# 《資訊管理與資通安全》

| | |
|---|---|
| **試題評析** | 在考試大綱變更後，試題命題方向也與往年有很大的不同，今年資訊安全相關的考題就佔了70%，可謂歷年來最重，且題目也變得較爲靈活，對於以往常出現的Porter競爭策略、整合型資訊系統已不復見。由於今年考題與以往考試題型與知識範圍差異甚大，程度好的同學若有實務經驗，應該可以達到70分左右，而程度中等的同學應該也能達到接近50分的水準。<br>第一題：考的是防火牆、入侵偵測與入侵防禦系統的比較。以往雖曾有相關考題，但本卷需要對觀念細部運作更爲了解者，才能拿到高分。<br>第二題：出現了XSS攻擊，屬於較實務的題目。若同學沒有相關的網頁工程經驗，很難憑空寫出。<br>第三題：爲持續營運管理的相關議題，也是以往無類似題的題目。不過已編入總複習，若同學能熟讀總複習講義，應不難作答。<br>第四題：出現服務水準與操作水準，同屬於ITIL中的細項，一樣是新的考點，對同學而言應該也較難掌握。<br>第五題：屬較基本的考題，若同學充分準備，應不難作答。 |
| **高分命中** | 第一題：《高點資訊管理與資通安全講義第三回》，金乃傑編撰，頁46~54。<br>第二題：《高點資訊管理與資通安全講義第三回》，金乃傑編撰，頁44。<br>第三題：《高點資訊管理與資通安全總複習講義》，金乃傑編撰，頁56。<br>第四題：《高點資訊管理與資通安全講義第一回》，金乃傑編撰，頁14~15、《高點資訊管理與資通安全講義第三回》，金乃傑編撰，頁25。<br>第五題：《高點資訊管理與資通安全講義第四回》，金乃傑編撰，頁34~39、《高點資訊管理與資通安全講義第一回》，金乃傑編撰，頁32。 |

一、試比較封包過濾防火牆(Packet Filter Firewall)、網路型入侵偵測系統(Network-based Intrusion Detection System, IDS)與網路型入侵防禦系統(Network-based Intrusion Prevention System, IPS)在資安防護上之功能區別。(15分)

**答**：

茲將封包過濾防火牆、網路型入侵偵測系統與網路型入侵防禦系統比較如下表：

| | 封包過濾防火牆 | 網路型入侵偵測系統 | 網路型入侵防禦系統 |
|---|---|---|---|
| 內容 | 具有過濾封包功能的路由器，可以根據IP或TCP標頭設定檢查規則，來檢驗IP封包進出以決定要放行或丟棄。 | 以原始網路封包作爲資料來源，偵測及分析整個網路所有過往的通訊，作爲事前預警。 | 作爲網路之間或網路組成部分之間的獨立硬體設備，對流經的封包透過病毒特徵和協議異常進行深層檢查，然後確定是否放行。 |
| 目標 | 資源控管 | 預警分析 | 入侵預防 |
| 檢查內容 | 通常只檢查IP、TCP、UDP、ICMP封包的標頭(包含來源/目的IP或埠號、協定)與網路介面，不會檢查資料段內容。 | 除了標頭外，也會檢查封包的內容。 | 除了標頭外，也會檢查封包的內容。 |
| 安全防護方法 | 丟棄惡意封包、中斷連線。 | 1.通知防火牆中斷連線。<br>2.提供通知管理者。<br>3.記錄入侵資料作爲事後稽核鑑識的證據。 | 1.丟棄惡意封包、中斷連線。<br>2.提供通知管理者。<br>3.記錄入侵資料作爲事後稽核鑑識的證據。 |
| 運作層次 | Layer 3 | Layer 7 | Layer 7 |
| 執行效率 | 快 | 較慢(注重分析與預警) | 較慢(封包深層檢查) |
| 建置成本 | 低 | 中等 | 很高 |

| | 封包過濾防火牆 | 網路型入侵偵測系統 | 網路型入侵防禦系統 |
|---|---|---|---|
| 限制 | 1.無法防止以特定應用程式的漏洞攻擊。<br>2.不支援進階的使用者認證。<br>3.記錄網路使用情況的功能有限。<br>4.可利用TCP/IP協定的問題攻擊。<br>5.易因爲錯誤設定而使防火牆不安全。<br>6.無法阻檔SQL Slammer網路蠕蟲。 | 1.對攻擊採用被動處理，無法立刻解除威脅。<br>2.若網路的型態過大，無法完全監控網路上所有流通的封包數。<br>3.若要擷取大型網路上的流量並分析，需要更有效率的CPU處理速度，以及更大的記憶體空間。<br>4.如果封包是已經加密過的，就無法調查其中的內容。<br>5.無法偵測是哪一個使用者正在使用該主機。 | 1.若要擷取大型網路上的流量並分析，需要更有效率的CPU處理速度，以及更大的記憶體空間。<br>2.如果封包是已經加密過的，就無法調查其中的內容。<br>3.無法偵測是哪一個使用者正在使用該主機。 |

二、跨網站腳本攻擊(Cross Site Script, XSS)與資料隱碼(SQL Injection)是目前政府機關網頁應用程式最常受到的兩大威脅。試說明SQL Injection與XSS弱點發生原因，並舉例說明測試方法以及其防範方式。(20分)

**答**：

(一)跨網站指令碼(Cross-site scripting, XSS)是一種網站應用程式的安全漏洞攻擊，是程式碼注入攻擊的一種。它允許惡意使用者將程式碼注入到網頁上，其他使用者在觀看網頁時就會受到影響。這類攻擊通常包含了HTML以及使用者端腳本語言。例如：當論壇可以輸入HTML標籤時，惡意的使用者先撰寫好具有攻擊性的JavaScript程式碼，再將論壇留言的內容加入HTML reference到惡意的JavaScript。如此在文章發布後，當其他使用者瀏覽到該篇嵌有惡意JavaScript的網頁，就會遭受攻擊。

(二)SQL攻擊(SQL injection)，又稱隱碼攻擊，是發生於應用程式之資料庫層的安全漏洞。這類攻擊的攻擊者在連結資料庫的表單中，加入具有SQL語法的特殊用字，破壞原本連接資料庫的SQL語法，使得資料庫出現異常，甚至可以爲造成授權的使用者或者讓網站印出其他的會員資料。例如：網站中原本驗證會員的SQL語法爲：

SELECT * FROM member WHERE id = '$uid' AND passwd = '$pass'

若攻擊者在表單中填入$uid爲0；$pass爲' OR '1' = '1；則SQL語法變爲：

SELECT * FROM member WHERE id = '0' AND passwd = '' OR '1' = '1'

由於通常網站管理者的ID爲0，且後面'1' = '1'一定會成立，因此就能僞裝成管理者登入了。

以下將測試方法與防範方法用表格整理之：

| | 跨網站攻擊 | SQL攻擊 |
|---|---|---|
| 造成的危害 | 1.盜用cookie ，獲取敏感信息。<br>2.植入Flash/Java，獲取更高許可權。<br>3.利用iframe、AJAX以被攻擊者的身份執行一些管理動作。<br>4.利用可被攻擊的區域受到其他區域信任的特點，以受信任來源的身份請求一些平時不允許的操作。<br>5.在流量極大的一些頁面上的XSS到小網站可以達到DDoS攻擊的效果。 | 1.資料表中的資料外洩。<br>2.資料結構被駭客探知，得以做進一步攻擊。<br>3.系統管理員帳戶被竄改。<br>4.取得系統較高權限後，有可能得以在網頁加入惡意連結以及XSS。<br>5.經由資料庫伺服器提供的作業系統支援，讓駭客得以修改或控制作業系統。 |
| 測試方法 | 只要在任何使用者可以字串的地方輸入「<script>alert("xss")</script>」，若網頁出現亂碼或跳出alert方塊，則代表具有被攻擊的可能。 | 只要在任何使用者可以字串的地方輸入單引號(')、雙引號(")、註解(/**/)、分號(;)，若網頁執行結果出現錯誤，則代表具有被攻擊的可能。 |

| | 跨網站攻擊 | SQL攻擊 |
|---|---|---|
| 防範方法 | 1.對使用者所提供的內容進行過濾，將HTML的特定標籤去除。<br>2.指定輸出的HTTP header，使得使用者輸入的資料以純文字解析，而非可以引發攻擊的HTML。<br>3.在瀏覽器中關閉JavaScript功能，或設定不允許的三方網站的JavaScript執行。 | 1.在設計應用程式時，完全使用參數化查詢(Parameterized Query)來設計資料存取功能。<br>2.在組合SQL字串時，先針對所傳入的參數作字元取代。<br>3.透過程式語言中特殊的功能，讓使用者輸入的特殊字串被加上反斜線去除其功能。<br>4.使用其他更安全的方式連接SQL資料庫。例如已修正過SQL資料隱碼問題的資料庫連接元件，例如ASP.NET的SqlDataSource物件或是 LINQ to SQL。 |

三、(一)請說明BS 25999標準中，營運持續管理(Business Continuity Management, BCM)實施的的四個階段內容，包括：「了解組織」、「決定營運持續管理策略」、「發展與執行營運持續管理作為」及「演練、維護與審查」。(20分)

(二)其中在「了解組織」中，最重要的就是以營運衝擊分析(Business Impact Analysis,BIA)與風險評鑑(Risk Assessments, RA)二大方法進行。試說明此二者實施目的之不同。(25分)

**答**：

(一)持續運作方法的四階段步驟說明如下：

1.瞭解組織：組織對其所處環境進行分析，從可能引起營運過程中斷的事件開始，如設備故障、水災和火災，瞭解組織所面臨風險發生的可能性和衝擊，依成本及效益考量預先部署所需機制，並鑑別出重要營運過程及排定優先順序，將促使組織及早建立緊急因應程序、備援方案及復原程序，避免或降低傷害。此步驟必須讓資源和作業擁有者完全參與，包括風險評鑑與營運衝擊分析兩項活動。

2.決定營運持續策略：瞭解可能的風險或災難後，應針對風險之優先順序決定將採取之策略。決定策略並不容易，須仔細考慮組織營運目標、資源、文化、流程及投入成本。一般來說，處理風險的策略可以從下列方向考慮：

(1)忽略風險：對於可接受之風險便可採取接受因應。

(2)避免風險：當該風險影響極大時，便應設法極力阻隔風險。

(3)降低風險：採取適當控制措施，當風險發生時可因適當控制而將損失減少。

(4)轉移風險：透過保險，將風險轉移到保險公司上，能夠有災後重建的經費。

3.發展與執行持續營運管理：組織應發展 BCP 計畫以維護營運操作，或在關鍵營運過程中斷或故障後在必要的時間內恢復營運，營運持續管理計畫作業應考慮以下內容：

(1)計畫啟動條件：應清楚說明各項計畫需遵守的啟動條件、評鑑辦法、應參與人員。

(2)權責說明：鑑別並協議所有權責，說明由誰負責執行計畫的那個部分，必要時應指定代理人。

(3)備援程序：必須在要求時間內完成最低營運水準復原工作，需特別注意與外部的營運依存要件與合約的適當性。

(4)復原程序：應採取那些行動以復原正常營運作業，包含鑑別必要的資源需求。

(5)維護時間表：應指定如何及何時測試該計畫，以說明及維護該計畫的程序。

(6)認知及教育訓練：旨在讓參與者瞭解營運持續過程，確保該過程持續有效。

4.演練、維護與審查：

(1)演練：由於假設錯誤、疏忽、或設備、人員之變動，可能造成持續營運計畫失敗，因此應定期演練，確保符合最新狀況及有效性。

(2)維護：透過定期審查和更新方式來維護營運持續計畫，確保其持續有效。應在計畫中加入維護的程序，以確保營運持續計畫的主要項目得到適當處理。

(3)審查：若發現營運持續計畫尚未反應營運作業的變更時，應對計畫作適當的更新，正式的變更管制應確保所公布的計畫都是最新版本，並且利用對整體計畫的定期審查來確保計畫處於最新狀況。

(二)茲將目的分述如下：

1.風險評鑑(RA, Risk Assessment)：鑑別、定義與評估組織資產所面對的威脅、弱點及其風險值，以便確立可接受風險程度及管理風險相關的行動計劃。
2.營運衝擊分析(BIA, Business Impact Analysis)：鑑別關鍵營運流程及鑑別關鍵營運流程中斷對組織造成之傷害或損失、及中斷後回復至可接受的作業水準之回復時間。

四、在資訊委外作業中，「委外服務水準的管控」被視為委外服務成敗的一個重要因素。
(一)何謂服務水準協定(Service-Level Agreements, SLA)與操作水準協定(Operational Level Agreements, OLA)？(10分)
(二)雲端環境的委外比傳統委外更需注重那三個因素？(10分)

**答**：

(一)
1.服務水準協議(Service Level Agreement, SLA)：服務提供者與使用者之間，就服務水準以及性能等方面達成的協議或契約。一般來說，訂定 SLA 需考量以下要點：
(1)SLA 必須以服務爲導向，而且這樣的服務可以創造商業利益。
(2)成本、價格以及服務內容應透明化。
(3)力求簡單明瞭，透過關鍵績效指標(KPI)避免過於繁複的細節。
(4)需排列優先順序，首重爲企業創造價值。
(5)應設立明確的服務經理人。
2.操作水準協議(Operational Level Agreement, OLA)：屬於組織內部的工具，定義的服務內容未必直接與使用者相關，但卻在實現 SLA 不可或缺。組織內部大家關心的首要問題是業務能不能正常的運作，如印表機是否可用，網路是否暢通等等。OLA 是制定 SLA 的先決條件之一。OLA 明確的指出服務提供者的角色和責任及服務提供者與使用者雙方的責任關係。

(二)雲端運算是以網絡運算技術，配合無所不在、隨選動態的網路，共享廣大的運算資源，透過最少的管理工作及服務供應者互動，快速提供各項服務。而雲端運算的委外就是將企業的應用系統以SaaS、PaaS或IaaS的方式建置在雲端供應商中，由雲端供應商進行維護，並依照使用量計費的一種營運模式。

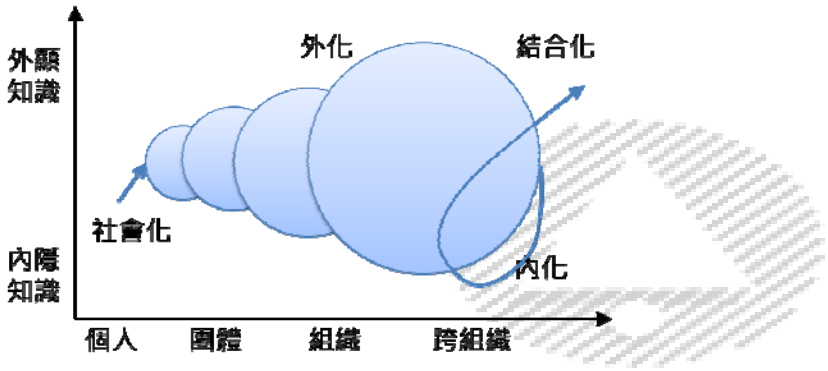
(三)在傳統的委外中，我們常需考量供應商的經營體質、產品技術能力、服務品質與口碑等面向。但由於雲端運算必須透過網路，增加了許多不確定性，因此必須要特別注重以下因素：
1.機密性(Confidentiality)：確保只有獲得授權的人才能存取資訊，保護資訊不被非法存取或揭露。在此強調組織營業的機密資料不會遭受他人檢視或揭露，以保護智慧財產、專利與商業機密。
2.完整性(Integrity)：保護資訊與處理方法的精確性與完整性，確保資訊沒有不適當的修改或損毀。在此強調資料的可靠性，不能發生如日本 Yahoo!子公司因更新而誤刪資料的狀況。
3.可用性(Availability)：經授權的使用者能適時的存取所需資訊，資料必需即時並可靠的提供給企業內部各個層級的使用需求。在此強調網路的穩定性，不能當需要使用資料時卻無法連線，造成營業損失。

(四)除了以上三個因素外，還要注意簽訂的合約與計價模式。因爲雲端運算通常會依照使用量計價，與傳統委外按使用內容計價不同，因此必須要進行審慎的計算，確保財務體系正常運作。

五、智慧資本是企業與政府組織的寶貴資產，為了創造與保存這項資產，可以透過組織管理與資訊科技的輔助而達成。
(一)請說明組織在知識創造過程所扮演的角色與作為，並請舉例說明。(10分)
(二)資料挖掘(Data Mining)具備那些功能？並各舉一應用例。(10分)

**答**：

(一)知識螺旋(Knowledge Spiral)是組織動員個人的內隱知識，經由社會化、外化、組合化、內化，將知識從個人擴大爲團體，最後到組織甚至是跨組職的外化、轉移與創造的過程。透過知識螺旋，可以從既有知識(Platform Knowledge)追求、創造目標知識(Target Knowledge)，創造知識的流程如下圖所示：




爲了使知識能夠順利的轉移與創造，組織必須要扮演下列角色：

1.文化促動：要鼓勵創新冒險、利用新知的文化，形成企業對知識分享的價值系統與目標。例如：在工作環境內，營造創新與分享的氣氛，洗手間內貼上新知的標語，都有助於員工建立分享的文化。

2.鼓勵分享：建立員工知識分享的共識、動機與價值觀，使員工間互相信任及良好的溝通，相信知識分享給對方後，對方就會有所回饋，不會獨占其功勞。很多員工不願分享知識是因爲怕自己被取代或搶功勞，若要建立信任，除了增加同儕互動的機會外，更有賴高階主管推動。高階主管絕不可以只聽信某些人的建議，這樣便會破壞員工間的信任。

3.獎勵制度：建立具體、分量的知識分享的獎賞制度。例如：透過知識管理系統，可以明確的紀錄員工分享的知識數量以及其他人對該知識的評價。在具體的獎勵之度下，可以讓員工更樂意分享，並且知道分享後會有實質的報酬，例如：加薪、放假或是獎金等等。

4.IT 支援：提供全面性、普及性的知識分享 IT。在知識螺旋的不同階段中，可以搭配不同的資訊科技使知識更便於分享或儲存。例如：在社會化階段，組織內部可建立社交網路讓員工間培養分享文化；外化階段，則可以用 WiKi 控管知識；組合化時則可藉由資料探勘的工具協助找出隱藏的知識價值；內化階段則可以透過 e-learning 系統進行員工的教育訓練。

(二)資料挖掘(Data Mining)是利用統計、人工智慧或其他的分析技術，在大量資料中找出未知、有效且可付諸行動的資料彼此間所隱藏的模式與關係，且中推論出規則，用以預測未來的行爲並作爲決策之依據。一般而言具備以下功能：

1.分類(Classification)：使用規則模型對未知資料進行類別判斷，達到預測。例如：依照財務狀況、年齡、性別與職業等資訊判斷信用卡申辦人的信用程度；或從股市交易資料判斷股市的漲跌情形。

2.分群(Clustering)：對已知資料進行歸納或判讀未知資料之群組。例如：從網站使用者的基本資料或購物習慣將使用者分成不同群組，對不同群組的使用者採用不同的行銷方法，以提升業績。

3.關聯(Association)：購物籃分析，找出商品間的關聯性。例如：在 Blog 中追蹤使用者的閱讀習慣，當閱讀完某篇文章後推薦其他閱讀該篇文章的使用者也會閱讀的文章，提升使用者黏著度。

4.次序(Sequence)：與關聯分析類似，一樣是找出特定品項間的關係，但不同的是次序分析特別著重於品項間的次序，強調從事 A 之後會從事 B。例如：可設計推薦系統當某人在某區的晚上看完電影後，可以到某家餐廳進行消費，作爲行程規畫的建議。