《資訊管理與資通安全概要》

試題評析	第一題：CRM之基礎概念，可參考講義內容作答。 第二題：Web 2.0之原則，屬於記憶題型。 第三題：可由知識與知識管理之定義切入。 第四題：認證與存取控制為資訊安全重要名詞，可參考講義內容作答；生物特徵認證的錯誤比率可由統計的Type I與Type II Error切入。
考點命中	第一題：《資訊管理與資通安全講義》第八回，張又中編撰，頁8~22。 第二題：《資訊管理與資通安全講義》第二回，張又中編撰，頁2-18~19。 第三題：《資訊管理與資通安全講義》第七回，張又中編撰，頁7-4、9與上課補充。 第四題：《資訊管理與資通安全講義》第三回，張又中編撰，頁3-5。

一、企業透過「顧客關係管理（CRM）系統」來蒐集與分析消費者的資訊，請條列並說明所需之資訊科技。（25分）

答：

(一)企業透過CRM來蒐集與分析消費者的資訊之步驟與所需之資訊科技如下：

1.顧客資料蒐集

所需資訊科技為POS、TPS、Internet、市調、客服中心、外部資料庫。

2.顧客資料儲存

所需資訊科技為資料庫(Database)、資料倉儲(Data Warehouse)、資料超市(Data Mart)。

3.顧客資料分析

所需資訊科技為SQL、OLAP、資料探勘(Data Mining)、企業智慧(Business Intelligence)。

二、Tim O'Reilly提出Web 2.0有「七項關鍵原則（Seven Principles of Web 2.0）」，請舉例並說明其中五項。（25分）

答：

(一)網站作為平台(The Web As Platform)

例如：Google，其以網站應用程式為基礎，將其遞送給使用者視為服務。顧客可以在其擁有的裝置上執行軟體，而不用轉至不同的平台。

(二)善用群體智慧(Harnessing Collective Intelligence)

例如：維基百科(Wikipedia)，匯集眾人的智慧，為強調自由內容、協同編輯以及多語言版本的網路百科全書，目前已收錄超過了3,000萬篇條目。

(三)資料是下一個Intel Inside(Data is the Next Intel Inside)

例如：第三方支付服務商Paypal，其利用電子郵件來標識用戶的身份以轉移資金，擁有超過1.8億的使用者，可為合法的身分識別資料庫並作為競爭優勢來源。

(四)終結軟體改版週期(End of the Software Release Cycle)

例如：Yahoo! Mail，使用者僅需連上Yahoo!的e-Mail平台進行使用，不用考量軟體的改版問題，其由Yahoo!負責進行持續的軟體改善。

(五)豐富的使用者經驗(Rich User Experiences)

以Facebook為例，其利用AJAX與DHTML技術開發許多的多媒體應用，例如：嵌入影音、照片標籤、打卡、群組訊息等，為使用者帶來更為豐富的體驗。

三、知識具有什麼特性？根據知識的特性，請列舉三種現代常見的工作型態，說明為何企業需要推行「知識管理（Knowledge Management）」的理由。（25分）

答：

知識是人類經過心智模式思考、處理過的資訊，經由學習、訓練、練習、模仿、經驗、資訊刺激與教育多重方式獲得。大部份為非結構化、內隱的，為主觀的詮釋、了解與判斷。是人類用來詮釋問題、解決問題、及制定

【版權所有，重製必究！】

決策及判斷的依據。
現代常見的工作型態有：
1.組織分散難以分享知識
2.人員流動造成知識流失
3.在相似的工作中重覆遭遇類似問題
知識管理乃是透過資訊與網路科技將原始資料整理成資訊，再將資訊加以篩選、萃取、提煉、利用、散播、分享，並且把使用過的知識再處理、再萃取、再提煉為更高階的知識，形成企業寶貴知識資產的過程。其增加了組織向環境學習的能力及吸收知識進入企業流程中，因而解決了上述三個問題。

四、「認證（Authentication）」與「存取控制」有何關係？何謂「生物特徵認（Biometric Authentication）」？使用生物特徵認證技術有那些型態的「錯誤比率」？錯誤比率與認證設備的「敏感度」有何關係（25分）

答：

(一)存取控制(Access Control)為限制資源存取的處理方式與程序，以保護系統資源不會被未經授權者存取或授權者本身的不當存取；認證(Authentication)為測試或檢查使用者所宣稱的身分是否屬實。認證為存取控制之基礎，確認使用者身分後制限其對資源的存取權限。

(二)生物特徵認證指利用數理統計方法對生物進行分析，現在多指對生物體本身的生物特徵來區分生物體個體的電腦技術，例如臉、語音、指紋、虹膜、視網膜、簽名等識別技術。

(三)使用生物特徵認證有兩種錯誤比率：原本合法的使用者在認證時卻被判斷為失敗，稱為Type I錯誤，所有合法使用者中出現Type I錯誤的比率稱為錯誤拒絕率(False Rejection Rate)；相對地，非法使用者被認證為通過，稱為Type II錯誤，所有非法使用者中出現Type II錯誤的比率稱為錯誤接受率(False Acceptance Rate)。

(四)當認證設備的敏感度越高，認證失敗越可能發生，錯誤拒絕率會相對提高；反之，如果降低敏感度，認證通過越可能發生，錯誤接受率就會相對提高。

【版權所有，重製必究！】