# 淺談資料庫安全

蕭正立 / 財金資訊公司研發部規劃組高級工程師

## 一、前言

隨著新版「個人資料保護法」(以下簡稱個資法)與「金融監督管理委員會指定非公務機關個人資料檔案安全維護辦法」相繼公告施行後，正式宣告政府明確要求金融相關產業對於個人資料(以下簡稱個資)安全相關議題，由原本的道義保管責任大幅提升為法定保護義務。對一般企業而言，其所持有的機敏資料愈多，相對在資料的蒐集、處理與使用過程中所承擔的風險亦愈高，而金融業務相關服務系統，其交易過程因涉及許多客戶資料，故須妥善規劃並落實個人資料之存取控制、保護及監控措施，以善盡個資防護之責。

由於資料在傳輸、儲存與操作的過程中，均可能面臨遺失與外洩的風險，因此要確保資料安全必須從資料產生、儲存、修改、備份直至刪除，亦即於其生命週期的各個階段，搭配運用各種資安技術與工具，以管控並保護企業所持有的機敏資料。現行多數企業之營運系統架構，仍以建置集中儲存於資料庫之資料中心，以提供其關鍵業務系統之查詢與存取需求，換言之，當大部分的機密資料集中儲存在資料庫中，益發使得資料庫日漸成為主要的攻擊目標，這或許也可以解釋歷年來多數資安事件統計中，為什麼 SQL (Structured Query Language) 隱碼攻擊的惡意攻擊次數年年激增，且排名居高不下，由此可知，保障資料庫安全是企業組織因應個資法首須正視的重點之一。

## 二、資料庫安全之威脅

近年來，資料庫遭駭客入侵的事件時有所聞，其結果不外乎造成機敏資料外洩、資料庫損毀、服務中斷…等，亦致使企業組織之信譽及營收受損。顯見當資料庫相關系統管理人員未能確實做好資料庫安全管控規劃與稽核作業，將使資料庫暴露於被攻擊的高風險之下。

從資訊安全概念架構(如圖 1 所示)中可得知，資料庫除存放資料外，亦有使用者身分、權限、稽核…等相關安全機制可供設定，以確保其穩定運作。因此，大多數企業或組織普遍認為只須強化部署防火牆、入侵預防系統 (Intrusion Prevention System，IPS) …等防護機制，即可有效阻絕駭客攻陷後端資料庫。倘若此舉真為萬無一失之防駭措施，何以每年仍有逾億筆資料外洩之情事？

根據美國資訊安全公司 SafeNet 所發布的 2013 年企業資料外洩研究報告所載，造成資料外洩的原因有高達 57% 係來自外部之惡意程式(如暗藏的惡意程式碼、惡意的外部連

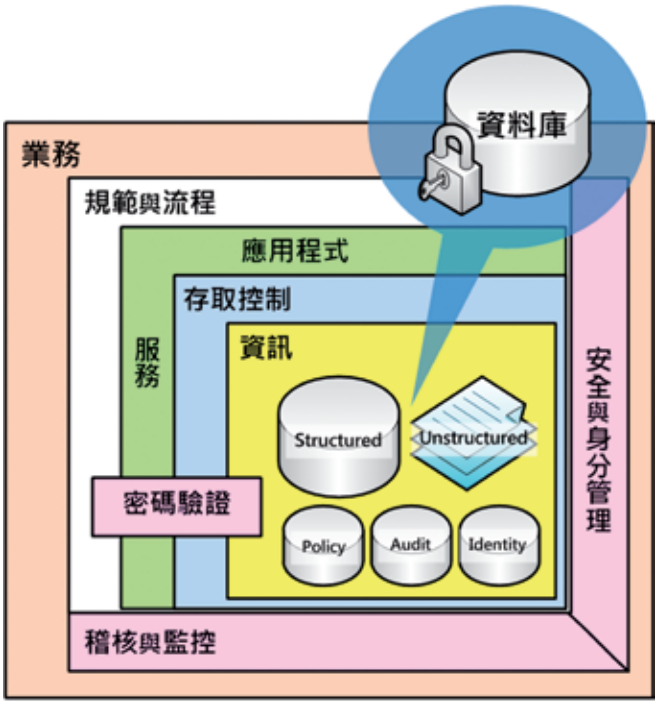


**圖 1　資訊安全概念架構**

( 資料來源：Oracle (April 2011))

結等 )，27% 為意外，13%為內部人員洩露，而真正遭外部駭客成功入侵，導致資料外洩者僅有 2%，至於組織級攻擊行動，如進階持續性滲透攻擊 (Advanced Persistent Threat，APT)，更未達 1%。這說明了在竊取資料技術日新月異的今天，須兼顧由企業內外存取資料的各種管道，才能使資料外洩風險降至最低。資料庫安全常見威脅來源如下：

### (一) 權限管控不當

當使用者被授予超出其所被定義的工作職掌時，此資料庫帳號權限便存在被用來執行未經授權的不當資料操作或破壞資料庫的風險。

### (二) 濫用合法授權

使用者有可能濫用合法授予的資料庫權限，進行未經授權之資料處理，例如經由應用系統查詢介面蒐集資料庫機敏資料，彙整後非法攜出。

### (三) SQL 隱碼攻擊

惡意使用者利用資料庫合法之查詢通道或系統介面，以遂行其非法取得資料、惡意破壞資料 ... 等目的。一般的做法是利用 Web 應用程式介面，在 SQL 查詢指令的輸入字串中，夾帶其他惡意或未經授權的 SQL 指令來入侵資料庫。

### (四) 惡意軟體滲透

惡意軟體包括病毒、蠕蟲、特洛伊木馬程式 ... 等惡意程式碼，為近年最熱門的入侵方式。具破壞性惡意軟體會利用網路通訊工具進行散佈，包括透過電子郵件與即時通訊傳遞，或者誘使使用者從釣魚網站載入木馬程式。惡

意軟體也會嘗試利用作業系統或資料庫系統所存在的漏洞，滲透企業系統或設備，以秘密收集使用者個人隱私及企業資料，而通常使用者多已遭惡意軟體感染而不自知，成為入侵者非法取得資料的代理人。

### （五）稽核軌跡不全

存留稽核軌跡的重點在於能夠在資料存取流程中，正確且有效地記錄進行資料操作的使用者、資料庫物件、資料存取動作及執行時間…等資訊，以便在異常事件發生時，可藉由此紀錄分析發生原因。在實務執行面上最大的挑戰在於稽核功能開啓後對資料庫存取效能的影響，以及資料庫稽核紀錄不易與前端稽核資訊進行勾稽。

### （六）備份資料遭竊

大部分企業對於資料庫備份儲存媒體常是疏於加密保護的，大多源於認為備份檔不過就是當資料庫毀損時，用以執行資料回存復原使用，就算遺失也應無法讀取備份檔內容。事實上當有心人取得資料庫備份檔，是有可能將資料庫還原到異機，以順利取得原資料庫中所存放之機敏資料。

### （七）資料庫安全漏洞

常見企業之資料庫未曾安裝任何修補程式、資料庫所建立預設帳號與密碼未刪除，或者所使用預設參數設定未修改，這些公開的資料庫安全漏洞均可能成為嘗試入侵資料庫者的攻擊點。

### （八）機敏資料管理失當

部分企業為求測試情境趨近實際營運環境，逕將營運資料匯入測試資料庫，此舉將使機敏資料暴露於權限未確實管控的環境中，相對亦導致資料遭竊的風險。

### （九）拒絕服務攻擊 (Denial of Service，DoS)

此類攻擊是針對提供特定服務之主機，執行大量且合法的操作請求，意圖占用大量網路頻寬及系統資源，以期造成資料庫主機資源耗盡及服務中斷之狀況。

### （十）資安專業知識不足

許多企業在資料安全防護的策略規劃與處理能力上，並未隨著其業績獲利與營運資料的成長而提升，加上對內部員工亦疏於加強資安知識宣導與專業培訓，均為資料安全之潛在威脅。

## 三、資料庫安全之防護策略

全球最具權威的IT研究與顧問諮詢公司－Gartner公司針對資料庫安全措施，為企業組織提供治理策略之建議，期協助擬定正確之資安策略。Gartner將資料庫安全治理策略（如圖2所示）分為三大部分，其下各再細分為三種解決方案，摘要說明如下：

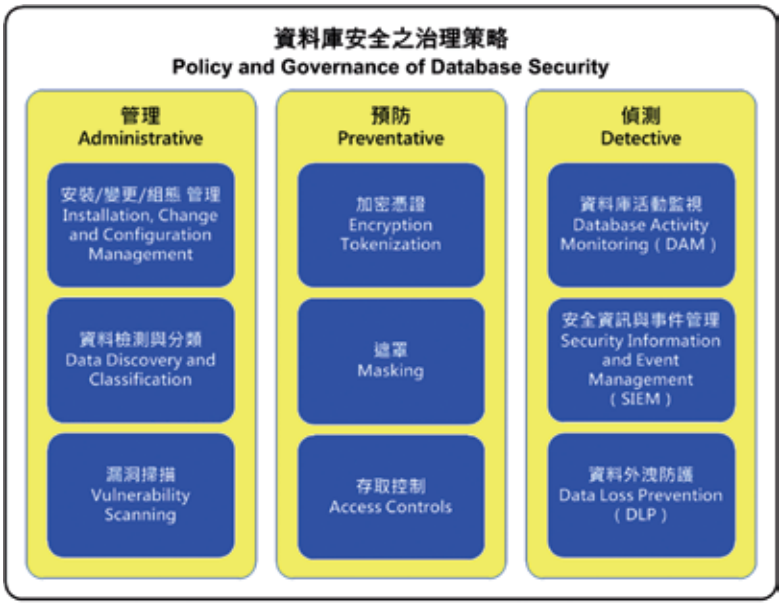


**圖 2　Gartner 資料庫安全模型**

( 資料來源：Gartner, November 2011)

### (一) 資料庫安全管理措施

#### 1.　安裝、變更與組態管理

資料庫系統的預設安裝程序，僅有部分安全性提醒，應於完成安裝後，參照資料庫廠商所提供的安全指南 (Security Guidelines) 逐步調整，使資料庫建置成為安全防護的第一步。實作評估要點如下：

(1) 於各層面強化資料庫系統，依使用功能定義其安全性設定，並規劃修補程式檢核與安裝程序。

(2) 整合資料庫管理系統至企業整體安全威脅與漏洞管理流程。

(3) 制定關鍵業務系統之版本控管作業流程。

#### 2.　資料檢測與分類

確實掌控營運資料的存放所在與安全分類，以界定機敏資料之範圍，是防護資料庫的重要先決條件。實作評估要點如下：

(1) 檢測企業 IT 環境中所有資料庫管理系統，並明確定義其角色屬單機系統或為業務系統的一部分。

(2) 找出資料庫中所存放之關鍵機敏資料，並因應業務需要與法定管理規範，分析定義需要被保護的資料類型。

(3) 落實資料庫個資檢測與盤點作業，可充分利用如資料庫個資盤點工具，查找機敏資料所存放於資料庫中之資料表及其欄位，以提高資料庫安全防護的正確性與完整性。

#### 3.　資安漏洞掃描

漏洞掃描工具是資料庫安全威脅與弱點防範的重要環節，能使用主動或被動之機制，對資料庫進行攻擊與探測，找出已知的漏洞、常見的錯誤配置…等弱點。實作評估要點如下：

(1) 優先考量使用企業現有之弱點掃描工具，執行資料庫漏洞掃描。

(2) 評估掃描報告之正確性，以決定是否採用專屬之資料庫漏洞掃描工具，並確保可執

行後續之修補程序。

(3) 落實執行資料庫弱點掃描，以協助建構資料庫變更與組態安全管理目標。

## （二）資料庫安全預防措施

### 1. 加密與憑證保護

大多數企業皆將資料庫加密機制視為資料庫安全防護的最終選擇，主要原因不外乎加解密過程可能造成資料庫運作效能負擔，但面對外部攻擊或內部使用者竊取之風險，任何措施均未能防堵資料外洩之可能性，故利用加密金鑰進行機敏資料加密處理，並配合妥善的帳號與權限控管，實為捍衛資料庫安全之最終極防線。實作評估要點如下：

(1) 審慎評估資料庫系統廠商或資料庫安全解決方案供應商所提供之資料加密解決方案，確實規劃對資料庫效能及應用系統修改之影響程度最小之加密方式，如透通資料加密 (Transparent Data Encryption，TDE) 機制。

(2) 在測試環境充分測試資料加密機制，以確保應用程式執行結果之正確性，並教育相關系統使用者瞭解加密工具之預期效益及其限制。

(3) 針對被定義為主鍵 (Primary Key) 或索引 (Index) 鍵之敏感性資料欄位加密，如信用卡號碼、身分證號碼…等，可評估採用標記化 (Token) 機制產生與原資料相同格式之代碼，以對應原資料加密後之密文，避免資料庫加密的效能問題。

### 2. 資料遮罩

資料遮罩 (Data Masking，DM) 技術是將機敏資料去識別化，有助於防範未經授權使用者檢視完整資料內容，通常為對個資防護要求較高的法律規範所建議使用之方式。可分為靜態與動態遮罩兩種方式，實作評估要點如下：

(1) 開發或測試環境建議採用靜態遮罩 (Static masking) 方式，將實際已去識別之敏感性資料存入資料庫，俾供測試使用。

(2) 營運環境則建議使用動態遮罩 (Dynamic masking) 技術，針對 SQL 指令中所查詢之敏感性資料，進行即時且動態的資料遮罩處理後呈現。

### 3. 存取控管

資料庫存取控管為資料庫安全防護最基本的預防措施，應就所有資料庫使用者之工作角色進行明確之定義，以期達成「僅授予最小且必要權限」之目標。實作評估要點如下：

(1) 建置邏輯之網路區隔或分層系統架構，並配合於資料庫層落實權限控管，以防範未經授權之連線登入資料庫存取資料。

(2) 規劃資料庫管理者之例行監控或維護作業流程，亦可限制使用者連線至資料庫所使用之工具軟體。

(3) 搭配身分識別與存取管理系統 (Identity and Access Management，IAM) 明確定義資料庫角色，並定期檢視角色成員之連線狀況，以確保相關使用者權限符合其工作要求。

## （三）資料庫安全偵測措施

### 1. 資料庫活動監控 (Database Activity Monitoring，DAM )

根據美國資安訓練與認證公司 SANS Institute 於 2008 年所公布的「Understanding and Selecting a Database Activity Monitoring

Solution」報告中定義：資料庫活動監控係指「即時擷取資料庫所有成員 ( 含資料庫管理員 ) 之資料存取動作，並可針對違反政策之行為發出警示」，是近期因應法規要求下最受關注的一環。實作評估要點如下：

(1) 評估導入 DAM 以減低資料庫漏洞遭入侵之高風險，並將資料庫存取活動稽核紀錄妥善存放於資料庫之外。
(2) 當有即時且完整監控資料庫之必要，或者資料庫本身的稽核機制不被接受時，應考慮導入 DAM 技術。
(3) 針對特殊權限用戶，DAM 可將其所有資料庫存取動作完整納入監控與稽核，且可建立其正常維護行為之限制。
(4) 評估導入 DAM 須考量其對資料庫效能之影響，以及須否具備稽核本機登入行為功能，並視需要選用納入資料庫防火牆功能之產品。

2. **安全資訊與事件管理**
(Security Information Event Management，SIEM)

SIEM 技術具備兩項主要的資料安全管理功能：(1) 日誌管理，含資料收集、分析與報表…等功能；(2) 安全事件管理，處理資安設備、網路設備、系統、應用程式…之訊息，並即時提供安全監控、事件關聯及事故反應。實作評估要點如下：

(1) 導入 SIEM 須考量企業對日誌管理、資源存取監控、事件反應、相關報表…等需求，以及產品本身的事件管理能力、系統建置成本及與應用程式架構的整合性。
(2) 配合 SIEM 導入其他監測解決方案，或者評估將現有 DAM 訊息紀錄納入 SIEM 中整合處理。

3. **資料外洩防護**
(Data Loss Prevention，DLP)

目前 DLP 技術以內容感知 (Content-Aware) 為主流，佈署於網路閘道端進行資料過濾，以監測、辨識、過濾、阻斷…等功能，防止授權之使用者將資料庫中未加密的敏感資料，直接或轉存為其他檔案格式，透過網路外流至用戶端或其他儲存設備。實作評估要點如下：

(1) 企業評估導入 DLP 產品前，應依資料安全之實際需求，明確制定資料外洩防護策略。
(2) 瞭解 DLP 產品應用於資料庫系統的局限性，DLP 主要係以識別資料防範資料外洩，而非直接辨識 SQL 指令；可定義資料庫及其需保護的資料表欄位，並設定過濾條件為判別依據，便可即時且有效防止資料外洩。

## 四、現況說明

財金資訊股份有限公司 ( 以下稱財金公司 ) 為我國金融資訊與跨行交易處理樞紐，除提供金融機構與社會大眾便利的金融資訊服務外，更要確保交易作業環境的穩定與相關資料的安全性。因此，為妥善保護交易資料安全，已陸續完成多項資料庫安全防護規劃，並依實施狀況及作業需求逐步調整，以期在兼顧安全與效能的原則下，有效降低機敏資料外洩之風險。財金公司資料庫相關安全管理政策簡要說明如下：

### （一）現行措施

1. 依各承辦單位作業分工區分權責，研發部門提供作業程序，經安控部門測試完成後，始可依權責申請授權至營運資料庫執行作業。
2. 營運系統相關作業均須填具表單經申請、覆核、主管核准，並經跨部門審議後，指派及授權專責人員執行。
3. 內部網路規劃實體區隔，OA 網段無法直接連線至營運網路區段，相關資料庫之變更維護作業僅可於特定端末室登入執行。
4. 架設防火牆，限制對資料庫主機之網路連線；另，資料庫主機設定為限制僅特定 IP 可連線存取。
5. 所有營運資料庫角色皆經明確之定義，個人帳號須經需求單位填單申請並經核准後，授予「最小且必要」之權限。另，定期進行帳號權限清整，以確保各帳號之權限與作業需求相符。
6. 關鍵營運系統之資料庫均啓用資料庫稽核功能，記錄資料庫授權使用者之資料存取動作，並定時彙整紀錄，以檢視違規之人員與操作行為。
7. 於營運資料庫與特定端末設備間架設資料庫遮罩系統，扮演資料庫代理伺服器角色；即當使用者以特定端末設備執行查詢時，於中途攔截改寫其 SQL 指令，依預先定義之規則，將所查詢之敏感性資料欄位以動態遮罩技術進行去識別化處理後，始呈現至前端。
8. 配合定期弱點掃描，如發現資料庫漏洞問題，則規劃安裝資料庫修補程式，依序於開發、測試環境驗證無誤後，再安裝於營運資料庫環境。

### （二）評估中方案

1. 已完成 ORACLE 與 SQL Server 資料庫透通資料加密機制 (TDE) 與 SafeNet ProtectDB 資料庫加密測試，現仍於評估階段。
2. 已完成 ORACLE 資料庫 Recovery Manager 加密備份及解密復原測試，現仍於評估階段。
3. 已完成 IBM InfoSphere Guardium 與 iMPERVA SecureSphere 資料庫活動監控測試，現仍於評估階段。

## 五、展望未來

近年資訊界最被熱烈討論的三大議題乃物聯網 (The Internet of Things)、雲端儲存 (Cloud Storage) 與巨量資料 (Big Data)，而隨著雲端時代的來臨，大量且快速產出的多元化資料即脫穎而出。這些巨量資料的處理要點為「儲存與運算」，先有具備「存取、分享、同步」功能的雲端儲存架構，再發展各項雲端運算應用供客戶端使用。一旦資料儲存於雲端，不僅方便內部存取，更易於與外部分享，然而外洩風險亦相對增加，這意謂著雲端資料庫除須滿足儲存、運算、分析…等需求外，安全議題的重要性也隨之提高。

傳統的資訊安全防護機制與設備，無法有效監控雲端環境所發生的事件，更遑論發生問題時，提供即時偵測與阻擋機制。故為作業周延計，雲端環境的資料安全防護設計，應包含「認證授權」、「資料加密」與「管理監控」三個面向，整合帳號認證系統，以管理權限授予、群組分派與儲存空間，強化使用者的安全保障；至少須對帳號密碼、資料儲存與傳輸進

行加密；亦須支援可設定限制流量與頻寬之管理機制，以提高安全等級。

所謂「資料之所在，商機之所在」，金融業當然不至於自外於此趨勢，在財政部的雲端計畫中，財金公司扮演提供「金融雲」服務的角色之一，故此，財金公司必當以多年所累積之系統維運經驗，建構安全、穩定與便捷之雲端資料儲存環境，與金融機構齊力守護雲端資料安全，使社會大眾更有信心地邁向未來生活的資訊環境。

## 六、結語

資料安全防護一直是企業不斷努力、希望達到的目標，不僅僅是被動地遵循法律規範，更應主動善盡資料保護之責任。但許多企業在評估導入資料庫安全措施時，卻因考量對資料庫效能的影響而猶豫不決，未能清楚認知網路環境所面對的挑戰是－在未知的地方，有著未知的人，以未知的方法，在未知的時間點，意圖對企業發動威脅或持續攻擊，藉以竊取資料或癱瘓服務，然現今並無任何單一技術可解決所有資訊安全的問題。

綜此，企業應盡最大努力降低資料外洩風險，分由技術面及管理面推動，先制定政策後評估導入工具，盡力做到所謂「4H 管理」－「Who did What at When and Where」，確實掌握資料庫存取活動的人、事、時、地、物等關鍵資料，並從資安的徵兆或事件中持續補強，加強資料庫系統的縱深防禦機制，以落實「事前管理預防、事中偵測阻斷、事後改善強化」的資訊安全治理策略，確保及持續提升資料庫與機敏資料的安全性。

※ 參考文獻 / 資料來源：


1. 美商甲骨文網站，www.oracle.com。
2. 台灣微軟網站，www.microsoft.com/zh-tw/。
3. 維基百科網站，en.wikipedia.org。
4. Establishing a Strategy for Database Security Is No Longer Optional (Jeffrey Wheatman, 2011, Gartner)。
5. Top Ten Database Threats (2013, Imperva)。
6. 資料庫保護解決方案停看聽 企業如何選擇？( 于子欣，2013，資安人 )。
7. 企業級資料庫資安維護解決方案 ( 陳擎民，聚碩資訊 )。
8. 以 8 步驟全方位保護資料庫 (Dr. Ron Ben Natan, 2010, IBM Guardium)。