CAA 電腦稽核

JOURNAL OF INFORMATION COMMUNICATION AND TECHNOLOGY AUDITING

組織資料保護與利益關係人隱私

Computer Audit Association

民國107年7月31日　第38期

個人資料管理系統驗證
要求事項標準化實施初論

大數據環境下
政府審計之查核風險

外掛式資料查核及保護方案探討

醫療隱私之法律保障

以 MitmProxy 窺探手機應用程式隱私

Location-based Privacy: Problems Analysis and Protection

歐盟GDPR與個人資料保護認證

編 輯 序

面對數位化的衝擊與創新經濟之發展，企業經常以服務為前提，運用各式各樣的資訊科技、通訊網路、雲端及物聯網設施來蒐集大量資料，以幫助組織達到獲取利潤、追求永續經營之目的。就資料應用層面而言，企業可透過各種技術來取得、傳遞及儲存各種樣態資料，並經由分析、比對、與組合之方式來進一步了解市場的現況與趨勢，讓資料成為企業有價值的重要資產。然而，就資料保護層面而言，目前雖有相關規範與個人資料法保護法（ Personal data protection act）等機制，可保護個人與組織的資料被不法蒐集、處理、利用或其他的侵害行為。但是眾多的保護措施若無法在組織中予以落實及貫徹內部控制與查核作業，則在相關機制欠缺周全的情況下，仍然容易衍生資料外洩或不當被運用的可能性，讓利益關係人的人格權或隱私權受到侵害而引起社會爭議。資料保護已儼然成為現今數位經濟環境下，做好組織內部稽核不可忽略的重要環節，更是強化營運生態體系的重要課題。國際電腦稽核協會（ISACA）目前已針對組織資料保護及利益關係人隱私權議題發起高峰會議，希望能透過此會議來獲得實務界 IS/IT 部門專業人士在這此議題的洞察力和建議，從而達到改善組織潛在風險、資料保護、與內部控制之目的。資料保護的落實，已成為組織日常運作的重要環節，也唯有從組織、個人、與法規等各個層面著手探討問題，並找出解決問題之方案與控管策略，如此才能收到應有的成效。

有鑑於此，電腦稽核期刊第三十八期以「組織資料保護與利益關係人隱私」為主軸，邀請國內外學者與專家，提出具創新性與實用性的論文，剖析數位時代環境下所衍生的資料保護問題，以及思考如何透過電腦稽核與內部控制機制來因應衝擊，從而達到保護組織與利益關係人資料、促進產業發展與國家政策制訂、及推動電腦稽核學術研究之目的。電腦稽核期刊強調理論和實務並重，本期收錄文章內容包括：「個人資料管理系統驗證要求事項標準化實施初論」、「資訊自動化下政府查核風險與資料探勘」、「醫療隱私之法律保障」、「外掛式資料查核及保護方案探討」、「以 MitmProxy 窺探手機應用程式隱私」、「Location-based Privacy Issues Analysis and Protection」、「歐盟 GDPR 與個人資料保護認證」、「機器人，流程改善的新工具」。本期刊希望透過優質文章的收錄，來啟發讀者在資料保護與利益關係人隱私等議題的關注與研究興趣，進而為電腦稽核領域帶來更成熟之發展。

最後，本期刊由衷感謝各位作者賜稿及協會祕書處之協助，更感謝各位審稿委員細心審閱。本期期刊若有不盡之處，敬請各位先進賜教。

編譯出版委員會主任委員

電腦稽核

目　錄

CONTENTS

會務交流

刊誤啟事

本刊上期期刊（37th）第 4 篇（第 45 頁）作者介紹缺漏，完整資訊應補上「林雨萱、國立雲林科技大學會計系、E-mail: m10425025@yuntech.org.tw」，特此更正致歉，不便之處，尚祈見諒！

發 行 人：張紹斌

總 編 輯：張碩毅

編輯委員：張碩毅、李順保、李興漢、孫嘉明、徐立群、黃劭彥、劉其昌、邵之美、諶家蘭

封面提字：林志雄

秘 書 長：黃涼澤

秘　　書：何慈雯、許秀玲、謝芷齡

展 售 處：中華民國電腦稽核協會

地　　址：11070 臺北市基隆路一段 143 號 2 樓之 2

電　　話：(02)2528-8875

網　　址：http://www.caa.org.tw

視覺設計：品晟股份有限公司

印　　刷：品晟股份有限公司

發行日期：2018 年 7 月 31 日

定　　價：新臺幣 250 元

電腦稽核
JOURNAL OF INFORMATION COMMUNICATION AND TECHNOLOGY AUDITING 第 38 期

個人資料管理系統驗證要求事項標準化實作初論：根基於ISO/IEC JTC 1/SC 27在2017-01公布的框架

Personal Information Management System Requirements Standardization and Implementation: Based on New Framework of ISO/IEC JTC 1/SC 27

蔡昀臻
國立交通大學管理科學研究所
E-mail:yct1230@gmail.com

樊國楨
臺灣經濟新報文化事業股份有限公司
E-mail:kjf.nctu@gmail.com

摘　要

個人資料保護法施行細則第 17 條闡明：「…… 所稱無從識別當事人，指個人資料以代碼、匿名、隱藏部分資料或其他方式，無從辨識該特定個人者 」亦即通稱「 去識別化 (De-identification)」之議題，自 2014 年 11 月 17 日法務部法律字第 10303513040 號函的函釋：「 去識別化之個人資料依其呈現方式已無從直接或間接識別該特定個人者即非屬個人資料 」起，其「 驗證 (Certification)」成為我國標準化工作項目的優先項目。根基於此，本文探討包含前述「 去識別化 」之歐盟「 一般資料保護條例 」規範的「 個人資料管理系統 」驗證，其遵循之國際標準化組織 (International Organization for Standardization, ISO) 於此議題的標準化作業之脈絡及前景，並在最後提出本文的觀察與建議代為結論。

關鍵字：驗證、個人可識別資訊、個人資料管理系統、資訊安全管理系統、標準化

Abstract

Enforcement Rules of the Personal Information Protection Act Article 17 states that "the Act shall mean the personal information processed by ways of code, anonymity, hiding parts of information or other manners so as to fail to identify such a specific person.", so as call the "De-identification" issue. Since 2014, Nov 17th the Ministry of Justice has explained that "De-identified personal information cannot identify directly or in-directly a specified individual." certification has become our standardization primary issue. Thus, we discuss EU's "General Data Protection Regulation" including "De-identification" mention before in "Personal information management system" certification , whose implementation follows International Organization for Standardization (ISO) standardization. The article is going to conclude with observation and suggestion to the status quo of protecting personal data in Taiwan subject to learning experience from the ISO standardization in striving for protecting personal data.

Keywords：

Certification, Personally Identifiable Information (PII), Privacy/ Personal Information Management System (PIMS), Information Security Management System (ISMS), Standardization

壹、前言

九十年代全球文明歷經了重大的轉變，品質、環境和職業安全衛生管理逐漸朝向一致化與標準化，而相關的國際標準也影響了許多國家經濟的發展以及組織管理與經營的方式，ISO 9000 品質管理和 ISO 14000 環境管理系列標準的遵循，就是最佳的佐證。2000 年 12 月 1 日，資訊安全管理系統 (Information Security Management System，ISMS) 控制措施之 ISO/IEC 17799: 2000(E) 公布，2002 年 12 月 5 日相對應之 CNS 國家標準正式頒布，建立 ISMS 並擴大推動驗證已成為資訊安全之工作項目的主軸之一。2006 年 6 月 16 日，經濟部標準檢驗局再公布了 ISO/IEC 27001: 2005(E) 之資訊安全管理系統的要求事項等國家標準，也成就了資安管理制度與國際化接軌的開端。

「讓過去與現在爭執不下，將錯失未來 (Opportunities for future will be missed if the past is allowed to argue with today)」，ISO/IEC JTC 1/SC 27 主席 Walter Fumy 先生，在世界資訊高峰會之邀請下，於 2004 年 9 月 24 日公布了 ISO 之深度防禦 (Defense in depth) 的資訊安全管理模型觀點；其標準組件 ISO 27001 標準系列之 ISO/IEC 27003 已於 2010

年 2 月 1 日正式發行，ISMS 標準化的第一階段工作已樹立第 1 座里程碑。

鑑於管理系統日益增多，其標準系列宜加以規範，國際標準組織 (International Organization for Standardization, ISO) 自 2000 年起即分 3 階段進行管理系統標準 (Management System Standards, MSS) 之標準化工作；已正式納入 ISO 之強制性規範 (Procedures specific to ISO)，期能在第 3 階段 (2011~ 2015 年) 完成各個管理系統要求事項的調和。ISO/IEC 27001 標準系列已遵循 MSS 逐步建立中，並納入個人資料 / 隱私管理系統 (Personal/Privacy Information System, PIMS) 安全規範之議題；以個人資料保護法施行細則第 17 條之規範為例，已公布 ISO/IEC 27009、ISO/IEC 29101、ISO/IEC 29191、ISO/IEC 20008 與 ISO/IEC 20009 標準系列，作為其 PIMS 中「 前檯匿名、後檯實名 」之實作要求事項的參考。2012 年 10 月，ISO/IEC JTC 1/SC 27 在進行為期 1 年之 2 階段的研究後，正式公布 PIMS 之要求事項遵循 ISO/IEC 27001，同時開展其標準系列 (ISO/IEC 27009、ISO/IEC 27018、ISO/IEC 27017、ISO/IEC 29134、ISO/IEC 29101、ISO/IEC 29151 以及預備文件 SD 4、SD 5 等) 的標準化計畫，已於 2017 年 8 月完成第 1 階段之工作項目；並根基於歐盟與美國聯邦政府實作意見分成「 管理 」、「 實作 」與「 技術 」3 個面向，進行第 2 階段的標準制訂之計畫。

研究「 標準化 」的人是需要有「 同情 」與「 推理 」兩種能力，所謂「 同情 」是指「 標準 」的制定者要有對等之情，那樣體驗的「 標準 」自然是立體、多元的；「 同情 」加上「 推理 」，則「 標準 」是活的，每一份「 標準 」的頒布是因或是果，是趨勢或是成績，「 標準 」的產生絕非偶然而是無數之努力的形成。「 標準化 」從長遠的角度來看，便可以體察出是有一股流勢，有無法阻擋的推移力量；MSS 與個人資料保護標準化及 ISMS&PIMS 的整合性安全管理系統 (Integrated(Information) Security Management System, IISMS) 之進程僅為一端。國際認證論壇 (International Accreditation Forum, IAF) 自 2013 年 3 月 25 日起，已發行整合性安全管理系統 (IISMS) 之第三方稽核的強制性文件 (IAF MD 11:2013)，除規範 ISMS 之第三方稽核的要求事項外並闡明其效益。根基於 IISMS 與雲端服務已成為資訊社會之基石，主責 ISMS&PIMS 標準化的 ISO/IEC JTC 1/SC 27 第一階段標準化之工作項目如圖 1. 1 所示，其中「 PII 原則係指國際公認之隱私原則 」(請參見附錄一)。

根基於 PIMS 標準化之歷程及 PIMS 資訊系統於「 PII 控制者 」即為「 雲端運算服務 」的事實，本文在第 2 節闡明個人資料管理系統要求事項標準化之進程；於第 3 節，探討雲端運算與資料去識別化等的新議題及其已納入 ISO/IEC CD 27552. 2 之擴增 ISO/IEC 27001 的 PIMS 驗證之要求事項進程的闡明；最後，在第 4 節提出借鏡個人資料管理系統標準化之進程與議題，作為我國 PIMS 及資料去識別化標準化藍圖參考的見解並代為本文之結論。

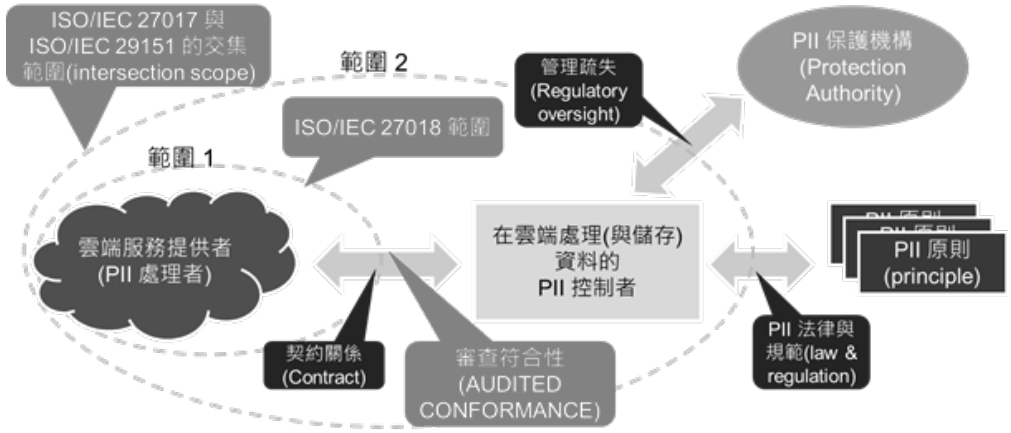


圖 1.1 雲端運算之 PIMS 控制措施的框架

說明：

1. PII 控制者 (PII controller)(或稱為資料控制者 (Data controller) 於某些管轄區 (Jurisdiction)) 意指決定個人資料處理或將要處理之目的 (Purpose) 與方法 (Manner) 之當事人 (單獨一人、與他人共同)。
2. PII 處理者 (PII processor) (或稱為資料處理者 (Data processor) 於某些管轄區 (Jurisdiction)) 意指代表 PII 控制者處理資料之任何人 (除了 PII 控制者的僱員外)。
3. 資料來源：Mitchell, C. (ISO/IEC 27018 編輯 (editor)), Outsourcing personal data processing to the cloud(presentation),2012-02-16，圖中之「交集範圍 (Intersection scope)」係指「聚集 (例：西江、北江與東江，三江匯流成為珠江)」。

貳、個人資料管理系統要求事項標準化之回顧與前瞻

2012 年 10 月，歷經 1 年 2 階段之研究，主責 PIMS 的要求事項之 ISO/IEC JTC 1/SC 27 的第 1 工作組 (Working Group 1, WG 1) 與主責隱私管理之第 5 工作組共同決定「個人資料管理系統」的要求事項根基於 ISO/IEC 27001 擴增之，同時立案進行其擴增 ISO/IEC 27002 控制措施的 ISO/IEC 29151 與擴增 ISO/IEC 27001 之規範的 ISO/IEC 27009 之標準化計畫；ISO/IEC 29151 已於 2017- 08 正式發行，「資訊技術 – 安全技術 – ISO/IEC 27001 特定領域應用系統 – 要求事項 (Information technology – sector – specific application of ISO/IEC 27001-requirements)」於 2016- 06- 15 已正式發行，完成 PIMS 標準化的第 1 階段工作項目。為因應實作之需求，2015 年 6 月 30 日，主責個人資訊安全標準化的 ISO/IEC JTC 1/SC 27/WG 5，根基於 ISO/IEC 27009 之標準化文件，先行公布擴增 ISO/IEC 27001 的 PIMS 要求事項之如圖 2. 1 所示的第 5 號《於隱私領域中 ISMS 的應用指導綱要 (Guidelines for the application of ISMS in the area of privacy)，簡稱 WG 5 SD 5》之預備文件 (Standing Document, SD) 的徵求意見稿，並更新其標準化計畫框架如圖 2. 1 所示；根基於此，公用雲 (Public clouds) 領域已據以 (ISO/IEC 27001+ISO/IEC 27002+ISO/IEC 27018) 進行驗證。2016 年 4 月，ISO/IEC JTC 1/SC 27/WG 1 根基於前述之 WG 5 SD 5 之 PIMS 要求事項的「資訊技術 – 安全技術 – 於隱私管理之 ISO/IEC 27001 擴增 - 要求事項 (Information techniques – security techniques – enhancement (extension)

to ISO/IEC 27001 for privacy management – requirements)」之 ISO/IEC 27552 之標準化計畫，並於 2016 年 12 月 5 日提出 ISO/IEC WD 27552. 1 的票決版。2012 年 1 月，歐盟開始整合「個人資料保護指令 (Directive 95/ 46/EC)」、「電子通訊隱私指令 (Directive 2002/ 58/EC)」與「電信網路改革指令 (Directive 2009/ 136/EC)」三大個人資料及隱私防護指令之法制，期以單一規則 (Regulation) 簡化機關 / 構以及企業的法規遵循義務並促進單一數位市場；2016 年 4 月 14 日經歐洲議會通過，於 2016 年 4 月 27 日公布之「一般資料保護規則 (General Data Protection Regulation，GDPR)」，已提出個人資料「擬匿名化」之新定義並於條款 11 闡明「去識別化」的應然，條款 25 闡明應根基於「從設計以及預設機制著手保護個人資料 (Data protection by design and by default)」實作 PIMS 之合適的「技術控制措施 (Technical measures)」與「組織控制措施 (Organizational measures)」（ENISA, 2014）。GDPR 於條款 40~ 43 規範其「行為準則及驗證 (Codes of conduct and certification)」，認證機構遵循產品驗證標準規範驗證機構；根基於 GDPR，相關機構幾均公布採用 ISO/IEC 27001 作為其包含資料去識別化的 PIMS 合規之驗證要求事項的規範（Official journal of the european union, 2016）。2017 年 1 月，依據 GDPR 第 42 條款，European Privacy Seal(EuroPrise) 公布 GDPR 驗證之共同準則，闡明於「資訊技術服務」將採用 ISO/IEC 27001 與 ISO/IEC 27009(未來為 ISO/IEC 27552) 作為驗證標準「產品 (含「軟體作為服務 (Software as a Services, SaaS)」等資訊系統)」採用 ISO/IEC 15408 標準系列作為驗證標準，以為 GDPR 條文中「組織控制」以及「技術控制」稽核的頂層設計原則，並於 2017 年 1 月公布其自 2007 年 8 月起準備之 GDPR 驗證準則，德國、英國、西班牙等試運行中 (EuroPriSe, 2017)；GDPR 第 41 條款規範 PIMS 之主責人員的「行為準則 (Codes of conduct)」，第 43 條款，

規範 ISO/IEC 17065 之「產品、過程與服務驗證機構認證規範」為認證機構稽核驗證機構的標準；並於條款 51~ 59，闡明其目的事業主管之「獨立監督機構 (Independent supervisory authorities)」的權責。

2015 年 7 月 31 日，院臺護字第 1040141147 號函頒「資訊系統分級與資安防護基準作業規定」之行政規則採用美國聯邦政府 ISMS 的安全及隱私控制措施之第 4 版，已整合 ISO/IEC 15408 標準系列於其中 (樊國楨、蔡昀臻，2016a)，其意旨與 EuroPriSe 相同。

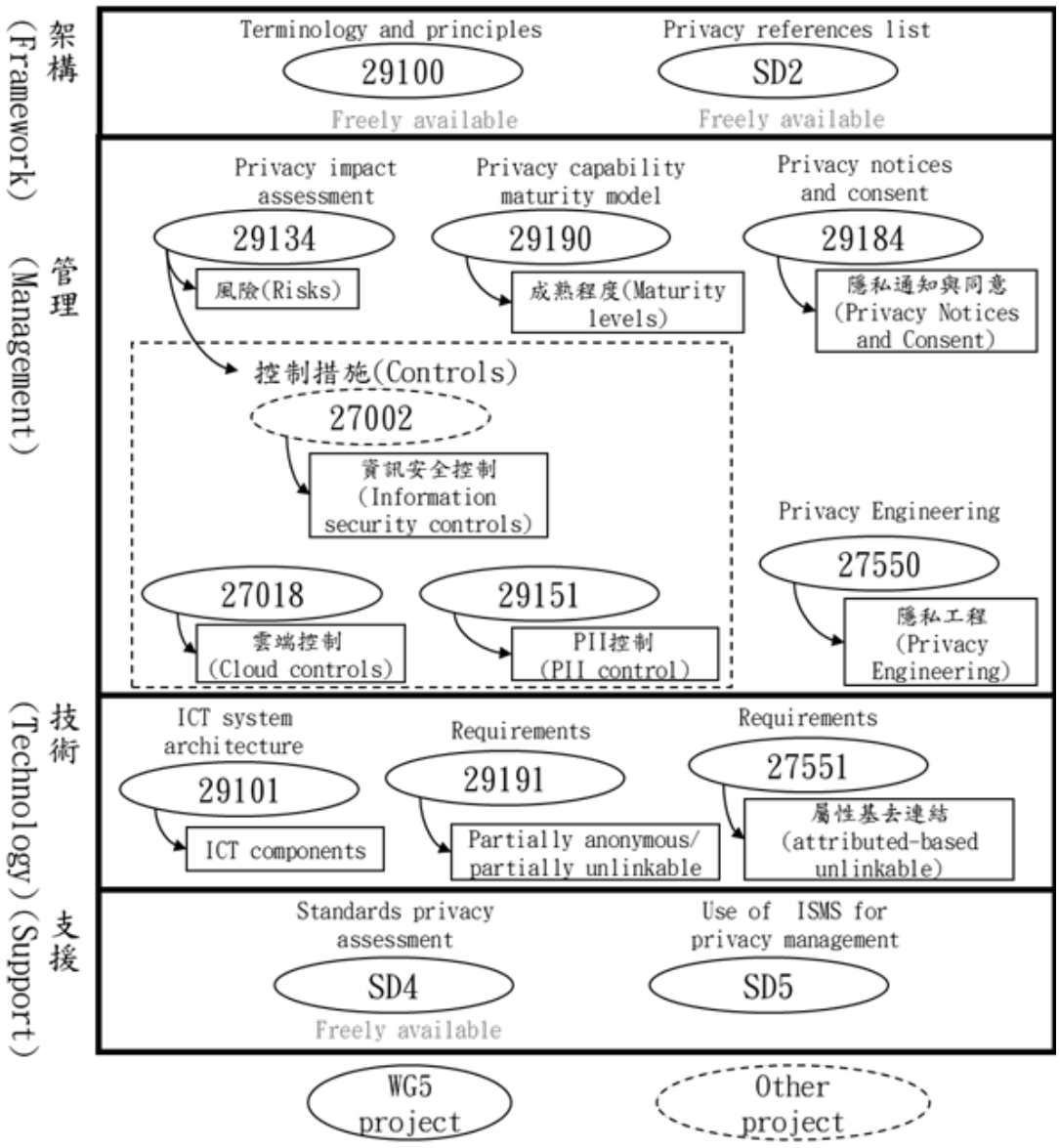


圖 2.1 身分管理與隱私科技標準框架

說明：

1. 參考資料：Rannenberg, Kai (2015) Standards contributing to the protection of consumers' privacy and personal data, ISO/COPOLCO (2015). The connected consumer in 2020- empowerment through standards, 2015-05-13, Geneve, Switzerland.
2. ISO/IEC 27551 為作者增列。

「使用與應用 ISO/IEC 27001 在特定領域與服務之被認證的第 3 方規範 (The use and application of ISO/IEC 27001 for sector/service-specific third-party accredited certifications，ISO/IEC DIS 27009: 2015- 07-27)」之附錄 B(Annex B)，已以「個人資訊管理系統 (Personal Information Management System, PIMS)」中的「隱私衝擊評鑑 (Privacy Impact Assessment, PIA)」為例闡明 ISO/IEC 27009 之運用方式；依此，分別探討 ISO 個人資料保護標準化之進程以及整合性個人資料管理與資訊安全管理的「整合性安全管理系統 (IISMS)」要求事項之脈絡。

2002 年，美國先於「電子化政府法案 (E-government act of 2002)」之第 208 節 (Section)」中規範 PIA 的工作項目；2008 年，進一步於「聯邦資訊安全管理法案 (Federal Information Security Management Act of 2002, FISMA 2002)」實作計畫中納入 PIA。2010 年 4 月美國國家標準與技術研究院 (National Institute of Standards and Technology, NIST) 公布「個人可識別資訊之機密性防護指引 (Guide to protecting the confidentially of Personally Identifiable Information (PII)) 的 NIST SP(Special Publications) 800 – 122，作為 FISMA 實作計畫控制措施之規範；2013 年 4 月，根基並修訂 NIST SP 800 – 122 的內容後併入第 4 版之 FISMA 實作計畫控制措施規範「聯邦資訊系統與組織的安全與隱私控制措施 (Security and privacy controls for federal information systems and organizations)」之 NIST SP 800 – 53 Revision 4 中，完成前述整合 ISMS 以及 PIMS 的標準化工作項目。2014 年 12 月 8 日，美國公布之「聯邦資訊安全現代法 (Federal Information Security Modernization Act of 2014，FISMA 2014) 的 3552(b)(3)(B) 條款沿用 FISMA 2002 之 3542(b)(1)(B) 條款，將「個人隱私 (Personal privacy)」納入；換言之，前述美國聯邦政府的「整合性安全管理系統 」已建立法規依據（OMB, 2016）。

ISO 自 2000 年起，即以試作 (Pilot: 2001~ 2005)、制定管理系統標準 (MSS) 之至次節的一致性高階規範程序 (Procedures specific to ISO: 2006~ 2010) 與完成各個管理系統之調合 (2011~ 2015) 的標準化工作項目；根基於此，ISO/IEC JTC 1/SC 27 於 2012 年 10 月決定 PIMS 直接使用 ISO/IEC 27001 之要求事項，並進行制定擴增其條款的 ISO/IEC 27009 之工作項目，在 2015- 07-27 提出意見及投票之 ISO/IEC DIS 27009 的附錄 B 中已以 PIMS 之 PIA 為例，闡明如何擴增 ISO/IEC 27001 的條款；並考量時效性，於 2014 年 4 月 9 日，先行公布 PIA 之 ISO/IEC JTC 1/SC 27/WG 5 SD 4 的預備文件，圖 2. 2 以及圖 2. 3 分別是其示意 明；圖 2. 3 之左下方敘明 PIMS 擴增 ISO/IEC 27001 要求事項部份與 PIMS 擴增 ISO/IEC 27002 控制措施部份遵循 ISO/IEC 27009 的規範於同一份標準中闡明。根基於此，各驗證機構紛紛公告以 ISO/IEC 27001 與 ISO/IEC 27009 作為 GDPR 之 PIMS 要求事項的驗證標準，應可作為我國落實「個人資料保護法 」之參考（行政院，2012）。

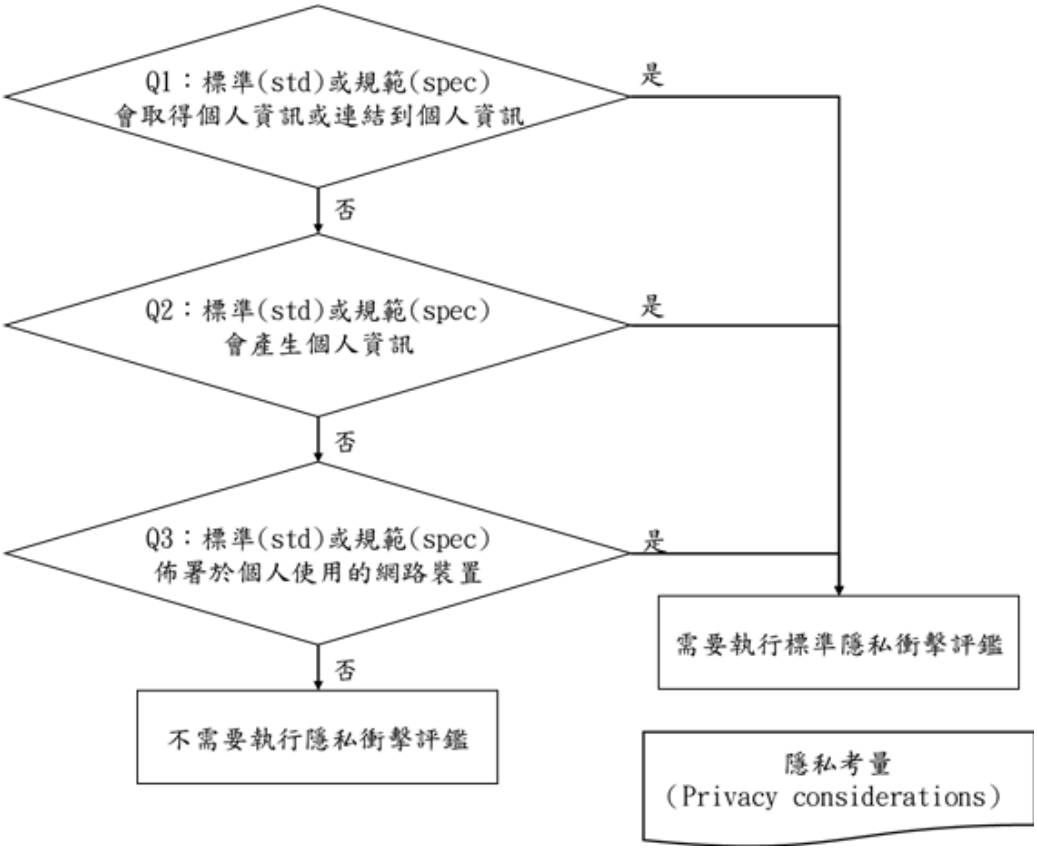


圖 2.2 判斷何時需要執行標準隱私評鑑 (Standards Privacy Assessment, SPA)

說明：ISO/IEC 29100：2012（E）中用語為：隱私衝擊評鑑（Privacy Impact Assessment, PIA）。

資料來源：ISO/IEC JTC 1/SC 27/WG 5 SD4: 2014

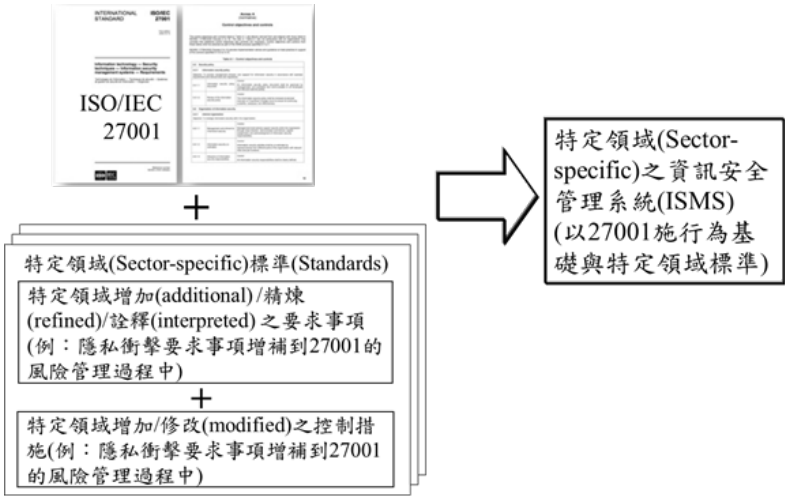


圖 2.3 ISO/IEC 27009 的應用

資料來源：ISO/IEC DIS 27009：2015-07-27.

未雨綢繆，主責個人資料管理系統標準化 (Personally Information Management System, PIMS) 之 ISO/IEC JTC 1/SC 27/WG 5 於2015- 06- 30已公布遵循圖2. 3之框架，如表 2. 1 所示的資訊安全管理系統 (Information Security Management System, ISMS) 要求事項宜擴增的 PIMS 之論題及其隱私防護的攸關標準，表 2. 2 是 PIMS 與 ISMS 間之用語對照。

表 2. 1 資訊安全管理系統要求事項與個人資料保護標準及論題之對應 (ISO/IEC JTC 1/SC 27/WG 5 N 110: 2015- 06- 30)

條款節碼	ISO/IEC 27001: 2013 要求事項	隱私攸關標準	論題
1	4. 組織全景 4. 1 瞭解組織及其全景 4. 2 瞭解關注方之需要及期望 4. 3 決定資訊安全管理系統之範圍 4. 4 資訊安全管理系統	ISO/IEC 29134 ISO/IEC 29100 ISO/IEC 29134	隱私風險準則 (Privacy risk criteria) 隱私保護要求事項 (Privacy safeguarding requirements) 隱私利益相關者 (Privacy stakeholder) 營運流程與目的 (Business process and purpose) 個人可識別資訊流程 , 隱私之支持資產 (PII flow, Privacy supporting assets)
2	5. 領導作為 5. 1 領導及承諾 5. 2 政策 5. 3 組織角色、責任及權限	ISO/IEC 29100	從設計著手 / 默認保護隱私 (Privacy by design/default) 隱私政策 (Privacy policy) 資料隱私管理官 (Data privacy officer) 隱私風險擁有者 (Privacy risk owners)
3	6. 規劃 6. 1 因應風險及機會之行動 6. 2 資訊安全目標及其達成之規劃	ISO/IEC 29134	隱私衝擊評鑑 (Privacy impact assessment) 隱私風險評鑑 (Privacy risk assessment) 隱私風險處理 (Privacy risk treatment)
4	7. 支援 7. 1 資源 7. 2 能力 7. 3 認知 7. 4 溝通或傳達 7. 5 文件化資訊		隱私事故管理 (Privacy incident mgmt) 隱私意識 (Privacy awareness) 隱私溝通 , 透明化 (Privacy communication,transparency)
5	8. 運作 8. 1 運作之規劃及控制 8. 2 資訊安全風險評鑑 8. 3 資訊安全風險處理	ISO/IEC 29134 ISO/IEC 29151	隱私生命週期管理 (Privacy life cycle mgmt) 隱私風險評鑑 (Privacy risk assessments) 隱私風險處理 (Privacy risk treatment)
6	9. 績效評估 9. 1 監督、量測、分析及評估 9. 2 內部稽核 9. 3 管理審查	ISO/IEC 29151 [ISO/IEC 291901]	隱私測量 (Privacy measurement) 隱私能力成熟度 [Privacy capability maturity]
7	10. 改善 10. 1 不符合項目及矯正措施 10. 2 持續改善		
8	附錄 A(規定) 參考控制目標及控制措施	ISO/IEC 29151 ISO/IEC 27018	隱私控制措施 (Privacy controls)

說明 1：編輯闡明，不適當待修定。

表 2. 2 對照 CNS 29100 概念與 CNS 27000 之隱私概念

CNS 29100 概念	對應 CNS 27000 概念
隱私權利害相關者	利害相關者
PII	資訊財產
隱私權違反	資訊安全事故
隱私控制措施	控制措施
隱私風險	風險
隱私風險管理	風險管理
隱私保全要求事項	控制目標

說明：個人可識別資訊 (Personally Identifiable Information, PII)

為易於特定隱私全景中使用 CNS 27000 系列標準及整合 CNS 27000 之隱私觀念，CNS 29100 於其附錄 A 已列出其主要概念間之關係；惟以 CNS 27001 第 6. 1. 2 節 (c)(2) 的風險擁有者為例，於資訊安全，其對應之資訊資產的當事人 (Principal) 幾均在組織內，而 PII 當事人大多在組織外，其歧異處具攸關性；根基於此，CNS 29100 再將組織內之風險擁有者區分為「判定 PII 處理之目的及方法的隱私權利害相關者，而非就個人目的使用資料之自然人」的「PII 控制者 (PII controller)」與「代表 PII 控制者並依其指示，處理 PII 之隱私利害相關者」的「PII 處理者 (PII processor)」，於公用雲的 CNS 27018 即為 PIMS 之 PII 處理者的擴增 CNS 27002 之控制措施標準，其與 2016 年 12 月 16 日提出之 ISO/IEC FDIS 29151 的票決版，已分別作為 2016 年 12 月 5 日提出之 ISO/IEC WD 27552. 1 之強制性的「附錄 A：PII 控制者之控制目的與控制措施」以及「附錄 B：PII 處理者之控制目的與控制措施」之參考藍本，於 PIMS，「PII 控制者」相似於「雲端運算」的使用者「PII 處理者」相似於「雲端運算」之提供者；圖 2. 3 所示的 PIMS 要求事項標準化第 1 階段如圖 2. 4 之工作項目已於 2017 年完成，圖 2. 5 是其實作過程的示意說明，宜作為我國建制 IISMS 之參考；此外，ISO/IEC 27005 已確認存在缺失（ISO, 2016c），實作時，宜關注此議題。

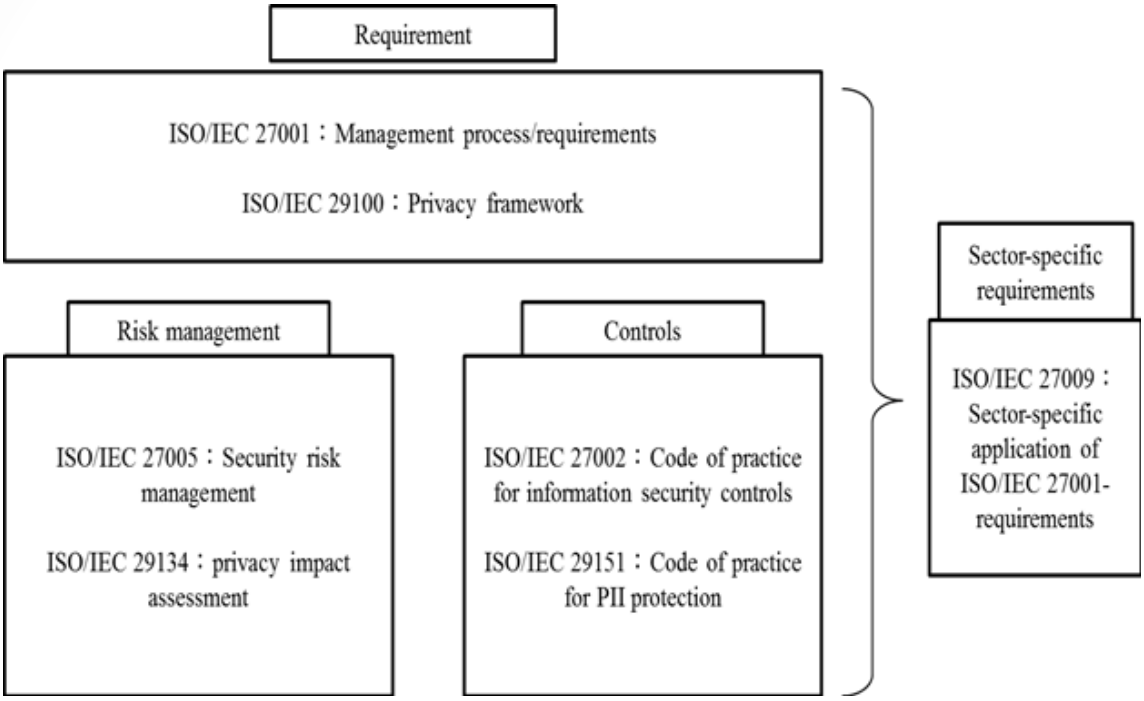


圖 2. 4 個人資料 / 隱私資訊管理系統驗證框架

說明：

1. 參考資料：ISO/IEC FDIS 29151, Figure 1, page X, 2016-12-20.
2. 隱私 / 個人資訊管理系統 (Privacy/Personal Information Management System, PIMS)。

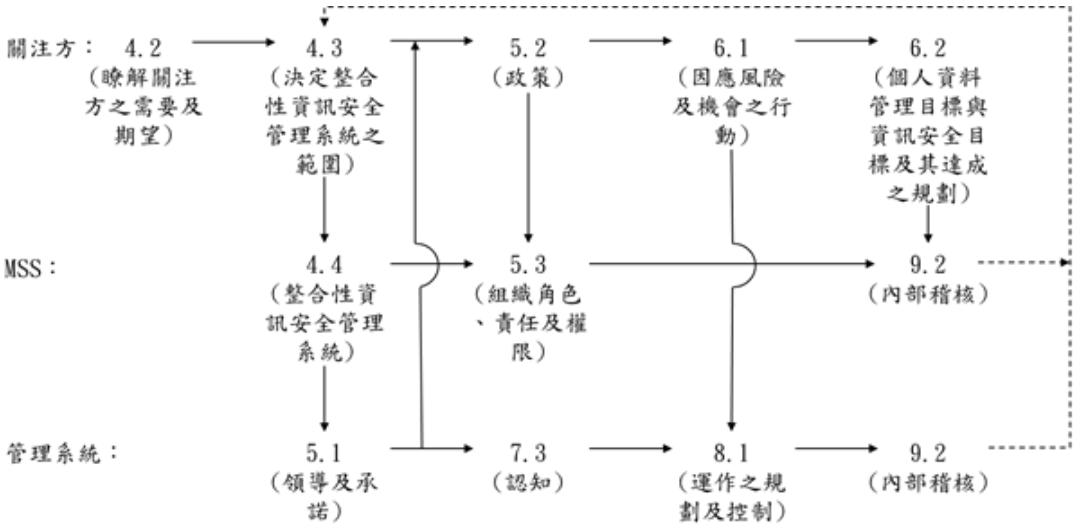


圖 2. 5 管理系統標準 (Management System Standard, MSS) 中之要求事項 (Requirement) 的分類與取徑示意 (Approach)：根基於 ISO/IEC 27001：2013(E)

說明：

1. 參考資料：Proposals for Management System Standards, ISO/IEC Directives Part 1, Consolidated ISO Supplement, Annex SL(Normative), 6th ed, 2015。
2. ISMS：Information Security Management System

2017年1月，ISO/IEC JTC 1 SC 27/WG 5公布了下一階段的個人資料/隱私管理之標準化框架，針對「智慧手機應用程式提供者」、「智慧城市」與「物聯網」的雲服務，其新增之應用範圍均涉及大數據分析的資料去識別化之議題。於圖2.3中的技術類，增列「資料去識別化」之ISO/IEC 20889標準化計畫；同時將「管理」類分成「管理」及「實施」2類，ISO/IEC 29134、ISO/IEC 27002、ISO/IEC 27018、ISO/IEC 29151與新增的ISO/IEC 27552為管理類，ISO/IEC 29184、ISO/IEC 29190及ISO/IEC 27550為實施類，作為支持PIMS要求事項標準化之準備；在另一方面，為因應GDPR規範之擬匿名化，針對PII去連結的需求與PIMS之控制措施應區分「PII控制者」及「PII處理者」等的不同之要求事項（ISO, 2017a）的控制措施，於立項進行ISO/IEC 27552的標準制定計畫中予以區分；換言之，內蘊資料去識別化的PIMS已成為數位社會之關鍵基礎建設。

2016年12月3日，因應圖2.4中之ISO/IEC 27005的缺失，經1年研究期之求索，ISO/IEC JTC 1/SC 27/WG 1已正式發出闡明ISO/IEC 27001: 2013(E)第6.1節以及第8節「因應風險與機會之行動」的「資訊安全風險與管理指南」之ISO/IEC 27005新版的設計規範草案，圖2.4框架中之ISO/IEC 27005已更新其內蘊；根基於表2.1的ISO/IEC 27552之標準制定計畫亦同。

ISO/IEC CD 27552.1：2017-12-08遵循ISO/IEC 27009：2016-06-15，於ISO/IEC 27001本文部分，參照SD 5，擴增第4節(組織全景)之4.0~4.4條款並闡明於第4~10節各條款中出現「資訊安全」之政策、目的、要求事項、風險評鑑、風險處理與風險管理均攸關於PII之處理(Processing of PII)；於ISO/IEC 27001附錄A(控制措施)部分，擴增31項控制措施；於PII控制者部分，增加4類共32項控制措施；於PII處理者部分，增加4類共19項控制措施；期於PIMS的實作，提供驗證之要求事項。舉例而言，於「資料去識別化」的工作項目，於ISO/IEC CD 27552.1：2017-12-08第7節「PII控制者的ISO/IEC 27002之增加」的第7.4.3~7.4.5條款：「PII之資料去識別化(PII data de-identification)」中闡明由PII控制者主責，其實作指引敘明其技術參照ISO/IEC 20889中描述(雲端運算於透明性(transparency)等宜遵循ISO/IEC 19944)（ISO, 2017a）；圖2.6是「資料去識別化」之「重新識別風險評鑑」與「隱私風險評鑑」關聯的參考（Garfinkel, 2015；蔡昀臻、樊國楨，2016b）。

綜上所述，於現階段，PIMS之實作除遵循ISO/IEC 27001、ISO/IEC 27002、ISO/IEC 27005、ISO/IEC 27009、ISO/IEC 27018、ISO/IEC 29100、ISO/IEC 29134、ISO/IEC 29191外、宜再增列ISO/IEC CD 27552.2：2018-06-04；若採行「從設計著手保護隱私(Privacy by Design, PbD)」與「以預設機制防護隱私(Data protection by Default或Privacy by Default, PbD)」之原則，ISO/IEC 29101、ISO/IEC CD 27550.2：2018-06-04亦宜增列；於歐盟，前述PbD係法規(GDPR條款25)的要求事項。

GDPR條款24與條款28敘明PII控制者及PII處理者嚴守被認可之條款40的行

為準則等同於通過條款 42 規範之驗證，作為證明符合 PII 控制者及 PII 處理者義務的要件；換言之，PIMS 的驗證於 GDPR 之遵循可以用已被主管 PIMS 驗證的「獨立監督機構」核准之行為準則替代。

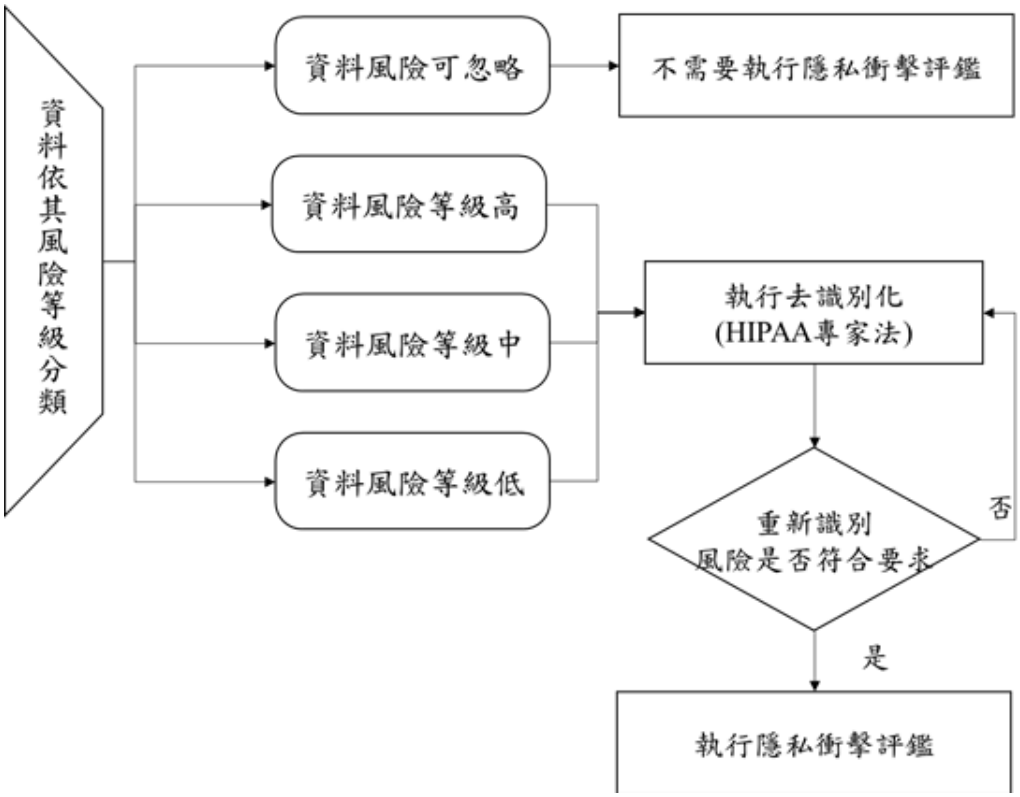


圖 2.6 HIPAA(Health Insurance Portability and Accountability) 風險評鑑流程圖

「他山之石，可以攻玉」，參照美國的 FISMA 實作計畫與歐盟 GDPR 之驗證規範，其以 ISO/IEC 27001 加 ISO/IEC 27009(ISO/IEC 27552) 作為 PIMS(含去識別化：於 ISO/IEC WD/CD/DIS/FDIS/IS 29151 均將資料去識別化納入其資料最小化的控制措施之中) 的「服務 (Services)」之要求事項，於「產品 (Products)」的安全功能則要求遵循 ISO/IEC 15408 標準系列；綜上所述，針對 PIMS 驗證標準之要求事項及其實作的標準化之工作項目，應是我國宜面對之議題。

參、雲端運算服務與個人資料管理之標準化初探

隨著雲端運算之日益普及，如何確保「雲服務客戶 (Cloud Service Customer，CSC)」的個人資料安全，已成為「雲服務提供者 (Cloud Service Provider，CSP)」與 CSC 必須共同面對之議題，亦為圖 2. 6 中各個應用範圍的基石；在另一方面，大數據分析已勢不可當，如何在其分析之過程中確保個人隱私已成為 PIMS 的新課題，表 3. 1 是雲服務標準化之此議題用語與資料去識別化標準化的對應；

以雲服務先行者之網飛 (Netflix) 公司為例，其 75 % 之影片瀏覽均來自「推薦服務 (Recommendation service)」;2013 年，網飛公司推出以政治權謀為主的第 1 部自製影片「紙牌屋」時，針對不同群組經由大數據分析設計了 7 種版本之預告片（INSIGHTS, 2014）; 如何探勘顧客的喜好予以分群 (例：同溫層 (Stratosphere)) 並產生推薦之剖繪 (Profile)，並且不侵犯隱私已成為「資料去識別化」求索的議題。2010 年 3 月 19 日，網飛公司即因推薦服務演算法競賽 (獎金 US$ 1, 000, 000) 事宜，因前述議題遭到 4 位顧客提告，以 US$ 9, 000, 000 和解。

表 3. 1 ISO/IEC 19944 與 ISO/IEC 20889 於資料去識別化用語之對應

ISO/IEC DIS 19944 資料識別限定符 (Qualifiers) 之資料狀態描述	隱私增強資料 (Privacy enhancing data) 之去識別技術，其應用產生的相對應狀態
識別資料 (Identified data)	包含識別符的原始、未處理的資料 ; 換句話說，即是還沒有應用去識別化技術 ; 對於其他限定符，識別符已被移除（遮蔽）。
擬匿名化資料 (Pseudonymized data)	使用具有可控制之重新識別的可能 / 實現之擬匿名化技術處理的資料。
不可連結之擬匿名化資料 (Unlinked pseudonymized data)	使用沒有可控制之重新識別的擬匿名化技術處理的資料。
不可連結之擬匿名化資料 (Unlinked pseudonymized data)	使用沒有可控制之重新識別的擬匿名化技術處理的資料。
聚集資料 (Aggregated data)	使用聚集 (Aggregation) 技術處理的數據。

資料來源：ISO/IEC CD 20889.2：2016-12-02, Information technology – Security technology – Privacy enhancing data de-identification techniques, Annex B

雲服務於 PIMS 之 CSC 與 CSP 的權責劃分如圖 3. 1 所示，其中 CSC 是資料控制者，CSP 是資料處理者，圖 2. 4 中的 ISO/IEC 29151 並未區分「PII 控制者之控制目的與控制措施」以及「PII 處理者之控制目的與控制措施」;2016 年 4 月，ISO/IEC JTC 1/SC 27 議決進行 ISO/IEC 27552 作為擴增 ISO/IEC 27001 之 PIMS 驗證要求事項的標準制定之工作項目。

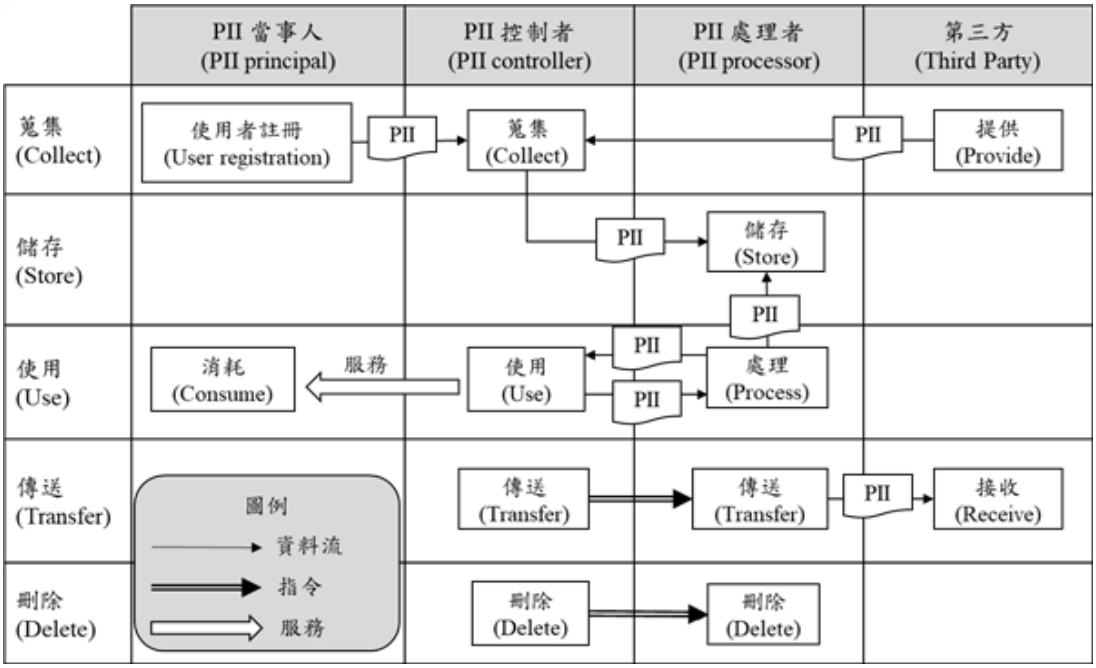


圖 3.1 PII 處理工作流程圖

說明：

1. PII：個人可識別資訊 (Personally identifiable information)
2. 資料來源：ISO/IEC 29134: 2017-06, Information technology – Security techniques – Privacy impact assessment – Methodology, p.41, Figure D.1(根據 ISO/IEC 29134：2017(E) 第 6.4.1 節) .

ISO/IEC JTC 1/SC 27 遵循 ISO/IEC 27009：2016- 06- 15，制定 ISO/IEC 27552，在 2017-12- 08 公布之 ISO/IEC CD 27552. 1，期於 PIMS 的實作，提供其驗證要求事項規範之準繩。舉例而言，於「資料去識別化 」的工作項目，在 ISO/IEC CD 27552. 1 之第 7. 4. 3~ 7. 4. 5 節：「 PII 控制者的 ISO/IEC 27002 之增加 」的 PIMS A. 4. 3~A. 4. 5 條款：「個人可識別資訊之資料去識別化 (PII data de-identification)」中闡明由 PII 控制者主責，其實作指引並敘明其技術在 ISO/IEC 20889 中描述；在「雲服務及其裝備：資料流、資料分類與資料利用 」的「透明性 (Transparency)」等，宜遵循 ISO/IEC 19944：2017- 08。在另一方面，在 ISO/IEC CD 27552. 1 之 PIMS A. 3. 7 條款：「蒐集或抹除 (Correction or erasure)」，已關聯至「雲服務層級框架協議 (Cloud Service Level(SLA) framework agreement)」的 ISO/IEC 19086-1：2016- 09- 21 第 10. 7. 2 與 10. 12. 8 節提出之如圖 3. 2 所示的「資料淨化 (Data sanitization)」中，「應用物理 (Physical) 或邏輯 (Logical) 之技術，確保標的資訊無法在實驗室之「發展中的科技之目前頂級能力 (State of the art)」中，致使其資料被「回復 (Recovery)」的「廢止 (Purge)」中之「抹除 (Erase)」的邏輯技術（ ISO, 2016b；R. Kissel et al, 2014），表 3. 2 是 ISO/IEC 27552 範疇合規之闡明，其中「抹除 」於 GDPR 的「被遺忘權 」之「實作 (控制措施)」係指圖 3. 2 中的「廢止 」之「密碼式抹除 」。

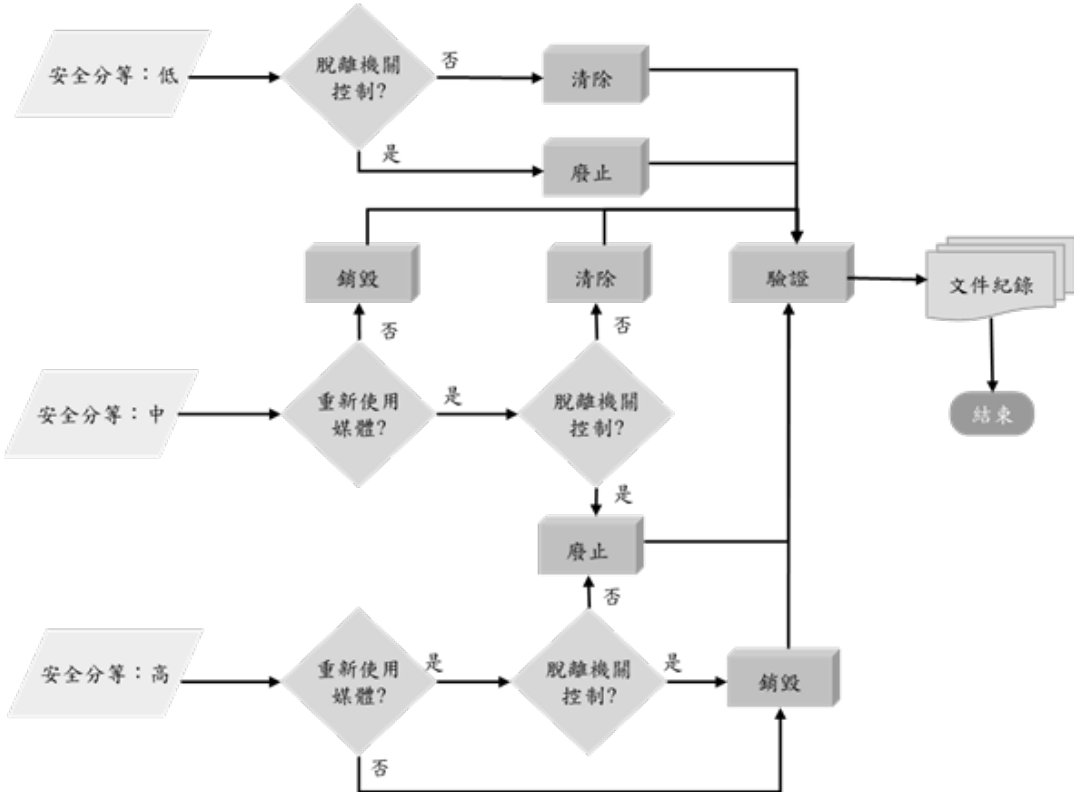


圖 3.2 資料清理 (Sanitization) 與處理 (Disposition) 決策流程

說明：

1. 清除 (Clear)：使用邏輯性技術 (Logical techniques) 來清理 (Sanitize) 所有用戶可定位 (User-addressable) 之儲存位置 (Storage locations) 的數據，以防止簡單的非侵入式 (Non-invasive) 資料恢復技術。
2. 廢止 (Purge)：使用最先進之實驗室的物理性 (Physical) 或邏輯性技術，使目標資料無法恢復。
3. 銷毀 (Destroy)：使用最先進的實驗室技術使目標資料無法恢復且使得後續無法使用該媒介 (Media) 儲存資料。

資料來源：Kissel, Richard, et al. NIST SP 800-88 Rev. 1. Guidelines for Media Sanitization, National Institute of Standards & Technology,Figure 4.1,Page 17, 2014-12.

表 3. 2 ISO / IEC 27552 之組織證據 (organizes evidence)

技術與組織之控制措施 (Technical & organizational measures)	● 去識別化 (De-identification)(ISO/IEC 20889) 與抹除 (Erasure)(ISO/IEC 27040) 以支持資料最小化 (Data minimization) ● 接收 (Receiving)、記錄 (Documenting) 和修改 (Modifying) 同意書 ● 支援資料主體之權利 (存取 (Access)、可攜帶 (Portability)、修正 (Correct) 及抹除 (Erase)) ● 資訊安全遵照 ISO/IEC 27001、ISO/IEC 27002 以及 ISO/IEC 29151
記錄保存 (Record keeping)	● 處理之目的 ● 處理之合法基礎 ● 對第三方單位之揭露 (Disclosure) 與傳輸 (Transfer) ● 地理位置 (Geolocation) ● 為了負責 (Accountability) 而保存紀錄

規範遵守之展示 (Demonstrate adherence)	● 處理者之義務遵照 ISO/IEC 27018 ● 資料主體之風險遵照隱私影響評鑑 (Privacy impact assessment)，即 ISO/IEC 29134，從設計著手及以預設機制進行保護資料 (Data protection by design and by default，PbD)(ISO/IEC 29101 以及 ISO/IEC 27550) ● 同意與告知 (Online)(ISO/IEC 29184)、資料可攜性 (ISO/IEC 19941)，自動決策以及剖析 (Profiling)（待定）
資料主體的透明性 (Transparency to data subjects)	● 資料主體之透明性遵照 ISO/IEC 19944 之資料使用之陳述 (Statements) ● 控制者、處理者之透明性遵照 ISO/IEC 19086

參考資料：Laura Lindsay, 2017, ISO/IEC JTC 1/ SC 27 Work in Support of Legislation, https://docbox.etsi.org/Workshop/2017/201706_SECURITYWEEK/01_STANDARDSandLEGISLATION/S01_SETTING_THE_SCENE/ISO_IECJTC1_SC27_LINDSAY.pdf

使用密碼學技術之「密碼式抹除 (Cryptographic erase)」亦可執行「清除」與邏輯性技術「廢止」的工作項目，並提供「金鑰回復 (Key recovery)」之選項，提供系統停機時自動保護資料的控制措施（ISO, 2016a）；以磁碟機為例，具備前述之整合「存取控制 (Access control)」的「密碼式抹除」之整體功能者名為「自加密磁碟機 (Self-Encrypting Drives, SED)」（R. Kissel et al, 2014），於「雲端運算服務水準協議」標準系列的 ISO/IEC 19086- 1:2016(E) 中之第 10. 12. 8. 1 條款敘明可以圖 3. 2 的「資料清理」過程代替「資料刪除 (Data deletion)」；換言之，於實作，SED 已是雲端運算供應者 (Cloud Service Provider, CSP)「資料刪除組件 (Data deletion component)」的元件 (Element) 之一（ISO, 2016b）；鑑於諸如離線磁碟機、暫存檔安全控制的攸關性，雲端運算服務將如圖 3. 2 所示的「事實標準 (De facto standard)」等擴增制定儲存安全之 ISO/IEC 27040，圖 3. 3 是「雲端運算服務」標準化的示意說明。

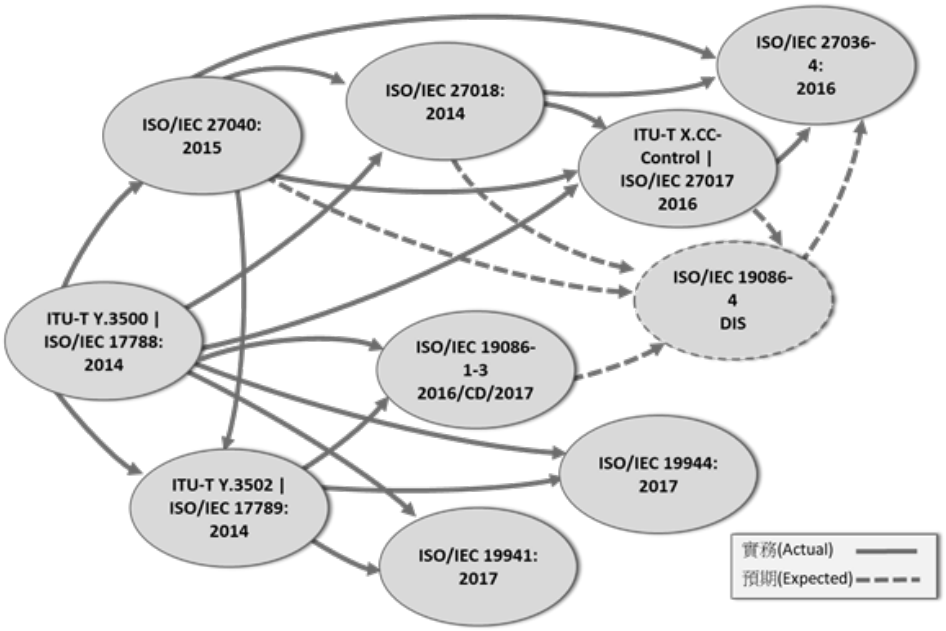


圖 3.3 雲端運算標準化 (Standardization of Y.3500 (e.g., ISO))

參考資料：NIST&ISO&ITU,2017-08-2

於美國，健康、金融等領域，如表 3. 3 所示，均以法規要求執行「資料清理 」工作項目以保護個人資料，並制定 US$ 10, 000~ 1, 000, 000 與「1% 之資產 (1% of assets)」等的未執行「資料清理 」之相關罰則。

表 3. 3　要求執行資料清理之美國相關法規列表

法規名稱
健康保險可攜與責任法 (Health Information Portability and Accountability Act , 簡稱 HIPAA)
個人資訊保護與電子文件法 (Personal Information Protection and Electronic Documents Act , 簡稱 PIPEDA)
格雷姆 - 里奇 - 比利雷法案 (Gramm-Leach-Bliley Act , 簡稱 GLBA)，亦稱金融服務現代化法案 (Financial services modernization act)
加州資料隱私法案 (California senate bill 1386)
沙賓法案 (SarBanes-oxley Act, 簡稱 SBA)
美國證券交易委員會 (United States Securities and Exchange Commission, 簡稱 SEC) 規定：第 17a 條 (SEC Rule 17a)

資料來源：Hughes, Gordon, and Tom Coughlin. "Tutorial on disk drive data sanitization." cmrr.ucsd.edu/people/Hughes/DataSanitizationTutorial.pdf (2006).

於「公開資料 」歐盟採用「匿名化 / 聚集化 」技術，非公開資料根基於「資料最小化原則 」採用「資料去識別化 」技術。「資料去識別化 」同表 3. 1 所示，ISO 尚在制定標準中（ ISO, 2018），表 3. 4 是 GDPR 於個人資料保護層級之框架，表 3. 5 是微軟公司 (Microsoft) 法務人員依據 ISO/IEC FDIS 20889 提出的去識化技術與大數據應用情境之框架，可作為其標準化法律遵循的參考；在另一方面，敘明資料去識別化與資訊公開之競合框架。

表 3. 4 GDPR 之層級

	已識別化 (Identified)	可識別化 (Identifiable)	Article 11 之去識別化 (De-identified)	匿名化 / 聚集化 Anonymous /aggregate
與識別資料 (identifying data) 直接連結 (Directly linked)	是	否	否	否
已知 (Known)、有系統性方法 (systematic way) 的 (重新) 識別 ((re) identify)	是	是	否	否
和特定對象 (specific person) 相關 (Relates)	是	是	是	否

說明：

1. GDPR article 11 規範不須識別時資料的處裡程序，其包含兩個部分：

a. 當個人資料無法 (再) 識別資料主體，PII 控制者不應再強制維持、取得、處理額外資訊以識別資料主體。

b. 當發生上述情形時，PII 控制者應有能力展示其資料無法識別該資料主體，(若可能) 並通知當事人。

2. 資料來源：Hintze, M. (2016). Viewing the GDPR Through a De-Identification Lens: A Tool for Clarification and Compliance.

表 3. 5 大數據應用情境及資料去識別化技術之隱私量測

	共享情境 (Sharing scenario) / 去識別化(De-identification) 技術(technique)	1 資料僅限於基元合法實體(Data is restricted to an atomic legal entity)	2 資料存取權僅限於合法實體(Access to data is provided within a legal entity)	3 資料公開僅限於合法實體(Data is published within a legal entity)	4 存取資料由服務層級協議或合約規範(Access to data is provided under SLA or contract)	5 公開資料由服務層級協議或合約規範(Data is published under SLA or contract)	6 資料提供公開存取(Public access is provided to data)	7 資料對一般大眾公布(Data is published to the general public)	8 由個體蒐集去識別化資料(De-identified data is collected from individuals)	9 由個體蒐集原始資料(Raw data is collected from individuals)
1	無	O	R	R	R	R	I	I	NA	FFS
2	可控制的重新識別之擬匿名化(Pseudonymization with controlled re-identification)	C	O	O	R	R	I	I	NA	FFS
3	擬匿名化(Pseudonymization)	C	O	O	R	R	I	I	FFS	FFS
4	遮罩識別符 (Masking of identifiers)	C	O	O	R	R	I	I	FFS	FFS
5	遮罩離群值與選擇的部分識別符 (Masking of outliers and selective quasi-identifiers)	C	O	O	R	R	I	I	FFS	FFS
6	泛化選擇的部分識別符(Generalization of selective quasi-identifiers)	C	O	O	R	R	I	I	FFS	FFS
7	隨機選擇的部分識別符(Randomization of selective quasi-identifiers)	C	O	O	R	R	I	I	FFS	FFS
8	針對部分識別符實作K匿名模型(Implementing K-anomymity model for quasi-identifiers)	C	O	O	O	O	R	R	NA	FFS
9	產生合成資料(Creating synthetic data)	C	C	C	O	O	R	R	NA	FFS
10	泛化彙集的資料/數據Generating aggregated data/statistics	C	C	C	O	O	R	R	NA	FFS
11	實做差分隱私伺服器模式(Implementing DP server model	C	C	C	O	O	O	O	NA	FFS
12	實做差分隱私局部模式(Implementing DP local model)	C	C	C	O	O	O	O	O	NA

C	O	R	I	FFS	NA
保守 (Conservative)	選擇性 (Optional)	有風險 (Risky)	不適宜 (Inappropriate)	待研究 (For future study)	不適用 (Not applicable)

註：論文中敘明表中所示的潛在風險水平僅僅是根據作者的知識和經驗來舉例 明不同利益關係者如何使用該框架的方法。

說明：DP 是「差分隱私 (differential privacy)」之縮寫，於資料集查詢過程中加入隨機「雜訊 (噪音)」以保證在數學上的「資料集之中的任一當事人 PII 之存在已被遮蔽」的 PII 去識別化方法 (ISO, 2017c)。

資料來源：Orit Levin and Javior Salido (2016)The Two Dimensions of Data Privacy Measures, page 3, Corporate External and Legal Affairs, Microsoft.

圖 3. 1 中，「PII 控制者」與「PII 處理者」之處理過程已與如圖 3. 4、表 3. 6 所示的「資訊與通訊技術 (Information and Communication Technology, ICT) 供應鏈風險管理 (Supply Chain Risk Management, SCRM)」相關；圖 3. 5 是 ICT SCRM 標準化

之產品 / 系統 / 服務的供給面之關聯示意及其角色的 明，於「 組件供應者 (Component suppliers)」， 圖 3. 6 是 前 述「 密 碼 式 抹除 」使用之「 密碼模組晶片 」已建立的驗證框架，表 3. 7 是其說明 (樊國楨、韓宜蓁，2015b）。

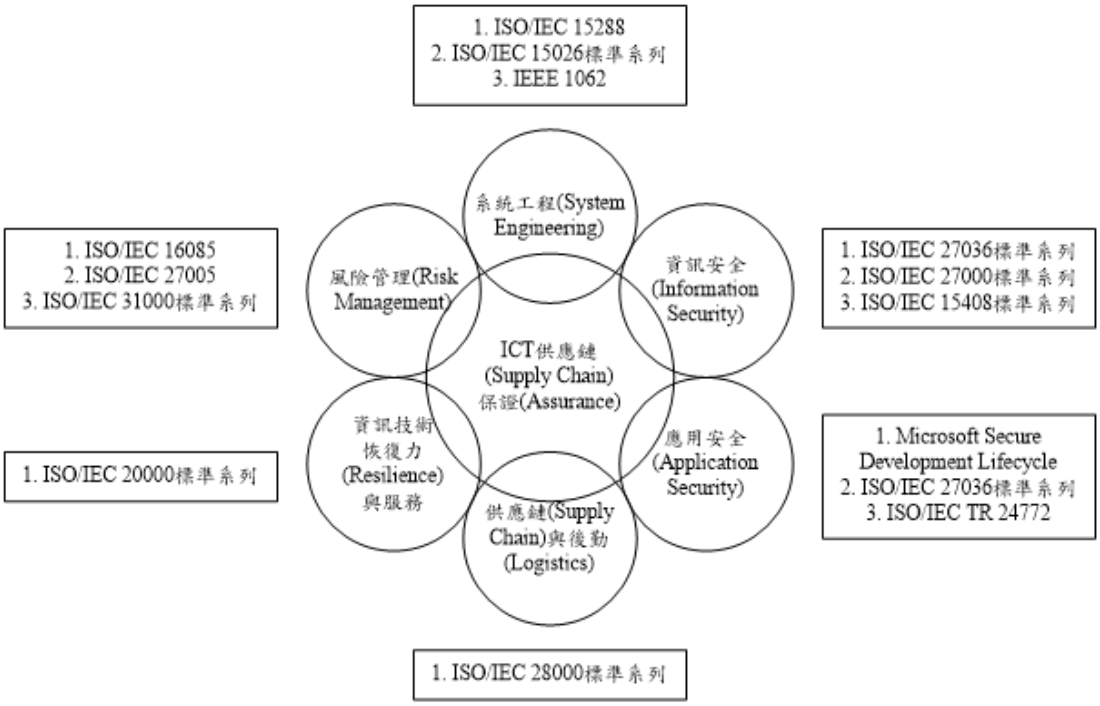


圖 3.4 資訊與通信技術 (Information and Communication Technology，簡稱 ICT) 供應鏈 (Supply chain) 風險管理 (Risk management) 要求規範之系列標準舉隅

資料來源：http://www.dhs.gov/ (2011-07-01) 與本研究

表 3. 6 ICT SCRM 系列標準 (ISO/IEC 27036: Information Technology - Security Techniques - Information security for supplier relationships) 表列

Part 1	Overview and concepts：2014- 04- 01。
Part 2	Requirements：2014- 08- 01。
Part 3	Guidelines for information and communication technology supply chain security：2013- 11- 15。
Part 4	Guidelines for security of cloud services：2016- 10- 01。

備考：計畫於 2011 年公布，2016 年完成。

PIMS 中執行抹除功能之 ICT 產品中諸如「 密碼模組晶片 」等是否存在弱點，「 PII 控制者 」及「 PII 處理者 」宜使用已建立 ICT SCRM 機制降低風險。

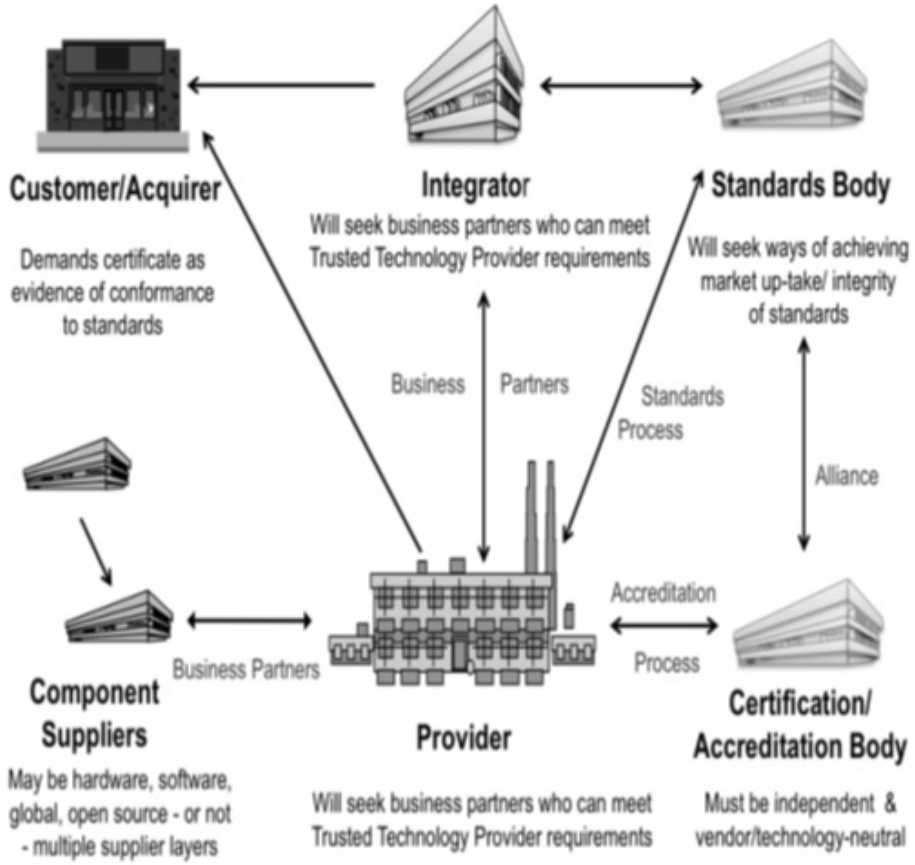


圖 3.5 ICT SCRM (Supply Chain Risk Management) 標準化之產品 / 系統 / 服務的供給面之關連 (ISO/IEC 27036-6) 示意

參考資料：The Open Group (2012) Open Trusted Technology Provider Standard (O-TTPS) – Mitigating Tainted and Counterfeit Products (Snapshot), Figure 1, Page 5, February 2012。

備考：O-TTPS 已於 2018-01 與 2018-02 成為 ISO/IEC 20243-2 及 ISO/IEC 20243-1 之國際標準，以「密碼模組晶片」為例，資訊系統的「整合者 (Integrator)」要求「供應者 (Provider)」使用使用經由遵循表 3.7 之「標準機構 (Standards body)」公布的 ISO/IEC 15408 標準系列等標準且其生產過程已通過「驗 / 認 (Certification/Accreditation) 機構 (Body)」之認證，「密碼模組晶片」亦通過圖 3.6 中「評估實驗室 (Evaluation laboratories)」的測試。

圖 3.6 ISCI WG 2012 Contributors

資料來源：Dr. Gutau, W. and J. Noller (2012) Minimum Site Security Requirements for the Smart Secure Device Supply Chain (Presentation), Sept. 2012, 13 ICCC, Paris.

表 3. 7「密碼模組晶片」之資訊與通信供應鏈驗證使用標準表列

1. ISCI: International Security Certification Initiative.
2. 遵循標準： 2. 1 資訊安全管理系統 (Information Security Management System，簡稱 ISMS)：ISO/IEC 27001。 2. 2 ISMS 之控制措施：53 項僅為資訊，大部分是強制性 (Mandatory) 要求事項。 2. 3 遵循 ISO/IEC 15408 標準系列之 Site certification。

參考資料：CCDB (2007) Site Certification, Version 1.0, Revision 1, CCDB-2007-11-001, October 2007。

綜前所述，於現階段，PIMS 之實作，除遵循 ISO/IEC 27001、ISO/IEC 27002、ISO/IEC 27005、ISO/IEC 27009、ISO/IEC 27018、ISO/IEC 29100、ISO/IEC 29134、ISO/IEC 29151 外，因已堪用且其控制措施優於 ISO/IEC 29151 宜再增列上 ISO/IEC CD 27552. 2；於雲端運算服務，則再增列雲端運算服務水準之 ISO/IEC 19086- 1、ISO/IEC 19086- 3 與 ISO/IEC 19944 以及 ISO/IEC 27017。

肆、個人資料管理系統標準化進程及議題於我國之借鏡：代結論

2015 年 7 月 17 日，面對「開放資料」與「大數據」之「去識別化」議題，前行政院張善政副院長根基於經濟部標準檢驗局 (Bureau of Standards, Metrology and Inspection，簡稱 BSMI) 提出如圖 4. 1 所示的方案規劃，公布如表 4. 1 所示之行政院推動大數據發展的個人資料保護之標準化工作項目。「CNS(ISO/IEC 29191) 29191 有要求事項，無控制措施；而 CNS(ISO/IEC 29100)

29100 是保護個人可識別資訊的高階框架，可引用作為『去識別化』控制措施」，是 BSMI 對其執行圖 4. 1 與表 4. 1 之思路的說明（行政院，2012；行政院，2015a；行政院，2015b；行政院，2016；法務部，2014；最高行政法院，2014；最高行政法院，2017；經濟部，2015；臺北高等行政法院，2016）。

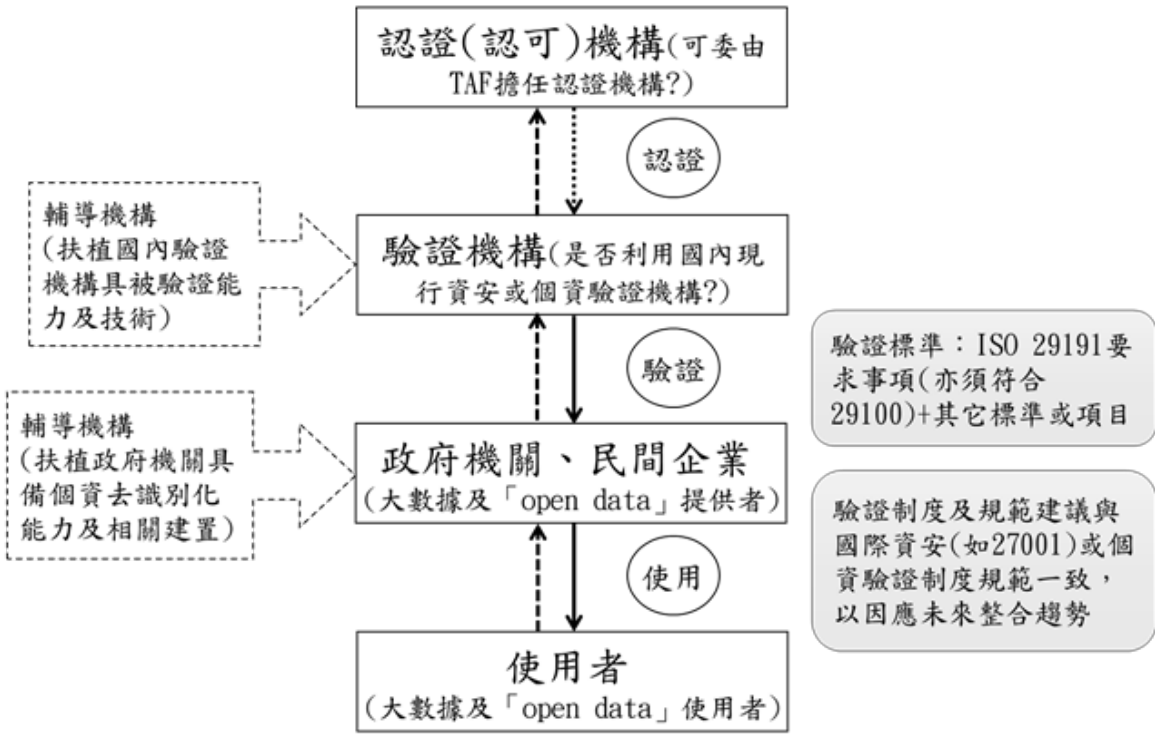


圖 4.1 個人資料去識別化方案規劃－個資去識別化驗證制度體系規劃

資料來源：個人資料去識別化之運作機制（簡報資料），經濟部，2015-07-14《研商因應大數據潮流個人資料去識別化可行機制》會議（前經濟部標準檢驗局許景行組長簡報）。

表 4. 1 行政院推動大數據之個人資料保護相關的 2 項國家標準

標準	CNS 29100：2014- 06- 04	有關如何管理、確保隱私權之原則框架的國家標準
	CNS 29191：2015- 06- 10	有關如何去識別化之部分匿名與部分去連結的國家標準
推動作法		● 政院月底將出爐如何取得符合兩標準的標準程序作法 ● 第一步先鼓勵部會取得驗證，下一步鼓勵金融、電信業取得驗證
用處		● 去除外界擔心敏感個資外洩疑慮 ● 各部會與業界可以合理應用大數據

資料來源：2015 年 7 月 17 日，大數據發展訂國家標準，經濟日報 A1，記者林安妮 / 台北報導。

因「個人資料去識別化」之「控制措施」宜參照「健康資訊資訊安全管理系統」驗證規範的 ISO 27799：2008- 07- 01 第 57 頁闡明其實作應遵循之 ISO/TS 25237：2008- 10- 01 內涵等觀點，於 2015 年 7 月 27 日「經濟部標準檢驗局」召開的「研議政府機關個人資料去識別化之適用標準」會議中，得出表 4. 1 的標準化框架先行加列其實作宜參考的已公布之 ISO/IEC 29101：2013- 10- 15 等標準的結論，如圖 4. 2 所示（經濟部，2015）。

圖 4.2 個人資料去識別化驗證標準規範

資料來源：http://vtaiwan.tw/personal-data-protection/「個人資料去識別化」驗證標準規範研訂及推廣，頁 12，《虛擬世界發展法規調適規劃方案》第 9 場會議，2016-02-23，簡報機關：經濟部標準檢驗局（檢索時間：2016-02-23）。

2015 年 9 月 17 日，法務部提出「我國個人資料保護法有關去識別化之標準」的法律意見書（行政院，2015），闡明「去識別化」於刑事、民事與行政責任之標準化實作的聯結性，提出遵循比例原則之風險管理及「開放資料 (Open data)」宜達「匿名化 (Anonymised) 資料 (Data)」與「不可逆 (Non-retraceable) 之擬匿名化 (Pseudonymised) 資料」的見解；經濟部標準檢驗局提出「個人資料去識別化過程驗證要求及控制措施」之驗證規範，經「行政院」函知相關機關 (構) （行政院，2015a；行政院，2015b）。

2015 年 12 月 21 日，「行政院國家資通安全會報第 29 次委員會議」，於會議紀錄中將「『個人資料匿名化、去識別化』分列」，同時要求相關機關善加推廣利用前述驗證規範（行政院資通安全辦公室，2016）。

圖 4. 1 中之 ISO/IEC 29100、ISO/IEC 29191 等標準與規範的用語並不一致，已如前述；其中 ISO/IEC 29191 僅為通稱「網路實名制」之「可控制的重新識別之擬匿名化」的管理控制措施之要求事項（ ISO, 2012）。

經過去識別化處理之資料將面對的重新識別攻擊之攻擊者可能來自各方，他們可能是為了展示自己的理論正確性或是想從資料中獲益。而成功之攻擊並不需要將資料庫完整重現才算成功的攻擊，攻擊者只要用各種方法取得相關去識別化資料，包含向資料庫提出詢問 (Query) 以及直接取得去識別化資料集，能夠在資料中分析出其目標即可以算是成功之攻擊。以目標分類的話，攻擊可以分為下列幾種：

1. 重新識別某筆紀錄是否在特定的資料主體中。
2. 重新識別特定資料主體中的特定紀錄。
3. 重新識別越多越好的紀錄與相對應

的資料主體。

4. 重新識別特定資料主體是否落在資料集中。

任何重新識別之攻擊一般而言都會組合多種技術，並搭配可使用的外部資訊作為分析資料庫內容之工具。儘管攻擊的目標多變，評估哪些重新識別技術可能會被使用於去識別化之資料庫仍是相當重要的，表 4. 2 是常用之重新識別的技術表列。

表 4. 2　重新識別 (Re-Identification) 技術舉隅

技術 (Techniques)	實作方法
單獨挑出 (Singling out)	透過觀察特定的特質，將單一資料或少數資料從資料主體 (Data principal) 分離。
連結 (Linking)	連接至少兩個以上在相關的資料主體中的紀錄，或是連接在不同資料集中的一組資料主體。
推斷 (Inference)	有不小的機率可以從某一組屬性 (Attribute) 推斷出另一組屬性。
不可分辨之分析 (Indistinguishability analysis)	針對特定資料，透過執行計算 (Computations) 或詢問以確定其是否存在於搜尋的資料主體中。

註：資料主體 (Data principal) 在此指的是單一主體 (個人、組織、設備、軟體程序、……) 其需要保護的敏感資料總稱。
參考資料：ISO/IEC 2nd CD 20889：2017-06-09 第 7 節。

前述「不可逆之擬匿名化」於我國已有使用其理論上的弱點之重新識別風險大於 1/ 30, 000 的實證情境與資安事故（ Blakley and Borosh, 1979; A. K. Lenstra et al, 2012; 周立平，2012; 樊國楨、蔡昀臻，2017a），且 GDPR 提出之新定義的擬匿名化亦不認定其為「開放資料」，前述的法律意見書宜修訂之。建議：

1. 參照 GDPR 之「擬匿名化」定義，重新定義我國「個人資料保護法有關去識別化之標準」中之「擬匿名化」。
2. 闡明重新定義之「擬匿名化」與供研究等使用的「去識別化」資料之關聯。
3. 敘明「重新識別風險評鑑」與「隱私風險評鑑」之過程。

綜前所述，PIMS 的「標準化」需要整合自然科學及社會科學之脈絡來解讀以及推理，才能融入文化與數位台灣混然為一體，參照 ISO/IEC FDIS 20889 徵求意見稿的思路，應先將「資料去識別化後之效用」與「差分隱私」納入前述「個人資料去識別化過程驗證要求及控制措施」的內容（中華人民共和國國家質量監督檢驗檢疫總局 / 中國國家標準化管理委員會，2017）；以及如圖 2. 4 與圖 2. 5 所示，進行擴增包含「資料去識別化」之「資訊安全管理系統的要求事項與控制措施之『個人資料管理系統』」的標準化之工作項目，並闡明「重新識別風險」與「隱私衝擊評鑑」之不同，不宜將前者作為後者的一項屬性，而僅實作隱私衝擊評鑑（ Brooks et al., 2017; Garfinkel, 2015; ISO, 2017a；ISO, 2017b；ISO, 2018; 行政院，2015; 樊國楨、蔡昀臻，2017b），並應遵循 GDPR 之意旨，將隱私工程的風險評鑑納入 (Garcia et al., 2015)。

2004 年 6 月 14 日，行政院院臺規字第 0930086121 號函頒之「行政院所屬各機關主管法案報院審查應注意事項」的第三點第 (四) 款規定：「法案衝擊影響層面及其範圍，包括成本、效益及對人權之影響等，應有完整之評估。」，以「個人資料去識別化過程驗證要求及控制措施」行政規則

的法制作業之過程與試辦機關的實作結果評估，其「法規影響評估 (Regulatory Impact Analysis，RIA)」作業宜精進之。

隨著「個人資料去識別化」等隱私防護議題實作之開展，僅確保資訊系統的機密性 (Confidentiality，C)、完整性 (Integrity，I) 與可用性 (Availability，A) 並不足以確保民眾的數位生活福祉；GDPR 第 4 條款第 (5) 項已提出「擬匿名 (Pseudonymisation)」之新定義：「意指個人資料經過處理後，在沒有提供其他額外資訊的情況下已無法將個人資料歸類於特定資料主體，且前述之額外資訊必須與個人資料分離、分別保管，並接受技術與組織的控制措施以確保該個人資料無法歸屬於已識別或可識別之自然人，即為例證；2014 年 12 月，歐盟已正式發布將 CIA 擴增如後之目標 (Goals)：

1. 去連結性 (Unlinkability)：隱私相關之資料不能跨資料庫彼此連結。
2. 透明性 (Transparency)：可以在任何時間理解與重建，包含法規、技術以及組織設置之所有隱私相關的資料處理。
3. 可調解性 (Intervenability)：對計畫與正在進行之隱私相關的資料處理，能進行合理的干預。

前述 CIA 定義之擴增目標，已納入於 2016 年 4 月成案的通稱為「從設計著手保護資料 (Data protection by design)」之「隱私工程 (Privacy engineering)」的 ISO/IEC 27550 標準化計畫之先期研究的內容之中（Garcia et al., 2015）；2013 年 10 月 15 日公布的「隱私架構框架 (Privacy architecture framework)」之 ISO/IEC 29101，通稱為「以預設機制進行資料保護 (Data protection by default)」的標準，附錄二是其實作之闡明；前述「隱私工程」與「隱私架構框架」均為通稱「從設計著手保護隱私 (Privacy-by-Design, PbD)」的標準，PbD 與「資料極小化 (Data minimization)」是個人資料防護實作之原則，PbD 已納入 GDPR（Official journal of the european union, 2016）；2017 年 1 月，美國亦公布同前述歐盟擴增 CIA 之「分離性 (Disassociability)」、「可預測性 (Predictability)」及「可管理性 (Manageability)」的 3 項目的 (objects) 之定義（Brooks et al., 2017；Garfinkel, 2015；OMB, 2016），亦已納入前述 ISO/IEC 27550。「他山之石，可以攻玉」，前述 PbD 等如圖 2. 6 所示的 PIMS 標準化之進程及其諸如 ISO/IEC 15408 標準系列的保護剖繪（樊國楨、蔡昀臻，2016a）之實作等相關的法制，宜關注之。

「標準可以累積知識與經驗，標準化則是冀求以系統的、共同的、協調一致的方法來強化標準實作之知識以供傳承。」15 年來，我國 ISMS 與 PIMS 的實作卻以通過驗證為標的，致使事倍功半，前述誤將「網路實名制」之「前檯匿名，後檯實名」的技術規範作為「PII 去識別化」的驗證標準即為例證。PIMS 標準化之研究與實施必須設法超越彷彿不證自明的 ISMS 之驗證與認證空間，使其成為資訊社會的基石；我國在 2000 年前後形成之 ISMS 驗證的空間，是不同利益之行動者追求商業利益將其「挪為己用」的「經營」之而形成的；以資安健診為例，行政院資通安全稽核作業計畫於 2013 年 9 月 2 日至 10 月 31 日，正式將取名「資安健診」之 ISMS 的技術控制措施之測試納入評分，開起我國 ISMS 稽核工作

的新姿，惟其範疇尚略小於「 PIMS 驗證機構認證規範 (ISO/IEC 27006:2011)」之「系統測試 」(例：ISO/IEC 27006:2011 將「路由器 (Router)」納入系統測試範疇，資安健診則無)，且目的事業主管機構財團法人全國認證基金會於 2007~ 2013 均將“Switches”譯為「開關 」，2014 年 2 月方更正為「交換器 」，一葉知秋，令人惆悵 (財團法人全國認證基金會，2007; 財團法人全國認證基金會，2016; 樊國楨、季祥、韓宜蓁，2015a)。「工欲善其事，必先利其器。」當美國與歐盟於系統測試外，更進一步將 ISO/IEC 15408 標準系列納入控制措施實作的此時；政府 (Government) 之對個人資料保護有監督管理權責的行政機關 (Administration) 之管理的當責 (Accountability) 實體，做為一個控制 PIMS 規範之集中式權力機構，其對 PIMS 驗證的觀點影響到 PIMS 標準化之進程；歐盟與美國的經由規範以及評鑑與測試 ISMS 及 PIMS「行為準則 」之遵循，及其經由法規制約 ISMS 與 PIMS 的標準化，是值得我們深入研究之議題 (樊國楨、季祥、蔡昀臻，2015a；樊國楨、蔡昀臻，2015b；樊國楨、蔡昀臻，2016a)，本文探討的內容應可作為 PIMS 標準化取徑之參考。

綜上所述，「借箸代籌 」，於「短程 (2018 年 ~ 2020 年)」宜要求「行政院 」建立我國 PIMS 之「行為準則 」的認可機制與如同圖 2. 1 之 PIMS 國家標準框架及其標準化計畫 ;「中程 (2020 年 ~ 2022 年)」，宜建立 PIMS 的圖 3. 5 與圖 3. 6 之評估以及測試規範及其評估與測試的能力 ;「長程 (2022 年 ~ 2024 年)」，建立 PIMS 之法制。

致謝詞：本文作者謹在此對 ISO/IEC JTC 1/SC 27/WG 1 之友人提供 ISO/IEC CD 20889. 2:2017- 06- 09、ISO/IEC CD 20889. 2:2017- 10- 23、ISO/IEC FDIS：2018- 06- 19、ISO/IEC PDTR 27550. 2:2018- 06- 04、ISO/IEC WD 27552. 2:2017- 06- 01、ISO/IEC WD 27552. 2:2017- 10- 17、ISO/IEC CD 27552. 1:2017- 12- 08 與 ISO/IEC CD 27552. 2:2018- 06- 04 的盛情，與審稿者提升內容水平之意見，致衷心的謝忱！

參考文獻

1. 中華人民共和國國家質量監督檢驗檢疫總局 / 中國國家標準化管理委員會，2017，信息安全技術　個人信息去標識化指南 (徵求意見稿)，2017- 08- 15。
2. 行政院，2012，< 個人資料保護法除第 6 條及第 54 條條紋外，其餘條文自 2012 年 10 月 1 日施行 >，行政院臺法字第 1010056845 號令。
3. 行政院，2015a，< 我國個人資料保護法有關去識別化之標準 >，院臺科字第 1040144764 號函 (附件 1)。
4. 行政院，2015b，< 個人資料去識別化過程驗證要求及控制措施 >，院臺科字第 1040144764 號函 (附件 2)。
5. 行政院，2016，< 個人資料保護法自 2016 年 3 月 15 日施行 >，行政院臺法字第 1050154280B 號函。
6. 行政院資通安全辦公室，2016，院臺護字第 1050150057 號函，2016- 01- 05。

7. 法務部，2014，法律字第 10303513040 號函。
8. 周立平，2012，Cryptoanalysis in Real Life (Presentation), 2012- 07- 21 P.M. 13: 00~ 13: 45, HITCON 2012(備考：周教授於 2012- 07- 21 簡報中提出之脆弱性為 - 若取得一定數量的公鑰資料，則 n 1=p 1xq&n 2=p 2xq → q=gcd(n 1，n 2)，謹此敘明)。
9. 最高行政法院，2014，103 年度判字第 600 號判決 (2014- 11- 13)。
10. 最高行政法院，2017，106 年度判字第 54 號判決 (2017- 01- 25)。
11. 經濟部，2015，經標授字第 10420050540 號函。
12. 臺北高等行政法院，2016，103 年度訴更一字第 120 號判決 (2016- 05- 19)。
13. 財團法人全國認證基金會，2007，ISO/IEC 27006：2007「資訊安全管理 - 安全技術 - 資訊安全管理系統稽核及驗證機構之規定 」(訓練教材 ：2017- 07- 27)。
14. 財團法人全國認證基金會，2016，資訊安全管理系統驗證機構認證規範 (ISO/IEC 27006：2015)，TAF-CBA-ICC-01/ISSUE 5/ 2016. 02。
15. 樊國楨、季祥、韓宜蓁，2015a，資訊安全管理系統稽核初論：根基於資安健診與標準化，資訊安全通訊，第 21 卷，第 1 期，頁 33~ 63。
16. 樊國楨、韓宜蓁，2015b，數位社會供應鏈風險管理的標準化 (ISO/IEC 27036 系列標準) 歷程初探，標準與檢驗，第 190 期，頁 65~ 74。
17. 樊國楨、蔡昀臻，2016a，隱私防護資料發布系統之保護剖繪初論：根基於個人資料去識別化的議題，前瞻科技與管理，第 6 卷，第 1 期，頁 47~ 114。
18. 蔡昀臻、樊國楨，2016b，大數據之資料去識別的標準化初探：根基於 ISO/IEC 2nd WD 20889：2016- 05- 30，資訊安全通訊，第 22 卷，第 4 期，頁 1~ 26。
19. 樊國楨、蔡昀臻，2017a，擬匿名化的大數據之安全標準初探：根基於支付卡的安全事故與公開基礎建設之技術脆弱性的議題，資訊安全通訊，第 23 卷，第 2 期，頁 24~ 42。
20. 樊國楨、蔡昀臻，2017b，大數據之資料去識別標準化的進程初論：根基於 ISO/IEC CD 20889. 2：2017- 10- 23，前瞻科技與管理，第 7 卷，第 2 期，頁 55~ 74。
21. Blakley, G.R. and Borosh, I., 1979, RSA Public Key Cryptosystems do not always conceal messages, Computers and Mathematics with Applications, Vol. 5, No. 3, pp. 169~ 178.
22. Brooks, S., Garca, M., Lefkovita, N., Lightman, S. and Nadeau, E., January 2017, Privacy Risk Management for Federal Information Systems, NISTIR 8062.
23. ENISA(European Union Agency for Network and Information Security), 2014, Privacy and Data Protection by Design-from policy to engineering, December 2014.
24. European Privacy Seal(EuroPriSe), 2017, EuroPriSe Criteria for the certification of IT products and IT-based services(“GDPR ready” version-January 2017).
25. Garcia, A.C. et al., 2015, Privacy-

and Security-by-Design Methodology Handbook(PRIPARE), TRiALOG, 31 December 2015.

26. Garfinkel, S. L., October 2015, De-Identification of Personal Information, NIST IR 8053.

27. INSIGHTS, 2014- 03, http://www.wired.com/insights/ 2014/ 03/big-data-lessons-netflix/(2017- 03- 09 檢索)。

28. ISO, 2012, ISO/IEC 29191: 2012- 12- 15, Information technology-Security techniques-Requirements for partially anonymous, partially unlinkable authentication.

29. ISO, 2016a, ISO/IEC JTC 1/SC 27/WG 1 N 715: 2016- 10- 26, Draft design specitification for revision of ISO/IEC 27005.

30. ISO, 2016b, ISO/IEC 19086- 1：2016- 09, Information technology – Cloud computing – Service level agreement(SLA) – Part 1：Overview and concepts.

31. ISO, 2016c, ISO/IEC JTC 1/SC 27/WG 1 N 711: 2016- 12- 08, Report of the meeting on N 615 (Defect Report on ISO/IEC 27005: 2011) held in Abu Dhabi Oct 2016.

32. ISO, 2017a, ISO/IEC CD 27552. 1：2017- 12- 08, Information technology – Security techniques – Enhancement to ISO/IEC 27001 for privacy management – Requirements.

33. ISO, 2017b, Disposition of comments report on document SC 27/WG 5 N 16908(WG 5 N 608) – ISO/IEC CD 20889：2017- 06- 09.

34. ISO, 2018, ISO/IEC FDIS 20889：2018- 06- 19, Information technology – Security technology – Privacy enhancing data de-identification techniques.

35. Kissel, R. et al., 2014, Guidelines for Media Sanitization, NIST SP 800- 88 Revision 1.

36. Lenstra, A. K. et al., 2012, Ron was wrong, Whit is right, ePrint(2012- 064), http://eprint.iacr.org/ 2012/ 064.pdf/(2017- 01- 31 檢索)

37. Official Journal of the European Union, 2016, General Data Protection Regulation (GDPR), REGULATION (EU) 2016/ 679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016.

38. OMB, 2016, Annual Report to Congress：Federal Information Security Modernization Act, March 18, 2016.

附錄一：隱私保護原則與其對應之資訊安全控制項目

隱私保護原則	資訊安全控制項目
同意與自主	PII 當事人宜受限於機密性規則，因為該規則依據組織內的角色與職責之受到同意。PII 控制者宜決定與實作其之最合理及適切，對個別隱私要求最少干擾的安全量測。舉例而言，適當時，可使用授權以協助確保提供同意之個人實際上是其宣稱的該個人。
目的合法與規格	實作適宜之存取控制措施以確保僅授權於 PII 的處理，確認 PII 資產之職責與管理的規範之個體，以及確認根基於隱私權的支持良好隱私管理之資訊技術 (Information Technology, IT) 系統的發展。
蒐集限制	降低風險的一般方法為減少需要保護的機密資訊與重要資產之數量。 限制 PII 資訊之蒐集到需要支援整體資訊安全目標的絕對極小值。
資料極小化	由於安全標準通常要求監視所有活動、日誌檔案，追蹤可能包含 PII 的系統與其它文件；因此可能與隱私衝突。建議施行資料分類程序以達到 PII 分開處理與 PII 極小化策略。亦建議使用虛擬假名與匿名。
利用、保留與揭露限制	除此之外，可藉由適當使用機密性協議、分類與存取控制來限制揭露予以控管。廣泛地保留資料從安全立場而言是可取的，但亦可能對隱私造成威脅。
精確與品質	由於資料之精確與品質在各方面均為基礎，多數組織內應已實作合理與適切之控制措施。該等控制措施可不用大幅修改而應用於 PII，並同時有助於控制 PII。
公開、透通性與通知	達成上述目標需要高等級之安全，因為涉及使資訊僅對 PII 當事人為可存取的。 合理與適切的控制措施與在交換與透露資訊時適用之安全方法亦可適用以達成上述目標。
個人參與與存取	存取控制規則宜存在於每個組織。PII 提供者亦可對各要求適用授權政策。現有之控制措施可延伸至包括上述要求而不需複雜改變。
可歸責性	在任一安全框架中特定角色與職責的指派扮演不可或缺之部份。 隱私相關的政策與程序之可歸責性宜視為一項指派，且藉由現有控制措施的方式予以實現。
資訊安全控制措施	如 ISO 27002 之現有安全標準對安全控制措施提供詳盡之建議，為確保資料安全宜明確地實作。尤其宜實作下列安全控制措施：(下列清單非窮盡列舉) ・ 對未經授權人員宜禁止存取資料處理設施 ・ 未經授權人員不宜被允許存取電腦系統 ・ 授權人員遺僅可在其存取權限範圍內存取 PII ・ PII 之實體與電子運送或傳輸宜合理與適切地保持安全以免未經授權的存取 ・ 宜保有日誌以記錄 PII 的任何存取與修改，特別是敏感 PII ・ 宜保持 PII 安全以免意外或未經授權的揭露、修改、喪失、移除或破壞 ・ 不同目的規格之 PII 宜分開處理 ・ 宜有適當的隱私危害管理程序
(隱私) 遵循	遵循如 ISO 27002: 2005(E) 之安全標準提供保護 PII 的安全控制要求項目之遵循，是執行隱私政策的前提。

資料來源：ISO/ IEC 29101: 2013-10-15, Table D, pp.45-46.

附錄二：個人資料保護目標 (Goals) 與 ISMS 相關之資訊安全與意見連結表

隱私層面 (aspects)	個人資料保護層面連結特徵	連接到資訊安全	關於資訊安全管理系統 (Information Security Management System, ISMS) 實作的意見
去連結性 (Unlinkability)	資料極小化 (Data minimization) 相關控制措施：ISO/IEC 27001 第 .4 節、附錄一第 A. 3/A. 4/A. 5 節、附錄二第 B. 3/B. 4/B. 5 節	這不算資訊安全層面的一部分	這個特徵與組織的業務目的與使用個人資料之原因密切相關。 使用資料極小化可以降低風險，從而成為降低資訊安全的需求之一般方法，即使它不是資訊安全的一部分。
去連結性 (Unlinkability)	知的必要 / 僅知原則 (Necessity / Need-to- know) 相關控制措施：ISO/IEC 27002 第 8. 2. 1/ 8. 2. 2/ 8. 2. 3/ 9/ 18. 2. 2 節	知的需要之概念經常用於資訊安全。 通常被認為是機密性 (Confidentiality) 的特徵。	關於個人資料保護層面它之意義更廣泛。 它同時指的是使用 / 提供服務之資料是完全必要的，以及為了執行該服務或任務而需要存取之人、事資訊的假定限制。
去連結性 (Unlinkability)	目的綁定 (Purpose binding) 相關控制措施：ISO/IEC 27002 第 18. 1. 1/ 18. 1. 4 節、附錄一第 A. 4 節、附錄二第 B. 4 節	這是存取控制和 / 或使用控制的擴充。	這個特徵指的是在理想情況下，除了收集的目的之外，無法處理資料。 然而，這是很難實施的，因為通常需要技術和組織措施才能得到維護。
去連結性 (Unlinkability)	權力分隔 (Separation of power) 相關控制措施：ISO/IEC 27002 第 6. 1. 1/ 6. 1. 2/ 8. 1. 2/ 9. 2. 3 節	角色和責任包括 (資訊) 資產之所有權。	所有資訊安全的責任應被定義與分配。 應分開職責及利益衝突之責任範圍，以減少未經授權或無意的修改或濫用組織資產之機會。清單中的資產應有特定之所有者。
去連結性 (Unlinkability)	可觀測性 (Observability) 相關控制措施：ISO/IEC 27002 第 18. 2. 3 節、附錄一第 A. 4. 4/A. 10. 1/A. 10. 4 節、附錄二第 B. 4/B 10. 2 節	在某種意義上，這是一個機密性的問題，但指的是所進行的活動而不是實際的資訊。	根據共同準則 (Common Criteria, CC) 第 2 部 3. 1 版之第 4 次修訂 (CC PART 2 V 3. 1R 4)，不可觀測性 (un-observability) 能確保使用者在沒有其他人 (特別是第三方) 能夠觀察到用戶正在使用資源或服務的情況下使用資源或服務。 在 ISMS 中，這應該被視為是為了減輕或減少與個人資料有關的風險而應考慮之一個層面，以及避免在不需要時創建個人資料的一種方法。
去連結性 (Unlinkability)	不可偵測性 (Undetectability) 相關控制措施：附錄一第 A. 4/A. 7. 1、附錄二第 B. 4/ B. 10. 2/B. 10. 6 節	這是事物存在之機密性的部分層面。 一妥善保護的資產應對未經授權的實體具有不可偵測性。	根據“ANON”v 034 版，不可偵測性定義如下：從攻擊者之角度來看，利益項目 (item of interest, IoI) 的不可偵測性意味著攻擊者無法充分判斷它是否存在。在 ISMS 中，這應該被視為是為了減輕或減少與個人資料有關之風險而應考慮的一個層面，以及避免在不需要時創建個人資料之一種方法。

透明性 (Transparency)	開放性 (Openness) 相關控制措施：ISO/IEC 27002 第 8. 2. 1 節、附錄一第 A 5. 1/ A. 8. 1/A. 8. 3/A. 8. 4/A. 8. 5/A. 10 節、附錄二第 B. 1/B. 10 節	開放性是資料主體和 / 或監督機構盡可能的要求文件、行動和活動開放且可理解的原則（另見政府開放性)。 這不是直接的資訊安全層面，而是間接影響 CIA 對公司相關資訊的要求。	在 ISMS 中，服務或處理之生命週期都應該被視為系統所有層面之要求。 它將影響必要的資訊安全控制措施以及將程序性活動 / 控制（如分類)之一部分的風險及需求納入考量。
透明性 (Transparency)	可歸責性 (Accountability) 相關控制措施： ISO/IEC 27002 第 6. 1. 1/ 8. 1. 2 節、附錄一第 A. 10/A. 11 節、附錄二第 B. 10/B. 11 節	可歸責性與資訊安全層面無關。 在與透明性相關聯的方面，透明性是可歸責性特徵的先決條件。	這是在 ISM 內的組織。 與角色、責任與有關當局相關 (如 : 資產所有權、治理、風險評鑑、供應商關係、監測、審計)。
透明性 (Transparency)	可重製性 (Reproducibility) 相關控制措施：ISO/IEC 27002 第 14. 1. 3 節、附錄一第 A. 8. 3/ A. 8. 4/A. 8. 5/A. 10 節、附錄二第 B. 10 節	這不是資訊安全的直接層面。 這個特徵是指重現資訊的處理方式以及其處理者的可能性。	在 ISMS 中，這將影響記錄流程、服務及系統之要求以及所需的可追溯性 (traceability) 與監控級別。 這很可能也會影響事件與其管理過程。 如果適當實行，這也可能協助處理需要描述與重新創建流程之商業連續性計畫。
透明性 (Transparency)	通知與選擇 (Notice and Choice) 相關控制措施：ISO/IEC 27002 第 15. 1. 2 節、附錄一第 A. 1/A. 7 節、附錄二第 B. 1/B. 7 節	資訊安全沒有類似的層面。 通知通常指的是向資料主體提供關於正在收集個人資料以及如何使用和處理數據之行為，因此是透明性的一部分。 另一方面，選擇是指資料主體限製或同意收集和 / 或使用個人資料的能力。這就是調解性 (Intervenability) 特徵。	在 ISMS 中，服務或處理之生命週期都應該被視為系統所有層面的要求措施。 它將影響必要之資訊安全控制措施以及將程序性活動 / 控制（如分類)的一部分的風險及需求納入考量。
透明性 (Transparency)	可審計性 (Auditability) 相關控制措施：ISO/IEC 27002 第 18. 2 節、附錄一第 A. 2/ A. 9. 1/A. 9. 2/A. 9. 3 節、附錄二第 B. 2/B. 9. 1/B. 9. 2/B. 9. 3 節	可審計性與與安全層面無直接關係，但對完整性 (integrity) 和可用性 (availability) 的依賴性很強。在與透明性相關聯的方面，透明性是可審計性特徵的先決條件。	在 ISMS 之概念中有控制等應具有可審計性之類似的基本要求。 然而，在 ISMS 案例中著重於審計與 ISMS 或標準相一致之可能性；而在隱私案例中，核心重點為符合 GDPR 及同意處理個人資訊。 這兩方面對於可審計性的需要可能有不同之要求。
可調解性 (Intervenability)	自主決定性 (Self-determination) 相關控制措施：ISO/IEC 27002 第 7. 1/ 7. 2/ 7. 3/ 15. 1. 2 節	自主決定性可以與資訊安全的完整性 (Integrity) 和機密性 (Confidentiality) 層面有關。 該面向涵蓋資料主體能夠決定其願意發布的資料的條件和用途的權利或能力。 它還藉由設計和資料極小化與隱私相關。	在 ISMS 中，服務或處理之生命週期都應該被視為系統所有層面的特定要求措施。 它將影響必要之資訊安全控制措施以及將程序性活動 / 控制（如分類)的一部分的風險和需求納入考量。
可調解性 (Intervenability)	使用者控制 (User control) 相關控制措施：ISO/IEC 27002 第 9. 1/ 9. 2/ 9. 3/ 9. 4 節	在隱私方面，這是指資料主體通過例如配置、流量管制或其他方式來控制個人資料使用的能力。它還藉由設計和資料極小化與隱私相關。	在 ISMS 中，這應被視為主要是為了設計、開發與取得流程及系統之要求以及風險來處理。 這種風險考量將影響必要的資訊安全控制措施以及將程序性活動 / 控制（如分類)的一部分的風險和需求納入考量。

可調解性 (Intervenability)	修正和抹除資料 (Rectification and erasure of data) 相關控制措施：ISO/IEC 27001 第 7. 5 節、ISO/IEC 27002 第 8. 1. 2/ 8. 1. 4/ 11. 2. 7 節、附錄一第 A. 4 . 4/A. 9. 1/A. 8. 4/A. 10. 9 節、附錄二第 B. 4. 1/B. 10. 7 節	這與完整性和可追溯性有關。 但也是正確性 (correctness) 的概念。 實際上，它要求資料主體有權修正資料，並可能有權刪除其資料。	在 ISMS 中，應將其作為系統與服務之設計、開發及取得的要求措施以及技術與組織處理過程實施之要求措施來處理。
可調解性 (Intervenability)	同意撤回 (Consent withdrawal) 相關控制措施：ISO/IEC 27002 第 7. 3. 1 節、附錄一第 A. 1/A. 9. 1/A. 9. 2 節、附錄二第 B. 1/B. 9. 3 節	這與資訊安全層面沒有直接關係。 然而，同意撤回可能是設定完整性和可用性要求的前置作業。 它還將對可追溯性甚至機密性產生影響，具體取決於所涵蓋的個人資料。	在 ISMS 中，應將此處理視為不可忽視之處理要求措施與與對商業模式的風險並透過其影響必要控制措施及將程序性活動 / 控制（如分類）之一部分的風險及需求納入考量。
可調解性 (Intervenability)	申索 / 損害控管 (Claim lodging / Dispute raising) 相關控制措施：ISO/IEC 27002 第 16 節	這不是資訊安全層面。 然而，為了記錄事件發展，需要可追蹤性。	這是一個可能需要資訊安全管理之控制措施來處理風險的正式程序性活動。
可調解性 (Intervenability)	中斷處理 (Process Interruption) 相關控制措施：ISO/IEC 27002 第 16 節	停止或更改進程的能力能允許更改資訊，可被視為資訊安全的完整性和可用性層面。 但這算是資訊的需求而非保護。	這是一個可能需要資訊安全控制措施來處理風險及可能的事件之正式程序性活動。 所需的控制措施需遵循與 GDPR 相關之 ISMS 的要求事項將影響技術與組織控制措施。

資料來源：Veriscan Security AB, Information Security Management System (ISMS) and Handling of Personal Data Version 1.0.0.1, annex C, 2017-01-28.

明（樊國楨、蔡昀臻，2016a)：

1. CC Part2 V3.1R4 是「“Common Criteria for Information Technology Security Evaluation”3.1 版第 2 部分 (Part 2) 之第 4 次修訂 (Revision)，2017-04 已發行第 5 次修訂版；於 ISO，CC 即為 ISO/IEC 15408 Part 1(Introduction)、Part 2(Security functional components) 與 Part 3(Security assurance components)。
2. “ANON” v034 是 “ Terminology for Talking about Privacy by Data Minimization: Anonymity, Unlinkability, Unobservability, Pseudonymity, and Identity Management,” by A. ANON_Terminology_V0.34(2010-08-10)。
3. 表中之相關控制措施係作者自行加入。

大數據環境下政府審計之查核風險
Government Aduit Risk in the Big Data Environment

黃劭彥
國立中正大學會計與資訊科技學系教授

陳俊志
國立中正大學會計與資訊科技學系研究所博士生

高懿柏
審計部臺灣省花蓮縣審計室審計員

摘　要

本文探討大數據環境下，政府財務資訊的改變，如何對我國審計機關之查核風險產生影響，及如何因應其變動。最後，就結論研提適當之建議，以降低審計機關可承受之查核風險。

關鍵詞：查核風險、大數據

Abstract

This paper explores how changes in government financial information can affect the audit risk of National Audit Office in the context of big data and how to respond to changes. Finally, from the conclusions to make appropriate recommendations to reduce the audit risk that auditors can afford.

Keywords：Audit risk, Big data

壹、政府財務資訊與審計之變革

行政院自 1998 年起開始推動電子化政府，期透過政府網路基礎建設、資訊服務系統整合等，提供優質政府服務，以提升國家競爭力，而各機關歲計會計相關作業，也從傳統人工帳務處理模式，逐步邁向電腦資訊帳務處理模式。審計機關為以更經濟、有效之方式監督政府財務收支，基於風險導向審計考量，運用各機關電腦資訊系統收支資料辦理查核，已成為日後政府審計實務之重心；另參酌先進國家之政府審計實務，已逐漸朝向更為關注政府效能之績效審計發展，乃於 2015 年 6 月 17 日修正審計法第 36 條，刪除「連同原始憑證」等之文字，增訂「…編製會計報告連同相關資訊檔案，依限送該管審計機關審核；審計機關並得通知其檢送原始憑證或有關資料。」，以簡化行政程序及增進審計資源之有效配置，使得原始憑證隨會計報告按月送審制度走入歷史。

麥肯錫公司於 2011 年發布《Big data：創新、競爭和生產力的下一個新領域》報告，宣布「Big data 時代」來臨，並拜科學普及之傳遞，使得大數據 (Big data) 漸受關注。從審計證據之觀點，資料的來源大致可分為內部與外部，資料內容可分為財務與非財務資料，資料格式可分為結構化與非結構化資料，這種不同的屬性，在不同組合下，所產生的審計證據將呈現多樣可變性。大數據環境中，資料蒐集的流通管道擴張，資訊系統運算、儲存能力大幅提升，採用原審計抽樣技術的方式，查核證據之蒐集仍不足，顯示著全面性查核的世代已來臨。

各機關歲計會計相關作業已由傳統人工帳務處理，邁向電腦資訊帳務處理模式，參據審計實務指引第 2 號「風險評估與內部控制 - 電腦資訊系統特點與考量」公報，電腦資訊系統存在無可避免之風險，使得審計機關依該等資訊予以查核，其足夠性與攸關性可能受到衝擊或影響。

貳、大數據下對查核風險之影響

美國會計準則委員會 (AICPA) 於 1983 年發布的第 47 號審計準則將查核風險公式定義為固有風險 (Inherent risk) 、控制風險 (Control risk) 及偵知風險 (Detection risk) 之乘積。這個審計模型涵蓋可能發生風險的因素，互相的數字關係，具有廣泛的適用性與可操作性，因此國際上大多數的會計事務所與審計組織均用來評估並衡量查核風險。惟 2003 年國際審計準則 ISA 200 提出了全新的觀念，將審計風險模型修正為重大不實表達風險 (Material misstatement risk) 與偵知風險 (DR) 之乘積，其中將固有風險和控制風險合併為重大不實表達風險。

將傳統審計風險模型中的固有風險與控制風險合併，係因在傳統模型中各風險要素被獨立分隔，但是實務上風險要素很難被獨立評估，例如：固有風險與內部控制環境息息相關，特別是會計資訊系統，因此固有風險會與控制風險有所關聯；實務上，各風險要素難以量化，沒辦法用精確的數字評估，如將可接受查核風險設定在 5%，在實務上又是難以想像的高風險，這意味著每提出 20 份意見就有一個是錯誤的，這些看似量化的數字卻充滿了很多主觀之判斷。

隨著組織規模的擴展、交易日漸複雜、數據資料的多樣化，及重大不實表達風險之提升，當審計人員無法透過有效的程序

以控制重大不實表達風險，因此須額外執行查核程序將偵知風險降至更低，才能將查核風險維持在可接受之水準。若在重大不實表達風險上升的情況下，審計人員仍然維持與過去相同的偵知風險，則查核風險將上升至比過去更高的水準。

進入大數據時代，審計人員蒐集證據的模式也隨著改變，以前強調證據間的因果關係，而今日則著重資料間的內在關聯與相互關係，大數據技術會提供審計人員更高的相關性與品質之財務資訊，審計人員所需執行審計的範圍不斷地擴大，逐漸實現以數據分析作為審計模型之基礎，並運用大數據分析的支持，發現以前傳統審計方法中無法發現的風險以提高查核工作的品質。審計人員運用大數據技術可以妥善使用他們的專業知識，針對風險值較高的科目進行重點分析，進而提升審計效率，以降低查核風險。傳統審計的方法主要是採用查帳、與現場核對實物以及調取相關資料佐證等手段，需要較長的時間來完成審計工作。

然而，降低偵知風險也意味著需要投入更多的時間與人力成本，查核效率的低落導致需要更多的時間來蒐集查核證據；再者，偵知風險也不可能無限制的降低，因此大數據技術在執行審計程序方面扮演一個突破性的角色，審計人員在使用大數據技術輔助查核時，可以在相同的時間內得到質量更高的查核證據，也可以改正錯誤的審計方向。如此，不但可以有效的增加查核效率、效果與蒐集審計證據的質量，還能降低偵知風險，進而再投入相同的時間與人力成本來降低查核風險。

參、政府財務資訊大數據之審核分析

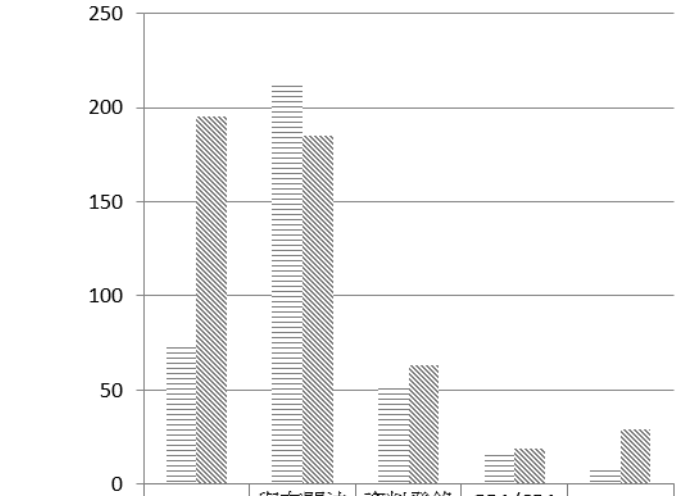
我國審計機關早於審計法於 2015 年 6 月 17 日修正前，已著手開發政府大數據審計輔助查核技術，又稱「歲計會計資訊審核分析系統 (下稱審核分析系統)」，並於 2016 年正式由各機關傳送財務資訊檔案，截至 2017 年設有 20 項查核控制點。從我國審計機關訂定各機關傳送相關資訊檔案內涵，其資料屬性係屬結構化之財務資訊，在憑證送審制度改變下，審計人員因無法立刻取據所需原始憑證資料，似乎僅能先透過結構化之財務資訊，瞭解受查單位及其環境，並透過這些資訊，辨識與評估重大不實表達風險，可能無法明確地瞭解各流程管控之過程。再參照審計法的設計，審計人員原則上係可無限制地取得查核所需的各項資料，然而當憑證送審制度走入歷史後，審計證據的範圍與品質，可能取決於與受查單位之互動關係。現行審計人員僅能透過微薄的結構化之財務資訊，經過大量的時間判斷所獲取資訊的真實性，經查各項法令規章，尚無任何規範著墨於各機關所傳送相關資訊檔案的範圍與品質，雖刑法第 213 條規範，公務員明知為不實之事項，而登載於職務上所掌之公文書，但其構成要件首重係出於公務員故意，然實務上不難發現，多數係因公務員過失所致，突顯出審計機關所取得的財務資訊，某種程度是受各受查單位所牽制。

隨行政院主計總處建置的政府歲計會計資訊處理系統 (GBA)，明確地顯示政府歲計會計資訊化的時代來臨，且隨憑證送審制度的變革，勢必參採財團法人會計研究發展基金會所訂頒之審計準則公報，強化對資訊系統內部控制查核程序，以評估受查單位

資訊系統中流程控制、資訊安全、存取控制等重大不實表達風險的程度，以確保資訊系統產製的資訊，具完整性、真實性。然而這樣的查核程序，與審計機關以往僅須透過瞭解相關書面資料，並可採行「繞過電腦的審計」模式之查核程序截然不同，此外，我國審計機關對單一受查機關辦理就地審計期間內，除先行評估資訊系統內部控制外，尚可透過所傳送之結構化財務資訊，加以分析，以採取實施必要的原始憑證抽核作業，並同時迅速閱讀、了解及分析有關非結構化之部分財務資訊與非財務資訊，非但使得審計人員短期間內，處於高壓的工作環境中，而有專業判斷上的失誤，更易使偵知風險上升，而提高整體的查核風險。

本文藉由審計部統計 105 年度與 106 年度第 1 至第 3 季中央及各地方審計機關運用該資訊審核分析系統發現各機關缺失情事，並依審計法規定通知各機關之件數統計情形，加以比較 (如圖 1)，發現屬於資訊登錄不全或錯誤者，可合理預期呈現成長或持平形態，顯示各受查單位所傳送的資訊，是有亟待改善之處。資訊系統化所帶來的效益是減少人工作業，卻也可能帶給資訊使用者面臨著不完整、不真實的風險存在，這樣的風險套在查核風險模式中，表徵著重大不實表達風險是呈現高度的水準；另在不使審計機關所面臨的查核風險提高變化下，中央及各地方審計機關，所承受之偵知風險，可合理估計僅能調降，審計機關為加以求證該等資訊的真實性與完整性，勢必耗費人力與時間予以驗證確認，以排除該等資訊無重大不實表達或舞弊情事，使得審計資源的配置，無法達到最適配置。

另分析內部審核缺失事項，有著顯著巨幅成長趨勢，這雖可加以解釋係因該審核分析系統發揮其所應有之成效，但由反面解釋，卻難表徵各機關內部審核人員執行



	內部審核缺失	與有關法令規定不合	資料登錄錯誤或不全	GBA/CBA系統功能缺失	其他
＝105(Q1-Q3)	75	213	52	16	9
▨106(Q1-Q3)	195	185	63	19	29

圖 1 資訊審核分析系統發現之缺失態樣情形比較圖

原始憑證合規性審核已趨健全，亦突顯出各地方政府內部控制制度，在行政院的強力推動下，儘管有著眾多設計範本可供參考，然實際執行之成效，卻有待檢驗，顯示審計機關於衡量受查單位重大不實表達風險僅能設於高點，為尋求因應且為使所承受的偵知風險趨於穩定，以及避免查核風險溢出可容忍範圍，似乎僅能放棄控制測試，並透過擴大證實測試的方式，以降低查核風險之擴張。

吳琮璠 (2002) 指出，資訊系統為確保交易資料輸入之合法、完整與正確，資料處理之完整與正確，資訊輸出之完整、正確與安全，因此資訊系統應置入應用控制，藉以預防與偵測可能的錯誤；黃文莉 (2005) 經運用複迴歸分析實證結果，顯示應用控制功能愈強，對於資訊系統之資訊品質愈有助益。周濟群 (2013) 指出，持續性稽核最主要的應用，是希冀透過資訊系統，找出傳統稽核或控制方法所無法發現的異常性風險問題，像是重複付款 (報支)、請購金額低於採購政策之限制條件、訂單金額高過其信用額度、無對應採購單的付款紀錄、分割採購等。為確保資訊的輸入、處理，及輸出均具質量，資訊系統導入能事前的預防，與即時偵測之應用控制功能，可說是相對重要的，這與持續性稽核中的 EAMs 有著異曲同工。本文試依審核分析系統所設計 20 項查核控制重點，並據持續性稽核中 EAMs 與 GAS 之定義 ，逐項分析辦別各項查核控制重點 (如表 1) 發現，審核分析系統所設計 20 項查核控制點中，像是統一發票有無重複報支、機關支付款項是否確為受款人領取、營利事業統一編號邏輯檢查、傳票號碼檢核、往來廠商已辦理註銷、廢止、撤銷或解散、往來廠商是否列入拒絕往來名單等查核控制點，均泛屬於 EAMs 的應用，但是這些查核控制重點，卻係由審計機關透過事後審計予以查核，而非由受查單位於資訊系統運行時，即予以監控，顯示未能善加有效地設計，並執行資訊系統內部控制，再次間接證實提升審計機關所面臨之重大不實表達風險，致使審計機關需耗費人力與時間，再予確認各種異常情事外，更亦使受查單位存有是否須設計，並切實執行內部控制之必要。

表 1 歲計會計資訊審核分析系統各項查核控制點

控制項名稱	持續性稽核之屬性
1. 統一發票有無重複報支	EAMs
2. 廠商每月銷售額逾 20 萬元	GAS
3. 支出用途查詢	GAS
4. 發票日期與付款憑單編製日期相距日數	GAS
5. 分批小額採購	EAMs 或 GAS
6. 機關支付款項是否確為受款人領取	EAMs
7. 營利事業統一編號邏輯檢查	EAMs
8. 支出收回	GAS
9. 對國內團體捐助之查核	GAS
10. 檢視註銷傳票內容	GAS
11. 歲入退還	GAS
12. 匯入傳票號碼檢核	EAMs
13. 半年結算、年度決算與會計月報核對	EAMs 或 GAS
14. 傳票編制日期與過帳日期相距日數	GAS

15. 歲入科目歸屬檢視	GAS
16. 應使用統一發票廠商開立收據情形	EAMs 或 GAS
17. 檢視往來廠商是否列入拒絕往來名單	EAMs
18. 公司組織開立收據情形	GAS
19. 受款人異常關聯	EAMs 或 GAS
20. 往來廠商已辦理註銷、廢止、撤銷或解散	EAMs

資料來源：作者整理繪製。

持續性稽核所運作原理，係基於電腦輔助稽核技術，目前常見的應用技術類型可分為：內嵌稽核模組 (Embedded Audit Modules：EAMs) 與通用稽核軟體 (General Audit Software：GAS) 等兩大類型。EAMs 其構想是於資訊系統內部加入測試控制有效性 (Control testing) 而設計的稽核模組程式，以達事前的預防與即時偵測控制功能。GAS 則是可使稽核人員獨立自行依所擷取的各種資料，運用內建查核分析功能，即可擷取資料進行分析，顯示該稽核技術須高度倚賴資訊科技，以自動化作業方式來減輕稽核人員的沉重負擔，然而 GAS 本質為一種事後稽核模式，致使較無法提供事前的預防與即時偵測控制功能。

綜上所述，任何受查者本身或多或少存有使其財務報表不實表達之風險，且即便透過內部控制制度加以控管，仍有其因控制設計不良或改變，導致可能發生錯誤，另雖有良好之內部控制制度，卻未能有效的去執行等情況發生，且在誘因或壓力、機會，及態度或行為合理化等舞弊因子存在下，將使審計人員處於一定的風險下，因此為使審計人員在可容忍或可接受的風險水準下，惟有加以規劃調整偵查風險，方可降低查核風險。

肆、結論與建議

隨著大數據的時代來臨，從傳統的統計分析到資料探勘，甚至能與文字探勘、圖像與影音分析等技術整合，以往因會計資訊需自行彙整交易事件的資訊處理成本過高，且不具備分析或解譯大量資料的能力，而審計重視的是因果關係，必須依賴有限的資訊，因此採行抽樣技術進行查核。然而在大數據環境下，隨資料流通管道均已趨向自動化，且運算、儲存能力大幅提升，抽樣的概念可能需要改變，在未來影響財務報表編製的資訊系統範圍，可預期將會擴大至各種新興資料來源，目前以資訊系統中的財務會計為主要查核標的之作法，勢必將有所變革，全面性查核將取代抽樣，特別是在查核舞弊等異常情境，須使用完整的資料集合來建立舞弊偵測模型，辨識及分析事件間之關連，預警性提出建議性意見將會來得更重要。

另外以風險為導向之審計方法，將因資訊和技術的充分運用與支持下，變得完善且多元，例如透過監控系統資料搭配流程探勘，評估內部控制設計及執行有無重大缺失，衛星定位系統則可運用於財產動態查核，會議紀錄可利用文字探勘技術找出有用的訊息，Yoon, Hoogduin and Zhang(2015) 認為甚至可連結至關於受查單位的動態性資料，如：新聞、部落格討論等，作為瞭解受查單位環境、評估查核風險之用。

正因如此，隨 2015 年 6 月 17 日通過修正審計法第 36 條，使得原始憑證按月送審制度走入歷史，且在受查單位以未導入持續性稽核概念的資訊系統，傳送資訊品質欠佳之結構化的財務資訊下，我國審計機關為維持一定的查核風險下，由於固有風險與控制風險的提高，所面臨的偵知風險確實有顯著降低，表徵著僅以「抽樣為原則、全查為例

外」、「財務為原則、非財務為例外」、「結構為原則、非結構為例外」的審計方法，顯然無法獲取足夠及適切之查核證據，為穩定維持審計機關所面臨的風險，本文提出下列之建議：

一、 依法辦理就地審計時，宜先就受查單位資訊系統的內部控制，加以評估相關流程控制、存取控制、資訊安全等重大不實表達風險的程度，藉以決定所產製結構化之財務資訊的可信賴程度，據以決定有無其必要擴大證實測試。且為因應送審憑證歷史化，無法再透過瞭解相關書面資料，加以確認受查單位是否確實依據已設計之內部控制切實執行，爰宜增加抽核原始憑證之時間、範圍等，並將有助於審計人員瞭解其受查機關之性質、目標、策略及營運風險。

二、 宜藉由不定時，與不定性方式，通知送審部分原始憑證，以降低受查機關投機取巧之預期心理，並適時採平行模擬方式，加以確認所傳送之資訊，係具真實、完整及可靠。同時為確保審計證據的範圍與品質，宜於審核分析系統導入內嵌稽核模組化的持續性審計，以增加查核的頻率，並提供更具即時性、攸關性的查核結果。另為避免審計機關，受限於受查單位所提供之資料，宜強化受查單位對於資訊之輸入、處理、及輸出等之有關規範，以切實落實課責機制，並確保資訊品質。

三、 宜於審核分析系統全面介接政府相關資訊系統，俾使審計人員於平時，先行評估受查單位內部控制作業流程，像是請購作業流程、付款作業流程等，並藉由該等資訊加以查核有無異常情事發生，例如往來廠商帳戶資料的異常更動、或員工薪資帳戶異常變動情形。經由以過往審計機關查核舞弊案例，找出大量資料中潛藏的特徵與規則，建置舞弊案例模型與紅旗警訊特徵，供各地方審計機關得以隨時加以運用。

參考文獻

1. 中華民國內部稽核協會，2011，全球科技稽核指引。
2. 吳琮璠，2002，會計財務資訊系統，台：智勝文化事業。
3. 周濟群，2013，談持續性稽核的新實務思維，內部稽核，7 月號：4- 10。
4. 財團法人會計研究發展基金會，審計實務指引，第二號，風險評估與內部控制 - 電腦資訊系統特點與考量。
5. 黃文莉，2005，資訊系統導入應用控制對資訊品質影響之研究，輔仁管 評 ，第 12 卷第 2 期：157- 188。
6. Yoon, K., L. Hoogduin, and L. Zhang. 2015. Integrating different forms of data for audit evidence: Markets research becoming relevant to assurance. Accounting Horizons 29 (2).

電腦稽核
JOURNAL OF INFORMATION COMMUNICATION AND TECHNOLOGY AUDITING 第 38 期

醫療隱私之法律保障

The Legal Protection of Health Information Privacy in Taiwan

黃維民
國立中正大學醫療資訊管理研究所
weimin950@gmail.com

摘 要

由於資訊科技產業的蓬勃發展，影響經濟甚巨，各先進國家紛紛推動跨國資訊整合計畫與相關政策。醫療隱私權為隱私權的一種，其與一般隱私權之不同在於，醫療隱私權除比一般隱私權更具有高度敏感性及隱密性外，醫療紀錄除記載一般性之個人資料外，往往記載個人身心之非常態描述，若醫療隱私予以揭示，容易使個人受到他人的品評、甚至歧視。

在法律機制的運作之下，給予病患一些例如告知後同意以及隱私與機密性的保障，讓病患得以透過這些方式來控制其資訊的運用；但是，因為醫療服務供給的特性，讓病患不得不放棄這些權利。因此，告知後同意的重點應該不是在狹義的同意，而是增加病患在資訊揭露時的選擇及參與。現今全球只有極少數國家針對醫療病例隱私保障訂立專法，就現有資料觀之，未來主要國家以制訂特別法方式，規範醫療資訊隱私之保護，應為大勢所趨。

本文參照國外相關的經驗，並就台灣目前現行的法律規範與未來發展趨勢，提出以下建議 : 第一、建議制定醫療隱私保護專法，第二、提高民眾的醫療隱私資訊保護意識，第三、建構資訊安全管理制度，第四、資訊財產權體系的建立，第五、強化告知後同意的法律機制，第六、建議嚴格推動去識別化之法律規範。。

關鍵詞：全民健保資料庫、電子病歷、資訊隱私、醫療資訊、個人資料保護法

Abstract

Since the vigorous development of IT industry and the great impact on economy, advanced countries have promoted transnational information integration plan and related policies. The right of health privacy is a kind of privacy, and the difference between it and the general right of privacy is that the right of health privacy than the general privacy is more highly sensitive and confidential. It is easy to make an individual subject to criticism and even discrimination from others.

Under the operation of the legal mechanism, it is possible for patients to control the use of their information through such means as giving consent to disclosure and privacy and confidentiality, but because of the nature of the supply of medical services, patients have to relinquish these rights. Therefore, the emphasis on informed consent should not be in the narrow sense of consent, but rather increase the patient's choice and participation in disclosure of information.

Referring to the relevant experiences of other developed countries, and the current legal norms and future development trends in Taiwan, the following recommendations : First, the proposed development of health privacy protection Law. Second, to improve the Health Privacy Information Protection awareness. Third, the construction of information security management system. Fourth, the establishment of the Information property system. Fifth, the strengthening of the legal mechanism on the consent after the notification. Sixth, the proposed strict promotion to identify the legal norms.

Keywords：National health insurance database, Electronic medical record systems, Information privacy, Medical information, Personal data protection law

壹、研究背景

近年來開放政府資料[1]在全球蔚為風潮，逐漸形成大數據[2]的概念。由於資訊科技產業的蓬勃發展，影響經濟甚巨，各先進國家紛紛推動跨國資訊整合計畫與相關政策。據經濟發展研究顯示，生技產業會是引領下一波經濟浪潮的關鍵。因此在配合推動生技產業的經濟發展架構下，將醫

1 開放資料指的是任何人能夠自由使用、重新使用與散佈的資料，最多也只能要求要有來源標示，並且以相同的方式來分享這些資料。開放資料的定義中有幾點重要的特性：例如這些資料是具有可得性與可讀性的，即是一般人能夠容易且方便獲得，與易於瞭解的資料；還有開放資料是大家可以重新使用與重新散佈，也就是開放資料它本身具有能夠分享的普遍性，也能夠讓彼此互相流通，不同的資料庫或是資料群組，可以彼此互用或是混合。呂宗學、邱伊翎、黃柔翡、馮瑜茜、呂家華、李宜卿、孫語辰，健康與醫療資料的加值應用公民論壇議題手冊，頁 19，2012 年 7 月。

2 大數據或稱巨量資料、海量資料、大資料，指的是所涉及的資料量規模巨大到無法透過人工，在合理時間內達到擷取、管理、處理、並整理成為人類所能解讀的形式的資訊。在總資料量相同的情況下，與個別分析獨立的小型資料集（Dataset）相比，將各個小型資料集合併後進行分析可得出許多額外的資訊和資料關聯性，可用來察覺商業趨勢、判定研究品質、避免疾病擴散、打擊犯罪或測定即時交通路況等；這樣的用途正是大型資料集盛行的原因。

療與健康資料加值應用的相關議題逐漸受到關注。就我國的現況而言，醫療與健康資料的主要來源是台灣全民健保資料庫，該資料庫保存所有國人的醫療與健康資料。然而，制度上卻缺乏完備的法律規範來監督或執行該資料庫的資料存取與使用。另外，就資訊科技與實務而言，該資料庫的資料是經由資訊整合與交換而來的電子病歷資料。在醫療雲端的概念下，所有醫療機構的病歷資料都必須逐步電子化和資訊管理化，再上傳至雲端的電子病歷交換平台上，經由資料整理並加密後分批匯入全民健保資料庫。

因此，從開放政府資料與大數據衍生而來的醫療與健康資料加值應用，配合醫療雲端的資訊與衛生政策，就必須透過電子病歷的揭露與交換，顯然對既有的醫療隱私人格權產生重大的衝擊。如果沒有完備的法律規範，日後難免引起諸多爭議，為防範未然以減少紛擾[3]，應對相關議題做通盤檢視與規劃，盡早做立法準備與討論，這是本研究最主要的目的。

貳、醫療隱私權的概念

醫療隱私權為隱私權的一種，其與一般隱私權之不同在於，醫療隱私權除比一般隱私權更具有高度敏感性及隱密性外，醫療紀錄除記載一般性之個人資料外，往往記載個人身心之非常態描述，若醫療隱私予以揭示，容易使個人受到他人的品評、甚至歧視。另外，醫療紀錄多為醫療人員或機關所記載及保存，個人控制可能性較低。醫療隱私因具有上開之特殊性，因此，其應較一般隱私權更需要受到較高密度之保護。

依據大法官解釋第 603 號所闡明，隱私權雖非憲法明文列舉之權利，惟基於人性尊嚴與個人主體性之維護及人格發展之完整，並為保障個人生活私密領域免於他人侵擾及個人資料之自主控制，隱私權乃為不可或缺之基本權利，而受憲法第 22 條所保障，個人自主控制個人資料之資訊隱私權而言，乃保障人民決定是否揭露其個人資料、及在何種範圍內、於何時、以何種方式、向何人揭露之決定權，並保障人民對其個人資料之使用有知悉與控制權及資料記載錯誤之更正權。但是憲法對資訊隱私權之保障並非絕對，國家得於符合憲法規定意旨之範圍內，以法律明確規定對之予以適當之限制，此可說明我國憲法承認資訊隱私的保護。我國對於資訊隱私的保護長久以來並沒有專法，而是透過刑法的妨害秘密罪章以及民法的侵權行為來保護資訊主體的權利，其他如醫師法與銀行法等，也規定了相關人員的保密義務。

憲法雖未明文規定隱私權為人民之基本權利，但依據司法院大法官釋字第 585 號解釋認為，隱私權為不可或缺之基本權利，並透過憲法解釋，將隱私權列入憲法第 22 條的權利之一[4]。從隱私權之內涵觀之，所謂資訊隱私權，乃係指個人對於自身領域內之資訊有自主控制並免於他人入侵之權利，而資訊隱私權可視為為隱私權的類型化。因

3 我國個人資料保護法於民國 99 年 5 月 26 日修正公佈，其中對於個人資料的蒐集、處理及利用之法律規範，個人資訊隱私保護的議題受到關注的程度 雖越來越高，因此目前對於醫療資訊的隱私權、醫療資訊的自主權，卻顯得保護不夠完善。謝志明，雲端運算健康資訊相關法律問題研究，頁 3，東吳大學法律學系研究所碩士論文，2013 年 7 月。

4 我國有關隱私權是受美國法與德國法兼具之影響，「資訊隱私權」在我國首見於司法院釋字第 603 號解釋文，其認為「就個人自主控制個人資料之資訊隱私權而言，乃保障人民決定是否揭露其個人資料、及在何種範圍內、於何時、以何種方式、向何人揭露之決定權，並保障人民對其個人資料之使用有知悉與控制權及資料記載錯誤之更正權。」

此，為保障人民的資訊隱私權，司法院大法官已在好幾號解釋中提及人民之資訊隱私權[5]。

資訊隱私權之作用與目的，在於限制他人蒐集與使用有關足以辨識自己的資料之權利，以確保個人自我界定的權利，但現今科技發達，若將個人資訊隱私所欲保護之對象侷限於個人私密之資訊，恐無法提供足夠保障，而不能因應資訊科技發展所造成對個人之侵害。在今日透過電腦處理技術，可將零碎、片段、無意義的個人資料，快速串連、比對歸檔與系統化。當大量資訊累積在一起時，經過電腦分析處理，即可顯現某特定個人之生活私密。誰掌握了這些技術與資訊，便掌握了監看他人的權力。為避免個人處於透明與被監視的隱憂之中，隱私權保障的範圍也應該隨之擴張到非私密或非敏感性質的個人資料保護。因此個人資料保護範圍包含涉及私密敏感事項之敏感性個資與非私密敏感但易與其他資料結合為個人檔案之一般性個資。但一般人格權並非完全不得干預，因此對資訊隱私權之保障並非絕對，端看個人對個人資訊之揭露是否屬無隱私或無秘密合理期待性，又國家得於符合憲法第 23 條規定意旨之範圍內，以法律明確規定對之予以適當之限制。

隨著時代演進，人權觀念日漸擴張。就現代社會而言，人權範疇已從最早的人身安全自由保護、私有財產的保護，擴及至言論自由保障、參與政治自由保障等，最後更將個人隱私權納入人權的保障範圍[6]。我國憲法雖未明文規定保障隱私權[7]，然相關立法例中仍存有保障隱私權之規定[8]。又因科技日新月異，隱私權之侵害類型有多樣化、新穎化之情事下，加上人民對隱私權保障之程度與範疇日益重視，傳統法律對隱私權保障規範密度顯有未足。因而我國在參酌經濟合作暨發展組織 (OECD) 於 1980 發布 OECD 隱私保護及個人資料之國際傳輸指導方針、亞太經濟合作組織（ APEC）隱私保護綱領及 1995 年歐盟資料保護指令 (95/ 46/EC) 等相關外國立法例後，於 2010 年 5 月 26 日修正公佈《個人資料保護法》，做為對於個人資訊自主權之概括性保護法規，而個資法第 6 條即明文將醫療資料列入特別敏感資料加強保護。新個資法對於適用主體及適用客體的限制均已放寬，除了不限於電腦處理之資料，並且其他得直接或間接識別個人身分的資料都納入規範。非公務機關亦取消行業

5 隱私權和大部分基本權比較，算是較新發現或主張之基本權利，因其內涵不明，故是個難以界定的概念，每個法律概念都有其核心與外緣，越是接近核心的部分，其意涵越清楚，故較不會有爭議，反之越靠近外緣之部分，則其意涵越模糊，而隱私權的核心十分狹小，甚至連核心都不清楚，此從隱私權的定義為不受侵擾之權利觀之，何種行為算是侵擾即不明確，實務上常以隱私之合理期待不受侵擾之自由來判斷，但合理期待即很抽象；再者，資訊隱私權衍生至今以個人資訊之自我控制為核心，即自身資訊揭露控制權，或稱資訊自主權，也很難清楚或完整表現出資訊隱私權之意涵；畢竟個人隱私不受侵擾之權利與個人資訊之自我控制是兩個不同之情境，故資訊隱私權與資訊自主權兩者並不相等。葉俊榮，政府資訊公開與隱私權－司法對基本權利的脈絡論證與空間構築，司法院大法官一百年度學術研討會－憲法解釋與隱私權之保障（上冊），頁 86-88，2011 年 12 月。

6 參世界人權宣言第 12 條：「任何人的私生活、家庭、住宅和通信不得任意干涉，他的榮譽和名譽不得加以攻擊。人人有權享受法律保護，以免受這種干涉或攻擊。」；公民與政治權利國際公約第 17 條：「一、任何人之私生活、家庭、住宅或通信，不得無理或非法侵擾，其名譽及信用，亦不得非法破壞。二、對於此種侵擾或破壞，人人有受法律保護之權利。」；兒童權利公約第 16 條：「一、兒童之隱私、家庭、住家或信函不可恣意或非法干預，其信用與名譽亦不可受到非法侵害。二、兒童對此等干預或侵害有依法受保障的權利。」。

7 參釋字第 585 號解釋理由書略以：隱私權雖非憲法明文列舉之權利，惟基於人性尊嚴與個人主體性之維護及人格發展之完整，並為保障個人生活秘密空間免於他人侵擾及個人資料之自主控制，隱私權乃為不可或缺之基本權利，而受憲法第 22 條所保障。

8 如民法第 195 條、刑法第 28 章等。

別的限制。此外，針對敏感性資訊作特殊規範，原則上雖禁止處理，然而卻可基於統計、研究與衛生之目的逕行蒐集處理與利用個人資訊，實有增加限制的必要。此外，新個資法亦未設有資料保護監察的專責機關，實有增設資料保護專責機關之必要。

參、文獻回顧

一、全民健保制度

全民健康保險制度秉持自助互助、共同分擔風險的原則，以全體國民為納保對象，是政府增進國民健康福祉的一項重大政策[9]，然而給付方式的改變，造成醫療院所之間競爭激烈，對於醫療產業的經營也是一大挑戰。全民健康保險實施後，病歷成為醫療機構申請健保給付，以及健保署進行審查稽核作業時的重要依據。所謂「病歷」意指醫事人員在執行業務時，針對病人實施各項醫療行為的相關記錄，依據我國醫師法第十二條規定，病歷除應載明病人基本資料（姓名、性別、生日、住址等），其內容還必須包含就診日期、主訴、檢查項目及結果、診斷或病名、治療、處置或用藥情形以及其他應記載事項，並交由醫療機構依醫療法之規定保存。病歷記錄除了能夠作為保險給付的依據以外，更有助於醫事人員快速掌握患者病史與病情，提供更有效率的醫療服務，進而提升醫療品質，因此病歷管理對於醫療機構的永續經營非常重要[10]。

然而近幾年，健保體制下的缺點一一浮現，如醫療支付費用逐年攀升、健保資源過度使用等問題，造成健保財務的虧損。且因為健保申報需依靠病人完整的就醫紀錄，來做為保險給付的重要憑證，故對於醫療院所而言，健康保險的施行是促使醫院開始使用紙本病歷的主要原因。但紙本病歷經年累月地大量增加，造成病歷室空間需求的增加也提升醫院內員工之工作量，故全民健康保險的開辦，間接促使醫院資訊系統的發展。

醫療資訊系統始於 1960 年代，發展初期主要以節省人力及提高工作效率，故未涉及全部範圍，僅以一般行政管理方面之功能為主，且資訊處理多為個人單一處理形式，且當時電腦科技與技術尚未成熟，還無法應用於醫療資訊系統；1970 年後，部分大型醫院開始在院內設立資訊部門；從 1980 年至今，資訊系統的發展已從一般行政擴大至管理、臨床及醫療作業上，此階段給予醫界極大的幫助。

在健保資料庫的應用上，常會涉及不同資料庫間的資料，互相對比參照，進而獲得研究者所需的結果。就國外醫療相關資料庫而言，以冰

9 全民健康保險法第 1 條。

10 醫療法第 68 條。

島為例，此資料庫之建置原為基因資料庫之準備，而所謂基因資料庫係以尋找疾病致病基因或其他致病因子為目的，而以人群研究之方法，樣本數量為高達數萬或數十萬以上的人群資料庫，至於其他 DNA 序列資料庫，犯罪嫌疑人的 DNA 資料庫等，並非以大規模人群樣本為內容。故基因資料庫之研究，其前提即為蒐集大量民眾基因樣本，而同時也必須蒐集這些民眾的醫療資料，兩者互相比對以得出何種基因變異可能與何種健康表現有關，在討論基因資料庫時實難僅以其本身為討論對象，自然必須加入醫療資料庫及其間兩者的比對方式，甚至需要蒐集家族族譜資料等共同研究，才能對多重因子所導致的疾病做有效的分析[11]。

至於資料庫建立所需之醫療資料，衛生部門資料庫法並未以法律直接規範醫療機構必須交出病患醫療紀錄給予特許機構來建構此一資料庫，而醫療資料來源係建立在特許機構與醫療機構兩者間自行協議，此處又包含一個前提，即病患的推定同意（Presumed consent），即該法明定，持有醫療紀錄之醫療機構已有病患的推定同意，同意醫療機構將其醫療紀錄交予特許機構，否則縱使醫療機構與特許機構間達成協議，醫療機構本來亦無權利將病患醫療紀錄提供予第三人，該行為顯然有違反醫療契約保密義務及醫學倫理，亦有可能違反 1997 年病患權利法（Act on the rights of patients）關於應取得病患告知後同意之要求。而醫療機構與特許機構達成協議後，在提供醫療紀錄前，需將紀錄中可識別個人身分的部分進行不可回溯的單向編碼（One-way coding），使特許機構僅能接觸到無法識別個人身分之資料，所謂無法識別，依衛生部門資料庫法第 3 條名詞定義，係指無法真接或間接辨識個人身分，包括透過個人身分編號或由一個或多個關於個人身體、生理、心理、經濟、或社會文化條件而可被辨識出個人身分前述單向編碼處理方式，須依個人資料保護委員會（Data protection commission）之規範進行。另外，若民眾不願自己的醫療紀錄被輸入資料庫，必須額外依該法規定申請選擇退出，否則均依法推定為同意將醫療紀錄納入資料庫，且若係死亡的病患其生前未選擇退出，無需經病患家屬同意，則當然可將其醫療紀錄加入資料庫。而造成後續爭議產生，主要部分就在於本法規定的「推定同意」，而衛生部門資料庫法會採取推定同意之理由，一個固然基於成本考量，若需向個別民眾逐一取得其同意，耗費成本過鉅，

11 Marta Gwinn & Muin J. Khoury, Epidemiologic Approach to Genetic Tests: Population-Based Data for Preventive Medicine, HUMAN GENOME EPIDEMIOLOGY (2003).

另一個則是認定已編碼過，無法識別個人身分之資料，自然無需視同個人資料予以保護。但此兩點理由是否足以支持「推定同意」的合憲性，顯然在後來的憲法訴訟中受到挑戰。後續在冰島最高法院 2003 年 11 月 27 日判決衛生部門資料庫法部分條文違反冰島憲法，判決理由指出所謂單向編碼處理後的資料，並非無法辨識個人身分的資料[12]，因此對於法規中「推定同意」的規定，以及對於死亡病人不承認家屬有權利得拒絕將其資料納入資料之規定，及相關安全保密措施不足，均已違反冰島憲法第 71 條保障的隱私權。

二、病歷與醫療資訊系統

因此，組織或醫療機構將金錢不斷投資在資訊科技上，並且逐漸關注影響使用者在科技採用與使用之重要關鍵因素，以透過資訊科技有效提升生產力。但當面對醫療照護成本的日益增加時，可藉由醫療資訊科技做出正確決策，有效提升醫療照護品質或降低醫療錯誤來提升病患安全，如電子病歷的推行[13]。故美國政府宣告在 2014 年要達到全面導入電子病歷在各醫院管理上，並強調透過 Medicare 跟 Medicaid 鼓勵醫療機構與醫師電子病歷必須有意義的使用（Meaningful use），才能獲得相當的補助[14]。

由於網際網路的蓬勃發展，透過網際網路之便利、快速等特性，各種形式的交易模式逐漸出現，企業與企業之間能夠以快速有效的方式進行資料交換，許多產業以此新興的商業模式發展相當多的實務應用，藉此改善產品與服務品質、減少產品與服務之提供時差，進而降低成本。其中醫療產業透過網際網路之應用進行遠距醫療、院際資訊分享、電子病歷資料存取與交換即是其中一項。醫療院所可藉由電子資料交換（Electronic Data Interexchange, EDI）的方式建立院際間共通的資訊平台，利用健康資訊交換第七層協定（Health Level7, HL7）[15]、醫療數位影像傳輸協定（Digital Imaging and Communications in Medicine, DICOM）等醫療資訊交換標準，醫療院所與相關單位能夠減少紙本病歷資料交換成本上的支出。醫師也

12 Arnason Einar, Personal Identifiability in the Icelandic Health Sector Database, 2 JOURNAL OF INFORMATION,LAW &TECHNOLOGY, (2002).

13 為因應醫療資訊電子化趨勢，新修正醫師法第六十八條中「醫療機構以電子文件方式製作及貯存之病歷，得免另以書面方式製作；其資格條件與製作方式、內容及其他應遵行事項之辦法，由中央主管機關定之。」規定病歷以電子文件方式製作及貯存者，得免另以書面製作，並授權中央主管機關就其資格條件與製作方式、內容及其他應遵行事項訂定辦法規範之。黃鼎佑、曾德宜，電子病歷管理與運用之相關法律議題初探，載：全國科技法律研討會論文集，頁 83-96，交大科法所，2006 年 6 月。

14 Schepps & Rosen（2002）及 Moore（2002）皆說明醫療資訊系統之功能，強調此系統利用電腦取代人工作業，有效降低醫療成本及作業流程，並提升工作效率及品質。隨著資訊科技日新月異的進步，醫院內資訊系統須因應趨勢的變化而有所演進，醫療機構也慢慢將紙本病歷電腦化進而再電子化。

15 電子病歷簡單來說，就是將傳統紙本的病歷改用電子化的方式儲存，由於牽涉到各個醫療機構間的病歷資訊交換，也因此促使各國進行電子病歷標準的制定，而目前台灣採用的是國際標準 HL7 CDA R2。

不再受限只能使用病人在單一醫療院所的就醫紀錄，因此能對病患的健康狀況有全盤掌握，可增加病人照護品質，減少醫療資源浪費。尤其政府相關衛生單位能夠從中萃取出有用之資訊以協助制訂衛生政策，因此電子病歷交換，對於政府、醫療院所、醫療人員與病患都將有顯著的效益。

隨著國內醫院電子病歷的實施情況普及，有關電子病歷交換之相關議題也逐漸受到關注。電子病歷交換的主要願景是希望提供給病患完整的醫療照護。由於台灣交通逐漸便利，民眾就醫可近性高，病歷資料極有可能分散在不同的醫療單位中，造成重複檢驗、檢查及用藥等醫療資源耗費。因此，在健保制度的環境下，透過實施電子病歷交換，醫療資源將得以有效利用，更避免不必要的醫療資源浪費。同時，醫師可以取得病患過去的就醫處置、家族病史、藥物過敏等資訊，提供更全面性的診斷與醫療決策。

根 據 The National Ambulatory Medical Care Survey（NAMCS）針對美國電子病歷使用現況做的最新調查指出，約 43.9％醫師使用過完整或部分電子病歷系統，其中只有 6.3％使用完整系統，相較於 2006 年的調查結果僅 29.2％醫師使用完整或部分電子病歷系統有明顯的提升。而就國內而言，衛生福利部自 1997 年起為推動電子病歷，陸續委外辦理諸多專案，為求謹慎及經驗的累積，初期的規模以小型或區域性質研究試辦計畫居多，2009 年依據醫療法所訂定「醫療機構電子病歷製作及管理辦法」來實施醫學影像報告之電子病歷，並成立全國醫療影像交換中心（Image Exchange Center, IEC），擴大電子病歷之交換分享及參與醫療機構之範圍。

另外，美國醫療資訊暨管理系統協會（The Healthcare Information and Management System Society；HIMSS），亦將評價醫療機構實施電子病歷分成 8 個層級，至於共同的電子病歷交換標準方面[16]，國際組織 HL7 的電子病歷系統功能，雖然於 2007 年 2 月獲得美國國家標準局（ANSI）正式批准，成為世界上第一個關於電子病歷的國家標準，但美國至今的電子病歷卻似乎並沒有完全按照這個標準進行設置。理由主要是，美國欠缺一個全體國民的保險制度，因此國民的健康資料會隨著其自身所納保之保險體系之不同而有所變動，而美國大部分都是多元保險人。即便美國健康保險可攜與責任法（The Health Insurance Portability and Accountability Act, HIPAA）與經濟與臨床健康資訊科技法（The Health Information Technology for

16 Healthcare Information and Management Systems Society (HIMSS), IMSS U.S. EMR Adoption Modelsm Trends, HIMSS ANALYTICS, http://www.himssanalyticsasia.org/docs/AAP_EMR_Adoption_Model_V1.1.pdf (last visited Jun. 1, 2015).

17 邱泓文，各國電子病歷趨勢分析及台灣電子病歷發展之研究，頁 12，臺北醫學大學醫學資訊研究所碩士論文 2013 年。

Economic and Clinical Health Act, HITECH）法，對於電子病歷多有規範[17]，甚至大 預算投入協助電子病歷使用[18]；但建構一套連結所有醫療服務提供者之資訊系統，尤其必須涵蓋每個國民保險資料的資訊，似乎才是根本解決之道。

三、電子病歷交換

由上述研究背景可知，國內政府對於電子病歷的發展積極推動，甚至期望能達到電子病歷跨院交換。衛生福利部於 2011 年建置完成電子病歷交換中心（Electronic Medical Record Exchange Center, EEC），先以 CT、MRI、PET 等影像進行交換，計畫跨展至其它電子病歷資料。由此可知推動實施電子病歷交換已是我國重要的健康政策。

當未來電子病歷實施普及後，病患可以透過健保 IC 卡的方式，在有合作的醫療機構，經病患同意以及醫師授權下，便可完整地取得病人以往的就醫紀錄，以達到連續不間斷的照護模式。目前在電子病歷推動上，政府的推動方向正確，醫院部分從較難的影像切入，帶領醫院與業者直接跨越門檻，減少後續推動困難。但是部分醫院和診所因為電子病歷帶來的醫療糾紛證據力與醫療利益等問題，使得建置上遇到相關阻力，尤其電子病歷因其資料過於敏感且私密，如何有效了解其安全性及隱私權之相關問題點，將成為電子病歷推動過程中的主要面臨的問題[19]。

電子病歷以電子化文件的形式將病人健康資訊記錄下來，並儲存在電腦資料庫中。病歷電子化不僅可以解決紙本病歷容易泛黃、潮濕、受損、醫護人員手寫字體難以辨認、佔用大量儲存空間、無法多人同時讀取、調閱及遞送困難等缺失，還有助於降低醫院的醫療成本、提升醫療服務效率、增進病人安全，在病歷管理發展過程中是一大進步。

有鑑於電子病歷的諸多好處，先進國家政府無不積極推動，然而各國電子病歷定義不一，又電子病歷在醫院資訊系統內牽涉層面複雜，造成醫療機構實際電子化程度難以衡量。美國醫療資訊暨管理系統協會（The Healthcare Information and Management Systems Society, HIMSS）為了瞭解醫院推行電子病歷之狀況，制定EMR採用模型（EMR adoption model），以八個階段檢視醫院電子病歷的應用情況，利用該模型評價醫療機構實施電子

18 黃維民，衛生行政與健康保險，華杏出版，頁 303，2012 年 9 月。

19 電子病歷在目前我國電子簽章法的架構下，視為電子紀錄的一種應用形式。然而，對於電子紀錄的製作，其選擇權並非交由病患當事人選擇，而是由醫療院所自行裁量決定，同時，在現行相關法律架構下，電子紀錄的管理與保護是否安全？是否可靠？尚有疑慮的情形下，如何克服管理與技術上的障礙，以兼顧保障當事人權益以及善用新科技便利性，遂成為今日健康資訊科技（Health information technology）應用的主要衝擊與挑戰。黃鼎佑、曾德宜，電子病歷管理與運用之相關法律議題初探，載：全國科技法律研討會論文集，頁 83-96，交大科法所，2006 年 6 月。

病歷之水準，幫助醫療機構達到電子病歷「有意義的使用」(Meaningful use)[20]。根據HIMSS所屬研究分析機構在2012年針對美國14,872家醫療機構採用門診電子病歷的最新報告結果顯示，只有10%左右的醫療院所達成以電子文件和電腦取代紙本病歷，30.54%開始使用臨床資料庫來保存醫囑和結果，更有超過半數仍然使用紙本文件來保存和管理病歷。

現行跨院調閱電子病歷[21]，其保護措施實屬不足。按照現行制度，病患必須簽屬其跨院互通之同意書，且必須確認其健保卡，而同意書可限定授權醫院、調閱單張類別以及有效期限，整個傳輸過程是在加密安全網路通道中進行。但是，即使這些說明出現在衛生福利部之宣傳檔案，卻未有明確的法律依據[22]。換言之，雖然衛生福利部立意良善，但現行這樣的跨院調閱電子病歷，的確需要有個法制化的解套方案。諸如同意書的內容、同意書使用或可為代筆之例外情況、傳輸過程的保密等級與認證機制等，其實都有詳加探討，看是否有法規化加以管制之必要。

肆、我國對醫療隱私的法律保障

我國許多學者對於隱私權有不同的定義。認為隱私權是個人對其私領域的自主權利，並認為隱私權係由「私領域」以及「自主權利」兩大核心因素所構成[23]。也認為隱私權是一種「保障個人對於其個人資訊的控制」、「滿足個人對於其獨立自主的要求」以及「提升個人自我表現與形成社會關係的能力」之權利。因此，隱私權可謂個人對於私人領域內事務的控制權，他人對於該領域內事務的不得侵犯，以及個人決定其私人領域內事務是否公開及公開程度之權利[24]。

---

20 美國病歷協會為電子病歷的發展定義出五個階段：

1. 醫療紀錄自動化（automated medical record，AMR）
2. 病歷資料電腦化（computerized medical records，CMR）
3. 電子病歷（electronic medical records，EMR）
4. 電子病患資料（electronic patient records，EPR）
5. 電子健康資訊（electronic health record，EHR）

由於全民健保制度的實施，台灣在第二階段的CMR已有很好的基礎，而目前正在第三階段努力推廣中。

21 進行電子病歷院際間的交換互通作業，必須先行建立共同的電子病歷交換標準，而衛生福利部即早於2008、2009年度制定符合國際規範之HL7 CDA R2之電子病歷標準架構，包含醫學影像報告、血液檢測報告、門診用藥紀錄以及出院病摘電子病歷單張標準，作為首先進行交 換的四大標準電子病歷單張。

22 醫療法第74條規定：「醫院、診所診治病人時，得依需要，並經病人或其法定代理人、配偶、親屬或關係人之同意，商洽病人原診治之醫院、診所，提供病歷複製本或病歷摘要及各種檢查報告資料。原診治之醫院、診所不得拒絕；其所需費用，由病人負擔。」，但用以規範跨院調閱電子病歷顯然規範密度不足。

23 王澤鑑，侵權行為法，頁26，2007年。

24 林子儀，從保障隱私的觀點論基因資訊的利用與法的規制，載：基因科技與法律研討會論文集，學林文化事業有限公司，頁264-266，2003年。

一、 憲法及大法官釋憲文

我國憲法並未明文列舉隱私權為憲法保障之權利，而至大法官第 293 號釋憲文，才首次出現「隱私權」一詞；而在大法官釋字第 585 號則明白承認隱私權乃我國憲法第 22 條概括規定範圍內的基本權利，受憲法所保障。該解釋文指出「維護人性尊嚴與尊重人格，乃自由民主憲政秩序之核心價值。隱私權雖非憲法明文列舉之權利，惟基於人性尊嚴之維護及人格發展之完整，並為保障個人生活私密領域免於他人侵擾及個人資訊之自主控制，隱私權乃不可或缺之基本權利，而受憲法第 22 [25]條所保障」，闡明隱私權的價值理念在維護人格尊嚴、個人主體性及人格發展自由。

而後大法官在釋字第 603 號文中又揭示個人擁有不受侵犯之控制自身資訊的權利：「隱私權雖非憲法明文列舉之權利，惟基於人性尊嚴與個人主體性之維護及人格發展之完整，並為保障個人生活私密領域免於他人侵擾及個人資料之自主控制，隱私權乃為不可或缺之基本權利，而受憲法第 22 條所保障 」。其中舉出許多憲法應保障的權利為「人性尊嚴」、「人格自由發展」、「隱私權」、「個人主體性」、「個人資料自主控制」等，以及「資訊隱私權」。「個人自主控制個人資訊之資訊隱私權而言，乃保障人民決定是否揭露其個人資訊、及在何種範圍內，於何時、以何種方式、向何人揭露之決定權，並保障人民對其個人資訊之使用有知悉與控制權及資訊記載錯誤之更正權」。

二、 我國保護隱私權的其他相關法規範

（一）1999 年民法債編第 195 條[26]修正，認為人格權為抽象概念，明文賦予「隱私 」受到侵害的請求權基礎，確認侵害人格及身分法益之非財產上損害賠償。在修正前原條文採列舉主義，侵害隱私權並無法請求非財產上之損害賠償。修正前原先對於人格權之保護採所謂的「特別人格權主義 」，認為僅及於條文所列舉之生命、身體、健康、名譽及自由等五項人格法益，修正後範圍擴及信用、隱私、貞操，並增加了「不法侵害其他人格法益而情節重大者 」以防疏漏或濫用。

（二）刑法第 133 條、第 306 條、第 315-1 條增訂、及第 316 條。隱私保護以「秘密 」之名，分別規定於刑法中，第 133 條為對郵電秘密之保護；第 306 條對於無故侵入他人住宅、建築物者加以處罰；第 315 條為對書信秘密之保護。而鑒於社會使用微型錄音錄影等電子設備普遍，而以此類工具窺視、竊聽、竊錄他人隱私活動、言談或談話者，故於

25 司法院釋字第 585 號。

26 民法第 195 條：「不法侵害他人之身體、健康、名譽、自由、信用、隱私、貞操，或不法侵害其他人格法益而情節重大者，被害人雖非財產上之損害，亦得請求賠償相當之金額。其名譽被侵害者，並得請求回復名譽之適當處分。」

第 315 條之 1 則增訂了對非公開活動、言論、談話、身體隱私部位之保護；第 316 條為禁止洩漏業務上知悉之秘密。上述條文亦規定了侵犯隱私權之法律責任。

（三）通訊保障及監察法。1999 年制訂的此法乃為保障人民秘密通訊自由不受非法侵害，第 13 條規定通訊監察以截收、監聽、錄音、錄影、攝影、開拆、檢查、影印或其他類似之必要方法為之。對於違法侵害通訊秘密之個人或公務員設有刑罰之規定，以保障電信、郵件、書信、言論及談話等有關隱私或秘密之合理期待。

（四）去氧核醣核酸採樣條例，於 1999 年制定的該法目的為了維護人民安全、協助司法鑑定、協尋失蹤人口、確定親子血緣、提昇犯罪偵查效能並有效防制性侵害犯罪。其第 3 條定義「去氧核醣核酸」為指「人體中記載遺傳訊息之化學物質」，包括人體血液、唾液、毛髮所攜之個人獨特去氧核醣核酸（Deoxyribonucleic Acid, DNA）足以辨識基因特徵之遺傳資訊，均非公開資訊，不可容許他人任意蒐集，但為犯罪偵查之必要，妨害性自主或者重大公共危險、殺人傷害等罪刑之被告或嫌疑犯，於法院或檢察官認為有必要時，得強制採樣。但 DNA 實屬個人之隱私，因此該條例第 10 條規定，採樣程序及方法「並應注意被採樣人之身體及名譽。」第 11 條規定，主管機關應妥為儲存該 DNA 樣本並建立紀錄及資料庫。受採樣者若受不起訴處分或經法院無罪判決確定者，則主管機關應刪除其 DNA 樣本及記錄。

（五）個人資料保護法對於個人資料之違法蒐集、使用、破壞等行為設有處罰規定。

（六）其他如銀行法第 48 條對顧客之存放款等有關資料應保守秘密；醫療法第 72 條則規定醫療機構及其人員因業務而知悉或持有病人之病情或健康資訊，不得無故洩漏。此外，刑事訴訟法第 11 章對於搜索、扣押之要件及程序均有嚴格之規範，以保障人身自由之隱私。

三、 隱私權相關釋憲文及重要實務判決案例

（一）民國 88 年發布實施的戶籍法第 8 條規定，請領國民身分證必須捺指紋並錄存。民國 94 年內政部計畫全面換發國民身分證時，訂於 94 年 7 月起全民必須按指紋才能領取新版身分證。後經大法官第 603 號釋文解釋，指紋乃重要之個人資訊，個人對其指紋資訊之自主控制，受資訊隱私權之保障。戶籍法強制要求按捺指紋，卻未明文規定目的為何，「於憲法保障人民資訊隱私權之意旨已有未合。… 縱用以達到國民身分證之防偽、防止冒領、冒用、辨識路倒病人、迷途失智者、無名屍體等目的而言，亦屬

損益失衡、手段過當，不符比例原則之要求。」故戶籍法該項規定違憲，不得再適用。

（二）台灣高等法院 87 年上字第 76 號，判決理由中指出，所謂隱私權乃係不讓他人無端地干預其個人私領域的權利，此種人格權，乃是維護個人尊嚴、保障追求幸福所必要而不可或缺者[27]。

（三）最高法院 92 年台上字第 164 號判例認為：「於他人居住區域發出超越一般人社會生活所能容忍之噪音，應屬不法侵害他人居住安寧之人格利益，如其情節重大，被害人非不得依民法第 195 條第 1 項規定請求賠償相當之金額」。而修正後民法第 195 條擴大了人格法益保護範圍，立法上擴張及於信用、隱私、貞操等之侵害，增訂其他人格法益之概括規定，並以侵害情節需為重大作為限制。故上述判決乃循此思維而來。

（四）至於對未被定罪者的嫌疑犯是否得以強制採集其 DNA 檢驗，則在美國出現一 Maryland v. King 訴訟案例[28]。美國有 29 個州均允許採集重大刑事嫌疑犯的 DNA 以進行偵查。2009 年美國馬里蘭州警方逮捕一名一級攻擊罪嫌疑犯 King，其 DNA 檢測結果，與 2003 年一樁未破案的強暴案中蒐集到的嫌犯 DNA 樣本吻合，故馬里蘭州審判法院依此證據判定 King 於 2003 年強暴案有罪。但該州最高法院駁回該項判決，認為該份 DNA 樣本乃於不當搜索下取得，違反美國憲法增修條文第 4 條，亦即保障人民不受非法搜索逮捕之權利，認為 King 對於受憲法增修條文第 4 條的隱私權保護期待之權利，高於馬里蘭州用其 DNA 來辨識犯罪的利益。此案經上訴聯邦最高法院後遭駁回，認為被告遭採集 DNA 樣本時，已因犯罪嫌疑重大被警方帶至警局準備拘留，故警察以棉花棒輕抹被告口腔內膜採取 DNA 樣本的動作，如同拍照、按指紋等作業，為合法的警方登記建檔程序，應為美國憲法增修條文第 4 條下的合理作為。故此情況下的 DNA 採樣僅會對被逮捕者利益產生微小侵害，而不致違反美國憲法增修條文第 4 條[29]。

上開論述大多是從美國普通法為說明，至於美國憲法對隱私權之保障上，一般認為是從 1965 年的 Griswold v. connecticut 案開始承認。該案簡之為，Griswold 為迪克州計畫生育中心之負責人，和另一名醫師 Lee Buxton 於執行業務過程當中，提供已婚之夫婦避孕之相關

27 台灣高等法院 87 年上字第 76 號民事判決。

28 Maryland v. King, Fourth Amendment search and seizure DNA expectation of privacy, Cornell University Law School, https://www.law.cornell.edu/supct/cert/12-207. (last visited Oct. 6, 2015). 以及美國聯邦上訴法院判決文 , SUPREME COURT, http://www.supremecourt.gov/opinions/opinions.aspx. . (last visited Oct. 6, 2015).

29 但參與審理的法官有 5 位同意，4 位不同意該項判決，可見爭議性仍相當大

意見，違反康乃迪克州法律中之規定：「任何人使用藥物、醫療用品或器具進行避孕，均必須被處罰金或監禁」與「任何人提供協助、諮詢、促使、僱用或命令他人為避孕之行為，必須受到起訴與處罰」的規定，因此於 1961 年被逮捕。在該州之地方法院以及上訴法院，被告被判有罪並各被科處美金 100 元，被告等人不服而上訴美國聯邦最高法院，認為州法之相關規定違反美國憲法第 14 條增修案之正當法律程序原則。

伍、結論與展望

在現今個人無法獨立於社會之外，每個人都是社會共同體的一份子，人與人互動時難免會相互涉及他人個人資料，當一方因某種目的蒐集取得另一方個人資料後即成為資料管理者。資料管理者基於各種目的產生蒐集、運用之需求，例如非公務機關與客戶間所訂立之契約，或者雙方因締約前之準備階段之類契約，而產生有蒐集、運用他方個人資料之需求與權利；或因公務機關因執行法定職務必要範圍，或法律明文規定，而產生有蒐集、運用人民個人資料之權利。

人對於屬於自己的資訊，固然有自主決定是否提供予他人知悉，以及選擇提供的範圍或項目、或者運用之特定目的與範圍之權利，相反的亦有不提供之權利；惟在人與人的交往過程中，提供足以辨識身分之個人資訊給與他人，亦是維持人與人的交往之間所不可或缺之信賴基礎；人民與國家間之權利義務關係，亦需藉由個人資訊始能將之具體化，因為國家機關擁有廣泛蒐集資訊之權力，並藉由所蒐集的資訊作為施政正當性之基礎，又政府蒐集、公開、運用資訊有維繫國家安全與創造社會人民福祉之憲法意涵，因此，在適當之情況下提供個人資訊，亦有其必要性。

換言之，資訊隱私權或資訊自主權亦非受到絕對之保護，從而，個人之資訊隱私權與公益之間要如何取得平衡，亦即如何取得「隱私權」與「知的權利」間之平衡關係，又隱私權在目前已非僅存在於私法領域，而已經提升至公法上之權利，國家要基於如何之公益目的始得要求人民提供個人資訊，人民在國家蒐集、儲存、整合、傳遞或提取使用屬於個人資訊之過程中，能否參與、更正或拒絕國家機關之行為。再者，另一方面人民有向政府要求資訊之權，國家基於行政或公益或其他原因而蒐集、儲存、整合、傳遞或處理利用之各種資訊，人民基於民主政治及資訊自由之理念下，可要求政府公開其所擁有之資訊，以提高行政透明度與人民對公共事務之參與及知的權利，意即國家的資訊公開已成為原則而非例外，在此情形下，國家的資訊公開制度應如何因應，才不至於在資訊公開時滿足請求資訊公開之人的權利，卻不當的侵害其他人之資訊隱私權，並能調和資訊自主與資訊自由之要求，為今日重要的議題之一。

近年來由於醫療資訊數位化之發展，加以通訊科技日新月異與進步與網路傳輸普及，使得利用網路通訊技術進行的遠距醫療方興未艾，是未來趨勢。而高齡化社會到來，民眾普遍對於健康的概念愈

加重視，也對相關醫療服務的可及性、方便性及品質期盼愈高。電子病歷在目前我國電子簽章法的架構下，視為電子紀錄的一種應用形式。然而，對於電子紀錄的製作，其選擇權並非交由病患當事人選擇，而是由醫療院所決定，同時，在現行相關法律架構下，電子紀錄的管理與保護是否安全可靠，在尚有疑慮的情形下，如何克服管理與技術上的障礙，以兼顧保障當事人權益以及善用新科技便利性，遂成為今日健康資訊科技應用的主要衝擊與挑戰。為創造一個安全、可信任的電子病歷使用環境，未來應朝向健全的電子病歷管理制度，以及強化資訊安全與當事人隱私權保護的方向發展，以實現資訊科技帶來的利益，滿足人類醫療與照護的需求。

現今全球只有極少數國家針對醫療病例隱私保障訂立專法，而針對 E 化健康醫療照護而立法者更為罕見。此種情況對於利用資訊通訊技術來進行醫療照護發展有負面影響。因為未有專法出現，代表該國尚未就資訊隱私的個人利益及國家在收集、使用、儲存該些資訊的利益兩者之間找到一個平衡點。就現有資料觀之，未來主要國家以制訂特別法方式，規範醫療資訊隱私之保護，應為大勢所趨。

本文參照國外相關的經驗，並就台灣現行的法律規範與未來發展趨勢，提出以下建議，可以作為未來的研究方向：第一、建議制定醫療隱私保護專法，第二、提高民眾的醫療隱私資訊保護意識，第三、建構資訊安全管理制度，第四、資訊財產權體系的建立，第五、強化告知後同意的法律機制，第六、建議嚴格推動去識別化之法律規範。

參考文獻

1. 王俊文，我國憲法上隱私權相關問題之釐清，東吳法研論集，第 25 卷，頁 189- 228，2006 年。
2. 王澤鑑，人格權保護的課題與展望（三）－人格權的具體化及保護範圍（6)- 隱私權（上），台灣本土法學雜誌， 第 96 期， 頁 21- 44，2007 年。
3. 李震山，基因資訊利用與資訊隱私權之保障，收錄於《法治與現代行政法學－法治斌教授紀念論文集》，2004 年 5 月。
4. 林子儀，從保障隱私的觀點論基因資訊的利用與法的規制，載：基因科技與法律研討會論文集，學林文化事業有限公司，頁 264- 266，2003 年。
5. 宋珮珊，個人醫療隱私保護之立法趨勢研究 — 以美國、加拿大為例， 科技法律透析，2010 年 5 月，頁 44- 63。
6. 楊漢 ，電子病歷與病人隱私權保護，澄清醫護雜誌，第 8 卷第 1 期，2012 年。
7. 政府資料開放加值應用研究分析，行政院發展考核委員會委託研究報告，民國 102 年 12 月。
8. 美國政府公開資料加值推動現況與執行經驗，美國聯邦政府總務署，民國 101 年 1 月。
9. 國人健康醫療資料加值應用之法律授權疑義，立法院公聽會，102 年

12 月 10 日。
10. 開放資料及其對政府治理與個人隱私影響之研究，行政院國家發展委員會委託研究報告，104 年 2 月。
11. 電子病歷法規強化，衛生福利部委託科技研究報告，103 年 5 月
12. 陳仲嶙，醫療隱私的法規範現況，醫事法學，第 11 卷第 2 期，2003 年 6 月。
13. 張乃文、宋珮珊，各國個人醫療資訊隱私標準之法制研析，醫事法學，第 17 卷第 2 期，2010 年 6 月。
14. 劉宏恩，< 冰島設立全民醫療及基因資料庫之法律政策評析> ，收錄於《基因科技倫理與法律－生物醫學研究的自律、他律與國家規範》，2009 年 6 月。

電腦稽核
JOURNAL OF INFORMATION COMMUNICATION AND TECHNOLOGY AUDITING 第 38 期

外掛式資料查核及保護方案探討

Explore on the data inspection and protection by external method

洪長宏
PMP, CISA, CRISC
臺灣網路認證股份有限公司 內部稽核部 協理
rogerhong05@hotmail.com

摘　要

組織資料保護為所有企業的重要議題，但因資訊系統的採購及建置時間點與設計考量並非所有系統均具備資料保護機制及留下查核軌跡。

以查核及資料保護的角度而言，任何資訊系統都應該能被有效查核，其資料都應該被保護。針對無法提供查核軌跡或資料保護的（舊）資訊系統，亦應想盡辦法進行有效資料查核及資料保護，本文提供一個外掛式的解決方案，其能為資料查核及保護提供另一種考量面向。同時，本文所提供之方法也實際運用於舊系統（一個簽章驗證系統）的實作，確實達到資料查核及保護之目的。

關鍵詞：外掛式資料查核、ISO 27001

Abstract

Organizational data protection is an important issue for all enterprises. However, due to the procurement and construction time and design considerations of information systems, not all systems have data protection mechanisms and leave a audit track.

From the perspective of audit and data protection, any information system should be effectively audited and its information should be protected. For the (old) information system that cannot provide audit track or data protection, we should also try our best to conduct effective data audit and data protection. This paper provides an external solution, which can provide another consideration for data audit and protection. At the same time, the method provided in this paper is also applied to the implementation of the old system (a signature verification system), and indeed achieves the purpose of data audit and protection.

Keywords：Audit track, ISO 27001

壹、導論

在當今的企業裡，資訊系統已成為必備之生財及管理工具。資訊系統包含處理業務的運算邏輯及相關業務資料。此處，業務是指處理標的的通稱，以訂單系統而言，其業務處理即指訂單新增、修改、拋轉至其他系統等等處理；以出勤系統而言，其業務處理即是指員工的上下班、請假等等處理。

資訊系統在業務邏輯處理方面，基本上是遵循各項業務的作業程序書，故不太會有處理邏輯是否恰當的問題，而是當作業程序書變更時，資訊系統亦須隨之調整。所以，以版本管控讓作業程序與系統邏輯一致是資訊系統程式的控制重點（因為，資訊系統更新需要一些時程，通常會落後作業程序書一段時間）。

但在資訊系統的資料維護上，就顯得困難許多。此是因為一般作業程序書僅會描述業務處理邏輯，不會有資料維護邏輯，也不會有查核程序之故。所以在資訊系統開發的當時也僅會考慮業務需求而忽略資料查核及保護的需求，因此，理所當然的，無留下查核所需的作業軌跡。

在上述情況下，一般對資料的保護則是著重於資料的資安議題，即資料不被惡意竄改，資料不被洩漏等等；遵循的邏輯則是 ISO 27001 的通用規範。並且資訊系統一旦開發完成，上線營運之後，系統穩定度就成為維運者的首要任務，需求變更更要層層控管；在此狀況下，任何的查核需求變更大部分是不會被核准。

另外，在傳統及舊式的資訊系統中，資料查核及資料保護往往不在系統設計範圍之內，故內部稽核所要求的稽核紀錄或資料隱密之功能，當然不會建置在此系統之內。

故本文以在不修改原資訊系統的原則下，提出一種外掛式資料查核及保護的觀點與作法，期能突破現有巢臼，讓資料維護及其查核能有寬廣的空間。

貳、外掛式資料查核及保護作法

一、 假設條件

所謂查核，其實是在作業事後進行，故查核通常以查看各項紀錄為基準。當系統設計時，若無留下適當的稽核軌跡，顯然是無法有效的查核（例如，資料被異動 10 次，若無每次的異動紀錄，則查核時僅會看到現況結果）。

在原系統變更的困難下，以外掛式系統針對資料進行偵測及留下軌跡可以是一個有效的補強(補償)方式。此處，外掛式系統指的是非原資訊系統的新增獨立系統（以下稱外掛查核系統），以讀取原資料庫方式產製查核紀錄的系統。因獨立於原資訊系統之外，故不會干擾到原系統的運作，又因僅對原資料庫做唯讀的存取，因此，並不影響資料庫之資料正確性及維護作業。

當然，查核系統要能運作也是需要一些環境假設，對欲查核的資料表應具備有 1 個唯一鍵值（Unique key）。一般而言，重要的資料表均具備此項。

二、 外掛查核系統之主要處理邏輯

對於資料異動的保護，以積極角度而言著重在資料存取控制，無權者無法接觸資料，故可有效保護資料，其次，是對資料進行轉換（例如，加密），無權者無法窺視資料內容（資訊不外洩），但無法防止資訊被破壞（資料更動將導致無法還原）；在消極角度而言，則是資料有被異動，甚至是不當的篡改等均可被偵測找出，但亦無法還原資料（當然，資料備份是另一種資料還原運作方式，但是甚少有系統執行即時備份。目前，火熱的區塊鏈技術則是可以滿足此點要求（即時同步備份要求））。本文所討論的資料查核及保護，因著重在不更動原資訊系統，所以，僅討論資料的消極保護，即偵測出資料的異動。

本外掛查核系統的主要組成為一張簡易的外掛資料表再加上一個外掛程式，如下：

1. 外掛資料表

一個外掛資料表僅針對一個被保護或被查核的對象，該對象可以是獨立的一張資料表或視圖（ View）或由程式邏輯組合而成的資料組合。本資料表如表一，應有下列 6 個欄位：

表一：外掛資料表概觀

欄位 A	欄位 B	欄位 C	欄位 D	欄位 E	欄位 F

註：欄位 A 為本表之主鍵值，欄位 C 為次索引

(1) 原資訊系統唯一鍵值（稱為欄位 A）
(2) 該鍵值原紀錄之上次檢核值（稱為欄位 B）
(3) 檢核值的上次產製時間（稱為欄位 C）
(4) 該鍵值原紀錄之本次檢核值（稱為欄位 D）
(5) 檢核值的本次產製時間（稱為欄位 E）
(6) 異動註記（本次與上次之比較 ）（稱為欄位 F）

2. 外掛程式之運作邏輯

本程式主要為讀取原系統資料，製作檢核值並儲存，如同快照(Snapshot)的概念。本作業的啟動時機可以依據保護查核標的而異，可以是每日一次，也可以每小時一次。其處理邏輯如下：

對保護查核的資料表，逐一讀取每筆紀錄：

(1) 讀取原系統之資料記錄。

(2) 計算該筆紀錄之檢核值。檢核值計算方式可以採用計算押碼值（須金鑰）或計算雜湊值（無須金鑰），其採用方式依需求而定，一般狀況建議採用雜湊值即可（免去金鑰保存管理的麻煩，而且速度快），雜湊算法可採用 SHA- 256。

計算方式：首先，將該筆紀錄的所有欄位以二進位方式合併成一個位元組串流（Byte stream），再將該串流進行 SHA- 256 運算，取得雜湊結果（256 位元 = 32 位元組）。

(3) 若該紀錄是首次取得（不存在於外掛資料表），則將資料存入外掛資料表，對應如下：

欄位 A：原資訊系統唯一鍵值

欄位 B：本次取得的檢核值

欄位 C：現在時間

欄位 D：本次取得的檢核值

欄位 E：現在時間

欄位 F：異動註記為 0（無異動）

(4) 若該紀錄不是首次取得（已存在於外掛資料表），則將資料存入外掛資料表，對應如下：

欄位 D：本次取得的檢核值

欄位 E：現在時間

欄位 F：若欄位 B 與欄位 D 之值相同，異動註記為 0（無異動），否則設為 1（有異動）

三、 外掛查核系統之日常運作

因本系統屬於外掛系統，因此，無法取得原資訊系統的連動驅動（當然，可以設用原資料庫的觸發（Trigger），但這會影響到原資訊系統及原資料庫的效能及穩定性）。故，本系統採用輪詢(Polling)模式，每間隔 N 小時執行一次，其執行頻率則依原資訊系統資料表控制的需求而定。

外掛查核系統執行一次的作業程序如下：

1. 執行上述二、2 之外掛程式之運作邏輯。
2. 針對有異動者（即欄位 F 的值為 1），彙整其紀錄產製匯出報表給查核單位。
3. 針對有異動者（即異動註記值為 1），將本次的檢核值與時間複製至上次檢核值及時間欄位（即複製欄位 D 至欄位 B，複製欄位 E 至欄位 C），並將欄位 F 設為未異動（即值設為 0）。

當然，有了異動報表，就可以根據一段時間的蒐集來做查核數據分析，包括異動的頻率、異動的時間、異動次數等等。當然如果，可以參照原資訊系統其他資料的話，也可歸納出何謂正常異動、何謂異常異動。

俗語說：巧婦難為無米之炊。查核人員手上若無原資訊系統提供的查核或異動紀錄將會是沒有施力點；船過水無痕，很難有查核能力或是遏止不法的行徑。故，本系統提供一個外掛方式取得異動及查核紀錄。

四、 外掛查核系統之精進及演化

1. 運作的可能精進方式

在上述二中，所提之方法係針對被查核的資料表進行全表掃描，故其在執行效率上，較為不佳且耗資源，故僅能於離峰時間執行。

但若被查核之資料表具備異動時間欄位且為索引時，則可省卻上述二之流程，直接以異動時間欄位差異做出快照即可。如此，則快照樣本數可以增加。例如，每 30 分鐘偵測（ Polling）一次，且僅針對異動時間在 30 分鐘前的資料做異動比對紀錄。

2. 運作的可能演化

因個人資料保護的議題不斷的發酵，所以，個人資料的保護常常被提出來檢討。舊有的系統一般不太考慮個資隱密性的問題，就算是沒使用到也把資料明碼留在資料庫內。

針對一次使用的流水帳紀錄，也可以使用外掛系統進行資料加密，使其在資料庫內保持加密資料，當要進行過期資料備份時，再將其還原為原始明碼資料。因資料記錄是一次性使用，故於加密解密過程並不會與原資訊系統爭搶紀錄，也不會有不同系統因爭搶紀錄造成資料鎖死的狀況。

以簽章驗證系統為例：

- 其功能為提供其他系統呼叫，驗證資料簽章是否正確？
- 其輸入有原始資料、簽章憑證及簽章值。
- 其輸出為驗證結果（簽章正確與否）與驗證時間。
- 其運作為一次性執行，就算是後台查詢也只是驗證紀錄及結果查詢，不做驗證資料原始內容查詢。

簽章驗證系統的業務處理邏輯如下：

(1) 驗證簽章值正確性

將簽章值以簽章憑證之公鑰解密取得雜湊值 A；再以原始資料進行雜湊計算，得到雜湊值 B。若雜湊值 A 等於雜湊值 B，則簽章值正確。

(2) 驗證簽章憑證之正確性

檢查簽章憑證的效期及金鑰用途。

(3) 驗證簽章憑證之憑證鏈正確性檢查

簽章憑證所串接的每一張憑證，其效期及金鑰用途。

檢查其憑證鏈之根憑證是否為信賴根憑證之一。

(4) 驗證簽章憑證之憑證狀態正確性應至憑證管理中心（Certification Authority；CA）處，查詢是否憑證被廢止。

由上述業務邏輯可知，原始資料在簽章驗證過程中是必要的，但不解讀其資料意義，僅做為雜湊計算用途。所以，一般的簽章驗證系統並不會對驗證資料做任何處理，僅是存於資料庫內，作為日後有異議時判定之用。

什麼資料需要被簽章？當然是重要資料才需要做數位簽章。所以，驗證的原始資料內容通常含有個資或敏感性資料，該資料就會暴露在資料表中，增加洩漏的風險。因此，採取了外掛程式方式，定時將驗證的原始資料欄位進行資料加密，而資料加密的金鑰則存於硬體加密器（ HSM）中，確保加密資料的安全性。因本驗證系統含有驗證時間，所以可使用該時間做外掛加密程式的執行判別之用，可縮短執行間距（例如，每 30

分鐘執行一次)。如此，則可免除原始資料洩漏的風險，也可有效的保護原始資料。

參、結論

現今而言，資料保護的意識抬頭，尤其是個人資料保護更是受到個人資料保護法的保護，所以，對於個人資料或敏感資料應盡其所能的保護或查核。

我們無法以舊系統不提供查核紀錄或資料保護，來當作不進行資料保護或查核的藉口，只要資料有被篡改、被洩露將使企業遭受損失，甚至遭致刑責 (如個人資料保護法第 41 條、第 42 條)。

本外掛查核系統的方法論將是解決資訊系統不提供查核紀錄或資料保護的一個有效的解決方案並且實務運用於簽章驗證系統。

參考文獻

1. 法務部，2015，全國法規資料庫 - 個人資料保護法，取自 http://law.moj.gov.tw/Law/LawSearchResult.aspx?p=A&k 1=%E 5% 80% 8B%E 4%BA%BA%E 8%B 3% 87%E 6% 96% 99%E 4%BF% 9D%E 8%AD% B 7%E 6%B 3% 95&t=E 1F 1A 1&TPage= 1
2. ISO/IEC 27001: 2013, Information technology – Security techniques – Information security management systems - Requirements.
3. ISO/IEC 27002: 2013, Information technology – Security techniques – Code of practice for information security controls

電腦稽核
JOURNAL OF INFORMATION COMMUNICATION AND TECHNOLOGY AUDITING 第 38 期

以MitmProxy檢測分析手機應用程式之安全性

謝致宏
朝陽科技大學　資訊管理所　研究生
kevin94006@yahoo.com.tw

洪朝貴
朝陽科技大學 資訊管理系(所) 副教授
ckhung@cyut.edu.tw

摘　要

手機應用程式近幾年發展快速，各式各樣的應用程式可提供多元的服務，讓我們迅速掌握最新資訊，生活因此變得更加簡單方便，也帶來更多樂趣。開發人員不斷努力改善手機應用程式功能，使得這些應用程式佔據我們生活很大的一部分，但同時也衍生資料隱私問題。即使現在使用者比較有隱私意識，往往還是會點選任何在手機上出現的訊息，因為他們只想能夠儘快開始使用他們的手機軟體。

本文使用 Wireshark 來偵測與分類手機 APP 隱私洩漏，接著以 Mitmproxy 中間人代理伺服器分析手機 App 發送之 HTTP(S) 網路封包內容，監測這些手機 App 是否在使用者未授權情況下擅自傳送資料封包給伺服器，並進一步觀察這些 App 傳送的封包是否含有不該取得之資料。

關鍵詞：手機 App、隱私洩漏、封包分析

Abstract

Mobile applications have developed rapidly in recent years. A wide variety of applications can help us organize our work, let us see all the latest information at a glance. So life becomes easier and more fun. Developers are working to improve their mobile applications constantly, making these applications occupy a large part of our lives.

However, the issue of data privacy has also emerged, and it has become a hot topic of discussion. Even everyone has become conscious of privacy, many users often click on any message that appears on their phone because they only want to be able to start using their phone software as soon as possible.

In this paper, we use wireshark to detect and classify the privacy risks of mobile applications. Then, we use Mitmprox (man-in-the-middle) to analyze HTTP (S) packets sent by the mobile applicatinons, monitoring whether these mobile apps send data to the server without the user's authorization. And observe whether packets sent by these Apps contain information that should not be obtained.

Keywords：Mobile apps, Privacy leak, Packet analysis

壹、前言

隨著科技進步，智慧型手機及平板電腦普及，正在改變民眾的生活習慣。行動上網技術的進步，人們可以隨時隨地上網，但在方便之餘，也衍生許多資訊安全的問題。近期部分智慧型手機或是 App 紛紛傳出內含程式漏洞，讓原廠或有心人士可透過一些方法取得使用者個資，或是直接將數據回傳至外部伺服器。由於大部分使用者並不具備資訊相關專長，無法輕易從程式看出有心廠商所做的手腳。資訊不對等，加上對於網路資安觀念的錯誤認知，造成人心惶惶，深怕不小心就讓身家背景全都露。

美國資安公司 Kryptowire 在 2016 年發現，總計有 7 億支 Android 手機的資料，會將用戶所發送之簡訊與通話紀錄透過後門發送到大陸某公司的伺服器內。市面上有多款 Android 手機會在未詢問用戶的同意下，直接把手機的資料傳給第三方伺服器，包括「簡訊、聯絡人、通話紀錄、GPS 位置 」等。在手機安裝 App 或存取重要資料前，真的要越來越小心，因為永遠不知道有誰會拿走你的資料，做出會傷害你的行為。

便捷的 App 商店讓使用者可以輕鬆安裝應用程式，也能享受各種即時服務，但使用者對於應用程式的安全性並不完全了解，不知道這些 App 是否私下傳出手機內個人或隱私資料。本文探討手機應用程式可能對使用者資料造成洩漏的行為，並且使用兩種封包分析檢測軟體來監測 Apps 傳輸之封包內容，嘗試抓包這些 Apps 是否在未經使用者授權情況下，就取得使用者個資甚至將這些個資傳送到外部伺服器，以增進使用者對於 Apps 洩漏手機資料風險之瞭解。

貳、研究架構與工具介紹

首先執行欲抓取封包之手機 Apps，透過 Wireshark 的監控，只要是傳送網路封包都會被記錄。倘若 Apps 使用 HTTP 協定，繼續使用 Wireshark 來檢視該 App 是否傳送手機個資並分析其正當性；如果 App 使用的

是 HTTPS 協定，則改以 Mitmproxy 分析這些網路封包傳輸資料之正當性。判斷的依據是這些 HTTP / HTTPS 封包傳輸之資料是否為使用者授權存取的，若是授權存取的資料顯示在封包內，就歸類成是正常存取並記錄結果，反之則歸類為可疑或非正當存取。最後將這些結果統整為表格並作出結論，研究架構如圖 1 所示。

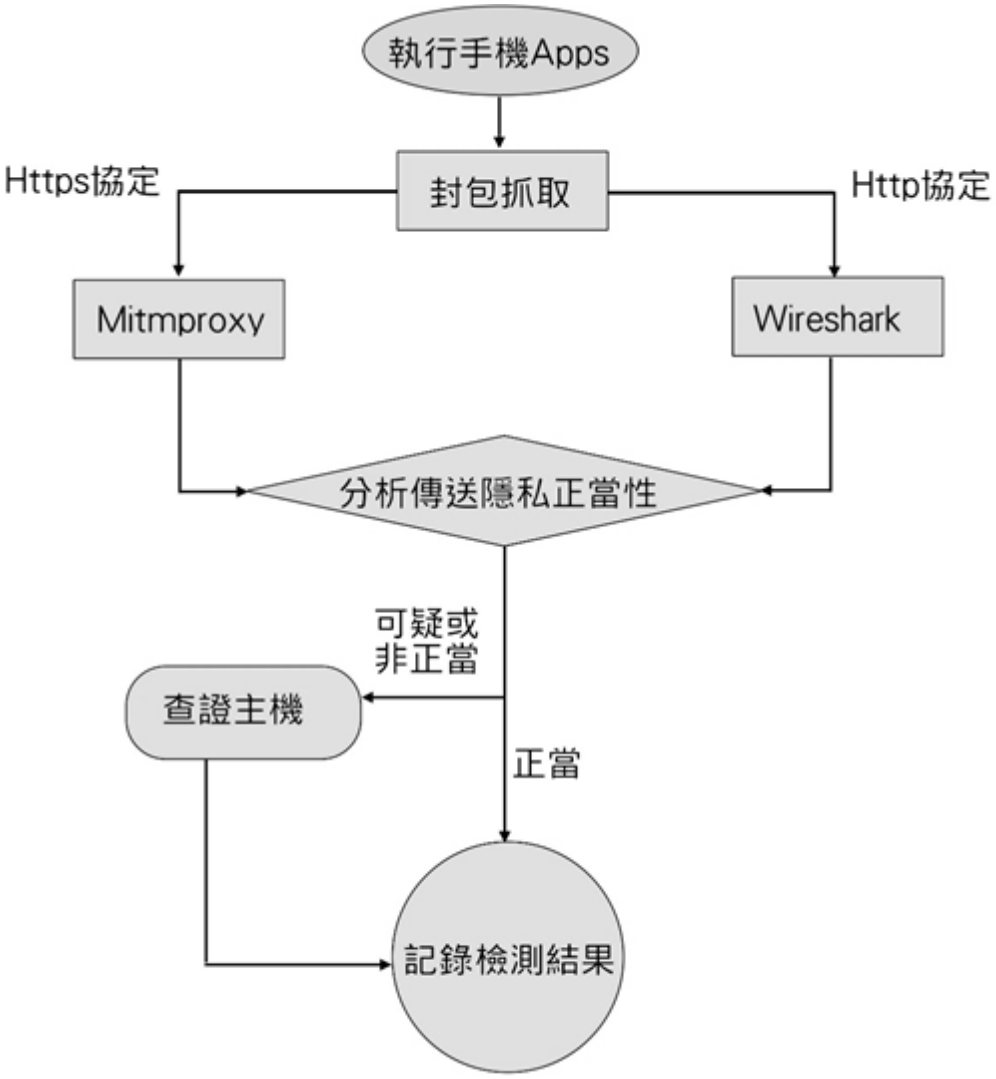


圖 1 研究架構圖

Mitmproxy 是一個開源代理應用程式，這個工具允許使用典型的中間人攻擊（ MITM）攔截任何 HTTP/HTTPS 用戶端（例如行動或桌面瀏覽器）及 Web 伺服器之間的 HTTP 和 HTTPS 連接。與其他代理伺服器例如 Squid 類似，Mitmproxy 接受來自用戶端的連接並將其轉發到目標伺服器，但其他代理伺服器通常是透過快取來做

內容過濾或者速度優化，而中間人的目標是能夠監控、抓取和更改這些網路連接。

Mitmproxy 原始的概念是假裝成發送回應 / 請求給用戶端的伺服器端，並且假裝成發送回應 / 請求給伺服器端的用戶端，而 Mitmproxy 實際上則是在中間解碼雙方的流量。比較棘手的部分是憑證授權單位（CA），數位憑證用於確認個人、電腦與網路上其他實體之身分的電子認證，由憑證授權單位 (CA) 所發行。此數位憑證功能類似護照或駕照，可用於證明身分，憑證授權單位必須在發行憑證前及憑證持有者使用憑證時驗證其身分。如果此簽章不匹配或來自不可信任方，則用戶端將停止該連接並拒絕繼續連接。Mitmproxy 可以即時產生攔截封包的憑證，為了讓用戶端的手機 Apps 信任這些數位憑證，需要手動將 Mitmproxy 註冊為欲監測手機的可信任 CA，如圖 2 所示。

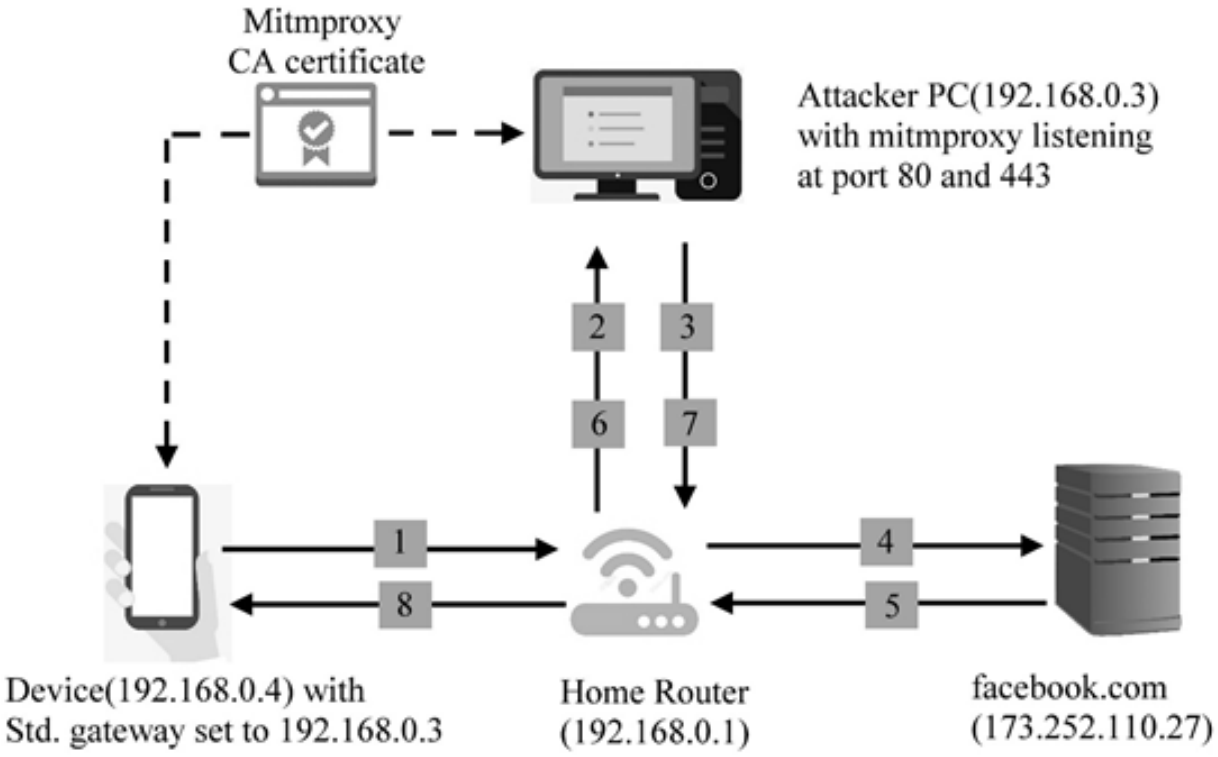


圖 2 Mitmproxy 扮演中間人

參、系統實作

一、安裝 Mitmproxy

Mitmproxy 的安裝非常簡單，因為是使用 Python 軟體打包管理系統（Pip）所打包的。其他的 Mitmproxy 依賴包則可以用 Apt-get 來安裝，以下為安裝 Mitmproxy 主程式與相關依賴包的指令。

```
1.sudo apt-get install python 3-dev python 3-pip libffi-dev libssl-dev  # 安裝 mitmproxy 依賴包
2.sudo pip 3 install mitmproxy  # 安裝 mitmproxy 主程式
```

二、啟用 IP 轉發和通訊埠重導向

Mitmproxy 應用程式內部在 TCP port 8080 上運行，但外部必須監聽 Port 80/HTTP 和 Port443/HTTPS。 因此，若要監聽被送來的 IP 封包，IP 轉發（系統充當路由器）以及從 Port 8080 到 80、443 的重新導向都是必要的預先準備工作

```
1.sysctl -w net.ipv 4.ip_forward= 1  # 開啟 IP 轉發
2.iptables -t nat -A PREROUTING -i eth 0 -p tcp --dport 80 -j REDIRECT --to-port 8080
3.iptables -t nat -A PREROUTING -i eth 0 -p tcp --dport 443 -j REDIRECT --to-port 8080
```

三、執行 Mitmproxy

如上所述，Mitmproxy 運行在 Port 8080 上，但同時也需要綁定 80 和 443，所以這三個 Port 不能同時被任何其他應用程式使用，需要停止任何可能占用這些 Port（Apache web 伺服器，Tomcat 等）的程式。如果不確定是否有其他軟體用到這三個 Port，可以用 Netstat-ntap 指令查看。接下來就開始執行 Mitmproxy，為了要正確地啟動 Mitmproxy，輸入此指令：Mitmproxy -T --host 來執行 Mitmproxy。

四、觀察可疑 App 之封包內容

本文從 Google play 商店的熱門下載榜，及揭露可疑軟體名單的網站挑選了幾款 Apps 做檢測，其中會挑選較多拍攝 Apps 的原因是近幾年直播平台及社群平台使用者數量迅速增加，也因此讓多款攝錄與編修 Apps 快速攀升到熱門 Apps 排行榜。

知名的來電辨識 App---Whoscall 在 2015 年 9 月 2 日 波卡搶購事件後，於 FB 官方粉絲頁公開一些統計數據，等於自己暴露會記錄用戶撥出的電話。 一名網友在 FB 貼文指出「何時在哪打電話給誰、當下網路環境、手機型號、對方有沒有接他全部記錄」都會傳送資料到 gga.whoscall.com。Whoscall 是知名的來電辨識 App，運用社群回報、演算法及比對雲端資料庫，讓使用者接到未知來電時，可以知道對方身份，判斷是否為詐騙電話或推銷電話，而因為公布了這組數字，意外讓網友驚覺，原來 Whoscall 會記錄使用者打出去的電話，並且記錄時間地點等詳細資訊。後來做了一些測試發現，在被網友怒喊拒絕使用後，Whoscall 似乎已經不再傳送資料到他們的伺服器。

我們從揭露可疑軟體名單的網站發現了一款類似 Whoscall 的辨識來電號碼 App - Truecaller，就下載安裝來檢視其傳送的封包內容。結果發現此 App 會在背景傳送出我的通訊錄資料，使用者安裝此 App 的用意

是不想接到騷擾電話或是詐騙電話，但 Truecaller 居然重蹈當年 Whoscall 的錯誤，會將使用者手機的通訊錄資料傳出（如圖 3）。


```
[
    {
        "CONTACT_ID": "BEC810F62A07E493EEC261AAADF0A1DA",
        "TEL_CELL": [
            "0988 123 456"
        ]
    },
    {
        "CONTACT_ID": "5177E4821F3F1352D3FD96CFCD56D150",
        "TEL_CELL": [
            "0966 123 456"
        ]
    },
    {
        "CONTACT_ID": "30718F8E39E69F575EF1DAC720D1F4A9",
        "TEL_CELL": [
            "0922 123 456"
        ]
    },
    {
        "CONTACT_ID": "50B1C831828BAC660AFD9BA5D3368C6E",
        "TEL_CELL": [
            "0911 123 456"
        ]
    },
    {
        "CONTACT_ID": "754747A8245DAAD94EC0F4BE84998052",
        "TEL_CELL": [
            "0977 123 456"
        ]
    },
    {
        "CONTACT_ID": "0B0449640CA08170AA514A6BDDAAE05B",
        "TEL_CELL": [
            "0900 123 456"
        ]
    }
]
```


圖 3 Truecaller 傳出使用者通訊錄資料

備註：為了方便解析封包內容，所以將通訊錄號碼以數字 123456 結尾。

近幾年很流行將拍攝創作的照片或影片編修後，上傳到網路社群或是分享給朋友。我們從可疑軟體名單的網站內安裝一款影片編修 App - 小影，安裝完成開啟後發現有一些資料被傳出去了，查看封包內容發現它傳送了我當下所在的經緯度位置且是正確的，我還沒使用此 App 的編修功能，竟然就暴露了我的 GPS 位置，且一款影片編修 App 怎麼會要知道使用者的所在位置，令人不得其解。

"area":" 台　",
"country":" 中国 ",
"city":" 台中市 ",
"latitude":" 120. 6736482",
"ip":" 122. 118. 216. 99",
"area_id":" 710300",
"country_id":"TW",
"longitude":" 24. 1477358"

這個 App 接著傳出我的一些手機資訊，包含網卡號碼、手機型號、目前使用的連線類型、作業系統等。用來剪輯影片的 App 竟會擅自傳輸使用者的手機資訊到軟體公司的伺服器，包含網卡號碼與聯網類型。

l= 201805241352012
a=de
i={
"a":"[A]ffffffff-ca 50-c 9be-d 851- 1bf 023596b 1b",
"b":"Android",
"c":" 5. 0",
"e":" 1C: 99: 4C:B 0:B 9: 55",
"f":"XYI 5e 148da 7-fa 36- 4771- 875b- 67605bf 6cbc 7",
"g":"SGH-N 075T",
"h":" 000000",
"i":"WIFI"
}
n=TW
b= 2. 0
c= 10008301

最後試著用小影這款影片編輯軟體，將相簿中的數張照片輸出為一個影片檔，影片輸出完成後，發現有幾個封包被送出。一一檢視這幾個封包內容，發現有一個副檔名是 "MP 4" 結尾的封包字串，覺得不對勁立刻查看剛剛輸出的影片檔名，正是封包內容所呈現的檔名，我只是將照片做成一個影片檔，而這個影片的資料竟然就被封包發送出去。

a= 558or
i=http://v-slideplus-sg.xiaoying.tv/ 20180614/ 558or/ 35fCUh 662.mp 4
b= 1
c=zef 8U
g= 5fCUh
e= 3e 436fc 9a 8b 8b 4c 698154c 8dbdb 6382c
d=SlidePlus_Video_ 1528956461900.mp 4
f= 3
h= 20180614/ 558or/ 35fCUh 662.mp 4

最後將所測試的幾個熱門 Apps 傳出之使用者資料整理如表所示。

表 1 手機 Apps 傳送之使用者資料檢測結果

測試項目 測試樣本	背景傳資料	封包內含之使用者資料			
		GPS	媒體資料		通訊錄
			照片	影片	
美圖秀秀	△	○			
Camera 360	△		○		
17 直播		○			
小影	△	○		○	
Truecaller	△				○
雙鐵時刻表		○			
KKBOX	△	○			
Garena 競時通	△				○

備註：

△表示該 App 會在未開啟狀態下發送手機資料

○表示該使用者資料被 App 傳出

每支 Android 的 Apps 下載安裝時，系統會提示你該 App 會取得哪些手機資料存取權限，但是大部分的使用者應該連看都沒看就按「接受」，反正都要使用該 App，看不看也沒差，就授權讓 Apps 讀取手機資料。

本文檢測發現有一些 App 會在使用者沒開啟該程式就自動傳出手機資料，舉如美圖秀秀會在背景發送手機的 IMEI 與 MAC address，但是美圖秀秀是一個拍照及修圖功能的軟體，讀取手機的這兩種資料的用意為何？讓人不解，並非沒有網路的狀態下就不能拍照及修圖。此外，小影這款 App 會在使用者編修完影片後，將影片相關資料上傳到網路，倘若使用者只是想存在手機內自己觀看，又或者是用來編輯不能公開的私密照片，在挑選 App 時真的要特別小心。

肆、結語

隨著網路技術的快速發展，手機上網的安全性已經成為大家關注的焦點問題。很多網站和手機 APP 會在用戶未知情的情況下，將用戶的隱私資訊傳遞出去，檢測和分析這種隱蔽通信，對於提高用戶的安全意識和採取進一步的應對措施具有重要意義。本文以 Wireshark 初步檢測出手機 Apps 是否傳送手機隱私資料，以及驗證封包回傳主機之合理性，接著使用 Mitmproxy 進一步監測 HTTP 和 HTTPS 的封包，詳細分析封包傳輸內容後，發現有部分 Apps 未經使用者授權，就將隱私資料傳出，甚至在未開啟該 App 時，也會擅自在背景傳輸資料。

市面上有多款手機 Apps 會在未詢問用戶同意下，直接把手機的資料傳給第三方伺服器。另外使用者在下載 Apps 時會跳出要求的權限，多數人都直接按同意，這就是個資曝露的開始。在安裝 Apps 或存取重要資料到手機前，真的要越來越小心，因為永遠

不知道有誰會拿我們的資料，做出會傷害我們的行為。本文實作之步驟與分析，希望能廣泛地應用在其他手機應用程式對隱私資料之存取權做進一步的管控。未經授權的手機資訊就不應該被 Apps 請求存取且傳出，更不應該在使用者沒有開啟 Apps 的情況下在背景執行資料傳輸；使用者提供任何存取權給應用程式之前，也得認真考慮這些 Apps 是否值得信賴去交付自己的資訊。遊戲軟體只為了要聯絡你的朋友一起共玩或分享分數成就，就需要存取你的社群網路帳號資料？使用者不需要因為 Apps 會要求存取手機資料，就放棄使用 Apps 提供的便捷服務，但應該要了解相關的風險，例如較為隱私的資料可能會外洩。因此建議使用者在安裝 Apps 之前，想清楚所得到的服務是否值得承擔這些風險。

參考文獻

1. 孔鴻濱、梅芳、薛崗，(2016)，「檢測分析隱蔽 HTTP ／ HTTPS 通信流量的方法及實現 」，雲南大學學報，第 56- 60 頁。
2. 張瑋倫 (2016 年 11 月 17 日)。 你的手機可能也中標了，全球 7 億支 Android 資料外洩到中國。科技報橘。檢自：

   https://buzzorange.com/techorange/ 2016/ 11/ 17/ 7-hundred-million-android-cell-phone-has-been-monitored/
3. 鳥哥的 Linux 私房菜 (2003)。網路概念。檢自：

   http://linux.vbird.org/linux_server/ 0110network_basic.php
4. 資安趨勢部落格 (2012)。你沒被告知的手機程式與資料外洩，檢自：https://blog.trendmicro.com.tw/?p= 1333
5. 盧永山 (2016 年 11 月 17 日)。中國藏「後門 」7 億 Android 手機遭監控。自由時報。檢自：http://news.ltn.com.tw/news/focus/paper/ 1052982
6. 謝宜蓁 (2014)，Android 應用程式安全性分析—以雲端資料櫃 App 為例，碩士論文，國防大學管理學院資訊管理學系碩士班，第 9- 13 頁。
7. iThome(2014)。HTTPS 網站居主流，資安重新定義。檢自：

   https://www.ithome.com.tw/tech/ 93108
8. Mitmproxy(2016). MitmProxy Docs. Retrieved from http://docs.mitmproxy.org/en/latest/mitmproxy.html. iThome(2014)。HTTPS 網站居主流，資安重新定義。檢自：

   https://www.ithome.com.tw/tech/ 93108
9. Tim Bray(2012, November 14). Re：What Android Is [Web log post]. Retrieved from http://www.tbray.org/ongoing/When/ 201x/ 2010/ 11/ 14/What-Android-Is
10. Karan Kumar(2015, January 22). Re：MITM Tools [Web log post]. Retrieved from http://karankumar.co.uk/ 2017/ 04/ 17/mitmproxy-mitm/
11. CloudShark(2017, June 29). Re：What can I do with my Aerohive captures once they are in CloudShark? [Web log post]. Retrieved from

    https://support.cloudshark.org/user-guide/https-interception.html

12. Philipp C. Heckel (2013, July 01). Re：How To: Use mitmproxy to read and modify HTTPS traffic[Web log post]. Retrieved from

https://blog.heckel.xyz/ 2013/ 07/ 01/how-to-use-mitmproxy-to-read-and-modify-https-traffic-of-your-phone/

13. Leavitt and N.(2013),“Today’s Mobile Security Requires a New Approach”, IEEE Computer Society (46: 11), pp. 16- 19.

電腦稽核
JOURNAL OF INFORMATION COMMUNICATION AND TECHNOLOGY AUDITING 第 38 期

Location-based Privacy: Problems Analysis and Protection

Daniel W.K. TSE
City University of Hong Kong

MO Chaoxun
City University of Hong Kong

ZHU Bihui
City University of Hong Kong

WANG Yukun
City University of Hong Kong

Abstract

The rapid development of mobile communication and mobile localization technology has created a new research area - Location-Based Services (LBS). Nowadays, the widely use of LBS increases the importance of location privacy protection. At present, researches on privacy protection in LBS have achieved certain results. However, in LBS, the quality of service and the privacy of users are contradictory, how to better balance the contradiction between them is the emphasis for research. Therefore, location privacy protection in LBS not only lays emphasis on how to protect the privacy of users but also a series of relevant issues brought by privacy protection. Thus, the best approach for such research is to investigate the nature of location privacy problems before relevant protection solutions are derived.

Keywords: Location-based service, Privacy protection, Location-aware location privacy protection, Anonymization, K-anonymity, NN query

1. Introduction

The rapid development of wireless communication and mobile database technology boosts the need of mobile users checking any information anytime and anywhere becomes true. The relevant development of location detection equipment (such as portable phone, GPS and RFID) provokes a new research area – Location-Based Services (LBS). LBS require users to provide their location information to LBS server when sending service request to LBS server. The server then provides the search based on location sent by users. LBS make the mobile users able to gain the service information related to its location.

Although the LBS and location technology provide users much convenience, LBS server needs to obtain the user's location information before it can provide the corresponding services to mobile users. However, LBS system cannot guarantee that the server would not leak or use the user's location information illegitimately. In other words, LBS bring the great challenge to the location privacy protection of users. In this information explosion era, data have become one of the critical resources. The emergence of the methods of large amount of data access, sharing and extracting information from data makes users pay more attention to privacy protection. Users need to gain the high-quality service under the premise of keeping the privacy information safe. In LBS, users expose their accurate location information to the server and such information severely affects the users' location privacy.

In this paper, the nature of various problems of location privacy is analyzed first. Different methods for current location privacy protection are then discussed.

2. Literature Review

Gruteser, M. and Liu, X. (2004) proposed a novel sliding window strategy based on the power spectrum analysis for the accurate location of eukaryotic coding regions. The proposed sliding window strategy was very simple and the sliding step of window was changeable. Their tests showed that the average location error for the novel method was 12 bases. Compared with the previous location error of 54 bases using the fixed sliding step, the novel sliding window strategy increased the location accuracy greatly. Besides, the consumed CPU time to run the novel strategy was much shorter than the strategy of the fixed-length sliding step. Thus, the computational complexity for the novel method reduces greatly.

Spatil and Sutar (2015) mentioned that various services are available to us by just one click on our mobile devices. One such service is Location-Based Service .User sends the query to service provider to get services like nearby restaurant, friends in vicinity, shared his/her location with other friends, rendezvous point to meet, etc. There are various threats

to privacy when user shared his/her location. The information could be misused for stalking, home invasion, political loss, etc.

3. The Analysis and Discussion of Location-based Services Privacy Problems

Location is very important for the future of mobility world. It creates a new social association layer that adds us to the background of posts, photos and helps us to discover the world around us. The success of the LBS industry depends on the public who are willing to use location-based services that also increase the security risks.

Deloitte (2017) released that nowadays tens of thousands of applications are developed for smartphone location capabilities, and 74 percent of US smartphone users use their phones to access real-time location-based information. Also in 2010, over 2. 5 billion photos were uploaded to Facebook in a single month and many individuals in these photos have been identified and tracked by facial recognition software. In addition, the rise of cloud computing has made storage of large amounts of data available to nearly everyone. As there are more and more LBS users, this motivates more criminals steal user information for commercial or illegal use. Every year, tens of thousands of people are affected because of privacy leaks. Sometimes, such privacy leaks may be used as forgery for illegal acts.

The following is an example illustrating the impact of privacy problem. Assume a user uses the phone with GPS function to find the nearest bank from where she is now. This is a common nearest neighbor query (NN queries) in the navigation system. This query is sent to the service provider, for instance Google Maps. The greatest privacy threat of using location-based services is the privacy leak. In other words, exposure to the user's location and the knowledge of the user's location is subject to time and space-related reasoning attacks, e.g. inference attack. Similar to the above example, another user may not want to let people know where she is now (e.g. hospital). Besides, this user may not want to let anyone know that she has made a certain aspect of the query similar to the first user who does not want to let people know that she will go to the bank to carry out some kinds of transaction.

In fact, location privacy is a kind of special information privacy. Information privacy is defined by an individual, an institution or an organization, when, where, and in what way to share information with others, as well as the contents of shared information. The location privacy is to prevent other people from learning about the past, and now the location of the object (e.g. the path walked regularly), the walk frequency, user's interests (like the preferred store, preferred club, preferred clinic, etc.) and other privacy information. While the threat of location privacy refers to the attacker in case of unauthorized access to the location of the original data, the use of transmission

equipment, eavesdropping on location information of transmission channel, etc.

Location information is about personal privacy, access to computing and reasoning. For example, the location information can help spreading malicious advertisements to users gaining access to medical conditions, lifestyle or political views. It can also be used to find out the location of the user who has visited which hospital, in which the entertainment center and so on. There are three ways to leak location privacy: The first way is via direct communication. It refers to the attacker who gets the user's location information from the location of the device or directly from the location of the server. The second way is through observation. It refers to attackers getting information directly by observing the behavior of object. The third way is through link attack. It refers to the attacker connecting external data sources or background knowledge through the location to determine the location.

From the above, we can come up with two main aspects of work to protect privacy. First aspect is location anonymization. Anonymous method (Mokbel 2006) is about separating user's information (such as location information) from user's real ID information. Anonymous refers to a state, which is composed of a collection of many objects. It is hard to distinguish every single object of the collection from external to inside and thus this collection is called anonymous set. Location anonymization refers to the system making sure that random location information cannot match to a specific individual, organization or institution by inference attack. The location of the LBS in the anonymous processing requires a certain means to handle user's location, making the individual location not able to be identified. Second aspect is in the LBS system inquiry processing. The location information is not processed by the user's real position. It may be a set of multiple locations or a fuzzy (obfuscation) location. Therefore, at the location of the server, the query processor cannot continue to use the traditional mobile object database query processing because the latter technology is based on the exact location information. It can be improved and modified based on the original technology, thus it can adapt to the new requirements of the query processing.

4. Protection Solutions to Location-based Services Privacy Problems

Location privacy protection is the ability to prevent other individuals or groups from knowing the location of a user's current or past. Location privacy information is composed of identification information and location information. A static attribute or characteristic of a user is used to uniquely identify a user. Location information describes the whereabouts of an individual or group. The traditional location privacy protection method

is mainly based on the two types of information that constitute the location privacy information. First method is to provide accurate location information of user to the server in order to obtain high quality information service and hide user's ID information (such as anonymous, false name etc.). Another method is to expose user's ID information completely to the server and hide user's location information in order to achieve the purpose of location privacy protection.

Mokbel, Chow and Aref (2007) described the location relationship between service / location privacy and the two types of privacy protection methods. The location of k-proposed anonymity technology mentioned by Mokbel and Aref (2007) is the first method to address the issue of privacy protection. The main idea of the method is to have k users at a certain location that users cannot identify each other by ID. Therefore, even if a malicious attacker acquires the location information of a user, the malicious attacker cannot accurately locate the user from k users. Fake name is a special type of anonymous method that user uses a fake name to hide ID. A malicious attacker may get accurate location information of users from the server but he cannot accurately connect location information using the user's real ID information, thus increasing difficulty of positioning, eventually achieving the purpose of protecting user's privacy location. Beresford and Stajano (2003) proposed an important identity protection method called the mix zone. This method defines two types of zone: using zone and mix zone. Both zones are space zone. In using zone, user can require service and receive service messages. In mix zone, user does not have communication. This method effectively uses fake name and better protect privacy location information. User has a time limit of using a fake name. For example, user should use a fake name before getting in mix zone and use another fake name after getting off mix zone. Because the user does not have any communication in the mix zone, it increases the difficulty of connecting fake name before and after the same user uses pseudonyms associated with protecting ID information.

Although anonymous and fake name is an important technology to hide user's real ID information, this method has some defects especially in space application area.

In order to get target information from a large amount of information, the data mining technology has been fully developed. Using data mining technology can easily figure out user's ID information from accurate location information. It is a big threat to anonymous and fake name technology. Besides, anonymous method has a troublesome ID authentication and personalization processes that are important in many applications. Anonymous technology does not provide adequate location privacy protection. Thus, anonymous name is not the best choice for location privacy protection.

On the contrary, location information protection method becomes more popular.

This method allows server to know the real ID information of users, achieving the purpose of location privacy protection by reducing the accuracy of user location information. Location privacy protection can be broadly divided into 3 categories. The first one is the False Location information: User sends various location information to server and only one such information can get the real location. Therefore, even if malicious attacker obtains the location information of a user on the server, he also cannot accurately figure out the user's exact location based on the location of those information. On the other hand, because each user provides multiple location information to the server leading to space overhead and increasing the server processing service request time, the mobile clients have to judge the accuracy of the information service.

The second one is Landmark Object: User sends to server a landmark location or an important object location instead of its real location. Although this method protects the user's location privacy, it needs the service information returned from the server to determine which information is interesting, thus increasing the workload of the mobile client.

The third one is Regionalization Location information: The main idea is to replace the user's accurate location with a spatial region containing the user's exact location. The space area can be constructed according to the idea of k-anonymity. For example, the location of the user provided to the server requires not only the location of the user's accurate location but also the region containing at least k mobile users. The disadvantage of this approach is that the quality of service will be greatly reduced. In addition, since the server does not know the position of user in the region, the server must select the position in the region as the reference point for query processing, selecting the number of reference points for query processing which can make more information that is accurate back to the service user. This increases the server's workload and the server's response time.

Duckham and Kulik (2005) proposed obfuscation as a mechanism for location privacy protection and proposed an algorithm that would not reduce the service quality according to the location information. This can effectively balance the contradiction between the location privacy protection and the quality of service. Obfuscation allows server know user's real information and reduce the accuracy of location information to protect location privacy. On the other hand, obfuscation does not require any centralized server as a location-based agent that is suitable for distributed environment, like peer-to-peer system.

However, the above location privacy studies focuses on hiding individual user's location information. Although these techniques are valuable in small-scale LBS, the value of the application on the actual location-based database server is questionable. These techniques lack two main properties: The first one is scalability. In a typical location based

service application, there are a large number of concurrent users, so the location privacy protection technology must be scalable. The second one is query processing. In order to protect user location privacy, the location-based database server cannot obtain the user accurate location information. Therefore, the server must provide efficient query processing based on user's fuzzy location information. This is a challenge for traditional query processing.

Mokbel (2006) proposed a method that can handle a large number of concurrent user's location privacy protection. This method combined the two methods of k-anonymity and regional position information and introduced a third party location anonymity. At the same time, in the server side, set up a query processor that can process the spatial area and the spatial region of the server, the candidate set of the query result is returned to the user. The method ensures that the result set returned to the user is as small as possible and contains information that the user is interested in. Although the proposed method is to solve the problem of location privacy protection, it also puts forward stricter requirements on the server processing capacity. On the other hand, the mobile user service request location will change over time. With the change of user's location service information, it also should make corresponding changes. Real-time service information is also an important measure of the quality of service based on the standard location. Therefore, server needs to have real-time ability and can adapt to the location of the service request. Using location information protection method is to realize user location privacy protection and making sure that the location information stored on the server is inaccurate data. How to query these data rapidly and accurately is another important issue in the field of location privacy protection. In the location-based service system, it is not only needed to provide privacy protection to the user's location information but also needed to provide users with accurate and efficient service.

5. Conclusion

After analyzing the nature of location privacy problems, this paper review methods and techniques of location-based services privacy protection based on location services. Besides, this paper summarizes the research methods of location privacy and the associated problems. With the further improvement of wireless communication and mobile technology, users will put forward stricter requirements on the location-based quality of service. At the same time, users will also pay more attention to the privacy issues that will bring new challenges to the location-based privacy research. Existing technologies (such as anonymous communication, etc.) will not be able to solve the complex problem. Thus, we need to put forward some better methods for the location-based privacy protection and technology.

Reference

1. Bamba B, Liu L. Privacy Grid (2007): supporting anonymous location queries in mobile environments[R]. Georgia Institute of Technology.
2. Bereford, Stajano (2003) ‘Location privacy in pervasive computing’, Pervasive Computing, IEEE CS and IEEE Communications Society, pp 46- 55.
3. Chow, C.Y., Mokbel, M.F. and Aref, W.G. (2009) ‘Casper*’, ACM Transactions on Database Systems, 34(4), pp. 1– 48. doi: 10. 1145/ 1620585. 1620591.
4. Chow, C.Y. and Mokbel, M.F. (2011) ‘Trajectory privacy in location-based services and data publication’, ACM SIGKDD Explorations Newsletter, 13(1), p. 19. doi: 10. 1145/ 2031331. 2031335.
5. Coppens, P., Veeckman, C. and Claeys, L. (2015) ‘Privacy in location-based social networks: Privacy scripts & user practices’, Journal of Location Based Services, 9(1), pp. 1– 15.
6. Deloitte, ‘2017 Global Mobile Consumer Survey: The dawn of next era in mobile’, Deloitte Consulting
7. Duckham, Kulik (2005) ‘A Formal Model of Obfuscation and Negotiation for Location Privacy’, Pervasive Computing, Springer, pp 152- 170.
8. Gruteser, M. and Liu, X. (2004) ‘Protecting privacy in continuous location-tracking applications’, IEEE Security & Privacy Magazine, 2(2), pp. 28– 34.
9. Mokbel M F. (2006) Towards Privacy-aware Location-based Database Services Proceedings of the 22nd International Conference on Data Engineering Workshops.
10. Mokbel M F, Chow Chi-Yin, Aref W G. (2006) The New Casper: Query Processing for Location Services Without Compromising Privacy Proceedings of the International Conference on Very Large Data Bases. VLDB, pp. 763- 774
11. Mokbel M F, Chow C, Aref W G. (2007) The new casper:a privacy- aware location - based database server [C]Proceedings of the International Conference on Data Engineering（ ICDE’ 07）,Istanbul, Turkey.
12. Rowan, T. (2010) ‘Negotiating WiFi security’, Network Security, 2010(2), pp. 8– 12. doi: 10. 1016/s 1353- 4858(10) 70024- 6.
13. Slee, T. (2011) Data Anonymization and re-identification: Some basics of data privacy. Available at: http://tomslee. net/ 2011/ 09/data-anonymization-and-re-identification-some-basics-of-data-privacy. html (Accessed: 12 November 2016).
14. Spatil, M. and Sutar, S. (2015) ‘Survey on location privacy in location based services’, International Journal of Science and Research (IJSR), 4(12), pp. 2170– 2173.

電腦稽核
JOURNAL OF INFORMATION COMMUNICATION AND TECHNOLOGY AUDITING 第 38 期

歐盟GDPR與個人資料保護認證

EU GDPR and the Certification

廖緯民*

國立中興大學法律系專任副教授

wmliao@dragon.nchu.edu.tw

摘　要

「個人資料保護法」(Data protection law) 已是國際上的重要法律；我國新法 (簡稱 PIPA) 於 2012 年 10 月 1 日施行。而稱號史上最嚴格個資法的歐盟「通用資料保護規定」(簡稱 GDPR) 則甫於今年 5 月 25 日正式施行。個資保護法制化、業務化、究責化的趨勢，使其成為現代公司中資料治理 (Data governance) 的重要內涵。然而企業界迄今對相關法制的掌握尚缺頭緒，以致法令遵循的業務難以開展。進一步言之，如何將企業的個資管理成果加以合理評價、以判定其是否達成法令遵循，尤其受到關注。國際上的法制經驗顯示：針對組織體個資保護的主要法律監管模式有行政監理制及民間認證制。本文介紹德國法制，評析其對「個資保護稽核」(Datenschutzaudit) 的法制經驗與實務內容；此足以顯示個資保護其實具有在地法規的內涵，而我國迄今的認證或輔導思維，則經常是受規範主體的政府與企業，被動接受套裝格式之輔導，因而欠缺本土化的實作深度。另一方面，本文再以歐盟法制為觀察重點，論述其個資保護認證 (Data protection certification) 的法律意義與發展趨勢，以資參照。在此基礎上，本文旁論及於國發會申請歐盟 GDPR「適足性」認定的現實目標，提出由現行台歐間會計稽核的架構、來進行初步「個資保護認證」的建議，期待能加速助成我國政策目標的達成。

關鍵詞：個資法、歐盟「通用資料保護規定」、安全維護措施、個資認證、會計稽核

* 作者現為國立中興大學法律系專任副教授。學歷：德國薩爾大學（Universität des Saarlandes）法學博士，德國特利爾（Trier）大學法學碩士（LL.M），台大法學士。

Abstract

The data protection law becomes more and more important, both nationally and internationally. In Taiwan, the Personal Information Protection Act (PIPA) was enacted in 1995 as the first example in Asia; and the newly amended version of PIPA comes into effect in 2012. In the meanwhile, the General Data Protection Regulation of European Union (EU GDPR) takes effect on May 25, 2018. The GDPR imposes stiff fines on data controllers and processors for non-compliance. The potential fines are substantial and a good reason for companies to ensure compliance with the Regulation. With such a legal trend, the data protection issues are becoming an indispensable element in modern corporate governance. Among the solutions to protect the business, the data protection audit or certification mechanism is highly evaluated. The author tries to introduce two models of legal institutionalization of it: the German audit model and the EU certification model. Nevertheless, emphasis is put on both the practical instructions in the local regulation and the operational content in the local compliance, which are the main shortcomings of the actual development in Taiwan. *Last but not least important*, the accounting audit is recommended to fulfill the relating competence, with the conception of helping Taiwanese government to apply for the EU GDPR equivalence decision.

Keywords：Taiwan's personal information protection act, EU general data protection regulation, Security safeguard, Data protection certification, Accounting audit

前言

企業經營需要建立各種各樣的人與事的檔案，且須加以特別的保護；其涉及的法律則有營業秘密、智慧財產權，以及員工、客戶、合作廠商、投資人等蒐錄資料的相對權益保護法令 … 等等。由於隱私權保護的意識日漸強化，以及個人資料保護法的快速發展，企業經營中所形成的資料檔案，如果符合法律上對「個人資料」(Personally identifiable information) 的定義，即必須接受法律的規範。在個資保護逐漸成為各方利害關係人重視的事項的同時，其專業化程度也成為現代公司治理的重要內涵。由於隱私權屬於民法上的人格權，其討論較為繁雜；本文針對「個人資料」著重討論。希望藉著相關法制，提供企業應有的法令遵循的基本認知與體制素養。

「個人資料保護法」(以下簡稱個資法) 已是國際上的熱門法律；我國新法也已於 2012 年 10 月 1 日開始施行。企業界迄今對相關規範的掌握並不熟悉，以致法令遵循 (Corporate compliance) 的業務化常感

難以開展。而有「史上最嚴格個資法」稱號的歐盟「通用資料保護規定」(General Data Protection Regulation，簡稱 GDPR)，甫於今年 5 月 25 日正式施行，以取代歐盟執委會 1995 年通過的《個人資料保護指令》(Directive 95/ 46/EC)。其違反效果，可能是高達 2 千萬歐元 (約新台幣 7 億元)、或全球總營業額 4% 的行政罰鍰。在此壓力下，企業更是備感焦慮。個資法的難以掌握，主要在於其高科技特性；即資訊科技之管理，或謂資料治理 (Data governance)。如何將企業的個資管理成果加以合理評價、以判定其是否達成法令遵循？

壹、企業利益關係人之個資保護：以「技術上與組織上措施」為觀察重點

個資保護法制歷來有人文權利面與技術管理面二個重點。隨著隱私保護議題與資訊網路發展的合流，個資保護在法律義務上的「技術上與組織上措施」(Technical and Organizational Measures，簡稱 TOM)、或者「安全維護義務」(Security safeguards) 已成為今日個資法的發展重點；德國有謂之「法律與技術交疊」(Wenn Recht und Technik aufeinandertreffen) (DR. DATENSCHUTZ，2018)。GDPR 第 2 節 (個人資料之安全) 之第 32 條 (處理之安全) 之第 1 項：「考量現有之技術水準」(英文：The state of the art；德文：aktueller Stand der Technik)，揭示了個資保護中法律與技術匯流之大趨勢。

但是究竟何謂「採取適當之科技化且有組織的措施，以確保對於風險之適當安全程度」(英文：To ensure a level of security appropriate to the risk；德文：um ein dem Risiko angemessenes Schutzniveau zu gewährleisten) ？依據法國個資保護監管機關 Commission Nationale de l'Informatique et des Libertés (CNIL) 2018 年 4 月的指導文件「Security of personal data」(英文) (The cnil's guides - 2018 edition)，可以總結出資訊安全的重點在於首先必須建置一個「風險管理系統」(Risk management system)，再結合操作以下四大面向：

1. 詳列所有要處理的個資；
2. 評估所引發的各種風險；
3. 轉置並查核所規劃的措施；
4. 進行定期的安全稽核。

以德國法制之發展經驗以觀，其重點即在於組織必須在其內部控管程序中，針對個資管理提出一個系統化、文件化、概念化的整體設想；之後必須建立起核實機制、亦即攸關主觀實踐力與客觀實現力的稽核程序；如此才構成一個組織法令遵循的完整方案。此即「Datenschutzkonzept」(個資保護個案構想；簡稱 DSK) 的旨趣 (activeMind AG，2018)。「個資保護個案構想」是一個組織對個資法上諸面向的統合性文件化工作；其包括目標、責任及記錄義務；堪稱是最重要的策略文件。在此一原則下，各家顧問與輔導機構提出有進一步的「模組化」(Template) 文件，以利於各家企業的作業；比如針對 GDPR 者 (activeMind AG，2018)；依據其概念，一個個資保護政策 (Data protection policy) 應包括以下六個大項：

1. 政策目標
   (Goal of the data protection policy)；

2. 前言 (Preamble)；
3. 資安政策與企業中之責任區分 (Security policy and responsibilities in the company)；
4. 企業中之法務架構 (Legal framework in the company)；
5. 文件化 (Documentation)；
6. 現行技術上與組織上措施 (Existing Technical and Organisational Measures；TOM)。

此種完整且成熟的文件化個資保護個案構想，初步顯示其制度的妥善性；而其客觀評價，即是「個資保護稽核」(Audit) 或「個資保護認證」(Certification) 制度崛起的基礎。一個組織個資保護法律義務的履行與否、資料流通相對人對其之肯定與否，以及被蒐集的個人資料主體對其之信賴與否，皆可藉此而客觀化。是以，以個資稽核或認證為重點，來觀察企業或組織在個資法上的法令遵循，最能顯現其專業化程度；而這也正是國際上個資保護法制的發展主軸。國際上的法制經驗顯示：其主要法制模式有直接的行政監理制、或者間接的民間認證制。本文以下介紹先以德國法制為例，評析其「個資保護稽核」的法律意義與規範內容；之後，再以歐盟法制為觀察重點，論述其個資保護認證的法律意義與規範內容。在此基礎上，希望也能提供國內各界，一個思考台灣個資法未來法制走向的參考。

貳、個資保護稽核的法律意義與規範內容：以德國法制為觀察重點

德國個資法具有悠長歷史與豐富經驗，應是歐盟國家中最具指標性的法制 (Peter Gola/Christoph Klug/Barbara Körffer/Rudolf Schomerus，2009)；也是我國個資法體系架構之所本。德國聯邦個人資料保護法 (簡稱 BDSG；原制定日：1990 年 12 月 20 日；2003 年 1 月 14 日重新公告制訂)；是為我國個人資料保護法參考之主要立法例。其後，德國許多相關法律文件與後續法制發展，多曾引進我國；尤其人文法律面之原理原則。至於技術管理面，我國自 2012 年新法施行後之討論多偏向英國與美國有關個資保護的資訊安全事項。以下引介德國相關規定，以資參照。按，德國個資法高度發展的三大骨幹，歷來為行政監理 (尤其是事先審查制 Vorabkontrolle)、個資保護監察人 (Datenschutzbeauftragter)，以及「個資保護稽核」(Datenschutzaudit)。一方面，德國式個資保護之行政監理，理論嚴謹、體系龐大、且隨個案而決定其核准個資處理申請案件；有待他日另外以專文探討。另一方面，我國個資保護業務化的現階段發展，還是以民間的顧問、輔導與認證最為活耀；因而先行介紹德國稽核與歐盟認證的發展脈絡。是以，德國式行政監理本文礙於主旨限定與篇幅限制，本文暫不論列。

另外，為了適用並銜接 GDPR 與 BDSG，德國於 2017 年 6 月 30 日頒布了 Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 016/ 679 und zur Umsetzung der Richtlinie (EU) 2016/ 680 (Datenschutz-Anpassungs- und –

Umsetzungsgesetz EU - DSAnpUG-EU) vom 30. Juni 2017 (BGBl. I S. 2097)。由於 GDPR 施行時間尚短，且德國歷來之個資保護配套制度已有相當根深蒂固的實務基礎，而不會輕易改變。故本文亦不論列此一過渡階段之面向。併此敘明。

一、技術上與組織上措施（簡稱 TOM）(Peter Münch，2010)

BDSG 第 9 條技術上與組織上之措施（德　文 Technische und Organisatorische Massnahmen；簡寫 TOM）規定：「公務單位或非公務單位自行或受託蒐集、處理或利用個人資料，應採取技術上與組織上之必要措施，尤其是本法附件所列舉之要求，以確保本法之執行。措施之必要性，以其所須支出之費用與所欲達成之保護目的間，符合適當之比例者為限。」就此要求，其隨後在 BDSG 第 9a 條資料保護之稽核中又規定有：「為加強資料保護及資料之安全性，資料處理系統或程式之提供者與資料處理單位，就其資料處理計畫與技術設備，得由獨立且合格之專家予以檢測與評鑑，並公開檢測之結果。關於檢測及評鑑之詳細規定、程序，以及專家之選擇與許可，另以法律定之。」

BDSG 第 9 條另有附件（Annex）進行更詳細的規定；亦即外界據以衍生操作實務的所謂「TOM 九大要項」，其內容為：

1. 組織管制（Organisationskontrolle），即個人資料如係透過自動化方式處理或利用時，行政機關內部或企業內部之組織設置，須能落實個人資料保護之特別要求。一般認為此一原則下，應提舉專業專職之此一職務，以帶領組織成員之共同合作，以完成以下之工作目標：（1）設置個資保護長；（2）要求團隊之保密義務；（3）員工之認知宣導與教育訓練；（4）個資保護之個案構想之提舉。
2. 接觸管制（Zutrittskontrolle），即防範無權限之人擅自進入處理或利用個人資料之資料處理設備內。
3. 進入管制（Zugangskontrolle），即禁止無權限之人使用資料處理系統。
4. 存取管制（Zugriffskontrolle），即確保有權利用資料處理系統之人，僅能接觸其接觸權限內之資料，且個人資料於處理、利用之時與儲存之後，不得由無權限之人閱讀、複製、變更或移除。
5. 傳送管制（Weitergabekontrolle），即確保個人資料於進行電子播送時，或於傳送至或儲存於資料載體時，不得經無權限之人閱讀、複製、變更或刪除，且應確保經由資料傳送設備接受個人資料傳遞之單位，為可得預見並可經查驗及確認。
6. 輸入管制（Eingabekontrolle），即確保資料處理系統內之個人資料是否經人輸入、變更及刪除，以及係由何人輸入、變更及刪除，於嗣後可得查驗及確認。
7. 委託管制（Auftragskontrolle），即確保於受託處理個人資料之情形，僅得依委託人之指示處理個人資料。
8. 可處分性管制（Verfügbarkeitskontrolle）

，即確保個人資料得免於意外之毀損或喪失；亦即資訊安全定義中之可用性(Availability)。

9. 分離原則(Trennungsgebot)，即確保依不同目的而蒐集之個人資料，應分別處理之。

德國個資保護監察人依據上述「TOM九大要項」，而頒發有諸多之指導文件。其同時亦經常成為德國「個資保護稽核」的基本要點。在其延伸下，德國發展出許多實務要素與創造性成果。而我國之相對法制，則可參照我國施行細則第12條之11項有關「安全維護措施」之工作內容「安全維護十一大要項」(見文末羅列之相關法條條文內容)。由條文觀察，德、台二者比較，各有其著重點與特色。德國著重分項工作可能風險的規畫必要；台灣則描繪一個體制性管理的可能細項，即現今所謂PIMS(Personal Information Management System)的雛形。然而，我國卻因為行政監理實際作為的遲遲無法展開，以致迄今少有依據「安全維護十一大要項」而進一步頒布之行政指示文件或指導原則。另外，我國亦無BDSG第9a條有關個資保護稽核之規定。是以，我國業界積極推行的所謂認證，事實上並無法律上的依據。

二、德國式個資保護稽核之法制化經驗

承上，雖然BDSG第9a條有規定「關於檢測及評鑑之詳細規定、程序，以及專家之選擇與許可，另以法律定之。」，然而個資保護稽核至今在德國的聯邦層次並未能取得直接的法律效力。2009年德國曾經嘗試制定個人資料保護稽核法(Datenschutz-Audit-Gesetz；DSAG)(Deutscher Bundestag，2009)；但是最終並無法通過國會議決；德國國會(Bundestag)於2009年7月3日決議擱置該法案。2009年DSAG草案失敗的主要原因，在於基本理論的爭議不斷(Uwe Dieckmann/Bernd Eitschberger/Harald Eul/Paul Schwarzhaupt/Gerwald Wohlrab，2001)；稽核的內容與標準亦難以確認(VolkerHammer/Karin Schuler，2007)。其次，亦未能觸及技術、組織與產業的發展動態；動搖了BDSG中最核心的告知同意法制；並挑戰了歷來的個資保護監察人行政監理體制。無論如何，各界對個資稽核法制化的呼聲依舊不斷(Frederick Kubin，2015)。德國的個資稽核，迄今在聯邦層次並無法律依據。

三、德國式個資保護稽核的種類

德國式「個資保護稽核」可分為二種(Brands Consulting，2016)：

(一)內部個資保護稽核(Internes Datenschutzaudit)

此種稽核可以提供被規範的公務機關/非公務機關以及個資保護官一個督看組織整體個資保護現狀的依據。稽核可以只針對區域、程式、部分部門或組織全部提出分析與評價。如此個資保護的「應然狀態」(Soll-Zustand)即可評述，「實然狀態」(Ist-Zustand)亦可記錄；而其間之落差即可據以掌握。後續稽核則可針對業經確認之已導入措施的細項，呈現其改善狀況。此種持續改

善的稽核報告，足以贏取外部形象、並增加社會的信任；對企業具有相當正面的助益。此種導入內部稽核的實務例證有：

1. 於遵守「關於行動終端機具 [Bring Your Own Device(BYOD)] 導入之指令」時；
2. 於遵守「關於社群媒體（如 Facebook, twitter, google+… 等等）導入之指令與其轉換」時；
3. 於遵守「網站首頁個資保護狀態」時；
4. 於遵守「應徵程序之個資保護」時；
5. 於遵守「網路私人使用之指令」時；
6. 於遵守「個資保護公告狀態」（即隱私權保護政策之公開）時；
7. 於遵守「個資保護教育訓練」時；
8. 於遵守「依據 § 9 BDSG 之技術上與組織上措施」時；
9. 於遵守「個資保護個案構想」時。

… 等等。

（二）外部個資保護稽核（Externes Datenschutzaudit）

此種稽核經常是因為公務 / 非公務機關進行 BDSG 第 9 條之個資處理委託業務（Auftragsdatenverarbeitung（ADV）gemäß § 11 BDSG）時所必要，比如導入「外部話務中心」（Externes callcenter）、或資料提供服務；BDSG 第 9 條規定：「因其他單位之委託蒐集、處理或使用個人資料時，委託人應對本法與其他資料保護規定之遵守，負責之。第六條、第七條、第八條列舉之權利，應向委託人主張。（第 1 項）選擇受託人時，應特別就其採用之技術上與組織上措施之適用性，審慎評估之。委託應以書面為之，並應特別就下列事項確定之：…（第 2 項）」此種外部稽核可於受託前、或委託期間進行；而此種稽核之義務最好以契約明文要求。與內部稽核不同的是，外部稽核並不需要針對組織全部進行分析與評價；比如委託人只將印刷或郵寄業務外包 Lettershop（即入信服務；包括：摺疊信紙或傳單、套入信封、貼上地址標籤、計算數量及包裝、安排送到郵局或客戶）時，就不需針對其薪資個資運用狀況進行稽核。該進行稽核的是 Lettershop 本身的個資保護官或其個資保護業務主管機關；其必須針對該 Lettershop 所蒐集、處理或利用之個資、或其因委託業務所必須啟動的部門進行 BDSG 之個資管理或行政監理。此種導入外部稽核的實務例證有：

1. 於遵守「外部話務中心委託業務導入規範」（ADV - Auftragsdatenverarbeitung）時；
2. 於遵守「受委託人關於文件與資料載體之運送規範」時；
3. 於遵守「IT 服務、IT 系統維修及電信設備之管控規範」時。

… 等等。

四、小結：在歐盟化潮流下德國式個資保護稽核的發展趨勢

德國針對「個資保護稽核」的內涵尚多爭議（von Frederick Kubin，2015）；歷來亦有二種評價：著重直接行政監理的保守力量，會覺得「個

資保護稽核」應有動搖或減損現行體制之疑慮；此種疑慮亦表現在歐盟的 GDPR 上（如第 42 條）認證之第 3、4 項，亦即 3. 認證應係志願性的，並透過透明程序取得。以及 4. 本條所定認證不減損控管者或處理者遵守本規則之責任，且不損及第 55 條或第 56 條所定主管監管機關之任務及權力。而支持之論述則有 (Frank Reiländer，2003)：

1.「個資保護稽核」可強化企業個資保護監察人 (Betrieblicher Datenschutzbeauftragter) 的自律 (Selbstkontrolle) 權能；
2. 一個有效且符合競爭旨趣的「個資保護稽核」程序可以防免國家公權力過於強勢的介入；
3. 可以阻止商業性認證標章制度 (Datenschutz-gütesiegeln) 的過度發展；
4. 逐漸演化出的標準可以產生綜效、進而加速品質標竿 (Qualitätsmerkmal) 的提煉。

雖然德國聯邦層次至今尚無個資保護稽核法，稽核的結果亦無法享有法律上的效果。但是德國稽核與認證的制度卻因有實務需求而不減其發展勢頭。「個資保護稽核員」(Datenschutz-Auditor) 在德國已是相當普遍認知的專業頭銜。若干稽核或認證的機構，其證書常能發生助益企業形象、強化消費者對企業信任感的效果。甚至，連許多公務機關亦積極自願參與稽核，以獲取社會形象。歸納德國現今對「個資保護稽核」的主要觀念約為 (Datenschutz.org，2018)：

1.「個資保護稽核」必須保證特定之個資保護個案構想或衍生產品，能夠滿足 BDSG 的要件，並且確保高標準的安全需求；
2.「個資保護稽核」並非強制性；公務機關或非公務機關皆可自願性地進行。具有稽核資格者為獨立鑑定專家或個資保護官。
3. 企業可以將稽核之結果作形式上的公開，以強化消費者對自家企業、程序或產品的信心。在此意義上，「個資保護稽核」可視為一種類似「個資保護認證」的公眾說服力。

德國個資法的三大骨幹中，迄今仍然偏重行政監理；個資保護監察人則主要在助成行政監理；至於「個資保護稽核」則一直屈居民間層次，以幫助政府機關或民間企業獲取公眾形象。由此亦可見，德國社會之重視個資保護，已形成輿論壓力。然而，未來在歐盟 GDPR 的架構下，其發展主力究竟會依舊是行政監理、或轉向自律稽核與認證？又或德國式行政監理制在 GDPR 民間認證制的挑戰下將有何發展？則有待觀察 (Roßnagel，2018)。

參、個資保護認證的法律意義與規範內容：以歐盟法制為觀察重點

號稱史上最嚴格個資法的歐盟「通用資料保護規定」（General Data Protection Regulation，簡稱 GDPR），甫於今年 5 月 25 日正式施行。歐盟在 2016 年即通過 GDPR 以取代先前的數個指令；並在實施之前給予

兩年的緩衝期。GDPR 規範的重點包括：擴大適用範圍及於歐盟境外、加重企業相關責任、賦予個資當事人更完整權利，以及個資跨境傳輸採「原則禁止、例外允許」模式。例外許可情形包括：企業自主採行符合規範的適當保護措施、取得個資當事人明確同意，或經歐盟認定個資保護水準與其相當的國家，即可自由與歐盟進行個資跨境傳輸。據報載，全球 60％的科技公司都還沒準備好。

一、歐盟GDPR中之個資保護認證(Certification)

歐盟 GDPR 針對個資保護認證制度的最核心規範，在於其第 42、43 條，亦即認證(Certification)及認證機構(Certification bodies)，以下論述相關重點與內涵。(法條全文請參照附錄)

由第 42、43 條以觀，認證乃指由公信第三人，針對是否符合法定要件予以進行核實驗證。此等法定要件或由某一標準、或由某一法規所訂定。GDPR 此部分由歐盟次級法規(Secondary EU legislation)來規範其評估架構。認證之結果為一份證書或標章，以確認該組織在該認證範圍中、已通過法定或標準要求之實質及程序要件；當然 GDPR 之法定要求與標準所要求之事項也可能相同。GDPR 之認證要求目前只到達「當責性」(Accountability)原則；亦即並非強制。而且，似乎也只要求到實質要件、而不及於程序要件。GDPR 第 42 條及第 43 條可視為一種目標導向型的認證，因為受認證者不但要具備該當個資保護措施，也必須證明其足已通過法定要求。

可見，歐盟事實上是支持個資保護認證制度的發展的；這符合歐盟 GDPR 追求資料跨國流通的原始目的。其力求民間認證與行政監理之分工；並於其後強調個人資料官(Data Protection Officer；DPO)介於二者之間協作實現的角色。德國式個資保護稽核在此被提升至認證的層次。此種認證思維，可以提供資料主體易於辨識、彈性化的保護方案；亦有利跨會員國、歐盟層級、開放標準、不涉會員內國法之客觀化品質標準之產生。歐盟 GDPR 有關個資保護認證制度的相關規範，尤其是與 ISO 相關系列的關係，其後續發展有待觀察。

二、依據 GDPR 而進行個資保護認證的重點內容

由於迄今有關 GDPR 的法令遵循與認證內容，多由民間整理提出，故本文依據至今較為完整、且具官方色彩的研究，即歐盟執委會 Joint Research Centre 於 2013 年所發行的 EU Privacy seals project 一書(Rowena Rodrigues, David Barnard-Wills, David Wright, Paul De Hert, Vagelis Papakonstantinou，2013)(雖然時效上較早)，以其研究成果為基準，整理出以下的工作項目、並初步探討個資認證應有的基本內容。依據 GDPR 而進行認證的重點內容應有以下 28 個基本項目：

1. 公平、合法且透明的個人資料處理；

2. 為特定、明示且正當的目的而進行個人資料之蒐集；
3. 適當、相關且有限的個人資料之蒐集；
4. 遵守資料正確原則；
5. 時效與目的皆限定的資料保存；
6. 資料處理由資料掌控者負行政責任與侵權責任；
7. 對 13 歲以下兒童所進行的資料處理須得到父母之同意；
8. 特種個資之處理須得到當事人之同意；
9. 針對個人資料的處理與資料主體權利的行使，具有透明且易讀取的政策；
10. 就有關個人資料處理的相關事項，具有對資料主體進行的智慧型、且清楚的資訊告知或通訊的方式，特別是針對兒童保護相關的任何資訊；
11. 針對資料主體的權利行使具有特定程序或機制；
12. 針對更正或刪除權利提供通訊方式；
13. 針對資料主體提供資訊；
14. 提供資料主體近用權的行使機會；
15. 提供資料主體更正權的行使機會；
16. 提供資料主體被遺忘權與刪除權；
17. 提供資料主體資料可攜權的行使機會；
18. 提供資料主體反對權的行使機會；
19. 在直接行銷的情況，提供反對個資處理的免費方式（明示的提供權利）；
20. 針對自動化處理事項提供相關權利；
21. 文件化相關要件的履行；
22. 執行資訊安全要件相關事項；
23. 針對個人資料洩漏事件向主管機關通報；
24. 針對個人資料洩漏事件向資料主體通知；
25. 執行資料保護衝擊評估；
26. 遵循向主管機關進行事前許可或諮詢的義務；
27. 任命個資保護長；
28. 稽核或外部監督機制、以確保資料掌控者或處理者的義務有效、核實履行。

三、依據 GDPR 而進行個資保護認證的法律效益

備受關注的毋寧在於認證之法律效益的規定；就此，GDPR 有關個資保護認證所可以產生的法律效益，經整理法條規定後，可知有以下數端：

（1）認證足以顯示個資掌控人或處理人之法令遵循（Art. 24(3), 25(3), 28(5) + 32(3))

第 24 條 控管者之責任

…3. 遵守第 40 條所定經批准之行為守則或第 42 條所定經核准之認證機制得作為控管者遵守其義務之證明。

第 25 條 設計及預設之資料保護

... 3. 第 42 條所定經核准之認證機制得用以證明符合本條第 1 項及第 2 項所定之要求。

第 28 條 處理者

…5. 處理者遵守第 40 條所定經核准

之行為守則或第 42 條所定經核准之認證機制者，得作為本條第 1 項及第 4 項所定充分保證之證明。

第 32 條 處理之安全

…3. 恪守第 40 條所稱經核准之行為守則或第 42 條所稱經核准之認證機制，得作為顯示遵循本條第 1 項要求之斟酌因素之一。

（2）將個資傳輸至歐盟以外第三國時所需之適當安全維護措施，可由認證機構提供證明；且可證明位於第三國之個資掌控人或處理人之法令遵循程度(Art. 46(2)(f))

第 46 條 須遵守適當保護措施之移轉

…(f) 依第 42 條經核准之驗證機制，及第三國之控管者或處理者有拘束力且可執行之協約，以適用適當保護措施，包括關於資料主體之權利。

（3）認證結果可作為減輕行政罰緩之依據(Art. 83(2)(j))

第 83 條 裁處行政罰鍰之一般要件(General conditions for imposing administrative fines)

…2. 依個案情形，行政罰鍰應附加或取代第 58 條第 2 項第 a 至 h 點及第 j 點所定措施。於個案中決定是否處以行政罰鍰及決定其數額時，應考慮下列因素：

…(j) 第 40 條所定經核准之行為守則(Codes of conduct)或依第 42 條所定經核准之認證機制(Certification mechanisms)之遵循(原文：(j) Adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42)；

如上，GDPR 並未針對認證的法律本質與效力直接予以規範；而僅規定了認證的可能效益。不過，其法制化(legal institutionalization)相較於德國式個資保護稽核已更為明朗。

四、結語：公權化或認證化、個案化或標準化？

歐盟個資保護認證制度的發展，不僅給予民間認證正面之支持，亦同時加速歐盟一般標準之提煉。這與更大格局之ISO之發展趨勢相符合。我國應特別注意此一歐盟一般標準的發展及民間認證制度的服務機能，以因應GDPR對我國的衝擊。又，台灣業界迄今的個資法「法令遵循」，其規章多來自「產業自主」式的民間標準，而非公權力之指令或技術規格要求；民間顧問公司或認證機構的版本或標準，主導了多數企業的個資保護格式與方法。此一現象，正面而言，似乎是國內企業積極運用具有國際背景的稽核或驗證機構所造成的效果；但負面而言，也有使得國內相關業務不僅陷於混亂無序，且相當不利於本土技術與管理模式發展的疑慮。商業性認證標章制度的過度發展，有待政府有關部門的行政監理來予以匡正與制衡。

我國業界歷來似乎存有一種通念，認為個資保護就是一種依附或追求標準化的過程；所謂個資保護即是取材於某一標準而輔導所有業者，

如 PIMS 或 ISO29100 系列。德國的發展過程顯示一種截然不同的觀點，亦即強調各別組織的「個資保護個案構想」(DSK)、而稽核的用意則著重在對此種個案構想的初步核實作用；換言之，其只是業者自律的工具性意義此一層次，無法產生較大範圍的標準公信力、以及法律上的效力。即連此種工具性的意義，德國都尚未立法予以釐清其內涵；可見德國至今尚相當堅持直接的行政監理。歐盟的認證則顯現另一種較大格局的客觀公信力與標準化取向；但是其亦非強制性、亦未挑戰監管機關的職權。可見，在個資保護標準化的議題上，我國尚有許多緩衝時間足以試驗本土方案，以及決定特有的法制化進程。

肆、附論(Exkurs)：借助台歐會計稽核架構助成歐盟適足性認定的可行性芻議

一、我國因應歐盟 GDPR 的最新政策

如上，歐盟 GDPR 此一「史上最嚴格個資法」自然引發國貿昌盛、資料流通的我國關注；朝野對加強個資保護的建設應有一定的共識。綜合報載資訊：行政院長賴清德強調，為協助企業因應 GDPR 施行後可能造成的衝擊，對內請各部會積極協助提供所轄產業相關輔導與諮詢服務；對外請國發會統籌相關部會儘速與歐盟洽商適足性認定事宜。國發會主委陳美伶表示已向歐盟表達取得 GDPR「適足性」(Adequate level of protection；adequacy decision)認定的意願，並正式啟動技術性對話(工商時報，2018)。目前，個資法業務由法務部負責(即所謂之法制機關兼協調機關)。由於個資法涉及 22 個目的事業主管機關，法務部建議改由國發會主管推動業務。據報載(綜合報刊報導，2018)：國發會副主委高仙桂表示，「個人資料保護專案辦公室」於 7 月 4 日在松江路法協中心正式成立。而為統一事權，行政院於月前已把個資法的主管機關由法務部移至國發會。國發會表示，未來有關取得 GDPR 適足性認定的相關工作的推展，將由「個人資料保護專案辦公室」統籌辦理。歐盟如果通過我國個資法的適足性認定，則我國與歐盟之間即可自由傳輸個人資料。在此之前，個別企業必須透過與歐盟往來企業簽署契約才能讓資料傳輸如常的運行。全世界目前已有 12 國家或地區取得歐盟的適足性認定。GDPR 個資保護適足性之規定見於其第 45 條。以下論述相關重點與內涵。(法條全文請參照附錄)

國發會「個人資料保護專案辦公室」(國發會，2018)的官方網站已經開始運作；其上之「歐盟一般資料保護規則專區」提供有以下五份之說明文件與法律資源：歐盟 GDPR 簡介；歐盟 GDPR 導讀；歐盟 GDPR 翻譯資料；歐盟 GDPR 與我國個人資料保護法之重點比較分析；以及

歐盟 GDPR 之相關部會諮詢窗口。

二、會計稽核對我國爭取歐盟適足性承認之階段性效益

歐盟於 2016 年 6 月 21 日正式決定我國金管會在審計監理資訊保密之法規架構與執行面，符合歐盟相關指令規範具適足性（Adequacy）（金管會，2018）。我國經歐盟認可整體對會計師之管理制度符合歐盟水準後，再進一步經歐盟認定資訊保密規範已完備，經過整體會計師監理制度及資訊保密之處理等兩層次的審核評估，可謂已完整符合與歐盟進行審計監理合作之條件，未來將可在此基礎上與歐盟會員國進行相關監理合作，除有助會計師事務所全球審計品質之一致性，因會計師毋須至歐盟國家進行登錄及受其監管，對其協助客戶赴海外籌資亦有相當助益。就此，歐盟執委會在今年一月九日的「適足性」行政決定中（European Commission，2018），台灣在「法定稽核」此一大項中的「稽核架構等價性」與「職權單位適足性」二個細項上，獲得承認（總共有十六大項）。是則，現階段我國似乎亦可優先規畫在「審計專業查核」或「外部審計確認」的架構下，引入個資保護認證或稽核，以協助、並加速歐盟對台灣的個資保護適足性的認定。

另外，歷來「審計專業查核」或「外部審計確認」與公司內部控制、風險控管或法令遵循部門極為接近；則由會計師多承擔個資稽核之業務，不但較為順手，而且也較易獲得企業之信任。企業之資訊系統與資料處理常涉及極深之經營機密；要在短期間建立一套全新的外部查察體制並非易事。按，金管會於 2018 年 3 月 31 日所修正頒佈之「金融控股公司及銀行業內部控制及稽核制度實施辦法」中，其第 28 條第 2 項亦已明文規範「主管機關得請銀行業委託會計師辦理個人資料保護與防制洗錢及打擊資恐機制專案查核。」可能的作法如在該法的適用範圍內，針對涉歐金融業者進行依據台灣個資法之「審計專業查核」或「外部審計確認」；嗣後再將此等稽核之範圍擴張及於重點涉歐企業（如航空航海、電信電商及資料處理業者）。另外，輔導我國會計師取得相關個資保護稽核的資格或證照、成立會計師個資保護稽核協會、建立會計師個資保護稽核的典章制度…等等。當然，體制面上個資保護還是必須建立獨立而完整的執法與認證機制。

伍、結語

個人資料保護（ Data protection）已是現今數位經濟環境下，組織內部稽核與強化營運生態體系的重要課題。個資法中之「現有之技術水準」此一法律概念，如何在實務中予以實現？攸關個資保護業務化與實作化。而眾多的保護措施若無法在組織中予以落實及貫徹內部控制與查核作業，則利益關係人的人格權或隱私權極易受到侵害、而引發高度的法律責任之追究。電腦稽核與會計

稽核歷來密切配合發展，是則以會計師來承擔個資保護稽核或認證，應是相關專業人員應戮力以赴的新領域。

在 GDPR 的催化下，個資保護的國際法制將日益嚴格與普及。我國必須盡快規劃個資保護認證的法制工作，以對應資訊時代中國際上個人資料高度流通的現狀。我國未來的個資保護認證，縱使能在民間得有產業界的積極配合發展以及國際個資保護標準的參考；但是，個資保護行政監理的虛弱，亦將使得該等國際標準中應有的本土法令項目內容出現大幅空白；則認證將如何展開？政府相關部門允應積極開展實質的行政監理，才能使台灣未來的個資保護認證具有完整且卓越的本土法令遵循內涵。本文著重呈現技術上與組織上措施的操作細節，用意亦在強調實作面向的國際法制經驗，對我國個資法的現階段發展應有相當重要的意義。

針對我國對歐盟的往來部門，則應積極輔導引入稽核或認證服務，以輔助企業的對歐業務能夠在本土即能獲取高水準的輔導與認證，而且具有相當的國際公信力。而就重點部門，更應密切注意歐盟一般標準的發展，一旦成熟、即應加速引進，以爭取歐盟式輔導與認證的在台生根、並嗣後向國際認證市場進展。而我國的會計稽核 (「審計專業查核」或「外部審計確認」)，由於在歐盟已經獲有相當的官方認定；則以會計稽核之架構、來進行個資保護的「審計專業查核」或「外部審計確認」，或許能階段性助成政府爭取歐盟的適足性認定。

附錄：相關法條之條文內容羅列 (GDPR 條文翻譯依據國發會之版本)

- 我國個資法施行細則第 12 條之「安全維護十一大要項

本法第六條第一項但書第二款及第五款所稱適當安全維護措施、第十八條所稱安全維護事項、第十九條第一項第二款及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間，具有適當比例為原則：

一、 配置管理之人員及相當資源。
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。

- GDPR 第 42 條 認證 (Certification)

1. 會員國、監管機關、委員會及執委會應鼓勵，尤其係歐盟層級，建立資料保護認證機制與資料保護標章及標誌，以證明控管者及處理者之處理活動遵守本規則。微型及中小型企業之具體需求應予考慮。
2. 本條第 5 項所定經核准之資料保護認證機制與資料保護標章及標誌，除

適用於受本規則拘束之控管者或處理者外，亦得為第 3 條所定不受本規則拘束之控管者或處理者依第 46 條第 2 項第 f 點規定將個人資料移轉至第三國或國際組織時，用以證明適當保護措施之存在。該等控管者或處理者應透過契約或其他具有法律拘束力之文書，做成具有拘束力且可得執行之承諾，以適用該等適當之保護措施，包括關於資料主體之權利。

3. 認證應係志願性的，並透過透明程序取得。
4. 本條所定認證不減損控管者或處理者遵守本規則之責任，且不損及第 55 條或第 56 條所定主管監管機關之任務及權力。
5. 本條所定之認證應由認證機構依第 43 條規定或主管監管機關依據第 58 條第 3 項所核准之標準或由委員會依第 63 條規定為之。委員會核准之標準得為通用性認證，即歐盟資料保護標章。
6. 將處理提交至認證機制之控管者或處理者應向第 43 條所定之認證機構或主管監管機關（如適用）提供認證程序所需關於其處理活動之所有資訊及接近使用之方式。
7. 對控管者或處理者所為之認證，最長期限應為三年，且在相同要件下並持續符合相關要求者，得更新之。第 43 條所定之認證機構或主管監管機關（如適用）於欠缺認證要件或不再符合認證要件之情況下，應撤回認證。
8. 委員會應將所有資料保護認證機制與資料保護標章及標誌整理登錄，並應以適當方式公開之。

・GDPR 第 43 條 認證機構 (Certification bodies)

1. 在不損及第 57 條及 58 條所定主管監管機關之任務及權力之情況下，具備關於資料保護之適當程度專業性之認證機構，於通知監管機關使其得於必要時依照第 58 條第 2 項第 h 點行使其權力後，核發及更新認證。會員國應確保該等認證機構通過下列一項或二項之認證：

(a) 第 55 條或第 56 條所定之主管監管機構；

(b) 依 EN-ISO/IEC 第 17065/ 2012 號標準以及主管監管機關依第 55 條或第 56 條規定所建立之附加要求，按歐洲議會及歐盟理事會（1）第

2. 第 1 項所定之認證機構應依該項規定通過認證，但必須符合以下要件：

(a) 證明其具備所涉及認證事件之獨立性及專業性至主管監管機關滿意；

(b) 承諾會遵守第 42 條第 5 項所定之標準，並經主管監管機關依第 55 條或第 56 條規定、或經委員會依第 63 條規定核准；

(c) 建立資料保護認證、資料保護標章及標誌的核准、定期審查及撤回之程序；

(d) 建立處理申訴之程序及組織，以處理違反資料保護認證或控管者或處理者執行之方式已違反或正違反資料保護認證之申訴，並向資料主體及公眾

公開該等程序及組織；及

(e) 證明其任務及責任不會產生利害衝突至主管監管機關滿意。

3. 本條第 1 項及第 2 項所定認證機構之認證應由主管監管機關依據第 55 條或第 56 條規定或由委員會依第 63 條規定依其核准之標準定之。依據本條第 1 項第 b 點之認證，該等要件應與第 765/ 2008 號規則及規範認證機構之方法及程序之技術規則相一致。

4. 第 1 項所定之認證機構應負責對於認證及撤回認證進行適當之評估，但不損及控管者或處理者遵守本規則之責任。認證最長期限為 5 年，且得在相同要件下更新，但該認證機構應符合本條所定之要求。

5. 第一項所定之認證機構應向主管監管機關提供核准或撤回認證之理由。

6. 本條第 3 項所定要件及第 42 條第 5 項所定標準應由監管機關以方便取得之格式公開之。監管機關亦應將該等要件及標準傳送至委員會。委員會應將所有資料保護認證機制與資料保護標章整理登錄，並應以適當方式公開之。

7. 在不損及第 8 章規定之情況下，主管監管機關或國家認證機構於欠缺認證要件或不再符合認證要件或認證機構之行為違反本規則之情況下，應依本條第 1 項規定撤銷該認證機構之認證。

8. 執委會應有權依據第 92 條規定通過授權法，以具體化第 42 條第 1 項所定資料保護認證機制應考慮的要件。

9. 執委會得通過施行法，為資料保護認證機制與資料保護標章及標誌制定技術性標準，以促進及認可該等資料保護認證機制與資料保護標章及標誌。該等施行法應依照第 93 條第 2 項所定之檢驗程序通過。

- 第 45 條 (Transfers on the basis of an a dequacy decision；基於充足程度保護決定之移轉)

1. 個人資料移轉至第三國或國際組織，僅於執委會決定該第三國、第三國內之領域或特定部門、或國際組織確有充足程度之保護時，方得為之。該移轉不須獲得任何特別授權。

2. 於評估保護程度之充足性時，執委會尤其應考量下列因素：

(a) 法治、對人權與基本自由之尊重、一般與部門之相關立法，包括有關公共安全、防衛、國家安全及刑法、公務機關對個人資料之接近使用權、及該等立法、資料保護規則、專業規則及安全措施之執行，包括個人資料向其他第三國或國際組織進一步移轉，該其他第三國或國際組織之規則、判例法、及有效且可執行之資料主體權利及個人資料受移轉之資料主體有效之行政與司法救濟；

(b) 第三國內有一個或以上獨立監管機關之存在及有效運作，或對象為國際組織時，確保及執行資料保護規則之遵守，包括充足之執行權，以協助及建議資料主體行使其權利，並與會員

國之監管機關合作；及

(c) 第三國或國際組織所加入之國際協定，或其他因具法律拘束力之合約或辦法、及從其參與多邊或區域體系而生之義務，尤其關於個人資料保護者。

3. 執委會於評估保護之充足程度後，得透過施行法決定第三國、第三國內之領域或單一或多數之特定部門、或國際組織依本條第 2 項之方式確保充足程度保護。施行法應提供定期檢驗機制，至少四年一次，並應考量第三國或國際組織之所有相關發展。施行法應特定其適用之領域及部門，且於得適用時，確認監管機關或本條第 2 項第 b 點所稱之機關。施行法應採行第 93 條第 2 項之檢驗程序。…

（第 4- 9 款省略）

參考文獻

1. 報刊資料：陳美伶：GDPR 適足性認定啟動，2018 年 06 月 05 日，工商時報；于國欽，台北報導 (讀取日期 :2018 年 6 月 28 日)。陳炳宏，個人資料保護辦公室 7 月 10 日正式上路，2018- 06- 26，自由時報，台北報導。GDPR 個資專案辦公室 今揭牌，工商時報 / 新聞發布，2018 年 7 月 4 日。葉基仁，個資保護專案辦公室成立後 才是挑戰的開始，2018 年 07 月 04 日，工商時報 (讀取日期 :2018 年 6 月 28 日)。
2. 國發會資料，請參照其官方網站：https://www.ndc.gov.tw/Content_List.aspx?n= 726A 44EA 5D 724473(讀取日期 :2018 年 6 月 28 日)。GDPR 條文翻譯：https://www.ndc.gov.tw/Content_List.aspx?n= 726A 44EA 5D 724473(讀取日期 :2018 年 6 月 28 日)。
3. 金管會資料，我國金管會新聞請參照：https://www.fsc.gov.tw/ch/home.jsp?id= 96&parentpath= 0, 2&mcustomize=news_view.jsp&dataserno= 201607210002&aplistdn= ou=news,ou=multisite,ou=chinese,ou=ap_root,o=fsc,c=tw&dtable=News；歐盟部分請參照：DECISIONS COMMISSION IMPLEMENTING DECISION (EU) 2016/ 1010 of 21 June 2016 on the adequacy of the competent authorities of certain third countries and territories pursuant to Directive 2006/ 43/EC of the European Parliament and of the Council (notified under document C(2016) 3727) (Text with EEA relevance)； 其 中 23) The Financial Supervisory Commission of Taiwan has competence in public oversight, external quality assurance and investigations of auditors and audit firms. It implements adequate safeguards prohibiting and sanctioning disclosure by its current or former employees of confidential information to any third person or authority. Under the laws and regulations of Taiwan, it may transfer to the competent authorities of the Member States documents equivalent to those referred to in Article 47(1) of Directive 2006/ 43/EC. On that basis, the Financial Supervisory Commission of Taiwan meets requirements

which should be declared adequate for the purposes of Article 47(1)(c) of Directive 2006/ 43/EC(讀取日期：2018 年 6 月 28 日).

4. 歐盟執委會 (European Commission) 資料，請參照：https://ec.europa.eu/info/sites/info/files/file_import/equivalence-table_en.pdf(讀取日期：2018 年 6 月 28 日)。
5. activeMind AG，2018， 請 參 照：https://www.activemind.de/datenschutz/dokumente/datenschutzkonzept/；https://www.activemind.de/en/data-protection/documents/data-protection-policy/(讀取日期：2018 年 6 月 28 日)。
6. Brands Consulting, Datenschutzauditor (Datenschutzaudit), 06. August 2016, https://brands-consulting.eu/datenschutz/datenschutzauditor-datenschutzaudit (讀取日期：2018 年 6 月 28 日)。
7. THE CNIL'S GUIDES - 2018 EDITION，請參照：https://www.cnil.fr/sites/default/files/atoms/files/cnil_guide_securite_personnelle_gb_web.pdf(讀取日期：2018 年 6 月 28 日)。
8. DR. DATENSCHUTZ, Aufsichtsbehörde äußert sich zur Datensicherheit nach Art. 32 DSGVO, 5. APRIL 2018, https://www.datenschutzbeauftragter-info.de/aufsichtsbehoerde-aeussert-sich-zur-datensicherheit-nach-art- 32-dsgvo/(讀取日期：2018 年 6 月 28 日)。
9. Datenschutz.org, Datenschutzaudit: Güteklasse A in Sachen Datenschutz?, https://www.datenschutz.org/datenschutzaudit/ (讀取日期：2018 年 6 月 28 日)。
10. Roßnagel, Das neue Datenschutzrecht Europäische Datenschutz-Grundverordnung und deutsche Datenschutzgesetze, Herausgegeben von Prof. Dr. Alexander Roßnagel, 2018, 477 S., Broschiert, ISBN 978- 3- 8487- 4411- 4.
11. Deutscher Bundestag – Drucksache 16/ 12011, 16. Wahlperiode, 18. 02. 2009, Gesetzentwurf der Bundesregierung Entwurf eines Gesetzes zur Regelung des Datenschutzaudits und zur Änderung datenschutzrechtlicher Vorschriften
12. Peter Gola/Christoph Klug/Barbara Körffer/Rudolf Schomerus, BDSG Bundesdatenschutzgesetz: Kommentar: November 2009 Gebundene Ausgabe – 11. August 2010, C.H. Beck.
13. Roßnagel, Handbuch Datenschutzrecht: Die neuen Grundlagen für Wirtschaft und Verwaltung, 2003, C.H.BECK ISBN 978- 3- 406- 48441- 4。
14. Uwe Dieckmann/Bernd Eitschberger/Harald Eul/Paul Schwarzhaupt/Gerwald Wohlrab, Datenschutzaudit – Quo Vadis ?, DuD • Datenschutz und Datensicherheit 25 (2001) 9, pp 549 - 552.
15. VolkerHammer/Karin Schuler, Cui bono? — Ziele und Inhalte eines Datenschutz-Zertifikats, DuD • Datenschutz und Datensicherheit, February 2007, Volume 31, Issue 2, pp 77– 83.
16. Frederick Kubin, Was ist ein Datenschutzaudit?, 06. 11. 2015, https://

www.datenschutz.com/magazin/was-ist-ein-datenschutzaudit(讀取日期：2018 年 6 月 28 日)。

17. Peter Münch, Technisch-organisatorischer Datenschutz: - Leitfaden für Praktiker, 27. April 2010, DATAKONTEXT; S. 323ff..

18. Frank Reiländer, Vorgehen beim Vorgehen beim Datenschutzaudit Datenschutzaudit mit SAVe, 2003, https://www.infodas.de/wp-content/uploads/ 2014/ 04/savedsa.pdf(讀取日期：2018 年 6 月 28 日)。

19. Rowena Rodrigues, David Barnard-Wills, David Wright, Paul De Hert, Vagelis Papakonstantinou，歐盟執委會 (European Commission) 的 Joint Research Centre - Institute for the Protection and Security of the Citizen，於 2013 年所發行的 EU Privacy seals project 一書 (Inventory and analysis of privacy certification schemes, Final Report Study Deliverable 1. 4)，作者為 Rowena Rodrigues, David Barnard-Wills, David Wright, Paul De Hert, Vagelis Papakonstantinou；編者為 Laurent Beslay, EC JRC–IPSC 及 Nicolas Dubois, EC DG JUST。書籍編號為 Report EUR 26190 EN。

機器人，流程改善的新工具

張騰龍
執行副總經理

陳宜宏
經理
安永企業管理諮詢服務股份有限公司

摘　要

你是否注意過一天的工作中，會接觸到多少軟體和系統嗎？也許數字會超過你的想像。由於商業環境與活動的日趨複雜，多數組織必須仰賴各種系統和軟體，透過美國 Gartner 產業觀察發現，80% 的企業並沒有單一 ERP 系統，許多大型企業 (市值超過 10 億美元) 甚至有至少來自 100 種不同應用程式和系統的資料。為了提供企業服務，這些不同類型的資訊需要被無縫匯出匯入地傳遞。許多員工每日的工作內容可能充斥著人工從 A 系統搬移資料至 B 軟體，然後一再地執行規律的刪除、複製、插入、整理、計算等工作。執行的過程和步驟是明確的，但在本質上卻是重複的，同樣的動作需要執行無數次，例如：接收包含客戶訂單的電子郵件，開啟附檔提取資料，然後將其輸入訂單管理系統；或是繁瑣的申請出貨程序、製作出貨批號貼標、冗長的出口報關作業、跟催船期、通知客戶應收帳款、彙總整理報表 … 等，而這些人工作業又經常伴隨著時間成本高、錯誤率高與時程延遲等負面影響。

根據 2015 年 6 月哈佛商業評論 (Harvard business review) 中 What knowledge workers stand to gain from automation 文章所述：「在 Peter Drucker 首創『知識工作者 , Knowledge worker』這個名詞 50 多年後，觀察他們在任何大型組織的工作內容是相當令人失望的，知識工作者花費在高級思維活動的時間很少。」顯而易見，這些重複而例行的作業占據了所謂知識工作者大多數的時間，故為了提高作業效率與競爭力，將人才放在恰當的位置上以發揮其效益，與持續的改善流程一直是每個企業必須深思並精益求精的課題。

普遍來說，流程簡化與降低人工錯誤率是企業進行流程改善的目標之一，其改善工具不外乎藉由導入整合性系統以彙整流程並借助程式系統的防呆設計或人員交互重複的檢查。導入新系統除需要挹注大量時間和金錢，更需要額外的人力投入。而現在若有

個改善工具，改善前無須龐大的財務資助，使用時不須投入額外的人力，且具有超高速和從不出錯，一天 24 小時，一年 365 天無休的特性，特別適合執行重複性高、出錯率高的人工作業，是否很令人心動？機器人流程自動化就是這樣流程改善的工具。

壹、什麼是機器人流程自動化？

根據安永企業管理諮詢於 2018 年發表的機器人流程自動化論壇中，對 RPA 有詳細的介紹：機器人流程自動化 (Robotic Process Automation, RPA) 是透過機器人作為虛擬勞動力的概念，依據預先設定的程式和既定邏輯，令程式通過模仿人類重複的行為，跨系統、跨平台、跨業務地取代滑鼠、鍵盤工作來達到自動化的目的，與現有使用者交互合作完成預期任務。它可適應並處理內部 / 外部各種不同的資料來源，適用於高重複性並且具有既定邏輯的處理流程，還具備以下特點：

圖 1：RPA 可以跨系統、跨平台、跨業務地取代滑鼠、鍵盤工作

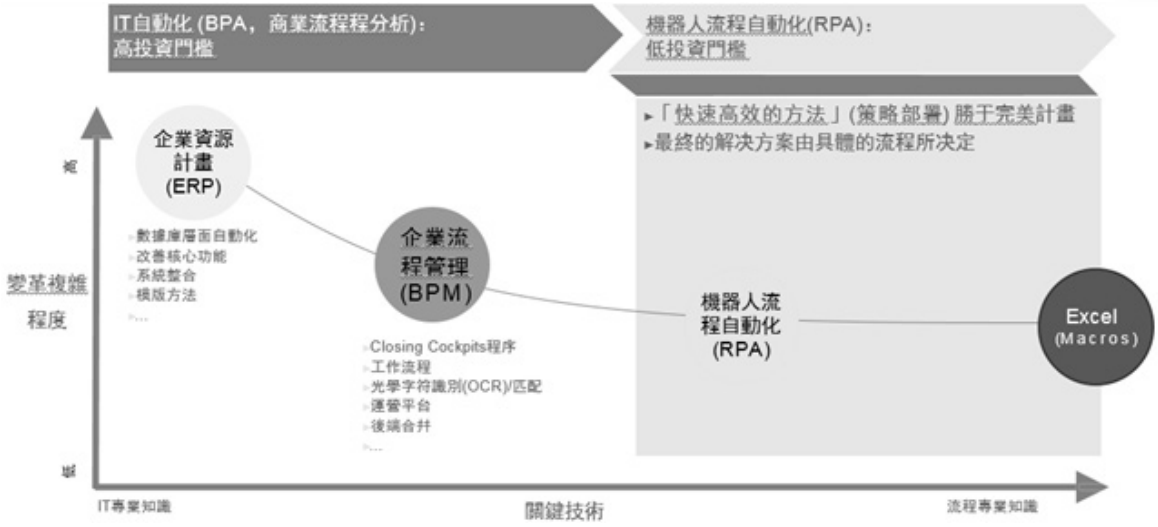


圖 2：RPA 具有快速部署、較友善且較經濟的低進入障礙門檻

一、 快速部署：還記得企業當時導入 ERP 系統漫長的轉換期和巨額成本嗎？導入 RPA 的過程自盤點現有流程、選擇與梳理流程、設計與測試、上線部署，一般而言多在數周之譜。不同於導入或轉換系統，RPA 不改變現有的基礎設施和系統，企業無需為其對現有系統進行修改，而是基於目前擁有的資訊架構與設備，以與使用者相同的方式與系統進行溝通和作業。因此可以快速部署於各種情況，像人一樣與多種系統進行合作，加速了開發週期並在短時間內帶來經濟效益。

二、 進入障礙較低：傳統的流程自動化工具是由資訊開發人員使用內部應用程序介面 (API) 或專用腳本語言自動完成任務並與後端系統連接。所有的自動化都需要仰賴與資訊人員的不斷溝通與測試；整個過程需要配置多位熟悉程式語言、企業系統架構和資料庫操作的資訊人員，單一需求自提出到上線需時不等，其中以來回地溝通測試佔據最多時間。RPA 則是由用戶直接執行應用程序的圖形用戶界面 (GUI) 程式，自行依據工作內容進行規劃與指派，具視覺化操作的特色，不需熟知程式語言與系統架構，故任何熟悉工作流程的一般使用者皆可進行設計，進入障礙較低。

三、 24/7 全年無休而精確地工作：因為 RPA 是自動運行的程式，可以每週 7 天，每天 24 小時運行，不休假，不會疲勞，不生病，能夠精確地執行繁瑣和重複的活動，非常適合應用在規律而出錯率高的工作，減少因人為錯誤造成的返工。以 RPA 作為例行性作業的執行者，企業無需擔心代理人問題，甚至它亦可作為代理人的選擇之一，提高勞動力運用的靈活性。

四、 完整保存作業軌跡：RPA 運行過程將可被嚴格記錄和監控，其所執行的每項任務皆可保留系統日誌 / 審

計記錄，用以進行流程處理完成後的責任劃分和事後檢視。此外，許多企業礙於人力限制，不得已需將某些具有職能衝突的業務同時派予同一人處理，再輔以定期覆核的偵測性控制來防止錯誤與舞弊風險。

RPA 因其程式特性，不會執行非指派的行為，故在良好的設計邏輯與管控條件下，RPA 可作為職能衝突的解決方案，其運作時得以降低隱私資料，如單價、成本、關鍵設計…的外流，亦可降低定期覆核的頻率並避免舞弊的風險。

圖 3：RPA 的多重特色

貳、 機器人流程自動化的應用案例與附加價值

因為 RPA 是模仿人類重複的行為，跨系統跨業務地取代滑鼠、鍵盤工作，故 RPA 不僅可廣泛應用於一般使用者業務，亦可應用在風險管理與稽核層面，根據安永企業管理諮詢輔導之國內外案例與經驗，因為有了 RPA 以下案例的協助後，使稽核人員原本耗時的稽核工作變得更有效率：

工作階段	RPA 可協助的內容	案例
資料蒐集	鑒於在收集的過程中可能需要在多套系統間重複地登入、輸入條件、輸出、拋轉，RPA 可協助蒐集企業內部及外部各系統、資料庫或其他非結構性的資料；亦可定期定時地寄發資料需求清單與回收、追蹤資料提供情形。	RPA 可自動於稽核前至訂單管理系統資料庫擷取與篩選特定條件之客戶信用額度、訂單明細和出退貨紀錄和價格主檔；至庫存管理系統擷取出入庫紀錄；至帳務管理系統擷取應收帳款等資料。
資料整理與驗證	因應各種報表格式琳瑯滿目，欄位不一，RPA 可協助整理報表資料（例如：欄位 / 格式 / 消除值為負或零 / 醒目標示），合併不同來源之資訊、驗證資料 (例如：完整性驗證)、初步進行分群 (例如：分期 / 分層 / 分類)。	礙於上述資料來自三套不同之系統，故報表格式、欄位皆不盡相同，RPA 可自動進行修正格式、比對名稱、彙整並合併為一完整報表，再依據預設定義進行分類。
資料分析	傳統礙於人力與系統限制，僅得仰賴檢舉熱線 (Hotline) 或抽樣技巧來發現異常情形；RPA 可透過數位化稽核以全面覆蓋的數據分析辨識異常情況、趨勢及潛在的舞弊指標來輔以樣本測試，能夠高效和全面地支持控制測試。	RPA 可自動比對各報表間的資料內容並回報差異，例如發現被取消或未完成之訂單、出貨單總計數量與庫存出貨數量之差異、信用額度超額情形 … 等資訊供稽核人員據以進行查核。
執行稽核	協助回填各稽核報告與底稿固定而需重複填寫的欄位；依據預先定義好的頻率和運作邏輯全面性地檢視樣本並從中發現異常。	於稽核人員查核的同時，RPA 已自動回填好稽核報告與底稿固定而需重複填寫的欄位，並自動稽核上述報表間發票價格與訂單價格和價格主檔的匹配情形、發票日 + 付款條件與付款到期日的匹配情形、出貨日期與發票日期的匹配情形 … 等。
稽核結果報告	為潛在缺失和例外情況提供可量化的、基於事實的資訊，降低各種判斷的主觀性；此外，也可輸出資料分析所產出之統計和圖形資訊提供予相關人員。	若上述稽核作業中發現異常，基於 RPA 全面檢視的基礎下，其異常發生概率更為準確，可做為公司投入改善成本的客觀參考。RAP 亦可自動繪製各類統計和分布圖供報告使用。
改善項目追蹤	RPA 可協助進行追蹤，寄發回報提醒，彙整改善情形予稽核人員；提供資訊予下次查核規劃參考。	RPA 可自動寄送郵件，包括複查或追蹤通知、自動追蹤特定天數後尚未回覆的人員名單並重新寄發提醒；並剪貼各部門之回覆內容與查核建議彙整，作為留底歸檔。

再以稽核資訊循環為例，在稽核授權管理作業時，RPA 可偵測正式區的程式與權限授予是否皆經過申請；針對主機除了能夠自動偵測主機異常設定外，對各排程作業的異常情形甚至可做到初步檢查與進一步排除；對權限管理作業，例如：對偵測共用帳號、權限衝突、離調職舊權限的及時停用進行檢視；或對使用者行為，例如：異常登入事件、使用者異常動作進行初步分析與回報。此外，原本礙於時間與資源限制僅得人工抽樣，甚至窒礙難行的稽核活動，藉由 24/ 7 全年無休的 RPA，可使稽核人員針對高風險區塊的母體進行較全面的查核。

更進一步以資訊循環項下的程式變更作業為例，從下圖可看出，在工時的縮減上，以往稽核人員執行 SAP 程式變更作業查核時，需與資訊人員來回溝通以便取得精準的特定日期區間且欄位完整正確的被異動的程式清單、使用者申請單清單、上線單清單、例外情形清單等；在取得清單後可能還需統整或合併各別清單以便進行後續分析和抽樣。在 RPA 的協助下，前述作業皆可移轉給 RPA 執行，稽核人員在這個過程中，僅需將時間投注在覆核 RPA 產出的結果並決定是否執行進一步查核。

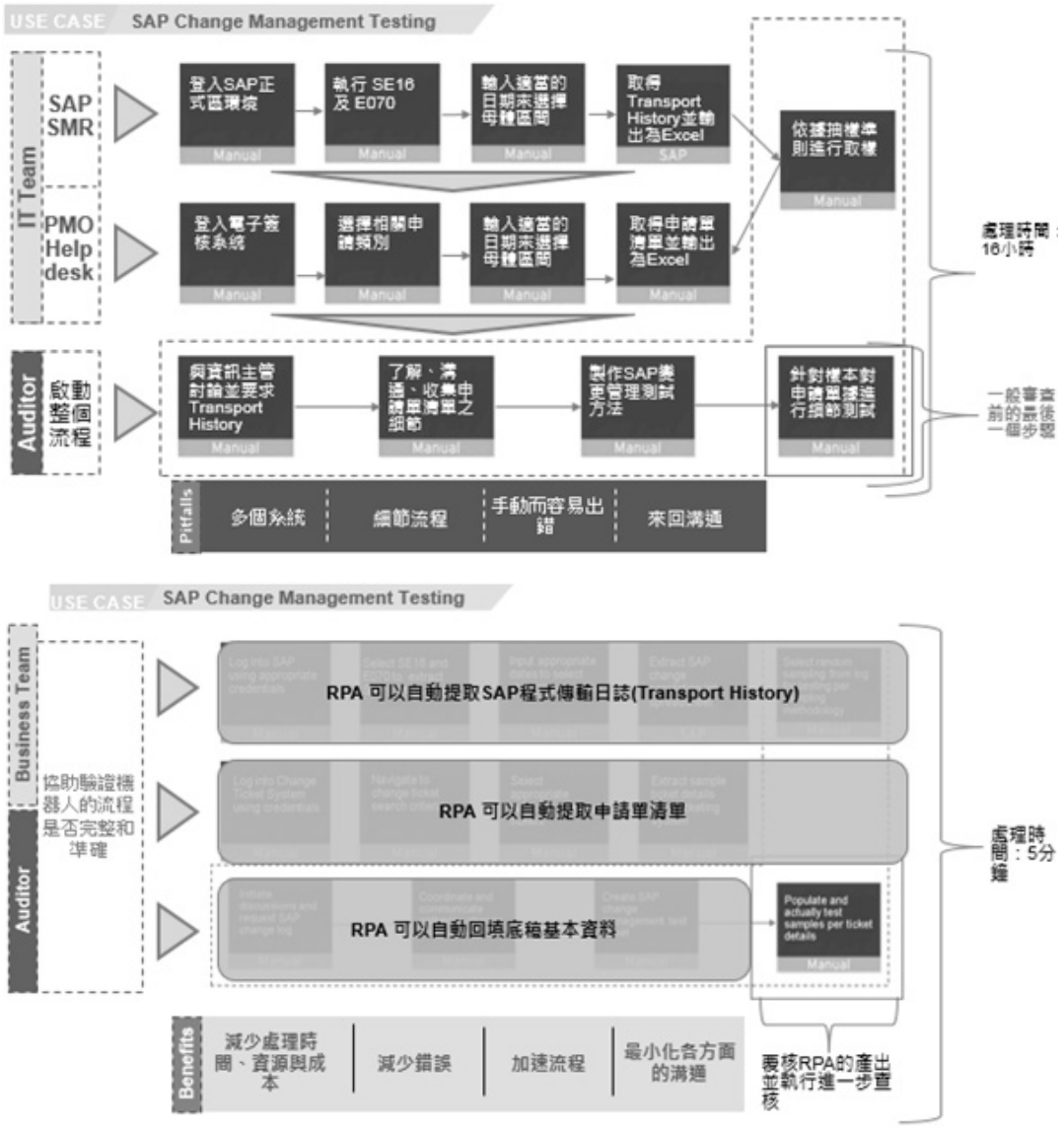


圖 4：RPA 在稽核資訊循環項下的程式變更作業時的工時比較

適當地導入 RPA 後，除了帶來顯著的工時縮短、返工次數降低外，因應 RPA 導入，現有流程必然在導入過程中透明化與標準化。其快速高效的運作特性，企業能夠賦予其相較於人工更大量的工作負荷，例如：傳統每年一次對採購循環樣本採取抽樣的方式，在 RPA 的協助下，能夠快速地全面覆蓋並串連採購品項之請購、採購、驗收、入庫、領用 (出庫) 等資訊，在既定的檢查規則下，任何異常皆無所遺漏；並能夠搭配企業評估之風險等級，彈性設定每季 / 每月 / 每日 / 每分鐘依時運行，以真正達到持續性稽核的精神；也因為各項查核資訊之蒐集與檢視係由機器人執行，使內部稽核之獨立性、客觀性得以確保，缺失風險量化也更為具體。而稽核人員在人工作業縮短的基礎下，進而能更聚焦於缺失之要因分析、稽核結果之溝通或針對來自主管交辦或

同仁舉報的特殊稽核業務深入設計稽核程式等擁有更高附加價值的活動，促使管理階層充分掌握現行不足之處以及未來改善之方向。

參、 機器人流程自動化的常見挑戰與事前準備

雖然前面敘述了許多 RPA 改變當前人工作業的經濟性和提升品質等優點，但若 RPA 未正確運作，業務中斷和低效率的問題仍極有可能發生，而對企業流程和財務造成負面影響。因此，企業在採行 RPA 前，應對其具有充分瞭解，明瞭 RPA 係流程改善的工具之一，它能夠降低 20％～35％以上的作業成本，但並非用以修復過時或低效的流程；它是一種通過自動化將傳統的、零散的系統和作業聯結在一起的技術，但並非所有的流程都可以通過 RPA 進行改進；它令人力勞動重點放在成果，分析和溝通連結上，而非取代現有勞動力。

為了充分利用 RPA，在企業現有架構、工作流程的熟悉度、人員相關培訓計畫和足夠的 RPA 安全措施間保持適當的配合亦非常重要。企業應適當辨識需求，專注於應用範圍及頻率，先完成基礎流程的操作，使人力有更多時間完成其他工作，再逐步增加各流程中自動化的比例，而不是過於追求整個流程從頭至尾 (End to end) 的自動化，以保持 RPA 的靈活性；在 RPA 上線前也應經過合理的測試，但要留意避免採用過於技術化的軟體實施 RPA 以避免複雜冗長的溝通和測試階段，使通常只需要幾周的 RPA 實施周期延長至幾個月。

此外，對於上線後的 RPA 亦應該建立治理 / 控管的方式，包括其上線後的管理權、安全措施、變更授權流程、執行狀態與運行績效的監控、異常修復等，避免 RPA 運行錯誤未得到有效的辨識和管理，導致無效果和低效率的流程自動化，無法支持和滿足企業需求。

結語

Techworld 2016 年 2 月 發 表 的 Technology is not about to steal your job 文中曾以一個小故事比喻：

某汽車產業的創辦人在展示自動裝配產線的機器人時，老闆問工會負責人：「你能要這些機器人支付工會會費嗎？」

工會負責人回答：「啊，那你能要他們買你的車嗎？」

意思是縱使產線自動化減少了工人的數量，但因為人員轉作研發、良率分析、製程改良和銷售業務，進而產出更有競爭力的產品，才是自動化帶來的真正價值。

在企業了解其限制並做好完善的導入規劃的前提下，藉由 RPA 作為流程改善的工具之一，利用其模仿人類重複地使用滑鼠、鍵盤來達到自動化，並在自動化的過程中迅速獲得流程標準化、透明化、優化的價值。而因為它能夠允許企業以現有的資訊環境為基礎進行導入，故具備快速部署與經濟的特性；而其全年無休規律地跨平台、跨系統地作業模式，預期能夠帶來工時的節省和正確性的提高，稽核人員更能將時間重新分配，運用在更有績效、更能彰顯其價值的作業上，方能使流程自動化發揮最大效益。

中華民國電腦稽核協會

中華民國電腦稽核協會（ CAA）自民國 83 年成立，舉辦過無數次有關資訊安全管理與電腦稽核等相關學術研討與實務運用之座談會，並舉辦各項資訊安全與電腦稽核講習課程，提供會員與外界人士一個提升專業知識及能力與分享經驗的場所。民國 85 年 ISACA TAIWAN CHAPTER 成立，為全球第 142 個支會，成為引領台灣與世界電腦稽核之先河，長期推廣國際電腦稽核師證照 (CISA)、國際資訊安全經理人證照 (CISM)、國際企業資訊治理師 (CGEIT)、國際資訊風險控制師認證 (CRISC)。民國 90 年與 BSI 開始合辦主導稽核員訓練及建置實務 … 等課程，例：資訊安全管理系統主導稽核員證照 (BS 7799/ISO 27001 Lead Auditor)、IT 服務管理系統主導稽核員證照 (ISO 20000 Lead Auditor)、營運持續管理系統主導稽核員證照 (ISO 22301 Lead Auditor)… 等，並配合政府各階段 ISMS 的推動計畫，承辦國家資通安全標準的翻譯專案，且已**成為證券期貨局、銀行局銀行業、銀行局票券商、投信投顧公會及保險局認可之內部稽核人員專業訓練機構暨公務人員終身學習訓練機構。**

協會簡介

願 景

願景：持續為資訊科技治理與電腦稽核之先導機構。

宗 旨

一、推動電腦稽核及系統控制安全之學術研究發展。
二、協助制訂電腦稽核、控制、安全之標準。
三、協助企業強化電腦系統之控制與電腦稽核功能。
四、與國際電腦稽核相關組織作資訊及技術之交流。
五、協助保護個人資料等事項。

任 務

一、舉辦有關電腦稽核、控制、安全之研討會、講習會。
二、舉辦企業及機關團體之教育講習，以推廣有關電腦稽核控制，安全之實施。
三、出版電腦稽核、控制、安全之刊物及著譯叢書。
四、聯繫企業、學術界及政府機構，以促進電腦稽核理論與實務之交流。
五、接受企業、政府機構委託協助建立電腦稽核功能與電腦安全及控制制度或辦理電腦稽核之研究。
六、舉辦對電腦稽核有貢獻之表揚事項。
七、接受政府相關機關之委託舉辦電腦稽核人員資格檢定。

八、聯繫國際電腦稽核組織、進行合作。

九、辦理其他為達成本會宗旨之必要事項。

沿 革

- 1994 年 7 月 14 日正式創立，由朱寶奎擔任第一屆理事長。秘書長由林秀玉會計師擔任。
- 1996 年 7 月由朱寶奎續任第二屆理事長。秘書長由林秀玉續任。
- 1998 年 7 月由魏忠華接任第三屆理事長。秘書長由陳瑞祥擔任。
- 2000 年 8 月由魏忠華續任第四屆理事長。秘書長由黃涼澤擔任。
- 2002 年 9 月由蔡蜂霖接任第五屆理事長。秘書長由莊盛祺擔任。
- 2004 年 9 月由吳琮璠接任第六屆理事長。秘書長由吳素環擔任。
- 2006 年 9 月由吳琮璠續任第七屆理事長。秘書長由許林舜擔任。
- 2008 年 9 月由黃明達接任第八屆理事長。副理事長由林宜隆擔任。秘書長由徐敏玲擔任。
- 2010 年 8 月由黃明達續任第九屆理事長。副理事長由林宜隆續任並暫代秘書長。
- 2012 年 8 月由林宜隆接任第十屆理事長。副理事長由楊期荔擔任。秘書長由黃涼澤擔任。
- 2014 年 8 月由林宜隆續任第十一屆理事長。副理事長由楊期荔續任。秘書長由黃涼澤續任。
- 2016 年 8 月由張紹斌接任第十二屆理事長。副理事長由蘇庭興擔任。秘書長由黃涼澤續任。

會員權益

一、可免費參加本協會定期舉辦之例會活動（含台北、新竹、南區），並獲得 CISA、CISM、CRISC 及 CGEIT 持續進修（CPE）學分。

二、參加 CISA、CISM 國際證照考試複習課程及本協會舉辦之課程可享有會員折扣價。

三、會員得以優惠價格購買協會出版品。

四、可免費獲得協會出版之《電腦稽核期刊》（一年兩期）。

五、透過電子郵件方式，可取得電腦稽核相關領域之最新訊息。

六、輔導會員取得國際電腦稽核師（CISA）、國際資訊安全經理人（CISM）、國際資訊風險控制師認證（CRISC）及國際企業資訊治理師（CGEIT）證照並提供會員專業認證管道。

七、參加協會各種活動、擔任協會委員會委員及出席會員大會等，並享有發言權、表決權、選舉權、被選舉權；團體會員得由五位代表人出席本協會會議並行使權利義務。

八、可進入協會會員專屬網站瀏覽各期刊物及下載各類電子文檔，如歷年期刊文章、ISACA 摘譯期刊、例會講義、職業道德規範、及提供各項查核指引等資料。

會員義務

- 本協會會員有繳納會費及遵守本會章程與決議事項之義務。

February-May 2018 Certification Exam Passers

ISACA Taiwan Chapter

	Exam Type	ID No.	Name	Top 3
1	CISA	613300	Ching Lee	
2	CISA	818173	Han Yu	
3	CISA	996022	Chia-Wen Yang	No.3
4	CISA	1052272	Lu-Chou Huang	No.2
5	CISA	1101224	Jia-Mian Wang	No.1
6	CISA	1113151	Hsuan-Yi Chen	
7	CISA	1131305	Yu-Kai Lin	
1	CISM	704606	Yu-Hao Chang	No.2
2	CISM	1049270	Yao-Hsun Chen	No.3
3	CISM	1112885	Cheng-Hao Chan	No.1
1	CRISC	348259	Chih-Sheng Lin	No.3
2	CRISC	704606	Yu-Hao Chang	No.2
3	CRISC	1101224	Jia-Mian Wang	No.1

※ 以上資料來源： ISACA總會201807更新。

2018 下半年度教育訓練課程列表

電腦稽核協會(CAA)為證期局、銀行局金控公司及銀行業、銀行局信用卡業務機構、銀行局電子支付機構、保險局保險業、保險局保險代理人/經紀人、投信投顧公會認可之內稽人員訓練機構及公務人員終身學習訓練機構

課程類別	課程主題	時數	預定開課時間	課程費用
ISACA 國際證照系列	CISA 國際電腦稽核師認證研習班_假日班	30	**9/1、8、15、29、10/6**	NT$ 30,000
	CISA 國際電腦稽核師認證研習班_平日班	30	**10/11-12、17-19**	NT$ 30,000
	CISM 國際資訊安全經理人認證研習班_假日班	18	**10/13、20、27**	NT$ 18,000
ISO 系列	ISO 27001:2013 資訊安全管理系統 主導稽核員 IRCA 國際登錄訓練課程	40	**9/3-7、11/19-23、12/3-7 假日班：10/4-6, 12-13 高雄班： 12/3-7**	NT$ 53,000
	ISO 27001:2013 資訊安全管理系統 內部稽核員訓練課程	16	**9/10-11**	NT$ 21,000
	ISO 27001:2013 資訊安全管理系統 建置實務課程	24	**9/17-19**	NT$ 36,000
	ISO 22301:2012 營運持續管理系統 主導稽核員 IRCA 國際登錄訓練課程	40	**9/10-14、11/12-16**	NT$ 55,000
	ISO 22301:2012 營運持續管理系統 基礎課程	16	**12/6-7**	NT$ 21,000
	ISO 20000-1:2011 IT 服務管理系統 主導稽核員 IRCA 國際登錄訓練課程	40	**12/24-28**	NT$ 55,000
	ISO 29100:2011(CNS 29100)隱私框架 主導稽核員訓練課程	36	**10/22-26、12/10-14**	NT$ 55,000
	ISO 29100:2011(CNS 29100)隱私框架 國際標準基礎課程	8	**10/19**	NT$ 8,000
	BS 10012:2009 個人資訊管理系統 國際標準建置課程	16	**10/15-16、12/3-4**	NT$ 15,000
	BS 10012:2009 個人資訊管理系統 國際標準基礎課程	8	**9/7**	NT$ 8,000
內稽系列	內部稽核實務作法**(初任課程)**	12	**11/7-8**	NT$ 6,600
	以電腦關鍵控制點查核舞弊實務案例	7	**8/23**	NT$ 3,850
	電腦稽核新法規一例一休特休加班輪班 Excel 實務試算演練	7	**8/27**	NT$ 3,850
	以電腦控制關鍵點查核銷售採購舞弊實作班	7	**9/17**	NT$ 3,850
	NEW!應用簡報視覺化技巧呈現經營分析與稽核報	7	**9/19、11/22**	NT$ 3,850
	透視樞紐分析查核銷售作業並提升呆帳預警能力	7	**9/20**	NT$ 3,850
	Excel 對稽核業務銷售應收帳款管理報表實務操作解析	7	**10/22**	NT$ 3,850
	個資法導入與查核企業內稽內控循環作業管理規範	7	**11/21**	NT$ 3,850
	自行評估問卷設計標準範本_內控法規 COSO 五大組成要素	7	**11/26**	NT$ 3,850
	內部稽核協助企業轉型升級實務作法★	6	**8/2**	NT$ 3,300
	內控 2.0：統計預測、大數據分析、物聯網、資安與舞弊偵防★	6	**9/11**	NT$ 3,300
	內部稽核有效協助企業 Q4 主要工作★	6	**12/6**	NT$ 3,300

中華民國電腦稽核協會 電話：(02)2528-8875 傳真：(02) 2528-8876 網站：www.caa.org.tw

課程類別	課程主題	時數	預定開課時間	課程費用
IT Audit與資訊治理系列治理系列	*NEW!*💻從 Big Data 偵測資料以預警防弊與興利_存貨固資查核作業	15	**8/28-29**	NT$ 7,500
	NEW!💻從 Big Data 偵測資料以預警防弊與興利_六大循環舞弊查核	15	**9/26-27**	NT$ 7,500
	NEW!💻從 Big Data 偵測資料以預警防弊與興利_企業特定圖表製作	15	**10/24-25**	NT$ 7,500
	NEW!💻從 Big Data 偵測資料以預警防弊與興利_企業採購查核作業	15	**10/29-30**	NT$ 7,500
	NEW!💻從 Big Data 偵測資料以預警防弊與興利_資處與經析(初級上)	15	**11/28-29**	NT$ 7,500
	NEW!💻從 Big Data 偵測資料以預警防弊與興利_企業銷售查核作業	15	**12/12-13**	NT$ 7,500
	NEW!💻從 Big Data 偵測資料以預警防弊與興利_企業樞紐分析應用	15	**12/17-18**	NT$ 7,500
	NEW!💻從 Big Data 偵測資料以預警防弊與興利_企業函數應用操作	15	**12/19-20**	NT$ 7,500
	NEW!💻從 Big Data 之關聯式資料以查核 Power BI_透視視覺化圖表分析	7	**8/22、11/20**	NT$ 3,850
	NEW!💻從 Big Data 之樞紐分析以查核 Power BI_擅用五大軟體繪製圖表	7	**10/23**	NT$ 3,850
	💻Excel 結合大數據分析(Ⅱ)：Power BI 視覺化分析與風險評估	6	**8/9**	NT$ 3,300
	NEW!💻稽核分析在採購付款循環稽核個案演練	6	**8/10**	NT$ 3,300
	ERP 系統應用控制與稽核分析實務★	6	**9/7**	NT$ 3,300
	數位時代電腦稽核起手式**(初任課程)**★	6	**9/10**	NT$ 3,300
	資安趨勢與企業因應管理(新竹班)★	6	**9/11**	NT$ 3,300
	新時代稽核變革及實務案例分享★	6	**9/28**	NT$ 3,300
	NEW!💻稽核分析在金融業以風險為導向內部稽核個案演練	6	**10/2**	NT$ 3,300
	作業系統與通信傳輸查核★	6	**10/4**	NT$ 3,300
	以數據分析解析營運流程與財務舞弊偵測★	6	**10/5**	NT$ 3,300
	💻採購及銷售循環數據稽核－高風險交易資料分析(新竹班)	6	**10/29**	NT$ 3,300
	ERP 系統控管與查核實務★	6	**10/31**	NT$ 3,300
	鼎新 Workflow ERP 系統控管與查核實務	6	**11/1**	NT$ 3,300
	*NEW!*談資安事件應變機制及稽核重點★	6	**11/5**	NT$ 3,300
	資訊時代稽核專業職能與倫理規範★	6	**11/12**	NT$ 3,300
	網路與系統安全實務查核★	6	**11/14**	NT$ 3,300
	資訊部門稽核與資訊系統控制查核★	6	**11/16**	NT$ 3,300
	金融 3.0 的創新應用與風險管理★	6	**12/5**	NT$ 3,300
	有效成本管控設計與分析★	6	**12/7**	NT$ 3,300
	內部稽核於資訊系統採購及委外之查核實務★	6	**12/14**	NT$ 3,300
個資外洩與保護系列	歐盟 GDPR 合規與個人資料保護(新竹班)★	6	**9/18**	NT$ 3,300
	*NEW!*如何建構個資管理機制★	6	**8/14**	NT$ 3,300
	資料庫稽核與個資保護★	6	**10/26**	NT$ 3,300
	個人資料保護稽核★	6	**12/21**	NT$ 3,300

中華民國電腦稽核協會　電話：(02)2528-8875　傳真：(02) 2528-8876　網站：www.caa.org.tw

課程類別	課程主題	時數	預定開課時間	課程費用
ISACA 專業系列	以提昇企業價值為核心之企業資訊治理架構 COBIT 5 理論與實務介紹★	6	**8/1**	NT$ 3,300
	網站安全與稽核簡介(Ⅰ)★	6	**8/20、11/15**	NT$ 3,300
	網站安全與稽核簡介(Ⅱ)★	6	**11/23**	NT$ 3,300
舞弊稽核與數位鑑識系列	企業舞弊各類案型與法律議題探討★	6	**8/16**	NT$ 3,300
	從實際法院判決掌握數位證據攻防之重點★	6	**8/21**	NT$ 3,300
	新興科技環境的數位鑑識挑戰與因應★	6	**9/6**	NT$ 3,300
	資安事件與資料外洩調查實務分享★	6	**9/14**	NT$ 3,300
	資安持續稽核與監控：組態安全管理之應用★	6	**9/21**	NT$ 3,300
	進階舞弊資料分析技巧	6	**10/9**	NT$ 3,300
	NEW!以舞弊稽核角度認識數位鑑識實務★	6	**11/2**	NT$ 3,300
	NEW!結合系統資料與網路資源透析潛在舞弊事件	6	**11/9**	NT$ 3,300
	全面舞弊風險管理－從預防、偵測、調查到危機處理★	6	**11/27**	NT$ 3,300
	應用鑑識資料分析(FDA)技術查核財務舞弊★	6	**11/30**	NT$ 3,300
	利用資料分析技術透視潛在舞弊事件★	6	**12/11**	NT$ 3,300
	數位證據與實例分享★	6	**12/24**	NT$ 3,300
數位金融與電子支付系列	PCI DSS 資料安全標準與電腦稽核實務★	6	**8/3**	NT$ 3,300
	以 PCI DSS 強化電子支付服務的資訊安全管理及法規遵循★	8	**9/3、12/10**	NT$ 8,000

※ **本會保有課程安排及師資調整異動之權利，實際課程請依本會網站公告為準**。

※ 本會會員課程費用另有優惠。

※ 「💻」為上機操作課程，學員需自備有 USB 孔的筆電。

※ 「★」為上市上櫃公司董事、監察人進修課程。

※ 可申報進修時數：實際可申報時數請依本會網站公告為準

- ■ 公開發行公司內部稽核人員訓練時數
- ■ 證券期貨局內部稽核人員初任職前訓練時數
- ■ 證券期貨局內部稽核人員在職或替代訓練時數
- ■ 銀行局金融控股公司及銀行業內部控制及稽核人員在職訓練時數
- ■ 銀行局信用卡業務內部稽核人員在職訓練時數
- ■ 銀行局電子支付機構內部稽核人員相關專業在職訓練時數
- ■ 保險局保險業內部稽核人員在職訓練時數
- ■ 保險局保險代理人及保險經紀人內部稽核人員在職訓練時數
- ■ 投信投顧公會內稽訓練時數
- ■ 公務人員終身學習時數(限 ISACA 證照及 ISO 課程)
- ■ CISA、CISM、CGEIT、CRISC、CIA 學習時數
- ■ 上市上櫃公司董事、監察人進修時數

※ 歡迎企業包班，為您量身訂做所需課程。

※ 詳細課程規劃請上本會網站 www.caa.org.tw 查詢，或來電(02)2528-8875 洽詢。

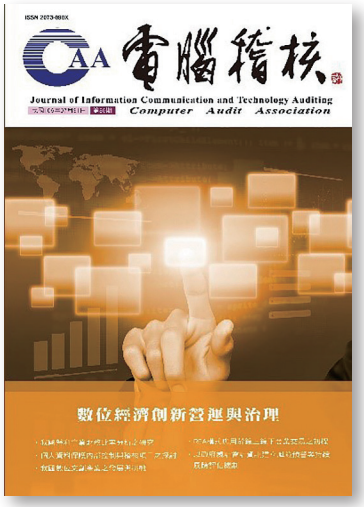
中華民國電腦稽核協會　電話：(02)2528-8875　傳真：(02) 2528-8876　網站：www.caa.org.tw

電腦稽核期刊前期篇名整理

第三十七期_金融科技環境下資安治理與人工智慧應用

- 以大學生角度探討影響第三方支付採用意圖的因素
- LINE 通訊軟體結合 Chatbot 改善設備連線測試效率與品質
- 我國電子化政府之發展與挑戰
- 結合自助式商業智慧技術之敏捷資料分析方法—以公部門為例
- 金融科技環境下銀行業風險管理因子與資訊治理稽核要項之探究
- 觀察「數據型態」進以提升營運效率

第三十六期_數位經濟創新營運與治理



- 我國營利事業財務比率分析之研究
- 個人資料保護內部控制與稽核項目之探討
- 我國數位文創產業之發展與挑戰
- REA 模式應用於線上線下商業交易之初探
- 以政府歲計會計資訊建立風險預警與持續風險評估機制

訂購詳見電腦稽核協會網站http://www.caa.org.tw/publish.asp

ISACA摘譯期刊近期篇名整理

第19期　　2017年12月出刊

- 敏捷專案風險管理
  Risk Management In Agile Projects
- 董事會如何實現資訊治理之透明性
  How Boards Realise IT Governance Transparency
- 將行動支付視為一個安全控制？
  Mobile Payments as a Security Control?
- 雲端風險管理
  Managing Cloud Risk
- 如何針對人為因素進行查核以及如何估量組織的安全風險
  How to Audit the Human Element and Assess Your Organization's Security Risk
- 資通訊保險（Cybersecurity）：是創造價值還是成本負擔？
  Cyberinsurance：Value Generator or Cost Burden?

第20期　　2017年06月出刊

- 二十一世紀中葉之資訊倫理
  Information Ethics in the Mid- 21st Century
- IT 查核人員所需的進階資料 (或數據) 分析
  Advanced Data Analytics for IT Auditors
- 以機器學習方法進行遠端醫療治理
  A Machine Learning Approach for Telemedicine Governance
- 使用開源工具協助科技治理
  Using Open Source Tools to Support Technology Governance
- 你需要災難復原計劃嗎 ・・・ ？
  Do You Need a Disaster Recovery Plan…?
- 如何將分析轉換為內部稽核
  How Analytics Will Transform Internal Audit

近期活動報導

2018.01.25

協辦「當法律遇見科技—以實務觀點探討 leagal tech 與鑑識」研討會

科技蓬勃發展的現今，各行各業持續引入最新科技達到事半功倍的效果。資料數位化讓資訊的保存與使用更加有效便利，用於法律相關事務上，則能改善過去仰賴大量人力、時間處理紙本資料的缺點，加上數位證據的數量及重要性與日俱增，法律人必然要有能力解讀與應用。

本次研討會邀請電腦稽核協會張紹斌理事長以「突破數位落差迷霧：數位鑑識與訴訟實務分享」為主題，介紹何為數位證據，以及企業對於鑑識應有的認知，並以標準線上及線下蒐證案例，和證據遭汙染的實際案例示範、解說數位鑑識的應用。同時也邀請勤業眾信風險諮詢股份有限公司曾韵副總經理分享「法律進化國際新潮流：LegalTech 業界實務運用」，東吳大學會計系李坤璋系主任分享「法律人的跨界利器：鑑識會計案例分享」，台灣高等法院檢察署許永欽主任檢察官擔任與談貴賓一同參與綜合座談，分享在訴訟中較常運用的數位鑑識及鑑識會計等技術。

◆「當法律遇見科技—以實務觀點探討 leagal tech 與鑑識」研討會 - 左起：勤業眾信風險諮詢股份有限公司曾韵執行副總經理、東吳大學會計系李坤璋主任、富邦金控股份有限公司李相臣資訊長、立法委員許毓仁、台灣高等法院檢察署許永欽檢察官、中華民國電腦稽核協會張紹斌理事長、勤業眾信風險諮詢股份有限公司萬幼筠總經理。

1 月新竹例會

2018.01.26

【 風險視覺化分析與稽核應用實例 】

科技的發展帶動網路資訊的進步，每時每刻都有大量的數據資料等待專業人員進行分析處理，以獲得最新資訊並洞察出其中的風險問題。而視覺化分析則是指使用者透過圖表、圖形或其他視覺化編排方式，快速、直觀地分析問題，理解大量數據資料並洞察複雜的問題。

本次例會活動邀請國立雲林科技大學會計系孫嘉明副教授以風險視覺化分析為主題，介紹什麼是視覺化分析、圖表設計、儀表板設計，以及風險管理的挑戰與風險評估的特質，並結合應用於稽核的實際案例，帶領學員了解風險視覺化分析的使用方法，以應用於實務工作中。

◆ 1 月新竹例會 - 國立雲林科技大學會計系孫嘉明副教授

2018.02.07

2 月台北例會

【 企業資安聯防—事件通報與情資分享 】

隨著科技發展，現今的生活已與網路密不可分，企業大量仰賴網路快速傳遞各類重要資訊，其背後潛伏著資訊安全的問題亦受到重視。政府因應資安風險評估，強調以「 早期預警、持續監控、通報應變，以及協助改善 」四個面相著手，落實資安防護。其中「 通報應變 」可透過台灣電腦網路危機處理暨協調中心（ TWCERT/CC ）與全球資安聯防體系搭上線，即時處理緊急資安事件，提供技術諮詢、處置建議與協助。

此次例會活動邀請台灣電腦網路危機處理暨協調中心吳專吉副主任以企業資安危機通報站— TWCERT/CC、企業通報應變機制之建立、事件應變作業與威脅分析實務三大主題進行分享，介紹 TWCERT/CC 的歷史、業務與發展現況，國內外情資通報流程與管道、近幾年國內情資通報狀況與分析、常見通報案例分享，並介紹民間企業組織 CSIRT 的建置與資安事件通報處理流程，最後分享資安威脅與防護方式，並以實際案例與實作情境題演練資安通報流程。

◆ 2 月台北例會 - 台灣電腦網路危機處理暨協調中心吳專吉副主任

2018.03.23

第 12 屆第六次理監事會議

106 年財務報表決算審查及討論各委員會工作事項。

◆ 第 12 屆第六次理監事會議

3 月新竹例會

2018.03.27

【GDPR 的衝擊與因應策略】

GDPR 歐盟一般資料保護規章正式於今年 5 月 25 日正式實施，其所保護之個人隱私資料範圍不單只局限於歐盟，凡活動內容包含歐盟的資料當事人，都屬於 GDPR 涵蓋對象，且其嚴格規定若發生資料外洩事件，必須於知悉後 72 小時內通報其監督機構，若違反規章，資料監管單位可開罰全球營業額的 2- 4% 作為罰款。全台受 GDPR 所規範的大小企業眾多，企業除須徹底了解 GDPR，更應做好相應的措施，避免受罰。

此次月例會邀請勤業眾信聯合會計師事務所風險諮詢服務陳鴻棋協理，以 GDPR 的衝擊與因應策略為主題，分享 GDPR 的重點剖析、其所面臨的遵循難題以及遵循的實施策略，並比較 GDPR 與我國個資法的差異，全方位的帶領大家了解 GDPR 各項規範，期望企業在資料保護上更為重視並做好萬全的準備。

◆ 3 月新竹例會 - 勤業眾信聯合會計師事務所風險諮詢服務陳鴻棋協理

3 月台北例會

2018.03.30

【 網路安全治理與資訊韌性 (CSIR) 國際標準發展 】

網路科技普及的時代，讓全球產業運作更加便利、快速，但相應而生的是其所面臨的風險與挑戰。對於金融保險業、服務業、資訊與通訊、製造業，亦或是公共行政與國防、能源和公共事業來說，常見的威脅像是網路攻擊、資料外洩，或是無預警的 ICT 中斷。而隨科技的演進，攻擊工具更加容易獲取、多樣化，利用互聯網進行惡意攻擊的趨勢更是屢見不顯，各行各業也將面臨各自未來可能的攻擊或風險趨勢。

◆ 3 月台北例會 - BSI 英國標準協會台灣分公司驗證部謝君豪協理

此次月例會邀請 BSI 英國標準協會台灣分公司驗證部謝君豪協理，以「 網路安全治理與資訊韌性 (CSIR) 國際標準發展 」為主題，分享組織推動資安時常面臨到的挑戰與困境，以及如何強化組織的網路安全治理及資訊韌性、提升組織既有的 ISMS 管理制度成熟度，並解說如何整合國際標準指引以提升關鍵威脅控管的有效性。

2018.04.30

4 月台北例會

【 由歐盟新法 (GDPR) 談數據變現與隱私保護的平衡 】

2018 年已是大數據時代，各產業利用低成本低污染高報酬的數據創造各種價值，「 數據變現 」便是應用不同屬性的數據到各類場景中以體現新價值的過程。而今年 5 月 25 日起歐盟新法 GDPR 歐盟一般資料保護規章正式上路，對收集、應用各類個人隱私相關數據的產業進行規範，在應用數據變現的同時，又該如何兩者兼顧呢？

◆ 4 月台北例會 - 美商安客誠公司亞太區首席數據治理官暨公共政策負責人潘兆娟博士

此次月例會邀請美商安客誠公司亞太區首席數據治理官暨公共政策負責人潘兆娟博士，以由歐盟新法 (GDPR) 談數據變現與隱私保護的平衡為主題，分享 GDPR 與最新國際趨勢，探討 GDPR 所帶來的關鍵影響與各國法規之差異，並以數據變現為出發點，帶領學員探討如何在數據變現的同時兼顧數據保護與合理化的使用方式。

2018.05.04

全國大專院校電腦稽核個案競賽暨專題研討會

為提供實務界與學術界之溝通平台，以建構國內企業發展電腦稽核技術，以及持續性稽核與監控的藍圖，並分享企業營運全球化與資訊科技發展的趨勢，本會特與台北商業大學協辦此次電腦稽和個案競賽活動，並以「大 (Big data) 人 (AI) 機 (Robot) 時代 E-Assurance 的因應對策 」為研討會主題，與實務界人士進行交流。

◆ 全國大專院校電腦稽核個案競賽暨專題研討會

5 月南區例會

2018.05.11

【大數據時代下的資訊安全巨變—對資訊安全控制與稽核之影響】

大數據時代下，各產業分析、應用巨量資料並找出對企業有益的資訊，進而帶來無限的商機。相應而生的是儲存資料的空間是否安全、資料隱私、資料管理、終端管理與監控等議題，如何建構穩健運作的資訊安全控制環境變得及其迫切需要。

此次例會首次在逢甲大學舉行，邀請資誠聯合會計師事務所風險與控制服務部王彥凱經理，以「大數據時代下的資訊安全巨變—對資訊安全控制與稽核之影響 」為主題，從大 據時代的資訊安全衝擊開始講起，分享如何建構穩健運作的資訊安全控制環境，進而談論到變動環境下的資訊安全稽核工作，期待稽核人員持續充實進修，為企業提供更有效的資安稽核手法以改善資安維運問題。

◆ 5 月南區例會 - 資誠連合會計師事務所風險與控制服務部王彥凱經理

5 月台北例會

2018.05.15

【 提昇組織對風險的洞察能力：運用監理科技 (RegTech) 與鑑識 】研討會暨第 10 屆會員代表選舉

此次活動以「 提昇組織對風險的洞察能力：運用監理科技 (RegTech) 與鑑識 」為主題，特別邀請中華民國金融監督管理委員會鄭貞茂副主任委員擔任致詞貴賓，本會理事長張紹斌先生主持研討會，以專題演講及綜合座談會為主軸，邀請各專家代表進行分享交流。

專題演講邀請財政部財政資訊中心陳泉錫主任以「 公務機關推動資安健檢與數位鑑識之經驗分享—以財政資訊中心為例 」為主題，分享現今資安風險與挑戰、財政資訊中心的資安防護策略以及未來挑戰。同時也邀請台灣舞弊防治與鑑識協會許順雄理事長以「 RegTech 在舞弊防治與財務鑑識之運用 」為主題，以各類實際案例分享 RegTech 的應用。

綜合座談會以「 站在監理科技 (RegTech) 的浪尖，洞見風險、掌握契機 」為主題，邀請金管會資訊服務處蔡福隆處長分享監理科技之發展、安永聯合會計師事務所朱家德會計師分享由數據分析偵防員工舞弊、安侯企業管理顧問公司謝昀澤執行副總經理分享大數據 - 人工智慧 - 機器人的風險控制實務，以及勤業眾信風險管理諮詢公司劉曉軒協理分享運用人工智慧提升法遵人員戰力。

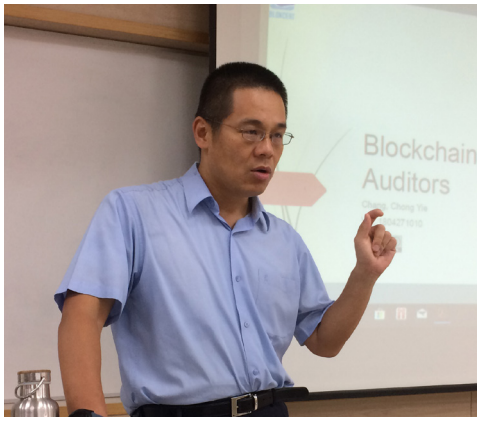
◆ 5 月台北例會 - 左起台灣舞弊防治與鑑識協會許順雄理事長、行政院主計總處主計資訊處潘城武處長、電腦稽核協會蘇庭興副理事長、金融監督管理委員會鄭貞茂副主委、電腦稽核協會張紹斌理事長及財政部財政資訊中心陳泉錫主任

2018.05.25

5 月新竹例會

【區塊鏈概念簡介、應用案例探討與稽核需求】

何為區塊鏈？區塊鏈的第一個應用便是比特幣。區塊鏈破除以往必須透過中介機構做謀合，保存所有交易紀錄，才可讓全球金融體系得以運轉，區塊鏈的去中心化，讓所有提供電腦硬體運算能力的礦工共同將交易資料上鏈，使得交易資料可以追蹤、加密且不得竄改，使交易無需透過中介機構，更加便利及安全。



◆ 5 月新竹例會 - 區塊證科技股份有限公司創辦人張中一先生

此次例會邀請區塊證科技股份有限公司創辦人張中一先生，以區塊鏈概念簡介、應用案例探討與稽核需求為主題，介紹什麼是區塊鏈，並以現有應用進行案例討論，連結到區塊鏈中的稽核需求，期待加入稽核的理念更加完善區塊鏈的應用。

2018.06.11

6 月南區例會

【人工智慧－內部稽核的未來】專題演講暨第 10 屆會代選舉（南區）

人工智慧 (AI) 現已進入日常生活中，近年來伴隨著深度學習，許多重複性高的工作被 AI 所取代，無論是處理複雜計算、客戶服務常見問題，甚至是影像處理與分析皆能藉由 AI 輔助或獨自完成。此次第 10 屆南區會員代表選舉結合 6 月例會於國立中正大學舉行，邀請勤業眾信聯合會計師事務所企業風險管理高智敏經理擔任講師，以「人工智慧－內部稽核的未來」為主題，分享介紹人工智慧的源起與演進，以及 AI 在各產業實務上的應用，並講述人工智慧除了帶給產業的各種機會與相應產生的風險，在這此同時，內部稽核應如何發揮其功效，降低或 AI 風險，並利用 AI 增強內部稽核效率與效果，建立更加安全的機制與環境。

◆ 6 月南區例會 - 勤業眾信聯合會計師事務所企業風險管理高智敏經理

6 月台北例會

2018.06.28

【 資通安全管理法子法說明與應用 】研討會

今年五月初，立法院三讀通過資通安全管理法；緊接著五月底，歐盟的 GDPR 正式上路實施，這是國內外資通安全產業與政府皆已關注許久的兩件大事。在資通安全管理法方面，雖然在實施初期，僅有政府機構與關鍵基礎設施服務提供者適用，但長期方向仍需民間企業配合推動，相關子法與實施細則的內容深具指標示範作用。再者，GDPR 的出發點雖以歐盟為主，但現今網路世代與資通信之快速，我國對於個資保護規範與運用，亦應在資安管理基礎上嚴陣以待。未來落實個資保護機制勢必與資訊安全會有高度連結，故希望藉由本次研討會的安排，讓大家能進一步深入了解兩者之互動關 。

此次例會活動與東吳大學法學院、東吳大學電算中心、台灣科技產業法務經理人協會協辦，於東吳大學城中校區舉行，由東吳大學法學院余啟民教授主持，邀請達文西高科技法務事務所葉奇鑫主持律師以「 資料在地化法制與 GDPR 跨境傳輸之趨勢與限制 」為主題，共同探討台灣企業面對 GDPR 的因應之道。同時也邀請行政院資通安全處簡宏偉處長、張小梅科長以「 資通安全管理法及子法適用說明 」為主題，詳細解說資通安全法的各項規定，為與會貴賓解答企業的因應策略。

◆ 6 月台北例會左起 - 東吳大學法學院余啟民教授、達文西高科技法律事務所葉奇鑫主持律師、行政院資通安全處簡宏偉處長及張小梅科長

ISACA®

Trust in, and value from, information systems

證明您的能力足夠帶領企業面臨新時代的挑戰

資訊化是21世紀重要的時代特性，大量的資訊與相對應的技術支援，雖將能促進企業的成功，但在此環境下，卻同時也增加了許多原本沒有而複雜且具有挑戰性的新管理議題。

ISACA®國際電腦稽核協會是一個屬於世界領先地位的全球性組織，提供資訊專業人士能以卓越的途徑進行個人專業的成長與發展。同樣的，全球資訊專業人士也認為，ISACA對於他們的職業生涯發展與企業價值的提升均提供了實質的幫助。

將 CISA、CISM、CGEIT或CRISC的認證名稱放置在您名字後面，將能證明您的專業能力、經驗與推廣。這可認定您是一位專業的資訊人才，擁有全面性的資訊系統視野，並關係到企業能透過價值傳遞(value delivery)且獲得成功的關鍵因素。

隨著現代企業越來越依賴資訊系統(IS)，對於技術與資訊系統專業人員的需求快速的上升，並且更著重於資訊與治理的能力。企業需要合格的資訊專業人才的實務知識與專長，來幫助確認關鍵性問題與制定具體作法以支持資訊與相關技術的治理作為。ISACA的認證將滿足企業如此的迫切需求。ISACA以全球公認的認證讓企業能識別具備豐富經驗與知

在國際的獨立研究報告中指出，ISACA名稱代表著：

- 高階資訊專業人士的薪資報酬
- 可信賴的專業能力與認可
- 招募程序中的高點選率與優先面試

如何取得更多的資訊

訪問ISACA認證網站：**www.isaca.org/certification-success**
ISACA認證部門：**certification@isaca.org**

CISA® Certified Information Systems Auditor®
An ISACA® Certification
國際電腦稽核師

CISM® Certified Information Security Manager®
An ISACA® Certification
國際資訊安全經理人

CGEIT® Certified in the Governance of Enterprise IT®
An ISACA® Certification
國際企業資訊治理師

CRISC® Certified in Risk and Information Systems Control™
An ISACA® Certification
國際資訊風險控制師

國際電腦稽核師(CISA)在稽核領域
如同註冊會計師(CPA)與公認會計師(CA)在會計領域一般

組織越來越依賴複雜的資訊作業來協助內部業務運作與控制措施的執行，企業需要擁有知識與技能的稽核專業人才，幫助企業找出關鍵問題與解決方案，以確認資訊系統的可信賴性與價值。

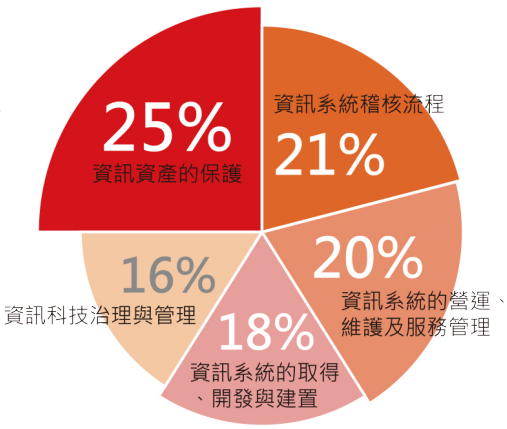
國際電腦稽核師證照(Certified Information Systems Auditor® , CISA®)是毋庸質疑的認證，當您擁有CISA證照，您的專業將立即得到理解與認同，CISA證照將讓您在國內與國際上對於使用標準、確認管理缺失、法規符合性，提供解決方案、發展控制措施以提供企業價值的專業知識、技能、經驗與可信賴的認可。

CISA認證是世界知名對於企業系統的稽核、控制、監控與資訊技術評估的標準。事實上在許多獨立的研究中指出，如資訊安全媒體集團(Information Security Media Group, ISMG)的每年就業趨勢調查，CISA始終是排名資訊證照中最搶手與薪資最高的認證。

歷經38年發展，現今CISA證照已是國際認可標準的具體實現，並且在162個國家有超過100,000位的專業人士獲得此項認證。

右表介紹CISA的專業工作活動項目，並指出每一專業領域的分配率。

CISA 專業領域考試範圍



證實您的資訊安全專業知識–提升競爭優勢

具備資訊安全管理專業人士的需求正呈現逐步上升的趨勢，國際資訊安全經理人(Certified Information Security Manager® , CISM®)是一項在資訊安全管理上全球公認的標準，現代企業必須保護自己免受網路犯罪與越來越多的惡意攻擊等問題，CISM以獨特並專注於資訊安全管理為著重點，提供資訊安全具體的實務做法。不同於其他的安全認證，CISM識別出個別的企業資訊安全管理、開發與佈建階段。

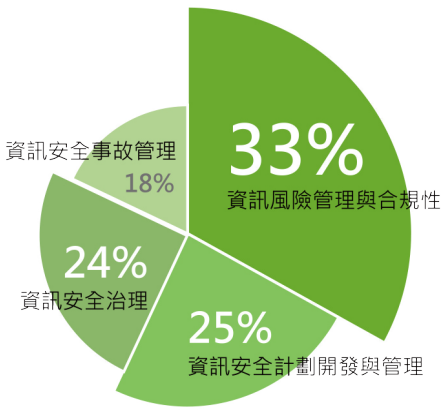
取得CISM的專業人士瞭解企業的需求，他們知道如何去管理和適應他們企業與行業的安全需求。CISM將不僅是具備資訊安全的專業知識，同時也在資訊安全的系統開發與管理上具有可靠的經驗。

CISM 驗證意涵著更高的收入潛力與職業發展。例如在最近的獨立研究2012年Foote Partners的資訊技能與證照報酬指數(IT Skills and Certifications Pay Index™ ,ITSCPI)中指出，CISM持續被列為高報酬與最受歡迎的資訊認證之一。

走過第13個年頭，目前已有超過21,300位專業人士取得CISM證照。

右表介紹CISM的專業工作活動項目，並指出每一專業領域的分配率。

CISM 專業領域考試範圍



展現您良好治理的能力
–對於您的企業與職業發展發揮廣大的影響力

避免發生意外(例如難以處理的資訊數據侵害)，對於企業來說是至關重要的，良好的治理將建立檢查與平衡機制，並對於發生意外事件能進行敏捷的反應。而當企業雇用了CGEIT，將可以確保具有良好的治理能力。

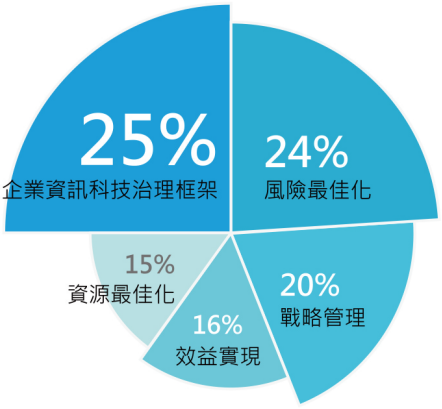
國際企業資訊治理師(Certified in the Governance of Enterprise IT® ,CGEIT®)認可的專業人士具備對於企業資訊治理的原則與實踐有廣泛的知識與經驗。作為一位CGEIT的專業人士，您將證明您具有在一個組織中資訊治理的能力，由整體面掌握複雜的議題，並因此而提升對企業的價值。

CGEIT專業人士具備公認可信賴的資訊治理與策略定位等關鍵議題的知識與實務經驗，其所提供的公信力將使CGEIT的專業人士晉升成為「C-suite」高階經理人。

自2008年以來，已有超過5,000位專業人士取得CGEIT認證。

右表介紹CGEIT的專業工作活動項目，並指出每一專業領域的分配率。

CGEIT 專業領域考試範圍



個人事業與企業組織未來的試煉

對於改善公司治理、營運績效與安全基礎設施的需求不斷的增長，意味著資訊風險管理對於要能適應未來發展的企業是至關重要的。

國際資訊風險控制師(Certified in Risk and Information Systems Control™ , CRISC™)是唯一針對資訊風險管理專業人士未來職業發展的驗證，其定位於有效連結資訊風險管理與企業風險管理，以成為企業戰略合作的夥伴。

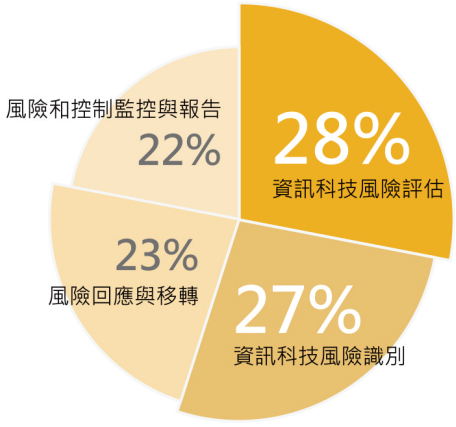
CRISC是最新且經過嚴格評核，具備識別資訊技術風險與評估資訊業務與風險管理的專業人士。CRISC證照將使您在企業內部資訊運作的未來發展上，提供更好的諮詢機會，並且使您在組織中的角色更顯重要；資訊風險將成為企業整體風險重要的組成部分，並使您在組織的資訊風險議題上成為知識型的領導者與內部規則變更的推動者。

2012年Foote Partners的資訊技能與證照報酬指數(IT Skills and Certifications Pay Index™ ,ITSCPI)，CRISC已擠身前10名薪資最高的認證之一。

自2010年以來，已有超過16,000位專業人士取得CRISC認證。

右表介紹CRISC的專業工作活動項目，並指出每一專業領域的分配率。

CRISC 專業領域考試範圍



ISACA

GET CERTIFIED.
GET AHEAD.

www.isaca.org/GetCertified-Jv1

CISA國際電腦稽核師認證研習班
假日班：9/1、9/8、9/15、
9/29、10/6(六) 確定開課
平日班：10/11-12、10/17-19

CISM國際資訊安全經理人認證研習班
假日班：10/13、10/20、10/27 (六)

CISA CRISC CISM CGEIT

日期	期程1 2/1~5/24	期程2 6/1~9/23	期程3 10/1~1/24
開放線上報名	12/1	3/1	7/1
報名截止日期	5/18	9/18	1/18
延期截止日期	5/24	9/23	1/24

※費用：ISACA 會員：US $575、早鳥優惠價US $525
非ISACA會員：US $760、早鳥優惠價US $710

Call for Papers
電腦稽核期刊
全年度徵稿邀約

電腦稽核期刊參與 2017 年「臺灣人文及社會科學期刊評比暨核心期刊收錄」評比，正式（首次）被「臺灣人文及社會科學引索資料庫」登錄為第三級期刊。

本期刊係中華民國電腦稽核協會為推動電腦稽核領域學術及實務發展，半年為一期出版電腦稽核期刊，任何與電腦稽核相關之學術論述或個案研究，未刊登於其他期刊者皆可投稿，敬邀各位會員與相關領域之先進們共襄盛舉，不吝將研究結果、工作上心得或經驗投稿於本期刊，共同支持電腦稽核產業發展。

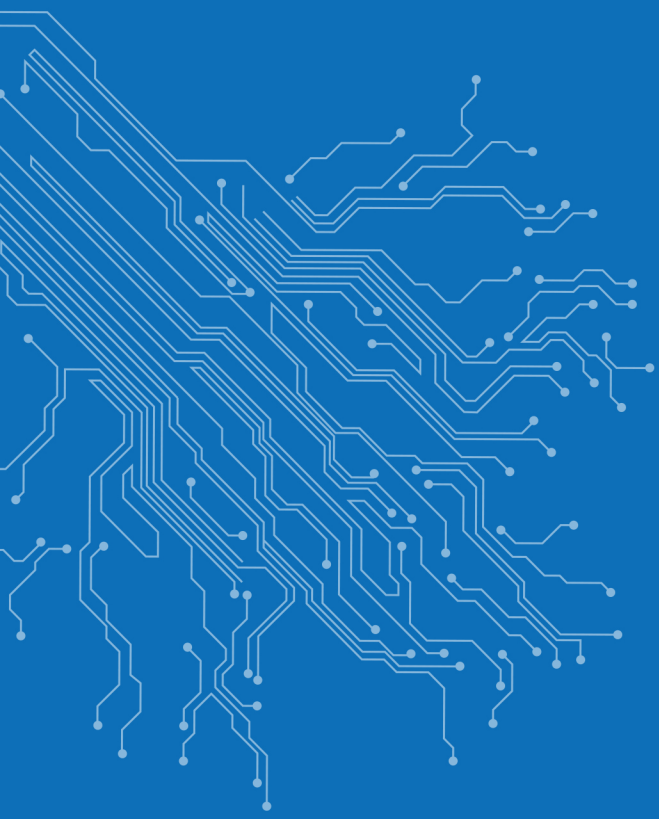
徵稿文章依論文內容分為二大主題：

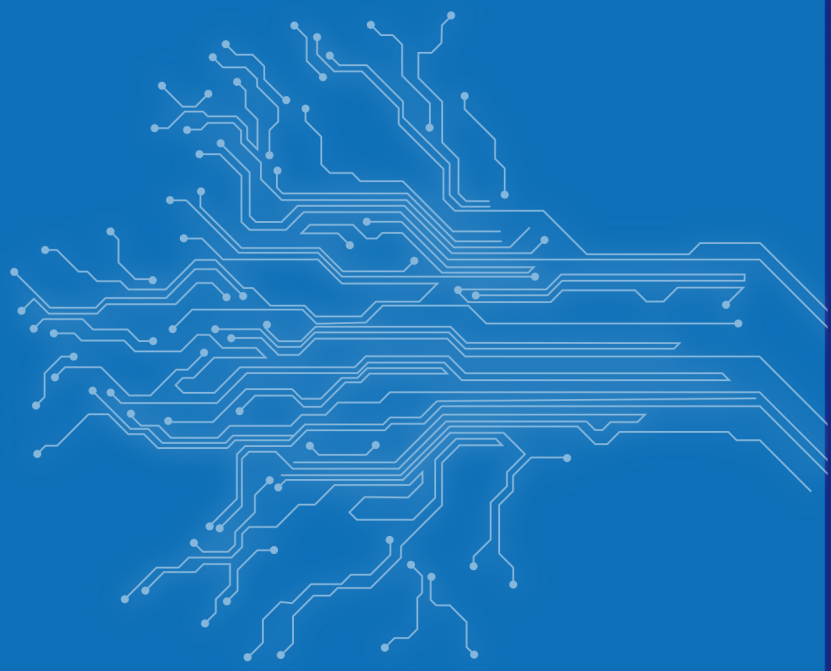
- **專業論壇：**
  強調理論及實務並重，一方面暢談電腦稽核各個面相，另一方面則從實務面檢視電腦稽核在政府部門、私人企業乃至於學術單位的建置與落實情形。

- **新知園地：**
  著重將電腦稽核經驗分享、最新訊息或發展介紹給全體會員及相關大眾知曉。

**** 徵稿簡約 ****

- 投稿文章請以中文或英文撰寫，文稿長度以 10 頁為限，文稿請用 MS Word 處理，表格請另提供一份可編輯檔案，圖片請另附原始檔 (像素 300dpi)。
- 來稿請寄電子檔至 member@caa.org.tw，主旨請標註：「投稿電腦稽核期刊 _ 篇名」，與投稿類別 (專業論壇或新知園地)。
- 投稿文章評審程序依本刊審查之原則辦理。
- 專業論壇包括封面頁，摘要頁，正文，參考文獻及附錄（文稿格式請參閱本會官網最新消息「邀稿通知之附件 - 投稿規範與標準」），並請依順序編入頁碼。作者姓名及相關資訊僅能出現於首頁
- 新知園地請依順序編入頁碼，作者姓名及相關資訊僅能出現於首頁。





CAA 電腦稽核

11070台北市信義區基隆路一段143號2樓之2

2F.-2, No.143, Sec. 1, Keelung Rd., Xinyi Dist., Taipei City 11070, Taiwan (R.O.C.)

886-2-2528-8875 Fax：886-2-2528-8876

www.caa.org.tw Web：www.isaca.org.tw

中華民國電腦稽核協會

第38期期刊

民國107年07月31日發行