



駭客止步！ 神通成立資安研發中心

文／神通資訊安全研發中心技術長朱欽浩 圖／神通電腦

網際網路給人們生活帶來便利，讓資訊隨手可得，也讓有心使壞的人有了舞台，或是惡作劇地讓人在使用電腦上造成不便，或是讓網站無法正常運作，更嚴重的是竊取資料，破壞資訊系統，甚至犯罪。

電腦連上網路使用，沒有資安防護是絕對危險的事，電腦會在使用者不知不覺的情況下中毒、被植入木馬、遭受遠端遙控，成為駭客攻擊網路上重要資源的工具，這並不是駭客刻意挑上自己，而是網路駭客群發展出自動化的工具，在網路上一台接著一台電腦的搜尋並嘗試攻擊；即使在電腦上啟動了資安防護，也可能在不知情的情況下落入各式陷阱，或是被新造的病毒成功入侵。網路上的攻擊與防守成了永無休止的戰爭。

最佳資安方案 神通提供

神通電腦鑒於資訊安全對電腦使用者的重要性，

特別成立了資訊安全研發中心，對於資訊安全進行長期的研究發展，以全方位提供客戶最佳的資訊安全解決方案，讓客戶在安全的使用環境下，得到電腦使用的便利。神通資訊安全研發中心由苗華斌副總領軍，下設網路威脅預防、資訊安全治理、資安基礎建設與資料保安防護等四組，針對網路及資訊系統上各種安全防護進行深入研究，並整合市面上排名領先的資訊安全產品，建構全方位資安解決方案，提供客戶完善資安管理服務。

神通資訊安全研發中心秉持SMS, ISO 27001 及ITIL 規範準則，提供完整的資訊安全 Frameworks 框架，資訊基礎架構庫〈IT infrastructure library；ITIL v3〉服務

管理是資訊管理中最佳的實務框架，其目的係針對整個服務管理週期中的各個過程，協助提供優質的服務，有助使用者結合資訊運作、應用方案及策略，讓整個資訊環境達到更好的監管、規範及效率，為客戶帶來更高的業務價值。執行ITIL 管理，有一套完整的控管軟體，不但可在管理流程中留下記錄，並可用雷達圖等圖表，顯現資安執行的狀況，改善措施與改進結果亦在整體的管理資訊之中。神通預定在今年完成 SOC 的建置，提供客戶遠端資安監控服務，由多位獲得 CISSP (Certified Information Systems Security Professional) 證照的資安專家，在不同資安領域中協同提供專業服務。

網路威脅預防組 滴水不漏

網路是威脅來源的主要通路，網路威脅預防組研究在網際網路／外部網路入口及內部網路設計適當的防護系統，以阻擋、偵測、修復、記錄及管理等措施，以及Firewall防火牆、IDS入侵偵測、NAC網路存取控制、防毒牆、實體隔離等設備，讓網路在層層關卡中得到適當的保護；對於外部使用者和單位，建立網路上VPN加密通道及權限認證，以防止資料被監聽、竊取或竄改；對於無線網路，建立電波的偵搜及阻絕能

力，防止區域內的非法使用，並用三點定位的方式找出非法使用者的所在位置；提供即時的聯防機制，讓資安設備對於威脅進行連鎖反應，將風險降至最低；對於未即時更新防護碼的電腦設備進行更新，對於已受感染而發動攻擊的電腦設備進行隔離。

網路使用順暢及系統備援機制也是網路威脅預防組關注的重點，使用廣域網路、網頁／應用程式／資料庫伺服器及資料加密設備的負載平衡和備援連線方式，加上IP位址管理系統建構完善的 DHCP (Dynamic Host Configuration Protocol) 和DNS (Domain Name System) 管理，並使用頻寬管理器及URL (Uniform Resource Locator) 過濾器將網路頻寬資源做有效的應用，讓需要即時作業的系統得到最佳回應時間。

網路安全管理平台是不可或缺的一環，神通資安管理中心以SIEM (Security Information and Event Management) 管理系統為平台，由紀錄伺服器收集網路上各網路設備、資安設備、電腦作業系統、伺服器、資料庫等每一紀錄 (Log)，進行分析、即時反應、自動協同比對，同時在監控電視牆上顯示各種即時管理圖表及事件條列，並對資安事件的處理進行流程管制，防止疏失造成損害。SIEM管理系統可將管理流程步驟與ISO 27002、沙賓法案、PCI、HIPAA、FISMA等資安法規中法條相對應，讓資安的管理更為

嚴謹。

端點安全管控是終端電腦設備必要的軟體，經由管控可限制 USB 介面只能使用於滑鼠、鍵盤、耳機等，而限制連接印表機、隨身硬碟、姆指碟、光碟燒錄器等記錄設備或是3.5G及Wi-Fi網卡，並可將儲存裝置中的資料加解密，對應用程式進行管控等，讓個人不會因為疏忽而造成損害。郵件防毒、垃圾郵件阻擋及網頁內容防護也屬於網路威脅預防組的專業技術範圍，在內部網路中加上蜜罐 (Honey Pot) 誘捕駭客也是一種必要的技能。為因應網路上不斷擴增的威脅，因此衍生出上列五花八門的種種防護措施，而網路資安的滴水不漏正是網路威脅預防組致力的目標。

資訊安全治理組 管理周全

有了完善的資安系統，還必須有良好的管理，ISMS (Information Security Management System) 是一套有系統地分析和處理資訊安全風險的方法，也是資安管理依循的作業流程，資訊安全管理的目標是透過系統安全、網路安全、實體安全、人員訓練或資產管理等控制的方法，把資訊風險降到可接受的程度內。資訊安全治理組的專長在於協助客戶導入ISMS，成立資安中心 (SOC) 或建立資安監控機制，並持續協助客戶做好資安管理。

導入ISMS由規劃資訊安全政策開始，進行組織業務分析，建立資安架構，成立資安組織，建構管理機制；進一步進行風險管理與評鑑，將資訊相關資產分類及管理，對資安訂定風險評鑑、風險管理及改善程序書，同時對組織提出適用性聲明；之後依所規劃資訊安全管理系統進行計畫、執行、檢查、改善 (Plan-Do-Check-Act; PDCA) 四階段循環並產出文件，由資安中心執行資安管理作業，先從風險評鑑確認的關鍵性資產開始管理，結合預防、應變及復原控制措施，將業務運作中所產生的災害或故障降低到可接受的範圍；最後落實於制度與稽核作業，利用定期的弱點掃描與滲透測試瞭解資安系統的防護能力，並由稽核報告及管理審查會議紀錄產生改善計畫，進入下一資安

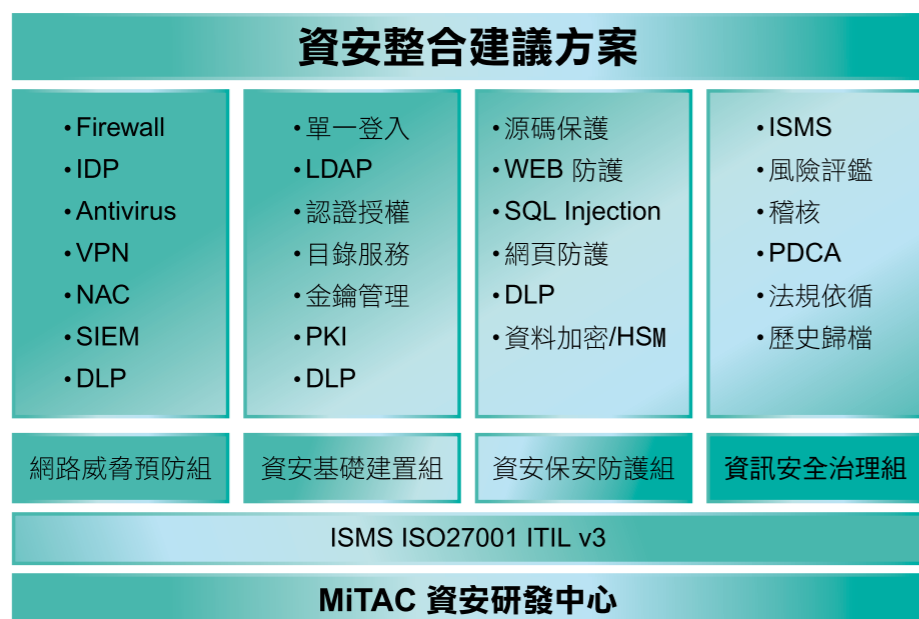
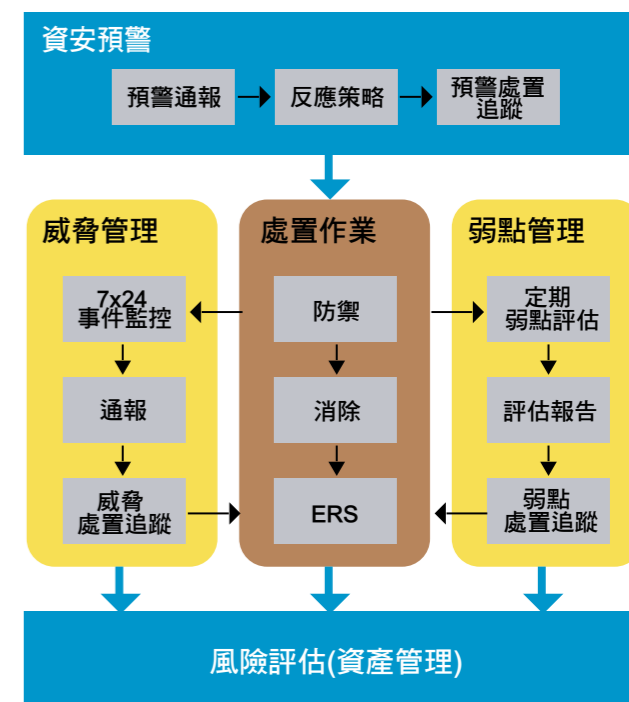
管理循環。

資訊安全治理組團隊已在政府重要專案中提供資訊安全管理服務，由於擁有豐富的管理實務經驗，可針對企業與政府機構不同的作業需求，提供完整的資安管理作業解決方案。資訊安全治理組整合E-mail分類存檔管理、運用SIEM (Security Information and Event Management) 即時辨識安全性事件，迅速提供資訊系統使用率分析報告、Policy 權限管理優化等服務，讓資安管理者享有更安全、方便的管理。

資安基礎建設組 層層把關

資訊安全管理基本架構中，使用者身份辨識及使用權限管理是相當重要的一環，因此建立單一入口平台、執行統一管控，成為資訊系統必備的設計。神通資安研發中心資安基礎建設組提供資安入口網站的建置服務，使用者驗證方式採用動態密碼 (One Time Password; OTP) 裝置，以確保密碼保管的安全；安控管理平台採用公開金鑰 (Public Key Infrastructure; PKI) 基礎架構及IC卡CA憑證進行認證管理。由單一簽入 (Single Sign On; SSO) 系統，結合應用程式目錄

SOC的服務範圍



完整的端點安全防護



服務與權限管理，以角色〈role-based〉為基礎授權方式，根據身分認證結果與服務需求，透過目錄服務取得授權角色及權限資料，由瀏覽器顯示使用者特定的應用程式多層次服務選項，依權限提供使用者資訊使用範圍。

個人資料安全是近來資安主要的管控項目，資料遺失防護系統〈Data Loss Prevention; DLP〉成為矚目的焦點，經由資安政策與資訊分類的指導，限制重要和

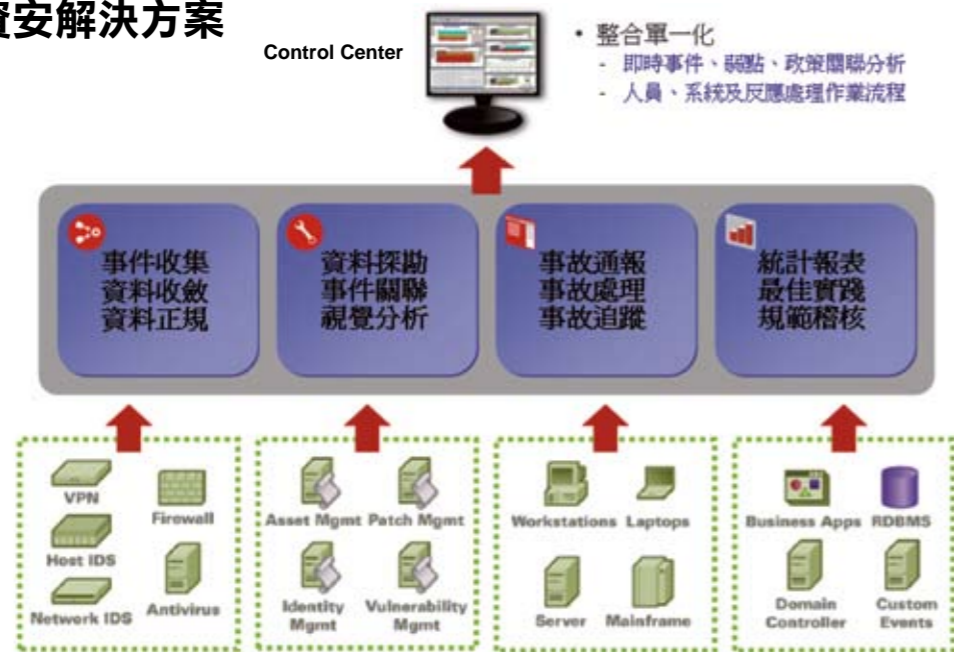
機敏的資料傳送、列印、複製等行為，在伺服器端、網路與使用終端，採用監控、管制及側錄的方式，將預設的格式，例如身份證字號、路巷弄號等特定文字或設計圖檔名稱、座標位置、地籍戶籍編號等，進行全資料比對檢查，防止資料的不當使用或外洩。基礎建設組的專家可提供資安管理條件設定工具，協助使用者建立最適用的資料保護管理模型。

資料保安防護組 防患未然

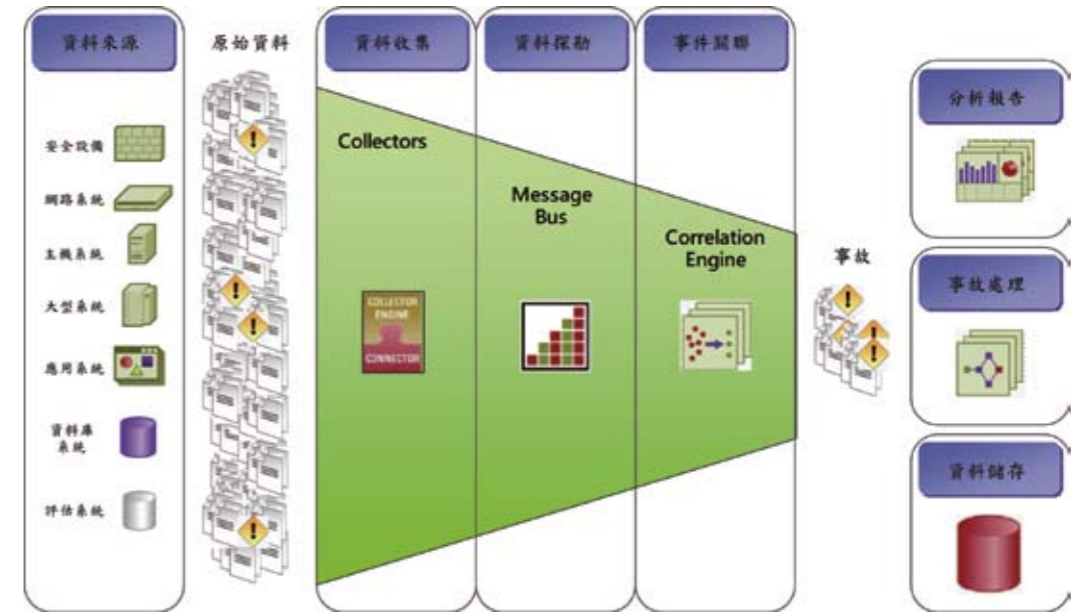
資訊系統受到攻擊時，通常是直接攻擊Web應用程式或網頁伺服器的資料庫，如果應用系統本身的程式碼受到攻擊，整個應用就會處於危險之中，因此安全的 Web 應用系統開發，需要即時對系統源碼進行安全檢查，防範於未然，避免日後修補；若於程式完成後再行檢測，則需用補釘的方式讓程式避免危險，或是利用網路設備的設定進行保護，這些作為仍有其風險。白箱測試在程式發展過程中是一個關鍵步驟，用於檢測 Web 應用系統的漏洞，如 SQL 資料隱碼攻擊和跨網站腳本攻擊〈Cross Site Scripting; XSS〉等。

神通資安研發中心資料保安防護組具有源碼檢測的能力，可依客戶需求，採用行為分析方式，對既有

完整的資安解決方案



SIEM 技術架構



完整解決 絕對安全

應用程式源碼直接進行掃描，經由分析器〈Parser〉與轉換功能，即時虛擬執行程式，評估程式中不安全撰寫問題，分析出每一行有問題程式碼的弱點，及各種輸入錯誤會衍生那些問題，可有效預防類似攻擊手法所造成的威脅，例如：注入式弱點〔Injection Flow〈SQL, File Command, XPATH, Refection〉〕、跨網站腳本攻擊〈XSS〉、Indusion檔案引用及資料流漏洞等。源碼檢測搭配WAF〈Web Application Firewall〉網頁應用防火牆可有效保護資訊的安全，網頁應用防火牆可即時觀看網站存取及惡意入侵與網路阻絕等行為，資安管理者可依需要適時調整資安設備防護設定，以保護網頁系統安全，網頁應用防火牆亦可提供各式管理報表，協助落實遵循法規。

為保護資料在傳輸中安全送達，廣域網路上常用SSL VPN 虛擬通道進行保護，當資料進入區域網路之後，仍有機會被有心人士監聽或複製。硬體加密模組〈Hardware Security Module; HSM〉的處理能力在這幾年有效提升之後，被廣泛運用於電子商務、檔案、資料庫及硬碟資料全程加密保護，資料保安防護組可提供完整的企業資料保護解決方案，資料加密涵蓋應用程式、網路和資料庫，可以保護關鍵資料遠離內部和外部的威脅，確保符合安全法規規範的要求，加密資料即使被側錄或竊取亦可避免風險。

神通資安研發中心執行長陳宏年協理表示，除了四個小組的資安管理能力之外，我們對於符合ISO 27001規範與達到綠色節能機房建置也有豐富的規劃、設計經驗，可以提供機房設施、機櫃、電力、監控、節能空調、節能照明、門禁、消防及備援等完整的解決方案。

面對各式各樣的資訊安全威脅，廠商不斷推出新產品，為達到資訊安全的管理目標，所使用的資訊與網路安全設備與軟體多達十餘種以上，未來增加配置的設備會越來越多，如何使用操作、如何聯防管理、如何鑑別網路安全等，將造成使用者沉重的負擔。新的資安威脅不斷發生，依ITIL 及ISMS的稽核進行管理，無法保證網路時時是安全的，建立SIEM 系統以收集各設備的資安資訊，可讓管理者瞭解資安現況；弱點掃描與滲透測試可瞭解資安的防護能力，當發現新的資安問題可立即調整、強化資安系統的配置。

神通苗華斌副總表示，完善的資安需要持續管理與強化，神通資安研發中心擁有資安系統整體規劃實力、完整建置經驗及維運管理能力，我們衷心期盼能與社會各界分享心得，為推廣資訊安全盡一份心力。☑