企業資安全五術．破敵寶典

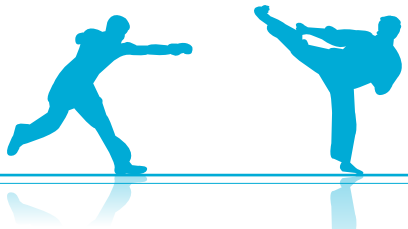
成就企業資安無敵手的IBM五大修鍊

內外兼修、實戰豐富

您最佳的資安戰友選擇－IBM

榮獲SC Magazine頒發「2010年最佳安全公司（Best Security Company）獎項」的 IBM，擁有超過40年的資訊安全研發和創新經驗，在全球各地擁有9個創新資訊安全技術研究實驗室及9個安全營運中心，以提供內容豐富又完整的資訊安全系列解決方案，協助客戶全面因應法規遵循、應用程式、資料、身分與存取管理、網路、威脅預防、系統安全、電子郵件、加密、虛擬化與雲端安全的需求，無論在深度或廣度上，都是您最佳的資訊安全戰友選擇！

SC MAGAZINE AWARDS 2010 WINNER
Honored in the U.S.



當資料如巨浪般一波一波拍打上岸，網路惡意行為如魅影般飄忽不定，行動介面、雲端服務不斷挑戰既有資安防線，政府法令又如緊箍咒般越唸越緊，而您還在堅守傳統思維下的資安解決對策嗎？

就如同把李小龍放到今天的時空，只怕也無法單憑昔日一副雙節棍繼續威震江湖。企業資訊安全在面對雲端運算（Cloud）、行動商務（Mobility）、社交商務（Social Business）、海量資料（Big Data）等質化與量化的巨幅變革，也唯有全方位的周密對策才能防範日益複雜的資訊安全威脅。

該是您全面檢視資訊安全對策，甚至改弦易轍的關鍵時刻了！讓精研企業資訊安全問題最為透徹的 IBM，協助您專注在當前企業資訊安全最核心的五項修鍊，以現代全五術的非凡身手，成就企業資安無敵手！

企業資安全五術・破敵寶典

群敵環伺．危機四伏

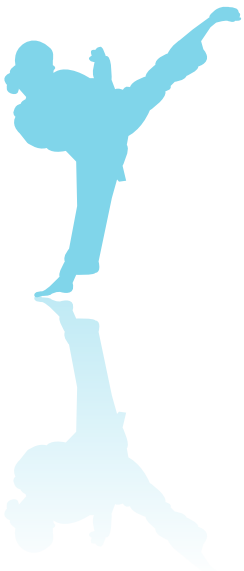
不容輕忽的企業資訊安全現況

第一章

當您的招式漏洞百出
別指望對手大發慈悲

2011年年中，IBM X-Force資安研發小組在所發表的年度《趨勢與風險評估報告》中，為該年下了一個聳動的註腳－「安全漏洞防護年」！這不僅因為2011年是在近乎每日爆炸性新增的安全漏洞案例下展開，而且大多數的受害者對這些新生的安全漏洞根本束手無策，毫無任何抵禦能力！

這樣的結果其實一點也不讓人意外。雲端運算（Cloud）、行動商務（Mobility）、社交商務（Social Business）、海量資料（Big Data）種種近乎革命性的企業經營變化，使企業基礎設施的範圍日益擴增，甚至沒有限制。另一方面，資安攻擊技術也愈來愈精密，惡意人士在攻擊前早已廣泛收集情報、做足了功課。換言之，企業所曝露的安全漏洞數量越來越多、次數越來越頻繁，而攻擊者的狡詐與火力卻是越來越高段、越凌厲。企業倘若毫無警覺與因應作為，結果自然是不言可喻。



IBM X-Force資安研發小組針對範圍廣大的電腦安全威脅及弱點，進行發掘、分析、監控及記錄，並從中歸納出當前企業資訊安全最令人憂心的風險：

- 駭客最喜愛的攻擊方法為資料隱碼（SQL injection）攻擊與對密碼、資料庫及Microsoft Windows檔案夾/磁碟共用的窮舉式攻擊（brute forcing）。駭客會掃描網路上的開放式服務（open services），找出是否有漏洞或弱點，趁勢入侵。
- 依2011年開始至第三季的數據顯示，軟體有重大漏洞之資安事件的數目已超過2010年同類事件的總數，重要企業級軟體產品因此在遠端執行程式碼上產生嚴重問題。
- 文件閱讀器與多媒體播放器漏洞大量增加。駭客攻擊以各種不同瀏覽器執行軟體的消費者，使得有特定軟體漏洞的受害者人數達到新高。
- 678家「財星雜誌500大」公司的網站及熱門網站中，有40%網站的客戶端有JavaScript漏洞。

簡單而言，傳統單點式、終端用戶佈防的資安架構思維，已經難以勝任資安攻擊者透過網路瀏覽、電子郵件、行動裝置、雲端服務…所發動的全面性入侵。IT人員不能再沿襲以往「頭痛醫頭、腳痛醫腳」的資安維護模式，必須快速提升企業資安問題的策略價值，從整合的至高點全盤檢視、佈局資安防線，才能完善結合不斷創新的商業模式，把任何蓄意來犯的明槍暗箭打得落荒而逃！

個資法細則步步進逼
守住要害莫輕敵

繼2010年4月立法院三讀通過「個人資料保護法」後，眾所矚目的施行細則草案也在2011年10月由法務部公告於官方網站。儘管仍有若干行政程序待完成，但各方一致認為2012年將是新法上路的確切時程。

新版個資法由於管轄範圍廣、規範內容嚴、舉證責任大、連坐罰責重，對企業資訊安全系統而言，勢必形成巨大的考驗壓力。企業資安規劃絕對無法漠視它所帶來的營運衝擊，務必要深入瞭解施行細則要點，嚴守要害以防中招。

告知從寬．舉證從嚴

新版個資法施行細則第13條規定：「告知之方式，得以書面、電話、傳真、電子文件或其他適當方式為之。」法務部法律事務司副司長鍾瑞蘭表示，只要能做到「一對一」，即符合告知義務。但不論何種告知方式，企業最終都必須擔負舉證義務，提出相對應的證據。

資料外洩．即時告知

為使個人資料發生被竊取、洩漏、竄改或其他侵害者，能即時通知當事人，並兼顧個人資料權益保護與通知效率，規定公務或非公務機關需依法即時通知當事人，告知個人資料被侵害之事實及已採取之因應措施。

安全維護・企業有責

明文規定公務機關或非公務機關為防止個人資料被竊取、竄改、毀損、滅失或洩漏，應採取技術及組織上之必要措施，以善盡適當安全維護之責。而企業投入這些必要措施的成本，以所須支出之費用與所欲達成之個人資料保護目的符合適當比例者為限。

委外業務・善盡監督

委託他人蒐集、處理或利用個人資料，委託人負有適當監督之責。除了定期確認受託人對個資的保護措施狀況，還要將確認結果予以記錄。同樣的，受委託的外包廠商也需在受委託期間善盡安全維護之責。

由此可見，新版個資法帶給企業的資訊安全考驗，絕不容您掉以輕心。而隨著施行細則正式頒佈的時間越來越逼近，您也該加速因應新法上路的資安規劃步伐！

四大宿敵聯手踢館
攘外安內費思量

捍衛企業資訊安全任務之所以艱鉅，就在於它必須關注的面向既深且廣，而且還得不時接受來自各種創新商業模式的挑戰。例如，當業務行銷人員振奮於行動商務或社交商務的蓬勃時，IT人員也同時在為解決層出不窮的資安風險絞盡腦汁。而現階段困擾企業最鉅的資安挑戰，正是來自網路犯罪、行動裝置、雲端服務與法令規範四大課題。

網路犯罪變本加厲，考驗資安防禦力

網站被惡意竄改或入侵、資料外洩以致個人隱私全都露、系統被駭導致服務中斷…已是屢見不鮮的新聞，尤其隨著網路犯罪的產業化與集團化，犯罪手法與頻率更是變本加厲。企業風險顧問公司Kroll的「2010年度全球詐欺報告（Annual Global Fraud Report）」指出，企業的資訊或電子資產遭竊盜的比例已由2009年的18%倍增到2010年的27.3%，相對地，實體偷竊則從2009年28%微幅下降至2010年的27.2%，顯見電子竊盜正取代傳統的實體偷竊。

行動裝置蔚為風氣，考驗資安應變力

隨著智慧手機、平板電腦等行動裝置快速普及，行動介面的應用性也日趨廣泛，未來更將衍生出可觀的行動商務。既然企業無法置外於行動世界的連結，資安罪犯們當然也不會放過任何入侵的可乘之機。企業如何在張開雙臂擁抱行動新商機的同時，展現高度的資安應變力，將是一門越來越關鍵的課題。

雲端服務千變萬化，考驗資安創新力

根據 IBM Market Insights、Cloud Computing Research調查顯示，近7成受訪者對公共雲服務最大的疑慮就是資料安全與隱私，其次才是服務品質。雲端運算必須共用大規模的基礎設施，相同運算資源必須支援來自不同公司的使用者交互存取，使安全問題變得更複雜，導致提高錯誤組態和惡意行為的發生率。雖然許多企業都認為雲端運算的安全風險更高，但若能善用雲端運算的標準化、自動化，以及對IT基礎架構掌握度的透明化，何嘗不是重新提升資訊安全水準的契機。

個資新法門檻墊高，考驗資安執行力

新版個人資料保護法施行細則頒佈之後，企業對付外部駭客攻擊以及預防內部資料洩漏的執行能力，將被嚴格檢驗。 IBM專家建議，企業針對個資法可採取評估個資外洩風險、建立符合需求的個人資料保護系統等兩大措施，建構企業安全平台來證明「無故意或過失責任」的免責。值得注意的是，除了個人資料，營業秘密也是企業必須併入生命週期防護架構的重點，一次做好完整的防護，避免直接且立即性的營業損失，甚至傷害企業競爭力及市場優勢的隱憂。

如您所見，影響企業資訊安全的風險因素複雜且隨時在變化，並沒有任何單一而簡便的方法可以「一勞永逸」。唯有善用各種創新方法，持續協助企業組織加強各種設施的安全機制，才是正本清源之道。

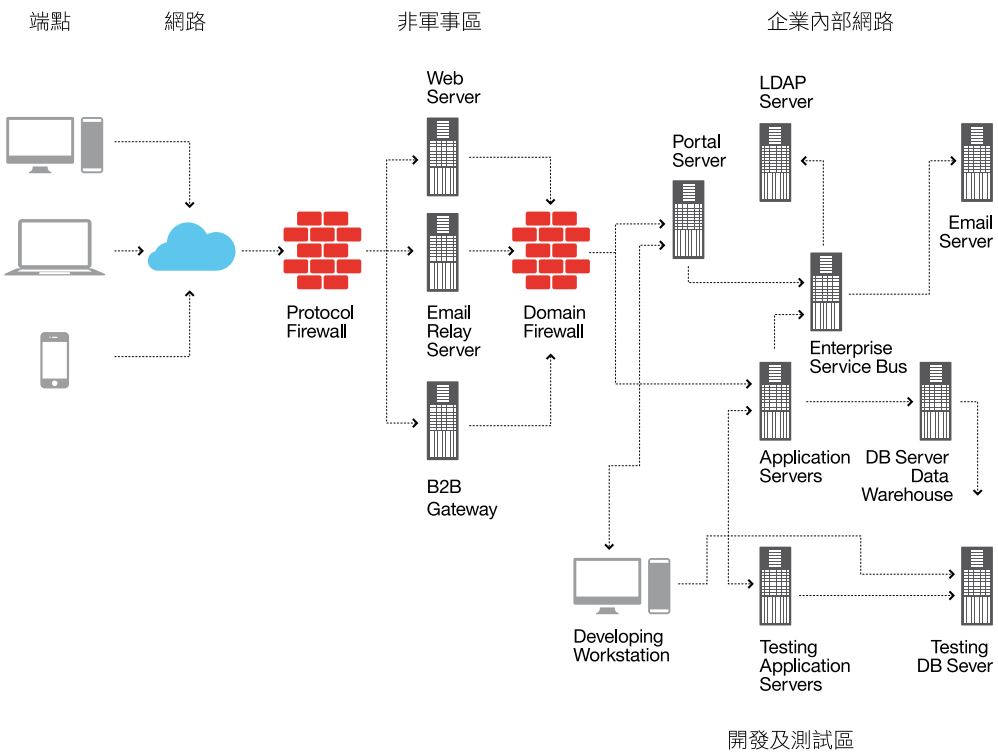
資安全五術．實戰全方位

滴水不漏的IBM資訊安全五大架構

第二章

五大架構、快速檢測，讓企業資安脫胎換骨

孕育稻穀的肥沃，同樣也能滋養雜草。無疑地，在企業資訊運用不斷創新且角色越趨關鍵的今日，捍衛資安絕對不能只依靠見招拆招式的僥倖！擁有與全球各地無數企業夥伴併肩作戰的 IBM資安專家們，在深入企業營運面向的實戰經驗累積下，歸納出當前企業在強化自身安全力上無可迴避的三大主要挑戰－安全治理、風險管理以及適法管理。企業如何針對這三大挑戰制定迎敵策略，加強弱點測試及早發現致命破綻，同時確保所做所為符合法規遵循，並且能快速應變安全事件衝擊，將決定企業資安體質的健全與否。

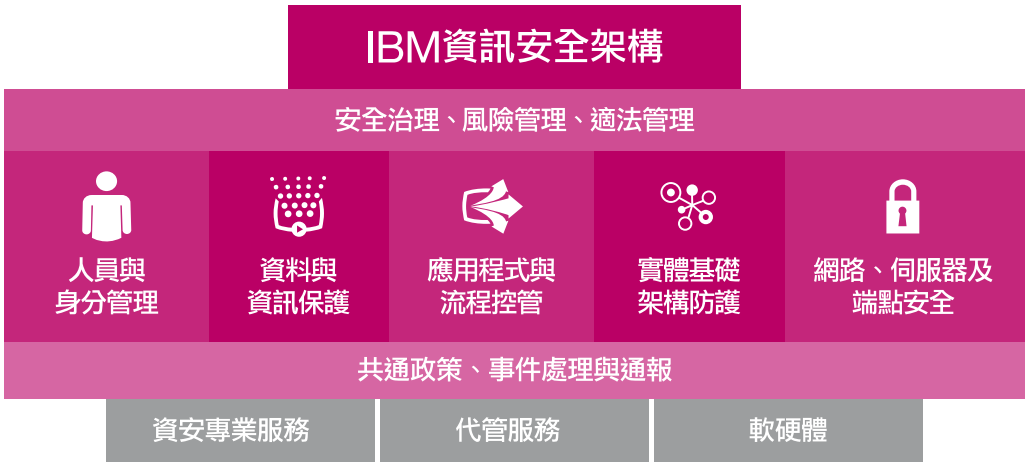


現有縱深防禦架構圖，各個端點的資安風險

而從實務面來檢視，新世代的資安管理應要包含安全治理、風險管理、適法管理，透過由先進事件關聯性分析和威脅分析，達到安全告警、適法報告呈現、廣泛資安事件收集、危機趨勢分析，我們特別提出量身訂製的 IBM Tivoli Q1 Labs全面的安全管理解決方案，助您迎戰資安管理的8大問題：

1. 數據管理的關鍵：事件減量和優先防護
2. 威脅管理：人（Who）、事（What）、地（Where）、時（When）、過程（How）？
3. 應用能見度和異常檢測
4. 用戶端的漏洞分析
5. 適法管理
6. 整合的直觀安全控制台
7. 可擴展性和高可用性
8. 異構設備支持

而為實現安全治理、風險管理、適法管理三大目標，IBM特別淬鍊出一套攻守兼備、滴水不漏的《企業資安全五術》，一旦您將這五大架構融會貫通，就算不敢自詡為無敵，也絕對能高枕無憂！



IBM資訊安全五大架構

- **人員與身分管理：**完善的身分與存取管理方案，保護寶貴的IT資產免於誤用及濫用，但又不必減損使用者的生產力。
- **資料與資訊保護：**無論資料存在於何處、何時進行移動或處理，都能即時以完整方案來監看、管理存取及加密。
- **應用程式及流程控管：**以攻擊者的角度了解各種駭客攻擊手法及使用工具，並以此查看企業Web應用程式安全問題，找出安全的死角及防治之道。
- **網路、伺服器與端點安全：**跳脫防火牆與防毒軟體思維，因應作業系統和應用程式不斷衍生的安全弱點，以整合性概念佈署核心安全機制。
- **實體基礎架構：**在企業致力建立低成本、高智慧化及安全的基礎架構同時，協助提供策略性解決方案以管理企業在動態基礎架構中的資安風險。

小檢測・大發現

這五大關鍵議題所涵蓋的資安範疇，堪稱面面俱到，足以讓資安威脅無所遁形。為了讓您能快速準確地發現自家企業在各面向面臨的挑戰，IBM資安專家們特別列出一份簡單的資安自我檢測表，讓您針對資安架構上潛伏的致命破綻加強改造，提升資安戰鬥力！

現在，就請您拿支筆，透過以下簡易的快速自我檢測重點，快速檢測企業資安現況。

請勾選以下符合您所面臨問題的描述

☐ 1. 當您委外開發Web應用系統，是否只能作功能性驗收，而無法驗收其安全性？是否擔心上線後產生無法預期的漏洞或弱點？

☐ 2. 您是否對目前的安全性檢測具備足夠信心？無法確知現有的檢測方式，是否能夠因應不斷推陳出新的Web應用服務？

☐ 3. 貴公司是否曾因網路攻擊而造成服務中斷？安全性補丁需求大量增加，卻依然缺乏即時性保護？

☐ 4. 您可有把握防火牆規則設定足以維護網路安全？防火牆的阻絕與入侵偵測系統總是如預期發揮功能？

☐ 5. 貴公司內部是否缺乏具備網站應用系統安全know-how的專業人員，無法針對日益複雜的網站應用安全提供讓您安心的解決方案？

☐ 6. 您是否希望能更有效地監管權限和授權用戶存取內部系統，以確保使用者只能存取正確的資訊？

☐ 7. 除了稽核與分析內部使用者行為之外，您是否清楚散佈在各地的安全防護是否有達成預定的效果？是否能端到端綜合分析，證明內部已善盡保管人責任？

☐ 8. 您的資料庫安全控管與稽核設計，是否具備阻斷高權限使用者在資料庫本機端（Local Access）的存取行為？

☐ 9. 您可瞭解企業內部的本機端監控代理程式，哪些可能嚴重影響資料庫的性能？

☐ 10. 當貴企業委外開發測試時，您是否將測試資料進行遮蔽或改造？當測試資料進行遮蔽或改造時，您是否有能力維持資料關聯的一致性？

如何因應看這裡

如果您勾選的資安疑慮，集中在前五題

這意味著貴企業當務之急應立即著手改善【應用程式與流程控管】及【網路、伺服器及端點安全】。IBM《資安全五術》對於企業如何因應蓬勃發展的網路應用安全，早有一套完備的破敵心法，歡迎您即刻參閱第21-23頁的詳細說明。

如果您勾選的資安疑慮，集中在後五題

IBM建議您優先展開《資安全五術》中有關【人員與身分管理】、【資料與資訊保護】與【實體基礎架構】方面的修鍊，依循 IBM自實戰中所淬鍊的精髓要義，一舉奠立資安深厚內力，歡迎您即刻參閱第16-20頁的詳細說明。

把鑰匙交給對的人
資安全五術之【人員與身分管理】

當大量企業員工頻繁地在不同系統間登入登出、進行存取，對任何一位資安管理者來說，每個ID、每次登入都是不可知的風險變數。

因此，企業的資安管理者必須經常問自己：

- 公司相對應的系統有正確反應即時的人事異動嗎？應用系統的使用授權是否受到安全即時的更新及控管？
- 組職異動時，相關的應用系統帳號與授權何時才能新增、更動、或刪除？1天、3天還是1周？
- 人員職位異動時，其相關的應用系統使用權限是否馬上生效？
- 人員離職後，確定所有相關系統權限都即時的刪除了嗎？AD、Mail、VPN帳號與其他應用系統是否已被告知需處理離職作業？若是緊急離職狀況，還需等內部離職流程處理完，IT系統才能生效？

如果您對前述任何問題有絲毫的不確定，別猶豫，讓 IBM來協助您擬定最佳解決方案！

Tivoli Access Manager

協助您以安全的方式，管理重要商業應用程式與資料的存取，同時讓客戶得以快速、方便地存取所需資訊。這些解決方案針對Web資源、系統及代管應用程式，提供集中化的鑑別、原則管理及存取控制服務。

- 使用者可利用「存取控制清單」（ACL）來劃分應用程式及作業系統資源的存取權，無需考慮使用者的UNIX專用權狀態
- 可集中管理整體企業一致的安全原則
- 可保護檔案系統物件，讓UNIX切換到使用者ID，以保護應用程式
- 可追蹤UNIX登入程序，並利用原則來防止非授權存取
- 更強大的平台日誌記載及審核功能

Tivoli Identity Manager

身份認證管理與應用系統單一簽入平台解決方案。將目前儲存於企業各個應用系統資料庫中的資料，做即時的雙向同步處理。並依據企業的需求自動產生相關的群組與角色，以利企業應用系統與網路資源的認證與授權所需：

- 跨平台的支援，可安裝在 Windows、Unix（IBM AIX / SUN Solaris / HP）、Linux、System z
- 可整合各種資料庫（IBM Informix、DB2、Oracle、Sybase、MySQL等）
- 可整合各種LDAP帳號（IBM、Oracle、SUN、AD、OpenLDAP、Novel 等）
- 可整合各種作業系統（AIX、Solaris、HP Unix、Linux、Windows）
- 完整的流程審核與自動化佈署

揭穿明修棧道、暗渡陳倉的偽裝
資安全五術之【資料與資訊保護】

過去保護資料的作法就是劃分內外界線，但當前環境已經愈來愈難區分界線所在，例如Web應用程式可提升員工、夥伴及客戶的生產力，但也將企業曝露於風險之中。因此，企業必須認知到，無論資料存在於何處、何時進行移動或處理，都必須以完整方案來監看、管理存取及加密。資安管理者必須對內部資料活動狀況異常敏感：

- 能否從系統、應用程式、資料庫或網路層面的日誌進行追蹤資料活動？
- 是否有人對敏感資料進行了不當地使用或修改？
- 誰正在改變資料庫結構或刪除資料表？
- 何時有未授權的程式正在改變資料？
- DBAs或外包維護人員正在對資料庫作什麼事？
- 誰正在擷取信用卡資料？

任何資料缺口都可能對企業造成負面影響。在保護資料以免導致損害企業聲譽或營運表現的同時，仍需提供合適的存取等級。如果您對前述任何問題有絲毫的不確定，別猶豫，讓 IBM來協助您擬定最佳解決方案！

IBM InfoSphere Guardium

提供簡單又強大的解決方案，將異質環境中的所有法規遵循審核程序自動化，以確保資料中心（SAP、PeopleSoft、Cognos、Siebel等）內可靠資訊的隱私和完整。Guardium可持續即時監控所有資料庫行動，但不需改變資料庫或應用程式配置，也幾乎不會影響效能表現。

- **非侵入性**：可持續即時監控所有資料庫行動，不需改變資料庫或應用程式配置
- **異質性**：支援各主要DBMS平台
- **降低作業成本**：自動化處理各種法規遵循報告及監管程序
- **擴充性**：具備多層式架構、網路管理主控台、集中處理的跨DBMS稽核儲存庫，能夠達到集中處理的目標
- **職權分立**：審核資料儲存於多個不同的實體或虛擬裝置中，內部人員或是駭客無法藉由竄改審核日誌資料來遮掩不法情事

IBM InfoSphere Optim

透過自動化的資料轉換、變形能力，能夠輕鬆地跨越多個資料庫，協助您主動偵測緊急問題、卸載閒置資料、簡化查詢，並提供專業建議以提升存取效能。更穩定的應用程式回應時間、高效率的主動式效能監控，以及簡單有效的保存策略，可讓公司更得心應手地控制資料環境。

- **加速遞送解決方案**：更快速地開發企業就緒應用程式以驅動業務成長
- **管理資料成長**：應用資料庫保存功能最佳作法
- **效能最佳化**：可將資料庫應用程式效能與正式作業前後工作最佳化
- **為應用程式淘汰與法規遵循做好準備**：存取淘汰已久的資料以因應法規遵循需求
- **保護資料隱私權並確保資料安全性**：應用簡易資料遮罩技術來保護有漏洞的測試環境
- **簡化測試資料管理**：增強應用程式測試與可靠性，並且縮短上市時程
- **簡化升級與移轉**：更快速地運用應用程式新功能以獲取競爭優勢

關鍵時刻，基本功才是救命丹
資安全五術之【實體基礎架構防護】

實體與數位世界越來越沒有界限，更多資料連線裝置隨時登入，更多金錢、權限及安全資訊的存取交易，更多來自員工、事業夥伴及消費市場的使用者...這一切都極仰賴強固的實體基礎架構。當企業致力於建立低成本、智慧化及安全的基礎架構，同樣迫切需要策略性管理所有資訊安全風險。

然而，企業資訊空間運用有限，各部門間都使用網路進行溝通，卻發現網路資料容易外洩、整合又困難。資料傳輸流向無法掌握，造成無法確實掌握資訊設備遺失、失竊、未完全清除的種種狀況。更甚者，天災人禍、意外事故頻傳，企業卻沒有完整的應變能力，一旦系統當機，不但恢復作業時間超長、資料更是救不回來！

您有把握對基礎架構各節點的事件有效地進行監看、報告並將稽核工作自動化及集中化？您能夠針對基礎架構安全的需求，評估、規劃及部署一套具延展性的資安解決方案，以加快企業對資安的回應速度與效率？讓 IBM協助您佈局一個更符合時代脈動的企業資訊基礎架構防護！

為保護實體的資訊資產，機房物理安全和視訊監控將是兩大主要課題。機房的物理安全必須兼顧物理環境的防護、機房及作業中心的場地安全。視訊監控也必須升級為智慧監控，兼具視訊/感測器分析能力、多重來源事件資訊的集中處理機制，達到統整IT安全和物理安全的目標。

如何用最少成本取得最多的有效內容與智慧數據，快速地回應潛在威脅，正是 IBM解決方案的精髓所在：

- 集中管理體系，讓不同來源的資訊能相互關聯，包括資材、員工、客戶、場所，甚至是地域及天氣。
- 採用工具來監看及分析人員的行為，正視來自組織內部的偷竊和舞弊威脅，以預防犯罪並保護資產。
- 傳統的視訊監控系統畫質低落、必須透過軟硬體及服務的整合，升級為智慧監控框架，提供即時決策的支援，以及事後在人員、活動和事件的關聯分析能力。

審慎出招，不讓敵人有可乘之機
資安全五術之【應用程式與流程控管】

「水能載舟，亦能覆舟」，應用程式之於企業也是如此！企業提供給客戶、員工及夥伴的服務愈創新、愈複雜，往往同步帶來更艱難的企業資安挑戰。因為惡意人士無不處心積慮刺探、利用應用程式的弱點，大肆蹂躪資安體系。

事前防範永遠比事後補救來得更符合經濟效益，在應用程式開發過程就儘早找出弱點，所需付出的修復代價也絕對遠低於應用程式上線運作後才發現問題。但隨著Web應用程式愈來愈多，企業被攻擊的弱點也隨之增多，現有的防火牆可能無法封鎖對新應用程式的攻擊。另一方面，必須遵循的企業標準與政府法規也愈來愈多，企業同時需要相關工具來協助登載應用程式的安全性狀態，在確保應用程式安全性的同時，同步提升應用程式可靠度以避免故障中斷。

研究指出，高達80%的開發成本是用於找出及修正程式裡的缺陷及問題。您想讓這個過程更具效益與可信賴性嗎？讓 IBM協助您架構出最佳解決方案！

Rational AppScan

網路應用程式零漏洞方案。Rational AppScan為Web應用程式安全性檢測軟體的先驅，市佔率世界第一。協助您擁有全面的應用程式安全管理平台，能為軟體開發過程各階段增添應用掃描與安全診斷功能，提供下列核心價值：

- 是一套自動化弱點掃描工具，用來檢測Web應用系統的安全性，找出系統的資安漏洞，並一一提供詳盡的處理建議。可簡化發現與修復Web應用系統安全性問題的工作，降低維護資訊安全的成本。
- 是市面上第一套同時整合黑箱測試和白箱測試技術的解決方案。
- **黑箱測試**：模擬各種駭客攻擊的手法，以無害的方式去使用運行中的Web應用系統，判斷系統是否存在各種安全性問題，並按照問題輕重緩急順序，提供可立即處理問題的建議做法。由於直接模擬駭客的攻擊，是應用程式安全的基礎設施，應優先考慮。
- **白箱測試**：分析提供的原始碼，判斷系統是否存在各種安全性問題，指出有安全問題的原始碼位置，並按照問題的輕重緩急順序，提供可立即處理問題的建議做法。

鍛鍊眼觀四面、耳聽八方的本能
資安全五術之【網路、伺服器及端點安全】

當前的資安惡意行為早已不僅僅是病毒和蠕蟲的年代，防火牆與防毒軟體根本已不敷使用。現今的網路威脅可以在短短的幾秒之內影響數千個網路，「被動式」的資安防護設計，只會在攻擊事件發生後才作出回應。一旦企業網路受到攻擊，都已經為時已晚，企業營運損失皆已造成。但是，資訊安全的層面多又複雜、難以管理，部署不同的獨立式解決方案來涵蓋每一種類型的網路威脅，會使管理工作難以執行，使安全風險及成本暴增。

左右為難嗎？讓 IBM協助您打造最佳解決方案！

IBM Internet Security System （ISS）

傳統的入侵防禦系統與防火牆技術已不足因應駭客攻擊，企業需以融合整合式網絡、伺服器保護技術。IBM ISS網路安全防護方案的策略架構，結合網路入侵防禦設備及掃描工具、主機防護系統並整合稽核及中控系統功能，以及虛擬伺服器，可提供具有彈性的主動式資訊安全解決方案整合平台，涵蓋了評估和探索、防禦、監控和報告分析，以克服不斷演變的網路安全挑戰。

- 利用桌上型電腦、伺服器、網路和閘道適用的解決方案，提供端對端的企業安全
- 協助施行符合成本效益的業務流程
- 支援法規遵循
- 支援風險管理要求
- 改善網路效能

Tivoli Endpoint Manager

管理整個企業組織端點安全的單一解決方案。可提供易於管理並且快速部署的解決方案，用於支援分散式端點的安全性，減少管理成本與複雜度，同時增進企業敏捷性、修復速度與精準度。

核心價值：

- 針對耗時的裝置設定及變更管理工作進行自動化
- 以持續的封閉迴路程序有效管理法規遵循生命週期
- 對動態及複雜的環境中的網路資源獲得更大的可見度
- 對安全性組態及修補程式提供精確、精準及最即時的可見性及持續執行能力
- 集中管理提供進階防毒及防火牆保護的功能
- 採用統一管理基礎建設，以協調 IT、安全性、桌面及伺服器的運作
- 全面化管理所有主要作業系統、協力廠商應用程式及原則式修補程式，無論端點的位置、連線類型或狀態為何

輝煌戰績・不勝枚舉

IBM資安成功案例，為您奠定必勝根基

第三章

全球資安領導品牌「趨勢科技」

採用 IBM Rational AppScan捍衛網頁安全

提高資安治理效能，有效防堵SQL injection與XSS攻擊！

身為全球網際網路防毒與內容安全領導品牌，趨勢科技（TrendMicro）致力於保障企業與消費者的數位資訊交換環境。從幾年前開始，該公司積極投入雲端運算領域，更以成為雲端資訊安全技術的第一把交椅為職志。

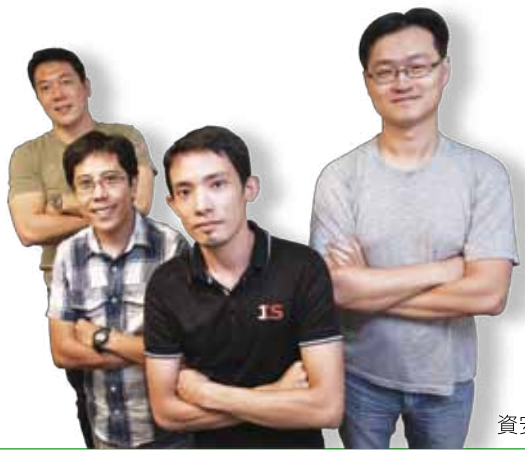
隨著Web應用服務日益普及，網頁成為有心人士惡意襲擊的目標，資料隱碼（SQL injection）或跨網站指令碼（cross-site scripting，XSS）等攻擊行為也愈形猖獗。為了加強防護內外部用戶的資訊安全，趨勢科技於三年多前導入 IBM Rational AppScan Standard Ed，並將網頁黑箱測試納入專案品質流程中，以為產品安全把關。

善用黑箱測試工具，杜絕網站安全漏洞與攻擊

趨勢科技股份有限公司協理馮志弘表示，趨勢科技既為資安專業廠商，對產品安全有不能妥協的堅持，所以把AppScan黑箱測試當成安全保障（security assurance）的重要關卡。趨勢科技組織龐大，全球共有近五十個分公司與辦事處，總公司資安部門鞭長莫及，以往無法確定各地是否確實遵循安全政策，在採用AppScan後，因為可清楚掌握掃描的規格與範圍，資安部門對測試結果有信心，也可更全面落實公司的安全政策。

「在趨勢科技全球的安全治理程序中，Rational AppScan掃描已是統一的固定流程。無論是對內或對外的產品與服務，都須先經過掃描，確認安全無虞後才可推出。依據三年多來的使用經驗，其效益確實符合期待」他說。

他進一步補充：「網站和網路服務最常見的的安全漏洞是SQL injection和XSS，前者尤為嚴重，一旦發生，駭客可能會取得管理者權限並竊取機密資料。過去有段時間，此類攻擊曾為我們帶來不小困擾，但在開始採用AppScan黑箱測試後，我們的站台已經有兩三年未曾爆發SQL injection的事件，而且XSS攻擊的頻率也遠較以往為低。」



資安研發團隊

以AppScan為安全查核基準，保障服務與產品品質

同樣自三年前開始，趨勢科技從「瀑布式（waterfall）」轉向「敏捷式（agile）」專案管理模式，大幅縮短產品開發週期。以往，產品開發從無到有需耗時至少四個月，現在則僅需三週便有初期成果，而在此新模式下，AppScan亦扮演關鍵的輔助性角色，有效協助專案人員從各階段測試中找出並修正問題。

馮志弘指出，AppScan可將掃描測試的結果迅速回饋給開發團隊，供工程師改善並從錯誤中學習，再加上開發週期縮短，團隊成員變動較小，彼此間可分享經驗，因此，工程師犯同樣錯誤的比率愈來愈低，整體素質顯著提升。就產品專案管理而言，AppScan和敏捷開發模式可謂相輔相成，有助於提升開發效率並確保產品品質。

有了AppScan黑箱測試的成功經驗後，趨勢科技已於2011年上半年導入白箱測試方案，未來計畫參考 IBM的技術開發藍圖進一步整合黑白箱測試，為專案開發週期打造更嚴謹、更有效率的控管流程，從而為員工與客戶提供更完善的網路安全服務。

（趨勢案例採訪於2011年）

國立臺灣師範大學六人小組抗駭祕技大公開

校園資安持續強化　達成最佳防駭記錄

對國立臺灣師範大學（以下簡稱臺師大）來說，網路就像校園的大門，資安就如校園的警衛，必須為校園安全嚴格把關。正因臺師大是如此重視網路安全，所以早在2008年啟動資安專案時，就已做好完善規劃，並達成上線六個月內未再被提報駭客入侵的最佳記錄。

個資外洩事件頻傳，凸顯網路資安問題，學校網站也不例外。過去就曾發生高中生入侵八十多所中小學網站，竊取十萬多筆學生資料轉賣給補教業者；警政署也曾發現某國立大學研究中心的主機，成為駭客攻擊的跳板主機，對國外軍事基地發動網路攻擊。學校網站擁有學生的學籍資料和成績等重要資料，可能面臨遭駭客入侵竊取或竄改的風險，甚至成為駭客攻擊其他企業或政府網站的跳板。

為了保護學校師生的個人資料安全，行政院要求大學必須在2008年底前建立「資訊安全管理系統」並通過認證。向來著重網路安全的臺師大於去年十月啟動資安防護專案，結合網頁應用防火牆交換器和 IBM Rational AppScan 等工具，採取事先防範的積極態度，將校園資安等級再提升。

善用工具　六人精兵掌管三大校區

目前臺師大資訊中心僅有六人負責三大校區的網路系統，由於各單位網站的複雜度和建置廠商不同，增加不少整合管理的難度。有鑑於此，臺師大資訊中心為了有效針對全校各單位網站的資訊安全進行把關，且考量軟體使用介面親和度和技術人員的回饋即時性，而選擇使用 IBM Rational AppScan。該工具所提供的中文化報表格式頗為充分，中文化環境設計完善，很適合給各系所的一般網管人員，否則上百頁的報表要花上許多時間才能消化吸收完畢。AppScan除了可針對運作中的網站程式面進行弱點掃瞄，也可針對相關的網路、應用程式伺服器等進行弱點測試。此外，還能針對安全漏洞提出有效的建議，提高程式碼本身的安全性，更有效阻擋漏洞，不但治標更能治本。臺師大資訊中心網管人員表示：「以前網站安全要依靠開發人員的自我要求，但現在有了AppScan，可以掌控開發的品質，並降低被駭客攻擊的危險。」

全面戒護　為兩百多單位網站安全把關

從2007年到2008年底為止，臺師大已知共有十四個單位網站被駭客入侵成功，但在導入AppScan後，已逐步獲得改善。按資訊中心原本的時程，沒有預計這麼快推動到各系所，但資訊中心主任卻認為校園資安的防護刻不容緩，不但發函通知校內各單位提供網站掃瞄服務，也透過教育訓練強化各單位網管人員資安防護觀念，讓全校上下都正視資安問題。

有了網頁應用防火牆交換器並搭配AppScan為網路安全把關，臺師大不僅能達到資訊安全管理系統標準，更可進一步降低學校網站遭駭客入侵影響校譽之風險。資訊中心主任說：「與其事後追究責任，不如事前做好網站安全的最佳防護，而AppScan讓資訊中心可將有限人力放在更重要資安防治工作上。」邁向全面數位化的時代，網路和生活已密不可分，要保護個人資訊安全，除了具備正確的資安防護知識，更要依賴安全可靠的網路環境，而臺師大絕對是最好的示範。

（臺師大案例採訪於2009年）

資拓科技選擇 IBM Rational AppScan

嚴守Web門戶、創造客戶價值，一年內達成300% ROI！

“這筆投資不僅可提升我們的專案資安品質與客戶服務水準，且由於資安需求高，IBM Rational AppScan這套工具比委外資安服務更顯經濟效益，幾乎在購買後就立即達到了ROI目標”

～資拓科技 蕭副總

資拓導入網頁安全解決方案，確保專案交付品質完美無瑕

為了提供最完善資訊服務、守護客戶的商譽，系統整合領導廠商資拓科技不僅通過CMMI軟體品質成熟度第三級認證，更率先將 IBM Rational AppScan導入專案品質流程，掃描Web應用程式的弱點與漏洞，並在專案遞交時，將掃描結果納入結案報告，讓客戶明確掌握專案的資安全貌。

資拓科技是資策會資訊工程研究所衍生獨立之公司，多年來專注於大型資訊系統整合開發，觀諸資拓科技的目前客戶專案，無論是戶役政資訊系統、醫療健保資訊系統、防災監控系統、航管自動化系統或銀行核心系統，都是高度專業、架構龐大、且攸關民生的重要系統，其資安防護更必須以最高標準以待之。

資拓科技顧問事業處陳保穎經理表示，資安弱點診測方案一般分為白箱測試（靜態程式碼掃描）、黑箱測試（模擬攻擊）、主機網路掃描與滲透測試四種。資拓團隊評估，黑箱測試具有誤判率低、成熟度高、持續更新等優勢，且具有急迫性，因此決定優先導入。陳保穎進一步以執行中專案實際「試車」後，便決定採用 IBM Rational AppScan。

事業發展部副總經理蕭偉政

中文化報表與整合介面，大幅節省作業時間、提高效率

「AppScan的獨到之處，在於其邏輯明確、資訊清晰的中文化報表，以及高度整合的操作介面。」陳保穎分析。中文化報表不僅方便內部判讀，更能提升與客戶溝通的效率與精確性。其操作介面不僅直覺化易於判讀，且在除錯時可以一個介面操作到底，不需在多個應用程式間切換，大幅減少作業時間。此外，還可以整合到CQ（ClearQuest）問題單的品管流程中，化為專案整體品管的一部份。

「簡單來說，他廠的優點AppScan都有，而AppScan的優勢別人卻沒有，因此我們很快下了決定。」陳保穎十分肯定AppScan的表現。事業發展部副總經理蕭偉政在考量ROI時，更認同這是必要的投資，「因網頁安全的需求強勁，若相較於委外掃描每次十萬元計，導入AppScan的投資報酬率在一年內就可達到300%以上！」

陳保穎相信，導入AppScan不僅有助於提升專案滿意度，其「資安品質保證」對新的客戶也極具吸引力。對於網站規模龐大、具有敏感資料、資安需求高的客戶，資拓也建議直接購買AppScan來定期掃描、維護網頁安全，將比委外掃描服務更為划算。

有了AppScan作為基礎，未來資拓更計畫加入白箱測試工具，並持續精進程式設計師的資安專業，專案生命週期全程嚴謹控管，為政府機構與企業提供更完善、更安全的資訊系統整合服務！

（資拓案例採訪於2009年）

*數據來源：市調機構 Gartner

機動與機密兩全其美

聖地牙哥證交所的資料/資訊保護良策

聖地牙哥證券交易所依靠相當多樣的電子交易及資訊系統，以及資金和投資組合管理應用程式，來支援其每日的商業營運。為遵守政府法規，該組織需要尋找一個方法，在不用禁止工作或可用性的狀況下，即能夠定義存取規則並監視其核心系統及應用程式的連線。儘管交易所考慮過一律禁止此資料的存取權，但是管理者仍需要進行存取，才能執行批次處理程序並實施維護及支援作業。

提升全方位資料監視，而不影響應用程式效能

為達成這項需求，聖地牙哥證券交易所選擇 IBM InfoSphere Guardium Database Activity Monitor軟體。這項解決方案能提升全方位的資料監視，而不影響應用程式效能，即使當龐大的線上交易數量進行時，也能夠執行下列事項：

- 管理一般使用者的資料庫存取權
- 監視存取或變更資料、在上班時段之外起始的資料存取，以及透過不適當或未核准的管道來起始存取的一般使用者
- 監視存取正式作業環境的開發人員、系統管理者及商業分析師
- 監視對資料庫或應用程式進行自發性變更，或起始非週期性正式作業系統維護的IT員工
- 產生反映所有一般使用者存取連線的每日活動報告
- 回應意外事件

看緊機密資訊，贏得客戶垂青

此外，IBM還幫助該客戶遵守政府的資料安全性相關法規，節省了龐大的罰金支出。而由於InfoSphere Guardium Database Activity Monitor軟體能藉由限制資料存取權給需要的人員，相對也讓客戶百分之百放心，因為他們相信資料會受到妥善監視及防護！

生產力與安全性完美連線

東芝與 IBM Tivoli Endpoint Manager的不解之緣

金融海嘯於2008年席捲全球，東芝（Toshiba）身處劇烈變更的經濟環境之中，致力於轉型為具全球競爭力且最具多樣性的電子商品製造商。

生產力・安全性・節能

然而，隨著企業IT基礎架構不斷升級及擴增，其複雜度也隨之提高，因此需要一個能保有高安全性的基礎架構，有條理的管理並控制各種網路裝置，以同時確保員工個人生產力與安全性。

「IBM全球服務事業部 – 全球企業諮詢服務事業部」藉由讓東芝的企業PC與 IBM Tivoli Endpoint Manager（TEM）互相連線，來提升效率及「端點管理」解決方案技術的可行性，達到：

管理最佳化・成本極簡化

- 整合管理 IT 及安全性，並透過簡易管理減少作業的負擔及成本：
  提供各種不同的安全性功能，包括修正程式管理、資產管理、漏洞管理、病毒處理方式，並容許伺服器群組及隨著受管理資料量增加而增加數量的代理程式進行整合，透過簡易的管理來降低作業負擔及成本。
- 對一般使用的影響降至最低，以進行最佳的管理：
  限制修補應用程式及收集配置資訊的代理程式資源使用率，以進行最佳的管理。
- 即時收集可以信賴的資訊：
  將規則與遵守內部規範標準的代理程式進行整合。代理程式會在偵測到違反安全規則時通知伺服器，或將配置資訊變更至管理者，以基於一律保持最新資訊的原則來進行用戶端管理。

在 IBM Tivoli解決方案的協助下，東芝實現讓企業PC環境具備高度安全性，同時維持個人作業生產力，進而提升整體企業的安全性及能源節約的新願景。

高價值資產的最佳護法

Tata Teleservice以IBM Proventia Network Intrusion Prevention System對抗惡意入侵

成立於1996年的Tata Teleservices Ltd.提供第三代（3G）通訊服務，提供包括行動電話服務、公共電話亭、室內無線電話及固定式無線網路服務給超過8,500萬名客戶，全球雇聘超過395,000名員工。

資安基礎架構是抵抗攻擊和威脅的根本

Tata Teleservices Ltd.以龐大的應用程式基礎架構來服務線上通訊用戶，這對該企業的通訊業務具極大重要性。對這間公司而言，相當重要的工作之一便是維護基礎架構的安全性，使其免於外界威脅或攻擊，以提升商業應用程式及其網路的可用性。為進一步改善現有狀況，Tata Teleservices著手尋找可以信賴的入侵防禦解決方案。

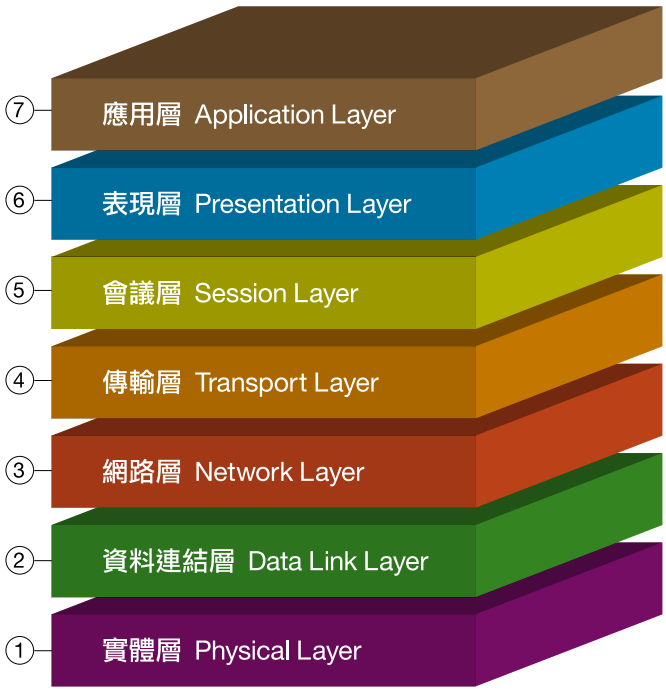
資安的萬里長城，始於一磚一土

Tata Teleservices Ltd.決定導入 IBM Proventia Network Intrusion Prevention System解決方案，以強大安全基礎架構來保護其環境，並防止針對高價值資產的攻擊。該方案可以保護其基礎架構免於即時網路攻擊和威脅， 同時得以使用由 IBM X-Force Research支援的強大安全性裝置來保護其環境，利用進階的威脅偵測和防護功能，客戶能夠防止外界攻擊高價值資產並保護其系統。

資訊長暨副總經理陳俊廷

「從OSI Model的七個層次來看，過去我們較為偏重一至三層的基礎架構安全，四至七層應用面的資安防護措施較少；」全球人壽資訊長暨副總經理陳俊廷回顧三年前導入IBM IPS入侵防禦系統的初衷，「基於對客戶資料的責任感，我們決定提前因應、做好防堵措施。」

OSI Model網路模型七層架構



全球人壽採用入侵防禦領導品牌-IBM IPS

IBM IPS是先進的企業入侵防禦系統，是隸屬於 IBM Internet Security System（ISS）主動式資安防護系統的網路安全方案。ISS系統是全球第一套入侵偵測系統、第一套主動式防入侵設備，在資安領域長年以來都扮演技術領導者的角色。尤其在全球知名的 IBM X-Force資安研發團隊加持下，ISS能提供最先進的技術、零時差攻擊防護力、立即性更新與虛擬補丁功能，確保資安防護滴水不漏。

全球人壽在評估導入入侵防護時，將當時業界主要解決方案依其需求進行評比，在幾項主要評比標準中，IBM IPS解決方案都展現絕佳優勢：

- **掌握風險源頭：**提供來源與目的端管理能力，協助資訊團隊快速掌握問題源頭、關聯機制與影響範圍，並提供解決方案建議，使資安問題更快獲得解決，並鎖定資安弱點加以改善。
- **完善防護功能：**對於日新月異的攻擊手段，IPS能夠提供最先進的防護措施，且其防護率、掃描結果分析的表現都令人滿意。
- **具體實用的資安報表：**IPS能夠即時產生易於解讀的中文報表，且能根據內部環境與管理需求，產生關鍵事件的客製化報表或統計排行。
- **人性化管理介面：**IPS提供便於管理、快速操控的人性化儀表板，可快速回應程式更新或資料庫更新，隨時保持在最新防護狀態。

「當事件發生時，資訊團隊需要工具告訴我們如何處理；」導入並運作了三年後，陳俊廷在拿出當時的檢驗標準來看，「審度當時的評估標準，IBM IPS的表現都令人滿意，如果滿分是十分，我會給八分評價！」

完美功能超乎預期，提升資安管理效率

此外，導入IPS前後，全球人壽也發現了IPS幾項超乎預期的功能優勢，令這筆投資大大加分。首先，是在測試過程當中，系統內部有一部被植入無害木馬但會濫發郵件的電腦，IPS發揮強大實力輕易鎖定這部電腦，大幅節省了逐台掃描過濾的時間，令資訊團隊感到印象深刻。

導入後，IPS強大的過濾功能也讓資安控管更加輕鬆。資訊團隊將過濾功能用在會影響整體系統資源的社交網站、影音網站與即時通訊，使有限運算資源能夠聚焦應用於業務上。同時，IPS也過濾掉許多惡意釣魚網站，避免員工誤觸地雷造成資安風險。

資安長路，一刻不得鬆懈

放眼未來，全球人壽在資訊安全防護的道路上還是採取嚴謹態度與前瞻思維。對於下一步資安規劃，陳俊廷點出幾項重點。首先，在個資法正式上路後，企業負舉證責任，因此必須有完整的系統紀錄（system log）管理機制。其次，會進一步從流程面與工具面加強控管資料拷貝下載行為，徹底杜絕數位資料外洩的可能性。最後，則是持續檢驗內控流程中的實體文件管理，確保實體資料也萬無一失。

企業生存的必要投資

陳俊廷語重心長地表示，資訊安全就是企業的國防政策，是個永無止境的工作，永遠可以做得更好。「資安系統難以評估投資報酬率（ROI），其效益不是反映在報酬，而是你不做，就無法在市場上存活下去；」陳俊廷總結，「我們絕不自滿於合乎法律遵循，一定要走在法律與趨勢之前，以更高標準自我要求，使每一個保護資料得到最安心的保護，朝向壽險業的專業典範邁進。」

全球人壽的資安政策

長久以來，全球人壽始終秉持著「尊重、誠信、專業、創新」的經營理念及「全心照顧」的企業精神，致力於提供保戶最專業的保險及退休規劃服務。

由於壽險業持有大量保戶隱私資料，因此全球人壽向來以高標準來看待資訊安全管理。自其1994年正式於台灣營運以來，就落實執行其全球一致的《資訊安全政策》。因此，在國內個資法通過前，全球人壽早已具備完整的資訊安全體系可符合法規遵循。

全球人壽設有獨立的「資訊安全官」（Information Security Officer, ISO）職位，跨部門統籌管理電子資訊、影音資料、實體文件與日常作業流程。另設置有「資訊安全指導委員會」，成員來自資訊部門主管、法務長、總稽核、總務主管等，負責資訊安全政策之制訂與推動，以確保資訊保護的全面性與完整性。

（全球人壽案例採訪於2011年）

Security Solutions

快撥打破敵專線：0800-016-888按1，了解更多優惠方案

台灣國際商業機器股份有限公司 台北市110松仁路7號3樓
IBM市場行銷處0800-016-888 按1 **www.ibm.com**/tw

TW2A301D