銀行實體與網路監控
從實體安全及網路資訊安全探討
陸銀行監控安全

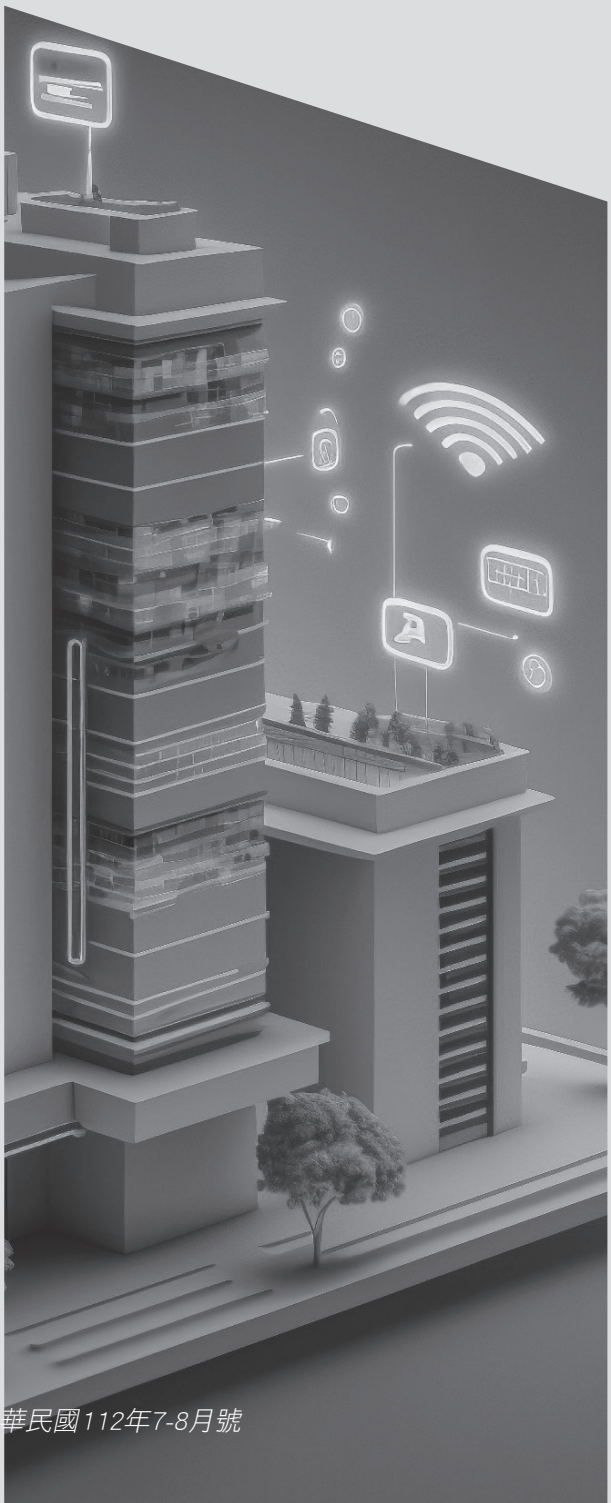
張潯福

數位金融快速發展下，帶動安全監控產品在銀行金融安全的需求逐步增溫，很多影像處理與儲存的應用與技術也相都漸趨穩定與成熟，IP數位網路化的銀行實體與資訊安全監控也越來越成為市場矚目的獲利項目，但這過程及發展中都是一路順遂嗎？傳統銀行安全監控設備就要成為古董設備了嗎？從實體到網路資安也銀行金融安全的重要課題，現在就本文金融銀行安全解決方案中以實體安全以及網路資訊安全來探討銀行的監控安全作為。

實體到資訊安全對銀行金融安全的衝擊

我們常說金融安全是一個封閉的安全需求項目，因為它是須要保密且不能公開談論的部份，從單純透過攝影機來錄影及人為操控的特定方法，已具有行之久遠的歷史，在以安全的觀念上來看它是符合金融保守及保密的要求的，不管這幾年安全監控的快速發展及網路數位化IP化的影響，銀行及金融安全仍然朝著比較務實的實體式得到摸的到的安全架構在建置銀行金融安全。但在慢慢的安全需求及管理模式變化下，金融安全在不得不面對資訊及客戶服務全面網路化的需求下，大幅提昇了銀行金融在安全的需求的應用模式，雖然全面網路化了，但在技術原則上則是仍然採用實體與網路安全監控並行漸進升級的方式，減少也降低了網路數位化對電信安裝商在實際工程轉變上的衝擊，也讓銀行安全監控得以仍然存在一些的實體化穩定應用面貌。這個說法我們可以從雖然網路

NVR技術讓安全監控的IP化加快，但所謂的數位化DVR實體安全應用仍然可以在大部分銀行營業廳安全監控使用上看得到，並且掌握到一些業主的需求，讓整體的銀行監控系統雖然號稱網路數位化，但仍然可以讓實體安全監控有實質存在意義且仍有發展的小空間。



銀行安全從實體到網路化的過程及效益

我們必須有所認知銀行金融安全監控市場，跟所有電器設備與電腦產業一樣都必須面對全面網路化、數位化及互通互聯的開放式架構的發展趨勢，銀行金融安全也一樣不可避免要面對激烈的類比數位轉換及操作上的變革，在此變格下，從類比影像轉移到數位網路影像，監控系統的架構也過去從封閉式系統轉換成為更容易調配的開放性系統環境，而傳統的同軸電纜的基礎架構，也開始導入高解析的TVI、CVI、AHD同軸及IP無線網路方式的連結寬頻無線網路，而原本單純的DVR錄影系統，也開始在NVR上整合了影像寬動態及背光等影像處理及報警和畫面動態感測等AI人工智慧影像分析加值應用，而這些新技術的整合，現階段也都為銀行金融安全監控帶來新的應用效能。而網路監控技術的導入順利則在於大量數位化的功能整合，讓更多新應用觀念及實體方式得以透過網路的環境傳輸及擷取，得到更多原本在金融安全始料未及的應用，而過去相對處於被動的平台軟體業者，也在網路化後得以在智慧監控上成為影響金融安全產監控的重要項目。

這些金融網路化的相關監控解決方案用於實際監控需求環境建置時，相對上會較傳統類比架構還要更快許多，因為網路化的建置，監控網路架設採用網路方式進行，可以不須再考量類比監控架構可能存在的距離過遠及訊號衰減、雜訊干擾與佈線限制，網路化對金融安防的各級監控要求條件來講相對也必較容易達成。銀行監控系統若選擇採「網路數位」化設備進行整合，也能將實體安全與網路技術進行資訊匯流處理，讓銀行用戶能得到更便捷的匯流優勢。而現在金融單位在建置安全監控解決方案時，也逐漸將規格設定與架設工程發包等工作，由原來的工務部門轉移到資訊部門來參與及發包處理，這個情況也跟以往由監控業者提供設備架構與規劃的方式不同，金融銀行在安全措施的運作角色也已經由可以過去的被動保守方式，轉而主動積極。而在眾多解決方案中，銀行也不會再只侷限於一定或特定專屬的網路監控架構。

AI智慧化實體的銀行安全監控網路整合

金融銀行對安全的需求已經從簡單的類比產品，轉向完善的智慧化網路監控產品和更精緻的AI人工智慧解決方案及高新技術的需求。在未來的金融安防市場競爭中，誰能更符合智慧化需求，並能提供更完美的AI解決方案，誰就是最後的贏家。網路化下智慧視頻技術在銀行中已引入廣闊的應用：解決銀行現有安防系統即時防範與降低事後調查效率差的關鍵在於引入智慧影像監控（IVS）。智慧影像監控技術能夠對影像錄影中的內容進行自動分析，利用電腦視覺與模式識別技術的最新研究成果比對與運算，還有畫面的影像資料進行推理與判斷，實現對異常事件的自動反應。目前較為成熟的AI智慧影像監控技術包括：人臉辨識、人流計算、穿著及行為辨識分析、移動偵測、盲區及重點區域防範、越區越線判斷、聚集、進出計數、鈔券辨識等。而其中更重專業的是在銀行中有著重大影響事件分析及辨識作用的一項智慧影像監控技術，那就是AI人工智慧的人臉識別技術提升應用。

AI智慧影像監控技術能夠大大地提高銀行安防系統即時防範與事後調查的效果與效率。由於智慧監控技術能夠對視頻內容進行自動分析，對場景內的異常事件進行報警，安全值守人員只需要關注異常的事件，而不再需要去回放全部的錄像，這將提高警情處理的效果和效率，降低銀行安全運營成本。智慧影像分析技術還可以對視頻錄影進行必要的壓縮比調整及搜尋索引，當有異常事件發生時，可以採用高壓縮比方式，以確保錄影採證的效果；而沒有事件發生時則可以自動降低碼率壓縮，以減少網路傳輸與存儲的負擔。藉由這些運算技術應用可以提升事件調查及破案率。同時藉由網路化的銀行聯網監控平台，加上人臉識別技術，則可以對使用ATM機的人員進行臉部影像採集，再與後台犯罪資料庫進行比對，可以達到協助警察及銀行進行違法犯罪嫌疑人員或不法分子辨識，做到金融智能犯罪預防功能。

實體到網路報警與門禁整合確保金融更安全

防盜報警系統是銀行的必要重點安防措施。銀行所有場所均需要安裝報警系統，通過多種入侵探測器和報警主機等共同組成報警系統，過去是通過電話線與當地110報警聯網。系統通過鍵盤啟動報警主機後，進入防範狀態。如有人非法進入防區，則會觸發入侵探測器，系統會檢測並確認報警信號，即發出警報聲，同時將信號傳送到控制主機發出報警，達到防範作用。工作人員進入時只需通過鍵盤解除防盜系統（即撤防），則防區內探測器暫時關閉。遇到不法之徒進行打劫時，按緊急按鈕或相應的緊急裝置，向銀行監控中心及當地派出所勤務中心求救，控制主機將針對預先設定的電信位址代碼及報警類別透過電話線發到報警中心（即110、派出所）從實體走到網路化後，報警中心電腦檢測到送來資料並進行識別，從資料庫調出相關資料，顯示警情資訊和位置等其他情況。另外，控制中心的報警主機自動不定時檢測前端各報警系統工作情況，如信號中斷或控制系統有故障即可自動提示並列印出故障發生在某個區域的系統；同時，報警資訊聯動CCTV數位監控系統，將報警現場附近的攝影機影像切換到監視畫面，並聯動數位錄影機進行錄影。

門禁整合網路化，門禁是感測器技術及資訊處理技術的發展而成的一種安全防範技術，它實現了人員出入的自動控制。與傳統的鑰匙和鎖頭相比，現代化的網路門禁出入控制技術安全程度高、功能多、易管理。近幾年隨著感應卡技術、生物識別技術的發展，門禁系統也得到了飛躍式的發展，進入到成熟期，出現了感應卡式門禁系統、指紋門禁系統、虹膜門禁系統、臉部識別門禁系統；它們在網路化安全性、方便性、易管理性等方面都各有特長，使銀行門禁系統的應用領域越來越廣。

數位網路化後銀行資訊安全的大小問題

目前在銀行網路化後銀行資訊安防系統都會存在一些或大或小的問題，銀行在安全防範中都採用了人防、物防和技防三種基本防範手段，建立了初步的安防系統，為確保銀行有關業務的安全運行發揮部份作用。但由於技術水準及網路安全維護的限制，這些運行的金融資訊就會存在以下這些資訊安全與如何最好網路安全的防禦問題，首先我們看到銀行內外資訊互不相通問題，在網路化下原本應該是網路暢通八達的結果才是，但事實上則是像資訊孤島現象嚴重。多數安防系統在網路化仍然各自獨立運行，安全保安管理的資訊也散佈於各個子系統中，沒有辦法充分運用。再來則是系統功能不統一、不規範，缺乏整體規劃和統一的建設標準，技術水準參差不齊。這也是一個重要問題之一。

台灣金融界大約從90年代開始陸續推動存款系統連線作業，但那個年代還沒未出現互網網路，整個金融連線都在一個封閉網路進行，所謂的資訊安全也就沒人看重甚至只在乎臨櫃的作業層面的安全控管。由此看來在沒有從實體走上網路化前，銀行資訊安全之意大概只是指總行與分行間的連線系統而已，因此資訊安全的範圍也就只局限於傳統資訊安全概念的銀行內部而已。然而到了金融安全網路化時代後資訊安全的範圍就不一樣了，隨著科技的發達，負責資安的銀行IT人員只要想到USB存取的控管，就倍感壓力，USB用於存取資料，具備便於攜帶的特點、儲存量也不小，若不控管，資料可能很容易就外洩。對於銀行各種作業上不管是客戶個資或是監控錄影；都無法嚴加控管加上網路普及，因此資料外洩時有可聞。但銀行資訊安全不該只是這個而已，銀行網路安全令另一個擔心是伴隨上網行為的駭客攻擊，網路攻防越演越烈，銀行很難落實防禦。因此在安全從實體走到網路化時，銀行對資訊安全應有更多的關心與責任，資訊安全的範圍更清楚的跨越出銀行內部，且應該達到監控以外的客戶及金融資訊安全部份。要知道這些資訊安全必須要做到比下三項銀行資訊安全防禦方可達成：首先是銀行端資訊安全之防禦，銀行端之防禦包含建立安全防護、提高系統可靠性之措施及制定作業管理規範等三方面。在建立安全防護，銀行可以採取建置安全防護軟硬體，如防火牆（Firewall）、安控軟體（弱點掃描機制Port Scan、安全評估機制Security Assessment或滲透測試Penetration Testing）、偵測軟體（入侵偵測

機制IDS，Intrusion Detection System或入侵防禦機制IPS，Intrusion Prevention System）等。設計存取權控制（Access Control），如使用密碼、身分證字號、磁卡、IC卡等機制。系統提供各項服務功能時，應確保個人資料保護措施，如網際網路連線通道安全機制（SSL，Secure Socket Layer）或虛擬專用網路（VPN：Virtual Private Network）。同時此外近年來，較受銀行採用的還有內容保護（Content Protection）相關安全機制，如文件管制機制、垃圾郵件過濾機制、郵件安全機制、網路內容過濾機制、即時通訊軟體（Instant Messenger，簡稱IM）過濾機制、網頁內容即時保護機制等。再來就是客戶端之防禦也就是身分識別（Identification），客戶簽入（Login）是網路銀行之身分識別的方法，目前銀行客戶簽入採「用戶代號」及「密碼」進行身分識別，根據「金融機構辦理電子銀行業務安全控管作業基準」之規定，「用戶代號」不得使用客戶之顯性資料(如統一編號、身分證號及帳號)，密碼與用戶代號不應相同，原則上密碼效期一年，變更密碼不得與前一次相同，首次登入時，應強制變更預設密碼，而且用戶代號及密碼均有複雜性之要求，如不得少於六位，不可訂為相同的英數字或連號數字，若連續錯誤達五次，不得再繼續執行交易等等安全設計規範。另一個`客戶端之資訊安全防禦就是交易認證（Authentication），金融界從1993年開始提供「稅費EDI服務」（EDI，Electronic Data Interchange，電子資料交換，係指透過共用的標準資料格式，經由電子傳遞方式，不同公司不需重複鍵入，讓電

腦能夠自動傳送處理資料的作業），當時EDI作業的安全核心就是使用PKI（Public Key Infrastructure，公共鑰匙基礎結構）技術，PKI係指傳送方與接收方使用非對稱性金鑰方式，以一對公開金鑰（Public Key）和私密金鑰（Private Key）來進行交易之電子簽章（Digital Signature），在執行交易的過程中，提供一個安全嚴密之平台。

實體到網路化在銀行安全的雲端應用

銀行安全從實體到網路化後，雲端智慧化概念已經成為安全解決方案另一層應用，但共享服務的概念服務卻使雲端的安全性成為多數銀行使用者心中的隱憂。儘管各大雲

端提供者皆表示有提供安全雲端服務的能力，可是根據研究顯示，安全性問題仍是銀行在網路化後決定採用雲端服務之前疑惑不前的主要因素，要說明雲端如何在安全監控上的安全性對於銀行資訊安防業來說是一個很大的考驗，以雲端服務SaaS來說可以更迅速和容易地去更新以及管理監控軟體和服務，它也提供更有彈性的整合能力和開放介面，許多SaaS雲端服務供應商開始提供安全監控模式的協作功能或開放介面（APIs）。雖然雲端架構能夠提供靈活和具有成本效益的應用使用環境來取代過去實體監控管理模式，但雲端監控並非完全沒有風險。因為轉移到託管平台，而不是留在銀行自己內部，金融單位勢必然會犧牲許多對於營運環境的控制。特別是在雲端SaaS裡，銀行安管單位幾乎只能選擇要上傳監控資料或不上傳部份數據，而剩下的就不是銀行本身能掌控的。但同時銀行還得為自己的資料保護負起法律和監管責任。所以銀行安全監控雖然已走到網路雲端化，但雲端的應用至今仍不普遍的現象是存在原因的。因為雲端SaaS監控環境下的風險其實有許多種，而且大部份都來自雲端所提供的好處相關。正如前面提到的，你的雲端服務供應商透過某些網路化來分析了解你對監控平台服務的使用狀況，既然他們能夠存取你所有的資料，這也代表會產生未經授權存取或被內部員工竊取或竄改監控資訊的風險。

目前大家都在強調金融機構及電子銀行的安全，且已從傳統銀行網路化延伸到ATM及無人化銀行，銀行對於安防系統建置的需求及技術也不斷的發展，政府金融監管單位也開始對銀行安防系統走向聯網化及智能預警要求的指令逐漸明確。而金融銀行安全技術研究發展部份，當前銀行安防行業從實體化已邁向網路化及AI智慧化方向發展，新的技術、產品和針對銀行現有金融安全監控系統不足部份不斷的推出各式不同設備及措施應用的解決方案，而實體化與網路化兩者的結合將推動銀行安防行業永續的發展。