

IBM Optim Data Privacy Solution

重要特色

- **保護非正式作業環境中的機密資料隱私權**
- **運用預先定義的遮罩技術，加速遞送時間**
- **保留資料完整性，同時保護隱私權**
- **改善非正式作業資料庫中的資料遮罩彈性**
- **支援隱私權規定及企業監管標準**

遵循資料隱私權規定 — 這是法律！

保護個人身分資料的隱私權不僅是良好的商業作法，也是法律規定！全球企業都受到防止濫用機密資訊的政府法規所約束。例如，歐盟已制定「個人資料保護法」(Personal Data Protection Directive)，作為隱私權的保護架構，以規範成員國。在加拿大，企業遵循「個人資料保護及電子文件法案」(Personal Information Protection and Electronic Documents Act, PIPEDA) 的規定；澳洲企業必須遵守「隱私權修訂法案」(Privacy Amendment Act)。美國則採用國家及各州所頒佈的不同法規。全球各地都有類似的法規。

此外，各產業聯盟也正在制定特定行業的監管標準。例如，為了因應排山倒海的資料盜用及詐騙事件，其他付款卡公

司也開始採用 Visa® 及 MasterCard® 發起的「付款卡產業資料安全標準」(Payment Card Industry Data Security Standard, PCI DSS)。該標準規定會員、商家及服務提供者採取 12 項安全預防措施，以保護智慧卡持有者的資料安全。特別是，PCI 6.3.4 項規定，測試資料庫不得包含正式作業資料的個人帳號 (PAN)。

無論在世界各地，任何產業的企業組織都必須保護員工及客戶的機密資訊，以及企業機密資料和智慧財產。越來越多企業開始瞭解到應用程式環境的安全漏洞。存取控制、鑑別方法，以及網路、應用程式和資料庫層級安全等，這些用來保護正式作業資料的方法也許並不符合保護非正式作業(開發、測試及訓練)環境的獨特需求。

儘管企業付出大量時間和金錢來避免系統受到外部攻擊，但許多企業並未意識到，70%的資料入侵是來自內部人員！¹ 例如，濫用付款卡號與其他機密性資訊的員工，或是將機密資料儲存在筆記型電腦上但該電腦卻被偷或盜用的員工。最後，若將應用程式開發及測試工作外包，就更難控制機密資料的存取了。

保護非正式作業環境隱私權的挑戰

那麼，為何非正式作業環境如此不安全？首先必須瞭解非正式作業資料庫的建立及使用方式。在大多數情況下，若要測試應用程式功能及確保精確度和可靠性，就需要真實資料。

最常見的作法是，直接複製正式作業資料庫複本，來建立測試環境。換言之，就是從安全的正式作業環境，將機密性資訊匯入一或多個不安全的非正式作業環境。非正式作業環境真的需要包含正式作業資料嗎？答案是「否」。雖然好的應用程式測試必須使用真實資料，但「去身分」或遮罩正式作業資料的功能可提供最佳作法，以保護隱私權。

所謂去除身分資料，是指有系統地刪除、遮罩或轉換可用來識別個人的元素。這個過程可讓開發人員、測試人員、訓練人員使用真實資料來產生有效的結果，同時遵守隱私權保護原則。用這種方式篩選或過濾的資料通常可用於非正式作業環境。資料經過遮罩後，即使被盜、外洩或遺失，此資料對任何人來說都沒有意義。

資料遮罩並不簡單！以技術觀點來看，資料遮罩並不是一次性的程序，而是必須符合現有開發、測試及訓練需求。從企業觀點而言，單點解決方案不是最符合成本效益的方法。理想的解決方案必須支援整個應用程式、資料庫、作業系統及硬體平台的資料隱私權遵循。

保護隱私權，降低揭露風險

去除資料的身分元素是保護隱私權及支援法規遵循措施的有效方法，也是公認的最佳實務。IBM® Optim™ Data Privacy Solution 可提供詳盡的功能，去除應用程式資料的身分元素，以便有效用於整個非正式作業環境。您可採取保護隱私權的必要步驟，同時提供開發、

測試、訓練或其他合法商業用途所需的「真實」資料。

Optim 具備可調式資料遮罩技術，可部署到各種應用程式、資料庫、作業系統及硬體平台，以滿足您目前及未來需求。去身分的資料既安全又有效，可用於非正式作業環境。對開發人員、測試人員及訓練人員來說，遮罩後的測試資料仍然有用，且可產生準確、可靠的結果，但對竊取者及駭客而言則毫無意義。若使用 Optim 去除機密測試資料的身分元素，可將外洩風險降到最低，避免竊盜犯案。

落實可靠的資料遮罩技術

若使用 Optim，開發人員及測試人員可採用各種可靠的資料轉換技術，以脈絡正確但經竄改的資料取代機密資料，來產生有效結果。Optim 支援一流的資料庫管理系統，也提供聯邦式存取功能，以便您在單一程序中，從多個正式作業資料來源擷取及遮罩相關資料。

此外，Optim 的「現成遮罩」(mask-in-place) 功能可讓您遮罩使用協力廠商工具擷取的資料，或者是已經在非正式作業環境中的資料。如果企業已經有測試資料，或使用備份類型工具來建立其測試資料庫，則可受惠於 Optim 的「現成遮罩」功能。使用 Optim 直接在來源端遮罩資料，就不必移動資料進行其他處理，而且可以保留資料的參照完整性。

Optim 具備應用偵測能力的遮罩功能，可確保遮罩資料（如名稱及地址）類似原始資料的外觀和操作方式。Optim 可保留資料完整性，並產生一致且有效的結果，以反映應用程式邏輯。例如，可用隨機姓氏（沒有意義的字串）來取代原始姓氏。

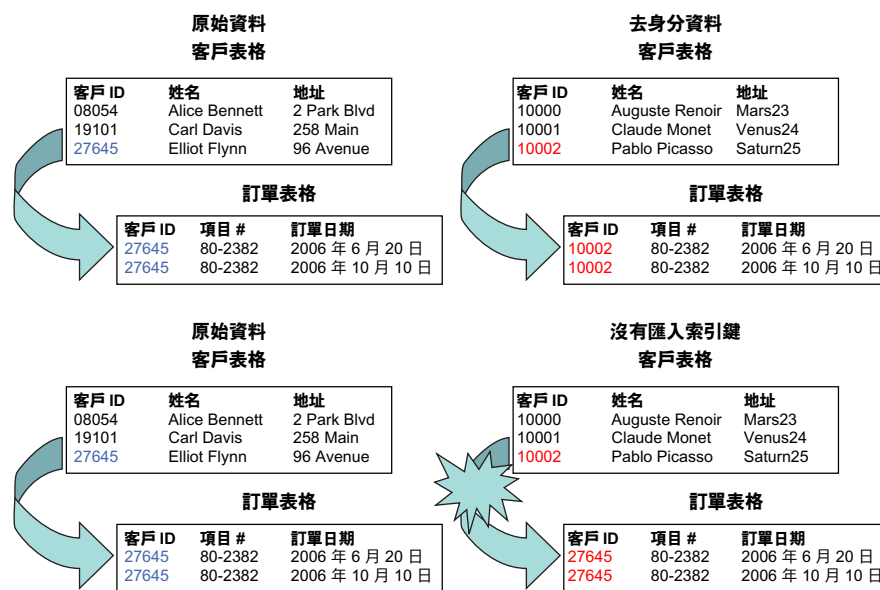
此外，環境定義察覺、預先封裝的資料遮罩常式 (routine) 可輕鬆去除多種機密性資訊的身分元素，如生日、銀行帳號、身分證號碼（如加拿大的社會保險號碼或義大利的稅務編號）、福利資訊、健康保險身分證號碼等。Optim 的部分遮罩技術範例包括：子字串、算術運算式、隨機或序號產生、日期增減或更改，以及連結。

其 Transformation Library™ 常式可準確遮罩複雜的資料元素，如社會保險號碼、信用卡號及電子郵件位址。內建的參考表支援遮罩姓名及地址。您也可以納入特定站台的資料轉換常式，整合多個相關應用程式及資料庫的處理邏輯，並且提供更大的彈性和創意來支援複雜的資料遮罩需求。

前述各種方法都是有效的遮罩資料方法，以確保其機密性。不過，若是關聯式資料庫應用程式，則更加複雜。尤其是，您需要將遮罩資料元素匯入資料庫中所有相關表格，以維護其參照完整性。比方說，如果遮罩資料元素（如

電話號碼）是資料庫表格關係中的主要或外部索引鍵，則必須將新遮罩的資料值匯入資料庫或整個資料來源中的所有相關表格。

匯入索引鍵可確保各應用程式、資料庫及作業環境中，轉換資料的參照完整性。如果沒有匯入索引鍵，母項和子項表格的關係就會中斷，以致測試資料不正確。因此，應用程式測試就會產生不可靠的結果。Optim 的持續遮罩功能可在多個資料來源之間，一致且精確地傳送遮罩取代值，以產生有效的測試結果。



Optim 還可以提供各種各樣的資料遮罩技術，保護專用資訊的機密性。

支援資料隱私權與安全措施

Optim 可提供單一、可調式資料隱私權解決方案，其彈性功能可輕鬆因應您目前及未來的需求。實作 Optim 可協助您遵守資料隱私權法規，並且保護整個企業的機密性資訊。此外，Optim 支援所有一流的企業資料庫及作業系統，包括 IBM DB2®、Oracle®、Sybase®、Microsoft® SQL Server®、IBM Informix®、IBM IMS™、IBM VSAM®、Teradata®、Adabas®、Microsoft Windows®、UNIX®、Linux® 及 IBM z/OS®，您可從中受惠。除了針對所有自訂及套裝應用程式提供資料管理支援，Optim 也支援現今主流的 ERP 及 CRM 應用程式：SAP® Applications、Oracle® E-Business Suite、PeopleSoft® Enterprise、JD Edwards® EnterpriseOne、Siebel® 及 Amdocs® CRM。

關於 IBM Optim Integrated Data Management Solution

IBM Optim Integrated Data Management Solution 可提供可靠的整合性功能，以管理從需求到退役的企業應用程式資料。有了 Optim，團隊即可分享資料成品（如模型、原則及 meta 資料），根據企業目標調整資料管理，並且改善協同作業。如今，各種規模的企業都善用 Optim 來提高效率、簡化資料庫管理、加速應用程式開發，以及使用有效的監管措施。Optim 可以低成本、低風險，提供較佳的商業成果，同時還可提供跨企業應用程式、資料庫及平台的調整功能。

更多資訊

如需更多有關 IBM Optim Integrated Data Management Solution 的資訊，請聯絡您的 IBM 業務代表或造訪：

www.ibm.com/software/data/optim-solutions/



台灣國際商業機器股份有限公司

台北市松仁路 7 號 3 樓

市場行銷處：0800-016-888 按 1

技術諮詢熱線：0800-000-700

© Copyright IBM Corporation 2009

台灣印製

2009 年 4 月

版權所有

DB2、IBM、IBM 標誌、IMS、Informix、Optim、VSAM 及 z/OS 皆為 IBM Corporation 在美國及（或）其他國家的商標或註冊商標。

Linux 是 Linus Torvalds 在美國及（或）其他國家或地區的註冊商標。UNIX 是 The Open Group 在美國及其他國家的註冊商標。Windows 及 SQL Server 為 Microsoft Corporation 在美國及（或）其他國家的註冊商標。其他公司或產品名稱是其個別公司的商標或註冊商標。

本文所提及的 IBM 產品、程式或服務，並不表示 IBM 有意在設有 IBM 據點或有業務的所有國家提供此類產品、程式或服務。

IBM 客戶需負責確保遵循法令規定。客戶本身需向合格的法律顧問諮詢，請其確認並解釋是否有任何相關法令規定可能影響客戶業務，以及客戶遵循法規所需採取之動作。IBM 並不提供任何法律建議，亦不表示或保證其服務或產品將確保客戶遵循任何法律。

¹ Gartner 資深分析師 Richard Mogul 於 2002 年 8 月發表，「Danger Within - Protecting your Company from Internal Security Attacks」。