八十八年度行政院國家科學委員會專題研究計畫成果報告

以 MIME 封裝爲基礎的商業網際網路電子資料交換之實作研究

The implementation of business Internet EDI with MIME Encapsulation

計畫編號：NSC 88-2416-H-009-022-
執行期限：87 年 8 月 1 日至 88 年 7 月 31 日

主持人：陳瑞順　　國立交通大學資訊管理研究所

一、中英文摘要

中文摘要

電子資料交換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的目的則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，進行資料間換與傳輸。

本計畫為網際網路電子資料交換在商業的實作及應用：目前網際網路正蓬勃發展中，所有網際網路所提供的服務（如：mail, ftp 等）所需的成本皆不高。在瞭解到將 EDI 封裝在 MIME 的可行性之後，利用 Internet 的低成本優點，將此封裝在 MIME 中的商業 EDI 資料藉由 Internet mail 的服務來達到交換的目的。

本計畫著重於商業 EDI 資料交換。由於商業的資料皆屬於高度安全性，故我們的實作及應用也將資料安全列入研究的範圍。我們也討論認證系統、密碼方法，使我們的成果具有高度可信賴性，俾成為商業界普遍應用的標準、降低資料傳輸成本、提高資料傳輸率。

本計畫在探討商業 EDI 資料交換的特性及 MIME 的規格與不同商業應用的方法後，設計一應用程式使其可達到將商業 EDI 封裝的 MIME 的 mail 收送及 EDI 編碼解碼功能外，也包含了網路安全的密碼方法及用戶端認證的項目。

本計畫擬應用本人前一個計畫之成果（以 MIME 封裝為基礎之 Internet EDI），所得之傳輸模式直接應用到商業界，實際程式製作、所得成果可提供給國內其他產業以 MIME 封裝下在 Internet EDI 上實作參考。

關鍵詞：MIME、電子資料交換、網際網路、網路安全、商業。

Abstract

EDI is defined as the corresponding standard of both multi-communities, which is used as the transferring protocol of the structured information through the electronic communication channels. However, the purpose of the Internet EDI emphasizes at the integration of many existing Internet transferring schemes and offers an open exchanging standard for the data interchange and communication.

The goal of this project is to develop the business reference key point over Internet EDI standard of industry. This project is to study the standard and the consideration of security over MIME based encapsulation of business EDI object.

Most research of EDI focus on general principle, but there is rare discussion to standard of MIME encapsulation of business EDI object. So in this topic, we have more research and implementation to the usage of integral standard on business industry.

We study the transmission characteristic of business EDI object. After analyzing the result of MIME and different commerce, we implement the MIME encapsulation on business EDI object and EDI encoding and

decoding functions. The security of Internet EDI is also considered.

We use last project results to implement the transmission model of business Internet EDI with MIME-based in this project, and results can support the other industry implementation reference.

Keywords: MIME, EDI, Internet, Commerce.

二、計畫緣由與目的

緣由 – 電子資料交換（EDI）是一種提供在商業雙方來定義交易架構訊息的工具，傳統用紙張來傳遞的資料信件所用的是郵政系統，但在電子資料交易的傳遞方式自然是用電子郵件。傳統EDI 只有在 text 的環境下，而商務多媒體的應用，其重要性將會與日遽增，同時，以指紋或視網膜紋路為身份認證的辨識資訊有可能成為網際網路電子資料交換中的必須元件，因此商業電子資料若包括語音、影像、圖形…等多媒體資料，我們就必須將這電子資料經由MIME 規格所制訂的特殊格式裡來傳遞。為了這規格的實現，我們需要建立一個使用 MIME 封裝為基礎的商業網際網路電子資料的基本格式。

資訊網路的網網相連，使資訊普及變為快速、方便、簡單。世界各角落的資訊可以透過 Internet 而整合在一起。資訊的互相傳遞需仰賴於標準的電子資料交換（Electronic Data Integration, EDI）。在標準化 EDI 架構運作之下，記錄才能在網路中正確的傳遞與使用。

而在一般的企業中，EDI 往往被視為企業再造，製造競爭力優勢的關鍵；不過，隨著電子商務時代的來臨，EDI 慢慢地從優勢關鍵變成為必要的元件、不可抗拒的趨勢。相較於加值網路，Internet Mail 的系統，在普及性、開放性和使用的便利性，都普遍優於封閉性的加值網路；而且，由於資訊安全的技術不斷的進步，密碼方法用於網際網路傳輸上的加解密已更為可靠，利用開放式的網際網路來達成 EDI 的實作應用，相信會比在建構成本高昂、擴充不易的加值網路上有更多的好處。

目的 – 在 EDIFACT 中，針對各種行業定義了 152 種 message type，包含了商業所需之 invoice message、extended payment order message、purchase order message…等。而本計畫主要是針對商業這方面的問題。探討商業 EDI 及 MIME 封裝之標準，尋求及制訂一個適合商業專用的標準，並以這種標準發展出一套應用程式，利用 Internet mail 現成的資源，來傳遞商業 EDI 的資料，使商業 EDI 的成本降低。而就使用者而言，只需簡單的操作就可以達到電子資料的交換並包含資料在網路傳輸上的安全性。

由於 MIME 是一種多功能的 Internet 電子郵件格式，只要將 Extension Set 擴充，而不會影響原來的運作，所以是一種可以將原本 MIME 功能保存，又增加 MIME 附加價值的方法。而利用商業 Internet 電子郵件傳輸的方便，使其大大地降低 EDI 的成本。

商業 EDI 結合在 MIME 的環境部分，利用本人前一個相關計畫之結果，利用其傳輸模式直接在商業實作出結果，以供其他產業實作應用參考。並期望此 Internet EDI 研究，對於創造台灣企業競爭優勢和電子商務普及化，有一定程度之貢獻。

三、本研究中以 **MIME** 封裝的商業 **Internet EDI** 物件

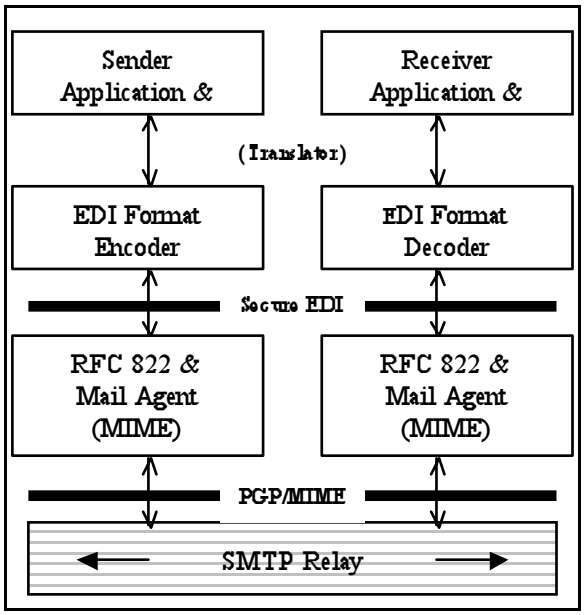
根據本人前一個相關計畫的成果，本計畫所應用 EDI 系統基本的架構，可簡單分為相對稱的兩端，一端為 EDI 訊息的發送者，另一端為接收者；而本計畫除了傳送 EDI 訊息之外，還考慮到使用 MIME 來封裝訊息之本身，所以會有 MIME 封裝之部分。而本計畫之重點，也就是商業 Internet EDI，利用技術成熟穩定、普遍、簡易可靠之 SMTP 郵件技術來傳送 EDI 之訊息。而進行 MIME 封裝的工作，便交給 Mail Agent。

此外，考慮到資訊安全的問題，我們

在 EDI 和 MIME 的層級之下，分別加上 Secure EDI 和 PGP/MIME 的加密與簽章兩層安全保護，此 EDI 訊息的安全性已大為提高。圖一便是整體層級架構之說明。

接下來我們分成幾個層級來個別說明，包括收發端、EDI Translator（Secure EDI）、Mail Agent（PGP/MIME）、SMTP：

收發端：此部分是使用者原先的資料，包含訂單、發票、收據、轉帳、貨品說明等等所有可能的商業訊息。商業 EDI 是以商業人員為主的工作，且最主要的目



圖一：整體層級架構說明

的是使用方便，在此部分的資料、格式等，都是在收發端使用者本業的領域所熟悉而瞭解的資料格式；在傳統的過程中，可能必須透過郵政系統，將這些資料格式寄于交易伙伴。而在本計畫之架構系統中，原先的操作人員只需將資料輸入到我們根據其要求設計好的應用程式資料格式中，再利用應用程式以 Internet mail 方式送出即可，無須再做其他操作。

EDI Translator：此層級便是 EDI 訊息產生處。從操作者輸入的資料中得到所欲傳送訊息，對映（Mapping）或轉承（Translating）到 EDI 的格式上，統一由 EDI 的標準來傳送。而 Translator 負責的工作，便是把操作者輸入的資料中得到所欲傳送的原始資料，編碼（Encode）成 EDI 之標準格式，接著送到下一層給 Mail Agent（MIME）來封裝；相對的，接收端從 Mail Agent 收到 EDI 之標準格式所表現的資料時，Translator 同樣將其解碼（Decode）成使用者端原先之資料格式（如上所述之發票、訂單等等）。另外，在此部分，本研究另行加入 Secure EDI 的安全機制於 EDI 標準格式中，確保 EDI 訊息傳送之安全性，做到安全控管的掌握。

Mail Agent：這個層級便是本研究之架構中，負責收發 EDI 訊息的部分。建構有 MIME 封裝功能和可定時取得訊息的 Mail Agent。負責的工作是，把 EDI Translator 層級傳送過來的 EDI 標準格式，經過 MIME 的 header 封裝，並且加上必要的安全機制（PGP/MIME），接著送信給下一層的 SMTP Relay。而接收端的工作則是收到 Mail 之後，先解讀 MIME header，並加以解封裝，接著呼叫上層的 EDI Translator，傳送解封裝之 EDI 標準格式資料給上層，做解碼的工作。

SMTP Relay：此層級負責傳送信件，將發送端 Mail Agent 所寄過來之 MIME 封裝的 EDI 物件，傳送到接收端之 Mail 帳號，而接收端之 Mail Agent 則透過此取回郵件之物件。

前述的收發端過程，便是此系統架構之簡單作業流程。原則上，本計畫所發展的架構，是兩邊對稱的，並無明顯發送端、接收端之區別。而主要強調的 EDI Translator 和 MIME Mail Agent 部分，更是收發端採用同樣的系統。

四、本研究採行之機制及實作過程簡介

本計畫由於要實現商業 Internet EDI 以及 MIME 的封裝，故需考慮到格式、協定、機制等的公開性和標準性。茲分為下面幾點來討論：EDI、Secure EDI、MIME。

EDI：鑑於標準、開放性質的考量，EDI 在此方面的選擇有兩種：ANSI X.12 及

UN/EDIFACT。根據本人前一個相關的計畫，本計畫在此同樣選擇使用 UN/EDIFACT 來作為研究之標準，主要是因為此標準為聯合國和 ISO 認定，以及國內多數機構皆採用此標準。版本為 UN/EDIFACT D97.B。

MIME：MIME 的規格於 RFC 1521, 2047, 2048 等已有詳細的協定建立，而且廣泛的使用於各種的 Mail Agent 上，故此部分的選擇考量不會太麻煩。而在層級和層級之間的傳遞，需在 Application 上進行型態的新增如，Application/edifact 等。版本為 MIME V1.0。其中的編碼機制則採用 base64 的方法來進行編碼和解碼。

Secure EDI：此部分採用 UN/EDIFACT D94.W 中的安控規格，並佐以金融資訊服務中心之安控管理建置草案，所簡化之標準。另外，採用 RSA 演算法，為安控管理之密法方法。

Secure MIME：參考 RFC 1521。

實作的過程，於 Win95 的個人電腦上，進行 UN/EDIFACT Translator 和 MIME Mail Agent 的系統建構，採用 Borland C++ Builder 3.0 為編譯器。而 Mail Agent 部分，則是利用 BCB 的 Mail Agent 相關元件為基礎架構。

之後，將此兩部分進行整合，形成此層級架構之核心部分。而採行的 EDI 系統領域則是屬於 D97.B 中規定的金融轉帳的 PAYMENT Extension 部分。而在此應用程式中，除可收發 EDI 的多媒體郵件外，亦可當作收發一般郵件的工具，操作方式和環境和市面上廣為使用的收發電子郵件軟體 Netscape Navigator 系列相近，因此操作者較不會有使用上的問題。

五、結果與討論

實作結果能夠在 Win95 環境底下進行 EDI 訊息的傳送工作。經過評估，若 SMTP 之伺服器維持穩定，則本層級架構的可靠度會大為增加。而 Secure EDI 和 PGP/MIME 的引進，使得 EDI 的安全控管得以實現，由各種網路監聽封包的軟體上，都無法明確的竊取信件內容，顯然的 EDI 訊息便得以保障。

而 MIME Mail Agent 的傳輸多媒體功能，經過 mime types 和 mailcap 的定義後，經由在 Win95 下的應用程式呼叫，如 image/jpeg 可由 ACDSee 程式來進行觀看、video/mpeg 可呼叫 Xing 程式等等，可以達成多媒體展示的效果，對於目前需要多媒體化的電子商務潮流，有相當大程度的幫助。

六、計畫成果自評

本計畫的成果符合原先的基本目標，能夠提供簡易的使用、低成本的安裝、安全的環境、具有效率的傳輸之電子資料交換環境；且環境除可以在本人前一個相關計畫中的 UNIX 平台上外，於本計畫中已可擴展到目前廣為大眾所使用的 Windows 系統上，對於操作者的使用及安裝上的成本都更為優異。

在 EDI 格式標準方面，仍有部分的爭議和作法上的認定問題，如金資中心的 EDI 安控規格等等；此部分本研究的作法是先行訂定有爭議的 EDI 安控內容，待此方面的疑慮解決後或有公開標準出現後，再予以嵌入本層級架構中。

七、未來展望

本計畫經過將近一年的研究，研究人員對於文獻的研讀、收集，以及團隊合作、管理協調等都有長足訓練和幫助。此外，對於本計畫尚未趨於完整部分有以下之展望：

- 各種平台之系統實現：可考慮將此系統搬上 World Wide Web，並可採用 Java 等各平台適用語言撰寫。
- 完整資訊安全的整合：完整考慮資訊安全，整合 Secure EDI 和 PGP/MIME 以充分滿足真確性、私密性、身份確認、不可否認性等。
- 對於 SMTP/POP3 伺服器的研究，使本層級架構更具有穩定性。

八、參考文獻

[1] UN/EDIFACT – D97B，1997。

[2] Electronic Commerce – A Manager's Guide，Ravi Kalakota、Andrew B. Whinston，1997。

[3] RFC 1767，MIME Encapsulation of EDI object

[4] RFC 1865，EDI Meets the Internet Frequently Asked Questions about EDI on the Internet

[5] RFC 822，Standard for the format of ARPA Internet message

[6] RFC 2045，MIME Format of Internet Messages Bodies

[7] RFC 2046，MIME Media Type

[8] RFC 2047，MIME Message Header Extension for Non-ASCII Text

[9] EDI Mapping Overview，財團法資訊工業策進會，1992。

[10] 金融 EDI 安控作業規格指引第一版，金融資訊服務中心，1995。

[11] EDI 數位簽章的安全管理 – 密碼金鑰的管理，吳國禎、黃景彰，1996。