

# 2006金融業務 電子化資訊安全研討會

金融產業因其獨特性，對資訊安全以高標準看待，面對電子化後的安全問題，2006金融業務電子化資訊安全研討會邀請產、官、學各方專家一同來探討。

文 | 王婉伶

Fortinet於11月16日在亞太會館舉辦「2006金融業務電子化資訊安全研討會」，以銀行、證券、保險業等金融相關產業為主要訴求對象，其主要目的在於協助金融機構電子化後，因應市場變化進行整體佈局，增加商機及競爭力。會中邀請產、官、學專家，依我國電子金融資訊安全政策、通訊及支付卡產業標準之發展(PCI Standard)等議題，提出相關的注意事項及解決方案，並佐以實例進行探討。

## 相關法規的需求與了解

研討會特別邀請到財金資訊公司資深工程師暨銀行公會資安小組成員范姜群暉以『個人網路銀行業務服務定型化契約範本』一對銀行資安衝擊及因應策略為題，針對目前金融業資訊安全相關法規及在明年1月1日即將正式實施的「個人網路銀行業務服務定型化契約範本」做一簡單的解釋。范姜群暉表示，金管會於今年六月公告「個人網路銀行業務服務定型化契約範本」新範本，其內容採納行



▲ 2006金融業務電子化資訊安全研討會以銀行、證券、保險等金融相關產業為主訴求對象，協助其在電子化後因應市場變化進行整體佈局。

政院消費者保護委員會、學者專家及業者代表等意見予以修正，由原來的24條，新增為27條，其中修改23條，新增3條。

新增的內容包含1.網頁之確認，意即為防堵詐騙集團偽造網路銀行網頁詐取客戶之帳號密碼，規定客戶在使用網路銀行前必須先確認網路銀行正確網址後方可使用該服務。而銀行也應盡善良管理人之義務，隨時注意有無偽造之網頁。2.電子訊息交換作

業時間，增訂「未到期之預約交易在銀行規定之期限內，得撤回、撤銷或修改」之條文。3.保密義務，意即若經他方同意，告知第三人時，第三人應負保密義務，若「前項第三人如不遵守此保密義務者，視為本人義務之違反」以加強保密責任。而修正的內容與資訊安全較為相關的部份，例如第13條，加重銀行舉證責任、第18條，紀錄保存，須由雙方共同保存交易指示類電子訊息記錄等，並增列客

戶使用網路銀行注意事項，讓兩造雙方都應盡其善良人的義務，保護雙方的權利及義務。

安侯企業管理顧問股份有限公司資訊風險管理部協理謝昀澤則從「法規與稽核規範到資安實現－談金融業資安應用的積極作為」來說明金融業常用的資安規範、常見的網路安全稽核發現及應有的積極作為。謝昀澤表示，現在金融業大量依賴網路系統來開拓新業務，從慣用的封閉性系統走向開放性的環境，往往有先天上的風險，且金融商品不斷推陳出新，流程控管的嚴謹度及自動化的程度往往無法配合；內部資訊人員權限控管不當，不易被發現；資安及稽核人員的不足也常給有心人士可乘之機；金融業大多採取對既有文件及機制作事後的監督，少有即時監控反應的機制等，這些都是造成金融資訊犯罪的主要因素。

因此金融業在資訊安全的要求上就要更加嚴謹，

目前金融業多必須遵循的資安法規有幾種，例如，新巴塞爾資本協定作業風險管理與資訊安全相關之要求、公開發行公司需建立內控制度、刑法及個資法等之電腦犯罪相關資安法令、VISA與Master等國際組織對資訊安全之查核要求及ISO27001等國際資安標準等。

除了法規遵從外，稽核也是金融業資訊安全要求上重要的一環，謝昀澤指出，在進行稽核時，有幾項常見的網路安全問題，例如對弱點的發現與管理不夠周全、網路使用者身分與設備的驗證不夠完整、網路事件的管理與事故的處理不夠周延等，我們可透過幾項通用網路安全稽核的準則來落實安全稽核，了解網路安全的基目標與程序、如何被落實、誰負責管理或執行、相關的方法及機制的執行證據在哪、何時執行等。金融業的網路安全不止是要抵抗外部的威脅，要轉移對網路安全的完整管理，提升金融網路的安全性。

## 整合式深度防禦

談完了法規的規定及金融業

該注意的事項，接著，來到實際應用面，Fortinet資深技術顧問劉乙，以UTM如何佈署資安整體解決方案之優勢為題，說明目前如何利用整合式防禦系統來做到深度防禦。劉乙表示，一個好的整合性防禦系統除了要全面性整合安全防護，還必須操作介面友善、建置容易，更要能建置企業之資安架構標準規範。

研討會中除了解解決方案的說明外，更以實際案例來加深與會者的印象，包含凌群電腦產品經理陳奇民以日盛國際商銀為例，說明如何對ATM進行安全控管，化被動為主動，防止異常情況發生；接著由台灣電訊技術部經理林傅凱以目前常見的幾項金融服務，如IP-ATM、證券交易系統、信用卡刷卡機為例說明如何建置有效的安全防護。除了國內的案例外，難得邀請到香港電訊盈科萃鋒公司資深副總裁陳真良博士帶來香港的金融交易網路之保安設計案例，除了說明目前所面臨的威脅外，也說明了其保安的設計理念，值得與會者參考。

## 結論

隨著金融產業邁向電子化的同時，其面臨的網路安全威脅因其產業特性而更加嚴重，如何落實並保護其內部機敏資料的安全，當為金融產業的首要之務。

網站文章編號：IS3727  
[www.informationsecurity.com.tw](http://www.informationsecurity.com.tw)

