳號權限管理人員只能依照每一種應用系統的特性，以人工處理方式進行帳號權限管理作業。

此外，一般套裝商業應用軟體通常較缺乏客製化的彈性，也會提高帳號權限管理作業整合的困難度。

(四) 虛擬環境與雲端運算之風險

在虛擬環境 (例如：VMware ESX/ESXi、Microsoft Hyper-V、Citrix XenServer 等) 中，有效管理實體主機是不容忽視的重要課題，因為每一部實體主機上都可能有數十部至數百部虛擬機器在運作，實體主機的管理者可以新建、複製、遷移及刪除任一部虛擬機器，也可以調配每一部虛擬機器的資源配置，包含 CPU、記憶體容量、硬碟空間等。對實體主機而言，每一部虛擬機器都是以映像檔的方式存放，只要取得映像檔，就等於取得整部虛擬機器及其存放的資料，影響範圍與程度不容小覷。

三、「特殊權限帳號」之存取管理

企業組織未將「個人資料」或機密文件的存取權限視為必須妥善管理的關鍵因素，經常是資料暴露於高風險下的主因。而帳號權限管理作業可能因為人員的離調異動或簽核流程的調整，出現不一致的狀況，如果想要即時監控，必須付出相當可觀的成本。

企業組織為強化個人或機敏資料的存取控管，必須規劃建立更完善的安全機制與管理作業。帳號權限管理的目的，就是經由監控帳號的存取活動，進行風險管理與合規檢查，偵測違反安全政策的不正常存取行為，並及時通報，以減輕駭客與惡意程式的威脅與衝擊，降低業務中斷及商譽毀損的風險。

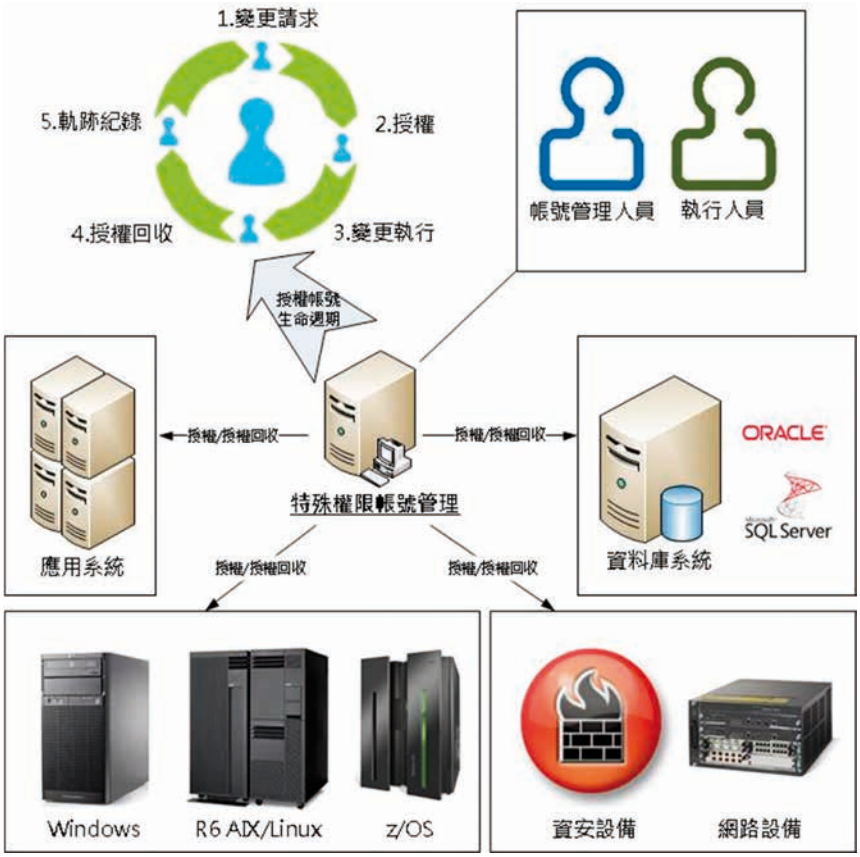

圖 1　「特殊權限帳號」管理

「特殊權限帳號」的權限通常高於一般帳號，因此，更須有效管理；「特殊權限帳號」管理作業內容如圖 1 所示，以下分段說明相關作業重點內容。

(一)「特殊權限帳號」之安全政策

企業組織制定統一的強制性存取安全政策，可確保使用者帳號之存取控管作業皆依循政策辦理，不會隨意調整或改變。特殊權限帳號的安全政策包含下列事項：

1. 「特殊權限帳號」的管理原則及可歸責性 (Accountability) 要求。
2. 「特殊權限帳號」與密碼的變更管理及各種系統管理方式的一致性。
3. 應用系統針對「特殊權限帳號」的認證方法與處理原則。
4. 「特殊權限帳號」存取活動的行為監控與軌跡留存原則。

(二)「特殊權限帳號」之管理作業

「特殊權限帳號」的管理作業包含政策管理、帳號管理、使用者管理、密碼管理等事項：

1. 政策管理：定義「特殊權限帳號」使用的生命週期，包含存取管理、稽核管理、權利管理、通知、自動化管理等。
2. 帳號管理：管理「特殊權限帳號」的異動作業，包含新增、修改、刪除等。

3. 使用者管理：管理使用者持有的帳號，一位使用者可能持有多個帳號，且在不同的系統均持有帳號。
4. 密碼管理：管理密碼的儲存方式（是否加密存放、是否具完整性與可用性）、保管方式（是否經由雙重控管機制保護「特殊權限帳號」）、更新頻率、複雜度或安全強度等。

（三）「特殊權限帳號」之軌跡紀錄管理

帳號軌跡紀錄管理包含紀錄管理、分析管理、通知管理、報表管理等作業：

1. 紀錄管理：考量軌跡紀錄的完整性及正確性，並依據相關法令規範，留存適當年限，除提供帳號管理人員查閱之外，萬一發生訴訟時，也可調閱作為證據。
2. 分析管理：提供帳號使用紀錄分析功能，支援帳號管理人員進行違例使用之行為分析與問題追蹤。
3. 通知管理：依據事件種類、影響範圍、衝擊程度等條件，定義觸發異常事件時，進行通知告警的方式。
4. 報表管理：提供各種帳號使用軌跡紀錄報表，支援帳號管理人員進行帳號授權與執行紀錄的覆核作業。

四、結語

「特殊權限帳號」之存取控管是企業維護業務系統正常與安全運作最重要的一道關卡，不論是作業系統、資料庫、應用系統、網路或資安設備，都必須建構一套完善的管理制度與維運機制，有效管理「特殊權限帳號」的生命週期，才能避免因不當使用而產生的風險。

經由事前控管「特殊權限帳號」的授權使用，以及事後專人檢視相關執行軌跡紀錄，觀察分析帳號的存取活動，即時處理不正常存取的違例事件，才能將「特殊權限帳號」的存取活動維持在安全可控制的環境之下。企業如果明確識別出主機系統的個人或機敏資料，輔以有效的帳號權限存取控管與監控，就能讓資料獲得更有效而完整的保護。

※ 參考文獻 / 資料來源：

1. http://windows.microsoft.com/zh-tw/windows/change-password-policy-settings
2. http://www-01.ibm.com/support/knowledgecenter/ssw_aix_61/com.ibm.aix.security/doc/security/aix_sec_expert_pwd_policy_settings.htm?lang=zh-tw
3. http://www.liebsoft.com
4. http://www.ca.com/us/securecenter/ca-controlminder.aspx
5. http://www.cyberark.com