跨越系統藩籬－淺談異質平台之使用者帳號管理

李中仁 / 財金資訊公司安控部資源控管組工程師

一、前言

企業在建構內部資訊系統時，常基於系統架構、成本預算、人員技能及公司政策等因素，而採用各種不同的作業系統平台與資訊設備。然而隨著企業的發展，員工數量不斷擴增及資訊系統的複雜度持續升高，帳號管理人員的工作量自然也越來越繁重，如何有效控管各種異質系統平台的使用者帳號，成為帳號管理人員必須面對的重要課題。

本文將先探討異質系統平台之使用者帳號管理所常見的安全風險，再分別從政策面與系統面介紹如何降低安全風險，並提升管理效率。

二、異質平台使用者帳號之安全風險

企業為提供各式各樣的資訊系統服務，經常需要結合各種不同的作業系統、資料庫、應用程式、資安設備及網路設備。目前絕大多數資訊系統為識別使用者，並且為不同使用者存取適合其職務的資訊，大部分仍採用以帳號與密碼為主的使用者驗證機制。

隨著企業發展與時間累積，資訊系統及使用者的數量不斷增長，如果帳號管理人員未規劃良好的因應策略，可能衍生各種潛在的安全風險。以下分別從管理者與使用者的角度，探討可能遭遇的困難及風險：

(一) 管理異質平台的困難及風險

1. 持有太多帳號密碼

使用者就不同系統自有其帳號與密碼，難以逐一記憶或保存，若不甚洩露或遭竊，機密資料即可能被盜；而帳號管理人員所使用的帳號，至少具備帳號管理的權限，甚至可能具備完全控制系統的權限，如果未能妥善管理帳號密碼致外洩或遭竊，所產生的危害程度將遠比一般使用者帳號更嚴重。

2. 系統平台特性不同

不同的作業系統、資料庫、應用程式或設備，經常有其特定的帳號權限設定方式，如果帳號管理人員未能深入瞭解各種平台的帳號權限管理特性，可能會因為權限開放不當，而發生不當存取的情事。

3. 帳號管理效率不彰

帳號管理人員必須配合人員的到職、離職或職務異動，進行使用者帳號的新增、刪除或權限異動，如新人員到職時，因為系統數量繁多，帳號管理人員可能需要數天甚至一、兩週，才能完成所有帳號的建置，嚴重影響企業資訊系統的維運效率；甚或人員離職或職務異動時，帳號管理人員可能不慎遺漏某些資訊系統，未及時刪除或停用相關使用者帳號，造成資訊安全管理疏失。此外，帳號管理人員須登入不同的系統進行人工作業，不僅耗費大量時間，如果未能建立標準作業程序及有效的覆核程序，可能因操作錯誤而衍生資安風險。

（二）存取異質平台的困難及風險

1. 多組帳號密碼不易保管

登入不同的資訊系統需要使用不同的帳號與密碼，對大多數人而言，同時記憶多組密碼實在難以招架，因而常會記載於紙本或其他容易取得的地方。一旦密碼不小心遺失或是遭有心人士竊取，就可能洩漏企業機密，造成財物及商譽損失。

2. 忘記較少使用的系統密碼

使用者嘗試登入平常較少使用的系統時，常會發現無法正確輸入密碼，於是只好依據企業的管理流程，求助系統管理人員進行密碼重置。這種情形不僅影響作業效率，更增加企業的營運成本。

三、異質平台之使用者帳號管理

企業在發展各項資訊服務時，經常使用不同的作業系統平台、資料庫與資訊設備，也會建置各種應用系統使用者介面，因此，異質平台的使用者帳號管理已經成為企業無法逃避的重要課題。藉由政策的制定以及相關系統的建立，企業才能達成降低營運風險及提升管理效率的目標。

（一）政策面的制定

為有效管理眾多平台的使用者帳號，必須建立良善的管理政策，以減少因人為蓄意或疏忽所衍生的安全風險。

1. 制定統一的帳號命名原則

為確立使用者帳號的單一性 (Unique) 及可歸責性 (Accountability)，企業應訂定統一的內部帳號命名原則，使帳號的名稱可明確關聯至特定個人，以利日後的帳號盤點整理及事件追蹤分析。

2. 依據角色進行授權

企業規劃帳號權限管理作業時，建議採用以角色為基礎的存取控制方式 (Role Based Access Control，RBAC)，依據使用者的職務角色 (群組)，賦予適當的權限，而不是直接授予個人帳號，以避免相同職務角色的人員具有不同的權限。

3. 建立各系統帳號管理的作業程序

大多數作業系統 (如 Windows、AIX、Linux、z/OS 等) 及資料庫 (SQL Server、Oracle、MySQL 等) 可利用腳本語言 (Scripting Language) 進行管理工作的標準化，對於帳號管理人員經常執行的作業，如新增帳號、刪除帳號、密碼重置及群組異動等，可撰寫各種不同的腳本 (Script)，日後進行帳號維護作業時，僅須輸入最少必要的相關參

數，即可執行腳本程式，順利完成任務。即使是剛走馬上任的帳號管理新手，亦可依據標準作業程序逐步完成管理工作，不僅降低操作錯誤風險，亦可提升執行效率，維持管理作業的一致性。

至於一般應用系統及資訊設備，帳號管理人員通常只能參考系統開發人員或設備原廠提供的說明文件，使用系統或設備提供的管理介面，執行帳號權限管理作業。

4. 監控系統日誌

帳號管理人員應定期查閱系統日誌，以確認各系統是否有異常的使用者帳號活動，高頻率的登入失敗或於異常時間的登入存取紀錄，都可能是帳號被盜用的跡證，帳號管理人員應聯繫帳號持有者查明原因，以防帳號被盜用。此外，特權帳號 (Privilege Account) 的使用紀錄亦須審慎檢核，以確認使用過程經過權責主管核可，而且執行內容正確無誤。

5. 定期進行帳號盤點

企業資產需要定期盤點，帳號管理人員亦須定期針對所管轄的主機設備進行帳號盤點。帳號盤點作業有下列主要目標：

(1) 確認使用者所擁有的帳號皆是職務所需的。
(2) 確認主機上沒有非經授權而產生的帳號。
(3) 確認沒有漏未刪除的幽靈帳號。

為進行帳號清點，帳號管理人員可透過系統排程方式，由受管理的系統主機定期匯出帳號清單，集中收存至帳號清單資料庫，日後即可經由此資料庫掌握各系統的帳號，對於無法以排程方式匯出帳號清單的應用系統或資訊設備，則由帳號管理人員以文件方式登載記錄之。

(二) 系統面的建立

企業即便制定帳號管理相關規範，仍然無法解決使用者及管理者共同的最大問題：帳號與密碼數量太多。配合企業的持續發展，帳號管理人員必須思考如何兼顧安全及效率，以達最佳平衡狀態。茲提供下列幾種技術，可有效減輕使用者及管理者的帳號管理問題供參：

1. 建置目錄服務 (Directory Service)

大多數系統本身即可進行帳號密碼驗證作業，管理者或使用者必須輸入系統認可的正確帳號與密碼，才可登入存取，帳號管理人員可建置目錄服務 (如微軟的 Active Directory 或 Linux 的 Open LDAP 等)，將使用者帳號驗證工作交由目錄服務主機負責，如圖 1 所示。

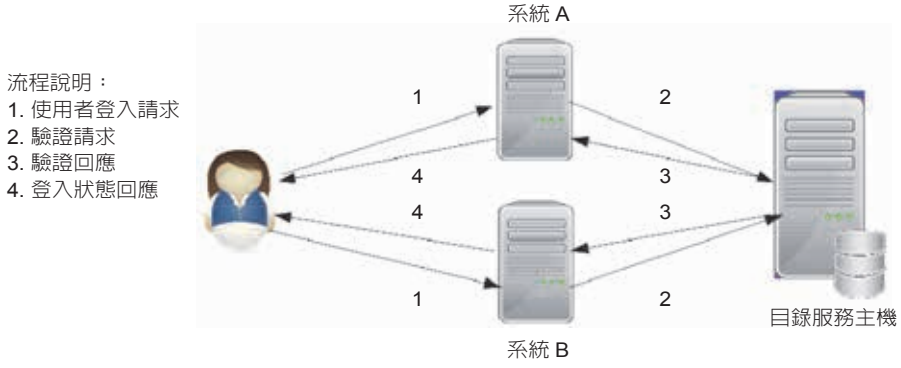

圖 1　目錄服務系統

將系統帳號來源設定為目錄服務主機後，使用者登入這些系統主機時，皆可使用同一組帳號密碼，有效減少記憶多組密碼的問題。目前市面上主流的作業系統及資料庫幾乎都支援以目錄服務為帳號驗證來源，企業開發或購置資訊系統時，應將支援目錄服務列為需求規格之必要項目，以減少帳號密碼數目太多的問題。

2. 建置使用者帳號識別存取管理服務 (Identity Access Management Service)

建置目錄服務雖可減少帳號數量，但帳號管理人員仍須逐一進入各系統進行帳號管理作業，利用使用者帳號識別存取管理 (Identity Access Management，簡稱 IAM) 服務，可有效減少帳號管理作業所耗費的時間，如圖 2 所示。

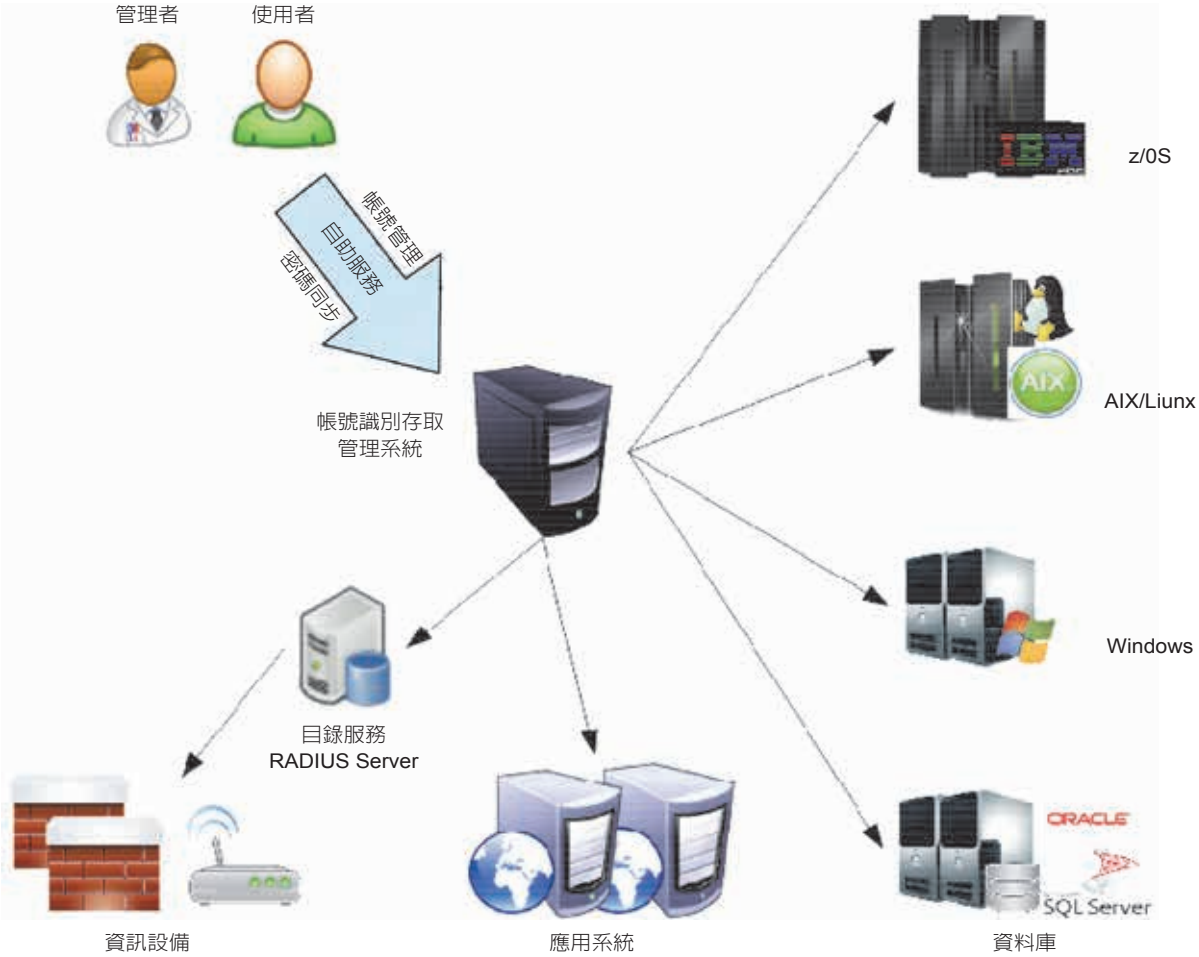

圖 2　帳號識別存取管理系統

企業建置使用者帳號識別存取管理系統，可獲得以下效益：

(1) 帳號管理人員可針對不同角色，分別定義各系統的帳號模板 (Account Template)，爾後建立新帳號時，即可套用該等設定，解決人工操作失誤的問題。

(2) 帳號管理人員可將數個帳號模板組合成一個角色 (Provisioning Role)，對於新增使

用者帳號的需求，只須設定帳號所欲加入的角色，使用者帳號識別存取管理系統即可迅速建立後端 (Endpoint) 系統的帳號。以往帳號管理人需要耗費數天才可完成的帳號管理作業，透過系統自動化管理，只要數分鐘就可大功告成。

(3) 使用者帳號識別存取管理系統可提供跨系統密碼同步化功能，即使是原本未使用目錄服務進行驗證的系統，使用者也可使用相同的密碼進行存取，減輕持有過多密碼的困擾。

(4) 以往使用者如果忘記密碼，必須提出申請，請帳號管理人員協助執行密碼重置作業；而利用使用者帳號識別存取管理系統提供的自助服務 (Self Service)，使用者即可自行操作以取得新的密碼。

(5) 使用者帳號識別存取管理系統可直接控管各系統的帳號，有助於帳號盤點作業之規劃執行，幽靈帳號自然隨之減少。

導入使用者帳號識別存取管理服務，可有效減輕帳號管理人員的繁重負擔，將時間利用於更重要的工作任務；另一方面，自助服務及密碼同步功能可協助使用者以更快速、便利而安全的方式存取相關系統，提升作業效率與安全強度。

3. 建置單一登入服務 (Single Sign On Service)

利用目錄服務及使用者帳號識別存取管理服務，雖可有效減少使用者持有過多帳號密碼的問題，但是使用者登入不同系統時，仍然需要逐一輸入帳號與密碼。有鑑於此，單一登入 (Single Sign On，簡稱 SSO) 服務提供使用者單一的登入入口 (Portal)，只要成功登入，存取其他不同系統就不需要再輸入帳號密碼，如圖 3 所示。

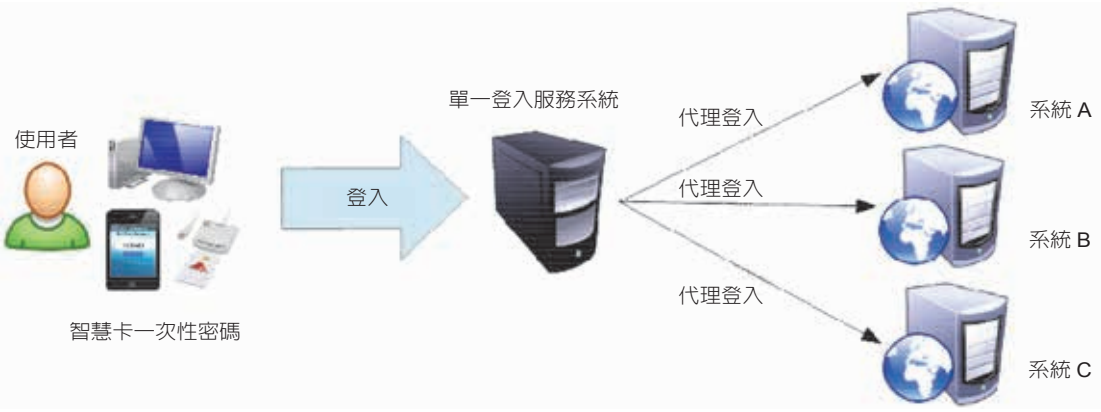

圖 3　單一登入系統

由於帳號密碼單一化，萬一帳號密碼不慎外洩或遭竊，有心人士即可存取此帳號可登入的所有系統，為提升安全強度，企業規劃建置單一登入系統時，可結合智慧卡 (Smart Card) 或一次性密碼 (One Time Password，OTP) 等安全機制，以降低帳號密碼外洩可能衍生之資安風險。

四、結語

良善的帳號管理是資訊安全管理的第一步，面對眾多使用者及各種資訊系統，如何有效落實帳號管理作業，是每一位帳號管理人員必須念茲在茲、審慎思考與面對的重要課題。

落實帳號管理安全政策，妥善利用各種系統服務，可建構一個「輕鬆管理」且「安全存取」的系統平台，提供前端使用者安全而便利的作業環境。帳號管理系統服務可減輕人工管理的繁複流程與作業負荷，提升管理效率，有效降低帳號管理人員操作不慎或疏失而發生嚴重後果的可能。對企業組織而言，帳號管理人員有更多時間投入重要任務，使用者可安全而快速地存取系統，可開創作業效率及資訊安全共同提升的多贏局面。

※ 參考文獻 / 資料來源：

1. http://en.wikipedia.org/wiki
2. http://www.ca.com/us/products/identity-management.aspx
3. http://www.microsoft.com/en-us/server-cloud/products/forefront-identity-manager/
4. https://docs.oracle.com/cd/B14099_19/idmanage.1012/b14084/intro.htm
5. Microsoft Developer Network (MSDN)