整合新版個資法與 ISO 27001&27011 於電信業客戶個資管理探討

林哲民　　陳致穎　　林宜隆
國立宜蘭大學 資訊工程研究所
cris_lin@cht.com.tw ; n0043006@ems.niu.edu.tw ; cyberpau747@mail.ypu.edu.tw

摘要

電信業務包含固網寬頻業務、數據業務、行動業務、國際業務、查號及查號加值業務、國內/國際長途電話人工業務轉接以及上述各業務之障礙申告受理、客戶申訴案件處理、資訊業務等，重新審視內部作業流程的個資保護措施，提升整體員工對於個資保護的意識。除業務範圍外尚有帳務處理、詐欺防制、客戶服務等關鍵營運流程，以及行動通訊維運支援系統之開發、運作及維護，及行動通訊網路活動監控中心之管理與防駭，各種流程與資訊系統，從流程管理與作業層次建立更完整與高規格的個資保護機制，以落實新版個資法施行細則安全維護事項。電信業者需訂定所有員工可依循之標準，並藉以建立所有人員重視個人資料保護之觀念，避免因一時之疏忽,造成客戶個人資料之毀損、遺失、外洩及其它無可彌補之損失。

為因應新版個資法的實施，對於已導入資訊安全管理系統之電信業者，應如何整合新版個資法，以達到法令所要求的對個人資料應善盡保管之職。藉由 ISO 27001 & ISO 27011 管理要項，對應新版個資法施行細則第 12 條中適當安全維護措施所訂定規範，電信業者如何加強管理與教育訓練以予符合其法令，藉以達到新版個資法規範個人資料之蒐集、處理及利用之適當之安全措施目的，為本研究所探討的主要重點。

關鍵詞：ISO 27001、ISO 27011、新版個資法、個資管理

Abstract

The telecommunications businesses include fixed broadband businesses , data services , mobile businesses , international businesses , inquiry numbers and inquiry number value-added services , domestic/international manual call transfers , as well as acceptance of fault declarations , customer complaints handling , and information businesses of the above mentioned businesses. The personal data protection measures of internal processes should be re-examined to enhance all personnel's awareness of personal data protection. In addition to the scope of business , there are still accounts processing , fraud prevention , customer service and other key operating processes , as well as the development , operation , and maintenance of mobile communication support system , monitoring center management for mobile communications network activity and anti-hacker , other various processes , and information systems. Process management and operational levels need to establish a more complete personal data protection mechanism with high specifications , in order to implement the security matters of the new Personal Data Protection Act Enforcement Rules.

In response to the new Personal Data Protection Act , how carriers with imported information security management system can integrate the new Personal Data Protection Act to achieve their custodial responsibility must be discussed. Through the key management elements of ISO 27001 & ISO 27011 that correspond to the norms set to the appropriate security maintenance measures in Article 12 of the new Personal Data Protection Act Enforcement Rules , how carriers can strengthen management and educational training in compliance with the Act also requires discussion. In order to achieve the appropriate security measures in the collection , processing and use of personal data as specified by the new Personal Data Protection Act are also focuses of discussion in this study.

Keywords: ISO 27001 , ISO 27011 , new Personal Data Protection Act , personal data

1. 前言

隨著個人資料保護法在2010年5月26日之公布，個人資料保護的資訊安全管理議題已成為眾所矚目之焦點，電信服務是國人生活最息息相關的服務之一，由於現今移動通信及網際網路業務的蓬勃發展，且在寬頻移動化及移動寬頻化的時代潮流下行動電話用戶與固網寬頻用戶日益快速增長，幾乎人人都有手持式的移動通訊設備。電信業擁有數量龐大的用戶個人資料，業者要如何將電信業藉由ISO 27001標準來導入新版個資中，做好ISO 27001與ISO 27011電信事業資訊安全管理實作指引,讓用戶可以放心、安心地享受電信服務，沒有後顧之憂！全台的語音或網路封包都需經過電信業者的電信設備，因此當資訊安全事件的威脅程度與日俱增，避免有心人士的監控、攔截與阻斷相關服務與盜取個資，電信業者就有責任與義務，做好把關的工作及確保使用者的資訊安全。

2. 個人資料保護法發展演進

我國於民國 99 年 5 月 26 日公布「個人資料保護法」條文，藉以規範公務和非公務機關對於個人資料的蒐集、處理及利用。為加入世界貿易組織，因考量歐盟對個人資料保護之重視程度，1992 年由法務部草擬「電腦處理個人資料保護法」送立法院審查，於 1995 年完成三讀立法程序，並經 總統於同年 8 月公布施行。該法係參照經濟合作暨發展組織揭示之資料保護八大原則所制訂。由於本法嚴格規範有關個人資料之蒐集、處理及利用行為，為避免對民間衝擊過大，並考量執法效能與社會各界之接受程度，參酌當時日本「電子計算機處理個人資料法」與英國 DPA 立法例，僅將經電腦處理之個人資料納入保護範疇。

為避免人格權受侵害，並促進個人資料之合理利用，我國「電腦處理個人資料保護法」因時代變遷已諸多不合時宜，故於 2010 年 4 月 27 日修法三讀通過並修正名稱為《個人資料保護法》(簡稱新版個資法) 新版個資法在 2010 年 5 月修正公布。新版個資法第 6 條特種個人資料蒐集處理利用要件太過嚴苛、第 54 條規定告知義務溯及完成的 1 年時限不合理等，法務部已提修正草案提報行政院，2012 年 8 月經行政院會通過後已送立法院審議。

2.1 新舊個資法比較

新版個資法不僅注重個人資料之安全防護，更特別強調在取得個人資料時，必須保障當事人之隱私自主權，其處理或利用應與蒐集目的有正當合法之關聯，根據新版個資法，媒體基於新聞報導的公益目的而蒐集醫療、基因、性生活等個人資料，個人資料之分類如**表 1**，基本上可不需告知當事人；非公務機關使用或處理個人資料，如果與公共利益有關，或個人資料取自於一般可得來源，且使用該資料有比保護資料更重大利益，不需要經過當事人同意即可使用[1]。

表 1 個人資料之分類

一般資料	特種資料
生存自然人之姓名、出生年月日、國民身份證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、聯絡方式、財務情況、社會活動	醫療、基因、性生活、健康檢查、犯罪前科
與客戶存有特定關係或當事人同意時即可利用，但要告知	原則不可蒐集處理，依法令才可!
及其他得以直接或間接方式識別該個人之資料(概括條款)	

表 2 新舊個資法及電信業客戶個資重點比較[2]

定義	
舊法	自然人之姓名、出生年月日、身份證統一編號、特徵、指紋、婚姻、家庭、教育、職業、健康、病歷、財務情況、社會活動及其他足資識別該個人之資料。
新法	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。
電信業客戶個人資料	身份證與第二證件影本、申請人之姓名(或公司行號、機關團體)、出生年月日、身份證統一編號、聯絡方式、帳單地址、電話號碼。
擴大適用主體	
舊法	公務機關與非公務機關（醫院、學校、電信業、金融業、證券業、保險業、大眾傳播業、徵信業等八類行業。）
新法	打破行業別限制，包含各行各業及個人。
電信業客戶個人資料	屬非公務機關(包含第一、二類電信業務及中華電信內所有提供之電信服務)。
擴大保護客體	
舊法	個人資料檔案：指基於特定目的儲存於電磁記錄物或其他類似媒體之個人資料之集合。 蒐集：指為建立個人資料檔案而取得個人資料。
新法	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。 蒐集：指以任何方式取得個人資料。
電信業客戶個人資料	所申請之電話號碼、ADSL帳號密碼、申請之IP位置。
增修行為規範	
舊法	個人資料之蒐集、電腦處理、利用、國際傳遞，依誠實及信用方法為之。
新法	醫療、基因、性生活、健康檢查及犯罪前科等五類資料，原則不得蒐集、處理或利用，特定目的外利用個資需當事人書面同意方式。
電信業客戶個人資料	不得蒐集、處理或利用客戶之通聯記錄、行動電話之客戶位置、使用 MOD 之收視習慣。

2.2 新版個資法中適當安全維護措施

而新版個資法「個人資料保護法施行細則」中 ，第 12 條與電信業資安及個資管理最為密切， 規範如下 :「個人資料保護法施行細則」第 12 條

本法第六條第一項第二款所稱適當安全維護措施、第十八條所稱安全維護事項、第二十七條第一項所稱適當之安全措施，指公務機關或非公務機關為防止個人資料被竊取、竄改、毀損、滅失或洩漏，採取技術上及組織上之措施。前項措施，得包括下列事項，並以與所欲達成之個人資料保護目的，具有適當比例為原則：

一、配置管理之專責人員及相當資源。
二、界定個人資料之範圍。
三、個人資料之風險評估及管理機制。
四、事故之預防、通報及應變機制。
五、個人資料蒐集、處理及利用之內部管理程序。
六、資料安全管理及人員管理。
七、認知宣導及教育訓練。
八、設備安全管理。
九、資料安全稽核機制。
十、使用紀錄、軌跡資料及證據保存。
十一、個人資料安全維護之整體持續改善。

此章後續將整合比較此細則與 ISO 27001 及 ISO 27011 的關係。

3. ISO/IEC 27000 系列介紹

在實務上要列出所有想得到的控制在一個通用的標準中是不太可能的。因此 ， 工業規範實作指引針對資安部分有了一系列的規範如表 **3** 及表 **4**:

表 3 ISO/IEC 27000 系列

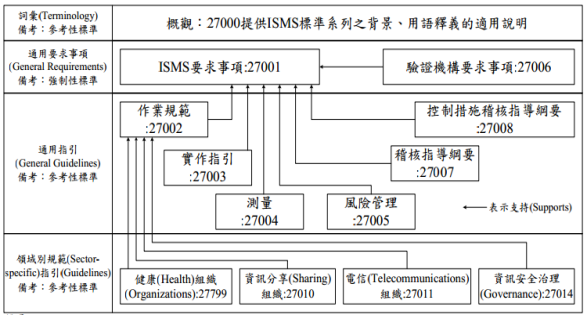

表 4 ISO 27000 標準整理

ISO/IEC 27000:2009	Overview & vocabulary 概觀與語彙
ISO/IEC 27001:2005	Requirements 要求 (可以驗證)
ISO/IEC 27002:2005	Code of practice for Information Security Management (教你怎麼做，不能驗證) Controls that match those in Annex A of ISO 27001資訊安全管理系統的作業規範與ISO 27001相配合的控制措施
ISO 27003	Implementation Guidance 實作指導方針
ISO 27004	Measurement 量測
ISO 27005	Risk Management 風險管理
ISO 27006	Requirements for Bodies providing Audit and Certification of ISMS 資訊安全管理系統驗證系統認證規範 ，驗證公司需遵守的要求，如 BSI 、SGS … 等 (例如：查核人天數的決定)
ISO/IEC 27011:2008	Information security management guidelines for telecommunications organizations based on ISO/IEC 27002 基於 ISO/IEC 27002 之電信組織的資訊安全管理指導綱要 (針對電信產業的額外參考)
ISO/IEC 27017	Information technology—Security techniques — Security in cloud computing (DRAFT) 雲端計算安全 (草案)
ISO/IEC 27018	Information technology —Security techniques — Privacy incloud computing (DRAFT) 雲端計算隱私 (草案)

3.1 資訊安全管理系統要求事項： ISO/IEC 27001

國際標準組織 ISO 於 2005 年 10 月 15 日公佈 ISO 27001 資訊安全標準，是一種國際認可的資訊安全管理體系驗證標準；ISO 27001 資訊安全標準是從英國標準協會提出之 BS7799-2 標準，延伸整合而成的國際資訊安全標準。

ISO/IEC 27001 的制訂宗旨是確保企業資訊的機密性、完整性及可用性，為達成這些宗旨，該標準共提出了 39 個控制目標及 133 項控制措施如表 **5** 所示，推行 ISO/IEC 27001 的企業可在其中自由選擇適用於其業務的控制措施，但亦可額外加進其它的控制措施[3]。

表 5 ISO 27001 中控制目標與控制措施

A.5 安全政策 (Security Policy)[1，2]					
A.6 資訊安全組織 (Organization of Information Security)[2，11]					
A.7 資產管理 (Asset Management) [2，5]					
A.8 人力資源安全 (Human Resources Security) [3，9]	A.9 實體與環境安全 (Physical and Environmental Security) [2，13]	A.10 通訊與作業管理 (Communications and Operations Management) [10，32]	A.11 存取控制 (Access Control) [7，25]	A.12 資訊系統之取得、開發與維護 (Information Systems Acquisition，Development and Maintenance) [6，16]	A.13 資訊安全事故管理 (Information Security Incident Management) [2，5]
A.14 營運持續管理 (Business Continuity Management) [1，5]					
A.15 遵循性 (Compliance) [3，10]					

附註：[m，n]－[控制目標的數目，控制措施的數目]

3.2 電信事業資訊安全管理實作指引: ISO 27011

第一類電信事業就包含電信基礎設備，像是行動基地台、ADSL、光纖等電信、網路服務是須經

主管機關特許的產業，倘若網路一旦被入侵可能就有上千、上萬筆資料被竊取，甚至攸關國家安全，為保障民眾個人資料、企業營運機密、電信網路設施及金融交易資訊等整體資通訊網路與服務之安全，因應政府於 99 年公告開放電信事業赴大陸地區投資電信業務之資通安全需求，於民國 97 年針對電信事業公布之資通安全管理實作指引（ISO/IEC 27011）[4]。

電信事業資通安全管理手冊依電信事業資訊通訊安全管理作業要點第二點之規定訂定之，包含下列要項:

（一）資通安全管理標準。參照:
1、資訊安全管理系統要求事項：ISO/IEC 27001。
2、資訊安全管理作業規範：ISO/IEC 27002。
3、資訊安全管理風險管理：ISO/IEC 27005。
4、電信事業資訊安全管理實作指引：ISO/IEC 27011
（二）資通安全等級評估。
（三）資通安全管理機制及教育訓練。
（四）資通安全應變通報。
（五）資通安全實施評鑑。
（六）年度提報資料要求。

3.3 整合 ISO 27001 與 ISO 27011 對應新版個資法

故企業當初在建置資訊安全管理系統(ISMS)，有涵蓋到個人資料的系統範圍，許多項目就不需重新規範。與 ISMS 相比，此安全維護事項直接要求界定個資範圍，因為有個資存放的設備就是高風險高機密區域了，整理相關對映如表 **6**。

表 6 ISO 27001 控制目標對應 ISO 27011 及新版個資法

ISO: 27001	ISO 27011 增項稽核表	新版個資法施行細則第 12 條
A.5 安全政策		十一、個人資料安全維護之整體持續改善。
A.6 組織資訊安全	1. 資訊安全組織 (ISO 27001 措施延伸:1 項，ISO 27011 新增措施:1 項)	一、配置管理之人員及相當資源
A.7 資產管理	1. 資產管理 (ISO 27001 措施延伸:0 項，ISO 27011 新增措施:1 項)	二、界定個人資料之範圍
A.8 人力資源安全	2. 人力資源安全 (ISO 27001 措施延伸:1 項，ISO 27011 新增措施:6 項)	七、認知宣導及教育訓練
A.13 資訊安全事件	8. 資安事故管理 (ISO 27001 措施延伸:2 項，ISO 27011 新增措施:2 項)	四、事故之預防、通報及應變機制
A.9 實體與環境安全	3. 實體及環境安全 (ISO 27001 措施延伸:13 項，ISO 27011 新增措施:2 項)	八、設備安全管理
A.10 通訊與作業管理	4. 通信與作業管理 (ISO 27001 措施延伸:3 項，ISO 27011 新增措施:5 項)	十、使用紀錄、軌跡資料及證據保存
A.11 存取控制	5. 存取控制 (ISO 27001 措施延伸:5 項，ISO 27011 新增措施:0 項)	九、資料安全稽核機制
A.12 資訊系統取得、開發與維護	6. 資訊系統獲取、開發及維護 (ISO 27001 措施延伸:1 項，ISO 27011 新增措施:4 項)	六、資料安全管理及人員管理
A.14 營運持續管理	(ISO 27001 措施延伸:1 項，ISO 27011 新增措施:1 項)	三、個人資料之風險評估及管理機制
A.15 遵循性	(ISO 27001 措施延伸:1 項，ISO 27011 新增措施:0 項)	五、個人資料蒐集、處理及利用之內部管理程序

4. 整合 ISO 27001 & 27011 與新版個資法於電信業客戶個資管理模式之建構

將個資保護整併至 ISMS 的第一步，就是導入 ISMS 或檢視範圍，確認其是否涵蓋組織內的個資相關流程。目前 ISMS 導入範圍多以資訊部門為主，但個資相關的作業或流程與其他部門有關，因此，首要就是進行業務流程普查，將握有個資的部門或相關作業流程納入ISMS 範圍內。確立範圍後，接下來就是盤點手中現有的個資，惟有清楚掌握保護標的，才能規劃恰當的安全控制措施。資訊安全事故管理、營運持續管理、個資風險作業流程；並確認適法性、解決方案建議、記錄保存與內部稽核完成所有資安程序機制後企業開始執行，並透過稽核的方式找出缺失已進行改善。落實 P-D-C-A 精神，讓實際運作能有不斷改善提升，強化資安防護之規

範。透過內部稽核、外部稽核協助企業找到弱點並有效改善，最終得到 ISO 認證，如圖 **1** 將 ISO 27001 & ISO 27011 整合與新版個資法安全措施導入 P-D-C-A[5]。

圖1整合ISO 27001 & ISO 27011與新版個資法安全措施導入P-D-C-A

建立整合以 ISO 27001 & ISO 27011 控制要項與控制措施為基礎的評核表，以表 **7** 為例:以個人資料保護法施行細則保護措施的 12 大項，且仿照 ISO 的稽核驗證方式，將電信業者的個資管理及保護措施狀況具體呈現並予以量化，以利分析歸納。個資保護與管理評核表其控制措施對要導入 ISO 27001 或新版個資法的機關、企業有相當大的參考價值，希望在提升電信業者的資訊安全強度，建立完整的安全防護體系，也希望各機關有所遵循，未來有更多機關通過 ISO 驗證增加民眾對資訊安全的信賴。惟有落實與時俱進的 ISMS 於日常生活中，才能成功邁向優質網路社會，確保人民生活之便利與安全；我們發現規範是控制犯罪者犯罪與否的外在主要因素，ISMS 資訊安全管理系統是針對網路情境犯罪所設計的預防措施，讓犯罪者要在網路世界裡獲得違法利益是很困難、高風險、且低報酬。電信業應建置一個具備完整良好資料治理，落實自我查察以及持續運作改進的制度與相關的內控流程，利用 PDCA 之方法對個人資料保護管理制度之計畫、執行、檢查與行動階段規劃細部工作內容，進而貫徹落實並持續維持個人資料保護管理制度之有效性。

表 7 以施行細則中 12 項保護措施建立評核表

一、配置管理之人員及相當資源。			
項次	評鑑項目	ISO 27001 相關條文編號	ISO 27011 相關條文編號
1.1	公司企業代表人是否指定管理階層為專人統籌、指揮企業內部個人資料保護事務事宜？	A.6.1.1 A.6.1.3	
1.2	公司是否以建置個人資料保護與管理制度？	A5.1.1 A5.1.2	1.1
1.3	公司是否配置有專責管理公司個人資料保護與管理之人員？或已就個人資料之保護與管理成立跨部門之常態任務編組？	A6.1.3	
1.4	公司負責個人資料管理的人員是否為對全公司之重要事務具有決策權之人，或其就個人資料保護與管理事務可直接向公司決策階層負責？	A6.1.3	
1.5	公司是否已提供必要資源（例如各項軟、硬體或經費），以進行公司之個人資料保護與管理？	A6.1.3	

參考文獻

[1] NII 產業發展協進會，2011，個資法說明與因應

[2] 行政院，電腦處理個人資料保護法修正草案總說明 http://www.moj.gov.tw/public/Attachment/622116374334.pdf

[3] 徐弘昌，2009，以 ISO 27001 為基礎評估電信業資訊安全管理 以第一類電信業者為例。

[4] 國家通訊傳播委員，2010，電信事業資訊通訊安全管理作業要點。

[5] 國家通訊傳播委員會，蘇思漢，2011，電信事業導入資訊安全管理系統（ISMS）訪談會議。