《資訊管理與資通安全》

一、何謂智慧代理人技術？（10分）請以供應鏈管理的實例說明企業如何應用智慧代理人。（15分）

試題評析	此題爲智慧型代理人名詞解釋，並搭配供應鏈管理說明應用。實際上在102年地方特考就已出現過智慧型代理人的名詞解釋，應屬熱點題目，相信充分準備之考生必感熟悉。若考生能掌握智慧型代理人之特點，並將之與供應鏈的需求（計畫、來源、製造、送貨與退貨）結合，則此題應可獲得不錯的分數。
考點命中	1.《高點・高上資訊管理講義》第二回，金乃傑編撰，頁46。 2.《高點・高上資訊管理講義》第二回，金乃傑編撰，頁16。

答：

(一)智慧型代理人（Intelligent Agent, IA）是具有某種學習能力或智慧的軟體程式，透過程式中的人工智慧技術，或使用資料探勘、專家系統等方式，使程式具有針對特定領域的決策能力，因此可以在不干擾使用者的情況下，幫使用者完成任務。智慧型代理人技術應用相當廣泛，如垃圾郵件分類，在使用者不參與的情況自動將信件歸類，提升使用者閱讀信件的效率；在金融業也常使用智慧型代理人，如設定程式在某股票升或降到某特定門檻時自動買入或賣出。

(二)在供應鏈管理領域中，智慧型代理人可以協助工廠升級爲「工業 4.0」的智慧工廠（Smart Factory）。在智慧工廠中，智慧型代理人可以根據天氣、公共運輸或內部生產狀態自動訂購原物料或調度生產線。如智慧型代理人根據颱風即將到來的天氣預報，自動安排供應鏈出貨時改用公路運輸而避免使用空運或鐵路降低延遲；在庫存的管理上，CR（Continuous Replenishment）或 VMI（Vendor Managed Inventory）現也都可以使用智慧型代理人完成，在 CR 系統中，可以在供應商使用智慧型代理人，在發現零售商庫存少於某門檻時自動派車出貨，或進一步安排生產、訂購原物料，減少供應鏈延遲；另一方面可以透過智慧型代理人蒐集網路上的顧客評價或競爭趨勢，用以調整商品以更符合使用者需求，使得生產與需求能有更緊密的連結。

二、「開放資料」（Open Data）因公共利益之必要，發布統計資料以供研究時，需將資料進行去識別化（De-identification）處理。請說明何謂「去識別化」？並解釋需去識別化的資料中，何謂「直接識別」資料與「間接識別」資料？（10分）請說明「K匿名框架」（k-Anonymity Framework）或「單元抑制」（Cell-suppression）其中任一種「去識別化」技術的實作方法。（15分）

試題評析	此題表面上爲開放資料，實際則爲個人資料保護法之題目延伸，需要對個資法中名詞如「直接識別」及「間接識別」有較深的認識才能作答。另外亦須結合資通安全中資料庫安全章節中的資料保護的實務方法，才能完整作答。程度不錯的考生應能在第一小題拿到不錯的分數，但第二小題則需要對名詞有更深的掌握才能得分。
考點命中	1.《高點・高上資訊管理講義》第三回，金乃傑編撰，頁99。 2.《高點・高上資通安全講義》第二回，金乃傑編撰，頁19。

答：

(一)去識別化（De-identification）：根據個資法第 2 條第 1 款可知，指透過一定程序的處理，移除識別資料與資料主體間之關聯，使個人資料不再具有直接或間接識別性。

1.直接識別資料指不需額外資訊或經由交互連結公開資訊中之其他資訊即可用以識別當事人之資料，如身分證號碼、指紋等。

2.間接識別資料（根據個資法施行細則第 3 條規定）指須與其他資料對照、組合、連結等，始能識別該特定之個人，個人必須是精準且確定地得以識別出特定個人，而非僅是利用專業知識推測可能爲某人之資

料，間接識別資料如郵遞區號、生日、年齡等。

(二)K 匿名框架（K-Anonymity）：用以判定在去識別化後是否揭露資料之限制條件。其中 K 是一個門檻，若揭露中的資料筆數有超過 K 組是一樣的內容，則可以揭露，因爲揭露後也無法直接判別該資料屬於何人；反之則必須隱藏。舉例而言，若揭露某公司之年薪資料，原始資料如下：

姓名	職稱	年薪
高尚上	總經理	500 萬
許證明	老師	200 萬
王自強	老師	200 萬
唐真	老師	200 萬
金乃潔	老師	200 萬
張幼中	老師	200 萬

假設將 K 設爲 3，則代表必須 3 筆資料一樣時才可以揭露，因此此資料表中總經理之薪水不能揭露，但是其他老師的薪水可以揭露，揭露結果如下：

姓名	職稱	年薪
OOO	老師	200 萬
OOO	老師	200 萬
OOO	老師	200 萬
OOO	老師	200 萬
OOO	老師	200 萬

(三)單元抑制（Cell Suppression）：用以避免去揭露識別化資料後，有心人士透過計算推估而使個人資料揭露之風險。單元抑制的重點在保護特定欄位之數值，考慮以下表格，假設不希望金同學之資訊管理與資通安全成績被揭露：

	資料結構	資料庫	資管資安	總分
王自強	100	80	60	240
唐真	60	100	90	250
金乃潔	80	90	O	270
總計	240	270	250	760

則以上保護仍可以從總分或總計計算出該成績爲 100 分，無法有效保護資料。因此在揭露時，可以考慮將唐同學的資管成績也隱藏、金同學的資料結構成績也隱藏，使得無法從總計推斷出金同學的資管成績，如下：

	資料結構	資料庫	資管資安	總分
王自強	100	80	60	240
唐真	60	100	O	250
金乃潔	80	O	O	270
總計	240	270	250	760

三、「國家資通安全會報」為明確規範政策機關（構）資通安全責任等級分級作業流程，透過資通安全管理，以防範潛在資安威脅，進而提升國家資安防護水準，訂定「政府機關（構）資通安全責任等級分級作業規定」。依據此作業規定，請說明A、B級單位在「稽核方式」、「業務持續運作演練」、「防護縱深」、「監控管理」及「安全性檢測」等五個項目的應辦理工作事項為何？（25分）

試題評析	此題完全出自資通安全會報內容之表格細項，完全屬於記憶型題目，缺乏鑑別力與難以檢驗人才解決問題之能力，有失高考水準。但相對的若能掌握表格內容，必能獲得滿分。
考點命中	1.《高點・高上資通安全講義》第一回，金乃傑編撰，頁75。 2.《高點・高上資通安全講義》第二回，金乃傑編撰，頁26、48-49。

答：

根據國家資通安全會報中之定義，A級單位如總統府、國安會、五院及勞保局健保署等保有全國性個人資料檔案之機關等；B級爲縣市政府、地戶政事務所等保有人民財產或個人檔案之機關。以下就其稽核方式、業務持續運作訓練、防護縱深、監控管理及安全性檢測之工作事項已表格說明之：

	A級機關	B級機關
稽核方式	每年至少2次內部稽核。	每年至少1次內部稽核。
業務持續運作	每年至少辦理1次核心資訊系統持續運作演練。	每2年至少辦理1次核心資訊系統持續運作演練。
防護縱深	防禦層次如下： 1.防毒、防火牆、郵件過濾裝置。 2.IDS/IPS、Web 應用程式防火牆。 3.APT 攻擊防禦。	防禦層次如下： 1.防毒、防火牆、郵件過濾裝置。 2.IDS/IPS 3.若機關具有對外服務之核心資訊系統，則需使用Web應用程式防火牆。
監控管理	104年年底前透過資安監控中心（Security Operation Center, SOC）監控。	105年年底前使用SOC監控。
安全性檢測	1.網站安全弱點檢測（每年至少辦理2次） 2.系統滲透測試（每年至少辦理1次） 3.資安健診（每年至少辦理1次）	1.網站安全弱點檢測（每年至少辦理1次） 2.系統滲透測試（每2年至少辦理1次） 3.資安健診（每2年至少辦理1次）

四、進階持續性威脅（Advanced Persistent Threat, APT）攻擊是一種有針對性的網路攻擊行動。請說明APT攻擊的流程，（15分）以及MIS管理人員應如何因應此種攻擊？（10分）

試題評析	與102年檢事官、103年調查局APT特色之題目不同，APT攻防應屬第一次出現，測驗考生對APT攻擊之流程及防禦方法掌握度。考試將流程比重增加，推斷是希望能更針對APT之特性做更具體之續寫，而避免流於一般性的資安防禦。此題若能有充分準備，要得滿分絕非難事。
考點命中	《高點・高上資通安全講義》第一回，金乃傑編撰，頁60，完全命中。

答：

(一)進階持續性威脅（Advanced Persistent Threat, APT）攻擊：爲一種綜合型的複雜網路攻擊。攻擊團隊以有組織的方式，透過長時間的蒐集資訊，並使用專業的攻擊技術，針對特定組織進行有系統的攻擊，以獲取目標大量敏感資訊，造成極大傷害。其攻擊流程如下：

1.初步的入侵：攻擊團隊透過釣魚網站或釣魚信件針對組織人員發送，騙取組織人員之帳號密碼或藉此在組織電腦中安裝木馬程式。

2.建立立足點：透過木馬程式在內部人員電腦中安裝監控程式，以掌握特定人員之電腦使用狀況，以待進一步攻擊。

3.取得管理者權限：透過先前釣魚取得之密碼或使用竊聽程式側錄之帳號密碼資訊，並配合已知系統漏洞破解目標電腦中系統管理者權限。當攻擊者能取得越高的權限，則攻擊的影響力越大。

4.內部偵查與平行擴散：當順利攻佔電腦後，便試圖增加攻陷電腦的範圍，例如找尋該主機附近的其他主機或伺服器，透過擴散取得更有破壞性的主機或資料資源。

5.持續監控並完成任務：此階段會根據任務不同而有不同，但通常都是以獲取重要資料爲主，並將資料匯出達到竊取機密的目的。

(二)MIS 管理人員可以使用 PDCA 的架構來制定 APT 攻擊的防護程序，並透過 ISO27002 的要求事項對組織中各安全點逐一檢查。但在執行面，可從觀察、偵測與阻擋三階段著手。說明如下：

1.觀察：透過蒐集伺服器、防火牆及路由器記錄檔（log），監控並記錄所有活動，以取得大量網路活動的樣本。此階段能蒐集到越多越詳細的資料，對下一階段的偵測分析能提供的幫助越大。

2.偵測：針對第一階段蒐集到的紀錄，透過 IDS 的偵測技術如誤用偵測或特徵偵測辨識潛在的攻擊事件。因爲 APT 的特性會長時間收集被害單位的資料，因此被害單位若有極高的警覺，也可以在此時收集攻擊活動的相關資料，以提升防禦或阻擋效果。

3.阻擋：阻擋 APT 攻擊，利用蒐集到的資料及對攻擊者的了解部屬防禦架構，並修改組織資訊安全政策以提升防禦完整性與人員訓練。具體而言，可以透過長時間對 APT 攻擊的了解，自我進行 APT 攻擊演練；並安排員工教育訓練，如使用測試的釣魚信件增進員工資訊安全意識；另外也必須使用「縱深防禦」的架構，建立防火牆、郵件過濾裝置等，使得釣魚信件不易入侵，也將蒐集到的資訊應用在 IPS、IDS 的部屬上，事先把可能攻擊的位置或行爲紀錄在這些防護裝置中，提升防護裝置的防禦力，惡意連線也能被及時攔截。

資訊安全專家建議，理想的資源配置是將30%的資源用來建立「觀察」與「偵測」機制，而70%的資源則是投入在APT「阻擋」機制上。