

國營事業聯招115年徵才589人



國營事業聯招

高薪多缺，連續上榜不費力



✓報名日期：115/6/25~7/13

✓筆試日期：115/10/18

國營事業3大報考優勢



- 1.具中華民國國籍，且不得兼具外國國籍
- 2.國內外公私立專科以上學校畢業，並符合甄試類別所訂科系者(輔系亦可)



績效/工作/三節獎金
生日/結婚禮金、
生育津貼、年假休假
等眾多福利



依分發之公司規定辦理，
每月約新台幣36-39000
之間，前四年每年加薪，
可調近約40,000元，另有
年終獎金最高4.4個月

國營事業專攻班 企管/財會/地政/資訊/政風/法務

類別	★投考策略★
共同科目	高普考考生多準備1~2科，即可連續上榜！
企管	高考金保、財稅 差異科目》企業概論、管理學
財會	高考會計 差異科目》政府採購法規、財務管理
地政	高考地政 差異科目》政府採購法規
資訊	高考資訊 科目全涵蓋
政風	高考法律廉政 差異科目》民法、政府採購法規
法務	司法四等 差異科目》商事法

115/7/31 前
憑『115高普考准考證』
享優惠

面授/網院全修
特價15,000元起

雲端全修
特價32,000元起

資訊組考衝班
特價3,000元起

企管組題庫班
特價4,000元起

【台北】台北市開封街一段2號8樓 02-2331-8268 【台南】台南市中西區北門路一段101號10樓之一 06-223-5868
【台中】台中市東區大智路36號2樓 04-2229-8699 【高雄】高雄市新興區中山一路308號8樓 07-235-8996

各分班立案核准



《資通網路與安全》

一、一網管工程師在為一棟新大樓建置網路架構，大樓內部有一個對外提供服務的學術網站伺服器機房。請回答以下問題：（每小題 10 分，共 30 分）

- (一)新大樓的路由器與學校機房之間接了兩條實體線路（一條主線、一條備援線）。若網管工程師放棄手動寫靜態路由，改為啟用 OSPF 動態路由協定。當某天主線路不小心被挖斷時，大樓的網路流量會發生什麼變化？請從動態路由協定的特點與選路依據來合理解釋。
- (二)學校將大樓的「學術網頁伺服器」放在防火牆的 DMZ (Demilitarized Zone)，而不是直接接在外網或安全的內網。當外網的使用者想要連進來瀏覽網頁時，防火牆的安全策略 (Security Policy) 應該要如何放行？請寫出必須設定的三個關鍵要素。
- (三)為了防止學生在教學實驗室連上惡意詐騙網站，網管工程師架設了一台 Proxy 伺服器，「代表學生（客戶端）」向外網發送請求並進行安全檢查。請問這台架設在學生前端、幫忙過濾外網網頁的設備，屬於「正向代理 (Forward Proxy)」還是「反向代理 (Reverse Proxy)」？請詳述兩者的本質區別。

試題評析	本題屬於理論與實務並重之整合性考題，其結合路由協定、代理伺服器，以及網路組態與資訊安全觀念，相當靈活。
考點命中	1.《高點・高上網路講義》第四回第 3 章，張又中編撰，頁 3-5~7、41。 2.《高點・高上網路講義》第五回第 4 章，張又中編撰，頁 4-12。

答：

(一)OSPF 屬於鏈結狀態路由協定，各路由器會交換鏈結狀態資訊，建立網路拓模資料庫，並利用最短路徑優先演算法計算到各目的網路的最佳路徑。其路由主要依據是路徑累計的 OSPF Cost，一般會依介面頻寬計算或由管理者手動設定，累計成本較低的路徑優先。正常情況下，若網管工程師已將主線路設定為較低的 OSPF Cost、備援線路設定為較高的 Cost，流量便會優先經由主線傳送。當主線路被挖斷時，流量變化如下：

1. 路由器偵測到介面狀態中斷，或因逾時未收到鄰居路由器的封包，而判定鄰接關係失效。
2. 路由器產生新的鏈結狀態通告，通知其他 OSPF 路由器該主線路已失效。
3. 各路由器更新鏈結狀態資料庫，重新執行最短路徑優先演算法。
4. 原經過主線的路由會從路由表中移除，改安裝經由備援線路的路由。
5. 後續流量自動改走備援線路，不需網管人員手動修改靜態路由。

在 OSPF 重新收斂的期間可能出現少量封包遺失、延遲增加或連線短暫中斷；收斂完成後即可恢復通訊。

(二)DMZ 是介於外部網路與內部網路(Intranet)之間的獨立網段，適合放置必須對外提供服務、卻又不宜直接進入 Intranet 的伺服器。外網、DMZ 與內網之間的流量仍須經過防火牆並受到安全策略控制。防火牆 Security Policy 至少應設定下列三個關鍵要素：

1. 來源條件
 - 來源安全區域：Internet、WAN 或 Untrust。
 - 來源位址：可設定為任何外網位址；若只有特定單位可存取，則應限制來源 IP 範圍。
2. 目的條件
 - 目的安全區域：DMZ。
 - 目的位址：學術網站伺服器的公網 IP，並透過 NAT 映射至 DMZ 伺服器的私有 IP。
3. 允許的服務及動作
 - 只放行網站所需的服務，例如 HTTP：TCP 80；HTTPS：TCP 443；FTP、SSH、資料庫連線及其他未明確允許的服務，均維持預設拒絕。
 - 防火牆若為狀態檢查型防火牆，網站伺服器的回應封包通常可依既有連線狀態自動返回，不必另外全面開放 DMZ 至外網的連線。

高點・高上公職

分|眾|課

容易
額滿

為好名次而來

高普特考資訊 經典題庫班

FOR: ☒ 資訊本科系大專/研究所畢業生 ☒ 曾報考公職資訊相關類科，但未能掌握上榜訣竅者

考前衝刺

海量解題

收集5~10年各類國家考試資訊類試題

題型按單元主題分類整理，有助最後複習

高分策略

講解重要觀念與解題技巧，藉此熟練不同答題方法

衝刺!

地方特考/國營事業聯招，現在報名立即上課！

115/7/31前 憑高普准考證享優惠

	單科	五科（資構、資管、資安、資庫、網路）全修
網院VOD	2,500 元起	13,500 元
雲端函授	單科 6 折	17,000 元



立即諮詢

【優惠詳情 & 報名，請洽各班櫃台或高點・高上公職生活圈！】

上榜必讀好書賞



高點網路書店夏季線上書展，全館 8 折起！

另有百元花車任你挑！



活動詳情

(三)本題的 Proxy 伺服器屬於正向代理，原因是該 Proxy 代表學生端的電腦向外部網站提出請求，並在請求送出前進行網址過濾、內容檢查、惡意網站封鎖或存取紀錄。客戶端不直接與外部網站建立端到端連線，而是先將請求送至 Proxy，再由 Proxy 另行連線至外部網站並代為轉送。

正向代理與反向代理的本質區別如下表所示：

代理面向	正向代理	反向代理
代理對象	代理用戶端	代理伺服器
部署位置	用戶端與外網之間	外網與後端伺服器之間
保護對象	學生、員工等用戶端	網站及應用伺服器
對外隱藏	用戶端身分與 IP	後端伺服器位置與架構
常見用途	上網過濾、存取控制、匿名連線	負載平衡、WAF、TLS 終止、網站保護
主要目的	● 隱藏內部用戶端的 IP 位址。 ● 過濾惡意、色情或詐騙網站。 ● 限制特定應用程式或檔案下載。 ● 控制學生或員工可以瀏覽哪些網站。 ● 進行身分驗證、上網紀錄及內容快取。	● 提供負載平衡。 ● 隱藏及保護後端網站伺服器。 ● 提供快取、WAF 及 DDoS 防護。 ● 將流量分配至多台後端伺服器。 ● 依網址將請求轉送至不同的應用系統。

二、在數位經濟與雲端運算高度發展的時代，個人資料（Personal Data）已成為組織核心的資訊資產，同時也是資安防範與法律合規的重中之重。依據我國個人資料保護法與歐盟一般資料保護規則（GDPR）之法理精神，企業在處理個人隱私時，必須將安全防護思維融入資料的完整生命週期中。為了在「數據分析利用」與「隱私保護」之間取得平衡，企業常採用「去識別化」（De-identification）技術。去識別化技術又包含「匿名化」（Anonymization）及「擬匿名化」（Pseudonymization）技術。請回答以下問題：（每小題 10 分，共 30 分）

（一）請解釋何謂「匿名化」（Anonymization）。

（二）請解釋何謂「擬匿名化」（Pseudonymization）。

（三）請舉一個例子說明「匿名化」及「擬匿名化」兩者之差異。

試題評析	為近年熱門之個人資料保護議題，可參考資通安全法規課程中提及之個人資料保護法、個人資料保護法施行細則之方向作答。
考點命中	《高點・高上資通安全法規講義》第一回第 1 章，張又中編撰，頁 1-16。

答：

- (一)匿名化係指對個人資料進行刪除、泛化、彙總、擾動或其他處理，使任何人依合理可能使用的手段，均無法直接或間接識別特定自然人，真正完成匿名化的資料，原則上不再屬於 GDPR 所稱的個人資料；但若仍可能透過其他資料對照、組合或連結而識別個人，則不能僅因刪除姓名而認定已匿名化。我國《個人資料保護法施行細則》也說明，必須與其他資料對照、組合或連結後才能辨識個人的情況，納入「間接識別」的範圍。
- (二)擬匿名化係指將身分證字號、姓名等識別資料，以代碼、假名、亂數編號、雜湊值或 Token 取代，使資料在沒有額外資訊的情況下，無法直接歸屬於特定個人。然而，組織仍保留一份額外的對照資訊或金鑰，只要取得該對照表或金鑰，仍可將資料重新連結至原本的個人。因此，擬匿名化是仍可透過額外資訊重新歸屬或重新連結至特定個人的資料保護措施，而非完全匿名化。
- (三)匿名化如永久刪除代碼及姓名對照表，此時任何人均無法透過對照表還原至特定學生；擬匿名化則保留代碼及姓名對照表，如 A001↔王小明、A002↔李小華。依據 GDPR，擬匿名化資料只有在結合額外資訊後才能歸屬於特定資料主體，而且該額外資訊必須分開保存並受到適當的技術及組織措施保護。由於資料仍可重新識別，擬匿名化資料仍然屬於個人資料，仍須遵守目的限制、存取控制、安全維護及個資當事人權利等規定。

【版權所有，重製必究！】

三、當代組織面臨的營運威脅日益複雜，從勒索軟體癱瘓機房到新興供應鏈中斷風險，皆可能對組織造成無法估計的損失。營運持續管理（Business Continuity Management, BCM）已成為企業與政府機構建構「數位韌性」的核心管理機制，旨在確保關鍵商務功能在遭受重大衝擊時仍能維持底線運作。組織在建構完整的 BCM 計畫前，必須透過「風險評估（Risk

Assessment, RA)」來掌握潛在威脅。請詳細列舉出風險評估流程中的五個核心執行步驟，並逐一扼要闡述各步驟的主要工作目標為何？（10分）

試題評析	為典型的風險管理考題，可由系統分析課程之風險管理章節內容切入。
考點命中	《高點・高上系統分析講義》第四回第10章，張又中編撰，頁10-3~6。

答：

1. 風險辨識

找出危害專案的風險項目，隱含設法找出潛藏的風險，並確認是否為危害專案的風險事項。

2. 風險評估

估計風險項目發生的機率與風險發生後可能造成的損失。

3. 風險分級

依風險的大小來決定納入風險管理的項目。由於專案的人力、時間、預算等資源均為有限，不可能無限制、全面性對每一種風險都實施風險管理計畫、風險控制策略以及風險監督活動。有效率的風險管理應選擇較重要的風險事項來做為實施對象。

4. 風險計畫

針對已納入風險管理之每一風險，擬定所採用的風險控制技術、評估可用風險降低比(Risk Reduction Leverage, RRL)成本效益，並且制定風險監督計畫等管理步驟。

5. 風險監督

為一項持續性工作，持續監督風險，一直至專案結束為止。

四、某公司使用一套由外部廠商提供的遠端管理工具，該工具平時用於協助資訊人員更新軟體、派送設定檔與維護內部主機。某次例行更新後，多台內部主機開始出現異常連線行為，但使用者並未點擊可疑郵件，也未下載未知檔案。初步調查發現，異常程式是透過該遠端管理工具的正常更新流程被派送到主機上，因此在部分紀錄中顯示為「合法更新」。請回答下列問題：（每小題15分，共30分）

（一）此事件中，攻擊者為何不一定需要直接攻擊公司內部系統，也能使內部主機執行惡意程式？請分析其可能涉及的攻擊方法，並說明此類攻擊與一般使用者自行下載惡意程式有何不同。

（二）若公司只檢查「員工是否點擊可疑郵件」或「主機是否存在未修補弱點」，為何可能無法發現此類攻擊的真正原因？請說明應如何從第三方風險管理、更新驗證與內部監控三個面向降低風險。

試題評析	係屬資通安全實務之考題，可由惡意程式分析與防制的角度思考。
考點命中	《高點・高上資訊安全實務講義》第三回第2章，張又中編撰，頁2-5。

答：

（一）此事件可能涉及軟體供應鏈攻擊(Software Supply Chain Attack)或受信任關係攻擊，攻擊者並未直接入侵該公司的內部主機，而是先攻擊上游的外部廠商、遠端管理工具或軟體更新流程，例如：入侵廠商的軟體開發或建置環境，在合法程式碼中植入惡意程式，再利用廠商原有的遠端派送權限，將惡意程式送入客戶主機。由於遠端管理工具本來就具有軟體安裝、系統設定及管理多台主機的高權限，攻擊者一旦控制該工具或其更新機制，就能利用組織原本信任的通道，使內部主機執行惡意程式。NIST的供應鏈風險管理指引也強調，組織必須辨識及降低產品、服務與第三方供應鏈各層級的資安風險。與一般使用者下載惡意程式的不同之處在於，一般惡意程式感染通常需要使用使用者點擊釣魚郵件、開啟惡意附件、造訪惡意網站，或是下載惡意程式；然軟體供應鏈攻擊不一定需要使用使用者進行操作，惡意程式經由原本可信任的廠商或工具派送，且因遠端管理工具通常擁有系統管理權限，一次更新便可能同時感染大量主機。因此，其危險之處在於攻擊者利用的不是使用者的不慎，而是組織對第三方軟體、更新機制及管理工具的信任。

（二）公司只檢查員工是否點擊可疑郵件，會將調查範圍限制在社交工程；只檢查主機是否存在未修補弱點，則會將原因限制在漏洞利用。然而，本事件的惡意程式是透過合法工具的正常更新流程進入主機，可能沒有釣魚郵件、沒有使用者下載，也未必利用公司主機的漏洞。降低風險可從以下三個面向進行。

高點・高上公職 函授課程

不用到教室，也能上到全國最好的公職課程！

知識達課輔戰隊

線上線下

全面應援你的上榜路！



① 社群互動

加入群組由老師親自釐清觀念及學習弱點，分析考情與備考策略，還能與同儕互相打氣！



② 課業諮詢

課業問題，直通授課老師、助教團，由授課老師或該科助教為你指點迷津。



③ 閱卷批改

提供手寫作答後、拍照上傳到「課業諮詢服務」專區，由老師／助教提供寫作指導。



④ 助教課輔

與助教面對面互動，汲取實戰經驗與答題訣竅！



⑤ 讀書會

老師助教共組，課前測驗、課後講解、強化答題技巧的課輔課！



⑥ 作題評量

平時練習驗收學習成效；考前勤練錯題，培養預試高分！



詳細服務
看更多 ▶

※以上服務僅限輔導期限內部分類科

115/7/31前

憑115高普考准考證享優惠

★116高普考全修課程，享常態特價**最高折5,000元**！

★另有單科、申論寫作正解班、經典題庫班、總複習。

優惠詳洽生活圈！



線上諮詢

線上試聽、購課&課程詳情，請見 知識達購課館 ec.ibrain.com.tw 或 高點網路書店 publish.get.com.tw

1. 第三方風險管理

在採購前評估廠商的資安能力、開發流程及事件紀錄，要求廠商提供軟體物料清單(SBOM)及元件來源資訊。此外，定期進行稽核、滲透測試或第三方驗證，對廠商帳號實施多因素驗證、最小權限及使用期限限制，避免讓單一遠端管理工具不受限制地控制所有主機。

2. 更新驗證與安全部署

驗證更新套件的數位簽章、憑證及雜湊值，並比對更新來源、版本、發布時間與廠商公告。此外，先在隔離測試環境或少數試驗主機進行更新，採用分批部署、金絲雀部署及觀察期。建立快速停止派送及回復至前一版本的機制，將更新伺服器與一般辦公網路分區隔離。

3. 內部監控與異常偵測

使用 EDR 監控遠端管理工具產生的程序、PowerShell 命令及檔案異動，委由 MDR 服務團隊整合 EDR、NDR 及 SIEM 資料，執行持續偵測、分析與事件回應。另建立遠端管理工具的正常行為基準，偵測非正常時段大量派送、短時間修改多台主機或連向陌生網域等行為；將關鍵主機進行網路分段，降低橫向移動與大規模感染。

高點
高上

【版權所有，重製必究！】



公職 高錄取時代

7/12前>>憑115高普考准考證
享考生紅利

弱科健檢 加入【高點·高上生活圈】可免費預約



- 【速攻班】網院/線上：特價23,000元起
雲端(兩年班)：特價31,000元起
- 【總複習班】網院：特價1,500元起、雲端：特價3,000元起
- 【申論寫作正解班】網院：特價3,000元起/科、雲端：特價6折起/科
- 【經典題庫班】網院：特價2,500元起/科、雲端：特價6折起/科



- 【全修班】面授/網院：高考36,000元起、普考31,000元起
雲端：高考46,000元起，普考41,000元起
- 【考取班】高考：特價65,000元、普考：特價55,000元(限面授/網院)
- 【狂作題班】面授：特價5,000元起/科



- 【115年度】網院：定價5折起、雲端：定價6折起
- 【116年度】面授/網院：定價65折起、雲端：定價85折

眾多考生證實，不止「快速上榜」還要「好名次」

勇奪高普考+地特三冠王，高點居功厥偉

陳○辰 應屆連續考取

(中興財金系) 114高考財稅行政【狀元】
114普考財稅行政【狀元】
113地特四等臺中市財稅行政【狀元】

施敏老師(張曉芬)表格整理清楚，記憶上省下相當多功夫，還會給一些口訣讓我方便記憶。考前總複習，老師在課堂上著重講解今年修法部分，加深考前的印象。

狂作題班專注破解難題，非本科也能高分上榜

趙○儀 跨系高分考取 114高考會計【榜眼】

(中正心理所)

中會的「狂作題班」對我幫助很大！鄭泓老師(鄭凱文)課堂上有建議，如果後期不知該如何複習，可加選這門課程，它是一系列模擬考及精選範例講解構成，不講基本觀念，專解決題，目的是除了複習也降低考試的緊張。

※以上優惠限商會/資訊/地政類科，詳細優惠辦法速洽高點·高上考場攤位或各地分班！

【台北】台北市開封街一段2號8樓 02-2331-8268 【台南】台南市中西區北門路一段101號10樓之一 06-223-5868
【台中】台中市東區大智路36號2樓 04-2229-8699 【高雄】高雄市新興區中山一路308號8樓 07-235-8996
各分班立案核准

