

IBM 資訊安全科技前瞻報告：新興安全科技趨勢展望

目錄

內容概要	1
前言.....	1
IBM技術與資安發展現況	4
趨勢一：保護虛擬環境	5
趨勢二：提升安全的多元選擇	7
趨勢三：管理風險與適法需求	8
趨勢四：用戶身分防護	9
趨勢五：資訊安全	10
趨勢六：應用程式安全可預測性.....	12
趨勢七：保障網絡安全	13
趨勢八：捍衛行動裝置	14
趨勢九：即時感應之實體安全防護	15
結論.....	16
更多資訊	16

內容概要

未來二到五年間，各種新興科技與社會趨勢將為企業資訊安全帶來重大衝擊。此報告旨在闡述後續幾年的技術發展態勢、形成這些趨勢的主因，以及 IBM 能透過哪些方式協助組織在風險與機會間取得策略平衡。

前言

隨著全球化腳步加快，人類溝通與貿易邁入全天候作業，消蝕了傳統時間與空間的疆界。在此嶄新態勢中，資源共享已成為企業營運常態，而組織間敏感性資訊分享更是前進全球經濟的必備門票。

與他者分享資訊或選擇自我孤立間的界線，也標誌出機會與風險的兩方。為了固守其中的分野，現今企業對商業系統與自動化政策的依賴更甚以往，以期杜絕安全威脅、捍衛智慧財產，及保障商譽與隱私。

每當新科技問世，機會與風險之間的界線便會些許挪移。在我們積極探索新技術所蘊含的機會與潛能的同時，有心人士也急於鎖定弱點發動攻擊。因此，隨著科技推陳出新，組織因應安全威脅的策略也可能產生根本的改變。

爲了探究組織在未來幾年間所面臨的安全挑戰，我們應思考下列幾個問題：在接下來的二至五年內，哪些科技趨勢將影響組織運作？哪些策略性因素能夠加速企業轉變？組織該如何掌握其中契機，並同時妥善管理相關風險？



透過「全球科技展望 (Global Technology Outlook, GTO)」與「全球創新展望 (Global Innovation Outlook, GIO)」論壇，IBM 不僅分享本身對安全挑戰的洞見，亦開啓業界在此領域的對話。IBM 力圖運用經數百項客戶專案與市場研究所產生的思維化爲行動，協助組織爲機會預做準備。經過多方深入分析，IBM 歸結下列九種將在未來二到五年間主導安全環境發展的重大趨勢與科技：

- 保護虛擬環境——從特殊目的之專用型硬體設備，轉以共享式硬體環境以支援專門應用
- 提升安全的多元選擇——以預製之安全方案簡化系統部署並加速投資回收
- 管理風險與適法需求——商業風險暨政策導向之 IT 安全管理取向
- 用戶身分防護——加強身分保障、隱私與共通性，並簡化身分管理機制
- 資訊安全——反映高風險資料的商業價值
- 應用程式安全的可預測性——將安全防護全面融入應用程式的生命週期
- 保障網路安全——不受網路傳輸速度限制的即時安全防護，並加強對應用程式攻擊的防護

- 捍衛行動裝置——得以信賴的商務平台，以及身分認證的主要管道
- 感測實體安全防護——快速有效的實體安全機制

以下將依循這些趨勢的脈絡，探討組織該如何因應伴隨新興科技與社會變革的安全挑戰，並一一檢視這些新技術的內涵與前景，以及 IBM 能透過哪些管道協助組織面對迎面而來的挑戰、風險與契機。

IBM 技術與資安發展現況

過去幾年間，從實體到數位的溝通演進促成安全管理的改變。IBM 匯整多項調查結果後發現，隨著愈來愈多的機密資訊上線，個人與企業的安全威脅不但愈形組織化，攻擊的頻率與複雜度也日益升高。此外，攻擊對象更為廣泛，從智慧型手機、RFID 及晶片卡等付費系統，乃至家用娛樂系統，都可能面臨更重大的安全威脅。

下列因素將推動安全需求未來幾年的發展：

- 可有效因應需求彈性擴充之高機動性 IT 環境
- 以電子身分執行機密及關鍵工作的能力
- 終端用戶對增加線上身分控管與自決力的要求
- 在安全、可靠、彈性、組合式（**composable**）方面的應用上提升對多變商業需求的應變能力
- 滿足組織需要的 IT 環境控管層級
- 依據風險來管理 IT 安全及其對營運和商業風險的影響
- 行動裝備成為身分安全保障的來源以及商務平台
- 以安全、高品質之資訊來源輔助高風險決策
- 可反應真實環境的 IT 系統

由於對個人身分與資訊安全的威脅警覺性日漸升高，消費者開始要求組織採取必要措施來捍衛寶貴的資料。為滿足消費者對資訊安全的期待，主管機關透過制定相關法律和規範來保障個人身份識別資料，包括信用卡號碼、病歷和其他潛在攻擊目標。同時，組織亦應保護其智慧財產與商譽免受重大安全漏洞損害。

這些科技環境的變遷與挑戰型塑出 IBM 的資訊安全策略。專為協助組織策略管理內部各環節風險所設計的 IBM 安全防護架構（IBM Security Framework），明確規劃出資訊安全的五大關鍵領域：人員與身分、資料與資訊、應用與流程、網絡、伺服器與端點，以及實體基礎架構。組織可藉由檢視各範疇內的潛在風險因素與影響，進一步了解安全風險與弱點，並依據不同風險層級研擬因應之道。

為持續建構資訊安全架構，IBM 持續推出一系列新型方案與服務，以回應日漸多樣與複雜之安全需求，並藉此協助組織從這些未來趨勢中獲益。

趨勢一：保護虛擬環境

過去二十年間，組織爲了因應技術需求的變遷，大幅擴增資料中心。隨著營運中心在能源、空間與人力資源消耗逼近臨界點，不斷飛漲的資本支出及能源開銷迫使組織開始找尋能提供更具能源效益之基礎架構。

爲支援共享式應用的快速成長，以及各項服務不時變動的資源需求，基礎架構應具備更優異的擴充性與回應力。雲端運算採共享式基礎架構，將大型虛擬化資源池連結起來，提供組織簡單、快速且具設備兼容性（**device-agnostic**）之服務，具備迅速調整資料中心作業模式的潛能。

透過資源定義及標準收集的能力，雲端運算能大規模簡化系統架構，將組織內各安全策略與系統設定精簡及標準化。由於所有資源都能以類似的方式管理，系統就能管理更多的虛擬資源，如此系統簡化就能更進一步提升其管理效益。

儘管雲端運算蘊藏無窮潛力，卻也可能帶來更多挑戰：

- 組織應強化隔離管理能力，把支援單一用戶（**tenant**）的應用、資料與基礎架構和其他用戶區隔開來，並落實此隔離政策用於不同的虛擬化平台上
- 虛擬環境的安全防護與管理層級應如實體狀態般的紮實。傳統的安全方案，如網絡監控與入侵偵測等，也須應用至虛擬環境上
- 虛擬資源是以資料影像的方式儲存，因此特別容易被毀損。組織應建立影像管理能力，如變革與修正管理流程，以保障並維護資源定義

「資訊系統的人員支出最多可佔所有 IT 營運預算的七成，能源與冷卻費用更飆漲至十幾年前的八倍多。」

—技術研究機構 **Clabby Analytics**¹

展望未來

IBM 自推出虛擬化技術以來，便持續推動虛擬化技術在 **System z®**與 **System p®**伺服器上的創新與突破。舉例來說，IBM 的 **z/VM®**系統可同時運行數千種完全獨立的 **Linux®**系統。隨著虛擬化技術延伸至大型主機之外，IBM 更致力將數十年來在此領域所累積的經驗與知識應用到其他虛擬平台上。

IBM 持續研發各項管理虛擬化系統的安全技術，推動「幻影（**Phantom**）」計畫保護虛擬機器（**VM**）及跨 **VM** 間交流的安全性，同時也透過「可信賴虛擬網域（**Trusted Virtual Domains**）」專案來強化對獨立架構的管理能力。

在增進虛擬環境安全防護的一貫理念下，IBM 將 **Internet Security Systems (ISS)**的 **Proventia®**產品線延伸至虛擬化平台上，**Tivoli®** 作業系統存取管理(**Access Manager**

for Operating Systems) 方案則增設 VM 內特定授權使用者的監控功能，而 WebSphere® DataPower® SOA Appliances 亦針對虛擬主機應用提供安全保障。

此外，IBM 「藍雲計畫」(Blue Cloud) 協助營運中心支援離散且遍佈全球的資源，而不僅侷限於本地設備或遠端伺服器群 (server farm)。

趨勢二：提升安全的多元選擇

為管理並運作複雜、專業化的 IT 安全服務，所提供服務的包裝與供應模式也愈形多元。促成此多元發展有兩大主因：

首先，IT 組織應決定需掌握多少主控權。是否放心讓其他公司提供安全防護服務？還是寧願自行管理？

其次，IT 環境的複雜度也會左右 IT 組織的安全服務選擇。有些企業的 IT 需求相較之下較為簡單及獨立，有些則需要高度機動靈活的環境，才能迅速調整 IT 服務來因應新業務需求。

除傳統軟體產品、代管式服務與委外方案外，IBM 亦掌握以下新興的安全服務趨勢：

IT 設備 (appliance)。過去 IT 設備意指「專門提供某種功能的主機」。今日設備已化身為完整的平台，不但內建各項預先安裝與設定之作業系統、中介軟體與應用程式，還可執行單一作業領域內多項功能。同時，IT 設備除外型逐漸走向模組化，虛擬化功能也增加不少。

軟體即服務 (Software-as-a-Service, SaaS)。相較於代管式服務為每位客戶提供專屬的基礎架構，SaaS 平台則供應「一對多」的服務，以單一平台同時為不同客戶提供特定的服務。此種共享式架構系統可針對無客製化需求的客戶提供標準化服務。

雲端運算 (Cloud computing)。虛擬化平台與雲端運算環境為具彈性擴充需求的高度機動環境提供支援。此機動的環境可統合管理資源池，標準化應用部署及其他 IT 服務的作業程序，在非常短的時間內導入大量服務，以公用事業的模式來提供安全服務。

趨勢三：管理風險與適法需求

許多組織正重新檢視其營運永續管理（**business continuity**）與備援策略。企業已逐漸體認到災害備援計畫的不足，因為即使是小規模的災害都可能對企業營運產生重大危害。

營運風險涵蓋所有可能影響業務流程的事項，包括偷竊、內部舞弊、設備或其他資產遺失，以及無法達到安全或其他規範標準等。由於 IT 與企業各項活動息息相關，IT 風險是企業營運風險的主要來源。舉例來說，若是未經授權但可通過安全機制進入財務報告系統，後果如何？萬一存有客戶資料的磁帶遺失該怎麼辦？資料中心停電應如何應變？企業的資安長（**chief information security officer, CISO**）若能從營運風險的觀點出發，檢視企業的 IT 安全與復原力，便能以最有利企業營運的方式來規劃時間與金錢的投資。

然而，愈來愈多 IT 作業已不受 CISO 直接管轄，隨著企業委外、商業夥伴之間的 IT 整合、採用其他企業代管安全服務或其他 IT 資源的比例增加，促使 CISO 的身分逐漸轉向政策導向與顧問角色。因此，IT 安全防護便逐漸集中於評估 IT 對營運風險的影響，以及開發能減低 CISO 管理的架構和外部 IT 資源之風險政策與管理方式。

展望未來

IBM 率先推出多項服務與方案，協助 IT 組織分析與了解營運風險。當銀行成立營運風險交換機制（**Operational Risk Exchange**）來分享營運風險資料並建立產業基準時，IBM 便提供專業分析供業者參考。IBM 銀行資料倉儲（**Banking Data Warehouse**）為一管理營運風險的有效架構，IBM Cognos 風險管理機台（**Risk Management Cockpit**）及 Cognos 商業智慧（**Business Intelligence**）系列產品則擁有單一環境內風險通報、儀表板、事件管理、計分板與風險分析等功能。

IBM SOA 政策管理策略能幫助企業追蹤安全防護策略在 SOA 服務上的成效，並將政策落實在安全標準與系統配置上。

針對安全配置的管理，IBM 以服務管理（**Service Management**）方案及 Tivoli zSecure 產品線來強化 IT 環境變革流程的控管，而 IBM Tivoli 適法管理（**Compliance Insight Manger**）、IBM Tivoli 安全規範遵循管理（**Security Compliance Manager**）與 IBM Tivoli 安全資訊與事件管理（**Security Information and Event Manager**）則可有效監控跨處理序（**out-of-process**）的安全問題。

趨勢四：用戶身分防護

在全球經濟中，數十億人每天在線上互動，身分管理成爲資訊安全的新焦點。每一筆交易的進行，都代表了用戶對交易對象及支援系統的信任。然而，隨著身分盜竊與詐騙事件層出不窮，此種信賴關係也面臨鬆動。

爲了改善身分認證品質，以及支援如醫療保健授權和銀行交易等高價值業務，政府及企業各方均積極發展身分管理系統，透過更強大的身分憑證管理系統來防堵竄改與偽造情事，以全面保障用戶的身分安全。

在商業範疇內，由於各式身分識別系統迅速蔓延，迫使個人管理自己的網路身分，在自創和第三單位設定的身分間，設法在逐漸增加的曝光中取得隱私與個人名譽之間的平衡。

未來企業的挑戰是要發展出一套共通的身分政策、流程、最佳實務、科技，以及跨服務供應商的多用途身分認證系統。這些系統需在支援複雜身分關係的同時，提供簡便的方法來管理各項共同身分識別流程及功能，包含用戶註冊與證明、憑證管理和身分應用。另一方面，身分認證系統也應適應不同社會文化情境的常規與限制，包括隱私權、個人名譽與權利等。

「我們的身分正遭受四面受敵，每隔兩秒就有人身分遭到竊取。」

—美國身份竊盜資源中心資料與統計，2007年4月30日。

展望未來

IBM建基在既有技術上，包括Tivoli身分與存取管理（Tivoli Identity and Access Management）系列產品、Tivoli zSecure套件及資源存取控管程序（Resource Access Control Facility, RACFR）等多項方案，針對現階段與未來的挑戰研擬具體持續的對策²。IBM積極與開放標準組織合作，致力爲一般用戶簡化身分管理程序。IBM一方面參與Eclipse開放原始碼基金會所主導的Higgins計畫，加入業界定義以使用者爲中心之身分後設系統（identity metasystem）的行列，以加強個人對身分憑證與資訊的掌控力；此外，IBM亦是開放標準第三單位憑證組織OpenID聯盟的一員，力圖落實用戶於多項線上服務中使用單一身分憑證的願景。IBM提供的Tivoli聯合身份管理（Federated Identity Manager）技術支援這些計畫發展。

IBM 成立可信賴身分認證（IBM Trusted Identity）計畫，旨在改良現階段身分識別系統中各種潛藏弱點與端對端整合問題，包括最易遭詐騙與竊盜攻擊之身分證明階段，以及在上線與離線狀態的身分應用層面。除此之外，IBM 亦提供技術展示與簡報，爲客戶示範如何運用 IBM 全球姓名辨別（Global Name Recognition）和客戶身分管理（Relationship Resolution）技術提升身分證明之安全防護。

趨勢五：資訊安全

在開放式協同作業環境、Web 2.0 混搭 (mashup) 技術及智慧型資料串流技術的推波助瀾下，日益增加的各型資料持續且不受限制地在企業、政府與社會網路內外流通。儘管資訊爆炸促成線上社群蓬勃發展，卻也對組織造成莫大威脅。隨著資料庫日益膨脹，資料外洩情事時有所聞，導致資料受損、不當揭露及智慧財產誤用的風險逐步升高。

愈來愈多企業高層已注意到資料受損的嚴重性，未來組織勢必得更積極地將資料外洩與遺失的風險極小化。因此，業界必須把焦點放在隱私權管理的遮蔽 (mask) 技術上，尤其是應用開發等資料保護工作中較鬆懈的非生產環境。此外，組織還應搭配加密技術，並透過簡化金鑰身分認證與金鑰生命週期的管理機制，讓隱私權管理更滴水不漏。

組織內部對整合資料管理與決策過程的需求將大幅增加。資訊安全防護，包括資料管理的任務分配、資料監控、政策導向資料分類與安全要求記錄等，應成為評估與反映特定資料庫資安成效的參考，進而形成「可信賴度指標」來輔助有關資料庫的決策過程。譬如，分數較高的資料庫可支援風險較高、較關鍵的應用，而分數較低者則僅用於較低風險的任務上。

美國隱私權益資料中心 (Privacy Rights Clearinghouse) 數據顯示³，自 2005 年統計以來，全球因安全漏洞所外洩之個人隱私資料已超過 2 億 2600 萬筆。

展望未來

IBM 具備獨步全球之硬體加密管理技術，旗下產品涵蓋一系列如 TS1120 和 TS1130 等加密磁帶機，以及具全硬碟加密技術之 IBM System Storage DS8000 磁碟系統，其中包括 IBM DB2® 伺服器的檔案系統層級加密技術。IBM Tivoli 生命週期管理器 (Tivoli Key Lifecycle Manager) 與產品生命週期管理工具能打造企業級金鑰管理架構，有助於組織以安全且一致的方式有效部署、備援、復原及刪除金鑰與憑證。

DB2 和 IBM Informix® 擁有多項存取控制功能，搭配 Kerberos 驗證後亦可支援單一登入。標籤式存取控制 (Label Based Access Control, LBAC) 機制讓系統管理員能在表、欄與列層級控制用戶的讀寫存取。

在整合性資料管理策略架構下，IBM 推出 Optim™ 資料隱私解決方案 (Data Privacy Solution) 與資料成長管理方案 (Data Growth Solution)。前者可依據 IT 政策指示執行身分刪除 (deidentification) 及身分遮蔽 (masking) 功能，確保機密資料不外洩，後者則能依照既有資料治理政策來捍衛存取歸檔資料的安全性。

這些資料保護技術能打造出可信賴的架構環境，讓企業能以充分反映資訊價值及保障用戶隱私的方式，安心地把資訊資產用於業務最佳化。IBM InfoSphere™ 與 IBM

Cognos 產品家族則能進一步建立安全架構，確保資訊的正確性、完整性、整體性與可回應性。

趨勢六：應用程式安全可預測性

2008 年，一種名為 SEO 程式碼植入（injection）或毒害（poisoning）的新型態資安威脅，影響全球高達 120 萬個網站，其中不乏一些相當知名者。隨著災情逐漸緩和，全世界開始慢慢體會到應用程式已成為駭客攻擊的首要目標。

應用程式之所以會成為駭客攻擊的對象，主要起源於應用從整體（monolithic）模式到組合（composite）模式的進展，不論是透過 SOA 式的服務編排（choreography）或 Web 2.0 式的介面工具（widget）和混搭（mashup）技術。組合應用架構廣泛採用各式來源程式碼的做法雖能大幅提升程式設計的效率，並讓非專業人員設計出精巧的應用，卻容易造成應用的安全弱點。

組合式應用最危險的地方，或許在於設計人員無法在程式部署完成以前全面掌握其組成成分與安全性，等到程式建置完成後，各種惡意程式與安全弱點可能早已嵌入應用內，任何改變也為時已晚。

為了因應這些挑戰，安全開發功能須被納入應用開發工具與平台中，才能在開發過程各個階段中執行安全診斷，並將組件掃描（component scanning）融入整合分析（composite analysis）內。組織也應追查軟體系統部署的來源，以確保關鍵應用不受侵害。由於惡意程式可以在應用程式生命週期的任何一個階段被植入，組織得建立一套嚴密的監管鏈（chain of custody）機制，以管理和追蹤軟體系統在生命週期不同階段的狀態。

展望未來

IBM Rational®軟體開發平台（Rational Software Delivery Platform）長久以來都是安全軟體開發之業界典範。此平台架構涵蓋多項產品，包括 Rational 團隊協同開發整合平台（Rational Team Concert）、Rational 資產管理（Rational Asset Manager）以及 IBM Rational AppScan®家族網頁應用安全方案，能管理軟體系統在應用程式不同生命週期階段的監管鏈，並強化軟體開發程序中的安全性測試。

IBM Tivoli 存取管理（Tivoli Access Management）產品家族與 WebSphere DataPower SOA Appliances 可保護應用程式不受未經授權存取與惡意訊息的侵害。

至於在資料層級，用戶可整合 IBM Optim 資料隱私解決方案與 IBM Rational 資料架構器（Rational Data Architect），並設定隱私權規範以應用於各測試資料庫中。

Rational AppScan 產品線能為軟體開發過程各階段增添應用掃描與安全診斷功能，並將之融入企業應用安全整體分析之中。

趨勢七：保障網絡安全

在 VoIP、視訊串流和線上遊戲等需要高頻寬的應用興起後，各界對速度與頻寬的要求愈來愈高。隨著網路傳輸速度達到每秒 10G 以上、網路流量屢創新高，服務供應商對自身系統網路流量的掌握與了解度也愈來愈低。在 IT 政策規範下，網路加密日趨嚴密，而虛擬化技術也在伺服器架構內創造出新的網路，可以預期的是，網路流量的能見度會持續下降。

如此一來，網絡安全將受到更大威脅。在虛擬化環境中，虛擬系統(guest host)可經由網絡對其他主機發動攻擊。其攻擊目標亦涵蓋會談啓始協議 (session initiation protocol, SIP) 代理主機、網域名稱系統 (domain name system, DNS)，以及包括應用協定與組織結構(schema) 在內之開放系統互聯 (open system interconnect, OSI) 堆疊。

傳統的入侵預防系統 (intrusion prevention systems, IPS) 與防火牆技術已不足以因應這些新型態的攻擊。企業需以融合整合式網絡、伺服器與端點保護技術，並具備高度擴充及協同合作功能的安全平台為基礎，擘畫完備的防護策略，才能克服這些不斷演變的安全挑戰。

「美國企業每筆受損資料的平均費用為 182 美元，換算下來，平均每一家企業損失高達 66 萬美元。」

—2006 年 10 月 Ponemon 機構調查

展望未來

IBM 在 RealSecure®家族入侵偵測解決方案 (intrusion detection solutions, IDS) 與 Proventia 產品線 IPS 方案的基礎上，致力打造新型態之整合性網絡安全架構。在 IBM ISS X-Force®研發團隊的支援下，IBM Proventia 網路入侵預防系統 GX 系列產品可為實體、虛擬及刀鋒設備提供堅實的安全後盾。此外，IBM 還有多項產品提供諸如網頁應用防護、資料遺失防治 (data loss prevention, DLP) 及入侵預防等功能，強化單一設備之安全保障。

為配合 ISS 網路安全防護方案的策略架構，IBM 為旗下產品增添更強大的內嵌式安全功能。此外，IBM 系統暨科技事業處 (STG) 和半導體團隊也透過 PRISM 計畫研發為矽晶片加入安全功能，並藉由開發以統一管理系統整合第三單位防護方案之架構，將防護延伸至企業 IT 社群的各層面。

趨勢八：捍衛行動裝置

在目前各式科技中，行動裝置的前景最令人期待，隨之而來的風險卻也最高。其多樣化的設計與應用，以及可以隨時隨地傳輸與執行資料、應用和服務的特性，皆有可能改變政府與企業管理高價值與關鍵應用交易的模式。

在行動裝置逐漸發展為新型商業通路與身分認證的主要平台之際，其安全性問題也浮上檯面。儘管行動裝置已迅速取代個人電腦的地位，手機也逐漸成為安全攻擊鎖定的目標，但相較之下，行動裝置的資安防護技術卻相當不成熟。

對此，業界須在短期內強化兩大領域：行動平台安全性及電信網絡安全防護。隨著行動平台日益開放，行動應用開發環境、部署流程和執行（run-time）環境都應加強授權與安全防護。此外，由於手機逐漸成為惡意程式與各種威脅的攻擊對象，電信業者必須在維持最佳服務層級之下，監控自身網絡內的安全威脅，以強化電信網絡的安全性。

「目前全球手機已高達 33 億支，而 Visa 信用卡的數量只有 16 億張。」 — IBM GIO⁴

展望未來

過去多年來，IBM 領先業界推出一系列服務、方案與技術標準，協助組織透過安全且穩定的方式開發行動裝置的潛能。為捍衛行動平台的安全，IBM Lotus® Expeditor 家族產品提供彙整身分認證與應用加密等安全功能的行動平台統包整合（turnkey）方案。IBM 亦推展 SecureBlue 研發計畫，以強化行動設備硬體元件的安全與防竄改技術。

在電信網絡安全防護方面，IBM 透過 BladeCenter® PN41 提供客製化的深層偵測（Deep Packet Inspection, DPI）安全功能，以協助電信網絡進防堵惡意程式與其他安全威脅。

趨勢九：即時感應之實體安全防護

IBM 在 2008 年 GTO 中曾指出，為滿足市場對系統在千分之一秒內完成感測與反應的需求，實體作業的分析時間必須縮短。舉例而言，如果在貨架上裝設 RFID 標籤，IT 系統便能隨時掌握貨物在供應鏈中的動態，並適時提出警示和執行之必要行動，以確保供應鏈運作順暢無礙。

這種「感測與回應式 (sense and respond)」的作業模式已逐漸應用於真實世界的安全防護上。影像分析技術使系統能夠透過物體、人像辨識及行為模式分析，自動執行監控。如此一來，保全人員可藉由 IT 系統，設定某一台監視攝影機來鎖定大樓內某一區域內停留超過 20 分鐘的可疑車輛，或分析歸檔畫面來找尋特定的對象或目標。

此種新型技術能加強 IT 系統對其觀測對象的理解與掌握。它與近來以行為活動模型為觀察活動分析基準的趨勢相當一致。隨著這些技術漸趨成熟，影像分析技術將被廣泛用於各型環境與研究上。

視訊監控系統的應用日益普及，其侷限性也愈形明確。最明顯的弱點是人為因素，儘管攝影機可監控一群人的動態，卻仍然需要有人盯著攝影機才能發揮效用。同時，人為監控也可能衍生侵犯隱私與個人資料外洩的問題。因此，監控攝影機的 IT 系統必須在保障個人隱私的同時，在需要人為介入的情況下適時發出警訊。

展望未來

IBM 智慧型視訊監控方案 (Smart Surveillance Solution) 採用即時感測反應科技，提供多款監控感應器與相機，強化一般數位科技的檢視功能。該方案適用於多種產業，可協助組織以開放架構平台感測並回應外界的趨勢與動態。用戶還可輕鬆地擴充此開放平台來支援新型監控科技或分析演算機制。

結論

這份白皮書指出未來二到五年間九大市場趨勢。隨著這些新趨勢興起，未來五年內，安全風險也將升高。然而，危機也是轉機。在新科技推陳出新之際，組織的風險管理策略將決定其市場成敗。

多數資安廠商專注於管理特定領域的安全風險，IBM 則致力於策略性地管理所有營運環節端對端的風險。此策略讓組織能夠由各項風險和弱點對關鍵業務流程的威脅程度，更具體地掌握和管理潛在威脅。

IBM 以其世界頂級的安全技術，滿足企業各營運流程的安全需求，協助貴公司提升整體組織的安全防護能力，進而在新興科技潮流中穩操勝券。

更多資訊

如需進一步了解新興安全科技趨勢，請與貴公司的 IBM 業務代表或 IBM 商業夥伴聯繫，或瀏覽 IBM 企業網站 ibm.com。

1. 《資料中心「內爆」……轉向新世代企業資料中心模式的必要性》，
www-03.ibm.com/systems/resources/systems_optimizeit_datacenter_pdf_nedc.pdf
2. IDC全球身分與存取管理2008-2012年預測暨2007年供應商市佔率報告，2008年8月出版（文件號#213650）
3. <http://www.privacyrights.org/>
4. ibm.com/gio