資通安全法律案例彙編

第 13 輯

行政院國家資通安全會報技術服務中心 編印

中華民國 105 年 12 月

序

隨著資通科技蓬勃發展，相關應用層面更是廣泛。無論民眾日常生活、企業發展或政府運作，處處可見資通科技之影響及其所帶來之效益。然而，在擘畫及推動資通科技發展之同時，對於背後所潛藏之資通安全風險亦不可輕視。「行政院國家資通安全會報技術服務中心」(以下簡稱技服中心)長期協助我國資通安全推動工作，自91年起即開始編撰「資通安全法律案例宣導彙編」，並於105年邁入第13輯。在第13輯的內容編排上，仍維持以「資訊保護」、「資訊公開」、「資訊監察」及「資訊應用」為四大主軸，收錄近期重要時事案例，透過法律概念剖析及資通安全管理(CNS 27001國家標準)觀念宣導之結合，提升讀者對於組織資通安全之重視與理解。

第13輯為增加相關案例素材之豐富度與實用性，收錄多則國外重要事件，例如美國政府機關委外廠商涉竊國家機密事件、記者提前洩漏紐西蘭儲備銀行官方利率調降訊息、香港某銀行網站遭駭客「分散式阻斷服務(DDoS)」攻擊並勒索比特幣事件等，並自我國法制角度出發，進行解析並提出相關資安管理與注意要領。此外，本輯亦針對國內重要事件，例如引起社會高度關切的一銀ATM盜領事件進行相關說明。

誠摯希望本輯案例彙編，能成為政府機關與社會大眾辦理資安法制與管理教育訓練之參考教材，並進一步建構良好的資安法律與管理觀念。

行政院國家資通安全會報技術服務中心

吳啟文主任 謹識

凡例

壹、本彙編案例依其內容及相關法律觀點之重要內容，分為以下類別：

一、資訊保護 (Security)

01 個人資料保護法

02 國家機密保護法

03 刑法

04 智慧財產權法

05 其他

二、資訊公開(Disclosure)

01 政府資訊公開法

三、資訊監察(Monitors)

01 通訊保障及監察法

四、資訊應用(Application)

01 電子簽章法

貳、本案例編碼共 8 位數字：編碼方式以上述四大類別之英文字首為第一碼，再加上年份三碼及上述各小類之編碼兩碼，最後兩碼為該小類中之第幾篇案例。例如：S1050101，即代表資訊保護類 105 年度之個人資料保護法第一則案例。

目次

壹、　資訊保護(Security)

一、個人資料保護法

類別：資訊保護【案號：S1050101】

肉搜匿名檢舉惹禍，公務員罰 4 萬

【焦點話題】

○市政府去(104)年 7 月收到「某局處工讀生穿著太清涼」檢舉信。該局處內部早已對工讀生的穿著議論紛紛，陳女收到案件資訊後，遂跟鄰座的黃女說「真的有人去投訴耶！」。黃女發現匿名檢舉的電子郵件信箱是局內公務信箱，好奇用該電子郵件在 GOOGLE 上進行搜尋，想找出檢舉人，事後並向其他同事提及此事。事件最後不但傳到當事人耳裡，且竟還有人向當事人求證，詢問「你是不是有寄信?」，匿名檢舉竟變成一樁公開事件。

陳女和黃女因涉及洩密遭法辦，檢方認為二人行為已構成刑法「公務員故意洩露國防以外秘密罪」，但考量都無前科，犯罪情節尚屬輕微且犯後深具悔意，因此予以緩起訴 1 年 6 月，但需支付國庫 3 萬元和 1 萬元緩起訴處分金，另需參加法治教育課程。

【資料來源：聯合新聞網，105/5/27】

【重點摘要】

1. 受理檢舉案件之該管公務員依法負有絕對保守政府機關機密之義務，即使是同事，也不能洩漏資訊。
2. 公務員負保密義務之公務機密，不限於特定形式，舉凡文書、圖畫、消息或物品，皆為受保護之客體。

【法律觀點】

公務員基於執行公務，往往會接觸機密資料，因此公務員服務法第 4 條[1]規範公務員負有絕對保守政府機關機密之義務，只要屬於政府的機密資料，不論是否為主管事務或是否在職，均不得洩漏。而公務機關常常接獲民眾的檢舉信件或陳情信，為避免檢舉人或陳情人挾怨報復或騷擾，是以行政程序法第 170 條亦規定若人民的陳情有保密必要者，受理機關應不予公開[2]。又依照○市政府及所屬各機關學校陳情檢舉人身分保密作業要點第 2 條第 4 點[3]，陳情檢舉案件內容應予保密者，收發人員不得談論或洩露案件內容。

如公務員洩漏檢舉內容時，因涉嫌違反前述保密依規定，恐違法刑法第 132 條洩漏國防以外機密罪[4]，將面臨處 3 年以下有期徒刑。在本案中，公務員陳女受理檢舉案件，檢舉人之身分與相關資訊，屬其應保密之資料，不得將資訊洩漏予他人，縱使洩漏的對象是同部門的同事亦不被允許；就黃女的部分，雖其並非受理該檢舉案的公務員，但是公務員保密義務，不限於「主管業務」，只要是該公務員負有保密義務之消息、文件，便不得向他人洩漏。另外，即使檢舉人為同一公務機關的同事，因檢舉人寄發檢舉信乃是基於一般人民的地位，循一般民眾之管道陳情，該管公務員不因此免除對於檢舉案件的保密義務。

【管理 Tips】

公務機關依法行政，但因具公務員身分，應時時謹言慎行，也因執行公務時往往可取得民眾特定資料，更應善盡保密義務，以免傷害公務員形象，甚或觸犯法律。

---

[1] 公務員服務法第 4 條：「公務員有絕對保守政府機關機密之義務，對於機密事件無論是否主管事務，均不得洩漏，退職後亦同。」

[2] 行政程序法第 170 條：「行政機關對人民之陳情，應訂定作業規定，指派人員迅速、確實處理之。人民之陳情有保密必要者，受理機關處理時，應不予公開。」

[3] ○市政府及所屬各機關學校陳情檢舉人身分保密作業要點第 2 條第 4 點：「陳情檢舉案件內容應予保密者，收發人員登錄之內容不得顯示陳情檢舉人姓名或身分辨識資料，並不得談論或洩露案件內容。」

[4] 刑法第 132 條第 1 項：「公務員洩漏或交付關於中華民國國防以外應秘密之文書、圖畫、消息或物品者，處 3 年以下有期徒刑。」

為建立正確之資訊安全管理及個人資料保護規範，政府機關應定期進行教育訓練及宣導，並且要求全員參與，依不同業務性質之單位，講解如何落實日常作業管理。如有違反資訊安全規範者，應有適當之方法要求改善或予以合理之懲處，方能使全體同仁建立一致之資訊安全及個人資料保護觀念。

【相關標準】

ISO 27001：2013(CNS 27001)

A.7.2.1 管理階層責任

管理階層應要求所有員工及承包者，依組織所建立政策及程序施行資訊安全事宜。

A.7.2.2 資訊安全認知、教育及訓練

組織所有員工及相關之承包者，均應接受與其工作職能相關的組織政策及程序之適切認知、教育及訓練，並定期更新。

A.7.2.3 懲處過程

應具備正式及已傳達之懲處過程，以對違反資訊安全之員工採取行動。

A.18.1.4 個人可識別資訊之隱私及保護

應依適用之相關法令、法規中之要求，以確保個人可識別資訊之隱私及保護。

類別：資訊保護【案號：S1050102】

出賣客戶，徵信公司副總被起訴

【焦點話題】

一名在高雄經營 A 整形診所的邱姓男子，視 B 診所為競爭對手，乃委託某徵信公司副總蔡女至 B 診所蒐證，調查競爭診所涉僱用密醫的不利證據。後來邱男又因夫妻不合，便蒐集妻子家人的個資和公司資料交給蔡女，委託她調查對前妻不利的證據。不料邱男與蔡女發生口角，蔡女在不滿之下，竟聯絡 B 診所人員，洩漏受邱男委託調查的內容。

另外，蔡女之後再跟邱男前妻聯繫，將邱男委託調查的資料交付邱男前妻，前妻得知後控告邱男，邱男認為被出賣，對蔡女提出告訴。某地檢署因而認定蔡女涉犯洩密及背信罪將她起訴。蔡女辯稱因對邱男不滿才如此做，她知道不應該，但是她已處理完成相關受託事務，並無違背職務。檢方指出，蔡女洩漏受託內容，損害邱男利益，以洩漏工商秘密和背信等罪嫌起訴蔡女。

【資料來源：蘋果日報，105/5/26】

【重點摘要】

1.組織對於個人資料之蒐集，除有得免告知之事由外，均應踐行告知義務，並符合得蒐集個資之法定事由。

2.從業人員受他人委託處理事務卻洩漏資訊，可能有洩漏工商秘密和背信罪等刑事責任。

【法律觀點】

徵信業之業務性質特殊，常常接受客戶委託調查他人資訊，因此在民國(下同)99 年 5 月個人資料保護法(以下簡稱個資法)修正前，原屬於應適用舊個資法的特定行業之一，經濟部並頒布有「徵信業電腦處理個人資料辦法」作為規範。在個資法於 99 年 5 月修正後，其適用主體不再以特定產業為限，

上開辦法雖經廢止，但徵信業蒐集、處理或利用他人個人資料，仍應適用個資法規範；此規定在個資法 104 年年底再次修正時，仍然維持。因此，依個資法第 8 條及第 9 條規定，徵信業者對於他人個人資料之直接或間接蒐集，除非有法定免為告知之事由外，均應於直接蒐集之蒐集前或間接蒐集之處理或利用前，向當事人踐行告知義務[1]，並且必須合乎同法第 19 條第 1 項列舉之法定事由，方能蒐集個人資訊[2]。其意圖為自己或第三人不法之利益而違法蒐集、處理或利用者，將可能處 5 年以下有期徒刑，得併科新臺幣 100 萬元以下罰金[3]。除了刑事責任外，依同法第 29 條[4]規定，亦可能遭到被害人請求損害賠償。

---

[1] 個人資料保護法第 8 條：「公務機關或非公務機關依第 15 條或第 19 條規定向當事人蒐集個人資料時，應明確告知當事人下列事項：一、公務機關或非公務機關名稱。二、蒐集之目的。三、個人資料之類別。四、個人資料利用之期間、地區、對象及方式。五、當事人依第三條規定得行使之權利及方式。六、當事人得自由選擇提供個人資料時，不提供將對其權益之影響。有下列情形之一者，得免為前項之告知：一、依法律規定得免告知。二、個人資料之蒐集係公務機關執行法定職務或非公務機關履行法定義務所必要。三、告知將妨害公務機關執行法定職務。四、告知將妨害公共利益。五、當事人明知應告知之內容。六、個人資料之蒐集非基於營利之目的，且對當事人顯無不利之影響。」第 9 條：「公務機關或非公務機關依第 15 條或第 19 條規定蒐集非由當事人提供之個人資料，應於處理或利用前，向當事人告知個人資料來源及前條第 1 項第 1 款至第 5 款所列事項。有下列情形之一者，得免為前項之告知：一、有前條第 2 項所列各款情形之一。二、當事人自行公開或其他已合法公開之個人資料。三、不能向當事人或其法定代理人為告知。四、基於公共利益為統計或學術研究之目的而有必要，且該資料須經提供者處理後或蒐集者依其揭露方式，無從識別特定當事人者為限。五、大眾傳播業者基於新聞報導之公益目的而蒐集個人資料。第一項之告知，得於首次對當事人為利用時併同為之。」

[2] 個人資料保護法第 19 條第 1 項：「非公務機關對個人資料之蒐集或處理，除第 6 條第 1 一項所規定資料外，應有特定目的，並符合下列情形之一者：一、法律明文規定。二、與當事人有契約或類似契約之關係，且已採取適當之安全措施。三、當事人自行公開或其他已合法公開之個人資料。四、學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。五、經當事人同意。六、為增進公共利益所必要。七、個人資料取自於一般可得之來源。但當事人對該資料之禁止處理或利用，顯有更值得保護之重大利益者，不在此限。八、對當事人權益無侵害。」

[3] 個人資料保護法第 41 條：「意圖為自己或第三人不法之利益或損害他人之利益，而違反第 6 條第 1 項、第 15 條、第 16 條、第 19 條、第 20 條第 1 項規定，或中央目的事業主管機關依第 21 條限制國際傳輸之命令或處分，足生損害於他人者，處 5 年以下有期徒刑，得併科新臺幣 100 萬元以下罰金。」

[4] 個人資料保護法第 29 條：「非公務機關違反本法規定，致個人資料遭不法蒐集、處理、利用或其他侵害當事人權利者，負損害賠償責任。但能證明其無故意或過失者，不在此限……。」

徵信業者在執行職務時，往往會接觸他人之個人資料或營業秘密，且多與客戶間訂有保密契約，因而徵信業者對客戶所委託徵信之案件資料，負有保密義務。而案件資料如涉及可用於生產、銷售或經營之資訊，且具有一定經濟價值時，則可能為營業秘密[5]，受營業秘密法之保護。本案蔡女為徵信業之從業人員，其所洩漏之資料中包括其客戶邱男委託調查之 B 診所及邱男前妻公司之資料，有涉及工商秘密或營業秘密的可能，蔡女可能因此涉犯刑法第 317 條妨害工商秘密罪。如果蔡女係基於損害營業秘密所有人之利益而洩漏上開資料時，尚可能構成營業秘密法第 13-1 條第 1 項第 2 款的洩漏營業秘密罪[6]。

另外，為他人處理事務，意圖損害本人之利益，違背其任務，致生損害於本人之財產或其他利益者，成立刑法第 342 條[7]的背信罪。本案蔡女受邱男委託調查特定人，屬於受他人委任處理事務[8]，其將邱男委託之內容洩漏予受調查對象，即使蔡女盡責調查，仍因為洩漏委託資料而屬於違背任務，致使邱男受其前妻控告，因此受有不利益，亦可能成立刑法第 342 條的背信罪。

【管理 Tips】

[5] 營業秘密法第 2 條：「本法所稱營業秘密，係指方法、技術、製程、配方、程式、設計或其他可用於生產、銷售或經營之資訊，而符合左列要件者：一、非一般涉及該類資訊之人所知者。二、因其秘密性而具有實際或潛在之經濟價值者。三、所有人已採取合理之保密措施者。」

[6] 刑法第 317 條：「依法令或契約有守因業務知悉或持有工商秘密之義務，而無故洩漏之者，處 1 年以下有期徒刑、拘役或 1,000 元以下罰金。」營業秘密法第 13-1 條第 1 項：「意圖為自己或第三人不法之利益，或損害營業秘密所有人之利益，而有下列情形之一，處 5 年以下有期徒刑或拘役，得併科新臺幣 100 萬元以上 1,000 萬元以下罰金：一、以竊取、侵占、詐術、脅迫、擅自重製或其他不正方法而取得營業秘密，或取得後進而使用、洩漏者。二、知悉或持有營業秘密，未經授權或逾越授權範圍而重製、使用或洩漏該營業秘密者。三、持有營業秘密，經營業秘密所有人告知應刪除、銷毀後，不為刪除、銷毀或隱匿該營業秘密者。四、明知他人知悉或持有之營業秘密有前三款所定情形，而取得、使用或洩漏者。」

[7] 刑法第 342 條：「為他人處理事務，意圖為自己或第三人不法之利益，或損害本人之利益，而為違背其任務之行為，致生損害於本人之財產或其他利益者，處 5 年以下有期徒刑、拘役或科或併科 50 萬元以下罰金。前項之未遂犯罰之。」

[8] 最高法院 49 年台上字第 1530 號刑事判例：「刑法第 342 條之背信罪，須以為他人處理事務為前提，所謂為他人云者，係指受他人委任，而為其處理事務而言。」

有關組織之資訊保護或管理，有兩個地方值得關注。其一，徵信業者蔡女因個人行為違反合約條款，隨意洩漏委託調查之事務，嚴重傷及他人隱私與聲譽。即使在處理完受委託事務後，依然須遵守合約內容，不得擅自公開受委託之資訊。其二，徵信公司副總竟將公司機密文件擅自攜出與利用，此行為突顯該公司對於公司機密文件控管與保存有嚴重的缺失，以致於讓機密文件有外洩之風險。

為因應以上問題，組織必須制定正確的資訊安全管理及個人資料保護規範，除了應定期做員工教育訓練與資訊安全政策宣導外，其所擁有之機密文件應做好資訊分級、標示與處置，依據不同機密等級規劃文件標示與保護方式。此資訊安全規劃應定期要求全體員工參與，建立一致性之資訊安全及個人資料保護觀念。

【相關標準】

ISO 27001：2013(CNS 27001)

A.7.2.1 管理階層責任

管理階層應要求所有員工及承包者，依組織所建立政策及程序施行資訊安全事宜。

A.7.2.2 資訊安全認知、教育及訓練

組織所有員工及相關之承包者，均應接受與其工作職能相關的組織政策及程序之適切認知、教育及訓練，並定期更新。

A.7.2.3 懲處過程

應具備正式及已傳達之懲處過程，以對違反資訊安全之員工採取行動。

A.8.2.1 資訊之分級

資訊應依法律要求、價值、重要性及對未經授權揭露或修改之敏感性分級。

A.8.2.2 資訊之標示

應依組織所採用之資訊分級方案，發展及實作一套適切的資訊標示程序。

A.8.2.3 資產之處置

應依組織所採用之資訊分級方案，發展及實作處置資產之程序。

A.18.1.1 適用之法規及契約的要求事項之識別

對每個資訊系統及組織，應明確識別、文件化及保持更新所有相關法律、法令、法規及契約要求事項，以及組織為符合此等要求之作法。

A.18.1.4 個人可識別資訊之隱私及保護

應依適用之相關法令、法規中之要求，以確保個人可識別資訊之隱私及保護。

類別：資訊保護【案號：S1050103】

空軍基地雪隧 驚現寶可夢

【焦點話題】

「精靈寶可夢 GO」成了全民運動，只要有精靈聚集地方，就會有玩家低頭抓寶，傳出國道 5 號頭城端雪隧前的蔣渭水紀念碑是寶可夢道場，雪隧彩繪也是驛站，讓玩家蠢蠢欲動，甚至連戒備森嚴的花蓮空軍基地也出現精靈妙蛙草。對於抓寶可能違規觸法，交通部長說，政府對此事應對太慢，將發函遊戲商要求撤除設在國道、鐵道、運輸場站、航空站等地的熱點和精靈，以免引發安全問題。

高公局表示，蔣渭水紀念碑是警方經常駐點處，若有人邊開車邊抓寶可開罰 3 千元，臨時停車抓寶開罰 3 千到 6 千元，強調將要求遊戲商勿將國道和服務區休息站列為熱點；航港局也表示，港區和港口尚未針對抓寶有相關規定，已去函船舶公司和地方政府，要求研究管理措施。

對於營區內有寶可夢，國防部通資室資通安全處長昨表示，國軍官兵在營區內不能使用智慧手機，「營區有怪也無法抓！」至於本周六花蓮空軍基地開放營區，民眾可攜智慧型手機進入，並在展覽區使用，「屆時大家可試試營區內有沒有寶可夢可抓。」

【資料來源：蘋果日報，105/8/10】

【重點摘要】

1. 玩家進行擴增實境遊戲前，對於遊戲將會記錄玩家位置、拍攝沿途實境等功能，涉及蒐集玩家行動位址，遊戲業者於蒐集玩家個人資料前原則上應事先踐行告知。

2. 寶可夢玩家在進行遊戲時，常會進入各機關或場所的管理範圍內進行「抓寶」，必須注意該行為是否違反各機關有關安全管制之規定。

【法律觀點】

時下流行的「寶可夢」，乃是一款擴增實境遊戲。利用「擴增實境(Augmented Reality，簡稱 AR)，是一種即時、實地計算攝影機影像之位置及角度，並加上相應圖像的技術，此技術的目標是在螢幕上把虛擬世界套在現實世界並進行互動。因此，在進行擴增實境遊戲時，無可避免地會記錄玩家的位置與路線，並且會將玩家活動周遭街道住家之實境拍攝下來。亦即，寶可夢遊戲業者將會蒐集玩家包括社會活動之個人資料，而有個人資料保護法的適用[9](以下簡稱個資法)。

依個資法第 8 條及第 9 條規定，對於他人個人資料之直接或間接蒐集，除非有法定免為告知之事由外，應於直接蒐集之蒐集前或間接蒐集之處理或利用前，向當事人踐行告知義務[10]；再者，遊戲業者蒐集玩家個資必須具備同法第 19 條第 1 項列舉之法定事由之一，方能蒐集個人資訊[11]；且對於個

[9] 個人資料保護法第 2 條第 1 款、第 2 款：「本法用詞，定義如下：一、個人資料：指自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料。二、個人資料檔案：指依系統建立而得以自動化機器或其他非自動化方式檢索、整理之個人資料之集合。」

[10] 個人資料保護法第 8 條第 1 項：「公務機關或非公務機關依第 15 條或第 19 條規定向當事人蒐集個人資料時，應明確告知當事人下列事項：一、公務機關或非公務機關名稱。二、蒐集之目的。三、個人資料之類別。四、個人資料利用之期間、地區、對象及方式。五、當事人依第三條規定得行使之權利及方式。」第 9 條第 1 項：「公務機關或非公務機關依第 15 條或第 19 條規定蒐集非由當事人提供之個人資料，應於處理或利用前，向當事人告知個人資料來源及前條第 1 項第 1 款至第 5 款所列事項。有下列情形之一者，得免為前項之告知：一、有前條第 2 項所列各款情形之一。二、當事人自行公開或其他已合法公開之個人資料。三、不能向當事人或其法定代理人為告知。四、基於公共利益為統計或學術研究之目的而有必要，且該資料須經提供者處理後或蒐集者依其揭露方式，無從識別特定當事人者為限。五、大眾傳播業者基於新聞報導之公益目的而蒐集個人資料。六、當事人得自由選擇提供個人資料時，不提供將對其權益之影響。」

[11] 個人資料保護法第19條第1項：「非公務機關對個人資料之蒐集或處理，除第6條第1項所規定資料外，應有特定目的，並符合下列情形之一者：一、法律明文規定。二、與當事人有契約或類似契約之關係，且已採取適當之安全措施。三、當事人自行公開或其他已合法公開之個人資料。四、學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。五、經當事人同意。六、為增進公共利益所必要。七、個人資料取自於一般可得之來源。但當事人對該資料之禁止處理或利用，顯有更值得保護之重大利益者，不在此限。八、對當事人權益無侵

資之利用，原則上應於蒐集之特定目的必要範圍內為之[12]。其意圖為自己或第三人不法之利益而違法蒐集、處理或利用者，將可能處 5 年以下有期徒刑，得併科新臺幣 100 萬元以下罰金[13]。故像寶可夢等擴增實境遊戲，遊戲業者在開始記錄玩家路線、拍攝實境或利用蒐集之資料前，必須事先依法對遊戲玩家踐行告知義務，並且其利用必須是在蒐集之特定目的必要範圍內，否則即有上述法律責任。

另外，寶可夢玩家在進行遊戲時，常會進入各機關或場所的管理範圍內進行「抓寶」，必須注意該行為是否違反各機關有關安全管制與行動設備使用之規定。例如該地點是否為「要塞堡壘或要塞堡壘地帶」，這可能影響玩家進行實境遊戲時涉及拍攝行為是否違法。所謂「要塞堡壘」指國防上所必須控制與確保之戰術要點、軍港及軍用飛機場；而要塞堡壘及其周圍之必要區域 (含水域)，稱為要塞堡壘地帶，由國防部核定並公告之[14]。而在堡壘要塞內，非受有國防部之特別命令，不得攝影[15]，違反者不論故意或過失，可能構成要塞堡壘地帶法第 9 條第 1 項或第 2 項，最高可處 7 年有期徒刑[16]。因此，玩家在進行實境遊戲時，應注意在特定機關場所週遭活動，有無安全管制上之特別規定，以避免不慎觸法。

【管理 Tips】

害。」

[12] 個人資料保護法第 20 條第 1 項前段：「非公務機關對個人資料之利用，除第 6 條第 1 項所規定資料外，應於蒐集之特定目的必要範圍內為之。」

[13] 個人資料保護法第 41 條：「意圖為自己或第三人不法之利益或損害他人之利益，而違反第 6 條第 1 項、第 15 條、第 16 條、第 19 條、第 20 條第 1 項規定，或中央目的事業主管機關依第 21 條限制國際傳輸之命令或處分，足生損害於他人者，處 5 年以下有期徒刑，得併科新臺幣 100 萬元以下罰金。」

[14] 要塞堡壘地帶法第 3 條第 2 項：「...各區及其與軍港、要港、海軍防禦建築物、飛機場、空軍防禦建築物等相關連之區域，均由國防部核定並公告之。」

[15] 參照要塞堡壘地帶法第 4 條第 1 款：「第一區內之禁止及限制事項：一、非受有國防部之特別命令，不得為測量、攝影、描繪、記述及其他關於軍事上之偵察事項」、同法第 5 條第第 1 款：「第二區內之禁止及限制事項：一、非經要塞司令之許可，不得為測量、攝影、描繪、記述及其他關於軍事上偵察事項。」

[16] 要塞堡壘地帶法第 9 條：「犯第 4 條第 1 款或第 5 條第 1 款之規定者，處 1 年以上、7 年以下有期徒刑。因過失犯前項之規定者，處 1 年以下有期徒刑、拘役或 100 元以下罰金。」

寶可夢為一種「擴增實境」遊戲，結合虛擬資訊擴增到現實空間中的技術。藉由攝影機的辨識技術、電腦程式與 GPS 定位的結合，所發展而成的遊戲。

此遊戲涉及到攝影與 GPS 功能。如使用不當，容易破壞機密設施的隱蔽性，造成保密場所曝光。使得重要區域成為攻擊目標的風險性增高。應以保護實體安全的原則，界定好保護區域，以防護場所內的資產安全。

為防範上述情況，應以迅速處理的態度，將危害的風險因素去除。積極防範外部所造成的威脅，需定期的審查風險因子以保護實體設施的安全。

【相關標準】

ISO 27001：2013(CNS 27001)

A.11.1.1 實體安全周界

宜定義及使用安全周界，以保護收容機敏或重要資訊及資訊處理設施之區域。

A.11.1.4 防範外部及環境威脅

應設計並施行實體保護，以防範天然災害、惡意攻擊或事故。

類別：資訊保護【案號：S1050104】

電商平台坦承兩年前遭駭客入侵，至少 5 億用戶帳號被竊

【焦點話題】

2016 年 8 月某電商網站傳出曾有 2 億用戶資料被盜，並流入黑市販售。美國媒體 Recode 報導實際外洩情形更為嚴重，某電商網站隨後於證實該公司於 2014 年遭駭入，至少 5 億美國用戶姓名、電子郵件信箱、電話、加密後的密碼及生日遭到竊取，另部份用戶的安全問題與答案亦有外流，但遭竊資料未涵蓋銀行帳號或信用卡資訊等。某電商網站表示已取消部分用戶以答覆安全問題登入的方式，並積極配合執法單位進行調查，該公司相信這樁駭客行動背後有國家力量的支持，同時呼籲 2014 年以後未變更密碼的用戶儘速更改密碼。

【資料來源：iThome，105/9/23】

【重點摘要】

1. 電商網站維護會員資料庫安全性，得採取的技術上措施可能包含主機架設防火牆、建立異常偵測機制或定期進行弱點掃描等。
2. 因應電商網站個資外洩規模與頻率迅速攀升，我國已由主管機關積極透過個資法上行政檢查措施，並配合相關改善輔導機制，督促業者落實相關義務，以從資訊安全角度根本降低外洩風險。

【法律觀點】

依我國個人資料保護法(簡稱個資法)規定，公務機關或非公務機關發生個資事故後，應查明後以適當方式通知當事人，通知內容應包含個人資料被侵害之事實，以及已採取之因應措施[17]。本案例中該電商網站雖為外國公司，但

[17] 個資法第 12 條：「公務機關或非公務機關違反本法規定，致個人資料被竊取、洩漏、竄改或其他侵害

事故發生後，亦取消部分用戶安全問答登入機制，且呼籲用戶更改密碼作為補救措施，以減少損害擴大。又，本案例之事件並非單一個案，隨著近來電商網站個資外洩規模迅速攀升，資訊安全議題更加引發社會大眾重視。企業依個資法須採取組織上與技術上適當安全維護措施，以妥善維護個資安全。對於電商網站維護會員資料庫安全性，得採取的技術上措施可能包含主機架設防火牆、建立異常偵測機制或定期進行弱點掃描等。本次事件中，某電商網站並非自行發現遭到駭客入侵，而是個資外洩長達兩年且傳出黑市交易傳聞後，啟動內部調查才證實確實發生個資事故，此亦突顯出駭客手法趨於隱蔽，致企業難以察覺或防範。

考量到個資外洩導致網路詐騙猖獗，進而造成民眾財產損失，經濟部商業司為促使業者正視問題並加強改進，已於 2015 年 4 月邀集相關部會與專家，共同組成「網際網路零售商品之公司行號個資保護行政檢查小組」，將發生重大個資外洩或突發性嚴重個資外洩業者列為行政檢查對象，依個資法辦理行政檢查[18]，以強化對於網路零售平台個資保護情形之監督，若業者經通知改善後仍未改善，則主管機關可按次依個資法處新臺幣(下同)2 萬至 20 萬元罰鍰[19]。故我國針對此類電子商務網站，已由主管機關積極透過行政檢查並配合相關輔導措施，督促業者落實相關義務，以從資訊安全角度根本降低外洩風險。

【管理 Tips】

者，應查明後以適當方式通知當事人」、本法施行細則第 22 條第 2 項：「依本法第 12 條規定通知當事人，其內容應包括個人資料被侵害之事實及已採取之因應措施」。

[18] 個資法第 22 條第 1 項：「中央目的事業主管機關或直轄市、縣（市）政府為執行資料檔案安全維護、業務終止資料處理方法、國際傳輸限制或其他例行性業務檢查而認有必要或有違反本法規定之虞時，得派員攜帶執行職務證明文件，進入檢查，並得命相關人員為必要之說明、配合措施或提供相關證明資料。」

[19] 個資法第 48 條：「非公務機關有下列情事之一者，由中央目的事業主管機關或直轄市、縣（市）政府限期改正，屆期未改正者，按次處新臺幣 2 萬元以上 20 萬元以下罰鍰：四、違反第 27 條第 1 項或未依第 2 項訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法。」、另參同法第 21 條：「非公務機關有違反本法規定之情事者，中央目的事業主管機關或直轄市、縣（市）政府除依本法規定裁處罰鍰外，並得為下列處分：一、禁止蒐集、處理或利用個人資料。二、命令刪除經處理之個人資料檔案。三、沒入或命銷燬違法蒐集之個人資料。四、公布非公務機關之違法情形，及其姓名或名稱與負責人。」

首先，組織是持續曝露在資訊安全風險的環境威脅下運作的。公司應當定期識別出相關技術脆弱性，並建立與支援脆弱性管理所需之資訊，包含脆弱性監視、風險評鑑、修補程式、資產追蹤及所有必要之協調責任，以降低組織受到的資訊安全風險的威脅。應定期審查組織內資訊系統的脆弱性威脅，包含運用滲透測試、弱點掃描及人工檢查等方式，檢驗運作之系統的安全性，並隨時關注新技術、新型病毒及駭客模式，以隨時更新資訊安全知識，讓組織保持受防護的狀態。

再者，組織在面對資訊安全事故時，需建立起管理責任及程序，以確保對事故的發生可以迅速、有效及有序的回應。為此，需規劃適當的通報管道、記錄事件發生的狀態及原因、對事故發生時的緊急回應以及從資訊安全事件中組織的成長與學習等等。以上皆為面對事故發生時的應變措施，這些程序都需事先做規劃，並定期的做演練，以避免實際發生時帶來負面的影響。

【相關標準】

ISO/IEC 27001：2013(CNS 27001)

A.12.6.1 技術脆弱性管理

宜及時取得關於使用中之資訊系統的技術脆弱性資訊，並宜評估組織對此等脆弱性之暴露，且宜採取適當措施以因應相關風險。

A.16.1 資訊安全事故及改善之管理

確保對資訊安全事故之管理的一致及有效作法，包括對安全事件及弱點之傳遞。

A.18.2.3 技術遵循性審查

應定期審查資訊系統對組織之資訊安全政策及標準的遵循性。

二、國家機密保護法

類別：資訊保護【案號：S1050201】

美國政府機密資料上雲端

【焦點話題】

美國聯邦風險與授權管理計畫(Federal Risk and Authorization Management Program，下稱 FedRAMP)宣布微軟 Azure GovCloud、亞馬遜 AWS GovCloud 及政府雲服務公司 CSRA 的政府雲服務 ARC-P IaaS 三項政府雲服務，取得美國聯邦政府高度機密資料的安全認證(High Baseline Requirements)。

FedRAMP 總監表示，在雲端服務公司尚未取得 FedRAMP 高度機密資料認證之前，美國聯邦政府僅能夠將低度至中等風險影響級別的資料上傳至雲端，但訂定高度機密資料的安全認證標準之後，已經有三家公司分別取得認證，使得聯邦政府能夠開始將政府內部高度機密資料搬上雲端，目前政府內部資料有 20%屬於高度機密資料，包含國民健康資料與政府財政資料等。

【資料來源：iThome，105/6/28】

【重點摘要】

1. 我國就機密文書區分為國家機密文書與一般公務機密文書，機關對於經核定為機密之公務文書須依機密檔案管理辦法妥為管理。
2. 我國得考量針對機密等級不同之政府資訊，建立雲端服務認證標準與管理措施，以利機關兼顧行動化、雲端化服務趨勢及資訊安全。

【法律觀點】

我國就機密文書區分為國家機密文書與一般公務機密文書，前者係依國家機

密保護法核定，後者由各機關依權責核定。機關對於經核定為機密之公務文書須依機密檔案管理辦法妥為管理，例如依機密等級分別保管並限制人員進出機密文書存放場所等；另，依行政院及所屬各機關資訊安全管理要點之規定，機密性資料與文件原則上不得以電子郵件或其他電子方式傳送[1]。因此，我國現前對於機密文書管理方式主要仍以實體紙本為考量，且對於如何確保檔案在網路傳送或存放作業的完整性與機敏性，欠缺可供機關參考遵循之管理措施，尤其機密資料若上傳至雲端平台，就存取權限設定、存取紀錄異常追蹤及資料刪除等更為重要管理議題。

然而，在數位資訊時代下，政府機關業務處理與服務傳遞日益仰賴強大的運算能力，而雲端方案能夠提供更靈活、快速、隨時隨地存取且不受空間設備限制的資料處理能力，有助於降低各機關自行建置資訊系統、重複投入成本之耗費。但因政府資訊基礎建設通常基於機密保護與檔案紀錄保存等考量，通常不易採納雲端方案，因此本案中，美國總務署、國家標準技術局、國土安全部及國防部等部會，與雲端服務、網路安全專家及民間產業共同合作，推動 FedRAMP 此政府計畫，旨在針對雲端產品暨服務建立安全評估、授權及持續監測的標準化作業，以利政府機關得使用通過該標準認證之雲端服務或產品，管理不同機密等級的政府資料，並依該標準要求服務或產品供應商確實管理並配合監督。

鑒於電子化政府服務的拓展與深化，某程度有賴跨部門資料交換而達到更精確的服務傳遞，故以政府機關間採用雲端方案作為資源共享平台，亦屬政府資訊應用趨勢。因此我國未來得參考 FedRAMP，針對機密等級不同之政府資訊，建立雲端服務認證標準與管理措施，以利機關兼顧行動化、雲端化服務趨勢與資訊安全。

[1] 行政院及所屬各機關資訊安全管理要點第 27 條：「各機關應訂定電子郵件使用規定，機密性資料及文件，不得以電子郵件或其他電子方式傳送。機密性資料以外之敏感性資料及文件，如有電子傳送之需要，各機關應視需要以適當之加密或電子簽章等安全技術處理。機關業務性質特殊，須利用電子郵件或其他電子方式傳送機密性資料及文件者，得採用權責主管機關認可之加密或電子簽章等安全技術處理。」

【管理 Tips】

資訊安全問題一直是政府使用雲端服務最大的限制，政府機關在進行資料存取時，需依照不同的資產進行分級，並依據各級別之資產進行處置。此外，在規劃雲端服務時，需考量執行雲端服務之供應商。挑選的供應商需簽署適切之合約，以符合資訊安全管理要求之規範，妥善執行資訊與個人資料的保護。

在 FedRAMP 高度機密資料安全認證的先例下，可仿效此安全認證原則，強化網路服務安全及存取限制，將資料控管與保存做好資訊安全管理規範，進一步打造更加完善且嚴密的政府雲。此外，包括雲端對於個人隱私資料的產生、儲存、管理、通知、消除、加密、傳輸等處理，以及公有雲維護之建置與維運上的安全控制措施，也都是可以進一步留意的細節。

【相關標準】

ISO/IEC 27001：2013(NS 27001)

A.8.2.1 資訊之分級

資訊應依法律要求、價值、重要性及對未經授權揭露或修改之敏感性分級。

A.8.2.3 資產之處置

應依組織所採用之資訊分級方案，發展及實作處置資產之程序。

A.9.1.2 對網路及網路服務之存取

應僅提供予使用者存取其已被特定授權使用之網路及網路服務。

A.9.4.1 資料存取限制

應依存取控制政策，限制對資訊及應用系統功能之存取。

A.13.1.2 網路服務之安全

應識別所有網路服務之安全機制、服務等級及管理要求事項，並應被納入

網路服務協議中，不論此等服務係由內部或委外提供。

A.15.1.2 於供應者協議中闡明安全性

應與每個可能存取、處理、儲存或傳達資訊，或提供 IT 基礎建設組件資訊之供應者，建立及議定所有相關資訊安全要求事項。

類別：資訊保護【案號：S1050202】

「魏男公然販售機密文件」軍方澄清：已視同解密

【焦點話題】

依據報載，魏姓民眾於民國(下同)104 年 9 月在國內某知名購物網站購得三份 50、60 年代戒嚴時期之共諜案文獻，之後在拍賣網頁上張貼訊息表示想要轉賣。國防部於 105 年 2 月接獲訊息發現可能有民眾在網頁進行「機密文件」販賣後，隨即通知相關單位展開犯罪調查。當時由於調查單位涉嫌透過釣魚方式進行誘捕，並以要求簽署「同意搜索」文件方式直接進入魏姓民眾家中進行搜索，因而扣得上開文件，此舉引發國內輿論嘩然。本案發生後，政府機密文件之保管及銷毀作業，引發各界廣泛討論。

某部會表示，魏姓民眾所取得的這 3 份歷史文獻，依據當時之國家機密保護辦法，有 2 件被列為機密等級，1 件則列為密等。不過，在國家機密保護法施行後，依據本法規定在施行後 2 年未依權責重新核定者，即予解密。因此，這批年代久遠之文件應屬於待銷毀文件，卻不慎在銷毀過程中對外流出，因而引發喧然大波。而對於類似文件如何處理，相關單位建議民眾最好交由政府處理，避免非法持有、私藏，或是公開販售政府機密文件所以發之觸法疑慮。

【資料來源：蘋果日報，105/3/7】

【重點摘要】

1.公務機關應就機密文件之性質及內容設定機密等級及保密期限，並在收發、傳遞、使用、持有、保管、複製及移交等環節進行分級管理。

2.機密文件逾保密期限時，可予以解密並進行銷毀，此時仍應加以控管以免不慎外流。

【法律觀點】

為了確保國家安全利益，我國於 92 年 2 月 6 日制定國家機密保護法(以下簡稱本法)作為保護國家安全之依據。參酌本法第 2 條之規定，「國家機密」指為確保國家安全或利益而有保密之必要，對政府機關持有或保管之資訊，經依本法核定機密等級者；由此可見，國家機密必須經由政府核定機密等級之程序。而同法第 4 條將機密等級分為三級[2]，分別為：絕對機密、極機密、機密。國家機密在收發、傳遞、使用、持有、保管、複製及移交時，亦應按本法第 15 條第 1 項規定，依其等級分別管制。因此，公務員如違反上開規定致洩漏或交付國家機密時，無論出於故意或過失，均有可能受到處罰，最高面臨 7 年有期徒刑[3]。在本案中，系爭文獻之性質與內容較為特殊且敏感，其未被銷毀而外流，本來或有國家機密外流之疑慮，惟系爭文獻之製作時間早於本法施行前，其並未依據本法第 39 條[4]規定於施行後二年內重新核定保密期限，故應「視為解密」。由此可見，系爭文獻在法律上已非「國家機密」，機關人員如不慎於文件解密後流出該文件，尚不至於違犯國家機密保護法之刑罰規定，惟仍可能涉及洩漏公務機密之問題。

從另一個角度來看，政府機密文件常因性質或內容特殊而成為收集、收藏或交易之客體，但於進行收集、收藏或交易時，仍應審慎留意可能之觸法風險。例如，本法第 34 條第 1 項[5]即針對收集國家機密之行為訂有罰則，如有違反者，最高可能面臨 5 年有期徒刑。而民眾判斷法律風險的重點之一，即在所收集之機密文件是否屬於「國家機密」。就本案而言，魏姓民眾因看重

---

[2] 國家機密保護法第 4 條：「國家機密等級區分如下：一、絕對機密：適用於洩漏後足以使國家安全或利益遭受非常重大損害之事項。二、極機密：用於洩漏後足以使國家安全或利益遭受重大損害之事項。三、機密：適用於洩漏後足以使國家安全或利益遭受損害之事項。」

[3] 國家機密保護法第 32 條：「洩漏或交付經依本法核定之國家機密者，處 1 年以上 7 年以下有期徒刑。因過失犯前項之罪者，處 2 年以下有期徒刑、拘役或科或併科新臺幣 20 萬元以下罰金。第一項之未遂犯罰之。」

[4] 國家機密保護法第 39 條：「本法施行前，依其他法令核定之國家機密，應於本法施行後 2 年內，依法重新核定，其保密期限溯自原先核定之日起算；屆滿 2 年尚未重新核定者，自屆滿之日起，視為解除機密，依第 31 條規定辦理。」

[5] 國家機密保護法第 34 條第 1 項：「刺探或收集經依本法核定之國家機密者，處 5 年以下有期徒刑。」

機密文件之特性，而於拍賣網站上買進並欲進行轉賣，若非系爭文獻恰好屬於已解密之文件，否則即可能涉及收集、交易國家機密而違法。

【管理 Tips】

在本案中，可以發現公務機關常掌控大量機密文件與個人資料，因而宜於機關內部建立資訊安全管理制度，以將資料、文件等機密資訊做嚴密控管與保護，避免發生外流或洩密事件。為此，公務機關需依據擁有的機密文件與個人資料訂定嚴謹之資訊資產分級，針對不同級別之資產做出相對應的保護處置。

除了適時審視各級別之保護措施是否恰當，公務機關並須定期清點各級別之資產是否被妥善保存在適當區域內。唯有建立完善之資訊管理標準作業程序，才能確保資訊之機密性、完整性及可用性，並確實地落實於公務機關內部管理。

【相關標準】

ISO 27001：2013(CNS 27001)

A.8.2.1 資訊之分級

資訊應依法律要求、價值、重要性及對未經授權揭露或修改之敏感性分級。

A.8.2.2 資訊之標示

應依組織所採用之資訊分級方案，發展及實作一套適切的資訊標示程序。

A.8.2.3 資產之處置

應依組織所採用之資訊分級方案，發展及實作處置資產之程序。

A.18.1.1 適用之法規及契約的要求事項之識別

對每個資訊系統及組織，應明確識別、文件化及保持更新所有相關法律、法令、法規及契約要求事項，以及組織為符合此等要求之作法。

類別：資訊保護【案號：S1050203】

史諾登再現？美政府機關委外廠商涉竊國家機密

【焦點話題】

美國某政府機關之外包廠商員工因涉嫌竊密遭到逮捕，引起輿論震驚。有媒體稱事件為「史諾登 2.0」(Snowden 2.0)，因為三年前爆料揭露美國政府秘密監控網路與電話計畫的史諾登，正好也是這個外包廠商之員工，而這個廠商主要協助美國政府機關規劃大部分敏感的網路行動。事件爆發後，美國聯邦檢察官在一份法庭文件中表示，該員工所竊取最高機密情報的「時間跨度和範圍令人驚訝」，甚至是「有史以來最大的政府機密文件竊賊」。

據檢察官透露，調查人員在該員工家中與車中，搜出高度機密文件的紙本和數位檔案，其中所竊取之電子資料高達 50TB，時間長達 20 年。而依據報載內容，該員工承認自己將政府機關之機密資料帶回家，以便「改進自己的技術」，但他堅稱未向任何人洩漏這些資料。

【資料來源：聯合新聞網，105/10/6】

【重點摘要】

1.未經授權即擅自複製或留存機密檔案，可能涉及刑事法律責任。

2.組織對於可能接觸機密資訊的委外廠商與其員工，應進行控管。

【法律觀點】

我國於民國(下同)92 年 2 月 6 日制定國家機密保護法(以下簡稱本法)，作為保護國家安全之依據。參酌本法第 2 條之規定，「國家機密」指為確保國家安全或利益而有保密之必要，對政府機關持有或保管之資訊，經依本法核定機密等級者；由此可見，國家機密必須經由政府機關核定機密等級之程

序。而同法第 4 條將機密等級分為三級[6]，分別為：絕對機密、極機密、機密。國家機密在收發、傳遞、使用、持有、保管、複製及移交時，亦應按本法第 15 條第 1 項規定，依其等級分別管制。而為確保國家機密之安全性，機關對於國家機密資料與檔案之存置場所或區域，得禁止或限制人員或物品進出，並為其他必要之管制措施[7]。如有刺探或收集國家機密資料者，最高可處以 5 年有期徒刑[8]。本案之情形如發生在我國，無論該員工刺探或收集機密之意圖為「改進自己的技術」或其他目的，均可能涉及本條犯罪，而依據其所試探或收集之機密資料屬性不同，最高可面臨 5 年的刑責。如有洩漏或交付國家機密者，更可能面臨 1 年以上 7 年以下有期徒刑。

而針對政府機關對資訊業務委外之部分，我國先前對於如何強化委外廠商之監督管理並無一般性之法律規範。然而，在現正研擬之資通安全管理法草案中，已意識到此一管理環節之重要性，其不僅要求政府機關將資訊業務委外營運時，除了慎選委外廠商外，並明訂其應善盡監督之責[9]；未來本法正式推動後，組織應配合新的法規內容做好因應準備。

【管理 Tips】

此事件的發生可以歸納出兩個關鍵點，第一，如何避免國家機密遭到竊取，其二則是對於委外廠商控管的程序。

針對前者，組織對於機敏性資料的管理，除了對於資料本身的遮蔽與隱藏的機制外，對於資訊及應用系統的存取權限需嚴格審查與開放。組織需制定存取控制政策，控管特定使用者可存取之資料，以及控制每位使用者的存取權

---

[6] 國家機密保護法第 4 條：「國家機密等級區分如下：一、絕對機密：適用於洩漏後足以使國家安全或利益遭受非常重大損害之事項。二、極機密：用於洩漏後足以使國家安全或利益遭受重大損害之事項。三、機密：適用於洩漏後足以使國家安全或利益遭受損害之事項。」

[7] 國家機密保護法第 19 條。

[8] 國家機密保護法第 34 條：「刺探或收集經依本法核定之國家機密者，處 5 年以下有期徒刑。刺探或收集依第 6 條規定報請核定國家機密之事項者，處 3 年以下有期徒刑。前 2 項之未遂犯罰之。」

[9] 資通安全管理法草案第 8 條：「　　公務機關或非公務機關，於本法適用範圍內，委外辦理資通系統之建置、維運或資通服務之提供，應考量受託者之專業能力與經驗、委外項目之性質及資通安全需求，選任適當之受託者，並監督其資通安全維護情形。」

限，包含讀取、寫入、刪除及執行等權限，限制系統輸出之資訊內容，並利用實體或邏輯的存取方式來區隔高機密等級資料。

針對後者，需與供應商及合作廠商進行合約簽署，並以文件型式紀錄雙方之協議，並仔細考量納入所有相關之資訊安全風險發生的可能性，以確保組織與供應者雙方間對履行相關資訊安全要求事項之義務沒有誤解。

【相關標準】

ISO 27001：2013(CNS 27001)

A.9.4.1 資料存取限制

應依存取控制政策，限制對資訊及應用系統功能之存取。

A.15.1.2 於供應者協議中闡明安全性

應與每個可能存取、處理、儲存或傳達資訊，或提供 IT 基礎建設組件資訊之供應者，建立及議定所有相關資訊安全要求事項。

三、刑法

類別：資訊保護【案號：S1050301】

攻擊網站，駭客向銀行勒索比特幣

【焦點話題】

○香港銀行之網站某日突然受「分散式阻斷服務」(DDoS)攻擊，銀行網路流量異常激增，造成網路大塞車。正當該銀行要尋找網路塞車的原因時，該銀行收到匿名電子郵件，要求支付比特幣，如果不在期限付款，將繼續癱瘓銀行網站。該銀行因此向警方報案，所幸客戶資料並未外洩，庫戶帳戶金額亦不受影響。

香港警方表示，該銀行遭受駭客攻擊後，警方初步調查顯示攻擊來自多個國家。駭客利用虛擬貨幣市場流通性較高、易兌換現金的特性，拿到比特幣後，即時轉去其他伺服器，避過偵查。香港警方於獲報後，將案件列為網路科技型態的勒索案，由香港網絡安全及科技罪案調查科偵辦。

【資料來源：香港蘋果日報，104/5/13】

【重點摘要】

1.隨著科技進步，新型態犯罪行為層出不窮，機關應與時俱進，加強資訊安全保護措施。

2.機關發生個資外洩，除依相關安全維護管理辦法通報主管機關以外，應採取應變措施並持續改善。

【法律觀點】

「阻斷服務攻擊」(”Denial of Service Attack”，以下簡稱”DoS”)亦稱洪水攻擊，是一種網路攻擊手法，當駭客使用網路上兩個以上被攻陷的電腦

作為「殭屍」向特定的目標發動阻斷服務攻擊時，稱為分散式阻斷服務攻擊(”Distributed Denial of Service attack”，以下簡稱”DDoS”)，其目的在於使目標電腦的網路或系統資源耗盡，使服務暫時中斷或停止，導致網站的目標客群無法正常使用。如果該案例發生在我國，此攻擊行為因會癱瘓機關的網站，造成使用者無法正常使用，駭客將構成刑法第 360 條之犯罪，面臨 3 年以下有期徒刑、拘役或科或併科 10 萬元以下罰金[1]。

值得注意的是，本案例出現以近年新興的比特幣(Bitcoin)作為勒索網站支付以解除癱瘓的對價。比特幣是一種全球通用的網路虛擬貨幣，並沒有一個類似「央行」的中央機構進行監管，也因為沒有政府機構監管，又可藉由網路跨國界的移轉，市場流通性較高，易兌換為現金，用戶拿到比特幣後，可即時轉去其他伺服器，避過偵查，比一般的實體貨幣難追尋。因此被犯罪者相中，作為移轉、藏匿不法所得的手段。

若駭客以威脅癱瘓網站為由，要求網站所有人支付比特幣，比特幣雖然是虛擬貨幣，但仍具有財產價值，具有市場流通性，依我國目前多數實務見解，虛擬貨幣仍可能該當刑法第 346 條第 2 項的「財產上利益」，駭客仍將成立恐嚇得利罪[2]。

【管理 Tips】

使用資訊科技已經成為無法避免之趨勢，但是在運用新興科技提供商業服務時，資訊安全應為首要考量。

此次攻擊事件主要來自網路，所有企業或政府機關都有可能成為被攻擊對象，如何強化網路管控措施是所有組織都需面對之議題。然而，技術控管雖

[1] 刑法第 360 條：「無故以電腦程式或其他電磁方式干擾他人電腦或其相關設備，致生損害於公眾或他人者，處 3 年以下有期徒刑、拘役或科或併科 10 萬元以下罰金。」

[2] 法務部法檢字第 (90) 法檢決字第 039030 號函認定電磁紀錄於竊盜罪以「動產」論，於詐欺罪亦屬「動產」，故虛擬物品得作為刑法竊盜罪及詐欺罪保護之客體。臺灣高等法院刑事判決 101 年度上易字第 494 號刑事判決認定虛擬世界的財物屬刑法詐欺罪保護之法益，「惟該等虛擬財物並無人類可以感觸之實體物存在，以詐術手段為之，應認係取得『財產上不法之利益』，應構成……詐欺得利罪。」

然能夠降低風險，卻無法保證擋下每次駭客攻擊。所以當資安事件發生時，應該及時通報並且迅速回應，同時保存相關紀錄做為證據，改善缺失後，從事件中學習相關經驗，以減少未來再度發生事故之風險。另外對於網路犯罪事件應該主動和執法機關合作，不讓駭客輕易獲取不當利益，增加更多受害單位。

【相關標準】

ISO 27001：2013(CNS 27001)

A.13.1.1 網路控制措施

應管理及控制網路，以保護資訊系統及應用。

A.16.1.2 通報資訊安全事件

應循適切之管理管道，儘速通報資訊安全事件。

A.16.1.5 對資訊安全事故之回應

應依文件化程序，回應資訊安全事故。

A.16.1.6 由資訊安全事故中學習

應使用獲自分析及解決資訊安全事故之知識，以降低未來事故之可能性或衝擊。

A.16.1.7 證據之收集

組織應定義及應用程序，以識別、收集、獲取及保存可用作證據之資訊。

類別：資訊保護【案號：S1050302】

紐西蘭儲備銀行官方利率調降訊息遭記者提前洩漏

【焦點話題】

紐西蘭儲備銀行固定在每季末當月初 9 點宣布貨幣政策季報，其中季報重要內容為官方利率(Official Cash Rate)變動情形與調整方向。儲備銀行針對季報發布前設有媒體封鎖機制(media lockup)，亦即新聞媒體與外部分析師在當天 7 點至 9 點間獲知即將發布的官方訊息期間，須待在媒體室，且在封鎖期間屆滿前不得對外傳布或發稿。然而，經第三方資安鑑識機構調查，發現任職於 Newshub Mediaworks 的記者，在當天 8 點左右於媒體室內，即透過筆記型電腦撰擬報導，並將尚在資訊封鎖階段的利率調降訊息提供給部分公司同仁，隨後其中一名同仁將該訊息傳達給某位經濟學領域的部落客。

紐西蘭儲備銀行首長表示此資訊外洩事件嚴重破壞多年來信任關係，造成從金融市場不當獲利的機會；另該行通訊部門首長亦表示長久來雖多方考量採取其他資訊安全替代措施，然而未能全面消弭技術與人為風險。

【資料來源：Bloomberg，105/4/16】

【重點摘要】

1.媒體封鎖機制為部分國家央行確保新聞媒體能在官方正式發布消息後，始進一步發表新聞或評論所採取之安全機制，以兼顧金融市場安定與新聞自由。

2.此案例如發生在我國，記者若洩漏經政府機關核定為媒體封鎖期間應保密的資訊，恐構成洩漏國防以外秘密罪。

【法律觀點】

為平衡新聞採訪自由、政府資訊公開與金融市場穩定並避免不肖人士投機，紐西蘭儲備銀行與部分國家中央銀行，採取媒體封鎖機制，透過此程序與新聞媒體進行資訊溝通，並同時限制其對外發布訊息，以確保新聞媒體能在官方正式發布後，始進一步發表新聞或評論，其目的在兼顧金融市場安定、資訊安全及新聞自由，盡可能降低新聞媒體在資訊未成熟前即洩漏重大政策、錯誤解讀，導致市場上不當投機行為。紐西蘭儲備銀行發現官方利率調升訊息遭到提前揭露後，即委託獨立第三方資安鑑識機構，透過訪談當天在場新聞記者與調閱監視錄影器畫面等方式，調查資料外洩方式與事件經過[1]。而此次外洩事件，即曝露出政府與媒體互動的信任危機，以及隨著網路技術演進，新聞記者無庸仰賴紙筆，即能透過通訊軟體或電子郵件方式傳遞資訊，造成以傳統媒體室隔離方式限制新聞記者發稿的困難。

依我國刑法第 132 條第 3 項規定，非公務員因職務或業務知悉或持有中華民國國防以外應秘密之文書、圖畫、消息或物品，而洩漏或交付之者，處 1 年以下有期徒刑、拘役或 300 元以下罰金。因此本案如發生於我國時，縱使新聞記者從獲知重大政策訊息至解除媒體封鎖限制的保密期間僅有 2 小時，但在該期間內，該資訊若經政府機構依內部程序核定為機密或已明文要求記者保密，則記者以任何方式洩漏或交付資訊給第三人，即可能構成洩漏國防以外秘密罪。再者，考量到媒體封鎖期限主要針對具有高度敏感的政府政策訊息，有保護之必要，且封鎖期限在官方正式宣布時即為解除，並無進一步限制新聞採訪自由，而事先資訊封鎖目的在於維護金融市場等公共利益，因此在利益權衡下，新聞記者恐難以新聞自由主張有提前洩漏該資訊之正當事由。是以，若因職務或業務關係知悉應保密之資訊時，應遵守保密義務，以免涉及相關刑責。

【管理 Tips】

[1] Deloitte, Reserve Bank of New Zealand, March 2016 OCR announcement Investigation into alleged leak, 12 April 2016, *available* at http://www.rbnz.govt.nz/-/media/ReserveBank/Files/News/2016/Investigation-into-leak-march-2016-OCR-announcement.pdf?la=en (latest visited:2016/6/28)

政府機構在重大政策與民眾溝通時，往往需要借助媒體之功能，如何在主動揭露和資訊洩漏兩者間劃出界線，應有明確之規範。

此案中，新聞記者違反與儲備銀行間多年互信基礎，將銀行透過媒體封鎖機制確保機密的資訊，提前在保密限制解除前洩露給其他人，因此發生市場重大資訊洩漏事件。此固然是記者破壞信任關係，但相似事件之起因，亦常有「慢藏誨盜」的成分。組織如對於重要資訊未能依其機密等級加以適當之保護，例如，和使用者之間未能簽署保密協議或未有明確而適當之懲處措施，恐怕類似的事件仍將持續出現。

【相關標準】

ISO/IEC 27001：2013(CNS 27001)

A.13.2.4 機密性或保密協議

宜識別、定期 審查及文件化，以反映組織對資訊保護之需要的機密性或保密協議之要求事項。

類別：資訊保護【案號：S1050303】

警察開單查個資，竟偷加 LINE 把妹

【焦點話題】

一名陳姓員警在市區執行交通違規之例行勤務時，發現一名女騎士違規左轉駛入待轉區內，因而當場以違規左轉為由對女騎士開單取締。遭到開單之女騎士，除了荷包受損之外，其在員警開單過程中所留給員警之車籍資料，也為她帶來意外困擾。

該員警因違規左轉之開單取締需要，要求女騎士提供自己之車籍資料，未料該員警事後竟透過該車籍資料查得女騎士手機號碼，並主動加 LINE、傳送訊息給女騎士，要求做朋友。此舉造成女騎士嚴重困擾，女騎士在自己之臉書上公布員警傳送之對話截圖，要求警局查辦員警侵害隱私之行為。依據報載，警局表示對於該員警之違法行為將嚴加查辦、決不護短。

【資料來源：蘋果日報，105/5/30】

【重點摘要】

1.機關所保有之個人資料，機關人員不得於執行職務以外之範圍利用。

2.機關人員擅自利用或洩漏他人個資之行為，可能涉及個人資料保護法及刑法洩漏國防以外機密罪。

【法律觀點】

依據個人資料保護法(以下簡稱個資法)第 15 條規定：「公務機關對個人資料之蒐集或處理，除第 6 條第 1 項所規定資料外，應有特定目的，並符合下列情形之一者：一、執行法定職務必要範圍內。二、經當事人同意。三、對當事人權益無侵害。」而同法第 16 條本文規定：「公務機關對個人資料之利用，除第 6 條第 1 項所規定資料外，應於執行法定職務必要範圍內為之，

並與蒐集之特定目的相符。」據此，公務機關(含公務員)蒐集或處理民眾個資時，應符合前開第 15 條所列情形，且除有第 16 條所列得特定目的外利用之情形外，僅得於執行法定職務之必要範圍內為之。在本案中，參酌警察法第 9 條有關警察職權規定[2]，因違規開單而向女騎士要求提供車籍資料，符合個資法第 15 條之規定。惟該員警在取得上開資料後，進一步利用該資料查詢女騎士手機號碼，並藉此加 LINE、傳訊息，要求交朋友等，顯非屬執行法定職務之範圍，構成該法第 16 條規定之違反。

其次，針對員警之行為，在個資法 104 年 12 月 30 日修正前，原可依第 41 條第 1 項[3]規定最高處以 5 年有期徒刑，惟修法後條文已刪除前述「非意圖營利」違法利用個資之情況，僅處罰具有「意圖為自己或第三人不法之利益或損害他人之利益」之情形，考量該員警擅自利用女騎士手機號碼之行為，乃係出於交友，非為自己或他人之不法利益，因而在新法規定下，員警之行為似不構成個資法上之犯罪。

進一步言，依據刑法第 132 條規定，公務員洩漏或交付關於中華民國國防以外應秘密之文書、圖畫、消息或物品者，處 3 年以下有期徒刑。而臺灣臺北地方法院 103 年度易字第 690 號刑事判決曾認為，公務員違反保密義務之行為，如洩漏之客體為個人資料時，並不影響刑法第 132 條犯罪之成立。在本案中，針對車籍資訊之管理，內政部警政署訂有車籍資訊系統查詢作業規定，其第 6 點即明確指出「各警察機關人員除執行犯罪偵查、治安維護、交通管理或其他於法令規定職掌必要範圍內之情形外，不得使用本系統查詢、下載、列印或公開相關車籍等資料，以確保民眾個人隱私，防止資料外洩。」可見「車籍資訊系統中之資料」亦屬於員警應予保密之資訊，因此如該員警擅自查詢及使用車及資訊系統中資料並對外洩漏，另可能涉犯刑

[2] 警察法第 9 條：「警察依法行使左列職權：一、發佈警察命令。二、違警處分。三、協助偵查犯罪。四、執行搜索、扣押、拘提及逮捕。五、行政執行。六、使用警械。七、有關警察業務之保安、正俗、交通、衛生、消防、救災、營業建築、市容整理、戶口查察、外事處理等事項。八、其他應執行法令事項。」

[3] 修法前個人資料保護法第 41 條第 1 項：「違反第 6 條第 1 項、第 15 條、第 16 條、第 19 條、第 20 條第 1 項規定，或中央目的事業主管機關依第 21 條限制國際傳輸之命令或處分，足生損害於他人者，處 2 年以下有期徒刑、拘役或科或併科新臺幣 20 萬元以下罰金。」

法第 132 條之洩漏國防以外機密罪，自不待言。

【管理 Tips】

機關推動公務之過程中，常有觸及民眾個人資料之情形。針對民眾個人資料，機關不僅應依據個資法及其他法令進行蒐集、處理及利用民眾個人資料，並確保機關人員不會將民眾個人資料挪為私用，致招民怨。

為確保機關人員能夠遵守個資法及其他法令規定，機關對於所屬人員應明確告知規範內容並要求遵守。其次，平日亦應實施教育訓練，以提高機關人員對於個資保護之意識，尤其是常見違規態樣，宜作為教育訓練之重點內容。而對於假借職務機會侵害他人個資之行為，機關亦應透過公正程序予以懲處，以確保機關規範之落實。

【相關標準】

ISO 27001：2013(CNS 27001)

A.7.2.1 管理階層責任

管理階層應要求所有員工及承包者，依組織所建立政策及程序施行資訊安全事宜。

A.7.2.2 資訊安全認知、教育及訓練

組織所有員工及相關之承包者，均應接受與其工作職能相關的組織政策及程序之適切認知、教育及訓練，並定期更新。

A.7.2.3 懲處過程

應具備正式及已傳達之懲處過程，以對違反資訊安全之員工採取行動。

A.18.1.4 個人可識別資訊之隱私及保護

應依適用之相關法令、法規中之要求，以確保個人可識別資訊之隱私及保護。

類別：資訊保護【案號：S1050304】

「定位手錶」涉妨害秘密 母：關心女兒

【焦點話題】

呂姓女子與先生分居，因近來兒童殺害事件層出不窮，所以購買「兒童定位手錶」送給女兒，將手錶戴在女兒手上。這種手錶裝有 SIM 卡可 4G 上網，可透過網路與手機連線，家長透過手機可以知道小孩、老人或寵物的所在位置，還能雙向通話，聽到手錶附近的環境聲音，若是被歹徒綁架，具有報警功能。

但女兒帶著該手錶回到父親家中，父親懷疑已分居的妻子不懷好意，想要窺探他的隱私，藉由女兒的手錶，知道他說了什麼話、做了什麼事情，因而控告呂女妨害秘密。

呂女則說，她與先生分居後不能見到女兒，當時又有孩童被殺害事件，她想要和女兒聯絡、講話，知道女兒過得好不好，有沒有去上學等，並沒有要監聽他人的想法。

檢察官調閱手機門號的通話紀錄，發現僅 3 次對話，但都沒有開啟監聽功能，且並無其他證據顯示先生的私生活遭到窺伺，故將這名關心女兒的母親不起訴處分。

【資料來源：中時電子報，105/7/19】

【重點摘要】

1.使用有監聽功能的穿戴式裝置窺探他人之非公開活動，可能會涉及侵害隱私權。

2.針對在公開環境內從事活動者認為私密之活動拍攝或錄音，若不具有客觀上之隱密性，尚不構成刑法妨害秘密。

【法律觀點】

我國刑法為避免使用各類電子設備危害個人隱私，於第 315 條之 1 規定[1]明確禁止無故利用工具竊錄他人非公開之言論。其中也包含具親密關係之夫妻在內，故夫妻間尚不能藉口懷疑或有調查配偶外遇之必要，即有恣意窺視或竊聽他方，甚至周遭相關人士非公開活動、言論、談話或身體隱私部位之舉動[2]。而「無故」是指欠缺法律上正當理由者而言[3]；「非公開之活動」則指活動者主觀上認定該活動之進行具有隱密性，且其具有不欲公開之期待或意願；惟有鑑於活動者主觀上之感受認定不易，且有隨時變更之可能，我國司法實務上對於非公開活動之判定，尚須客觀上活動者已利用相當環境或採取適當設備，用以確保其活動之隱密性方為充足[4]。

就本案而言，因呂女未開啟監聽功能，尚不能認定其已構成妨害秘密罪。此外，呂女即使開啟監聽功能，若符合「監察者為通訊之一方或已得通訊之一方事先同意，而非出於不法目的」之情形，亦不會構成通訊保障及監察法第 24 條第 1 項的違法監察他人通訊罪[5]。值得注意的是，依照民法第 1084 條第 2 項規定，父母對於未成年之子女，有保護及教養之權利義務。本案呂女基於安全考量讓 9 歲女兒配戴定位手錶，在合乎比例原則下監聽未成年子女，而屬履行父母的法定義務時，對子女應可免除相關刑事責任[6]。惟因該定位手錶亦會監聽子女以外之人的對話，若使用監聽功能者明知未經通訊任一方事先同意而監聽，或其監聽乃出於不法目的時，對於第三人恐將仍無

---

[1] 刑法第 315 條之 1：「有下列行為之一者，處 3 年以下有期徒刑、拘役或 30 萬元以下罰金：一、無故利用工具或設備窺視、竊聽他人非公開之活動、言論、談話或身體隱私部位者。二、無故以錄音、照相、錄影或電磁紀錄竊錄他人非公開之活動、言論、談話或身體隱私部位者。」

[2] 參照最高法院 103 年度台上字第 3893 號刑事判決。

[3] 參照最高法院 103 年度台上字第 3893 號刑事判決。

[4] 參照最高法院 101 年度台上字第 6343 號刑事判決。

[5] 通訊保障及監察法第 24 條第 1 項：「違法監察他人通訊者，處 5 年以下有期徒刑。」第 29 條第 1 項：「監察他人之通訊，而有下列情形之一者，不罰：一、依法律規定而為者。二、電信事業或郵政機關(構) 人員基於提供公共電信或郵政服務之目的，而依有關法令執行者。三、監察者為通訊之一方或已得通訊之一方事先同意，而非出於不法目的者。」

[6] 刑法第 21 條第 1 項：「依法令之行為，不罰。」邱忠義，刑法通則新論，頁 219。元照出版，104 年 9 月 3 版。

法免責。

科技的進步能讓父母更方便的維護未成年子女之安全。然而，私人對話仍屬於個人隱私，使用科技產品掌握子女行蹤時，仍應注意是否獲得通訊者同意，是否侵犯第三人的隱私，以及是否合乎比例原則並基於合法目的，以避免侵害他人隱私權而觸犯法律相關責任。

【管理 Tips】

在科技產品不斷創新進步的時代，科技逐漸影響我們的日常生活。科技產品的創造產生正面效益與負面議題，如同此事件般，將個人資訊與科技衝突的議題浮上了檯面。從產品的角度來說，業者在販售自家產品時，除了檢視產品有無違反現行法律外，應當以使用者角度，設想使用時應該注意的事項，以及警示可能發生的危害，並於說明書中加以規範並提醒使用者，以確保使用者可以安心的享受產品。

再者，業者對於產品的保護需更加謹慎，應防止產品被外部的破壞，以及受到內部病毒的入侵與駭客的威脅。產品於開發前，應制定完善的開發規劃，並將資訊安全考量在內；開發時，確保程式碼撰寫與開發環境的安全性；開發後，做精密的產品安全測試。綜上所述，組織應適當規範使用者行為與產品安全性考量，盡可能降低個人隱私與科技的衝突發生。

【相關標準】

ISO 27001：2013(CNS 27001)

A.12.2.1 防範惡意軟體之控制措施

宜實作防範惡意軟體之偵測、預防及復原控制措施，並合併適切之使用認知。

A.14.1.1 資訊安全要求事項分析及規格

資訊安全相關要求事項，宜納入新資訊系統或既有資訊系統之強化的要求事項中。

A.14.2.1 保全開發政策

宜建立軟體及系統開發之規則，並應用至組織內之開發。

A.14.2.6 安全開發環境

對涵蓋整個系統開發生命週期之系統開發及整合工作，組織宜建立並適切保護安全開發環境。

A.14.2.8 系統安全測試

於開發中，宜實施安全功能性之測試。

A.14.2.9 系統驗收測試

宜建立新資訊系統、系統升級及新版本之驗收測試計畫及準則。

A.18.1.1 適用之法規及契約的要求事項之識別

對每個資訊系統及組織，宜明確識別、以文件記錄及保持更新所有相關法律、法令、法規及契約要求事項，以及組織為符合此等要求之作法。

類別：資訊保護【案號：S1050305】

預醫所副所長拉傷獸醫 稱「防機密外洩」

【焦點話題】

某軍事院校預防醫學研究所(下稱預醫所)陳姓副所長，因認為趙姓研究助理兼獸醫，有竊取秘密嫌疑，在大門衛哨前，拉扯趙男背包，致趙左上臂擦傷。

陳男辯稱，當時他是預醫所的主官，依法具有軍事警察身分，當天接到報告，趙男涉嫌到第三等級動物實驗室拍照，有竊取秘密之嫌，經調閱監視器，確有此事。之後他成立調查小組，通知趙男與另一涉嫌之李姓員工說明，並追回照片，李有寫下自白書，趙男卻不接電話，才到樓下設攔查哨，由於趙有犯罪嫌疑重大及逃逸情形，在急迫情形下，軍事警察可依法逕行拘提，當時他是執行職務及任務。

趙男解釋，實驗室廢水處理箱有採購問題，他打電話給調查局，對方建議拍照存證，自己才會拍攝違法證據，絕非竊密。

法官認為，國防部軍醫局雖核定預醫所是國軍機敏處所，但與國家機密保護法中的國家機密程度有別，也無相關權責單位核准公文，可證明預醫所是「機密」處所，且該研究室相關規定是基於傳染病防治法及動物傳染病防治條例，與防範機密一事無關。

法官認為，縱如陳男所稱，當時趙男攜帶照片出所，僅構成刺探或收集程度，與洩漏或交付程度有別，且預醫所也非屬要塞保壘地帶法所稱要塞保壘地帶，國防醫學院也未認定趙男有涉洩漏或交付機密刑事責任問題。最後，法院依傷害罪判處陳男拘役 30 日，得易科罰金 3 萬元。

【資料來源：自由電子報，105/7/30】

【重點摘要】

1.「國家機密」之認定，必須是基於國家安全或利益而有保護必要，且經核定機密等級的資訊。

2.「要塞堡壘地帶」指國防上所必須控制與確保之戰術要點、軍港及軍用飛機場及其周圍之必要區域，應由國防部核定並公告之。

【法律觀點】

本案陳男是否應論以刑法上的強制罪或傷害罪，重點在於陳男對於趙男有無法律上拘提或逮捕的權利[7]。除依刑事訴訟法第 88 條規定，對現行犯或準現行犯[8]得在沒有拘票的情況下逮捕嫌疑人外，依同法第 88 條之 1 第 1 項第 3 款[9]規定，司法警察偵查犯罪，有事實足認為犯罪嫌疑重大，經被盤查而逃逸者，原則上司法警察亦得逕行拘提。因此，本案法院審判的重點之一，即在於「趙男是否竊取機密而涉有刑事責任」。

為建立國家機密保護制度，確保國家安全及利益，我國制定有國家機密保護法。然而，並非所有機敏性公務資訊都屬於本法保護的客體，必須是基於國家安全或利益而有保護必要，且經核定機密等級的資訊[10]，才是所謂「國家機密」。如經核定為國家機密的資訊，不論是絕對機密、極機密或機密，在知悉、持有、使用、收發、傳遞、保管、複製、移交、銷毀及解除等作業，法令都有非常嚴謹的規定[11]。如違反規定而有洩密之情形，可處以 7 年

---

[7] 參見台灣新北地方法院 104 年度易字 1801 號刑事判決。

[8] 刑事訴訟法第 88 條規定：「現行犯，不問何人得逕行逮捕之。犯罪在實施中或實施後即時發覺者，為現行犯。有左列情形之一者，以現行犯論：一、被追呼為犯罪人者。二、因持有兇器、贓物或其他物件、或於身體、衣服等處露有犯罪痕跡，顯可疑為犯罪人者。」

[9] 刑事訴訟法第 88 條之 1 第 1 項第 3 款：「檢察官、司法警察官或司法警察偵查犯罪，有左列情形之一而情況急迫者，得逕行拘提之： 三、有事實足認為犯罪嫌疑重大，經被盤查而逃逸者。但所犯顯係最重本刑為 1 年以下有期徒刑、拘役或專科罰金之罪者，不在此限。」軍事審判法第 58 條第 1 項第 4 款「下列人員為軍法警察官，於其管轄或防區內，有協助軍事檢察官偵查犯罪之職權：四、軍事機關、部隊、學校、獨立或分駐之長官或艦船長。」

[10] 國家機密保護法第 2 條規定：「本法所稱國家機密，指為確保國家安全或利益而有保密之必要，對政府機關持有或保管之資訊，經依本法核定機密等級者。」

[11] 國家機密保護法第 14 條：「國家機密之知悉、持有或使用，除辦理該機密事項業務者外，以經原核定機關或其上級機關有核定權責人員以書面授權或核准者為限。」第 15 條第 1 項：「國家機密之收發、傳遞、

以下有期徒刑[12]；如刺探或收集國家機密者，亦可處 5 年以下有期徒刑[13]。

就本案而言，趙男到預醫所之動物實驗室拍照，雖試圖將照片攜出，但尚未將照片提供給他人，其行為僅構成「刺探」或「收集」程度，與洩漏或交付程度尚屬有間。從而，法院認為因相關資訊並未依「國家機密保護法」核定為國家機密，預醫所雖經核定為國軍機敏處所，但主要規範目的為防疫作用，與國家機密程度有別，故趙男拍攝的內容尚不涉及刺探或收集國家機密之行為。又我國刑法對於一般公務機密，雖就公務員洩漏或交付關於中華民國國防以外應秘密之文書、圖畫、消息或物品者設有刑責[14]，但趙男的行為亦不構成洩漏或交付，自無上開罰則之適用。

另外，預醫所是否為法律上所稱之要塞堡壘地帶？亦可能影響趙男之拍照行為是否違法。所謂「要塞堡壘」，指國防上所必須控制與確保之戰術要點、軍港及軍用飛機場；而要塞堡壘及其周圍之必要區域(含水域)，稱為要塞堡壘地帶[15]，應由國防部核定並公告之[16]。在堡壘要塞地帶內，非受有國防部之特別命令或非經要塞司令之許可，不得為測量或攝影等軍事上偵察事項[17]，違反者最高可處 7 年以下有期徒刑[18]。本案中，法院認為預醫所雖

使用、持有、保管、複製及移交，應依其等級分別管制；遇有緊急情形或洩密時，應即報告機關長官，妥適處理並採取必要之保護措施。」

[12] 國家機密保護法第 32 條：「洩漏或交付經依本法核定之國家機密者，處 1 年以上 7 年以下有期徒刑。因過失犯前項之罪者，處 2 年以下有期徒刑、拘役或科或併科新臺幣 20 萬元以下罰金。第一項之未遂犯罰之。」第 33 條：「洩漏或交付依第 6 條規定報請核定國家機密之事項者，處 5 年以下有期徒刑。因過失犯前項之罪者，處1年以下有期徒刑、拘役或科或併科新臺幣10萬元以下罰金。第一項之未遂犯罰之。」

[13] 國家機密保護法第 34 條：「刺探或收集經依本法核定之國家機密者，處 5 年以下有期徒刑。刺探或收集依第 6 條規定報請核定國家機密之事項者，處 3 年以下有期徒刑。前二項之未遂犯罰之。」

[14] 刑法第 132 條：「公務員洩漏或交付關於中華民國國防以外應秘密之文書、圖畫、消息或物品者，處 3 年以下有期徒刑。因過失犯前項之罪者，處 1 年以下有期徒刑、拘役或 300 元以下罰金。非公務員因職務或業務知悉或持有第一項之文書、圖畫、消息或物品，而洩漏或交付之者，處 1 年以下有期徒刑、拘役或 300 元以下罰金。」

[15] 要塞堡壘地帶法第 1 條：「國防上所必須控制與確保之戰術要點、軍港及軍用飛機場，稱為要塞堡壘；要塞堡壘及其周圍之必要區域(含水域)，稱為要塞堡壘地帶。」

[16] 要塞堡壘地帶法第 3 條第 2 項：「前項所列各區及其與軍港、要港、海軍防禦建築物、飛機場、空軍防禦建築物等相關連之區域，均由國防部核定並公告之。」

[17] 要塞堡壘地帶法第 4 條第 1 款：「第一區內之禁止及限制事項：一、非受有國防部之特別命令，不得為

被國防部軍醫局核定為「國軍機敏處所」，但該函令僅是軍事機關內部行政規則，並無法律依據，而預醫所非屬要塞堡壘地帶法所稱之要塞堡壘地帶，自無該法適用，故趙男對該場所本身拍照，並不違反上述規定。

【管理 Tips】

由於科技產品的創新，資訊的型態可變為文字、電子檔、音訊或視訊等各種形式保存下來，並可藉由不同媒介傳遞。此事件的發生呼籲各單位需制定場所內使用設備的規範，以及設備攜出入的管制，以防機密資訊不慎外洩。

從管理角度來說，對於機密場所內之管制，除了實體安全的維護外，且包含場所內人員之控管。人員進出場所需經單位申請表明意圖，並由負責人核准許可，方可進入。且進出入場所內攜帶之設備需經核准許可，才可攜帶或使用。以上過程皆需保留紀錄，並定期審查。機密場所內需配置監視設備，留存影像證據，以防資訊安全事故的發生。

對於資訊安全事故之管理，需規範資訊安全事故管理程序，制訂相關通報流程及負責通報之窗口，並迅速依據程序作出回應。過程必須蒐集相關證據並加以保存。最後，定期檢討資訊安全事故管理程序是否符合單位之需求。

綜合以上論述，各單位需規範嚴格的實體安全維護，與進出入人員的控管外，如發生意外事件，需有一套緊急的應變措施，並確保員工可完整執行與應對，且需有相關證據留存以便後續追蹤與檢討。

【相關標準】

ISO 27001：2013(CNS 27001)

測量、攝影、描繪、記述及其他關於軍事上之偵察事項。……」第 5 條第 1 款：「第二區內之禁止及限制事項：一、非經要塞司令之許可，不得為測量、攝影、描繪、記述及其他關於軍事上偵察事項。……」

[18] 要塞堡壘地帶法第 9 條：「犯第 4 條第 1 款或第 5 條第 1 款之規定者，處 1 年以上、7 年以下有期徒刑。因過失犯前項之規定者，處 1 年以下有期徒刑、拘役或 500 元以下罰金。」

A.11.1.1 實體安全周界

宜定義及使用安全周界，以保護收容機敏或重要資訊及資訊處理設施之區域。

A.11.1.2 實體進入控制措施

保全區域宜藉由適切之進入控制措施加以保護，以確保僅允許經授權人員進出。

A.11.1.5 於保全區域內工作

宜設計並施行於保全區域內工作之程序。

A.11.2.5 資產之攜出

未經事前授權，不得將設備、資訊或軟體帶出場域外。

A.16.1 資訊安全事故及改善之管理

確保對資訊安全事故之管理的一致及有效作法，包括對安全事件及弱點之傳達。

A.16.1.2 通報資訊安全事件

宜循適切之管理管道，儘速通報資訊安全事件。

A.16.1.7 證據之蒐集

組織宜定義及應用程序，以識別、蒐集、獲取及保存可用作證據之資訊。

四、智慧財產權法

類別：資訊保護【案號：S1050401】

遊戲業者架私服吸收 17 萬會員獲利千萬

【焦點話題】

保二總隊刑事警察大隊偵一隊日前就破獲一起架設遊戲私服的侵權案件，逮補嫌犯 A 與嫌犯 B，並查扣伺服器主機 32 台與其他網路設備。

A、B 二人自兩年前起，創設知名電腦遊戲的私人伺服器(下稱私服)，會員累積人數達 17 萬人次之多，甚至以贊助為名，向使用者收取費用。遊戲官方得知相關訊息時，也曾行文給 A 嫌警示，卻不見改善，因此委任律師提告。

據報導指出，兩嫌之所以能夠招攬到 17 萬會員，主因是兩嫌將原本單機版的遊戲，改成連線型態，因此廣受該遊戲玩家好評，再以一次贊助 900 元便可獲取永久會員的模式招攬會員，兩年來不法所得粗估在新台幣一千萬元以上。

【資料來源：蘋果日報 105/10/03】

【重點摘要】

1. 對於電腦遊戲，擅自複製、改寫或提供連結以供下載，將分別被論以「違法重製」、「違法改作」及「違法公開傳輸」。
2. 即使未違法重製、改作或公開傳輸電腦程式，僅是破解其防止複製或改寫的程式，仍屬於「違法破解防盜拷措施」而涉有刑責。

【法律觀點】

電腦遊戲的「私人伺服器」，是指由個人架設的網路遊戲伺服器，提供終

端使用者與官方網站相同之服務。原本網路遊戲玩家是連線到遊戲公司去進行遊戲，若使用私人伺服器，則是連線到特定玩家架設的伺服器進行遊戲。而私服業者常以低於官網之月費(甚至不收月費)以及低於官網之寶物價格吸引玩家使用「私服」，因此「私服」對遊戲公司之獲利會造成一定的影響[1]。因為電腦遊戲私人伺服器的架設，是在電腦遊戲的基礎上進行改寫或增加功能，因電腦遊戲屬於著作權法所保障的「著作」，若未得網路遊戲製造商的授權，便會因此會觸犯著作權法。

若「私服」業者未經遊戲公司授權，將原有的網路遊戲程式內容加以複製以供其架設「私服」收取費用，依著作權法第 91 條[2]規定，涉及「意圖銷售或出租而重製」該款網路遊戲，將成立刑事責任。再者，「私服」業者修改原遊戲，而仍承繼原遊戲的「表達」[3]而非僅是其「抽象概念」，例如承繼原遊戲的劇本、設計或角色設計，而另外加入新的創意表現[4]，則可能涉及著作權法第 92 條[5]規定之「違法改作」行為。

至於「私服」業者透過網路主動或被動地向公眾提供或傳達著作內容(例如：主動寄電子郵件給多數人或提供連結供人連線下載)，只要是使著作處於其他人可以隨時接取或下載的狀態[6]，依著作權法第 92 條規定，亦將成立「違法公開傳輸」之刑責。

另外，通常網路遊戲都會設有「防盜拷措施」，用來防止使用者重製或改

---

[1] 智慧財產法院 101 年刑智上訴字第 42 號刑事判決參照。

[2] 著作權法第 91 條第 2 項：「意圖銷售或出租而擅自以重製之方法侵害他人之著作財產權者，處 6 月以上 5 年以下有期徒刑，得併科新臺幣 20 萬元以上 200 萬元以下罰金。」

[3] 著作權法第 10-1 條：「依本法取得之著作權，其保護僅及於該著作之表達，而不及於其所表達之思想、程序、製程、系統、操作方法、概念、原理、發現。」

[4] 著作權法第 3 條第 11 款：「……十一、改作：指以翻譯、編曲、改寫、拍攝影片或其他方法就原著作另為創作。……」

[5] 著作權法第 92 條：「擅自以公開口述、公開播送、公開上映、公開演出、公開傳輸、公開展示、改作、編輯、出租之方法侵害他人之著作財產權者，處 3 年以下有期徒刑、拘役，或科或併科新臺幣 75 萬元以下罰金。」

[6] 著作權法第 3 條第 10 款：「……十、公開傳輸：指以有線電、無線電之網路或其他通訊方法，藉聲音或影像向公眾提供或傳達著作內容，包括使公眾得於其各自選定之時間或地點，以上述方法接收著作內容。」

寫遊戲。為了避免用來保護著作的科技措施被規避[7]，依著作權法第 80-2 條[8]規定，未經合法授權不得對防盜拷措施予以破解、破壞或以其他方法規避。因此，若「私服」業者或是遊戲玩家破解遊戲的防盜拷措施，即使未違反其他著作權法之規定，仍會成立刑事責任[9]。

【管理 Tips】

從技術層面來說，公司在設計產品時，需事先考量產品的安全性以及被盜用的可能性。於 ISO27001 的資訊安全管理制度的理念上，需於組織內部建立系統開發的安全工程原則，宜在所有營運相關的系統上進行安全設計以及安全要求。持續記錄、維護，並針對新技術進行安全風險分析與審核，防止已知的資訊安全攻擊。適當設計用戶身分鑑別技術與防盜措施，避免非法人士擅自更動產品設計，以達到主動防禦的概念。

產品受到技術攻擊是不可避免的。從法律層面來說，公司可運用適當的法律依據，來規範產品相關的智慧財產權、所有權與著作權等的使用規定，並符合法律、法規和合約的要求，達到保護組織資產與權益之目的。

【相關標準】

ISO 27001：2013(CNS 27001)

A.14.2.5 安全系統設計原則

設計安全系統的原則應加以建立、文件化、維護並應用於所有資訊系統實作成果。

---

[7] 著作權法第 80-2 條之立法理由：「……二、科技保護措施規定僅係於著作權之外，於著作權人採取科技措施保護其著作時，以著作權法再給予額外之保護，確保其所採取之科技措施不被規避，惟其對於原本依法享有之著作權並未增減，亦不影響著作權受侵害時之救濟，更不得使利用人合理使用之權益受到限制，為避免科技保護措施規定引發適用上之疑義。」

[8] 著作權法第 80-2 條第 1 項：「著作權人所採取禁止或限制他人擅自進入著作之防盜拷措施，未經合法授權　不得予以破解、破壞或以其他方法規避之。」

[9] 著作權法第 96-1 條：「有下列情形之一者，處 1 年以下有期徒刑、拘役，或科或併科新臺幣 2 萬元以上 25 萬元以下罰金：一、違反第 80 條之 1 規定者。二、違反第 80 條之 2 第 2 項規定者。」

A.18.1.1 適用之法規及契約的要求事項之識別

對每個資訊系統及組織，應明確識別、文件化及保持更新所有相關法律、法令、法規及契約要求事項，以及組織為符合此等要求之作法。

五、其他

類別：資訊保護【案號：S1050501】

ATM 資安危機，政府急滅火

【焦點話題】

第一銀行自動櫃員機(下稱 ATM)遭盜領，金融監督管理委員會(下稱金管會)要求一個月內解決國內 ATM 資安危機。金管會發函要求銀行公會研擬強化 ATM 安全控管基準，並要求銀行建立 ATM 運作監控機制，1 個月內要把具體方案送交金管會。

據悉，銀行公會已初步對強化 ATM 管理擬具四大措施：第一、建議 ATM 委外管理部分，應交回銀行內部執行運作；第二、建立 ATM 汰換機制，讓一定年限以上 ATM 淘汰，避免過時；第三、強化技術面的硬體操作，例如拿掉 USB 埠、光碟機，或在 ATM 植入監控程式，隨時監測領錢狀況是否異常，並即時回報；第四、列出程式白名單，不在名單上的程式就予以監控或刪除，讓惡意程式較難有機可趁。

金管會銀行局局長表示，未來是否要求銀行 ATM 不得委外維護，或是對國外 ATM 機器設備廠商有更嚴格的要求，像是主動通報問題設備等，「要等檢調機關先調查本次犯罪事件發生的詳細原因，才能進一步檢討」，但已要求銀行公會 1 個月內要對強化 ATM 安全控管提出報告。

【資料來源：工商時報，105/7/14】

【重點摘要】

1. 金融機構安全維護管理辦法已要求銀行就 ATM 安全維護措施，除應評估其安全性並慎選設置地點以外，尚須建立異常提領監控機制，以利銀行於偵測有異常情形時，盡速採取適當措施。

2. 因應 ATM 遭大量盜領事件，銀行須檢討現行 ATM 設備本身安全防護機制能否有效防堵此類攻擊事件，以及既有異常監控與內部應變流程能否因應新興詐騙手法，以降低此類事件發生並降低風險。

【法律觀點】

第一銀行 ATM 遭盜領事件引發社會大眾關注，並促使主管機關要求銀行檢討如何改善安全防護措施，以提高應變因應能力並降低日後再度發生此類盜領事件之風險。財政部早於民國 85 年時核備「金融機構自動櫃員機安全防護準則」，該準則提供銀行針對 ATM 安裝地點、機體及周遭設備、警報系統、閉路電視錄影監視系統、補鈔安全及其他相關安全防護機制，尤其該準則已規定「金融機構宜視需要，裝設具有偵測自動櫃員機運作狀態之遠程監控系統，藉由其對狀況或故障原因之自動分析、自動叫修等功能，提昇管理效率及安全防護」，建議銀行於必要時，得透過遠端監控系統即時掌握 ATM 運作情形。

另，金管會依銀行法授權訂定之「金融機構安全維護管理辦法」，更進一步要求銀行就 ATM 安全維護措施，除應評估其安全性並慎選設置地點以外，尚須「建立自動櫃員機異常提領監控機制，指定專人負責。如查有異常情形，應儘速採取適當措施，妥善處理。不定時巡查自動櫃員機，防範歹徒破壞(假日及非營業時間尤為重要)，並予以記錄」[1]，規定銀行應建立異常監控機制。是以，本次第一銀行 ATM 遭大量盜領事件發生後，銀行恐須檢討現行採取安全防護機制是否有效防堵此類攻擊事件，以及既有異常監控與內部應變機

[1] 金融機構安全維護管理辦法第 6 條：「金融機構對其營業處所、金庫、出租保管箱（室）、自動櫃員機及運鈔業務等執行安全維護措施，應依下列規定辦理：.....三、自動櫃員機安全維護措施（一）自動櫃員機裝置時，應詳確評估其安全性，慎選設置地點。對非設置於營業處所之行外自動櫃員機，須考量管轄單位是否方便監督管理，並優先選擇有保全設備或有警衛、值勤人員巡守 之處所。（二）自動櫃員機應裝置於明亮處所。 （三）對設置之自動化服務設備，應張貼進行交易應注意事項，設置防盜安全設備、防止他人窺視與使用者得察覺後方情況之設施、照明及必要之防火逃生設備等。（四）應督導營業單位，加強派員巡查行內外設置之自動櫃員機使用情形、門禁及相關防護設施。（五）建立自動櫃員機異常提領監控機制，指定專人負責。如查有異常情形，應儘速採取適當措施，妥善處理。不定時巡查自動櫃員機，防範歹徒破壞（假日及非營業時間尤為重要），並予以記錄.....。」

制能否因應新興詐騙手法，以降低此類事件發生並盡可能透過強化監控機制而降低損害。

【管理 Tips】

第一銀行 ATM 遭盜領事件震驚社會，此事件不只是給銀行業一個警訊，更是提醒各大企業與政府單位，需嚴肅面對資訊安全議題。此事件的發生，並非僅是 ATM 設備的問題，而是反映出管理面的議題。各大企業與政府單位皆需有適切的資訊安全管理系統，並將其融入至日常作業中。首先，在人員方面，組織需定期向員工宣導資訊安全政策以及執行資訊安全認知訓練。在駭客攻擊與社交工程手法層出不窮的環境下，需定期更新資訊安全管理系統以及教育訓練內容，讓員工可以隨時瞭解企業規範與外在環境的威脅，並做出適當的回應。

其次，在軟體方面，組織需定期更新系統版本以及維持防毒軟體為最新版本。定期執行弱點掃描與滲透測試，以瞭解內外部網路的漏洞，並做及時的修補。防火牆需定期更新，並嚴格控管開放的通信埠。再者，在存取權限方面，需規劃組織人員的職掌清冊。依據權責分工的觀念給予員工適當的存取權限，且妥善保管通行碼，並做好內部網路之區隔，加強內部網路之安全性。

最後，在供應商方面，視單位需求規劃服務契約。組織需將資訊安全考量納入契約之要求，令供應商嚴格遵守，並定期對供應商執行監督與審查程序。綜合上述幾項，皆為資訊安全的控制點，但要做好完善的資訊安全，光靠這些是遠遠不夠。組織需依據各單位實際狀況，建立與規劃適切的資訊安全管理系統，傳達至全體員工並落實於日常作業，才能達到有效的防範與管理。

【相關標準】

ISO/IEC 27001：2013(CNS 27001)

A.7.2.2 資訊安全認知、教育及訓練

組織所有員工及相關之約用人員，均宜接受與其工作職能相關的組織政策

及程序之適切認知、教育及訓練，並定期更新。

A.9.2.2 使用者存取權限之配置

宜實作正式之使用者存取權限配置程序，以對所有形式之使用者對所有系統及服務，指派或撤銷存取權限。

A.9.4.3 通行碼管理系統

通行碼管理系統宜為互動式，並宜確保嚴謹通行碼。

A.12.2.1 防範惡意軟體之控制措施

宜實作防範惡意軟體之偵測、預防及復原控制措施，並合併適切之使用認知。

A.12.6.1 技術脆弱性管理

宜及時取得關於使用中之資訊系統的技術脆弱性資訊，並宜評估組織對此等脆弱性之暴露，且宜採取適當措施以因應相關風險。

A.13.1.3 網路之區隔

宜區隔各群組織資訊服務、使用者及資訊系統使用的網路。

A.15.1.1 供應商關係之資訊安全政策

宜與供應商議定並以文件記錄，降低與供應商存取組織資產關聯之風險的資訊安全要求事項。

A.15.2.1 供應者服務之監視及審查

組織宜定期監視、審查及稽核供應者服務交付。

類別：資訊保護【案號：S1050502】

美政府發布第一份政府部門資安事件應變指導指令

【焦點話題】

據報載，由於部分美國政府部門承認面對駭客攻擊時缺少明確的因應對策，所以歐巴馬總統在今(105)年 7 月 26 日發布一份名「美國政府網路事件協調之總統政策指令」(Presidential Policy Directive on United States Cyber Incident Coordination)，試圖在這份指令當中提出具體方向。這份指令是美國第一次針對網路攻擊應變之政府部門分工所發布，希望能夠因應越來越多且變化多端的網路攻擊事件。

這份指令最大的特點之一，是定義網路事件的範圍及處理原則。除此之外，也指出資安事件應變工作應有的三大軸線。首先，應包含網路事件之執法及國家安全調查工作，因而聯邦調查局及國家網路調查聯合行動小組必須出面處理事件調查及蒐證工作。其次，為對受影響單位提供技術性援助，以縮小或控制影響範圍，國土安全部應會同國家網路安全及通訊調查中心出面主導資產應變工作。至於情報相關支援工作，則由國家情報總監辦公室會同國家網路安全及通訊調查中心負責辦理。在這份指令中特別表示，網路事件應變的三大軸線缺一不可，遇有特別嚴重之網路事件時，將適度安排其他政府部門介入以提供必要協助。

【資料來源：REUTERS，105/7/26】

【重點摘要】

1.為妥善處理網路事件應變工作，應先定義網路事件範圍，並訂定應變處理原則。

2.為縮小或控制網路事件影響範圍，應考量事件調查、資產協助及情報支援等層面之應變，並適度安排及協調相關政府部門之工作。

【法律觀點】

為處理政府部門資訊安全之議題，美國今年 7 月發布一份名「美國政府網路事件協調之總統政策指令」，在這份指令中首先定義網路事件範圍，凡可能對於國家安全利益、外交關係、美國經濟、公眾信心、民眾自由或大眾健康與安全產生危害之網路攻擊事件，均屬之；而網路事件將依嚴重程度不同，從 0 至 5 分為 6 個不同等級。為聚焦網路事件處理成效，這份指令特別提出處理原則，包括：責任分擔、資安應變以風險為基礎、尊重受影響單位、追求整理作業效益考量，以及盡可能恢復原狀。

對照之下，我國主要以「行政院及所屬各機關資訊安全管理要點」，以及「行政院及所屬各機關資訊安全管理規範」進行處理，惟上述規範僅為行政規則之位階，且設計之初主要著眼於個別機關內之政策制定或具體措施執行，對於不同機關對於資安工作之分工協調等事項著墨較少，其面對重大資安事件時是否及如何採取有效應變，實不無疑問。為突破此一現實狀況，日前國內著手研議「資通安全管理法」草案，從其立法意旨來看[1]，本草案將資通安全提升為國家安全之層次，並將資通安全推動組織提升為行政院層級[2]，其規範幅展實不同於以往。其中，針對資通安全事件處理，本草案[3]主要明定公務機關應制定預防、通報及應變機制；遇有重大資通安全事件時，應向主管機關通報並提出矯正預防計畫；至於資安事件如涉有刑責之虞，相關之公務機關應妥適保全相關資料，並通報司法機關。

整體而言，美國新指令在資安事件定義、應變原則及政府部門分工協調等，均有不同以往之設計；尤其是政府部門間之分工，其不僅著重於資安事件之

---

[1] 資通安全管理法草案第 1 條：「為積極推動國家資通安全政策及加速建構國家資通安全環境，以確保民眾數位生活福祉、資通安全產業發展及數位國土國家安全，特制定本法。」

[2] 資通安全管理法草案第 7 條第 1 項：「行政院為推動國家資通安全政策，應設國家資通安全會報，並設行政院資通安全辦公室，置專職人員，處理有關業務，其組織由行政院定之。」

[3] 資通安全管理法草案第 14 條：「公務機關為因應資通安全事件，應制定預防、通報及應變機制。公務機關遇有重大資通安全事件者，應向主管機關通報，並應於事件發生次日起一定期間內，向主管機關提出矯正預防計畫。資通安全事件如有涉及刑責之虞，相關之公務機關應妥適保全相關資料，包括但不限於數位證據及軌跡紀錄，並應通報司法機關。第一項預防、通報及應變機制之內容、第二項重大資通安全事件矯正預防計畫之內容及第三項之資料保全內容及方式及其他應遵循事項，由主管機關定之。」

調查及蒐證，更從資產及情報支援之角度切入納入相關單位之協助，對於協助受影響單位及早回復業務運作將更具正面效益，值得我國推動後續立法之參考。

【管理 Tips】

就本案而言，網路事件可能危害國家安全、經濟利益、外交關係、公眾信心、健康安全與公民自由等議題，因而此項議題別具重要性，政府與企業必須投入更多的資源方能防範未然。而在此項議題之因應上，政府與企業不僅應事先規畫適宜之網路安全架構，尚應進一步考量面臨特定資安事件(例如，駭客攻擊、病毒入侵等)時如何執行緊急應變措施，才能將資產損失降到最低，並且盡可能回復單位業務運作。

面對網路上不可預期的威脅，組織應先建立資安事件應變之政策，並使組織成員確實知悉。而在具體作法上，除了需要對於本身弱點有所了解，並應事前預測特殊事件發生時之可能危害，並將不同危害予以分級，而後規劃相對應之應變策略或處理方式，才能在資安事件發生時發揮最大的防護效果。

【相關標準】

ISO 27001：2013(CNS 27001)

A.5.1.1 資訊安全政策

資訊安全政策宜由管理階層定義並核准，且對所有員工及相關外部各方公布及傳達。

A.7.2.2 資訊安全認知、教育及訓練

組織所有員工及相關之約用人員，均宜接受與其工作職能相關的組織政策及程序之適切認知、教育及訓練，並定期更新。

A.13.1.1 網路控制措施

宜管理及控制網路，以保護資訊系統及應用。

A.16.1 資訊安全事故及改善之管理

確保對資訊安全事故之管理的一致及有效作法，包括對安全事件及弱點之傳遞。

A.16.1.4 對資訊安全事件之評鑑及決策

宜評鑑資訊安全事件，並決定是否將其歸類為資訊安全事故。

A.16.1.5 對資訊安全事故之回應

宜依以文件記錄程序，回應資訊安全事故。

貳、資訊公開(Disclosure)

一、政府資訊公開法

類別：資訊公開【案號：D1050101】

政府農安資訊公開有落差？90 件資訊申請僅 4 件給資訊！

【焦點話題】

在全民環保意識高漲之今日，農地污染防制問題日益受到各界重視，日前國內知名環境保護團體發起「守護農地計畫」，特別針對政府農地安全資訊公開情形進行研究，在做法上透過政府資訊公開平臺及公文兩種途徑，向農地相關之中央及地方機關提出資訊公開申請，申請資訊項目包括農地污染源、灌溉水質追蹤、農業區工廠及農舍興建等資訊。

然而，依據該團體針對調查結果之研究分析，發現其所提出之 90 件政府資訊申請案，截至民國(下同)105 年 3 月底為止，僅有 86 件獲得回覆，其餘則全無音訊；而在所收到之回覆內容中，絕大多數案件均係拒絕提供資訊，其理由不外於：(1)現有資訊不足；(2)資訊尚未整理完成；(3)該機關不具提供之資訊之權限；(4)該資訊涉及個人資訊保護，或屬於限制公開之資訊，而無法提供。自上述研究分析結果中，可歸納政府並未提供資訊之原因有兩大類，其一是機關目前尚未建置完整之業務資訊而無法進一步提供，其二則是機關基於法律上之理由而無法提供資料。

依據報載，在該團體所提出之 90 件政府資訊申請中，最後僅有 4 件獲提供完整原始資訊，分別來自澎湖及屏東。此一調查結果公布後，外界針對政府是否確實掌握農地資訊，或是否確實依法公開政府資料，引發不同之揣測聲音，就此，政府宜再思考正面且適切之因應處理方式。

【資料來源：環境資訊電子報，105/5/26】

【重點摘要】

1. 機關對其於職權範圍內作成或取得之政府資訊，原則上應依法對外公開特定資訊項目。

2. 政府資訊涉及個人資料時，如符合公益目的、經當事人同意或具備其他法定要件時，機關依法仍應公開資訊、不得任意拒絕。

【法律觀點】

為便利人民共享與公平利用政府資訊，增進人民對公共事務之瞭解、信賴及監督，我國早在 94 年即制定政府資訊公開法作為準據，其第 9 條[1]、第 10 條[2]規定，民眾得依法定申請程序向政府申請提供資訊。而針對機關於職權範圍作成或取得之政府資訊，如民眾依法申請提供時，除非符合該法第 18 條所定限制公開或不予公開之情形[3]，受理之機關即應予提供。在本案中，

---

[1] 政府資訊公開法第 9 條：「具有中華民國國籍並在中華民國設籍之國民及其所設立之本國法人、團體，得依本法規定申請政府機關提供政府資訊。持有中華民國護照僑居國之國民，亦同。外國人，以其本國法令未限制中華民國國民申請提供其政府資訊者為限，亦得依本法申請之。」

[2] 政府資訊公開法第 10 條：「向政府機關申請提供政府資訊者，應填具申請書，載明下列事項：一、申請人姓名、出生年月日、國民身分證統一編號及設籍或通訊地址及聯絡電話；申請人為法人或團體者，其名稱、立案證號、事務所或營業所所在地；申請人為外國人、法人或團體者，並應註明其國籍、護照號碼及相關證明文件。二、申請人有法定代理人、代表人者，其姓名、出生年月日及通訊處所。三、申請之政府資訊內容要旨及件數。四、申請政府資訊之用途。五、申請日期。前項申請，得以書面通訊方式為之。其申請經電子簽章憑證機構認證後，得以電子傳遞方式為之。」

[3] 政府資訊公開法第 18 條：「政府資訊屬於下列各款情形之一者，應限制公開或不予提供之：一、經依法核定為國家機密或其他法律、法規命令規定應秘密事項或限制、禁止公開者。二、公開或提供有礙犯罪之偵查、追訴、執行或足以妨害刑事被告受公正之裁判或有危害他人生命、身體、自由、財產者。三、政府機關作成意思決定前，內部單位之擬稿或其他準備作業。但對公益有必要者，得公開或提供之。四、政府機關為實施監督、管理、檢 (調) 查、取締等業務，而取得或製作監督、管理、檢 (調) 查、取締對象之相關資訊，其公開或提供將對實施目的造成困難或妨害者。五、有關專門知識、技能或資格所為之考試、檢定或鑑定等有關資訊，其公開或提供將影響其公正效率之執行者。六、公開或提供有侵害個人隱私、職業上秘密或著作權人之公開發表權者。但對公益有必要或為保護人民生命、身體、健康有必要或經當事人同意者，不在此限。七、個人、法人或團體營業上秘密或經營事業有關之資訊，其公開或提供有侵害該個人、法人或團體之權利、競爭地位或其他正當利益者。但對公益有必要或為保護人民生命、身體、健康有必要或經當事人同意者，不在此限。八、為保存文化資產必須特別管理，而公開或提供有滅失或減損其價值之虞者。九、公營事業機構經營之有關資訊，其公開或提供將妨害其經營上之正當利益者。但對公益有必要者，得公開或提供之。政府資訊含有前項各款限制公開或不予提供之事項者，應僅就其他部分公開或提供之。」

各主管機關所保有之農地安全資訊(以下簡稱農安資訊)屬於政府資訊，因而其本應依循政府資訊公開法之規定確實辦理。如機關人員在不符合法定事由之情形下無故拒絕提供政府資訊，可能因此構成該法第 23 條[4]而受到懲戒或懲處。

其次，針對政府資訊限制公開或不予公開之事由，政府資訊公開法第 18 條業已明定其具體情形。其中，針對涉及個人資料之部分雖屬於限制公開或不予公開之範圍，惟該條第 6 款規定亦指出，如對公益有必要或為保護人民生命、身體、健康有必要或經當事人同意者，不在此限。法務部法律字第 10100253980 號函中曾明確表示，針對姓名或其他個人資訊以編號顯示，僅公開其餘未涉隱私部分，且匿名化或去識別化處理，此種情形無從識別特定個人而無侵害隱私權之虞。因此，在本案中，從環保團體所公布之調查結果，可以發現農地相關主管機關拒絕提供政府資訊之理由，「該資訊涉及個人資訊保護，或屬於限制公開之資訊」為其中大宗。惟自法律觀點以觀，農地安全之資訊涉及公眾利益，符合資訊限制公開之例外，機關本應依法公開；如認為有損及個人資料或民眾隱私之虞，實可考慮提供其他未涉隱私之部分，或以匿名化或去識別化之方式處理，不宜一概地以「涉及個人資料」為由，一概地拒絕提供農安資訊，因而限制人民對公共事務之瞭解、信賴及監督等權利之行使，致使人民對政府之信賴受到影響。

【管理 Tips】

政府機關對於公眾事務本應依法善盡職責，如有蒐集或作成資訊之權責時，面對尚未整理完成而無法對外提供之情形，宜進一步說明預計完成之時點。而政府資訊公開為既定政策，因而機關不僅應仔細盤點所保有之政府資料並擬訂利用政策，同時對於相對產生之資訊安全風險，亦宜採取適當之管理措施。

另由於政府資訊公開法第 20 條規定：「申請人對於政府機關就其申請提供、

[4] 政府資訊公開法第 23 條：「公務員執行職務違反本法規定者，應按其情節輕重，依法予以懲戒或懲處。」

更正或補充政府資訊所為之決定不服者，得依法提起行政救濟。」因此，機關因應政府資訊公開政策時，宜建立完善之資訊管理標準作業程序，不僅可以避免申請人之疑義，也可減少行政訴訟之成本。

【相關標準】

ISO 27001：2013(CNS 27001)

A.18.1.1 適用之法規及契約的要求事項之識別

對每個資訊系統及組織，應明確識別、文件化及保持更新所有相關法律、法令、法規及契約要求事項，以及組織為符合此等要求之作法。

A.18.1.4 個人可識別資訊之隱私及保護

應依適用之相關法令、法規中之要求，以確保個人可識別資訊之隱私及保護。

類別：資訊公開【案號：D1050102】

公告欠稅戶洩個資？ 賦稅署：公平正義

【焦點話題】

財政部每年 7 月 1 日必須針對個人累計欠稅超過新臺幣(下同)1000 萬元或企業累計欠稅超過 5,000 萬元的確定案件辦理公告，且公告資訊必須在各稅捐稽徵機關網站刊登 6 個月，一直到每年 12 月 31 日為止才移除。至於欠稅大戶的公告內容，依法規定包括欠稅人姓名或名稱(如果是公司，一併公告其負責人姓名及地址)、欠稅稅目、欠稅年度、欠稅或罰鍰金額(含滯納金、利息、滯報金、怠報金)及欠稅人地址等。

國稅局官員表示，過去也曾經有民眾因為不想被公告為欠稅大戶，在國稅局公告前一刻出面繳納稅金，例如某高球好手的叔叔曾經是欠稅大戶，就因此由家人出面代繳稅款並協商繳稅事宜，後來都沒有再被列為欠稅大戶。對此，民眾質疑公告欠稅大戶姓名有違反個人資料保護法的嫌疑，賦稅署則回應，相關公告依照「稅捐稽徵機關依稅捐稽徵法第 34 條第 1 項」規定辦理，公告重大欠稅案件目的在於維護租稅公平正義，希望透過公告達成追稅效果，並無違反個人資料保護法的規定。

【資料來源：蘋果日報，105/7/02】

【重點摘要】

1.稅務人員對於納稅義務人提供之財產、所得、營業及納稅等資料，除符合例外情形外，負有絕對保密義務。

2.對於公告重大欠稅案件或重大逃漏稅捐案件，稅捐稽徵機關應於執行法定職務必要範圍內為之，並與蒐集之特定目的相符。

【法律觀點】

課稅資料常涉及納稅人之身分、所得、財產或營業狀況，例如綜合所得稅牽涉個人所得來源、投資狀況、存款機構及扶養親屬等個人資料，而房屋稅、地價稅及使用牌照稅的資料，涉及個人名下的高價值資產，營業稅涉及營業收入、客戶、進貨廠商等資訊，甚者公司組織之營利事業辦理所得稅結算申報，其所檢附之人才培訓、研究發展等資料，更可能涉及智慧財產權。稅務人員對於納稅義務人提供之財產、所得、營業及納稅等資料，依照稅捐稽徵法第 33 條[1]規定，原則上負絕對秘密義務，若稅務人員因公務疏失洩漏上開資料，除得處以 1 萬元以上 5 萬元以下罰鍰外[2]，亦可能因此觸犯刑法第 132 條「公務員洩漏國防以外秘密罪」，得處 1 年以下有期徒刑、拘役或 300 元以下罰金[3]。

另外，稅捐稽徵機關對已確定的重大欠稅案件或重大逃漏稅捐案件，依稅捐稽徵法第 34 條第 1 項規定，得公告其欠稅人或逃漏稅捐人姓名或名稱與內容，以有效防止大戶逃漏稅捐。依個人資料保護法第 16 條，公務機關對個人資料之利用，應於執行法定職務必要範圍內為之，並與蒐集之特定目的相符。本案國稅局除了公布欠稅人姓名、欠稅稅目、欠稅年度、欠稅金額等資料外，亦一併公布欠稅人地址，恐有疑義。在實務作業上僅公告欠稅人地址所在路段，並未公布完整門牌號碼。此項資訊雖非法定應公告事由，惟可避免同名之其他無辜民眾遭誤認為欠稅人，以防止他人權益受損。不過，在處理個案地址資訊之揭露時，國稅局仍應注意所公告之內容有無逾越必要範圍之情形。

【管理 Tips】

為確保國家稅收，機關應加強宣導民眾繳納稅賦義務，與民眾持續適切的溝

---

[1] 稅捐稽徵法第 33 條第 1 項：「稅捐稽徵人員對於納稅義務人之財產、所得、營業、納稅等資料，除對下列人員及機關外，應絕對保守秘密：一、納稅義務人本人或其繼承人。二、納稅義務人授權代理人或辯護人。三、稅捐稽徵機關。四、監察機關。五、受理有關稅務訴願、訴訟機關。六、依法從事調查稅務案件之機關。七、經財政部核定之機關與人員。八、債權人已取得民事確定判決或其他執行名義者。」

[2] 稅捐稽徵法第 43 條第 3 項：「稅務稽徵人員違反第 33 條規定者，處 1 萬元以上 5 萬元以下罰鍰。」

[3] 刑法第 132 條第 1、2 項：「公務員洩漏或交付關於中華民國國防以外應秘密之文書、圖畫、消息或物品者，處 3 年以下有期徒刑。因過失犯前項之罪者，處 1 年以下有期徒刑、拘役或 300 元以下罰金。」

通，使民眾瞭解繳納稅賦之意義與責任。除此以外，對於未依法繳稅之民眾，依稅捐稽徵法第 34 條規定，機關可公開欠稅人之姓名及欠稅內容。

在本案中，機關公開欠稅人資料雖有法可循，惟仍不免引發疑慮，因而必須格外審慎。詳言之，除了法律允許公開之個資項目及內容外，其餘無論是欠稅人地址、欠稅或罰鍰金額與稅目別，均須受到妥善保護。政府機關執行業務之過程中，往往掌握大量民眾資訊，因而需有完善的資訊管理程序與個人資料保護作業，以保護資訊的安全，降低其風險。

【相關標準】

ISO 27001：2013(CNS 27001)

A.18.1.1 適用之法規及契約的要求事項之識別

對每個資訊系統及組織，應明確識別、文件化及保持更新所有相關法律、法令、法規及契約要求事項，以及組織為符合此等要求之作法。

A.18.1.4 個人可識別資訊之隱私及保護

應依適用之相關法令、法規中之要求，以確保個人可識別資訊之隱私及保護。

類別：資訊公開【案號：D1050103】

某政府機關拒絕陸港澳學者調閱資料

【焦點話題】

某政府機關收藏大量 1949 年前政府相關檔案，一直是兩岸研究近代中國史學者重要的學術資源，但某政府機關近來修訂相關檔案文件借閱規定，拒絕陸港澳學者申請調閱館藏，並將國內學者申請預約時間延長為 15 天，一改過去到館「隨借隨看」模式，引發學界質疑。

某政府機關表示，「跟任何政治因素都無關，是依規定來做的」。某政府機關是依據政府資訊公開法(下稱政資法)規定與檔案管理局借閱資料相關規範，修訂某政府機關資料閱覽規定。鑒於依政資法規定，非中華民國國民之外國人申請借閱資料，乃依據平等互惠原則開放，而中國大陸地區一直沒有對我方開放資料查閱，故某政府機關的做法只是依法行政。

另外，某政府機關訂定資料閱覽規定，將國內學者申請借閱檔案的作業時間延長至 15 天，同樣是根據檔案管理局行之有年的規範。由於事涉機密或含有個人資料的檔案，需經主管機關逐件審查並准駁，故審查期間調整為 15 日。

【資料來源：聯合晚報，105/7/29】

【重點摘要】

1.具有我國國籍並在我國設籍之國民及其所設立之本國法人與團體、持有我國護照之僑民，以及該國法令未限制我國國民申請提供其政府資訊之外國人，得依法向我國政府機關申請閱覽政府資料。

2.政府機關原則上應於受理申請更正或補充政府資訊之日起 30 日內為准駁決定。

【法律觀點】

依我國政資法規定，具有中華民國國籍並在中華民國設籍之國民及其所設立之本國法人與團體、持有我國護照之僑民，以及該國法令未限制我國國民申請提供其政府資訊之外國人等三類民眾，得依該法規定申請政府機關提供政府資訊。因此，若不屬上開三類申請對象，則無從依政資法向其他機關申請檔案資料。另外，就「是否提供外國人閱覽我國政府資料」，政資法為便於資訊跨國流通並兼顧我國民權益，係採取平等互惠原則，對於外國人向我國政府機關申請提供政府資訊者，以其本國法令未限制我國國民申請提供其政府資訊者，始能依該法規定申請。

故某政府機關訂定之「檔案及政府資訊開放應用須知」第 2 條，即依前開規定限定某政府機關未公開資料閱覽之申請資格[4]，而陸港澳學者非屬我國國民[5]，且中國大陸亦未依平等互惠原則給予我國國民申請其政府資料之權利，故其民眾自不得依政資法規定向我國機關申請提供政府資訊。

又，政府機關依政資法第 15 條及檔案法第 19 條規定，原則上應於受理申請更正或補充政府資訊之日起 30 日內為准駁決定[6]，故政府機關應於前開期限內決定是否提供閱覽。因此，某政府機關若修訂本身政府資訊申請作業相關規定，規定於受理後 15 日作成准駁決定，尚符合相關法規規定之審酌期間。

【管理 Tips】

某政府機關掌理中華民國史與臺灣史的修纂和研究，館內藏有豐富的史料與

---

[4] 國史館民國 98 年 10 月 2 日國秘字第 0980003882 號函訂定發布國史館檔案及政府資訊開放應用須知第 2 條：「具有下列資格者得申請閱覽政府資訊：（一）中華民國國民及其所設立的法人、團體。（二）持有中華民國護照之僑胞。（三）平等互惠國之外國人。已開放閱覽之檔案不受上述限制。」

[5] 法務部 97 年 5 月 19 日法律字第 0970009804 號函、法務部 104 年 7 月 29 日法律字第 10403509360 號參照

[6] 政資法第 15 條：「政府機關應於受理申請更正或補充政府資訊之日起三十日內，為准駁之決定；必要時，得予延長，延長之期間不得逾三十日。第 9 條、第 11 條及第 12 條第 2 項至第 4 項之規定，於申請政府機關更正或補充政府資訊時，準用之。」檔案法第 19 條：「各機關對於第 17 條申請案件之准駁，應自受理之日起三十日內，以書面通知申請人。其駁回申請者，並應敘明理由。」

重要的歷史檔案。此情形下，應有妥善的資產管理、維護以及人員的行為控管。從管理面的觀點來說，政府單位需規劃明確的資產管理措施。

首先，需識別出管轄內的所有資產，再依據單位環境制定出適切的資產分類級別。接著，依據資產的重要性歸納至各分類級別中，根據不同分類級別進行資產標示，以提醒使用者。再依照各分類級別所規劃的資產管理方式，確實地進行控管與維護。以此，來制定各分類之資產借出與歸還制度。

其次，對於管轄內的人員控管，不管是內部職員或是外來訪客，都需制定相關規範。對於內部職員，需在聘用前做嚴密的篩選程序，任職期間需參與資訊安全認知訓練與了解應盡的責任義務，解聘後需終止相關權限與歸還單位資產；對於外來訪客，需執行訪客進出入紀錄與訪客設備攜出入紀錄，可過濾有心訪客與防止資產透過媒體外洩。

綜合以上描述，可加強政府單位在資產管理面有更嚴謹的程序，並搭配實體環境的監控設備，以達到更有效的控管以降低外洩疑慮。

【相關標準】

ISO/IEC 27001：2013(CNS 27001)

A.7.1.1 篩選

對所有可能被聘用者所進行之背景調查，宜依相關法律、法規及倫理，並宜相稱於營運要求及其將存取之資訊的保密等級及組織所察覺之風險聘用。

A.7.2.2 資訊安全認知、教育及訓練

組織所有員工及相關之約用人員，均宜接受與其工作職能相關的組織政策及程序之適切認知、教育及訓練，並定期更新。

A.7.3.1 聘用責任之終止或變更

宜對員工及約用人員定義、傳遞於聘用終止或變更後，資訊安全責任及義

務仍保持有效，並執行之。

A.8.1.1 資產清冊

宜識別資訊，並識別與資訊及資訊處理設施相關聯之其他資產，且宜製作並維護此等資產之清冊。

A.8.1.4 資產之歸還

所有員工及委外方使用者於其聘用、契約或協議終止時，宜歸還其據有之全部組織資產。

A.8.2.1 資訊之分級

資訊應依法律要求、價值、重要性及對未經授權揭露或修改之敏感性分級。

A.8.2.3 資產之處置

應依組織所採用之資訊分級方案，發展及實作處置資產之程序。

A.9.2.1 使用者註冊及註銷

宜實作正式之使用者註冊及註銷過程，俾能指派存取權限。

A.11.1.2 實體進入控制措施

保全區域宜藉由適切之進入控制措施加以保護，以確保僅允許經授權人員進出。

類別：資訊公開【案號：D1050104】

Google 釋出開放圖片資料輯，供社群用以訓練機器學習模型

【焦點話題】

Google 與美國卡內基美隆大學、康乃爾大學合作建立 Open Images 資料輯，Open Images 資料輯含有高達 900 萬筆、涵蓋 6,000 種圖片的 URL，且圖片標籤所涉及的實體品項類別，比目前 ImageNet 電腦視覺模型的 1,000 種更多。Google 表示，這些圖片種類的數量足以用來訓練深度神經網路，且這些圖片是採用「創用 CC-姓名標示」通用版條款授權。

根據 Google 的說明，圖片中的標籤是用類似 Google 雲端視覺 API(Google Cloud Vision API)的視覺模型自動標註，這個視覺模型能夠分析圖片中的內容並加以歸類。Google 表示，平均每張圖片會有 8 個標籤，需要透過人工驗證自動標籤正確性，以移除錯誤的標籤。

【資料來源：iThome，105/10/3】

【重點摘要】

1.Google 與學術機構蒐集以「創用 CC-姓名標示」條款授權釋出之圖片，建立開放圖片資料輯，以利在最開放的授權條款下，提供機器學習社群或任何使用者自由取用。

2.創用 CC 是一套制式化開放授權契約條款，符合著作權人所設定之授權條件所為之利用，即視同已取得著作權人授權，而無庸再行取得同意，以降低授權成本與合理使用空間模糊的問題。

【法律觀點】

電腦科學與相關領域中的機器學習是下一代人工智慧發展的重要關鍵，因此 Google 與學術機構共同合作，釋出開放圖片資料輯，該資料輯包含大量以「創

用 CC-姓名標示」授權釋出的圖片 URL，以及對應圖片內容的標籤。

所謂創用 CC 是一套制式化開放授權契約條款，提供著作權人從「姓名標示」、「非商業性」、「禁止改作」及「相同方式分享」四大要素中，自行排列組合選擇適當的授權條件[7]，當使用者符合著作權人所設定的授權條件時，即等同已取得著作權人之授權，而無庸另行取得同意。例如當著作權人選擇以「創用 CC-姓名標示-非商業性-相同方式分享」釋出攝影作品時，任何人只要標示作者姓名並從事非商業性用途時，即符合授權條件，至於使用者若欲調整攝影作品光影、粒度或修改圖片內容而涉及改作時，改作完成作品亦須以相同條款即「創用 CC-姓名標示-非商業性-相同方式分享」釋出，始符合前述授權條件，否則即須另行取得著作權人授權或由法院認定是否屬於合理使用，故此類開放授權條款相對降低授權成本與合理使用空間模糊造成的風險。

研究社群為開發圖像辨識技術，須要大量圖片素材作為測試分析資源，然而圖片著作權人未必同意使用者複製圖片或進行編輯調整，因此 Google 與學術機構蒐集以「創用 CC-姓名標示」條款授權釋出之圖片，並結合圖片主題標籤內容建立一開放資料輯後，以最為寬鬆的創用 CC 授權釋出[8]，讓機器學習社群或任何使用者在標示資料貢獻者後即可取用，有助於運用充分、免費且允許自由運用的圖像與實物標籤資源，讓研究者從資料抓取與分類過程，訓練深度神經網絡。

【管理 Tips】

組織在對外分享資訊資產時，應確保開放之資產符合公司規定，且資產有受到法律效力的規範，更無違反任何法令、法規之要求。以此為前提下，組織應明確界定公開之資產，才可有效的運用其價值。而外部組織在使用此資訊資產時，可瞭解此資產的使用方式與使用條件，免於擔憂觸碰法律限制。

---

[7] 因姓名標示為必要授權條件，而禁止改作與相同方式分享本質互斥，故四個授權要素共組成六種授權條款。

[8] 故「創用 CC-姓名標示」是六大授權條款中最為寬鬆者，但目前有 CCO 條款，亦即不要求使用者須標示著作人姓名，對使用者而言等若在著作利用上無特別限制。

法律、法規和合約的要求可以對具有所有權的資產進行限制，而創用 CC 授權是在既有著作權法架構下，由著作權人透過契約方式聲明授權條件，以利使用者在符合授權條件時即可取得授權，因此當使用者利用以創用 CC 授權釋出的著作時，須受授權條件所拘束，否則即非屬著作權人事先授權範圍。

【相關標準】

ISO/IEC 27001：2013(CNS 27001)

A.18.1.1 適用之法規及契約的要求事項之識別

對每個資訊系統及組織，應明確識別、文件化及保持更新所有相關法律、法令、法規及契約要求事項，以及組織為符合此等要求之作法。

A.18.1.2 智慧財產權

適當程序應加以實作，以確保遵循智慧財產權與所使用的專屬軟體產品的相關法律、法規及契約要求。

參、資訊監察(Monitors)

一、通訊保障及監察法

類別：資訊監察【案號：M1050101】

檢查賄選監聽掛錯線　里長獲國賠 10 萬

【焦點話題】

某地檢署於民國(下同)99 年查察賄選案件時，曾至 A 議員服務處進行搜索，B 辦案人員當場查獲 1 只公事包內有 1 支手機，隨即將手機號碼抄錄在紙條上，並確認該手機為 A 議員所有。B 辦案人員在完成搜索後，不慎將抄錄手機號碼紙條遺失，並在陰錯陽差下將 C 里長手機號碼誤認是 A 議員之手機號碼，於是持該手機號碼向法院聲請核發通訊監察書後，進行長達 26 天之監聽。

本案發生之後，C 里長因為受到地方耳語指為賄選而困擾不已，在輾轉查訪後發現自己竟在地檢署一連串錯誤下遭到監聽，憤而以侵害秘密通訊自由、隱私權及人格權為由，向法院對該地檢署提出高達新臺幣(下同)160 萬元國賠，並要求地檢署在四大報登報道歉，最後法院判決地檢署應賠償 10 萬元。

【資料來源：蘋果日報 105/1/11】

【重點摘要】

1. 監聽涉及秘密通訊自由之侵害，因而公務機關應在符合監聽要件與程序之情形下始得為之。
2. 公務機關如違反監聽規定致他人權益受有損害時，須依國家賠償法負損害賠償責任。

【法律觀點】

為保障人民秘密通訊自由與隱私權不受非法侵害，並確保國家安全，維護社會秩序，我國於 88 年 7 月 14 日即制定通訊保障及監察法，並於 105 年

4 月 13 日修正。依據本法第 5 條[1]規定，如有事實足認被告或犯罪嫌疑人涉犯特定罪嫌，並危害國家安全、經濟秩序或社會秩序情節重大，而有相當理由可信其通訊內容與本案有關，且不能或難以其他方法蒐集或調查證據者，得向法院申請核發通訊監察書。由於監聽行為涉及對秘密通訊自由之侵害，因而必須符合上開嚴格法定要件及程序，始得為之；而對於違法監聽致遭他人權益受到侵害之情形，本法第 19 條與第 24 條分別訂有民事賠償責任及相關刑事罰則；本法第 23 條並進一步規定，民事賠償責任原則

[1] 通訊保障及監察法第 5 條：「有事實足認被告或犯罪嫌疑人有下列各款罪嫌之一，並危害國家安全、經濟秩序或社會秩序情節重大，而有相當理由可信其通訊內容與本案有關，且不能或難以其他方法蒐集或調查證據者，得發通訊監察書。一、最輕本刑為 3 年以上有期徒刑之罪。二、刑法第 100 條第 2 項之預備內亂罪、第 101 條第 2 項之預備暴動內亂罪或第 106 第 3 項、第 109 條第 1 項、第 3 項、第 4 項、第 121 條第 1 項、第 122 條第 3 項、第 131 條第 1 項、第 142 條、第 143 條第 1 項、第 144 條、第 145 條、第 201 條之 1、第 256 條第 1 項、第 3 項、第 257 條第 1 項、第 4 項、第 298 條第 2 項、第 300 條、第 339 條、第 339 條之 3 或第 346 條之罪。三、貪污治罪條例第 11 條第 1 項、第 4 項關於違背職務行為之行賄罪。四、懲治走私條例第 2 條第 1 項、第 2 項或第 3 條之罪。五、藥事法第 82 條第 1 項、第 4 項或第 83 條第 1 項、第 4 項之罪。六、證券交易法第 173 條第 1 項之罪。七、期貨交易法第 112 條或第 113 條第 1 項、第 2 項之罪。八、槍砲彈藥刀械管制條例第 12 條第 1 項、第 2 項、第 4 項、第 5 項或第 13 條第 2 項、第 4 項、第 5 項之罪。九、公職人員選舉罷免法第 102 條第 1 項第 1 款之罪。十、農會法第 47 條之 1 或第 47 條之 2 之罪。十一、漁會法第 50 條之 1 或第 50 條之 2 之罪。十二、兒童及少年性剝削防制條例第 32 條第 1 項、第 3 項、第 4 項、第 5 項之罪。十三、洗錢防制法第 11 條第 1 項至第 3 項之罪。十四、組織犯罪防制條例第 3 條第 1 項後段、第 2 項後段、第 6 條或第 11 條第 3 項之罪。十五、陸海空軍刑法第 14 條第 2 項、第 17 條第 3 項、第 18 條第 3 項、第 19 條第 3 項、第 20 條第 5 項、第 22 條第 4 項、第 23 條第 3 項、第 24 條第 2 項、第 4 項、第 58 條第 5 項、第 63 條第 1 項之罪。十六、營業秘密法第 13 條之 2 第 1 項、第 2 項之罪。十七、森林法第 52 條第 1 項、第 2 項之罪。十八、廢棄物清理法第 46 條之罪。前項通訊監察書，偵查中由檢察官依司法警察機關聲請或依職權以書面聲請該管法院核發。聲請書應記載偵、他字案號及第 11 條之事項，其監察對象非電信服務用戶，應予載明；並檢附相關文件及監察對象住居所之調查資料，釋明有相當理由可信其通訊內容與本案有關，且曾以其他方法調查仍無效果，或以其他方法調查，合理顯示為不能達成目的或有重大危險情形。檢察官受理聲請案件，應於四小時內核復；如案情複雜，得經檢察長同意延長四小時。法院於接獲檢察官核轉受理聲請案件，應於四十八小時內核復。審判中由法官依職權核發。法官並得於通訊監察書上對執行人員為適當之指示。前項聲請不合法定程序、不備理由、未經釋明或釋明不足者，法院應予駁回。其聲請經法院駁回者，不得聲明不服。執行機關應於執行監聽期間內，每十五日至少作成一次以上之報告書，說明監聽行為之進行情形，以及有無繼續執行監聽之需要。檢察官或核發通訊監察書之法官並得隨時命執行機關提出報告。法官依據經驗法則、論理法則自由心證判斷後，發現有不應繼續執行監聽之情狀時，應撤銷原核發之通訊監察書。通訊監察書之聲請，應以單一監察對象為限，同一偵、他字或相牽連案件，得同時聲請數張通訊監察書。」

上適用民法及國家賠償法之規定。

有關本案，針對錯誤監聽之行為，台南地方法院 103 年度國字第 9 號判決表示：「任何人皆享有其私人生活、家庭生活、居住與通訊受尊重之權利，該權利之行使，不受公權力之侵犯；而電話監聽乃對人民權利之嚴重干預，僅能在存有合理懷疑人民涉及『嚴重犯罪活動』等重大事由時，始得據以核發監聽許可。」、「原告因本件錯誤監聽，致使其自 99 年 12 月 6 日 10 時起至同年月 31 日 10 時止，其秘密通訊自由權、隱私權遭受侵害，則被告所屬公務員之過失行為與原告之損害結果間，具有相當因果關係，應堪認定，從而，原告之秘密通訊自由以及隱私權因被告職員過失不法侵害行為生損害，自應負國家賠償責任。」由此可知，對於 B 辦案人員之烏龍監聽行為，雖然並非出於故意，法院仍認為構成違法監聽，而有國家賠償法之適用，即地檢署應負賠償責任。是以，未來機關如有需要進行監聽之情形，宜特別審慎檢視是否確實符合法定要件及程序，特別是監聽對象之正確性，以免無端造成民眾權益之受損，同時背負法律責任。

【管理 Tips】

公務機關依法行使公權力應謹慎小心，執行過程需確保資訊之完整性。在程序上有如此重大疏失，導致政府機關名譽受損，浪費警力資源，更影響民眾生活。以檢警監聽為例，為符合通訊保障及監察法之資訊安全管理要求及程序，公務機關需建立正確之驗證機制與簽核制度，並將其融入所有流程制度中；檢警人員在執行監聽工作前，需確認每個環節的正確性，並在確認後提交管理階層簽核，以確保所有執行工作之完整性，之後才開始執行監聽工作。而在執行監聽工作時，亦應有適當之監督機制以確保工作過程之正確與完整，如有疏失亦可及早發現。

除此以外，公務機關需依照資訊安全管理及個人資料保護規範，定期進行教育訓練及宣導，除了要求全員參與外，必須依不同業務性質之單位，講解如何落實日常作業管理。如有違反資訊安全規範者，應規劃適當處置方

式與改善措施，藉此讓全體同仁皆有資訊安全管理之觀念。

【相關標準】

ISO 27001：2013(CNS 27001)

A.7.2.1 管理階層責任

管理階層應要求所有員工及承包者，依組織所建立政策及程序施行資訊安全事宜。

A.7.2.2 資訊安全認知、教育及訓練

組織所有員工及相關之承包者，均應接受與其工作職能相關的組織政策及程序之適切認知、教育及訓練，並定期更新。

A.7.2.3 懲處過程

應具備正式及已傳達之懲處過程，以對違反資訊安全之員工採取行動。

A.12.4.1 事件存錄

應產生、保存並定期審查紀錄使用者活動、異常、錯誤及資訊安全事件之事件日誌。

A.18.1.4 個人可識別資訊之隱私及保護

應依適用之相關法令、法規中之要求，以確保個人可識別資訊之隱私及保護。

類別：資訊監察【案號：M1050102】

網購竊聽軟體探人私密 使用者及販賣者都判刑

【焦點話題】

某縣檢調單位於民國(下同)104 年間接獲民眾檢舉，指稱某網站，刊有以「Android Remote Backup Tools」(安卓遠端備份工具)為題之廣告，內文提供手機監控軟體檔案下載，並附有軟體安裝與操作之教學影片連結。檢調人員循線偵辦後，發現該網站由甲所架設與經營，而其於網站所推銷之手機監控軟體，宣稱具有竊聽通話紀錄、簡訊紀錄、衛星定位、網路定位及 LINE 文字訊息等功能，其並提供民眾 3 天試用期，試用後如感到滿意，則可以每月使用費新臺幣(下同)600 元之代價訂購該竊聽軟體。

乙受到該網站廣告內容吸引，因而向經營該網站的甲購買，並將該竊聽軟體下載並安裝於友人丙手機中，藉此竊聽其電話聊天內容以及掌握手機定位。本案查獲後，乙犯行連帶曝光，丙才發現自己之通話紀錄、簡訊、手機定位及 LINE 的聊天紀錄等私密通訊內容，早就被乙一覽無遺，因此憤而向法院提告。

【資料來源：自由時報，105/7/19】

【重點摘要】

1. 透過非法軟體竊聽或竊錄他人非公開談話，不僅侵害他人隱私，也可能涉犯妨害秘密或違法監察之犯罪。

2. 販賣竊聽或竊錄軟體屬意圖營利而供給工具或設備，將面臨較重之刑責。

【法律觀點】

我國於 88 年 4 月在刑法第 315 條之 1 增訂「無故利用設備窺視竊聽他人非公開活動及談話罪」後，如無故利用工具或設備窺視、竊聽他人非公開

之活動或談話者，最高可處 3 年有期徒刑[2]，當時的立法理由即明確表示：「目前社會使用照相、錄音、錄影、望遠鏡及各種電子、光學設備者，已甚普遍。惟以之為工具，用以窺視、竊聽、竊錄他人隱私活動、言論或談話者，已危害社會善良風氣及個人隱私，實有處罰之必要，爰增列本條，明文處罰之」。除了窺視或竊聽行為會受到處罰以外，如意圖營利供給場所、工具或設備，便利他人進行窺視竊聽行為者，同法第 315 條之 2 第 1 項則有加重規定，最高可處 5 年有期徒刑[3]。此外，我國通訊保障及監察法(以下簡稱通保法)為保障人民秘密通訊自由及隱私權不受非法侵害，該法第 24 條第 1 項即對違法監察他人通訊者定有刑責，可處以 5 年以下有期徒刑；針對意圖營利之行為，同條第 3 項更有加重處罰之規定。

在本案中，針對乙購買軟體安裝於丙手機以竊聽通話之行為，檢方原以違反刑法第 315 條之 1 第 1 項第 1 款為由提起公訴。惟一審法院認為[4]，通保法第 24 條第 1 項並未限定於公務員，乙雖非公務人員仍有本項規定之適用[5]。最後以乙的行為，同時涉犯通保法第 24 條第 1 項之違法監察他人通訊罪，以及刑法第 315 條之 1 第 1 款之無故利用設備窺視、竊聽他人非公開活動及談話罪，判處 3 個月有期徒刑。

至於甲販售竊聽軟體的行為，檢方原以違反刑法第 315 條之 2 第 1 項提起公訴。惟一審法院認為，通保法第 24 條第 1 項及第 3 項均未限制犯罪主體為公務員，因而甲雖非公務人員仍有此二項規定之適用。最後以甲之行為，

---

[2] 刑法第 315 條之 1：「有下列行為之一者，處 3 年以下有期徒刑、拘役或 30 萬元以下罰金：一、無故利用工具或設備窺視、竊聽他人非公開之活動、言論、談話或身體隱私部位者。二、無故以錄音、照相、錄影或電磁紀錄竊錄他人非公開之活動、言論、談話或身體隱私部位者。」

[3] 刑法第 315 條之 2：「意圖營利供給場所、工具或設備，便利他人為前條第 1 項之行為者，處 5 年以下有期徒刑、拘役或科或併科 5 萬元以下罰金。意圖散布、播送、販賣而有前條第 2 款之行為者，亦同。製造、散布、播送或販賣前 2 項或前條第 2 款竊錄之內容者，依第 1 項之規定處斷。前 3 項之未遂犯罰之。」

[4] 通保法第 24 條：「違法監察他人通訊者，處 5 年以下有期徒刑。執行或協助執行通訊監察之公務員或從業人員，假借職務或業務上之權力、機會或方法，犯前項之罪者，處 6 月以上 5 年以下有期徒刑。意圖營利而犯前 2 項之罪者，處 1 年以上 7 年以下有期徒刑。」

[5] 另可參最高法院 101 年度台上字第 3416 號刑事判決。

同時涉犯通保法第 24 條第 3 項之意圖營利違法監察他人通訊罪，以及刑法第 315 條之 2 第 1 項之意圖營利而提供窺視竊聽設備罪，判處 1 年 2 個月有期徒刑。

綜上所述，使用竊聽軟體侵害他人隱私甚鉅，將同時違反刑法第 315 條之 1 與通保法第 24 條之規定，如販賣竊聽或竊錄軟體屬意圖營利而供給工具或設備，將面臨較重之刑責。因此不論是販售或使用相關產品者，均應注意產品功能是否涉及不法侵害他人隱私，以避免觸法。

【管理 Tips】

此事件可以由兩個面向來探討。首先，從軟體開發的角度來看，廠商在軟體開發前需規劃完整的軟體開發生命週期，其中包含各階段的資通安全要求事項與查核點；在開發中，需遵守制定的開發原則，並於適當的環境下進行研究；在最後，需進行安全與驗收測試，經此流程才可確保軟體的安全性。

其次，從軟體使用的角度來看，使用過程中如接觸到個人資料與隱私資訊時，系統需具備保護機密資訊的功能。且軟體在使用消費者資料時，需設定告知使用者是否同意授權之互動式流程，讓使用者瞭解個人資料的流向、面臨的風險與受到的保護措施。

上述為軟體基本具備的條件，開發商與消費者皆需瞭解自身的義務與權利，才能妥善保護機密資料的安全，將風險降到最低。

【相關標準】

ISO 27001：2013(CNS 27001)

A.14.2.1 保全開發政策

宜建立軟體及系統開發之規則，並應用至組織內之開發。

A.18.1.4 個人可識別資訊之隱私及保護

應依適用之相關法令、法規中之要求，以確保個人可識別資訊之隱私及保護。

類別：資訊監察【案號：M1050103】

側錄員工電郵挨告 前董座與代總經理無罪

【焦點話題】

甲控訴公司前董事長與代總經理指示部屬側錄其電子郵件，涉犯刑法妨害秘密罪與通訊保障及監察法等規定。甲提告時表示，公司未在勞動契約或員工工作規則規定得監控或側錄員工電子郵件，亦未曾公告公司會進行監控與側錄。在此情形下，前董事長指示代總經理與其他部屬側錄包含甲與其他員工之非公開電子郵件，認為前董事長與代總經理侵犯員工隱私，且已違反刑法妨害秘密罪、通訊保障及監察法(以下簡稱通保法)，以及個人資料保護法(以下簡稱個資法)等規定，因而對二人提出告訴。

法官調查後認為，該公司有權稽核員工的公務電子郵件，且本案是因為公司調查一件合約洩密案才查到甲之電子郵件，並非專門針對甲個人進行調查，因而判決前董事長與前代總經理均無罪。

【資料來源：自由時報，105/7/14】

【重點摘要】

1. 員工之職場隱私權應受到保護與重視，公司如無故監看或側錄員工電子郵件，仍有誤觸民事、刑事責任之風險。
2. 對於公務電子郵件之監看、側錄或稽核，公司應建立明確的政策，並使員工清楚知悉，以避免後續爭議。

【法律觀點】

有關公司可否監看(聽)或側錄員工之電子郵件或電話，我國先前曾引發討論。而此一問題之最大困難點，主要在於公司內部管理與員工隱私權如何取得平衡。以目前司法實務見解而言，多會取決於兩項判斷因素，其一是「員工有無合理之隱私期待」，其二則是「公司管理手段是否符合目的性與

比例性」。針對「員工有無合理之隱私期待」，國內司法實務多認為員工於職場上之活動仍具有合理隱私期待。而為確保員工之合理隱私期待，公司倘欲進行監看或監聽，應符合以下要件：(一)告知後取得員工同意，或揭示公司資訊監看政策且員工未表示反對；(二)應具有正當理由，例如保護營業秘密或公司其他權利；(三)與工作相關且符合目的性與比例性。至於「公司管理手段是否符合目的性及比例性」，則是指公司如欲採取監看或監聽之行為，必須與其管理目的有合理的關聯，且不得對於員工權益造成過度侵害。而公司在未遵循前述原則的情況下，對員工進行監看或監聽，仍可能構成對員工隱私權之侵害，而因此負有民、刑事責任。

在本案中，甲認為公司在未取得員工同意或進行公開之情形下，擅自對員工之電子郵件進行監看或側錄，已然侵害其職場隱私權，因而以刑法第 315 條之 1[6]第 2 款之妨害秘密罪、通保法第 24 條[7]第 1 項之違法監察他人通訊罪、以及個資法第 41 條[8]第 1 項等罪名向法院提起自訴。

在一審判決[9]中，法院延續國內司法實務見解，認同員工於公司中具有職場隱私權，惟認為公司前董事長及代總經理之行為並不涉及違法。首先，本案起因於公司追查某件合約洩密案件，而以該合約部分名稱為關鍵字進行搜尋與側錄，由於所搜尋者為員工之公務電子郵件，不涉及其私人通訊，因而認為不構成刑法第 315 條之 1 第 2 款的妨害秘密罪。其次，公司對於電子郵件搜尋或側錄之結果多為甲的郵件一事，應無法事先預見，因而欠缺蒐集或處理其個人資料之犯意，因而也不構成個資法第 41 條之罪。最

[6] 刑法第 315 條之 1：「有下列行為之一者，處 3 年以下有期徒刑、拘役或 30 萬元以下罰金：一、無故利用工具或設備窺視、竊聽他人非公開之活動、言論、談話或身體隱私部位者。二、無故以錄音、照相、錄影或電磁紀錄竊錄他人非公開之活動、言論、談話或身體隱私部位者。」

[7] 通保法第 24 條：「違法監察他人通訊者，處五年以下有期徒刑。執行或協助執行通訊監察之公務員或從業人員，假借職務或業務上之權力、機會或方法，犯前項之罪者，處 6 月以上 5 年以下有期徒刑。意圖營利而犯前 2 項之罪者，處 1 年以上 7 年以下有期徒刑。」

[8] 個資法第 41 條：「意圖為自己或第三人不法之利益或損害他人之利益，而違反第 6 條第 1 項、第 15 條、第 16 條、第 19 條、第 20 條第 1 項規定，或中央目的事業主管機關依第 21 條限制國際傳輸之命令或處分，足生損害於他人者，處 5 年以下有期徒刑，得併科新臺幣 100 萬元以下罰金。」

[9] 臺南地方法院 104 年度自字第 11 號刑事判決。

後，公司前董事長及代總經理之行為，乃是出於追查公司弊案，而公司員工對於公司之電子信箱僅可作為公司業務使用、公司得隨時進行稽查之要求應可預見，故亦不構成通保法第 24 條第 1 項之違法監察他人通訊罪。

【管理 Tips】

首先，組織與員工之間的各種權利義務關係，需在勞動或聘用合約內盡可能詳細闡明。同時，組織應主動且明確地告知員工公司相關規範，並要求詳細閱讀自身權利後，雙方再行簽署合約。

組織內的各項規定須透過電子檔或紙本之形式，有效地傳達給全體同仁瞭解，且盡可能擺放至公共區域讓同仁可隨時取閱。而組織需定期舉辦認知教育訓練，以確保同仁們確實明白相關規範內容，以避免後續爭議。

就本案而言，組織可否監看或側錄員工電子郵件，原則上應視組織之規範內容而言，而該規定應有效地傳達給全體同仁。員工固然具有職場隱私權，惟組織如有明確規定且在工作範圍內，應盡可能予以配合組織規範。

【相關標準】

ISO 27001：2013(CNS 27001)

5.2 政策

最高管理階層應建立包含下列事項之資訊安全政策

(e) 以文件化資訊提供。

(f) 於組織內傳遞。

(g) 適用時，提供給關注方。

A.7.2.1 管理階層責任

管理階層應要求所有員工及承包者，依組織所建立政策及程序施行資訊安全事宜。

A.7.2.2 資訊安全認知、教育及訓練

組織所有員工及相關之承包者，均應接受與其工作職能相關的組織政策及程序之適切認知、教育及訓練，並定期更新。

類別：資訊監察【案號：M1050104】

不能移送帳號 網路性騷難法辦

【焦點話題】

網路陌生人性騷擾案件有增加趨勢，卻難以究責，曾有當事人的臉書連日收到陌生帳號私訊傳送女子性愛照片，覺得很噁心，截圖後報案遭性騷擾；檢警認為性騷擾事證明確，卻因臉書公司不提供加害人資料，難以究責，當事人只能將對方「封鎖」，希望別再被騷擾。

某縣市家防中心表示，以往性騷擾案件以肢體碰觸居多，較易揪出加害人，如今網路性騷擾案增加，105 年 1 到 8 月接到 22 件性騷擾申訴案，半數是陌生人騷擾，其中 8 案是陌生網友透過臉書或 LINE 傳送猥褻訊息，受害者多為未成年少女及妙齡女子。

追查臉書使用者的身分，雖可請臉書公司配合提供使用者申請資料、登入紀錄，檢方說，臉書是外國公司，不在我國司法主權裡，不一定能如願；目前實務上，臉書只提供關於涉及殺人、重傷害等犯罪者的註冊人個資。

【資料來源：聯合新聞網 105/09/21】

【重點摘要】

1. 外國公司在境外蒐集、處理或利用我國人民之個人資料，仍應適用我國個人資料保護法規定。
2. 保管個人資料之機關，基於協助調查社會秩序維護事件之目的，得交付警察機關個人資料，而不違反個資法。

【法律觀點】

近來許多犯罪常以網路作為傳播媒介，藉由網路的匿名性與傳播性，達到其犯罪目的及隱藏其真實身分。為了犯罪偵查或維護自身權益，警察機關

或被害人，往往會要求網站管理者提供加害人的個人資料，藉此追查其真實身分及取得其犯罪證據。

臉書公司雖設在國外，但依個資法第 51 條第 2 項：「公務機關及非公務機關，在中華民國領域外對中華民國人民個人資料蒐集、處理或利用者，亦適用本法。」臉書公司如欲將我國用戶的個資提供與第三人使用，仍適用我國個資法規定。

依個資法第 15 條[10]第 1 款，公務機關在符合特定目的且於執行法定職務必要範圍內，得對個人資料之蒐集或處理。關於性騷擾事件，依性騷擾防治法第 13 條第 2 項[11]規定，在性騷擾加害人不明時，主管機關應移請事件發生地主管機關調查；且依社會秩序維護法第 39 條[12]及第 83 條[13]第 3 款規定，對於有猥褻之言語、舉動或其他方法，調戲異性者，警察機關亦有立即調查之義務。顯見調查此類網路性騷擾案件，乃是屬警察機關的「執行法定職務必要範圍內」，得依個資法第 15 條向其他機關蒐集資料[14]。

另外，非公務機關對於個人資料的利用，僅有個資法第 20 條[15]列舉的事由

---

[10] 個人資料保護法第 15 條：「公務機關對個人資料之蒐集或處理，除第 6 條第 1 項所規定資料外，應有特定目的，並符合下列情形之一者：一、執行法定職務必要範圍內。二、經當事人同意。三、對當事人權益無侵害。」

[11] 性騷擾防治法第 13 條第 2 項後段：「加害人不明或不知有無所屬機關、部隊、學校、機構或僱用人時，應移請事件發生地警察機關調查。」

[12] 社會秩序維護法第 39 條：「警察機關因警察人員發現、民眾舉報、行為人自首或其他情形知有違反本法行為之嫌疑者，應即開始調查。」

[13] 社會秩序維護法第 83 條：「有左列各款行為之一者，處新臺幣 6000 元以下罰鍰：一、故意窺視他人臥室、浴室、廁所、更衣室，足以妨害其隱私者。二、於公共場所或公眾得出入之場所，任意裸體或為放蕩之姿勢，而有妨害善良風俗，不聽勸阻者。三、以猥褻之言語、舉動或其他方法，調戲異性者。」

[14] 法務部 104 年 1 月 27 日法律字第 10403501210 號函參照。

[15] 個人資料保護法第 20 條第 1 項：「非公務機關對個人資料之利用，除第 6 條第 1 項所規定資料外，應於蒐集之特定目的必要範圍內為之。但有下列情形之一者，得為特定目的外之利用：一、法律明文規定。二、為增進公共利益所必要。三、為免除當事人之生命、身體、自由或財產上之危險。四、為防止他人權益之重大危害。五、公務機關或學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。六、經當事人同意。七、有利於當事人權益。」

下，才能例外為特定目的外之利用。而參考法務部見解[16]，警察機關基於調查社會秩序維護事件之需要，而由非公務機關提供個人資料，亦應符合個資法第 20 條第 1 項第 2 款「為增進公共利益所必要」之要件。因此，臉書得基於協助調查社會秩序維護事件之目的，交付警察機關個人資料，並不違反個資法之規定 。

然而據報導，臉書公司目前受理協助調查的案件，僅有殺人、毒品、組織犯罪、擄人勒贖、兒少、妨害電腦使用等 6 大犯罪類型。對於性騷擾等案件，並不接受。由於臉書公司設在境外，無法直接受我國主管機關規範，惟實務上，警察機關仍可透過加害人遺留之資料，查出其實際身分，以保障被害人權益。

【管理 Tips】

此事件可以從兩個角度來思考，其一，以廠商與消費者之間；其二，以廠商與警方之間。

首先，當民眾在網路上面對到類似事件時，需先留存訊息、紀錄以求自保，可利用複製、拍照等方式，將記錄用電子的方式儲存下來，以利後續報案程序。而廠商在提供服務時，需有儲存客戶資料的相關設計，以輔助事件發生時可調閱紀錄。要注意的是，資料儲存設計是存放在客戶端，只需提供操作手冊教導客戶如何獲取訊息，但如果資料是儲存在廠商伺服器，則廠商有義務事先告知消費者，讓其瞭解個人資料會被如何運用，並承諾保護機敏資料，以防止資料外洩的風險。

再者，當廠商面對警方類似事件的要求，需參考現行法律、法令之要求制定相關對應程序，並符合公司規範的前提下全力協助，以防止類似事件的延續。且公司需讓消費者瞭解個人機敏資料所受到的保護與運用，經由使用者的同意，並確保隱私及個人可識別資訊受到管控。

[16] 法務部 104 年 1 月 27 日法律字第 10403501210 號函參照。

【相關標準】

ISO 27001：2013(CNS 27001)

A.18.1.3 紀錄之保護

宜依法令、法規、契約及營運要求保護紀錄，免於遺失、毀損、偽造、未經授權存取及未經授權發布。

A.18.1.4 個人可識別資訊之隱私及保護

應依適用之相關法令、法規中之要求，以確保個人可識別資訊之隱私及保護。

肆、資訊應用(Application)

一、電子簽章法

類別：資訊應用【案號：A1050101】

日本政府測試指紋支付系統，外國旅客購物一指搞定

【焦點話題】

據報載，為刺激觀光，日本政府已規劃測試並可能採納一套指紋支付系統，讓國外觀光客可以憑指紋即在日本當地消費購物。國外旅客前往日本觀光，基於防範恐怖攻擊需求，入境審查時必需註冊指紋與拍攝臉部照片，而日本政府希望進一步將指紋辨識從安全拓展到觀光應用，讓國外觀光客訪日旅遊時，能夠在指定商家以指紋取代信用卡或現金付款，日本政府長期目標是希望在 2020 年前將該系統擴展至日本各地熱門景點，趕上東京奧運熱潮。

國外觀光客在使用這項服務前，必須先註冊個人的指紋與信用卡等資料，以利後續確認付款人身分與支付工具。日本政府推動指紋支付系統，除提高消費購物上的便利並交易驗證安全以外，亦擬透過此系統蒐集國外觀光客在日本各地旅遊的資料，例如觀光地點、頻率及消費金額，透過這些資料分析擬定進一步的觀光策略。

【資料來源：iThome，105/4/11】

【重點摘要】

1. 日本政府推動以生物辨識為識別機制之支付服務，提供外國觀光客以指紋作為授權特約商店自其指定銀行帳戶或信用卡等支付工具扣款之確認機制。

2. 我國公務機關或非公務機關在我國境內蒐集外國人個資仍應遵守個資法相關作業要求，以符合保障個人資訊自主與資訊隱私之權利。

【法律觀點】

鑒於聲紋、虹膜或指紋等生物辨識機制係運用個人具有識別性之特徵，有助於提高身分檢核正確性與確保使用者同一性，故隨著生物辨識技術發展，越來越多服務導入生物辨識作為身分識別機制，而日本政府即在此風潮下，希望能提供外國觀光客以指紋作為辨識、確認之機制，讓授權特約商店能從外國觀光客指定之銀行帳戶或信用卡等支付工具扣款，以簡化消費付款流程，日後亦希望能進一步將指紋辨識作為觀光客入住旅館時出示護照辦理登記時的輔助查核措施。

然而，日本政府導入此服務需先將外國觀光客生物辨識與支付工具資料進行建檔，始能提供特約商店連線至該系統確認指紋是否相符，故涉及大規模個人資料蒐集、處理及利用。若我國政府欲採取相似作法，應先進行評估，例如，依我國個人資料保護法，公務機關在我國境內蒐集、處理、利用外國人個資時，應符合特定目的，因此，是否得直接將原意在保護國家安全而蒐集之資料，用於觀光客進行支付時之身分確認，或應否另取得當事人同意或甚至須透過立法或修法方式始得為之，均應進行評估，以確認其合法性。且即使在可合法建置外國觀光客支付服務系統之情形，就資料之保有及提供以進行身分確認，均應進一步採取適當安全維護措施。且若政府機關日後欲從指紋使用紀錄，分析研究外國觀光客消費情形，亦應判斷是否符合原初蒐集之特定目的範圍，若否，即應符合特定目的外利用之其一事由，以符合保障個人資訊自主與資訊隱私之權利。

【管理 Tips】

使用資訊科技已經成為無法避免之趨勢，但是在運用新興科技提供商業服務時，資訊安全應為首要考量。根據個人資料保護法第 2 條第 1 款 5 之規定，指紋乃屬於個人資料之範疇。個人資料之保存與運用，蒐集指紋應具備特定目的與符合法定事由。企業及政府機關在決定蒐集、處理、利用個人資料時，需事先做好合法性評估，後續對資料之保管及使用，亦須謹慎做好安全措施，確實建立起資訊安全管理機制，並落實於組織作業流程中。

指紋辨識雖不是新技術，但將其運用在支付消費上卻是新的模式，當大量指紋資料建檔後的資料庫管理，應有嚴密且高規格之控管措施。新的商業模式，勢必會面臨新的風險考量。如防止指紋被竊取、盜用之議題等等，將會是此類服務推廣的第一道難題。

【相關標準】

ISO/IEC 27001：2013(CNS 27001)

A.8.1.3 資產之可被接受使用

對與資訊及資訊處理設施相關聯之資訊及資產，應識別、文件化及實作可被接受使用之規則。

A.8.2.3 資產之處置

應依組織所採用之資訊分級方案，發展即時作處置資產之程序。

A.9.2.1 使用者註冊及註銷

應實作正式之使用者註冊及註銷過程，俾能指派存取權限。

A.9.2.2 使用者存取權限之配置

應限制及控制具特殊存取權限之配置及使用。

類別：資訊應用【案號：A1050102】

銀行業護資安 三招出擊

【焦點話題】

為迎接 Bank 3.0 時代、因應金管會有關金融科技(FinTech)之新政策，國內銀行業者主動採取三大資安防護措施，以力保網路安全，讓民眾安心透過行動式載具享受金融機構提供的服務。而這三大資安防護措施包括：善用行動載具或銀行提供的生物辨識功能、動態密碼以及銀行加密系統。

針對生物辨識，以聲紋為例，係採用聲音的波長、頻率、強度或節奏等逾 130 種特徵值組成，每個人的聲紋都獨一無二。據報載，目前已有國內銀行業者主動導入「聲紋辨識」，讓聲音直接成為客戶的密碼，15 秒可以完成身分認證，採用自然對談驗證，以提高偽造冒用之難度。針對動態密碼，目前許多國內銀行業者在網路辦理信用貸款、信用卡網路交易過程，即透過動態密碼來進行客戶身分認證；而所謂動態密碼採取二階段身分認證機制，過去使用者在提供帳號與密碼之後，會被要求再輸入一組由系統發送到手機的認證碼，該認證碼是一次性使用。除此以外，因應數位金融服務之開放，國內銀行業者另會針對客戶資料傳輸至銀行後端系統之過程，透過資料加密方式嚴加控管。透過各項資安防護措施，對於客戶進行網路交易應能提供更有效之保障。

【資料來源：經濟日報，105/8/2】

【重點摘要】

1.有關電子銀行之交易安全，除身分認證及交易確認外，交易過程中就所傳輸之資料予以加密，也是必要之資安防護措施。

2.除電子簽章外，目前金融實務針對低風險交易允許使用動態密碼、生物辨識或其他認證方式。

【法律觀點】

為因應行動通訊、社群媒體、大數據及雲端科技等資通訊技術之進步，銀行業者必順應時代潮流，以及配合資訊發展，以提升消費者便利性。基於此一考量，我國金融監督管理委員會(以下簡稱「金管會」)於民國(下同)104年1月宣布全面啟動「打造數位化金融環境3.0」計畫，放寬既有存款戶在現行電子銀行與行動銀行得辦理金融業務類型，並鬆綁銀行辦理低風險交易電子銀行業務報部核備程序規定。在同一時間，美國商會於同一年6月4日提出「2015臺灣白皮書」，其中對於我國銀行業務，建議參採國際間銀行業者之營運慣例，修改相關法規及自律規範，使銀行業者可採用不同之身分認證技術以進行大額支付之銀行服務。為此，銀行公會乃推動相關規範之檢視及調整工作，並於105年3月18日發布金融機構辦理電子銀行業務安全控管作業基準之最新修正版本。

依據新規定，電子銀行之各項交易依其交易風險類別分為高風險及低風險類別；如非低風險類別所列舉之交易活動，則屬於高風險交易。客戶進行低風險交易時，銀行業者得提供動態密碼、視訊會議或其他方式作為交易介面之安全設計[1]；所謂其他方式包含生物辨識技術在內，即由客戶提供給銀行業者其所擁有之生物特徵(例如指紋、臉部、虹膜、聲音、掌紋或靜脈等)，而由銀行業者依其風險承擔能力來調整生物特徵之錯誤接受度，以有效識別客戶身分。而針對法人客戶之高風險交易，為確保對客戶之權益保障，新規定「交易再確認機制」可採取動態密碼、生物辨識或其他方式，尚且要求銀行業者在傳送敏感資料時，應提供端點對端點加密機制(如end-to-end encryption, E2EE)，於客戶端輸入資料時立即加密，傳送至銀行端之硬體安全模組，以避免中間人竊取[2]。上述新規定攸關客戶權益保障，銀行業者應充分留意新規定發布後之因應策略，而此等規定之落實未來也會成為金融監理的查核重點之一。

---

[1] 金融機構辦理電子銀行業務安全控管作業基準第7條第3款及第4款內容。

[2] 金融機構辦理電子銀行業務安全控管作業基準第9條第9款。

【管理 Tips】

面對近期國內外金融業資安事件，使得國內銀行業者開始產生警覺，並且化被動為主動，透過各項資安措施之採取，來抑止資訊安全漏洞之惡化，並消除民眾使用服務之顧慮。

以國內銀行業者常採取之資安防護措施來看，無非是透過個人識別性與金鑰複雜度之強化，來提高網路攻擊之難度。例如，生物辨識之獨特性，能讓客戶密碼不易竊取、仿造及遺失。例如，動態密碼則是附加驗證機制，再次確認使用者身分。至於加密系統，則是強化相關資料在傳輸時的安全，避免遭到破解或竊取。而需要提醒的是，除了強化前端服務線之資訊安全，仍需防護後台設備之資訊安全；包括定期維護硬體設備與更新系統、防毒軟體版本，且隨時保持監控並留下紀錄追蹤，均為可考慮的防護措施。

【相關標準】

ISO 27001：2013(CNS 27001)

A.9.4.3 通行碼管理系統

通行碼管理系統宜為互動式，並宜確保嚴謹通行碼。

A.10.1.1 使用密碼式控制措施之政策

宜發展及實作政策，關於資訊保護之密碼式控制措施的使用。

A.10.1.2 金鑰管理

宜發展及實作政策，關於貫穿其整個生命週期之密碼金鑰的使用、保護及生命期。

A.11.2.4 設備維護

宜正確維護設備，以確保其持續知之可用性及完整性。

A.12.2.1 防範惡意軟體之控制措施

宜實作防範惡意軟體之偵測、預防及復原控制措施，並合併適切之使用認知。

A.16.1.7 證據之蒐集

組織宜定義及應用程序，以識別、蒐集、獲取及保存可用作證據之資訊。

類別：資訊應用【案號：A1050103】

金管會修法鬆綁電子支付相關法規，改善行動支付體驗

【焦點話題】

考量到約定連結存款帳戶付款的便利性及適度降低電子支付機構作業成本，金融監督管理委員會日前修正電子支付機構業務管理規則第２條及第１２條條文，關於約定連結存款帳戶付款機制等規定。

金管會表示，考量約定連結存款帳戶付款的便利性，並適度降低電子支付機構作業成本，所以修正電子支付機構業務管理規則第２條第８款有關約定連結存款帳戶付款的業務運用範圍，也擴及收受儲值款項業務及電子支付帳戶間款項移轉業務。

此外，電子支付機構提供使用者以約定連結存款帳戶付款進行儲值服務，其方式包括由使用者自行發動的「主動儲值」，以及在支付款項餘額不足支付時發動的「自動儲值」，為適度控管風險及維護使用者權益，所以增列電子支付機構業務管理規則第１２條第６項規定，要求電子支付機構提供使用者以約定連結存款帳戶付款進行自動儲值服務，應與使用者約定每筆及每日自動儲值的限額，並提供使用者隨時調整限額及停止自動儲值的機制。

【資料來源：法源編輯室，105/9/3】

【重點摘要】

1.本次電子支付法規修正後，電子支付業者得提供消費者以連結存款帳戶，進行電子帳戶款項移轉與儲值。

2.消費者可透過約定連結存款帳戶，進行轉帳並儲值於電子支付帳戶，當電子支付帳戶餘額不足時，亦得由電子支付業者自動向金融機構發出扣款指示進行加值，以提升電子支付帳戶管理之便利性。

【法律觀點】

金融監督管理委員會(下稱金管會)在 105 年 8 月陸續研訂「電子支付機構使用者身分確認機制及交易限額管理辦法」、「電子支付機構資訊系統標準及安全控管作業基準辦法」及「電子支付機構業務管理規則」修正草案，並自同年 9 月 10 日起公布施行。本次修法重點，包含簡化電子支付機構使用者身分確認流程、適度降低電子支付機構作業成本及提高使用者之便利性。

依修正前電子支付機構業務管理規則之規定，電子支付業者提供消費者代理收付服務時，消費者可設定「約定連結存款帳戶」付款服務[3]，消費者若有以電子支付帳戶進行款項支付，均可由電子支付業者直接向該金融機構提出扣款指示，或間接透過金融資訊服務事業、票據交換所等機構向金融機構提出扣款指示。本次修正後，將電子支付業者提供消費者以「約定連結存款帳戶」進行收付之範圍，從原本代理收付業務擴大至電子支付帳戶間款項移轉與儲值等服務，並進一步開放電子支付業者可提供消費者以約定連結存款帳戶付款進行自動儲值。

又，為避免消費者藉由以信用卡扣款儲值於電子支付帳戶，進而透過電子支付帳戶代理收付或款項移轉而有套取現金之不當行為，現行法令禁止消費者以信用卡從事電子支付帳戶儲值[4]，而消費者使用網路銀行或便利商店繳款等方式儲值又不甚方便。前開規則修正後，消費者即可主動透過約定連結存款帳戶轉帳或儲值於電子支付帳戶，亦可選擇當電子支付帳戶餘額不足時，由電子支付業者自動向金融機構發出扣款指示進行加值，以提升電子支付帳戶管理之便利性。

【管理 Tips】

[3] 依電子支付機構業務管理規則第 2 條第 8 款，就約定連結存款帳戶付款服務定義為「電子支付機構辦理電子支付機構業務，依使用者與開戶金融機構間之約定，向開戶金融機構提出扣款指示，連結該使用者存款帳戶進行轉帳，由電子支付機構收取支付款項，並於該使用者電子支付帳戶記錄支付款項金額及移轉情形之服務」。

[4] 電子支付機構業務管理規則第 12 條第 1 項：「電子支付機構不得受理使用者利用信用卡進行儲值及電子支付帳戶間款項移轉。」

在大眾翹首盼望下，金管會開始正視電子支付法規過於嚴謹的議題。先前有過多的限制，導致銀行業者與電子支付業者都有所怯步。如今放寬部分管制，改善消費者體驗，這對於消費者的使用意願有很大的提升，並有助於促進電子支付的推廣。

然而，電子支付平台的安全管理顯得尤為重要。間接連結機制的規範，使得多數的金流與資訊流會掌握在電子業者手上。電子支付平台將面臨到許多資訊安全的隱憂，例如需加強對消費者與平台之間的身分驗證機制、資訊傳輸過程的機密性問題、交易訊息的完整性與不可否認性問題等皆為需考量的控制點。

綜上說明，本次電子支付相關法規修正方向，朝向兼顧資訊安全管理以及消費者體驗，並嚴格監控每筆平台上的交易，以確實保護整個交易流程的安全。

【相關標準】

ISO/IEC 27001：2013(CNS 27001)

A.9.1.2 對網路及網路服務之存取

應僅提供予使用者存取其已被特定授權使用之網路及網路服務。

A.13.2.3 電子傳訊

應適切保護電子傳訊時所涉及之資訊。

類別：資訊應用【案號：A1050104】

美國 NIST 提出數位認證指引草案

【焦點話題】

在美國國家標準技術局(America's National Institute for Standards and Technology，簡稱 NIST)新發布的數位認證指引草案中指出，資訊服務業者經常以「簡訊發送驗證碼」作為雙因素認證的其一方式，但考量到使用者行動裝置可能遭他人控制、密碼容易遭他人截取，且在網路電話服務(VoIP)中，使用此簡訊驗證機制更具有遭到駭客遠端操控的風險，因此 NIST 表示未來指引將不再鼓勵業者使用簡訊發送驗證碼作為身分認證機制，並建議業者考量採取其他替代方案。

草案規定表示，若一服務仍使用簡訊認證，必須確認使用者事先註冊之手機號碼並非使用網路電話服務後，才能發送認證訊息；再者，為避免接收認證訊息的設備號碼遭第三人變更，該要引要求資訊服務業者接受使用者變更手機號碼時，必須進行雙因素認證。本次的指引草案，NIST 將置於 GitHub 平台上公開閱覽，以徵詢公眾意見。

【資料來源：The Register，105/7/25】

【重點摘要】

1.考量到以簡訊回傳驗證碼之驗證機制具有遭到駭客遠端操控的風險，因此美國 NIST 數位認證指引草案已不再鼓勵業者使用簡訊發送驗證碼作為身分認證機制。

2.金融機構採用簡訊動態密碼作為電子銀行低風險交易的安全設計時，不得運用於設定約定轉入帳戶，並應加強防護措施，以確保網路交易安全。

【法律觀點】

過去，許多國內銀行業者在提供網路銀行辦理轉帳或信用卡等金融交易服

務時，為了提高網路銀行的安全性，常會提供雙因素(two-factor)認證機制，常見的方式是：除了要求用戶輸入帳號及密碼外，另外還會透過 SMS 簡訊傳送一組認證碼到用戶手機，以做第二層的認證。

然而，美國國家標準技術局(NIST)新發布的數位認證指引草案，指出使用簡訊回傳驗證碼作為身分認證機制，並非安全的認證方式。鑒於目前許多手機病毒與電腦病毒的互通，尤其在使用網路電話之情形下，簡訊將可能遭駭客攔截，亦可能遭駭客以告知用戶電話號碼變更等社交工程方式竊取，故 NIST 本次草案已明確表示不再鼓勵業者使用簡訊驗證作為雙因素驗證可採取之方式。其他用戶資訊。

對此，我國銀行公會於 105 年 3 月 18 日修正頒布的「金融機構辦理電子銀行業務安全控管作業基準」(下稱電子銀行安控基準)，即考量不同交易型態之安全風險，規定電子銀行各項交易之交易面介面安全設計，使用動態密碼(One Time Password，以下簡稱 OTP)原則上僅限應用於低風險交易[5]，且如採用軟體 OTP(含簡訊傳送 OTP)時，不得運用於設定約定轉入帳戶[6]，另考量電腦或行動裝置，可能同時遭植入惡意程式竊取登入密碼及 OTP，故應用於非約定轉入帳戶轉帳交易時，應加強其防護機制(如設備指定、推播確認、郵件回覆、採用非交易設備確認交易內容等)[7]。至於法人客戶的高風險交易，此次電子銀行安控基準的修正雖配合國際趨勢，允許使用動態密碼作為交易再確認機制之一，但其必須使用硬體設備(如動態密碼產生器)保護敏感資料，無法使用簡訊 OTP，並同時要求金融機構應符合多項嚴格的安控要求，包括須進行風險評估、偵測異常交易、防範網路釣魚、加強客戶教育，以及傳送敏感資料時應提供端點對端點加密機制避免中間

[5] 電子銀行安控基準第 7 條第 3 款。關於高風險及低風險交易的區別，參電子銀行安控基準第 4 條第 1 款第 2 目，例如就非約定轉入帳戶之情形，網際網路之低風險性交易，以每一帳戶每筆不超過新臺幣 5 萬元、每天累積不超過新臺幣十萬元、每月累積不超過新臺幣 20 萬元為限。

[6] 電子銀行安控基準第 9 條第 3 款第 1 目。

[7] 電子銀行安控基準第 9 條第 3 款第 3 目。

人竊取等[8]，以確保網路銀行的交易安全。

【管理 Tips】

美國 NIST 提出的數位認證機制，依據技術複雜度不同制定三種驗證等級，適用於各種風險等級情況。從單因素、雙因素到結合物理因素的驗證，複雜度的提升加強了資訊安全的保護。

反觀台灣，從過去使用的簡訊服務(SMS)到現在的動態密碼(OTP)，在身分認證機制的使用上，逐漸考量個人資料與機密資訊的安全。而近年來隨著自然人憑證的出現，政府便積極推廣將其使用在認證機制上，此舉不但提升民眾的便利性，更降低資訊被竊取盜用的風險。

這些規範的制定，都是提高身分驗證的控制點，使其更具安全防護功效。組織在實施密碼政策時，可以考量世界各地適用的加密技術，以確保資訊具備機密性、完整性、不可否認性與鑑別性等保護。

【相關標準】

ISO 27001：2013(CNS 27001)

A.10.1.1 使用密碼式控制措施之政策

宜發展及實作政策，關於資訊保護之密碼式控制措施的使用。

A.10.1.2 金鑰管理

宜發展及實作政策，關於貫穿其整個生命週期之密碼金鑰的使用、保護及生命期。

[8] 電子銀行安控基準第 9 條第 9 款。

類別：資訊應用【案號：A1050105】

自然人憑證線上投保，限制尺度將開放

【焦點話題】

網路投保過去限制要保人與被保險人須為同一人，且身故受益人限制為直系血親及配偶，亦即線上買保單限制本人投保，且受益人只能是父母、子女或配偶。金融監督管理委員會(下稱金管會)在 105 年 3 月推動第四波網路投保開放範圍，未來要保人及被保險人不同人時，要保人仍可以自然人憑證線上投保，且增加法定繼承人得為身故受益人，因此媽媽未來可用自己的自然人憑證線上為子女辦理投保事宜。

此外，金管會此次擴增投保商品險種，將自行車綜合保險、傳統型年金保險、利率變動型年金保險、保險年期不超過 20 年及歲滿期不超過 75 歲之生死合險等保險商品，納入網路投保商品險種。

【資料來源：中央社，105/3/15】

【重點摘要】

1. 金管會逐步開放要保人網路投保無庸以紙本方式為書面同意，而能以電子方式作業後，網路身分認證機制成為保險業網路投保平台運作關鍵。

2. 自然人憑證實務作業基準擴大適用範圍，明確釐清憑證使用範圍不限於電子化政府相關應用，金融業者可提供客戶以自然人憑證進行身分驗證與文件簽署。

【法律觀點】

依電子簽章法第 9 條第 1 項規定：「依法令規定應簽名或蓋章者，經相對人同意，得以電子簽章為之。」同法第 10 條規定：「以數位簽章簽署電子文件者，應符合下列各款規定，始生前條第 1 項之效力：一、使用...憑證機構依法簽發之憑證。二、憑證尚屬有效並未逾使用範圍。」鑒於我國民事

訴訟法第 358 條規定：「私文書經本人或其代理人簽名、蓋章或按指印或有法院或公證人之認證者，推定為真正」，當事人若以內政部憑證管理中心簽發，且尚在憑證效期內之自然人憑證簽署電子文件，且其簽署目的，符合內政部憑證管理中心公告「憑證實務作業基準」載明之使用範圍內時，該電子文件即依法推定為當事人所製作，主張該電子文件為偽造或否認當事人有簽署行為者，須負擔舉證責任。

內政部憑證管理中心於 104 年 8 月 25 日，公告憑證實務作業基準第 1.8 版，就憑證適用範圍從「開放網路中電子化政府相關應用服務所需的身分認證及資料加密」，調整為「網路中的身分識別與資料保護」，已明確釐清憑證使用範圍，不限於電子化政府相關應用服務。因此，金融保險等私部門相關網路應用服務，均可使用自然人憑證作為身分認證與確保資料完整性之保護機制。

隨著金管會逐步開放要保人網路投保無庸以傳統紙本方式為書面同意，而能以電子方式作業後，網路身分認證機制即成為保險業網路投保平台運作的關鍵。自然人憑證實務作業基準擴大適用範圍後，將有助於確保要保人使用該憑證線上簽署要保書等文件之效力。

【管理 Tips】

在網路上進行資料交換時，電子簽章如同網路身分證可辨識雙方身分。利用非對稱式加密技術將傳送的資料加密，並具有可識別身分的特性。

依金管會公布之「保險業辦理電子商務應注意事項」，保險業若有辦理電子商務，應於106年7月1日前取得資訊安全管理系統國際標準(ISO 27001)認證，顯見保險業務朝向網路化發展同時，應強化客戶資料保護。因此，網路投保平台不僅須採取適當的身分認證機制，更應提升本身安全防護，以從資訊安全面向奠定網路投保業務的發展基礎。

【相關標準】

ISO 27017：2015

ISO/IEC 27001：2013(CNS 27001)

A.10.1.2 金鑰管理

宜發展及實作政策，關於貫穿其整個生命週期之密碼金鑰的使用、保護及生命期。

A.13.2.2 資訊傳送協議

協議應闡明組織與外部各方間營運資訊之安全傳送。

類別：資訊應用【案號：A1050106】

金融科技產品或服務受限於現有法規 各界呼籲儘速推動監理沙盒

【焦點話題】

在國內首度提出監理沙盒(Regulatory Sandbox)之立法倡議後，此一議題隨即成為金融圈最為熱烈的話題之一，不僅若干新創公司與既有金融產業紛紛表示聲援，政府也透過 vTaiwan 平臺展開大規模的公眾諮詢，希望能夠找到更多創新構想及作法，有效解決國內新興科技應用服務之瓶頸。

在日前舉辦的一場公聽會上，專營財務報表教學與分析之某公司即分享親身經驗，表示在資訊應用風潮下，其曾規畫利用公開財報資訊搭配財務教科書公式等運用，對外推出「可推測合理股價」之新興金融科技產品。不過，由於認為一金融科技產品有牴觸證券交易法中禁止操縱股價之疑慮，而向主管機關詢問時也未能得到正面答覆，因而目前處於暫緩推動之狀況。該業者表示，法規之模糊或過度限制，輕則讓新創事業錯失市場先機，嚴重則可能造成臺灣金融科技發展之絆腳石。

【資料來源：iThome，105/9/18】

【重點摘要】

1.金融科技產品或服務之推出，因涉及相關金融法令，需先做好法律風險之評估，以避免觸法。

2.政府刻正研議導入之「監理沙盒」制度，將允許業者事先向主管機關就其實驗性開發項目提出申請，以免除既有法令之管制或相關法律責任。

【法律觀點】

「監理沙盒」制度源自英國，原係為了推動金融科技(FinTech)之發展與應用需求，希望為創新產品、服務及商業模式之試驗，提供一個安全空間，是以由 FCA(Financial Conduct Authority)開始研究並加以推動。而新加坡

所採行之制度構想，基本上係參考英國制度而來，在金融管理局(Monetary Authority of Singapore, MAS)主導下，對金融科技相關企業推出監理沙盒指引，凡向主辦機關提出監理註冊的金融科技相關公司，在事先報備的範圍內，可以從事推動各項實驗性業務，日後不會遭到追究相關法律責任。

為推動金融科技之發展，我國於民國(下同)105 年 10 月 14 日將攸關「監理沙盒」機制之相關法案一讀。而與「監理沙盒」機制相關之法案包括：銀行法、證券交易法、期貨交易法、保險法、投信投顧法、電子票證發行管理條例、電子支付機構管理條例，以及信託業法等。以證券交易法為例，即為納入監理沙盒機制而進行相關規範調整。首先，為促使主管機關主動參與新創企業產品、服務、企業模式及給付機制等之開發測試，以移除對於金融創新不必要的管制障礙，主管機關得受理企業對於監理沙盒之試驗申請[9]。其次，主管機關除受理監理沙盒之試驗申請外，應同步針對申請案所涉及之管制法令進行通盤檢討[10]。此外，為進行既有法律之調整檢討，主管機關應邀請利害關係人進行政策諮詢；前項政策諮詢，其範圍應包含市場公平競爭、交易安全、消費者權益與保護、資安及主管機關認為必要之事項[11]。最後，主管機關應就政策諮詢之結果進行法令應否修改之建議方案，並得附監理沙盒試驗申請案函送行政院及立法院備查[12]。

以本案而言，某公司曾規畫利用公開財報資訊搭配財務教科書公式之應用，對外推出「可推測合理股價」之新興金融科技產品，而此一產品之推出可能涉及證券交易法第 155 條第 1 項第 7 款[13]規定，惟其癥結恐在於其

[9] 證券交易法修正草案第 18 條之 4。

[10] 證券交易法修正草案第 18 條之 5。

[11] 證券交易法修正草案第 18 條之 6。

[12] 證券交易法修正草案第 18 條之 7。

[13] 證券交易法第 155 條第 1 項規定：「對於在證券交易所上市之有價證券，不得有下列各款之行為：一、在集中交易市場委託買賣或申報買賣，業經成交而不履行交割，足以影響市場秩序。二、（刪除）三、意圖抬高或壓低集中交易市場某種有價證券之交易價格，與他人通謀，以約定價格於自己出售，或購買有價證券時，使約定人同時為購買或出售之相對行為。四、意圖抬高或壓低集中交易市場某種有價證券之交易價格，自行或以他人名義，對該有價證券，連續以高價買入或以低價賣出，而有影響市場價格或市場秩序之虞。五、意圖造成集中交易市場某種有價證券交易活絡之表象，自行或以他人名義，連續委託

所提供之資訊是否屬於「流言或不實資訊」。惟如為排除該公司在開發金融科技產品或服務時之疑慮，避免金融科技發展受阻，未來在證券交易法修正草案通過後，即可向主管機關提出試驗申請，先行免除相關管制及法律責任。

【管理 Tips】

本案例可以從兩個不同觀點進行探討。首先，金融科技其實就是運用網際網路科技來執行金融服務，此一科技之應用可以帶來龐大的經濟效益，卻也可能同時隱藏許多資訊安全層面之風險。舉例來說，第三方驗證與防護機制、雲端服務廠商之監管，以及個人交易紀錄之維護等，皆為金融科技業務相關之業界需正視的問題。

另一方面，當推動監理沙盒之後，組織在提交測試資料於監管單位時，必須小心選擇、保護及控制測試資料。由於測試資料與實際運作資料為相近資訊，應避免測試內容包含個人可識別資訊或其他機密資訊之運作資料，若不得已將此資料運用於測試用途，須經由移除或修改後才可執行。而在每次測試完成後，應立即將資訊由測試環境中抹除。

而執行測試的監管單位，需嚴格規範與監控安全周界，以保護收容機敏或重要資訊及資訊處理設施之區域。除了實體環境的保護、進出人員的監控以及網路線路的遮蔽與區隔，監管單位均須予以嚴密控管。

【相關標準】

ISO 27001：2013(CNS 27001)

A.11.1.1 實體安全周界

宜定義及使用安全周界，以保護收容機敏或重要資訊及資訊處理設施之區域。

買賣或申報買賣而相對成交。六、意圖影響集中交易市場有價證券交易價格，而散布流言或不實資料。七、直接或間接從事其他影響集中交易市場有價證券交易價格之操縱行為。」

A.14.3.1 測試資料之保護

應小心選擇、保護及控制測試資料。

類別：資訊應用【案號：A1050107】

網路報稅開放使用健保卡

【焦點話題】

目前綜合所得稅報稅管道共有網路申報、稅額試算申報、二維條碼申報以及人工申報等 4 種，其中以網路申報使用率最高。據財政部統計，民國(下同)104 年有 57.6%申報戶使用，但其中有近一半是以「身分證字號加上戶號」方式登入，並非使用自然人憑證或金融憑證。

由於「身分證字號加上戶號」僅能登入報稅系統或上傳資料，民眾仍得自行輸入或搭配「查詢碼」載入所得資料，因此為提升便利性，105 年首度將健保卡納入報稅憑證。民眾使用健保卡報稅前，要先至健保署網站完成註冊並取得密碼；之後申報時，只要將健保卡插入讀卡機後再輸入註冊時設定的密碼，便可查到所得及扣除額資料並載入申報軟體，進行修改、上傳。

【資料來源：自由時報，105/4/25】

【重點摘要】

1. 健保署核發憑證並提供身分驗證服務，以利其他政府機關在其身分檢核之信賴基礎上，提供持卡人以健保卡與密碼作為其網路服務之認證方式。
2. 財政部擴大網路報稅系統採認憑證類型，提供民眾以健保卡等其他憑證完成網路申報，有助於提升多元認證而促進電子化政府服務。

【法律觀點】

全民健康保險憑證(以下簡稱健保卡)是由衛生福利部中央健康保險署(以下簡稱健保署)核發給民眾即保險對象，作為在健保特約機構醫療使用，以及申辦服務或健保業務跨機關網路服務使用。因應網路普及，財政部於 105 年開放健保卡作為網路報稅憑證，可用以查詢 104 年度所得、扣除額資料及辦理綜合所得稅網路申報，以提供民眾更多元而便利的身分認證機制。

依全民健康保險網路服務註冊管理作業要點第 5 點規定，健保署得提供行政機關(構)全民健康保險服務身分查證機制，供完成註冊之使用者申辦其他網路服務。因此，民眾須以臨櫃或網路方式向健保署提交基本資料，進行「健保卡網路服務註冊」並設定密碼，經健保署檢核申請人與持卡人本人同一後，始核發註冊完成通知。故財政部網路報稅系統開放健保卡憑證之運作方式，即類似我國電子簽章法下，憑證機構提供憑證用戶以憑證作為存取信賴憑證者服務之方式；健保署作為憑證機構，負責核發憑證並提供身分驗證服務，而其他政府機關(構)等信賴憑證者，即可在健保署已完成持卡人身分檢核與確認之基礎上，提供憑證用戶以健保憑證與密碼作為其網路服務之認證方式。

又，全民健康保險法第 16 條雖規定，健保卡「不得存放非供醫療使用目的及與保險對象接受本保險醫療服務無關之內容」，然而健保署此項身分查證服務，僅執行身分查證並回覆驗證訊息，而健保卡本身並未儲存任何報稅資料，不會有存放與健保醫療服務無關內容或資料外洩的疑慮。因此，財政部擴大網路報稅系統採認之憑證類型，以提供未持有自然人憑證或金融憑證之民眾，能夠以健保卡等其他憑證完成網路申報，有助於提升多元認證而促進電子化政府服務。

【管理 Tips】

健保卡功能擴充固然有利民眾使用，相對資訊風險也因此提高。以往使用自然人憑證報稅，其技術上採用較高安全性之公開金鑰基礎建設架構，且有電子簽章法認可其法律效力。

今(105)年使用健保卡報稅前，民眾要先註冊並取得密碼，其帳號及密碼儲存於健保局主機，安全管理責任將落在健保署肩上。而對於民眾應如何保管、使用相關設備及密碼，健保署亦應訂定相關規範並加以宣導或說明，以免發生誤用或盜用之情形。

【相關標準】

ISO/IEC 27001：2013(CNS 27001)

A.9.2.1 使用者註冊及註銷

應實作正式之使用者註冊及註銷過程，俾能指派存取權限。

A.9.2.2 使用者存取權限之配置

應實作正式之使用者存取權限配置程序，以對所有型式之使用者對所有系統及服務，指派或撤銷存取權限。

A.9.2.4 使用者之秘密鑑別資訊的管理

應以正式之管理過程控制秘密鑑別資訊的配置。

A.9.3.1 秘密鑑別資訊之使用

於使用秘密鑑別資訊時，應要求使用者遵循組織之實務規定。

自我評量

6 月分自我評量

是非題：

1. (O) 政府資訊公開法中，對於政府機關公開資訊之義務，以及限制公開之事由，皆有明確規定。如公務員執行職務時，擅自決定拒絕公開政府資訊，可按其情節輕重予以懲戒或懲處？【資訊公開 D1050101】

   解析：

   政府資訊公開法第 23 條：「公務員執行職務違反本法規定者，應按其情節輕重，依法予以懲戒或懲處。」解析：新修正之個資法第 41 條規定，增加「意圖為自己或第三人不法之利益或損害他人利益」之主觀要件，對於此種可受非難程度較高之行為，始以刑罰加以處罰。

2. (X) 依據民國 104 年 12 月 30 日修正之個人資料保護法第 41 條規定，對於侵害他人個資之行為，無論是不是出於「意圖為自己或他人不法之利益或損害他人利益」之想法，一概可以刑罰加以處罰？【資訊保護 S1050303】

   解析：

   新修正之個資法第 41 條規定，增加「意圖為自己或第三人不法之利益或損害他人利益」之主觀要件，對於此種可受非難程度較高之行為，始以刑罰加以處罰。

3. (X) 財政部開放健保卡作為網路報稅憑證，民眾只要持讀卡機並插入健保卡，即可登入財政部網路報稅系統查詢報稅資料，無庸先向健保署「健保卡網路服務註冊」？【資訊應用 A1050107】

   解析：

   民眾須以臨櫃或網路方式向健保署提交基本資料，進行「健保卡網路服務註冊」並設定密碼，經健保署檢核申請人與持卡人本人同一後，始能以註冊通過的密碼，登入財政部網路報稅系統。

4. (X) 基於新聞自由與確保公眾知的權利，記者只要在媒體封鎖期間內，配合不要外出或直播即可，仍能以電子郵件或通訊軟體提前散布訊息？【資訊保護 S1050302】

   解析：

媒體封鎖機制在確保新聞媒體於官方正式發布後，始進一步發表新聞或評論，其目的在兼顧新聞自由與公共利益，故負有媒體封鎖保密義務的新聞記者不得以任何方式洩漏或揭露訊息。

5. (O) 銀行遭受駭客攻擊，出現網頁大塞車，但用戶個資並未外洩，駭客仍成立刑法第 360 條干擾電腦或其相關設備罪？【資訊保護 S1050301】

解析：

刑法第 360 條：「無故以電腦程式或其他電磁方式干擾他人電腦或其相關設備，致生損害於公眾或他人者，處三年以下有期徒刑、拘役或科或併科十萬元以下罰金。」該條文僅要求「致生損害於公眾或他人」的具體危險，並不一定是要造成用戶個資外洩。本題駭客攻擊銀行網頁，造成網頁大塞車，已該當「致生損害於公眾或他人」，違反刑法第 360 條規定。

6. (X) 行政機關受理人民陳情，如果陳情人是機關內同事，便不需要保密。【資訊保護 S1050101】

解析：

行政程序法第 170 條：行政機關對人民之陳情，應訂定作業規定，指派人員迅速、確實處理之。人民之陳情有保密必要者，受理機關處理時，應不予公開。本條明文規定行政機關對人民之陳情，有保密必要者，應不予公開。課與行政機關對於陳情案件的保密義務。解釋上，人民向行政機關檢舉，亦可以解釋為該條的「陳情」，行政機關應遵守一定的保密義務。即使檢舉人為同一公務機關的同事，因檢舉人寄發檢舉信乃是基於一般人民的地位，循一般民眾之管道，該管公務員不因此免除對於檢舉案件的保密義務。

選擇題：

1. (4) 依據政府資訊公開法之規定，政府資訊符合特定事由時，可以限制公開或不予提供。請問，政府資訊如涉及個人隱私時，申請人不得主張下列事由而要求提供？(1)對公益有必要。(2)為保護人民生命、身體、健康有必要。(3)經當事人同意。(4)政府資訊不具經濟價值。【資訊公開 D1050101】

解析：

政府資訊公開法第 18 條第 1 項：「政府資訊屬於下列各款情形之一者，應限制公開或不予提供之：……六、公開或提供有侵害個人隱私、職業上秘密或著作權人之公開發表權者。但對公益有必要或為保護人民生命、身體、健

康有必要或經當事人同意者，不在此限。……」。選項 1-3 皆為依法可主張之理由，故選項 4 正確。

2. (3) 依據個人資料保護法之規定，公務機關對於個人資料利用所應注意之事項，以下何者最為正確？(1)應於執行法定職務必要範圍內為之。(2)與蒐集之特定目的相符。(3)以上皆是。(4)經行政院核可。【資訊保護 S1050303】

   解析：

   個人資料保護法第 18 條第 1 項前段：「 」公務機關對個人資料之利用，除第 6 條第 1 項所規定資料外，應於執行法定職務必要範圍內為之，並與蒐集之特定目的相符。」。選項 1 及 2 僅涵蓋部分注意事項，選項 4 則法無明文，故選項 3 正確。

3. (1) 在財政部網路報稅系統開放健保卡憑證之運作架構中，健保署角色相當於以下何者？(1)憑證機構。(2)憑證用戶。(3)信賴憑證者。(4)外部稽核機構。【資訊應用 A1050107】

   解析：

   財政部網路報稅系統開放健保卡憑證之運作方式，即類似我國電子簽章法下憑證機構提供憑證用戶以憑證作為存取信賴憑證者服務之方式，健保署負責核發憑證並提供身分驗證服務，而其他政府機關(構)即可在健保署已完成持卡人身分檢核與確認之信賴基礎上，提供持卡人以健保卡與密碼作為其網路服務之認證方式。

4. (2) 新聞記者在媒體封鎖期間內，若洩漏政府機關核定為機密且即將發布的重大訊息，在我國可能的法律責任為何？(1)新聞自由受絕對保障，因此記者沒有任何責任。(2)可能構成洩漏國防或國防以外秘密罪。(3)若重大訊息即將於 2 小時內公開，則記者不構成犯罪。(4)視新聞記者是否取得合法記者證而定。【資訊保護 S1050302】

   解析：

   在媒體封鎖期間內，該資訊若經政府機構依內部程序核定為機密或已明文要求記者保密，則以任何方式洩漏或交付資訊給第三人致違反保密義務者，在我國即可能構成洩漏國防以外機密罪。

5. (2) 甲拿槍恐嚇乙交出其所有的比特幣，甲該當下列何者？(1)。因比特幣是虛擬貨幣，不是我國法定貨幣，只能論以刑法第 360 條無故以電腦程式干擾他人電腦罪。(2)刑法第 346 條恐嚇得利罪。(3)詐欺罪。(4)違反個人資料保護法。【資訊保護 S1050301】

解析：

法務部法檢字第(90)法檢決字第 039030 號函認定電磁紀錄於竊盜罪以「動產」論，於詐欺罪亦屬「動產」，故虛擬物品得作為刑法竊盜罪及詐欺罪保護之客體。比特幣雖然是虛擬貨幣，並無實體，但仍具有財產價值，具有市場流通性，依我國目前多數實務見解，恐嚇他人使人交付虛擬貨幣，虛擬貨幣仍該當刑法第 346 條的 2 項的「財產上利益」，仍該當恐嚇得利罪。另外本題不涉及個人資料的外洩，甲的手段是拿槍恐嚇，並無以電腦程式干擾他人電腦使用，並非無故以電腦程式干擾他人電腦罪；亦未使他人陷入錯誤交付財產利益，並非詐欺罪，故選項(1)、(2)、(4)錯誤。

6. (2) 阿呆是公務機關的公務員，平常工作會接觸許多民眾的個資，為了滿足好奇心，會將經手的個資拿去網路人肉搜索，但這些個資及人肉搜索的事情，只有他一人知道，並沒有洩漏給其他人，請問阿呆違反什麼法律？(1)刑法第 132 洩漏國防以外機密罪。(2)個人資料保護法。(3)政府資訊公開法。(4)民法。【資訊保護 S1050101】

解析：

個人資料保護法第 16 條規定，原則上公務機關對個人資料之利用，應於執行法定職務必要範圍內為之，並與蒐集之特定目的相符。此為公務機關對於個人資料之利用的概括規定，原則上個人資料之利用不得逾越執行法定職務必要範圍。本條的適用客體著重於個人資料的「利用」，以公務上取得之個人資料進行「人肉搜索」，顯然逾越執行法定職務必要範圍。阿呆並未將資料外洩，故選項錯誤；本題不涉及政府資訊公開的問題，亦非民事爭議，故選項(3)、(4)錯誤。

7 月分自我評量

是非題：

1. (X)　依據通訊保障及監察法之規定，僅有故意違法監聽行為始負有民事賠償責任？【資訊監察 M1050101】

   解析：

   監聽行為涉及秘密通訊自由之侵害，因而必須遵循嚴格之要件及程序，而對於違法監聽行為，無論是故意違法監聽或過失監聽，皆應負有民事賠償責任。

2. (X) 依據國家機密保護法，國家機密分為極機密、機密及密等三種？【資訊保護 S1050202】

   解析：

   國家機密保護法第 4 條規定：「國家機密等級區分如下：一、絕對機密：適用於洩漏後足以使國家安全或利益遭受非常重大損害之事項。二、極機密：適用於洩漏後足以使國家安全或利益遭受重大損害之事項。三、機密：適用於洩漏後足以使國家安全或利益遭受損害之事項。」

3. (X)　我國對於機密文書透過網路傳輸並無任何限制，無論機密等級為何，均可以電子郵件寄送？【資訊保護 S1050201】

   解析：

   依行政院及所屬各機關資訊安全管理要點之規定，機密性資料及文件原則上不得以電子郵件或其他電子方式傳送。

4. (X) 外國人並非我國國民，不受個資法保護，因此公務機關在我國境內蒐集外國人個資，無須依個資法規定進行告知或限於特定目的內利用？【資訊應用 A1050101】

   解析：

   我國公務機關或非公務機關在我國境內蒐集外國人個資仍應遵守個資法相關作業要求。

5. (X) 依照稅捐稽徵法第 34 條，稽徵機關對重大欠稅案件，得公告其欠稅人姓名，其他與防杜大戶逃稅之目的顯然無關的資訊，也可以一併公告。【資

訊公開 D1050102】

解析：

稅捐稽徵法第 34 條第 1 項僅規定，稅捐稽徵機關，對重大欠稅案件或重大逃漏稅捐案件經確定後，得公告其欠稅人或逃漏稅捐人姓名、名稱、內容。依個人資料保護法第 16 條，公務機關對個人資料之利用，應於執行法定職務必要範圍內為之，並與蒐集之特定目的相符。依照稅捐稽徵法第 34 條立法理由，該條立法目的乃為有效防止大戶逃漏稅捐，是故其他與防杜大戶逃稅之目的顯然無關的資訊，應回歸稅捐稽徵法第 33 條，仍有保密義務。

6. (X) 徵信業的業務性質，常常接受客戶委託調查他人的資訊，對於被調查對象，因為徵性業的特殊性，故不須尊重當事人之權益，對其並無告知義務。【資訊保護 S1050102】

解析：

依個人資料保護法第 5 條，對於個人資料之蒐集、處理或利用，應尊重當事人之權益，不得逾越特定目的之必要範圍，並不排除徵信業。且依個人資料保護法第 8 條第 1 項，於蒐集個人資料時，對於名稱、蒐集之目的、個人資料之類別等事項，對當事人有告知義務，並未排除徵信業對該告知義務之適用。故本題敘述錯誤。

選擇題：

1. (4) 依據通訊保護及監察法第 5 條之規定，下列何者不是進行監聽之要件或程序？(1)涉犯特定嚴重犯罪。(2)危害國家安全、經濟秩序或社會秩序情節重大。(3)有相當理由可信其通訊內容與本案有關。(4)在偵查中應向檢察長申請核發通訊監察書。【資訊監察 M1050101】

解析：

通訊保障及監察法第 5 條第 2 項：「前項通訊監察書，偵查中由檢察官依司法警察機關聲請或依職權以書面聲請該管法院核發。」選項 1-3 皆為同條第 1 項所定要件，至於通訊監察書則應向法院申請核發，故選項(4)錯誤。

2. (4) 公務機關對於機密文件之保存，以下何者不正確？(1)於機關內部建立資訊安全管理制度。(2)訂定嚴謹之資訊資產分級。(3)定期清點各級別之資產是否被妥善保存在適當區域內。(4)一律委外保存以減輕行政負擔。【資訊保護 S1050202】

解析：

可以發現公務機關常掌控大量機密文件與個人資料，因而宜於機關內部建立資訊安全管理制度，以將資料、文件等機密資訊做嚴密控管與保護，避免發生外流或洩密事件。為此，公務機關需依據擁有的機密文件與個人資料訂定嚴謹之資訊資產分級，針對不同級別之資產做出相對應的保護處置，故選項(4)不正確。

3. (4) 以下何者為政府機密資料上傳至雲端平台後，應注意之管理面向？(1)存取權限設定。(2)存取紀錄異常追蹤。(3)資料變更與刪除。(4)以上皆是。【資訊保護 S1050201】

解析：

機關應確保檔案在網路傳送或存放作業的完整性與機敏性，尤其機密資料若上傳至雲端平台，就存取權限設定、存取紀錄異常追蹤及資料刪除等更為重要管理議題。

4. (2) 關於個人生物辨識資料是否屬於個人資料之敘述，何者正確？(1)生物辨識資料無法以感官確認資料內容，非屬個資。(2)若生物辨識資料能與個人身分資料連結而識別特定個人，即屬個人資料。(3)生物辨識資料具有被竄改或複製可能性，故非屬個人資料。(4)生物辨識資料均屬特種個資。【資訊應用 A1050101】

解析：

個人生物辨識資料具有唯一識別性，且與個人身分資料連結下可識別特定個人，符合我國關於間接識別個資之定義；又，虹膜、指紋等生物辨識資料屬身體特徵資料，非醫療或健康檢查紀錄等特種個資。

5. (４) 欠稅人王董是有名的欠稅大戶，稅務稽徵人員 A 依法公告其姓名與欠稅金額，而後 A 愈想愈憤怒，覺得應該替天行道，遂將王董之財產、所得、營業及親朋好友的資料一併公告，並將相關資料傳給有興趣的記者朋友，有關 A 的法律責任，下列敘述何者為非？(1) A 將王董其他與欠稅無關的資料公告，可能已逾越執行法定職務必要範圍。(2) A 洩漏欠稅人之資料，可能違反刑法第 132 條「洩漏國防以外秘密罪」。(3) A 違反稅捐稽徵法第 33 條稅捐稽徵人員的保密義務。(4) 稅捐稽徵法既規定可以公布欠稅人之姓名，所以洩漏其他資料也一定不違法。【資訊公開 D1050102】

解析：

依個人資料保護法第 16 條，公務機關對個人資料之利用，應於執行法定職

務必要範圍內為之，並與蒐集之特定目的相符，A 將王董的親友資訊一併公告，與防範欠稅、逃漏稅的目的顯然無關，故(1)正確。依刑法第 132 條，公務員洩漏或交付關於中華民國國防以外應秘密之文書、圖畫、消息或物品者，處三年以下有期徒刑。欠稅人之財產、所得、營業資料，依稅捐稽徵法第 33 條，稽徵人員有保密義務，稽徵人員洩漏這些資料，成立刑法第 132 條公務員洩漏國防以外機密罪，故(2)(3)正確。稅捐稽徵法第 34 條，得公告其欠稅人之姓名、名稱、內容，且稅捐稽徵法第 34 條立法理由：「前條係對納稅義務人提供財產資料規定保密，惟為有效防止大戶逃漏稅捐，本條特規定得公布逃漏稅捐人之姓名與事實經過。」，顯見並不包括與防範逃稅目的無關之事項，故(4)錯誤。

6. （2）A 女為徵信業者，因不滿客戶 B 生性小氣，故憤而將 B 委託調查的事項，以及 B 有關的工商秘密一併洩漏，致使 B 及受到損害，有關 A 女的法律責任，下列何者錯誤？(1) A 女將 B 委託之內容洩漏，洩漏委託資料屬於違背任務，致使 B 受有不利益，成立刑法第 342 條的背信罪。(2) A 女可能洩漏成立刑法第 339 條詐欺罪。(3) A 女可能成立刑法第 317 條妨害工商秘密罪。(4)除了刑事責任，A 女對 B 可能有民事賠償責任。【資訊保護 S1050102】

解析：

依民法第 342 條第 1 項，為他人處理事務，意圖為自己或第三人不法之利益，或損害本人之利益，而為違背其任務之行為，致生損害於本人之財產或其他利益者，處五年以下有期徒刑、拘役或科或併科五十萬元以下罰金，A 女將 B 委託之內容洩漏，致使 B 因此受有不利益，成立刑法第 342 條的背信罪，故(1)正確。A 女並無對 B 施行詐術，並無詐欺罪的問題，故(2)錯誤。依刑法第 317 條，依法令或契約有守因業務知悉或持有工商秘密之義務，而無故洩漏之者，處一年以下有期徒刑、拘役或一千元以下罰金，故(3)正確。B 與 A 有民事契約關係，即使 A 受刑事追訴，B 仍可對 A 進行民事求償，故(4)正確。

8 月分自我評量

是非題：

1. (X) 使用穿戴式裝置的錄音功能，竊錄他人在公開場所的演講，違反刑法第 315 條之 1 妨害秘密罪。【資訊保護 S1050304】

   解析：

   刑法第 315 條之 1：「有下列行為之一者，處三年以下有期徒刑、拘役或三十萬元以下罰金：一、無故利用工具或設備窺視、竊聽他人非公開之活動、言論、談話或身體隱私部位者。二、無故以錄音、照相、錄影或電磁紀錄竊錄他人非公開之活動、言論、談話或身體隱私部位者。」該條針對的是竊錄他人「非公開之言論」，如果竊錄的內容是無合理隱私或秘密期待之公開言論，即不受到該條保障。

2. (X) 依國家機密保護法，只要是公務上可以接觸到的所有機敏性資料，都是該法所保護的「國家機密」。【資訊保護 S1050305】

   解析：

   依國家機密保護法第 2 條規定：「本法所稱國家機密，指為確保國家安全或利益而有保密之必要，對政府機關持有或保管之資訊，經依本法核定機密等級者。」因此，須依國家機密保護法核定機密等級者，始為國家機密，並非所有機敏性資料皆是「國家機密」。

3. (X) 為鼓勵跨國資訊流通、提高公眾監督，任何人都可依政府資訊公開法向我國政府機關申請閱覽，該法對於申請對象無任何資格限制？【資訊公開 D1050103】

   解析：

   依我國政府資訊公開法規定，具有中華民國國籍並在中華民國設籍之國民及其所設立之本國法人與團體、持有我國護照之僑民，以及該國法令未限制我國國民申請提供其政府資訊等三類，因此若不屬上開三類申請對象，尚無從依政資法向其他機關申請檔案資料。

4. (X) ATM 為銀行業務機器設備，由銀行自主管理，主管機關對於 ATM 安裝與服務運作過程所應採取的安全防護，並無任何規範或要求？【資訊保護 S1050501】

解析：

財政部早於 85 年核備「金融機構自動櫃員機安全防護準則」，該準則提供銀行針對 ATM 安裝地點、機體及周遭設備、警報系統、閉路電視錄影監視系統、補鈔安全及其他相關安全防護機制。另金融機構安全維護管理辦法更進一步要求銀行就 ATM 安全維護措施，除應評估其安全性、慎選設置地點以外，尚須建立自動櫃員機異常提領監控機制。

5. (X) 依據銀行公會 105 年 3 月 18 日所發布金融機構辦理電子銀行業務安全控管作業基準之最新修正版本，電子銀行交易依其風險等級分為 A、B、C、D 四個不同等級。【資訊應用 A1050102】

解析：

依據金融機構辦理電子銀行業務安全控管作業基準之新規定，電子銀行之各項交易依其交易風險類別分為高風險及低風險類別；如非低風險類別所列舉之交易活動，則屬於高風險交易。

6. (X) 美國政府網路事件協調之總統政策指令是第一份針對私部門因應網路攻擊事件之建議文件？【資訊保護 S1050502】

解析：

這份指令是美國第一次針對網路攻擊應變之公部門分工所發布，希望能夠因應越來越多且變化多端的網路攻擊事件。

選擇題：

1. (4) 以下行為，依刑法妨害秘密之規定，何者並非受該法處罰之態樣？(1)竊錄 KTV 包廂內唱歌之明星朋友，以公開販售。(2)在丈夫/妻子的手機上裝竊聽器，蒐集外遇證據。(3)在心儀對象家裝隱藏式攝影機，以確認其是否

有正在交往之對象。(4)拍攝在街頭打架之情侶，提供給警察作為證據。【資訊保護 S1050304】

解析：

刑法第 315 條之 1：「有下列行為之一者，處三年以下有期徒刑、拘役或三十萬元以下罰金：一、無故利用工具或設備窺視、竊聽他人非公開之活動、言論、談話或身體隱私部位者。二、無故以錄音、照相、錄影或電磁紀錄竊錄他人非公開之活動、言論、談話或身體隱私部位者。」拍攝街頭打架之緣由為蒐集證據，非無正當理由；且街頭屬公開之場合，沒有合理隱私權期待，亦非刑法妨害秘密保障之態樣。

2. (1) 有關國家機密保護法所保障之「國家機密」，下列何者錯誤？(1)只要是公務上可以接觸到的所有機敏性資料，都是該法所保護的「國家機密」。(2)必須是基於國家安全或利益而有保護必要。(3)必須是依該法核定機密等級的資訊。(4)依照機密等級分為絕對機密、極機密或機密。【資訊保護 S1050305】

解析：

依國家機密保護法第 2 條規定：「本法所稱國家機密，指為確保國家安全或利益而有保密之必要，對政府機關持有或保管之資訊，經依本法核定機密等級者。」所以並非所有機敏性資料皆是「國家機密」，必須限於「為確保國家安全或利益而有保密之必要」，以及「經依本法核定」，故選項(1)錯誤、(2)、(3)正確，又依同法第 4 條：「國家機密等級區分如下：一、絕對機密：適用於洩漏後足以使國家安全或利益遭受非常重大損害之事項。二、極機密：適用於洩漏後足以使國家安全或利益遭受重大損害之事項。三、機密：適用於洩漏後足以使國家安全或利益遭受損害之事項。」依照機密等級分為絕對機密、極機密或機密，故選項(4)正確。

3. (3) 以下何者享有向我國政府機關申請政府資料之資格？(1)我國財政部。(2)香港公民。(3)財團法人創世社會福利基金會。(4)來台旅遊之大陸人民。【資訊公開 D1050103】

解析：

依我國政府資訊公開法規定，具有中華民國國籍並在中華民國設籍之國民及其所設立之本國法人與團體、持有我國護照之僑民，以及該國法令未限制我國國民申請提供其政府資訊等三類，因此若不屬上開三類申請對象，例如政府機關，尚無從依政資法向其他機關申請檔案資料。

4. (4) 以下為我國針對 ATM 安全防護所要求銀行應採取之措施？(1)自動櫃員機裝置時，應詳確評估其安全性，慎選設置地點。(2)建立自動櫃員機異常提領監控機制。(3)設置防盜安全設備。(4)以上皆是。【資訊保護 S1050501】

解析：

金管會依銀行法授權訂定之金融機構安全維護管理辦法，要求銀行就 ATM 安全維護措施，除應評估其安全性、慎選設置地點以外，並應設置防盜安全設備、防止他人窺視與使用者得察覺後方情況之設施等，且須建立自動櫃員機異常提領監控機制。

5. (1) 下列何者不是國內銀行業者對於電子銀行交易常採取之資安防護措施？(1)全程錄音錄影。(2)透過行動載具或生物辨識來確認身分或交易。(3)透過動態密碼來進行身分辨識。(4)交易訊息傳送採取加密措施。【資訊應用 A1050102】

解析：

為確保對客戶之權益保障，金融機構辦理電子銀行業務安全控管作業基準規定，銀行業者可採取動態密碼、生物辨識或其他方式作為身分或交易確認，尚且要求銀行業者在傳送敏感資料時，應提供端點對端點加密機制(如 end-to-end encryption, E2EE)，於客戶端輸入資料時立即加密，傳送至銀行端之硬體安全模組，以避免中間人竊取。故選項(1)錯誤。

6. (2) 有關美國政府網路事件協調之總統政策指令之說明，下列敘述何者錯誤？(1)美國政府網路事件協調之總統政策指令將網路事件分為 6 個不同等級。(2)美國政府網路事件協調之總統政策指令並未定義網路事件範圍。(3)公部門面對資安事件時，不僅應著重於事件調查及蒐證，更要從資產及情報支援之角度切入納入相關單位之協助，並協助受影響單位及早回復業務運作。(4)美國政府網路事件協調之總統政策指令提出處理原則，包括：責任分擔、資安應變以風險為基礎、尊重受影響單位、追求整理作業效益考量，以及盡可能恢復原狀。【資訊保護 S1050502】

解析：

這份指令首先定義網路事件範圍，凡可能對於國家安全利益、外交關係、美國經濟、公眾信心、民眾自由或大眾健康與安全產生危害之網路攻擊事件，均屬之。故選項(2)為錯誤。

9 月分自我評量

是非題：

1. (O) 擴增實境遊戲(例如寶可夢)，在進行遊戲時會記錄玩家的位置與拍攝周遭實境而涉及蒐集玩家個人資料時，遊戲業者應事先告知玩家。【資訊保護 S1050103】

   解析：

   依個資法第 8 條及第 9 條規定，對於他人個人資料之直接或間接蒐集，除非有法定免為告知之事由外，均應於直接蒐集之蒐集前或間接蒐集之處理或利用前，向當事人踐行告知義務，並且必須合乎同法第 19 條第 1 項列舉之法定事由，方能蒐集個人資訊。

2. (X) 依 105 年金融機構辦理電子銀行業務安全控管作業基準，電子銀行不論是高風險或低風險交易， 皆是用同樣程度的身分驗證安全標準。【資訊應用 A1050104】

   解析：

   依 105 年金融機構辦理電子銀行業務安全控管作業基準，電子銀行之各項交易依其交易風險類別分為高風險與低風險；關於高風險交易，要求更高的身分驗證安全標準。例如電子銀行各項交易之交易面介面安全設計，依該基準第 7 條第 3 款，使用動態密碼原則上僅限應用於低風險交易；反之，依該基準第 9 條第 9 款，法人客戶的高風險交易，雖允許使用動態密碼作為交易再確認機制之一，但其必須符合多項嚴格的安控要求。

3. (X) 透過非法軟體竊聽或竊錄他人非公開談話，可能侵害他人隱私，不過目前僅得請求民事損害賠償，而沒有其他刑罰規定。【資訊監察 M1050102】
   解析：

   透過非法軟體竊聽或竊錄他人非公開談話，不僅侵害他人隱私，也可能涉犯妨害秘密或違法監察之犯罪。

4. (X) 職場就是公開環境，因而員工不具有隱私保障。【資訊監察 M1050103

   解析：

   國內司法實務多認為員工於職場上之活動仍具有合理隱私期待，因而員工仍

具有隱私保障。因此，雇主如欲對員工進行監看(聽)或側錄，必須符合一定要件，否則恐涉及侵害隱私之行為。

5. (X) 為鼓勵民眾能夠以多元管道在電子支付帳戶進行儲值，我國現行電子支付法令開放民眾能夠以超商繳款、網路銀行線上轉帳及信用卡等方式進行儲值。【資訊應用 A1050103】

解析：

為避免消費者藉由以信用卡扣款儲值於電子支付帳戶，進而透過電子支付帳戶代理收付或款項移轉而有套取現金之不當行為，現行法令禁止消費者以信用卡從事電子支付帳戶。

6. (X) 我國自然人憑證僅限於使用電子化政府相關網路服務申辦，不能作為私部門─例如銀行或保險公司網路服務之身分認證機制？【資訊應用 A1050105】

解析：

自然人憑證屬於電子簽章，本可作為網路身份認證機制，而內政部憑證管理中心於 104 年修正實務作業基準後，擴大適用範圍，已明確釐清憑證使用範圍不限於電子化政府相關應用服務，因此金融或保險業者均可提供客戶以自然人憑證進行身份驗證與文件簽署，且經客戶以有效憑證簽署之電子文件依法推定為真正。

選擇題：

1. (1) 小華迷上了近來流行的擴增實境遊戲「寶可夢」，常特地到不同地點抓寶，小華以下行為所涉及之法律問題，何者正確？(1)小華進入各機關或場所的管理範圍內進行「抓寶」，必須注意該行為是否違反各機關有關之規定。(2)小華進入要塞堡壘地帶從事擴增實境遊戲，至多負有民事賠償責任，無刑事責任風險。(3)依擴增實境遊戲顯示路線到機關抓寶，為小華受憲法保障之行動自由，機關不得禁止。(4)「要塞堡壘」指經濟上所必須控制與確保之民生基礎設施。【資訊保護 S1050103】

解析：

所謂「要塞堡壘」指國防上所必須控制與確保之戰術要點、軍港及軍用飛機場；而要塞堡壘及其周圍之必要區域(含水域)，稱為要塞堡壘地帶，由國防部核定並公告之。而在堡壘要塞內，非受有國防部之特別命令，不得攝影，

違反者不論故意或過失，可能構成要塞堡壘地帶法第 9 條第 1 項或第 2 項，最高可處 7 年有期徒刑。

2. (1) 有關銀行公會於 105 年修正的電子銀行業務安全控管作業基準，下列何者敘述正確？(1)電子銀行之各項交易依其交易風險類別分為高風險與低風險類別。(2)高風險交易可以只用動態密碼、視訊會議或其他方式作為身分驗證。(3)銀行對於法人客戶的高風險交易，不允許使用動態密碼作為交易再確認機制。(4)對於大額、高風險交易的身分驗證，銀行不需要採取安全性較高的驗證方法。【資訊應用 A1050104】

   解析：

   依 105 年金融機構辦理電子銀行業務安全控管作業基準，電子銀行之各項交易依其交易風險類別分為高風險與低風險類別，故選項(1)正確；關於高風險交易，要求更高的身分驗證安全標準。例如電子銀行各項交易之交易面介面安全設計，依該基準第 7 條第 3 款，使用動態密碼原則上僅限應用於低風險交易；反之，依該基準第 9 條第 9 款，法人客戶的高風險交易，雖允許使用動態密碼作為交易再確認機制之一，但其必須使用硬體設備(如動態密碼產生器)保護敏感資料，無法使用簡訊 OTP，並同時要求金融機構應符合多項嚴格的安控要求，包括須進行風險評估、偵測異常交易、防範網路釣魚、加強客戶教育，以及傳送敏感資料時應提供端點對端點加密機制避免中間人竊取等。故(2)、(3)、(4)錯誤。

3. (1) 有關竊聽他人非公開對話之行為可能觸犯之相關刑罰規定，下列何者敘述可能不正確？(1)通保法第 24 條第 1 項之違法監察罪，只處罰公務員，而不包括一般人。(2)販售竊聽軟體屬營利行為，將面臨較重之刑罰。(3)窺視或竊聽之行為會受到處罰，依據刑法第 315 條之 1 規定，最高可處 3 年有期徒刑。(4)我國制定通訊保障及監察法，主要是為了保障人民秘密通訊自由及隱私權不受非法侵害。【資訊監察 M1050102】

   解析：

   通保法第 24 條第 1 項並未限定於公務員，故選項(1)不正確。

4. (1) 雇主如欲對員工進行監看(聽)或側錄，下列哪一項不是必要的注意事項：(1)對該員工提供足額之事後補償。(2)事先告知員工並取得同意。(3)與該員工之工作相關且符合目的性與比例性。(4)事先揭示公司資訊監看政策讓員工知悉。【資訊監察 M1050103】

   解析：

為確保員工之合理隱私期待，公司倘欲進行監看或監聽，應符合以下要件之一：(一)告知後取得員工同意，或揭示公司資訊監看政策且員工未表示反對；(二)具有正當理由；(三)與工作相關且符合目的性與比例性。故選項(1)不正確。

5. (4) 小美完成某電子支付帳號註冊程序，並設定可從其銀行約定存款帳戶連結扣款後，小美未來使用以下何項電子支付服務，可以直接從該存款帳戶扣款？(1)支付款項。(2)電子支付帳戶款項移轉。(3)儲值。(4)以上皆是。【資訊應用 A1050103】

解析：

本次電子支付相關法規修正後，將電子支付業者提供消費者以「約定連結存款帳戶」進行收付之範圍，從原本代理收付業務擴大至電子支付帳戶間款項移轉與儲值等服務。

6. (2) 以下何者不是憑證用戶使用數位簽章簽署電子文件時，該電子文件經用戶完成簽署後，依法可推定為真正之要件？(1)憑證為合法憑證機構簽發。(2)憑證外觀完整、目視未有毀損。(3)憑證仍在使用效期內。(4)憑證使用範圍符合憑證實務作業基準公告適用範圍。【資訊應用 A1050105】

解析：

依電子簽章法第 10 條規定：「以數位簽章簽署電子文件者，應符合下列各款規定，始生前條第 1 項之效力：一、使用...憑證機構依法簽發之憑證。二、憑證尚屬有效並未逾使用範圍」，另我國民事訴訟法第 358 條規定：「私文書經本人或其代理人簽名、蓋章或按指印或有法院或公證人之認證者，推定為真正」，因此憑證用戶若以合法憑證機構簽發且尚在憑證效期內之憑證簽署電子文件，且簽署目的符合憑證機構公告憑證實務作業基準載明之使用範圍內時，該電子文件即依法推定為真正。

10 月分自我評量

是非題：

1. (X) 監理沙盒機制之導入，主要是為了強化金融科技產品或服務之監理，並加重企業責任。【資訊應用 A1050106】

   解析：

   政府刻正研議導入之「監理沙盒」(Regulatory Sandbox)制度，將允許業者事先向主管機關就其實驗性開發項目提出申請，以免除既有法令之管制或相關法律責任。

2. (X) 依據我國國家機密保護法之規定，如係基於「改進自己的技術」目的，而刺探或收集國家機密或相關資訊文件，因為出發點沒有惡意，所以並不會構成犯罪。【資訊保護 S1050203】

   解析：

   依據國家機密保護法第 34 條規定，有刺探或收集國家機密資料者，最高可處以 5 年有期徒刑。因而行為人刺探或收集機密之意圖為「改進自己的技術」或其他目的，均可能涉及本條犯罪，而依據其所試探或收集之機密資料屬性不同，最高可面臨 5 年的刑責。

3. (O) 小明從網站下載知名攝影師王大頭以「創用 CC-姓名標示」授權釋出的山景照片後，可以大圖輸出成掛幅並標示王大頭姓名及授權資料後，銷售給其他人？【資訊公開 D1050104】

   解析：

   當使用者符合著作權人所設定的授權條件時，即等同已取得著作權人之授權，而無庸另行取得同意。本題中王大頭選擇以「創用 CC-姓名標示」釋出攝影作品時，任何人只要標示作者姓名及其授權資料，即可從事任何利用，包含營利目的重製發行等。

4. (X) 業者於個資事故發生後，僅須通知受害當事人個資外洩情形，無庸進一步採取任何因應或補救措施？【資訊保護 S1050104】

   解析：

   依個資法施行細則規定，個資事故通知內容應包括個人資料被侵害之事實及

已採取之因應措施，故電子商務網站業者若發生個資外洩，除應通知受害人可能個資外洩內容以外，亦應說明已採取的因應或補救措施。

5. (O) 遊戲玩家小華覺得某網路遊戲官方版有太貴，便把盜版的遊戲程式放在網路上供人下載，除非得到遊戲公司的授權，否則將違反著作權法。【資訊保護 S1050401】

解析：

提供連結供人連線下載盜版程式，依著作權法第 92 條，擅自以公開傳輸之方法侵害他人之著作財產權，屬於「違法公開傳輸」，將被處三年以下有期徒刑、拘役，或科或併科新臺幣 75 萬元以下罰金。

6. (O) 警察機關因調查網路性騷擾案，請求民間網站管理者提供相關個人資料，網站管理者如因此提供個人資料，並不違反個人資料保護法。【資訊監察 M1050104】

解析：

非公務機關對於個人資料的利用，僅有個人資料保護法第 20 條列舉的事由下，才能例外為特定目的外之利用。參考法務部見解，警察機關基於調查社會秩序維護事件之需要，而由非公務機關提供個人資料，亦應符合個資法第 20 條第 1 項第 2 款「為增進公共利益所必要」之要件，並不違反個資法。

選擇題：

1. (4) 有關監理沙盒機制之導入，下列敘述何者正確？(1)目前只有英國導入。(2)我國將是第一個導入監理沙盒機制之國家。(3)目前只有新加坡導入。(4)目前已有英國及新加坡導入此一機制，而國內政府目前刻正研議相關法制修正。【資訊應用 A1050106】

解析：

「監理沙盒」制度源自英國，新加坡亦參考英國制度而為推動，我國則嘗試導入此一機制，目前已於 105 年 10 月 14 日將攸關「監理沙盒」機制之相關法案於立法院進行一讀，故(4)正確。

2. (4) 有關避免或防範國家機密遭竊，下列何者敘述錯誤？(1)為確保國家機密之安全性，機關對於國家機密資料與檔案之存置場所或區域，得禁止或限制人員或物品進出。(2)機關將資訊業務委外營運時，除了慎選委外廠商外，並明訂其應善盡監督之責。(3)控制相關資訊使用者之存取權限，包含讀取、

寫入、刪除及執行等權限，限制系統輸出之資訊內容。(4)組織應充分信賴委外廠商，而不應該考量監督管理之問題，以避免破壞合作關係。【資訊保護 S1050203】

解析：

組織對於可能接觸機密資訊的委外廠商與其員工，應進行控管。故(4)錯誤。

3. (4) 以下何者非屬創用 CC 授權條款的四大要素之一？(1)姓名標示。(2)禁止改作。(3)非商業性。(4)禁止公開傳輸。【資訊公開 D1050104】

解析：

創用 CC 是一套制式化開放授權契約條款，提供著作權人從「姓名標示」、「非商業性」、「禁止改作」及「相同方式分享」四大要素中，自行排列組合選擇適當的授權條件，創用 CC 授權要素未包含對於公開傳輸或播送等利用態樣相關限制。

4. (4) 請問以下何者可以依據個資法對於主管行業進行行政檢查？(1)總統府。(2)行政院院會。(3)各中央目的事業主管機關。(4)無論行業別，均由法務部統一辦理個資業務行政檢查。【資訊保護 S1050104】

解析：

依個資法第 22 條第 1 項中央目的事業主管機關或直轄市、縣(市)政府有權就個資業務執行行政檢查。

5. (4) 小劉迷上了某款線上遊戲，除了進行遊戲外，也投入該遊戲的其他活動，小華以下行為所涉及之法律問題，何者錯誤？(1)小劉想藉此賺錢，便利用自己的資訊專長，將遊戲的程式複製下來，出租給其他玩家，小劉此舉違反著作權法。(2)小劉承繼原有的遊戲劇情設定，將原來的遊戲進行修改，仍違反著作權法。(3)小劉將遊戲放在其網站上供人連線下載，違反著作權法。(4)小劉並無複製或修改遊戲程式，只是破解程式上的防盜拷措施，並不違反著作權法。【資訊保護 S1050401】

解析：

將網路遊戲程式內容加以複製以供出租，則屬於「意圖銷售或出租而重製」該款網路遊戲，依著作權法第 91 條，將面臨 6 月以上 5 年以下有期徒刑，得併科 20 萬元以上 200 萬元以下罰金，故(1)正確。且小劉在不影響原遊戲劇情設定下，修改原遊戲及提供連結供人連線下載，依著作權法第 92 條分別成立「違法改作」及「違法公開傳輸」，將被處三年以下有期徒刑、拘

役，或科或併科新臺幣 75 萬元以下罰金，故(2)、(3)正確。另外，依著作權法第 80-2 條，若破解遊戲的防盜拷措施，即使未違反其他著作權法之規定，仍將面臨一年以下有期徒刑、拘役，或科或併科新臺幣 2 萬元以上 25 萬元以下罰金 ，故(4)錯誤。

6. (2) A 警察偵辦網路性騷擾案，發現嫌犯的犯罪證據及個人資料可能與 B 網站有關，下列何者敘述錯誤？(1)A 依其法定職權，得請求該網站管理者協助，提供相關的資料。(2)B 網站若未經當事人同意提供個人資料，一定違反個人資料保護法。(3)因為涉及調查社會秩序維護事件，B 網站增進公共利益所必要，得提供個人資料給 A。(4)若 A 警察若僅是基於私人目的，請求 B 提供個人資料，B 應拒絕。【資訊監察 M1050104】

解析：

依個資法第 15 條 第 1 款，公務機關在符合特定目的且於執行法定職務必要範圍內，得對個人資料之蒐集或處理。且依社會秩序維護法第 39 條 及第 83 條 第 3 款規定，對於有猥褻之言語、舉動或其他方法，調戲異性者，警察機關亦有立即調查之義務，故 A 得依其法定職權，得請求該網站管理者協助，提供相關的資料，(1)正確。非公務機關對於個人資料的利用，僅有個人資料保護法第 20 條列舉的事由下，才能例外為特定目的外之利用，因(4)並無任何個資法第 20 條列舉事由，故 B 應拒絕，故(4)正確。參考法務部見解，警察機關基於調查社會秩序維護事件之需要，而由非公務機關提供個人資料，亦應符合個資法第 20 條第 1 項第 2 款「為增進公共利益所必要」之要件，並不違反個資法，故(2)錯誤，(3)正確。