# ～實務新知～

## 由英國證券市場「網路交易安全」架構看我國現行網路交易安全機制

周子元（證期會管理師）

### 壹、前　言

隨著網際網路發達、電子商務日益蓬勃，致使越來越多人嘗試著線上交易，國內網路委託下單、基金申請、承銷案件公開申購等證券業務亦陸續開放以得透過網路辦理，惟同時，聽聞某大型網站被駭客入侵、某網站發生當機等事件，引發投資人對網路交易安全之疑慮，目前亦值證交所重新規劃新一代交易系統之際，希望藉由研究英國證券相關單位電腦網路交易系統之架構及網路安全實務做法，來檢視目前國內證券市場網路安全機制之充足與否，並為新一代交易系統設計及未來網路作業環境之參考。

### 貳、英國證券業之電腦架構

一、證券市場上各單位間關係說明

本節擬先對倫敦證券、期貨市場之交易、結算、交割等單位間之電腦連線關係加以說明，次再介紹各單位與其周邊單位間之電腦架構。

圖一、英國整體證券市場各單位關聯圖

證券市場上各單位間之流程說明：

1a.交易會員輸入證券委託資料至 SETS 電腦交易系統。

1b.LSE 將已經確認之證券委託、成交回報資料傳給交易會員。

2a.LSE 將證券行情資訊廣播給各資訊公司。

2b.資訊公司接收 LSE 行情資訊，加值後傳給交易會員、客戶。

3. LSE 將成交資料經由連線網路傳給 CREST。

4.交易雙方（或其交割代理商）傳送交割指令給 CREST，指示以 LCH 作為其交割相對方，並指定交割順序及方式。

5.CREST 將結算會員最新之開倉股票及現金部位資料傳送給 LCH。

6.LCH 將計算出之該結算會員保證金數量及其它報告資料傳回給 CREST。

7a.CREST 將依照結算會員之要求回覆保證金數量及相關報告資料。

7b. LCH 提供相關紀錄資料給結算會員。

## 二、各單位電腦硬體及對外連線架構說明

(一)倫敦證券交易所（LSE）

因倫敦證券交易所為一知名國際性交易所，其網路交易安全更顯重要，下圖為 LSE 與交易會員間之連線架構：

圖二、LSE 與交易會員間之連線架構

其主要的傳輸要點及安全機制如下：

(1)LSE 與各交易會員間主要採 64Kbps 專線連線( 採用 X.21 傳輸介面，使用 Ericsson 之 ERIPAX X.25 網路系統），用 X.25 協定以 SVC（Switch Virtual Circuit）與交易會員電腦通訊，並以 ISDN X.25 網路作為備援連線方式。

(2)每一筆交易訊息皆需加密及權限確認處理。

(3)使用 X3.92（DES）資料加密標準，每筆交易訊息皆帶有 32 bits 之訊息確認碼（MAC），該碼係依 X9.19 標準產製。

④ (4)使用私鑰（PRIVATE KEY）加密方式對交易資料做加解密處理。

(5)LSE 公開交易、資訊傳輸格式，供各資訊廠商開發交易連線系統及行情揭示系統。

(6)目前 Bloomberg 等資訊公司提供工作站給交易會員，其可在工作站上下委託、查看市場行情資訊、作風險管理或股票部位管理，該工作站將客戶之指令透過 Bloomberg 等公司專屬網路傳送給 LSE。

(7)交易會員可選擇以 64Kbps 或 256Kbps 傳輸速率（皆採用 X.25 協定）與 LSE 連線接收行情資訊。

另 LSE 與資訊公司間的連線主要以 64Kbps 專線相連（可選擇以 64Kbps 或 256Kbps 傳輸速率），均採 X.25 協定，並以 ISDN X.25 網路作為備援連線方式。

(8)在實體安全方面，採 Tandem Himalaya 系列 non-stop 的主機，以 ISDN 為交易網路的備援線路，並有第二資料中心。如不幸整個主機當機，可由第二資料中心的系統進行接管。因有備援線故可確保交易系統及交易網路的正常運作。

(9)在資料傳輸安全方面，則採用 Triple-DES 的加密技術，此為一對稱式金鑰加密法（Symmetric Key Encryption），又稱為私密金鑰加密法。LSE 將 Triple-DES 的加密技術以硬體實作方式做成一安全模組，資料的進出必須經過該安全模組方能進入交易系統，其安全性高。

(10)在網路安全方面，因系統委外開發，為控管協力廠商由外部撥回交易所系統做維護或系統開發測試等事情，採回撥及帳號控管；除建置防火牆分隔內、外部網路，以防非法人士入侵外，更設專人隨時監控網路以期能早期偵測可能的入侵行為並找出問題所在及解決問題。

(二)倫敦證券交割公司（CREST）

CrestCo 提供了一套安全及效率的電子化交割系統供其會員使用，此套系統連接了證券商、保管人及商品供應者做為商品的交割之用。其系統架構與倫敦證券交易所類似，且必須是與 CrestCo 簽約的會員方能連接此系統。CREST 與各單位間之連線架構如下：

圖三、CREST 與各單位間之連線架構

而相關之功能及安全機制說明如下：

(1)連接 S.W.I.F.T.網路系統之連線主機：負責接收或傳送與交割會員、LSE、LCH 間之資料，採用 X.25 傳輸協定，使用 X3.92（DES）加密資料，每筆交易訊息皆帶有 128 bit 之 MAC，與交割會員間使用 1024bits 之 RSA 加密標準，係使用硬體解密設備解傳輸資料，
且每週更換密碼鍵值。

(2)連接 Syntegra 網路系統之連線主機：負責接收或傳送與交割會員間之資料，連線雙方採 TCP/IP 傳輸協定，使用 X3.92（DES）資料加密標準，每筆交易訊息皆帶有 128 bit 之 MAC，與交割會員間使用 1024bits 之 RSA 加密標準。

(3)交割會員可自行選擇使用 X.25（透過 S.W.I.F.T.網路系統）或 TCP/IP（透過 Syntegra 網路系統）與 CREST 系統連線主機進行資料傳輸。

(4)在實體安全方面，該公司如 LSE 一樣，採用 Tandem 系列不停機系統做為主交易系統，亦建置第二資料中心做為備援，確保主機系統可穩定運作及當主交易系統無法運作時可由第二資料中心之系統加以接管運作。至於線路方面也建置有備

援線路，較為特別的是該系統的主線路與備援線路乃分屬不同的電信公司，如此不僅線路故障時有備援線路可取代，即使電信公司發生無法運作的情形時，仍可利用另一家電信公司之線路來取代，故可隨時保持線路之暢通。

(5)在資料傳輸安全方面：CrestCo 在連線主機前裝置了安全模組，負責資料傳輸安全。CrestCo 定義了應用程式介面（API）及軟體安全規格，以利會員開發能相連接之系統，並達到安全交易之目的。在與會員資料傳輸方面也是採取 Triple-DES 的技術來加密所傳送的資料，然而在金鑰的交換機制方面則不同於倫敦證券交易所，乃採取 RSA 的技術來傳遞資料加解密金鑰，及做為傳送端與接收端雙方的身份鑑別。

(三)倫敦國際金融期貨及選擇權交易所（LIFFE）

LIFFE 之電腦硬體及其與各單位間之連線架構如下圖所示：

圖四、LIFFE 電腦架構與各單位間之連線架構

從 1998 年起，LIFFE 建立了一套專供交易用的開放性架構電子交易平台，稱為 LIFFE CONNECT，任何金融中心或個人電腦皆可連上此系統進行所有 LIFFE 衍生性商品的自動交易。依據 LIFFE 的介紹，LIFFE CONNECT 提供了三種連接方式：

a.經由國際連接網路直接連接至 LIFFE 的專屬交易網路。

b.倫敦地區的會員則經由會員所屬的專屬網路連接。

c.透過全球網路加值業者（如 Bloomberg），再連接至 LIFFE。

為了確保網路交易安全，LIFFE 除建置穩定的交易網路外，也致力於防範非法人員的入侵，以確保系統免於被攻擊、破壞以及資料免於被竊取、損毀，其主要之安全機制如下：

(1)在實體安全方面，LIFFE 建置第二資料中心，以預防主資料中心無法運作時可立即由第二資料中心備援。此外，因 LIFFE 採用唯有與其簽約的會員方可連上此系統的專屬網路，故在使用者身份識別及權限控管方面較易管理，另因屬封閉性網路，除非是簽約會員，一般外部人員將無法連接至此系統進行入侵，而非簽約會員如須下單則必須透過簽約會員方能為之。

(2)在資料傳輸安全方面，LIFFE 使用電子憑證的機制來進行資料傳輸時的身份認證，其所使用的憑證技術規範為 X.509V3。LIFFE 採自行擔任憑證認證中心（CA）

的方式簽發所有參予交易之會員其所屬 之憑證，並負擔其會員憑證之所需費用。

(3)在網路安全方面，LIFFE 為了避免非法人士侵入其內部網路，乃採用防火牆的機制來分隔內、外部網路，以加強兩個網路間存取控制的安全機制，只允許獲授權的資料通過，以減少系統受侵入而造成內部資源損壞。LIFFE 表示依其經驗，上述安全機制的建立並不因難，而最困難的部份乃是內部人員的控管，如果管理不善的話，將使得未經授權的人員可輕易接近系統而進行放置病毒、安裝程式後門或竊取資料、破壞系統等活動，故對人員的控管其制訂了安全政策來規範，以達有效的人員控管。

## 參、我國證券業之電腦架構

我國證券市場集中交易系統之網路架構圖如下所示：

臺灣證券交易所交易主機連線架構圖

①台灣證券交易所（TSE）與各證券商、證金公司、集保公司間均係透過 X.25 分封專屬網路相線。在各券商、證金公司欲與證交所連線時，證交所即進行帳號、密碼之確認要求，惟後續資料傳輸時並無進行資料加密亂碼化及數位簽章認證之處理。

②在實體安全方面，採用 Tandem 系列不停機系統做為主交易系統，並建置當日及時異地備援系統，確保主機系統可穩定運作及當主交易系統無法運作時可由備援系統接管運作，唯有與其簽約的券商、證金公司方可連上此專屬網路，故在使用者身份識別及權限控管方面較易控管，一般外部人員較無法連接至此系統進行入侵。

③在上市公司網路申報及證券商網路申報方面，透過網際網路（TCP/IP 協定）傳送申報資料，除連線時對申報者進行帳號、密碼之要求確認外，於傳輸資料時，尚進行資料加密亂碼化措施及採數位簽章認證申報者身分。

## 肆、結　語

資訊時代電腦系統攸關企業生死存亡之關鍵，在網路的環境下，電腦安全之維護更形重要，除原本封閉型系統所要求之電腦安全外，用來隔絕機關的內、外部網路，保障機關知識財產安全之防火牆（Firewall）、代理伺服器（Proxy server）、防毒軟體等軟、硬體安全機制，更不可缺少。

對於網路交易資料傳輸部分，由倫敦證交所、CrestCo 證券交割公司、LIFFE 金融期貨及選擇權交易所等單位所採取之措施可以得知，除均要求與之連線單位

需合乎(一)身份確定性(上開公司各自簽發連線單位所屬之帳號、密碼)、(二)資料隱密性(強制要求資料需經加密、解密之措施)、(三)資料完整性(傳輸交易資料時,均會附上資料數值檢查碼)等三項外,已全面開放網際網路交易之LIFFE,其更強制所有與其連線參予交易者,均需達到(四)交易資料之不可否認性之要求,即需做到身份認證之要求,並自行擔任認證中心,自己簽發電子憑證予所有與之連線之客戶。

我國亦已邁入網路交易時代,經由研究英國證券各單位之電腦安全實務措施來檢視我國證券業相關之安全措施,發現尚有改進空間,如(一)備援線路方面,TSE 的主備援線路均係透過中華電信的實體線路進行傳輸,現在隨著電信事業之開放,似乎可考慮像 CrestCo 一樣,採第二家電信公司之線路,來當備援線路;(二)網路委託下單交易部分,應要求證券商需全面採用網路認證機制、傳輸交易資訊時需經加密處理(金鑰長度至少 128bits)等。這些均是未來於督導台灣證券交易所規劃新一代交易系統時,可以納入考量之點,屆時新系統將既有之電腦安全加上資料傳輸安全,定能提供一更健全之網路交易環境,如此投資者當能更放心、安心的從事網路交易。