網際網路電子資料交換支援商務多媒體的整合技術—以電子郵件為傳輸模式之系統研究

The Integrated Technology of EDI over Internet Supporting Multimedia Applications: A System Study of the Collaboration Model Using SMTP and Mail Agent

蔡銘箴* 吳泰宏*

Min-Jen Tsai **Tai-Hong Wu**

(Received Feb. 11, 1999; Revised July 22, 1999; Accepted July 29, 1999)

摘要

電子資料交換（EDI）是在雙方或多方同意的標準下，從一個資訊系統到另一個系統，以資訊、通訊的方式傳輸結構化資料的基礎；而網際網路電子資料交換 – 則是以網際網路的系統架構來傳輸、支援電子資料交換的整合機制，也就是網際網路電子資料交換（EDIINT，EDI over Internet Integration），它的目的是強調整合現有多種網際網路傳輸的機制與協定及開放的交換標準，進行資料交換與傳輸。本研究針對 EDIINT 各方面的整合，從企業競爭力經營的角度，提出為何使用 EDIINT 的理由，以各種封閉、開放性質之網路及電子資料交換標準，說明其演進的過程；並從公開標準轉換和網路傳輸通訊這兩方面 EDIINT 之重要概念，配合上 UN/EDIFACT 和 MIME 的規格，建立一個完整的 EDIINT 經由 Mail System 來完成商業資料通訊的實證架構。

同時，隨著數位浮水印影像、影訊、音訊等具商業價值的商務多媒體使用度的增加，利用 EDI 的標準，設計 EDI 和多媒體之間的連結，提供商務多媒體的服務，證實其整合上的可行性。在傳輸的過程中，同時嵌入了交換安全控管機制，對於安全的電子資料交換標準與傳輸，在 UNIX 和 Windows 的測試環境下，完成實測驗證。結果顯示了 EDI Translator 可以很容易地和 Mail Agent 及 SMTP Services 進行整合，並且提供雙方在安全的 PGP/MIME 機制下，在網際網路上傳輸交換訊息和商務多媒體資料，因此，本研究可做為電子商務系統整合的參考。

關鍵詞：網際網路電子資料交換、MIME 封裝、SMTP、商務多媒體、資訊安全

Abstract

Electronic Data Interchange (EDI) is defined as the corresponding standard of both or multi-communities which is used as the transferring protocol of the structured information through the electronic communication channels. However, the electronic data interchange over Internet

* 國立交通大學資訊管理研究所

Institute of Information Management, National Chiao Tung University

Integration(EDIINT) is an integrated mechanism which does not only support the EDI standard but also can be used under the Internet environment. Its purpose emphasizes at the integration of many existing Internet transferring schemes and offers an open exchanging standard for the data interchange and communication. In this study, we focus at the EDIINT integration from different aspect. Besides, we provide the evidence of supporting EDIINT from the business operation point of view, examine the evolution of this standard by comparing the criterion of either the close or open property of the network and the EDI standard . Fulfilling the requirement of open transferring standard and network communication, we propose a complete business EDIINT approach through mail system by combining existing UN/EDIFACT and MIME format and prove its feasibility.

In addition, there are increasing need for business multimedia applications such as digital watermarking image, video and audio data. To provide the interre lationship between the EDI standard and the multimedia information, our system supports the business multimedia service and confirms its capability of integration.

At the stage of communication, we also encapsulate the security control mechanism. The schem e completes the actual implementation for the safe Internet business electronic data interchange and transmission under UNIX and MS' Windows testing environment . Our study shows that it is easy to integrate the EDI translator with the mail agent for SMTP service, transfer EDI strings and business multimedia under the reliable PGP/MIME protocol. Due to the speedy commercialization of the Internet and the fast prosperity of the E-commerce, we expect that our integrated technology study could behave as the ref erence for the development and the applications in the associated fields.

Keywords: EDI over Internet integration (EDIINT), MIME encapsulation, SMTP, business multimedia, information security

壹、前言

一、歷史背景

電子資料交換（EDI，Electronic Data Interchange）是電子商務（EC，Electronic Commerce）的基本文件流通格式，此種資料交換格式的標準化與接受程度，是商務交易普及的重要指標；最早商務上 EDI 的應用，可信的實例據傳是 1857 年間克里米亞半島的戰爭，英軍將領廣泛地運用歐洲電報傳訊，對倫敦股票交易所進行的遠距離商務交易，成爲以電報進行的商務傳奇(Kimberley, 1991)。前述的例子可說是最早型態的 EDI，而現今，資訊科技所定義的電子資料交換則是：「在雙方或多方同意的標準下，從一個資訊系統到另一個系統，以資訊、通訊的方式傳輸結構化的資料」(ANSI ASC X.12; Kimberley, 1991; Pageant, 1996; UN/EDIFACT; Veijalainen, 1992)；這個正式概念的形成，可追朔到 1940 年代末期，但卻遲至 1970 年代才有實際可行的系統出現，如 EFT（Electronic Funds Transfer 提供的 Private Payment Network）(III(1) , 1998; Sokol, 1994)。到了 1980 年代，個人電腦和迷你電腦系統逐漸被企業所接受，以加值網路（VAN，Value Added Network）爲基礎的電子資料交換系統，亦即所謂的 VAN-EDI，開始出現於企業內部和企業之間、使用自行訂定於企業間的電子商務交易和資訊交換流通標準 (III(1), 1998; III(2), 1998; Kimberley, 1991; Sokol, 1994)。而在此時已逐漸成熟的網際網路，於 1990 年代初期至今日，歷經正式商業化之進程後，使 EDI 進入到另外一個使用公開的網際網路和開放標準的時代 – 支援網際網路的電子資料交換（EDIINT，EDI over Internet 或稱 EOI）的概念，隨之成型。

二、研究動機

正如前段所述，近年來因爲資訊技術和通訊科技的急速進步，電腦和通訊網路成本地降低，使得電子商務和 EDI 的研究，以及其格式、機制的制定，成爲商務交易流通的首要課題，再加上網際網路的快速興起和普及、輔助文字或電子資料之商務多媒體使用率的增加，更使得電子資料交換步入一個嶄新的境界。

在網際通訊中，「格式標準化」和「通訊公開化」這兩個重點，佔有重要的份量。而商務多媒體的應用，其重要性將會與日遽增，更是網路行銷必需的環節；同時，在以指紋或視網膜紋路爲辨識資訊的身份認證，亦有可能成爲 EDIINT 中的必需元件；因此聲音、影像，甚至動畫都有可能成爲 EDI 的交換資訊之一；而現行的 EDI 架構中，並未正式定義其封裝的規格，有鑑於此，本研究會在此補充其不足。

是故，本研究針對上述幾個方向，利用網際網路上 SMTP 傳輸的 MIME Enveloped Internet EDIINT 進行研究探討，使用 ISO 認可的 UN/EDIFACT 公開標準作爲

交換的標準，並嘗試嵌入商務多媒體於EDIINT 中，建構合理的架構模型，和實體之研究設計；並輔之以實際系統的驗證，探討其可行性和整合成效，以及此架構在實作上應注意的要項。

貳、電子資料交換之概念簡介

一、企業競爭力與電子資料交換

從 1980 年代的無紙化（Paperless）環境、辦公室自動化（OA），JIT（Just In Time）、全面品質管理 TQM（Total Quality Management），以及商業快速反應 QR/ECR（Quick Response or Efficient Consumer Response），到 1990 年代，企業程序再造 BPR（Business Process Redesign）、企業資源規劃 ERP（Enterprise Resource Planning）等的企業改造過程中，電子商務和 EDI 往往是企業在商務上追求競爭力過程中，首要的考量之一(III(1), 1998; III(2), 1998; Kimberley, 1991; Sokol, 1994)。在能夠降低人事成本、減低紙張和郵資的花費、降低人為因素造成之錯誤、改善顧客服務及產品品質、縮短交易時程、增進資料安全等誘因下，企業將無可避免地進入以電子資料交換為主體的網際商務進程，例如，網路電子下單查詢、票據交換、虛擬企業（如台積電張忠謀董事長所提及的 Virtual Fab）的建構和連結等。

二、互通性的考量：交換標準和通訊網路

而在企業進行的傳統商務資料交換，所賴以溝通的通訊機制，乃是建立於其間特有的管道（如，郵件、FAX、快遞等），而藉由此通訊機制，商務間往來的入帳、轉帳、詢問、報價、採購等行為，則根據雙方或多方的商務格式標準，以共有的通訊管道，方得以順利地進行。同樣地，EDI 所進行的資料交換，也遵循著相同的原則，此機制大致可從兩方面來探討，一方面是交換標準（Interchange Standards），另一方面則是通訊網路（Communication Networking）。

這兩方面的考量，可用以下三種型態的 EDI 來進行說明（圖 1）。假設存在有 A,B,C,D 四個企業網路，第一種的架構為專屬的 EDI 交換標準和封閉型網路（Proprietary Standards over Closed Network），這通常需要商務伙伴以一對一型態，建立資料交換網路協定，及其隨之而生的 EDI 交換機制和標準；無可諱言的，要支援此種封閉型態的專屬 EDI 系統，必須要面對可觀的通訊網路、軟體開發成本和維護費用（參見圖 1，對 A 網路而言，極可能需要三種不同的通訊機制，才能同時對 B、C、D 企業體的網路進行通訊，整體而言，對這四個商務伙伴來說，要進行商務上的資料交換，就要有至多六種的標準和網路）。當然，上述架構的建置成本由於過高，進而導致獲利的降低，所以對於第二種型態 – 開放標準（Open Standards）需求的聲浪便提高；開放標準隨著規模和需求的大小而定，有產業間的標準

（Industry-Specific），也有跨產業（Cross-Industry）的標準；遵循著這一套開放式準則，軟體開發和通訊網路的建置維護費用，便可以降低，而其獲利，則可因爲 EDI 帶來的便捷隨之提高；然而這特定的標準，還是在遵循特定標準的商業聯盟內之封閉型網路上執行，無法和未加入此封閉網路的商務伙伴，進行電子商務上的交易，其使用層面則較爲地域性所限制（參見圖 2）。

三、開放型標準和網際網路的結合：網際網路電子資料交換

上述的圖 1、圖 2 兩種型態的缺點在於其開放性的不足，以及專屬網路所產生的昂貴初期建置、後續維護成本，這些缺點在第三種型態的架構中可加以克服（圖 3），此架構建構於 EDI 開放型標準，並透過網際網路傳送，爲 EDIINT（EDI over Internet）的基本傳輸模式。第二種和第三種型態（圖 2 和圖 3）最主要的不同，同樣可以從「交換標準」和「通訊網路」兩方面來比較：就「交換標準」而言，第二種型態的標準並非公開認定的標準，而只是業界內的標準，第三種型態的架構，則是採用由國際組織制訂的公開標準；而「通訊網路」更是這兩者最主要的差別，前者雖能夠在其伙伴之間互通，但是和後者以網際網路爲通訊骨幹的便利性相較，仍有顯著的差異。

就企業界或組織間目前應用之商務公開格式標準而言，廣被採納的有兩種：一是由 ANSI 授權制訂的 ANSI ASC X.12 標準 (ANSI ASC X.12)；另一則是由聯合國制訂、ISO 認可的 UN/EDIFACT（Electronic Data Interchange for Administration, Commerce and Transport）標準 (UN/EDIFACT)。其中前者在北美的接受度較高，發展也較早，於管理、

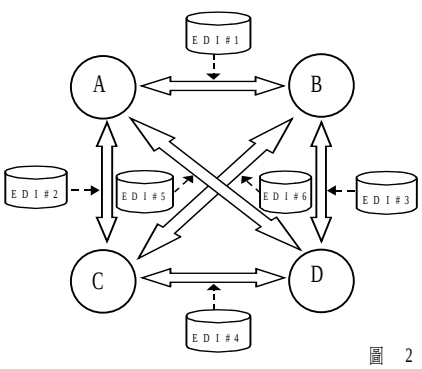

圖 1 專屬網路及專屬標準（專屬 EDI 規格 #1~#6）

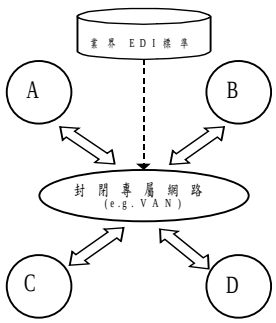

圖 2 封閉網路及業界標準（業界定義之專屬標準）

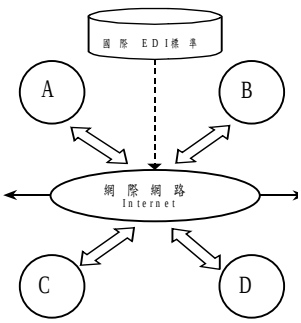

圖 3 開放網路(網際網路)及開放標準(國際標準)

圖 1~3 假設 A、B、C、D 爲四個有商務來往的企業，箭頭表其網路傳輸連結，虛線代表 EDI 規格

商務、教育、運輸等方面皆有規格上的敘述；而後者 UN/EDIFACT，參考了 ASC X.12 的規格，發展較晚，和 ASC X.12 的差異性並不大，定義則較爲完善。在亞洲（包括台灣）和歐洲的電子資料交換應用，則以 UN/EDIFACT 較爲普遍。

而不論使用何種的規格、標準和傳輸，不可否認的，在現今企業中，EDI 往往被視爲企業再造，製造競爭力優勢的關鍵；同時，隨著電子商務時代的來臨和網際網路的盛行，使用 EDI 建構標準格式的商業交易已成爲不可抗拒的趨勢。部分企業使用的 EDI 系統，多建構於封閉性質的加值網路上；相較於加值網路，使用開放標準和網際網路的系統，在普及性和使用的便利性，都普遍優於封閉型的加值網路；只要資訊安全及密碼技術能使網際網路傳輸更爲可靠，利用開放式的網際網路來達成 EDI 的實作應用，會比建構在成本高昂、擴充不易的加值網路上有更多的好處。

參、網際網路電子資料交換

一、各類型網際網路電子資料交換傳輸方式

確定了交換標準和通訊網路爲發展 EDI 的重點後，首先來討論傳輸交換的格式。在網際網路上可用來進行的傳輸方式基本上有下列幾種 (Kilpatric, 1996)：

- FTP（File Transfer Protocol）：爲網際網路上傳輸文字和二進位檔案之協定，同時兼具速率和穩定性，適合大量檔案的傳輸 (Postel and Reynolds, 1985)。
- HTTP（Hypertext Transfer Protocol）：WWW 所使用的協定，佔目前大部分網際網路的使用量，適合用於包裝多媒體 (Fielding, 1997)。
- IRC（Internet Relay Chat Protocol）：具互動性質的網際網路討論環境，適合即時互動的資料、訊息交換 (Oikarinen, 1993)。
- NNTP（News Network Transfer Protocol）：網際網路討論區之協定，適合具有分散性討論區文件的包裝與傳送 (Kantor, 1986)。
- SMTP（Simple Mail Transfer Protocol）：用以傳輸電子郵件的協定，配合上適當的介面和封裝機制，如 MIME（Multipurpose Internet Mail Extensions）機制，適合一般郵件交換與傳輸 (Postel, 1982; Postel and Reynolds, 1985)。
- Socket Transmission：Host-to-Host 的封包直接傳送方式。

大部分的機制或協定都有相當程度的應用軟體及使用者，協定的標準也大致完整，這使得 EDIINT 能夠迅速地透過上述多種通訊傳輸協定，完成 EDI 的訊息交換。而完

整的系統，則仍需要成本效益的考量及安全傳輸的機制。

二、使用 **MIME** 封裝、**SMTP** 傳送達成的 **EDIINT**

從上述多種的通訊傳輸協定中，若以系統建置成本及頻寬資源限制來考量，則效益/成本比數值最高，使用率最普及的，便是利用 SMTP 傳輸協定的網際網路電子郵件機制。IETF（Internet Engineering Task Force）的 EDIINT 工作小組建議使用以 MIME 封裝（Envelope or Encapsulate）EDI 物件之後，再進行 SMTP 上協定之傳輸。而 SMTP 所擁有的點對點（Peer-to-Peer）傳遞特性，可同時傳輸多筆資料給多方的交易伙伴，在傳輸的過程中，若發生錯誤，如：Host Unreachable 產生無法傳送信件的狀況，SMTP Daemon 會迅速讓發送方得知。

在過去，於 Netnews 或 E-Mail 傳遞之間，爲了使多媒體或者非 7-Bit ASCII 之歐亞語系文字訊息能夠傳送，往往必須要使用 uuencode/uudecode 等程式來包裝，這在使用上並非十分便利，故 MIME 的出現，利用其特有之 Multi-Part Entity 和 Content-Transfer-Encode 的特性，可以讓一般附有多媒體資料的商務訊息，得以方便地利用 MIME 來封裝，透過 SMTP 進行傳送。整合並解決了上述問題；MIME 主要的這兩種技術將於下面的章節加以介紹。

肆、以 **MIME** 封裝的網際網路電子資料交換基礎架構

一、**EDIINT** 的基礎架構

IETF 之 EDIINT Work Group 主持人 Rik Drummond 等人提出 EDIINT 的基本資料的流程 (Crocker, 1982)（參考圖 4，四個 EDIINT 資料的流程）包含四個系統處理步驟。這四個部分分別爲：

（一）企業內部資訊系統（Company's Internal Information Systems）：如企業內部的會計資訊系統、財物控管系統、物流管理系統。

（二）電子資料交換格式標準轉換系統（EDI Translator – converts internal formats to standard purchase order and invoice formats, and so on）：依照交換標準的需求所制訂的格式轉換系統。

（三）通訊介面（Communications Interface – TCP/IP, SMTP and S/MIME）：封裝資料之機制、傳送資料之協定，如 MIME、SMTP 等。

（四）網際網路或 TCP/IP 連結機制（Internet or direct TCP/IP Connection）：網際網路上的傳輸機制。

這四個步驟是形成 EDIINT 資料傳送之基本架構，簡單陳述如下：首先傳統的商務資料在企業內部（如採購單）經由內部的財務系統，轉成 EDI Translator 可辨識之檔案或資料，進而由 EDI Translator 轉換成公開交換的格式，稱之爲電子資料交換字串（EDI Strings）；接著由 RFC 822/RFC 1767 (Crocker, 1982; Crocker, 1995) 的 Mail 和 MIME 封裝，將其封裝成 E-Mail 信封，透過 SMTP 和 Internet 的傳輸協定傳送到商務伙伴的系統上（可參考相對應的圖 5 之架構）。這四個系統處理步驟及資料流程，根據本文先前提到的「交換標準」和「通訊網路」分爲兩類階段於接下來的章節，對其標準轉換和通訊傳送的細節來討論其架構。

二、公開標準的轉換

在開始進行 EDIINT 的系統建置之前，企業首先選定一公開標準作爲其電子資料交換標準參考，本研究採用在台灣普遍使用的 UN/EDIFACT 標準架構（參見圖 6）爲例。公開標準轉換，包含對應和轉換（Mapping and Translating）兩個主要的部分，但一般通稱這兩個步驟爲轉換（Translating）或轉化

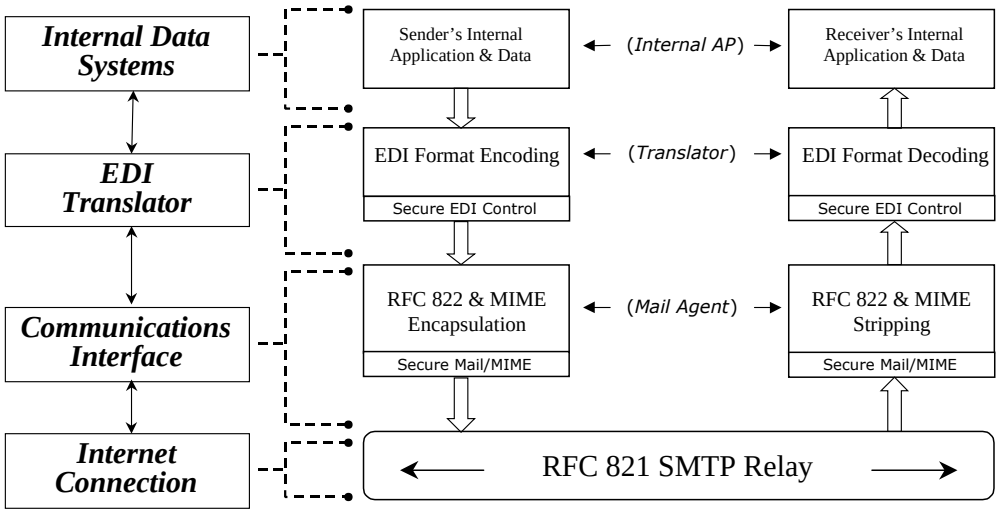

圖 4

圖 5

圖 4 基礎架構　　圖 5，對照於 Drummond 等人所建議的四個資料流程 圖 4

（Converting）。

最先的步驟爲企業內部產生一般型態的資料（例如前述之採購單，或本研究實例之轉帳單），此文件單據爲傳統商務活動所廣爲通行，經由其內部的軟體建檔後，先對應成數位化的循序檔案（Sequential File）。此循序檔案內含所有前述文件單據的資料，但是型態是以數位和循序型態出現，也就是說，資料是一個緊接著一個排序下來；此循序檔案，可以是資料庫檔案、純文字循序檔案等任何有序的數位資料（參見圖 7）。以上轉換成內部循序檔的步驟，本研究稱之爲「內部對應」（Internal Mapping）。

接著，由 EDI Translator 中 Mapping 功能，將循序檔案辨識爲 Translator 第二步驟的前置檔案，稱之爲商務平坦檔案（Flat File）。我們稱此步驟爲「外部對應」（External Mapping）。Flat File 並無一定之格式 (Kimberley, 1991; Sokol, 1994)，端視所使用的 Translator 如何讀取和應用，而且 Flat File 無須包含所有循序檔案的內容，譬如網路傳輸並不需要實體的郵遞區號作爲傳送上的參考，「郵遞區號」的資訊便可以省略（EDIFACT 中有許多的 Message types，都

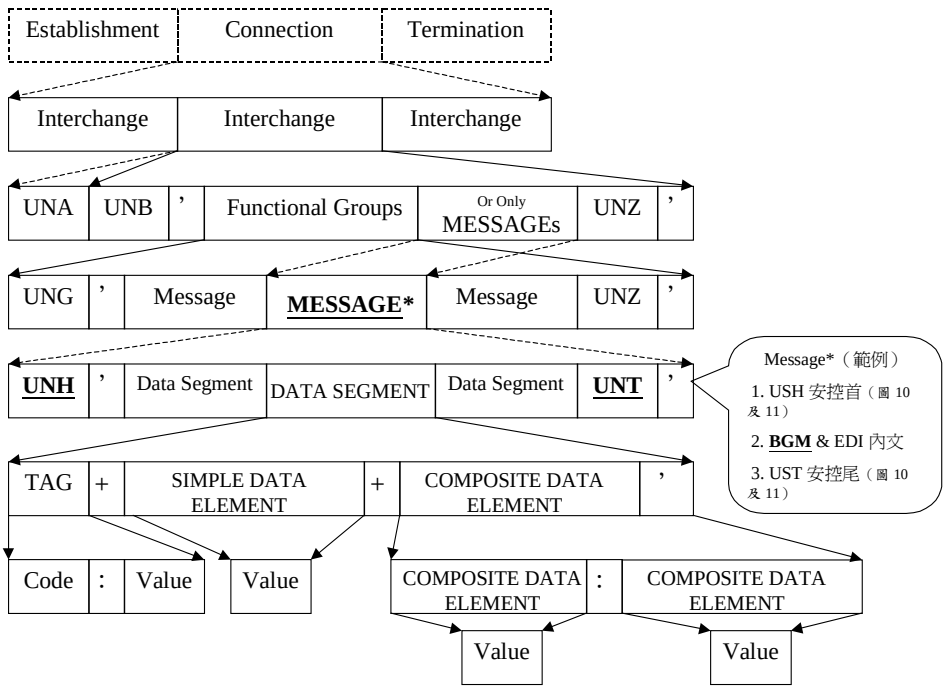

圖 6 EDIFACT 的層級示意圖。安控服務部分包含在內文資料段之前後（參見圖 10）

包含 NAD segment，也就是 name and address，所以基本上，公司地址爲電子資料交換之必要元件，如定貨、送貨、維修、運輸，都牽涉到實體上的位址，但是並無 zip code 相關的 segment；雖然 zip code 在電子資訊交換的過程中，並無其必要性，但是也可由 translator 內建的 address-to-zipcode 的 lookup table 找出 zip code，這也是其爲何可以省略的原因）。

由於 Flat File 已經具備 EDIFACT 字串之前身，各個資料段（Data Segment）都已按照標準格式排好，內容按照其訊息格式（Message Type）的定義，例如訊息標頭（UNH，Message Header）、訊息標尾（UNT，Message Trailer）和訊息內文首（BGM，Begin of Message）（圖 6）等。此 Flat File 的資料，除了尚未計算或加入的資料段，以及未加上資料段標籤外（Segment Tag，如 UNH、UNT、BGM），大致上已趨於完整。因此，我們綜合前述對應的步驟，並根據對應函示所產生的檔案，提出 Translator 對應部分，有內、外部對應的區別。

EDI Translator 第二步驟根據資料段的順序（Order）、進行資料欄位的壓縮和重複取代（Compression and Repetition）、計算資料段數目、嵌入時間日期和其他需要計算的

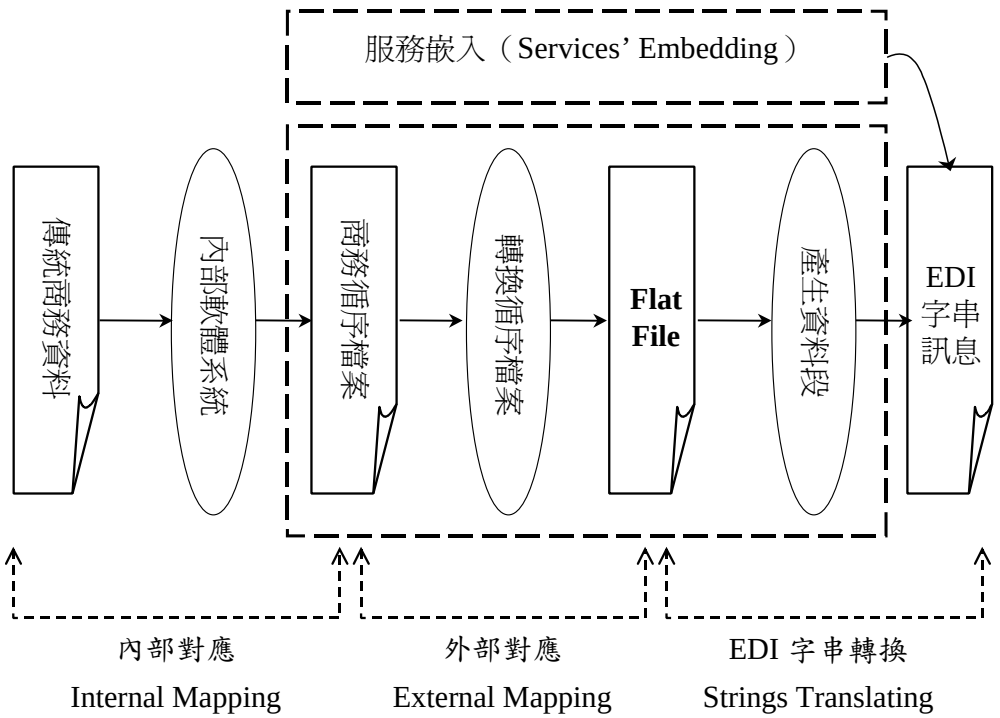

圖 7 公開標準的轉換程序（虛線內部爲 EDI Translator 所應進行的服務）

資料等轉換步驟，產生 EDI Strings，如：DTM+138:19981003:102'

至於更詳細的 UN/EDIFACT 訊息請參考其標準 (UN/ECE, 1998; UN/EDIFACT)。一個交換訊息應包含由許多此種資料段。至此，整個公開標準的轉換到此完成，這一部份包含整體的流程，可以參考圖 7 之流程圖。接下來便是「通訊網路傳送」的部分，此部分將在下一節介紹。

而當交易伙伴收到 EDI 字串訊息，其解碼轉換的流程便如圖 7 所示，但以反方向來做所有的解碼工作（可參考相對應的圖 5），轉換過程在發送端可稱爲編碼，在接收端可稱爲解碼，兩者可通稱爲轉換。原則上，本研究所發展的架構，是兩邊對稱的，皆具有發送、接收之能力，可供跨平台應用的參考。而主要強調的 EDI Translator 和 MIME Supported Mail Agent 部分，亦是收、發端採用相同的系統，只要有適當的設定或者 Plug-Ins 機制，具有瀏覽器或 Mail User Agent 的環境便可收發訊息，整合上十分地容易；此概念也簡化了商用上所碰到的系統接受和互通程度，以及建置維護成本考量的問題。

三、通訊網路的傳送 – 支援 MIME 的 Agent

通訊網路的封裝部分包含 RFC 821&822（SMTP，Simple Mail Transfer Protocol & Standard For The Format of ARPA Internet Text Messages），此部分包括傳送 E-Mail 訊息的應用層機制，和訊息的交換標準。負責封裝訊息的 RFC 2045/2046/2047(Freed and Borenstein(1), 1996; Freed and Borenstein(2), 1996; Moore, 1996) 定義 MIME 內容、編碼定義和 RFC 1767（MIME Enveloped EDI）等 EDI 和電子郵件的封裝；以上這些部分，都可選擇適當的 Mail Agent 予以支援，不需重新自行設計和實作傳輸的系統。封裝完成後，藉由 SMTP 傳送此包含 EDI 資訊的電子郵件。RFC 822 規定了電子郵件之標頭（Header）欄位，包含 From、To、Date、Subject 等等；而 RFC 1767 中定義之 MIME 封裝 EDI 物件的規格，利用成熟普遍之 SMTP Relay 郵件技術，建構出成本低廉，具有效率、安全、並且使用簡易的 EDI 系統；此種方法，可以將平台之相容性問題所造成之影響降到最低，只要有相關之轉換 Application 和支援 MIME 格式的 Mail Agent（如：Mutt、Netscape Mailbox、Euroda 等），便可進行傳遞。

而 MIME 封裝能有如此表現的關鍵技術，一爲 Multi-Part Entity 的功能，另一爲 Content-Transfer-Encode 的功能。前者能使在 RFC822 規定的本文外，另外 attach 上延伸的文件、檔案、訊息等；根據各個文件的 Content-Type 和 Content-Description 等重要的 MIME Headers，將其依照各個不同的 Entity 分類，便能夠傳送多個檔案資料。後者則是利用各種 Encoding 的方式，將資

料予以編碼成爲 7-Bit ASCII 便利於傳輸，在此方面的編碼有 7bit、8bit、binary、quoted-printable、base64 等；此部分則有利於傳輸商務多媒體和非 7-Bit 語系的文字訊息。因此，如果要傳遞商務多媒體，如聲音、影像、圖形，只要有相關的 Translator 和支援多媒體的 Application 之引入，在 MIME-Types 定義和 Application 開啓設定上進行編輯，便可很有彈性地進行 EDI Translator 和 Mail Agents 之間的整合，這是本研究之所以使用支援 MIME 之 Mail Agents 和 SMTP 來進行 EDIINT 建構的原因。

四、多媒體的嵌入

前面的段落陸續提到了：透過 MIME 的封裝、以及 Translator 和 Mail Agent 的整合，可以讓我們除了傳送 UN/EDIFACT 的交換字串外，另一方面亦可藉由前述的技術，來傳送商務多媒體相關資料。而關於嵌入商務多媒體於此 EDIINT 系統的整合作法，本研究採取的概念如下：

MIME 的 Multi-Part 以及 Content-Transfer-Encode 能使我們容易地對多媒體資料進行編碼和封裝，使其能在 7-Bit 的 SMTP 下傳送；但其 Attach 的多媒體檔案，雖說可和此信件一起傳送到收信者，但是其關連性卻未在 EDIFACT 字串上有任何著墨，僅可靠著信件中出現的 Text Message Attachment 來描述、或者是利用本身 Attachment 的 Content-Description Header 來描述此多媒體圖像、音訊、動畫等資料和商務 EDIFACT 字串的關係；然而，此種作法並非十分嚴謹，和 EDI 字串的關連性也不大。因此本研究嘗試利用在各種 Message Type 皆存在的「具有彈性之 Segment」，如：FTX，Free Text 此類 Segment，來定義多媒體資料和商務 EDI 字串的連結；方法如下：

FTX+MULTIMEDIA_RELATION_EXTENSION+2+IMAGE:00001:JPEG:DESK0008.JPG:DESK_0008_NEW_CATALOG+VIDEO:00002:MPEG:HELLO.MPG:HELLO_TO_PARTNERS_MESSAGE'

以此爲例，該 Interchange Message 爲一個商品目錄資訊的交換，除了發送方傳送給對方除了 EDI 商務字串外，並 attach 上兩個商務多媒體檔案，一個爲 DESK0008.JPG，展示此種類型的桌子（Desk_0008_new_catalog），另外附上一段給商務伙伴的招呼影片檔 HELLO.MPG，進行對商務伙伴的介紹（Hello_to_partners_message）；這段 Segment 最前面便說明了這個是「多媒體訊息的相關擴充」，可充分地形容所附加的商務多媒體檔案，並且和 MIME 封裝所產生的 Headers，如 Content-Type / Content-Description 等進行 EDI 和多媒體檔案間的連結和嵌入。

伍、模型架構的建立和實測

一、架構與流程建立

綜合以上概念，本研究嘗試建立一個完整的系統模型和流程，並實際對此系統的可行性進行實驗測試（參見圖 8 及 圖 9）。而在此部分，本研究首先利用 UNIX 爲作業環境進行模擬測試，詳細測試環境的背景資料可參見 附表 1。以下爲流程的說明：

公開標準的轉換程序 – 在圖 8 中，說明了第一個流程，也就是發信者到收信者的流程（又稱爲商務交換傳送流程）。步驟ı 將企業內部資料經由內部軟體系統（參考商務伙伴資料庫），轉換爲 Flat File 和相關之商務多媒體資料。Flat File 經過 EDI 公開標準轉換器（EDIFACT Standard Translator），進行步驟ɱ 參考 UN/EDIFACT 格式及安控管理格式轉換成 EDI 交換字串之過程。而同時產生之商務多媒體資料，則直接傳送至 Mail Agent 部分，準備進行 MIME Multi-Part 的封裝。如前面「多媒體嵌入」章節所述，此部分也利用 Translator 和 Mail Agent 的整合，在訊息內中具彈性的 Segment 內（本研究以 FTX 此 Segment 爲主），加入和 EDI 商務訊息字串的連結關係。

通訊網路的傳送程序 – Mail Agent 參考其 MIME 設定（MIME-Types 和 Metamail Capabilities，參考表 2 之定義的模式），對所附的 Attachments 進行 Content-Transfer-Encoding，根據各種不同的內容而有 8-Bit、7-Bit、Quote-Printable、Base-64 (Freed and Borenstein(1), 1996; Freed and Borenstein(2), 1996)等幾種常見的編碼方式。於是經過步驟ɳ 後，產生了包含安控管理首尾 PAYEXT EDI 的 Mail，並包含相關連的商務多媒體資料。此封 Mail 經過 MIME 的封裝，可經由 Mail Agent 呼叫 PGPv2 予以加密，傳送至 SMTP Server，進行步驟ə 的信件傳送。

對稱逆向解碼過程 – 在步驟ə 中，Mail Agent 將 MIME 封裝解開，Mail Agent 判定其中 EDI 字串的 attachment 爲 edifact 的 MIME-Type，於是呼叫 edifact-decode（本研究的 decode 應用程式），來解開 PAYEXT 的 EDI 字串；經過逆向步驟的轉換（步驟ə 和ə），變成傳統的內部商務資料。而步驟ə，同樣地，商務多媒體資料經由 Mail Agent 和 Translator 判定其 MIME-Types 和與 EDI 商務字串的相關性，呼叫其所屬的多媒體應用程式，分別予以展示執行。例如，交換訊息附上 HELLO.MPG，便可呼叫 Mpeg-Player 的應用程式來展示，而此多媒體影片的相關參考資訊，也存在於 EDI 字串中(如圖 8 中，＊處之虛線箭頭所示)。

在收信者完成 EDI 和其他多媒體內容的解碼和展示、處理後，本研究使 EDI 交流的雙方增加了互動性，譬如說 edifact-decode 會要求收信者選擇是否寄回收據（參考圖 9），若答案是肯定的，則緊接著在圖 9 的步驟ı 便會成立；此步驟，edifact-decode 會呼叫安控回應程式，產生 AUTACK 回應訊息 (UN/ECE, 1998)，並呼叫 Mail Agent 將此附

有 AUTACK 訊息的 Mail 送回原發信者；本範例雖只有示範 AUTACK 的互動訊息，然而基本上，只要有接續的訊息傳達，互動的交流便可以持續進行。

接著圖 9 的步驟ⓜ ⓝ ⓐ ⓐ ⓐ 和圖 8 的ⓝ ⓐ ⓐ ⓐ ⓐ 步驟幾乎相同，差別的是，一個呼叫 edifact-decode 進行解碼轉換，而另外一個呼叫 edifact_ack-decoder（AUTACK Decoder）。

二、安控的嵌入

安控的格式（AUTACK）包含兩部分：傳送端的安控標頭、標尾規格，以及收信端的安控回應收據。將安控首和安控尾所嵌入於 PAYEXT (見附表 1) 的內文前後（圖 6），其詳細格式請參考圖 10 和圖 11 之安控規格。值得一提的是資料段 USR 擺放是數位簽章的部分，因此模型架構必須要考慮到引入 SHA、DSS、MD5 (Rivest, 1992)等摘要（Digest）和數位簽章等模組程式。架構中把嵌入安控管理的工作交給圖 8 步驟ⓜ 的 EDI Translator，理由是安控規格也是 EDI 訊息的一部份。而安控回應訊息則是依據雙方所協定之安控首尾，加以鑑別後，所產生的回應訊息，同樣地有 USR 的安控演算結果，以及其他安控管理參考號碼、連結號碼等。安控的目的在於增進資訊的安全，而在本研究的系統中，除了上述的 EDI 安控管理，確保了資料的真確性和不可否認性，另外還有封裝層面的 PGP/MIME 機制，可用來保護第二層次的資料隱密性和身份鑑別的功能，因此整體而言，如此的結構，可有雙重的資料安控機制。

三、實測與結果

利用前述之模型架構（圖 8 及 9），並使用實作之作業環境（參考表 1），撰寫此模型之測試系統，所得到的正如結果預期一般，能夠以 MIME 封裝 EDI 訊息，此 EDIINT 的模型架構因此得到初步的確認（參見圖 12 和 圖 13）。在圖 12 中，利用金融交易的 Payment Instruction 表單（根據 EDIFACT 之 PAYEXT 訊息種類），進行實例傳送、轉換成字串、封裝、加密、簽章、解碼、逆向轉換解碼，經由此架構的傳輸，達成利用電子郵件系統進行 EDIINT 的實作。實作的背景爲：

- 使用者 T.H.Wu（統一編號 11027686）想要轉三張支票給 M.J.Tsai（統一編號 11027687），金額分別是 $250,000.00、$100,000.00 和 $150,000.00，轉帳方式爲藉由其所屬銀行扣款及入帳。
- 而 T.H.Wu 所屬的銀行爲 IIM-Bank（銀行代號 1116），其所在之銀行帳號爲 00010061072156，M.J.Tsai 所屬的銀行爲 NCTU-Bank（銀行代號 1126），其銀行帳號爲 00076154100786。
- 核定轉帳日期爲 1998/10/03 早上九

點三十分，由 IIM-Bank 發出此內部編號爲 #00001 的轉帳單據，審核者爲 K-Department 的 J.Stanton。

– 在發送端（應爲 T.H.Wu 所屬銀行，以 T.H.Wu 之 E-Mail Address – thwu@iimserv.iim.nctu.edu.tw 表示）將此張 Payment Instruction 紙張單據，經內部軟體、Translator 轉換，再傳送到收送端入帳（應爲 M.J.Tsai 所屬銀行，以 M.J.Tsai 之 E-Mail 地址 mjtsai@cc.nctu.edu.tw 表示）。

而完整的流程如下：

1. 首先發信者端經由內部軟體和 Translator 將 Payment Instruction 的內部商務文件，轉換成 EDIFACT 字串，並嵌入安控管理機制（參考圖 12 步驟 ㄧ）。
2. 經由 mutt 的 MIME 封裝，從 T.H.Wu 傳送給 M.J.Tsai，並透過呼叫 PGPv2 來進行數位簽署和加密，包含內文說明 [text/plain] 的 attachment #1 和轉帳訊息的 EDIFACT 字串 – [application/x-edifact] result.edifact 的 attachment #2，和一個原始文件掃瞄稿

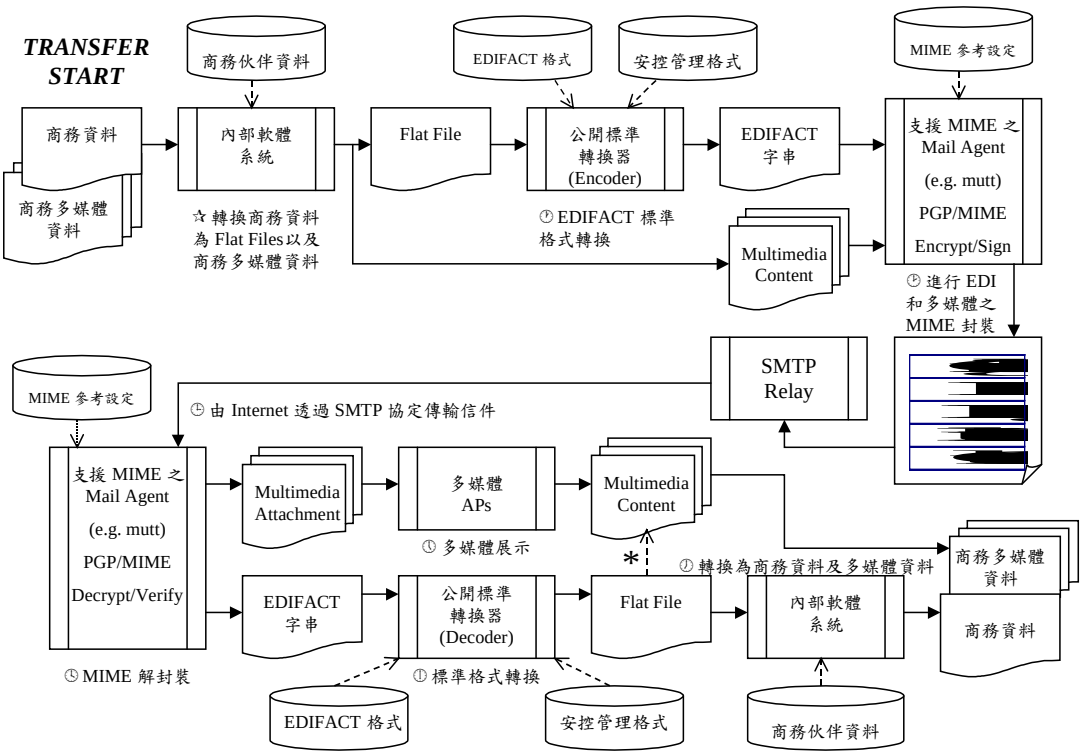

圖 8 本研究之 EDIINT 模式（商務交換傳送流程）

的數位影像檔案 – [image/jpeg] scanned_original_doc.jpg 的 attachment #3（參考圖 12 步驟ⓜ）。

3. 經由 SMTP 的傳送，將含 EDI 的電子郵件，從發信者 T.H.Wu 傳送到收信者端 M.J.Tsai，而經由 PGP 的解密，以及 MIME 的解封裝，觀看到此信件（參考圖 12 步驟ⓝ）。可觀察到這三份文件（或稱 entities），分別由 8bit、7bit 和 base64 的編碼，而多媒體的 JEPG 檔案，經由 base64 編碼過後，從 55K 變成 74K 大小。

件之 attachment #2 爲 EDI 字串爲 EDIFACT 規格，呼叫 Translator 之 edifact_decoder 部分予以解碼；最後透過內部軟體，再還原成原先之訊息，予以 M.J.Tsai 入款（參考圖 12 步驟ⓐ）。而該份原文件之掃瞄稿 JPEG 檔案，則可由 MIME-Types 和 Mailcap 判斷，並呼叫影像應用程式如 xv 予以展示（參考附表 2）。

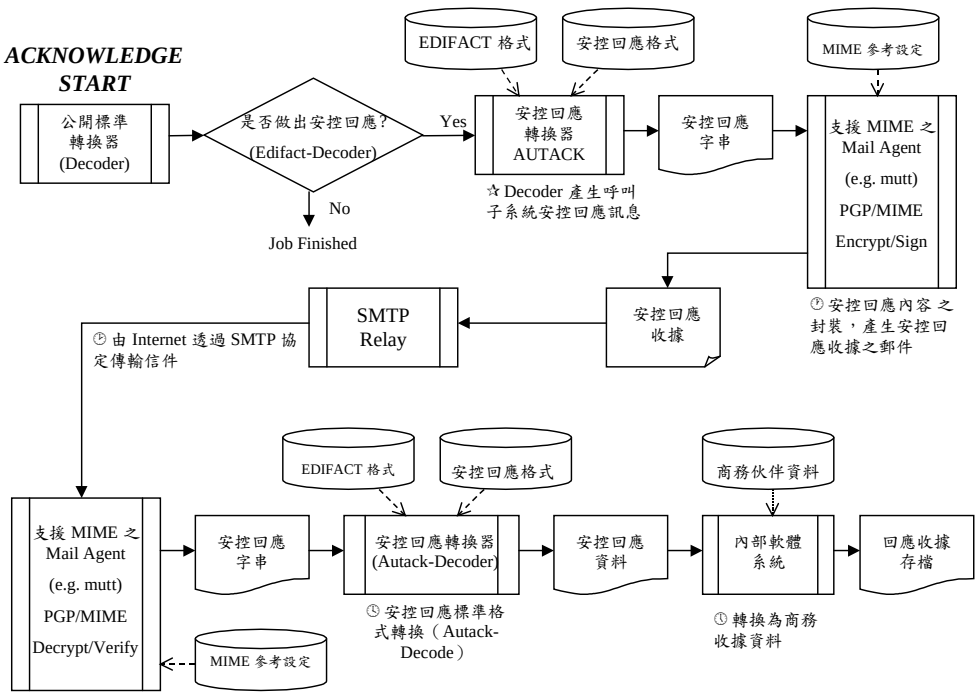

圖 9 本研究之 EDIINT 模式（安控回應流程）

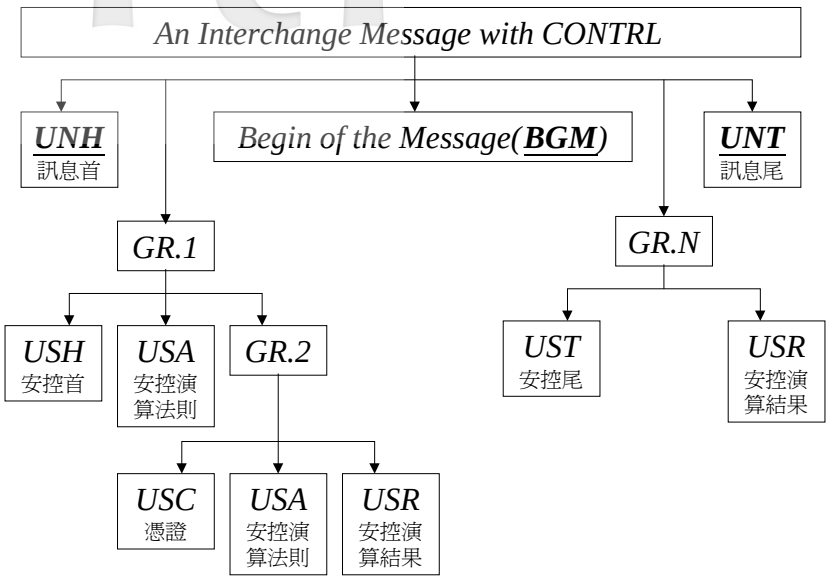

圖 10 安控訊息服務的嵌入層級

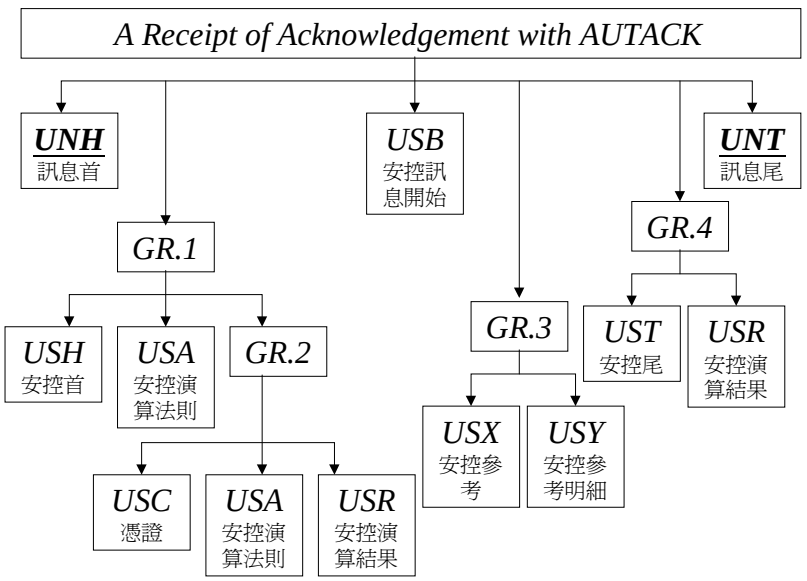

圖 11 安控回應服務的嵌入層級

回應收據，則在圖 13 中展現其回應方式：

5. 接續著上述步驟，在將 EDIFACT 字串解碼後以及一連串內部入帳處理後，詢問收信者 M.J.Tsai 是否傳回安控回應收據給 T.H.Wu（參考圖 13 步驟ə ）。
6. 收信端 M.J.Tsai 產生安控回應 EDI 字串，同樣透過 SMTP 來傳送到原發信者端 T.H.Wu（參考圖 13 步驟ə ）。
7. 原發信者端 T.H.Wu 判定爲其 MIME-Types 爲 EDIFACT-ACK 回應收據（參考圖 13 步驟ə ）。
8. 呼叫其相關之解碼程式 edifact_ack-decode 進行收據 EDIFACT 字串的解碼，並加以歸檔、建檔（參考圖 13 步驟ə ）。

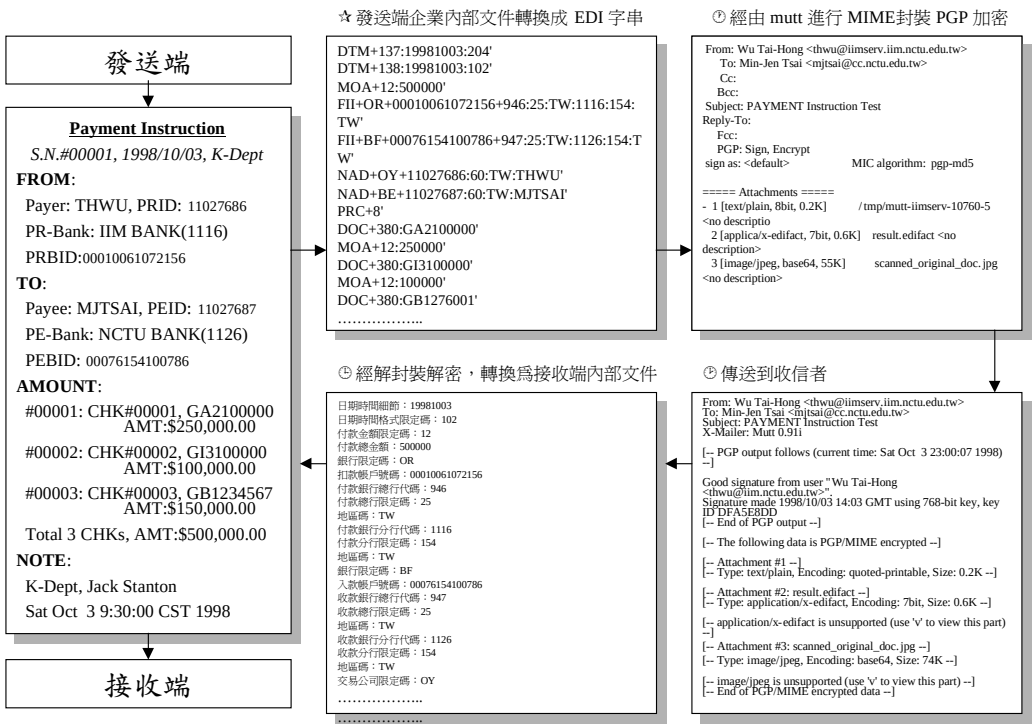

圖 12 EDIINT 架構之實驗結果：發送端到接收端

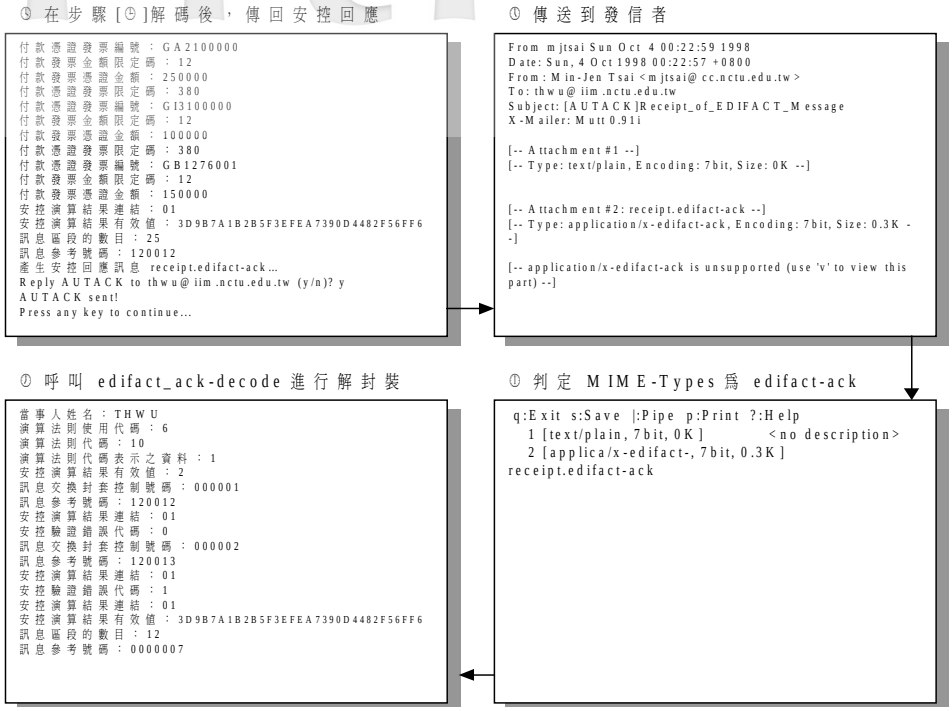

圖 13 續圖 12 ，在步驟[⑤]後，接收端同時進行安控回應

以上的八個實測步驟，便是本系統所產生之一個完整的電子資料交換實例 – 由內部系統、EDIFACT 標準轉換、MIME 封裝、PGP 加密、SMTP 傳送、接收、解密、解封裝、傳回收據、建檔過程便宣告完成。至於在圖 12 和圖 13 中 EDIFACT 和實際的表單對應和轉換，同樣請參見相關之規格標準 (UN/ECE, 1998; UN/EDIFACT)。

而以 MS-Windows 作業環境所做的研究，其交換標準和通訊網路與 Unix 的環境相同，測試環境請見附表 3；在 Windows 的環境中，增添了以圖形介面增加使用者方便性的功能，圖 14 顯示了 EDIINT 的程式介面，輸入 PAYEXT 所需要的資訊，使用者除了可直接輸入之外，也可以直接從資料庫中取得資訊；透過畫面中的選項，可以嵌入多媒體及安控的服務，進入傳送的程序。

此程式透過 MAPI 介面呼叫 Mail Agent ，在此，我們使用 Euroda with PGPi Plug in 來傳輸。詳細的過程類似圖 12 中的流程，在此不再多做敘述。而在圖 15 中，顯示了接收端所得到的交換訊息內容，證實了整個系統之可行性及方便性。

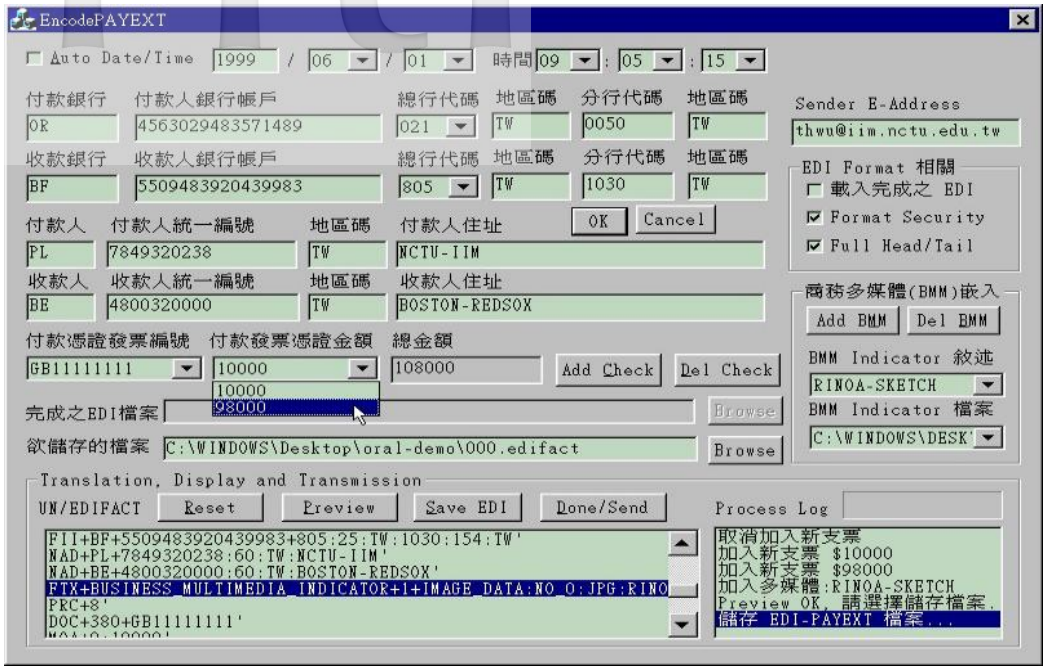

圖 14 在 Sender 端所使用的 EDIINT 的程式介面

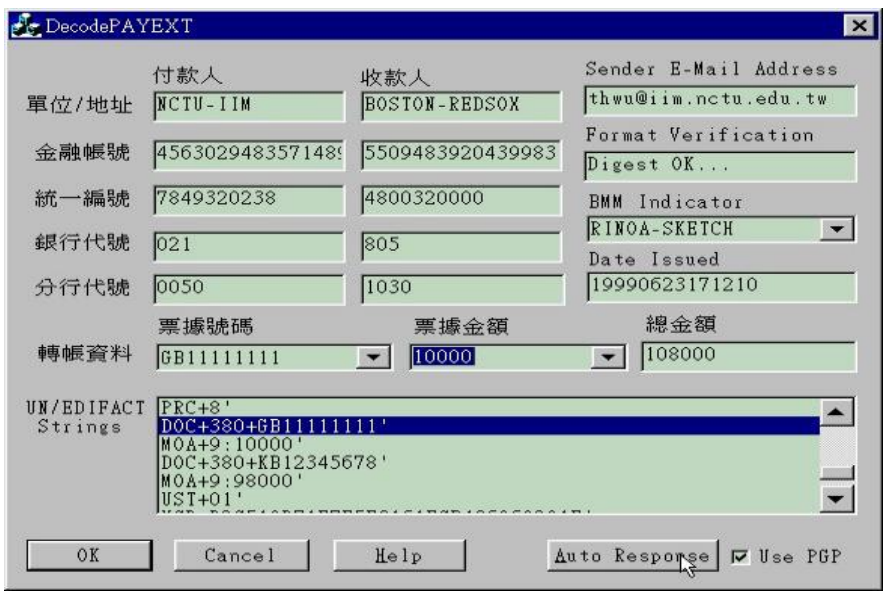

圖 15 在 Receiver 端所使用的 EDIINT 的程式介面

陸、研究心得

本文嘗試建構一個 MIME-EDI Based EDIINT 系統，目的在於利用技術成熟、使用廣泛的 Internet 電子郵件機制來達到商務電子資料的傳輸，使得企業的競爭力，能夠藉由 EDIINT over SMTP 來提升；從通訊網路的角度來看，利用簡便的 E-Mail 機制和開放成熟的 Internet，其使用的效率和建置成本的考量，都遠比封閉性網路來的有競爭力。此系統中還包括 UN/EDIFACT PAYEXT 的公開標準轉換器，同樣地從 EDI 的交換標轉來看，使用廣泛被接受的 UN/EDIFACT，比自行制訂交換規格還來的有擴充性和互通性；而安全控管訊息的傳送和安控回應機制，則可利用 MD5 和 PGPv2 進行數位簽署和公開金鑰加密，而 RFC 822/RFC 2045~2047/RFC 1767 等的封裝，則是利用廣爲使用的 mutt 及 Eudora 來進行測試；綜合以上各個部分實際驗證的結果，證明此架構是可行的。

而系統採用之 UN/EDIFACT 標準，在 D97B (UN/EDIFACT)的標準中，定義了 152 種對於管理、商務和運輸三方面運用的訊息種類。針對企業或組織的需求，從存貨、設備、員工、財務、會計、採購、訂購、回應、銷售、運輸等等不一而足；只要能夠對於所需要的部分，和內部系統協調、撰寫出一個適當的 Translator，那麼配合上本研究之模型，要整合一個利用 MIME 封裝和 SMTP 傳送的安全 EDI 系統，是相當可行的。

而使用 MIME 封裝，更可以在 SMTP 上傳輸商務多媒體資料，如影像、影訊和音訊等；雖然 UN/EDIFACT 並無提到多媒體的嵌入，但在商務、運輸工程和經營管理等應用方面，以 Optional Attachment 的方式(如本研究利用 EDIFACT 中，具彈性的 Segment，如 FTX，記載多媒體資料和商務訊息的關係，達成嵌入的效果)，對於資料的說明和補充，以及和伙伴的互動有更佳的輔助作用。本研究在此更強調其互動性，其原因在於商場瞬息萬變，商務通訊強調及時的反應、與伙伴良好的互動，而商務多媒體的嵌入和安控回應訊息等，在互動性的表現上，無論是從管理層面或技術層面，都能讓我們能夠迅速、有效地和對方進行資料的交換、交易，並擁有一定程度的說服力。

柒、未來的發展與目標

最先我們提到，傳統 EDI 是建構於封閉的網路(如：加值網路上)，由於資訊科技的進步和全球化經營等大環境因素，所以 EDIINT 是無可避免的趨勢；然而對於那些已在加值網路 EDI 投入大筆經費、人才、時間，而且系統運作正常，交易伙伴也充分瞭解目前營運狀況的企業，不論從軟體工程管理或商業上成本考量，都很難有充分的理由使他們放棄目前的穩定系統來進行 EDIINT 的重建。這時候可能的方案就是，

建立一個介於 VAN-EDI 和 EDIINT 之間的通訊閘道（EDI Gateway），使其能夠達到互相連通運作（Inter-Operable），此概念在 IETF EDIINT Working Group 的 Req-05 文件中有所著墨(Shih(2), 1998)，不過仍舊要視封閉型網路所使用的 Protocol 和 EDI 規格而定。

在 MIME-based Secure EDI 上的議題，絕對是不可忽視的。而在此存在兩種可用於 EDIINT 的加密和簽章機制，分別是 PGP/MIME 和 S/MIME (Crocker, 1995; Dusse(2), 1998; Elkins, 1996; Shih, 1998)。此方面的研究實作（本研究採用 PGPv2）和兩種方法的比較，同樣也是一個相當有潛力的研究議題。而 PGP/MIME 和 S/MIME 都會牽涉到公開金鑰的加解密系統，以及管理公開金鑰的憑證機構（CA，Certificate Authority），對交易伙伴間的金鑰進行註冊與管理、認證核發等公開金鑰管理工作，所以，認證中心的建置研究，和 SMTP Service 的結合，亦是未來 EDIINT 發展的重點之一。

此外，除了利用 MIME-Based 封裝方法和 SMTP Relay 來達到 EDIINT 的實作外，近來亦有人提出 S-HTTP（HTTP over SSL，Secure Socket Layer） EDIINT 的概念(Shih(1), 1998; Shih(2), 1998)，可使用如 HTML/SGML/XML 等語言作爲 EDI 交換格式的表示語言，並利用 Java Applet 和 Plug-Ins 等技術，從遠端的商務 Server 下載相關的 EDI 系統和相關設定，可大幅降低終端商務使用者的系統建置、維護成本，此種方式更可以說服消費者和商務伙伴採用 EDIINT 來進行商務上的資料交換及線上交易；而利用 HTTP 也同時引發另外一個可探討的方向，也就是比傳統 Batch EDI 更能夠達到及時互動回應效果的 Interactive EDIINT(Barrett, 1995)。

至於資訊安全方面的議題，未來的 MIME 電子郵件支援的 EDIINT 系統，在其他的機制和系統輔助下，如 S/MIME 和其 Certificate Handling (Dusse(1), 1998; Dusse(2), 1998)， PCKS#10 (Kaliski, 1998)等，可預期的是，其安全的發展空間更能夠具有可靠性，且容易被接受；而這些未來發展的議題，如 S/MIME EDI、Interactive EDI、S-HTTP EDI ， EDI Inter-operable Gateway 和 EDI-Public Key CA 等，對於企業採用此系統進行商務上的電子資料交換，在企業經營、提升競爭力方面將有莫大的助益。

在考諸電子商務的應用，目前，歐洲的汽車產業，如德國已藉由在 Automotive Supply Chain (ANX) (http://www.geis.com)上的 EDI 訊息傳送使得 B-2-B 的交易更爲迅速，同時汽車業的供應鏈反應也更爲及時，這股風氣同時也在塑膠業和鋼鐵業造成流行。而在美國的電信業如 Sprint 和 BellSouth 也將完成由 Bellcore 所主持的以 EDI 爲架構的 clearinghouse network; 而 Procter & Gamble (P&G)在 1999 年六月藉由 GE 所建立的資訊服務(GE Information Service, GEIS)

(http://www.geis.com)來達成全球的 EDI 供應鏈系統。然而，以上所提的產業及公司，仍以架構在 VAN 上爲主，所需費用相當昂貴，並未利用到網際網路的普及性來做 B-2-C 的服務。

而軟體的服務廠商，包括 IBM、Microsoft、SUN、HP 等，更是不遺餘力的在推動符合網際網路傳輸標準的各式軟體模組，譬如 IBM 的 Application Framework for E-Business，利用 Enterprise JavaBeans 和 Extensible Markup Language (http://www.software.ibm.com)發展系統，並且可和 ERP 等軟體組合，共同使用。然而這些軟體並非購買安裝後即可使用，仍須由 IBM 的配合廠商（有 certificate 的）爲公司量身定做所需的格式及功能，所需的時間及金錢是可想而知。

就目前台灣的 EDI 環境而言，大抵仍以 VAN 爲主，能夠做到以網際網路來做 EDI 資料傳輸的公司及行業，仍占相當少數；國人亦有發展以 Web 爲架構的 EDI 系統，由於剛推出，效能亦待考驗。國外最近也有以 XML 發展 EDI 系統的組織出現 (http://www.xmledi.com)，除了標準尚未完全統一外，當 EDI 字串轉換成 XML 格式時，其對頻寬的需求，可增加高達 50%以上，這昂貴的負擔，絕非網際網路的使用者所樂見的(http://www.commerce.net)。而本文系統除了考慮效率及成本外，對頻寬的需求量小，並使用現成可行的軟體支援，即可使 EDIINT 完成系統的整合，其便利性是不可忽視的。

捌、結論

即將進入以網際網路爲主要通訊幹道的二十一世紀，商務上的資訊交換，以傳統的紙上郵件、FAX、電話或者快遞傳送等方法，已經不能滿足對於資訊快速取得的要求；採用電子資料交換，在雙方或多方同意的標準下，進行結構化資料的交換與傳輸，使得內部和外部組織的運作能夠加速進行，毫無疑問的是步入二十一世紀不可避免的趨勢。而在採用電子資料交換系統時，爲了降低建置和維護 EDI 系統的成本，朝著開放標準、協定和傳輸模式的架構，採用網際網路電子資料交換（EDIINT），則可符合以上概念的要求。迅速及時的 B-2-B 與 B-2-C 的交流，將是電子商務發展最重要的需求。

而廣泛應用的多媒體、安控規格、PGP/MIME 等機制的引入，也是 EDIINT 整合上的重點，包含：利用 EDIFACT 具彈性的 Segment 嵌入商務多媒體和 EDI 訊息間的關係、以安控管理及安控回應訊息嵌入 EDI 安控、利用 PGP/MIME 之公開金鑰加密與數位簽署對封裝後的電子郵件進行資訊安全上的保護，皆是必須包含的關鍵技術。

本研究所提出之整合系統，經實際驗證後，符合容易建構整合的條件，並具有原先要求的「交換標準」與「通訊網路」皆能夠公開、標準化的特色，多媒體和資訊安全也

能夠予以支援。在這些特點下，跨平台移植與內部財務、會計系統整合的工作將可成爲全面的商業資訊自動化；從實際應用的角度而言，本研究所提出的系統模式擁有良好的架構基礎和互動性系統，將能給企業或組織實際應用上的參考。

表1 UNIX下的EDIINT測試環境說明

測試環境需求之元件	採用之元件及版本
作業環境	Sun Sparc 10 / SunOS 4.1.4
電子資料交換轉換程式（EDI Translator）	Writing in GNU gcc/g++ 2.7.2.1
電子資料交換公開標準和訊息型別	EDIFACT 97B / PAYEXT
電子資料交換安控管理標準	EDIFACT 94W / PAYEXT AUTACK
安控管理數位簽章演算法	MD5 / perl md5[1,24] & PGPv2(2.7.1)
安控管理公開金鑰加密演算法	RSA / lib_rsa-0.80[29]
支援 MIME 封裝之 Mail Agent	Mutt 0.91i / with HAVE_PGP2(2.7.1)

表2 MIME 封裝的 EDI 相關參考設定

(a) Configuration of MIME Types

application/x-zip-compressed	zip
application/x-edifact	**edifact**
application/x-edifact-ack	**edifact-ack**
audio/midi	mid midi
audio/x-wav	wav
image/gif	gif
image/jpeg	jpe jpeg jpg

(b)Metamail Capabilities

image/gif; xv %s
image/jpg; xv %s

application/x-edifact; edifact-decode %s
application/x-edifact-ack;
edifact_ack-decode %s

表 3 Microsoft Windows 95 下的 EDIINT 測試環境說明

測試環境需求之元件	採用之元件及版本
作業環境	OS: Microsoft Windows 95 OSR2 MAPI: Eudora Light 3.0.6 MAPI Server PGP Key Server: http://keys.pgp.com:11371/
電子資料交換轉換程式	Microsoft Visual C++ 5.0 & MAPI SDK
電子資料交換公開標準和訊息型別	EDIFACT 98B / PAYEXT
電子資料交換安控管理標準	CONTRL / AUTACK
安控管理數位簽章 Digest 演算法	MD4 SDK Library
安控管理數位簽章 Sign 演算法	RSA / lib_rsa-0.80[29]
支援 MIME, PGP/MIME 封裝之 Mail Agent	Eudora Light 3.0.6 with PGP freeware 6.0.2i Plug-In

參考文獻

1. Allen, J. “MD5 in 8 lines of perl5,” available at http://www.physics.adelaide.edu.au/~swright/crypto/rsa/md5.html.
2. ANSI ASC X.12 Work Group. “ANSI ASC X.12,” available on http://www.disa.org/.
3. Barrett, A. P. “Interactive EDI – IT and Commerce in the 21st Century,” *IEEE Telecommunications*, Mar. 1995. pp. 164-169.
4. Crocker, D. H. “Standard for ARPA Internet Text Messages,” RFC822, 1982.
5. Crocker, D. H. “MIME Encapsulation of EDI Objects”, RFC 1767, Mar. 1995.
6. Drummond, R. “Signed, Sealed & Delivered: CommerceNet Test Results,” *IEEE Network Computing*, Sep. 1997. pp. 88-96.
7. Dusse, S., Hoffman, P., Ramsdell, B., Lundblade, L., and Repka, L. (1). “S/MIME Version 2 Message Specification,” RFC 2311, Mar. 1998.
8. Dusse, S., Hoffman, P., Ramsdell, B., and Weinstein, J. (2). “S/MIME Version 2 Certificate Handling,” RFC 2312, Mar. 1998.
9. Elkins, M. “MIME Security with Pretty Good Privacy (PGP),” RFC 2015, Oct. 1996.
10. Freed, N., and Borenstein, N. (1). “(MIME) Part One: Format of Internet Message Bodies,” RFC 2045, Nov. 1996.
11. Freed, N., and Borenstein, N.(2). “MIME Part Two: Media Types,” RFC 2046, Nov. 1996.
12. Fielding, R., Gettys, J., Mogul, J., Frystyk, H., and Berners-Lee, T. “Hypertext Transfer Protocol -- HTTP/1.1,” RFC 2068, Jan. 1997.
13. III(1), Institute for Information Industry. “Frequently Asked Questions about Electronic Business,” Institute for Information Industry Taiwan, 1998.
14. III(2), Institute for Information Industry. “QR/ECR Technical Handbook,” Institute for Information Industry Taiwan, 1998.
15. Kaliski, B. “PKCS 10: Certification Request Syntax Version 1-5,” RFC 2314, Mar. 1998.
16. Kantor, B., and Lapsley, P. “Network News Transfer Protocol,” RFC 977, Feb. 1986.
17. Kilpatric. “Standards and Electronic Commerce,” *The E-Commerce Handbook 1996*, NCC BlackWell, 1996, pp. 89-94.
18. Kimberley, P. *Electronic Data Interchange*, McGraw-Hill, 1991. pp. 5-16, 19-31.

19. Moore, K. “MIME Part Three: Message Header Extensions for Non-ASCII,” RFC 2047, Nov. 1996.
20. Oikarinen, J., and Reed, D. “Internet Relay Chat Protocol,” RFC 1459, May 1993.
21. Pageant Ltd. *The Electronic Commerce Handbook*, NCC BlackWell, 1996, pp. 41-44.
22. Postel, J. “SMTP - Simple Mail Transfer Protocol,” RFC 821, Aug. 1982.
23. Postel, J., and Reynolds, J.K. “File Transfer Protocol,” RFC 959, Oct. 1985.
24. Rivest, K. “The MD5 Message-Digest Algorithm,” RFC 1321, Apr 1992.
25. Shih, C. Jansson, M., and Drummond, R.(1). “MIME-Based Secure EDI,” draft-ietf-ediint-as1-08, May 1998.
26. Shih, C., Jansson, M., and Drummond, R. “Requirements for Inter-Operable Internet EDI,” draft-ietf-ediint-req-05, Jul. 1997.
27. Shih, C., Moberg, D., and Drummond, R.(2). “HTTP Transport for Secure EDI,” draft-ietf-ediint-as2-02, Sep. 1998.
28. Sokol, P.K. *From EDI to Electronic Commerce*, McGraw-Hill, 1994. pp. 2-11, 13-49, 212-227.
29. Tsai, M.G. “Librsa Version 0.80,” M. G. Tsai, 1996.
30. UN/ECE TRADE/WP.4, “UN/EDIFACT Syntax, Part6, Secure authentication and acknowledgement message (message type-AUTACK),” ISO 9735-6, R1246, Mar. 1998.
31. UN/EDIFACT Work Group. “UN/EDIFACT D97B,” available at http://www.unece.org/trade/untdid/.
32. Veijalainen, J. “Issues in Open EDI,” *IEEE Telecommunications*, 1992, pp. 401-412.

作者簡介

蔡銘箴
國立台灣大學電機工程學系畢業，美國加州大學柏克萊分校工業工程與作業研究碩士，美國加州大學洛杉磯分校電機工程博士。
曾任職於美國線上(AOL，America Online Inc.)爲資深研發工程師，目前任職於國立交通大學，資訊管理研究所；研究興趣包含商務多媒體系統與應用，網際電子商務與通訊，數位影像浮水印，網路資訊整合系統及管理等。

吳泰宏
國立交通大學資訊管理碩士，目前於資訊工業策進會選服國防役；研究興趣爲電子商務、電子資料交換、商務多媒體與資訊管理。