行政院及所屬各機關出國報告

（出國類別：實習）

網路銀行的金融監理機制探討

服務機關：中央銀行金融業務檢查處

出國人　職　　稱：辦事員

姓　　名：吳宗錠

出國地區：美國

出國期間：九十年五月十三日至六月十一日

報告日期：九十年十二月七日

系統識別號:C09002952

公 務 出 國 報 告 提 要

頁數: 35　含附件: 否

報告名稱:

網路銀行的金融監理機制探討

主辦機關:

中央銀行

聯絡人／電話:

／

出國人員:

吳宗錠　中央銀行　金融業務檢查處　辦事員

出國類別: 實習

出國地區: 美國

出國期間: 民國 90 年 05 月 13 日 -民國 90 年 06 月 11 日

報告日期: 民國 90 年 12 月 10 日

分類號/目: E0／綜合（經濟類）　E0／綜合（經濟類）

關鍵詞.　網路安全,電子銀行,知識經濟,金融監理

內容摘要: 網路安全在過去的幾年內一直都是重要的議題。由於網際網路的蓬勃發展，網際網路的安控就成爲系統管理者關心的主題。因爲網際網路的普及性與其上網的便利性，任何人只要具有相當電腦基礎的人都可以在世界的任何角落侵入電腦系統。而在網際網路普及以前，這種情形則十分罕見。網路安全包含了藉由設置防火牆，封包過濾法，入侵偵測系統以及經常地檢查網路的漏洞等方式來防範遠端攻擊。網路銀行由於在公開環境下傳送極機密與敏感性的客戶個人及交易資料，因此對安全性的要求程度自不待言，甚至可謂網路安全是網路銀行的核心產品，面對銀行業對資訊系統的日益依賴，金融監理機構所面臨的挑戰也遠甚以往，除了以往對金融機構點狀項目查核外，更需要提出前瞻性的綜合安全風險評估。本文最後並建議建構知識經濟指標資料庫，以瞭解掌握知識經際對我國總體經濟的衝擊與影響，並可作爲制定政策與金融監理之輔著工具。

本文電子檔已上傳至出國報告資訊網

目　　錄

圖

表

網路銀行的金融監理機制探討[1]

中央銀行金融業務檢查處
吳宗錠

網路安全在過去的幾年內一直都是重要的議題。由於網際網路的蓬勃發展，網際網路的安控就成為系統管理者關心的主題。因為網際網路的普及性與其上網的便利性，任何人只要具有相當電腦基礎的人都可以在世界的任何角落侵入電腦系統。而在網際網路普及以前，這種情形則十分罕見。網路安全包含了藉由設置防火牆，封包過濾法，入侵偵測系統以及經常地檢查網路的漏洞等方式來防範遠端攻擊。網路銀行由於在公開環境下傳送極機密與敏感性的客戶個人及交易資料，因此對安全性的要求程度自不待言，甚至可謂網路安全是網路銀行的核心產品，面對銀行業對資訊系統的日益依賴，金融監理機構所面臨的挑戰也遠甚以往，除了以往對金融機構點狀項目查核外，更需要提出前瞻性的綜合安全風險評估。本文主要對網路銀行核心資訊系統提出風險評估模式，信用風險、法律風險、利率風險等屬於經濟、策略、產品層次風險則非本文探討重點。

第一章　前言

職奉派赴美國研習網路銀行的金融監理機制探討，期間自民國九十年五月十三日至六月十一日，共計三十天 ，研習單位為 THE BANK OF NEW YORK、STATE OF NEW YORK、CITIBANK、FEDERAL RESERVE BANK OF NEW YORK、FEDERAL DEPOSIT INSURANCE CORPORATION、COMPTROLLER OF THE CURRENCY ADMINISTRATOR OF NATIONAL BANKS、BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM 等七個單位，以會議討論方式進行[2]。

---

[1]感謝中央銀行金檢處陳處長上程、胡稽核亞生、檢查科張科長英吉、電腦科李科長俊勳提供專業見解、中央銀行駐紐約代表辦事處孫代表全玉及代表處同仁的協助與行程安排，賴副處長鎮戊、徐副處長仁光、賴副處長武吉、管理科曾科長仲達、調研科林科長華亭、海外科許科長國勝、資料科林科長銘寬、考核科謝科長秀鳳、馬專員裕豐的鼓勵、指導，調查研究科吳專員秋月、林平專員、考核科李專員佩真的行政支援，以及出國期間本處檢查科同仁於工作上的分勞，在此一併致謝，本文所有觀念上及文字上之謬誤由作者自負。

[2] 感謝 William W Ferguson, David Solo(Citibank),Edward Valdes, Ganny Y Kwan, Regina A Stone, Jacob Joseph(State of New York), Michael P Wallas(Board of Governors of the Federal Reserve System), Jean M Dugan(Chase), Lanu T Duffy, Kenyon T Kilber, Thomas Tuzinski(Federal Deposit Insurance Corporation); Hugh C Kelly, Clifford A Wilke, Susan C Hopkins(Comptroller of the Currency

網路發展已使企業或銀行由傳統的區域網路轉向網際網路，由使用網路傳送資訊及提供資訊、廣告，轉向透過網路提供服務、進行電子商務，由單純的想要趕上網路熱潮轉向真正由網路來增加產能、提升競爭力而獲取賺錢的機會。因此愈來愈多的人對電子商務感到興趣。對多數的人而言，電子商務或許只是在網路上販售產品，屬於新興的通路之一，但事實上，電子商務決不止於如此：透過網際網路提供客戶服務、金融商品、提供上下游廠商技術支援資料、甚至於在網站上進行財務調度，這些都是電子商務的範圍。無論如何，廠商都會思考是否能透過網際網路來增加新的商機，以及和客戶、廠商們做更密切的連繫、擴大業務市場、提高產能、增加客戶滿意度及降低成本。可以確定的是，企業或銀行透過網路傳遞的資訊將越來越重要而且需要受到保護。而銀行也因為客戶對網路的需求，而加強其網路產品的開發，但在一連串的動態反應中，是否市場中存在有動態一致性的問題（dynamic consistency）[3]及道德危機的現象，這些都是在發展網路銀行業務及對其監理時所必須的考量。在探討網路銀行的經濟現象與對通路的衝擊前，我們將研討的範圍縮減到網路經濟的基礎—安全假設，因為資訊安全是網路銀行或電子商務的核心產品，而對於網路銀行的金融監理，本文也試圖提供一內在性質的評估模型，因為點狀的檢查表已採用多年，而綜合的風險評估則仍持續建構中，對網路安全的評量架構有著整體的看法，將有助於整合所檢查得知的點狀現象。

本報告分為五章，第一章為前言，說明本次研習主要內容；第二章為介紹網路銀行網頁及業務內容；第三章為說明網路銀行之風險評估；第四章簡介資訊安全政策的觀念建構；第五章為此次研習之結論與建議。

職才疏學淺，倉促成筆，漏誤之處，尚請指正。

第二章　網路銀行網頁服務及業務內容

網路銀行特質，不僅使用者容易使用，也容易執行，而且也可用以訓練及研究等目的。網路銀行主要的服務項目大約可以分為下列二類：

Administrator of National Banks), Monroe L Davis (The bank of New York)寶貴意見與資料。

[3] 動態一致性係賽局理論中動態賽局由於不可信的威脅或訊息所產生的不合理的均衡解。

金融商品及服務

線上銀行（on-line banking）

可以隨時查看存戶的帳戶餘額及交易明細

個人理財（personal finance）

可以容易以網路銀行所提供的附加價值服務處理存戶本身財務活動

小企業銀行（small business banking）

專為小企業的創新產品

商業銀行

為中型企業與大型企業提供財務金融服務

國際貿易與金融

幫助企業找尋所有的全球財務利基

特殊特質

新事務（what's new）

有關本銀行位址新進的消息

經濟評論（economic commentary）

對當地及國際經濟趨勢的深度分析

工作機會（employment opportunities）

尋找高能力之員工

購物（shopping@wwwbank）

安全地在虛擬的 mall 購物

其他網址（netsites）

探尋其他有趣及廣泛的網頁

雖然網路銀行並非是完全新的領域，但仍然有某些特質與向度對銀行家與監理機構構成新的挑戰，聯邦存款保險公司（FDIC）將網路銀行可能面對到的風險大致劃分如下：

作業風險

消費者預期高度可靠的系統可以使得他們能夠使用他們的帳戶並且可以線上

完成他們的交易。不可靠的系統可能使得消費者對銀行有負面的看法。

關於作業風險的管理包含了擬定應變計劃提供另一種方式的服務以滿足客戶的需求（如 1-800-numbers），並對資料備份的完善的管理，以及對作業系統、伺服器、其它的電腦硬體建立備援單位等措施。同時也應該擬定公共關係處理準則以處理由於系統嚴重中斷服務所造成的負面影響。

技術風險

網路銀行的主要核心產品就是安全與完善地管理技術風險的能力。這意謂著對銀行系統適當的安控及監督，以及整合不同軟體及平台的介面能力。技術風險的管理包含了適當的管理，技術性層面委外製作，監督及測試系統績效，設置防火牆與其它的網路監控軟體，以及整合的技術計劃的更新。

信用風險

信用風險通常是指借款客戶到期無法還款的風險。網路銀行的信用風險對金融監理產生了新的挑戰。網路銀行可以提供世界各地的客戶服務，因而地域對網路銀行已不構成重大的限制。但是透過網路銀行來處理客戶的申貸資料使得傳統認識客戶的面對面方法來驗證客戶資料的正確合法性有所限制。另外網路銀行的借貸行為可能集中於據點區域外的客戶或是集中於某一產業。因此管理當局必須小心地對網路銀行的借貸仔細評估。在評估後網路銀行以也必須衡量那種型態的借貸對網路銀行是不適當的。

從以上網路銀行的服務內容及聯邦存款保險公司劃分的風險而言，我們可以瞭解網路銀行主要依靠資訊系統的資料處理能力，以提供客戶安全、隱密及快速的金融服務並且可以以無實體商店的方式存在提供客戶購物轉帳等以往傳統銀行所無法提供的附加價值的商品服務[4]。因此整個系統的穩定性與高度的安全控管措施幾乎是網路銀行的商品核心。惟有使客戶信賴網路銀行的交易、資料安全性才可以避免顧客對銀行服務的品值產生懷疑進而產生反向選擇的效果而使得網路銀

[4] 網路銀行由於進入成本低，致使進入市場者眾，競爭激烈，而其競爭策略常為價格競爭，反致無利可圖，且其無法提供面對面的金融服務，故無法取代傳統銀行的功能，目前反倒是傳統銀行都或多或少具有網路銀行部們，主因是提供客戶多點選擇，且競爭銀行也有此服務。

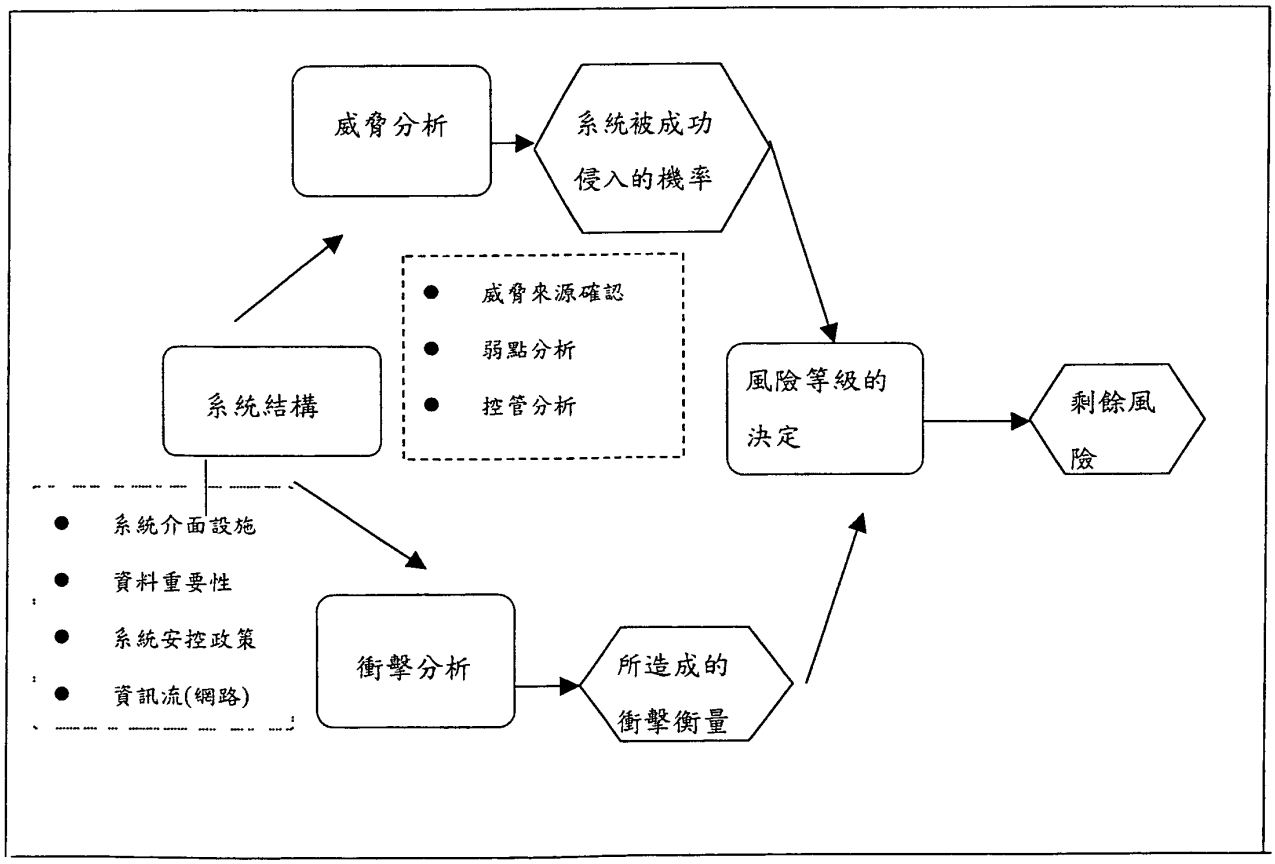
行市場的失敗。因此本文主要以綜合風險的角度來探討網路銀行的監理機制並以提供金檢人員對資訊系統查核有著全面性的考量與判斷。

的權限不設限所引發的問題會較少些。經常我們可以聽到在分公司的職員也可以直接到總公司的伺服器環境中截取資料，或是總公司可以不受限地直接進入分公司的系統。因此必須小心地規劃使用者的權限。

風險管理的基石就是風險評估，也就是銀行對其資訊系統的評量並決定系統的風險水準的過程。這一過程的結果是剩餘風險及決定是否剩餘風險是可接受的或是必須採用額外的控管措施以進一步降低風險。

風險實際上是安全事件發生的概率與這事件對銀行的衝擊的程度的函數。安全事件發生的概率主要在於對系統的威脅程度與系統本身的弱點的綜合分析。衝擊程度則是對系統支援銀行服務的重要性評估。圖一是上述觀念的描述，各別的細節將在以下說明。

圖 一　　風險評估觀念圖



3.1 系統介面設施及相關設備

界定資訊系統的範圍可以建立風險管理的範疇與深度，並進而搜集相關主要資訊來訂定風險。此一步驟不僅可以使得檢查人員瞭解資訊單位的任務及系統作業與來自資訊科技（IT）對銀行可能的潛在衝擊。因此在此一階段，構成資訊系統的資源與資訊範圍將被確認。基本上可以劃分如下：

- 資訊架構
- 硬體設施
- 資料與資訊
- 人員
- 系統介面與連接點

另外也可以多蒐集系統資訊與資料，如：

- 單位的任務
- 系統處理資料的過程
- 系統所須的功能
- 系統使用者
- 所有應用系統的安控政冊（使用者權限、金監機構的要求、法令規範..）
- 系統的安控架構
- 系統的作業環境
- 與系統相關的設備(機房)
- 系統儲存媒體容量
- 系統資訊的流動情形

對一個已存在的作業系統，資料的蒐集不限於已文件化的訊息，儲存於系統中的所有資訊都應涵蓋。而對於正發展中的系統，則必須界定主要的安控法則及未來系統的屬性。

對系統的描述也應包含發展系統的假設及相關的資訊來源。在某個問題上，

文件可能是缺乏的，或是討論可能不是那麼週全的情況下，假設可能是必須的。因為在目前架構上或是未來系統架構上的假設，才能使檢查人員作一合理的推論與評估。

3.2 威脅分析

沒有系統上的弱點，威脅源並不構成風險，因此在決定入侵的可能性，必須同時考量威脅源、弱點與現時的控管措施。

3.2.1 威脅源的認定

威脅源可以定義為在認何情況或事件存在可能性使得資訊系統受損。在此定義下我們可以將威脅源區分為三類：

- 自然威脅—洪水、地震、颱風、土石流等等及其它非人力可控制之事件。
- 人類威脅—由人類的故意或隨意或種種意圖的行為（如散播病毒、所撰寫的程式有漏洞、網路上的攻擊、未經授權的讀取機密性資料）。
- 環境威脅—長時間的停電，污染，化學或有毒液體的溢流。

自然威脅與環境威脅主要由系統所在位置來決定，例如系統設置在沙漠則無須考慮洪水的威脅。

人如果要成為威脅源，動機及其完成攻擊所擁有的資源就必須列為考慮。表一對攻擊者的類型、動機與方式作一個概述。因此我們必須使用系統特質的資訊，來決定該將攻擊者歸類。一旦攻擊者已被歸類，我們就必須對完成攻擊所需具備的能力與資源作一分析。這類分析涵蓋了使用自動登入軟體從外部連線到系統完成攻擊到普通不為人知的系統弱點。

威脅源	動機	方法
駭客；cracker	自我實現、挑戰、反抗心	入侵系統、未經授權進入系統
犯罪者	不法資訊的取得、金錢利益	犯罪/入侵、賄賂
恐怖份子	黑函、破壞、利用	系統攻擊/入侵
國外利益團體	分類的資訊、其它政府的訊息	入侵/滲透
內部員工（舞弊、疏忽或是不誠實）	智慧、收入、自我實現、金錢利益	入侵、電腦的濫用、未經授權進入系統

3.2.2 弱點分析（Vulnerability Analysis）

弱點分析主要是找出可能被潛在威脅源使用的系統本身規劃疏失或是弱點。這一步驟系統性分析和系統規劃相關的技術與非技術的弱點。現場觀察、與系統或資訊人員面談、以及詳閱所有相關的系統及組織文件都是搜集作弱點分析所須訊息的方法。弱點分析的型態與所用的方法隨著系統規劃時的理念與系統本身的特質不同而異。

如果系統尚未規劃，那弱點分析的重點主要在於安全政策、程序與系統定義。如果系統已經在規劃測試階段，弱點分析則要包含系統設計文件。如果系統已經上線作業，弱點分析則要決定及分析系統本身安全特質與安控程序是否可以抑制風險的產生。

弱點分析主要應用的方法有：

- 自動弱點掃描
- 網路對映
- 安控測試與評估
- 滲透測試 [6]

[6] 滲透分析及弱點分析等概念，請見附錄2。

另外可以蒐集相關文件或資料，如：

- 前次風險評估
- 稽核報告、安全評估報告、系統測試及評估報告。
- 系統已知弱點資料庫
- 系統安全顧問諮詢
- 廠商諮詢
- 系統軟體安全分析
- 系統異常報告

銀行應該主動尋找或是分析所有可以幫助弱點分析的資源。如果威脅源的能力不足或是銀行有一套有效的安控程序，系統的缺失並不會被威脅源利用而使系統暴露風險中。

3.2.3 控制分析

控制分析的主要目的是對先前所蒐集的系統資訊判斷是否與目前的安控制度相符。系統的安全控管情形可以從以下的資料來做判斷：

- 安控政冊與指導方針
- 系統操作程序
- 系統安全設定
- 產業安全標準與實例

安全控管大致上可分為三個領域。在每個領域中，有的控管是用來預防安全控管事件，有的則是用來偵測安控事件。

技術控管[7]包含了電腦硬體、軟體與韌體。表一列舉一些技術控管的方式來降低風

---

[7] 讀者如想對技術控管有基礎概念，可參酌各類技術手冊，或中央存保股份公司一等專員紀慧敏

險。

表 一　　技術控管的例子

預防	偵測
登入控管機制[8] 防毒軟體 認證機制 防火牆 加密	稽核軌跡 入侵偵測系統

作業控管主要指作業程序、人員與實體安控措施以確保電腦資源的安全。表二列舉一些作業控管的例子以降低風險。

表 二　　作業控管的例子

預防	偵測
安全的認知與訓練 災難復原計劃、緊急應變計畫 背景調查	安控評估與稽核

管理控管主要指的是系統管理與風險控管。本質上管理控管都是屬於預防性的措施。包含了安控評量、風險評估與行為法則。

3.2.4 風險可能性的決定

風險評估的最後一個步驟就是風險可能性的決定。影響風險機率的因素有威脅源的動機與能力、系統弱點的性質與相關防範措施的效度。基本上我們可以將

89.11.9 出國報告「美國金融業電子銀行業務之網路架構安全控管及稽核方式之研究」第四章第三節第四節之查核重點簡介。

風險機率概分為高、中、低度風險。表三簡述了這三個風險衡量。

表 三　　風險可能性的定義

風險可能性	描述
高	威脅源有著高度的動機與足夠的能力且防範措施並不有效。
中	威脅源有動機與足夠的能力但防範措施可以有效阻擋。 或 威脅源並無特定動機或是只具備粗淺的知識與能力。
低	威脅源無動機或能力或防範措施可以完全的遏阻或偵測攻擊行為。

3.3 衝擊分析

由於威脅源所造成的安控衝擊主要可說是資訊安控五個目標—整合性、可用性、隱密性、記錄性、可靠性--的喪失或降等。

- 整合性損失。如果系統資料或設定有過未經授權的變更，無論這種變更是無意的或是有意的。系統資料與設定所造成的整合性損失與可用性損失所造成的衝擊有些類似。但是，如果系統或資料的整合性問題一直都沒有發現，繼續使用系統或資料未來可能會有問題。而且，違反整合性(1)可能是要達成對隱密性或可用性成功攻擊的第一步。(2)降低系統的可靠性。
- 可用性損失。如果系統使得授權人員的授權功能部分或完全無法使用，那任務可完成性就受到影響。例如，系統功能及作業效度受損可能導致公眾對系統的信賴度或是損失寶貴的生產時間及效能。而且系統資源未經授權的使用將會導致額外的信賴度損失與義務。
- 私密性損失。私密性指的是指防止資料（使用者及系統資料）避免未經授權的公開或揭露。未經授權資料的公開與揭露所造程的影響程度嚴

[8] 有關登入控制方式，詳見附錄 1。

重可能使銀行遭到控訴或倒閉，最輕可能使得公司難堪。

- 記錄性損失。記錄性指的是追蹤個別使用者使用記錄及其於系統中行為的能力。記錄性可以協助不可否認性、嚇阻、錯誤認定、入侵偵測與防止、事後的復原與法律行動。記錄性損失的衝擊就是對實行上述能力所造成的影響。除此之外，降低系統或是銀行記錄性的能力通常是為了達到其它目的，如可用性、私密性、整合性的攻擊行為的一部分。
- 可靠性損失。可靠性是其它四項目標（整合、可用、私密、記錄）已被適當的執行的信賴基礎。缺乏可靠性意味著無法有效管制無意的使用者或是軟體錯誤與誤用，或是對有意的滲透或跳板平台沒有適當的防制能力。一個成功的利用系統弱點的滲透攻擊行為意指系統的信賴度的降低。

有些衝擊可以量化，如以損失的收入，系統修復的成本，或是系統被成功攻擊後找出問題所在的努力成本。也有無法量化的無形衝擊成本，如公眾的信賴度、系統的可信度，因此必須以質化的觀念來衡量，如高、中、低等質化單位。表四簡述上述質化的觀念。

表 四　　衝擊衡量

衝擊	描述
緊急	寶貴資料無法使用、竄改、揭露、毀損或是系統資產與服務無法使用導致重大的立即性損失
高	重要資料無法使用、竄改、揭露、毀損或是系統資產與服務無法使用導致任務完成的程度受到嚴重的影響。
中	重要資料無法使用、竄改、揭露、毀損或是系統資產與服務無法使用導致任務完成的程度受到影響。
低	重要資料無法使用、竄改、揭露、毀損或是系統資產與服務無法使用導致任務完成的程度受到輕微影響但不致於造成重大損失。

量化的標準與質化的標準各有優缺點，量化的標準可以使我們進行成本—效益分析但衡量的單位可能無法明確區分，而質化的標準雖然是主觀的判斷，但確

對問題的改善與風險程度的高低作一評估。最終的風險衝擊分析則須植基於這兩種標準的總合橫量。

3.4 風險程度的決定

風險程度的決定主要根據上述威脅與衝擊的程度來決定。表五是威脅發生的可能性與衝擊所決定的風險程度。

表 五　　風險程度的決定

衝擊	威脅發生的可能性		
	高	中	低
緊急	緊急	高	中
高	高	中	低
中	中	中	低
低	低	低	低

3.5 風險降低

經過風險評估後所發現組織的風險，額外的控管措施是否需要以求降低風險？控管措施選擇的主要目的是在降低風險到可接受的水準—並且不致於過份影響到其它系統的運作效能。完全將風險降至為零是不可能也不太實際。因此目標是選擇可以應用於系統環境及完成任務目標的成本效率最高的可行性安控措施。

通常降低風險的方法可概分為三類：

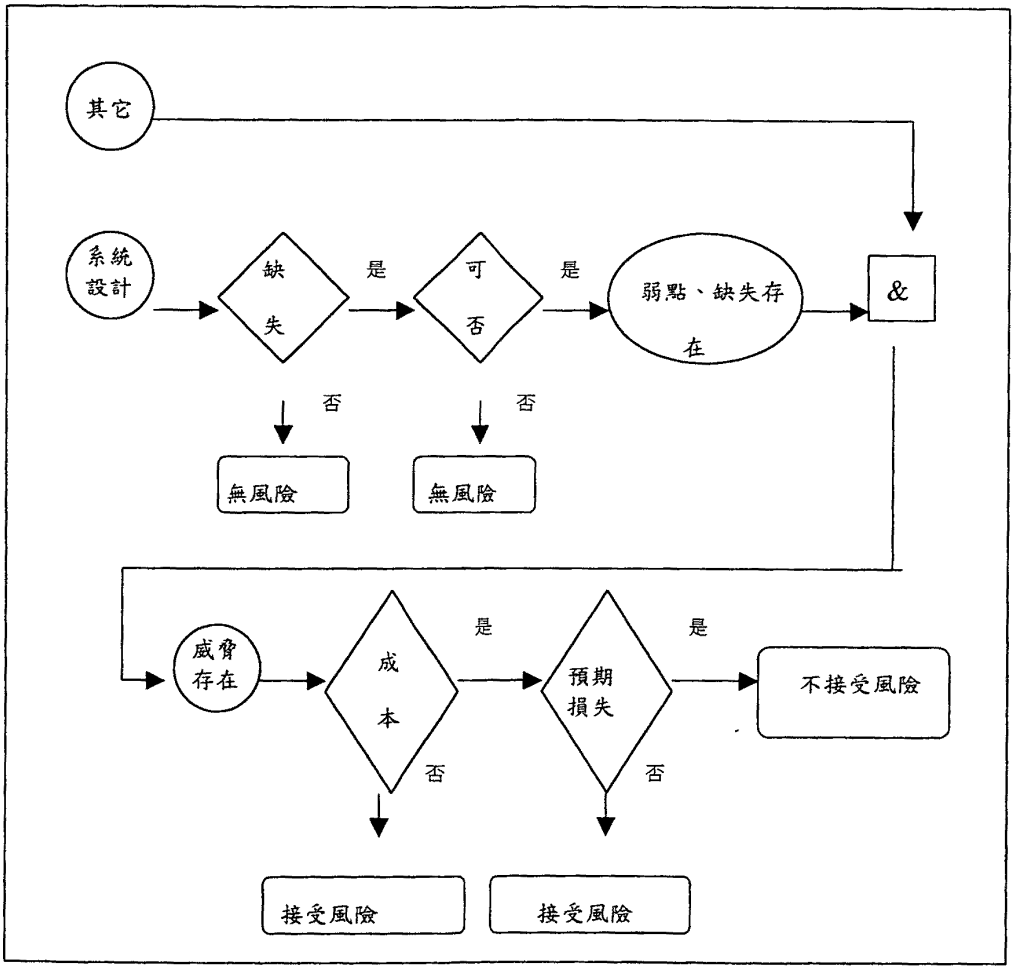
1. 預防：消滅威脅源，如：移除系統的缺點或弱點。

2. 限制：對威脅源限制其衝擊，如：對使用者的授權、資料的存取限制、及群組的控管。

3. 偵測與反應：偵查入侵或不當使用情形並採取行動以降低不利的結果[9]。

在規劃降低風險的制度時，並須考量銀行的目的與不同的特質。

圖 二　　風險降低圖



- 缺失存在—執行確定措施來降低缺失的機率
- 缺失可被利用—應用分層保護、階層設計及行政上的控管來防範缺失被利用
- 攻擊者的成本低於利得—應用種種保護措施來增加攻擊者的成本。例如：限

[9] 附錄 3 提供一些簡單的判別入侵現象，主要以 unix 系統為基礎，其它系統之安控規劃，基本理念相近，判別入侵主要根據所蒐集的資訊充份性與檢查人員本身專業素養。

制使用者的權限。

- 損失過大—應用分層保護、階層設計及行政上的控管來限制攻擊的型態，因而減少損失。

完成了整個的風險評估，最終仍須作一成本效益分析，往往安全控管的成本與效益極難界定，但配合檢查項目缺失，本模式可幫助檢查人員與受檢單位溝通時，有一清楚的概念與修正方式。

第四章　資訊安全政策機制（控管措施的實體化）

在闡述風險評估模型後，本文再提供除了技術層面上之控管外，對於一些重要的資訊安全控管觀念，以輔助瞭解建構風險管理模型之理念。

4.1 密碼政策

○建立有效之密碼政策

＊密碼須設定最小長度，並且是由數字、字母與符號的組合。

＊系統必須自動提示使用者定期更改密碼。

＊使用者不應和其他人共用密碼及將密碼寫下。

＊使用者不應使用易被猜測之密碼。

○對可重複使用之密碼於傳送及儲存過程中加密

因為網路易遭受 sinffing，hi jacking，Trojan horses 及其他不同型態的攻擊，所以對密碼加密後儲存及於網路上傳輸或是使用一次密碼可以減少此項風險。

○限制使用者使用過密碼之重複次數

為防止使用者重複使用最近使用過之密碼，可以選用安控子系統或應用軟體來記錄密碼之歷史紀錄。此項限制可根據時間（例如：一年）或是先前使用過密碼次數紀錄。

○使用商業用軟體測試使用者密碼的有效性

對使用者密碼是否易於猜測，可使用應用程式來檢視使用者密碼是否易於遭受"字典攻擊"而遭猜中。

○對一段期間未能使用之使用者帳號應予停用；而已停用後一段時間未能再次使用之使用者帳號則應予取消

○在多次登入失敗後，應停用該使用者代碼

為了防止攻擊者運用自動登入程式猜測使用者登入代碼及密碼的組合，應設定多次登入失敗後，自動鎖定使用者代碼的機能。但是對系統管理者的使用者代碼則必須小心應用此項限制，因為要回復系統最高權限使用者的權限

會比較麻煩。

○顯示使用者最後登入成功的路徑及未登入成功的次數

顯示使用者最後成功登入的時間及日期，是為了避免未經授權使用者以非法方式取得有效使用者密碼而侵入系統。訓練使用者觀察登入日期及時間並且報告任何不正常情形。觀察未登入成功次數使得使用者可以判斷是否有人嘗試猜測他們的密碼。

○採用"單次登入（single sign on）"產品

目前有產品可以允許使用者登入網路一次後，即可使用該使用者所有授權的應用程式，而無須每次進入不同的應用程式則須鍵入密碼，但是此項技術尚未完全成熟到可以廣泛應用，對於高度敏感性資料則需要更完整及安全的版本。此項產品除了可以增進作業效率外，單次登入的方式也使得使用者較不需將其密碼寫下，而避免為未經授權使用者取得。

4.2 人員訓練

○ 用嚴格的篩選程序選用可以接觸敏感性資料的員工

＊ 完整的背景查核確保員工履歷表上的每個項目都是正確的，例如：教育背景、前次工作職務及負責內容、交友情形等。

＊ 指紋查核以確保員工未曾有過犯罪紀錄。

＊ 完整及深度的訪談以確保員工具有履歷表上所填寫的技術訓練及知識。

＊ 信用調查以確保申請者或員工並無負債或不良的信用紀錄。

＊ 藥物測試以確定員工並無使用非法藥物情形。

○ 對顧問等之遴選應採用與員工相同之篩選標準

因為顧問等人具有特殊技術或知識可能有能力接觸到隱密性資料，或是可以知道金融機構網路配置情形，進出控管程序與其他的安全控管上的弱點。因此應對顧問等之遴選應採用與員工相同之篩選標準。

4.3 防火牆安全政策

安全政策是決定防火牆是否能有效保護內部網路安全的另一個重要因素，若選擇了一個具有最安權的作業系統以及最安全的控制機制的防火牆，但是卻決定讓所有的服務都通過防火牆，則安裝這樣的防火牆之後和沒有安裝防火牆一點區別都沒有。

要制定防火牆的安全政策，必須將各種不同存取方向列出，以一個具有兩個網路界面的防火牆為例就有內部網路存取外部網路、外部網路存取內部網路、內部網路存取防火牆及外部網路存取防火牆四種方向。再搭配將所有可能用到的服務列出一個存取列表，在表中將需要開放的服務列出，最後再設定應該開放那些使用者使用那些服務。

雖然一般人認為防火牆能支援越多的服務越好，但是支不支援是一回事，真正要決定那些服務通過防火牆時還是必須要慎重考慮，開放越多的服務往往也代表了越多可能被攻擊者利用的管道。

4.4 其它考量

外部對內部網路進行存取時通常都會帶來特定的風險，因此有許多的問題必須再特別考慮，透過適當的設定及規劃可以降低風險。這種存取可以分為兩種：提供特定對像的遠端存取以及開放給所有人用的網際網路服務。提供特定對像的遠端存取是一個複雜且重要的問題，本文中將不做額外的探討。

有許多服務是必須開放給網際網路上的不特定人存取的，例如：Web、Mail及DNS等。這些服務對大部份企業及網路銀行是必須的，而且沒有辦法預期使用者會來自何方，因此必須完全開放。為確保安全，企業及網路銀行應作好適當的規劃。WEB Server本身是危險的，應該放置在內部及外部網路之外的一個獨立網路，這個獨立的第三個網路稱為DMZ(De Militarized Zone)或SSN(Secure Server Network)。將Web Server獨立在DMZ或SSN中可以得到防火牆的保護又不會因為

開放這個通道給外界存取而造成內部網路的安全風險。

當防火牆使用 IP 位址轉換時，就有必要建立雙重 DNS Server，以處理內外部 IP 不一致的問題，有的防火牆上內建 Dual DNS，可以直接處理，有的防火牆上可以安裝一個 DNS Server，內部則必須另外架設一 DNS Server。由防火牆上提供 Mail Server 可以作為內外部網路間的信件轉傳通道，但 Mail Server 是經常發現安全問題服務之一，避免讓外界有機會直接接觸到內部的 Mail Server 對內部網路的保護可以有效的提昇。

所有的密碼政策、防火牆政冊、人員權限政冊等都必須依據銀行本身的需要而制定，考量本身的風險與產品的特質及對敏感性資料的定義，一間小雜貨店並不需要金庫，也無須雙控的觀念，一台機車該上幾道鎖才能防盜，這些觀念都是因時因地因人而有不同的設計理念與方式，但可以判斷的是應用上述的觀念便可架構本身的攻擊—反應安全機制，許多的人將制定安全政策視為表面文章，而安全政策卻是安全機制啟動的鑰匙。

第五章 結論與建議

5.1 結論

無論企業或銀行購買或架設多少的安全防護軟體，企業本身的資訊安全政策以及安全政策的執行狀況才是真正影響資訊安全的重點。一個世界上最安全的防盜設備，卻為了方便使用而關掉，則此一防盜設備就沒有任何的作用，資訊安全也是如此。

資訊安全始於可行的安全政策。銀行若想要保護資訊安全首先要明確定義企業內部認為重要的資訊資產，判斷各種資產的重要程度，評估各種不同身份的人員對資訊資產的存取權限，甚至決定各個不同人員、網路、系統之前的互動關係以及這種關係是否必須存在。最後再制訂企業的安全政策以及對違反安全政策的舉動應該作出的反應。

在作出安全政策之後，必須妥善的對員工進行足夠的教育訓練以培養其安全體認，如此安全政策才能真正執行並且產生效用。

資訊安全是一個不斷調整的過程，隨著銀行業務的創新、人員的更替，各種攻擊技術的翻新，銀行無論在安全防護設施或是安全政策都應隨著外在環境的改變進行調整。同樣地，金融監理對銀行的網路資訊安全的查核也必須隨時調整其評估模型及哲學，以創造網路銀行運行的基本市場機制及規範，使銀行業者得以在一自由且公平的環境創造高附加價值的產品。

5.2 建議

根據本文簡介之資訊系統風險評估模式，金融監理單位可依本身之需求，建立量化模型或調整其檢查項目，最後參酌本文之論證及我國目前監理狀況，提供下列建議。

⑴擬定電子銀行查核程序及各項技術文件

網路資訊的傳遞，可以缩減顧客與銀行間的距離，大幅度的減少交易成本與增強銀行對客戶交易的搓合能力，然大多數銀行業者只追求資訊的快速應用，而對資訊的專業知識的植基與認知則有待加強，對資訊系統的安全控管與稽核等基礎領域則未加重視，而未來銀行業對資訊的依賴愈來愈甚，各項貨幣支付系統，如：票債券無實體交易及清算系統、網頁上存款帳戶的轉帳提領等，都漸漸將進入人們的日常生活中，因此為提昇我國銀行進入世貿組織後所面臨的競爭與機會，健全本身的競爭體質是最重要的，而金融商品所有的特質中，最重要的就是交易的安全，惟有提供安全的交易環境才是網路銀行發展的基礎。因此根據風險評估模式擬定電子銀行稽核手冊、檢查行前請受檢機構提供準備書面文件之清單及各式工作底稿將有助於稽核工作之進行。

⑵培養電子銀行檢查之專業人才、加強專業交流

金融監理的角色在未來將更吃重，由於銀行業者是在成本最小的情況下追求最高的利潤，往往會忽視了安控的問題，而安控的問題一旦發生卻會造成巨大的社會成本，而且在訊息不完全的經濟環境下，金融監理實是有提高整體金融效率的功能[10]，因此金融監理機構更應對銀行業者實施持續性的管理（on-going basis）以減少資源誤置的現象。

對資訊系統風險評估是否應成立一專責單位進行檢查評估，以避免多頭馬車問題，事實上所有的金融檢查均屬事後觀念，也就是在事件發生後，根據所留存之軌跡來作專業之管理，藉由事後行為之查核而影響市場上所有參與者之決策及信念，因此不同單位不同的功能與角色的考量而有創新的角度對金融監理才是有益的，中央銀行金融檢查處處長陳上程[11]認為各金融檢查機關依職責分工檢查，並無產生金融監理死角問題，這是從金融監理的競爭與創新的制度面思考，各金檢單位間及與銀行業者溝通、協調則屬實務性細節，所以對新型態的網路銀行監理應在現行架構下，各金融監理機構自行建立風險評估方式，調整檢查項目，並

---

[10] Laffont and Tirole 在 "A Theory of Incentives in Procurement and Regulation" 中有相關的論證，惟本文非探討此項經濟議題，有興趣者可自行參閱。

[11] 見 90 12 7 工商時報第 6 版。

舉辦專業訓練，加強監理經驗的交流。

(3)建構知識經濟績效指標資料庫並設立模式以供分析衡量新經濟現象

創造、傳遞及運用資訊知識的能力已被視為經濟成長、提昇生活品質的潛在動力。因此金融監理機關為了制定政策與評估政策成效，必須有能力監控科技、資訊技術、產業的趨勢變化與結構改變。雖然衡量知識經濟的指標可能難以確定且有爭議，不過仍需建立本身的監控機制。知識經濟指標約可區分為三大類，第一類衡量產業、技術等結構變化，第二類則衡量知識創新，又可細分兩細目，第一細目為人力資本指標，第二細目為科技指標，第三類則為知識擴張指標，其中又區分三項細目，第一項細目為知識網路指標，第二細目為資訊與通訊科技指標，第三細目則為網路及電子商務指標。建立知識經濟指標資料庫[12]，即可建立知識經濟模型，以掌握電子商務及知識經濟的現象，並供政策的制定與金融監理。

[12] 澳洲 Knowledge-based Economy branch, Department of Industry, Science and Resources 正研擬知識經濟資料庫的建立，以瞭解知識經濟對目前澳洲經濟體的影響。

附錄

㈠ 最高使用者之管理機制

1.1 雙人雙密碼同時登入認證程序

對於作業系統中最高使用者之管理，國外金融機構多另購安全控管軟體，用以監督最高權限使用者的使用情形及登入登出等認證過程，目前我國票券公司對最高使用者的認證控管過程，係將最高使用者的密碼分成兩部份，分由兩人控管，以收相互牽制之效。實際上，這仍屬一人的登入認證，因為密碼只有一組，而密碼的更改或查詢可能造成兩人都知道密碼。一種常見的增強登入認證的方法是登入時須要兩個密碼。這假設是兩個擁有自己個別的密碼不同的人必須同時輸入個別的密碼以完成登入程序。而這兩種不同密碼則分屬系統中的兩個帳號。這種加強登入認證的方法，稱之為兩人登入法（Two-person Login）。兩人登入法可以適用於所有的帳號登入程序，因此各系統管理者可以根據自己或公司的安控政策或管理哲學，擬定不同的認證程序。

1.2 自製密碼認證程序

在登入認證的過程中，也可以自行撰寫一隻程式作額外的認證。自行開發的程式在登入認證的過程中可以取得主機控制權，並進行所設定的認證程序。如果程式傳回的值為 0，那登入程序繼序進行，如果程式傳回的值為其它異於 0 的值，登入程序就會終止並傳送「You entered an invalid login name or password」的訊息。這隻額外的認證程式以 root 的權限進行

㈡ 入侵偵測系統

偵測：探討入侵偵測系統（intrusion detection systems），並應用這些偵測工具架構金融機構資訊安全計劃。

弱點評估（vulnerability）及滲透分析（penetration analysis）有助於評估金融機構是否對於資訊安全已有適當的注意以及系統安全設定是否合適。在完成上二項評估分析後，下一步就是監控系統入侵及其它不正

常的事件與活動。入侵偵測系統可以充當警鈴，將潛在的入侵行為報告給適當的安控人員。藉由分析入侵偵測系統所產生的訊息，可以有助於決定安控架構是否有效足以保護資訊系統的安全。除此之外，入侵偵測系統也可以架構成對入侵活動自動反應。

電腦系統及應用程式本身都可以產生詳細、冗長的活動記錄及稽核軌跡，系統管理者或安控人員可以以人工方式去審查不尋常的事件。但是入侵偵測系統可以自動的去審查這些記錄與稽核資料，這樣可以減少審查所須的時間與成本，並且也大幅減少審閱這些記錄及稽核資料所須的技術水平。

基本上構成入侵偵測系統有三種元件。第一項是資料搜集員(agent)，這是實際上負責資料的搜集。第二是管理員（manager)，負責對資料搜集員所搜集的資料作轉換及處理。第三是安控管理員（console)，可以授權資訊系統人員安裝或升級資料搜集員的版本，定義何種行為為入侵，並且對入侵行為進行追蹤。根據入侵偵測系統不同的複雜性，可以有多個資料搜集員與管理員。

入侵偵測系統通常使用三種不同的方法來偵測入侵行為。第一，它們尋找已備認定的入侵徵兆，像是先前已被認定為攻擊型態的資料或資料流。第二，它們觀察系統被誤用的情形，例如未經授權的讀取、更新或執行檔案或是在防火牆內不被允許的資料傳輸。第三，它們觀察系統或使用者異於平日使用情形的活動。

這些應用人工智慧的「異常基礎（anomaly-based)」入侵偵測系統，主要設計來偵測系統細微的變化及新型的入侵方式，並進而通知安控人員可能的入侵。有些則設計可以定期更新平常的使用型態。但是設計不良的「異常基礎(anomaly-based)」入侵偵測系統則可能經常產生錯誤的反應。

雖然入侵偵測系統是金融機構全面安全控管的一部分，它們並不能防

止系統避免未知的威脅與弱點。它們並無法補救脆弱的認證程序（例如：侵入者已知道進入系統的密碼）。同時，入侵偵測系統通常和現有的安控產品（如：防火牆）有重覆的功能。但入侵偵測系統可以檢查防火牆是否設定正確及是否存在內部誤用等額外防護功能。防火牆與入侵偵測系統都必須適當地設定及更新以對抗新型態的攻擊。除此之外，管理階層必需瞭解這些產品的功能是隨時更新的。

入侵偵測系統工具可以產生技術性與管理性的報表，包含文字、表格及圖形。入侵偵測報告也提供攻擊型態的背景資料以及建議處理方案。當偵測到入侵行為時，入侵偵測系統可以自動搜集關於攻擊者的額外訊息，以供稍後的分析報告之用。

入侵偵測系統通常分為兩類：主機基礎（host-based）及網路基礎（network-based）。第三類入侵偵測系統產品用來偵測主機上不正常的應用事件（應用基礎 application-based）。主機基礎及網路基礎的產品各有其特點，風險評估的過程應該幫助金融機構決定是否其中之一，或是兩者的組合最為適合他們的需求。

主機基礎的入侵偵測系統亦被稱之為稽核軌跡分析工具或是伺服器基礎入侵偵測系統（sever-based，通常掛在伺服器上）。主機基礎入侵偵測系統藉由監控主機事件活動，稽核軌跡及其它與安控相關活動來偵測可能的入侵與誤用。這些工具可以追蹤作業系統，應用軟體，web 伺服器，路由器（router），防火牆等的稽核軌跡，並且可以控管特洛依木馬程式所需的重要程式以及未經授權的變動。這可以提供可貴的強行侵入（break-in）證據，以及入侵者登入系統後所造成的損害評估。如果以即時（real time）方式運行，它可以立即通知銀行有未經授權者想得到系統管理者的權限，或是想得到重要檔案，或是想更改程式記錄檔。

主機基礎的入侵偵測系統的一項重要利益是它可以有效偵查內部使用者的誤用，因為它可以監控特定主機上的活動。例如，它可以偵查到使用

者嘗試讀取未經授權的檔案，或是嘗試執行系統管理者的指令。除此之外，它也可以監看資料的加密傳輸。

主機系統的入侵偵測系統存在一個問題，如果沒法即時查看稽核軌跡，則入侵訊息的通知就會延遲。這問題主要存在於即時模式的監控會占據大量的系統資源，並且系統處理的速度也大受影響。如果不以即時模式監控，它也可以為銀行指出安控上的較大問題及趨勢。

至於網路基礎入侵偵測系統，軟體或是 sniffer 被放置於網路上的一個或多個點。Sniffer 分析網路上可能入侵的訊息封包。網路封包包含了資料及可以認證收受雙方的訊息表頭。網路基礎入侵偵測系統可以偵測誤用的型態，特定型態的攻擊及一些不尋常的活動，如未預期到的網路流量及形態。與主機基礎入侵偵測系統比較，某些網路導向攻擊，如：IP spoofing, 封包攻擊（packet flood）及 denial of service，最好透過封包檢查方式偵測。

網路基礎入侵偵測系統可以即時偵測到可能的入侵，並且對可能的入侵提供即時的警訊及反應。它並不需要在網路上每台主機上裝置，因此它比主機基礎的入侵偵測系統更容易監控入侵行為，也較便宜。

網路基礎入侵偵測系統有時會把正常的流量誤認為入侵，也會將入侵誤認為是正常的流量。它們難以偵測到流量慢攻擊（slow attacks），而且當網路忙碌時也會出問題，網路基礎入侵偵測系統無法監控加密後的傳輸（只能偵測到在網路上傳輸的資料），而且對內部使用者的誤用偵測也較無效率，因為網路封包分析沒有辦法監看特定主機的活動。

㈢ 尋找系統可能被侵入的跡象

準則：注意所有的調查行動應該符合公司的政策及規範

雖然入侵偵測系統可以偵查大多數的入侵現象，但人的因素及持續的判斷還是最重要的，因此本節簡介一些初步的資料蒐集與結果判斷。

(1)檢查來自不常見的連線位址或是特殊動作指令的軌跡檔. 例如, 用' last' 指令檢查登入軌跡, 過程軌跡(process accounting), 所有由 syslog 所產生的軌跡檔, 以及其它的安全性的軌跡紀錄檔. 如果防火牆或是路由器也有產生軌跡記錄並且存放於不同的地方, 也必須同時加以檢查. 入侵者或非法使用者也會去修改這些軌跡檔案試圖去隱藏他們的使用情形或行為.

(2)檢查全系統 setuid 及 setgid 的檔案(特別是 setuid root 檔). 侵入者通常會留下/bin/sh 或 /bin/time 的 setuid 複製檔以備他們可以以後使用 root 的權限. unix 系統內建指令 find 可以用來找尋 setuid 或 setgid 檔案. 例如, 你可以使用下列的指令去找到 setuid root 檔案及 setgid kmem 檔案.

```
find / -user root -perm -4000 -print
find / -group kmem -perm -2000 -print
```

注意上述的例子搜尋整個系統目錄的樹狀結構, 包含了 NFS/AFS 的檔案系統. 有些 unix 版本的 find 指令可以使用 "-xdev"的選項來避免作全面性的搜尋. 例如:

```
find / -user root -perm -4000 -print -xdev
```

另一種尋找 setuid 檔案的方式是在每個磁碟分區使用 ncheck 指令. 例如, 使用下列指令來尋在磁碟分區上/dev/rsd0g 的 setuid 檔案及特殊裝置

```
ncheck -s /dev/rsd0g
```

(3)檢查系統執行檔以確保它們未被更改. 入侵者經常會更改系統上的程式如 login, su, telnet, netstat, ifconfig, ls, find, du, dj, libc, sync, 以及所有在/etc/inetd.conf 上所規範的執行檔及其它重要的網路或系統程式及共享的資料庫. 比較系統上的版本與已知的安全複制版本, 例如, 系統啟始設定的版本. 但是要確定備份的版本是安全的版本, 備份的版本也有可能隱藏特若依木馬程式.

特若依木馬程式可能產生與合法版本相同的檢查位元與時間標記. 正因為如此,

標準的系統指令 sum 以及程式的時間標計記並不足以判斷程式是否已被置換. 但 cmp, MD5, Tripwire 以及其它的加密檢查工具則足以用來偵測特若依木馬程式, 如果這些檢查工具藏放的安全的話. 另外也可以再使用另一種工具(如 PGP)來加註由 MD5 或 Tripwire 所產生的結果, 來做進一步的佐證.

(4)檢查系統看看是否有未經授權的網路監控軟體的使用, 例如 sniffer 或是 packet sniffer. 入侵者可能使用 sniffer 來取得使用者帳號及密碼等訊息.

(5)檢查所有在'cron'及'at'執行的檔案. 入侵者經常在'cron'及'at'所執行的程式中留下後門. 這些技術可以使入侵者再回到系統中(即使你相信你已經找到系統被破解的軌跡之後). 再來也要確定由'cron'及'at'所執行的工作的程式或工作本身權限並不是毫無限制的(world-writable).

(6)檢查未經授權的服務. 檢查/etc/inetd.conf 看看是否有未經授權的服務增加或更改. 特別是要檢查那些執行 shell 程式的分錄(如:/bin/sh, /bin/csh)並檢查所有在/etc/inetd.conf 中出現的所有程式以確定它們是否被特若依木馬程式置換過. 也檢查那些已經關閉使用的服務. 因為侵入者可能打開你先前認為已經關閉的服務或是用特若依木馬程式來取代 inetd 程式.

(7)檢查/etc/passwd 檔案是否有過任何的修改. 特別檢查未經授權的新帳號增加, 沒有密碼的帳號, 或是現存使用者帳號 UID 的更改(特別是 UID 0)

(8)檢查系統檔案及網路設定檔案, 看看是否有非法的分錄. 特別是在 /etc/hosts.equiv, /etc/hosts.lpd 及所有的.rhosts 檔案(如:root, uucp, ftp 及其它系統帳號) 有無'+'或是不適當的主機名稱.

(9)檢查系統所有的隱藏檔或不尋常的檔案(通常是以'.'開始, 而且無法用 ls 指令看到)以及密碼破解程式. 在 unix 系統中通常是將隱藏目錄放置於使用者帳號內並以特殊型態命名, 例如'...'或'..'或'..^G'. 我們可以使用 find 程式來找出這些隱藏的檔案, 例如:

```
find / -name ".. " -print -xdev

find / -name ".*" -print -xdev | cat -v
```

⑽檢查所有的區域網路上的主機. 如果一台主機被侵入, 在區域網路上的其它主機被侵入的可能性也很大. 尤其在網路上是由 NIS 或是主機間藉由.rhosts 與 /etc/hosts.equiv 來做聯繫. 因此檢查主機上有那些使用者是使用.rhosts 來做網路上的使用與認證.

參考資料

一、英文部份

1 Federal Deposit Insurance Corporation(1997). Electronic Banking:Safety and Soundness Examination Procedures, March.

2 FDIC，Web Site Audit Checklist

3.FDIC，Electronic Banking Technical Procedures for FIREWALLS

4.FDIC，Electronic Banking Glossary

5 Faulkner & Gray (1997). Bank Technology Directory 1998.

6.Mentis Corporation (1998). 1997 Remote Electronic Banking.

7.Office of the Comptroller of the Currency(1998a)."Technology Risk Management," OCC Bulletin 98-3, February 4.

8 Office of the Comptroller of the Currency(1998b)."Technology Risk Management: PC Banking," OCC Bulletin 98-38, August 24.

9.Office of Thrift Supervision(1997). Guidance to Thrifts on Retail Online PC banking, June 23.

10.Richards, Heidi(1997). "New Electronic Payment Technologies:A Look at Security Issues," Journal of Retail Banking Services, vol.19, no.3, Autumn.

11.Federal Reserve Bank of New York (1997). Sound Practices Guidance on Information Security, Septemper.

12.Federal Reserve Bank of New York(1997). Sound Practices Guidance on Information Security, September.

13.Group of Ten (1997). Electronic Money: Consumer Protection, Law Enforcement, Supervisory and Cross Border Issues, Bank for International Settlements, April.

14. Information systems handbook, FFIEC 1996.

15.FDIC's Electronic Banking Initiatives, June 6 2001.

16. Internet Banking , Comptrolller's Handbook, October 1999.

17. CSBS ınternet banking taskforce supervısory guidance draft, October 12 2000.

18 Rısk-Focused Examinatıon Case Study Sachı Bank, Ltd., semınar ın Federal Reserve of New York, May 2001.

19. Understanding 3G, summer 2001

二、中文部份

1、吳维修，由電子商務熱潮看銀行業的發展趨勢

2、調查資料第 423 期，國內網路銀行業務之開放及其因應課題

3、黃景彰，網際網路電子商務的付款機制

4、廖啟泰，電子商務之數位貨幣

5、張真誠、林祝興、江季翰，電子商務安全

6、傅成仕，銀行業之新趨勢－網路銀行