



軟體 成功案例

IBM InfoSphere Guardium

協助雙和醫院 建立完美合規與免責雙重防線

發佈 2013 - 7 - 01

客戶：
雙和行業：
Healthcare發表國家/地區：
Taiwan

概觀

個資法通過後，儲存大量病歷資料的醫院更不敢輕忽個資外洩或濫用的風險。因此，資料庫安全管理與稽核是刻不容緩的防護措施。

業務需求：

雙和醫院資訊室主任陸偉輝表示，「我們必須把個資安全看得與客戶健康一樣重要，用最嚴謹的防護措施來加以保護。」

解決方案：

IBM InfoSphere Guardium

利益：

1. 採用獨步全球的 Agent 技術，不須改變資料庫或應用程式配置，亦不影響系統日常運作即可部署完成，也能隨系統架構改變而靈活擴充。2. Guardium 平均在 UNIX 平台僅需3%效能、Windows 平台則低於5%，系統負擔低且穩定，適合經常吞吐大量資料的資料庫。3. 「不可否認性」與「資料完整性」兩項設計使其證據能力具有十足公信力。

成功案例

個資法通過三讀後，不僅企業界備感壓力，儲存大量病歷資料的各級醫院也不敢掉以輕心。這些病歷紀錄不僅事關病患隱私，一旦有個資外洩或濫用的風險，醫院所要負擔的賠償恐怕遠超過自身所能負荷！

根據報載，國內知名保險業者因評估難以滿足個資法要求，決定終止電話行銷業務，可見企業寧可損失部分營業額，也不願承受無法控管的個資風險。然而醫院肩負照護病人健康的社會責任，不可能採取同樣的作法。

「合規與免責，是醫院保護客戶、保護自己的雙重防線！」臺北醫學大學、署立雙和醫院資訊室主任陸偉輝表示，「我們必須把個資安全看得與客戶健康一樣重要，用最嚴謹的防護措施來加以保護。」

守護個資，從資料庫做起

根據統計，資料外洩事件有75%來自資料庫伺服器，而且當個資爭議發生時，資料庫系統稽核報告也將成為責任判別的依據。資料庫安全管理與稽核，是刻不容緩的防護措施。

陸偉輝主任指出，在評估資料庫安全解決方案時，雙和醫院資訊團隊訂立五項重要指標：品牌與口碑、即時防護能力、免責舉證力、導入與擴充的便利性、運作效能。

經過多方比較，IBM InfoSphere Guardium 在五大指標均有優異表現，再加上過去導入IBM Power System 伺服器作為醫院核心資訊管理系統，IBM 的專業度與支援能力都令 IT 團隊感到滿意。因此，雙和醫院經過嚴謹評估後，決定採用 InfoSphere Guardium 作為資料庫安全防護與稽核的守護者。

Guardium 獲 Forrester Wave 最高評價

全球權威市調機構 Forrester 針對市面上所有資料庫安全監控管理解決方案進行評比，在「The Forrester Wave™: 資料庫稽核與即時防護」(The Forrester Wave™: Database Auditing And Real-Time Protection, Q2 2011)報告中指出，IBM 是該領域中的領導者，在產品面、策略面、市場面共17項指標中，每一項都高居榜首，最高評價實至名歸。

此外，全球前五大跨國銀行、20家電信業領導者、兩大最受歡迎飲料品牌與知名防毒軟體公司 McAfee.com 等都選擇 InfoSphere Guardium，「資安解決方案講求實績；」陸偉輝主任表示，「最重視資安的銀行與電信業者的選擇，等於幫我們做了最好的篩選。」

全生命週期，完整即時防護

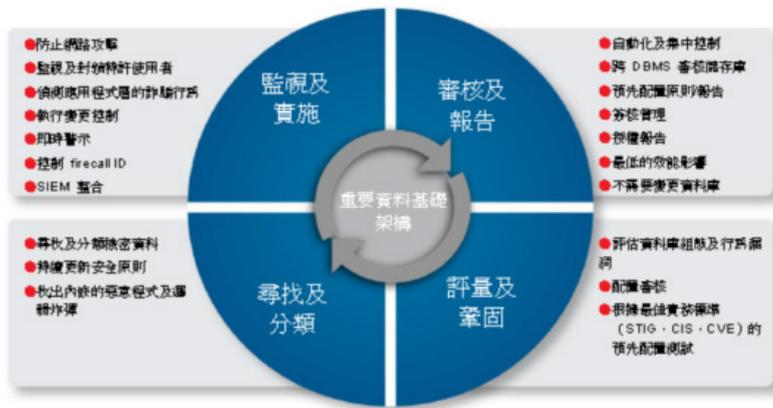
IBM 產品協理胡育銘說明，InfoSphere Guardium 的設計是從全生命週期的進行資料庫安全管理：

一，尋找及分類：組織長期累積的龐大數位資料，InfoSphere Guardium 可自動探索與分類，找出機密資料儲存位置並強制套用安全規則。

二，評量及鞏固：安全評量功能會根據 CVE、CIS、STIG 等業界最新標準，掃描資料庫基礎架構，找出系統配置與使用者行為中的潛在漏洞，並提出強化建議，建立資安基準線。

三，監視及實施：InfoSphere Guardium 具備強大的監控能力與完整安全原則管理，可即時監測並主動控管未獲授權的可疑動作、外來攻擊與詐欺行為、基準線異常變更、特許使用者異常行為等。儀錶板可呈現完整「who, what, when, where, how」監控記錄，以及自動化安全事件工作流程，以符合法規遵循。

四，審核及報告：以連續而精細的方式追蹤所有資料庫活動，跨 DBMS 儲存審核資料以確立職權分立的監管制度，並讓法規遵循報告與監管程序全面自動化。



圖說：IBM InfoSphere Guardium: 一個解決方案，滿足全生命週期的資料庫安全與法規遵循

獨步全球 **Agent** 技術，安全與效能兼具

InfoSphere Guardium 與其他解決方案最大的不同之處，在於採用了獨步全球的 **Agent** 技術，與他廠以封包為基礎的技術有著本質上的差異。**Agent** 技術採取非侵入性的即時監控，不須改變資料庫或應用程式配置，亦不影響系統日常運作即可快速部署完成，未來也能隨系統架構的改變而靈活擴充。

相較於他廠解決方案動輒占用10%-15%系統效能，InfoSphere Guardium 平均在 UNIX 平台僅需3%效能、Windows 平台則低於5%，系統負擔低，運作更為穩定順暢。對於經常吞吐大量資料的資料庫系統，效能差異將會嚴重影響業務運作與使用者體驗，這項輕量化優勢使得 InfoSphere Guardium 受到全球企業青睞。

「舉例來說，Guardium 就像是高速公路上的攝影機，拍下經過的每一台車子，立即傳送到獨立監控系統去比對與應變；且不會因為攝影機壞掉而造成交通阻塞」IBM 產品協理胡育銘說明，「他廠解決方案就必須占用車道、把每一個台車攔下來檢查拍照，效能差異顯而易見。」

完整證據力，確保企業免責

個資法規定，當有個資爭議發生時企業必須負舉證責任以證實沒有疏失。因此，資料庫安全管理系統所提供的稽核報表，成為企業自保的最後一道防線。為確保稽核報表證據力，InfoSphere Guardium 提供層層防護機制：

- 具「不可否認性」的稽核資料：職權分立機制，將稽核資料儲存於多個不同的實體與虛擬裝置中，任何人均無權篡改。
- 三層式架構的使用者追蹤：完全對應應用伺服器使用者資料與 database session 及 SQL 資訊，為全球唯一100%完全正確追蹤使用者的解決方案。
- 資料完整性設計：**Buffer** 機制在網路忙碌或中斷時可先暫存交易資料，網路恢復後立即續傳到稽核資料庫，不漏失封包，確保稽核資料完整。
- 高可用性與附載平衡設計：無論發生天災人禍、或資料庫交易附載過大，都能夠透過備援或分散式收錄來確保稽核資料完整無缺。

陸偉輝主任認為，「不可否認性」與「資料完整性」這兩項設計使其證據能力具有十足公信力，「若企業被質疑洩漏個資、或特許使用者與管理者被質疑有異常行為時，Guardium 的稽核資料將是保護雙和醫院與 IT 管理者、證明行為合規的重要證據。」

面對日新月異的資安風險，以及個資法嚴格的合規與舉證要求，雙和醫院已經做好完全準備，在 IBM InfoSphere Guardium 的把關下，不僅能即時守護客戶資料安全，並能在必要時刻提出完美無缺的稽核證據，保護企業權益！

(採訪於2013年)

文件選項

[列印此頁](#)