

## 第三章 研究方法

本研究探討製作數位教材之模式，以「資訊安全概念」為教材主題，發展數位教材。本教材用於某公務機構員工資訊安全教育概念訓練，學習過程由系統紀錄，訓練結束後以問卷方式收集學習者對於該數位教材之意見。透過分析閱讀及測驗的學習歷程以及員工所填之問卷內容，探討數位教材訓練成效。本章就研究對象、研究歷程、及研究工具依序作說明。

### 第一節 研究對象

本研究以某公務機構95位員工為研究對象，這些員工均配置一部個人電腦，平日工作需使用文書處理軟體。該機構計有26個應用系統，員工透過intranet網站為入口，並依業務權責設定應用系統使用權限。員工透過電子表單線上簽核方式處理差假，故均熟悉IE瀏覽器的操作，具備基本的資訊操作能力。該機構以outlook Express 收發電子郵件，員工習慣以電子郵件進行資訊交換。本研究所完成之資訊安全概念訓練數位教材，即透過電子郵件方式告知本課程之網址，通知員工上網學習。該機構已建置 ISMS(資訊安全管理系統)，每半年辦理一次資訊安全內部稽核工作，以加強員工資訊安全概念。

### 第二節 研究歷程

本研究的研究歷程如圖3.1所示，分為五個階段：確定研究主題、收集及整理素材、教材設計及發展、架設網站及發佈教材進行訓練等。分別說明如後。

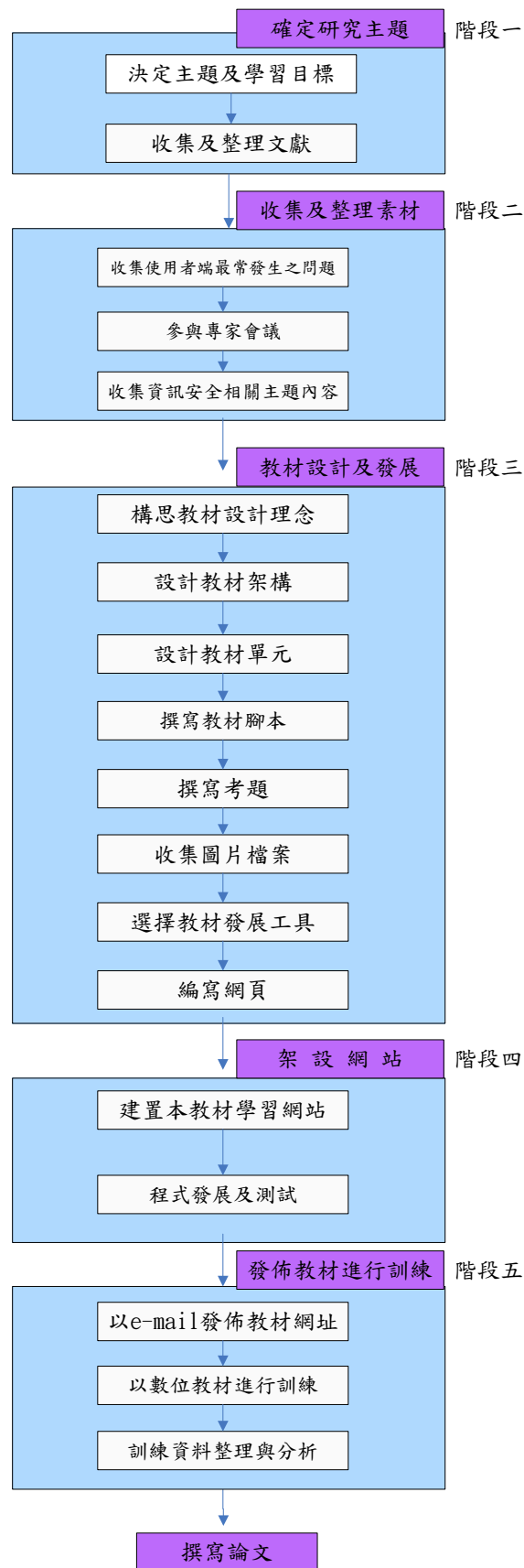


圖 3.1 研究歷程

## 一、確定研究主題

政府大力推動建立資訊安全管理系統，以確保組織資訊的安全，避免資訊遭到破壞，故對於資訊安全相關運用技術及觀念推廣不遺餘力。組織內部可藉由數位教材傳播之快速及方便性，提供員工方便、彈性的學習管道。本研究著力於短時間內發展適合員工資訊安全訓練之數位教材，故第一階段工作著重於「決定教材主題及學習目標」、「收集及整理文獻」兩項工作。

### (一)、決定教材主題及學習目標

以「資訊安全概念訓練」作為主題，訂定主題之學習目標如下：

- 1.列出資訊安全威脅的種類
- 2.指出維護資訊安全的方法
- 3.學會基本安全防技巧
- 4.學會常用的電腦操作

### (二)、收集及整理文獻

由研讀文獻瞭解資訊安全管理相關規範，並探討數位教材製作原則及成人學習特性，俾依文獻資料發展本研究之數位教材。

## 二、收集及整理素材

### (一)、收集使用者端最常發生之問題

本研究對象所處之公務單位由兩位工程師，協助員工解決電腦之操作障

礙，工程師可透過電話或親自至使用者所在，協助處理問題。因長期接觸組織內部員工，故對於員工之操作習慣及問題多能掌握，服務人員完成服務工作後，需填寫工作紀錄單，描述員工請求協助之問題及工程師處理問題結果。研究者利用2天時間，分析1,265件工作紀錄單，了解員工使用電腦常見問題，內容如表3.1所示：包括「電腦中毒」、「電子郵件異常」、「使用者登入帳號／密碼問題」、「印表機故障」、「硬體故障」、「作業系統異常」、「應用系統操作障礙」、「Office軟體操作」及「其他問題諮詢」等九大項目。

**表 3.1 電腦故障排除統計**

員工使用電腦常見問題	件數
電腦中毒	37
電子郵件異常	163
使用者登入帳號／密碼問題	58
印表機故障	281
硬體故障	153
作業系統異常	28
應用系統操作障礙	95
Office 軟體操作	78
其他問題諮詢	372

排除硬體及印表機故障之問題，經彙整其他常見問題及發生原因如

下：

1.電腦中毒中問題：

由於電子郵件的方便性，故電子郵件已成為員工工作上傳遞資料的主要工具，但方便性也成電腦病毒傳播的重要途徑。員工對於電子郵件的附件檔案缺乏警覺性，一旦開啟夾帶病毒的郵件附件檔，即導致電腦中毒。部分員工使用電子郵件的習慣往往將Outlook Express郵件預覽功能設定為「開啟」狀態，一旦電子郵件夾帶電腦病毒，則電腦立即受到病毒感染。此外，瀏覽網站，下載來源不明之檔案，也是導致電腦中毒的原因之一。

## 2. 電子郵件異常：

研究對象所服務之機構採用Exchange Server作為電子郵件主機，使用者端則以Outlook Express收發電子郵件。新進及部分員工不熟悉Outlook Express之使用設定，無法正確設定電子郵件主機名稱、使用者帳號、密碼等資料；尤其更換密碼後，電子郵件之密碼未同步更改設定，故需請求服務人員協助排除障礙。

## 3. 使用者登入帳號／密碼問題：

員工服務之機構透過「帳號稽核原則」強制網域內的使用者帳號之密碼的最長使用期限為三個月，故使用期限到期，即強迫進行密碼變更，且密碼需符合含有英文大小寫、特殊符號、長度8位以上之複雜性原則。部分員工對於該項措施頗感困擾，通常會請求服務人員或同事協助變更密碼，並將新舊密碼告知對方。部分員工因為無法記住8碼以上具複雜性原則之密碼，故將密碼貼在電腦螢幕前。另外，時常忘記密碼之員工亦不在少數。

#### 4.其他問題諮詢：

部分員工派駐國外服務後，常諮詢如何解決電腦中毒問題。此外，有關「取得電腦使用帳號之程序」、「身份識別之權責」、「網站封鎖」、「啟動電腦螢幕保護程式」、「安裝免費軟體」等，為員工經常諮詢的問題。

#### (二)、參與專家會議

使用本教材之公務機構已建置ISMS(資訊安全管理系統)，並有2位人員取得BS7799「資訊安全主導稽核員」認證資格。研究者歸納員工常發生之使用電腦相關問題，並決定如表3.2所列之教材範圍，包括「使用電子郵件」等8項訓練主題，透過會議方式與「資訊安全主導稽核員」討論教材範圍之可行性。經專家建議：「Outlook Express郵件規則之操作設定」易造成誤用，導致漏收重要電子郵件。「弱點補強程序」包括主機之弱點及client機器之弱點，建議將教材內容界定在與員工有直接關係之作業系統弱點補強範圍(表3.3)。此外，建議增加表3.4所示：「網際網路安全問題」及「資訊安全政策」兩個範圍。本項工作共進行兩次討論，每次會議時間為一小時。

表 3.2 資訊安全概念教材範圍

教材範圍	理由	採納作為資訊安全概念訓練教材	
		是	否
使用電子郵件	<ol style="list-style-type: none"> <li>1. 因常透過電子郵件進行業務溝通，而資訊安全問題常因電子郵件夾帶之附件檔案而引發，故需納作訓練教材。</li> <li>2. 廣告電子郵件經常夾帶惡意程式</li> </ol>	V	
郵件規則之操作設定	介紹 Outlook Express 之「郵件規則」，以過濾郵件。		V
密碼複雜性原則及密碼變更	組織之資訊安全政策對於密碼長度及使用期限已作明確規範，故需對員工宣導，並提供變更密碼基本操作訓練。	V	
防毒軟體及病毒碼更新	<ol style="list-style-type: none"> <li>1. 員工有機會派駐國外服務，駐外工作人力有限，且無資訊人力協助處理基本電腦防護問題，故提供防毒軟體相關使用概念，防範基本資安問題。</li> <li>2. 防毒軟體為重要之資安防護工具，應澄清該工具之功能。</li> </ol>	V	
電腦病毒	電腦中毒為常見之事件，應介紹病毒及電腦中毒之原因。	V	
尊重軟體智慧財產	員工習慣自網路上下載不明軟體安裝，容易導致電腦中毒及被植入後門程式。此	V	

	外，建立軟體有價之觀，尊重智慧財產亦為宣導重點。		
安全意識 防範中毒的技巧	資訊安全強調預防重於治療，應介紹簡單的防範中毒技巧及「良好的使用習慣」之重要性	V	
弱點補強程序	補強電腦之弱點		V

表 3.3 修正之教材主題

教材範圍	理由	意見
郵件規則之操作設定	容易誤用，可能造成漏收重要郵件。建議增加「如何避免收到垃圾郵件」之教材。	修正
弱點補強程序	僅介紹安裝 client 端作業系統修正程式之相關內容	修正



表 3.4 增加之教材範圍

教材範圍	理由
網際網路安全問題	1. 以木馬程式、網路釣魚及社交工程為主題，以提高資訊安全防護概念為學習目的。 2. 外部安全威脅及內部脆弱點之介紹
安全防護及資訊安全政策	1. 資訊安全政策為執行資安的首要步驟，讓組織內員工了解資安政策，進而要求守遵守政策。 2. 安全防護網包括：管理階層支持、訂定資訊安全政策、辦理教育訓練。
防火牆功能介紹	導正員工對於防火牆功能之錯誤觀念，排除過分倚賴科技產品之心態；惟需以簡單易懂之方式介紹該主題，避免使用過分技術性的術語。

### (三)、收集資訊安全相關主題內容

政府為加強推動各主管機關及重要資訊單位建立資通安全稽核制度及落實增進行資通安全內部稽核工作，故辦理「政府機關資通安全稽核作業研討會」及「加強電腦使用安全實作」等資通安全議題研討會。研究者多次參加政府舉辦之研討會，經收集相關資料，並列出與員工相關之資訊安全問題如下：

- 1、忽略帳號密碼的重要性。
- 2、使用同一套密碼。
- 3、缺乏對木馬程式之認識。

4、過分依賴資訊科技作為資訊安全防範工具。

員工缺乏資訊安全概念，為資訊安全防護之最大弱點，故教材範圍必需著重

上述問題之描述，提供正確之資安防護概念。

### 三、教材設計理念及架構

#### (一)、構思教材設計理念

##### 1.以工作及生活上之題材為導向

網路的興盛，帶動使用風潮，政府及民間組織的資訊化作業程度也逐日提高，透過資訊作業處理之結果，已成為組織重要的資產。多數的員工雖然使用電腦及網路資源達成指定任務，但許多員工尚未具備正確的資訊安全概念，也感受不到資訊安全和己身之關係，故無法參與資訊安全防護工作。為了喚起員工重視網路世界的問題，故構思以「工作及生活上可能碰到之資訊安全問題」作為教材設計理念之一，讓教材內容與真實世界作銜接。(表3.5)

表 3.5 生活化及工作上資訊安全題材。

類別	題材
生活	身分證件、信用卡資料、金融卡資料、帳單資料資訊被冒用或竊取。
生活	網路釣魚詐騙案例。
生活	有趣的遊戲、螢幕保護程式、動畫影片可能夾帶木馬程式及病毒。
生活	翻版 CD 也可能夾帶電腦病毒程式。
生活	海棠颱風期郵局 ATM 當機
工作	所分享的檔案含病毒。
工作	洩露公文及機密資料。 個人電腦硬碟的資訊被竊。 實體安全之需求：門禁管制。
工作	無意的情況下破壞資訊之案例。
工作	富邦證券因交易員輸入錯誤委託指令，導致錯帳金額達新臺幣 77 億元之案例。
工作	電腦中毒主要途徑：軟體分享及電子郵件的附加檔案。 下載的不明軟體安裝至電腦也可能是電腦中毒的途徑。
工作	外交部受駭客入侵透過木馬程式，取得機密檔案。
生活及 工作	經常收到垃圾郵件。

## 2. 導正錯誤觀念

教材應具有改造經驗的功能，本教材設計理念之一，以導正員工對於資

訊安全防護的錯誤觀念為目的。員工大多認為組織已購置防火牆、防毒軟體等軟硬體科技設備，故資訊安全問題不存在於組織內部；甚至認為資訊安全議題不涉及一般員工，而是資訊單位需處理的問題。在處理諸多員工電腦中毒事件時，經常受到的質疑問題即為：「不是裝了防毒軟體了嗎？為何還會中毒」。需導正之錯觀念如下：

- (1). 郵件主機具掃毒功能，故工作環境內的電腦應該不會中毒。
- (2). 個人電腦安裝防毒軟體即不會中毒。
- (3). 推動資訊安全作業，僅需要買許多的電腦硬體主機及相關軟體。
- (4). 防火牆可以防止病毒。
- (5). 因公務需求可以安裝免費軟體。
- (6). 開啟電子郵件預覽功能，可提高閱覽郵件之方便性。
- (7). 防毒軟體和防火牆能確保資訊安全。
- (8). 發現電腦中毒之處理程序。
- (9). 員工的身份識別與密碼鑑別由資訊單位執行。
- (10). 資訊安全業務是資訊單位的事。

### **3· 解決常見的問題**

資訊安全防護涉及組織內所有成員，除了需運用資訊安全防護工具之外，員工需建立資訊安全概念，防止資訊安全漏洞。電腦是工作上用來處理資訊的工具之一，常見的電腦操作問題一直存在組織內，這些問題間接造成

資訊安全防範漏洞，例如不熟密碼變更程序而委由他人協助變更密碼，造成密碼透明化。又例如不熟悉電子郵件使用設定，而委由他人代為設定，亦造成密碼透明化。為了配合密碼的複雜性原則，密碼之長度不得小於8碼，而許多員工常忘記密碼或將密碼貼在電腦螢幕前。教材之設計理念之一，希望能協助員工學會取用好用又好記的密碼，並且提供密碼變更及電子郵件使設定之操作模擬，協助員工解決常見之操作問題，長期目標則是落實資訊安全概念。此外，員工對於螢幕淨空、設定螢幕保護程式、定期修補軟體漏洞等作業大多不重視。教材內亦介紹使用電腦應具備之良好習慣。

## (二)、設計教材架構

本研究所規劃之教材架構係依研究者所訂之教材範圍、相關研討會資料，及研究對象所服務之機構所訂之「資訊安全政策」、「系統帳號密碼設定及管理要點」、「人員安全管理作業說明書」、「電子郵件管理作業說明書」等文件。教材含蓋「資訊安全威脅」、「維護資訊安全」、「基本安全防護技巧」、及「常用電腦操作」等主要主題。教材架構如表3.6所示。

表 3.6 教材架構

名稱	參考依據
資訊安全威脅	1. 本研究所定義之「資訊安全概念教材範圍」 2. 資訊安全相關議題研討會資料
維護資訊安全	1. 「資訊安全政策」 2. 「人員安全管理作業說明書」
基本安全防護技巧	1. 「系統帳號密碼設定及管理要點」 3. 資訊安全相關議題研討會資料 4. 「人員安全管理作業說明書」
常用電腦操作	1. 本研究所定義之「資訊安全概念教材範圍」 2. 「電子郵件管理作業說明書」

### (三)、設計教材單元

教材單元為最小之學習單位，其依循教學設計理念、教材架構而設計，單元架構如圖3.2所示。各單元內容，依「資訊安全威脅」、「維護資訊安全」、「基本安全防護技巧」、「常用電腦操作」4個主題分別發展，每一個主題架構細分多個單元。各主題所對應之單元，如表3.7至3.10所示。為了讓學習者認識各單元內容之教學目的，故需列出教學目標。

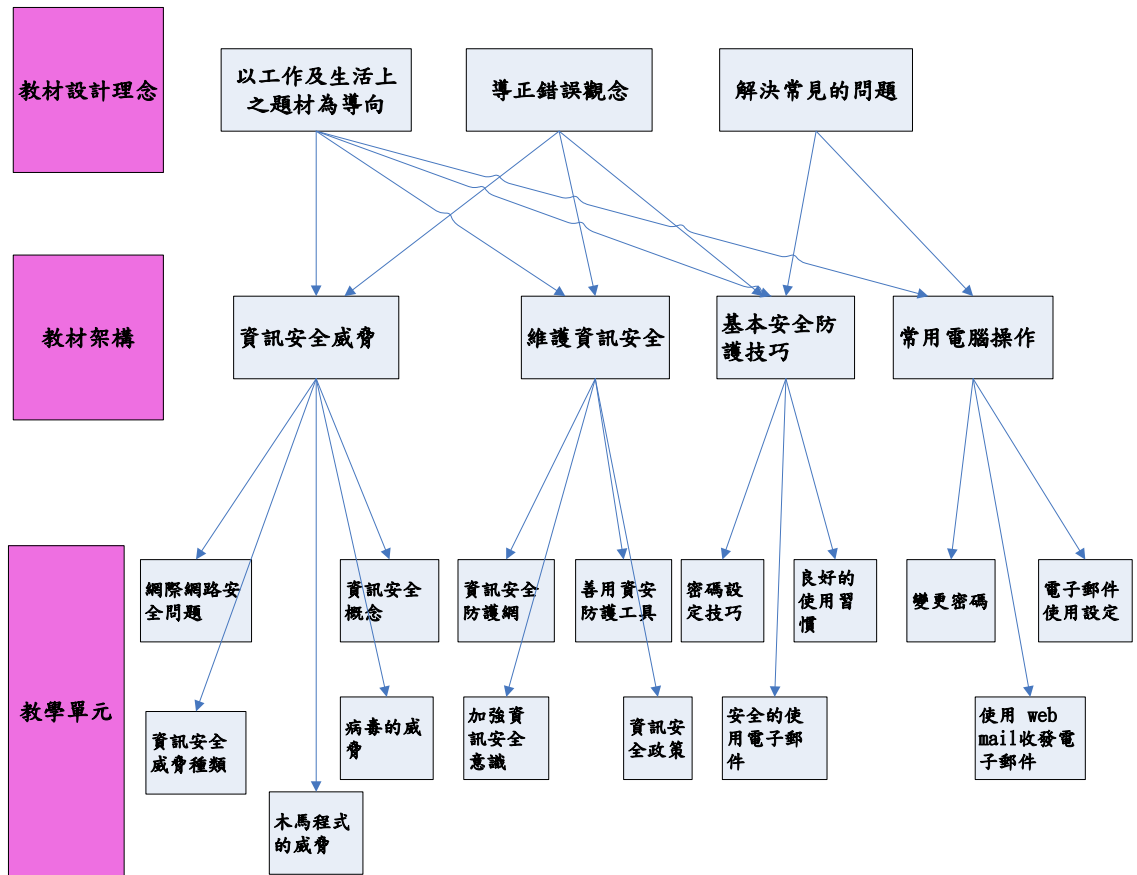


圖 3.2 學習單元架構

表 3.7 「資訊安全威脅」主題

單元名稱	教學目標
<p>第一單元 網際網路安全問題</p>	<ol style="list-style-type: none"> <li>1. 指出網際網路安全問題</li> <li>2. 描述資訊安全威脅來源</li> <li>3. 簡述防毒軟體與防火牆</li> </ol>
<p>第二單元 資訊安全概念</p>	<ol style="list-style-type: none"> <li>1. 指出「資訊」的內容</li> <li>2. 分辨「生活上的資訊安全」及「辦公環境的資訊安全」</li> <li>3. 闡釋「資訊安全的最高原則」導正「資訊安事件係指駭客的入侵」之觀念。組織內部人員有意或無意的破壞資訊，亦為資安事件。</li> </ol>
<p>第三單元 資訊安全威脅種類</p>	<ol style="list-style-type: none"> <li>1. 辨別資訊安全威脅的內容。</li> <li>2. 闡釋威脅與脆弱之關係。</li> </ol>
<p>第四單元 病毒的威脅</p>	<ol style="list-style-type: none"> <li>1. 分辨病毒及病毒碼</li> <li>2. 指出病毒對電腦的影響</li> <li>3. 列出電腦中毒的症狀</li> <li>4. 學會處理電腦中毒的狀況</li> </ol>
<p>第五單元 木馬程式的威脅</p>	<ol style="list-style-type: none"> <li>1. 指出木馬程式對電腦的影響</li> <li>2. 列出木馬程式的來源</li> <li>3. 學會防範木馬程式的方法</li> </ol>



表 3.8 「維護資訊安全」主題

單元名稱	教學目標
<p>第一單元 資訊安全防護網</p>	<ol style="list-style-type: none"> <li>1. 列舉維護資訊安全之要素</li> <li>2. 指出「資訊安全政策」</li> <li>3. 辨別資安防護工具能防護的範圍</li> </ol>
<p>第二單元 善用資安防護工具</p>	<ol style="list-style-type: none"> <li>1. 列舉資安防護工具</li> <li>2. 區分資安防護工具的功能</li> </ol>
<p>第三單元 加強資訊安全意識</p>	<ol style="list-style-type: none"> <li>1. 簡述網際網路環境下應具備的資訊安 意識內容</li> <li>2. 描述「社交工程」的作法</li> <li>3. 列舉使用者最常見的兩個缺乏資訊安 全意識的問題</li> </ol>
<p>第四單元 資訊安全政策</p>	<ol style="list-style-type: none"> <li>1. 簡述資訊安全政策內容</li> <li>2. 描述本局資訊安全政策制定之原由</li> </ol>

表 3.9 「基本安全防護技巧」主題

單元名稱	教學目標
第一單元 密碼設定技巧	應用小技巧設定符合安全性原則的密碼
第二單元 良好的使用習慣	<ol style="list-style-type: none"> <li>1. 學會將電腦螢幕淨空</li> <li>2. 指出螢幕保護程式閒置時間</li> <li>3. 指出變更密碼的必要性</li> <li>4. 認識資料備份之重要性</li> </ol>
第三單元 安全的使用電子郵件	<ol style="list-style-type: none"> <li>1. 列出避免收到垃圾郵件的方法</li> <li>2. 學會關閉電子郵件預覽視窗</li> </ol>


表 3.10 「常用電腦操作」主題

單元名稱	教學目標
第一單元 變更密碼	學會變更密碼之操作步驟
第二單元 電子郵件使用設定	<ol style="list-style-type: none"> <li>1. 學會設定電子郵件使用環境</li> <li>2. 描述電子郵件主機名稱</li> <li>3. 解決郵件只能收，不能發送的問題</li> </ol>
第三單元 使用 web mail 收發電子郵件	學會 Web Mail 的操作使用

#### (四)、撰寫教材文字腳本

為方便編輯，將每一個單元教材文字，以表格化的腳本作紀錄，用以描述教材容、標題及教材所對應之考題(表3.11)。

表 3.11 文字腳本範例

頁數	圖示	主標題	副標題	內容/Audio	考題										
1		資訊安全威脅	兩大類威脅	<p>資訊安全威脅可分為故意及意外兩大類，由威脅的來源則可區分為「外部」及「內部」。一般而言，由外部而來的資訊安全威脅通常是「故意的」，內部的資訊安全問題大多為意外，但也不排除員工故意破壞資訊而造成資訊安全事件。</p> <table border="1" data-bbox="790 1146 1104 1541"> <thead> <tr> <th>故意</th> <th>意外</th> </tr> </thead> <tbody> <tr> <td>詐欺、偷竊及破壞</td> <td>無知</td> </tr> <tr> <td>駭客</td> <td>錯誤與忽略</td> </tr> <tr> <td>惡意攻擊程式碼</td> <td>喪失基礎建設</td> </tr> <tr> <td>商業間諜</td> <td>新技術</td> </tr> </tbody> </table>	故意	意外	詐欺、偷竊及破壞	無知	駭客	錯誤與忽略	惡意攻擊程式碼	喪失基礎建設	商業間諜	新技術	<p>資訊安全威脅的問題完全是因為網路駭客入侵所造成。--- n 員工阿隆因為公司新換 windows XP作業系統，他不熟悉新系統操作方式，所以誤刪了重要檔案，這是資訊安全事件的一種。--- Y</p>
故意	意外														
詐欺、偷竊及破壞	無知														
駭客	錯誤與忽略														
惡意攻擊程式碼	喪失基礎建設														
商業間諜	新技術														

#### (五)、撰寫考題

考題之設計需與教材各單元內容相配合，以達到考題與教材融合為一之目標。考題類型採取5種型式；包括是非題、選擇題、簡答題、配對題及操

作模擬。考題內容仍編輯於腳本表格內，方便與教材內容作對應及修改。

#### (六)、收集圖片檔案

網際網路上有些共享的圖形檔案，將該類檔案稍經修改，即可運用於數位教材。微軟公司的 Office 多媒體藝廊提供許多的圖片、動畫、聲音檔可供下載使用。本研究以Office多媒體藝廊網站作為圖形檔之主要來源，取得圖形檔之後再以freeware圖形工具軟體（Slowview）調整圖形檔尺寸。

#### (七)、撰擇教材發展工具

由於數位學習之風行，市面上亦發展出各式各樣的authoring tool。本研究所製作之數位教材內容大多以陳述性知識為主要內容，但部分單元涉及電腦操作使用，故選擇簡單易用的教材製作工具，有助於快速完成教材製作。Authoring tool的選擇依循「快速製作」、「快速更新」、支援「application simulations」及「製作考題」四原則，經收集相關工具產品之資訊，採用Macromedia 公司之captivate作為authoring tool。

#### (八)、編寫網頁

利用authoring tool，將文字腳本內容製作成為數位教材。

### 四、架設網站

#### (一)、系統環境

採用Windows 2000作為作業平台，IIS 5.0作為網頁伺服器，資料庫則採用SQL 2000 SERVER。資料庫儲存學習者基本資料、課程單元、考題、考試

發布資料以及學習者之學習歷程等內容。學習者透過 IE 瀏覽器進入系統，進行課程訓練。

## (二)、系統功能

數位教材之優點係因能提供員工隨時閱讀之彈性，由於組織的員工常有異動之情形，且依據研究對象服務之服務機構所訂之「人員安全管理作業說明書」規定，組織內之員工每年必須接受資訊安全概念教育訓練。為了配合教材內容及考題之修定，故系統提供考題資料維護，設定考題屬性，在不必修改程式之情況下，讓每一批次的學習得以選定不同的考題數及考題內容。

## 五、發佈教材進行訓練

透過電子郵件方式告知本課程之網址，通知員工上網學習。由於該公務機構係第一年建置ISMS系統，故「資訊安全概念」訓練課程採取實體及線上兩種方式進行。線上課程公布後，依員工意願自由參加。

## 第三節 研究工具

本研究所使用之研究工具包括資訊安全概念訓練數位教材(含考題)、教材網站及訓練後之學習態度問卷，其內容分述如下：

### 一、數位教材及考題

本研究設計發展之「資訊安全概念」數位教材，分為4章，共15小節，考題數為107題，每一小節有對應的考題。本次研究，由總考題中挑選30

個題目作為測驗題，挑選方式採優先挑選必考題，再依各小節平均分配對應的題目，故各單元均有對應之考題。考題順序依所對應之學習內逐一呈現，學習者依指示循序操作考題，並視答題之正確與否，強迫閱讀教材或選擇閱讀教材；即答錯題目者由系統強迫引導閱讀該考題所對應之教材；答對考題則由學習者選擇是否閱讀教材。學習時間預估為 4 小時。學習閱讀教材及答題情形均由系統紀錄至資料庫，作為資料分析來源。

## 二、教材網站

採用 Windows 2000 作為作業平台，IIS 5.0 作為網頁伺服器，資料庫則採用 SQL 2000 SERVER，本網站提供學習者作為學習入口，網頁架構如圖 3.3 所示，畫面最上方顯示操作區，分為「管理作業」及「一般作業」。管理作業主要功能如下：

- (一)、發布資訊：配合教育訓練實施期限，發布學習期間，學習者於該期間內進入學習網站方能進行教材閱讀及測驗。發布資訊之際同時可以設定考試題目，以本次訓練為例，發布之考題數為 30 題。(圖 3.4)。
- (二)、教材資料維護：設定教材編號、名稱、各章對應之單元明細及各單元所對應之考題 (圖 3.5)。
- (三)、考題資料維護：設定考題類型 (是非、選擇、簡答、操作模擬)、適用對象 (資訊人員、一般員工)、考題難易度及是否為必考題等資訊 (圖 3.6)。

(四)、呈現教材：紀錄學習者閱讀教材之 bookmarking，依學習者學習進度

顯示教材或考題。



圖 3.3 網頁架構



圖 3.4 發布資訊





圖 3.5 教材基本資料維護



圖 3.6 考題資料維護

### 三、學習態度問卷

為了解學習者對於本研究所發展之數位教材之看法，研究者自行編製學習態度問卷，並於學習者完成課程訓練後進行調查。本研究之學習態度問卷內容包含四個項目，分別為「對教材操作介面的滿意度」、「對教材內容的滿意度」、「對學習流程的滿意度」及「對考題內容的滿意度」，內容詳附錄 1。

「對教材操作介面的滿意度」項目包含 9 題，是為了瞭解學習者使用數位教材之後，對於教材操作介面的滿意度。「對教材內容的滿意度」包含 8 題，其目的為了解學習者對於資訊安全概念數位教材內容之滿意度。「對學習流程的滿意度」包含 5 題，是為了瞭解學習者對於將測驗穿插於教材之間的學習方式之看法。「對考題內容的滿意度」包含 3 題，則是為了瞭解學習者對於考題型態及操作模擬題目之看法。本研究之態度問卷採用五等量表，1 代表「非常不同意」；2 代表「不同意」；3 代表「普通」；4 代表「同意」；5 代表「極同意」。評分方式為：回答 1 者給 1 分，回答 2 者給 2 分，依此類推。